THÈSE DE DOCTORAT DE L'UNIVERSITÉ PARIS 6

Spécialité

Mathématiques

Présentée par

M. Wilfrid IVORRA

Pour obtenir le grade de

Docteur de l'Université PARIS 6

Sujet de la thèse :

Équations diophantiennes ternaires de type $(p, p, 2)$ et courbes elliptiques

soutenue le 13 février 2004

devant le jury composé de

M. John CREMONA	Rapporteur
M. Gerhard FREY	Rapporteur
M. Alain KRAUS	Directeur de thèse
M. Jean-François MESTRE	Examinateur
M. Joseph OESTERLÉ	Examinateur
M. Michel WALDSCHMIDT	Examinateur

Remerciements

Mes remerciements vont tout d'abord à mon directeur de thèse, Alain Kraus, qui m'a aidé tout au long de l'élaboration de ce travail. Sa disponibilité, son écoute et ses conseils m'ont été très précieux.

Tous mes remerciements également aux mathématiciens avec lesquels j'ai été en contact pendant la rédaction de cette thèse. En particulier à Yann Bugeaud et Nils Bruin pour les échanges que nous avons eus concernant certains points de ce travail.

Je suis reconnaissant à John Cremona et Gerhard Frey d'avoir accepté d'être rapporteurs de ma thèse. Je remercie par ailleurs Gerhard Frey, Jean-François Mestre, Joseph Oesterlé et Michel Waldschmidt de m'avoir fait l'honneur de participer au Jury de ma soutenance de thèse.

Je souhaite encore remercier l'équipe de théorie des nombres et plus généralement l'ensemble des membres de l'institut de mathématiques de Jussieu qui m'ont accueilli.

Enfin, pour terminer, un petit clin d'œil à ma famille qui m'a soutenu pendant ces quatre années.

À tous merci encore.

Table des matières

Introduction

Dans le cadre de l'étude des équations de Fermat généralisées, la motivation principale de cette thèse concerne le cas particulier des équations diophantiennes ternaires de type $(p, p, 2)$, où p est un nombre premier supérieur ou égal à 5. Il s'agit d'équations de la forme

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

où a, b, c sont des entiers naturels non nuls. On s'intèresse à la détermination de l'ensemble $S_p(a, b, c)$ des solutions propres non triviales de cette équation ; suivant une terminologie parfois utilisée, on dira qu'une solution $(x, y, z) \in \mathbb{Z}^3$ de l'équation (1) est non triviale si xyz est non nul et qu'elle est propre si x, y et z sont premiers entre eux dans leur ensemble. D'après les travaux de H. Darmon et A. Granville, $S_p(a, b, c)$ est un ensemble fini ([Da-Gr]).

Étant donnés trois entiers naturels non nuls a, b, c, premiers entre eux deux à deux, on examinera les problèmes suivants :

Problème 1. Supposons que les trois entiers $a+b$, $a-b$ et $b-a$ n'appartiennent pas à $c\mathbb{Z}^2$. Pour tout nombre premier p assez grand, en fonction de a, b, c, l'ensemble $S_p(a, b, c)$ est-il vide ?

Problème 2. Supposons que l'un des entiers $a + b$, $a - b$ et $b - a$ appartienne à $c\mathbb{Z}^2$. Pour tout nombre premier p assez grand, en fonction de a, b, c, l'implication suivante est-elle vraie :

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

Problème 3. Le nombre premier $p \geqslant 5$ étant fixé, comment déterminer $S_p(a, b, c)$?

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

Afin d'aborder ces problèmes, on emploie principalement deux méthodes. La première est la méthode modulaire qui utilise les travaux de G. Frey, J.-P. Serre, K. Ribet et A. Wiles sur les représentations modulaires, qui ont conduit à la démonstration du théorème de Fermat (cf. [Fr], [Ri], [Se2], [Wi]). En ce qui concerne les problèmes 1 et 2, l'approche modulaire permet de relier la description de $S_p(a, b, c)$ à l'existence d'une courbe elliptique définie sur $\mathbb{Q}$, dont le conducteur ne dépend essentiellement que de a, b, c, et possédant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. C'est la raison pour laquelle on a été amené à examiner le problème suivant :

Problème 4. Étant donné un entier naturel N, comment déterminer les classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ de conducteur N et possédant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$?

Si N est un nombre premier, ce problème a été résolu par B. Setzer en 1975 ([Set]). On généralisera ses travaux au cas où N est le produit d'une puissance de 2 par un nombre premier.

Dans certaines situations, la description de $S_p(a,b,c)$ est par ailleurs liée à la recherche des points rationnels sur $\mathbb{Q}$ de courbes hyperelliptiques de genre $\geqslant 2$. La deuxième méthode que l'on utilisera dans cette direction est la méthode dite de Chabauty elliptique, basée sur les travaux de C. Chabauty ([Ch]), et qui a été développée ces dernières années, du point de vue de l'effectivité, par V. Flynn, N. Bruin, J. Wetherell et S. Duquesne (cf. [Bru1], [Fl], [Fl-We], [Du]).

Cette thèse comporte quatre chapitres. Donnons maintenant un aperçu du contenu de chacun d'eux.

Chapitre I

Ce chapitre est consacré à l'étude de l'équation (1) dans le cas où abc est une puissance de 2. Pour tout nombre premier $p \geqslant 7$ et tout entier β tels que $1 < \beta < p-1$, on détermine les ensembles $S_p(1,2^\beta,1)$ et $S_p(1,1,2)$. En application, on obtient des résultats nouveaux concernant certaines équations diophantiennes. Par exemple, $(78,23,3)$ est le seul triplet d'entiers naturels vérifiant l'égalité $2x^2-1=y^n$ avec $x \geqslant 1$, $y \geqslant 2$ et $n \geqslant 3$. À des modifications mineures près, le contenu de ce chapitre est paru dans la revue Acta Arithmetica ([Iv]). Les résultats qui s'y trouvent ont par ailleurs été obtenus indépendamment par M. Bennett et C. Skinner ([Be-Sk]).

Chapitre II

Dans ce chapitre, on décrit toutes les classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$ et de conducteur de la forme $2^N p$, où p est un nombre premier impair. On a toujours $N \leqslant 8$ (cf. par exemple [Pa]). Au cours de cette description, on a été amené à déterminer les solutions entières de certaines équations diophantiennes ternaires. Signalons que l'on a utilisé pour cela les résultats obtenus dans le chapitre I, ainsi que des résultats concernant des minorations de formes linéaires en deux logarithmes ([Mi]). Les entiers N et p étant donnés, on peut trouver à l'adresse http://www.math.jussieu/~ivorra, un programme fonctionnant sous le logiciel de calculs PARI, donnant la liste effective des classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques comme ci-dessus. Ce chapitre a été soumis pour publication dans la revue Dissertationes Mathematicae en février 2003.

Chapitre III

On s'intéresse dans ce chapitre à l'étude de l'équation (1) dans le cas où le produit des diviseurs premiers de abc divise 2ℓ, où ℓ est un nombre premier impair. En utilisant

les résultats du chapitre II, on résoud de manière effective le problème 1 pour le triplet (a, b, c) si certaines conditions sont satisfaites par ℓ et par l'exposant de 2 dans abc. Par exemple, dans le cas où $\ell \equiv 5$ mod. 8, on démontre que pour tout $m \geqslant 1$, si l'on a

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

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

Pour certains triplets (a, b, c) pour lesquels on ne sait pas traiter le problème 1, on apporte une réponse partielle en prouvant l'existence d'un ensemble $\mathscr{P}$ de nombres premiers, de densité $\delta > 0$, tel que $S_p(a, b, c)$ soit vide pour tout $p \in \mathscr{P}$. Il en est ainsi, par exemple, du triplet $(1, \ell, 1)$ si l'on a $\ell \equiv 7$ mod. 8 et $\ell \neq 7$; si de plus ℓ n'est pas un nombre de Mersenne, on a $\delta \geqslant \frac{1}{4}$. Ce type de résultats peut s'obtenir en utilisant un complément de la méthode modulaire, appelé méthode symplectique dans [Ha-Kr-2]. Dans cette direction, signalons que l'on obtient des informations nouvelles sur une conjecture de J.H.E. Cohn relative à la recherche des couples $(x, z) \in \mathbb{N}^2$ tels que $z^2 + 7 = x^p$ (cf. [Co2], p. 380).

En ce qui concerne le problème 2, on détermine dans ce chapitre les ensembles $S_p(4, 1, 3)$ et $S_p(64, 1, 7)$ en utilisant des propriétés arithmétiques des courbes elliptiques sur $\mathbb{Q}$ à multiplications complexes (cf. [Mom] et [Da-Me]).

Comme conséquence des résultats obtenus, on peut parfois déterminer les points rationnels sur $\mathbb{Q}$ des courbes hyperelliptiques d'équation

$$C_{d,p} : y^2 = x^p + d \qquad \text{où} \quad d \in \mathbb{Z}.$$

Par exemple, si ℓ est un nombre premier congru à 3 modulo 8 et distinct de 3, les ensembles $C_{\ell,p}(\mathbb{Q})$ et $C_{-\ell,p}(\mathbb{Q})$ sont vides si p est assez grand en fonction de ℓ. Un complément de la méthode modulaire, appelé méthode de réduction dans [Ha-Kr-2], permet de démontrer que $C_{-3,p}(\mathbb{Q})$ est vide si l'on a $5 \leqslant p < 10^4$. Ce chapitre a été soumis pour publication, en collaboration avec A. Kraus, au Journal Canadien de Mathématiques en octobre 2003.

Chapitre IV

Ce chapitre concerne le problème 3 dans le cas où $a = b = 1$. On aborde la question suivante qui est un cas particulier d'une question posée dans [Kr6] :

Question. *Soient p un nombre premier $\geqslant 7$ et $\mathfrak{N}_p$ l'ensemble des entiers $c \geqslant 3$ possédant les deux propriétés suivantes :*

(i) c est sans facteurs carrés ;

(ii) pour tout diviseur premier ℓ de c, on a $\ell \not\equiv 1$ mod. p.

Existe-t-il $c \in \mathfrak{N}_p$ tel que $S_p(1, 1, c)$ soit non vide ?

Le nombre premier p étant donné, l'ensemble des entiers $c \in \mathfrak{N}_p$ susceptibles de répondre positivement à cette question est fini. (*loc. cit.*). Par ailleurs, on ne connait

aucun exemple de tel entier c. L'étude de cette question se ramène en fait à celle de la détermination des points rationnels sur $\mathbb{Q}$ des courbes hyperelliptiques $C_p/\mathbb{Q}$ et $D_p/\mathbb{Q}$, de genre $\frac{p-3}{2}$, d'équations

$$C_p \ : \ y^2 = \Phi_p(x) \qquad \text{et} \qquad D_p \ : \ py^2 = \Phi_p(x),$$

où Φ_p est le p-ième polynôme cyclotomique (*loc. cit.*). La méthode de Chabauty elliptique permet parfois cette détermination. On démontre par cette méthode que, dans le cas où $p \in \Big\{7, 11, 13, 17\Big\}$, on a

$$C_p(\mathbb{Q}) = \Big\{(-1,-1), (-1,1), (0,-1), (0,1)\Big\} \quad \text{et} \quad D_p(\mathbb{Q}) = \Big\{(1,-1), (1,1)\Big\}.$$

Pour ces nombres premiers p, cela entraîne qu'il n'existe pas d'entiers $c \in \mathfrak{N}_p$ répondant positivement à la question posée.

Chapitre I

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

Introduction

Soient p un nombre premier $\geqslant 5$ et β un entier tels que $0 \leqslant \beta \leqslant p-1$. On s'intéresse dans ce chapitre 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 x et y deux entiers *relatifs* et z un entier *naturel*. Nous dirons que (x, y, z) est une solution de l'équation (1) si l'on a $x^p + 2^\beta y^p = z^2$, que cette solution est *propre* si l'on a $\mathrm{pgcd}(x, y, z) = 1$ et qu'elle est *non triviale* si xyz est non nul. Nous définissons de même le fait pour (x, y, z) d'être une solution propre non triviale de l'équation (2). On notera dans ce chapitre $S_0(\beta, p)$ 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 $p \geqslant 17$ et $p \equiv 1$ mod. 4 (cf. [Da1]). En 1997, H. Darmon et L. Merel ont ensuite prouvé que $S_0(0, p)$ est vide pour tout $p \geqslant 7$ ([Da-Me]), et B. Poonen a étendu ce résultat au cas où $p = 5$ ([Po]). Par ailleurs, les travaux de N. Bruin en 1999 permettent de prouver que l'on a (cf. [Bru1] et [Bru2]) :

$$S_0(1,5) = \big\{(-1,1,1)\big\}, \quad S_0(2,5) = \big\{(2,1,6)\big\}, \quad S_0(3,5) = \big\{(1,1,3)\big\},$$

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

De plus, $S_1(\beta, 5)$ est vide si β est non nul. On le vérifie facilement si β est pair ; si β 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 $p \geqslant 7$, en utilisant les travaux de A. Wiles et K. Ribet sur les représentations modulaires ([Ri] et [Wi]), on détermine dans ce chapitre les ensembles $S_0(\beta, p)$ si β est distinct de 1 et $p-1$, ainsi que les ensembles $S_1(\beta, p)$. 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 ([Bu]). Les résultats que l'on démontre sur l'équation (1) permettent de déterminer ces quadruplets dans le cas où $m \geqslant 2$.

Je remercie M. Bennett et C. Skinner pour m'avoir signalé qu'ils avaient obtenu par ailleurs les résultats présentés ici ([Be-Sk]).

1. Énoncé des résultats

Soient p un nombre premier supérieur ou égal à 7 et β un entier naturel vérifiant les inégalités $0 \leqslant \beta \leqslant p-1$.

Théorème 1.

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

2) On a $S_0(3,p) = \Big\{(1,1,3)\Big\}$.

3) On a $S_0(p-3,p) = \Big\{\big(2,1,3.2^{\frac{p-3}{2}}\big)\Big\}$.

4) Si (x,y,z) est un élément de $S_0(1,p)$, l'entier xy est impair.

5) Si (x,y,z) est un élément de $S_0(p-1,p)$, on a $x \equiv 2 \bmod 4$.

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

Corollaire 1. *Soit S l'ensemble des quadruplets $(x,y,m,n) \in \mathbb{Z}^4$ vérifiant les conditions suivantes :*

(i) on a $x^2 - 2^m = y^n$;
(ii) on a $x \geqslant 1$ et y est distinct de 0 et ± 1 ;
(iii) on a $\text{pgcd}\,(x,y) = 1$;
(iv) on a $m \geqslant 2$ et $n \geqslant 3$.

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

Théorème 2.

1) Si β est non nul, l'ensemble $S_1(\beta,p)$ est vide.

2) On a $S_1(0,p) = \Big\{(1,1,1)\Big\}$.

On en déduit le résultat ci-dessous :

Corollaire 2. *Soit (x,y,n) un triplet d'entiers naturels vérifiant les conditions suivantes :*

(i) on a $2x^2 - 1 = y^n$;
(ii) on a $x \geqslant 1$ et $y \geqslant 2$;
(iii) on a $n \geqslant 3$.

Alors, on a $(x,y,n) = (78,23,3)$.

2. Démonstration du théorème 1

On considère un élément (x, y, z) de $S_0(\beta, p)$. Compte tenu des résultats de [Da-Me] rappelés dans l'introduction, on supposera désormais que l'on a $\beta \geqslant 1$.
Étant donné un entier n, on notera $v_2(n)$ la valuation 2-adique de n.

2.1. Cas où x est impair

Démontrons l'énoncé suivant :

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

1) *on a $\beta = 1$ et y est impair ;*
2) *on a $\beta = 3$ et $(x, y, z) = (1, 1, 3)$.*

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

$$Y^2 = X^3 + 2zX^2 + x^pX. \tag{3}$$

Les invariants standard c_4, c_6 et Δ associés à cette équation sont ([Ta], p. 36) :

$$c_4 = 2^4(4z^2 - 3x^p), \qquad c_6 = 2^6z(9x^p - 8z^2) \qquad \text{et} \qquad \Delta = 2^{6+\beta}x^{2p}y^p.$$

On a $\Delta \neq 0$. Par suite, E_0 est une courbe elliptique définie sur $\mathbb{Q}$. On désigne par N_{E_0} son conducteur.

Lemme 1.

1) *Soit ℓ un nombre premier impair. L'équation* (3) *est minimale en ℓ. Si ℓ ne divise pas xy, E_0 a bonne réduction en ℓ. Si ℓ divise xy, E_0 a réduction multiplicative en ℓ.*
2) *Supposons y impair. Si β est distinct de* 1 *et* 3, *on a $v_2(N_{E_0}) \leqslant 4$. On a*

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

3) *Supposons y pair. On a $v_2(N_{E_0}) \leqslant 4$.*

Démonstration : Par définition, si ℓ ne divise pas xy, E_0 a bonne réduction en ℓ. Si ℓ divise xy, le fait que les entiers x, y et z soient premiers entre eux entraîne que ℓ ne divise pas c_4, puis l'assertion 1. Par ailleurs, si y est impair, on a (x étant impair)

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

La classification qui se trouve dans le tableau IV de [Pa] implique alors directement l'assertion 2. De même, si y est pair, on a

$$v_2(\Delta) = 6 + \beta + pv_2(y), \quad v_2(c_4) = 4 \quad \text{et} \quad v_2(c_6) = 6,$$

et le tableau IV de *loc. cit.* entraîne l'assertion 3. 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 $E_0\big(\overline{\mathbb{Q}}\big)$. 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

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

la représentation ainsi obtenue. Soient k et $N\big(\rho_p^{E_0}\big)$ le poids et le conducteur de $\rho_p^{E_0}$ respectivement, qui sont définis par J.-P. Serre dans [Se2].

Lemme 2.

1) On a $k = 2$.

2) Supposons y impair. Si β est distinct de 1 et 3, il existe un entier $s \leqslant 4$ tel que $N\big(\rho_p^{E_0}\big) = 2^s$. On a

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

3) Supposons y pair. Il existe un entier $s \leqslant 4$ tel que $N\big(\rho_p^{E_0}\big) = 2^s$.

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 [Se2] implique alors $k = 2$. Les assertions 2 et 3 sont des conséquences directes du lemme 1 et de la proposition p. 28 de [Kr2].

Lemme 3. *La représentation $\rho_p^{E_0}$ est irréductible.*

Démonstration : On suppose que $\rho_p^{E_0}$ est réductible. Puisque E_0 a un point d'ordre 2 rationnel sur $\mathbb{Q}$, à savoir le point $(0, 0)$, il en résulte que E_0 possède alors un sous-groupe d'ordre $2p$ stable par $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$. On en déduit que $p = 7$ (cf. [Ke], th. 1). La courbe modulaire $X_0(14)$ est une courbe elliptique de rang 0 sur $\mathbb{Q}$ ([Li], th. 5.1.1) D'après le corollaire 4.3 de [Ma], E_0 a donc potentiellement bonne réduction en tout nombre premier impair. Par suite, d'après l'assertion 1 du lemme 1, on a $x = \pm 1$ (car x est impair) et $y = \pm 2^r$ où $r \geqslant 0$. On obtient ainsi $2^{\beta + rp} = z^2 \pm 1$ et l'on vérifie que cela entraîne $\beta + rp \in \big\{1, 3\big\}$, d'où $z \in \big\{1, 3\big\}$. Cela conduit à $N_{E_0} \in \big\{32, 128, 640\big\}$ et à une contradiction (cf. [Cr1], pages 111, 122 et 195). D'où le lemme.

Terminons maintenant la démonstration de la proposition 1. Étant donné un entier $n \geqslant 1$, notons $S_2\big(\Gamma_0(n)\big)$ 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 $S_2\big(\Gamma_0(n)\big)$ engendré par les *newforms* au sens de [At-Le] ; c'est un espace vectoriel de dimension finie $g_0^+(n)$ sur $\mathbb{C}$; on pourra trouver dans [Kr4] la détermination de $g_0^+(n)$.

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

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

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

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

(On pourra consulter à ce sujet la remarque 2, p. 325 de [Se3]).

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

Si $\beta = 1$, l'assertion 3 du lemme 2, et le même argument que celui utilisé ci-dessus entraînent que y est impair.

Supposons $\beta = 3$. Comme ci-dessus y est impair ; on a $N\big(\rho_p^{E_0}\big) = 32$ 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 [Cr1]. C'est une courbe à multiplications complexes par l'anneau d'entiers de $\mathbb{Q}(i)$.
Soit $\rho_p^E : \mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big) \longrightarrow \mathrm{Aut}(E[p])$ la représentation donnant l'action de $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ sur le sous-groupe des points de p-torsion de $E\big(\overline{\mathbb{Q}}\big)$. Il résulte de la condition (4) que $\rho_p^{E_0}$ et ρ_p^E ont des semi-simplifiées isomorphes. Puisqu'elles sont irréductibles, elles sont donc isomorphes. L'image de $\rho_p^{E_0}$ est donc contenue dans le normalisateur d'un sous-groupe de Cartan C de $\mathrm{Aut}\big(E_0[p]\big)$ (cf. [Se1]).

1) Supposons que C soit déployé. On a alors $p \equiv 1$ mod. 4. Si l'on a $p \geqslant 17$, le théorème 1 de [Ha-Kr-1] implique $N_{E_0} = 32$. L'entier y étant impair, on déduit de là que $xy = \pm 1$ (lemme 1), puis $(x, y, z) = (1, 1, 3)$. On a la même conclusion si $p = 13$ (cf. [Da-Me], p. 89, deuxième alinéa de la démonstration de la prop. 4.2).

2) Supposons que C soit non déployé. L'image de $\rho_p^{E_0}$ est alors le normalisateur de C (cf. [Se1], 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 $\mathbb{Z}[\frac{1}{p}]$ ([Da-Me], th. 8.1). On a l'égalité

$$j = \frac{8(4z^2 - 3x^p)^3}{(x^2y)^p}.$$

Les entiers $8(4z^2 - 3x^p)^3$ et xy sont premiers entre eux. On en déduit que xy est au signe près une puissance de p, puis que p divise xy ou bien que $xy = \pm 1$.
Supposons que p divise xy. Dans ce cas, E_0 a mauvaise réduction de type multiplicatif en p. Soit I un sous-groupe d'inertie en p de $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ (qui est bien défini à conjugaison près). L'ordre de $\rho_p^{E_0}\big(I\big)$ est $p - 1$ ou $p(p - 1)$ (cf. [Se1], prop. 13). Par ailleurs, E a par hypothèse bonne réduction de hauteur 2 en p, donc l'ordre de $\rho_p^E(I)$ est $p^2 - 1$ (*loc. cit.*, prop. 12). Cela contredit le fait que ρ_p^E et $\rho_p^{E_0}$ sont isomorphes ; ainsi p ne divise pas xy. Par conséquent, $xy = \pm 1$ et l'on a de nouveau $(x, y, z) = (1, 1, 3)$.

Cela termine la démonstration de la proposition 1.

2.2. Cas où x est pair

On va démontrer dans ce cas l'énoncé suivant :

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

1) on a $\beta = p-1$ et $v_2(x) = 1$;

2) on a $\beta = p-3$ et $(x,y,z) = \big(2, 1, 3.2^{(p-3)/2}\big)$.

Démonstration : On remarque d'abord que z est pair et par suite y est impair. Il existe donc un entier impair $z_1 \geqslant 1$ tel que l'on ait $z^2 = 2^\beta z_1^2$. Par ailleurs, il existe un entier $r \geqslant 1$ et un entier impair x_1 tels que $x = 2^r x_1$. On a $2^{rp-\beta} x_1^p + y^p = z_1^2$. Soient u et t des entiers tels que $rp - \beta = up + t$ avec $1 \leqslant t \leqslant p-1$. On a l'égalité

$$y^p + 2^t (2^u x_1)^p = z_1^2.$$

Les entiers y, x_1 et z_1 sont non nuls et premiers entre eux. On en déduit que $(y, 2^u x_1, z_1)$ appartient à $S_0(t,p)$. Puisque y est impair, il résulte de la proposition 1 que l'on est dans l'un des deux cas suivants :

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

2) On a $t = 3$. Dans ce cas, on a $(y, 2^u x_1, z_1) = (1,1,3)$ (*loc. cit.*). On obtient ainsi $y = 1$. De plus, on a $u = 0$, puis $r = 1$ et par suite $\beta = p-3$. On déduit ensuite que $x = 2$ et que $z = 3.2^{(p-3)/2}$. 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 (x,y,z) appartient à $S_0(1,p)$ et si x est impair, on a $N\big(\rho_p^{E_0}\big) = 2^7$ (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 dcterminer $S_0(1,p)$.

Cela étant, la conjecture ci-dessous concernant la comparaison galoisienne des points de torsion des courbes elliptiques, entraîne que l'on a $S_0(1,p) = \big\{(-1,1,1)\big\}$ dès que p est assez grand (cf. par exemple [Da2], 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 (x,y,z) appartient à $S_0(p-1,p)$ l'équation (3) n'est pas minimale en 2 : on a $v_2(x)=1$, $v_2(z^2)=p-1$, et si l'on pose $x=2x_1$, $z^2=2^{p-1}z_1^2$, $p=4t+r$ avec $r=1$ ou 3, le changement de variables $X=2^{2t}X'$, $Y=2^{3t}Y'$ transforme (3) en le modèle

$$Y'^2 = X'^3 + 2^{\frac{r+1}{2}} z_1\ X'^2 + 2^r x_1^p\ X',$$

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

3. Démonstration du corollaire 1

Soit (x,y,m,n) un élément de S. Puisque x et y sont premiers entre eux, x et y sont impairs. Par ailleurs, n est impair ([Bu], p. 3205, 4).

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

$$(y^r)^p + 2^u(2^t)^p = x^2,$$

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

Si $p \geqslant 7$, 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 $(y^r,2^t,x)=(1,1,3)$, d'où $y=1$;

(iii) $u=p-3$ et $(y^r,2^t,x)=\big(2,1,3.2^{\frac{p-3}{2}}\big)$, d'où $y=2$;

(iv) $u=p-1$ et y 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

$$(u,y^r,2^t,x) \in \Big\{(1,-1,1,1),(2,2,1,6),(3,1,1,3),(4,2,-1,4)\Big\},$$

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

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

$$(x,y^r,m) \in \Big\{(13,-7,9),(71,17,7)\Big\},$$

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

4. Démonstration du théorème 2

On considère un élément (x,y,z) de $S_1(\beta,p)$.

Démontrons l'assertion 1 du théorème :

Proposition 3. *On a $\beta = 0$.*

Démonstration : Supposons que l'on ait $\beta \geqslant 1$. On a alors

$$x \equiv 0 \text{ mod. } 2, \quad y \equiv 1 \text{ mod. } 2 \quad \text{et} \quad \beta = 2v_2(z) + 1. \tag{5}$$

Posons $x = 2^r x_1$ où x_1 impair et $r \geqslant 1$, et $z = 2^{\frac{\beta-1}{2}} z_1$. On a l'égalité

$$2^{rp-\beta} x_1^p + y^p = z_1^2. \tag{6}$$

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

$$y^p + 2^u (2^q x_1)^p = z_1^2.$$

Le triplet $(y, 2^q x_1, z_1)$ appartient donc à $S_0(u, p)$. Puisque y est impair, la proposition 1 implique $u = 1$ ou $u = 3$. Par ailleurs, on a la congruence $\beta \equiv -u$ mod. p. On en déduit que $\beta = p - u$, ce qui contredit le fait que β soit impair. D'où le résultat.

Prouvons maintenant l'assertion 2. Il résulte de la proposition 3 que l'on a

$$xy \equiv 1 \text{ mod. } 2. \tag{7}$$

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

$$Y^2 = X^3 + 4zX^2 + 2y^p X. \tag{8}$$

Les invariants standard c_4, c_6 et Δ associés à cette équation sont (cf. [Ta]) :

$$c_4 = 2^5(8z^2 - 3y^p), \qquad c_6 = 2^8 z(9y^p - 16z^2) \qquad \text{et} \qquad \Delta = 2^9 x^p y^{2p}.$$

On a $\Delta \neq 0$, donc E_1 est une courbe elliptique sur $\mathbb{Q}$. Soit N_{E_1} son conducteur.

Lemme 4.

1) *Soit ℓ un nombre premier. L'équation* (8) *est minimale en ℓ. Si ℓ ne divise pas $2xy$, E_1 a bonne réduction en ℓ. Si ℓ divise xy, E_1 a réduction multiplicative en ℓ.*
2) *On a $v_2(N_{E_1}) = 8$.*

Démonstration : La condition (7) implique la minimalité de l'équation (8) en 2. Si ℓ est un diviseur premier de xy, ℓ ne divise pas c_4 car x, y et z sont premiers entre eux ; d'où l'assertion 1. Par ailleurs, on a

$$v_2(c_4) = 5, \qquad v_2(c_6) \geqslant 8 \qquad \text{et} \qquad v_2(\Delta) = 9,$$

ce qui entraîne l'assertion 2 ([Pa], tableau IV).

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

Lemme 5. *On a $k = 2$ et $N\big(\rho_p^{E_1}\big) = 2^8$.*

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

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

Démonstration : Supposons que $\rho_p^{E_1}$ soit réductible. Comme dans la démonstration du lemme 3, cette condition entraîne $p = 7$ et que E_1 a potentiellement bonne réduction en tout nombre premier impair. D'après (7), cela implique $xy = \pm 1$, puis $(x, y, z) = (1, 1, 1)$. On en déduit que $N_{E_1} = 2^8$, d'où une contradiction (cf. [Cr1], p. 139) et le lemme.

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

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

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

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

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

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

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

a) la newform f correspond à l'une des quatre classes d'isogénie de courbes elliptiques sur $\mathbb{Q}$ de conducteur 2^8 (cf. [Cr1]) ;
b) les coefficients $a_n(f)$ appartiennent à un corps quadratique K_f.

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

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

Il en résulte que $K_f = \mathbb{Q}\big(\sqrt{2}\big)$, 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

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

$$a_3(f) \equiv \pm 4 \text{ mod. } \mathfrak{P}, \qquad \text{si 3 divise } xy.$$

Cela entraîne une contradiction et prouve notre assertion.

On est donc dans le cas a). 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 $\mathbb{Q}\big(\sqrt{-2}\big)$. On en déduit que l'image de $\rho_p^{E_1}$ est contenue dans le normalisateur d'un sous-groupe de Cartan C de $\mathrm{Aut}\big(E_1[p]\big)$.

a.1) Supposons que C soit déployé. Dans ce cas, p est décomposé dans K et l'on a $p \geqslant 11$. Si p est distinct de 13, on doit avoir $N_{E_1} = 2^8$ ([Ha-Kr-1], th. 1), ce qui entraîne $(x, y, z) = (1, 1, 1)$. Si $p = 13$, on a la même conclusion (cf. [Da-Me], p. 89, deuxième alinéa de la preuve de la prop. 4.2).

a.2) Supposons que C soit non déployé. L'image de $\rho_p^{E_1}$ est alors le normalisateur de C (cf. [Se1], prop. 12). D'après le théorème 8.1 de [Da-Me], l'invariant modulaire de E_1 doit appartenir à $\mathbb{Z}[\frac{1}{p}]$. Cela entraîne $xy = \pm 1$ puis $(x, y, z) = (1, 1, 1)$, ou bien que p divise xy ; 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.

5. Démonstration du corollaire 2

1) Supposons qu'il existe un nombre premier $p \geqslant 5$ qui divise n. En posant $n = rp$, on vérifie alors que $(y^r, 1, x)$ appartient à $S_1(0, p)$. Lorsque $p \geqslant 7$, le théorème 2 entraîne une contradiction. Si $p = 5$ les travaux de Bruin rappelés dans l'introduction conduisent à la même conclusion.

2) Supposons que 3 divise n : posons $n = 3r$. Dans ce cas, on vérifie que $(2y^r, 4x)$ est un point entier sur la courbe elliptique d'équation

$$Y^2 = X^3 + 8.$$

C'est la courbe notée 576A1 dans [Cr1]. Elle est de rang 1 sur $\mathbb{Q}$ et l'on vérifie en utilisant le logiciel de calcul Magma que les points entiers de cette courbe elliptique sont $(-2, 0)$, $(1, \pm 3)$, $(2, \pm 4)$, $(46, \pm 312)$ (cf. [Magma]). Cela conduit à $(x, y, n) = (78, 23, 3)$.

3) Supposons n pair. D'après les alinéas précédents, on peut supposer que n est une puissance de 2. Puisque l'on a $n \geqslant 3$, on a $n = 4r$ et $(y^r, 1, x)$ est une solution de l'équation

$$X^4 + Y^4 = 2Z^2.$$

On obtient ainsi une contradiction (cf. par exemple [Mor] p.18). D'où le résultat.

Appendice

Sur la détermination des ensembles $S_0(\beta, 5)$ et $S_1(0, 5)$

On se propose ici de fournir quelques indications sur la méthode décrite par Bruin dans [Bru1] 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 [Bru1] (signalons que dans l'énoncé de la proposition 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 *loc. cit.*.

Indiquons la démarche suivie pour la détermination de l'ensemble $S_0(1, 5)$. Considérons pour cela un élément (x, y, z) de $S_0(1, 5)$. On a

$$x^5 + 2y^5 = z^2.$$

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

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

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

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

$$C_1 : Y^2 = Q(X) \quad \textit{et} \quad C_2 : \big(\alpha - 1\big)Y^2 = Q(X).$$

Alors, il existe $\delta \in K$ tel que $\big(-\frac{x}{y}, \delta\big)$ appartienne à $C_1(K)$ ou à $C_2(K)$.

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

$$(x + \alpha y)\tilde{Q}(x, -y) = z^2.$$

L'anneau des entiers O_K de K est principal (cf. [Pari]). Soit π un élément irréductible de O_K dont l'exposant dans la décomposition de $x + \alpha y$ en produit d'éléments irréductibles de O_K est impair. On vérifie que π divise 2 ou 5, puis que π est associé à α 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 $\big\{\pm 1\big\}$ (cf. *loc. cit.*) On en déduit l'existence d'entiers n_i égaux à 0 ou 1 tels que l'on ait

$$x + \alpha y \equiv \pm\ u_1^{n_1}\ u_2^{n_2}\ \alpha^{n_3}\ (\alpha^2 + 1)^{n_4} \text{ mod. } K^{*2}.$$

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

$$x+\alpha y \equiv u_1^{n_1}\ u_2^{n_2} \text{ mod. } K^{*2}.$$

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 x et y étant premiers entre eux, x est impair et $x+\alpha y$ 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 x et y modulo 8. En utilisant le fait que

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

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

Les quartiques C_1 et C_2 sont birationnellement équivalentes à deux courbes elliptiques sur K et une 2-descente permet de démontrer qu'elles sont de rang 2 sur K. 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 [Bru1] ou dans le chapitre IV de cette thèse. Les détails des arguments qui interviennent sont trop longs pour être présentés ici. Signalons simplement que l'on peut par exemple déterminer ces points à l'aide du logiciel de calculs ALGAE qui a été écrit par Bruin (cf. [Bru2]). On constate alors que si $u \in \mathbb{Q}$ est l'abscisse d'un point de $C_1(K)$, on a $u \in \{0, 3/4\}$. De même, si $u \in \mathbb{Q}$ est l'abscisse d'un point de $C_2(K)$, on a $u=1$ ou $u=-3$. On obtient ainsi le fait que $S_0(1,5) = \big\{(-1,1,1)\big\}$.

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

Chapitre II

Courbes elliptiques sur $\mathbb{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, de conducteur $2^N p$

Introduction

Soient p un nombre premier impair et N un entier naturel. On s'intéresse dans ce chapitre au problème suivant :

Problème 1. *Déterminer toutes les classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$.*

D'après les résultats de I. Papadopoulos ou bien de P. Lockhart, M. Rosen et J. H. Silverman, il n'existe pas de courbes elliptiques définies sur $\mathbb{Q}$ dont le conducteur soit divisible par 2^9 ([Pa] ou [Lo-Ro-Si]). On supposera donc dans toute la suite que l'on a

$$0 \leqslant N \leqslant 8.$$

Par ailleurs, d'après le théorème de Shafarevich, il n'existe qu'un nombre fini de telles classes d'isomorphisme ([Si1], p. 263). Dans le cas où N est nul, B. Setzer a obtenu en 1974, le résultat ci-dessous (cf. [Set]) :

Théorème. *Soit p un nombre premier distinct de 17. Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur p et possédant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si $p-64$ est un carré dans $\mathbb{Z}$. Dans ce cas, il existe à $\mathbb{Q}$-isomorphisme près deux telles courbes elliptiques. Des équations de ces courbes sont*

$$y^2 \;=\; x^3 \;+\; \sqrt{p-64}\; x^2 \;-\; 16\; x,$$

$$y^2 \;=\; x^2 \;-\; 2\sqrt{p-64}\; x^2 \;+\; p\; x,$$

où $\sqrt{p-64}$ désigne la racine carrée de $p-64$ congrue à 1 modulo 4.

Des modèles minimaux de ces courbes sont donnés par les équations

$$y^2 + xy = x^3 + \left(\frac{\sqrt{p-64}-1}{4}\right)x^2 - x,$$

$$y^2 + xy = x^3 + \left(\frac{\sqrt{p-64}-1}{4}\right)x^2 + 4x + \sqrt{p-64},$$

pour lesquelles les discriminants sont respectivement p et $-p^2$. Il se trouve aussi dans [Set] la liste des quatre classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ qui sont de conducteur 17.

Dans ce travail, on obtient des résultats analogues au théorème de Setzer pour les entiers $N \leqslant 8$. Pour cela, on est principalement confronté, comme dans *loc. cit.*, au problème de la détermination des solutions entières de certaines équations diophantiennes ternaires (cf. le paragraphe 2.2). Un problème typique auquel on est conduit est celui de la détermination, pour tous les entiers naturels r et s non nuls, des entiers $x \in \mathbb{Z}$ vérifiant l'égalité

$$x^2 - 2^r = p^s.$$

Si $r = 1$, en utilisant les résultats de M. Mignotte sur les minorations de formes linéaires en deux logarithmes qui se trouvent dans [Mi], on démontre que l'on a

$$s \leqslant 164969.$$

Cette inégalité nous suffit en pratique pour obtenir les entiers x cherchés. Supposons $r \geqslant 2$. Si l'on a $s \geqslant 2$, on est amené à utiliser les résultats démontrés dans le chapitre I. Si $s = 1$, les travaux de F. Beukers ([Beu], cor. 1 et 2) permettent de borner l'entier r par une fonction qui ne dépend que du logarithme de p (formule (1)). Là encore, la majoration obtenue nous suffit pour les résultats que l'on a en vue.
Signalons que dans le cas où p est congru à 3 ou 5 modulo 8 et distinct de 3, T. Hadano a déterminé en 1974 les entiers x vérifiant l'égalité ci-dessus, à condition de supposer que les conjectures d'Ankeny-Artin-Chowla et ses analogues sont vraies (cf. [Had], lemma p. 200). Ces conjectures ne sont toujours pas démontrées aujourd'hui.

Afin de simplifier la présentation des résultats, on s'est limité au cas où $p \geqslant 29$. Ce choix n'est pas restrictif, puisque J. Cremona a explicité toutes les classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ dont le conducteur est plus petit que 15000 (cf. [Cr1], [Cr2]). En particulier, le problème 1 est résolu si l'on a $2^N p \leqslant 15000$. Les lemmes diophantiens se trouvant dans la partie 2.2 de ce travail permettent aussi de résoudre le problème posé si $p \leqslant 29$.

On pourra trouver à l'adresse, http://www.math.jussieu.fr/~ivorra, un programme fonctionnant sous le logiciel de calculs PARI (cf. [Pari]) permettant, un nombre premier p étant donné, de résoudre le problème 1. À titre indicatif, pour $p = 414977$, les courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$ et ayant au moins un point d'ordre 2 sur $\mathbb{Q}$ sont, à $\mathbb{Q}$-isomorphisme près, celles indiquées dans les tableaux ci-dessous. Elles sont données par des équations minimales de la forme

$$y^2 \ + \ a_1\, xy \ = \ x^2 \ + \ a_2\, x^2 \ + \ a_4\, x \ + \ a_6.$$

a_1	a_2	a_4	a_6	m
1	160	-64	0	1
1	160	256	41024	1
0	-641	-1024	0	4
0	1282	414977	0	4

a_1	a_2	a_4	a_6	m
0	1282	-4096	0	6
0	-2564	1659908	0	6
0	-1282	-4096	0	6
0	2564	1659908	0	6

Par exemple, si $p = 4000237$, il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$ ayant un point d'ordre 2 sur $\mathbb{Q}$.

Le problème 1 est un cas particulier du problème suivant, que nous ne savons pas traiter en général :

Problème 2. *Déterminer toutes les classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$.*

Il semble que les premiers résultats démontrés sur ce problème soient dûs à A. Ogg en 1966. Il a déterminé les courbes elliptiques définies sur $\mathbb{Q}$ dont le conducteur est de la forme 2^N ou $2^N.3$ (cf. [Og1] et [Og2]). Celles de conducteur 11 ont été ensuite explicitées par J. Vélu (cf. [Ve1]). En ce qui concerne la recherche des courbes elliptiques de conducteur premier p, J.-F. Mestre et J. Oesterlé ont obtenu des tables de courbes de Weil fortes de conducteur $p < 10000$; A. Brumer et O. McGuinness ont déterminé les courbes elliptiques de conducteur $p < 10^8$. Ces travaux ne sont pas publiés dans la littérature. Par ailleurs, comme nous l'évoquions ci-dessus, le problème 2 est résolu si $2^N p$ est plus petit que 15000. Ce sont, à notre connaissance, les principaux travaux existant concernant ce problème.

Pour certains nombres premiers p, toute courbe elliptique sur $\mathbb{Q}$ ayant un conducteur de la forme $2^N p$ possède un point d'ordre 2 rationnel sur $\mathbb{Q}$. Pour un tel nombre premier p, les résultats que l'on obtient permettent ainsi de résoudre le problème 2. Rappelons un critère pour qu'il en soit ainsi (cf. [Set] et [Had]) :

Proposition. *Soit p un nombre premier.*

1. *Supposons que les nombres de classes des deux corps*

$$\mathbb{Q}(\sqrt{p}) \quad et \quad \mathbb{Q}(\sqrt{-p})$$

ne soient pas divisibles par 3 et que p soit congru à 1 ou 7 modulo 8. Alors, toute courbe elliptique sur $\mathbb{Q}$ de conducteur p a au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$.

2. *Supposons que les nombres de classes des quatre corps*

$$\mathbb{Q}(\sqrt{p}), \quad \mathbb{Q}(\sqrt{-p}), \quad \mathbb{Q}(\sqrt{2p}) \quad et \quad \mathbb{Q}(\sqrt{-2p})$$

ne soient pas divisibles par 3.

(i) Si p est congru à 3 *ou* 5 *modulo* 8, *il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur* $2p$.

(ii) Si p est congru à 1 *ou* 7 *modulo* 8, *toute courbe elliptique sur $\mathbb{Q}$ de conducteur* $2^N p$, *avec* $N \geqslant 1$, *a au moins un point d'ordre* 2 *rationnel sur $\mathbb{Q}$.*

Les nombres premiers $p < 1000$ congrus à 1 ou 7 mod. 8 pour lesquels les nombres de classes des corps $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{-p})$, $\mathbb{Q}(\sqrt{2p})$ et $\mathbb{Q}(\sqrt{-2p})$ ne sont pas divisibles par 3 sont les suivants :

$$\Big\{7, 17, 41, 47, 73, 97, 103, 113, 191, 193, 281, 409, 463, 479, 577, 607\Big\}$$

$$\Big\{647, 719, 769, 887, 911, 919, 937, 953, 967\Big\}$$

Par exemple, si $p = 967$, on peut ainsi démontrer qu'il n'existe pas de courbes elliptiques sur $\mathbb{Q}$, de conducteur $2^N p$ si $N = 0$, 2, 3, 5 ou 7. Si $N = 1$, 4, 6 ou 8, la liste exhaustive des courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$ est donnée, comme précédemment, dans les tableaux ci-dessous.

a_1	a_2	a_4	a_6	m
1	21	128	0	1
1	21	−512	−10880	1
0	−85	2048	0	4
0	170	−967	0	4
0	170	8192	0	6
0	−340	−3868	0	6
0	−170	8192	0	6
0	340	−3868	0	6

a_1	a_2	a_4	a_6	m
0	88	2	0	8
0	−176	7736	0	8
0	−88	2	0	8
0	176	7736	0	8
0	88	1934	0	8
0	−176	8	0	8
0	−88	1934	0	8
0	176	8	0	8

Si $N = 1$ les courbes sont, à $\mathbb{Q}$-isomorphisme près, celles notées $1934A1$ et $1934A2$ dans les tables de Cremona (cf. [Cr2]).

Signalons enfin que si $p = 1299709$, l'hypothèse de l'assertion 2 de la proposition est aussi satisfaite, et il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^N p$.

1. Énoncé des résultats

Soient p un nombre premier et N un entier vérifiant les inégalités

$$p \geqslant 29 \quad \text{et} \quad 1 \leqslant N \leqslant 8.$$

Nous énonçons dans ce qui suit huit théorèmes qui décrivent, à $\mathbb{Q}$-isomorphisme près, toutes les courbes elliptiques sur $\mathbb{Q}$, de conducteur $2^N p$, ayant au moins un point d'ordre 2 sur $\mathbb{Q}$. Chaque théorème correspond à une valeur de N. Les résultats que l'on a obtenus sont présentés sous forme de tableaux analogues à ceux de [Cr1]. Dans chaque ligne on explicite une courbe elliptique E définie sur $\mathbb{Q}$ réalisant les conditions souhaitées. Les colonnes des tableaux fournissent les données suivantes sur E :

1. Un modèle minimal de E de la forme

$$y^2 \ + a_1\ xy \ = \ x^3 \ + \ a_2\ x^2 \ + \ a_4\ x \ + \ a_6,$$

   où les a_i sont dans $\mathbb{Z}$. Si l'on a $N \geqslant 2$, on peut choisir un tel modèle avec $a_1 = a_6 = 0$. Dans les énoncés des théorèmes 2 à 8, on a donc omis les colonnes qui correspondent à ces coefficients.
2. L'ordre $|T_2|$ du groupe T_2 des points de 2-torsion de E rationnels sur $\mathbb{Q}$.
3. La factorisation du discriminant minimal Δ de E.
4. Les symboles de Kodaira de E en 2 et p.
5. Les courbes elliptiques liées à E par une isogénie sur $\mathbb{Q}$ de degré 2.

Il apparaît par ailleurs dans les tableaux des lettres d'identifications (A, $B, \cdots$) pour chaque courbe elliptique. Les courbes elliptiques qui sont libellées par une même lettre sont liées par une isogénie sur $\mathbb{Q}$ de degré 2 ou un composé de deux telles isogénies. Elles sont de plus numérotées dans l'ordre où elles ont été déterminées. Dans la colonne Isogénies, nous avons indiqué par leurs numéros les courbes liées à E par une isogénie de degré 2. Ce degré est rappelé en gras.

Notations

a) Pour toute courbe elliptique E sur $\mathbb{Q}$, on désignera par E' la courbe elliptique sur $\mathbb{Q}$ déduite de E par torsion par $\sqrt{-1}$.

b) On notera f la fonction réelle définie sur $\mathbb{N}^*$ par

$$f(n) = \begin{cases} 18 + 2\ \dfrac{\log n}{\log 2} & \text{si } n < 2^{96} \\ \\ 435 + 10\ \dfrac{\log n}{\log 2} & \text{si } n \geqslant 2^{96}. \end{cases} \tag{1}$$

c) Étant donné un entier n qui soit un carré dans $\mathbb{Z}$, on désignera, pour toute la suite, par $\sqrt{n}$ la racine carrée de n vérifiant la condition suivante :

$$(2) \qquad \begin{cases} \sqrt{n} \equiv 1 \bmod. 4 & \text{si } n \text{ est impair} \\ \sqrt{n} \geqslant 0 & \text{si } n \text{ est pair.} \end{cases}$$

Théorème 1. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $2p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles il existe un entier k vérifiant les inégalités*

$$7 \leqslant k < f(p),$$

tel que l'une des conditions suivantes soit satisfaite :

1) l'entier $p - 2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	1	$\frac{\sqrt{p-2^k}-1}{4}$	-2^{k-6}	0	2	$2^{2k-12}p$	I_{2k-12},I_1	**2 :** 2
A2	1	$\frac{\sqrt{p-2^k}-1}{4}$	2^{k-4}	$2^{k-6}\sqrt{p-2^k}$	2	$-2^{k-6}p^2$	I_{k-6},I_2	**2 :** 1

2) l'entier $p + 2^k$ est un carré, k est impair et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	1	$\frac{\sqrt{p+2^k}-1}{4}$	2^{k-6}	0	2	$2^{2k-12}p$	I_{2k-12},I_1	**2 :** 2
B2	1	$\frac{\sqrt{p+2^k}-1}{4}$	-2^{k-4}	$-2^{k-6}\sqrt{p+2^k}$	2	$2^{k-6}p^2$	I_{k-6},I_2	**2 :** 1

3) l'entier k est pair, on a $p = 2^{\frac{k}{2}+1} + 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	1	$\frac{1-p}{4}$	$\frac{1-p}{16}$	0	4	$2^{k-6}p^2$	I_{k-6},I_2	**2 :** 2, 3, 4
C2	1	$\frac{p-1}{2}$	$\frac{(p-1)(p+5)}{16}$	$\frac{(p-1)(p+3)}{64}$	2	$-2^{\frac{k}{2}-3}p^4$	$I_{\frac{k}{2}-3}$,I_4	**2 :** 1
C3	1	$\frac{p-1}{8}$	$\frac{(p-1)^2}{2^8}$	0	2	$2^{2k-12}p$	I_{2k-12},I_1	**2 :** 1
C4	1	$1-p$	$\frac{1-p}{2}$	$\frac{1-p}{16}$	2	$2^{\frac{k}{2}-3}p$	$I_{\frac{k}{2}-3}$,I_1	**2 :** 1

4) l'entier $2^k - p$ est un carré, k est impair et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
D1	1	$\frac{\sqrt{2^k-p}-1}{4}$	2^{k-6}	0	2	$-2^{2k-12}p$	I_{2k-12},I_1	**2 :** 2
D2	1	$\frac{\sqrt{2^k-p}-1}{4}$	-2^{k-4}	$-2^{k-6}\sqrt{2^k-p}$	2	$2^{k-6}p^2$	I_{k-6},I_2	**2 :** 1

5) l'entier k est pair, on a $p = 2^{\frac{k}{2}+1} - 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
E1	1	$\frac{p+1}{4}$	$\frac{p+1}{16}$	0	4	$2^{k-6}p^2$	I_{k-6},I_2	**2 :** 2, 3, 4
E2	1	$-\frac{p+1}{2}$	$\frac{(p+1)(p-5)}{16}$	$\frac{(p+1)(p-3)}{64}$	2	$2^{\frac{k}{2}-3}p^4$	$I_{\frac{k}{2}-3}$,I_4	**2 :** 1
E3	1	$-\frac{p+1}{8}$	$\frac{(p+1)^2}{2^8}$	0	2	$-2^{2k-12}p$	I_{2k-12},I_1	**2 :** 1
E4	1	$p+1$	$\frac{p+1}{2}$	$\frac{p+1}{16}$	2	$2^{\frac{k}{2}-3}p$	$I_{\frac{k}{2}-3}$,I_1	**2 :** 1

Corollaire. *Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $2p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si il existe un entier k vérifiant les inégalités*

$$7 \leqslant k < f(p),$$

tel que l'un des entiers $p - 2^k$, $p + 2^k$ et $2^k - p$ soit un carré. Si tel est le cas, p est congru à 1 ou 7 modulo 8.

Théorème 2. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $4p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles la condition suivante est satisfaite :*

l'entier $p - 4$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$\sqrt{p-4}$	-1	2	2^4p	IV,I_1	**2 :** 2
A2	$-2\sqrt{p-4}$	p	2	-2^8p^2	IV^*,I_2	**2 :** 1

Corollaire. *Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $4p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si $p-4$ est un carré. Si tel est le cas, p est congru à 5 modulo 8.*

Théorème 3. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $8p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles l'une des conditions suivantes est satisfaite :*

1) l'entier $p-16$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$\sqrt{p-16}$	-4	2	2^8p	I_1^*,I_1	**2 :** 2
A2	$-2\sqrt{p-16}$	p	2	$-2^{10}p^2$	III^*,I_2	**2 :** 1

2) l'entier $p-32$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	$\sqrt{p-32}$	-8	2	$2^{10}p$	III^*,I_1	**2 :** 2
B2	$-2\sqrt{p-32}$	p	2	$-2^{11}p^2$	II^*,I_2	**2 :** 1

3) l'entier $p+32$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$\sqrt{p+32}$	8	2	$2^{10}p$	III^*,I_1	**2 :** 2
C2	$-2\sqrt{p+32}$	p	2	$2^{11}p^2$	II^*,I_2	**2 :** 1

4) on a $p=31$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
D1	1	8	2	$-2^{10}.31$	III^*,I_1	**2 :** 2
D2	-2	-31	2	$2^{11}.31^2$	II^*,I_2	**2 :** 1

Corollaire. *Supposons $p > 31$. Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $8p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si l'un des entiers $p-16$, $p-32$ et $p+32$ est un carré. Si tel est le cas, p est congru à 1 modulo 8.*

Théorème 4. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $16p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles il existe un entier k vérifiant les inégalités*

$$4 \leqslant k < f(p),$$

tel que l'une des conditions suivantes soit satisfaite :

1) l'entier $p - 2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$-\sqrt{p-2^k}$	-2^{k-2}	2	$2^{2k}p$	I^*_{2k-8},I_1	**2 :** 2
A2	$2\sqrt{p-2^k}$	p	2	$-2^{k+6}p^2$	I^*_{k-2},I_2	**2 :** 1

2) l'entier $p + 2^k$ est un carré, k est impair et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	$-\sqrt{p+2^k}$	2^{k-2}	2	$2^{2k}p$	I^*_{2k-8},I_1	**2 :** 2
B2	$2\sqrt{p+2^k}$	p	2	$2^{k+6}p^2$	I^*_{k-2},I_2	**2 :** 1

3) l'entier k est pair, on a $p = 2^{\frac{k}{2}+1} + 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$p+1$	p	4	$2^{k+6}p^2$	I^*_{k-2},I_2	**2 :** 2, 3, 4
C2	$-\frac{p+1}{2}$	$\frac{(p-1)^2}{16}$	2	$2^{2k}p$	I^*_{2k-8},I_1	**2 :** 1
C3	$2(2p-1)$	1	2	$2^{9+\frac{k}{2}}p$	$I^*_{\frac{k}{2}+1}$,I_1	**2 :** 1
C4	$2(2-p)$	p^2	2	$-2^{9+\frac{k}{2}}p^4$	$I^*_{\frac{k}{2}+1}$,I_4	**2 :** 1

4) l'entier $p - 4$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
D1	$-\sqrt{p-4}$	-1	2	2^4p	II,I_1	**2 :** 2
D2	$2\sqrt{p-4}$	p	2	-2^8p^2	I^*_0,I_2	**2 :** 1

5) l'entier $2^k - p$ est un carré, k est impair et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
E1	$-\sqrt{2^k - p}$	2^{k-2}	2	$-2^{2k}p$	I^*_{2k-8},I_1	**2 :** 2
E2	$2\sqrt{2^k - p}$	$-p$	2	$2^{k+6}p^2$	I^*_{k-2},I_2	**2 :** 1

6) l'entier k est pair, on a $p = 2^{\frac{k}{2}+1} - 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
F1	$1 - p$	$-p$	4	$2^{k+6}p^2$	I^*_{k-2},I_2	**2 :** 2, 3, 4
F2	$\frac{p-1}{2}$	$\frac{(p+1)^2}{16}$	2	$-2^{2k}p$	I^*_{2k-8},I_1	**2 :** 1
F3	$2(p+2)$	p^2	2	$2^{\frac{k}{2}+9}p^4$	$I^*_{\frac{k}{2}+1}$,I_4	**2 :** 1
F4	$-2(2p+1)$	1	2	$2^{\frac{k}{2}+9}p$	$I^*_{\frac{k}{2}+1}$,I_1	**2 :** 1

Corollaire. *Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $16p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si il existe un entier k vérifiant les inégalités*

$$4 \leqslant k < f(p),$$

tel que l'un des entiers $p-4$, $p-2^k$, $p+2^k$ et $2^k - p$ soit un carré. Si tel est le cas, p est congru à 1, 5 ou 7 modulo 8.

