THÈSE DE DOCTORAT DE L'UNIVERSITÉ PARIS 6

Spécialité

Mathématiques

Présentée par

M. Élie CALI

Pour obtenir le grade de

Docteur de l'Université PARIS 6

Sujet de la thèse :

Points de torsion des courbes elliptiques et quartiques de Fermat

Soutenue le 15 septembre 2005

Devant le jury composé de :

M. Henri COHEN	Rapporteur
M. Marc HINDRY	Examinateur
M. Alain KRAUS	Directeur de thèse
M. Loïc MEREL	Examinateur
M. Jean-François MESTRE	Examinateur
M. Joseph OESTERLÉ	Examinateur
M. Michel WALDSCHMIDT	Examinateur

Remerciements

Je tiens à remercier en premier lieu mon directeur de thèse, Alain Kraus, qui m'a apporté une aide considérable sur l'ensemble des tâches à accomplir : le choix des sujets traités, le défrichement des travaux existant sur ces sujets, la mise au point de nombreuses démonstrations, la rédaction des articles, ainsi que la rédaction finale de la thèse. Ma situation de salarié ne me permettait généralement pas d'être disponible dans la semaine, et je n'aurais pas pu mener à bien ce travail s'il n'avait été en permanence disponible, aussi bien le week-end que pendant les périodes de congés.

Je remercie par ailleurs Emmanuel Halberstadt de m'avoir transmis le résultat de l'appendice 3 du chapitre V qui lui est dû.

Je remercie Henri Cohen et Joseph Silverman qui ont bien voulu être rapporteurs de cette thèse, ainsi que Marc Hindry, Loïc Merel, Jean-François Mestre, Joseph Oesterlé et Michel Waldschmidt qui m'ont fait l'honneur de composer mon jury. Je remercie en particulier Henri Cohen de m'avoir suggéré l'ajout du chapitre 0, et pour les remarques qu'il m'a faites concernant le paragraphe 5 du chapitre IV.

J'adresse aussi des remerciements à Thierry Bousch, mathématicien et ami, qui m'a très fortement aidé à redémarrer des études en mathématiques.

Je remercie enfin chaleureusement toutes les personnes, et en particulier tous mes proches, qui m'ont soutenu et supporté pendant l'élaboration de cette thèse.

Table des matières

Seconde partie

Introduction

Cette thèse est constituée de deux parties indépendantes. Dans la première partie, on s'intéresse à l'étude des points de torsion des courbes elliptiques. La seconde est relative à l'étude des points rationnels sur les corps de nombres de certaines tordues galoisiennes de la quartique de Fermat d'équation $x^4 + y^4 = z^4$.

Première partie

Elle comporte principalement trois chapitres. Après un chapitre 0 de rappels, le premier concerne la détermination de la différente des extensions de $\mathbb{Q}$ engendrées par les points de torsion, d'ordre un nombre premier, des courbes elliptiques sur $\mathbb{Q}$. Dans le deuxième chapitre, on se préoccupe du défaut de semi-stabilité des courbes elliptiques qui sont définies sur une extension finie non ramifiée de $\mathbb{Q}_2$ ayant réduction de type additif. Le troisième chapitre est consacré à des exemples d'application des résultats obtenus dans le chapitre I et de travaux antérieurs sur le sujet, au calcul du discriminant des corps des points de torsion des courbes elliptiques.

Chapitre I

Soit E une courbe elliptique définie sur $\mathbb{Q}$ par une équation de Weierstrass minimale :

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

les coefficients a_i étant des entiers relatifs. Soient ℓ un nombre premier et $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. Notons E_ℓ le sous-groupe des points de ℓ-torsion de $E\big(\overline{\mathbb{Q}}\big)$ et $\mathbb{Q}(E_\ell)$ le corps des points de ℓ-torsion de E, i.e. le sous-corps de $\mathbb{C}$ engendré par les coordonnées des points de E_ℓ. C'est une extension galoisienne finie de $\mathbb{Q}$. On s'intéresse au problème suivant :

Problème 1. *Comment calculer le discriminant de $\mathbb{Q}(E_\ell)$ en fonction des entiers a_i ?*

Soit $D(\ell)$ ce discriminant. Pour le déterminer, on est amené à envisager trois étapes. La première consiste à calculer le degré de l'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$. On utilise pour cela les travaux de J.-P. Serre qui se trouvent dans [Se1]. Dans une deuxième étape, il s'agit de déterminer, pour tout nombre premier p, l'indice de ramification de p dans l'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$. On peut trouver dans [Se1] et [Kr3] les informations utiles à ce sujet. La dernière étape consiste, pour tout nombre premier p, à calculer l'exposant d'un idéal premier de l'anneau d'entiers de $\mathbb{Q}(E_\ell)$ au-dessus de p dans la différente de l'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$. Le cas où $\ell = p$ a été traité dans [Kr4]. L'objectif du chapitre I est de calculer cet exposant si ℓ est distinct de p. Ce chapitre a été publié en 2002 dans la revue Acta Arithmetica en collaboration avec A. Kraus ([Ca-Kr]).

Chapitre II

Les calculs des indices de ramification intervenant dans la deuxième étape signalée ci-dessus, nécessitent, lorsque E n'est pas semi-stable en dehors de ℓ, de déterminer le défaut de semi-stabilité de E en les nombres premiers distincts de ℓ où E a réduction de type additif (cf. [Se1]). Ce défaut est mesuré localement par l'ordre d'un certain groupe fini (*loc. cit.*). Il a été explicité dans [Kr2], dans le cadre local, pour les courbes elliptiques qui sont définies sur $\mathbb{Q}_2$ ou bien sur une extension finie de $\mathbb{Q}_p$ si p est impair. Si l'on souhaite aborder le problème 1 en remplaçant $\mathbb{Q}$ par une extension finie, il importe ainsi d'étendre les résultats de [Kr2] aux extensions finies de $\mathbb{Q}_2$. C'est l'objectif de ce chapitre en se limitant aux extensions finies non ramifiées de $\mathbb{Q}_2$. Ce chapitre a été publié en 2004 dans le Journal Canadien de Mathématiques ([Cal]).

Chapitre III

À titre d'illustration, nous explicitons dans ce chapitre deux exemples de calcul de discriminant des corps des points de ℓ-torsion d'une courbe elliptique sur $\mathbb{Q}$.

Dans le premier exemple, on considère la courbe elliptique E sur $\mathbb{Q}$ d'équation de Weierstrass

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

où a est un entier relatif non nul sans puissances quatrièmes. C'est une courbe elliptique à multiplications complexes d'invariant modulaire 1728. Pour tout nombre premier ℓ, on détermine le discriminant $D(\ell)$ du corps $\mathbb{Q}(E_\ell)$. Notons que $D(2)$ est déjà connu car on a $\mathbb{Q}(E_2) = \mathbb{Q}\big(\sqrt{-a}\big)$. Par exemple, si $a = 1$, on a

$$D(\ell) = \begin{cases} 2^{\frac{9(\ell-1)^2}{2}}\ \ell^{2(\ell-1)(\ell-2)} & \text{si } \ell \equiv 1 \text{ mod. } 4 \\ 2^{\frac{9(\ell^2-1)}{2}}\ \ell^{2(\ell^2-2)} & \text{si } \ell \equiv 3 \text{ mod. } 4. \end{cases}$$

Dans le cas particulier où $a = 2p$, p étant un nombre premier impair, on obtient le résultat suivant :

1) supposons $\ell \equiv 1$ mod. 4. On a

$$D(\ell) = \begin{cases} 2^{6(\ell-1)^2}\ \ell^{2(\ell-1)(\ell-2)} & \text{si } p = \ell \\ 2^{6(\ell-1)^2}\ \ell^{2(\ell-1)(\ell-2)}\ p^{\frac{3(\ell-1)^2}{2}} & \text{si } p \neq \ell. \end{cases}$$

2) Supposons $\ell \equiv 3$ mod. 4. On a

$$D(\ell) = \begin{cases} 2^{6(\ell^2-1)}\ \ell^{2(\ell^2-2)} & \text{si } p = \ell \\ 2^{6(\ell^2-1)}\ \ell^{2(\ell^2-2)}\ p^{\frac{3(\ell^2-1)}{2}} & \text{si } p \neq \ell. \end{cases}$$

Le second exemple concerne la courbe elliptique E, de conducteur 11, d'équation

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

Dans ce cas, la détermination du discriminant $D(\ell)$ de $\mathbb{Q}(E_\ell)$, pour un nombre premier ℓ en lequel E a bonne réduction ordinaire, dépend de la congruence modulo ℓ^2 de l'invariant modulaire du relèvement canonique sur $\mathbb{Z}_\ell$ de la courbe déduite de E par réduction modulo ℓ (cf. [Kr 4]). À titre indicatif, pour les petites valeurs de ℓ, on obtient :

$$D(2) = -2^4 11^3, \;\; D(3) = 3^{56} 11^{32}, \;\; D(5) = 5^{15} 11^{16}, \;\; D(7) = 7^{2256} 11^{1728}, \;\; D(11) = 11^{26280}.$$

Seconde partie

Étant donnés un corps de nombres K et un élément non nul b de K, notons C_b la courbe définie sur K d'équation

$$x^4 + y^4 = bz^4.$$

On s'intéresse dans cette partie à l'étude de l'ensemble $C_b(K)$, des points de C_b rationnels sur K, à travers le problème suivant :

Problème 2. *Comment démontrer que $C_b(K)$ est vide, si tel est le cas ?*

Dans le chapitre IV, on aborde ce problème par des méthodes locales. Le chapitre V est consacré à l'effectivité de certaines méthodes globales qui permettent parfois de conclure.

Chapitre IV

Une méthode possible pour démontrer que $C_b(K)$ est vide, si tel est le cas, consiste à examiner l'existence éventuelle d'un complété de K, archimédien ou non, sur lequel C_b ne possède pas de points rationnels. Comme il est d'usage, s'il existe un tel complété, on dit alors que C_b possède une obstruction locale sur K.

On obtient un énoncé fournissant des conditions nécessaires et suffisantes simples portant sur b et K pour qu'il en soit ainsi. Si K ne contient pas le corps $\mathbb{Q}(\mu_8)$ des racines huitièmes de l'unité, on constate en pratique qu'il est très fréquent que C_b possède des obstructions locales. On notera que si K contient $\mathbb{Q}(\mu_8)$, alors pour tout $b \in K^*$, le point $[\zeta, 1, 0]$, où ζ est un générateur de μ_8, appartient à $C_b(K)$, ce qui interdit la présence d'obstructions locales pour C_b. On démontre en fait que si K ne contient pas $\mathbb{Q}(\mu_8)$, il existe une infinité de $b \in K^*$ modulo K^{*4} tels que C_b n'ait pas de points rationnels sur un complété non archimédien de K.

Dans le cas particulier où $b \in \mathbb{Q}^*$, on obtient par ailleurs des critères simples pour que C_b possède une obstruction locale sur K. Par exemple, si b est un entier naturel sans puissances quatrièmes ayant un diviseur premier impair non congru à 1 modulo 8, et si le degré de K sur $\mathbb{Q}$ est impair, alors C_b a une obstruction locale sur K. Ces courbes C_b n'ont donc pas de points rationnels sur les extensions de degré impair de $\mathbb{Q}$; dans le cas particulier où b est congru à 3 ou 6 modulo 8, on démontrera de plus que C_b ne possède pas non plus de points quadratiques, là encore pour des raisons locales.

On explicitera par ailleurs une infinité de classes de $\mathbb{Q}$-isomorphisme de courbes C_b sur $\mathbb{Q}$ qui contredisent le principe de Hasse, i.e. qui ont des points rationnels sur tous les complétés de $\mathbb{Q}$, mais pas sur $\mathbb{Q}$.

Chapitre V

On s'intéresse dans ce chapitre au problème de l'effectivité de méthodes globales permettant parfois de démontrer que $C_b(K)$ est vide. Pour tout $b \in K^*$ notons E_b la courbe elliptique sur K d'équation de Weierstrass

$$Y^2 = X^3 - bX.$$

On dispose de deux morphismes indépendants (cf. [Se4]) définis sur K de C_b sur E_b. Dans le cas où $K = \mathbb{Q}$, V. A. Dem'janenko a démontré en 1968 que pour tout entier $b \geqslant 3$ sans puissances quatrièmes, si $E_b(\mathbb{Q})$ est de rang $\leqslant 1$, alors $C_b(\mathbb{Q})$ est vide ([De]). Ce chapitre concerne certaines généralisations de ce résultat.

J. Silverman a prouvé en 1986, dans [Si3], l'existence d'une constante absolue c_0, qui dépend seulement du degré de K sur $\mathbb{Q}$, telle que la condition suivante soit réalisée :

soit b un élément de K^* qui ne soit pas dans K^4 et L une extension de K obtenue en adjoignant à K une racine quatrième de b. Alors, si $E_b(K)$ est de rang 1 et si la norme de K sur $\mathbb{Q}$ du discriminant relatif de l'extension L/K est plus grande que c_0, l'ensemble $C_b(K)$ est vide. En particulier, pour toute classe d'élément b dans K^*/K^{*4} sauf un nombre fini, si le rang de $E_b(K)$ est 1, alors $C_b(K)$ est vide.

Silverman avait démontré que c_0 dépend exponentiellement du degré n de K sur $\mathbb{Q}$. À notre connaissance, une telle constante n'a pas été explicitée numériquement. Dans la première partie de ce chapitre, on se propose d'en préciser une effectivement. La méthode suivie repose sur des arguments de hauteurs et sur l'effectivité du théorème des zéros de Hilbert dans un cas particulier. On démontrera que l'on peut prendre par exemple $c_0 = \exp(169 + 6n)$. Comme on le constate, ce résultat n'est pas utilisable en pratique.