Théorème 5. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $32p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles l'une des conditions suivantes est satisfaite :*

1) l'entier $p - 1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$2\sqrt{p-1}$	-1	2	2^6p	III,I_1	**2 :** 2
A2	$-4\sqrt{p-1}$	$4p$	2	$-2^{12}p^2$	I^*_3,I_2	**2 :** 1
A1'	$-2\sqrt{p-1}$	-1	2	2^6p	III,I_1	**2 :** 2
A2'	$4\sqrt{p-1}$	$4p$	2	$-2^{12}p^2$	I^*_3,I_2	**2 :** 1

2) l'entier $p-8$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	$\sqrt{p-8}$	-2	2	2^6p	III,I_1	**2 :** 2
B2	$-2\sqrt{p-8}$	p	2	-2^9p^2	I_0^*,I_2	**2:** 1
B1'	$-\sqrt{p-8}$	-2	2	2^6p	III,I_1	**2 :** 2
B2'	$2\sqrt{p-8}$	p	2	-2^9p^2	I_0^*,I_2	**2:** 1

3) l'entier $p+8$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$\sqrt{p+8}$	2	2	2^6p	III,I_1	**2 :** 2
C2	$-2\sqrt{p+8}$	p	2	2^9p^2	I_0^*,I_2	**2 :** 1
C1'	$-\sqrt{p+8}$	2	2	2^6p	III,I_1	**2 :** 2
C2'	$2\sqrt{p+8}$	p	2	2^9p^2	I_0^*,I_2	**2 :** 1

Corollaire. *Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $32p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si l'un des entiers $p-1$, $p-8$ et $p+8$ est un carré. Si tel est le cas, p est congru à 1 modulo 4.*

Théorème 6. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $64p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles il existe un entier k vérifiant les inégalités*

$$2 \leqslant k < f(p),$$

tel que l'une des conditions suivantes soit satisfaite :

1) l'entier $p-1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$2\sqrt{p-1}$	p	2	-2^6p^2	II,I_2	**2 :** 2
A2	$-4\sqrt{p-1}$	-4	2	$2^{12}p$	I_2^*,I_1	**2 :** 1
A1'	$-2\sqrt{p-1}$	p	2	-2^6p^2	II,I_2	**2 :** 2
A2'	$4\sqrt{p-1}$	-4	2	$2^{12}p$	I_2^*,I_1	**2 :** 1

2) l'entier $p-2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
B1	$2\sqrt{p-2^k}$	-2^k	2	$2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 2
B2	$-4\sqrt{p-2^k}$	$4p$	2	$-2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 1
B1'	$-2\sqrt{p-2^k}$	-2^k	2	$2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 2
B2'	$4\sqrt{p-2^k}$	$4p$	2	$-2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 1

3) l'entier $p+2^k$ est un carré, k est impair et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$2\sqrt{p+2^k}$	2^k	2	$2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 2
C2	$-4\sqrt{p+2^k}$	$4p$	2	$2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 1
C1'	$-2\sqrt{p+2^k}$	2^k	2	$2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 2
C2'	$4\sqrt{p+2^k}$	$4p$	2	$2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 1

4) l'entier k est pair, on a $p=2^{\frac{k}{2}+1}+1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
D1	$2(p+1)$	$4p$	4	$2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 2, 3, 4
D2	$4(2p-1)$	4	2	$2^{\frac{k}{2}+15}p$	$I^*_{\frac{k}{2}+5}$,I_1	**2:** 1
D3	$4(2-p)$	$4p^2$	2	$-2^{\frac{k}{2}+15}p^4$	$I^*_{\frac{k}{2}+5}$,I_4	**2 :** 1
D4	$-(p+1)$	$\frac{(p-1)^2}{4}$	2	$2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 1
D1'	$-2(p+1)$	$4p$	4	$2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 2, 3, 4
D2'	$-4(2p-1)$	4	2	$2^{\frac{k}{2}+15}p$	$I^*_{\frac{k}{2}+5}$,I_1	**2 :** 1
D3'	$-4(2-p)$	$4p^2$	2	$-2^{\frac{k}{2}+15}p^4$	$I^*_{\frac{k}{2}+5}$,I_4	**2 :** 1
D4'	$p+1$	$\frac{(p-1)^2}{4}$	2	$2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 1

5) l'entier $2^k - p$ est un carré, k est impair et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
E1	$2\sqrt{2^k - p}$	2^k	2	$-2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 2
E2	$-4\sqrt{2^k - p}$	$-4p$	2	$2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 1
E1'	$-2\sqrt{2^k - p}$	2^k	2	$-2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 2
E2'	$4\sqrt{2^k - p}$	$-4p$	2	$2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 1

6) l'entier k est pair, on a $p = 2^{\frac{k}{2}+1} - 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
F1	$-2(p-1)$	$-4p$	4	$2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 2, 3, 4
F2	$-4(2p+1)$	4	2	$2^{\frac{k}{2}+15}p$	$I^*_{\frac{k}{2}+5}$,I_1	**2 :** 1
F3	$4(p+2)$	$4p^2$	2	$2^{\frac{k}{2}+15}p^4$	$I^*_{\frac{k}{2}+5}$,I_4	**2 :** 1
F4	$p-1$	$\frac{(p+1)^2}{4}$	2	$-2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 1
F1'	$2(p-1)$	$-4p$	4	$2^{k+12}p^2$	I^*_{k+2},I_2	**2 :** 2, 3, 4
F2'	$4(2p+1)$	4	2	$2^{\frac{k}{2}+15}p$	$I^*_{\frac{k}{2}+5}$,I_1	**2 :** 1
F3'	$-4(p+2)$	$4p^2$	2	$2^{\frac{k}{2}+15}p^4$	$I^*_{\frac{k}{2}+5}$,I_4	**2 :** 1
F4'	$-(p-1)$	$\frac{(p+1)^2}{4}$	2	$-2^{2k+6}p$	I^*_{2k-4},I_1	**2 :** 1

Corollaire. *Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $64p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si il existe un entier k vérifiant les inégalités*

$$2 \leqslant k < f(p),$$

tel que l'un des entiers $p-1$, $p-2^k$, $p+2^k$ et $2^k - p$ soit un carré.

Théorème 7. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $128p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles l'une des conditions suivantes est satisfaite :*

1) il existe $k \in \{1, 2\}$ tel que $2p^k - 1$ soit un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$2\sqrt{2p^k-1}$	-1	2	2^7p^k	II,I_k	**2 :** 2
A2	$-4\sqrt{2p^k-1}$	$8p^k$	2	$-2^{14}p^{2k}$	III^*,I_{2k}	**2 :** 1
A1'	$-2\sqrt{2p^k-1}$	-1	2	2^7p^k	II,I_k	**2 :** 2
A2'	$4\sqrt{2p^k-1}$	$8p^k$	2	$-2^{14}p^{2k}$	III^*,I_{2k}	**2 :** 1
B1	$2\sqrt{2p^k-1}$	$2p^k$	2	-2^8p^{2k}	III,I_{2k}	**2 :** 2
B2	$-4\sqrt{2p^k-1}$	-4	2	$2^{13}p^k$	I_2^*,I_k	**2 :** 1
B1'	$-2\sqrt{2p^k-1}$	$2p^k$	2	-2^8p^{2k}	III,I_{2k}	**2 :** 2
B2'	$4\sqrt{2p^k-1}$	-4	2	$2^{13}p^k$	I_2^*,I_k	**2 :** 1

2) il existe un entier impair k vérifiant les inégalités $1 \leqslant k \leqslant 164969$, tel que $p^k + 2$ soit un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$2\sqrt{p^k+2}$	p^k	2	2^7p^{2k}	II, I_{2k}	**2 :** 2
C2	$-4\sqrt{p^k+2}$	8	2	$2^{14}p^k$	III^*, I_k	**2 :** 1
C1'	$-2\sqrt{p^k+2}$	p^k	2	2^7p^{2k}	II, I_{2k}	**2 :** 2
C2'	$4\sqrt{p^k+2}$	8	2	$2^{14}p^k$	III^*, I_k	**2 :** 1
D1	$2\sqrt{p^k+2}$	2	2	2^8p^k	III, I_k	**2 :** 2
D2	$-4\sqrt{p^k+2}$	$4p^k$	2	$2^{13}p^{2k}$	I_2^*, I_{2k}	**2 :** 1
D1'	$-2\sqrt{p^k+2}$	2	2	2^8p^k	III, I_k	**2 :** 2
D2'	$4\sqrt{p^k+2}$	$4p^k$	2	$2^{13}p^{2k}$	I_2^*, I_{2k}	**2 :** 1

3) l'entier $p-2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
E1	$2\sqrt{p-2}$	p	2	-2^7p^2	II, I_2	**2 :** 2
E2	$-4\sqrt{p-2}$	-8	2	$2^{14}p$	III^*, I_1	**2 :** 1
E1'	$-2\sqrt{p-2}$	p	2	-2^7p^2	II, I_2	**2 :** 2
E2'	$4\sqrt{p-2}$	-8	2	$2^{14}p$	III^*, I_1	**2 :** 1
F1	$2\sqrt{p-2}$	-2	2	2^8p	III, I_1	**2 :** 2
F2	$-4\sqrt{p-2}$	$4p$	2	$-2^{13}p^2$	I_2^*, I_2	**2 :** 1
F1'	$-2\sqrt{p-2}$	-2	2	2^8p	III, I_1	**2 :** 2
F2'	$4\sqrt{p-2}$	$4p$	2	$-2^{13}p^2$	I_2^*, I_2	**2 :** 1

Corollaire. *Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $128p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si il existe un entier impair k vérifiant les inégalités*

$$1 \leqslant k \leqslant 164969,$$

tel que l'un des entiers p^k+2, $2p-1$, $2p^2-1$ et $p-2$ soit un carré.

Théorème 8. *Les courbes elliptiques E définies sur $\mathbb{Q}$, de conducteur $256p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, sont celles pour lesquelles l'une des conditions suivantes est satisfaite :*

1) il existe $k \in \{1,2\}$ tel que $\frac{p^k-1}{2}$ soit un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
A1	$4\sqrt{\frac{p^k-1}{2}}$	-2	2	2^9p^k	III, I_k	**2 :** 2
A2	$-8\sqrt{\frac{p^k-1}{2}}$	$8p^k$	2	$-2^{15}p^{2k}$	III^*, I_{2k}	**2 :** 1
A1'	$-4\sqrt{\frac{p^k-1}{2}}$	-2	2	2^9p^k	III, I_k	**2 :** 2
A2'	$8\sqrt{\frac{p^k-1}{2}}$	$8p^k$	2	$-2^{15}p^{2k}$	III^*, I_{2k}	**2 :** 1
B1	$4\sqrt{\frac{p^k-1}{2}}$	$2p^k$	2	-2^9p^{2k}	III, I_{2k}	**2 :** 2
B2	$-8\sqrt{\frac{p^k-1}{2}}$	-8	2	$2^{15}p^k$	III^*, I_k	**2 :** 1
B1'	$-4\sqrt{\frac{p^k-1}{2}}$	$2p^k$	2	-2^9p^{2k}	III, I_{2k}	**2 :** 2
B2'	$8\sqrt{\frac{p^k-1}{2}}$	-8	2	$2^{15}p^k$	III^*, I_k	**2 :** 1

2) il existe $k \in \{1,2\}$ tel que l'entier $\frac{p^k+1}{2}$ soit un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques :

	a_2	a_4	$\lvert T_2\rvert$	Δ	Kodaira	Isogénies
C1	$4\sqrt{\frac{p^k+1}{2}}$	2	2	2^9p^k	III, I_k	**2 :** 2
C2	$-8\sqrt{\frac{p^k+1}{2}}$	$8p^k$	2	$2^{15}p^{2k}$	III^*, I_{2k}	**2 :** 1
C1'	$-4\sqrt{\frac{p^k+1}{2}}$	2	2	2^9p^k	III, I_k	**2 :** 2
C2'	$8\sqrt{\frac{p^k+1}{2}}$	$8p^k$	2	$2^{15}p^{2k}$	III^*, I_{2k}	**2 :** 1
D1	$4\sqrt{\frac{p^k+1}{2}}$	$2p^k$	2	2^9p^{2k}	III, I_{2k}	**2 :** 2
D2	$-8\sqrt{\frac{p^k+1}{2}}$	8	2	$2^{15}p^k$	III^*, I_k	**2 :** 1
D1'	$-4\sqrt{\frac{p^k+1}{2}}$	$2p^k$	2	2^9p^{2k}	III, I_{2k}	**2 :** 2
D2'	$8\sqrt{\frac{p^k+1}{2}}$	8	2	$2^{15}p^k$	III^*, I_k	**2 :** 1

Corollaire. *Il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $256p$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, si et seulement si l'un des entiers $\frac{p-1}{2}$, $\frac{p^2-1}{2}$, $\frac{p+1}{2}$ et $\frac{p^2+1}{2}$ est un carré.*

2. Lemmes préliminaires

2.1. Modèles de Weierstrass

Considérons une courbe elliptique E définie sur $\mathbb{Q}$, de conducteur 2^Np avec $N \geqslant 1$, ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. On utilisera dans toute la suite du texte le résultat suivant :

Lemme 1. *Il existe un modèle de Weierstrass de E de la forme*

$$y^2 = x(x^2 + ax + b), \tag{3}$$

où a et b sont des entiers sans diviseurs communs impairs. Ce modèle est minimal en dehors de 2. Les invariants standard c_4, c_6 et Δ qui lui sont associés sont

$$c_4 = 2^4(a^2 - 3b), \quad c_6 = 2^5a(9b - 2a^2) \quad et \quad \Delta = 2^4b^2(a^2 - 4b). \tag{4}$$

Dans le cas où l'on a $N \geqslant 2$, l'équation (3) est un modèle minimal de E.

Démonstration : Si $N = 1$ cet énoncé est une version particulière du lemme 1 de [Me-Oe].

Supposons $N \geqslant 2$, autrement dit, que E ait mauvaise réduction de type additif en 2. Considérons un modèle de Weierstrass minimal de E sur $\mathbb{Z}$

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

Posons comme dans [Ta],

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4 \quad \text{et} \quad b_6 = a_3^2 + 4a_6.$$

En effectuant le changement de variables

$$X = x \quad \text{et} \quad Y = y + \frac{a_1x + a_3}{2}, \tag{5}$$

On obtient comme nouveau modèle de E

$$Y^2 = X^3 + \frac{b_2}{4}\ X^2 + \frac{b_4}{2}\ X + \frac{b_6}{4}. \tag{6}$$

C'est un modèle entier de E. En effet, il résulte de l'hypothèse faite sur E que l'on a les congruences (cf. [Pa], tableau IV, p. 129)

$$c_4 \equiv 0 \text{ mod. } 16 \quad \text{et} \quad c_6 \equiv 0 \text{ mod. } 32.$$

D'après les égalités

$$c_4 = b_2^2 - 24b_4 \quad \text{et} \quad c_6 = -b_2^3 + 32b_2b_4 - 216b_6,$$

on a ainsi

$$b_2 \equiv 0 \text{ mod. } 4, \quad b_4 \equiv 0 \text{ mod. } 2 \quad \text{et} \quad b_6 \equiv 0 \text{ mod. } 4,$$

ce qui prouve notre assertion. Vu le changement de variables (5), le modèle (6) est donc minimal. Soit u l'abscisse d'un point d'ordre 2 de E dans ce modèle ; c'est un entier relatif. Le changement de variables

$$X = x + u \quad \text{et} \quad Y = y,$$

conduit alors à un modèle minimal de E de la forme $y^2 = x(x^2 + ax + b)$ où a et b sont des entiers. On vérifie que l'on a les formules (4) (cf. [Ta]). Le fait que E ait réduction semi-stable en dehors de 2 entraîne que a et b n'ont pas de diviseurs communs impairs. D'où le lemme.

2.2. Lemmes diophantiens

Dans ce paragraphe, la lettre p désigne un nombre premier impair. On explicite ici des résultats concernant certaines équations diophantiennes qui interviendront dans la suite.

Les lemmes 2 et 3 ci-dessous se trouvent respectivement dans les alinéas 1 et 2 du lemme p. 200 de [Had].

Lemme 2. *Soient m et n deux entiers naturels. Soit x un entier $\geqslant 1$ tel que l'on ait*

$$x^2 - 1 = 2^m p^n.$$

On est dans l'un des cas suivants :

1. $p = 3$ *et* $(x, m, n) \in \Big\{(2, 0, 1), (3, 3, 0), (5, 3, 1), (7, 4, 1), (17, 5, 2)\Big\}$;
2. $p = 5$ *et* $(x, m, n) \in \Big\{(3, 3, 0), (9, 4, 1)\Big\}$;
3. $p = 2^{m-2} + 1$ *avec* $m \geqslant 5$ *et* $(x, n) = \big(2p - 1, 1\big)$;
4. $p = 2^{m-2} - 1$ *avec* $m \geqslant 5$ *et* $(x, n) = \big(2p + 1, 1\big)$.

Lemme 3. *Soient m et n deux entiers naturels. Soit x un entier $\geqslant 1$ tel que l'on ait*

$$x^2 + 1 = 2^m p^n.$$

On est dans l'un des cas suivants :

1. $p \equiv 3$ mod. 4 *et* $(x, m, n) = (1, 1, 0)$;
2. $p = 13$ *et* $(x, m, n) \in \Big\{(5, 1, 1), (239, 1, 4)\Big\}$;
3. $p \neq 13$, $p \equiv 1$ mod. 4 *et* $(m, n) \in \Big\{(0, 1), (1, 1), (1, 2)\Big\}$.

Lemme 4. *Soient m et n deux entiers naturels $\geqslant 1$. Soit x un entier $\geqslant 2$ tel que l'on ait*

$$x^2 + 2^m = p^n.$$

On est dans l'un des cas suivants :

1. $p = 3$ *et* $(x, m, n) \in \Big\{(5, 1, 3), (7, 5, 4), (1, 3, 2)\Big\}$;
2. $p = 5$ *et* $(x, m, n) \in \Big\{(11, 2, 3), (3, 4, 2)\Big\}$;
3. $p = 2^{m-2} + 1$ *avec* $m \geqslant 5$ *et* $(x, n) = \big(p - 2, 2\big)$;
4. $n = 1$ *et* $m < \frac{\log(p)}{\log(2)}$.

Démonstration : Le cas où $n \geqslant 3$ est traité dans [Le]. Supposons $n = 2$. On a dans ce cas $(p - x)(x + p) = 2^m$. D'où l'existence de deux entiers naturels u et v tels que $u \geqslant v$, $p + x = 2^u$, $p - x = 2^v$ et $u + v = m$. On a $2p = 2^u + 2^v$, d'où $p = 2^{u-1} + 2^{v-1}$. Puisque

$u \geqslant v$ et que p est impair, on a $v = 1$. On a donc $m \geqslant 2$, $p = 2^{u-1} + 1$, puis $p = 2^{m-2} + 1$. On en déduit les triplets (x, m, n) intervenant dans l'énoncé du lemme lorsque $n = 2$. Si $n = 1$, $p - 2^m$ est positif, d'où $m < \frac{\log(p)}{\log(2)}$, et le lemme.

Lemme 5. *Soient m et n deux entiers naturels tels que $m \geqslant 2$ et $n \geqslant 1$. Soit x un entier naturel non nul tel que l'on ait*

$$x^2 - 2^m = p^n.$$

On est dans l'un des cas suivants :

1. *$p = 17$ et $(x, m, n) = (71, 7, 3)$;*
2. *$p = 2^{m-2} - 1$ avec $m \geqslant 4$ et $(x, n) = \big(p + 2, 2\big)$;*
3. *$n = 1$ et $m < f(p)$.*

Démonstration : Si l'on a $n \geqslant 3$, le corollaire 1 du chapitre I montre que l'assertion 1 est satisfaite.

Supposons $n = 2$. Dans ce cas, on a $(x + p)(x - p) = 2^m$. Par conséquent, puisque x et p sont des entiers positifs, il existe deux entiers naturels u et v vérifiant $u + v = m$ et $u \geqslant v$, tels que

$$p + x = 2^u \qquad \text{et} \qquad x - p = 2^v.$$

Cela conduit à $x = p + 2^v$ et à $p = 2^{u-1} - 2^{v-1}$. Comme les entiers u et v vérifient l'inégalité $u \geqslant v$ et que p est impair, ceci entraîne $v = 1$, puis $u = m - 1$. Par conséquent, on a

$$p = 2^{m-2} - 1 \qquad \text{et} \qquad x = p + 2,$$

ce qui entraîne en particulier $m \geqslant 4$.

Si l'on a $n = 1$, les corollaires 1 et 2 de [Beu] conduisent alors à la majoration de m se trouvant dans l'assertion 3.

Lemme 6. *Soient m et n deux entiers naturels $\geqslant 1$. Soit x un entier $\geqslant 1$ tel que l'on ait*

$$x^2 - 2^m = -p^n.$$

On est dans l'un des cas suivants :

1. *$p = 7$ et $(x, m, n) = (13, 9, 3)$;*
2. *$n = 1$ et $m < f(p)$.*

Démonstration : D'après le théorème p. 3204 de [Bu], l'entier n est impair. Si $n = 1$, la majoration de m résulte des corollaires 1 et 2 de [Beu]. Supposons $n \geqslant 3$; on a $m \geqslant 2$, et le corollaire 1 du chapitre I entraîne que l'assertion 1 est satisfaite.

Lemme 7. *Soient n et x des entiers naturels $\geqslant 1$.*

1. *Supposons que l'on ait*
$$2x^2 + 1 = p^n.$$
On est dans l'un des cas suivants :

(i) $p = 3$ et $(x, n) = (11, 5)$;

(ii) $n = 1$ ou 2.

2. *Supposons que l'on ait*
$$2x^2 - 1 = p^n.$$
On est dans l'un des cas suivants :

(i) $p = 23$ et $(x, n) = (78, 3)$;

(ii) $n = 1$ ou 2.

Démonstration : L'assertion 1 est une reformulation de l'alinéa 4 du lemme de [Had]. L'assertion 2 est une conséquence directe du corollaire 2 du chapitre I.

Lemme 8. *Supposons $p \geqslant 29$. Soient n et x des entiers $\geqslant 2$ tels que*
$$x^2 - 2 = p^n.$$
Alors, n est impair et on a $n \leqslant 164969$.

Démonstration : Dans toute la suite, pour tout $z \in \mathbb{C}$, on désigne par $|z|$ le module de z. Supposons qu'il existe deux entiers naturels non nuls x et n tels que l'on ait
$$x^2 - 2 = p^n.$$
Le fait que n soit impair se vérifie directement. Pour démontrer l'inégalité annoncée, nous allons utiliser des minorations de formes linéaires de logarithmes qui se trouvent dans [Mi].

Notons $\sqrt{2}$ la racine carrée positive de 2. Soient A l'anneau d'entiers de $\mathbb{Q}\big(\sqrt{2}\big)$ et u l'unité fondamentale de A. On a
$$u = \sqrt{2} - 1.$$
Dans A, on a
$$p^n = (x - \sqrt{2})(x + \sqrt{2}). \tag{7}$$
Puisque p est impair, il en est de même de x. Il en résulte que les entiers $x - \sqrt{2}$ et $x + \sqrt{2}$ sont premiers entre eux. De plus, 2 étant un carré modulo p, l'entier p est décomposé dans $\mathbb{Q}(\sqrt{2})$. Il existe ainsi deux éléments irréductibles conjugués et positifs π_1 et π_2 de A vérifiant les conditions suivantes :

1. on a $p = \pi_1\pi_2$;
2. il existe deux entiers relatifs t et k vérifiant $0 \leqslant t < n$ tels que l'on ait

$$x + \sqrt{2} = u^{t+kn}\pi_1^n \quad \text{et} \quad x - \sqrt{2} = (-u)^{-t-kn}\pi_2^n. \tag{8}$$

Pour tout nombre réel x non nul, on note $\log x$ le logarithme de x : si $x > 0$, c'est le logarithme usuel ; si $x < 0$ on le définit par l'égalité

$$\log x = \log|x| \ + \ i\pi.$$

En suivant les notations de [Mi], posons

$$b_1 = t, \quad b_2 = n, \quad \alpha_1 = -\frac{1}{u^2}, \quad \alpha_2 = (-1)^k u^{2k}\frac{\pi_1}{\pi_2} \quad \text{et} \quad \Lambda = t\ \log\alpha_1 - n\ \log\alpha_2. \tag{9}$$

En utilisant la remarque 4 p. 111 de *loc. cit.* avec la forme linéaire de logarithme Λ, on va démontrer l'inégalité

$$\log|\Lambda| \geqslant -634,304\left(\operatorname{Max}\left\{0,06 + \log\left(\frac{n}{\log p + 3,604} + \frac{n}{3,604}\right), \frac{21}{2}\right\}\right)^2 \times \left(\frac{\log p}{2} + 1,802\right). \tag{10}$$

Par ailleurs, on va prouver l'inégalité

$$\log|\Lambda| \leqslant \log 2\sqrt{2} - \frac{n}{2}\log p + 0,103. \tag{11}$$

On déduit alors de (10) et (11) la majoration de n indiquée dans l'énoncé du lemme.

Commençons par démontrer l'inégalité (11). On a

$$\Lambda = \log\left(\frac{\alpha_1^t}{\alpha_2^n}\right).$$

Posons

$$\alpha = \frac{2\sqrt{2}}{u^{t+kn}\pi_1^n}.$$

On a

$$\frac{\alpha_1^t}{\alpha_2^n} = 1 - \alpha.$$

Puisque $x \geqslant 2$, on a $u^{t+kn}\pi_1^n = x + \sqrt{2} \geqslant 2 + \sqrt{2} \geqslant 2\sqrt{2}$, d'où

$$\alpha \leqslant 1.$$

On en déduit que

$$|\Lambda| = -\log\bigl(1-\alpha\bigr).$$

Il en résulte l'inégalité

$$|\Lambda| \leqslant \frac{\alpha}{1-\alpha}.$$

Par ailleurs, on a

$$\frac{\alpha}{1-\alpha} = \frac{2\sqrt{2}}{u^{t+kn}\pi_1^n - 2\sqrt{2}}.$$

D'après (7), on a

$$u^{t+kn}\pi_1^n \geqslant p^{\frac{n}{2}},$$

d'où l'on déduit l'inégalité

$$\log|\Lambda| \leqslant \log\left(\frac{2\sqrt{2}}{p^{\frac{n}{2}} - 2\sqrt{2}}\right).$$

On obtient ainsi

$$\log|\Lambda| \leqslant \log 2\sqrt{2} - \frac{n}{2}\log p - \log\left(1 - \frac{2\sqrt{2}}{p^{\frac{n}{2}}}\right).$$

Les inégalités $p \geqslant 29$ et $n \geqslant 2$ entraînent alors (11).

Démontrons maintenant l'inégalité (10). Vérifions pour cela les deux conditions suivantes :

3. les nombres réels α_1 et α_2 sont multiplicativement indépendants ;
4. on a $|\alpha_1| \geqslant 1$ et $|\alpha_2| \geqslant 1$.

Supposons qu'il existe deux entiers relatifs n_1 et n_2 tels que l'on ait

$$\alpha_1^{n_1}\alpha_2^{n_2} = 1.$$

En considérant la valuation en π_1 des deux membres de cette égalité, on constate que $n_2 = 0$. Par suite, on a $\alpha_1^{n_1} = 1$, d'où $n_1 = 0$ et l'assertion 3. On a $|\alpha_1| \geqslant 1$. Par ailleurs, l'inégalité

$$\bigl|x + \sqrt{2}\bigr| \geqslant \bigl|x - \sqrt{2}\bigr||u^{2t}|,$$

entraîne

$$\left|\frac{u^{2kn}\pi_1^n}{\pi_2^n}\right| \geqslant 1,$$

d'où $|\alpha_2| \geqslant 1$ et l'assertion 4.

Déterminons les constantes qui interviennent dans la remarque 4 de [Mi] dont on reprend les notations sans autre précision. On a $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}\bigl(\sqrt{2}\bigr)$, d'où

$$D = 2.$$

Il s'agit ensuite de choisir des nombres réels A_i, pour $i \in \{1,2\}$, tels que l'on ait

$$\log A_i \geqslant \mathrm{Max}\left\{h(\alpha_i), \frac{|\log \alpha_i|}{2}, \frac{1}{2}\right\},$$

où $h(\alpha_i)$ est la hauteur logarithmique absolue de α_i.

On vérifie que l'on a $h(\alpha_1) = -\log u$, d'où $h(\alpha_1) \approx 0,8813$. De plus $|\log(\alpha_1)/2| \approx 1,8011$, de sorte que l'on peut prendre

$$\log A_1 = 1,802.$$

Calculons $h(\alpha_2)$. La norme sur $\mathbb{Q}$ de α_2 est égale à 1 ; en utilisant l'assertion 4 ci-dessus, on vérifie que l'on a

$$h(\alpha_2) = \frac{\log |\alpha_2|}{2}.$$

Démontrons que l'on a

$$h(\alpha_2) \leqslant \frac{\log p}{2} + 0,882. \tag{12}$$

On a $|\alpha_2| = \left|u^{2k}\frac{\pi_1}{\pi_2}\right|$. On déduit de $p = \pi_1\pi_2$ que l'on a

$$|\alpha_2| = p\left|\frac{u^{2k}}{\pi_2^2}\right|.$$

Remarquons que puisque l'on a $p \geqslant 29$, l'entier x est supérieur ou égal à 3, ce qui entraîne $x - \sqrt{2} > 1$. Il résulte alors de (8) que l'on a

$$\left|\frac{u^{2k}}{\pi_2^2}\right| \leqslant |u|^{-\frac{2t}{n}},$$

d'où

$$\log |\alpha_2| \leqslant \log p + \frac{2t}{n}\log\frac{1}{u},$$

puis

$$\log |\alpha_2| \leqslant \log p + 1,763,$$

ce qui conduit à l'inégalité (12).

Il reste à majorer $|\log \alpha_2|$. D'après (9), on a les égalités

$$\log \alpha_2 = \log(-1)^k + \log |\alpha_2| = i\pi + \log |\alpha_2|.$$

On obtient alors

$$|\log \alpha_2| \leqslant \log p + |1,763 + i\pi| \leqslant \log p + 3,603,$$

de sorte que

$$\frac{|\log \alpha_2|}{2} \leqslant \frac{\log p}{2} + 1,802.$$

Il en résulte que l'on peut prendre

$$\log A_2 = \frac{\log p}{2} + 1,802.$$

La remarque 4 de [Mi] conduit alors à l'inégalité

$$\log|\Lambda| \geqslant -352\left(\operatorname{Max}\left\{0,06 + \log\left(\frac{t}{\log p + 3,604} + \frac{n}{3,604}\right), \frac{21}{2}\right\}\right)^2 \times 1,802\left(\frac{\log p}{2} + 1,802\right).$$

L'inégalité (10) résulte alors du fait que l'on a $t \leqslant n$.

Posons

$$A = \operatorname{Max}\left\{0,06 + \log\left(\frac{n}{\log p + 3,604} + \frac{n}{3,604}\right), \frac{21}{2}\right\}.$$

Les inégalités (10) et (11) entraînent que l'on a

$$\log 2\sqrt{2} - \frac{\log p}{2}n + 0,103 \geqslant -634,304\ A^2\ \times\left(\frac{\log p}{2} + 1,802\right),$$

d'où

$$\log 2\sqrt{2} + 0,103 + 634,304\ A^2\ \times\left(\frac{\log p}{2} + 1,802\right) \geqslant \frac{\log p}{2}n,$$

et

$$2\left(\frac{\log 2\sqrt{2} + 0,103}{\log p}\right) + 634,304\ A^2\ \times\left(1 + \frac{3,604}{\log p}\right) \geqslant n.$$

Puisque l'on a $p \geqslant 29$, on a

$$2\left(\frac{\log 2\sqrt{2} + 0,103}{\log 29}\right) \geqslant 2\left(\frac{\log 2\sqrt{2} + 0,103}{\log p}\right), \qquad 1 + \frac{3,604}{\log 29} \geqslant 1 + \frac{3,604}{\log p},$$

$$\operatorname{Max}\left\{0,06 + \log\left(\frac{n}{\log 29 + 3,604} + \frac{n}{3,604}\right), \frac{21}{2}\right\} \geqslant A.$$

On en déduit l'inégalité

$$0,679 + 1313,197\ \operatorname{Max}\left\{0,06 + \log\left(\frac{n}{\log 29 + 3,604} + \frac{n}{3,604}\right), \frac{21}{2}\right\}^2 \geqslant n. \tag{13}$$

Supposons $n \geqslant 81254$.

$$\operatorname{Max}\left\{0,06 + \log\left(\frac{n}{\log 29 + 3,604} + \frac{n}{3,604}\right), \frac{21}{2}\right\} = 0,06 + \log\left(\frac{n}{\log 29 + 3,604} + \frac{n}{3,604}\right).$$

D'après (13), on a ainsi

$$0,679 + 1313,197\left(0,06 + \log\left(\frac{n}{\log 29 + 3,604} + \frac{n}{3,604}\right)\right)^2 \geqslant n.$$

Cela entraîne l'inégalité

$$n \leqslant 164969.$$

D'où le lemme.

3. Démonstration des résultats

3.1. Principe de la démonstration

On démontre d'abord que les courbes elliptiques se trouvant dans les énoncés des théorèmes 1 à 8 vérifient bien les propriétés voulues. On utilise pour cela la classification obtenue par I. Papadopoulos (cf. [Pa]) des types de Néron des courbes elliptiques en fonction de leurs invariants minimaux. On explicite ensuite toutes les classes de $\mathbb{Q}$-isomorphisme possibles de courbes elliptiques définies sur $\mathbb{Q}$, de conducteur $2^N p$ (avec $N \geqslant 1$) et possédant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. Le lemme 1 permet de ramener ce problème à la recherche des entiers a et b sans diviseurs premiers communs impairs, pour lesquels il existe des entiers naturels m et n vérifiant l'égalité

$$b^2(a^2 - 4b) = \pm 2^m p^n.$$

Les lemmes diophantiens permettent la détermination de ces entiers. On en déduit alors que, à $\mathbb{Q}$-isomorphisme près, les courbes elliptiques indiquées dans les théorèmes 1 à 8 sont les seules à avoir les propriétés annoncées.

3.2. Les courbes elliptiques intervenant dans les énoncés des théorèmes

Dans cette partie, nous allons démontrer que les courbes elliptiques figurant dans les énoncés des théorèmes 1 à 8 vérifient bien les propriétés annoncées.

Pour cela, il nous faut vérifier :

(i) que les modèles indiqués dans les tableaux sont entiers ;

(ii) les factorisations indiquées dans la colonne Δ ;

(iii) l'ordre du groupe T_2 ;

(iv) les informations données dans la colonne isogénies ;

(v) que le conducteur des courbes elliptiques est bien celui annoncé ;

(vi) que les modèles se trouvant dans les tableaux sont minimaux ;

(vii) les symboles de Kodaira indiqués.

1. En ce qui concerne les théorèmes 2 à 8, le point (i) se vérifie directement à partir des conditions précédant chaque tableau. Pour les modèles se trouvant dans l'énoncé du théorème 1, on utilise de plus la condition (2).

2. Pour le point (iii), on vérifie que les courbes elliptiques indiquées dans l'énoncé des résultats ont toutes au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. On a donc $|T_2| = 4$ si le discriminant de l'équation considérée est un carré et $|T_2| = 2$ sinon.

Considérons alors une courbe elliptique E intervenant dans l'un des énoncés des théorèmes 1 à 8 et donnée par l'équation

$$E \ : \ y^2 \ + \ a_1 \ xy \ = \ x^3 \ + \ a_2 \ x^2 \ + \ a_4 \ x \ + \ a_6,$$

où les a_i sont dans $\mathbb{Z}$. Soient b_2, b_4, b_6, b_8, c_4, c_6 et Δ les invariants standard qui lui sont associés par les formules qui se trouvent dans [Ta], p. 36.

3. Les factorisations indiquées dans la colonne Δ des tableaux se déduisent de *loc. cit.*. Dans certains cas, on est amené à utiliser la remarque ci-dessous :

Remarque 1. Soit k un entier naturel pair.

(i) l'entier $p + 2^k$ est un carré si et seulement si $p = 2^{\frac{k}{2}+1} + 1$;

(ii) l'entier $2^k - p$ est un carré si et seulement si $p = 2^{\frac{k}{2}+1} - 1$.

En effet, soit u l'entier positif tel que $p + 2^k = u^2$. On a $(u + 2^{\frac{k}{2}})(u - 2^{\frac{k}{2}}) = p$, de sorte que $u + 2^{\frac{k}{2}} = p$ et $u - 2^{\frac{k}{2}} = 1$, puis $p - 1 = 2^{\frac{k}{2}+1}$. De même, soit v l'entier positif tel que $2^k - p = v^2$. On a $(2^{\frac{k}{2}} + v)(2^{\frac{k}{2}} - v) = p$, d'où $2^{\frac{k}{2}} + v = p$, $2^{\frac{k}{2}} - v = 1$ et $p + 1 = 2^{\frac{k}{2}+1}$. Les implications réciproques sont immédiates.

4. Les informations qui se trouvent dans la colonne Isogénies des tableaux s'obtiennent à partir des résultats de J. Vélu [Ve2]. Plus précisément, si P est un point d'ordre 2 de E, notons $< P >$ le sous-groupe de E engendré par P. Il existe une courbe elliptique $E/ < P >$ sur $\mathbb{Q}$, unique à $\mathbb{Q}$-isomorphisme près, qui est liée à E par une isogénie sur $\mathbb{Q}$ de degré 2 et de noyau $< P >$. Nous indiquons dans les tableaux ci-dessous, en utilisant les résultats de *loc. cit.*, une équation de $E/ < P >$. Les isogénies indiquées dans l'énoncé des résultats se déduisent alors de ces tableaux par spécialisation des paramètres a et b. On utilise les tableaux des alinéas 1 et 2 pour le théorème 1 et les tableaux des alinéas 3 et 4 pour les autres théorèmes.

Lemme 9.

1) Supposons qu'il existe a et b dans $\mathbb{Z}$ tels que E ait pour modèle de Weierstrass

$$y^2 \ + \ xy \ = \ x^3 \ + \ a \ x^2 \ + \ b \ x.$$

Le point $(0,0)$ *est d'ordre* 2 *dans* $E(\mathbb{Q})$ *et une équation de* $E/<(0,0)>$ *est donnée ci-dessous :*

	a_1	a_2	a_4	a_6	Isogénies
E	1	a	b	0	**2 :** 2
$E/<(0,0)>$	1	a	$-4b$	$-b(1+4a)$	**2 :** 1

2) Supposons qu'il existe a *et* b *dans* $\mathbb{Z}$ *tels que* E *ait pour modèle de Weierstrass*

$$y^2 \ + \ xy \ = \ x^3 \ + \ a\,x^2 \ + \ \frac{a}{4}\,x.$$

Les points $(0,0)$, $(-\frac{1}{4},\frac{1}{8})$ *et* $(-a,\frac{a}{2})$ *sont d'ordre* 2 *dans* $E(\mathbb{Q})$ *et l'on a le tableau ci-dessous :*

	a_1	a_2	a_4	a_6	Isogénies
E	1	a	$\frac{a}{4}$	0	**2 :** 2, 3, 4
$E/<(0,0)>$	1	$-2a$	$\frac{a}{2}(2a-3)$	$\frac{a}{4}(a-1)$	**2 :** 1
$E/<(-\frac{1}{4},\frac{1}{8})>$	1	$-\frac{a}{2}$	$\frac{a^2}{16}$	0	**2 :** 1
$E/<(-a,\frac{a}{2})>$	1	$4a$	$2a$	$\frac{a}{4}$	**2 :** 1

3) Supposons qu'il existe a et b dans $\mathbb{Z}$ tels que E ait pour modèle de Weierstrass

$$y^2 \ = \ x^3 \ + \ a\,x^2 \ + \ b\,x.$$

Le point $(0,0)$ est d'ordre 2 dans $E(\mathbb{Q})$ et une équation de $E/<(0,0)>$ est donnée ci-dessous :

	a_1	a_2	a_4	a_6	Isogénies
E	0	a	b	0	**2 :** 2
$E/<(0,0)>$	0	$-2a$	a^2-4b	0	**2 :** 1

4) Supposons qu'il existe a et b dans $\mathbb{Z}$ tels que E ait pour modèle de Weierstrass

$$y^2 \ + \ xy \ = \ x^3 \ - \ (a+b)\,x^2 \ + \ ab\,x.$$

Les points $(0,0)$, $(a,0)$ et $(b,0)$ sont d'ordre 2 dans $E(\mathbb{Q})$ et l'on a le tableau ci-dessous :

	a_1	a_2	a_4	a_6	Isogénies
E	0	$-(a+b)$	ab	0	**2 :** 2, 3, 4
$E/<(0,0)>$	0	$\frac{a+b}{2}$	$\frac{(a-b)^2}{16}$	0	**2 :** 1
$E/<(a,0)>$	0	$2(b-2a)$	b^2	0	**2 :** 1
$E/<(b,0)>$	0	$2(a-2b)$	a^2	0	**2 :** 1

Démonstration : 1) L'alinéa 1 s'obtient directement à partir des formules de [Ve2].

2) Vérifions les assertions relatives à l'alinéa 2. On vérifie directement que les points indiqués sont d'ordre 2 dans $E(\mathbb{Q})$. Soit P l'un de ces points. L'équation de $E/<P>$ que l'on obtient en utilisant les formules de Vélu est :

$$y^2 + xy = x^3 + a\,x^2 - a\,x - (1+4a)\frac{a}{4} \qquad \text{si} \quad P=(0,0),$$

$$y^2 + xy = x^3 + a\,x^2 + \left(\frac{3}{2}a - \frac{5}{16}\right)x + a^2 - \frac{7}{16}a + \frac{3}{64} \qquad \text{si} \quad P=\left(-\frac{1}{4},\frac{1}{8}\right),$$

$$y^2 + xy = x^3 + a\,x^2 - \left(5a^2 - \frac{3}{2}a\right)x + 3a^3 - \frac{7}{4}a^2 + \frac{1}{4}a \qquad \text{si} \quad P=\left(-a,\frac{a}{2}\right).$$

Les changements de variables

$$x = X - a, \qquad y = Y + \frac{a}{2} \quad \text{si} \quad P=(0,0),$$

$$x = 4X + \frac{1}{4} - a, \qquad y = 8Y + 2X + \frac{a}{2} - \frac{1}{8} \quad \text{si} \quad P=\left(-\frac{1}{4},\frac{1}{8}\right),$$

$$x = X + a, \qquad y = Y - \frac{a}{2} \quad \text{si} \quad P=\left(-a,\frac{a}{2}\right),$$

conduisent alors aux équations indiquées dans le tableau.

3) En ce qui concerne l'alinéa 3, une équation de $E/<(0,0)>$ est

$$y^2 = x^3 + a\,x^2 - 4b\,x - 4ab.$$

Le changement de variables

$$x = X - a, \qquad y = Y,$$

conduit alors au modèle indiqué.

4) Vérifions les assertions relatives à l'alinéa 4. Soit P l'un des points d'ordre 2 indiqués dans l'énoncé. L'équation de $E/<P>$ obtenue en utilisant les formules de Vélu est :

$$y^2 = x^3 - (a+b)\,x^2 - 4ab\,x + 4ab(a+b) \qquad \text{si} \quad P=(0,0),$$

$$y^2 = x^3 - (a+b)\,x^2 + a(6b-5a)\,x + a(7ab-4b^2-3a^2) \qquad \text{si} \quad P=(a,0),$$

$$y^2 = x^3 - (a+b)\,x^2 + b(6a-5b)\,x + b(7ab-4a^2-3b^2) \qquad \text{si} \quad P=(b,0).$$

Les changements de variables

$$x = 4X + a + b, \qquad y = 8Y \quad \text{si} \quad P=(0,0),$$

$$x = X + b - a, \qquad y = Y \quad \text{si} \quad P=(a,0),$$

$$x = X + a - b, \qquad y = Y \quad \text{si} \quad P=(b,0),$$

entraînent alors le résultat.

Cela termine la démonstration du lemme 9.

5. Compte tenu de ce qui précède, il nous reste à vérifier les points (v) à (vii). On utilise pour cela les résultats de [Pa]. Après avoir vérifié que le conducteur de E est bien celui annoncé, les symboles de Kodaira et la minimalité du modèle considéré se déduisent des tableaux de *loc. cit.*.

La suite de ce paragraphe est donc désormais consacrée à la détermination du conducteur de E. Le calcul des invariants c_4, c_6 et Δ montre que E a bonne réduction en dehors de 2 et p, et que E a réduction multiplicative en p. Par suite, le conducteur de E est de la forme $2^N p$ où N est un entier tel que $0 \leqslant N \leqslant 8$. Deux courbes elliptiques sur $\mathbb{Q}$ qui sont $\mathbb{Q}$-isogènes ont le même conducteur. Par suite, il nous suffira de choisir pour E une seule courbe elliptique parmi celles identifiées par la même lettre dans les énoncés des théorèmes.

Dans toute la suite, étant donné un entier relatif n, on désignera par $v(n)$ sa valuation 2-adique.

3.2.1. Le théorème 1

On est amené à déterminer les conducteurs des courbes elliptiques notées A1, B1, C1, D1 et E1 dans l'énoncé du théorème 1. Soit k un entier naturel vérifiant les inégalités $7 \leqslant k < f(p)$. Les invariants standard de ces courbes sont donnés dans le tableau suivant :

	A1	B1	C1	D1	E1
c_4	$p - 2^{k-2}$	$p + 2^{k-2}$	$p + 2^{k+2}$	$2^{k-2} - p$	$2^{k+2} - p$
Δ	$2^{2k-12}p$	$2^{2k-12}p$	$2^{k-6}p^2$	$-2^{2k-12}p$	$2^{k-6}p^2$

On constate alors que les entiers c_4 et Δ sont premiers entre eux. Ces courbes ont donc réduction multiplicative en 2 et p et leur conducteur est $2p$.

3.2.2. Le théorème 2.

Vérifions que la courbe elliptique A1 est de conducteur $4p$. On a

$$c_4 = 2^4(p-1), \qquad c_6 = -2^5\sqrt{p-4}(2p+1) \qquad \text{et} \qquad \Delta = 2^4 p.$$

On en déduit que $v(c_4) = 6$, $v(c_6) = 5$ et $v(\Delta) = 4$. D'après le tableau IV p. 129 de [Pa], on est dans le cas 3 ou 5 de Tate. Utilisons la proposition 1 p. 124 de *loc. cit.* avec $r = t = 1$. On a $r^2 - 1 = 0$ et $t^2 - \sqrt{p-4}$ est pair. D'après la condition (2), 4 divise $-1 + \sqrt{p-4}$. On est donc dans le cas 5 de Tate, d'où l'assertion.

3.2.3. Le théorème 3

1) Vérifions que la courbe elliptique A1 est de conducteur $8p$. On a

$$a_1 = 0, \quad a_2 = \sqrt{p-16}, \quad a_3 = 0, \quad a_4 = -4, \quad a_6 = 0,$$

$$b_2 = 4\sqrt{p-16}, \quad b_4 = -2^3, \quad b_6 = 0, \quad b_8 = -2^4,$$

$$c_4 = 2^4(p-4), \qquad c_6 = -2^6\sqrt{p-16}(p+2), \qquad \Delta = 2^8 p.$$

On a

$$v(c_4) = 4, \qquad v(c_6) = 6, \qquad v(\Delta) = 8.$$

D'après le tableau IV p. 129 de [Pa], on est dans le cas de Tate 6, 7 ou 8. Utilisons les propositions 3 et 4 de *loc. cit.*. Posons $r = 2$ et $t = 2$. On a la congruence

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

Par ailleurs, en utilisant la condition (2), on vérifie que l'on a

$$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv 0 \text{ mod. } 16.$$

On est donc dans un cas de Tate $\geqslant 7$. De plus, si s est un entier, on a

$$a_2 + 3r - sa_1 - s^2 \equiv \sqrt{p-16} + 2 - s^2 \equiv 3 - s^2 \text{ mod. } 4.$$

Il n'existe donc pas d'entier s tel que $a_2 + 3r - s^2 \equiv 0$ mod. 4. On est donc dans le cas de Tate 7 et le conducteur de A1 est $8p$.

2) Vérifions que la courbe elliptique B1 est de conducteur $8p$. On a

$$a_1 = 0, \quad a_2 = \sqrt{p-32}, \quad a_3 = 0, \quad a_4 = -8, \quad a_6 = 0,$$

$$b_2 = 4\sqrt{p-32}, \quad b_4 = -2^4, \quad b_6 = 0, \quad b_8 = -2^6,$$
$$c_4 = 2^4(p-8), \qquad c_6 = -2^6\sqrt{p-32}\ (p+4), \qquad \Delta = 2^{10}p.$$

On a

$$v(c_4) = 4, \qquad v(c_6) = 6, \qquad v(\Delta) = 10.$$

On est dans le cas de Tate 7 ou 9. Utilisons la proposition 4 de *loc. cit.*. L'entier $r = 4$ vérifie la congruence

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

L'entier $s = 1$ vérifie la congruence $a_2 + 3r - sa_1 - s^2 \equiv 0$ mod. 4. On est donc dans le cas de Tate 9, d'où l'assertion.

3) Vérifions que la courbe elliptique C1 est de conducteur $8p$. On a

$$a_1 = 0, \quad a_2 = \sqrt{p+32}, \quad a_3 = 0, \quad a_4 = 8, \quad a_6 = 0,$$

$$b_2 = 4\sqrt{p+32}, \quad b_4 = 2^4, \quad b_6 = 0, \quad b_8 = -2^6,$$
$$c_4 = 2^4(p+8), \qquad c_6 = -2^6\sqrt{p+32}\ (p-4), \qquad \Delta = 2^{10}p.$$

On a

$$v(c_4) = 4, \qquad v(c_6) = 6, \qquad v(\Delta) = 10.$$

On est dans le cas de Tate 7 ou 9. Comme ci-dessus, l'entier $r = 4$ vérifie la congruence

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

L'entier $s = 1$ vérifie donc la congruence $a_2 + 3r - sa_1 - s^2 \equiv 0$ mod. 4. On est dans le cas de Tate 9, d'où le résultat.

4) Supposons que p soit égal à 31. Dans ce cas, on vérifie par exemple à l'aide du logiciel de calculs PARI (cf. [Pari]) que le conducteur de D1 est $8 \times 31 = 248$.

3.2.4. Le théorème 4

Soit k un entier naturel vérifiant les inégalités $4 \leqslant k < f(p)$.

1) Vérifions que la courbe A1 est de conducteur $16p$. On a

$$a_1 = 0, \quad a_2 = -\sqrt{p-2^k}, \quad a_3 = 0, \quad a_4 = -2^{k-2}, \quad a_6 = 0,$$

$$b_2 = -4\sqrt{p-2^k}, \quad b_4 = -2^{k-1}, \quad b_6 = 0, \quad b_8 = -2^{2k-4},$$
$$c_4 = 2^4(p-2^{k-2}), \qquad c_6 = 2^6\sqrt{p-2^k}\ (p+2^{k-3}) \quad \text{et} \quad \Delta = 2^{2k}p.$$

On a

$$v(c_4) = 4, \qquad v(c_6) = 6 \quad \text{et} \quad v(\Delta) = 2k.$$

On est dans un cas de Tate $\geqslant 6$. On utilise les propositions 3 et 4 de [Pa].

1.1) Supposons $k = 4$. L'entier $r = 2$ vérifie la congruence

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

Avec $t = 2$, on a

$$v(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1) = 3.$$

On est alors dans le cas 6 de Tate et le conducteur de A1 est $16p$.

1.2) Supposons $k \geqslant 5$. On est dans un cas de Tate $\geqslant 7$. L'entier $r = 4$ vérifie la congruence

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

Par ailleurs, il n'existe pas d'entier s vérifiant la congruence

$$a_2 + 3r - sa_1 - s^2 \equiv 0 \text{ mod. } 4.$$

On est donc dans le cas 7 de Tate et le conducteur de $A1$ est $16p$.

2) Vérifions que la courbe B1 est de conducteur $16p$. La démonstration est la même que celle de l'alinéa 1.2) ci-dessus. On a

$$c_4 = 2^4(p + 2^{k-2}), \qquad c_6 = 2^6\sqrt{p + 2^k}\ (p - 2^{k-3}) \quad \text{et} \quad \Delta = 2^{2k}p,$$

d'où

$$v(c_4) = 4, \qquad v(c_6) = 6 \quad \text{et} \quad v(\Delta) = 2k,$$

et l'on est dans un cas de Tate $\geqslant 7$. La proposition 4 de [Pa], utilisée avec $r = 4$, entraîne alors notre assertion.

3) Vérifions que la courbe elliptique C1 est de conducteur $16p$. On a

$$a_1 = 0, \quad a_2 = p + 1, \quad a_3 = 0, \quad a_4 = p, \quad a_6 = 0,$$

$$b_2 = 4(p + 1), \quad b_4 = 2p, \quad b_6 = 0, \quad b_8 = -p^2,$$

$$c_4 = 2^4(p^2 - p + 1), \qquad c_6 = -2^5(p + 1)(2p^2 - 5p + 2) \quad \text{et} \quad \Delta = 2^{k+6}p^2.$$

On a

$$v(c_4) = 4, \qquad v(c_6) = 6 \quad \text{et} \quad v(\Delta) = k + 6.$$

On est dans un cas de Tate $\geqslant 7$. L'entier $r = -1$, vérifie la congruence

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

Par ailleurs, il n'existe pas d'entier s vérifiant la congruence $a_2+3r-sa_1-s^2 \equiv 0$ mod. 4. D'après la proposition 4 de [Pa], on est dans le cas 7 de Tate, ce qui entraîne notre assertion.

4) Vérifions que la courbe elliptique D1 est de conducteur $16p$. On a

$$a_1 = 0, \quad a_2 = -\sqrt{p-4}, \quad a_3 = 0, \quad a_4 = -1, \quad a_6 = 0,$$

$$c_4 = 2^4(p-1), \qquad c_6 = 2^5\sqrt{p-4}\ (2p+1) \quad \text{et} \quad \Delta = 2^4 p.$$

On a

$$v(c_4) = 6, \qquad v(c_6) = 5 \quad \text{et} \quad v(\Delta) = 4.$$

On est dans un cas de Tate 3 ou 5. Utilisons la proposition 1 de *loc. cit.* avec $r = t = 1$. Les entiers $a_4 + r^2$ et $t^2 + a_4a_2 - a_6$ sont pairs. De plus d'après la condition (2), 4 ne divise pas $a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$. On est donc dans le cas 3 de Tate, d'où l'assertion.

5) Vérifions que la courbe elliptique E1 est de conducteur $16p$. La démonstration est la même que celle de l'alinéa 1.2) ci-dessus. On a

$$c_4 = 2^4(2^{k-2} - p), \qquad c_6 = -2^6\sqrt{2^k - p}\ (p + 2^{k-3}) \quad \text{et} \quad \Delta = -2^{2k}p,$$

d'où

$$v(c_4) = 4, \qquad v(c_6) = 6 \quad \text{et} \quad v(\Delta) = 2k,$$

et l'on est dans un cas de Tate $\geqslant 7$. La proposition 4 de [Pa], utilisée avec $r = 4$, entraîne alors notre assertion.

6) Vérifions que la courbe elliptique F1 est de conducteur $16p$. On a

$$a_1 = 0, \quad a_2 = 1 - p, \quad a_3 = 0, \quad a_4 = -p, \quad a_6 = 0,$$

$$b_2 = 4(1-p), \quad b_4 = -2p, \quad b_6 = 0, \quad b_8 = -p^2,$$

$$c_4 = 2^4(p^2 + p + 1), \qquad c_6 = 2^5(p-1)(2p^2 + 5p + 2) \quad \text{et} \quad \Delta = 2^{k+6}p^2.$$

On a

$$v(c_4) = 4, \qquad v(c_6) = 6 \quad \text{et} \quad v(\Delta) = k + 6.$$

On est dans un cas de Tate $\geqslant 7$. L'entier $r = -1$, vérifie la congruence

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

Il n'existe pas d'entier s tel que $a_2 + 3r - sa_1 - s^2 \equiv 0$ mod. 4, donc on est dans le cas 7 de Tate et le conducteur de F1 est $16p$.

3.2.5. Le théorème 5

1) Vérifions que la courbe A1 est de conducteur $32p$. On a

$$a_1 = 0, \quad a_2 = 2\sqrt{p-1}, \quad a_3 = 0, \quad a_4 = -1, \quad a_6 = 0,$$

$$c_4 = 2^4(4p-1), \qquad c_6 = -2^6\sqrt{p-1}\ (8p+1) \quad \text{et} \quad \Delta = 2^6 p.$$

On a

$$v(c_4) = 4, \qquad v(c_6) \geqslant 6 \quad \text{et} \quad v(\Delta) = 6.$$

On est donc dans le cas 3 ou 4 de Tate. Posons $r = 1$ et $t = 0$. Les entiers $a_4 + r^2$ et $t^2 + a_4a_2 - a_6$ sont pairs. De plus, l'entier $a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$ est un multiple de 4. D'après la proposition 1 de *loc. cit.*, on est dans le cas 4 de Tate. Le conducteur de A1 est donc $32p$.

2) Vérifions que la courbe A1' est de conducteur $32p$. On a

$$a_1 = 0, \quad a_2 = -2\sqrt{p-1}, \quad a_3 = 0, \quad a_4 = -1, \quad a_6 = 0,$$

$$c_4 = 2^4(4p-1), \qquad c_6 = 2^6\sqrt{p-1}\ (8p+1) \quad \text{et} \quad \Delta = 2^6 p.$$

On a

$$v(c_4) = 4, \qquad v(c_6) \geqslant 6 \quad \text{et} \quad v(\Delta) = 6.$$

On est donc dans le cas 3 ou 4 de Tate. On démontre alors comme dans l'alinéa 1 ci-dessus que l'on est dans le cas 4 de Tate, d'où l'assertion.

3) Vérifions que les courbes B2, B2', C2, C2' sont de conducteur $32p$. Les invariants standard des courbes B2 et C2 sont donnés dans le tableau ci-dessous :

	B2	C2
c_4	$2^4(p-32)$	$2^4(p+32)$
c_6	$-2^6\sqrt{p-8}(p+64)$	$-2^6\sqrt{p+8}(p-64)$
Δ	-2^9p^2	2^9p^2

On constate que l'on a dans les deux cas $v(c_4) = 4$, $v(c_6) = 6$ et $v(\Delta) = 9$. On utilisera à plusieurs reprises la remarque suivante :

Remarque 2. Soient W et W' deux équations de Weierstrass sur $\mathbb{Q}$ qui sont tordues quadratiques l'une de l'autre par $\sqrt{-1}$. Soient c_4, c_6 et Δ les invariants standard associés à W et c_4', c_6' et Δ' ceux de W'. On a les égalités

$$c_4 = c_4', \quad c_6 = -c_6' \quad \text{et} \quad \Delta = \Delta'.$$

Les courbes B2' et C2' sont les tordues quadratiques respectivement de B2 et C2 par $\sqrt{-1}$. D'après la remarque 2, les valuations des invariants de B2 et C2 sont les mêmes que celles des invariants de B2' et C2'. Notre assertion se déduit alors directement du tableau IV p. 129 de [Pa].

3.2.6. Le théorème 6

Soit k un entier vérifiant les inégalités

$$2 \leqslant k < f(p).$$

1) Vérifions que la courbe A1 est de conducteur $64p$. On a

$$a_1 = 0, \quad a_2 = 2\sqrt{p-1}, \quad a_3 = 0, \quad a_4 = p, \quad a_6 = 0,$$

$$c_4 = 2^4(p-4), \qquad c_6 = 2^6\sqrt{p-1}\ (p+8) \quad \text{et} \quad \Delta = -2^6p^2.$$

On a

$$v(c_4) = 4, \qquad v(c_6) \geqslant 6 \quad \text{et} \quad v(\Delta) = 6.$$

On est dans le cas 3 ou 4 de Tate. Posons $r = 1$ et $t = 0$. Les entiers $a_4 + r^2$ et $t^2 + a_4a_2 - a_6$ sont pairs. Puisque $p - 1$ est un carré on a $p \equiv 1 \bmod. 4$. On vérifie alors que l'entier $a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$ n'est pas divisible par 4. On est dans le cas 3 de Tate, d'où l'assertion.

2) Vérifions que la courbe A1' est de conducteur $64p$. On a

$$a_1 = 0, \quad a_2 = -2\sqrt{p-1}, \quad a_3 = 0, \quad a_4 = p, \quad a_6 = 0,$$

$$c_4 = 2^4(p-4), \qquad c_6 = -2^6\sqrt{p-1}\ (p+8) \quad \text{et} \quad \Delta = -2^6p^2.$$

On a

$$v(c_4) = 4, \qquad v(c_6) \geqslant 6 \quad \text{et} \quad v(\Delta) = 6.$$

On est dans le cas 3 ou 4 de Tate et la même démonstration que celle de l'alinéa 1 ci-dessus montre que l'on est dans le cas 3 de Tate, d'où l'assertion.

3) Vérifions que les courbes B2, B2', C2, C2', D1, D1', E2, E2', F1 et F1' sont de conducteur $64p$. Les invariants standard des courbes B2, C2, D1, E2 et F1 sont donnés dans les tableaux ci-dessous :

	B2	C2	D1
c_4	$2^6(p - 2^{k+2})$	$2^6(p + 2^{k+2})$	$2^6(p^2 - p + 1)$
c_6	$-2^9\sqrt{p - 2^k}(p + 2^{k+3})$	$-2^9\sqrt{p + 2^k}(p - 2^{k+3})$	$-2^8(p-2)(2p-1)(p+1)$
Δ	$-2^{k+12}p^2$	$2^{k+12}p^2$	$2^{k+12}p^2$

	E2	F1
c_4	$2^6(2^{k+2}-p)$	$2^6(p^2+p+1)$
c_6	$2^9\sqrt{2^k-p}(p+2^{k+3})$	$2^8(p-1)(2p+1)(p+2)$
Δ	$2^{k+12}p^2$	$2^{k+12}p^2$

On constate que l'on a dans tous les cas $v(c_4)=6$, $v(c_6)=9$ et $v(\Delta)\geqslant 14$. Compte tenu de la remarque 2, notre assertion se déduit directement du tableau IV p. 129 de [Pa].

3.2.7. Le théorème 7

Vérifions que les courbes A1, B1, C1, D1, E1 et F1 , ainsi que leurs tordues quadratiques par $\sqrt{-1}$, sont de conducteur $128p$. Leurs invariants standard sont donnés dans les tableaux ci-dessous :

	A1	B1	C1	D1
c_4	$2^4(8p^i-1)$	$2^5(p^i-2)$	$2^4(p^k+8)$	$2^5(2p^k+1)$
c_6	$-2^6\sqrt{2p^i-1}(16p^i+1)$	$2^7\sqrt{2p^i-1}(p^i+4)$	$2^6\sqrt{p^k+2}(p^k-16)$	$-2^7\sqrt{p^k+2}(4p^k-1)$
Δ	2^7p^i	-2^8p^{2i}	2^7p^{2k}	2^8p^k

	E1	F1
c_4	$2^4(p-8)$	$2^5(2p-1)$
c_6	$2^6\sqrt{p-2}(p+16)$	$-2^7\sqrt{p-2}(4p+1)$
Δ	-2^7p^2	2^8p

On constate alors que l'on est dans l'un des cas suivants :

1) on a $v(c_4)=4$, $v(c_6)=6$ et $v(\Delta)=7$;

2) on a $v(c_4)=5$, $v(c_6)=7$ et $v(\Delta)=8$.

La remarque 2 et le tableau IV p. 129 de [Pa] entraînent alors notre assertion.

3.2.8. Le théorème 8

Vérifions que les courbes A1, B1, C1 et D1, ainsi que leurs tordues quadratiques par $\sqrt{-1}$, sont de conducteur $256p$. Les invariants standard des courbes A1, B1, C1 et D1 sont donnés dans le tableau ci-dessous :

	A1	B1	C1	D1
c_4	$2^5(4p^k-1)$	$2^5(p^k-4)$	$2^5(4p^k+1)$	$2^5(p^k+4)$
c_6	$-2^8\sqrt{\frac{p^k-1}{2}}(8p^k+1)$	$2^8\sqrt{\frac{p^k-1}{2}}(p^k+8)$	$-2^8\sqrt{\frac{p^k+1}{2}}(8p^k-1)$	$2^8\sqrt{\frac{p^k+1}{2}}(p^k-8)$
Δ	2^9p^k	-2^9p^{2k}	2^9p^k	2^9p^{2k}

On constate alors que l'on a dans tous les cas $v(c_4)=5$, $v(c_6)\geqslant 8$ et $v(\Delta)=9$. La remarque 2 et le tableau IV p. 129 de [Pa] entraînent alors notre assertion.

Cela termine la vérification du fait que les courbes elliptiques qui interviennent dans les énoncés des théorèmes satisfont aux conditions annoncées.

3.3. Liste des classes de $\mathbb{Q}$-isomorphisme

Soit E une courbe elliptique définie sur $\mathbb{Q}$, ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$ et de conducteur de la forme $2^N p$ avec $N\geqslant 1$. D'après le lemme 1, il existe deux entiers a et b sans diviseurs communs impairs tels que E possède un modèle de Weierstrass, minimal en dehors de 2, de la forme

$$y^2 = x^3 + a\,x^2 + b\,x.$$

Rappelons que les invariants standard c_4, c_6 et Δ associés à ce modèle sont

$$c_4 = 2^4(a^2-3b),\quad c_6 = 2^5a(9b-2a^2)\quad\text{et}\quad \Delta = 2^4b^2(a^2-4b).$$

On déduit de l'hypothèse faite sur le conducteur de E, l'existence de deux entiers naturels m et n, avec $n\neq 0$, tels que l'on ait l'égalité

$$b^2(a^2-4b) = \pm 2^m p^n. \tag{14}$$

On a $b\neq 0$. Dans ce qui suit, on va examiner les quatre cas suivants :

A) on a $b>0$ et p ne divise pas b.

B) on a $b>0$ et p divise b.

C) on a $b<0$ et p ne divise pas b.

D) on a $b < 0$ et p divise b.

A) Cas où b est positif et p ne divise pas b

On a le lemme ci-dessous :

Lemme 10. *Supposons $b > 0$ non divisible par p. Alors, on est dans l'un des cinq cas suivants :*

1. *il existe un entier k vérifiant les inégalités $2 \leqslant k < f(p)$ tel que l'une des conditions ci-dessous soit vérifiée :*

   (i) l'entier $p + 2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques

   $$y^2 = x^3 \pm \sqrt{p+2^k}\, x^2 + 2^{k-2}\, x, \qquad y^2 = x^3 \pm 2\sqrt{p+2^k}\, x^2 + 2^k\, x.$$

   (ii) l'entier $2^k - p$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques

   $$y^2 = x^3 \pm \sqrt{2^k-p}\, x^2 + 2^{k-2}\, x, \qquad y^2 = x^3 \pm 2\sqrt{2^k-p}\, x^2 + 2^k\, x.$$

2. *il existe un entier $k \geqslant 5$ tel que l'une des conditions ci-dessous soit vérifiée :*

   (i) on a $p = 2^k + 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques

   $$y^2 = x^3 \pm 2(2p-1)\, x^2 + x, \qquad y^2 = x^3 \pm 4(2p-1)\, x^2 + 4\, x.$$

   (ii) on a $p = 2^k - 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques

   $$y^2 = x^3 \pm (p+2)\, x^2 + (p+1)\, x, \qquad y^2 = x^3 \pm 2(p+2)\, x^2 + 4(p+1)\, x,$$
   $$y^2 = x^3 \pm 2(2p+1)\, x^2 + x, \qquad y^2 = x^3 \pm 4(2p+1)\, x^2 + 4\, x.$$

3. *il existe un entier impair k vérifiant $1 \leqslant k \leqslant 164969$ tel que $p^k + 2$ soit un carré et que E soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

   $$y^2 = x^3 \pm 2\sqrt{p^k+2}\, x^2 + 2\, x, \qquad y^2 = x^3 \pm 4\sqrt{p^k+2}\, x^2 + 8\, x.$$

4. *l'entier $(p^2+1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

   $$y^2 = x^3 \pm 4\sqrt{\frac{p^2+1}{2}}\, x^2 + 2\, x, \qquad y^2 = x^3 \pm 8\sqrt{\frac{p^2+1}{2}}\, x^2 + 8\, x.$$

5. *l'entier $(p+1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

   $$y^2 = x^3 \pm 4\sqrt{\frac{p+1}{2}}\, x^2 + 2\, x, \qquad y^2 = x^3 \pm 8\sqrt{\frac{p+1}{2}}\, x^2 + 8\, x.$$

Démonstration : Il résulte de (14) que les seuls diviseurs premiers positifs possibles de b sont 2 et p. Il existe donc un entier i tel que l'on ait

$$0 \leqslant 2i \leqslant m \quad \text{et} \quad b = 2^i.$$

On obtient ainsi

$$a^2 - 2^{i+2} = \pm 2^{m-2i} p^n. \tag{15}$$

On est donc dans l'un des trois cas 1), 2) et 3) ci-dessous :

1) On a $i + 2 > m - 2i$. Dans ce cas, $v(a^2) = m - 2i$. On a donc

$$m \equiv 0 \text{ mod. } 2.$$

En posant

$$u = \frac{a}{2^{\frac{m}{2}-i}}, \tag{16}$$

on déduit de (15) que l'on a

$$u^2 - 2^{3i+2-m} = \pm p^n.$$

1.1) Supposons que l'on ait

$$u^2 - 2^{3i+2-m} = p^n. \tag{17}$$

1.1.1) Supposons l'on ait

$$3i + 2 - m \geqslant 2. \tag{18}$$

D'après le lemme 5, on est dans l'un des cas ci-dessous :

(i) on a $p = 2^{3i-m} - 1$ avec $3i - m \geqslant 5$, $n = 2$ et $u = \pm(p + 2)$.

(ii) on a $n = 1$, $3i + 2 - m < f(p)$.

Supposons que l'on soit dans le cas (i). La courbe E a alors pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{m}{2}-i}\,(p+2)\,x^2 \;+\; 2^i\,x.$$

Il existe deux entiers q_1 et r_1 tels que l'on ait

$$\frac{m}{2} - i = 2q_1 + r_1 \text{ avec } r_1 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_1}} \quad \text{et} \quad Y = \frac{y}{2^{3q_1}}, \tag{19}$$

on obtient comme nouveau modèle de E :

$$Y^2 \;=\; X^3 \;\pm (p+2)\; X^2 \;+\; (p+1)\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 2(p+2)\; X^2 \;+\; 4(p+1)\; X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On se trouve ainsi dans le cas 2 (ii) de l'énoncé du lemme avec $k = 3i - m$.

Supposons que l'on soit dans le cas (ii). D'après (16) et (17), l'entier $p + 2^{3i+2-m}$ est un carré et l'on a

$$a = \pm 2^{\frac{m}{2}-i}\; \sqrt{p + 2^{3i+2-m}}.$$

La courbe E a donc pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{m}{2}-i}\; \sqrt{p + 2^{3i+2-m}}\; x^2 \;+\; 2^i\; x.$$

En effectuant le changement de variables (19), on obtient comme modèle de E

$$Y^2 \;=\; X^3 \;\pm \sqrt{p + 2^{3i+2-m}}\; X^2 \;+\; 2^{3i-m}\; X,$$

ou bien

$$Y^2 \;=\; X^3 \;\pm 2\sqrt{p + 2^{3i+2-m}}\; X^2 \;+\; 2^{3i+2-m}\; X,$$

selon que $r = 0$ ou $r = 1$. On est donc dans le cas 1 (i) du lemme avec $k = 3i + 2 - m$. D'après (18) et la condition (ii) envisagée ci-dessus on a $2 \leqslant k < f(p)$.

1.1.2) Supposons l'on ait

$$3i + 2 - m = 1. \tag{20}$$

D'après (17) on a l'égalité

$$u^2 - 2 = p^n.$$

D'après le lemme 8, n est impair et on a $n \leqslant 164969$. L'entier $p^n + 2$ est un carré et l'on a

$$a = \pm 2^{\frac{m}{2}-i}\sqrt{p^n + 2}.$$

La courbe E a donc pour modèle de Weierstrass

$$y^2 \;=\; x^3 \pm 2^{\frac{m}{2}-i}\sqrt{p^n + 2}\; x^2 \;+\; 2^i\; x.$$

Il existe deux entiers q_2 et r_2 tels que l'on ait

$$\frac{m}{2} - i - 1 = 2q_2 + r_2 \text{ avec } r_2 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_2}} \quad \text{et} \quad Y = \frac{y}{2^{3q_2}},$$

on obtient, en utilisant la condition (20), comme nouveau modèle de E :

$$Y^2 \ = \ X^3 \ \pm 2\sqrt{p^n + 2}\ X^2 \ + \ 2\ X \quad \text{ou} \quad Y^2 \ = \ X^3 \ \pm 4\sqrt{p^n + 2}\ X^2 \ + \ 8\ X.$$

suivant que $r_2 = 0$ ou $r_2 = 1$. On est ainsi dans le cas 3 du lemme avec $k = n$.

1.2) Supposons que l'on ait

$$u^2 - 2^{3i+2-m} = -p^n.$$

D'après le lemme 6, on a $n = 1$ et $3i + 2 - m < f(p)$. L'entier $2^{3i+2-m} - p$ est un carré et l'on a

$$a = \pm 2^{\frac{m}{2}-i}\sqrt{2^{3i+2-m} - p}.$$

La courbe E a pour modèle de Weierstrass

$$y^2 \ = \ x^3 \ \pm 2^{\frac{m}{2}-i}\sqrt{2^{3i+2-m} - p}\ x^2 \ + \ 2^i\ x.$$

Le changement de variables (19) conduit au nouveau modèle de E

$$Y^2 \ = \ X^3 \ \pm \sqrt{2^{3i+2-m} - p}\ X^2 \ + \ 2^{3i-m}\ X,$$

ou bien

$$Y^2 \ = \ X^3 \ \pm 2\sqrt{2^{3i+2-m} - p}\ X^2 \ + \ 2^{3i-m+2}\ X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On est donc dans le cas 1 (ii) du lemme avec $k = 3i + 2 - m$. Notons que l'on a $2 \leqslant k < f(p)$.

2) On a $i + 2 = m - 2i$. D'après (15), on a dans ce cas

$$v(a^2) \geqslant i + 2.$$

On est alors dans l'un des cas ci-dessous :

2.1) l'entier i est pair. Dans ce cas, on a

$$v(a) \geqslant \frac{i}{2} + 1.$$

Posons

$$u = \frac{a}{2^{\frac{i}{2}+1}}.$$

Il résulte de (15) que l'on a

$$u^2 - 1 = p^n.$$

Le lemme 2 entraîne alors une contradiction.

2.2) l'entier i est impair. Dans ce cas, on a

$$v(a) \geqslant \frac{i+1}{2} + 1.$$

Posons

$$u = \frac{a}{2^{\frac{i+1}{2}+1}}.$$

Il résulte de (15) que l'on a

$$2u^2 - 1 = p^n.$$

D'après l'alinéa 2 du lemme 7, on a $n = 1$ ou $n = 2$.

(i) Supposons $n = 2$. L'entier $(p^2+1)/2$ est un carré, on a $u = \pm\sqrt{(p^2+1)/2}$ et E a pour modèle de Weierstrass

$$y^2 \ = \ x^3 \ \pm 2^{\frac{i+1}{2}+1}\sqrt{\frac{p^2+1}{2}}\ x^2 \ + \ 2^i \ x.$$

Il existe deux entiers q_3 et r_3 tels que

$$\frac{i-1}{2} = 2q_3 + r_3 \text{ avec } r_3 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_3}} \quad \text{et} \quad Y = \frac{y}{2^{3q_3}}, \tag{21}$$

on obtient comme nouveau modèle de E :

$$Y^2 \ = \ X^3 \ \pm 4\sqrt{\frac{p^2+1}{2}}\ X^2 \ + \ 2\ X \quad \text{ou} \quad Y^2 \ = \ X^3 \ \pm 8\sqrt{\frac{p^2+1}{2}}\ X^2 \ + \ 8\ X,$$

suivant que $r_3 = 0$ ou $r_3 = 1$. On est donc dans le cas 4 du lemme.

(ii) Supposons $n = 1$. L'entier $(p+1)/2$ est un carré. On a $u = \pm\sqrt{(p+1)/2}$ et E a pour modèle de Weierstrass

$$y^2 \ = \ x^3 \ \pm 2^{\frac{i+1}{2}+1}\sqrt{\frac{p+1}{2}}\ x^2 \ + \ 2^i \ x.$$

Le changement de variables (21) conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 4\sqrt{\frac{p+1}{2}}\; X^2 \;+\; 2\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 8\sqrt{\frac{p+1}{2}}\; X^2 \;+\; 8\; X,$$

suivant que $r_3 = 0$ ou $r_3 = 1$. On est alors dans le cas 5 du lemme.

3) On a $i + 2 < m - 2i$. D'après (15), on a $v(a^2) = i + 2$, de sorte que i est pair. On a donc $v(a) = i/2 + 1$. Posons

$$u = \frac{a}{2^{\frac{i}{2}+1}}.$$

On déduit de (15) que l'on a

$$u^2 - 1 = 2^{m-3i-2}p^n.$$

D'après le lemme 2, on est dans l'un des cas ci-dessous :

(i) on a $p = 2^{m-3i-4} + 1$ avec $m - 3i - 2 \geqslant 5$, $n = 1$ et $u = \pm(2p - 1)$;

(ii) on a $p = 2^{m-3i-4} - 1$ avec $m - 3i - 2 \geqslant 5$, $n = 1$ et $u = \pm(2p + 1)$.

Supposons que l'on soit dans le cas (i). La courbe E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i}{2}+1}(2p-1)\; x^2 \;+\; 2^i\; x.$$

Il existe deux entiers q_4 et r_4 tels que

$$\frac{i}{2} = 2q_4 + r_4 \text{ avec } r_4 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_4}} \quad \text{et} \quad Y = \frac{y}{2^{3q_4}}, \tag{22}$$

on obtient comme nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2(2p-1)\; X^2 \;+\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4(2p-1)\; X^2 \;+\; 4\; X,$$

suivant que $r_4 = 0$ ou $r_4 = 1$. On constate alors que l'on est dans le cas 2 (i) du lemme avec $k = m - 3i - 4$.

Supposons que l'on soit dans le cas (ii). La courbe E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i}{2}+1}(2p+1)\; x^2 \;+\; 2^i\; x.$$

Le changement de variables (22) conduit au nouveau modèle

$$Y^2 \;=\; X^3 \;\pm 2(2p+1)\; X^2 \;+\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4(2p+1)\; X^2 \;+\; 4\; X,$$

suivant que $r_4 = 0$ ou $r_4 = 1$. On est ainsi dans le cas 2 (ii) du lemme avec $k = m - 3i - 4$.

Cela termine la démonstration du lemme.

B) Cas où b est positif et p divise b

On a le lemme ci-dessous :

Lemme 11. *Supposons $b > 0$ divisible par p. Alors, on est dans l'un des neuf cas suivants :*

1. *il existe un entier k vérifiant les inégalités $0 \leqslant k < f(p)$ tel que l'une des conditions ci-dessous soit vérifiée :*

   (i) l'entier $p - 2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques

   $$y^2 = x^3 \pm 2\sqrt{p-2^k}\, x^2 + p\, x, \qquad y^2 = x^3 \pm 4\sqrt{p-2^k}\, x^2 + 4p\, x.$$

   (ii) l'entier $p + 2^k$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques

   $$y^2 = x^3 \pm 2\sqrt{p+2^k}\, x^2 + p\, x, \qquad y^2 = x^3 \pm 4\sqrt{p+2^k}\, x^2 + 4p\, x.$$

2. *il existe un entier $k \geqslant 5$ tel que l'une des conditions ci-dessous soit vérifiée :*

   (i) on a $p = 2^k + 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques

   $$y^2 = x^3 \pm (2p-1)\, x^2 + (p-1)p\, x, \qquad y^2 = x^3 \pm 2(2p-1)\, x^2 + 4(p-1)p\, x,$$

   $$y^2 = x^3 \pm 2(p-2)\, x^2 + p^2\, x, \qquad y^2 = x^3 \pm 4(p-2)\, x^2 + 4p^2\, x.$$

   (ii) on a $p = 2^k - 1$ et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques

   $$y^2 = x^3 \pm (2p+1)\, x^2 + (p+1)p\, x, \qquad y^2 = x^3 \pm 2(2p+1)\, x^2 + 4(p+1)p\, x,$$

   $$y^2 = x^3 \pm 2(p+2)\, x^2 + p^2\, x, \qquad y^2 = x^3 \pm 4(p+2)\, x^2 + 4p^2\, x.$$

3. *l'entier $2p^2 - 1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

   $$y^2 = x^3 \pm 2\sqrt{2p^2-1}\, x^2 + 2p^2\, x, \qquad y^2 = x^3 \pm 4\sqrt{2p^2-1}\, x^2 + 8p^2\, x.$$

4. *l'entier $2p - 1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

   $$y^2 = x^3 \pm 2\sqrt{2p-1}\, x^2 + 2p\, x, \qquad y^2 = x^3 \pm 4\sqrt{2p-1}\, x^2 + 8p\, x.$$

5. *l'entier* $(p^2-1)/2$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 4\sqrt{\frac{p^2-1}{2}}\; x^2 \;+\; 2p^2\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 8\sqrt{\frac{p^2-1}{2}}\; x^2 \;+\; 8p^2\; x.$$

6. *l'entier* $(p-1)/2$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 4\sqrt{\frac{p-1}{2}}\; x^2 \;+\; 2p\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 8\sqrt{\frac{p-1}{2}}\; x^2 \;+\; 8p\; x.$$

7. *l'entier* $(p^2+1)/2$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 4\sqrt{\frac{p^2+1}{2}}\; x^2 \;+\; 2p^2\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 8\sqrt{\frac{p^2+1}{2}}\; x^2 \;+\; 8p^2\; x.$$

8. *l'entier* $(p+1)/2$ *est un carré et* E *est* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 4\sqrt{\frac{p+1}{2}}\; x^2 \;+\; 2p\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 8\sqrt{\frac{p+1}{2}}\; x^2 \;+\; 8p\; x.$$

9. *il existe un entier impair* k *vérifiant* $1 \leqslant k \leqslant 164969$ *tel que* p^k+2 *soit un carré et que* E *soit* $\mathbb{Q}$*-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 2\,\sqrt{p^k+2}\; x^2 \;+\; p^k\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 4\,\sqrt{p^k+2}\; x^2 \;+\; 4p^k\; x.$$

Démonstration : D'après (14), les seuls diviseurs premiers positifs possibles de b sont 2 et p. Puisque a et b n'ont pas de diviseur commun impair, p ne divise pas a et on a

$$n \equiv 0 \text{ mod. } 2.$$

Il existe donc un entier i tel que l'on ait

$$0 \leqslant 2i \leqslant m \quad \text{et} \quad b = 2^i p^{\frac{n}{2}}.$$

En utilisant (14), on obtient ainsi

$$a^2 - 2^{i+2} p^{\frac{n}{2}} = \pm 2^{m-2i}. \tag{23}$$

On est donc dans l'un des trois cas 1), 2) et 3) ci-dessous :

1) On a $i+2 > m-2i$. Dans ce cas, on a $v(a^2) = m-2i$. On a donc

$$m \equiv 0 \text{ mod. } 2.$$

En posant

$$u = \frac{a}{2^{\frac{m}{2}-i}}, \tag{24}$$

on déduit de (23) que l'on a

$$u^2 - 2^{3i+2-m} p^{\frac{n}{2}} = \pm 1.$$

1.1) Supposons que l'on ait

$$u^2 - 2^{3i+2-m} p^{\frac{n}{2}} = 1.$$

D'après le lemme 2, on est dans l'un des cas suivants :

(i) on a $p = 2^{3i-m} + 1$ avec $3i + 2 - m \geqslant 5$, $\frac{n}{2} = 1$ et $u = \pm(2p-1)$;

(ii) on a $p = 2^{3i-m} - 1$ avec $3i + 2 - m \geqslant 5$, $\frac{n}{2} = 1$ et $u = \pm(2p+1)$.

Supposons que l'on soit dans le cas (i). D'après (24), la courbe E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{m}{2}-i}\,(2p-1)\,x^2 \;+\; 2^i p\,x.$$

Il existe deux entiers q_1 et r_1 tels que l'on ait

$$\frac{m}{2} - i = 2q_1 + r_1 \text{ avec } r_1 = 0 \text{ ou } 1.$$

Posons

$$X = \frac{x}{2^{2q_1}} \quad \text{et} \quad Y = \frac{y}{2^{3q_1}}. \tag{25}$$

En effectuant ce changement de variables, on obtient comme nouveau modèle de E

$$Y^2 \;=\; X^3 \pm (2p-1)\,X^2 + (p-1)p\,X \quad \text{ou} \quad Y^2 \;=\; X^3 \pm 2(2p-1)\,X^2 + 4(p-1)p\,X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. Puisque $p \geqslant 29$, on a $3i - m \geqslant 5$; on est ainsi dans le cas 2 (i) du lemme avec $k = 3i - m$.

Supposons que l'on soit dans le cas (ii). Il résulte de (24) que la courbe E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{m}{2}-i}\,(2p+1)\,x^2 \;+\; 2^i p\,x.$$

En effectuant le changement de variables (25), on obtient comme nouveau modèle de E

$$Y^2 \;=\; X^3 \pm (2p+1)\,X^2 + (p+1)p\,X \quad \text{ou} \quad Y^2 \;=\; X^3 \pm 2(2p+1)\,X^2 + 4(p+1)p\,X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On est dans le cas 2 (ii) du lemme avec $k = 3i - m$.

1.2) Supposons que l'on ait

$$u^2 - 2^{3i+2-m} p^{\frac{n}{2}} = -1.$$

D'après le lemme 3, on est dans l'un des cas suivants :

(i) on a $3i + 2 - m = 1$ et $\frac{n}{2} = 2$;

(ii) on a $3i + 2 - m = 1$ et $\frac{n}{2} = 1$.

Supposons que l'on soit dans le cas (i). L'entier $2p^2 - 1$ est un carré et $u = \pm\sqrt{2p^2 - 1}$. On déduit de (24) que la courbe E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{m}{2}-i}\; \sqrt{2p^2-1}\; x^2 \;+\; 2^i p^2\; x.$$

Il existe deux entiers q_2 et r_2 tels que l'on ait

$$\frac{m}{2} - i - 1 = 2q_2 + r_2 \text{ avec } r_2 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_2}} \quad \text{et} \quad Y = \frac{y}{2^{3q_2}}, \tag{26}$$

on obtient comme nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2\; \sqrt{2p^2-1}\; X^2 \;+\; 2p^2\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4\; \sqrt{2p^2-1}\; X^2 \;+\; 8p^2\; X,$$

selon que $r_2 = 0$ ou $r_2 = 1$. On est dans le cas 3 du lemme.

Supposons que l'on soit dans le cas (ii). Dans ce cas, l'entier $2p - 1$ est un carré et $u = \pm\sqrt{2p - 1}$. On déduit de (24) que la courbe E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{m}{2}-i}\; \sqrt{2p-1}\; x^2 \;+\; 2^i p\; x.$$

Le changement de variables (26) conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2\; \sqrt{2p-1}\; X^2 \;+\; 2p\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4\; \sqrt{2p-1}\; X^2 \;+\; 8p\; X,$$

selon que $r_2 = 0$ ou $r_2 = 1$. On est dans le cas 4 du lemme.

2) On a $i + 2 = m - 2i$. On a alors, d'après (23) :

$$v(a^2) \geqslant i + 2.$$

On est donc dans l'un des cas ci-dessous :

2.1) l'entier i est pair. On a

$$v(a) \geqslant \frac{i}{2} + 1.$$

Posons

$$u = \frac{a}{2^{\frac{i}{2}+1}}. \tag{27}$$

On déduit de (23) que l'on a

$$u^2 - p^{\frac{n}{2}} = \pm 1.$$

On est donc dans l'un des cas suivants :

2.1.1) Supposons que l'on ait

$$u^2 - p^{\frac{n}{2}} = -1.$$

D'après le lemme 3, on a $\frac{n}{2} = 1$. L'entier $p-1$ est donc un carré et $u = \pm\sqrt{p-1}$. On déduit de (27) que la courbe E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i}{2}+1}\;\sqrt{p-1}\;x^2 \;+\; 2^i p\;x.$$

Il existe deux entiers q_3 et r_3 tels que l'on ait

$$\frac{i}{2} = 2q_3 + r_3 \text{ avec } r_3 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_3}} \quad \text{et} \quad Y = \frac{y}{2^{3q_3}},$$

on obtient comme nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2\sqrt{p-1}\;X^2 \;+\; p\;X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4\sqrt{p-1}\;X^2 \;+\; 4p\;X,$$

selon que $r_3 = 0$ ou $r_3 = 1$. On est dans le cas 1 (i) du lemme avec $k = 0$.

2.1.2) Supposons que l'on ait

$$u^2 - p^{\frac{n}{2}} = 1.$$

On déduit alors du lemme 2 une contradiction.

2.2) l'entier i est impair. On a alors

$$v(a) \geqslant \frac{i+1}{2} + 1.$$

Posons

$$u = \frac{a}{2^{\frac{i+1}{2}+1}}. \tag{28}$$

On déduit de (23) que l'on a

$$2u^2 - p^{\frac{n}{2}} = \pm 1.$$

On est donc dans l'un des cas suivants :

2.2.1) Supposons que l'on ait

$$2u^2 - p^{\frac{n}{2}} = -1.$$

D'après l'alinéa 1 du lemme 7, on est dans l'un des cas ci-dessous :

(i) on a $\frac{n}{2} = 2$;
(ii) on a $\frac{n}{2} = 1$.

Supposons que l'on soit dans le cas (i). L'entier $(p^2-1)/2$ est un carré et $u = \pm\sqrt{\frac{p^2-1}{2}}$. On déduit de (28) que E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i+1}{2}+1}\,\sqrt{\frac{p^2-1}{2}}\;x^2 \;+\; 2^i p^2\;x.$$

Il existe deux entiers q_4 et r_4 tels que l'on ait

$$\frac{i-1}{2} = 2q_4 + r_4 \text{ avec } r_4 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_4}} \quad \text{et} \quad Y = \frac{y}{2^{3q_4}}, \tag{29}$$

on obtient comme nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 4\sqrt{\frac{p^2-1}{2}}\;X^2 \;+\; 2p^2\;X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 8\sqrt{\frac{p^2-1}{2}}\;X^2 \;+\; 8p^2\;X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 5 du lemme.

Supposons que l'on soit dans le cas (ii). L'entier $(p-1)/2$ est un carré et $u = \pm\sqrt{\frac{p-1}{2}}$. On déduit de (28) que E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i+1}{2}+1}\,\sqrt{\frac{p-1}{2}}\;x^2 \;+\; 2^i p\;x.$$

En utilisant le changement de variable (29), on obtient comme nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 4\sqrt{\frac{p-1}{2}}\;X^2 \;+\; 2p\;X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 8\sqrt{\frac{p-1}{2}}\;X^2 \;+\; 8p\;X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 6 du lemme.

2.2.2) Supposons que l'on ait

$$2u^2 - p^{\frac{n}{2}} = 1.$$

D'après l'alinéa 2 du lemme 7, on est dans l'un des cas ci-dessous :

(i) on a $\frac{n}{2} = 2$;
(ii) on a $\frac{n}{2} = 1$.

Supposons que l'on soit dans le cas (i). L'entier $(p^2+1)/2$ est un carré et $u = \pm\sqrt{\frac{p^2+1}{2}}$. On déduit de (28) que E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i+1}{2}+1}\,\sqrt{\frac{p^2+1}{2}}\;x^2 \;+\; 2^i p^2\;x.$$

Le changement de variables (29), conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 4\sqrt{\frac{p^2+1}{2}}\;X^2 \;+\; 2p^2\;X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 8\sqrt{\frac{p^2+1}{2}}\;X^2 \;+\; 8p^2\;X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 7 du lemme.

Supposons que l'on soit dans le cas (ii). L'entier $(p+1)/2$ est un carré et $u = \pm\sqrt{\frac{p+1}{2}}$. On déduit de (28) que E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i+1}{2}+1}\,\sqrt{\frac{p+1}{2}}\;x^2 \;+\; 2^i p\;x.$$

En utilisant le changement de variables (29), on obtient comme nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 4\sqrt{\frac{p+1}{2}}\;X^2 \;+\; 2p\;X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 8\sqrt{\frac{p+1}{2}}\;X^2 \;+\; 8p\;X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 8 du lemme.

3) On a $i + 2 < m - 2i$. On déduit de (23) que $v(a^2) = i + 2$. Par conséquent, i est pair et l'on a $v(a) = \frac{i}{2} + 1$. Posons

$$u = \frac{a}{2^{\frac{i}{2}+1}}. \tag{30}$$

Il résulte de (23) que l'on a

$$u^2 - p^{\frac{n}{2}} = \pm 2^{m-3i-2}.$$

On est donc dans l'un des cas ci-dessous :

3.1) Supposons que l'on ait

$$u^2 - p^{\frac{n}{2}} = -2^{m-3i-2}.$$

On déduit du lemme 4 que l'on est dans l'un des cas suivants :

(i) on a $p = 2^{m-3i-4} + 1$ avec $m - 3i - 2 \geqslant 5$, $\frac{n}{2} = 2$ et $u = \pm(p-2)$;

(ii) on a $\frac{n}{2} = 1$ et $m - 3i - 2 < \frac{\log(p)}{\log(2)}$.

Supposons que l'on soit dans le cas (i). Il résulte de (30) que E a pour modèle de Weierstrass

$$y^2 \ = \ x^3 \ \pm 2^{\frac{i}{2}+1} \ (p-2) \ x^2 \ + \ 2^i p^2 \ x.$$

Il existe deux entiers q_5 et r_5 tels que l'on ait

$$\frac{i}{2} = 2q_5 + r_5 \text{ avec } r_5 = 0 \text{ ou } 1.$$

En posant

$$X = \frac{x}{2^{2q_5}} \quad \text{et} \quad Y = \frac{y}{2^{3q_5}}, \tag{31}$$

on obtient comme nouveau modèle de E

$$Y^2 \ = \ X^3 \ \pm 2(p-2) \ X^2 \ + \ p^2 \ X \quad \text{ou} \quad Y^2 \ = \ X^3 \ \pm 4(p-2) \ X^2 \ + \ 4p^2 \ X,$$

selon que $r_5 = 0$ ou $r_5 = 1$. On a $m - 3i - 4 \geqslant 5$ et l'on est dans le cas 2 (i) du lemme avec $k = m - 3i - 4$.

Supposons que l'on soit dans le cas (ii). L'entier $p - 2^{m-3i-2}$ est un carré et l'on a $u = \pm\sqrt{p - 2^{m-3i-2}}$. Il résulte de (30) que E a pour modèle de Weierstrass

$$y^2 \ = \ x^3 \ \pm 2^{\frac{i}{2}+1} \ \sqrt{p - 2^{m-3i-2}} \ x^2 \ + \ 2^i p \ x.$$

Le changement de variables (31) conduit au nouveau modèle de E

$$Y^2 \ = \ X^3 \ \pm 2\sqrt{p - 2^{m-3i-2}} \ X^2 \ + \ p \ X \quad \text{ou} \quad Y^2 \ = \ X^3 \ \pm 4\sqrt{p - 2^{m-3i-2}} \ X^2 \ + \ 4p \ X,$$

selon que $r_5 = 0$ ou $r_5 = 1$. On est dans le cas 1 (i) du lemme avec $k = m - 3i - 2$.

3.2) Supposons que l'on ait

$$u^2 - p^{\frac{n}{2}} = 2^{m-3i-2}.$$

Distinguons les cas suivants :

3.2.1) Supposons que l'on ait $m-3i-2 \geqslant 2$. D'après le lemme 5, on est dans l'un des cas ci-dessous :

(i) on a $p = 2^{m-3i-4}-1$ avec $m-3i-2 \geqslant 4$, $\frac{n}{2} = 2$ et $u = \pm(p+2)$;

(ii) on a $\frac{n}{2} = 1$ et $m-3i-2 < f(p)$.

Supposons que l'on soit dans le cas (i). Il résulte de (30) que E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i}{2}+1}\,(p+2)\,x^2 \;+\; 2^i p^2\,x.$$

Le changement de variables (31) conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2(p+2)\,X^2 \;+\; p^2\,X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4(p+2)\,X^2 \;+\; 4p^2\,X,$$

selon que $r_5 = 0$ ou $r_5 = 1$. On a $m-3i-4 \geqslant 5$ et l'on est dans le cas 2 (ii) du lemme avec $k = m-3i-4$.

Supposons que l'on soit dans le cas (ii). L'entier $p + 2^{m-3i-2}$ est un carré et l'on a $u = \pm\sqrt{p+2^{m-3i-2}}$. Il résulte de (30) que E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i}{2}+1}\,\sqrt{p+2^{m-3i-2}}\,x^2 \;+\; 2^i p\,x.$$

Le changement de variables (31) conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2\sqrt{p+2^{m-3i-2}}\,X^2 \;+\; p\,X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4\sqrt{p+2^{m-3i-2}}\,X^2 \;+\; 4p\,X.$$

On est dans le cas 1 (ii) du lemme avec $k = m-3i-2$.

3.2.2) Supposons que l'on ait $m-3i-2 = 1$. On a

$$u^2 - p^{\frac{n}{2}} = 2.$$

D'après le lemme 8, $\frac{n}{2}$ est impair et on a $\frac{n}{2} \leqslant 164969$. L'entier $p^{\frac{n}{2}}+2$ est un carré, on a $u = \pm\sqrt{p^{\frac{n}{2}}+2}$ et E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i}{2}+1}\,\sqrt{p^{\frac{n}{2}}+2}\,x^2 \;+\; 2^i p^{\frac{n}{2}}\,x.$$

Le changement de variables (31) conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2\,\sqrt{p^{\frac{n}{2}}+2}\,X^2 \;+\; p^{\frac{n}{2}}\,X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4\,\sqrt{p^{\frac{n}{2}}+2}\,X^2 \;+\; 4p^{\frac{n}{2}}\,X.$$

On est donc dans le cas 9 du lemme avec $k = \frac{n}{2}$.

Cela termine la démontration du lemme.

C) Cas où b est négatif et p ne divise pas b

On a le lemme suivant :

Lemme 12. *Supposons $b < 0$ non divisible par p. Alors on est dans l'un des huit cas ci-dessous :*

1. *il existe un entier k vérifiant les inégalités $2 \leqslant k < f(p)$ tel que l'entier $p - 2^k$ soit un carré et que E soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm \sqrt{p-2^k}\; x^2 \;-\; 2^{k-2}\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 2\sqrt{p-2^k}\; x^2 \;-\; 2^k\; x.$$

2. *il existe un entier $k \geqslant 5$ tel que l'on ait $p = 2^k + 1$ et que E soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm (p-2)\; x^2 \;-\; (p-1)\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 2(p-2)\; x^2 \;-\; 4(p-1)\; x.$$

3. *l'entier $p - 2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 2\sqrt{p-2}\; x^2 \;-\; 2\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 4\sqrt{p-2}\; x^2 \;-\; 8\; x.$$

4. *l'entier $p - 1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 2\sqrt{p-1}\; x^2 \;-\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 4\sqrt{p-1}\; x^2 \;-\; 4\; x.$$

5. *l'entier $(p^2 - 1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 4\sqrt{\frac{p^2-1}{2}}\; x^2 \;-\; 2\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 8\sqrt{\frac{p^2-1}{2}}\; x^2 \;-\; 8\; x.$$

6. *l'entier $(p - 1)/2$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 4\sqrt{\frac{p-1}{2}}\; x^2 \;-\; 2\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 8\sqrt{\frac{p-1}{2}}\; x^2 \;-\; 8\; x.$$

7. *l'entier $2p^2 - 1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 2\sqrt{2p^2-1}\; x^2 \;-\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 4\sqrt{2p^2-1}\; x^2 \;-\; 4\; x.$$

8. *l'entier $2p - 1$ est un carré et E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 2\sqrt{2p-1}\; x^2 \;-\; x, \qquad\qquad y^2 \;=\; x^3 \;\pm 4\sqrt{2p-1}\; x^2 \;-\; 4\; x.$$

Démonstration : Il résulte de (14) que le seul diviseur premier positif possible de b est 2. Il existe donc un entier i tel que l'on ait

$$0 \leqslant 2i \leqslant m \quad \text{et} \quad b = -2^i.$$

On déduit de (14) que l'on a

$$a^2 + 2^{i+2} = 2^{m-2i} p^n. \tag{32}$$

On est donc dans l'un des trois cas 1), 2) et 3) ci-dessous :

1) On a $i + 2 > m - 2i$. Dans ce cas, on a $v(a^2) = m - 2i$. On a donc

$$m \equiv 0 \text{ mod. } 2.$$

En posant

$$u = \frac{a}{2^{\frac{m}{2}-i}}, \tag{33}$$

on déduit de (32) que l'on a

$$u^2 + 2^{3i+2-m} = p^n.$$

D'après le lemme 4, on est dans l'un des cas suivants :

(i) on a $p = 2^{3i-m} + 1$, $3i - m + 2 \geqslant 5$, $n = 2$ et $u = \pm(p-2)$;

(ii) on a $n = 1$ et $3i + 2 - m < \frac{\log(p)}{\log(2)}$.

Supposons que l'on soit dans le cas (i). On déduit de (33) que E a pour modèle de Weierstrass

$$y^2 \ = \ x^3 \ \pm 2^{\frac{m}{2}-i}(p-2)\ x^2 \ - \ 2^i\ x.$$

Il existe deux entiers q_1 et r_1 tels que l'on ait

$$\frac{m}{2} - i = 2q_1 + r_1 \text{ avec } r_1 = 0 \text{ ou } 1.$$

Posons

$$X = \frac{x}{2^{2q_1}} \quad \text{et} \quad Y = \frac{y}{2^{3q_1}}. \tag{34}$$

En effectuant ce changement de variables, on obtient comme nouveau modèle de E

$$Y^2 \ = \ X^3 \ \pm (p-2)\ X^2 \ - \ (p-1)\ X \quad \text{ou} \quad Y^2 \ = \ X^3 \ \pm 2(p-2)\ X^2 \ - \ 4(p-1)\ X,$$

selon que $r_1 = 0$ ou $r_1 = 1$. On est dans le cas 2 (i) du lemme avec $k = 3i - m$.

Supposons que l'on soit dans le cas (ii). Dans ce cas, l'entier $p-2^{3i+2-m}$ est un carré et $u=\pm\sqrt{p-2^{3i+2-m}}$. On déduit de (33) que E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{m}{2}-i}\sqrt{p-2^{3i+2-m}}\;x^2 \;-\; 2^i\;x.$$

Supposons $3i+2-m \geqslant 2$. Le changement de variables (34) conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm \sqrt{p-2^{3i+2-m}}\;X^2 \;-\; 2^{3i-m}\;X,$$

ou bien

$$Y^2 \;=\; X^3 \;\pm 2\sqrt{p-2^{3i+2-m}}\;X^2 \;-\; 2^{3i+2-m}\;X,$$

selon que $r_1=0$ ou $r_1=1$. On est dans le cas 1 du lemme avec $k=3i+2-m$.

Supposons $3i+2-m=1$. Il existe deux entiers q_2 et r_2 tels que l'on ait

$$\frac{m}{2}-i-1=2q_2+r_2 \text{ avec } r_2=0 \text{ ou } 1.$$

Le changement de variables

$$X=\frac{x}{2^{2q_2}} \quad \text{et} \quad Y=\frac{y}{2^{3q_2}},$$

conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2\sqrt{p-2}\;X^2 \;-\; 2\;X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4\sqrt{p-2}\;X^2 \;-\; 8\;X,$$

selon que $r_2=0$ ou $r_2=1$. On est dans le cas 3 du lemme.

2) On a $i+2=m-2i$. D'après (32), on a $v(a^2)\geqslant i+2$. On est dans l'un des cas suivants :

2.1) l'entier i est pair. En posant

$$u=\frac{a}{2^{\frac{i}{2}+1}},$$

on obtient d'après (32)

$$u^2+1=p^n.$$

D'après le lemme 3, on a $n=1$. L'entier $p-1$ est un carré, $u=\pm\sqrt{p-1}$ et E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i}{2}+1}\sqrt{p-1}\;x^2 \;-\; 2^i\;x.$$

Il existe deux entiers q_3 et r_3 tels que l'on ait

$$\frac{i}{2}=2q_3+r_3 \text{ avec } r_3=0 \text{ ou } 1.$$

Le changement de variables

$$X = \frac{x}{2^{2q_3}} \quad \text{et} \quad Y = \frac{y}{2^{3q_3}},$$

conduit au mouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2\sqrt{p-1}\; X^2 \;-\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4\sqrt{p-1}\; X^2 \;-\; 4\; X.$$

selon que $r_3 = 0$ ou $r_3 = 1$. On est dans le cas 4 du lemme.

2.2) l'entier i est impair. Dans ce cas on a

$$v(a) \geqslant \frac{i+1}{2} + 1.$$

En posant

$$u = \frac{a}{2^{\frac{i+1}{2}+1}},$$

on déduit de (32) que l'on a

$$2u^2 + 1 = p^n.$$

D'après l'alinéa 1 du lemme 7, on est dans l'un des cas suivants :

(i) on a $n = 2$;

(ii) on a $n = 1$.

Supposons que l'on soit dans le cas (i). Dans ce cas, l'entier $(p^2-1)/2$ est un carré. On a $u = \pm\sqrt{(p^2-1)/2}$ et E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i+1}{2}+1}\sqrt{\frac{p^2-1}{2}}\; x^2 \;-\; 2^i\; x.$$

Il existe deux entiers q_4 et r_4 tels que l'on ait

$$\frac{i-1}{2} = 2q_4 + r_4 \text{ avec } r_4 = 0 \text{ ou } 1.$$

Le changement de variables

$$X = \frac{x}{2^{2q_4}} \quad \text{et} \quad Y = \frac{y}{2^{3q_4}}, \tag{35}$$

conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 4\sqrt{\frac{p^2-1}{2}}\; X^2 \;-\; 2\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 8\sqrt{\frac{p^2-1}{2}}\; X^2 \;-\; 8\; X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 5 du lemme.

Supposons que l'on soit dans le cas (ii). L'entier $(p-1)/2$ est alors un carré. On a $u = \pm\sqrt{(p-1)/2}$ et E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm 2^{\frac{i+1}{2}+1}\sqrt{\frac{p-1}{2}}\; x^2 \;-\; 2^i\; x.$$

Le changement de variables (35) conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 4\sqrt{\frac{p-1}{2}}\; X^2 \;-\; 2\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 8\sqrt{\frac{p-1}{2}}\; X^2 \;-\; 8\; X,$$

selon que $r_4 = 0$ ou $r_4 = 1$. On est dans le cas 6 du lemme.

3) On a $i + 2 < m - 2i$. Il résulte de (32) que l'on a $v(a^2) = i + 2$, de sorte que i est pair. On a donc $v(a) = \frac{i}{2} + 1$. Posons

$$u = \frac{a}{2^{\frac{i}{2}+1}}. \tag{36}$$

On déduit alors de (32) que l'on a

$$u^2 + 1 = 2^{m-3i-2}p^n.$$

Rappelons que n est non nul. D'après le lemme 3, on est dans l'un des cas suivants :

(i) on a $m - 3i - 2 = 1$ et $n = 2$;

(ii) on a $m - 3i - 2 = 1$ et $n = 1$.

Supposons que l'on soit dans le cas (i). L'entier $2p^2 - 1$ est alors un carré et l'on a $u = \pm\sqrt{2p^2 - 1}$. Il résulte de (36) que E a pour modèle de Weierstrass

$$Y^2 \;=\; X^3 \;\pm\; 2^{\frac{i}{2}+1}\sqrt{2p^2-1}\; X^2 \;-\; 2^i\; X.$$

Il existe deux entiers q_5 et r_5 tels que l'on ait

$$\frac{i}{2} = 2q_5 + r_5 \text{ avec } r_5 = 0 \text{ ou } 1.$$

Le changement de variables

$$X = \frac{x}{2^{2q_5}} \quad \text{et} \quad Y = \frac{y}{2^{3q_5}}, \tag{37}$$

conduit au mouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2\sqrt{2p^2-1}\; X^2 \;-\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4\sqrt{2p^2-1}\; X^2 \;-\; 4\; X,$$

selon que $r_5 = 0$ ou $r_5 = 1$. On est dans le cas 7 du lemme.

Supposons que l'on soit dans le cas (ii). Dans ce cas, l'entier $2p-1$ est un carré et l'on a $u = \pm\sqrt{2p-1}$. On déduit de (36) que E a pour modèle de Weierstrass

$$y^2 \;=\; x^3 \;\pm\; 2^{\frac{i}{2}+1}\sqrt{2p-1}\,x^2 \;-\; 2^i\,x.$$

Le changement de variables (37) conduit au nouveau modèle de E

$$Y^2 \;=\; X^3 \;\pm 2\sqrt{2p-1}\,X^2 \;-\; X \quad \text{ou} \quad Y^2 \;=\; X^3 \;\pm 4\sqrt{2p-1}\,X^2 \;-\; 4\,X,$$

selon que $r_5 = 0$ ou $r_5 = 1$. On est dans le cas 8 du lemme.

Cela termine la démonstration du lemme.

D) Cas où b est négatif et p divise b

On a le lemme ci-dessous :

Lemme 13. *Supposons $b < 0$ divisible par p. Alors, il existe un entier k vérifiant les inégalités $2 \leqslant k < f(p)$ tel que l'entier $2^k - p$ soit un carré et que E soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques*

$$y^2 \;=\; x^3 \;\pm 2\sqrt{2^k-p}\,x^2 \;-\; p\,x, \qquad\qquad y^2 \;=\; x^3 \;\pm 4\sqrt{2^k-p}\,x^2 \;-\; 4p\;.$$

Démonstration : D'après (14), les seuls diviseurs premiers positifs possibles de b sont 2 et p. Puisque a et b n'ont pas de diviseur commun impair, p ne divise pas a et l'on a

$$n \equiv 0 \text{ mod. } 2.$$

Il existe donc un entier i tel que l'on ait

$$0 \leqslant 2i \leqslant m \quad \text{et} \quad b = -2^i p^{\frac{n}{2}}.$$

Il résulte alors de (14) que l'on a

$$a^2 + 2^{i+2}p^{\frac{n}{2}} = 2^{m-2i}. \tag{38}$$

On est donc dans l'un des trois cas 1), 2) et 3) ci-dessous :

1) On a $i+2 > m-2i$. Dans ce cas, on a $v(a^2) = m-2i$. On a donc

$$m \equiv 0 \text{ mod. } 2.$$

En posant

$$u = \frac{a}{2^{\frac{m}{2}-i}},$$

on déduit de (38) que l'on a

$$u^2 + 2^{3i+2-m} p^{\frac{n}{2}} = 1,$$

d'où une contradiction

2) On a $i + 2 = m - 2i$. On a alors, d'après (38) l'inégalité

$$v(a^2) \geqslant i + 2.$$

On est donc dans l'un des cas ci-dessous :

2.1) l'entier i est pair. Posons

$$u = \frac{a}{2^{\frac{i}{2}+1}}.$$

D'après (38), on a

$$u^2 + p^{\frac{n}{2}} = 1,$$

ce qui est impossible.

2.2) l'entier i est impair. On a alors

$$v(a) \geqslant \frac{i+1}{2} + 1.$$

Posons

$$u = \frac{a}{2^{\frac{i+1}{2}+1}}.$$

On déduit de (38) que l'on a

$$2u^2 + p^{\frac{n}{2}} = 1.$$

On obtient de nouveau une contradiction.

3) On a $i + 2 < m - 2i$. D'après (38), on a $v(a^2) = i + 2$, donc i est pair et l'on a $v(a) = \frac{i}{2} + 1$. Posons

$$u = \frac{a}{2^{\frac{i}{2}+1}}.$$

Il résulte de (38) que l'on a

$$u^2 + p^{\frac{n}{2}} = 2^{m-3i-2}.$$

D'après le lemme 6, on a $\frac{n}{2} = 1$ et $m-3i-2 < f(p)$. On en déduit que l'entier $2^{m-3i-2}-p$ est un carré et que l'on a $u = \pm\sqrt{2^{m-3i-2} - p}$. Ainsi E a pour modèle de Weierstrass

$$y^2 \;=\; x^2 \;\pm 2^{\frac{i}{2}+1}\sqrt{2^{m-3i-2} - p}\; x^2 \;- 2^i p\; x.$$

Il existe deux entiers q et r tels que l'on ait

$$\frac{i}{2} = 2q + r \text{ avec } r = 0 \text{ ou } 1.$$

Le changement de variables

$$X = \frac{x}{2^{2q}} \quad \text{et} \quad Y = \frac{y}{2^{3q}},$$

conduit au mouveau modèle de E

$$Y^2 \;=\; X^3 \pm 2\sqrt{2^{m-3i-2} - p}\, X^2 \;-\; p\, X \quad \text{ou} \quad Y^2 \;=\; X^3 \pm 4\sqrt{2^{m-3i-2} - p}\, X^2 \;-\; 4p\, X,$$

selon que $r = 0$ ou $r = 1$. Posons $k = m - 3i - 2$. On a $2 \leqslant k < f(p)$ et la conclusion du lemme avec l'entier k.

3.4. Fin de la démonstration

Dans ce paragraphe, nous allons démontrer que les courbes elliptiques indiquées dans les énoncés des théorèmes 1 à 8 sont les seules, à $\mathbb{Q}$-isomorphisme près, vérifiant les propriétés annoncées. Il suffit pour cela de démontrer l'assertion ci-dessous :

$(*)$ *Soit F une courbe elliptique se trouvant dans les énoncés des lemmes* 10, 11, 12 *ou* 13. *Alors, F est de conducteur p ou est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques intervenant dans les énoncés des théorèmes* 1 *à* 8.

En effet, soient N un entier tel que $1 \leqslant N \leqslant 8$ et E une courbe elliptique sur $\mathbb{Q}$, de conducteur $2^N p$, ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. D'après l'étude faite au paragraphe précédent, E est $\mathbb{Q}$-isomorphe à une courbe elliptique F se trouvant dans les énoncés des lemmes 10, 11, 12 ou 13. Elle n'est pas de conducteur p. D'après l'assertion $(*)$, F est donc $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques se trouvant dans les énoncés des théorèmes 1 à 8. Par suite, tel est aussi le cas pour E. Puisque E est de conducteur $2^N p$, il résulte alors du paragraphe 3.2 que E est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques indiquées dans les tableaux du théorème portant le numéro N. Cela termine alors la démonstration des théorèmes.

Vérifions que l'assertion $(*)$ est une conséquence de l'assertion $(**)$ suivante :

$(**)$ *Soit F une courbe elliptique se trouvant dans les énoncés des lemmes* 10, 11, 12 *ou* 13. *Soit F' la tordue quadratique de F par $\sqrt{-1}$. Alors, l'une des courbes F et F' est de conducteur p ou est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques intervenant dans les énoncés des théorèmes* 1 *à* 8.