Si K est un corps totalement réel, on démontre dans la deuxième partie de ce chapitre un énoncé qui généralise le théorème de Dem'janenko sur K, et qui est plus satisfaisant du point de vue de l'effectivité. On s'est inspiré pour cela d'une méthode décrite par G. Grigorov et J. Rizov dans le cas particulier où $K = \mathbb{Q}$, permettant d'obtenir des estimations uniformes pour la différence entre la hauteur de Weil et la hauteur de Néron-Tate sur la courbe elliptique E_b ([Gr-Ri]). Un cas particulier du résultat que l'on obtient est le suivant :

soit b un élément non nul de l'anneau d'entiers O_K de K. Supposons que les exposants des idéaux premiers intervenant dans la décomposition de bO_K soient strictement inférieurs à 4 et que pour tout plongement σ de K dans $\mathbb{R}$, on ait $\sigma(b) \geqslant 1$. Alors, si $E_b(K)$ est de rang $\leqslant 1$, et si la norme sur $\mathbb{Q}$ de b est supérieure à $2^{11n/2}$, l'ensemble $C_b(K)$ est vide.

Pour exploiter numériquement ce type d'énoncés, il importe évidemment de savoir démontrer que, b étant donné, le rang de $E_b(K)$ est au plus 1, si tel est le cas. On peut

effectuer pour cela une 2-descente comme il est expliqué dans [Si2]. Signalons à ce propos qu'il existe un programme, écrit par D. Simon, s'appuyant sur le logiciel de calculs Pari ([Pari]), qui permet parfois de déterminer le rang d'une courbe elliptique sur un corps de nombres de degré sur $\mathbb{Q}$ assez petit ([Sim]).

Dans la dernière partie de ce chapitre, dans le cas où $K = \mathbb{Q}$, on fait quelques remarques sur le problème suivant :

Problème 3. *Dans quelle mesure peut-on obtenir un énoncé analogue à celui démontré par Dem'janenko si l'on ne suppose plus que le rang de $E_b(\mathbb{Q})$ est au plus 1 ?*

Soit b un entier naturel non nul sans puissances quatrièmes. On prouvera dans cette direction que si la conjecture de parité pour $E_b/\mathbb{Q}$ est vraie, ou bien si la partie 2-primaire du groupe de Tate-Shafarevitch de $E_b/\mathbb{Q}$ est finie, alors $C_b(\mathbb{Q})$ est vide, pour des raisons locales, dans les deux cas suivants :

1) le rang de $E_b(\mathbb{Q})$ est impair et $b \equiv 1$ mod. 16.

2) Le rang de $E_b(\mathbb{Q})$ est pair et $b \equiv 2$ mod. 16.

Si b est congru à 1 ou 2 modulo 16, l'ensemble $C_b(\mathbb{Q}_2)$ n'est pas vide. On prouvera en fait l'existence d'un diviseur premier p de b tel que $C_b(\mathbb{Q}_p)$ soit vide.

Chapitre 0

Rappels

L'objectif de ce chapitre est de rappeler quelques résultats connus que l'on va utiliser dans la première partie de la thèse, afin d'éviter au lecteur d'avoir à se référer systématiquement à la littérature lors des démonstrations techniques des deux premiers chapitres.

Soient p un nombre premier et K une extension finie de $\mathbb{Q}_p$. Notons v la valuation discrète standard sur K normalisée par l'égalité $v(K^*) = \mathbb{Z}$. Soient $\overline{K}$ une clôture algébrique de K et K_{nr} l'extension non ramifiée maximale de K dans $\overline{K}$. Considérons une courbe elliptique E définie sur K ayant mauvaise réduction de type additif et dont l'invariant modulaire j vérifie $v(j) \geqslant 0$. Il existe une plus petite extension L de K_{nr} sur laquelle E acquiert bonne réduction. Si E_n désigne le sous-groupe des points de n-torsion de $E\big(\overline{K}\big)$, on a $L = K_{nr}(E_n)$ pour tout entier $n \geqslant 3$ premier à p ([Se-Ta], 2. cor. 3). Notons Φ le groupe de Galois de l'extension L/K_{nr}. Si $p \geqslant 5$, le groupe Φ est cyclique d'ordre $2, 3, 4$ ou 6. Si $p = 3$, il est soit cyclique d'ordre $2, 3, 4$ ou 6, soit d'ordre 12 et produit semi-direct non abélien d'un groupe cyclique d'ordre 4 par un sous-groupe distingué d'ordre 3. Si $p = 2$, il est soit cyclique d'ordre $2, 3, 4$ ou 6, soit d'ordre 8 et isomorphe au groupe quaternionien, soit d'ordre 24 et isomorphe à $\mathbb{S}L_2(\mathbb{F}_3)$ (cf. [Se1], 5.6).

L'ordre de Φ a été déterminé dans certains cas particuliers, par exemple si $p \geqslant 3$ ou bien si $K = \mathbb{Q}_2$ ([Kr2]). On utilisera dans les chapitres I et II de cette thèse certains résultats obtenus à ce sujet dans *loc. cit.*, que l'on rappelle ci-dessous. Notons pour cela c_4, c_6 et Δ les invariants standard associés à un modèle minimal de E. Le choix d'un autre modèle minimal de E conduirait à les remplacer respectivement par c_4u^4, c_6u^6 et Δu^{12}, où u est un élément de K de valuation nulle. Par suite, les entiers $v(c_4)$, $v(c_6)$ et $v(\Delta)$ ne dépendent pas du modèle minimal choisi.

Proposition 1. *Si l'on a $p \geqslant 5$, l'ordre de Φ est le dénominateur de $v(\Delta)/12$.*

Proposition 2. *Si $p = 3$ et si K est absolument non ramifié (i.e. $v(3) = 1$), on est dans l'un des cas des tableaux suivants :*

$v(\Delta)$	3	4
$v(c_6) = 3$	$\lvert\Phi\rvert = 4$ *ou* $\lvert\Phi\rvert = 12$ $(*)$	$\lvert\Phi\rvert = 3$
$v(c_6) = 4$	$\lvert\Phi\rvert = 12$	
$v(c_6) \geqslant 5$	$\lvert\Phi\rvert = 4$	

(∗) *on a* $|\Phi| = 4$ *si et seulement si la congruence* $4x^3 - (c_4/3)x - c_6/27 \equiv 0$ mod. 9 *a une solution dans l'anneau des entiers de* K.
Si $K = \mathbb{Q}_3$, *on a* $|\Phi| = 4$ *si et seulement si* $\Delta/27$ *est congru à* 2 *ou* 4 *modulo* 9.

$v(\Delta)$	5	6	7
$v(c_6) = 3$	$\lvert\Phi\rvert = 12$	$\lvert\Phi\rvert = 2$	
$v(c_6) = 4$	$\lvert\Phi\rvert = 12$		
$v(c_6) = 5$		$\lvert\Phi\rvert = 6$	$\lvert\Phi\rvert = 12$
$v(c_6) \geqslant 6$		$\lvert\Phi\rvert = 2$	

$v(\Delta)$	9	10	11
$v(c_6) = 6$	$\lvert\Phi\rvert = 4$ *ou* $\lvert\Phi\rvert = 12$ (∗∗)	$\lvert\Phi\rvert = 6$	$\lvert\Phi\rvert = 12$
$v(c_6) = 7$	$\lvert\Phi\rvert = 12$		$\lvert\Phi\rvert = 12$
$v(c_6) \geqslant 8$	$\lvert\Phi\rvert = 4$		

(∗∗) *on a* $|\Phi| = 4$ *si et seulement si la congruence* $4x^3 - (c_4/27)x - c_6/729 \equiv 0$ mod. 9 *a une solution dans l'anneau des entiers de* K.
Si $K = \mathbb{Q}_3$, *on a* $|\Phi| = 4$ *si et seulement si* $\Delta/3^9$ *est congru à* 2 *ou* 4 *modulo* 9.

$v(\Delta)$	12	13
$v(c_6) = 8$	$\lvert\Phi\rvert = 3$	$\lvert\Phi\rvert = 12$

Le résultat suivant peut servir à la détermination générale de l'ordre de Φ. On l'utilise de façon essentielle dans le chapitre II.

Proposition 3. *Supposons* $p = 2$. *Soit* $\Delta^{1/3}$ *une racine cubique de* Δ *dans* $\overline{K}$. *Posons :*

$$A = c_4 - 12\Delta^{1/3} \quad et \quad B = c_4^2 + 12c_4\Delta^{1/3} + \big(12\Delta^{1/3}\big)^2.$$

On a $AB = c_6^2$. *Soit* $B^{1/2}$ *une racine carrée de* B *dans* $\overline{K}$. *Posons :*

$$C = 2\big(c_4 + 6\Delta^{1/3} + B^{1/2}\big).$$

(i) Supposons $v(\Delta) \equiv 0 \bmod 3$. *Dans ce cas,* $\Delta^{1/3}$ *appartient à* K_{nr}.
a) Supposons que A *et* B *soient des carrés dans* K_{nr}. *On a* $|\Phi| = 2$ *si* C *est un carré dans* K_{nr}, *et* $|\Phi| = 4$ *sinon.*
b) Supposons que A *ou* B *ne soit pas un carré dans* K_{nr}. *On a* $|\Phi| = 4$ *si* C *est un carré dans* $K_{nr}\big(A^{1/2}, B^{1/2}\big)$, *et* $|\Phi| = 8$ *sinon.*

(ii) Supposons $v(\Delta) \not\equiv 0 \bmod 3$ *; soit* M *l'unique extension de degré* 3 *de* K_{nr}. *Elle est engendrée par* $\Delta^{1/3}$.
a) Supposons que A *et* B *soient des carrés dans* M. *On a* $|\Phi| = 3$ *si le type de Néron de* E *est* IV *ou* IV^*, *et* $|\Phi| = 6$ *sinon.*
b) Si A *ou* B *n'est pas un carré dans* M, *on a* $|\Phi| = 24$.

En explicitant la proposition précédente dans le cas particulier où $K = \mathbb{Q}_2$, on obtient le résultat suivant :

Proposition 4. *Supposons* $K = \mathbb{Q}_2$. *Posons* $c_4 = 2^{v(c_4)}c_4'$, $c_6 = 2^{v(c_6)}c_6'$ *et* $\Delta = 2^{v(\Delta)}\Delta'$. *Désignons par* $\overline{c_4'}$, $\overline{c_6'}$ *et* $\overline{\Delta'}$ *respectivement les classes de* c_4', c_6' *et* Δ' *modulo* 4. *On est dans l'un des cas des tableaux suivants :*

$v(\Delta)$	4	6
$v(c_4) = 4$	$\begin{cases} \overline{c_4'} = -1 \\ \overline{c_6'} = 1 \end{cases} \Rightarrow \lvert\Phi\rvert = 3$ $\begin{cases} \overline{c_4'} = -1 \\ \overline{c_6'} = -1 \end{cases} \Rightarrow \lvert\Phi\rvert = 6$ $\overline{c_4'} = 1 \Rightarrow \lvert\Phi\rvert = 24$	$\lvert\Phi\rvert = 8$
$v(c_4) = 5$	$\lvert\Phi\rvert = 24$	$\lvert\Phi\rvert = 8$
$v(c_4) \geqslant 6$	$\overline{c_6'} = 1 \Rightarrow \lvert\Phi\rvert = 3$ $\overline{c_6'} = -1 \Rightarrow \lvert\Phi\rvert = 6$	$\lvert\Phi\rvert = 2$

$v(\Delta)$	7	8
$v(c_4)=4$	$\lvert\Phi\rvert=24$	$\begin{cases}\overline{c_6'}=-1\\ \overline{\Delta'}=-1\end{cases}\Rightarrow\lvert\Phi\rvert=3$ $\begin{cases}\overline{c_6'}=1\\ \overline{\Delta'}=-1\end{cases}\Rightarrow\lvert\Phi\rvert=6$ $\overline{\Delta'}=1\Rightarrow\lvert\Phi\rvert=24$
$v(c_4)=5$		$\lvert\Phi\rvert=24$
$v(c_4)=6$		$\lvert\Phi\rvert=24$
$v(c_4)\geqslant 7$		$\overline{c_6'}=1\Rightarrow\lvert\Phi\rvert=3$ $\overline{c_6'}=-1\Rightarrow\lvert\Phi\rvert=6$

$v(\Delta)$	9	10	11
$v(c_4)=4$	$\lvert\Phi\rvert=8$	$\lvert\Phi\rvert=24$	$\lvert\Phi\rvert=24$
$v(c_4)=5$	$v(c_6)=8\Rightarrow\lvert\Phi\rvert=4$ $v(c_6)>8\Rightarrow\lvert\Phi\rvert=8$		
$v(c_4)=6$		$\overline{c_4'}=-1\Rightarrow\lvert\Phi\rvert=6$ $\overline{c_4'}=1\Rightarrow\lvert\Phi\rvert=24$	
$v(c_4)=7$		$\lvert\Phi\rvert=24$	
$v(c_4)\geqslant 8$		$\lvert\Phi\rvert=6$	

$v(\Delta)$	12	13	14
$v(c_4)=4$	$\lvert\Phi\rvert=2$		
$v(c_4)=6$	$\lvert\Phi\rvert=8$	$\lvert\Phi\rvert=24$	$\overline{\Delta'}=-1\Rightarrow\lvert\Phi\rvert=6$ $\overline{\Delta'}=1\Rightarrow\lvert\Phi\rvert=24$
$v(c_4)=7$	$\lvert\Phi\rvert=8$		$\lvert\Phi\rvert=24$
$v(c_4)=8$	$\lvert\Phi\rvert=2$		$\lvert\Phi\rvert=24$
$v(c_4)\geqslant 9$	$\lvert\Phi\rvert=2$		$\lvert\Phi\rvert=6$

$v(\Delta)$	15	16	17	18
$v(c_4)=6$	$\lvert\Phi\rvert=8$	$\lvert\Phi\rvert=24$	$\lvert\Phi\rvert=24$	$\lvert\Phi\rvert=2$
$v(c_4)=7$	$v(c_6)=11\Rightarrow\lvert\Phi\rvert=4$ $v(c_6)>11\Rightarrow\lvert\Phi\rvert=8$			

Chapitre I

Sur la p-différente du corps des points de ℓ-torsion des courbes elliptiques, $\ell \neq p$

Introduction

Soient p un nombre premier, K une extension finie *non ramifiée* de $\mathbb{Q}_p$ et $\overline{K}$ une clôture algébrique de K. Soient E une courbe elliptique définie sur K et ℓ un nombre premier. On désigne par E_ℓ le sous-groupe des points de ℓ-torsion de $E(\overline{K})$ et par $K(E_\ell)$ l'extension de K obtenue en adjoignant à K les coordonnées des points de E_ℓ. On s'intéresse dans ce travail à la détermination de l'entier D, caractérisé par les propriétés équivalentes suivantes :

a) la différente de l'extension $K(E_\ell)/K$ est la puissance D-ième de l'idéal de valuation de $K(E_\ell)$;
b) l'idéal discriminant de l'extension $K(E_\ell)/K$ est engendré par $p^{nD/e}$, où n est le degré et e l'indice de ramification de l'extension $K(E_\ell)/K$.