Considérons en effet une courbe elliptique F se trouvant dans les énoncés des lemmes 10, 11, 12 ou 13. D'après $(**)$, on peut supposer que F' est de conducteur p ou est $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques intervenant dans les théorèmes 1 à 8.

a) Supposons F' de conducteur p. Puisque F a un point d'ordre 2 sur $\mathbb{Q}$, tel est aussi le cas de F'. On en déduit que F' est $\mathbb{Q}$-isomorphe à l'une des deux courbes de Setzer se trouvant dans l'introduction. On constate alors que F est $\mathbb{Q}$-isomorphe à l'une des courbes A1 et A2 du théorème 4 avec $k = 6$. L'assertion $(*)$ est donc démontrée dans ce cas.

b) Supposons que F' soit $\mathbb{Q}$-isomorphe à l'une des courbes intervenant dans les théorèmes 1 à 8.

b.1) Si F' est isomorphe à l'une des courbes des théorèmes 5 à 8, on vérifie qu'il en est de même de F.

b.2) Si F' est isomorphe à l'une des courbes des théorèmes 2 et 3, alors F est isomorphe à l'une des courbes du théorème 4.

b.3) Si F' est isomorphe à l'une des courbes du théorème 1, alors F est isomorphe à l'une des courbes du théorème 4 ; on le vérifie en effectuant les changements de variables qui se trouvent dans le tableau ci-dessous.

	changement de variables	nouveau modèle
A1	$x = \frac{X}{4} \quad y = \frac{Y-X}{8}$	$Y^2 = X^3 + \sqrt{p-2^k}\ X^2 - 2^{k-2}X$
A2	$x = \frac{X-\sqrt{p-2^k}}{4} \quad y = \frac{Y-X+\sqrt{p-2^k}}{8}$	$Y^2 = X^3 - 2\sqrt{p-2^k}\ X^2 + pX$
B1	$x = \frac{X}{4} \quad y = \frac{Y-X}{8}$	$Y^2 = X^3 + \sqrt{p+2^k}\ X^2 + 2^{k-2}X$
B2	$x = \frac{X-\sqrt{p+2^k}}{4} \quad y = \frac{Y-X+\sqrt{p+2^k}}{8}$	$Y^2 = X^3 - 2\sqrt{p+2^k}\ X^2 + pX$
C1	$x = \frac{X-1}{4} \quad y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - (p+1)X^2 + pX$
C2	$x = \frac{X-1}{4} \quad y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - 2(2-p)X^2 + p^2X$
C3	$x = \frac{X}{4} \quad y = \frac{Y-X}{8}$	$Y^2 = X^3 + \frac{p+1}{2}X^2 + \frac{(p-1)^2}{16}X$
C4	$x = \frac{X-1}{4} \quad y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - 2(2p-1)X^2 + X$
D1	$x = \frac{X}{4} \quad y = \frac{Y-X}{8}$	$Y^2 = X^3 + \sqrt{2^k-p}\ X^2 + 2^{k-2}X$
D2	$x = \frac{X-\sqrt{2^k-p}}{4} \quad y = \frac{Y-X+\sqrt{2^k-p}}{8}$	$Y^2 = X^3 - 2\sqrt{2^k-p}\ X^2 - pX$
E1	$x = \frac{X-1}{4} \quad y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - (1-p)X^2 - pX$
E2	$x = \frac{X-1}{4} \quad y = \frac{Y-X+1}{8}$	$Y^2 = X^3 - 2(p+2)X^2 + p^2X$
E3	$x = \frac{X}{4} \quad y = \frac{Y-X}{8}$	$Y^2 = X^3 - \frac{p-1}{2}X^2 + \frac{(p+1)^2}{16}X$
E4	$x = \frac{X-1}{4} \quad y = \frac{Y-X+1}{8}$	$Y^2 = X^3 + 2(2p+1)X^2 + X$

b.4) Supposons maintenant que F' soit $\mathbb{Q}$-isomorphe à l'une des courbes elliptiques se trouvant dans l'énoncé du théorème 4.

Si F' est isomorphe à l'une des courbes A1 et A2 : si $k = 4$ ou $k = 5$, la courbe F est isomorphe à la courbe A1 ou A2 du théorème 3 ; si $k = 6$, le conducteur de F est p ; si l'on a $k \geqslant 7$, la courbe F est isomorphe à la courbe A1 ou A2 du théorème 1, comme on le constate à l'aide du tableau ci-dessus.

Si F' est isomorphe à la courbe B1 ou B2 : si $k = 5$, alors F est isomorphe à la courbe B1 ou B2 du théorème 3 ; si l'on a $k \geqslant 7$, F est isomorphe à l'une des courbes B1 et B2 du théorème 1.

Si F' est isomorphe à l'une des courbes intervenant dans les alinéas 3) et 6) du théorème 4, alors F est isomorphe à l'une des courbes Ei et Ci du théorème 1.

Si F' est isomorphe à la courbe D1 ou D2, alors F est isomorphe à la courbe A1 ou A2 du théorème 2.

Si F' est isomorphe à la courbe E1 ou E2 : si $k = 5$, F est isomorphe à la courbe D1 ou D2 du théorème 3 ; si l'on a $k \geqslant 7$, F est isomorphe à l'une des courbes D1 et D2 du théorème 1.

Cela prouve que l'assertion $(*)$ est de nouveau vérifiée dans ce cas.

Tout revient ainsi à démontrer l'assertion $(**)$ pour chacun des lemmes 10 à 13.

3.4.1. Le lemme 10

I) Considérons un entier k vérifiant les inégalités $2 \leqslant k < f(p)$.

1. Supposons que $p + 2^k$ soit un carré. Rappelons que si k est pair, compte tenu de la remarque 1 et de la condition (2), on a

$$p = 2^{\frac{k}{2}+1} + 1, \quad \sqrt{p + 2^k} = \frac{p+1}{2} \quad \text{et} \quad k \geqslant 8 \quad (\text{car } p \geqslant 29).$$

(i) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 \;=\; x^3 \;-\; \sqrt{p + 2^k}\; x^2 \;+\; 2^{k-2}\; x.$$

Supposons k pair, le modèle ci-dessus s'écrit

$$y^2 \;=\; x^3 \;-\; \frac{p+1}{2}\; x^2 \;+\; \frac{(p-1)^2}{16}\; x.$$

On obtient dans ce cas la courbe C2 du théorème 4. Supposons k impair. Si $k = 3$, on retrouve la courbe C1' du théorème 5. Si $k \geqslant 5$, on retrouve la courbe B1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 2\sqrt{p + 2^k}\; x^2 \;+\; 2^k\; x.$$

Supposons k pair. L'équation ci-dessus s'écrit

$$y^2 \;=\; x^3 \;+\; (p+1)\; x^2 \;+\; \frac{(p-1)^2}{4}\; x.$$

On obtient alors la courbe D4' du théorème 6. Si k est impair, on retrouve la courbe C1 du théorème 6.

2. Supposons que $2^k - p$ soit un carré. Dans le cas où k est pair, compte tenu de la remarque 1 et de la condition (2), on a

$$p = 2^{\frac{k}{2}+1} - 1, \quad \sqrt{2^k - p} = \frac{1-p}{2} \quad \text{et} \quad k \geqslant 8 \quad (\text{car } p \geqslant 29).$$

(i) Considérons la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;-\; \sqrt{2^k - p}\, x^2 \;+\; 2^{k-2}\, x.$$

Si k pair, le modèle ci-dessus s'écrit

$$y^2 \;=\; x^3 \;+\; \frac{p-1}{2}\, x^2 \;+\; \frac{(p+1)^2}{16}\, x,$$

et l'on obtient la courbe F2 du théorème 4. Si k impair, on a $k \geqslant 5$ et l'on obtient la courbe E1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 2\sqrt{2^k - p}\, x^2 \;+\; 2^k\, x.$$

Si k est pair, l'équation s'écrit

$$y^2 \;=\; x^3 \;+\; (1-p)\, x^2 \;+\; \frac{(p+1)^2}{4}\, x,$$

et l'on obtient la courbe F4' du théorème 6. Si k est impair, on retrouve la courbe E1 du théorème 6.

II) Soit k un entier $\geqslant 5$.

1. Supposons que l'on ait $p = 2^k + 1$. En posant $k = \frac{t}{2} + 1$, on a $t \geqslant 8$ et t est pair. Il en résulte que :

(i) la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 2(2p-1)\, x^2 \;+\; x$$

est la courbe C3 du théorème 4.

(ii) La courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 4(2p-1)\, x^2 \;+\; 4x$$

est la courbe D2 du théorème 6.

2. Supposons que l'on ait $p = 2^k - 1$. Comme ci-dessus, si $k = \frac{t}{2} + 1$, on a $t \geqslant 8$ et t est pair.

(i) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 \ = \ x^3 \ - \ (p+2)\ x^2 \ + \ (p+1)\ x.$$

Le changement de variables $x = X + 1$ et $y = Y$, conduit à la courbe F1 du théorème 4.

(ii) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 \ = \ x^3 \ + \ 2(p+2)\ x^2 \ + \ 4(p+1)\ x.$$

Le changement de variables $x = X - 2$ et $y = Y$, conduit à la courbe F1' du théorème 6.

(iii) La courbe elliptique d'équation

$$y^2 \ = \ x^3 \ - \ 2(2p+1)\ x^2 \ + \ x.$$

est la courbe F4 du théorème 4.

(iv) La courbe elliptique d'équation

$$y^2 \ = \ x^3 \ + \ 4(2p+1)\ x^2 \ + \ 4\ x.$$

est la courbe F2' du théorème 6.

III) On vérifie que les courbes elliptiques intervenant dans l'alinéa 3 du lemme sont les courbes D1, D1', C2 et C2' du théorème 7. Celles des alinéas 4 et 5 sont les courbes C1, C1', D2 et D2' du théorème 8.

3.4.2. Le lemme 11

I) Soit k un entier vérifiant les inégalités $0 \leqslant k < f(p)$.

1. Supposons que $p - 2^k$ soit un carré.

(i) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 \ = \ x^3 \ + \ 2\sqrt{p-2^k}\ x^2 \ + \ p\ x.$$

On retrouve les courbes A1 du théorème 6, E1 du théorème 7, D2 du théorème 4, B2' du théorème 5 ou A2 du théorème 4, selon respectivement que l'on ait $k = 0$, 1, 2, 3 ou $k \geqslant 4$.

(ii) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 \ = \ x^3 \ + \ 4\sqrt{p-2^k}\ x^2 \ + \ 4p\ x.$$

On retrouve les courbes A2' du théorème 5, F2' du théorème 7, B2' du théorème 6, respectivement selon que $k = 0$, 1, ou $k \geqslant 2$.

2. Supposons que $p + 2^k$ soit un carré. Si k est pair, compte tenu de la remarque 1 et de la condition (2), rappelons que l'on a

$$p = 2^{\frac{k}{2}+1} + 1, \quad \sqrt{p + 2^k} = \frac{p+1}{2} \quad \text{et} \quad k \geqslant 8 \quad (\text{car } p \geqslant 29).$$

(i) Considérons la courbe elliptique d'équation

$$y^2 \ = \ x^3 \ + \ 2\sqrt{p + 2^k}\ x^2 \ + \ p\ x.$$

Si k est impair, on retrouve les courbes elliptiques C1 du théorème 7, C2' du théorème 5 et B2 du théorème 4, respectivement selon que $k = 1$, 3 ou $k \geqslant 5$. Si k est pair, l'équation ci-dessus s'écrit

$$y^2 \ = \ x^3 \ + \ (p+1)\ x^2 \ + \ p\ x,$$

qui est la courbe C1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 \ = \ x^3 \ + \ 4\sqrt{p + 2^k}\ x^2 \ + \ 4p\ x.$$

Si k est impair, on retrouve les courbes D2' du théorème 7 ou C2' du théorème 6, respectivement selon que $k = 1$ ou $k \geqslant 3$. Si k est pair, l'équation ci-dessus s'écrit

$$y^2 \ = \ x^3 \ + \ 2(p+1)\ x^2 \ + \ 4p\ x,$$

qui est la courbe D1 du théorème 6.

II) Soit k un entier $\geqslant 5$.

1. Supposons que l'on ait $p = 2^k + 1$. Si $k = \frac{t}{2} + 1$, on a $t \geqslant 8$ et t est pair.

(i) Considérons la courbe elliptique d'équation

$$y^2 \ = \ x^3 \ - \ (2p-1)\ x^2 \ + \ (p-1)p\ x.$$

Le changement de variables $x = X + p$ et $y = Y$, conduit à la courbe C1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 \ = \ x^3 \ + \ 2(2p-1)\ x^2 \ + \ 4(p-1)p\ x.$$

Le changement de variables $x = X - 2p$, $y = Y$, conduit à la courbe D1' du théorème 6.

(iii) La courbe elliptique d'équation

$$y^2 \;=\; x^3 \;-\; 2(p-2)\; x^2 \;+\; p^2\; x.$$

est la courbe C4 du théorème 4.

(iv) La courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 4(p-2)\; x^2 \;+\; 4p^2\; x.$$

est la courbe D3' du théorème 6.

2. Supposons que l'on ait $p = 2^k - 1$. Comme ci-dessus, en posant $k = \frac{t}{2} + 1$, on a $t \geqslant 8$ et t est pair.

(i) Considérons la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; (2p+1)\; x^2 \;+\; (p+1)p\; x.$$

Le changement de variables $x = X - p$ et $Y = y$, conduit à la courbe F1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 2(2p+1)\; x^2 \;+\; 4(p+1)p\; x.$$

Le changement de variables $x = X - 2p$ et $Y = y$ conduit à la courbe F1 du théorème 6.

(iii) La courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 2(p+2)\; x^2 \;+\; p^2\; x.$$

est la courbe F3 du théorème 4.

(iv) La courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 4(p+2)\; x^2 \;+\; 4p^2\; x.$$

est la courbe F3 du théorème 6.

III) On vérifie que les courbes elliptiques intervenant dans les alinéas 3 et 4 du lemme sont les courbes B1, B1', A2 et A2' du théorème 7. Les courbes les alinéas 5, 6, 7 et 8 du lemme sont les courbes B1, B1', A2, A2', D1, D1', C2 et C2' du théorème 8. Celles de l'alinéa 9 du lemme sont les courbes C1, C1', D2 et D2' du théorème 7.

3.4.3. Le lemme 12

I) Soit k un entier vérifiant les inégalités $2 \leqslant k < f(p)$ et tel que $p - 2^k$ soit un carré.

(i) Considérons la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;-\; \sqrt{p-2^k}\; x^2 \;-\; 2^{k-2}\; x.$$

On retrouve les courbes elliptiques D1 du théorème 4, B1' du théorème 5 ou A1 du théorème 4, respectivement selon que $k = 2$, 3 ou $\geqslant 4$.

(ii) La courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 2\sqrt{p-2^k}\; x^2 \;-\; 2^k\; x,$$

est la courbe B1 du théorème 6.

II) Soit k un entier $\geqslant 5$ tel que $p = 2^k + 1$. En posant $k = \frac{t}{2} + 1$, on a $t \geqslant 8$ et t est pair.

(i) Considérons la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; (p-2)\; x^2 \;-\; (p-1)\; x.$$

Le changement de variables $x = X + 1$ et $Y = y$, conduit à la courbe C1 du théorème 4.

(ii) Considérons la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 2(p-2)\; x^2 \;-\; 4(p-1)\; x.$$

Le changement de variables $x = X + 2$ et $Y = y$, conduit à la courbe D1 du théorème 6.

III) On vérifie que les courbes elliptiques intervenant dans l'alinéa 3 du lemme sont les courbes F1, F1', E2 et E2' du théorème 7. Les courbes de l'alinéa 4 du lemme sont les courbes A1, A1' du théorème 5 et A2, A2' du théorème 6. Les courbes des alinéas 5 et 6 sont les courbes A1, A1', B2 et B2' du théorème 8. Celles des alinéas 7 et 8 sont les courbes A1, A1', B2 et B2' du théorème 7.

3.4.4. Le lemme 13

Soit k un entier vérifiant les inégalités $2 \leqslant k < f(p)$ tel que $2^k - p$ soit un carré. Si k est impair, on a $k \geqslant 5$. Si k est pair, compte tenu de la remarque 1 et de la condition (2), on a

$$p = 2^{\frac{k}{2}+1} - 1, \quad \sqrt{2^k - p} = \frac{1-p}{2} \quad \text{et} \quad k \geqslant 8 \quad (\text{car } p \geqslant 29).$$

(i) Considérons la courbe elliptique d'équation

$$y^2 \;=\; x^3 \;+\; 2\sqrt{2^k-p}\; x^2 \;-\; p\; x.$$

Si k est impair, on retrouve la courbe E2 du théorème 4. Si k est pair, le modèle s'écrit

$$y^2 \;=\; x^3 \;+\; (1-p)\; x^2 \;-\; p\; x,$$

et l'on obtient la courbe F1 du théorème 4.

(ii) Considérons la courbe elliptique de modèle de Weierstrass

$$y^2 \;=\; x^3 \;+\; 4\sqrt{2^k - p}\; x^2 \;-\; 4p\; x.$$

Si k est impair, on retrouve la courbe E2' du théorème 6. Si k est pair le modèle s'écrit

$$y^2 \;=\; x^3 \;+\; 2(1-p)\; x^2 \;-\; 4p\; x,$$

qui est la courbe F1 du théorème 6.

Cela termine la démonstration de l'assertion $(**)$ et des théorèmes.

Compte tenu de la remarque 1, les corollaires résultent directement des théorèmes.

Chapitre III

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

Introduction

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

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

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

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

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

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

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

Comme on le signalait dans l'introduction, ces conjectures sont des conséquences de la conjecture (abc), et l'on a la conclusion annoncée dès que $p > \alpha + \beta \log(abc)$, où α et β sont deux constantes absolues > 0. Rappelons que sous les hypothèses de la conjecture 2, si ab est distinct de 1, on dispose d'un point «évident» $(x, y, z) \in S_p(a, b, c)$ tel que $xy = \pm 1$.

La méthode, aujourd'hui classique, que nous utiliserons pour aborder ces conjectures est la méthode modulaire, qui repose sur les travaux de G. Frey, K. Ribet, J.-P. Serre et A. Wiles sur les représentations modulaires (cf. [Fr], [Ri], [Se2] et [Wi]). Sans rentrer ici dans les détails, elle consiste à associer à tout élément de $S_p(a,b,c)$ une courbe elliptique sur $\mathbb{Q}$, appelée parfois courbe de Hellegouarch-Frey ou courbe de Frey, et à exploiter les propriétés galoisiennes de ses points de p-torsion. Signalons que, dans notre contexte, on peut associer à chaque élément de $S_p(a,b,c)$ deux courbes elliptiques définies sur $\mathbb{Q}$, qui ne sont pas isogènes en général, et qui permettent chacune la mise en œuvre de la méthode. Nous rappellerons son principe et certains de ses compléments au paragraphe 4. Cette approche permet par ailleurs de relier les conjectures 1 et 2 à d'autres plus centrales en théorie des nombres. Par exemple, elles se déduisent de la conjecture suivante concernant la comparaison galoisienne des points de torsion des courbes elliptiques (cf. [Da2] et le paragraphe 4) :

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

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

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

1. Sur la conjecture 1

Le premier résultat la concernant est dû à H. Darmon qui, en 1993, a démontré que $S_p(1,4,1)$ est vide si $p \geqslant 17$ ([Da1]). Il se trouve dans [Kr3] un résumé du fait que si ℓ est un nombre premier congru à 3 modulo 8, autre que 3, l'ensemble $S_p(1,\ell,1)$ est vide si p est assez grand en fonction de ℓ ; ce résultat n'a pas été rédigé par la suite. M. Bennett et C. Skinner en 2002 ont prouvé la conjecture 1 pour certains triplets d'entiers (a,b,c), pour lesquels abc est de la forme $2^\alpha \ell_1^\beta \ell_2^\gamma$, où ℓ_1 et ℓ_2 sont des nombres premiers inférieurs à 80 ([Be-Sk]). Par ailleurs, on peut trouver dans le chapitre I des résultats sur les ensembles $S_p(a,b,c)$ si abc est une puissance de 2. Ils ont été obtenus indépendamment par Bennett et Skinner dans *loc. cit.*. Par exemple, la conjecture 1 est vraie si ab est une puissance de 2 et $c = 1$. Ce sont à notre connaissance les seuls travaux déjà publiés sur cette conjecture.

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

À titre indicatif, considérons un entier $m \geqslant 1$. Explicitons l'énoncé de la conjecture 1 pour les triplets de la forme $(1,\ell^m,1)$: si $\ell^m + 1 \in \mathbb{Z}^2$ on vérifie que $m = 1$ et $\ell = 3$, et

si $\ell^m - 1 \in \mathbb{Z}^2$ on a $m = 1$ (cf. le lemme 3 du chapitre II). Par suite, si la condition suivante est satisfaite :

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

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

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

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

1) on a $\ell \equiv 1$ mod. 8 *et les deux assertions suivantes sont satisfaites :*

(i) les entiers $\ell - 1$, $\ell - 8$ *et* $\ell + 8$ *ne sont pas des carrés ;*

(ii) pour tout k *tel que* $7 \leqslant k < f(\ell)$, *les entiers* $\ell - 2^k$ *et* $\ell + 2^k$ *ne sont pas des carrés.*

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

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

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

Alors, pour tout nombre premier p *tel que*

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

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

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

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

Pour certains triplets (a, b, c) pour lesquels on ne sait pas démontrer la conjecture 1, on apporte dans le théorème 3 une réponse partielle en démontrant l'existence d'un en-

semble $\mathscr{P}$ de nombres premiers p de densité > 0 (dépendant de a, b, c), tels que $S_p(a, b, c)$ soit vide. On utilise pour cela un complément de la méthode modulaire, appelé méthode symplectique dans [Ha-Kr-2] (cf. 4.2). Tel est par exemple le cas des triplets $(1, \ell^m, 1)$ si $\ell \equiv 7$ mod. 8, $\ell \neq 7$ et si m est impair. Lorsque ℓ n'est pas trop grand, on peut expliciter un tel ensemble $\mathscr{P}$. On pourra trouver au paragraphe 7 des exemples illustrant cette situation, notamment si $\ell = 23$ (la condition 4 du théorème n'est pas vérifiée si $\ell = 23$: on a $2^{11} - 23 = 45^2$).

2. Sur la conjecture 2

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

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

1) En 1997, H. Darmon et L. Merel l'ont prouvée si $a = b = c = 1$ ([Da-Me]). Ils ont démontré que $S_p(1, 1, 1)$ est vide si $p \geqslant 7$. Il en est de même si $p = 5$ ([Po]).

2) On peut trouver dans le chapitre I une démonstration du fait que, pour tout $p \geqslant 7$, l'on a les égalités

$$S_p(1, 1, 2) = \Big\{(1, 1, -1), (1, 1, 1)\Big\} \quad \text{et} \quad S_p(8, 1, 1) = \Big\{(1, 1, 3), (1, 1, -3)\Big\}.$$

3) M. Bennett et C. Skinner dans [Be-Sk] ont aussi traité les cas où

$$a = b = 1 \quad \text{et} \quad c \in \Big\{2, 3, 5, 6, 10, 11, 13, 14, 15, 17, 19\Big\},$$

en montrant que $S_p(1, 1, c)$ est vide si $p \geqslant 7$ ne divise pas c (*loc. cit.*, th. 1.1 : le cas où p divise c semble avoir été omis).

Dans l'énoncé du théorème 1.2 de [Be-Sk] il y a des imprécisions concernant les triplets $(8, 1, 1)$, $(4, 1, 3)$ et $(64, 1, 7)$. On fournit au paragraphe 6 une preuve du fait que l'on a

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

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

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

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

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

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

Un nombre premier $p \geqslant 7$ étant donné, signalons qu'un cas particulier de l'étude faite dans [Kr6] est celui de la description des ensembles $S_p(1,1,c)$ pour les entiers $c \geqslant 3$ sans facteurs carrés vérifiant la condition suivante :

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

On démontre dans *loc. cit.*, en utilisant les résultats de [Da-Gr], que l'ensemble des entiers $c \geqslant 3$ sans facteurs carrés vérifiant cette condition, pour lesquels $S_p(1,1,c)$ est non vide, est fini. On prouve dans le chapitre IV qu'il n'existe pas de tels entiers c si $p \in \Big\{7,11,13,17\Big\}$ en utilisant la méthode de Chabauty elliptique.

Pour aborder ce problème, outre la méthode modulaire classique, on utilisera ici la méthode symplectique et un autre de ses compléments appelé méthode de réduction dans [Ha-Kr-2]. La méthode de réduction a aussi été utilisée pour la résolution de certaines équations ternaires dans [Kr5] et [Cr-Si]. On rappelera au paragraphe 4.1 son principe dans le cadre considéré ici. On l'illustrera à travers des exemples numériques au paragraphe 7. Elle permet par exemple de démontrer que $S_p(1,7,1)$ est vide si l'on a $11 \leqslant p < 10^4$. De même, $S_{11}(1,11^m,1)$ est vide pour tout $m \leqslant 10$. On obtiendra par ailleurs des informations nouvelles sur une conjecture de J.H.E. Cohn concernant la recherche des couples $(x,z) \in \mathbb{N}^2$ tels que $z^2+7=x^p$ ([Co2], p. 380).

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

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

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

En fait, si $S_p(1,|d|,1)$ est vide, alors si $(x,y) \in C_{d,p}(\mathbb{Q})$, on a $xy=0$ (lemme 11). Il résulte par exemple du théorème énoncé précédemment que pour tout nombre premier ℓ, si l'on a :

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

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

qu'il est vide si l'on a $5 \leqslant p < 10^4$; on démontre qu'il en est de même pour les nombres premiers $p \equiv 3$ mod. 4 tels que $2p+1$ soit premier.

Ces résultats permettent par ailleurs d'expliciter de nombreux exemples de courbes $C_{d,p}$ qui contredisent le principe de Hasse. En effet, $C_{d,p}$ possède des points rationnels sur tous les complétés de $\mathbb{Q}$. Par suite, si $C_{d,p}(\mathbb{Q})$ est vide, $C_{d,p}$ est un contre exemple à ce principe. Il en est ainsi des courbes $C_{11,p}$ et $C_{-11,p}$ pour tout $p \geqslant 7$.

Sommaire

1. Énoncé des résultats sur la conjecture 1

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

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

Introduisons la terminologie suivante :

1) on dira que ℓ vérifie la propriété (A) si les deux conditions suivantes sont réalisées :

(i) on a $\ell \equiv 1$ mod. 8 ;

(ii) pour tout k tel que $7 \leqslant k < f(\ell)$, les entiers $\ell - 2^k$ et $\ell + 2^k$ ne sont pas des carrés.

2) on dira que ℓ vérifie la propriété (B) si les deux conditions suivantes sont réalisées :

(i) on a $\ell \equiv 7$ mod. 8 ;

(ii) pour tout k tel que $7 \leqslant k < f(\ell)$, l'entier $2^k - \ell$ n'est pas un carré.

3) on dira que ℓ vérifie la propriété (C) si les deux conditions suivantes sont réalisées :

(i) on a $\ell \equiv 7$ mod. 8 ;

(ii) pour tout entier impair k tel que $1 \leqslant k \leqslant 164969$, l'entier $\ell^k + 2$ n'est pas un carré.

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

Théorème 1. *Soit n un entier naturel. Supposons que le couple (ℓ, n) vérifie l'une des quatre conditions suivantes :*

1) ℓ vérifie la propriété (A) et l'une des assertions suivantes est satisfaite :

(i) on a $n \geqslant 7$;
(ii) on a $n = 6$ et $\ell - 64$ n'est pas un carré ;
(iii) on a $n \in \{4, 5\}$ et les entiers $\ell - 16$, $\ell - 32$ et $\ell + 32$ ne sont pas des carrés ;
(iv) on a $n \in \{0, 3\}$ et les entiers $\ell - 1$, $\ell - 8$ et $\ell + 8$ ne sont pas des carrés ;
(v) on a $n = 2$ et pour tout $k \in \{4, 5, 6\}$, $\ell - 2^k$ et $\ell + 2^k$ ne sont pas des carrés ;
(vi) on a $n = 1$ et les entiers $2\ell - 1$ et $2\ell^2 - 1$ ne sont pas des carrés.

2) On a $\ell \equiv 3$ mod. 8 et l'une des assertions suivantes est satisfaite :

(i) on a $n \geqslant 6$;
(ii) on a $n \in \{0, 2, 3, 4, 5\}$ et $\ell \neq 3$;
(iii) on a $n = 1$ et $\ell - 2$ n'est pas un carré.

3) On a $\ell \equiv 5$ mod. 8 et l'une des assertions suivantes est satisfaite :

(i) on a $n \geqslant 6$;
(ii) on a $n \in \{4, 5\}$ et $\ell \neq 5$;
(iii) on a $n \in \{0, 3\}$ et $\ell - 1$ n'est pas un carré ;
(iv) on a $n = 2$ et $\ell - 4$ n'est pas un carré ;
(v) on a $n = 1$ et les entiers $2\ell - 1$ et $2\ell^2 - 1$ ne sont pas des carrés.

4) ℓ vérifie la propriété (B) et l'une des assertions suivantes est satisfaite :

(i) on a $n \neq 1$;
(ii) on a $n = 1$ et ℓ vérifie la propriété (C).

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

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

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

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

Théorème 2. *Supposons que l'une des quatre conditions suivantes soit réalisée :*

1) on a $\ell \equiv 1$ mod. 8 et les entiers $\frac{\ell^2+1}{2}$, $\frac{\ell+1}{2}$ et $\frac{\ell-1}{2}$ ne sont pas des carrés.

2) On a $\ell \equiv 3 \bmod 8$ *et* $\frac{\ell-1}{2}$ *n'est pas un carré.*

3) On a $\ell \equiv 5 \bmod 8$.

4) On a $\ell \equiv 7 \bmod 8$, $\ell \neq 23$ *et les entiers* $\frac{\ell^2+1}{2}$ *et* $\frac{\ell+1}{2}$ *ne sont pas des carrés.*

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

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

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

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

Corollaire.

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

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

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

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

1) on a $\ell \equiv 1 \bmod 8$ *et l'une des assertions suivantes est satisfaite :*

(i) on a $n = 1$ *et les entiers* $2\ell - 1$ *et* $2\ell^2 - 1$ *ne sont pas des carrés ;*
(ii) on a $n \in \{0, 3\}$ *et les entiers* $\ell - 1$, $\ell - 8$ *et* $\ell + 8$ *ne sont pas des carrés ;*
(iii) on a $n = 5$ *et les entiers* $\ell - 16$, $\ell - 32$ *et* $\ell + 32$ *ne sont pas des carrés.*

2) On a $\ell \equiv 7 \bmod 8$ *et l'une des assertions suivantes est satisfaite :*

(i) on a $n = 1$ *et* ℓ *vérifie la propriété* (C) *;*
(ii) on a $n \in \{0, 3\}$ *et* $\ell \neq 7$ *;*
(iii) on a $n = 5$ *et* $\ell \neq 7, 23, 31$.

Alors, pour tout entier naturel impair m, *il existe deux ensembles* $\mathscr{P}$ *et* $\mathscr{P}'$ *de nombres premiers (dépendant de* ℓ, m *et* n), *dont les densités sont* > 0, *tels que pour tout* p *dans* $\mathscr{P}$ *(resp.* $\mathscr{P}'$*), l'ensemble* $S_p(2^n, \ell^m, 1)$ *(resp.* $S_p(2^n\ell^m, 1, 1)$*) soit vide.*
Si δ *est la plus petite des densités de* $\mathscr{P}$ *et* $\mathscr{P}'$, *on a :*

$$\delta \geqslant \frac{1}{4^r} \quad si \quad n = 0 \quad et \quad \delta \geqslant \frac{1}{2^r} \quad si \quad n \in \{1, 3, 5\}.$$

Remarque 1.

1) Les propriétés (A), (B) et (C) sont souvent réalisées en pratique. En effet :

1.1) il y a 2384 nombres premiers congrus à 1 modulo 8 plus petits que 10^5 et il y en a 1812 qui vérifient la propriété (A).

1.2) Il y a 2399 nombres premiers plus petits que 10^5 congrus à 7 modulo 8. Il y en a 2256 qui vérifient la propriété (B) et 2333 qui vérifient la propriété (C). Les propriétés (B) et (C) sont toutes les deux satisfaites pour 2201 d'entre eux.

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

2. Courbes elliptiques

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

$$a,\ b \text{ et } c \text{ sont premiers entre eux deux à deux.}$$

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

(C_1) b est impair.

(C_2) c est sans facteurs carrés.

(C_3) Si cz est impair, on choisit z de sorte que l'on ait $cz \equiv -1$ mod. 4.

(C_4) Les entiers ax et by sont premiers entre eux.

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

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

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

alors, la condition (C_4) est satisfaite.

2.1. La courbe E_1

Soit E_1 la courbe d'équation de Weierstrass

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

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

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

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

Lemme 1. *Soit ℓ un nombre premier impair.*

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

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

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

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

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

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

Lemme 2.

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

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

3) Supposons ac impair.

3.1) Supposons y pair.

Si $p = 5$ et $v_2(y) = 1$, E_1 a réduction additive en 2, et l'on a $v_\ell\big(N_{E_1}\big) = 3$.

Si $p \geqslant 7$ ou $v_2(y) \geqslant 2$, E_1 a réduction multiplicative en 2, et l'on a $v_2\big(N_{E_1}\big) = 1$.

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

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

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

Comme conséquence directe des lemmes 1 et 2, on obtient :

Corollaire 1. *Soit Δ_{E_1} le discriminant minimal de E_1. On a*

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

Démonstration du lemme 2 : Les invariants standard b_2, b_4, b_6 et b_8 associés à l'équation (6) sont (cf. [Ta]) :

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

1) Si c est pair, $abxy$ est impair (condition (C_4)). Puisque c est sans facteur carré (condition (C_2)), on a donc

$$v_2(c_4) = 5, \quad v_2(c_6) \geqslant 8 \quad \text{et} \quad v_2(\Delta) = 9.$$

D'après le tableau IV de p.129 de [Pa], on a alors $v_2\big(N_{E_1}\big) = 8$. D'où l'assertion 1.

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

2.1) Supposons x pair. On a alors

$$v_2(c_4) = 6, \quad v_2(c_6) = 9 \quad \text{et} \quad v_2(\Delta) \geqslant 18.$$

Le tableau IV de *loc. cit.* entraîne alors $v_2\big(N_{E_1}\big) = 6$.

2.2) Supposons x impair. On a

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

Le tableau IV de *loc. cit.* entraîne le résultat si $v_2(a) \neq 3$.

Supposons $v_2(a) = 3$. Il s'agit de démontrer que le type de Néron de E_1 est I_2^*. On utilise pour cela l'algorithme de Tate (cf. [Ta], p. 49, 8.). Les conditions intervenant dans cet algorithme sont réalisées. Avec ses notations, on a

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

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

3) On suppose ac impair.

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

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

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

$$ax^p \equiv cz^2 \text{ mod. } 32.$$

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

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

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

3.1.1) Supposons $p = 5$ et $v_2(y) = 1$. Compte tenu du fait que b est impair (condition (C_1)), on a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, 11),$$

de sorte que le type de Kodaira de E_1 est II^* et l'on a $v_2\big(N_{E_1}\big) = 3$.

3.1.2) Supposons $p \geqslant 7$ ou bien $v_2(y) \geqslant 2$. Dans ce cas, on a

$$v_2(c_4) = 4, \quad v_2(c_6) = 6, \quad \text{et} \quad v_2(\Delta) \geqslant 13,$$

et l'on déduit de ce qui précède que l'équation (6) n'est pas minimale en 2, ce qui entraîne le résultat.

3.2) Supposons y impair.

3.2.1) Si x est pair, cz est impair (condition (C_4)). On a ainsi

$$v_2(c_4) = 6, \quad v_2(c_6) = 9 \quad \text{et} \quad v_2(\Delta) \geqslant 16.$$

Il en résulte que $v_2\big(N_{E_1}\big) = 6$.

3.2.2) Supposons x impair. Puisque ax^p et by^p sont impairs, z est pair. On a donc

$$v_2(c_4) = 4, \quad v_2(c_6) \geqslant 7 \quad \text{et} \quad v_2(\Delta) = 6.$$

On est dans le cas 3 ou 4 de Tate. On utilise la proposition 1 de [Pa] avec $r = 1$ et $t = 0$, ce qui entraîne le résultat.

4) L'assertion 4 est une conséquence de l'étude des cas précédents.

Cela termine la démonstration du lemme 2.

2.2. La courbe E_2

Soit E_2 la courbe d'équation de Weierstrass :

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

Les invariants standard associés à ce modèle sont

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

On a $\Delta \neq 0$, donc E_2 est une courbe elliptique sur $\mathbb{Q}$. On note N_{E_2} son conducteur.

Lemme 3. *Soit ℓ un nombre premier impair.*

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

La démonstration du lemme 3, étant directe et identique à celle du lemme 1, est omise ici. En revanche, bien qu'étant analogue à celle du lemme 2, nous détaillerons ici, vue la longueur des calculs et son importance dans la suite, la preuve du lemme qui suit.

Lemme 4.

1) Si c est pair, E_2 a réduction additive en 2, et l'on a $v_2\big(N_{E_2}\big) = 8$.

2) Supposons a pair.

2.1) Supposons x pair.

Si $p = 5$, $v_2(a) = 1$ et $v_2(x) = 1$, E_2 a bonne réduction en 2.

Si $p \geqslant 7$, ou $v_2(a) \geqslant 2$, ou $v_2(x) \geqslant 2$, E_2 a réduction multiplicative en 2, et l'on a $v_2\big(N_{E_2}\big) = 1$.

2.2) Supposons x impair. Dans ce cas, E_2 a réduction additive en 2 sauf si $v_2(a) \geqslant 6$.

Si $v_2(a) = 1$, *on a* $v_2\big(N_{E_2}\big) = 7$.
Si $v_2(a) = 2$, *on a*

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

Si $v_2(a) = 3$, *on a* $v_2\big(N_{E_2}\big) = 5$.
Si $v_2(a) \in \big\{4, 5\big\}$, *on a* $v_2\big(N_{E_2}\big) = 3$.
Si $v_2(a) = 6$, E_2 *a bonne réduction en* 2.
Si $v_2(a) \geqslant 7$, E_2 *a réduction multiplicative en* 2, *et l'on a* $v_2\big(N_{E_2}\big) = 1$.

3) Supposons ac impair.

3.1) Si y est pair, E_2 *a réduction additive en* 2, *et l'on a* $v_2\big(N_{E_2}\big) = 6$.

3.2) Supposons y impair et x pair.

Si $p = 5$ *et* $v_2(x) = 1$, E_2 *a réduction additive en* 2, *et l'on a* $v_2\big(N_{E_2}\big) = 3$.

Si $p \geqslant 7$ *ou* $v_2(x) \geqslant 2$, E_2 *a réduction multiplicative en* 2, *et l'on a* $v_2\big(N_{E_2}\big) = 1$.

3.3) Si xy est impair, E_2 *a réduction additive en* 2, *et l'on a*

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

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

On en déduit le résultat suivant :

Corollaire 2. *Soit* Δ_{E_2} *le discriminant minimal de* E_2. *On a*

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

Démonstration du lemme 4 : Les invariants b_2, b_4, b_6 et b_8 associés à l'équation (8) sont :

$$b_2 = 8cz, \quad b_4 = 2bcy^p, \quad b_6 = 0, \quad b_8 = -b^2c^2y^{2p}.$$

1) Si c est pair, $abxy$ est impair (condition (C_4)). Puisque c est sans facteurs carrés, on a donc

$$v_2(c_4) = 5, \quad v_2(c_6) \geqslant 8 \quad \text{et} \quad v_2(\Delta) = 9,$$

et le tableau IV de [Pa] entraîne le résultat.

2) Supposons a pair. D'après la condition (C_4), $bcyz$ est impair.

2.1) Supposons que l'on soit dans l'un des cas suivants :

$$x \text{ est pair ou bien } \Big(x \text{ est impair et } v_2(a) \geqslant 6\Big).$$

On a

$$v_2(c_4) = 4, \quad v_2(c_6) = 6 \quad \text{et} \quad v_2(\Delta) \geqslant 12.$$

On est donc dans un cas de Tate $\geqslant 7$. Par ailleurs, on a

$$by^p \equiv cz^2 \text{ mod. } 32.$$

Cela conduit à

$$b^2y^{2p} \equiv c^2z^4 \text{ mod. } 32 \quad \text{et} \quad 6bcy^p \equiv 6c^2z^2 \text{ mod. } 32.$$

Il s'agit alors de déterminer un entier r tel que

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \text{ mod. } 32, \tag{10}$$

autrement dit, tel que

$$-c^4z^4 + 6c^2z^2r^2 + 8czr^3 + 3r^4 \equiv 0 \text{ mod. } 32.$$

Compte tenu du fait que $cz \equiv -1$ mod. 4 (condition (C_3)), on vérifie que $r = 1$ convient. D'après l'assertion (b) de la proposition 4 de [Pa], utilisée avec $s = 1$, on constate que l'on est dans un cas de Tate $\geqslant 8$. D'après le tableau IV de *loc. cit.* l'équation (8) n'est donc pas minimale en 2. D'où l'assertion dans les cas envisagés.

2.2) Supposons x impair et $v_2(a) \leqslant 5$.

2.2.1) Si $v_2(a) = 1$, on a

$$v_2(c_4) = 4, \quad v_2(c_6) = 6 \quad \text{et} \quad v_2(\Delta) = 7,$$

et le tableau IV de [Pa] entraîne directement le résultat.

2.2.2) Supposons $v_2(a) = 2$. On a

$$v_2(c_4) = 4, \quad v_2(c_6) = 6 \quad \text{et} \quad v_2(\Delta) = 8.$$

On est dans un cas de Tate $\geqslant 6$. On utilise la proposition 3 de *loc. cit.* ; on a

$$bcy^p = c^2z^2 - acx^p \equiv c^2z^2 - 4 \text{ mod. } 8.$$

Puisque $cz \equiv -1$ mod. 4, on a donc

$$bcy^p \equiv 5 \text{ mod. } 8.$$

On vérifie alors, en considérant les deux restes de bcy^p modulo 16, que l'entier $r = 1$ satisfait la congruence (10). Par ailleurs, en posant $t = 2$, on a

$$bcy^p + 2cz + 1 - t^2 \equiv 0 \text{ mod. } 8.$$

On constate alors que la condition

$$\Big(bcy^p \equiv 5 \text{ mod. } 16 \text{ et } cz \equiv 3 \text{ mod. } 8\Big) \quad \text{ou} \quad \Big(bcy^p \equiv 13 \text{ mod. } 16 \text{ et } cz \equiv 7 \text{ mod. } 8\Big),$$

implique $v_2(bcy^p + 2cz + 1 - t^2) = 3$. De même, on vérifie que si l'on a

$$\Big(bcy^p \equiv 5 \text{ mod. } 16 \text{ et } cz \equiv 7 \text{ mod. } 8\Big) \quad \text{ou} \quad \Big(bcy^p \equiv 13 \text{ mod. } 16 \text{ et } cz \equiv 3 \text{ mod. } 8\Big),$$

alors $v_2(bcy^p+2cz+1-t^2) \geqslant 4$. Les propositions 3 et 4 de [Pa] entraînent alors le résultat.

2.2.3) Si $v_2(a) = 3$, on a

$$v_2(c_4) = 4, \quad v_2(c_6) = 6 \quad \text{et} \quad v_2(\Delta) = 9,$$

d'où le résultat (tableau IV de [Pa]).

2.2.4) Supposons $v_2(a) \in \big\{4, 5\big\}$. On a

$$(v_2(c_4), v_2(c_6), v_2(\Delta) \in \big\{(4, 6, 10), (4, 6, 11)\big\}.$$

On est dans un cas de Tate $\geqslant 7$. Par ailleurs, on a

$$bcy^p = c^2z^2 - acx^p \equiv c^2z^2 \text{ mod. } 16.$$

Puisque $cz \equiv 3$ ou 7 mod. 8, on a donc

$$bcy^p \equiv 1 \text{ ou } 9 \text{ mod. } 16.$$

On vérifie alors que l'entier $r = 1$ satisfait la congruence (10). En posant $s = 1$, on a $2cz + 3 - s^2 \equiv 0$ mod. 4, on est ainsi dans un cas de Tate $\geqslant 8$, ce qui entraîne le résultat.

3) On suppose ac impair.

3.1) Supposons y pair. Dans ce cas, z est impair (condition (C_4)) et l'on a

$$v_2(c_4) = 6, \quad v_2(c_6) = 9 \quad \text{et} \quad v_2(\Delta) \geqslant 16,$$

d'où l'assertion (tableau IV de [Pa]).

3.2) Supposons y impair et x pair. L'entier z est impair. On a donc

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

On est dans un cas de Tate $\geqslant 7$. On a

$$by^p \equiv cz^2 \text{ mod. } 32.$$

On en déduit que l'entier $r = 1$ vérifie la congruence (10). On a $v_2(2cz + 3 - s^2) \geqslant 2$ avec $s = 1$, donc on est dans un cas de Tate $\geqslant 8$.

3.2.1) Si $p = 5$ et $v_2(x) = 1$, compte tenu du fait que b est impair, on a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, 11),$$

le type de Kodaira de E_2 est II* et l'on a $v_2\big(N_{E_2}\big) = 3$.

3.2.2) Si $p \geqslant 7$ ou bien $v_2(x) \geqslant 2$, on a

$$v_2(c_4) = 4, \quad v_2(c_6) = 6 \quad \text{et} \quad v_2(\Delta) \geqslant 13,$$

et l'équation (8) n'est pas minimale en 2, d'où le résultat.

3.3) Supposons xy impair. Dans ce cas, z est pair et l'on a

$$v_2(c_4) = 4, \quad v_2(c_6) \geqslant 7 \quad \text{et} \quad v_2(\Delta) = 6.$$

On est dans le cas 3 ou 4 de Tate. La proposition 1 de [Pa], utilisée avec $r = 1$ et $t = 0$, entraîne alors le résultat.

4) L'assertion 4 se déduit de ce qui précède.

Cela termine la démonstration du lemme 4.

3. Représentations galoisiennes

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

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

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

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

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

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

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

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

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

2) Supposons $p = 7$. La courbe modulaire $Y_0(14)$ est la courbe elliptique notée 14A1 dans les tables de [Cr1] ([Li], p. 45). On en déduit que $Y_0(14)$ possède exactement deux points rationnels sur $\mathbb{Q}$. Ils correspondent à deux classes de $\overline{\mathbb{Q}}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ d'invariants modulaires -15^3 et 255^3 : en effet, ce sont les invariants modulaires respectivement des courbes notées 49A1 et 49A2 dans [Cr1] et elles ont un sous-groupe 14 stable par Galois.

Notons j_{E_i} l'invariant modulaire de E_i.

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

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

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

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

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

Il résulte alors des assertions 1 des lemmes 2 et 4 que c est impair. D'après les lemmes 1 et 3 on a donc $c = 7$ et $b = 1$.

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

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

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

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

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

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

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

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

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

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

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

Si $p = 5$, il est plus difficile d'obtenir un énoncé analogue à la proposition 1 permettant de décider à priori si $\rho_p^{E_i}$ est ou non irréductible. Cela est dû au fait que la courbe modulaire $Y_0(10)$ est isomorphe sur $\mathbb{Q}$ à la droite projective $\mathbb{P}^1$. Néanmoins, il y a des situations simples, dans lesquelles on peut conclure (cf. le paragraphe 7).

On suppose désormais que la condition suivante est réalisée :

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

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

Pour $i \in \{1, 2\}$, soit k le poids de $\rho_p^{E_i}$ défini par Serre dans [Se2] : il est le même pour E_1 et E_2, comme on le constate ci-dessous tout au moins si p ne divise pas c, ce qui est le cas qui nous intéressera dans la suite :

Proposition 2.

1) Si p divise ab, on a $k = p + 1$.

2) Si p ne divise pas abc, on a $k = 2$.

Démonstration : 1) Si p divise ab, E_i a réduction multiplicative en p (lemmes 1 et 3). D'après la condition (C_5), p ne divise pas $v_p(ab)$, i.e. p ne divise pas $v_p(j_{E_i})$. La proposition 5 de [Se2] implique alors $k = p + 1$.

2) Supposons que p ne divise pas abc. Si p ne divise pas xy, E_i a bonne réduction en p. Si p divise xy, E_i a réduction multiplicative en p et dans ce cas, p divise $v_p(j_{E_i})$. Cela entraîne $k = 2$ (*loc. cit.*). D'où le résultat.

Soit $N\big(\rho_p^{E_i}\big)$ le conducteur de $\rho_p^{E_i}$ défini par Serre dans [Se2]. C'est un entier premier à p qui divise N_{E_i}. Il est donné dans les deux énoncés suivants, qui résultent directement des lemmes 1 à 4, des corollaires 1 et 2, et par exemple de la proposition p. 28 de [Kr2].

Proposition 3. *On a*

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

où t est l'entier défini ci-dessous.

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

2) Si a est pair, on a

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

3) Supposons ac impair.

3.1) Supposons y pair.

Si $p = 5$ et $v_2(y) = 1$, on a $t = 3$.

Si $p \geqslant 7$ ou $v_2(y) \geqslant 2$, on a $t = 1$.

3.2) Si y est impair, on a

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

Proposition 4. *On a*

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

où t est l'entier défini ci-dessous.

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

2) Supposons a est pair.

2.1) Supposons x pair.

Si $p = 5$, on a

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

Si $p \geqslant 7$, on a

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

2.2) Supposons x impair.

Si $v_2(a) = 1$, on a $t = 7$.
Si $v_2(a) = 2$, on a

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

Si $v_2(a) = 3$, on a $t = 5$.
Si $v_2(a) \in \{4, 5\}$, on a $t = 3$.

Si $v_2(a) = 6$, on a $t = 0$.
Si $v_2(a) \geqslant 7$, on a $t = 1$.

3) Supposons ac impair.

3.1) Si y est pair, on a $t = 6$.

3.2) Supposons y impair et x pair.

Si $p = 5$ et $v_2(x) = 1$, on a $t = 3$.

Si $p \geqslant 7$ ou $v_2(x) \geqslant 2$, on a $t = 1$.

3.3) Si xy est impair, on a

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

4. La méthode modulaire

Cette méthode est maintenant bien connue et a été exposée dans de nombreux travaux (cf. par exemple [Se3]). Rappelons en quoi elle consiste dans notre contexte.

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

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

Dans le cas où f est normalisée, i.e. si $a_1(f) = 1$, les $a_n(f)$ sont des entiers algébriques, et l'extension $\mathbb{Q}(f)$ de $\mathbb{Q}$ obtenue en adjoignant à $\mathbb{Q}$ les coefficients $a_n(f)$ est une extension finie de $\mathbb{Q}$ qui est totalement réelle. Pour tout nombre premier ℓ ne divisant pas N, $a_\ell(f)$ est valeur propre de l'opérateur de Hecke T_ℓ opérant sur $S_k^+(N)$. Il existe exactement $g_k^+(N)$ newforms normalisées. Elles forment une base de $S_k^+(N)$.

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

Dans ce qui suit, l'indice i désigne l'un des entiers 1 ou 2 : on a $i \in \big\{1, 2\big\}$. Considérons la courbe elliptique $E_i/\mathbb{Q}$ associée à (x, y, z) et à (a, b, c) comme dans le paragraphe 2.

Soient $\rho_p^{E_i}$ la représentation de $G_{\mathbb{Q}}$ dans $\mathrm{Aut}\big(E_i[p]\big)$, k son poids et $N\big(\rho_p^{E_i}\big)$ son conducteur : ils sont donnés dans les propositions 2, 3 et 4. Soit

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

la fonction L de Hasse-Weil de E_i. Il est maintenant démontré que E_i est modulaire ([Wi], [Br-Co-Di-Ta]). Supposons que $\rho_p^{E_i}$ soit irréductible. Dans ce cas, il existe une newform normalisée f_i de $S_k^+\Big(N\big(\rho_p^{E_i}\big)\Big)$,

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

et une place $\mathfrak{P}_i$ de $\overline{\mathbb{Q}}$ de caractéristique résiduelle p telles que, pour tout nombre premier ℓ, on ait (cf. par exemple [Se3], 2) :

$$a_\ell(f_i) \;\equiv\; a_\ell(E_i) \bmod \mathfrak{P}_i, \qquad \text{si } \ell \text{ ne divise pas } pN_{E_i}, \tag{11}$$

$$a_\ell(f_i) \equiv \pm(\ell+1) \bmod \mathfrak{P}_i, \qquad \text{si } \ell \text{ divise } N_{E_i} \text{ et } \ell \text{ ne divise pas } pN\big(\rho_p^{E_i}\big). \tag{12}$$

Pour démontrer que l'existence du point (x, y, z) envisagé conduit à une contradiction, il suffit donc de prouver, en considérant au choix $\rho_p^{E_1}$ ou $\rho_p^{E_2}$, qu'il n'existe pas de tel couple $(f_1, \mathfrak{P}_1)$ ou $(f_2, \mathfrak{P}_2)$, pour lequel les congruences (11) et (12) soient satisfaites. En pratique, ce choix est dicté par les conducteurs de ces représentations.

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

(i) on a $k = 2$;

(ii) pour tout $n \geqslant 1$ le coefficient $a_n(f_i)$ appartient à $\mathbb{Z}$.

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

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

où $a_n(F_i)$ est le n-ième coefficient de la fonction de L de F_i. La courbe F_i est unique à $\mathbb{Q}$-isogénie près. Le $G_{\mathbb{Q}}$-module $F_i[p]$ des points de p-torsion de F_i est isomorphe à $E_i[p]$ et l'on a ([Kr-Oe], prop. 3) :

$$a_\ell(F_i) \;\equiv\; a_\ell(E_i) \bmod p, \qquad \text{pour tout } \ell \text{ premier ne divisant pas } N_{E_i}\,. \tag{13}$$

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

$$\mu(n) = n \prod_{\substack{l \mid n \\ l \text{ premier}}} \left(1 + \frac{1}{l}\right), \quad F(n) = \left(\sqrt{\frac{\mu(n)}{6}} + 1\right)^{2\, g_2^+(n)}, \quad G(n) = \left(\sqrt{\frac{\mu\big(\text{ ppcm } (4, n)\big)}{6}} + 1\right)^2. \tag{14}$$

Proposition 5. *Pour $i = 1$ ou $i = 2$, supposons que l'on ait*

$$abc \not\equiv 0 \text{ mod. } p \quad et \quad p > \mathrm{Max}\Big(F\Big(N\big(\rho_p^{E_i}\big)\Big), G\Big(N\big(\rho_p^{E_i}\big)\Big)\Big).$$

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

Démonstration : Puisque p ne divise pas abc, on a $k = 2$ (prop. 2). D'après l'inégalité $p > F\Big(N\big(\rho_p^{E_i}\big)\Big)$, il existe une courbe elliptique $F_i/\mathbb{Q}$, de conducteur $N\big(\rho_p^{E_i}\big)$, telle que les $G_{\mathbb{Q}}$-modules $E_i[p]$ et $F_i[p]$ soient isomorphes ([Kr4], th. 3). Par ailleurs, en utilisant l'inégalité $p > G\Big(N\big(\rho_p^{E_i}\big)\Big)$, on déduit, de la même façon que dans la démonstration du théorème 4 de *loc. cit.*, que l'on a l'assertion suivante :

$$a_\ell(F_i) \equiv \ell + 1 \text{ mod. } 2, \qquad \text{pour tout nombre premier } \ell \text{ qui ne divise pas } 2N\big(\rho_p^{E_i}\big).$$

Compte tenu du théorème de densité de Chebotarev, cela entraîne que F_i a un point d'ordre 2 rationnel sur $\mathbb{Q}$. D'où le résultat.

Lorsqu'il n'existe pas de courbes elliptiques sur $\mathbb{Q}$, de conducteur $N\big(\rho_p^{E_i}\big)$ et ayant au moins un point d'ordre 2 sur $\mathbb{Q}$, ce résultat permet d'obtenir la contradiction souhaitée, tout au moins si p est assez grand. Nous l'utiliserons pour démontrer les théorèmes 1 et 2. La proposition 5 permet par ailleurs de démontrer que la conjecture 3 énoncée dans l'introduction entraîne les conjectures 1 et 2.

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

4.1. La méthode de réduction

On conserve les hypothèses faites et les notations utilisées précédemment. En particulier, pour $i \in \{1, 2\}$, il existe un couple $(f_i, \mathfrak{P}_i)$ vérifiant les congruences (11) et (12). La méthode de réduction permet d'éliminer certains couples $(f, \mathfrak{P})$ comme ci-dessus parmi ceux susceptibles de vérifier ces congruences.

Considèrons un nombre premier q satisfaisant les deux conditions suivantes :

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

La condition (ii) signifie que q ne divise pas $abcxy$ (lemmes 1 et 3). Par suite, E_1 a bonne réduction en q si et seulement si tel est le cas de E_2. Par exemple, la condition (ii) est satisfaite si pour $i = 1$ ou $i = 2$:

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

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

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

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

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

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

$$\alpha^n = \beta^n = 1 \quad \text{et} \quad \bar{a}\alpha + \bar{b}\beta = \bar{c}\,\gamma^2. \tag{15}$$

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

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

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

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

Lemme 5. *Il existe un élément $\xi \in R_q$ tel que l'on ait*

$$a_q(f_i) \equiv a\big(\widetilde{E_{i,\xi}}\big) \bmod . \mathfrak{P}_i. \tag{16}$$

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

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

vérifie les égalités (15) i.e. ξ appartient à R_q. Soit $\widetilde{E_i}$ la courbe elliptique sur $\mathbb{F}_q$ déduite de E_i par réduction modulo q. On a $\widetilde{E_i} = \widetilde{E_{i,\xi}}$, d'où l'on déduit que $a_q(E_i) = a\big(\widetilde{E_{i,\xi}}\big)$. La congruence (11) entraîne alors le résultat.

La méthode de réduction consiste en pratique à sélectionner un nombre premier q congru à 1 modulo p satisfaisant la condition (iii). On explicite ensuite tous les éléments ξ de R_q et on calcule les entiers $a\big(\widetilde{E_{i,\xi}}\big)$ correspondants. Si aucun de ces entiers ne vérifie la congruence (16), le couple $(f_i, \mathfrak{P}_i)$ ne satisfait pas les congruences (11) et (12) et est ainsi écarté. Cette méthode utilisée avec un nombre premier $q \not\equiv 1 \bmod . p$ ne permet pas d'éliminer un tel couple $(f_i, \mathfrak{P}_i)$ car dans ce cas on a $\mathbb{F}_q^{*p} = \mathbb{F}_q^*$ et en pratique le lemme 5 ne peut pas être contredit.