L'article [Kr4] est consacré au cas où $\ell = p$. On se préoccupera ici du cas où ℓ et p sont *distincts*, ce que l'on supposera dans toute la suite.

I. Énoncé des résultats

Considérons un corps K comme ci-dessus. Soit v la valuation de K qui prolonge celle de $\mathbb{Q}_p$; on suppose que v est normée : on a $v(p) = 1$. Soient E une courbe elliptique définie sur K et j son invariant modulaire. On note c_4, c_6 et Δ les invariants standards associés à un modèle minimal de E sur K ([Ta], 1.). Les entiers $v(c_4)$, $v(c_6)$ et $v(\Delta)$ sont indépendants du modèle minimal choisi (cf. *loc. cit.*, 2.).

I.1. Cas où E a bonne réduction sur K

Rappelons pour mémoire l'énoncé suivant :

Proposition 1. *Si E a bonne réduction sur K, on a $D = 0$.*

C'est une conséquence directe du critère de Néron-Ogg-Shafarevich (cf. [Si2], p. 184, th. 7.1).

I.2. Cas où $v(j) < 0$

Théorème 1.
(a) Supposons que E ait réduction de type multiplicatif sur K. On a

$$D = \begin{cases} 0 & \text{si } \ell \text{ divise } v(j) \\ \ell - 1 & \text{si } \ell \text{ ne divise pas } v(j). \end{cases}$$

(b) Supposons que E ait réduction de type additif sur K et que $v(j) < 0$.

(i) Si $p \neq 2$, on a

$$D = \begin{cases} 1 & \text{si } \ell \text{ divise } v(j) \text{ ou bien si } \ell = 2 \\ 2\ell - 1 & \text{si } \ell \text{ ne divise pas } v(j) \text{ et } \ell \neq 2. \end{cases}$$

(ii) Si $p = 2$, on est dans l'un des cas suivants :

(ii.1) $v(c_6) = 6$

$$D = \begin{cases} 2 & \text{si } \ell \text{ divise } v(j) \\ 3\ell - 1 & \text{si } \ell \text{ ne divise pas } v(j). \end{cases}$$

(ii.2) $v(c_6) = 9$

$$D = \begin{cases} 3 & \text{si } \ell \text{ divise } v(j) \\ 4\ell - 1 & \text{si } \ell \text{ ne divise pas } v(j). \end{cases}$$

I.3. Cas où E a réduction de type additif sur K et où $v(j) \geqslant 0$

I.3.1. Cas où $p \geqslant 5$

Théorème 2. *Supposons que E ait réduction de type additif sur K, et que l'on ait $v(j) \geqslant 0$ et $p \geqslant 5$. Soit m le dénominateur de $v(\Delta)/12$. On a*

$$D = \begin{cases} m - 1 & \text{si } \ell \neq 2 \\ 1 & \text{si } \ell = 2 \text{ et } v(\Delta) \text{ est impair} \\ 2 & \text{si } \ell = 2 \text{ et } v(\Delta) \text{ est pair et distinct de } 6 \\ 0 & \text{si } \ell = 2 \text{ et } v(\Delta) = 6. \end{cases}$$

I.3.2. Cas où $p = 3$

Théorème 3. *Supposons que E ait réduction de type additif sur K, et que l'on ait $v(j) \geqslant 0$ et $p = 3$.*

(a) Supposons $\ell \geqslant 5$. On est dans l'un des cas suivants :

$v(\Delta)$	3	4
$v(c_6) = 3$	$D = 3$ *ou* 15 $(*)$	$D = 4$
$v(c_6) = 4$	$D = 15$	
$v(c_6) \geqslant 5$	$D = 3$	

$(*)$ *on a $D = 3$ si et seulement si la congruence $4x^3 - (c_4/3)x - c_6/27 \equiv 0$ mod. 9 a une solution dans l'anneau des entiers de K.*

Si $K = \mathbb{Q}_3$, on a $D = 3$ si et seulement si $\Delta/27$ est congru à 2 ou 4 modulo 9.

$v(\Delta)$	5	6	7
$v(c_6) = 3$	$D = 15$	$D = 1$	
$v(c_6) = 4$	$D = 23$		
$v(c_6) = 5$		$D = 9$	$D = 23$
$v(c_6) \geqslant 6$		$D = 1$	

$v(\Delta)$	9	10	11
$v(c_6) = 6$	$D = 3$ *ou* 15 $(**)$	$D = 9$	$D = 15$
$v(c_6) = 7$	$D = 15$		$D = 23$
$v(c_6) \geqslant 8$	$D = 3$		

$(**)$ *on a $D = 3$ si et seulement si la congruence $4x^3 - (c_4/27)x - c_6/729 \equiv 0$ mod. 9 a une solution dans l'anneau des entiers de K.*

Si $K = \mathbb{Q}_3$, on a $D = 3$ si et seulement si $\Delta/3^9$ est congru à 2 ou 4 modulo 9.

$v(\Delta)$	12	13
$v(c_6) = 8$	$D = 4$	$D = 23$

(b) Supposons $\ell = 2$. On est dans l'un des cas suivants :

$v(\Delta)$	3	4
$v(c_6) = 3$	$D = 1$ *ou* 7 $(*)$	$D = 4$
$v(c_6) = 4$	$D = 7$	
$v(c_6) \geqslant 5$	$D = 1$	

$(*)$ *on a $D = 1$ si et seulement si la congruence $4x^3 - (c_4/3)x - c_6/27 \equiv 0$ mod. 9 a une solution dans l'anneau des entiers de K.*

Si $K = \mathbb{Q}_3$, on a $D = 1$ si et seulement si $\Delta/27$ est congru à 2 ou 4 modulo 9.

$v(\Delta)$	5	6	7
$v(c_6) = 3$	$D = 7$	$D = 0$	
$v(c_6) = 4$	$D = 11$		
$v(c_6) = 5$		$D = 4$	$D = 11$
$v(c_6) \geqslant 6$		$D = 0$	

$v(\Delta)$	9	10	11
$v(c_6) = 6$	$D = 1$ *ou* 7 $(**)$	$D = 4$	$D = 7$
$v(c_6) = 7$	$D = 7$		$D = 11$
$v(c_6) \geqslant 8$	$D = 1$		

$(**)$ *on a $D = 1$ si et seulement si la congruence $4x^3 - (c_4/27)x - c_6/729 \equiv 0$ mod. 9 a une solution dans l'anneau des entiers de K.*

Si $K = \mathbb{Q}_3$, on a $D = 1$ si et seulement si $\Delta/3^9$ est congru à 2 ou 4 modulo 9.

$v(\Delta)$	12	13
$v(c_6) = 8$	$D = 4$	$D = 11$

I.3.3. Cas où $p = 2$

On suppose dans ce paragraphe que l'on a $K = \mathbb{Q}_2$. On notera

$$c_4' = \frac{c_4}{2^{v(c_4)}}, \quad c_6' = \frac{c_6}{2^{v(c_6)}} \quad \text{et} \quad \Delta' = \frac{\Delta}{2^{v(\Delta)}}.$$

On désignera respectivement par $\overline{c_4'}$, $\overline{c_6'}$ et $\overline{\Delta'}$ les classes modulo $4\mathbb{Z}_2$ de c_4', c_6' et Δ'.

Théorème 4. *Supposons que E ait réduction de type additif sur $\mathbb{Q}_2$, et que $v(j) \geqslant 0$. On est dans l'un des cas suivants :*

$v(\Delta)$	4	6
$v(c_4) = 4$	$\begin{cases} \overline{c_4'} = -1 \\ \overline{c_6'} = 1 \end{cases} \Rightarrow D = 2$ $\begin{cases} \overline{c_4'} = -1 \\ \overline{c_6'} = -1 \end{cases} \Rightarrow D = 8$ $\begin{cases} \overline{c_4'} = 1 \\ \overline{c_6'} = -1 \end{cases} \Rightarrow D = 32$ $\begin{cases} \overline{c_4'} = 1 \\ \overline{c_6'} = 1 \end{cases} \Rightarrow D = 38$	$\overline{c_4'} = -1 \Rightarrow D = 16$ $\overline{c_4'} = 1 \Rightarrow D = 18$
$v(c_4) = 5$	$\overline{c_6'} = 1 \Rightarrow D = 32$ $\overline{c_6'} = -1 \Rightarrow D = 38$	$D = 18$
$v(c_4) \geqslant 6$	$\overline{c_6'} = 1 \Rightarrow D = 2$ $\overline{c_6'} = -1 \Rightarrow D = 8$	$D = 3$

$v(\Delta)$	7	8
$v(c_4) = 4$	$D = 68$	$\begin{cases} \overline{\Delta'} = -1 \\ \overline{c_6'} = 1 \end{cases} \Rightarrow D = 8$ $\begin{cases} \overline{\Delta'} = -1 \\ \overline{c_6'} = -1 \end{cases} \Rightarrow D = 2$ $\begin{cases} \overline{\Delta'} = 1 \\ \overline{c_6'} = 1 \end{cases} \Rightarrow D = 32$ $\begin{cases} \overline{\Delta'} = 1 \\ \overline{c_6'} = -1 \end{cases} \Rightarrow D = 38$
$v(c_4) = 5$		$D = 68$
$v(c_4) = 6$		$\overline{c_6'} = 1 \Rightarrow D = 32$ $\overline{c_6'} = -1 \Rightarrow D = 38$
$v(c_4) \geqslant 7$		$\overline{c_6'} = 1 \Rightarrow D = 2$ $\overline{c_6'} = -1 \Rightarrow D = 8$

$v(\Delta)$	9	10	11
$v(c_4)=4$	$D=16$	$\overline{c_6{}'}=1\Rightarrow D=38$ $\overline{c_6{}'}=-1\Rightarrow D=32$	$\overline{c_6{}'}=1\Rightarrow D=38$ $\overline{c_6{}'}=-1\Rightarrow D=32$
$v(c_4)=5$	$v(c_6)=8\Rightarrow D=11$ $v(c_6)>8\Rightarrow D=24$		
$v(c_4)=6$		$\overline{c_4{}'}=-1\Rightarrow D=11$ $\overline{c_4{}'}=1\Rightarrow D=50$	
$v(c_4)=7$		$D=50$	
$v(c_4)\geqslant 8$		$D=11$	

$v(\Delta)$	12	13	14
$v(c_4)=4$	$D=2$		
$v(c_4)=6$	$\overline{c_4{}'}=1\Rightarrow D=16$ $\overline{c_4{}'}=-1\Rightarrow D=18$	$D=68$	$\overline{\Delta'}=-1\Rightarrow D=11$ $\overline{\Delta'}=1\Rightarrow D=50$
$v(c_4)=7$	$D=16$		$D=68$
$v(c_4)=8$	$D=2$		$D=50$
$v(c_4)\geqslant 9$	$D=2$		$D=11$

$v(\Delta)$	15	16	17	18
$v(c_4)=6$	$D=18$	$D=50$	$D=50$	$D=3$
$v(c_4)=7$	$v(c_6)=11\Rightarrow D=11$ $v(c_6)>11\Rightarrow D=24$			

II. Démonstrations

Dans toute la suite on désignera par K_{nr} l'extension non ramifiée maximale de K contenue dans $\overline{K}$. On notera encore v le prolongement à $\overline{K}$ de la valuation de K.

Rappel ([Kr4], p. 411). Soient N une extension finie de K_{nr} et M une extension galoisienne finie de N. La différente de l'extension M/N s'obtient de la façon suivante : soit $(G_i)_{i\geqslant 0}$ la suite des sous-groupes de ramification de l'extension M/N. Si π est une uniformisante de M, le groupe G_i est le sous-groupe du groupe de Galois $\mathrm{Gal}(M/N)$ formé des éléments σ tels que

$$v\big(\sigma(\pi)-\pi\big) \geqslant \frac{i+1}{[M:K_{nr}]},$$

où $[M:K_{nr}]$ est le degré de M sur K_{nr}. Le groupe G_i est réduit à l'élément neutre si i est assez grand. On a $G_0=\mathrm{Gal}(M/N)$ et G_1 est le p-sous-groupe de Sylow de $\mathrm{Gal}(M/N)$. La différente de l'extension M/N est alors la puissance γ-ième de l'idéal de valuation de M, où

$$\gamma = \sum_{i\geqslant 0}\big(|G_i|-1\big). \tag{1}$$

Si le degré de l'extension M/N est premier à p, on a donc

$$\gamma = |G_0|-1. \tag{2}$$

II.1. Le théorème 1

On a par hypothèse $v(j)<0$. Il existe donc une unique extension minimale L de K, de degré au plus 2 sur K, sur laquelle E est isomorphe à la courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$, où q est l'élément entier de K^* défini par l'égalité (cf. [Se3], IV, p. 29-30, ou [Si2], p. 355-357) :

$$j = \frac{1}{q}+744+196884q+\cdots. \tag{3}$$

Rappelons le lemme suivant (cf. [Se1], p. 276, si E a réduction multiplicative) :

Lemme 1. *On a* $L=K\big(\sqrt{-c_6}\big)$.

Démonstration : La courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$ admet un modèle de Weierstrass de la forme

$$y^2 = x^3-\frac{c_4(q)}{48}x-\frac{c_6(q)}{864},$$

tel que l'on ait (cf. *loc. cit.*)

$$-c_6(q)\equiv 1-504q \text{ mod. } q^2. \tag{4}$$

Les courbes elliptiques E et $\mathbb{G}_m/q^{\mathbb{Z}}$ étant isomorphes sur L, il existe un élément u de L tel que l'on ait

$$c_4 = u^4 c_4(q) \quad \text{et} \quad c_6 = u^6 c_6(q).$$

On a $L = K(u)$ et u^2 appartient à K. Par suite, on a l'égalité

$$L = K\left(\sqrt{\frac{c_6}{c_6(q)}}\right).$$

Par ailleurs, d'après la congruence (4), $-c_6(q)$ est un carré dans K. Cela entraîne le lemme.

Choisissons une racine ℓ-ième $q^{1/\ell}$ de q dans $\overline{K}$.

Proposition 2. *1) Supposons que E ait réduction de type multiplicatif sur K. Alors, on a $K_{nr}(E_\ell) = K_{nr}\big(q^{1/\ell}\big)$.*
2) Supposons que E ait réduction de type additif sur K. Alors, $-c_6$ n'est pas un carré dans K_{nr} et l'on a $K_{nr}(E_\ell) = K_{nr}\big(\sqrt{-c_6}, q^{1/\ell}\big)$.

Démonstration : Soit μ_ℓ le sous-groupe des racines ℓ-ièmes de l'unité de $\overline{K}$. Puisque E est isomorphe à la courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$ sur L, on a l'égalité

$$L(E_\ell) = L\big(\mu_\ell, q^{1/\ell}\big). \tag{5}$$

(La preuve de la formule (5) est la même que celle de l'égalité (4) p. 413 de [Kr4] ; le fait que, dans notre situation, ℓ soit distinct de p n'intervient pas.)

Supposons que E ait réduction multiplicative sur K. Alors, L est une extension non ramifiée de K (cf. [Si2], th. 14.1). D'après (5), on a donc $K_{nr}(E_\ell) = K_{nr}\big(\mu_\ell, q^{1/\ell}\big)$. Puisque ℓ est distinct de p, le groupe μ_ℓ est contenu dans K_{nr} ; d'où l'assertion 1).

Supposons que E ait réduction additive sur K. Dans ce cas, L est une extension ramifiée de K (cf. *loc. cit.*). D'après le lemme 1, $-c_6$ n'est donc pas un carré dans K_{nr}. Par ailleurs, il résulte du lemme 1 et de l'égalité (5) que $K_{nr}(E_\ell)$ est contenu dans $K_{nr}\big(\sqrt{-c_6}, q^{1/\ell}\big)$. Inversement, démontrons l'inclusion

$$K_{nr}\big(\sqrt{-c_6}, q^{1/\ell}\big) \subseteq K_{nr}(E_\ell). \tag{6}$$

Considérons pour cela le caractère quadratique ε associé à l'extension $K_{nr}\big(\sqrt{-c_6}\big)/K_{nr}$. La courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$ possède un point d'ordre ℓ rationnel sur K_{nr} (cf. [Se3], IV, p. 31, en tenant compte du fait que μ_ℓ est contenu dans K_{nr}). Puisque les courbes elliptiques E et $\mathbb{G}_m/q^{\mathbb{Z}}$ sont isomorphes sur $K_{nr}\big(\sqrt{-c_6}\big)$, elles se déduisent l'une de l'autre par torsion par le caractère ε. On déduit de là qu'il existe une base de E_ℓ dans laquelle la représentation donnant l'action de $\mathrm{Gal}(\overline{K}/K_{nr})$ sur E_ℓ s'écrit matriciellement sous la forme $\begin{pmatrix} \varepsilon & * \\ 0 & \varepsilon \end{pmatrix}$. Par conséquent, si σ est un élément de $\mathrm{Gal}\big(\overline{K}/K_{nr}\big(E_\ell\big)\big)$, on a $\varepsilon(\sigma) = 1$, autrement dit, σ fixe

$\sqrt{-c_6}$. D'après (5), σ fixe aussi $q^{1/\ell}$, ce qui prouve l'inclusion (6), puis l'assertion 2). D'où la proposition.

Notons n_ℓ le degré de l'extension $K_{nr}(E_\ell)/K_{nr}$.

Corollaire 1. *1) Si E a réduction de type multiplicatif sur K, on a*

$$n_\ell = \begin{cases} 1 & \text{si } \ell \text{ divise } v(j) \\ \ell & \text{si } \ell \text{ ne divise pas } v(j). \end{cases} \tag{7}$$

2) Si E a réduction de type additif sur K, on a

$$n_\ell = \begin{cases} 2 & \text{si } \ell \text{ divise } v(j) \text{ ou bien si } \ell = 2 \\ 2\ell & \text{si } \ell \text{ ne divise pas } v(j) \text{ et } \ell \neq 2. \end{cases} \tag{8}$$

Démonstration : D'après (3), on a $v(j) = -v(q)$. Puisque ℓ et p sont distincts, q est une puissance ℓ-ième dans K_{nr} si et seulement si ℓ divise $v(q)$. Par ailleurs, si $\ell = 2$, on a $p \geqslant 3$, et dans ce cas il existe une unique extension quadratique de K_{nr}. Compte tenu de ces remarques, le corollaire est une conséquence directe de la proposition 2.

Démonstration du théorème 1

1) Supposons que E ait réduction multiplicative sur K. Les formules (2) et (7) entraînent alors l'assertion (a) du théorème.

2) Supposons que E ait réduction additive sur K.

2.1) Si l'on a $p \neq 2$, le théorème résulte directement des formules (2) et (8).

2.2) Supposons $p = 2$. Il résulte de l'inégalité $v(j) < 0$, que l'on a (cf. [Pa], p. 129)

$$v(c_6) = 6 \quad \text{ou bien} \quad v(c_6) = 9.$$

Notons D' l'entier tel que la différente de l'extension $K_{nr}(E_\ell)/K_{nr}\big(\sqrt{-c_6}\big)$ soit la puissance D'-ième de l'idéal de valuation de $K_{nr}(E_\ell)$. Soit D'' l'analogue de D' en ce qui concerne la différente de l'extension $K_{nr}\big(\sqrt{-c_6}\big)/K_{nr}$.

Lemme 2. *On a*

$$D'' = \begin{cases} 2 & \text{si } v(c_6) = 6 \\ 3 & \text{si } v(c_6) = 9. \end{cases}$$

Démonstration : Posons $c_6' = c_6 2^{-v(c_6)}$. Soient $(H_i)_{i \geqslant 0}$ la suite des sous-groupes de ramification de l'extension $K_{nr}\big(\sqrt{-c_6}\big)/K_{nr}$ et σ l'élément non trivial du groupe de Galois de $K_{nr}\big(\sqrt{-c_6}\big)$ sur K_{nr}. L'indice de ramification absolu de K étant égal à 1, le groupe H_3 est trivial $\big($cf. [Se2], p. 79, 3) alinéa c)$\big)$.

Supposons $v(c_6) = 6$. On a dans ce cas $K_{nr}\big(\sqrt{-c_6}\big) = K_{nr}\big(\sqrt{-c_6'}\big)$. On a l'égalité $v\big(\sigma(\sqrt{-c_6'}) - \sqrt{-c_6'}\big) = 1$, ce qui entraîne que H_2 est trivial (cf. *loc. cit.*, p. 69, lemme 1). D'après la formule (1) on a donc $D'' = 2$.

Supposons $v(c_6) = 9$. On a alors $K_{nr}\big(\sqrt{-c_6}\big) = K_{nr}\big(\sqrt{-2c_6'}\big)$. L'élément $\pi = \sqrt{-2c_6'}$ est une uniformisante de $K_{nr}\big(\sqrt{-c_6}\big)$, et l'on a $v\big(\sigma(\pi) - \pi\big) = 3/2$. On en déduit que H_2 est d'ordre 2, puis que $D'' = 3$. D'où le lemme.

Supposons que ℓ divise $v(j)$. D'après (8), on a $n_\ell = 2$ et $K_{nr}(E_\ell) = K_{nr}\big(\sqrt{-c_6}\big)$. On a donc $D = D''$ et le résultat dans ce cas (lemme 2).

Supposons que ℓ ne divise pas $v(j)$. On a $\ell \neq 2$ et le degré de $K_{nr}(E_\ell)$ sur $K_{nr}\big(\sqrt{-c_6}\big)$ est égal à ℓ. On a par transitivité des différentes $D = D' + \ell D''$ (cf. *loc. cit.*, p. 60, prop. 8). L'égalité $D' = \ell - 1$ (car $\ell \neq p$) et le lemme 2 entraînent alors le résultat.

Cela termine la démonstration du théorème 1.

II.2. Le théorème 2

1) Supposons $\ell \neq 2$. Puisque ℓ est distinct de p, $K_{nr}(E_\ell)$ est l'extension minimale de K_{nr} sur laquelle E acquiert bonne réduction ([Og], p. 6, prop.). Par ailleurs, p étant supérieur ou égal à 5, l'extension $K_{nr}(E_\ell)/K_{nr}$ est modérément ramifiée de degré m ([Kr2], prop. 1). D'après la formule (2), on a donc $D = m - 1$.

2) Supposons $\ell = 2$. Notons d le degré de l'extension $K_{nr}(E_2)/K_{nr}$. D'après la proposition de [Og] p. 6, on a

$$d = m \quad \text{ou} \quad d = \frac{m}{2}.$$

2.1) Supposons que $v(\Delta)$ soit impair. On a alors $v(\Delta) \in \{3, 9\}$ (cf. [Ta], p. 46), puis $m = 4$. Puisque d divise 6, on a donc $d = 2$, et d'après la formule (2), on a $D = 1$.

2.2) Supposons que $v(\Delta)$ soit pair. Dans ce cas, Δ est un carré dans K_{nr}, ce qui entraîne $d = 1$ ou $d = 3$. Par ailleurs, on a $v(\Delta) \in \{2, 4, 6, 8, 10\}$ (cf. *loc. cit.*). Si $v(\Delta) \neq 6$, on a $m \in \{3, 6\}$, d'où $d = 3$, et par suite $D = 2$. Si $v(\Delta) = 6$, on a $m = 2$, puis $d = 1$, ce qui conduit à $D = 0$. D'où le théorème 2.

II.3. Les théorèmes 3 et 4

II.3.1. Préliminaires

Soit r un nombre premier impair et distinct de p. On désignera désormais par

. L l'extension minimale de K_{nr} sur laquelle E acquiert bonne réduction. On a l'égalité $L = K_{nr}(E_r)$ ([Og], p. 6, prop.) ;

. Φ le groupe de Galois $\mathrm{Gal}(L/K_{nr})$ (cf. [Se1], p. 311-312 et [Kr2]) ;

. $(G_i)_{i \geqslant 0}$ la suite des sous-groupes de ramification de l'extension L/K_{nr}. On a $G_0 = \Phi$. Pour tout $i \geqslant 0$, G_i est un sous-groupe distingué de Φ qui contient G_{i+1} ;

. I l'ensemble des entiers $i \geqslant 1$ tels que G_i ne soit pas le groupe réduit à l'élément neutre. C'est un ensemble fini ; plus précisément, on a $\big($cf. [Se2], p. 79, 3) alinéa c)$\big)$

$$|G_i| = 1 \quad \text{dès que} \quad i > \frac{|\Phi|}{p-1}; \tag{9}$$

. δ l'invariant sauvage du $\mathrm{Gal}(\overline{K}/K_{nr})$-module E_r (cf. [Og], p. 2-4). On a

$$\delta = \sum_{i\in I} \frac{|G_i|}{|G_0|} \dim_{\mathbb{Z}/r\mathbb{Z}}\big(E_r/E_r^{G_i}\big), \tag{10}$$

où $E_r^{G_i}$ est l'ensemble des points de E_r fixés par G_i. D'après le théorème 1 de *loc. cit.* δ ne dépend pas du nombre premier r choisi.

Lemme 3. *On a l'égalité*

$$\delta|\Phi| = 2\ \sum_{i\in I} |G_i|.$$

Démonstration : Les deux membres de l'égalité à démontrer étant indépendants de r, on peut supposer que l'on a $r \geqslant 5$. Soit i un élément de I. Montrons que $E_r^{G_i}$ est le groupe trivial. Supposons pour cela qu'il existe un point P non nul de E_r fixé par G_i. D'après la proposition de [Og], p. 6, on a $L = K_{nr}(P)$. On déduit de là que G_i est réduit à l'élément neutre, ce qui conduit à une contradiction et prouve notre assertion. Le fait que $G_0 = \Phi$, et que E_r soit de dimension 2 sur $\mathbb{Z}/r\mathbb{Z}$, entraînent alors le lemme.

L'invariant δ peut se calculer en utilisant la formule de Ogg (cf. [Og], th. 2) : soit n le nombre de composantes connexes géométriques de la fibre spéciale du modèle de Néron de E. Alors, on a

$$v(\Delta) = n + \delta + 1. \tag{11}$$

Cette formule a été démontrée par Ogg dans *loc. cit.* si p est distinct de 2. Le cas général a par la suite été prouvé par Saito ([Sa]).

II.3.2. Démonstration du théorème 3

Les invariants c_4, c_6 et Δ étant ceux associés à un modèle minimal de E sur K, $\big(v(\Delta), v(c_6)\big)$ est l'un des couples intervenant dans les tableaux figurant dans l'énoncé du théorème 3 (cf. [Kr2], p. 365).

II.3.2.1. Cas où $\ell \geqslant 5$

Notons O_K l'anneau des entiers de K.

A) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(\Delta), v(c_6)\big) = (3,3)$ et la congruence $4x^3 - (c_4/3)x - c_6/27 \equiv 0$ mod. 9 a une solution dans O_K ;
. $\big(v(\Delta), v(c_6)\big) = (9,6)$ et la congruence $4x^3 - (c_4/27)x - c_6/729 \equiv 0$ mod. 9 a une solution dans O_K ;
. $\big(v(\Delta), v(c_6)\big) \in \big\{(3, \geqslant 5), (9, \geqslant 8)\big\}$.

On a $|\Phi| = 4$ ([Kr2], cor. p. 355-356) et donc G_1 est trivial ; d'où $D = 3$ $\big($formule (2)$\big)$.

B) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(\Delta), v(c_6)\big) = (3,3)$ et la congruence $4x^3 - (c_4/3)x - c_6/27 \equiv 0 \bmod. 9$ n'a pas de solution dans O_K ;

. $\big(v(\Delta), v(c_6)\big) = (9,6)$ et la congruence $4x^3 - (c_4/27)x - c_6/729 \equiv 0 \bmod. 9$ n'a pas de solution dans O_K ;

. $\big(v(\Delta), v(c_6)\big) \in \big\{(3,4), (5,3), (9,7), (11,6)\big\}$.