4.2. La méthode symplectique

Pour $i = 1$ ou $i = 2$, considérons un couple $(f_i, \mathfrak{P}_i)$ vérifiant les congruences (11) et (12). On suppose que f_i « correspond » à une courbe elliptique $F_i/\mathbb{Q}$ de conducteur $N\big(\rho_p^{E_i}\big)$ (auquel cas on peut prendre $\mathfrak{P}_i = p\mathbb{Z}$). Les $G_{\mathbb{Q}}$-modules $F_i[p]$ et $E_i[p]$ sont isomorphes. Afin d'écarter cette situation, la méthode envisagée ici consiste à utiliser le résultat suivant, obtenu à partir d'un critère permettant de décider si les modules $E_i[p]$ et $F_i[p]$ sont ou non symplectiquement isomorphes ([Ha-Kr-2]). On note Δ_{F_i} le discriminant minimal de F_i.

Proposition 6. *Soient ℓ_1 et ℓ_2 deux nombres premiers distincts, autres que p. Supposons que les deux conditions suivantes soient réalisées (pour $i = 1$ ou $i = 2$) :*

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

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

Alors,

$$v_{\ell_1}\big(\Delta_{E_i}\big)v_{\ell_2}\big(\Delta_{E_i}\big) \bmod p \quad \textit{et} \quad v_{\ell_1}\big(\Delta_{F_i}\big)v_{\ell_2}\big(\Delta_{F_i}\big) \bmod p,$$

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

5. Démonstrations des théorèmes

On pose

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

5.1. Démonstration du théorème 1

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

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

Pour certaines autres valeurs de n, quant à l'effectivité du théorème 1, on peut diminuer sensiblement la constante $C(\ell)$ comme dans le cas où $n = 0$. Les constantes obtenues étant néanmoins loin d'êtres optimales, nous ne les avons pas explicitées dans l'énoncé du théorème 1 afin d'en simplifier sa présentation.

5.1.1. Cas où $n = 0$

Démontrons le lemme suivant :

Lemme 6. *Soient M un entier naturel non nul et p un nombre premier tels que*

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

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

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

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

Par suite, $\rho_p^{E_1}$ et $\rho_p^{E_2}$ sont irréductibles (prop. 1) et l'on est dans l'un des quatre cas suivants (prop. 3 et 4) :

(i) v est pair et $N\big(\rho_p^{E_1}\big) = 2\ell$;

(ii) u est pair et $N\big(\rho_p^{E_2}\big) = 2\ell$;

(iii) v est impair, on a $u \equiv -1$ mod. 4 et $N\big(\rho_p^{E_1}\big) = 32\ell$;

(iv) v est impair, on a $u \equiv 1$ mod. 4 et $N\big(\rho_p^{E_2}\big) = 32\ell$.

Par ailleurs, on a (cf. par exemple [Ha-Kr-2]) :

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

Dans chacun des cas ci-dessus, on vérifie que l'on a l'inégalité (cf. formules (14))

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

Puisque l'on a $p \neq \ell$, on déduit alors de la proposition 5 qu'il existe une courbe elliptique sur $\mathbb{Q}$ de conducteur 2ℓ ou 32ℓ possédant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. Si l'on a $\ell \geqslant 31$, compte tenu des hypothèses faites sur ℓ, les corollaires des théorèmes 1 et 5 du chapitre II entraînent une contradiction à l'existence d'une telle courbe elliptique. Si l'on a $\ell < 31$, on obtient directement une contradiction en utilisant les tables de [Cr1]. D'où le lemme.

Le théorème se déduit comme suit : considérons un entier $m \geqslant 1$ et un nombre premier p vérifiant les égalités (2) et supposons qu'il existe un élément (x, y, z) de $S_p(1, \ell^m, 1)$. D'après le lemme 6, ℓ divise x. Les entiers x, y et z étant premiers entre eux, on en déduit que ℓ ne divise pas y. L'inégalité $m < p$ entraîne alors que m est pair et que $2v_\ell(z) = m$. Posons $x = \ell^\alpha x_1$, $z = \ell^{\frac{m}{2}} z_1$ avec $\alpha \geqslant 1$ et $v_\ell(x_1) = v_\ell(z_1) = 0$. On a

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

Il en résulte que $(y, \ell^{\alpha-1}x_1, z_1)$ appartient à $S_p(1, \ell^{p-m}, 1)$. Par ailleurs, on a $1 \leqslant m < p$, d'où les inégalités $p > p - m > 0$. Puisque ℓ ne divise pas y, le lemme 6, utilisé avec $M = p - m$, conduit alors à une contradiction. D'où le théorème 1 si $n = 0$.

5.1.2. Cas où $n \geqslant 1$

On utilise dans ce cas le résultat suivant :

Lemme 7. *Soient M un entier naturel non nul et p un nombre premier tels que*

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

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

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

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

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

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

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

On est amené à distinguer les deux cas ci-dessous.

1) Supposons $s \in S_p\big(2^n, \ell^M, 1\big) \bigcup S_p\big(2^n\ell^M, 1, 1\big)$. La représentation $\rho_p^{E_2}$ est irréductible et l'on a (prop. 4) :

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

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

On vérifie par ailleurs que l'on a

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

Il en résulte l'inégalité

$$\mathrm{Max}\Big(F\Big(N\big(\rho_p^{E_2}\big)\Big), G\Big(N\big(\rho_p^{E_2}\big)\Big)\Big) \leqslant C(\ell). \tag{17}$$

D'après la proposition 5, il existe donc une courbe elliptique de conducteur $N\big(\rho_p^{E_2}\big)$ ayant au moins un point d'ordre 2 sur $\mathbb{Q}$. Les hypothèses faites sur le couple (ℓ, n) entraînent

alors une contradiction : dans le cas où $\ell \geqslant 31$, cela résulte du théorème 2 de B. Setzer [Set] et des corollaires des théorèmes 1 à 5 et 7 du chapitre II (dans le cas où $n = 1$, on notera que si $2\ell^2 - 1$ est un carré on a $\ell \equiv 1 \bmod. 4$ (lemme 3 de *loc. cit.*)). Si $\ell \leqslant 31$, on le constate en utilisant les tables de [Cr1] et [Cr2] (on utilise cette dernière référence si $n = 1$ et $\ell = 19$).

2) Supposons $s \in S_p\big(2^{p-n}, \ell^M, 1\big) \bigcup S_p\big(2^{p-n}\ell^M, 1, 1\big)$. Par hypothèse, on a $p - n \geqslant 7$. On a ainsi (prop. 4) :

$$N\big(\rho_p^{E_2}\big) = 2\ell.$$

L'inégalité (17) est satisfaite. Comme ci-dessus, on déduit de la proposition 5 l'existence d'une courbe elliptique sur $\mathbb{Q}$ de conducteur 2ℓ et ayant au moins un point d'ordre 2 sur $\mathbb{Q}$. Les hypothèses faites sur le couple (ℓ, n) conduisent de nouveau à une contradiction. En effet, si ℓ vérifie la propriété (A) ou (B), il n'existe pas de telles courbes elliptiques et il en est de même si ℓ est congru à 3 ou 5 modulo 8 (cf. le chapitre II et [Cr1]). D'où le lemme.

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

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

1) Supposons que (x, y, z) appartienne à $S_p(2^n, \ell^m, 1)$. D'après l'assertion (i) du lemme 7, il existe deux entiers naturels α et β tels que l'on ait

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

On distingue alors plusieurs cas.

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

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

d'où il résulte que $(2^{\beta-1}y_1, x, z_1)$ appartient à $S_p(2^{p-n}\ell^m, 1, 1)$. Puisque x est impair et que ℓ ne divise pas x, l'assertion (ii) du lemme 7 entraîne ainsi une contradiction.

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

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

et $(\ell^{\alpha-1}x_1, y, z_1)$ appartient à $S_p(2^n\ell^{p-m}, 1, 1)$. Compte tenu du fait que y est impair et que ℓ ne divise pas y, l'assertion (ii) du lemme 7, utilisée avec $M = p - m$, conduit de nouveau à une contradiction.

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

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

et $(2^{\beta-1}y_1, \ell^{\alpha-1}x_1, z_1)$ appartient à $S_p(2^{p-n}, \ell^{p-m}, 1)$. Par ailleurs, l'hypothèse faite entraîne que ℓ ne divise pas y et que x est impair. On obtient ainsi une contradiction (assertion (i) du lemme 7).

2) Si (x, y, z) appartient à $S_p(2^n\ell^m, 1, 1)$, il existe, d'après le lemme 7, deux entiers naturels α et β tels que l'on ait

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

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

Cela termine la démonstration du théorème 1.

5.2. Démonstration du théorème 2

Posons

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

Lemme 8. *Soient M un entier naturel non nul et p un nombre premier tels que*

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

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

Démonstration : On suppose que ℓ ne divise pas u, les conditions $(C_1), \cdots, (C_5)$ étant satisfaites par (u, v, w) et $(1, \ell^M, 2)$. Soit E_2 la courbe elliptique associée à ces triplets par l'équation (8). On a $p \geqslant 11$ et $p \neq \ell$, $\rho_p^{E_2}$ est irréductible et l'on a (prop. 4) :

$$N\big(\rho_p^{E_2}\big) = 256\ell.$$

On a $g_2^+(256\ell) = 8(\ell-1)$, d'où l'inégalité

$$\mathrm{Max}\Big(F\Big(N\big(\rho_p^{E_2}\big)\Big), G\Big(N\big(\rho_p^{E_2}\big)\Big)\Big) \leqslant H(\ell).$$

Il existe donc une courbe elliptique sur $\mathbb{Q}$ de conducteur 256ℓ ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$ (prop. 5). Si $\ell \geqslant 31$, le corollaire du théorème 8 du chapitre II entraîne une contradiction (on notera que si $\ell \equiv 1, 5$ mod. 8 et si $\frac{\ell+1}{2}$ n'est pas un carré, tel est aussi le cas de $\frac{\ell^2-1}{2}$; la même conclusion vaut si $\ell \equiv 3, 7$ mod. 8 et si $\frac{\ell-1}{2}$ n'est pas un carré). Si $\ell < 31$, on obtient une contradiction en utilisant [Cr1] et [Cr2]. D'où le résultat.

Considérons alors un entier $m \geqslant 1$ et un nombre premier p vérifiant l'inégalité (4). Supposons qu'il existe un élément (x, y, z) de $S_p(1, \ell^m, 2)$. D'après le lemme 8, ℓ divise x. Puisque l'on a $m < p$, l'entier m est pair et $2v_\ell(z) = m$. Posons $x = \ell^\alpha x_1$ et $z = \ell^{\frac{m}{2}} z_1$ où l'on a $v_\ell(x_1) = v_\ell(z_1) = 0$. On a l'égalité

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

d'où l'on déduit que $(y, \ell^{\alpha-1}x_1, z_1)$ appartient à $S_p(1, \ell^{p-m}, 2)$. L'entier y n'est pas divisible par ℓ. Par suite, le lemme 8, utilisé avec $M = p - m$, entraîne une contradiction. D'où le théorème 2.

5.3. Démonstration du théorème 3

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

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

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

$$p > \mathrm{Max}\Big(m, C(\ell)\Big). \tag{18}$$

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

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

5.3.1. Cas où $n = 0$

On peut supposer que (x, y, z) appartient à $S_p\big(1, \ell^m, 1\big)$. Soient E_1 et E_2 les courbes elliptiques associées à (x, y, z) et $(1, \ell^m, 1)$. On est dans l'un des quatre cas suivants (prop. 3 et 4) :

(i) y est pair et $N\big(\rho_p^{E_1}\big) = 2\ell$;

(ii) x est pair et $N\big(\rho_p^{E_2}\big) = 2\ell$;

(iii) y est impair, on a $x \equiv -1$ mod. 4 et $N\big(\rho_p^{E_1}\big) = 32\ell$;

(iv) y est impair, on a $x \equiv 1$ mod. 4 et $N\big(\rho_p^{E_2}\big) = 32\ell$.

D'après les hypothèses faites sur ℓ, il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur 32ℓ ayant au moins un point d'ordre 2 sur $\mathbb{Q}$ (cf. cor. du th. 5 du chap. II et [Cr1]). On déduit alors de la proposition 5 et de (18) que l'on est en fait dans le cas (i) ou (ii). Il résulte de plus de cette proposition, que l'une des assertions suivantes est vérifiée :

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

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

Si y est pair, E_1 a réduction multiplicative en 2 et en ℓ (lemmes 1 et 2). D'après le corollaire 1, on a dans ce cas :

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

Par ailleurs, si y est impair et x est pair, E_2 a aussi réduction multiplicative en 2 et en ℓ (lemmes 3 et 4) et l'on a (cor. 2) :

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

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

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

En utilisant la proposition 6, avec $\ell_1 = 2$ et $\ell_2 = \ell$, on déduit de l'assertion (v) ou (vi) que l'on a :

$$\left(\frac{n_h}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{t_k}{p}\right) = 1. \tag{19}$$

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

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

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

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

Posons $\mathscr{P} = \mathscr{P}_1 \cap \mathscr{P}_2$. D'après la condition (19), p n'appartient pas à $\mathscr{P}$. Tout revient alors à démontrer que $\mathscr{P}$ est de densité $1/2^s$ pour un certain entier $s \leqslant 2r$. D'après le théorème de densité de Chebotarev, il suffit pour cela de vérifier que $\mathscr{P}$ n'est pas vide. Soit S l'ensemble des nombres premiers q vérifiant les deux conditions suivantes :

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

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

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

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

5.3.2. Cas où $n \in \{1, 3, 5\}$

Posons $t := (x, y, z)$. Soit E_2 la courbe elliptique associée à t et l'un des triplets $(2^n, \ell^m, 1)$ et $(2^n\ell^m, 1, 1)$. D'après la proposition 4, on est dans l'un des deux cas suivants :

(i) x est pair et $N(\rho_p^{E_2}) = 2\ell$;

(ii) x est impair et l'on a

$$N\big(\rho_p^{E_2}\big) = \begin{cases} 128\ell & \text{si } n = 1 \\ 32\ell & \text{si } n = 3 \\ 8\ell & \text{si } n = 5. \end{cases}$$

Il résulte des hypothèses faites sur ℓ et de la proposition 5, que l'on est dans le cas (i) (cf. cor. des th. 3, 5 et 7 du chap. II et [Cr1], [Cr2]). La courbe E_2 a donc réduction multiplicative en 2 et ℓ, et l'on a :

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

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

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

On déduit des propositions 5 et 6 l'existence de $h \in \{1, \cdots, r\}$ tel que

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

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

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

dont on vérifie qu'il est de densité $1/2^s$ avec $s \leqslant r$. D'où le théorème 3.

6. Description de $S_p(4, 1, 3)$ et $S_p(64, 1, 7)$

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

Rappelons le résultat bien connu suivant que l'on utilisera à plusieurs reprises, qui est une conséquence de la théorie de la courbe de Tate (cf. [Si1], p. 355) :

Lemme 9. *Soient $A/\mathbb{Q}$ une courbe elliptique et ℓ, p deux nombres premiers distincts. Supposons que A ait en ℓ réduction additive et que $v_\ell(j_A) < 0$. Soit n_ℓ l'ordre de l'image par ρ_p^A d'un sous-groupe d'inertie en ℓ de $G_\mathbb{Q}$. On a $n_\ell = 2$ si p divise $v_\ell(j_A)$ et $n_\ell = 2p$ sinon.*

6.1. L'équation $4x^p + y^p = 3z^2$

Soit p un nombre premier $\geqslant 7$. On va démontrer que l'on a

$$S_p(4,1,3) = \big\{(1,-1,1),(1,-1,-1)\big\}. \tag{20}$$

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

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

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

autrement dit, $s := (2^{n-1}y_1, x, z_1)$ appartient à $S_p(2^{p-2},1,3)$. La représentation $\rho_p^{E_2(s)}$ est irréductible de poids 2 (prop. 1 et 2) et l'on a (prop. 4) :

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

On a $g_2^+(18) = 0$ et $g_2^+(72) = 1$. Par suite, on a $n = 1$, $p = 7$ et $\rho_7^{E_2(s)}$ est isomorphe à ρ_7^E, où E est la courbe elliptique notée 72A1 dans les tables de [Cr1]. La courbe E a réduction additive en 3, et l'on a $v_3(j_E) = -1$. D'après le lemme 9, l'image par ρ_7^E d'un sous-groupe d'inertie en 3 de $G_\mathbb{Q}$ est d'ordre 14. Par ailleurs, $E_2(s)$ a réduction additive en 3 et $j_{E_2(s)}$ est entier en 3. Le défaut de semi-stabilité de $E_2(s)$ en 3 étant d'ordre 4 ou 12 (lemme 3 et [Kr1], p. 356), cela conduit à une contradiction. D'où notre assertion.

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

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

3) Prouvons maintenant l'égalité (20). Puisque x est impair, on a :

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

On a $g_2^+(36) = 1$ et $g_2^+(144) = 2$. Par ailleurs, il existe deux classes de $\mathbb{Q}$-isogénie de courbes elliptiques de conducteur 144 ([Cr1], p. 124). On en déduit que $\rho_p^{E_2(t)}$ est isomorphe à ρ_p^F, où F est une courbe elliptique de conducteur 36 ou 144. On peut supposer que F est l'une des trois courbes elliptiques notées 36A1, 144A1 et 144B1 dans les tables de *loc. cit.*. Le cas où F est la courbe 144B1 ne peut se produire : on le vérifie en utilisant le lemme 9, en remarquant que l'invariant modulaire de la 144B1 n'est pas entier en 3. Ainsi,

$\rho_p^{E_2(t)}$ est isomorphe à ρ_p^F, où F est l'une des courbes 36A1 et 144A1. Ces courbes sont à multiplications complexes par l'anneau d'entiers de $\mathbb{Q}\big(\sqrt{-3}\big)$. Il en résulte que l'image de $\rho_p^{E_2(t)}$ est contenue dans le normalisateur d'un sous-groupe de Cartan C de $\mathrm{Aut}\big(E_2(t)[p]\big)$ (cf. [Se1]).

3.1) Supposons $p \equiv 1$ mod. 3. Dans ce cas, C est déployé. Si l'on a $p \geqslant 17$, les conducteurs de F et $E_2(t)$ sont égaux ([Ha-Kr-1]) ; puisque xy est impair, le lemme 3 entraîne alors $xy = \pm 1$, puis $x = 1$, $y = -1$, et le résultat. Supposons $p = 13$. La courbe $E_2(t)$ correspond alors à un point de la courbe modulaire $X_0(26)$ rationnel sur $\mathbb{Q}\big(\sqrt{-3}\big)$. Par ailleurs, la jacobienne $J_0(26)$ de $X_0(26)$ est isogène sur $\mathbb{Q}$ au produit des courbes elliptiques notées 26A1 et 26B1 dans les tables de [Cr1]. Les tordues quadratiques de ces courbes par $\sqrt{-3}$ sont de rang 0 sur $\mathbb{Q}$. En particulier, $J_0(26)$ possède un quotient non trivial de rang 0 sur $\mathbb{Q}\big(\sqrt{-3}\big)$. Compte tenu du fait que xy est impair, il résulte alors du corollaire 4.3 de [Ma] que l'on a de nouveau $xy = \pm 1$. Le même argument vaut si $p = 7$, car la tordue quadratique par $\sqrt{-3}$ de la courbe elliptique $Y_0(14)$, notée 14A1 dans [Cr1], est aussi de rang 0 sur $\mathbb{Q}$.

3.2) Supposons $p \equiv 2$ mod. 3. Dans ce cas, C est non déployé et $E_2(t)$ ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, $j_{E_2(t)}$ appartient à $\mathbb{Z}\left[\frac{1}{p}\right]$ ([Da-Me]). Par ailleurs, on a

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

On vérifie que xy et $6(4z^2 - y^p)$ sont premiers entre eux. Par suite, xy est une puissance de p. Si p divise xy, la courbe $E_2(t)$ a réduction multiplicative en p et l'on a $a_p\big(E_2(t)\big) = \pm 1$. On en déduit que $a_p(F) \equiv \pm 1$ mod. p. Cela conduit à une contradiction, car on a $a_p(F) = 0$. D'où le résultat dans ce cas et l'égalité (20).

6.2. L'équation $64\boldsymbol{x^p} + \boldsymbol{y^p} = 7\boldsymbol{z^2}$

Soit p un nombre premier $\geqslant 11$. On a l'égalité

$$S_p(64, 1, 7) = \big\{(1, -1, 3), (1, -1, -3)\big\}. \tag{21}$$

La démonstration de (21) étant analogue à celle de l'égalité (20), on se limitera ici à indiquer brièvement les arguments utilisés. Soit $t := (x, y, z)$ un élément de $S_p(64, 1, 7)$.

1) On montre que y est impair : dans le cas contraire, il existe $n \geqslant 1$ et deux entiers impairs, y_1 et z_1 tels que $s := (2^{n-1}y_1, x, z_1)$ appartienne à $S_p(2^{p-6}, 1, 7)$. La représentation $\rho_p^{E_2(s)}$ est irréductible de poids 2 et l'on a :

$$N\big(\rho_p^{E_2(s)}\big) = \begin{cases} 98 & \text{si } n \geqslant 2 \text{ ou } p \geqslant 13 \\ 392 & \text{si } n = 1 \text{ et } p = 11. \end{cases}$$

On a $g_2^+(98) = 3$ et $g_2^+(392) = 10$. Supposons $N\big(\rho_p^{E_2(s)}\big) = 98$. En utilisant les tables de W. Stein on constate que l'on est dans l'un des cas suivants ([St]) :

(i) $\rho_p^{E_2(s)}$ est isomorphe à ρ_p^E, où E la courbe elliptique notée 98A1 dans [Cr1] ;

(ii) $\rho_p^{E_2(s)}$ provient, au sens du paragraphe 4, d'une newform normalisée $f \in S_2^+(98)$ telle que $\mathbb{Q}(f) = \mathbb{Q}\big(\sqrt{2}\big)$.

La courbe E a réduction additive en 7 et $v_7(j_E) = -1$; le lemme 9 permet ainsi d'écarter le cas (i). Par ailleurs, quitte à conjuguer f par un élément convenable de $G_{\mathbb{Q}}$, on a l'égalité $a_5(f) = 2\sqrt{2}$. Si $E_2(s)$ a bonne réduction en 5, on a $a_5\big(E_2(s)\big) \in \big\{0, \pm 2, \pm 4\big\}$ et la congruence (11) conduit à une contradiction. De même, la norme de $\mathbb{Q}\big(\sqrt{2}\big)$ sur $\mathbb{Q}$ de $a_5(f) \pm 6$ est égale à 28, ce qui contredit la congruence (12). Le cas (ii) est donc aussi écarter.

On a donc $N\big(\rho_p^{E_2(s)}\big) = 392$ et l'on est dans l'un des cas suivants :

(iii) $\rho_p^{E_2(s)}$ est isomorphe à ρ_p^F, où F est l'une des courbes elliptiques notée $392A1, \cdots,$ $392F1$ dans [Cr1] ;

(iv) $\rho_p^{E_2(s)}$ provient d'une newform normalisée $f \in S_2^+(392)$ telle que $\mathbb{Q}(f) = \mathbb{Q}\big(\sqrt{2}\big)$.

Les courbes 392A1 et 392D1 ne conviennent pas (lemme 9). Les autres possibilités contredisent les congruences (11) et (12) utilisées avec $\ell = 5$. D'où le fait que y soit impair.

2) On déduit de ce qui précéde que $N\big(\rho_p^{E_2(t)}\big) = 49$ (prop. 4). On a $g_2^+(49) = 1$ et la courbe elliptique notée 49A1 dans [Cr1] est à multiplications complexes par l'anneau d'entiers de $\mathbb{Q}\big(\sqrt{-7}\big)$. L'image de $\rho_p^{E_2(t)}$ est donc contenue dans le normalisateur d'un sous-groupe de Cartan de $\mathrm{Aut}\big(E_2(t)[p]\big)$. Il est déployé si et seulement si $p \equiv 1, 2, 4$ mod. 7. Les mêmes arguments que ceux utilisés dans les alinéas 3.1 et 3.2 du paragraphe 6.1 conduisent alors à l'égalité (21). D'où le résultat.

7. Exemples numériques

Nous allons illustrer dans ce paragraphe la méthode modulaire et ses compléments afin de résoudre le problème énoncé dans l'introduction dans certains cas particuliers. On explicitera par ailleurs numériquement le théorème 3 sur quelques exemples. Pour chacun d'entre eux, les calculs nécessaires ont été réalisés à l'aide du logiciel PARI (cf. [Pari]) et du programme *metmod* qui est disponible à l'adresse : http://www.math.jussieu.fr/~ivorra.

Exemple 1. On considère l'équation

$$x^p + 7y^p = z^2. \tag{22}$$

On ne sait pas démontrer l'existence d'une infinité de nombres premiers p pour lesquels $S_p(1, 7, 1)$ soit vide. En revanche, si l'on se donne p explicitement, la méthode de réduction est un moyen efficace de prouver que $S_p(1, 7, 1)$ est vide.

Considérons un nombre premier $p \geqslant 11$. Soit (x, y, z) un élément de $S_p(1, 7, 1)$. Les représentations $\rho_p^{E_1}$ et $\rho_p^{E_2}$ sont irréductibles de poids 2 et l'on est dans l'un des cas ci-dessous :

(i) y est pair et $N\big(\rho_p^{E_1}\big) = 14$;

(ii) on a $x \equiv -1$ mod. 4, y est impair et $N\big(\rho_p^{E_1}\big) = 224$;

(iii) x est pair et $N\big(\rho_p^{E_2}\big) = 14$;

(iv) on a $x \equiv 1$ mod. 4, y est impair et $N\big(\rho_p^{E_2}\big) = 224$.

On a $g_2^+(14) = 1$ et $g_2^+(224) = 6$. Il existe deux classes de $\mathbb{Q}$-isogénie de courbes elliptiques de conducteur 224. Par ailleurs, à conjugaison près par un élément de $G_{\mathbb{Q}}$, il existe deux newforms normalisées f et g de $S_2^+(224)$ dont les q-développements sont à coefficients dans $\mathbb{Q}\big(\sqrt{5}\big)$. On peut supposer que $a_3(f) = 1 + \sqrt{5}$ et $a_3(g) = -1 + \sqrt{5}$. En utilisant les congruences (11) et (12) avec $\ell = 3$, on vérifie alors que, dans les cas (ii) et (iv) ci-dessus, $\rho_p^{E_i}$ ($i = 1$ ou $i = 2$) ne provient pas de f ni de g. Par suite, dans chacun des cas considérés, $\rho_p^{E_i}$ est isomorphe à ρ_p^E, où E est l'une des courbes elliptiques notées 14A1, 224A1 et 224B1 dans les tables de [Cr1].

1) En utilisant la méthode de réduction, on constate que :

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

Afin de vérifier cette assertion, pour chacune des courbes E ci-dessus et chaque nombre premier p, on a explicité le plus petit entier $n(E) \geqslant 1$ tel que les conditions suivantes soient satisfaites (cf. le lemme 5) :

(i) $q = n(E)p + 1$ est premier ;

(ii) $a_q(E) \not\equiv \pm 2$ mod. p ;

(iii) pour $i = 1$ et $i = 2$, on a :

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

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

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

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

2) Un cas particulier de l'étude de l'équation (22) consiste en la recherche des couples $(x, z) \in \mathbb{N}^2$ vérifiant l'égalité

$$z^2 + 7 = x^p. \tag{23}$$

J.H.E. Cohn a entrepris cette recherche en 1993 ([Co2], p. 380) et a formulé à ce propos la conjecture suivante :

Conjecture. *Les solutions de l'équation* $z^2 + 7 = x^m$ *avec* $(x, z) \in \mathbb{N}^2$ *et* $m \geqslant 3$ *sont telles que* $z \in \Big\{1, 3, 5, 11, 181\Big\}$.

Il n'y a pas d'autres solutions si x est impair, ou bien si m est pair, ou bien si 3 divise m (*loc. cit.*). J.-L. Lesage a prouvé en 1998 que tel est aussi le cas si $m \in \big\{5, 7, 13\big\}$ et, en utilisant des minorations de formes linéaires de logarithmes, qu'il n'existe pas de solutions si $m > 6,6.10^{15}$ ([Les]). Par ailleurs, J. Cremona et S. Siksek ont démontré en 2001, par une méthode de réduction analogue à celle présentée ici, que l'équation (23) n'a pas de solutions si l'on a $11 \leqslant p < 10^8$ ([Cr-Si]). Afin de prouver la conjecture de Cohn, il reste donc à vérifier que l'équation (23) n'a pas de solutions pour les nombres premiers p tels que

$$10^8 < p < 6,6.10^{15}. \tag{24}$$

En application de la méthode symplectique, on obtient le résultat suivant :

Lemme 10. *Si l'on a* $p \equiv 13, 17, 19, 23$ mod. 24, *alors l'équation* (23) *n'a pas de solutions.*

Démonstration : Considérons un couple $(x, z) \in \mathbb{N}^2$ tel que $z^2 + 7 = x^p$. L'élément $(x, -1, z)$ appartient à $S_p(1, 7, 1)$. D'après un résultat rappelé ci-dessus, x est pair. Si E désigne la courbe elliptique 14A1, ρ_p^E est isomorphe à $\rho_p^{E_2}$. On a

$$\Delta_E = -2^6.7^3 \quad \text{et} \quad \Delta_{E_2} = 2^{-6}.7^2.x^p.$$

On en déduit que -6 est un carré dans $\mathbb{F}_p$ (prop. 6). Cela entraîne le résultat.

Admettons que les nombres premiers p vérifiant les inégalités (24) soient équirépartis dans leurs classes de congruences modulo 24, ce qui est conforme au théorème de Dirichlet. Le lemme 10 montre alors que l'équation (23) n'a pas de solutions pour environ la moitié des nombres premiers p vérifiant (24), soit plus de 10^{14} nombres premiers p.

Exemple 2. On démontre ici l'assertion suivante :

$$S_{11}(1, 11^m, 1) \text{ est vide si l'on a } \ 1 \leqslant m \leqslant 10. \tag{25}$$

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

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

(i) y est pair et $N(\rho_{11}^{E_1}) = 2$;

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

(iii) x est pair et $N(\rho_{11}^{E_2}) = 2$;

(iv) on a $x \equiv 1$ mod. 4, y est impair et $N(\rho_{11}^{E_2}) = 32$.

On a $g_{12}^+(2) = 0$ et $g_{12}^+(32) = 11$. Par suite, on est dans l'un des cas (ii) et (iv). Il existe ainsi une newform normalisée $f \in S_{12}^+(32)$ et une place $\mathfrak{P}$ de $\overline{\mathbb{Q}}$ de caractéristique résiduelle 11 telles que les congruences (11) et (12) soient satisfaites avec E_1 ou E_2. En utilisant les tables de Stein, on constate que f est l'un des éléments notés $32k12A1, \cdots,$ $32k12E1$ ([St]). On vérifie alors que cela n'est possible que si f est la newform $32k12A1$. La méthode de réduction utilisée avec

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

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

2) Comme dans la démonstration du théorème 1 (si $n = 0$), on déduit de là l'existence de deux entiers u et v tels que (y, u, v) appartienne à $S_{11}(1, 11^{11-m}, 1)$. Puisque 11 ne divise pas y, l'alinéa précédent entraîne une contradiction. D'où l'assertion (25).

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

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

On peut supposer $p \neq 11$ (exemple 2). Supposons qu'il existe $(x, y, z) \in S_p(1, 11, 1)$. Dans ce cas, les représentations $\rho_{11}^{E_1}$ et $\rho_{11}^{E_2}$ sont de poids 2, et l'on est dans l'un des cas suivants :

(i) y est pair et $N(\rho_{11}^{E_1}) = 22$;

(ii) on a $x \equiv -1$ mod. 4, y est impair et $N(\rho_{11}^{E_1}) = 352$;

(iii) x est pair et $N(\rho_{11}^{E_2}) = 22$;

(iv) on a $x \equiv 1$ mod. 4, y est impair et $N(\rho_{11}^{E_2}) = 352$.

On a $g_2^+(22) = 0$ et $g_2^+(352) = 10$. Puisque $g_2^+(22) = 0$, on est dans l'un des cas (ii) et (iv). Si l'on a $p \geqslant 13$, en utilisant les tables de Stein, on contredit alors directement les congruences (11) et (12) avec le nombre premier $\ell = 3$ ou $\ell = 5$. Si $p = 7$, la méthode de réduction permet de conclure.

Exemple 4. Bennett et Skinner ont démontré que $S_p(1, 5, 2)$ est vide dès que l'on a $p \geqslant 11$ ([Be-Sk]). Vérifions ici que $S_7(1, 5, 2)$ est vide. Supposons qu'il existe un élément de $S_7(1, 5, 2)$. La représentation $\rho_7^{E_1}$ correspondante est irréductible de poids 2 et de conducteur $2^8.5$. Soient $f \in S_2^+(1280)$ et $\mathfrak{P}$ une place de $\overline{\mathbb{Q}}$ au-dessus de 7, vérifiant (11) et (12). On a $g_2^+(1280) = 32$. On obtient directement une contradiction sauf si f est l'une des newforms notées $1280A1$, $1280D1$, $1280E1$, $1280I1$, $1280J1$ ou $1280N1$ dans les tables de Stein. On élimine ensuite ces newforms en utilisant la méthode de réduction : avec le

nombre premier $q = 43$ si f est la $1280A1$ ou $1280D1$, et avec $q = 29$ dans les autres cas. D'où l'assertion.

Exemple 5. On va préciser le théorème 3 si $\ell = 23$ et $n = 0$. Soient m un entier naturel impair et p un nombre premier tels que $p \geqslant 11$, $p \neq 23$ et $m < p$. Vérifions que :

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

On considère pour cela un élément $(x, y, z) \in S_p(1, 23^m, 1)$. Les représentations $\rho_p^{E_1}$ et $\rho_p^{E_2}$ correspondantes sont de poids 2, et l'on est dans l'un des cas suivants :

(i) y est pair et $N(\rho_p^{E_1}) = 46$;

(ii) on a $x \equiv -1$ mod. 4, y est impair et $N(\rho_p^{E_1}) = 736$;

(iii) x est pair et $N(\rho_p^{E_2}) = 46$;

(iv) on a $x \equiv 1$ mod. 4, y est impair et $N(\rho_p^{E_2}) = 736$.

On a $g_2^+(46) = 1$ et $g_2^+(736) = 22$. Les cas (ii) et (iv) ne peuvent se produire : on utilise les tables de Stein et on contredit les congruences (11) et (12). Soit E la courbe notée 46A1 dans [Cr1]. On en déduit que ρ_p^E est isomorphe à $\rho_p^{E_1}$ ou $\rho_p^{E_2}$. On a $\Delta_E = -2^{10}.23$. La proposition 6 entraîne alors (26).

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

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

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

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

Pour le vérifier, on procède comme dans l'exemple 1 ci-dessus avec la courbe E. Avec ses notations, l'entier $n(E)$ utilisé si $p < 80$ est donné ci-dessous :

p	13	17	19	29	31	37	41	43	47	53	59	61	67	71	73	79
$n(E)$	4	14	10	2	10	4	20	4	6	44	12	6	28	8	12	28

Si $p < 10^4$, le plus grand entier $n(E)$ intervenant est 96 pour $p = 5641$. Notons que $(2, -1, 45)$ appartient à $S_{11}(1, 23, 1)$. On ne sait pas décider si $S_7(1, 23, 1)$ est vide ou non.

Exemple 6. On explicite ici le théorème 3 pour $\ell = 19249$, qui est congru à 1 modulo 8, et $n = 1$. L'entier ℓ ne vérifie pas la propriété (A) : on a $\ell - 2^{10} = 135^2$. Par suite, ℓ ne vérifie pas les hypothèses faites dans le théorème 1. Néanmoins, dès que p est assez grand, par exemple si $p > C(\ell)$, on a les implications suivantes :

(27) $\qquad p \equiv 11, 13, 17, 19 \text{ mod. } 20 \Longrightarrow S_p(2, \ell, 1)$ est vide,

(28) $\qquad p \equiv 3, 17, 21, 27, 29, 31, 33, 39 \bmod. 40 \Longrightarrow S_p(2\ell, 1, 1)$ est vide.

En effet, soit $t := (x, y, z)$ un élément de $S_p(2, \ell, 1) \bigcup S_p(2\ell, 1, 1)$ où $p \geqslant 7$ et $p \neq \ell$. La représentation $\rho_p^{E_2}$ associée à t et $(2, \ell, 1)$ ou $(2\ell, 1, 1)$ est de poids 2 et l'on a :

$$N\big(\rho_p^{E_2}\big) = \begin{cases} 2\ell & \text{si } x \text{ est pair} \\ 128\ell & \text{sinon.} \end{cases}$$

D'après le chapitre II, il existe une unique classe de $\mathbb{Q}$-isogénie de courbes elliptiques sur $\mathbb{Q}$ de conducteur 2ℓ ayant un point d'ordre 2 sur $\mathbb{Q}$. Cette classe est représentée par la courbe elliptique $E/\mathbb{Q}$ d'équation minimale (*loc. cit.*) :

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

On a $\Delta_E = 2^8\ell$. Par ailleurs, il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur 128ℓ ayant un point d'ordre 2 sur $\mathbb{Q}$ (*loc. cit*). On en déduit que si $p > C(\ell)$ les représentations ρ_p^E et $\rho_p^{E_2}$ sont isomorphes (prop. 5). D'après le corollaire 2, on a

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

La proposition 6 entraîne alors les implications (27) et (28). On obtient ainsi des ensembles de nombres premiers p de densité $\frac{1}{2}$ pour lesquels $S_p(2, \ell, 1)$ et $S_p(2\ell, 1, 1)$ sont vides.

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

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

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

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

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

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

Lemme 11. *Soit (x, y) un point de $C_{\varepsilon d,p}(\mathbb{Q})$. Supposons qu'il n'existe pas d'éléments $(\alpha, \beta, \gamma) \in S_p(1, d, 1)$ tels que $\varepsilon\beta$ soit un carré. Alors, on a $xy = 0$.*

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

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

On en déduit l'égalité

$$w^2 = u^p + d(\varepsilon v^2)^p. \tag{29}$$

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

Corollaire 3. *Soit (x, y) un point de $C_{\varepsilon d,p}(\mathbb{Q})$. Si $S_p(1, d, 1)$ est vide, on a $xy = 0$.*

Il résulte par ailleurs de la démonstration du lemme 11 que la description de l'ensemble $S_p(1, d, 1)$ permet la détermination des ensembles $C_{-d,p}(\mathbb{Q})$ et $C_{d,p}(\mathbb{Q})$.

8.2. Applications

Soient ℓ un nombre premier impair et m, n deux entiers naturels. Posons $d = 2^n \ell^m$. En application des résultats obtenus on peut parfois décrire les ensembles $C_{\varepsilon d,p}(\mathbb{Q})$. Le théorème 1 et le corollaire 3 entraînent le résultat suivant :

Corollaire 4. *Soit (x, y) un point de $C_{\varepsilon d,p}(\mathbb{Q})$. Supposons $m \geqslant 1$ et que (ℓ, n) vérifie l'une des quatre conditions de l'énoncé du théorème* 1. *Alors, si p est assez grand, par exemple si p vérife les inégalités* (3), *on a $xy = 0$.*

Dans le cas où $m = 0$, on déduit du théorème 1 du chapitre I l'énoncé suivant :

Corollaire 5. *Supposons $m = 0$, $p \geqslant 7$ et $n < p$. Soit (x, y) un point de $C_{\varepsilon d,p}(\mathbb{Q})$.*

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

Par ailleurs, comme on le signalait dans l'introduction, ces résultats permettent d'expliciter de nombreux exemples de courbes $C_{\varepsilon d,p}$ qui contredisent le principe de Hasse. En effet, la compactifiée lisse de $C_{\varepsilon d,p}$ possède un unique point au-dessus du point à l'infini de $C_{\varepsilon d,p}$. Ce point est rationnel sur $\mathbb{Q}$. Par suite, $C_{\varepsilon d,p}$ a des points rationnels sur tous les complétés de $\mathbb{Q}$. Si $C_{\varepsilon d,p}$ est vide, $C_{\varepsilon d,p}$ fournit alors un contre-exemple au principe de Hasse. Tel est par exemple le cas des courbes $C_{\varepsilon \ell,p}$ si ℓ est un nombre premier, distinct de 3, congru à 3 modulo 8 et si p est assez grand en fonction de ℓ. Par exemple, si $\ell = 11$, on déduit des exemples numériques 2 et 3 que pour tout $p \geqslant 7$ les courbes $C_{-11,p}$ et $C_{11,p}$ contredisent le principe de Hasse.

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

Parmi les nombres premiers ℓ congrus à 3 modulo 8, l'entier $\ell = 3$ est le seul pour lequel on ne dispose d'aucune information sur la description de $S_p(1, \ell, 1)$. Que peut-on néanmoins démontrer quant à la détermination $C_{-3,p}(\mathbb{Q})$ et $C_{3,p}(\mathbb{Q})$? L'étude de $C_{3,p}(\mathbb{Q})$ s'avère plus difficile que celle de $C_{-3,p}(\mathbb{Q})$; cela est dû au fait que les points $(1, -2)$ et

$(1,2)$ appartiennent à $C_{3,p}(\mathbb{Q})$ et l'on est dans ce cas dans une situation analogue à celle de la conjecture 2. Nous ne savons pas décider si ce sont les seuls points de $C_{3,p}(\mathbb{Q})$. En revanche, on dispose de quelques informations sur $C_{-3,p}(\mathbb{Q})$, que l'on va décrire dans ce qui suit.

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

(30) $$C_{-3,p}(\mathbb{Q}) \text{ est vide si l'on a } \quad 5 \leqslant p < 10^4.$$

Pour vérifier cette assertion, on procède comme suit : supposons $C_{-3,p}(\mathbb{Q})$ non vide. D'après l'égalité (29), il existe des entiers non nuls u, v et w, premiers entre eux dans leur ensemble, tels que l'on ait $w^2 = u^p - 3v^{2p}$ et $s := (u, -v^2, w)$ appartient à $S_p(1,3,1)$. Afin de démontrer que $C_{-3,5}(\mathbb{Q})$ est vide, on est amené à prouver l'énoncé suivant :

Lemme 12. *La représentation $\rho_5^{E_1(s)}$ est irréductible.*

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

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

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

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

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

qui est la courbe notée 20A1 dans [Cr1] (cf. [Ha]). Elle possède exactement six points rationnels sur $\mathbb{Q}$, qui sont des pointes, et qui forment ainsi le complémentaire de Y dans X.

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

D'après la proposition 1 et le lemme 12, $\rho_p^{E_1(s)}$ est irréductible pour tout $p \geqslant 5$. Son poids vaut 2. Par ailleurs, l'égalité $w^2 = u^p - 3v^{2p}$ entraîne

$$u \equiv 1 \text{ mod. } 2.$$

On en déduit que v est impair : sinon v est pair et l'on a alors $N\big(\rho_p^{E_1(s)}\big) = 6$ (prop. 3), ce qui conduit à une contradiction car $g_2^+(6) = 0$. Ainsi uv est impair, et cela entraîne $u \equiv -1$ mod. 4. Il en résulte que l'on a (*loc. cit.*)

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

On a $g_2^+(96) = 2$. Par suite, $\rho_p^{E_1(s)}$ est isomorphe à ρ_p^E, où E est l'une des courbes elliptiques notée 96A1 et 96B1 dans [Cr1]. Ces courbes elliptiques se déduisant l'une de l'autre par torsion quadratique par $\sqrt{-1}$, on peut supposer que E est la 96A1. Elle possède tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$. La méthode de réduction permet alors de contredire cette situation si l'on a $5 \leqslant p < 10^4$. D'où l'assertion (30).
Nous indiquons dans le tableau ci-dessous, comme dans l'exemple numérique 1, l'entier $n(E)$ avec lequel la mèthode de rèduction permet de conclure si $p < 80$.

p	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79
$n(E)$	2	18	2	6	6	34	2	2	10	6	2	30	6	2	14	6	66	18	6	34

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

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

Lemme 13. *Supposons que $q := 2p+1$ soit un nombre premier et que l'une des conditions suivantes soit réalisée :*

1) on a $p \equiv 3$ mod. 4 ;

2) on a $a_q(F)^2 \neq a_q(E)^2$.

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

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

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

$$a_q(E) \not\equiv \pm 2 \text{ mod. } p. \tag{31}$$

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

$$a_q(E) \equiv 0 \text{ mod. } 4. \tag{32}$$

D'après l'inégalité $|a_q(E)| \leqslant 2\sqrt{q}$ ([Si1], p. 131), on a $|a_q(E) \pm 2| \leqslant 2(\sqrt{q}+1)$, d'où l'on déduit que $|a_q(E) \pm 2| < p$ (cette inégalité est aussi vraie si $p = 11$ car $a_{23}(E) = 0$). Cela entraîne (31) : en effet, dans le cas contraire, on aurait $a_q(E) = \pm 2$, ce qui contredit (32). D'où notre assertion.

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

$$-2 \quad \text{est un carré dans } \mathbb{F}_q. \tag{33}$$

Par ailleurs, on en déduit les congruences,

$$u^p \equiv 1 \text{ mod. } q \quad \text{et} \quad w^2 \equiv -2 \text{ mod. } q. \tag{34}$$

1) Si $p \equiv 3$ mod. 4, on a $q \equiv 7$ mod. 8, ce qui contredit (33). D'où le résultat dans ce cas.

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

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

Le discriminant de A est $-2^6.3.(uv)^{2p}.w^6$. D'après (34), q ne divise pas w. Ainsi, A a bonne réduction en q, et $E_1(s)$ ayant aussi bonne réduction en q, on a donc

$$a_q(A) = \pm a_q\big(E_1(s)\big). \tag{35}$$

Il résulte de (34) que les courbes elliptiques sur $\mathbb{F}_q$ déduites de F et A par réduction sont les mêmes. On a ainsi

$$a_q(A) = a_q(F). \tag{36}$$

Par ailleurs, les réprésentations $\rho_p^{E_1(s)}$ et ρ_p^E étant isomorphes, on a (formule (13))

$$a_q(E) \equiv a_q\big(E_1(s)\big) \text{ mod. } p.$$

On déduit alors de (35) et (36) que l'on a

$$a_q(E) \equiv \pm a_q(F) \text{ mod. } p.$$

Afin de démontrer que $C_{3,p}(\mathbb{Q})$ est vide, on peut supposer, compte tenu de (30), que $p > 31$. L'inégalité $|a_q(E) \pm a_q(F)| \leqslant 4\sqrt{q}$ entraîne alors $|a_q(E) \pm a_q(F)| < p$, puis $a_q(E) = \pm a_q(F)$. D'où une contradiction et le lemme.

Il y a conjecturalement une infinité de nombres premiers $p \equiv 3$ mod. 4 tels que $2p+1$ soit premier. Ceux plus petits que 500 sont $\{3, 11, 23, 83, 131, 179, 191, 239, 251, 359, 419, 431, 443, 491\}$. Par ailleurs, la conclusion du lemme est aussi vraie si $p = 3$. En effet, la courbe elliptique d'équation $y^2 = x^3 - 3$, de conducteur 972, n'a pas de points rationnels sur $\mathbb{Q}$ (autre que le point à l'infini) ([Cr1], p. 249). La conique d'équation $y^2 = x^2 - 3$ a une infinité de points rationnels sur $\mathbb{Q}$. En revanche, la courbe $y^2 = x^4 - 3$ n'en possède pas, comme on peut le vérifier en remarquant qu'elle est birationnellement équivalente à la courbe elliptique notée 576F2 dans [Cr1]. Au vue des résultats obtenus, il semble donc naturel de conjecturer que pour tout entier $n \geqslant 3$, la courbe d'équation $y^2 = x^n - 3$ n'a pas de points rationnels sur $\mathbb{Q}$. Signalons qu'il se trouve dans [Co1] une démonstration du fait qu'elle ne possède pas de points entiers.

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

Les résultats obtenus dans ce travail permettent parfois la détermination des points rationnels sur $\mathbb{Q}$ de certaines tordues quadratiques de courbes $C_{d,p}$. Il s'agit de courbes sur $\mathbb{Q}$ ayant une équation de la forme $ey^2 = x^p + d$ où e est un entier sans facteurs carrés. Les théorèmes 1 et 2 permettent notamment d'obtenir des résultats dans cette direction si $e = 2$. On se limitera ici à indiquer le résultat suivant qui est une conséquence de la description de l'ensemble $S_p(4, 1, 3)$ (égalité (20)).

Proposition 7. *Soient p un nombre premier $\geqslant 7$ et $X_p/\mathbb{Q}$ la courbe d'équation*

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

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

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

1) Supposons $v_3(y) \geqslant 0$. Il existe des entiers non nuls u, v et w tels que $\text{pgcd}(u, v) = 1$ et $\text{pgcd}(w, v) = 1$ avec

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

On a $3w^2 = u^p + 4v^{2p}$, de sorte que (v^2, u, w) appartient à $S_p(4, 1, 3)$. Cela conduit à $(x, y) \in \{(-1, -1), (-1, 1)\}$.

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

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

$$x = \frac{u}{3^s v^2} \quad \text{et} \quad y = \frac{w}{3^r v^p}.$$

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

Chapitre IV

Sur les courbes hyperelliptiques cyclotomiques et les équations $x^p - y^p = cz^2$

Introduction

Étant donnés un nombre premier $p \geqslant 7$ et un entier naturel non nul c sans facteurs carrés, on va s'intéresser dans ce chapitre à l'étude de l'équation diophantienne

$$x^p - y^p = cz^2. \tag{1}$$

Conformément au chapitre précédent, une solution $(x, y, z) \in \mathbb{Z}^3$ de l'équation (1) sera dite propre si l'on a $\mathrm{pgcd}(x, y, z) = 1$, et non triviale si xyz n'est pas nul. On note ici $S_p(c)$ l'ensemble des solutions propres non triviales de l'équation (1). C'est un ensemble fini.

On a vu au chapitre I que $S_p(1)$ est vide et que $S_p(2) = \big\{(1, -1, -1), (1, -1, 1)\big\}$. On considère ici l'ensemble $\mathfrak{N}_p$ des entiers $c \geqslant 3$, sans facteurs carrés, possédant la propriété suivante :

$$\text{pour tout diviseur premier } \ell \text{ de } c, \text{ on a } \ell \not\equiv 1 \text{ mod. } p. \tag{2}$$

On obtient dans ce chapitre quelques résultats nouveaux sur la question ci-dessous, qui est un cas particulier de celle posée dans [Kr6] :

Question 1. *Soit p un nombre premier $\geqslant 7$. Existe-t-il un entier $c \in \mathfrak{N}_p$ tel que $S_p(c)$ soit non vide ?*

L'analogue de cette question avec $p = 3$ ou $p = 5$ a une réponse positive. À titre indicatif, on a les égalités suivantes :

$$11^3 - 2^3 = 3.21^2 \quad \text{et} \quad 8^5 + 11^5 = 19.101^2.$$

En fait, si $p = 3$ ou $p = 5$, il est plausible de penser qu'il existe une infinité d'entiers $c \in \mathfrak{N}_p$ tel que $S_p(c)$ soit non vide (cf. *loc. cit.*). En revanche, on ne connait pas d'exemples d'entiers $c \in \mathfrak{N}_p$ répondant positivement à la question 1. Il est démontré dans *loc. cit.* les résultats suivants :

1. pour tout $p \geqslant 7$, l'ensemble des entiers $c \in \mathfrak{N}_p$ tels que $S_p(c)$ soit non vide est fini.
2. Supposons $p \in \big\{5, 7\big\}$. Pour tout $c \in \mathfrak{N}_p$ divisible par p, l'ensemble $S_p(c)$ est vide.

On va prouver ici le résultat suivant :

Théorème 1. *Supposons que l'on ait* $p \in \{7, 11, 13, 17\}$. *Alors, pour tout* $c \in \mathfrak{N}_p$ *l'ensemble* $S_p(c)$ *est vide.*

Au vu de ces résultats et de certaines constatations numériques il est tentant de conjecturer que la réponse à la question 1 est négative dès que p est plus grand qu'une constante absolue. Néanmoins, on ne sait pas démontrer par exemple que la conjecture (abc) entraîne cette assertion.

Notons $\Phi_p(X) \in \mathbb{Z}[X]$ le p-ième polynôme cyclotomique. On a $\Phi_p(X) = \sum X^k$, pour $0 \leqslant k \leqslant p-1$. Soient $C_p/\mathbb{Q}$ et $D_p/\mathbb{Q}$ les courbes hyperelliptiques d'équations :

$$C_p : y^2 = \Phi_p(x) \quad \text{et} \quad D_p : py^2 = \Phi_p(x).$$

Ce sont des courbes de genre $\frac{p-3}{2}$.

L'étude de la question 1 se ramène en fait à la détermination des points rationnels sur $\mathbb{Q}$ de C_p et D_p ([Kr6], lemme 1). Rappelons quelle en est la raison : soient c un entier de $\mathfrak{N}_p$ et (u, v, w) un élément de $S_p(c)$. Un nombre premier ℓ qui divise $u^p - v^p$ sans diviser $u - v$ est congru à 1 modulo p ; en effet, ℓ ne divise pas v et p est l'ordre de u/v mod. ℓ dans $\mathbb{F}_\ell^*$. Il en résulte que c divise $u - v$. On a $u \neq v$. Posons

$$\Phi_p(u, v) = \frac{u^p - v^p}{u - v}.$$

Les entiers $u - v$ et $\Phi_p(u, v)$ sont premiers entre eux en dehors de p et l'on a $\Phi_p(u, v) \geqslant 0$. On en déduit l'existence d'un entier s tel que

$$\Phi_p(u, v) = s^2 \quad \text{ou} \quad \Phi_p(u, v) = ps^2.$$

Par suite, en posant

$$x = \frac{u}{v} \quad \text{et} \quad y = \frac{s}{v^{\frac{p-1}{2}}}, \tag{3}$$

on constate que (x, y) appartient à $C_p(\mathbb{Q})$ ou à $D_p(\mathbb{Q})$. D'où notre assertion. Si l'on a $p \geqslant 7$, les courbes C_p et D_p sont de genre $\geqslant 2$, donc les ensembles $C_p(\mathbb{Q})$ et $D_p(\mathbb{Q})$ sont finis. On démontre dans cette direction l'énoncé suivant :

Théorème 2. *Supposons que l'on ait* $p \in \Big\{7, 11, 13, 17\Big\}$. *On a alors :*

$$C_p(\mathbb{Q}) = \Big\{(-1, -1), (-1, 1), (0, -1), (0, 1)\Big\} \quad \textit{et} \quad D_p(\mathbb{Q}) = \Big\{(1, -1), (1, 1)\Big\}. \tag{4}$$

Le théorème 2 suggère en fait de poser la question suivante :

Question 2. *Les égalités* (4) *sont-elles valables pour tout* $p \geqslant 7$ *?*

Si les égalités (4) sont vraies pour un nombre premier $p \geqslant 7$, alors pour tout $c \in \mathfrak{N}_p$ l'ensemble $S_p(c)$ est vide : considérons en effet un entier $c \in \mathfrak{N}_p$ et supposons qu'il existe un élément $(u, v, w) \in S_p(c)$. Les entiers u et v sont premiers entre eux. D'après les égalités (3) et (4), on a donc $u = 0$ ou bien $uv = \pm 1$. La condition $uv = \pm 1$ conduit à $c = 2$ ou $w = 0$. On obtient ainsi une contradiction et notre assertion. En particulier, le théorème 2 entraîne le théorème 1. Toute la suite est consacrée à la démonstration du théorème 2.

1. Principe de démonstration du théorème 2

Le principe de démonstration que l'on utilise est le même pour la description de $C_p(\mathbb{Q})$ et de $D_p(\mathbb{Q})$. Voici comment l'on procède pour déterminer $C_p(\mathbb{Q})$.

On commence par expliciter, dans le paragraphe 2, deux courbes hyperelliptiques $Y_p/\mathbb{Q}$ et $Z_p/\mathbb{Q}$ et deux applications rationnelles définies sur $\mathbb{Q}$ de degré 2 :

$$\varphi_1 : C_p \to Y_p \quad \text{et} \quad \varphi_2 : C_p \to Z_p.$$

Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. Pour tout point $P = (x, y) \in C_p(\overline{\mathbb{Q}})$ tel que $x \neq 0$, les abscisses de $\varphi_1(P)$ et de $\varphi_2(P)$ sont égales à $\frac{x^2+1}{x}$. On décrit dans la suite les images $\varphi_1\big(C_p(\mathbb{Q})\big)$ et $\varphi_2\big(C_p(\mathbb{Q})\big)$, ce qui permet alors de démontrer directement notre résultat.

Soit ζ un générateur du sous-groupe μ_p des racines p-ièmes de l'unité de $\overline{\mathbb{Q}}^*$. Posons $m = \frac{p-1}{2}$ et notons G_m le polynôme minimal sur $\mathbb{Q}$ de $\zeta + \zeta^{-1}$. C'est un polynôme unitaire de $\mathbb{Z}[X]$, de degré m, qui définit le sous-corps réel maximal $\mathbb{Q}(\mu_p)^+$ du corps $\mathbb{Q}(\mu_p)$. Soit $G_m(X, Y) \in \mathbb{Z}[X, Y]$ l'homogénéisé de G_m : on a $G_m(X, Y) = Y^m G_m(X/Y)$. Considérons un point $M = (\alpha, \beta)$ appartenant par exemple à $\varphi_1\big(C_p(\mathbb{Q})\big)$ et posons

$$\alpha = \frac{s}{t},$$

où s et t sont deux entiers premiers entre eux. On démontre dans la proposition 3 qu'en changeant au besoin (s, t) en $-(s, t)$, la condition suivante est satisfaite :

$$s^2 - 4t^2 \in \mathbb{Z}^2 \quad \text{et} \quad G_m(s, t) \in \mathbb{Z}^2.$$

On choisit ensuite un sous-corps K convenable de $\mathbb{Q}(\mu_p)^+$ sur lequel on factorise le polynôme $G_m(X, Y)$ en produit de polynômes irréductibles sur K. Soit A l'anneau des entiers de K. On obtient une décomposition de $G_m(s, t)$ en un produit d'éléments $F_i \in A$ qui sont conjugués sur $\mathbb{Q}$ et qui dépendent de s et t. En utilisant le fait que $G_m(s, t)$ est un carré dans $\mathbb{Z}$, on vérifie alors que les F_i sont, à des unités près, des carrés dans K. On en déduit l'existence d'un polynôme homogène non nul $P(X, Y) \in A[X, Y]$ de degré 4 (qui a priori n'est pas unique) tel que l'on ait

$$P(s, t) \in A^2. \tag{5}$$

On a $\alpha \neq 0$ et il résulte de (5) que $\frac{1}{\alpha}$ est l'abscisse d'un point rationnel sur K d'une quartique $\mathscr{D}/K$ donnée par une équation de la forme

$$v^2 = au^4 + bu^3 + cu^2 + du + e \quad \text{avec} \quad a, b, c, d \in A \quad \text{et} \quad e \in \{0, 1\}.$$

On est ainsi amené à rechercher l'ensemble des points $(u, v) \in \mathscr{D}(K)$ tels que u appartienne à $\mathbb{Q}$. La méthode de Chabauty elliptique permet dans notre situation de le déterminer. La démarche que l'on a suivie dans son application est précisée dans les appendices 1 et 2 de ce chapitre. La désingularisée de $\mathscr{D}/K$ est une courbe elliptique E/K. On explicite dans l'appendice 1 une équation de Weierstrass de E/K de la forme

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

où les $a_i \in A$ sont fonctions de a, b, c et d, et l'on décrit un isomorphisme birationnel défini sur K entre E et $\mathscr{D}$, i.e. un isomorphisme ψ sur K d'un ouvert de E sur un ouvert de $\mathscr{D}$: pour tout $N = (x, y) \in E(\overline{\mathbb{Q}})$, on a $\psi(N) = (u, v)$ où u et v sont des fractions rationnelles en x et y. En considérant l'application de première projection sur $\mathscr{D}$, on obtient ainsi une fonction sur E, que l'on note encore u, dont la définition se trouve dans le paragraphe 3 de l'appendice 1. Notre problème est alors équivalent à la recherche des points $N \in E(K)$ pour lesquels $u(N)$ appartient à $\mathbb{Q}$. Dans l'appendice 2, on décrit la façon dont on applique la méthode de Chabauty elliptique pour résoudre ce problème.

Tous les calculs nécessaires à la démonstration du théorème 2 ont été effectués à l'aide du logiciel PARI ([Pari]). Dans le formulaire p. 163, il se trouve, pour chacun des nombres premiers intervenant dans l'énoncé du théorème, des tableaux qui fournissent les informations suivantes :

1) les données arithmétiques de K utilisées : un élément primitif de $K/\mathbb{Q}$, ses conjugués sur $\mathbb{Q}$, une $\mathbb{Z}$-base de A, un système d'unités fondamentales u_i de A, qui figure dans la ligne "unités" du tableau, leurs normes $N_{K/\mathbb{Q}}(u_i)$ de K sur $\mathbb{Q}$. Pour chacun des corps K envisagés, l'anneau d'entiers A est principal, nous omettons ainsi cette information dans les tableaux. On fournit par ailleurs des générateurs de certains idéaux premiers de A ; par exemple, l'égalité $2A = \mathfrak{p}_2$ signifie que $2A$ est un idéal premier $\mathfrak{p}_2$ de A. On indique aussi la factorisation de $G_m(s, t)$ mentionnée plus haut.

2) La liste des quartiques sur $\mathscr{D}/K$ dont il nous faut effectuer la recherche des points d'abscisses dans $\mathbb{Q}$.

3) Les courbes elliptiques E/K qui sont les désingularisées des quartiques $\mathscr{D}/K$ précédentes. Elles sont obtenues par les formules (3), (10) et (11) de l'appendice 1.
Dans l'utilisation de la méthode de Chabauty elliptique, il est nécessaire de connaître le rang r de $E(K)$ ainsi que r points de $E(K)$ qui sont $\mathbb{Z}$-linéairement indépendants. C'est une condition difficile à réaliser en pratique. On a utilisé pour cela le programme écrit par D. Simon fonctionnant avec le logiciel PARI, qui permet d'obtenir ces informations pour les courbes elliptiques intervenant dans la démonstration ([Sim]). Dans l'utilisation

de ce programme, on a procédé de la façon suivante : on a principalement utilisé le sous-programme de 2-descente via une 2-isogénie. Il fournit en particulier les dimensions sur $\mathbb{F}_2$ des deux groupes de Selmer intervenant dans cette 2-descente. Le calcul de ces dimensions, disons d_1 et d_2, nécessite des arguments de nature locale, et l'on a $r \leqslant d_1 + d_2 - 2$ (cf. [Si1], Chap. X). Si l'on dispose par ailleurs de $d_1 + d_2 - 2$ points de $E(K)$ qui sont $\mathbb{Z}$-indépendants, on a alors $r = d_1 + d_2 - 2$.
Pour chaque courbe elliptique E/K, on précise dans un tableau ces données, ainsi que le sous-groupe de torsion de $E(K)$ qui est facile à obtenir par des arguments standard de réduction. Au cours de la démonstration, si $p = 7, 11$ ou 13 on constate que l'on a toujours $r \leqslant 1$. Seul le cas où $p = 17$ nécessite l'étude d'une courbe elliptique de rang 2.

On pourra trouver à l'adresse http://www.math.jussieu.fr/~ivorra, le programme *Chab* permettant de vérifier tous les calculs numériques intervenant dans la démonstration. On a aussi utilisé des sous-programmes écrits par Simon dans [Sim] permettant de décider si un élément donné de K est un carré dans un complété de K.

La méthode suivie pour déterminer $D_p(\mathbb{Q})$ est la même. Signalons que les courbes elliptiques sur K intervenant dans la description de $D_p(\mathbb{Q})$ sont toutes de rang au plus 1.

2. Courbes quotients de $C_p/\mathbb{Q}$ et $D_p/\mathbb{Q}$

Soit p un nombre premier $\geqslant 5$. Étant donné un entier $d \geqslant 1$, sans facteurs carrés, on note $X_{d,p}/\mathbb{Q}$ la courbe d'équation

$$X_{d,p} : dy^2 = \Phi_p(x).$$

On va expliciter deux courbes $Y_{d,p}/\mathbb{Q}$ et $Z_{d,p}/\mathbb{Q}$ et des applications rationnelles, que l'on notera simplement

$$\varphi_1 : X_{d,p} \to Y_{d,p} \quad \text{et} \quad \varphi_2 : X_{d,p} \to Z_{d,p},$$

qui sont définies sur $\mathbb{Q}$ et de degré 2. La définition de ces courbes va dépendre en fait de la parité de $\frac{p-1}{2}$. On obtiendra en particulier, avec $d \in \{1, p\}$, deux courbes quotients de C_p et D_p.

On considère la suite $(T_j)_{j\geqslant 0}$ des polynômes de Tchebycheff de $\mathbb{Z}[X]$, qui est définie par les conditions

$$T_0 = 1, \quad T_1 = X \quad \text{et} \quad T_{j+2} = 2X\ T_{j+1} - T_j \quad \text{pour} \quad j \geqslant 0.$$

Le degré de T_j est j et si $j \geqslant 1$ son terme dominant est 2^{j-1}. Posons

$$m = \frac{p-1}{2}, \quad H_m(X) = 1 + 2\sum_{j=1}^{m} T_j \in \mathbb{Z}[X] \quad \text{et} \quad G_m(X) = H_m\left(\frac{X}{2}\right).$$

Le polynôme $G_m(X)$ appartient à $\mathbb{Z}[X]$ et est irréductible unitaire de degré m. C'est le polynôme minimal de $\zeta + \zeta^{-1}$ où ζ est un générateur de μ_p. On a l'égalité :

$$\Phi_p(X) = X^m \; G_m\left(X + \frac{1}{X}\right). \tag{6}$$

On en déduit les deux énoncés ci-dessous :

Proposition 1. *Supposons m pair. Soient $Y_{d,p}/\mathbb{Q}$ et $Z_{d,p}/\mathbb{Q}$ les courbes d'équations :*

$$Y_{d,p} : \; dv^2 = G_m(u) \quad et \quad Z_{d,p} : \; dv^2 = (u^2-4)G_m(u).$$

Il existe deux applications rationnelles définies sur $\mathbb{Q}$, de degré 2,

$$\varphi_1 : X_{d,p} \to Y_{d,p} \quad et \quad \varphi_2 : X_{d,p} \to Z_{d,p},$$

définies pour tout point $P = (x,y) \in X_{d,p}\big(\overline{\mathbb{Q}}\big)$ tel que $x \neq 0$, par les égalités

$$\varphi_1(P) = \left(\frac{x^2+1}{x}, \frac{y}{x^{\frac{m}{2}}}\right) \quad et \quad \varphi_2(P) = \left(\frac{x^2+1}{x}, \frac{y(x^2-1)}{x^{\frac{m+2}{2}}}\right). \tag{7}$$

Proposition 2. *Supposons m impair. Soient $Y_{d,p}/\mathbb{Q}$ et $Z_{d,p}/\mathbb{Q}$ les courbes d'équations :*

$$Y_{d,p} : \; dv^2 = (u+2)G_m(u) \quad et \quad Z_{d,p} : \; dv^2 = (u-2)G_m(u).$$

Il existe deux applications rationnelles définies sur $\mathbb{Q}$, de degré 2,

$$\varphi_1 : X_{d,p} \to Y_{d,p} \quad et \quad \varphi_2 : X_{d,p} \to Z_{d,p},$$

définies pour tout point $P = (x,y) \in X_{d,p}\big(\overline{\mathbb{Q}}\big)$ tel que $x \neq 0$, par les égalités

$$\varphi_1(P) = \left(\frac{x^2+1}{x}, \frac{y(x+1)}{x^{\frac{m+1}{2}}}\right) \quad et \quad \varphi_2(P) = \left(\frac{x^2+1}{x}, \frac{y(x-1)}{x^{\frac{m+1}{2}}}\right). \tag{8}$$

Remarque 1.

1) Soient $g(Y_{d,p})$ le genre de $Y_{d,p}$ et $g(Z_{d,p})$ celui de $Z_{d,p}$.

a) Si m est pair on a

$$g(Y_{d,p}) = \frac{p-5}{4} \quad \text{et} \quad g(Z_{d,p}) = \frac{p-1}{4}.$$

b) Si m est impair on a

$$g(Y_{d,p}) = g(Z_{d,p}) = \frac{p-3}{4}.$$

2) La courbe $X_{d,p}$ possède deux involutions σ_1 et σ_2 définies pour tout point $M = (x, y)$ de $X_{d,p}(\overline{\mathbb{Q}})$ tel que $x \neq 0$, par

$$\sigma_1(M) = \left(\frac{1}{x}, \frac{y}{x^m}\right) \quad \text{et} \quad \sigma_2(M) = \left(\frac{1}{x}, -\frac{y}{x^m}\right).$$

La courbe $Y_{d,p}$ (resp. $Z_{d,p}$) est, à $\mathbb{Q}$-isomorphisme près, la courbe quotient de $X_{d,p}$ modulo le sous-groupe des automorphismes de $X_{d,p}$ engendré par σ_1 (resp. σ_2) (pour cette notion, voir par exemple [Si1], p. 107, ex. 3.13).

3. Résultats préliminaires

On reprend les notations du paragraphe précédent. On utilisera de manière essentielle la proposition 3 ci-dessous. Elle repose sur le lemme suivant, qui est une conséquence immédiate de la définition des applications rationnelles φ_1 et φ_2.

Lemme 1. *L'ensemble des abscisses des points de $\varphi_1\big(X_{d,p}(\mathbb{Q})\big)$ est égal à l'ensemble des abscisses des points de $\varphi_2\big(X_{d,p}(\mathbb{Q})\big)$.*

Supposons désormais, ce qui n'est pas restrictif pour les applications que l'on a en vue, que d soit *impair*.

Proposition 3. *Soit α l'abscisse d'un point de $\varphi_1\big(X_{d,p}(\mathbb{Q})\big)$. Posons*

$$\alpha = \frac{s}{t} \quad \textit{et} \quad G_m(s,t) = t^m G_m\left(\frac{s}{t}\right) \in \mathbb{Z},$$

où s et t sont deux entiers premiers entre eux.

1) Si m est pair, on a $G_m(s,t) \in d\mathbb{Z}^2$ et $s^2 - 4t^2$ est un carré.

2) Si m est impair, quitte à changer (s,t) en $-(s,t)$, la condition suivante est réalisée :

$$s + 2t \in \mathbb{Z}^2, \quad s - 2t \in \mathbb{Z}^2 \quad \textit{et} \quad G_m(s,t) \in d\mathbb{Z}^2. \tag{9}$$

3) L'entier st est pair.

Démonstration : Le polynôme G_m est de degré m dans $\mathbb{Z}[X]$, donc $G_m(s,t)$ est un entier. Par hypothèse, Il existe $\beta \in \mathbb{Q}$ tel que (α, β) appartienne à $\varphi_1\big(X_{d,p}(\mathbb{Q})\big)$. D'après le lemme 1, il existe $\gamma \in \mathbb{Q}$ tel que (α, γ) soit dans $\varphi_2\big(X_{d,p}(\mathbb{Q})\big)$.

1) Supposons m pair. Dans ce cas, on a

$$G_m(s,t) = d\Big(\beta t^{\frac{m}{2}}\Big)^2 \quad \text{et} \quad (s^2 - 4t^2)G_m(s,t) = d\Big(\gamma t^{\frac{m+2}{2}}\Big)^2.$$

Puisque d est sans facteurs carrés et que $G_m(s,t)$ est dans $\mathbb{Z}$, le rationnel $\beta t^{\frac{m}{2}}$ appartient à $\mathbb{Z}$. Par suite, $G_m(s,t)$ est dans $d\mathbb{Z}^2$, ce qui entraîne l'assertion 1.

2) Supposons m impair. On a les égalités

$$(10) \qquad (s+2t)G_m(s,t) = d\Big(\beta t^{\frac{m+1}{2}}\Big)^2 \quad \text{et} \quad (s-2t)G_m(s,t) = d\Big(\gamma t^{\frac{m+1}{2}}\Big)^2.$$

Comme ci-dessus, puisque d est sans facteurs carrés et que $G_m(s,t) \in \mathbb{Z}$, on a

$$(11) \qquad \beta t^{\frac{m+1}{2}} \in \mathbb{Z} \quad \text{et} \quad \gamma t^{\frac{m+1}{2}} \in \mathbb{Z}.$$

Les entiers s et t étant premiers entre eux et d étant impair, on en déduit que

$$(12) \qquad d \text{ divise } G_m(s,t).$$

D'après l'égalité (6), on a $\Phi_p(-1) = -G_m(-2)$. Puisque $\Phi_p(-1) = 1$, on a $G_m(-2) = -1$, ce qui entraîne que

$$X+2 \quad \text{divise} \quad 1 + G_m(X),$$

autrement dit, qu'il existe un polynôme $R \in \mathbb{Z}[X]$ de degré $m-1$ tel que l'on ait

$$1 = (X+2)R(X) - G_m(X).$$

En posant $R(s,t) = t^{m-1}R\Big(\frac{s}{t}\Big)$, on obtient l'égalité

$$t^m = (s+2t)R(s,t) - G_m(s,t).$$

Il en résulte que les entiers $s+2t$ et $G_m(s,t)$ sont premiers entre eux. D'après (10) et les conditions (11) et (12), on a ainsi

$$\pm(s+2t) \in \mathbb{Z}^2 \quad \text{et} \quad \pm\, G_m(s,t) \in d\mathbb{Z}^2.$$

Par ailleurs, $G_m(s,t)$ étant un polynôme homogène de degré impair m en s et t, on a

$$G_m(-s,-t) = -G_m(s,t).$$

Quitte à changer (s,t) en $-(s,t)$, on obtient donc la condition

$$s+2t \in \mathbb{Z}^2 \quad \text{et} \quad G_m(s,t) \in d\mathbb{Z}^2.$$

D'après la deuxième égalité de (10), $s-2t$ est alors un carré. D'où le résultat.

3) Il résulte de ce qui précède que s^2-4t^2 est un carré. Si st était impair, on aurait $s^2-4t^2 \equiv 1 \bmod. 8$, ce qui n'est pas si $s^2 \equiv t^2 \equiv 1 \bmod. 8$. D'où la proposition.

Dans le cas où m est impair, on supposera implicitement, dans toute la suite, que pour tout point de $\varphi_1\big(X_{d,p}(\mathbb{Q})\big)$, la condition (9) est satisfaite.

4. Notations

Précisons quelques notations que l'on utilisera dans toute la suite. On reprendra librement toutes les notations et les informations qui se trouvent dans le formulaire. Précisons à ce propos que, dans les tableaux, les courbes elliptiques notées E/K, E'/K, E''/K et E'''/K sont les désingularisées respectivement des quartiques $\mathscr{D}/K$, $\mathscr{D}'/K$, $\mathscr{D}''/K$ et $\mathscr{D}'''/K$.

Considérons l'un des corps K intervenant dans ces tableaux. Étant donné un idéal premier $\mathfrak{p}$ de l'anneau d'entiers A de K, on notera :

. $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$;

. $v_\mathfrak{p}$ la valuation $\mathfrak{p}$-adique de $K_\mathfrak{p}$ normalisée par $v_\mathfrak{p}(K_\mathfrak{p}^*) = \mathbb{Z}$;

. $A_\mathfrak{p}$ l'anneau de valuation de $K_\mathfrak{p}$;

. $\mathfrak{M}_\mathfrak{p}$ l'idéal maximal de $A_\mathfrak{p}$;

. $k_\mathfrak{p} = A_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}$ le corps résiduel ;

. $\eta_\mathfrak{p} : K_\mathfrak{p}^* \to k_\mathfrak{p}^*$ l'application de projection définie par (appendice 2, paragraphe 2.5) :

$$\eta_\mathfrak{p}(x) = \frac{x}{p^{v_\mathfrak{p}(x)}} \text{ mod. } \mathfrak{M}_\mathfrak{p} \quad \text{pour} \quad x \in K_\mathfrak{p}^*.$$

Soit θ l'élément primitif implicitement choisi de K sur $\mathbb{Q}$. C'est une unité de A. On constate que le nombre premier 3 est inerte dans K : on a $3A = \mathfrak{p}_3$. On désignera par ξ l'image de θ dans $k_{\mathfrak{p}_3}$: on a ainsi

$$\xi = \eta_{\mathfrak{p}_3}(\theta) \in k_{\mathfrak{p}_3} \quad \text{et} \quad k_{\mathfrak{p}_3} = \mathbb{F}_3(\xi).$$

Si E/K est une courbe elliptique, ayant bonne réduction en $\mathfrak{p}$, on notera par ailleurs :

. $\widetilde{E_\mathfrak{p}}$ la courbe elliptique sur $k_\mathfrak{p}$ déduite de E par réduction modulo $\mathfrak{p}$;

. $\pi_\mathfrak{p} : E(K_\mathfrak{p}) \to \widetilde{E_\mathfrak{p}}(k_\mathfrak{p})$ l'homomorphisme de réduction ;

. $E_1(K_\mathfrak{p})$ le noyau de $\pi_\mathfrak{p}$;

. $E_1(K)$ l'intersection de $E_1(K_\mathfrak{p})$ avec $E(K)$; on omettra dans cette notation de préciser $\mathfrak{p}$, le contexte ne prêtera pas à confusion ;

. $z(R)$ la z-coordonnée d'un point R de $E_1(K)$; on a $z(O) = 0$.

Sauf précisions supplémentaires comme ci-dessus, on ne redéfinira pas les notations utilisées dans les appendices 1 et 2 que l'on conserve systématiquement. En particulier, étant donnée une quartique $\mathscr{D}/K$ définie par une équation de la forme (2) ou (9) de l'appendice 1 et la courbe elliptique E/K déduite de $\mathscr{D}$ par les formules (3), (10) et (11) de cet appendice, on évoquera dans la suite :

. l'isomorphisme birationnel $\psi : E \to \mathscr{D}$,

. l'ouvert U de E,

. la fonction u sur E,

. les points O et M_1 de $E(K)$,

sans plus de précision.

5. Détermination de $C_7(\mathbb{Q})$ et $D_7(\mathbb{Q})$

Les courbes C_7 et D_7 sont de genre 2. L'assertion concernant l'ensemble $D_7(\mathbb{Q})$ est démontrée dans [Kr6], p. 14-15 : elle s'obtenait en remarquant que D_7 possède une courbe elliptique quotient de rang 0 sur $\mathbb{Q}$. Il n'en va pas de même pour la courbe C_7, ses deux courbes elliptiques quotients (uniques à $\mathbb{Q}$-isogénie près) étant de rang 1 sur $\mathbb{Q}$.

L'ensemble $C_7(\mathbb{Q})$

Décrivons maintenant $C_7(\mathbb{Q})$. On considère un point (α, β) de $\varphi_1\big(C_7(\mathbb{Q})\big)$ et l'on pose

$$\alpha = \frac{s}{t},$$

où s et t sont deux entiers premiers entre eux. D'après la proposition 3, on a

$$G_3(s,t) = (s - t\theta)(s - t\theta_2)(s - t\theta_3) \in \mathbb{Z}^2. \tag{13}$$

Lemme 2. *L'élément $s - t\theta$ est un carré dans K.*

Démonstration : Les éléments $s - t\theta$, $s - t\theta_2$ et $s - t\theta_3$ sont premiers entre eux deux à deux en dehors de π_7 : on peut le vérifier en remarquant que le produit des $(\theta_i - \theta_j)^2$ pour $i < j$ vaut 49. D'après la condition (13), il existe donc des entiers n_i égaux à 0 ou 1, tels que l'on ait

$$s - t\theta \equiv (-1)^{n_0} u_1^{n_1} u_2^{n_2} \pi_7^{n_3} \text{ mod. } K^{*2}. \tag{14}$$

Par ailleurs, on a $\mathrm{N}_{K/\mathbb{Q}}(s - t\theta) = G_3(s,t)$ qui est donc un carré. On en déduit que

$$n_0 + n_1 + n_2 \equiv 0 \text{ mod. } 2 \quad \text{et} \quad n_3 = 0. \tag{15}$$

On utilise alors le fait que la congruence (14) vaut en particulier modulo les carrés du complété $K_{\mathfrak{p}_2}$. On a $v_{\mathfrak{p}_2}(s - t\theta) = 0$: en effet, θ est une unité de A, st est pair (prop. 3) et s et t sont premiers entre eux. Par ailleurs, une unité de $A_{\mathfrak{p}_2}$ congrue à 1 modulo 8 est un carré dans $K_{\mathfrak{p}_2}$. La classe de $s - t\theta$ modulo $K_{\mathfrak{p}_2}^{*2}$ ne dépend donc que des classes de s et t modulo 8. On distingue alors deux cas :

1) supposons s pair et t impair. Puisque $s + 2t$ est un carré (prop. 3), on en déduit que $s \equiv 2$ ou 6 mod. 8. Pour $s \in \{2, 6\}$ et $t \in \{1, 3, 5, 7\}$, on a donc

$$(s - t\theta)(-1)^{n_0} u_1^{n_1} u_2^{n_2} \in K_{\mathfrak{p}_2}^{*2}.$$

En tenant compte de la condition (15), on vérifie que cela entraîne $n_0 = n_1 = n_2 = 0$. La congruence (14) entraîne alors le résultat dans ce cas.

2) Supposons s impair et t pair. Les entiers $s + 2t$ et $s^3 + s^2t - 2st^2 - t^3$ sont des carrés impairs, donc sont congrus à 1 modulo 8. Il en résulte que $(s, t) \equiv (1, 0)$ mod. 8. On vérifie que cela conduit de nouveau à $n_0 = n_1 = n_2 = 0$. D'où le lemme.

On déduit alors du lemme 2 et de la proposition 3 qu'il existe $\delta \in K$ tel que l'on ait :

$$(s^2 - 4t^2)(s - t\theta)(s - t\theta_2) = \delta^2,$$

et l'on obtient ainsi la condition (5) du paragraphe 1. On a $\alpha \neq 0$ i.e. $s \neq 0$. Il en résulte que l'on a

$$\left(\frac{t}{s}, \frac{\delta}{s^2}\right) \in \mathscr{D}(K),$$

où $\mathscr{D}/K$ est la quartique définie dans le formulaire (pour $p = 7$). On est ainsi amené à déterminer les points $(u, v) \in \mathscr{D}(K)$ tel que u soit dans $\mathbb{Q}$.

Proposition 4. *Soit (u, v) un point de $\mathscr{D}(K)$ tel que u soit dans $\mathbb{Q}$. On a*

$$(u, v) \in \left\{\left(-\frac{1}{2}, 0\right), \left(\frac{1}{2}, 0\right), (0, -1), (0, 1)\right\}.$$

Admettons ce résultat. On en déduit que $\alpha = \pm 2$. D'après la proposition 2, si (x, y) est un point de $C_7\big(\mathbb{Q}\big)$ avec $x \neq 0$, on a donc

$$\frac{x^2 + 1}{x} = \pm 2,$$

d'où $x = \pm 1$, puis $x = -1$. On obtient alors l'ensemble $C_7(\mathbb{Q})$ annoncé.

Tout revient alors à déterminer les points N de $E(K)$ tels que $u(N)$ soit dans $\mathbb{Q}$. On a toujours $u(O) = u(-M_1) = 0$. Par ailleurs, on vérifie que l'on a :

$$\psi(2N_1) = \left(-\frac{1}{2}, 0\right) \quad \text{et} \quad \psi(T_0 + 2N_1) = \left(\frac{1}{2}, 0\right),$$

autrement dit, on a $u(2N_1) = -\frac{1}{2}$ et $u(T_0 + 2N_1) = \frac{1}{2}$. Compte tenu du lemme 6 de l'appendice 1, la proposition 4 est une conséquence du résultat suivant :

Proposition 5. *Les seuls points $N \in E(K)\backslash\big\{O, -M_1\big\}$ tels que $u(N) \in \mathbb{Q}$ sont $2N_1$ et $T_0 + 2N_1$.*

Démonstration de la proposition 5

Considérons un point $N \in E(K)\backslash\{O, -M_1\}$ tel que

$$N \neq 2N_1 \quad \text{et} \quad N \neq T_0 + 2N_1. \tag{16}$$

Il faut démontrer que $u(N)$ n'est pas dans $\mathbb{Q}$. On peut supposer que N appartient à U. On utilise la méthode de Chabauty elliptique avec le nombre premier 3. La courbe elliptique E/K a bonne réduction en $\mathfrak{p}_3$: la norme de K sur $\mathbb{Q}$ du discriminant de E est $2^{24}.7^6$. On vérifie que le groupe $\widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$ est d'ordre 32 et que le point $\pi_{\mathfrak{p}_3}(N_1) \in \widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$ est d'ordre 16. On pose

$$Q_1 = 16N_1 \in E_1(K).$$

Soit $\mathfrak{S}$ l'ensemble des points de $E(K)$ qui s'écrivent sous la forme

$$hT_1 + jN_1 \qquad h = 0, 1 \quad \text{et} \quad j = -7, \cdots, 8.$$

Lemme 3. *L'application $\pi_{\mathfrak{p}_3}$ induit une bijection de $\mathfrak{S}$ sur $\widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$.*

Démonstration : On a les égalités

$$\pi_{\mathfrak{p}_3}(T_1) = (2\xi^2 + \xi + 2, 0) \quad \text{et} \quad \pi_{\mathfrak{p}_3}(8N_1) = (\xi^2, 0).$$

Par suite, $\pi_{\mathfrak{p}_3}(T_1)$ n'appartient pas au sous-groupe de $\widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$ engendré par $\pi_{\mathfrak{p}_3}(N_1)$, d'où le lemme.

On déduit du lemme 3 l'existence de $S \in \mathfrak{S}$ tel que $N - S \in E_1(K)$.

Lemme 4. *Supposons que $u(N)$ soit dans $\mathbb{Q}$. Quitte à remplacer N par $-M_1 - N$, on a*

$$N = S + P \quad \textit{où} \quad S \in \Big\{-6N_1, -4N_1, O, 2N_1\Big\} \ \textit{et} \ P \in E_1(K). \tag{17}$$

Démonstration : D'après le lemme 3, le seul point $S \in \mathfrak{S}$ qui soit dans $E_1(K)$ est $S = O$. Si $S \neq O$, le point N n'est donc pas dans $E_1(K)$. En utilisant le lemme 10 de l'appendice 1, on constate alors que l'on doit avoir

$$(h, j) \in \big\{(0, -6), (0, -4), (0, 0), (0, 2), (0, 4)\big\}.$$

Par ailleurs, on a $M_1 = -4N_1$. Le fait que l'on ait $I(4N_1) = O$ entraîne alors le résultat.

Lemme 5. *Soit R un point de $E_1(K)$ non nul. On a*

$$\eta_{\mathfrak{p}_3}\big(z(R)\big) = \pm(\xi^2 + 2\xi + 2).$$

Démonstration : On vérifie la congruence $z(Q_1) \equiv 3\theta^2 + 6\theta + 6$ mod. 9 et l'égalité $v_{\mathfrak{p}_3}(3\theta^2 + 6\theta + 6) = 1$, de sorte que l'on a $\eta_{\mathfrak{p}_3}\big(z(Q_1)\big) = \eta_{\mathfrak{p}_3}(3\theta^2 + 6\theta + 6)$. Par suite, on a

$$\eta_{\mathfrak{p}_3}\big(z(Q_1)\big) = \xi^2 + 2\xi + 2.$$

Le sous-$\mathbb{F}_3$-espace vectoriel Γ de $k_{\mathfrak{p}_3}$ intervenant dans le paragraphe 3 de l'appendice 2 est donc ici la droite vectorielle engendrée par $\xi^2 + 2\xi + 2$. Par ailleurs, les points T_0, T_1 et T_2 ne sont pas dans $E_1(K)$ ([Si1], prop. 3.1, p. 176 ; on peut aussi vérifier notre assertion directement). D'après le lemme 2 de l'appendice 2, $\eta_{\mathfrak{p}_3}\big(z(R)\big)$ est donc dans Γ, d'où le résultat.

D'après le lemme 4, on peut supposer dans la suite que N est de la forme (17). Dans le cas où $S \in \Big\{-4N_1, O\Big\}$, on démontre que $\eta_{\mathfrak{p}_3}\big(u(N)\big)$ n'est pas dans $\mathbb{F}_3$, ce qui prouve en particulier que $u(N)$ n'est pas dans $\mathbb{Q}$. Si $S = 2N_1$, on vérifie que $\eta_{\mathfrak{p}_3}\big(u(N) + \frac{1}{2}\big)$ n'est pas dans $\mathbb{F}_3$, donc $u(N) + \frac{1}{2}$ et $u(N)$ ne sont pas dans $\mathbb{Q}$. On procède de même si $S = -6N_1$ en montrant que $\eta_{\mathfrak{p}_3}\big(u(N) - \frac{1}{2}\big)$ n'appartient pas à $\mathbb{F}_3$.

1) Supposons $S = O$. On a $N = P \in E_1(K)$. Puisque N est dans U, on a $u(N)z(P) \neq 0$. D'après la formule (32) de l'appendice 2 (avec $e = 1$), on a la congruence

$$u(N) \equiv -2z(P) \text{ mod. } z(P)^2.$$

On en déduit les égalités $\eta_{\mathfrak{p}_3}\big(u(N)\big) = \eta_{\mathfrak{p}_3}\big(-2z(P)\big) = \eta_{\mathfrak{p}_3}\big(z(P)\big)$. D'après le lemme 4, on a donc $\eta_{\mathfrak{p}_3}\big(u(N)\big) = \pm(\xi^2 + 2\xi + 2)$.

2) Supposons $S = 2N_1$. On vérifie que l'on a $v_{\mathfrak{p}_3}\Big(y_S - \frac{dx_S}{2} - b\Big) = 0$, de sorte que la condition 8 de l'appendice 2 est réalisée. En explicitant le développement (33) de cet appendice, on constate que l'on a

$$u(N) \equiv -\frac{1}{2} + (\theta + 1)^2 z(P)^2 \text{ mod. } z(P)^3.$$

On a $v_{\mathfrak{p}_3}(\theta + 1) = 0$ et d'après la condition (16) on a $u(N) \neq -1/2$ et $P \neq O$. On vérifie alors que l'on a les égalités

$$\eta_{\mathfrak{p}_3}\left(u(N) + \frac{1}{2}\right) = \eta_{\mathfrak{p}_3}(\theta + 1)^2 \eta_{\mathfrak{p}_3}\big(z(P)\big)^2 = 2\xi + 2.$$

3) Supposons $S = -6N_1$. Posons $S' = T_0 + 2N_1$. On a $\pi_{\mathfrak{p}_3}(8N_1) = \pi_{\mathfrak{p}_3}(T_0)$, d'où l'on déduit que $S - S' \in E_1(K)$, i.e. il existe $P' \in E_1(K)$ tel que l'on ait $N = S' + P'$. Comme ci-dessus, on vérifie que l'on a

$$u(N) \equiv \frac{1}{2} + (3\theta^2 + 2\theta - 9)z(P')^2 \text{ mod. } z(P')^3.$$

On a $v_{\mathfrak{p}_3}(3\theta^2+2\theta-9)=0$, $u(N)\neq 1/2$ et $P'\neq O$ (condition (16)), ce qui conduit à

$$\eta_{\mathfrak{p}_3}\left(u(N)-\frac{1}{2}\right)=\eta_{\mathfrak{p}_3}(3\theta^2+2\theta-9)\eta_{\mathfrak{p}_3}\big(z(P')\big)^2=\xi^2+2.$$

4) Supposons $S=-4N_1$, autrement dit, $S=M_1$. En posant $S=(x_S,y_S)$, on vérifie que $v_{\mathfrak{p}_3}(3x_S^2+2a_2x_S+a_4-dy_S)=0$ et la condition 9 de l'appendice 2 est donc satisfaite. On obtient dans ce cas

$$u(N)\equiv\theta^2+\theta+2 \text{ mod. } 3,$$

et l'égalité $v_{\mathfrak{p}_3}(\theta^2+\theta+2)=0$ entraîne alors $\eta_{\mathfrak{p}_3}\big(u(N)\big)=\xi^2+\xi+2$.

Cela termine la démonstration de la proposition 5 et du théorème 2 si $p=7$.

6. Détermination de $C_{11}(\mathbb{Q})$ et $D_{11}(\mathbb{Q})$

6.1. L'ensemble $C_{11}(\mathbb{Q})$

On considère un point (α,β) de $\varphi_1\big(C_{11}(\mathbb{Q})\big)$ et l'on pose $\alpha=\frac{s}{t}$, où s et t sont deux entiers premiers entre eux.

Lemme 6. *L'élément $s-t\theta$ est un carré dans K.*

Démonstration : Pour $i\neq j$, les éléments $s-t\theta_i$ et $s-t\theta_j$ sont premiers entre eux en dehors de π_{11} et $G_5(s,t)\in\mathbb{Z}^2$ (prop. 3). Il existe donc des entiers n_i égaux à 0 ou 1 tels que l'on ait

$$s-t\theta\equiv(-1)^{n_0}\prod_{i=1}^{4}u_i^{n_i}\ \pi_{11}^{n_5} \text{ mod. } K^{*2}.$$

Puisque $N_{K/\mathbb{Q}}(s-t\theta)\in\mathbb{Z}^2$, on $n_5=0$ et n_0+n_1 est pair. En exprimant cette congruence dans $K^*_{\mathfrak{p}_2}$, on constate comme dans le lemme 2, que les n_i sont nuls. D'où le lemme.

On en déduit que l'on a (lemme 6 et prop. 3) :

$$(s^2-4t^2)(s-t\theta)(s-t\theta_2)\in K^2.$$

On a $s\neq 0$ d'où il en résulte que $\left(\frac{t}{s},\frac{\delta}{s^2}\right)\in\mathscr{D}(K)$, où $\mathscr{D}/K$ est la quartique indiquée dans le formulaire (pour $p=11$). Compte tenu des égalités

$$\psi(2N_1)=\left(-\frac{1}{2},0\right)\quad\text{et}\quad\psi(T_0+2N_1)=\left(\frac{1}{2},0\right),$$

l'assertion du théorème 2 relative à $C_{11}(\mathbb{Q})$ est une conséquence du résultat suivant :

Proposition 6. *Les seuls points $N\in E(K)\backslash\{O,-M_1\}$ tels que $u(N)\in\mathbb{Q}$ sont $2N_1$ et T_0+2N_1.*

Démonstration de la proposition 6

Considérons un point $N \in E(K)\backslash\{O, -M_1\}$ tel que

$$N \neq 2N_1 \quad \text{et} \quad N \neq T_0 + 2N_1,$$

et prouvons que $u(N)$ n'est pas dans $\mathbb{Q}$. On peut supposer que $N \in U$. La courbe E/K a bonne réduction en $\mathfrak{p}_3$. Le groupe $\widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$ est d'ordre $240 = 2^4.3.5$ et $\pi_{\mathfrak{p}_3}(N_1)$ est d'ordre 15. On pose

$$Q_1 = 15N_1 \in E_1(K). \tag{18}$$

Notons G le sous-groupe de $E(K)$ engendré par $\{O, T_0, T_1, T_2\}$ et le point N_1.

Lemme 7. *On a* $\pi_{\mathfrak{p}_3}\big(E(K)\big) = \pi_{\mathfrak{p}_3}(G)$.

Démonstration : Il s'agit de démontrer que la condition 7 de l'appendice 2 est satisfaite, i.e. que l'indice de G dans $E(K)$ est premier à 30 (lemme 1 de l'appendice 2). Supposons le contraire. Dans ce cas, il existe $q \in \{2, 3, 5\}$ et $M \in E(K)$ tel que qM soit dans G sans que M le soit. Considérons un entier $n \in \mathbb{Z}$ et un point $T \in \{O, T_0, T_1, T_2\}$ tels que l'on ait $qM = T + nN_1$. L'entier n n'est pas divisible par q : sinon, $M - \frac{n}{q}N_1$ est un point de torsion (d'ordre divisant $2q$), par suite M est dans G, ce qui n'est pas. On en déduit que la condition suivante est réalisée :

$$N_1 + T \in qE(K) \quad \text{ou bien} \quad 2N_1 + T \in 5E(K) \quad (\text{si } q = 5).$$

Supposons qu'il existe $R \in E(K)$ tel que $N_1 + T = 2R$. On a $2N_1 = 4R$. Considérons l'idéal $\mathfrak{p}$ de A engendré par $-1+2\theta+\theta^2$. C'est l'un des cinq idéaux premiers de A au-dessus de 23. On vérifie que $\widetilde{E_{\mathfrak{p}}}(k_{\mathfrak{p}})$ est d'ordre 24 et que le point $\pi_{\mathfrak{p}}(N_1)$ est d'ordre 12. Par ailleurs, $\pi_{\mathfrak{p}}(T_0)$ et $\pi_{\mathfrak{p}}(N_1)$ engendrent $\widetilde{E_{\mathfrak{p}}}(k_{\mathfrak{p}})$. En particulier, $\widetilde{E_{\mathfrak{p}}}(k_{\mathfrak{p}})$ n'est pas un groupe cyclique. Si d est l'ordre de $\pi_{\mathfrak{p}}(R) \in \widetilde{E_{\mathfrak{p}}}(k_{\mathfrak{p}})$, on a l'égalité 6 $\operatorname{pgcd}(d, 4) = d$. Cela entraîne $d = 24$ puis une contradiction.

Supposons qu'il existe $R \in E(K)$ tel que $N_1 + T = 3R$. On a $2N_1 = 6R$. Soit d l'ordre de $\pi_{\mathfrak{p}_3}(R) \in \widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$. On a $d = 15$ $\operatorname{pgcd}(6, d)$. Puisque 3 divise d, on a $\operatorname{pgcd}(6, d) = 3$ ou 6 et d est multiple de 9. Le fait que d divise 240 entraîne alors une contradiction.

Supposons qu'il existe $R \in E(K)$ tel que $2N_1 + T = 5R$. On a $4N_1 = 10R$. Si d est l'ordre de $\pi_{\mathfrak{p}_3}(R)$, on a $d = 15$ $\operatorname{pgcd}(10, d)$. On a $\operatorname{pgcd}(10, d) = 5$ ou 10 et d est multiple de 25, d'où une contradiction. En particulier, $N_1 + T$ n'est pas dans $5E(K)$. D'où le lemme.

On considère alors l'ensemble $\mathfrak{S}$ des points de $E(K)$ qui s'écrivent sous la forme

$$T + jN_1 \quad \text{où} \quad T \in \{O, T_0, T_1, T_2\} \quad \text{et} \quad j = -7, \cdots, 7.$$

D'après le lemme 7 et la condition (19), il existe $S \in \mathfrak{S}$ tel que $N - S \in E_1(K)$. En utilisant le lemme 10 de l'appendice 1, quitte à remplacer N par $-M_1 - N$, on peut supposer que l'on a

$$N = S + P \quad \text{où} \quad S \in \Big\{ -4N_1, O, 2N_1, T_0 + 2N_1 \Big\} \quad \text{et} \quad P \in E_1(K).$$

Lemme 8. *Soit R un point de $E_1(K)$ non nul. On a*

$$\eta_{\mathfrak{p}_3}\big(z(R)\big) = \pm(\xi^4 + 2\xi + 2).$$

Démonstration : On a $z(Q_1) \equiv 3\theta^4 + 6\theta + 6$ mod. 9 et $v_{\mathfrak{p}_3}(3\theta^4 + 6\theta + 6) = 1$, d'où l'on déduit que

$$\eta_{\mathfrak{p}_3}\big(z(Q_1)\big) = \xi^4 + 2\xi + 2,$$

ce qui entraîne le résultat (cf. dém. du lemme 5).

1) Supposons $S = O$. On a $u(N) \equiv -2z(P)$ mod. $z(P)^2$, ce qui d'après le lemme 8, conduit à l'égalité $\eta_{\mathfrak{p}_3}\big(u(N)\big) = \pm(\xi^4 + 2\xi + 2)$.

2) Si $S = 2N_1$, on vérifie que l'on a

$$u(N) = -\frac{1}{2} + (\theta^3 + 2\theta^2)z(P)^2 \text{ mod. } z(P)^3.$$

Puisque $v_{\mathfrak{p}_3}(\theta^3 + 2\theta^2) = 0$, on déduit du lemme 8 que $\eta_{\mathfrak{p}_3}\big(u(N) + \frac{1}{2}\big) = \xi^4 + 2\xi^3 + \xi^2 + \xi + 1$.

3) Si $S = T_0 + 2N_1$, on obtient

$$u(N) = \frac{1}{2} + (-\theta^3 + 2\theta^2 + 4\theta - 8)z(P)^2 \text{ mod. } z(P)^3,$$

ce qui conduit à $\eta_{\mathfrak{p}_3}\big(u(N) + \frac{1}{2}\big) = 2\xi^4 + \xi^2 + 2$.

4) Si $S = -4N_1$, on constate dans ce cas que l'on a $\eta_{\mathfrak{p}_3}\big(u(N)\big) = \xi^4 + \xi^3 + 2\xi^2$.

Dans tous les cas, les projections considérées ne sont pas dans $\mathbb{F}_3$, ce qui prouve que $u(N)$ n'est pas dans $\mathbb{Q}$. D'où la proposition 6.

Cela termine la démonstration du théorème en ce qui concerne l'ensemble $C_{11}(\mathbb{Q})$.

6.2. L'ensemble $D_{11}(\mathbb{Q})$

Soit (α, β) un point de $\varphi_1\big(D_{11}(\mathbb{Q})\big)$. On pose $\alpha = \frac{s}{t}$, où s et t sont deux entiers premiers entre eux. Posons

$$\tau_1 = \theta^4 + \theta^3 - \theta \quad \text{et} \quad \tau_2 = -\theta^4 - 2\theta^3 - \theta^2 + \theta + 1.$$

Ce sont des éléments de A associés à π_{11}.

Lemme 9. *L'un des éléments $(s-t\theta)\tau_1$ et $(s-t\theta)\tau_2$ est un carré dans K.*

Démonstration : On a $N_{K/\mathbb{Q}}(s-t\theta) = G_5(s,t) \in 11\mathbb{Z}^2$ (prop. 3). Les $s-t\theta_i$ étant premiers entre eux en dehors de π_{11}, il existe donc des entiers n_i égaux à 0 ou 1 tels que

$$s - t\theta \equiv \pi_{11}(-1)^{n_0} \prod_{i=1}^{4} u_i^{n_i} \text{ mod. } K^{*2} \quad \text{et} \quad n_0 + n_1 \equiv 1 \text{ mod. } 2.$$

En exprimant de nouveau cette congruence dans $K^*_{\mathfrak{p}_2}$, on vérifie que cela entraîne

$$(n_0, n_1, n_2, n_3, n_4) \in \big\{(1,0,0,1,1), (0,1,1,0,1)\big\}.$$

Le lemme en résulte compte tenu du fait que l'on a $u_1u_2u_4\pi_{11} = \tau_1$ et $-u_3u_4\pi_{11} = \tau_2$.

On note dans la suite σ_j l'élément du groupe de Galois de K sur $\mathbb{Q}$ tel que $\sigma_j(\theta) = \theta_j$ $(1 \leqslant j \leqslant 5)$.

Supposons que $(s-t\theta)\tau_2$ est un carré dans K. Il existe alors $\delta \in K$ tel que l'on ait

$$\prod_{j=1}^{4} \sigma_j(\tau_2)(s - t\theta_j) = \delta^2,$$

d'où il résulte que l'on a

$$\left(\frac{t}{s} - \frac{1}{\theta}, \frac{\delta}{s^2}\right) \in \mathscr{D}''(K).$$

Par ailleurs, on a $E''(K) = \Big\{O, T_0, T_1, T_2\Big\}$. D'après la proposition 1 de l'appendice 1, on a donc $\mathscr{D}''(K) = \Big\{(0,0), \psi(T_0), \psi(T_1), \psi(T_2)\Big\}$. En explicitant les coordonnées des points $\psi(T_i)$, on constate que cela contredit le fait que t/s soit dans $\mathbb{Q}$. Par suite, $(s-t\theta)\tau_2$ n'est pas un carré dans K. On déduit alors du lemme 9 que l'on a

$$(s - t\theta)\tau_1 \in K^2.$$

Posons $\pi = \tau_1\sigma_2(\tau_1)\sigma_3(\tau_1)$. On a $\pi = 4\theta^4 - 8\theta^2 + 3\theta + 6$. Il existe $\nu \in K$ tel que l'on ait (lemme 9 et prop. 3) :

$$\pi(s-2t)(s-t\theta)(s-t\theta_2)(s-t\theta_3) = \nu^2.$$

Il en résulte que l'on a

$$\left(\frac{t}{s} - \frac{1}{2}, \frac{2\nu}{s^2}\right) \in \mathscr{D}'(K).$$

La description annoncée de $D_{11}(\mathbb{Q})$ se déduit alors du résultat suivant :

Proposition 7. *Soit (u,v) un point de $\mathscr{D}'(K)$ tel que u soit dans $\mathbb{Q}$, alors $(u,v)=(0,0)$.*

La proposition 7 est une conséquence de l'énoncé qui suit (prop. 1 de l'appendice 1) :

Proposition 8. *Il n'existe pas de points $N \in E'(K)\backslash\{O\}$ tels que $u(N)$ soit dans $\mathbb{Q}$.*

Démonstration de la proposition 8

Soit N un point de $E'(K)\backslash\{O\}$. La courbe elliptique E'/K a bonne réduction en $\mathfrak{p}_3$, le groupe $\widetilde{E'_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$ est d'ordre $248 = 2^3.31$ et $\pi_{\mathfrak{p}_3}(N_1)$ est d'ordre 62. On pose

$$Q_1 = 62N_1 \in E'_1(K). \tag{19}$$

Soit G le sous-groupe de $E'(K)$ engendré par $\{O, T_0, T_1, T_2\}$ et le point N_1.

Lemme 10. *On a $\pi_{\mathfrak{p}_3}\big(E'(K)\big) = \pi_{\mathfrak{p}_3}(G)$.*

Démonstration : Elle est identique à celle du lemme 7 : il s'agit ici de prouver que l'indice h de G dans $E'(K)$ est premier à 62.

1) Supposons que h soit pair. Il existe alors un point de torsion T de $E'(K)$ tel que $N_1 + T \in 2E'(K)$. On a $2N_1 = 4R$ avec $R \in E'(K)$. Soit $\mathfrak{p}$ l'idéal de A au-dessus de 23 engendré par $2 - 3\theta - 3\theta^2 + \theta^3 + \theta^4$. Le groupe $\widetilde{E_{\mathfrak{p}}}(k_{\mathfrak{p}})$ est d'ordre 16 et l'ordre de $\pi_{\mathfrak{p}}(N_1)$ est 8. Ainsi, l'ordre de $\pi_{\mathfrak{p}}(R)$ est 16 et l'on vérifie par ailleurs que $\widetilde{E_{\mathfrak{p}}}(k_{\mathfrak{p}})$ n'est pas cyclique, d'où une contradiction.

2) Si 31 divise h, il existe $j \in \{1, \ldots, 30\}$ tel que l'on ait $jN_1 + T \in 31E'(K)$. Soit R un point de $E'(K)$ tel que $jN_1 + T = 31R$. On a $2jN_1 = 62R$ et l'ordre de $\pi_{\mathfrak{p}_3}(2jN_1)$ est 31. Si d est l'ordre de $\pi_{\mathfrak{p}_3}(R)$, on a donc $d = 31$ pgcd $(62, d)$, et 31^2 doit diviser d, ce qui n'est pas. D'où le lemme.

Soit $\mathfrak{S}$ l'ensemble des points de $E'(K)$ qui s'écrivent sous la forme

$$T + jN_1 \quad \text{où} \quad T \in \{O, T_0, T_1, T_2\} \quad \text{et} \quad j = -30, \cdots, 31.$$

Il existe $S \in \mathfrak{S}$ tel que $N - S \in E'_1(K)$ (lemme 10 et (19)). En utilisant le lemme 10 de l'appendice 1, on vérifie que l'on se ramène au cas où $S = O$, autrement dit, on peut supposer que N appartient à $E'_1(K)$. On a $u(N)z(N) \neq 0$ et d'après la formule (32) de l'appendice 2 (avec $e = 0$), on a

$$u(N) \equiv dz(N)^2 \text{ mod. } z(N)^3.$$

On a $v_{\mathfrak{p}_3}(d) = 0$, d'où $\eta_{\mathfrak{p}_3}\big(u(N)\big) = \eta_{\mathfrak{p}_3}(d)\eta_{\mathfrak{p}_3}\big(z(N)\big)^2$. Par ailleurs, d'après le lemme 2 de l'appendice 2, on a $\eta_{\mathfrak{p}_3}\big(z(N)\big) = \pm\eta_{\mathfrak{p}_3}\big(z(Q_1)\big)$ et l'on vérifie que l'on a

$$\eta_{\mathfrak{p}_3}\big(z(Q_1)\big) = \xi^4 + 2\xi^3 + \xi^2 + \xi + 1.$$

Il en résulte que $\eta_{\mathfrak{p}_3}\big(u(N)\big) = 2\xi^4 + 2\xi^3 + \xi + 2$, qui n'est pas dans $\mathbb{F}_3$, ce qui prouve que $u(N)$ n'est pas dans $\mathbb{Q}$. D'où la proposition 8.

Cela termine la démonstration du théorème si $p = 11$.

7. Détermination de $C_{13}(\mathbb{Q})$ et $D_{13}(\mathbb{Q})$

7.1. L'ensemble $C_{13}(\mathbb{Q})$

Soit (α, β) un point de $\varphi_1\big(C_{13}(\mathbb{Q})\big)$. On pose $\alpha = \frac{s}{t}$, où s et t sont deux entiers premiers entre eux.

Lemme 11. *L'élément $F_1 = s^2 - \theta st + (\theta^2 + \theta - 3)t^2$ est un carré dans K.*

Démonstration : Pour tous i et j distincts, F_i et F_j sont premiers entre eux en dehors de π_{13} : en effet, en posant

$$h_1 = (3\theta^2 + 2\theta - 4)s + (2\theta^2 + 10\theta - 7)t, \quad h_2 = (-3\theta^2 - 2\theta + 4)s + (-2\theta^2 + 3\theta + 7)t,$$

on vérifie que l'on a $h_1F_1 + h_2F_2 = 13t^3$, ce qui compte tenu de l'action du groupe de Galois de K sur $\mathbb{Q}$, entraîne notre assertion. On a $G_6(s,t) \in \mathbb{Z}^2$, donc il existe des entiers $n_i = 0, 1$ tels que l'on ait (cf. la factorisation du formulaire) :

$$F_1 \equiv (-1)^{n_0} u_1^{n_1} u_2^{n_2} \pi_{13}^{n_3} \text{ mod. } K^{*2}.$$

On a $n_3 = 0$ et $n_0 + n_1$ est pair. Par ailleurs, on a $v_{\mathfrak{p}_2}(F_1) = 0$. En effet, si t est pair, alors s est impair, et l'on a $F_1 \equiv s^2 \equiv 1$ mod. 2. Si s est pair, t est impair, on a dans ce cas $F_1 \equiv \theta^2 + \theta - 3$ mod. 2 et $\theta^2 + \theta - 3$ est une unité de A, d'où l'assertion. La classe de F_1 modulo les carrés du complété $K_{\mathfrak{p}_2}$ ne dépend donc que des classes de s et t modulo 8. On constate alors que cela conduit à $n_0 = n_1 = 0$. D'où le lemme.

On en déduit qu'il existe $\delta \in K$ tel que l'on ait (lemme 9 et prop. 3) :

$$(s^2 - 4t^2)\big(s^2 - \theta st + (\theta^2 + \theta - 3)t^2\big) = \delta^2,$$

et l'on a $\big(\frac{t}{s}, \frac{\delta}{s^2}\big) \in \mathscr{D}(K)$. Comme dans les cas précédents, on démontre alors que si (u, v) un point de $\mathscr{D}(K)$ tel que u soit dans $\mathbb{Q}$, on a

$$(u, v) \in \left\{ \left(-\frac{1}{2}, 0\right), \left(\frac{1}{2}, 0\right), (0, -1), (0, 1) \right\}.$$

On a

$$\psi(2N_1) = \left(-\frac{1}{2}, 0\right) \quad \text{et} \quad \psi(T_0 + 2N_1) = \left(\frac{1}{2}, 0\right),$$

et l'on est ainsi amené à prouver le résultat suivant :

Proposition 9. *Les seuls points $N \in E(K)\backslash\{O, -M_1\}$ tels que $u(N) \in \mathbb{Q}$ sont $2N_1$ et $T_0 + 2N_1$.*

Démonstration de la proposition 9

Soit N un point de $E(K)\backslash\{O, -M_1\}$ distinct de $2N_1$ et de T_0+2N_1. On suppose que $N \in U$, ce qui n'est pas restrictif. La courbe E/K a bonne réduction en $\mathfrak{p}_3$. Le groupe $\widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$ est d'ordre 24 et $\pi_{\mathfrak{p}_3}(N_1)$ est d'ordre 12. On pose

$$Q_1 = 12N_1 \in E_1(K). \tag{20}$$

Soit G le sous-groupe de $E(K)$ engendré par T_0 et N_1.

Lemme 12.

1) On a $\pi_{\mathfrak{p}_3}(G) = \pi_{\mathfrak{p}_3}\big(E(K)\big)$.

2) L'indice dans $E_1(K)$ du sous-groupe engendré par Q_1 est premier à 3.

Démonstration : 1) On démontre que l'indice h de G dans $E(K)$ est premier à 6 : si h est pair, il existe $T \in \{O, T_0\}$ tel que $N_1 + T \in 2E(K)$; on vérifie que ni $\pi_{\mathfrak{p}_3}(N_1)$ ni $\pi_{\mathfrak{p}_3}(N_1 + T_0)$ ne sont des doubles dans $\widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$, d'où une contradiction. Si 3 divise h, il existe $T \in \{O, T_0\}$ tel que $N_1 + T \in 3E(K)$. On a $2N_1 = 6R$ avec $R \in E(K)$. Si d est l'ordre de $\pi_{\mathfrak{p}_3}(R)$, on a $d = 6\text{pgcd}(d, 6)$ donc 9 divise d, et l'on obtient de nouveau une contradiction. D'où l'assertion 1.

2) Supposons le contraire. Dans ce cas, il existe $M \in E_1(K)$ tel que l'on ait $3M = Q_1$. D'après (20), on obtient $3(M - 4N_1) = O$. Cela entraîne $M = 4N_1$, puis une contradiction car $4N_1$ n'appartient pas à $E_1(K)$. D'où le lemme.

Soit $\mathfrak{S}$ l'ensemble des points de $E(K)$ qui s'écrivent sous la forme

$$hT_0 + jN_1 \quad \text{avec} \quad h = 0, 1 \quad \text{et} \quad j = -5, \cdots, 6.$$

D'après l'assertion 1 du lemme 12 et la condition (20), il existe $S \in \mathfrak{S}$ tel que $N - S \in E_1(K)$. Par ailleurs, quitte à remplacer N par $-M_1 - N$ on peut supposer que l'on a (lemme 10 de l'appendice 1) :

$$N = S + P \quad \text{où} \quad S \in \{-5N_1, -4N_1, -3N_1, O, 2N_1, T_0 + 2N_1\} \quad \text{et} \quad P \in E_1(K).$$

Pour tout point S comme ci-dessus non nul, on pose $S = (x_S, y_S)$.