Si $\big(v(\Delta), v(c_6)\big) \in \big\{(3,3), (3,4)\big\}$ le type de Néron de E est II ([Pa], p. 126 et [Kr2], p. 356), et l'on a ainsi $n = 1$ ([Ta], p. 46) ; si $\big(v(\Delta), v(c_6)\big) \in \big\{(9,6), (9,7)\big\}$, E de type est IV* et l'on a $n = 7$; si $\big(v(\Delta), v(c_6)\big) = (5,3)$, E est de type IV et $n = 3$; si $\big(v(\Delta), v(c_6)\big) = (11,6)$, E est de type II* et $n = 9$. D'après la formule (11), on constate que sous l'hypothèse B), l'on a $\delta = 1$.

Par ailleurs, le groupe Φ est d'ordre 12. D'après le lemme 3, on a donc $\sum_{i\in I} |G_i| = 6$. Puisque le groupe G_1 est d'ordre 3, on déduit de là que l'on a $|G_2| = 3$ et $|G_i| = 1$ si $i \geqslant 3$. La formule (1) conduit alors à $D = 15$.

C) Supposons que l'on ait

. $\big(v(\Delta), v(c_6)\big) \in \big\{(4,3), (12,8)\big\}$.

Si $\big(v(\Delta), v(c_6)\big) = (4,3)$, E est de type II, et l'on a $n = 1$. Si $\big(v(\Delta), v(c_6)\big) = (12,8)$, E est de type II* et par suite $n = 9$. D'après la formule (11), on a donc $\delta = 2$.

On a dans ce cas $|\Phi| = 3$. D'après le lemme 3, on a ainsi $\sum_{i\in I} |G_i| = 3$. Le groupe G_1 est d'ordre 3. On déduit de là que G_2 est trivial, puis que $D = 4$.

D) Supposons que l'on ait

. $\big(v(\Delta), v(c_6)\big) \in \big\{(5,4), (7,5), (11,7), (13,8)\big\}$.

Si $\big(v(\Delta), v(c_6)\big) = (5,4)$, E est de type II et $n = 1$. Si $\big(v(\Delta), v(c_6)\big) = (7,5)$, E de type est IV et $n = 3$. Si $\big(v(\Delta), v(c_6)\big) = (11,7)$, E est de type IV* et $n = 7$. Si $\big(v(\Delta), v(c_6)\big) = (13,8)$, E est de type II* et $n = 9$. Dans tous ces cas on a donc $\delta = 3$.

Le groupe Φ est d'ordre 12 ; d'où l'égalité $\sum_{i\in I} |G_i| = 18$. On déduit de là que l'on a $|G_i| = 3$ si $1 \leqslant i \leqslant 6$ et $|G_i| = 1$ si $i \geqslant 7$; d'où $D = 23$.

E) Supposons que l'on ait :

. $\big(v(\Delta), v(c_6)\big) \in \big\{(6,3), (6, \geqslant 6)\big\}$.

Dans ce cas, on a $|\Phi| = 2$, et donc le groupe G_1 est trivial ; d'où $D = 1$.

F) Supposons que l'on ait

. $\big(v(\Delta), v(c_6)\big) \in \big\{(6,5),(10,6)\big\}$.

Si $\big(v(\Delta), v(c_6)\big) = (6,5)$, E est de type IV, et l'on a $n = 3$. Si $\big(v(\Delta), v(c_6)\big) = (10,6)$, E est de type IV* et l'on a $n = 7$. On a donc $\delta = 2$.

Le groupe Φ est d'ordre 6. On a ainsi $\sum_{i\in I} |G_i| = 6$. Puisque $|G_1| = 3$, on en déduit que $|G_2| = 3$, et $|G_i| = 1$ si $i \geqslant 3$; d'où $D = 9$.

Cela termine la démonstration de l'assertion (a) du théorème 3.

II.3.2.2. Cas où $\ell = 2$

Soit $\Delta^{1/4}$ une racine quatrième de Δ dans $\overline{K}$. On a l'égalité ([Kr2], p. 362, cor.)

$$L = K_{nr}\big(E_2, \Delta^{1/4}\big). \tag{12}$$

Lemme 4. *Soit s le degré de l'extension $L/K_{nr}(E_2)$. On a*

$$s = \begin{cases} 1 & \textit{si } 4 \textit{ divise } v(\Delta) \\ 2 & \textit{si } 4 \textit{ ne divise pas } v(\Delta). \end{cases}$$

Démonstration : Si 4 divise $v(\Delta)$, alors Δ est une puissance quatrième dans K_{nr}, et d'après l'égalité (12), on a $L = K_{nr}(E_2)$, i.e. on a $s = 1$. Supposons $v(\Delta) \not\equiv 0 \bmod 4$. D'après la proposition de [Og] p. 6, on a $s \leqslant 2$. Il suffit donc de prouver que les corps L et $K_{nr}(E_2)$ sont distincts. Supposons le contraire, autrement dit que $\Delta^{1/4}$ appartienne à $K_{nr}(E_2)$. Puisque 4 ne divise pas $v(\Delta)$, $\Delta^{1/4}$ n'est pas dans K_{nr}, et donc 2 divise le degré $[K_{nr}(\Delta^{1/4}) : K_{nr}]$. D'après l'hypothèse faite, 2 divise donc $[K_{nr}(E_2) : K_{nr}]$, et Δ n'est pas un carré dans K_{nr}. Il en résulte que $[K_{nr}(\Delta^{1/4}) : K_{nr}] = 4$, puis que 4 divise $[K_{nr}(E_2) : K_{nr}]$. Cela conduit à une contradiction car $[K_{nr}(E_2) : K_{nr}]$ divise 6. D'où le lemme.

Notons alors D' l'exposant de la différente de l'extension L/K_{nr}. D'après la formule de transitivité des différentes, on a $D' = sD + s - 1$, autrement dit, on a

$$D = \begin{cases} D' & \text{si } 4 \text{ divise } v(\Delta) \\ (D'-1)/2 & \text{si } 4 \text{ ne divise pas } v(\Delta). \end{cases}$$

La valeur de l'entier D' est donnée dans l'énoncé de l'assertion (a) du théorème 3 qui a été démontrée ci-dessus. L'on vérifie alors les valeurs de D indiquées dans les tableaux intervenant dans l'assertion (b) du théorème. Cela termine sa démonstration.

II.3.3. Démonstration du théorème 4

On suppose désormais $K = \mathbb{Q}_2$. Le groupe Φ est isomorphe à un sous-groupe de $\mathbb{S}L_2(\mathbb{F}_3)$ ([Se1], p. 312). On utilisera à plusieurs reprises le lemme suivant :

Lemme 5. *Le groupe $\mathbb{S}L_2(\mathbb{F}_3)$ ne possède pas de sous-groupe distingué d'ordre 4.*

Démonstration : Il existe un unique 2-sous-groupe de Sylow dans $\mathbb{S}L_2(\mathbb{F}_3)$. Il est d'ordre 8 isomorphe au groupe quaternionien. Il en résulte que $\mathbb{S}L_2(\mathbb{F}_3)$ a exactement trois sous-groupes d'ordre 4, qui sont cycliques. Ces trois sous-groupes sont engendrés respectivement par $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ et $\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$. On vérifie ensuite qu'ils ne sont pas distingués dans $\mathbb{S}L_2(\mathbb{F}_3)$. D'où le lemme.

Démontrons maintenant le théorème 4. Les invariants c_4, c_6 et Δ étant ceux associés à un modèle minimal de E sur $\mathbb{Q}_2$, $\big(v(c_4), v(\Delta)\big)$ est l'un des couples intervenant dans l'énoncé du théorème 4 (cf. [Kr2], p. 374).

A) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (4, 4)$ et $\overline{c'_4} = -1$, $\overline{c'_6} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (\geqslant 6, 4)$ et $\overline{c'_6} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (4, 8)$ et $\overline{\Delta'} = -1$, $\overline{c'_6} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (\geqslant 7, 8)$ et $\overline{c'_6} = 1$.

On a $|\Phi| = 3$ (*loc. cit.*, cor. p. 357-358) et donc G_1 est trivial ; d'où $D = 2$ $\big($formule(2)$\big)$.

B) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (4, 4)$ et $\overline{c'_4} = -1$, $\overline{c'_6} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (\geqslant 6, 4)$ et $\overline{c'_6} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (4, 8)$ et $\overline{\Delta'} = -1$, $\overline{c'_6} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (\geqslant 7, 8)$ et $\overline{c'_6} = -1$.

On a $|\Phi| = 6$. D'après l'Appendice, on a $\delta = 2$. On a donc $\sum_{i \in I} |G_i| = 6$ (lemme 3). Puisque le groupe G_1 est d'ordre 2, on déduit de là que l'on a $|G_i| = 2$ pour $1 \leqslant i \leqslant 3$ et $|G_i| = 1$ si $i \geqslant 4$. D'après la formule (1), on a donc $D = 8$.

C) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (4, 4)$ et $\overline{c'_4} = 1$, $\overline{c'_6} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (5, 4)$ et $\overline{c'_6} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (4, 8)$ et $\overline{\Delta'} = 1$, $\overline{c'_6} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (6, 8)$ et $\overline{c'_6} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (4, 10)$ et $\overline{c'_6} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (4, 11)$ et $\overline{c'_6} = -1$.

Le groupe Φ est d'ordre 24 et est isomorphe au groupe $\mathbb{S}L_2(\mathbb{F}_3)$. Par ailleurs, on a $\delta = 1$. On a ainsi l'égalité $\sum_{i \in I} |G_i| = 12$. Le groupe G_1 est d'ordre 8. Puisque les sous-groupes

G_i sont distingués dans $G_0 = \Phi$, on déduit alors du lemme 5 que l'on a $|G_2| = |G_3| = 2$, puis que $|G_i| = 1$ si $i \geqslant 4$. Cela conduit à $D = 32$.

D) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (4,4)$ et $\overline{c'_4} = 1$, $\overline{c'_6} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (5,4)$ et $\overline{c'_6} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (4,8)$ et $\overline{\Delta'} = 1$, $\overline{c'_6} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (6,8)$ et $\overline{c'_6} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (4,10)$ et $\overline{c'_6} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (4,11)$ et $\overline{c'_6} = 1$.

On a $|\Phi| = 24$ et $\delta = 2$. On a donc

$$\sum_{i \in I} |G_i| = 24. \tag{13}$$

Prouvons que l'on a

$$|G_2| = 2. \tag{14}$$

Remarquons d'abord que l'on a l'égalité $G_2 = G_3$ (cf. [Se2], p. 79, 3) alinéa e)). Puisque G_1 est d'ordre 8, l'ordre de G_2 divise 8. Supposons que l'on ait $|G_2| = 8$. On a alors $G_1 = G_2 = G_3$, et l'égalité (13) implique $|G_4| = 1$. Par ailleurs, G_1 est isomorphe au 2-sous-groupe de Sylow de $\mathbb{S}L_2(\mathbb{F}_3)$, qui est quaternionien d'ordre 8. Ainsi G_2 possède un élément s d'ordre 4. D'après *loc. cit.*, s^2 appartient à G_4, et en particulier, G_4 n'est pas trivial. On obtient ainsi une contradiction et donc $|G_2| \neq 8$. D'après le lemme 5 le groupe G_2 n'est pas d'ordre 4, et la formule (13) entraîne $|G_2| \neq 1$. D'où l'égalité (14).

On déduit alors de (13) et (14) que l'on a $|G_i| = 2$ pour $2 \leqslant i \leqslant 9$, et $|G_i| = 1$ si $i \geqslant 10$. On obtient ainsi $D = 38$.

E) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (4,6)$ et $\overline{c'_4} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (6,12)$ et $\overline{c'_4} = 1$;
. $\big(v(c_4), v(\Delta)\big) \big\{(4,9), (7,12)\big\}$.

On a $|\Phi| = 8$ et $\delta = 3$, de sorte que $\sum_{i \in I} |G_i| = 12$. Le groupe G_1 est d'ordre 8. Par ailleurs, on a $|G_2/G_3| \leqslant 2$ ([Se2], p. 79, 3) alinéa e)). On déduit de là que l'on a $|G_2| = |G_3| = 2$ et $|G_i| = 1$ si $i \geqslant 4$. D'où $D = 16$.

F) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (4, 6)$ et $\overline{c_4'} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (6, 12)$ et $\overline{c_4'} = -1$;
. $\big(v(c_4), v(\Delta)\big)\big\{(5, 6), (6, 15)\big\}$.

On a $|\Phi| = 8$, $\delta = 4$ et $\sum_{i\in I} |G_i| = 16$. On a $G_1 = \Phi$, et G_1 est donc d'ordre 8 isomorphe au groupe quaternionien. Vérifions que l'on a

$$|G_2| = 2. \tag{15}$$

On remarque pour cela que $|G_2| \neq 8$: sinon G_3 est trivial, ce qui contredit l'inégalité $|G_2/G_3| \leqslant 2$ (*loc. cit.*). Supposons $|G_2| = 4$. Puisque les entiers $i \geqslant 1$ tels que $G_i \neq G_{i+1}$ sont congrus entre eux modulo 2 (*loc. cit.*, p. 77, prop. 11), on a donc $G_2 = G_3$, ce qui entraîne que G_4 est trivial. Par ailleurs, G_2 étant un sous-groupe d'ordre 4 de G_1, il est cyclique. Si s est un élément d'ordre 4 de G_2, s^2 appartient à G_4 $\big($*loc. cit.*, p. 79, 3), e)$\big)$. Cela conduit à une contradiction et implique l'égalité (15). On déduit de là que $|G_i| = 2$ si $2 \leqslant i \leqslant 5$ et $|G_i| = 1$ si $i \geqslant 6$. Cela entraîne $D = 18$.

G) Supposons que l'on ait

. $\big(v(c_4), v(\Delta)\big) \in \big\{(\geqslant 6, 6), (6, 18)\big\}$.

On a $|\Phi| = 2$, $\delta = 4$ et $\sum_{i\in I} |G_i| = 4$. Le groupe G_1 étant d'ordre 2, il en résulte que $|G_2| = 2$, puis que $|G_i| = 1$ si $i \geqslant 3$. Par suite $D = 3$.