Lemme 13. *Soit R un point de $E_1(K)$ non nul. On a $\eta_{\mathfrak{p}_3}\big(z(R)\big) = \pm 1$.*

Démonstration : On a $z(Q_1) \equiv 6 \bmod. 9$. Par suite, $\eta_{\mathfrak{p}_3}\big(z(Q_1)\big) = -1$. Le lemme 2 de l'appendice 2 entraîne alors le résultat.

La condition 12 de l'appendice 2 n'est donc pas satisfaite et, tout au moins en ce qui concerne l'étude du cas où $S = O$, on ne peut pas conclure directement. Cela étant, la condition 13 de cet appendice est réalisée (assertion 2 du lemme 12). Par suite, il existe $n_1 \in \mathbb{Z}_3$ tel que l'on ait $P = n_1 Q_1$. En utilisant l'égalité (36) de l'appendice 2, on constate que l'on a

$$z(P) \equiv (9\theta^2 + 9\theta + 18)n_1^3 + (45\theta^2 + 63\theta + 42)n_1 \text{ mod. } 3^4. \tag{21}$$

1) Supposons $S = O$ i.e. $N = P$. On a

$$u(N) \equiv -2z(P) - \theta z(P)^2 + (-2\theta^2 - 2\theta + 14)z(P)^3 \text{ mod. } z(P)^4. \tag{22}$$

Il résulte alors des congruences (21) et (22) que l'on a

$$u(N) = \Phi_S^{(0)} + \Phi_S^{(1)}\theta + \Phi_S^{(2)}\theta^2,$$

avec

$$\Phi_S^{(0)} \equiv 27n_1^4 + 72n_1^3 + 54n_1^2 + 78n_1 \text{ mod. } 3^4,$$

$$\frac{\Phi_S^{(1)}}{9n_1} \equiv 4n_1^2 + 5n_1 + 4 \text{ mod. } 9, \quad \frac{\Phi_S^{(2)}}{9n_1} \equiv 4n_1^2 + 3n_1 + 8 \text{ mod. } 9.$$

On constate que la série $\frac{\Phi_S^{(1)}(X_1)}{9X_1}$ n'a pas de zéro modulo 9, en particulier elle n'a pas de zéro dans $\mathbb{Z}_3$. Cela prouve que $u(N)$ n'est pas dans $\mathbb{Q}$.

2) Supposons $S = -5N_1$ i.e. $N = -5N_1 + n_1 Q_1$. On a $v_{\mathfrak{p}_3}(x_S - \lambda) = 0$ et la condition 8 de l'appendice 2 est vérifiée. On obtient dans $A_{\mathfrak{p}_3}$ la congruence

$$\frac{1}{u(N)} \equiv \sum_{i=0}^{3} \rho_i z(P)^i \text{ mod. } 3^4, \tag{23}$$

$$\text{avec} \qquad \rho_0 = 45\theta^2 + 27\theta + 57, \quad \rho_1 = 52\theta^2 + 29\theta + 48, \quad \rho_2 = 6\theta^2 + \theta + 66,$$

$$\rho_3 = 12\theta^2 + 74\theta + 28.$$

On a $v_{\mathfrak{p}_3}(\rho_0) = 1$ et $v_{\mathfrak{p}_3}(\rho_1) = 0$, par suite, on ne peut pas conclure directement. On déduit de (21) et (23) que l'on a

$$\frac{1}{u(N)} = \Phi_S^{(0)} + \Phi_S^{(1)}\theta + \Phi_S^{(2)}\theta^2,$$

avec

$$\Phi_S^{(0)} \equiv 54n_1^4 + 9n_1^3 + 54n_1^2 + 18n_1 + 57 \text{ mod. } 3^4,$$

$$\Phi_S^{(1)} \equiv 18n_1^3 + 36n_1^2 + 12n_1 + 27 \text{ mod. } 3^4, \quad \Phi_S^{(2)} \equiv 27n_1^2 + 6n_1 + 45 \text{ mod. } 3^4.$$

On constate alors que les séries formelles $\Phi_S^{(1)}(X_1)$ et $\Phi_S^{(2)}(X_1)$ n'ont pas de zéros communs modulo 3^4. Cela prouve de nouveau que $u(N)$ n'est pas dans $\mathbb{Q}$.

3) Supposons $S = -4N_1$ i.e. $S = M_1$. La condition 9 de l'appendice 2 est satisfaite. On vérifie que $u(N) \equiv 2\theta + 1 \bmod. 3$, d'où $\eta_{\mathfrak{p}_3}\big(u(N)\big) = 2\xi + 1$.

4) Supposons $S = -3N_1$. On a $v_{\mathfrak{p}_3}(x_S - \lambda) = 0$, et l'on obtient

$$\frac{1}{u(N)} \equiv \sum_{i=0}^{3} \rho_i z(P)^i \bmod. 3^4, \tag{24}$$

$$\text{avec} \qquad \rho_0 = 78\theta^2 + 12\theta + 30, \quad \rho_1 = 2\theta^2 + 4\theta + 60, \quad \rho_2 = 78\theta^2 + 79\theta + 15,$$

$$\rho_3 = 24\theta^2 + 13\theta + 32.$$

On a $v_{\mathfrak{p}_3}(\rho_0) = 1$, $v_{\mathfrak{p}_3}(\rho_1) = 0$ et de nouveau on ne peut pas conclure directement. Il résulte de (21) et (24) que l'on a dans ce cas

$$\frac{1}{u(N)} = \Phi_S^{(0)} + \Phi_S^{(1)}\theta + \Phi_S^{(2)}\theta^2,$$

avec

$$\Phi_S^{(0)} \equiv 54n_1^4 + 18n_1^3 + 36n_1 + 30 \bmod. 3^4,$$

$$\Phi_S^{(1)} \equiv 63n_1^3 + 9n_1^2 + 24n_1 + 12 \bmod. 3^4, \quad \Phi_S^{(2)} \equiv 27n_1^2 + 21n_1 + 78 \bmod. 3^4.$$

On constate de nouveau que les séries formelles $\Phi_S^{(1)}(X_1)$ et $\Phi_S^{(2)}(X_1)$ n'ont pas de zéros communs modulo 3^4, par suite $u(N)$ n'est pas dans $\mathbb{Q}$.

5) Si $S = 2N_1 + T_0$, on constate que l'on a

$$u(N) - \frac{1}{2} \equiv (-\theta^2 + \theta - 1)z(P)^2 \bmod. z(P)^3.$$

On a $v_{\mathfrak{p}_3}(-\theta^2 + \theta - 1) = 0$ et l'on déduit alors du lemme 13 que l'on a :

$$\eta_{\mathfrak{p}_3}\left(u(N) - \frac{1}{2}\right) = \eta_{\mathfrak{p}_3}(-\theta^2 + \theta - 1) = 2\xi^2 + \xi + 2.$$

6) Si $S = 2N_1$, on a

$$u(N) + \frac{1}{2} \equiv (\theta^2 + 3\theta + 1)z(P)^2 \bmod. z(P)^3,$$

et $v_{\mathfrak{p}_3}(\theta^2 + 3\theta + 1) = 0$, d'où $\eta_{\mathfrak{p}_3}\big(u(N) + \frac{1}{2}\big) = \xi^2 + 1$.

Cela termine la démonstration de la proposition 9 et la description de $C_{13}(\mathbb{Q})$.

7.2. L'ensemble $D_{13}(\mathbb{Q})$

On considère un point (α, β) de $\varphi_1\big(D_{13}(\mathbb{Q})\big)$ et l'on pose $\alpha = \frac{s}{t}$, où s et t sont deux entiers premiers entre eux. Rappelons que l'on note $F_1 = s^2 - \theta st + (\theta^2 + \theta - 3)t^2$. Posons $\tau = \theta^2 - \theta + 1$. C'est un élément de A associé à π_{13}.

Lemme 14. *L'élément τF_1 est un carré dans K.*

Démonstration : On a $N_{K/\mathbb{Q}}(F_1) \in 13\mathbb{Z}^2$ et les F_i sont premiers entre eux en dehors de π_{13}, donc il existe des entiers n_i égaux à 0 ou 1 tels que l'on ait

$$F_1 \equiv \pi_{13}(-1)^{n_0} u_1^{n_1} u_2^{n_2} \text{ mod. } K^{*2} \quad \text{et} \quad n_0 + n_1 \equiv 0 \text{ mod. } 2.$$

En exprimant cette congruence dans $K^*_{\mathfrak{p}_2}$, on vérifie que cela entraîne $(n_0, n_1, n_2) = (1, 1, 0)$. Le lemme en résulte car on a $-u_1\pi_{13} = \tau$.

On déduit du lemme 14 et de la proposition 3 que l'on a

$$\tau\big(s^2 - 4t^2\big)\big(s^2 - \theta st + (\theta^2 + \theta - 3)t^2\big) \in K^2,$$

et $\frac{t}{s} + \frac{1}{2}$ est l'abscisse d'un point de $\mathscr{D}'(K)$. Par ailleurs, on a $E'(K) = \big\{T_0\big\}$ et $\psi(T_0) = (1, 0)$. Il en résulte que les seuls points de $\mathscr{D}'(K)$ sont $(0, 0)$ et $(1, 0)$, ce qui conduit à $\alpha = \pm 2$ et à l'ensemble $D_{13}(\mathbb{Q})$ annoncé.

Cela termine la démonstration du théorème si $p = 13$.

8. Détermination de $C_{17}(\mathbb{Q})$ et $D_{17}(\mathbb{Q})$

8.1. L'ensemble $C_{17}(\mathbb{Q})$

Soit α l'abscisse d'un point de $\varphi_1\big(C_{17}(\mathbb{Q})\big)$. On pose $\alpha = \frac{s}{t}$, où s et t sont deux entiers premiers entre eux et $F_1 = s^2 - \theta_4 st + \theta t^2$ (cf. le formulaire).

Lemme 15. *L'un des éléments F_1 et θF_1 est un carré dans K.*

Démonstration : Les conjugués de F_1 sont premiers entre eux deux à deux en dehors de π_{17}. Puisque $G_8(s, t) \in \mathbb{Z}^2$, il existe des entiers n_i égaux à 0 ou 1 tels que l'on ait

$$F_1 \equiv (-1)^{n_0} \prod_{i=1}^{3} u_i^{n_i} \pi_{17}^{n_4} \text{ mod. } K^{*2}. \tag{25}$$

On a $n_3 = n_4 = 0$. On exprime alors la condition (25) dans les complétés de K en les deux idéaux premiers $\mathfrak{p}_2$ et $\mathfrak{p}'_2$ de A. En utilisant le fait que l'on a $v_{\mathfrak{p}_2}(F_1) = v_{\mathfrak{p}'_2}(F_1) = 0$, on obtient le résultat.

1) Cas où $F_1 \in K^2$

Supposons que F_1 soit un carré dans K. Dans ce cas, on a

$$(s^2 - 4t^2)F_1 \in K^2,$$

d'où il résulte que $\frac{t}{s}$ est l'abscisse d'un point de $\mathscr{D}(K)$. Démontrons que si $(u, v) \in \mathscr{D}(K)$ est un point d'abscisse dans $\mathbb{Q}$, on a

$$(u, v) \in \left\{ \left(-\frac{1}{2}, 0\right), \left(\frac{1}{2}, 0\right), (0, -1), (0, 1) \right\}.$$

On a $\psi(T_0 + 2N_1) = \left(\frac{1}{2}, 0\right)$, $\psi(2N_1) = \left(-\frac{1}{2}, 0\right)$ et il s'agit de démontrer l'énoncé suivant :

Proposition 10. *Les seuls points $N \in E(K)\backslash\{O, -M_1\}$ tels que $u(N) \in \mathbb{Q}$ sont $2N_1$ et $T_0 + 2N_1$.*

Démonstration de la proposition 10

Vérifions d'abord que les points N_1 et N_2 de $E(K)$ sont $\mathbb{Z}$-linéairement indépendants. On calcule pour cela le régulateur R_E de E/K (cf. [Si1], p. 233), en utilisant l'algorithme écrit par J.Silverman permettant de déterminer la hauteur canonique d'un point d'une courbe elliptique sur un corps de nombres ([Si2]). On a programmé cet algorithme et l'on pourra trouver à l'adresse http://www.math.jussieu.fr/~ivorra, le programme *hc* fonctionnant avec le logiciel PARI, où cet algorithme est implanté. En notant $\widehat{h_E}$ la hauteur canonique sur E, on constate que l'on a

$$\widehat{h_E}(N_1) \approx 0.0694452, \quad \widehat{h_E}(N_2) \approx 0.2957562 \quad \text{et} \quad \widehat{h_E}(N_1 + N_2) \approx 0.5491700,$$

ce qui conduit à $R_E \approx 0.048311$. Puisque R_E est non nul, cela prouve notre assertion.

Considérons alors un point $N \in E(K)\backslash\{O, -M_1\}$ distinct de $2N_1$ et de $T_0 + 2N_1$. On peut supposer comme dans les cas précédents que N appartient à U. La courbe E/K a bonne réduction en $\mathfrak{p}_3$. Le groupe $\widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$ est d'ordre 86 et les points $\pi_{\mathfrak{p}_3}(N_1)$, $\pi_{\mathfrak{p}_3}(N_2)$ sont d'ordre 43. On pose

$$Q_1 = 43N_1 \in E_1(K) \quad \text{et} \quad Q_2 = 43N_2 \in E_1(K).$$

On a

$$\widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3}) = \mathbb{Z}\ \pi_{\mathfrak{p}_3}(N_1) \bigoplus \mathbb{Z}\ \pi_{\mathfrak{p}_3}(T_0). \tag{26}$$

Soit $\mathfrak{S}$ l'ensemble des points de $E(K)$ qui s'écrivent sous la forme

$$hT_0 + jN_1 \qquad h = 0, 1 \quad \text{et} \quad j = -21, \cdots, 21.$$

On a $M_1 = -4N_1$. D'après (26), l'application $\pi_{\mathfrak{p}_3}$ induit une bijection de $\mathfrak{S}$ sur $\widetilde{E_{\mathfrak{p}_3}}(k_{\mathfrak{p}_3})$. Il existe donc $S \in \mathfrak{S}$ tel que $N-S$ soit dans $E_1(K)$. En utilisant le lemme 10 de l'appendice 1, on constate qu'en changeant au besoin N par $-M_1 - N$, on peut supposer que l'on a

$$N = S + P \quad \text{où} \quad S \in \Big\{ -6N_1, -4N_1, O, 2N_1, T_0 + 2N_1 \Big\} \quad \text{et} \quad P \in E_1(K).$$

Soient H le sous-groupe d'indice fini de $E_1(K)$ engendré par Q_1 et Q_2 et Γ le sous-$\mathbb{F}_3$-espace vectoriel de $k_{\mathfrak{p}_3}$ engendré par les $\eta_{\mathfrak{p}_3}\big(z(Q)\big)$ où $Q \in H\backslash\big\{O\big\}$ (cf. l'appendice 2). Notons Γ' le sous-$\mathbb{F}_3$-espace vectoriel de $k_{\mathfrak{p}_3}$ engendré par $1 + 2\xi + 2\xi^2 + \xi^3$ et $2\xi + \xi^2$.

Lemme 16. *On a $\Gamma = \Gamma'$. En particulier, pour tout $R \in E_1(K)$ non nul, $\eta_{\mathfrak{p}_3}\big(z(R)\big)$ appartient à Γ' et l'on a $\eta_{\mathfrak{p}_3}\big(z(R)\big) \neq \pm 1$.*

Démonstration : On a

$$\eta_{\mathfrak{p}_3}\big(z(Q_1)\big) = 1 + 2\xi + 2\xi^2 + \xi^3 \quad \text{et} \quad \eta_{\mathfrak{p}_3}\big(z(Q_2)\big) = 2\xi + \xi^2.$$

Par suite, Γ' est contenu dans Γ. Inversement, soit Q un élément de $H\backslash\big\{O\big\}$. Il s'agit de démontrer que $\eta_{\mathfrak{p}_3}\big(z(Q)\big)$ appartient à Γ'. Il existe n_1 et n_2 dans $\mathbb{Z}$ tels que $Q = n_1Q_1 + n_2Q_2$.
Si $n_1n_2 = 0$, alors $\eta_{\mathfrak{p}_3}\big(z(Q)\big)$ est égal à $\pm\eta_{\mathfrak{p}_3}\big(z(Q_1)\big)$ ou bien à $\pm\eta_{\mathfrak{p}_3}\big(z(Q_2)\big)$, d'où le résultat dans ce cas.
Supposons $n_1n_2 \neq 0$. Posons $z_1 = z(n_1Q_1)$ et $z_2 = z(n_2Q_2)$. On a

$$\eta_{\mathfrak{p}_3}(z_1) = \pm(1 + 2\xi + 2\xi^2 + \xi^3) \quad \text{et} \quad \eta_{\mathfrak{p}_3}(z_2) = \pm(2\xi + \xi^2).$$

Puisque l'on a $\eta_{\mathfrak{p}_3}(z_1) + \eta_{\mathfrak{p}_3}(z_2) \neq 0$, $\eta_{\mathfrak{p}_3}(z_1 + z_2)$ appartient à Γ' (condition (23) de l'appendice 2). Par ailleurs, on a

$$z(Q) = \mathfrak{F}(z_1, z_2).$$

Le fait que $v_{\mathfrak{p}_3}(z_1 + z_2) = \mathrm{Min}\big(v_{\mathfrak{p}_3}(z_1), v_{\mathfrak{p}_3}(z_2)\big)$ (car $\eta_{\mathfrak{p}_3}(z_1) + \eta_{\mathfrak{p}_3}(z_2) \neq 0$) et l'égalité (11) de l'appendice 2 impliquent alors

$$\eta_{\mathfrak{p}_3}\big(z(Q)\big) = \eta_{\mathfrak{p}_3}(z_1 + z_2),$$

ce qui prouve notre assertion. Le lemme 2 de l'appendice 2 entraîne alors le résultat.

Lemme 17. *L'indice de H dans $E_1(K)$ est premier à 3.*

Démonstration : Supposons que cet indice soit divisible par 3. Dans ce cas, il existe un point $P \in E_1(K)$ tel que $3P$ soit dans H sans que P le soit. Compte tenu du fait que le sous-groupe de torsion de $E(K)$ soit d'ordre 2, il en résulte que l'un des points N_1, N_2, $N_1 + N_2$ et $N_1 - N_2$ appartient à $3E(K)$.

Supposons qu'il existe $R \in E(K)$ tel que $N_1 = 3R$. Considérons l'idéal $\mathfrak{p}$ de A engendré par $-\theta^3 - 2\theta^2 + 5\theta + 5$. C'est l'un des quatre idéaux de A au-dessus de 47. L'ordre de $\widetilde{E_{\mathfrak{p}}}(k_{\mathfrak{p}})$ est 54 et celui de $\pi_{\mathfrak{p}}(N_1)$ est 27. On en déduit que $\pi_{\mathfrak{p}}(R)$ est d'ordre multiple de 81, d'où une contradiction dans ce cas. De même, on vérifie que $\pi_{\mathfrak{p}}(N_2)$ et $\pi_{\mathfrak{p}}(N_1 - N_2)$ sont d'ordre 54, ce qui entraîne de nouveau que N_2 et $N_1 - N_2$ ne sont pas dans $3E(K)$.

Supposons qu'il existe $R \in E(K)$ tel que $N_1 + N_2 = 3R$. On considère l'idéal $\mathfrak{p}'$ de A engendré par $-\theta^3 + 7\theta - 1$. C'est l'un des quatre idéaux de A au-dessus de 89. L'ordre de $\widetilde{E_{\mathfrak{p}'}}(k_{\mathfrak{p}'})$ est 90 et celui de $\pi_{\mathfrak{p}'}(N_1)$ est 45. Par suite, l'ordre de $\pi_{\mathfrak{p}'}(R)$ est multiple de 27, d'où une contradiction et le lemme.

1) Supposons $S = O$. On a $u(N) \equiv -2z(P) \bmod z(P)^2$, et donc par conséquent $\eta_{\mathfrak{p}_3}\big(u(N)\big) = \eta_{\mathfrak{p}_3}\big(z(P)\big)$, qui, d'après le lemme 16, n'est pas dans $\mathbb{F}_3$, donc $u(N)$ n'est pas dans $\mathbb{Q}$.

2) Supposons $S = -6N_1$. La condition 8 de l'appendice 2 est réalisée et l'on a dans $A_{\mathfrak{p}_3}$ la congruence

$$\frac{1}{u(N)} \equiv \sum_{i=0}^{3} \rho_i z(P)^i \bmod 3^4,$$

avec

$$\rho_0 = 3\theta^3 + 75\theta^2 + 45\theta + 6, \qquad \rho_1 = 78\theta^3 + 73\theta^2 + 14\theta + 4,$$
$$\rho_2 = 37\theta^3 + 35\theta^2 + 17\theta + 6, \qquad \rho_3 = 70\theta^3 + 61\theta^2 + 59\theta + 29.$$

On a $v_{\mathfrak{p}_3}(\rho_0) = 1$ et $v_{\mathfrak{p}_3}(\rho_1) = 0$, de sorte que l'on ne peut pas conclure directement. D'après le lemme 17, il existe deux éléments n_1 et n_2 de $\mathbb{Z}_3$ tels que $P = n_1 Q_1 + n_2 Q_2$. On déduit alors de l'égalité (36) de l'appendice 2 que l'on a

$$\frac{1}{u(N)} = \Phi_S^{(0)} + \Phi_S^{(1)}\theta + \Phi_S^{(2)}\theta^2 + \Phi_S^{(3)}\theta^3,$$

avec

$$\Phi_S^{(0)} = 54n_1^4 + (27n_2 + 45)n_1^3 + 72n_1^2 + (27n_2^3 + 54n_2^2 + 63n_2 + 21)n_1 + (27n_2^4 + 72n_2^3 + 9n_2^2 + 15n_2 + 6),$$
$$\Phi_S^{(1)} = 63n_1^3 + (54n_2 + 9)n_1^2 + 72n_2n_1 + (45n_2^3 + 72n_2^2 + 9n_2 + 45),$$
$$\Phi_S^{(2)} = 27n_1^4 + 27n_2n_1^3 + (27n_2 + 18)n_1^2 + (27n_2^2 + 63n_2 + 69)n_1 + (54n_2^4 + 72n_2^3 + 9n_2^2 + 51n_2 + 75),$$
$$\Phi_S^{(3)} = 54n_1^4 + 72n_1^3 + 54n_2n_1^2 + (54n_2^3 + 27n_2^2 + 45n_2 + 75)n_1 + (27n_2^4 + 27n_2^3 + 36n_2^2 + 54n_2 + 3).$$

On constate alors que les séries $\Phi_S^{(j)}(X_1, X_2)$ pour $j = 1, 2, 3$ n'ont pas de zéros communs modulo 81, ce qui prouve que $u(N)$ n'est pas dans $\mathbb{Q}$.

3) Supposons $S = -4N_1$ i.e. $S = M_1$. On a $v_{\mathfrak{p}_3}(3x_S^2 + 2a_2x_S + a_4 - dy_S) = 0$, la condition 9 de l'appendice 2 est satisfaite et l'on a

$$u(N) \equiv \theta^3 + \theta^2 + 2\theta + 2 \bmod 3,$$

et puisque $v_{\mathfrak{p}_3}(\theta^3+\theta^2+2\theta+2)=0$, on obtient $\eta_{\mathfrak{p}_3}\big(u(N)\big)=\xi^3+\xi^2+2\xi+2$.

4) Supposons $S=2N_1$. On a dans ce cas

$$u(N)+\frac{1}{2}\equiv\rho_2 z(P)^2 \text{ mod. } z(P)^3,\quad \rho_2=-\theta^3-2\theta^2+5\theta+7\quad\text{et}\quad v_{\mathfrak{p}_3}(\rho_2)=0.$$

Il en résulte que

$$\eta_{\mathfrak{p}_3}\left(u(N)+\frac{1}{2}\right)=\eta_{\mathfrak{p}_3}(\rho_2)\eta_{\mathfrak{p}_3}\big(z(P)\big)^2.$$

D'après le lemme 16, il existe α_1 et α_2 dans $\mathbb{F}_3$ non tous les deux nuls tels que l'on ait

$$\eta_{\mathfrak{p}_3}\big(z(P)\big)=\alpha_1(1+2\xi+2\xi^2+\xi^3)+\alpha_2(2\xi+\xi^2)\in\Gamma'.$$

Par ailleurs, on a $\eta_{\mathfrak{p}_3}(\rho_2)=2\xi^3+\xi^2+2\xi+1$. On vérifie alors que $\eta_{\mathfrak{p}_3}(\rho_2)\eta_{\mathfrak{p}_3}\big(z(P)\big)^2$ n'est pas dans $\mathbb{F}_3$ et $u(N)$ n'est pas dans $\mathbb{Q}$.

5) Supposons $S=T_0+2N_1$. On a

$$u(N)-\frac{1}{2}\equiv\rho_2 z(P)^2 \text{ mod. } z(P)^3,\quad \rho_2=-\theta^3-2\theta^2+3\theta-1\quad\text{et}\quad v_{\mathfrak{p}_3}(\rho_2)=0.$$

et l'on vérifie comme ci-dessus de $\eta_{\mathfrak{p}_3}(\rho_2)\eta_{\mathfrak{p}_3}\big(z(P)\big)^2$ n'est pas dans $\mathbb{F}_3$.

Cela prouve la proposition 10. On a ainsi démontré que si F_1 est un carré dans K, alors on a $\alpha=\pm2$.

2) Cas où $F_1\in\theta K^2$

On suppose que θF_1 est un carré dans K. Dans ce cas, on a

$$(s^2-4t^2)\theta F_1\in K^2,$$

d'où il résulte que $\frac{t}{s}+\frac{1}{2}$ est l'abscisse d'un point de $\mathscr{D}'(K)$. Par ailleurs, $E'(K)$ est de rang 0 et l'on a $E'(K)=\Big\{O,T_0\Big\}$. Les égalités $\psi(O)=(0,0)$ et $\psi(T_0)=(1,0)$ entraînent alors $\frac{t}{s}=\pm\frac{1}{2}$.

Dans les deux cas envisagés ci-dessus, on a $\alpha=\pm2$, et l'on obtient ainsi la description de $C_{17}(\mathbb{Q})$.

8.2. L'ensemble $D_{17}(\mathbb{Q})$

Soit α l'abscisse d'un point de $\varphi_1\big(D_{17}(\mathbb{Q})\big)$. On pose $\alpha=\frac{s}{t}$, où s et t sont deux entiers premiers entre eux.

Lemme 18. *L'un des éléments $-u_3\pi_{17}F_1$ et $-u_1u_3\pi_{17}F_1$ est un carré dans K.*

Démonstration : On a $G_8(s,t) \in 17\mathbb{Z}^2$, donc il existe des entiers n_i égaux à 0 ou 1 tels que l'on ait

$$F_1 \equiv \pi_{17}(-1)^{n_0} \prod_{i=1}^{3} u_i^{n_i} \text{ mod. } K^{*2}.$$

On a dans ce cas $n_3 = 1$. En exprimant cette congruence dans $K^*_{\mathfrak{p}_2}$ et $K^*_{\mathfrak{p}'_2}$, on vérifie que cela entraîne $(n_0, n_1, n_2) = (1, 0, 0)$ ou $(1, 1, 0)$. D'où le lemme.

1) Supposons que $-u_3\pi_{17}F_1$ soit un carré dans K. Dans ce cas, on a

$$-(s^2 - 4t^2)u_3\pi_{17}F_1 \in K^2,$$

d'où il résulte que $\frac{t}{s} + \frac{1}{2}$ est l'abscisse d'un point de $\mathscr{D}''(K)$. On a $E''(K) = \left\{O, T_0\right\}$, ce qui conduit, comme ci-dessus, à $\alpha = \pm 2$.

2) Si $-u_1u_3\pi_{17}F_1$ est un carré dans K, on écrit que

$$-(s^2 - 4t^2)u_1u_3\pi_{17}F_1 \in K^2,$$

et l'on constate que $\frac{t}{s} + \frac{1}{2}$ est l'abscisse d'un point de $\mathscr{D}'''(K)$. On a $E'''(K) = \left\{O, T_0\right\}$ et l'on obtient de nouveau $\alpha = \pm 2$.

On en déduit alors la détermination de $D_{17}(\mathbb{Q})$.

Cela termine la démonstration du théorème 2.

FORMULAIRE

1. Cas où $p = 7$

1.1. Le corps K

K	$K = \mathbb{Q}(\theta)$	$\theta^3 + \theta^2 - 2\theta - 1 = 0$	
Conjugués de θ	$\theta_1 = \theta$	$\theta_2 = \theta^2 - 2$	$\theta_3 = -\theta^2 - \theta + 1$
Anneau d'entiers	$A = \mathbb{Z}[\theta]$		
Unités	$u_1 = \theta^2 - 1$	$u_2 = \theta + 1$	
	$N_{K/\mathbb{Q}}(u_1) = -1$	$N_{K/\mathbb{Q}}(u_2) = -1$	
Idéaux	$2.A = \mathfrak{p}_2$	$3.A = \mathfrak{p}_3$	
	$7.A = (\pi_7 A)^3$	$\pi_7 = \theta^2 + 2\theta - 1$	$N_{K/\mathbb{Q}}(\pi_7) = 7$
$G_3(s,t)$	$s^3 + s^2 t - 2st^2 - t^3$		
Factorisation	$\prod_{i=1}^{3}(s - t\theta_i)$		

1.2. La quartique

Quartique $v^2 = au^4 + bu^3 + cu^2 + du + e$					
$\mathscr{D}/K$	$a = 4\theta^2 - 4$	$b = 4\theta^2 + 4\theta - 8$	$c = -\theta^2 - 3$	$d = -\theta^2 - \theta + 2$	$e = 1$

1.3. La courbe elliptique

E/K $y^2 = x^3 + a_2x^2 + a_4x + a_6$			
Coefficients	$a_2 = -\theta^2 - 3$	$a_4 = -8\theta^2 + 4\theta - 4$	$a_6 = 56\theta^2 - 28\theta$
Torsion : $(\mathbb{Z}/2\mathbb{Z})^2$	$T_0 = (\theta^2 + 3, 0)$	$T_1 = (2\theta^2 - 2\theta - 4, 0)$	$T_2 = (-2\theta^2 + 2\theta + 4, 0)$
Rang r de $E(K)$	$r = 1$		
Point d'ordre infini	$N_1 = (2\theta^2 - 4\theta, -6\theta^2 + 10\theta + 4)$		

2. Cas où $p = 11$

2.1. Le corps K

K	$K = \mathbb{Q}(\theta)$	$\theta^5 + \theta^4 - 4\theta^3 - 3\theta^2 + 3\theta + 1 = 0$	
Conjugués de θ	$\theta_1 = \theta$	$\theta_2 = \theta^2 - 2$	$\theta_3 = -\theta^4 - \theta^3 + 3\theta^2 + 2\theta - 1$
	$\theta_4 = \theta^3 - 3\theta$	$\theta_5 = \theta^4 - 4\theta^2 + 2$	
Anneau d'entiers	$A = \mathbb{Z}[\theta]$		
Unités	$u_1 = \theta$	$u_2 = \theta^4 - 3\theta^2 + 1$	$u_3 = \theta^3 - 2\theta$
	$u_4 = \theta^2 + \theta - 1$		
	$N_{K/\mathbb{Q}}(u_1) = -1$	$N_{K/\mathbb{Q}}(u_2) = 1$	$N_{K/\mathbb{Q}}(u_3) = 1$
	$N_{K/\mathbb{Q}}(u_4) = 1$		
Idéaux	$2.A = \mathfrak{p}_2$		
	$3.A = \mathfrak{p}_3$		
	$11.A = (\mathfrak{p}_{11}.A)^5$	$\pi_{11} = \theta^4 + \theta^3 - 3\theta^2 - \theta + 1$	$N_{K/\mathbb{Q}}(\pi_{11}) = -11$
$G_5(s,t)$	$s^5 + s^4t - 4s^3t^2 - 3s^2t^3 + 3st^4 + t^5$		
Factorisation	$\prod_{i=1}^{5}(s - t\theta_i)$		

2.2. Les quartiques

Quartiques $v^2 = au^4 + bu^3 + cu^2 + du + e$		
$\mathscr{D}/K$	$a = -4\theta^3 + 8\theta$	$b = 4\theta^2 + 4\theta - 8$
	$c = \theta^3 - 2\theta - 4$	$d = -\theta^2 - \theta + 2$
	$e = 1$	
$\mathscr{D}'/K$	$a = -64\theta^3 - 56\theta^2 + 24\theta - 16$	$b = 48\theta^4 - 120\theta^3 - 36\theta^2 + 180\theta - 112$
	$c = -88\theta^3 + 198\theta^2 + 242\theta - 220$	$d = -44\theta^4 - 22\theta^3 + 165\theta^2 + 55\theta - 132$
	$e = 0$	
$\mathscr{D}''/K$	$a = -8\theta^4 - 24\theta^3 + 17\theta^2 + 58\theta + 15$	$b = -44\theta^4 - 99\theta^3 + 99\theta^2 + 242\theta + 55$
	$c = -66\theta^4 - 99\theta^3 + 154\theta^2 + 275\theta + 77$	$d = -22\theta^4 - 33\theta^3 + 66\theta^2 + 110\theta + 11$
	$e = 0$	

2.3. Les courbes elliptiques

E/K $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = \theta^3 - 2\theta - 4 \qquad a_4 = -4\theta^4 + 8\theta^3 + 12\theta^2 - 16\theta - 16$ $a_6 = 28\theta^4 - 56\theta^3 - 72\theta^2 + 108\theta + 72$
Torsion : $(\mathbb{Z}/2\mathbb{Z})^2$	$T_0 = (-\theta^3 + 2\theta + 4, 0) \qquad T_1 = (2\theta^2 - 2\theta - 4, 0)$ $T_2 = (-2\theta^2 + 2\theta + 4, 0)$
Rang r de $E(K)$	$r = 1$
Point d'ordre infini	$N_1 = (-2\theta^4 + 2\theta^3 + 8\theta^2 - 8\theta, 10\theta^4 - 8\theta^3 - 36\theta^2 + 30\theta + 10)$

E'/K $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = -88\theta^3 + 198\theta^2 + 242\theta - 220$ $a_4 = -484\theta^4 + 10648\theta^3 - 10164\theta^2 - 19360\theta + 17424$ $a_6 = -53240\theta^4 - 234256\theta^3 + 308792\theta^2 + 393976\theta - 383328$
Torsion : $(\mathbb{Z}/2\mathbb{Z})^2$	$T_0 = \Big(-44\theta^3 - 66\theta^2 + 22\theta + 44, 0\Big), \quad T_1 = \Big(44\theta^4 + 44\theta^3 - 154\theta^2 - 110\theta + 88, 0\Big)$ $T_2 = \Big(-44\theta^4 + 88\theta^3 + 22\theta^2 - 154\theta + 88, 0\Big)$
Rang r de $E'(K)$	$r = 1$
Point d'ordre infini	$N_1 = \Big(-44\theta^4 + 44\theta^3 + 66\theta^2 - 22\theta + 88, -1232\theta^4 + 2464\theta^2 + 528\theta + 88\Big)$

E''/K	
$y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = -66\theta^4 - 99\theta^3 + 154\theta^2 + 275\theta + 77$ $a_4 = -55566\theta^4 - 100043\theta^3 + 13068\theta^2 + 26741\theta + 6413$ $a_6 = -1450790\theta^4 - 2715240\theta^3 + 3527150\theta^2 + 736043\theta + 175692$
Torsion : $(\mathbb{Z}/2\mathbb{Z})^2$	$T_0 = \left(33\theta^4 + 55\theta^3 - 88\theta^2 - 165\theta - 44, 0\right)$, $T_1 = \left(22\theta^4 + 11\theta^3 - 55\theta^2 - 44\theta - 11, 0\right)$ $T_2 = \left(11\theta^4 + 33\theta^3 - 11\theta^2 - 66\theta - 22, 0\right)$
Rang r de $E''(K)$	$r = 0$

3. Cas où $p = 13$

3.1. Le corps K

K	$K = \mathbb{Q}(\theta)$	$\theta^3 + \theta^2 - 4\theta + 1 = 0$	
Conjugués de θ	$\theta_1 = \theta$	$\theta_2 = -\theta^2 - 2\theta + 2$	$\theta_3 = \theta^2 + \theta - 3$
Anneau d'entiers	$A = \mathbb{Z}[\theta]$		
Unités	$u_1 = \theta$	$u_2 = \theta - 1$	
	$N_{K/\mathbb{Q}}(u_1) = -1$	$N_{K/\mathbb{Q}}(u_2) = 1$	
Idéaux	$2.A = \mathfrak{p}_2$		
	$3.A = \mathfrak{p}_3$		
	$13.A = (\pi_{13}.A)^3$	$\pi_{13} = \theta^2 - 3$	$N_{K/\mathbb{Q}}(\pi_{13}) = 13$
$G_6(s,t)$	$-t^6 + 3st^5 + 6s^2t^4 - 4s^3t^3 - 5s^4t^2 + s^5t + s^6$		
Factorisation	$(s^2 - \theta st + \theta_3t^2)(s^2 - \theta_2st + \theta t^2)(s^2 - \theta_3st + \theta_2t^2)$		

3.2. Les quartiques

Quartiques $v^2 = au^4 + bu^3 + cu^2 + du + e$				
$\mathscr{D}/K$	$a = -4\theta^2 - 4\theta + 12$	$b = 4\theta$	$c = \theta^2 + \theta - 7$	$d = -\theta$
	$e = 1$			
$\mathscr{D}'/K$	$a = -8\theta^2 + 4\theta + 8$	$b = 8\theta^2 + 12\theta - 20$	$c = -2\theta^2 - 21\theta + 12$	$d = 2\theta^2 + 5\theta$
	$e = 0$			

3.3. Les courbes elliptiques

E/K $y^2 = x^3 + a_2x^2 + a_4x + a_6$			
Coefficients	$a_2 = \theta^2 + \theta - 7$	$a_4 = 12\theta^2 + 16\theta - 48$	$a_6 = -84\theta^2 - 108\theta + 320$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (-\theta^2 - \theta + 7, 0)$		
Rang r de $E(K)$	$r = 1$		
Point d'ordre infini	$N_1 = (-2\theta^2 - 4\theta + 8, 2\theta)$		

E'/K $y^2 = x^3 + a_2x^2 + a_4x + a_6$			
Coefficients	$a_2 = -2\theta^2 - 21\theta + 12$	$a_4 = 36\theta^2 + 76\theta - 48$	$a_6 = -52\theta^2 - 104\theta + 52$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (2\theta^2 + 5\theta, 0)$		
Rang r de $E(K)$	$r = 0$		

4. Cas où $p = 17$

4.1. Le corps K

K	$K = \mathbb{Q}(\theta)$	$\theta^4 + \theta^3 - 6\theta^2 - \theta + 1 = 0$	
Conjugués de θ	$\theta_1 = \theta$	$\theta_2 = \theta^3 + \theta^2 - 6\theta - 1$	$\theta_3 = -\frac{1}{2}\theta^3 + 3\theta - \frac{3}{2}$
	$\theta_4 = -\frac{1}{2}\theta^3 - \theta^2 + 2\theta + \frac{3}{2}$		
Anneau d'entiers	$A = \mathbb{Z}\left[1, \theta, \theta^2, \frac{\theta^3+1}{2}\right]$		
Unités	$u_1 = \theta$	$u_2 = \frac{1}{2}\theta^3 + \theta^2 - 2\theta - \frac{3}{2}$	$u_3 = \frac{1}{2}\theta^3 + \theta^2 - 3\theta - \frac{3}{2}$
	$N_{K/\mathbb{Q}}(u_1) = 1$	$N_{K/\mathbb{Q}}(u_2) = 1$	$N_{K/\mathbb{Q}}(u_3) = -1$
Idéaux	$2.A = \mathfrak{p}_2\mathfrak{p}_2'$	$\mathfrak{p}_2 = (\theta + 1)A$	$\mathfrak{p}_2' = \left(-\frac{1}{2}\theta^3 - \theta^2 + 2\theta + \frac{1}{2}\right)A$
	$3.A = \mathfrak{p}_3$		
	$17.A = (\pi_{17}.A)^4$	$\pi_{17} = -\frac{1}{2}\theta^3 - \theta^2 + \theta + \frac{3}{2}$	$N_{K/\mathbb{Q}}(\pi_{17}) = -17$

$G_8(s,t)$	$t^8 - 4st^7 - 10s^2t^6 + 10s^3t^5 + 15s^4t^4 - 6s^5t^3 - 7s^6t^2 + s^7t + s^8$
Factorisation	$(s^2 - \theta_4 st + \theta t^2)(s^2 - \theta_3 st + \theta_2 t^2)(s^2 - \theta st + \theta_3 t^2)(s^2 - \theta_2 st + \theta_4 t^2)$

4.2. Les quartiques

Quartiques $v^2 = au^4 + bu^3 + cu^2 + du + e$			
$\mathscr{D}/K$	$a = -4\theta$	$b = -2\theta^3 - 4\theta^2 + 8\theta + 6$	$c = \theta - 4$
	$d = \frac{1}{2}\theta^3 + \theta^2 - 2\theta - \frac{3}{2}$	$e = 1$	
$\mathscr{D}'/K$	$a = -4\theta^2$	$b = -2\theta^3 + 4\theta^2 + 4\theta + 2$	$c = 3\theta^3 + \theta^2 - 10\theta - 3$
	$d = -\theta^3 - \theta^2 + 6\theta + 1$	$e = 0$	
$\mathscr{D}''/K$	$a = 2\theta^3 - 8\theta^2 - 8\theta - 2$	$b = -14\theta^3 + 56\theta + 26$	$c = \frac{39}{2}\theta^3 + 18\theta^2 - 90\theta - \frac{91}{2}$
	$d = -\frac{15}{2}\theta^3 - 10\theta^2 + 42\theta + \frac{43}{2}$	$e = 0$	
$\mathscr{D}'''/K$	$a = -10\theta^3 + 4\theta^2 - 2$	$b = 14\theta^3 - 28\theta^2 + 12\theta + 14$	$c = -\frac{3}{2}\theta^3 + 27\theta^2 - 26\theta - \frac{39}{2}$
	$d = -\frac{5}{2}\theta^3 - 3\theta^2 + 14\theta + \frac{15}{2}$	$e = 0$	

4.3. Les courbes elliptiques

E/K $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = \theta - 4 \qquad a_4 = 2\theta^3 - 4\theta - 10 \qquad a_6 = -10\theta^3 + 8\theta^2 + 8\theta + 38$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (4 - \theta, 0)$
Rang r de $E(K)$	$r = 2$
Points d'ordre infini	$N_1 = (-2\theta + 4, \theta^3 - 4\theta + 1)$
$\mathbb{Z}$-indépendants	$N_2 = (-\theta^3 - \theta^2 + 7\theta + 1, \theta^3 - \theta^2 - 4\theta + 2)$

E'/K $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = 3\theta^3 + \theta^2 - 10\theta - 3, \quad a_4 = -2\theta^3 - 4\theta^2 + 16\theta + 6 \qquad a_6 = -4$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (-\theta^3 - \theta^2 + 6\theta + 1, 0)$
Rang r de $E'(K)$	$r = 0$

E''/K $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = \frac{39}{2}\theta^3 + 18\theta^2 - 90\theta - \frac{91}{2} \qquad a_4 = -328\theta^3 - 456\theta^2 + 1848\theta + 972$ $a_6 = 1448\theta^3 + 1936\theta^2 - 8016\theta - 4204$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = \Big(-\frac{15}{2}\theta^3 - 10\theta^2 + 42\theta + \frac{43}{2}, 0 \Big)$
Rang r de $E''(K)$	$r = 0$

E'''/K $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = -\frac{3}{2}\theta^3 + 27\theta^2 - 26\theta - \frac{39}{2} \qquad a_4 = 8\theta^3 - 124\theta^2 + 200\theta + 128$ $a_6 = -12\theta^3 + 144\theta^2 - 304\theta - 184$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = \Big(-\frac{5}{2}\theta^3 - 3\theta^2 + 14\theta + \frac{15}{2}, 0 \Big)$
Rang r de $E'''(K)$	$r = 0$

Appendice 1. Quartiques et équations de Weierstrass

Soient K_0 un corps algébriquement clos de caractéristique différente de 2 et K un sous-corps de K_0. On considère des éléments a, b, c, d et e de K et le polynôme

$$f = aX^4 + bX^3 + cX^2 + dX + e \in K[X].$$

Soit $\mathscr{D}/K$ la courbe affine d'équation

$$v^2 = f(u). \tag{1}$$

On suppose que les conditions suivantes sont satisfaites :

1. on a $a \neq 0$;
2. $\mathscr{D}$ est lisse, i.e. le discriminant de f est non nul ;
3. $\mathscr{D}$ possède un point (α, β) rationnel sur K.

On note $\widehat{\mathscr{D}}$ la complétée projective de $\mathscr{D}$ d'équation homogène

$$v^2w^2 = w^4 f\Big(\frac{u}{w}\Big).$$

Le point $J = [0, 1, 0] \in \widehat{\mathscr{D}}(K)$ est l'unique point à l'infini de $\mathscr{D}$. C'est un point singulier de $\widehat{\mathscr{D}}(K)$. La compactifiée lisse de $\mathscr{D}$ est une courbe de genre 1. Plus précisément, il résulte des hypothèses faites qu'il existe une courbe elliptique E/K et un isomorphisme birationnel $\psi : E \to \widehat{\mathscr{D}}$ défini sur K. La détermination d'équations explicites décrivant cette équivalence birationnelle est bien connue. On pourra à ce sujet consulter par exemple le chapitre II de [Si1]. On explicite dans cet appendice les équations que l'on utilisera dans le texte d'un tel couple (E, ψ). Elles s'obtiennent par des procédés standard utilisant le théorème de Riemann-Roch que l'on ne rappelera pas ici (cf. *loc. cit.*). On définit par ailleurs au paragraphe 3 une fonction sur E obtenue en composant la première fonction coordonnée sur $\mathscr{D}$ avec ψ. Au cours de la démonstration du théorème 2, on est confronté à l'étude de certaines propriétés de rationnalité de cette fonction. On démontre aux paragraphes 4 et 5 certains résultats que l'on utilisera concernant cette étude.

Quitte à effectuer une translation sur u, on peut supposer que l'on a $\alpha = 0$; on a alors $e = \beta^2$. On examinera dans la suite deux cas selon que β est nul ou non.

1. Le cas $\beta = 0$

Si β est nul, l'équation (1) s'écrit

$$v^2 = au^4 + bu^3 + cu^2 + du. \tag{2}$$

On dispose du point $P = (0, 0) \in \mathscr{D}(K)$. On a $d \neq 0$.

1.1. La courbe elliptique E/K

Soit E/K la cubique définie sur K par l'équation

$$y^2 = x^3 + c\ x^2 + bd\ x + ad^2. \tag{3}$$

Son discriminant est 16 fois celui de f, de sorte que E est une courbe elliptique sur K. Comme il est d'usage, on notera encore E la complétée projective de E d'équation

$$y^2 z = x^3 + c\ x^2 z + bd\ xz^2 + ad^2\ z^3.$$

On note $O = [0, 1, 0] \in E(K)$ le point à l'infini de E.

1.2. Les ouverts U et V

Soit γ une racine carré de ad^2 dans K_0. On considère les points de $E(K_0)$ suivants :

$$M_1 = (0, \gamma) \quad \text{et} \quad M_2 = (0, -\gamma). \tag{4}$$

On note U et V les ouverts de E et $\mathscr{D}$ respectivement, définis par :

$$U = E \backslash \{O, M_1, M_2\} \quad \text{et} \quad V = \mathscr{D} \backslash \{P\}. \tag{5}$$

1.3. L'isomorphisme de U sur V

On a l'énoncé suivant :

Proposition 1. *L'application $\psi : U \to \mathscr{D}$ définie pour tout point $M = (x, y) \in U$ par $\psi(M) = (u, v)$ où*

$$u = \frac{d}{x} \quad et \quad v = \frac{dy}{x^2}, \tag{6}$$

est un isomorphisme de U sur V.
L'application réciproque $\varphi : V \to U$ est définie pour tout point $N = (u, v) \in V$ par $\varphi(N) = (x, y)$ où

$$x = \frac{d}{u} \quad et \quad y = \frac{dv}{u^2}. \tag{7}$$

Démonstration : Les formules (6) et (7) sont bien définies sur les ouverts U et V respectivement. On vérifie ensuite directement les assertions annoncées.

1.4. Le morphisme $\psi : E \to \widehat{\mathscr{D}}$

Puisque E est lisse et que $\widehat{\mathscr{D}}$ est projective, l'application rationnelle ψ se prolonge en un unique morphisme, que l'on notera encore ψ, de E sur $\widehat{\mathscr{D}}$. Il est donné par l'énoncé suivant :

Lemme 1.

1) Pour tout point $M = [x, y, z] \in E\backslash\{O\}$ on a

$$\psi(M) = [dxz, dyz, x^2]. \tag{8}$$

En particulier, on a $\psi(M_1) = \psi(M_2) = J$.

2) On a $\psi(O) = P$.

Démonstration : En homogénéisant les formules (6), on obtient la formule (8) tout au moins si M est distinct de M_1 et M_2. Par ailleurs, la formule (8) définit un morphisme de $E\backslash\{O\}$ dans $\widehat{\mathscr{D}}$ qui se prolonge en un morphisme χ de E sur $\widehat{\mathscr{D}}$. Les morphismes ψ et χ coïncident sur l'ouvert $E\backslash\{O, M_1, M_2\}$, ils sont donc égaux ; d'où l'assertion 1. Puisque ψ est surjectif de E sur $\widehat{\mathscr{D}}$ et que P n'appartient pas à $\psi\Big(E\backslash\{O\}\Big)$, on a donc $\psi(O) = P$.

2. Le cas $\beta \neq 0$

Quitte à remplacer v par $\frac{v}{\beta}$ et f par $\frac{f}{\beta^2}$, on peut supposer que $\beta^2 = 1$. L'équation (1) s'écrit dans ce cas

$$v^2 = au^4 + bu^3 + cu^2 + du + 1, \tag{9}$$

et l'on dispose des points $P = (0, -1)$ et $Q = (0, 1)$ de $\mathscr{D}(K)$.

2.1. La courbe elliptique E/K

Soit E/K la cubique définie sur K par l'équation

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \tag{10}$$

où les coefficients a_2, a_4 et a_6 sont :

$$a_2 = c, \quad a_4 = bd - 4a \quad \text{et} \quad a_6 = ad^2 + b^2 - 4ac. \tag{11}$$

Son discriminant est 16 fois celui de f, c'est donc une courbe elliptique définie sur K. On note encore E la complétée projective de E et $O = [0, 1, 0] \in E(K)$.

2.2. Les ouverts U et V

On définit ici des ouverts U et V de E et $\widehat{\mathscr{D}}$ respectivement, analogues à ceux intervenant dans le paragraphe 1.2. Considérons une racine carrée γ de $4a$ dans K_0. Posons

$$\lambda = \frac{d^2}{4} - c. \tag{12}$$

Lemme 2. *Les points $(x, y) \in E(K_0)$ tels que $y - \frac{dx}{2} - b = 0$, sont*

$$M_1 = \left(\lambda, \frac{d\lambda}{2} + b\right), \quad M_2 = \left(\gamma, \frac{d\gamma}{2} + b\right) \quad et \quad M_3 = \left(-\gamma, -\frac{d\gamma}{2} + b\right).$$

Démonstration : L'équation (10) s'écrit aussi :

$$y^2 - \left(\frac{dx}{2} + b\right)^2 = (x - \lambda)(x^2 - 4a),$$

d'où le lemme.

On définit U comme étant l'ouvert de E formé des points à distance finie $(x, y) \in E(K_0)$ tels que $x - \lambda \neq 0$ et $y - \frac{dx}{2} - b \neq 0$. D'après le lemme 2, on a

$$U = E \backslash \Big\{O, -M_1, M_1, M_2, M_3\Big\}. \tag{13}$$

Posons

$$u_0 = \frac{2(\lambda d + 2b)}{\lambda^2 - 4a} \quad \text{et} \quad P' = \left(u_0, \frac{\lambda u_0^2}{2} - \frac{du_0}{2} - 1\right) \quad \text{si} \quad \lambda^2 \neq 4a, \tag{14}$$

$$P' = P \quad \text{si} \quad \lambda^2 = 4a. \tag{15}$$

On vérifie que P' appartient à $\mathscr{D}(K)$. L'ouvert V est alors défini par l'égalité

$$V = \mathscr{D} \backslash \Big\{P, P', Q\Big\}. \tag{16}$$

Remarque. On utilisera le fait que l'on a

$$\lambda^2 \neq 4a \quad \text{ou bien} \quad \lambda d + 2b \neq 0. \tag{17}$$

En effet, les égalités $\lambda^2 = 4a$ et $\lambda d + 2b = 0$ conduisent à une équation de $\mathscr{D}$ de la forme

$$v^2 = \left(\frac{\lambda u^2}{2} - \frac{du}{2} - 1\right)^2,$$

ce qui contredit la condition 2 du début.

2.3. L'isomorphisme de U sur V

Il est donné par l'énoncé suivant :

Proposition 2. *L'application $\psi : U \to \mathscr{D}$ définie pour tout point $M = (x, y) \in U$ par $\psi(M) = (u, v)$ où*

$$u = \frac{2(x-\lambda)}{y - \frac{dx}{2} - b}, \tag{18}$$

$$v = -1 + \frac{(x-\lambda)\big(2x^2 + 2cx + bd - dy\big)}{\big(y - \frac{dx}{2} - b\big)^2}, \tag{19}$$

est un isomorphisme de U sur V.
L'application réciproque $\varphi : V \to U$ est définie pour tout point $N = (u, v) \in V$ par $\varphi(N) = (x, y)$ où

$$x = \frac{2(v+1) + du}{u^2}, \tag{20}$$

$$y = \frac{(du+4)(v+1) + 2du + 2cu^2 + bu^3}{u^3}. \tag{21}$$

Démonstration : On remarque d'abord que les formules (18) et (19) sont bien définies sur $E \backslash \Big\{O, M_1, M_2, M_3\Big\}$. Soit M un point de U. On vérifie formellement que $\psi(M)$ appartient à $\mathscr{D}$; le fait que M soit distinct de $-M_1$ et M_1 entraîne l'inclusion $\psi(U) \subseteq V$.

Inversement, on observe que les formules (20) et (21) sont bien définies sur $\mathscr{D} \backslash \Big\{P, Q\Big\}$. Soit $N = (u, v)$ un point de V. On vérifie que $\varphi(N) \in E$. Démontrons que l'on a

$$\varphi(N) \neq \pm M_1. \tag{22}$$

Supposons le contraire. On a alors $x - \lambda = 0$, où x est donné par la formule (20). On a ainsi

$$v = -1 + \frac{u(\lambda u - d)}{2},$$

et en utilisant l'égalité (9), on obtient

$$u^3 \left((4a - \lambda^2)\frac{u}{4} + b + \frac{\lambda d}{2} \right) = 0.$$

On déduit alors de (17) que l'on a $N = P'$, d'où une contradiction et l'assertion (22). On constate de manière analogue que $\varphi(N)$ est distinct de M_2 et M_3, d'où $\varphi(V) \subseteq U$.

On constate enfin que les applications ψ et φ sont inverses l'une de l'autre.

2.4. Le morphisme $\boldsymbol{\psi : E \to \widehat{\mathscr{D}}}$

L'application $\psi : U \to V$ se prolonge en un morphisme que l'on note encore ψ de E sur $\widehat{\mathscr{D}}$. L'objectif de ce paragraphe est de l'expliciter.

Lemme 3. *Pour tout point $M = [x, y, z] \in E(K_0)$ distinct de O et M_1 on a l'égalité $\psi(M) = [u, v, w]$ où*

$$u = 2z\big(x - \lambda z\big)\bigg(y - \frac{dx}{2} - bz\bigg), \tag{23}$$

$$v = \big(x - \lambda z\big)\big(2x^2 + 2cxz + bdz^2 - dyz\big) - z\bigg(y - \frac{dx}{2} - bz\bigg)^2, \tag{24}$$

$$w = z\bigg(y - \frac{dx}{2} - bz\bigg)^2. \tag{25}$$

Démonstration : En homogénéisant les formules (18) et (19), on obtient les formules ci-dessus. Il s'agit alors de montrer que u, v et w ne s'annulent pas simultanément si M est distinct de O et M_1. Supposons pour cela que l'on ait $u = v = w = 0$ et $M \neq O$; on peut supposer $z = 1$. On a alors

$$y = \frac{dx}{2} + b \quad \text{et} \quad (x - \lambda)(2x^2 + 2cx + bd - dy) = 0. \tag{26}$$

On en déduit que $x = \lambda$ ou $x^2 = 4a$ (cf. la preuve du lemme 2). Si l'on a $x \neq \lambda$, il résulte de la deuxième égalité de (26) que $x = 0$, d'où $a = 0$, ce qui conduit à une contradiction. On obtient ainsi $x = \lambda$, $y = \frac{d\lambda}{2} + b$ i.e. $M = M_1$ et le résultat.

Déterminons $\psi(M_1)$. On considère pour cela l'ouvert W de E formé des points à distance finie $(x, y) \in E(K_0)$ tels que

$$x \neq \lambda \quad \text{et} \quad y + \frac{dx}{2} + b \neq 0. \tag{27}$$

On a

$$W = E\backslash\Big\{O, M_1, -M_1, -M_2, -M_3\Big\}. \tag{28}$$

Lemme 4. *Soit $M = (x, y)$ un point de W. On a $\psi(M) = [u', v', w']$ avec*

$$u' = 2(x^2 - 4a)\left(y + \frac{dx}{2} + b\right), \tag{29}$$

$$v' = 2x\left(y + \frac{dx}{2} + b\right)^2 - d(x^2 - 4a)\left(y + \frac{dx}{2} + b\right) - (x^2 - 4a)^2, \tag{30}$$

$$w' = (x^2 - 4a)^2. \tag{31}$$

Démonstration : On a l'égalité

$$\frac{y - \frac{dx}{2} - b}{x - \lambda} = \frac{x^2 - 4a}{y + \frac{dx}{2} + b}.$$

Par ailleurs, on vérifie que

$$2x^2 + 2cx + bd - dy = (x - \lambda)(4\lambda + 2c) + 2(x - \lambda)^2 - d\left(y - \frac{dx}{2} - b + \frac{d}{2}(x - \lambda\right).$$

D'après les formules (23), (24) et (25), on a donc

$$\frac{u}{(x - \lambda)^2} = 2\left(\frac{x^2 - 4a}{y + \frac{dx}{2} + b}\right),$$

$$\frac{v}{(x - \lambda)^2} = 2x - d\left(\frac{x^2 - 4a}{y + \frac{dx}{2} + b}\right) - \left(\frac{x^2 - 4a}{y + \frac{dx}{2} + b}\right)^2,$$

$$\frac{w}{(x - \lambda)^2} = \left(\frac{x^2 - 4a}{y + \frac{dx}{2} + b}\right)^2.$$

On en déduit que $\psi(M) = [u', v', w']$.

Corollaire 1. *On a*

$$\psi(M_1) = \begin{cases} P' & si \quad \lambda^2 \neq 4a \\ J & si \quad \lambda^2 = 4a. \end{cases} \tag{32}$$

Démonstration : Les formules (29), (30) et (31) définissent un morphisme $\chi : E \to \widehat{\mathscr{D}}$ qui coïncide avec ψ sur un ouvert non vide de E. Il en résulte que χ et ψ sont égaux sur E. Par ailleurs, compte tenu de (17), on constate que χ est défini au point M_1. On a donc $\psi(M_1) = \chi(M_1)$, d'où le corollaire.

Corollaire 2. *On a*

$$\psi(M_2) = \psi(M_3) = J. \tag{33}$$

Démonstration : Si $\lambda^2 \neq 4a$, le point M_1 est distinct de M_2 et M_3. Les formules (23), (24) et (25) impliquent alors (33). Supposons $\lambda^2 = 4a$ et par exemple $\lambda = \gamma$. Dans ce cas, on a $M_1 = M_2$, d'où $\psi(M_2) = J$. Par ailleurs, puisque γ est non nul (car $a \neq 0$), M_3 est distinct de $\pm M_1$ et de $-M_2$, $-M_3$. Le lemme 4 entraîne alors le résultat.

Corollaire 3. *On a*

$$\psi(-M_1) = P. \tag{34}$$

Démonstration : Si $M_1 \neq -M_1$, les formules (23), (24) et (25) impliquent (34). Supposons $M_1 = -M_1$, autrement dit que

$$\frac{d\lambda}{2} + b = 0.$$

D'après (17), on a $\lambda^2 \neq 4a$ et l'on a $\psi(M_1) = P'$ (cor. 1). D'après (14), on a $u_0 = 0$ puis $P' = P$, d'où le résultat.

Lemme 5. *On a*

$$\psi(O) = Q. \tag{35}$$

Démonstration : En considérant l'équation projective de E, on vérifie que pour tout point $M = [x, y, z]$ dans un ouvert de $E(K_0)$ qui contient O, on a $\psi(M) = [u, v, w]$ avec

$$u = 2\big(x - \lambda z\big)\left(y - \frac{dx}{2} - bz\right),$$

$$v = 2(y^2 - a_2x^2 - a_4xz - a_6z^2) - 2\lambda x^2 + \big(x - \lambda z\big)\big(2cx + bdz - dy\big) - \left(y - \frac{dx}{2} - bz\right)^2,$$

$$w = \left(y - \frac{dx}{2} - bz\right)^2.$$

On en déduit l'égalité (35).

Cela termine la détermination de ψ.

On utilisera l'énoncé suivant :

Lemme 6. *L'application ψ induit une surjection de $E(K)\backslash\big\{O, -M_1\big\}$ sur $\mathscr{D}(K)\backslash\big\{P, Q\big\}$.*

Démonstration : Considérons un point $R \in \mathscr{D}(K)\backslash\big\{P, Q\big\}$. Si R est distinct de P', alors R est dans l'ouvert V, et il existe $M \in E(K) \cap U$ tel que $\psi(M) = R$. Supposons que

l'on ait $R = P'$. On a alors $P \neq P'$. Cela entraîne que $M_1 \neq -M_1$; en effet, si $M_1 = -M_1$, on a $d\lambda + 2b = 0$ et d'après (17), cela implique $\lambda^2 \neq 4a$. La formule (14) conduit alors à $P = P'$, d'où une contradiction et notre assertion. Par ailleurs, on a $\psi(M_1) = P'$ (cor. 1) d'où $\psi(M_1) = R$ et le résultat.

3. La fonction u sur E

En composant la première fonction coordonnée sur $\mathscr{D}$ avec le morphisme ψ, on obtient une fonction sur E, que l'on notera u, i.e. un morphisme $u : E \to \mathbb{P}^1$ que l'on va expliciter. Considérons pour cela un point $M \in E(K_0)$. En utilisant les propositions 1 et 2, le lemme 1 et les résultats ci-dessus, on constate que l'on a les formules suivantes :

1) si $\beta = 0$:

$$u(M) = \frac{d}{x} \quad \text{si} \quad M = (x, y) \in U,$$

$$u(M_1) = u(M_2) = \infty \quad \text{et} \quad u(O) = 0.$$

2) si $\beta \neq 0$:

$$u(M) = \frac{2(x - \lambda)}{y - \frac{dx}{2} - b} \quad \text{si} \quad M = (x, y) \in U,$$

$$u(O) = u(-M_1) = 0 \quad \text{et} \quad u(M_2) = u(M_3) = \infty,$$

$$u(M_1) = \begin{cases} \frac{2(\lambda d + 2b)}{\lambda^2 - 4a} & \text{si } \lambda^2 \neq 4a \\ \infty & \text{sinon.} \end{cases}$$

4. L'involution hyperelliptique

La courbe $\widehat{\mathscr{D}}$ possède un automorphisme d'ordre 2, à savoir l'involution hyperelliptique $i : \widehat{\mathscr{D}} \to \widehat{\mathscr{D}}$ qui est définie pour tout point $(u, v) \in \widehat{\mathscr{D}}(K_0)$ par

$$i\big((u, v)\big) = (u, -v) \quad \text{et} \quad i(J) = J.$$

On en déduit l'existence d'un unique automorphisme I d'ordre 2 de E tel que l'on ait

$$\psi \circ I = i \circ \psi. \tag{36}$$

On se propose ici de décrire I.

4.1. Cas où $\beta = 0$

Lemme 7. *Pour tout $M \in E(K_0)$, on a $I(M) = -M$.*

Démonstration : Soit $M = (x, y)$ un point de U. Il suffit de démontrer que l'on a

$$\psi(-M) = i \circ \psi(M).$$

Il existe un point $(u, v) \in V$ tel que l'on ait $x = \frac{d}{u}$ et $y = \frac{dv}{u^2}$. Par définition, on a

$$I(M) = \Big(\frac{d}{u}, -\frac{dv}{u^2}\Big),$$

d'où le lemme.

4.2. Cas où $\beta \neq 0$

Lemme 8. *Pour tout $M \in E(K_0)$, on a $I(M) = -M_1 - M$.*

Démonstration : Soit $M = (x, y)$ un point de U. Vérifions que l'on a

$$\psi(-M_1 - M) = i \circ \psi(M).$$

Il existe un point $(u, v) \in V$ tel que l'on ait $x = x(u, v)$ et $y = y(u, v)$, où $x(u, v)$ et $y(u, v)$ sont donnés par les formules (20) et (21). Par définition, on a

$$I(M) = \big(x(u, -v), y(u, -v)\big).$$

Notons (x_1, y_1) les coordonnées de M_1. On vérifie que le déterminant de la matrice

$$\begin{pmatrix} x(u,v) & x(u,-v) & x_1 \\ y(u,v) & y(u,-v) & y_1 \\ 1 & 1 & 1 \end{pmatrix}$$

est nul, ce qui signifie que les points M, M_1 et $I(M)$ sont alignés, autrement dit, qu'ils sont de somme nulle. D'où le résultat.

Dans les deux cas, que β soit nul ou non, on a l'énoncé suivant :

Lemme 9. *Pour tout $M \in E(K_0)$, on a $u(M) = u\big(I(M)\big)$.*

Démonstration : Cela résulte des définitions de u et i ainsi que de l'égalité (36).

5. Une condition de rationnalité

On suppose dans ce paragraphe que K est un corps de nombres et que $K_0 = \mathbb{C}$. On est confronté dans ce chapitre au problème de la détermination des points de $M \in E(K)$

tels que $u(M)$ appartienne à $\mathbb{Q}$. Notre objectif est ici de démontrer un résultat que l'on utilise pour la résolution de ce problème.

Soit A l'anneau des entiers de K. On suppose que la condition suivante est réalisée :

(37) $\qquad a,\ b,\ c\ \text{ et } d\ \text{ appartiennent à } A.$

Soit $\mathfrak{p}$ un idéal premier de A, de caractéristique résiduelle $p \geqslant 3$, en lequel E/K a bonne réduction. On note :

. $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$, $A_\mathfrak{p}$ son anneau de valuation et $\mathfrak{M}_\mathfrak{p}$ l'idéal maximal de $A_\mathfrak{p}$;

. $k = A_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}$ le corps résiduel. C'est une extension finie de $\mathbb{F}_p$;

. $\nu : A_\mathfrak{p} \to k$ la surjection canonique ;

. $\widetilde{E}$ la courbe elliptique sur k déduite de E par réduction ;

. $\pi : E(K_\mathfrak{p}) \to \widetilde{E}(k)$ le morphisme de réduction ;

. $E_1(K_\mathfrak{p})$ le noyau de π et $E_1(K)$ son intersection avec $E(K)$. Rappelons que les points à distance finie $(x, y) \in E(K_\mathfrak{p})$ qui n'appartiennent pas à $E_1(K_\mathfrak{p})$ sont caractérisés par le fait que x et y sont dans $A_\mathfrak{p}$ (cf. par exemple [Si1], chapitre VII).

Considérons alors deux points N et S de $E(K)$ vérifiant les conditions suivantes :

(i) N n'appartient pas à $E_1(K)$;

(ii) $N - S$ est dans $E_1(K)$;

(iii) $u(N)$ est dans $\mathbb{Q}$.

On a $S \neq O$; posons $S = (x_S, y_S)$. Voici le résultat que l'on a en vue :

Lemme 10.

1) Si $\beta = 0$, la condition suivante est satisfaite :

$$x_S \in \mathfrak{M}_\mathfrak{p} \quad \textit{ou bien} \quad \nu\Big(\frac{d}{x_S}\Big) \in \mathbb{F}_p.$$

2) Si $\beta \neq 0$, la condition suivante est satisfaite :

$$y_S - \frac{dx_S}{2} - b \in \mathfrak{M}_\mathfrak{p} \quad \textit{ou bien} \quad \nu\left(\frac{2(x_S - \lambda)}{y_S - \frac{d\ x_S}{2} - b}\right) \in \mathbb{F}_p.$$

Démonstration : Posons $N = (x, y)$. Remarquons d'abord que d'après (37) et le fait que N et S ne soient pas dans $E_1(K)$, les éléments

$$x_S,\ y_S,\ x,\ y,\ y_S - \frac{dx_S}{2} - b \quad \text{et} \quad x_S - \lambda,$$

sont dans $A_{\mathfrak{p}}$. Par ailleurs, on a $\pi(N) = \pi(S)$. On a donc les égalités

$$\nu(x) = \nu(x_S) \quad \text{et} \quad \nu(y) = \nu(y_S). \tag{38}$$

1) Supposons $\beta = 0$. Il résulte des hypothèses faites que N appartient à l'ouvert U. Par suite, on a $u(N) = \frac{d}{x}$ (formule (6)). Supposons que x_S ne soit pas dans $\mathfrak{M}_{\mathfrak{p}}$ i.e. que $\nu(x_S) \neq 0$. D'après (38), on a $\nu(x) \neq 0$ et

$$\nu\Big(\frac{d}{x}\Big) = \nu\Big(\frac{d}{x_S}\Big).$$

Puisque $u(N)$ est dans $\mathbb{Q} \cap A_{\mathfrak{p}}$, on a $\nu\Big(\frac{d}{x}\Big) \in \mathbb{F}_p$, d'où notre assertion.

2) Supposons $\beta \neq 0$.

2.1) Supposons que N soit dans U. Dans ce cas, $u(N)$ est donné par la formule (18). Si l'on a

$$y_S - \frac{dx_S}{2} - b \notin \mathfrak{M}_{\mathfrak{p}},$$

alors, d'après (38), $y - \frac{dx}{2} - b$ n'est pas non plus dans $\mathfrak{M}_{\mathfrak{p}}$. Le fait que $u(N)$ soit dans $\mathbb{Q} \cap A_{\mathfrak{p}}$ entraîne, comme ci-dessus, le résultat.

2.2) Si N n'est pas dans U, on a $N \in \big\{-M_1, M_1, M_2, M_3\big\}$. Puisque $u(M_2)$ et $u(M_3)$ ne sont pas dans $\mathbb{Q}$, on a en fait $N = \pm M_1$. Si $N = M_1$, on a $y = \frac{dx}{2} + b$, et d'après (38), $y_S - \frac{dx_S}{2} - b$ est dans $\mathfrak{M}_{\mathfrak{p}}$. Si $N = -M_1$, on a $x = \lambda$ d'où $\nu(x_S - \lambda) = 0$, ce qui entraîne de nouveau le résultat. D'où le lemme.

Appendice 2. Méthode de Chabauty elliptique

Soient K un corps de nombres contenu dans $\mathbb{C}$ et A l'anneau d'entiers de K. On considère des éléments a, b, c et d de A et $\mathscr{D}/K$ la quartique affine d'équation

$$v^2 = au^4 + bu^3 + cu^2 + du + e \quad \text{avec} \quad e = 0 \text{ ou } e = 1. \tag{1}$$

Comme dans l'appendice 1, on suppose que a est non nul et que $\mathscr{D}$ est lisse. Les points $(0, e)$ et $(0, -e)$ appartiennent à $\mathscr{D}(K)$. Dans la démonstration du théorème 2 de ce chapitre, on est confronté au problème suivant :

Problème. *Comment déterminer tous les points $(u, v) \in \mathscr{D}(K)$ tels que $u \in \mathbb{Q}$?*

Ce problème est facile si $\mathscr{D}(K)$ est fini. Dans le cas où $\mathscr{D}(K)$ est infini, on utilise la méthode dite de Chabauty elliptique, qui permet parfois la détermination complète de ces points. Cette méthode a déjà été présentée dans de nombreux travaux. On pourra à ce sujet consulter par exemple [Fl], [Bru1], [Fl-We] et [Du]. L'objectif de cet appendice est d'exposer la démarche que l'on suivra dans son utilisation.

1. Reformulation du problème

D'après l'étude faite dans l'appendice 1, la quartique $\mathscr{D}$ est birationnellement équivalente à la courbe elliptique E/K d'équation de Weierstrass

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

à coefficients dans A, qui est définie par les formules (3) et (11) de *loc. cit.*, suivant que e soit 0 ou 1. Afin de résoudre notre problème, on est ainsi amené à déterminer les points $N \in E(K)$ tels que

$$u(N) \in \mathbb{Q},$$

où $u : E \to \mathbb{P}^1$ est la fonction sur E définie dans le paragraphe 3 de l'appendice 1. Rappelons que sur des ouverts de E convenables, si $N = (x, y)$ est un point de $E(K)$ à distance finie, on a

$$u(N) = \frac{d}{x} \quad \text{si} \quad e = 0 \quad \text{et} \quad u(N) = \frac{2(x - \lambda)}{y - \frac{dx}{2} - b} \quad \text{avec} \quad \lambda = \frac{d^2}{4} - c \quad \text{si} \quad e = 1. \tag{3}$$

La détermination des points $N \in E(K)$ tels que $u(N) \in \mathbb{Q}$ est simple si le rang r de $E(K)$ est nul, car dans ce cas il est facile d'expliciter $E(K)$ et donc aussi $\mathscr{D}(K)$. Si l'on a $r \geqslant 1$, on utilise des arguments de nature locale que l'on a va présenter maintenant.

2. Groupe formel associé à E

Pour tout ce qui concerne ce paragraphe, on pourra par exemple consulter le chapitre IV de [Si1] ainsi que [Fl-We].

Soient p un nombre premier impair et $\mathfrak{p}$ un idéal premier de A au-dessus de p. On suppose que les deux conditions suivantes sont satisfaites :

1. l'idéal $\mathfrak{p}$ est non ramifié ;
2. la courbe elliptique E/K a bonne réduction en $\mathfrak{p}$.

Soient $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$, $A_\mathfrak{p}$ son anneau de valuation, $\mathfrak{M}_\mathfrak{p}$ l'idéal maximal de $A_\mathfrak{p}$. On pose $k = A_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}$; c'est une extension finie de $\mathbb{F}_p$. Notons v la valuation $\mathfrak{p}$-adique de $K_\mathfrak{p}$ normalisée par $v(K_\mathfrak{p}^*) = \mathbb{Z}$: on a $v(p) = 1$. Une clôture algébrique $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$ étant choisie, on identifie $K_\mathfrak{p}$ avec l'extension finie non ramifiée de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}_p}$ dont le degré sur $\mathbb{Q}_p$ est celui de k sur $\mathbb{F}_p$. On identifie par ailleurs K à un sous-corps de $K_\mathfrak{p}$.

2.1. Développements formels

Le changement de variables

$$z = -\frac{x}{y} \quad \text{et} \quad w = -\frac{1}{y}, \tag{4}$$

conduit au nouveau modèle de E :

$$w = z^3 + a_2 z^2 w + a_4 z w^2 + a_6 w^3. \tag{5}$$

Dans l'anneau des séries formelles $A[[z]]$, il existe une unique série formelle w vérifiant l'égalité (5). On a

$$w = z^3 + a_2 z^5 + (a_2^2 + a_4) z^7 + (a_2^3 + 3a_2 a_4 + a_6) z^9 + O\big(z^{11}\big). \tag{6}$$

En posant

$$x = \frac{z}{w} \quad \text{et} \quad y = -\frac{1}{w},$$

on obtient dans le modèle (2) x et y comme série de Laurent de z à coefficients dans A,

$$x = \frac{1}{z^2} - a_2 - a_4 z^2 - (a_2 a_4 + a_6) z^4 + O\big(z^6\big), \tag{7}$$

$$y = -\frac{1}{z^3} + \frac{a_2}{z} + a_4 z + (a_2 a_4 + a_6) z^3 + \big(a_2^2 a_4 + 2a_2 a_6 + a_4^2\big) z^5 + O\big(z^7\big). \tag{8}$$

Le couple (x, y) est alors un point de E rationnel sur le corps $K((z))$. Soit $S = (x_S, y_S)$ un point de $E\big(K_\mathfrak{p}\big)$ vérifiant l'équation (2) tel que x_S et y_S soient dans $A_\mathfrak{p}$. On peut considérer le nouveau point de E rationnel sur $K_\mathfrak{p}((z))$:

$$M = S + (x, y).$$

En posant $M = (x_M, y_M)$, la formule d'addition sur E conduit à des développements en série de x_M et y_M en fonction de z à coefficients dans $A_{\mathfrak{p}}$,

$$x_M = x_S + 2y_S z + (3x_S^2 + 2a_2 x_S + a_4)z^2 + O(z^3), \tag{9}$$

$$y_M = y_S + (3x_S^2 + 2a_2 x_S + a_4)z + 2y_S(3x_S + a_2)z^2 + O(z^3). \tag{10}$$

2.2. Loi de groupe formelle

On dispose d'une loi de groupe formelle $\mathfrak{F}$ associée au modèle (2) de E sur $K_{\mathfrak{p}}$. C'est une série formelle en deux indéterminées z_1, z_2 à coefficients dans A et l'on a

$$\mathfrak{F}(z_1, z_2) = z_1 + z_2 - a_2 z_1 z_2 (z_1 + z_2) + \text{ des termes de degré } \geqslant 5. \tag{11}$$

On notera log et exp le logarithme et l'exponentielle associés à $\mathfrak{F}$. Ce sont deux séries formelles de $K_{\mathfrak{p}}[[z]]$ réciproques l'une de l'autre, que l'on peut écrire sous la forme

$$\log = \sum_{n \geqslant 1} \frac{\alpha_n}{n}\, z^n \quad \text{et} \quad \exp = \sum_{n \geqslant 1} \frac{\beta_n}{n!}\, z^n,$$

où les α_n, β_n appartiennent à A. On a

$$\log = z + \frac{a_2}{3} z^3 + \frac{a_2^2 + 2a_4}{5} z^5 + O(z^7), \tag{12}$$

$$\exp = z - \frac{a_2}{3} z^3 + \frac{2a_2^2 - 6a_4}{15} z^5 + O(z^7). \tag{13}$$

2.3. Groupe formel associé à $E/K_{\mathfrak{p}}$

En prenant pour z_1 et z_2 des élément de $\mathfrak{M}_{\mathfrak{p}}$, la série (11) est convergente à valeurs dans $\mathfrak{M}_{\mathfrak{p}}$. Le groupe formel associé à $E/K_{\mathfrak{p}}$ est le groupe, parfois noté $\mathfrak{F}\big(\mathfrak{M}_{\mathfrak{p}}\big)$, ayant pour ensemble sous-jacent $\mathfrak{M}_{\mathfrak{p}}$ et dont la loi interne $\oplus$ est définie pour tout $z_1, z_2 \in \mathfrak{M}_{\mathfrak{p}}$ par

$$z_1 \oplus z_2 = \mathfrak{F}(z_1, z_2). \tag{14}$$

De même, si z est un élément non nul de $\mathfrak{M}_{\mathfrak{p}}$, les séries (7) et (8) sont convergentes dans $K_{\mathfrak{p}}$. On obtient ainsi une application

$$\varphi : \mathfrak{M}_{\mathfrak{p}} \to E\big(K_{\mathfrak{p}}\big),$$

définie pour tout z non nul dans $\mathfrak{M}_\mathfrak{p}$ par

$$\varphi(z) = \big(x(z), y(z)\big), \tag{15}$$

où $x(z)$ et $y(z)$ sont les éléments de $K_\mathfrak{p}$ définis par les égalités (7) et (8).

Soit $\widetilde{E}$ la courbe déduite de E par réduction. D'après la condition 2, $\widetilde{E}$ est une courbe elliptique définie sur k. Soient

$$\pi : E\big(K_\mathfrak{p}\big) \to \widetilde{E}(k),$$

le morphisme de réduction et $E_1\big(K_\mathfrak{p}\big)$ son noyau. L'application φ réalise un isomorphisme de groupes

$$\varphi : \mathfrak{F}\big(\mathfrak{M}_\mathfrak{p}\big) \simeq E_1\big(K_\mathfrak{p}\big),$$

de $\mathfrak{F}\big(\mathfrak{M}_\mathfrak{p}\big)$ sur $E_1\big(K_\mathfrak{p}\big)$. L'application réciproque

$$\varphi^{-1} : E_1\big(K_\mathfrak{p}\big) \simeq \mathfrak{F}\big(\mathfrak{M}_\mathfrak{p}\big)$$

associe à tout point à distance finie $P = (x, y) \in E_1\big(K_\mathfrak{p}\big)$ l'élément

$$z(P) = -\frac{x}{y} \in \mathfrak{M}_\mathfrak{p}. \tag{16}$$

On dira que $z(P)$ est la z-coordonnée de P. Si P, P' sont dans $E_1\big(K_\mathfrak{p}\big)$, on a donc (cf. (14))

$$z\big(P + P'\big) = \mathfrak{F}\big(z(P), z(P')\big). \tag{17}$$

D'après la condition 1 et l'inégalité $p \geqslant 3$, pour tout $z \in \mathfrak{M}_\mathfrak{p}$, les séries log et exp sont convergentes dans $\mathfrak{M}_\mathfrak{p}$. On notera $\log(z)$ et $\exp(z)$ leurs sommes. Le logarithme induit un isomorphisme de groupes de $\mathfrak{F}\big(\mathfrak{M}_\mathfrak{p}\big)$ sur $\mathfrak{M}_\mathfrak{p}$ et l'isomorphisme réciproque est donné par l'exponentielle. Pour tout $z \in \mathfrak{M}_\mathfrak{p}$, on a les congruences

$$\log(z) \equiv z \equiv \exp(z) \text{ mod. } p^{1+v(z)}. \tag{18}$$

En effet, il suffit de prouver que si n est un entier $\geqslant 2$, on a

$$v\left(\frac{z^n}{n!}\right) \geqslant v(z) + 1,$$

ce qui résulte de l'inégalité

$$v(n!) \leqslant \frac{n-1}{2}.$$

Par ailleurs, pour tout point $P \in E_1\big(K_\mathfrak{p}\big)$ et tout entier $n \in \mathbb{Z}$, on a

$$z\big(nP\big) = \exp\Big(n \log\big(z(P)\big)\Big). \tag{19}$$

Étant donnés un entier $k \geqslant 1$, des points $P_1, \cdots, P_k \in E_1\big(K_\mathfrak{p}\big)$ et des entiers $n_1, \cdots, n_k$, on en déduit l'égalité

$$z\Big(\sum_{i=1}^{k} n_i P_i\Big) = \exp\Big(\sum_{i=1}^{k} n_i \log\big(z(P_i)\big)\Big). \tag{20}$$

2.4. Le $\mathbb{Z}_p$-module $E_1\big(K_\mathfrak{p}\big)$

L'application $z \mapsto \log(z)$ réalise un isomorphisme de groupes de $\mathfrak{F}\big(\mathfrak{M}_\mathfrak{p}\big)$ sur $\mathfrak{M}_\mathfrak{p}$. On en déduit que $\mathfrak{F}\big(\mathfrak{M}_\mathfrak{p}\big)$ est muni d'une structure de $\mathbb{Z}_p$-module telle que cette application soit un morphisme de $\mathbb{Z}_p$-modules : elle est donnée par la formule

$$n.z = \exp\big(n \log(z)\big) \quad \text{pour} \quad n \in \mathbb{Z}_p \text{ et } z \in \mathfrak{F}\big(\mathfrak{M}_\mathfrak{p}\big).$$

Par ailleurs, les groupes $\mathfrak{F}\big(\mathfrak{M}_\mathfrak{p}\big)$ et $E_1\big(K_\mathfrak{p}\big)$ sont isomorphes via l'application φ. Il en résulte l'existence d'une structure de $\mathbb{Z}_p$-module sur $E_1(K_\mathfrak{p})$ telle que l'on ait

$$n.z(P) = z(nP) \quad \text{pour} \quad n \in \mathbb{Z}_p \text{ et } P \in E_1(K_\mathfrak{p}).$$

On a ainsi l'égalité

$$z(nP) = \exp\Big(n \log\big(z(P)\big)\Big) \quad \text{pour} \quad n \in \mathbb{Z}_p \text{ et } P \in E_1(K_\mathfrak{p}), \tag{21}$$

et la formule (20) est alors valable en prenant pour les n_i des éléments de $\mathbb{Z}_p$.

2.5. La projection $\eta : K_\mathfrak{p}^* \to k^*$

Soit $\eta : K_\mathfrak{p}^* \to k^*$ l'application de $K_\mathfrak{p}^*$ dans k^* définie par

$$\eta(x) = \frac{x}{p^{v(x)}} \text{ mod. } \mathfrak{M}_\mathfrak{p}. \tag{22}$$

C'est un homomorphisme de groupes surjectif de $K_\mathfrak{p}^*$ sur k^*. L'objectif de ce paragraphe est de préciser quelques propriétés de η que l'on utilise dans le chapitre IV.

Soient x et x' deux éléments de $K_\mathfrak{p}^*$. On pose

$$y = x + x', \quad \frac{x}{p^{v(x)}} = u, \quad \frac{x'}{p^{v(x')}} = u'.$$

1) Si $v(x) < v(x')$, on a $\eta(y) = \eta(x)$.

En effet, on a l'égalité

$$y = up^{v(x)}\Big(1 + p^{v(x')-v(x)}\frac{u'}{u}\Big),$$

On a $\eta\Big(1+p^{v(x')-v(x)}\,\frac{u'}{u}\Big)=1$, d'où l'assertion.

2) Supposons $\eta(x)+\eta(x')\neq 0$. Vérifions que l'on a

$$y\neq 0 \quad \text{et} \quad \eta(y)\in\Big\{\eta(x),\eta(x'),\eta(x)+\eta(x')\Big\}. \tag{23}$$

On a $y\neq 0$, sinon $\eta(x)=\eta(-x')=-\eta(x')$, ce qui n'est pas. Par ailleurs, on peut supposer d'après l'alinéa 1) que $v(x)=v(x')$. On a alors $v(y)=v(x)$. En effet, l'inégalité $v(y)>v(x)$ conduit à

$$\eta(x)+\eta(x')=\frac{y}{p^{v(x)}} \text{ mod. } \mathfrak{M}_{\mathfrak{p}}=0.$$

On obtient ainsi $\eta(y)=\eta(x)+\eta(x')$. D'où la condition (23).

3) Supposons que x soit dans $\mathbb{Q}_p^*$. Vérifions que $\eta(x)$ appartient à $\mathbb{F}_p^*$. Il existe un entier a compris entre 1 et $p-1$ et $b\in\mathfrak{M}_p$ tels que

$$u=a+b.$$

On a $\eta(u)=\eta(x)$ et d'après 1), $\eta(u)=\eta(a)\in\mathbb{F}_p^*$, d'où l'assertion.

4) Soit z un élément non nul de $\mathfrak{M}_{\mathfrak{p}}$. On a

$$\eta\big(\log(z)\big)=\eta(z)=\eta\big(\exp(z)\big). \tag{24}$$

Ces égalités résultent de 1) et des congruences (18).

5) Soient $P\in E_1(K_{\mathfrak{p}})$ et $m\in\mathbb{Z}_p$ tels que mP soit non nul. On a

$$\eta\big(z(mP)\big)=\eta(m)\eta\big(z(P)\big). \tag{25}$$

D'après (21) et (24), on a

$$\eta\big(z(mP)\big)=\eta\Big(\exp\Big(m\log\big(z(P)\big)\Big)\Big)=\eta\Big(m\log\big(z(P)\big)\Big),$$

d'où

$$\eta\big(z(mP)\big)=\eta(m)\eta\Big(\log\big(z(P)\big)\Big)=\eta(m)\eta\big(z(P)\big),$$

puis l'égalité (25).

3. Méthode de Chabauty elliptique

Cette méthode consiste, dans sa généralité, à majorer le nombre de points (u,v) de $\mathscr{D}(K)$ tel que u soit dans $\mathbb{Q}$. Les points $(0,e)$ et $(0,-e)$ de $\mathscr{D}(K)$ réalisent cette condition. En pratique, on dispose parfois d'autres points «évidents» $(u,v)\in\mathscr{D}(K)$ tels que u soit dans $\mathbb{Q}$. Si le majorant obtenu coïncide avec le nombre de points déjà connus sur $\mathscr{D}(K)$

possédant cette propriété, le problème du début est alors résolu. On va décrire ici cette méthode et présenter les étapes que l'on suivra dans la démonstration du théorème 2.

Première étape

Le groupe $E(K)$ est de type fini. La première étape consiste à déterminer :

1. le sous-groupe de torsion de $E(K)$;
2. le rang r de $E(K)$;
3. un système de r points $(N_1, \cdots, N_r)$ de $E(K)$ qui sont $\mathbb{Z}$-linéairement indépendants.

Cette étape est en général difficile à réaliser. Il existe néanmoins des algorithmes, implantés par D. Simon sur le logiciel de calculs PARI, qui permettent parfois cette détermination (cf. [Sim]). Il est important de noter que, tout au moins pour les applications que l'on a en vue, il est inutile de se préoccuper de savoir si le système $(N_1, \cdots, N_r)$ forme ou non une base de $E(K)$ modulo son sous-groupe de torsion. Par ailleurs, dans les situations rencontrées dans ce chapitre, on a toujours $r \leqslant 2$. Cela étant, la suite de ce paragraphe est valable pour r quelconque.

Deuxième étape

On suppose qu'il existe un nombre premier $p \geqslant 3$ tel que :

4. p ne divise pas le discriminant de K ;
5. il existe un idéal premier $\mathfrak{p}$ de A au-dessus de p dont le degré résiduel f sur p vérifie l'inégalité

$$r \leqslant f - 1. \tag{26}$$

6. La courbe elliptique E/K a bonne réduction en $\mathfrak{p}$.

Soit $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$, $A_\mathfrak{p}$ son anneau de valuation et k le corps résiduel. On conserve les identifications faites au début du paragraphe 2. Soient $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$ et ξ un élément de $\overline{\mathbb{F}_p}$ tel que $k = \mathbb{F}_p(\xi)$. Si $\tau \in A_\mathfrak{p}$ est un relèvement de ξ, on a

$$K_\mathfrak{p} = \mathbb{Q}_p(\tau) \quad \text{et} \quad A_\mathfrak{p} = \mathbb{Z}_p[\tau]. \tag{27}$$

L'anneau $A_\mathfrak{p}$ est un $\mathbb{Z}_p$-module libre de base $\big(1, \tau, \cdots, \tau^{f-1}\big)$.

La courbe elliptique E a bonne réduction sur $K_\mathfrak{p}$. Soient $\widetilde{E}$ la courbe elliptique sur k déduite de E par réduction et

$$\pi : E\big(K_\mathfrak{p}\big) \to \widetilde{E}(k)$$

le morphisme de réduction. Soit $E_1(K)$ l'intersection du noyau de π avec $E(K)$. L'objectif de cette étape est alors d'expliciter un système de représentants de $E(K)/E_1(K)$ qui

contient O. Il est facile d'obtenir un tel système de représentants pour peu que l'on sache démontrer, si tel est le cas, que $\Big\{N_1, \cdots, N_r\Big\}$ est une base de $E(K)$ modulo son sous-groupe de torsion. On procède ici autrement : on considère le sous-groupe G de $E(K)$ engendré par son sous-groupe de torsion et $\Big\{N_1, \cdots, N_r\Big\}$. Notons h l'indice de G dans $E(K)$ et supposons que la condition suivante soit satisfaite :

7. h est premier avec l'ordre de $\widetilde{E}(k)$.

Cette condition est souvent réalisée en pratique, et est toujours vérifiée dans les applications que l'on a en vue. Elle implique le résultat suivant :

Lemme 1. *On a* $\pi(G) = \pi\big(E(K)\big)$.

Démonstration : L'application π induit un morphisme de groupes surjectif de $E(K)/G$ sur $\pi\big(E(K)\big)/\pi(G)$. En particulier, l'indice de $\pi(G)$ dans $\pi\big(E(K)\big)$ divise h. Par ailleurs, $\pi\big(E(K)\big)$ étant un sous-groupe de $\widetilde{E}(k)$, l'indice de $\pi(G)$ dans $\pi\big(E(K)\big)$ divise aussi l'ordre de $\widetilde{E}(k)$. La condition 7 entraîne alors le résultat.

Pour tout i entre 1 et r, notons ensuite m_i l'ordre de $\pi(N_i)$ et posons

$$Q_i = m_i N_i. \tag{28}$$

Les points Q_i appartiennent à $E_1(K)$. Soit $\mathfrak{S}$ le sous-ensemble de $E(K)$ formé des points qui s'écrivent sous la forme

$$T + \sum_{i=1}^{r} k_i N_i,$$

où T est un point de torsion de $E(K)$ et où les k_i sont des entiers tels que

$$\Big[\frac{-m_i}{2}\Big] + 1 \leqslant k_i \leqslant \Big[\frac{m_i}{2}\Big].$$

Il résulte alors du lemme 1 que tout point N de $E(K)$ s'écrit sous la forme :

$$N = S + P \quad \text{où} \quad S \in \mathfrak{S} \text{ et } P \in E_1(K). \tag{29}$$

Cette condition permet alors d'expliciter un système de représentants comme souhaité. Dans certaines situations favorables, on constate qu'il existe un sous-ensemble $\mathfrak{S}'$ de $E(K)$ tel que π induise une bijection de $\mathfrak{S}'$ sur $\widetilde{E}(k)$; on obtient alors directement un tel système de représentants et l'on évite ainsi de vérifier la condition 7.

Signalons que dans les situations rencontrées au cours de la démonstration du théorème 2, on considère toujours le nombre premier $p = 3$.

Troisième étape

Comme on le signalait au paragraphe 1, on est amené pour résoudre notre problème à déterminer les points $N \in E(K)$ tels que $u(N)$ soit dans $\mathbb{Q}$. On connait en pratique un

certain ensemble $\mathcal{P}$ formé de points «évidents» de $E(K)$ ayant cette propriété qui sont en fait implicitement liés à la situation considérée. Notre objectif est de démontrer, si tel est le cas, qu'il n'y en a pas d'autres.

Considérons pour cela un point $N \in E(K)$ qui n'appartienne pas à notre ensemble $\mathcal{P}$ dont on dispose a priori. On suppose, ce qui n'est pas restrictif, que N appartient à l'ouvert U de E défini aux paragraphes 1.2 et 2.2 de l'appendice 1. La valeur de $u(N)$ est alors donnée par la formule (3). Il s'agit de prouver si possible que $u(N)$ n'est pas dans $\mathbb{Q}$.

1) Le lemme 10 de l'appendice 1 apporte déjà une contrainte sur les éventuels points $S \in \mathfrak{S}$ pour lesquels, N s'écrivant sous la forme (29), $u(N)$ appartient à $\mathbb{Q}$. En tenant compte du fait que la fonction u est invariante par l'involution hyperelliptique (lemme 9 de l'appendice 1), cela permet de remplacer $\mathfrak{S}$ par un ensemble $\mathfrak{S}_0$ contenant O, qui est en pratique strictement contenu dans $\mathfrak{S}$. On a alors :

$$N = S + P \quad \text{où} \quad S \in \mathfrak{S}_0 \text{ et } P \in E_1(K). \tag{30}$$

On peut supposer de plus que N n'est pas dans $\mathfrak{S}_0$, auquel cas P est non nul.

2) Posons $z = z(P)$ et $N = (x, y)$. Pour chaque point $S \in \mathfrak{S}_0$, on exprime $u(N)$ ou $1/u(N)$ à partir de la formule (3), en série entière de z. Dans le cas où S est non nul cela est possible pour peu que certaines conditions soient satisfaites par S. On obtient ces développements comme suit :

2.1) supposons $S = O$. On a alors $N = P \in E_1(K)$ et l'on dispose des développements en série de Laurent de x et y en fonction de z donnés par les formules (7) et (8). On peut ainsi développer $u(N)$ en série :

$$u(N) = \sum_{n \geqslant 1} \nu_n z^n \quad \text{où} \quad \nu_n \in A_{\mathfrak{p}}. \tag{31}$$

On vérifie que l'on a

$$u(N) \equiv -2z \text{ mod. } z^2 \quad \text{si} \quad e = 1 \quad \text{et} \quad u(N) \equiv dz^2 \text{ mod. } z^3 \quad \text{si} \quad e = 0. \tag{32}$$

2.2) Supposons $S \neq O$. Posons $S = (x_S, y_S)$ et notons v la valuation $\mathfrak{p}$-adique de $K_{\mathfrak{p}}$. On suppose que l'une des conditions suivantes est réalisée :

8. on a $e = 1$ ainsi que $v(x_S - \lambda) = 0$ ou $v\Big(y_S - \frac{dx_S}{2} - b\Big) = 0$;
9. on a $e = 1$, $S = M_1$ (lemme 2 de l'appendice 1) et $v(3x_S^2 + 2a_2x_S + a_4 - dy_S) = 0$;
10. on a $e = 0$ et $v(x_S) = 0$.

En utilisant les formules (9) et (10), on obtient alors un développement de la forme :

$$u(N) \ \text{ ou } \ \frac{1}{u(N)} = \sum_{n \geqslant 0} \rho_n z^n \,, \tag{33}$$

où les ρ_n sont dans $A_{\mathfrak{p}}$. Dans le cas simple où $e = 0$ on a

$$u(N) \equiv \frac{d}{x_S}\Big(1 - \frac{2y_S z}{x_S}\Big) \text{ mod. } z^2.$$

3) Soient H le sous-groupe d'indice fini de $E_1(K)$ engendré par $\Big\{Q_1, \cdots, Q_r\Big\}$ et Γ le sous-$\mathbb{F}_p$-espace vectoriel de k engendré par les $\eta\big(z(Q)\big)$ où $Q \in H\backslash\big\{O\big\}$.
Dans certains cas favorables, la connaissance d'une $\mathbb{F}_p$-base de Γ ainsi que celle des premiers coefficients des développements en série entières de $u(N)$, suffit pour démontrer directement que $\eta\big(u(N)\big)$ n'appartient pas à $\mathbb{F}_p^*$, ce qui entraîne alors la conclusion souhaitée. Illustrons ce propos à travers un exemple typique. Supposons pour cela que la condition suivante soit satisfaite :

11. l'intersection de $E_1(K)$ et du sous-groupe de torsion de $E(K)$ est réduite à $\Big\{O\Big\}$.

On a alors l'énoncé suivant :

Lemme 2. *Pour tout point $R \in E_1(K)$ non nul, l'élément $\eta\big(z(R)\big)$ appartient à Γ.*

Démonstration : Soit R un point non nul de $E_1(K)$. Puisque H est d'indice fini dans $E_1(K)$, il existe un entier n non nul tel que nR appartienne à H. D'après la condition 11, on a $nR \neq O$ et il résulte alors de la formule (25) que l'on a

$$\eta\big(z(R)\big) = \frac{\eta\big(z(nR)\big)}{\eta(n)} \in \Gamma.$$

Dans le cas particulier où l'on a $S = O$ et $e = 1$, il est alors facile de conclure si la condition suivante est réalisée :

12. L'élément 1 n'appartient pas à Γ.

En effet, on a $u(N)z \neq 0$ et d'après (32) on a l'égalité :

$$\eta\big(u(N)\big) = -2\eta(z). \tag{34}$$

On déduit alors du lemme 2 que $\eta\big(u(N)\big)$ n'est pas dans $\mathbb{F}_p^*$ et ainsi $u(N)$ n'est pas dans $\mathbb{Q}$.

La plupart des cas auxquels on est confronté dans la démonstration du théorème 2 se traitent en fait suivant cette idée en utilisant le lemme 2, à des modifications mineures près qui correspondent au choix de S. Toutefois, on est amené dans cette démonstration à l'étude de certains cas pour lesquels la condition 12 n'est pas réalisée. Comme il est classique dans la méthode de Chabauty elliptique, il nous faut alors examiner les zéros communs éventuels de certaines séries formelles à coefficients dans $\mathbb{Z}_p$.

Rappelons plus précisément en quoi cela consiste. Considérons un point quelconque $S \in \mathfrak{S}_0$ pour lequel les arguments présentés ci-dessus ne permettent pas de conclure. On construit alors f séries formelles

$$\Phi_S^{(j)} \in \mathbb{Z}_p[[X_1, \cdots, X_r]] \qquad j = 0, \cdots, f-1,$$

telles que le coefficient de $X_1^{j_1}\cdots X_r^{j_r}$ converge vers 0 quand $j_1+\cdots+j_r$ tend vers plus l'infini, et que les zéros dans $\mathbb{Z}_p^r$ de $\Phi_S^{(j)}$, avec $1\leqslant j\leqslant f-1$, correspondent aux éventuelles possibilités que $u(N)$ soit dans $\mathbb{Q}$. La condition (26) sert en fait à assurer qu'il y a au moins autant d'équations $\Phi_S^{(j)}=0$ que de variables.
Indiquons comment construire ces séries formelles. On suppose pour cela que la condition suivante est satisfaite :

13. L'indice de H dans $E_1(K)$ est premier à p ;

Dans ce cas, il existe un entier n, non divisible par p, tel que nP appartienne à H. En utilisant la structure de $\mathbb{Z}_p$-module de $E_1(K)$, on en déduit l'existence d'éléments $n_1,\cdots,n_r$ de $\mathbb{Z}_p$ tels que l'on ait :

$$P=\sum_{i=1}^{r} n_iQ_i. \tag{35}$$

Pour tout i entre 1 et r, posons $z_i=z(Q_i)$. On a l'égalité (cf. 2.4) :

$$z=\exp\biggl(\sum_{i=1}^{r} n_i\log(z_i)\biggr). \tag{36}$$

Remarque. Si $r=1$ et $p=3$, on vérifie que l'on a

$$z\equiv n_1\log(z_1)-a_2n_1^3\frac{\bigl(\log(z_1)\bigr)^3}{3}\ \text{mod. } 3z_1^3,$$

ce qui conduit à la congruence

$$z\equiv\biggl(z_1+a_2\frac{z_1^3}{3}\biggr)n_1-a_2\ \frac{z_1^3}{3}n_1^3\ \text{mod. } 3z_1^3, \tag{37}$$

et l'on obtient ainsi z modulo 3^4 (au moins).

En utilisant (31) ou (33) ainsi que (36), on constate qu'il existe des éléments $a_{j_1\cdots j_r}$ qui appartiennent à $A_{\mathfrak{p}}$ tels que

$$(a_{j_1\cdots j_r})\ \text{converge vers 0 quand } j_1+\cdots+j_r\to+\infty, \tag{38}$$

et que

$$u(N)\ \text{ ou }\ \frac{1}{u(N)}=\sum_{j_1,\cdots,j_r\geqslant 0} a_{j_1\cdots j_r}n_1^{j_1}\cdots n_r^{j_r}. \tag{39}$$

En décomposant les éléments $a_{j_1 \cdots j_r}$ dans la base $\left(1, \tau, \cdots, \tau^{f-1}\right)$ de $A_{\mathfrak{p}}$ sur $\mathbb{Z}_p$, on obtient ainsi f séries formelles

$$\Phi_S^{(j)}(X_1, \cdots, X_r) \in \mathbb{Z}_p[[X_1, \cdots, X_r]] \qquad j = 0, \cdots, f-1,$$

telles que le coefficient de $X_1^{j_1} \cdots X_r^{j_r}$ converge vers 0 quand $j_1 + \cdots j_r$ tend vers plus l'infini, et que

$$u(N) \text{ ou } \frac{1}{u(N)} = \Phi_S^{(0)} + \Phi_S^{(1)}\tau + \cdots + \Phi_S^{(f-1)}\tau^{f-1}, \tag{40}$$

où $\Phi_S^{(j)} = \Phi_S^{(j)}(n_1, \cdots, n_r)$. On en déduit que si $u(N)$ appartient à $\mathbb{Q}$, on a

$$\Phi_S^{(j)} = 0 \quad \text{pour} \quad j = 1, \cdots, f-1. \tag{41}$$

On est ainsi amené à examiner les zéros communs dans $\mathbb{Z}_p^r$ des $f-1$ séries formelles $\Phi_S^{(j)}(X_1, \cdots, X_r)$ pour j compris entre 1 et $f-1$. En connaissant ces séries modulo une puissance de p assez grande, on peut alors parfois démontrer qu'il n'existe pas de tels zéros, auquel cas on déduit que $u(N)$ n'est pas dans $\mathbb{Q}$. La situation rencontrée à ce sujet dans la démonstration du théorème 2 est assez simple, car on démontre directement qu'il n'existe pas de zéros communs à ces séries modulo la puissance de p considérée.

Bibliographie

[At-Le] A.O.L. Atkin et J. Lehner, Hecke operators on $\Gamma_0(N)$, *Math. Ann.* **185** (1970), 134-160.

[Be-Sk] M. A. Bennett and C. M. Skinner, Ternary diophantine equations via Galois representations and modular forms, à paraître dans la revue *Canad. J. Math.* (2003).

[Beu] F. Beukers, On the generalized Ramanujan-Nagell equation. I, *Acta Arith.* **38** (1981), 389-410.

[Bi-Ku] B. J. Birch and W. Kuyk, editors, Modular functions of one variable IV, *Lecture Notes in Math.* **476**, Springer-Verlag, (1975).

[Br-Co-Di-Ta] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843-939.

[Bru1] N. Bruin, Chabauty methods and covering techniques applied to generalised Fermat equations, *PhD Leiden University*, Niederland, (1999).

[Bru2] N. Bruin, ALGAE Package and documentation, (2001), disponible à l'adresse
http ://www.cecm.sfu.ca/˜bruin/#Software

[Bu] Y. Bugeaud, On the diophantine equation $x^2 - 2^m = \pm y^n$, *Proc. Amer. Math. Soc.* **125** (1997), 3203-3208.

[Ch] C. Chabauty, Sur les points rationnels des courbes algébriques de genre supérieur à l'unité, *C.R.A.S.* **212** (1941), 882-885.

[Co1] J.H.E. Cohn, The diophantine equation $x^2 + 3 = y^n$, *Glasgow Math. J.* **35** (1993), 203-206

[Co2] J.H.E. Cohn, The diophantine equation $x^2 + C = y^n$, *Acta Arith.* **65** (1993), 367-381

[Cr1] J. E. Cremona, Algorithms for modular elliptic curves, Second edition, Cambridge University Press (1997).

[Cr2] J. E. Cremona, Elliptic curves data, disponible à l'adresse
http://www.maths.nott.ac.uk/personal/jec/ftp/data/

[Cr-Si] J. E. Cremona et S. Siksek, On the diophantine equation $x^2 + 7 = y^m$, *Acta Arith.* **109** (2003), 143-149.

[Da1] H. Darmon, The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$, *Intern. Math. Research Notices* **10** (1993), 263-274.

[Da2] H. Darmon, Serre's Conjectures, *Canadian Math. Society*, Conference proceeding, Volume **17**, 1995.

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

[Da-Me] H. Darmon et L. Merel, Winding quotients and some variants of Fermat's Last Theorem, *J. reine angew. Math.* **490** (1997), 81-100.

[Di] F. Diamond, On deformation rings and Hecke rings, *Ann. of Math.* **144** (1996), 137-166.

[Du] S. Duquesne, Rational points on hyperelliptic curves and an explicit Weierstrass preparation theorem, *Manuscripta Math.*, **108** (2002), 191-204.

[Fl] E.V. Flynn, A flexible method for applying Chabauty's theorem, *Compositio Math*, **105** (1997), 79-94.

[Fl-We] E.V. Flynn et J.L. Wetherell, Finding rationnal points on bielliptic genus 2 curves, *Manuscripta Math.* **100** (1999), 519-533.

[Fr] G. Frey, Links beetween stable elliptic curves and certain diophantine equations, *Ann. Univ. Sarav. Ser. Math. I* **1** (1986), 1-40.

[Had] T. Hadano, On the conductor of an elliptic curve with a rational point of order 2, *Nagoya Math. J.* **53** (1974), 199-210.

[Ha-Kr-1] E. Halberstadt et A. Kraus, Sur les modules de torsion des courbes elliptiques, *Math. Ann.* **310** (1998), 47-54.

[Ha-Kr-2] E. Halberstadt et A. Kraus, Courbes de Fermat : résultats et problèmes, *J. reine angew. Math.* **548** (2002), 167-234.

[Ha] E. Halberstadt, manuscrit (2003).

[Iv] W. Ivorra, Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$, *Acta. Arith.* **108** (2003), 327-338.

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

[Kr1] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, *Manuscripta Math.* **69** (1990), 353-385.

[Kr2] A. Kraus, Détermination du poids et du conducteur associés aux représentations des points de p-torsion des courbes elliptiques, *Dissertationes Math.* **364** (1997).

[Kr3] A. Kraus, Sur l'équation $La^p + b^p = c^2$, Huitièmes rencontres arithmétiques de Caen, 6-7 juin 1997.

[Kr4] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Can. J. Math.* **49** (1997), 1139-1161.

[Kr5] A. Kraus, Sur l'équation $a^3 + b^3 = c^p$, *Experiment. Math.* **7** (1998), 1-13.

[Kr6] A. Kraus, Une question sur les équations $x^m - y^m = Rz^n$, *Compositio Math.* **132** (2002), 1-26.

[Kr-Oe] A. Kraus et J. Oesterlé, Sur une question de B. Mazur, *Math. Ann.* **293** (1992), 259-275.

[Le] M. Le, Diophantine equation $x^2 + 2^m = y^n$, *Chinese Sci. Bull.* **42** (1997), 1515-1517.

[Les] J.-L. Lesage, Différence entre puissances et carrés d'entiers, *J. Number Theory* **73** (1998), 390-425.

[Li] G. Ligozat, Courbes modulaires de genre 1, *Bull. Soc. Math. France. Mém.* **43**, (1975).

[Lo-Ro-Si] P. Lockhart, M. Rosen et J. H. Silverman, An upper bound for the conductor of an abelian variety, *J. Algebraic Geometry* **2** (1993), 569-601.

[Ma] B. Mazur, Rational Isogenies of prime degree, *Invent. Math.* **44** (1978), 129-162.

[Magma] The Magma Computational System, disponible à l'adresse
http://magma.maths.usyd.edu.au/magma/

[Me-Oe] J.-F. Mestre et J. Oesterlé, Courbes de Weil semi-stables de discriminant une puissance m-ième, *J. reine angew. Math.* **400** (1989), 173-184.

[Mi] M. Mignotte, A corollary to a theorem of Laurent-Mignotte-Nesterenko, *Acta. Arith.* **86** (1998), 101-111.

[Mom] F. Momose, Rational points on the modular curves $X_{split}(p)$, *Compositio Math.* **52** (1984), 115-137.

[Mor] L.J. Mordell, Diophantine equations, Academic Press, London, (1969).

[Og1] A. P. Ogg, Abelian curves of 2-power conductor, *Proc. Camb. Phil. Soc.* **62** (1966), 143-148.

[Og2] A. P. Ogg, Abelian curves of small conductor, *J. reine angew. Math.* **226** (1967), 205-215.

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

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

[Po] B. Poonen, Some diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith.* **86** (1998), 193-205.

[Ri] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431-476.

[Se1] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259-331.

[Se2] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* **54** (1987), 179-230.

[Se3] J.-P. Serre, Travaux de Wiles (et Taylor,...), Partie I, *Astérisque* **237** (1996), Séminaire Bourbaki **803**, 1994-95.

[Set] B. Setzer, Elliptic curves of prime conductor, *J. London Math. Soc.* **10** (1975), 367-378.

[Si1] J. H. Silverman, The Arithmetic of Elliptic Curves, GTM **106** Springer, 1986.

[Si2] J. H. Silverman, Computing heights on elliptic curves, *Math. Comp.* **51** (1988), 339-358.

[Sim] D. Simon, Programme de calcul du rang des courbes elliptiques dans les corps de nombres, disponible à l'adresse
http://www.math.unicaen.fr/~simon/

[St] W. Stein, Modular forms database, disponible à l'adresse
http://modular.fas.harvard.edu/Tables/

[Ta] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, *in Modular Functions of One Variable IV*, Lecture Notes in Math. **476** (1975), 33-52.

[Ve1] J. Vélu, Courbes elliptiques sur $\mathbb{Q}$ ayant bonne réduction en dehors de 11, *C. R. Acad. Sci.* **273** (1971), 73-75.

[Ve2] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci.* **273** (1971), 238-241.

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

Résumé :

Le sujet principal de cette thèse concerne l'étude des équations diophantiennes ternaires de type $(p, p, 2)$. Pour cela on utilise la méthode modulaire et la méthode de Chabauty. Dans le chapitre I, on étudie les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$ et l'on déduit de cette étude des résultats concernant les équations $x^2 - 2^m = y^n$ et $2x^2 - 1 = y^n$. Dans le chapitre II, on détermine toutes les classes de $\mathbb{Q}$-isomorphismes de courbes elliptiques définies sur $\mathbb{Q}$ ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. Dans le chapitre III, on donne des résultats concernant les équations $ax^p + by^p = cz^2$ dans le cas où ab est de la forme $2^n\ell^m$ avec ℓ nombre premier impair. Enfin dans le chapitre IV, on donne des résultats concernant l'équation $x^p + y^p = cz^2$ dans le cas où $p \in \{7, 11, 13, 17\}$ et c ne possède pas de diviseurs premier impair congru à 1 modulo p.

Mots-clefs : équations diophantiennes, courbes elliptiques, méthode modulaire, méthode de Chabauty.

Abstract :

The main subject of this thesis is the study of ternary diophantine equations of signature $(p, p, 2)$. At this aim, we use the modular method and the Chabauty's method. In chapter I, we study the diophantine equations $x^p + 2^\beta y^p = z^2$ and $x^p + 2^\beta y^p = 2z^2$. From this study, we deduce new results about the equations $x^2 - 2^m = y^n$ and $2x^2 - 1 = y^n$. In chapter II, we find, up to $\mathbb{Q}$-isomorphism, all the elliptic curves defined over $\mathbb{Q}$ having at least a point of order 2 rationnal over $\mathbb{Q}$. In chapter III, we give some results about the equation $ax^p + by^p = cz^2$ in the case where ab is of the form $2^n\ell^m$ with ℓ an odd prime number. In chapter IV, we study the equation $x^p - y^p = cz^2$ in the case where $p \in \{7, 11, 13, 17\}$ and c do not have a prime divisor ℓ satisfying $\ell \equiv 1$ mod. p.

Key words : diophantine equations, elliptic curves, modular method, Chabauty method

---