H) Supposons que l'on ait

. $\big(v(c_4), v(\Delta)\big) \in \big\{(4, 7), (5, 8), (6, 13), (7, 14)\big\}$.

On a $|\Phi| = 24$ et $\delta = 5$. On a ainsi

$$\sum_{i\in I} |G_i| = 60. \tag{16}$$

Prouvons que l'on a

$$|G_i| = 8 \quad \text{si} \quad 1 \leqslant i \leqslant 5, \quad |G_i| = 2 \quad \text{si} \quad 6 \leqslant i \leqslant 15, \quad \text{et} \quad |G_i| = 1 \quad \text{si} \quad i \geqslant 16. \tag{17}$$

On remarque d'abord que l'on a les égalités

$$G_1 = G_2 = G_3 \quad \text{et} \quad G_4 = G_5. \tag{18}$$

En effet, supposons $G_1 \neq G_2$. Puisque G_1 est d'ordre 8, il résulte du lemme 5 que $|G_2| = 2$. Cela entraîne les inégalités $|G_i| \leqslant 2$ si $i \geqslant 2$; le fait que G_i soit trivial si $i \geqslant 25$ $\big($formule (9)$\big)$ contredit alors (16) : d'où $G_1 = G_2$. Par ailleurs, l'alinéa 3) e) p. 79 de [Se2] entraîne $G_2 = G_3$ et $G_4 = G_5$. D'où les égalités (18).

Vérifions que l'on a l'égalité

$$G_3 = G_4. \tag{19}$$

On considère pour cela un élément s d'ordre 3 de Φ et un élément t d'ordre 4 de G_3 (un tel élément t existe, car d'après (18), G_3 est quaternionien d'ordre 8). Le corollaire 1, p. 77 de [Se2], appliqué avec $i = 3$, implique que $sts^{-1}t^{-1}$ appartient à G_4. En identifiant Φ et $\mathbb{S}L_2(\mathbb{F}_3)$, on constate que quelque soit le choix de s et t, l'élément $sts^{-1}t^{-1}$ est d'ordre 4. On déduit de là que l'ordre de G_4 est divisible par 4, ce qui implique $|G_4| = 8$ (lemme 5) et l'égalité (19).

On remarque ensuite que l'on a

$$G_6 = G_7. \tag{20}$$

En effet, si $G_6 \neq G_7$, les entiers $i \geqslant 1$ tels que $G_i \neq G_{i+1}$ sont pairs ([Se2], p. 77, prop. 11), et le groupe G_1 devrait alors être cyclique, ce qui n'est pas $\big($cf. *loc. cit.*, p. 79, alinéa f$\big)$.

On déduit de là que

$$G_5 \neq G_6. \tag{21}$$

En effet, supposons $G_5 = G_6$. D'après les égalités (18) à (20) les groupes G_i sont alors d'ordre 8 pour $1 \leqslant i \leqslant 7$. L'égalité (16) implique $|G_{10}| = 1$. Puisque l'on a $G_1 = G_5$, le groupe G_5 possède un élément σ d'ordre 4. L'élément σ^2, qui est d'ordre 2, appartient à G_{11} $\big($cf. *loc. cit.*, p. 79, alinéa e$\big)$, ce qui conduit à une contradiction et prouve (21).

D'après (21) et le lemme 5 on a donc $|G_6| = 2$. L'égalité (16) entraîne alors les formules (17). On obtient ainsi $D = 68$.

I) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (5, 9)$ et $v(c_6) = 8$;

. $\big(v(c_4), v(\Delta)\big) = (7, 15)$ et $v(c_6) = 11$.

Le groupe Φ est cyclique d'ordre 4 et l'on a $\delta = 6$, puis $\sum_{i \in I} |G_i| = 12$. On a $|G_1| = 4$ et $|G_i| = 1$ pour tout $i \geqslant 5$ $\big($formule (9)$\big)$. Il en résulte que $|G_2| \neq 2$, et donc $|G_2| = 4$. Si s est un élément d'ordre 4 de G_2, s^2 appartient à G_4, de sorte que G_4 n'est pas le groupe trivial. Par suite, on a $G_1 = G_2$ et $|G_3| = |G_4| = 2$. D'où $D = 11$.

J) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (5, 9)$ et $v(c_6) > 8$;

. $\big(v(c_4), v(\Delta)\big) = (7, 15)$ et $v(c_6) > 11$.

On a $|\Phi| = 8$, $\delta = 6$, et l'égalité

$$\sum_{i\in I} |G_i| = 24. \tag{22}$$

On a $G_1 = \Phi$. Prouvons que l'on a

$$|G_2| = |G_3| = 4, \quad |G_i| = 2 \quad \text{si} \quad 4 \leqslant i \leqslant 7, \quad \text{et} \quad |G_i| = 1 \quad \text{si} \quad i \geqslant 8. \tag{23}$$

Puisque G_1 n'est pas cyclique, on a $G_{2i} = G_{2i+1}$ pour tout $i \geqslant 1$ (cf. [Se2], p. 77, prop. 11 et p. 79 alinéa f)). On déduit de là que l'on a $G_1 \neq G_2$: en effet, si $G_1 = G_2$, le groupe G_4 est trivial (cf. (22) et le fait que $G_2 = G_3$), et G_2 possède un élément d'ordre 4, ce qui conduit à une contradiction. D'après la formule (9) on a $|G_9| = 1$; l'égalité (22) implique alors $|G_2| = 4$. Il en résulte que G_8 est trivial, puis que $|G_4| \neq 4$: si $|G_4| = 4$, G_4 est cyclique d'ordre 4, ce qui entraîne de nouveau une contradiction. On a ainsi $|G_4| = 2$. D'où les formules (23) et le fait que $D = 24$.

K) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (6, 10)$ et $\overline{c_4'} = -1$;
. $\big(v(c_4), v(\Delta)\big) = (6, 14)$ et $\overline{\Delta'} = -1$;
. $\big(v(c_4), v(\Delta)\big) \in \big\{(\geqslant 8, 10), (\geqslant 9, 14)\big\}$.

On a $|\Phi| = 6$ et $\delta = 4$, d'où $\sum_{i\in I} |G_i| = 12$. Le groupe G_1 est d'ordre 2. On a donc les égalités $|G_i| = 2$ pour $1 \leqslant i \leqslant 6$, ce qui conduit à $D = 11$.

L) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) = (6, 10)$ et $\overline{c_4'} = 1$;
. $\big(v(c_4), v(\Delta)\big) = (6, 14)$ et $\overline{\Delta'} = 1$;
. $\big(v(c_4), v(\Delta)\big) \in \big\{(7, 10), (8, 14), (6, 16), (6, 17)\big\}$.

On a $|\Phi| = 24$, $\delta = 4$, et donc

$$\sum_{i\in I} |G_i| = 48. \tag{24}$$

Vérifions que l'on a les égalités

$$|G_1| = 8, \quad |G_i| = 2 \quad \text{si} \quad 2 \leqslant i \leqslant 21, \quad \text{et} \quad |G_i| = 1 \quad \text{si} \quad i \geqslant 22. \tag{25}$$

Tout revient à démontrer que G_2 est d'ordre 2. Puisque G_1 est d'ordre 8 et non cyclique, on a $G_{2i} = G_{2i+1}$ pour tout $i \geqslant 1$. Supposons $|G_2| = 8$. Dans ce cas, on a $G_1 = G_2$, et G_2 possède un élément t d'ordre 4. Si s est un élément d'ordre 3 de Φ, l'élément $sts^{-1}t^{-1}$

est d'ordre 4 et appartient à G_4 (cf. l'alinéa H) ci-dessus). D'après le lemme 5, on a alors $|G_4| = 8$. On a donc aussi $|G_5| = 8$ et l'on déduit de (24) que le groupe G_{10} est trivial. Cela conduit à une contradiction, car G_5 a un élément d'ordre 4, et G_{11} ne peut donc être trivial. D'où $|G_2| \neq 8$. Puisque $|G_2| \neq 4$ (lemme 5), on a donc $|G_2| = 2$. D'où les formules (25) et le fait que $D = 50$.

M) Supposons que l'on soit dans l'un des cas suivants :

. $\big(v(c_4), v(\Delta)\big) \in \big\{(4, 12), (\geqslant 8, 12)\big\}$.

On a $|\Phi| = 2$ et $\delta = 2$, d'où $\sum_{i \in I} |G_i| = 2$. On a donc $|G_1| = 2$ et $|G_i| = 1$ si $i \geqslant 2$. On obtient dans ce cas $D = 2$.

Cela termine la démonstration du théorème 4.

Appendice

Types de Néron des courbes elliptiques sur $\mathbb{Q}_2$ d'invariant modulaire entier

Soit E une courbe elliptique définie sur $\mathbb{Q}_2$ ayant mauvaise réduction de type additif. Soit v la valuation 2-adique de $\mathbb{Q}_2$. On suppose que l'invariant modulaire j de E vérifie $v(j) \geqslant 0$. Soient c_4, c_6 et Δ les invariants standards associés à un modèle *minimal* de E sur $\mathbb{Q}_2$. Le triplet $\big(v(c_4), v(c_6), v(\Delta)\big)$ ne dépend pas du modèle minimal choisi. On détermine dans cet Appendice le type de Néron de E sur $\mathbb{Q}_2$ en fonction du triplet $\big(c_4, c_6, \Delta\big)$, ainsi que la valeur de l'entier $\delta = v(\Delta) - 1 - n$, où n est le nombre de composantes connexes géométriques de la fibre spéciale du modèle de Néron de E (cf. [Ta], p. 46) , que l'on a utilisée dans la démonstration du théorème 4.

On note

$$c'_4 = \frac{c_4}{2^{v(c_4)}}, \quad c'_6 = \frac{c_6}{2^{v(c_6)}} \quad \text{et} \quad \Delta' = \frac{\Delta}{2^{v(\Delta)}},$$

et l'on désigne par $\overline{c'_4}$, $\overline{c'_6}$ et $\overline{\Delta'}$ les classes modulo $4\mathbb{Z}_2$ respectivement de c'_4, c'_6 et Δ'.

Théorème. *On est dans l'un des cas des tableaux suivants :*

$v(\Delta)$	4				4		4		6	
$v(c_4)$	4				5		$\geqslant 6$		4	
$v(c_6)$	5				5		5		$\geqslant 7$	
$\overline{c_4{}'}$	1	1	-1	-1					1	-1
$\overline{c_6{}'}$	1	-1	1	-1	-1	1	-1	1		
Type de Néron	*II*	*III*	*IV*	*II*	*II*	*III*	*II*	*IV*	*II*	*III*
δ	2	1	0	2	2	1	2	0	4	3

$v(\Delta)$	6	7	8				8	8		8	
$v(c_4)$	$\geqslant 5$	4	4				5	6		$\geqslant 7$	
$v(c_6)$	6	6	6				7	7		7	
$\overline{c_6{}'}$			-1	1	1	-1		-1	1	-1	1
$\overline{\Delta'}$			1	-1	1	-1					
Type de Néron	*II*	*II*	I_0^*	I_0^*	I_1^*	IV^*	*III*	I_0^*	I_1^*	I_0^*	IV^*
δ	4	5	2	2	1	0	5	2	1	2	0

$v(\Delta)$	9	9	10		10	11		12	12		12
$v(c_4)$	4	5	4		$\geqslant 6$	4		4	6		7
$v(c_6)$	6	$\geqslant 8$	6		8	6		6	$\geqslant 10$		9
$\overline{c_4{}'}$									-1	1	
$\overline{c_6{}'}$			1	-1		1	-1				
Type de Néron	I_0^*	III	I_2^*	III^*	I_0^*	I_3^*	II^*	I_4^*	I_2^*	I_3^*	III^*
δ	3	6	2	1	4	2	1	2	4	3	3

$v(\Delta)$	12	13	14	14	14	15	15	16	17	18
$v(c_4)$	$\geqslant 8$	6	6	7	$\geqslant 8$	6	7	6	6	6
$v(c_6)$	9	9	9	10	10	9	$\geqslant 11$	9	9	9
Type de Néron	II^*	I_2^*	I_4^*	III^*	II^*	I_5^*	III^*	I_6^*	I_7^*	I_8^*
δ	2	5	4	5	4	4	6	4	4	4

Démonstration

Le fait que l'on parte d'un modèle minimal de E sur $\mathbb{Q}_2$ implique que le triplet $\big(v(c_4), v(c_6), v(\Delta)\big)$ est l'un de ceux indiqués dans les tableaux ci-dessus (cf. [Kr2], p. 374). Dans tous les cas, l'équation de Weierstrass

$$(W) \qquad y^2 = x^3 - \left(\frac{c_4}{48}\right)x - \frac{c_6}{864},$$

est un modèle entier minimal de E (cf. [Ta]). Afin de déterminer le type de Néron de E, nous allons utiliser principalement l'article de Papadopoulos ([Pa]). Avec les notations de *loc. cit.*, on a

$$a_1 = a_2 = a_3 = 0,\ a_4 = -2^{v(c_4)-4}\left(\frac{c_4'}{3}\right),\ a_6 = -2^{v(c_6)-5}\left(\frac{c_6'}{27}\right),$$

$$b_2 = 0,\ b_4 = -2^{v(c_4)-3}\left(\frac{c_4'}{3}\right),\ b_6 = -2^{v(c_6)-3}\left(\frac{c_6'}{27}\right),\ b_8 = -2^{2v(c_4)-8}\left(\frac{c_4'^2}{9}\right).$$

Étant donnés deux éléments r et t de $\mathbb{Z}_2$, on notera (cf. *loc. cit.*, prop. 1-3, p. 124)

$$A(r,t) = a_6 + ra_4 + r^3 - t^2 \quad \text{et} \quad B(r) = b_8 + 3rb_6 + 3r^2b_4 + 3r^4.$$

A) Supposons $\big(v(c_4), v(c_6), v(\Delta)\big) = (4, 5, 4)$.

Le type de Néron de E est II, III ou IV (*loc. cit.*, p. 129). On utilise la proposition 1 de *loc. cit.* avec $r = 1$ et $t = 1$. On est alors amené à décider si 4 divise $A(1, 1)$. On vérifie pour cela que l'on a

$$A(1, 1) \equiv c'_4 + c'_6 \text{ mod. } 4.$$

On déduit de là que le type de Néron de E est II si l'on a $c'_4 \equiv c'_6$ mod. 4. Supposons maintenant $c'_4 \not\equiv c'_6$ mod. 4. D'après la proposition 2 de *loc. cit.*, utilisée avec $r = 1$, il s'agit alors de décider si $B(1)$ est multiple de 8. On constate que l'on a

$$B(1) \equiv 2(3 - c'_4) \text{ mod. } 8.$$

Ainsi, 8 divise $B(1)$ si et seulement si $c'_4 \equiv -1$ mod. 4. Cela entraîne le résultat.

B) Supposons $\big(v(c_4), v(c_6), v(\Delta)\big) = (\geqslant 5, 5, 4)$.

Le type de Néron de E est II, III ou IV. On a

$$A(0, 1) \equiv c'_6 - 1 \text{ mod. } 4.$$

Il en résulte que si $c'_6 \equiv -1$ mod. 4, le type de Néron de E est II (*loc. cit.*, prop. 1). Supposons $c'_6 \equiv 1$ mod. 4. On a $B(0) = b_8$, de sorte que $B(0)$ est multiple de 8, i.e. le type de Néron de E est IV, si et seulement si $v(c_4) \geqslant 6$ (*loc. cit.*, prop. 2). D'où le résultat dans ce cas.

C) Supposons $\big(v(c_4), v(c_6), v(\Delta)\big) = (4, \geqslant 7, 6)$.

Le type de Néron de E est II ou III. Par ailleurs, on a

$$A(1, 0) = c'_4 + 1 \text{ mod. } 4.$$

Cela entraîne notre assertion (*loc. cit.*, prop. 1).

D) Supposons $\big(v(c_4), v(c_6), v(\Delta)\big) = (4, 6, 8)$.

Le type de Néron de E est I_0^*, I_1^* ou IV^*. Remarquons que l'égalité $c_4^3 - c_6^2 = 1728\Delta$ implique la congruence

$$c'_4 \equiv 5 \text{ mod. } 8. \tag{1}$$

On utilise alors la proposition 3 de *loc. cit.* : on a

$$9B(c'_6) = -c_4'^2 - 8c_6'^2 - 18c'_4c_6'^2 + 27c_6'^4.$$

On vérifie que l'on a la congruence

$$B(c'_6) \equiv 0 \text{ mod. } 32. \tag{2}$$

Par ailleurs, on a

$$27A(c_6', 2) \equiv -2c_6' - 9c_4'c_6' + 27c_6'^3 + 4 \text{ mod. } 16. \tag{3}$$

D'après (1), on a $c_4'^2 \equiv 9$ mod. 16, et de l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on déduit alors que l'on a $9c_4' \equiv -4\Delta' + c_6'^2$ mod. 16. La congruence (3) conduit ainsi à

$$27A(c_6', 2) \equiv 4(3 + \Delta' c_6') \text{ mod. } 16.$$

En particulier, on a $A(c_6', 2) \equiv 0$ mod. 8. Si $\Delta' \equiv -c_6'$ mod. 4, le type de Néron de E est donc I_0^* (*loc. cit*, prop. 3). Si l'on a $\Delta' \equiv c_6'$ mod. 4, la proposition 4 de *loc. cit.*, utilisée avec $r = c_6'$ $\big($cf. (2)$\big)$, entraîne alors le résultat.

E) Supposons $\big(v(c_4), v(c_6), v(\Delta)\big) = (6, 7, 8)$.

Le type de Néron de E est I_0^* ou I_1^*. On constate que l'on a

$$B(2) \equiv 0 \text{ mod. } 32.$$

Par ailleurs, on a

$$A(2, 2) \equiv 4(c_6' - 1) \text{ mod. } 16.$$

D'où notre assertion (*loc. cit.*, prop. 3).

F) Supposons $\big(v(c_4), v(c_6), v(\Delta)\big) = (\geqslant 7, 7, 8)$.

Le type de Néron de E est I_0^* ou IV^*. On a

$$B(0) \equiv \text{ mod. } 32.$$

On vérifie par ailleurs que l'on a

$$A(0, 2) \equiv 4(c_6' - 1) \text{ mod. } 16,$$

ce qui entraîne le résultat (cf. *loc. cit.*).

G) Supposons $\big(v(c_4), v(c_6), v(\Delta)\big) = (4, 6, 10)$.

Le type de Néron de E est I_2^* ou III^*. D'après l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on a les congruences $c_4' \equiv 1$ mod. 8 et $c_4' \equiv c_6'^2$ mod. 16. Par ailleurs, on a

$$9B(c_6') = -c_4'^2 - 8c_6'^{\,2} - 18c_4'c_6'^{\,2} + 27c_6'^{\,4}.$$

On déduit de là que

$$B(c_6') \equiv 0 \text{ mod. } 32.$$

La proposition 4 de *loc. cit.* entraîne alors le résultat.

H) Supposons $\big(v(c_4), v(c_6), v(\Delta)\big) = (4, 6, 11)$.

Le type de Néron de E est I_3^* ou II^*. L'égalité $c_4^3 - c_6^2 = 1728\Delta$ implique de nouveau $c_4' \equiv c_6'^2$ mod. 16 et l'on a encore

$$9B(c_6') = -c_4'^2 - 8{c_6'}^2 - 18c_4'{c_6'}^2 + 27{c_6'}^4.$$

On a donc $B(c_6') \equiv 0$ mod. 32, et l'on conclut comme dans l'alinéa G) ci-dessus.

I) Supposons $\big(v(c_4), v(c_6), v(\Delta)\big) = (6, \geqslant 10, 12)$.

Le type de Néron de E est I_2^* ou I_3^*. On va utiliser dans ce cas l'algorithme de Tate ([Ta], p. 49-51).

I.1) Supposons $c_4' \equiv -1$ mod. 4. Le changement de variables

$$\begin{cases} x = X + 2 \\ y = Y, \end{cases}$$

transforme le modèle initial (W) en l'équation

$$Y^2 = X^3 + 6X^2 + A_4X + A_6,$$

avec

$$A_4 = 12 - \frac{c_4}{48} \quad \text{et} \quad A_6 = -\left(\frac{c_6}{864} + \frac{c_4}{24} - 8\right).$$

On a $v(A_4) = 3$ et $A_6 \equiv 0$ mod. 32. Le polynôme $3T^2 + (A_4/8)T + (A_6/32)$ a ainsi deux racines distinctes modulo 2. Le type de Néron de E est donc I_2^* (cf. *loc. cit.*, p. 50).

I.2) Supposons $c_4' \equiv 1$ mod. 4. Le changement de variables

$$\begin{cases} x = X + 2 \\ y = Y + 4, \end{cases}$$

transforme le modèle (W) en l'équation

$$Y^2 + 8Y = X^3 + 6X^2 + A_4X + A_6,$$

avec

$$A_4 = 12 - \frac{c_4}{48} \quad \text{et} \quad A_6 = -\left(\frac{c_6}{864} + \frac{c_4}{24} + 8\right).$$

On a $A_4 \equiv 0$ mod. 16 et $A_6 \equiv 0$ mod. 32. Le polynôme $3T^2 + (A_4/8)T + (A_6/32)$ a donc une racine double modulo 2. On déduit de là que le type de Néron de E est dans ce cas I_3^* (cf. *loc. cit.*). D'où le résultat.

J) En ce qui concerne les autres cas qui figurent dans les tableaux intervenant dans l'énoncé du théorème, les types de Néron de E se lisent directement dans le tableau IV de [Pa], p. 129.

Cela termine la démonstration du théorème.

Chapitre II

Défaut de semi-stabilité des courbes elliptiques dans le cas non ramifié

Introduction

Étant donné un nombre premier p, soient $\overline{\mathbb{Q}_p}$ une clôture algébrique de $\mathbb{Q}_p$ et K une extension finie de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}_p}$. Soit E une courbe elliptique définie sur K ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire j est entier, i.e. j appartient à l'anneau de valuation de K. Soit K_{nr} l'extension non ramifiée maximale de K contenue dans $\overline{\mathbb{Q}_p}$. Il existe une plus petite extension finie L de K_{nr} sur laquelle E acquiert bonne réduction. Si E_n désigne le sous-groupe des points de n-torsion de $E(\overline{\mathbb{Q}_p})$, on a $L = K_{nr}(E_n)$ pour tout entier $n \geqslant 3$ non divisible par p ([Se-Ta], 2, cor.3). Le groupe de Galois Φ de L sur K_{nr} est connu dans le cas où $p \geqslant 3$ (cf. [Kr2]). Si $p = 2$, le groupe Φ n'est connu que dans certains cas particuliers, par exemple si $K = \mathbb{Q}_2$ (*loc. cit.*). Dans ce chapitre, on détermine Φ dans le cas où K est une extension finie *non ramifiée* de $\mathbb{Q}_2$. Les résultats que l'on obtient permettent de calculer directement l'ordre de Φ en fonction des coefficients d'une équation de Weierstrass minimale de E sur K.

Signalons par ailleurs que ces résultats permettent de compléter, dans le cas non ramifié, ceux obtenus dans le théorème 4 du chapitre I sur la détermination de la différente du corps des points de ℓ-torsion des courbes elliptiques dans le cas où $\ell \neq 2$.

1. Énoncé des résultats

Soit K une extension finie non ramifiée de $\mathbb{Q}_2$. On note v le prolongement à K de la valuation de $\mathbb{Q}_2$. On suppose que v est normée : on a $v(K^*) = \mathbb{Z}$, autrement dit, on a $v(2) = 1$. Étant donné un entier $n \geqslant 1$, on notera μ_n le sous-groupe des racines n-ièmes de l'unité de $\overline{\mathbb{Q}_2}^*$. Soit r le cardinal du corps résiduel k de K. L'ensemble $\mu_{r-1} \cup \{0\}$ est un système de représentants de k.

Soit E une courbe elliptique définie sur K ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire j vérifie $v(j) \geqslant 0$. Soient c_4, c_6 et Δ les invariants standard associés à un modèle minimal de E sur K. Leur valuation ne dépend pas du modèle minimal choisi. On a $c_4^3 = \Delta j$. Dans le cas où jc_6 est non nul, on pose

$$c_4' = \frac{c_4}{2^{v(c_4)}}, \quad c_6' = \frac{c_6}{2^{v(c_6)}} \quad \text{et} \quad j' = \frac{j}{2^{v(j)}}.$$

On désigne dans toute la suite par (C_1), (C_2) et (C_3) les conditions suivantes :

(C_1) : il existe $\gamma \in \mu_{r-1}$ tel que l'on ait $j' \equiv \gamma^4 + 2\gamma^5 \bmod 4$.

(C_2) : il existe un élément γ de μ_{r-1} qui n'appartient pas à μ_3 tel que l'on ait $j' \equiv \gamma^6 + 2\gamma^5\big(1+\gamma^2\big) \bmod 4$.

(C_3) : il existe $\gamma \in \mu_{r-1}$ tel que l'on ait $j' \equiv \gamma^4 + 2\gamma^3 \bmod 4$.

Le groupe $\Phi = \mathrm{Gal}\big(L/K_{nr}\big)$ est soit cyclique d'ordre 2, 3, 4 ou 6, soit d'ordre 8 et isomorphe au groupe quarternionien, soit d'ordre 24 et isomorphe à $\mathbb{S}L_2(\mathbb{F}_3)$. Son ordre est donné par l'énoncé suivant :

Théorème.

1. *Si $v(j) = 0$, on a $|\Phi| = 2$.*
2. *Si $v(j) \in \big\{1, 2, 5, 7, 10, 11\big\}$, on a $|\Phi| = 24$.*
3. *Si $v(j) \in \big\{3, 9\big\}$, on a $|\Phi| = 8$.*
4. *Supposons $v(j) = 4$.*

   (a) Si la condition (C_1) est satisfaite, on a

   $$|\Phi| = \begin{cases} 3 & \text{si le type de réduction de } E \text{ est } IV^* \\ 6 & \text{sinon.} \end{cases}$$

   (b) Si la condition (C_1) n'est pas satisfaite, on a $|\Phi| = 24$.
5. *Supposons $v(j) = 6$.*

   (a) Si $2v(c_6) = 3v(c_4)$, on a

   $$|\Phi| = \begin{cases} 4 & \text{si la condition } (C_2) \text{ est vérifiée} \\ 8 & \text{sinon.} \end{cases}$$

   (b) Si $2v(c_6) = 3v(c_4) + 1$, on a

   $$|\Phi| = \begin{cases} 4 & \text{si } j' \equiv 1 \bmod 4 \\ 8 & \text{sinon.} \end{cases}$$

   (c) Supposons $2v(c_6) > 3v(c_4) + 1$.

   (c.1) Supposons $v(c_4)$ pair. On a $|\Phi| = 4$ s'il existe $t \in \mu_3$, $t \neq 1$, et $\zeta \in \mu_{r-1}$ tels que

   $$c_4' \equiv \zeta(t+2) \bmod 4.$$

   On a $|\Phi| = 8$ sinon.

   (c.2) Si $v(c_4)$ est impair, on a $|\Phi| = 8$.
6. *Supposons $v(j) = 8$.*

(a) Si la condition (C_3) est satisfaite, on a

$$|\Phi| = \begin{cases} 3 & \text{si le type de réduction de } E \text{ est } IV \\ 6 & \text{sinon.} \end{cases}$$

(b) Si la condition (C_3) n'est pas satisfaite, on a $|\Phi| = 24$.

7. *Supposons $v(j) \geqslant 12$.*

   (a) Si 3 divise $v(\Delta)$, on a $|\Phi| = 2$.

   (b) Si 3 ne divise pas $v(\Delta)$, on a

$$|\Phi| = \begin{cases} 3 & \text{si le type de réduction de } E \text{ est } IV \text{ ou } IV^* \\ 6 & \text{sinon.} \end{cases}$$

Remarques

1) Nous avons vérifié que pour chacun des cas intervenant dans l'énoncé du théorème, il existe des corps K et des courbes elliptiques définies sur K réalisant les conditions envisagées.

2) On ne dispose pas d'énoncés généraux simples, portant sur les invariants standard associés à E, permettant de décider si le type de réduction de E est IV ou IV^*.

Néanmoins, dans le cas où $v(j) \geqslant 12$, le type de réduction de E est IV ou IV^* si et seulement si les conditions suivantes sont réalisées :

(i) on a $v(\Delta) = 4$ ou bien $v(\Delta) = 8$;

(ii) il existe $\zeta \in \mu_{r-1}$ tel que $c_6' \equiv \zeta$ mod. 4.

Par exemple, si K est le corps $\mathbb{Q}_2(\mu_3)$, qui est l'extension quadratique non ramifiée de $\mathbb{Q}_2$, on obtient l'énoncé suivant :

Corollaire. *Supposons $K = \mathbb{Q}_2(\mu_3)$.*

1. *Si $v(j) = 0$, on a $|\Phi| = 2$.*
2. *Si $v(j) \in \{1, 2, 5, 7, 10, 11\}$, on a $|\Phi| = 24$.*
3. *Si $v(j) \in \{3, 9\}$, on a $|\Phi| = 8$.*
4. *Supposons $v(j) = 4$.*

   (a) Supposons qu'il existe $\gamma \in \mu_3$ tel que $j' \equiv \gamma + 2\gamma^2$ mod. 4. On a $|\Phi| \in \{3, 6\}$.

   Soit $\zeta \in \mu_3$ tel que $c_6' \equiv \zeta$ mod. 2. On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont réalisées :

   (i) on a $v(\Delta) = 8$;

(ii) on a $\Big(\gamma = 1$ *et* $c_6' \equiv -\zeta \bmod. 4\Big)$ *ou bien* $\Big(\gamma \neq 1$ *et* $c_6' \equiv \zeta \bmod. 4\Big)$.

(b) On a $|\Phi| = 24$ *sinon.*

5. *Supposons* $v(j) = 6$.

(a) Si $2v(c_6) = 3v(c_4)$, *on a* $|\Phi| = 8$.

(b) Si $2v(c_6) = 3v(c_4) + 1$, *on a*

$$|\Phi| = \begin{cases} 4 & \text{si } j' \equiv 1 \bmod 4 \\ 8 & \text{sinon.} \end{cases}$$

(c) Supposons $2v(c_6) > 3v(c_4) + 1$.

(c.1) Supposons $v(c_4)$ *pair. On a* $|\Phi| = 4$ *s'il existe* $t \in \mu_3$, $t \neq 1$, *et* $\zeta \in \mu_3$ *tels que*

$$c_4' \equiv \zeta(t+2) \bmod. 4.$$

On a $|\Phi| = 8$ *sinon.*

(c.2) Si $v(c_4)$ *est impair, on a* $|\Phi| = 8$.

6. *Supposons* $v(j) = 8$.

(a) Supposons qu'il existe $\gamma \in \mu_3$ *tel que* $j' \equiv \gamma + 2 \bmod 4$. *On a* $|\Phi| \in \big\{3, 6\big\}$.

On a $|\Phi| = 3$ *si et seulement si les conditions suivantes sont réalisées :*

(i) on a $v\big(\Delta\big) = 4$;

(ii) on a $\Big(\gamma = 1$ *et* $c_6' \equiv 1 \bmod. 4\Big)$ *ou bien* $\Big(\gamma \neq 1$ *et* $c_6' \equiv -\gamma \bmod. 4\Big)$.

(b) On a $|\Phi| = 24$ *sinon.*

7. *Supposons* $v(j) \geqslant 12$.

(a) Si 3 *divise* $v(\Delta)$, *on a* $|\Phi| = 2$.

(b) Supposons que 3 *ne divise pas* $v(\Delta)$. *On a* $|\Phi| = 3$ *si les conditions suivantes sont réalisées :*

(i) on a $v(\Delta) = 4$ *ou bien* $v(\Delta) = 8$;

(ii) il existe $\zeta \in \mu_3$ *tel que* $c_6' \equiv \zeta \bmod. 4$.

On a $|\Phi| = 6$ *sinon.*

2. Préliminaires

Pour toute la suite, on note encore v le prolongement à $\overline{\mathbb{Q}_2}$ de la valuation de K. Soit μ l'ensemble des racines de l'unité d'ordre impair de $\overline{\mathbb{Q}_2}$. Il est contenu dans l'extension non ramifiée maximale de $\mathbb{Q}_2$ dans $\overline{\mathbb{Q}_2}$, i.e. dans K_{nr}.

Lemme 1. *Soient γ et γ' deux éléments de μ.*

1. *Si l'on a $v(\gamma-\gamma')>0$, alors $\gamma=\gamma'$.*
2. *Si γ n'est pas d'ordre 3, alors $1+\gamma+\gamma^2$ est une unité de K_{nr}.*
3. *Soient x et y des éléments de K_{nr} de valuation $\geqslant 0$ tels que $v(x-y)=1$. Alors, l'un des éléments x ou y n'est pas un carré dans K_{nr}.*
4. *Soit x un élément de K_{nr} de valuation 0. Alors, x est un carré dans K_{nr} si seulement si il existe $\xi\in\mu$ telle que $x\equiv\xi \bmod 4$.*
5. *Soit d un élément de K_{nr} tel que $v(d-1)=1$. Soit x un élément de $K_{nr}\big(\sqrt{d}\big)$ tel que l'on ait $x\equiv 2y \bmod 4$, où y est un élément de K_{nr} de valuation 0. Alors, x n'est pas un carré dans $K_{nr}\big(\sqrt{d}\big)$.*
6. *Soit x une unité de K_{nr}. Alors, les trois racines cubiques de x sont dans K_{nr}.*

Démonstration : 1. Les éléments γ et γ' étant dans K_{nr}, on a $\gamma\equiv\gamma' \bmod 2$. On peut supposer $\gamma'=1$. Soit n l'ordre de γ. On a l'égalité $(\gamma-1)(1+\cdots+\gamma^{n-1})=0$. Puisque n est impair et que $\gamma\equiv 1 \bmod 2$, on en déduit que $1+\cdots+\gamma^{n-1}\equiv 1 \bmod 2$. En particulier, $1+\cdots+\gamma^{n-1}$ n'est pas nul, donc $\gamma=1$.

2. Supposons que l'on ait $v\big(1+\gamma+\gamma^2\big)>0$. On a alors $\gamma\neq 1$ et $\gamma^3\equiv 1 \bmod 2$, d'où $\gamma^3=1$ (assertion 1), et ainsi γ est d'ordre 3.

3. Supposons que l'on ait $x=a^2$ et $y=b^2$, où a et b sont dans K_{nr}. On a $v(a^2-b^2)=1$ et $a-b=a+b-2b$, de sorte que $v(a-b)\geqslant 1$ et $v(a+b)\geqslant 1$, ce qui implique $v(x-y)\geqslant 2$. D'où l'assertion.

4. Supposons qu'il existe $\xi\in\mu$ d'ordre n tel que l'on ait $x\equiv\xi \bmod 4$. On a l'égalité

$$\left(\xi^{\frac{n+1}{2}}\right)^2=\xi,$$

ce qui montre que ξ est un carré dans K_{nr}. D'après le lemme 7 de [Kr2], x est donc un carré dans K_{nr}.

Inversement, supposons que x soit un carré dans K_{nr}. Il existe $\xi\in\mu$ et $\xi'\in\mu\cup\{0\}$ tels que l'on ait $x\equiv\xi+2\xi' \bmod 4$. Si $\xi'\neq 0$, on a $v(x-\xi)=1$, et ξ étant un carré dans K_{nr}, cela conduit à une contradiction (assertion 3). D'où $\xi'=0$ et l'implication.

5. D'après l'assertion 3, d n'est pas un carré dans K_{nr} et l'extension $K_{nr}\big(\sqrt{d}\big)/K_{nr}$ est de degré 2. Il existe un entier z de $K_{nr}\big(\sqrt{d}\big)$ tel que l'on ait $x=2y+4z$. Posons $\pi=1+\sqrt{d}$. Supposons que x soit un carré dans $K_{nr}\big(\sqrt{d}\big)$; il existe alors a et b dans K_{nr} tels que l'on ait $x=(a+b\pi)^2$. On a donc l'égalité

$$2y+4z=a^2+(d-1)b^2+2b(a+b)\pi.$$

Puisque π est une uniformisante de $K_{nr}\big(\sqrt{d}\big)$, on peut écrire $z=f+g\pi$, où f et g sont des entiers de K_{nr}. On obtient alors :

$$a^2+(d-1)b^2=2y+4f \quad \text{et} \quad b(a+b)=2g.$$

On a donc $v\big(a^2+(d-1)b^2\big)=1$, d'où $v(a)\geqslant 1$ et $v(b)=0$, et ainsi $v\big(b(a+b)\big)=0$, ce qui contredit l'égalité ci-dessus. D'où l'assertion.

6. Il existe $\xi\in\mu$ et une unité x' de K_{nr} congrue à 1 modulo, 2 telles que $x=\xi x'$. L'élément ξ, qui est dans μ, est un cube dans μ. Par ailleurs, le lemme de Hensel appliqué avec le polynôme X^3-x' montre que x' est un cube dans K_{nr}. Le fait que μ_3 soit contenu dans K_{nr} entraîne alors notre assertion.

Lemme 2. *Soit x un élément de $K\big(\sqrt{3}\big)$ de valuation 0 ; posons $\pi=1+\sqrt{3}$. Pour que x soit un carré dans $K_{nr}\big(\sqrt{3}\big)$ il faut et il suffit qu'il existe $\gamma\in\mu_{r-1}$ et $\gamma'\in\mu_{r-1}\cup\{0\}$ tels que l'on ait*

$$x\equiv\gamma+\gamma'^2\pi^2+\gamma^{\frac{r}{2}}\gamma'\pi^3 \bmod 4. \tag{1}$$

Démonstration : Supposons la condition (1) réalisée. On a $2\equiv\pi^2-\pi^3 \bmod 4$, d'où

$$\gamma+\gamma'^2\pi^2+\gamma^{\frac{r}{2}}\gamma'\pi^3\equiv\big(\gamma^{\frac{r}{2}}+\gamma'\pi\big)^2 \bmod 4.$$

Il en résulte que $\gamma+\gamma'^2\pi^2+\gamma^{\frac{r}{2}}\gamma'\pi^3$ est un carré dans $K_{nr}\big(\sqrt{3}\big)$, et que tel est aussi le cas de x (cf. [Kr2], lemme 7).

Inversement, supposons qu'il existe $y\in K_{nr}\big(\sqrt{3}\big)$ tel que $x=y^2$. Puisque π est une uniformisante de $K\big(\sqrt{3}\big)$ et que l'extension $K\big(\sqrt{3}\big)/K$ est totalement ramifiée, il existe $\gamma\in\mu_{r-1}$ tel que $x\equiv\gamma \bmod \pi$. On en déduit que $y\equiv\gamma^{\frac{r}{2}} \bmod \pi$, autrement dit, qu'il existe deux entiers a et b dans K_{nr} tels que l'on ait $y=\gamma^{\frac{r}{2}}+(a+b\pi)\pi$. Compte tenu du fait que $2\equiv\pi^2-\pi^3$ mod. 4, on obtient ainsi la congruence

$$x\equiv\gamma+a^2\pi^2+a\gamma^{\frac{r}{2}}\pi^3 \bmod 4.$$

Si l'on a $v(a)\geqslant 1$, la condition (1) est satisfaite avec $\gamma'=0$. Supposons $v(a)=0$. Il existe alors une racine de l'unité γ' d'ordre impair telle que $a\equiv\gamma'$ mod. 2. Il reste à vérifier que γ' appartient à μ_{r-1}. L'extension $K\big(\sqrt{3}\big)/K$ étant totalement ramifiée, il existe des éléments α_1, α_2, α_3 dans $\mu_{r-1}\cup\big\{0\big\}$ tels que l'on ait $x\equiv\alpha_1+\alpha_2\pi+\alpha_3\pi^2$ mod. π^3. Il résulte alors de l'assertion 1 du lemme 1 que l'on a $\alpha_1=\gamma$, $\alpha_2=0$ et $\alpha_3=\gamma'^2$. Ainsi γ' est dans μ_{r-1}. D'où le lemme.

3. Démonstration du théorème

Les assertions 1 et 7 résultent directement du théorème 2 de [Kr2]. On supposera donc désormais que l'on a

$$1\leqslant v(j)\leqslant 11.$$

En particulier, on a $j\neq 0$.

3.1. Notations

On choisit, *pour toute la suite*, une racine cubique $\Delta^{1/3}$ de Δ dans $\overline{\mathbb{Q}_2}$. Notons, à l'instar de [Kr2] :

$$A = c_4 - 12\Delta^{1/3} \quad \text{et} \qquad B = c_4^2 + 12c_4\Delta^{1/3} + \big(12\Delta^{1/3}\big)^2.$$

On choisit par ailleurs une racine carrée $B^{1/2}$ de B dans $\overline{\mathbb{Q}_2}$. On pose

$$C = 2\big(c_4 + 6\Delta^{1/3} + B^{1/2}\big).$$

Pour toute racine cubique de l'unité t dans $\overline{\mathbb{Q}_2}$, on pose

$$A_t = c_4 - 12t\Delta^{1/3} \quad \text{et} \qquad B_t = c_4^2 + 12c_4t\Delta^{1/3} + \big(12t\Delta^{1/3}\big)^2.$$

On a $A_1 = A$ et $B_1 = B$. On vérifie que l'on a l'égalité

$$A_tB_t = c_6^2. \tag{2}$$

Les éléments A_t et B_t appartiennent à K_{nr} si et seulement si 3 divise $v(\Delta)$, autrement dit, si et seulement si 3 divise $v(j)$ (lemme 1, assertion 6).
On désigne par $j^{1/3}$ la racine cubique de j dans $\overline{\mathbb{Q}_2}$ définie par l'égalité

$$j^{1/3} = \frac{c_4}{\Delta^{1/3}}.$$

On choisit désormais une racine cubique θ de 2 dans $\overline{\mathbb{Q}_2}$. On pose

$$u = \frac{j^{1/3}}{\theta^{v(j)}}.$$

On a $u^3 = j' \in K$ et $v(u) = 0$. D'après l'assertion 6 du lemme 1, on en déduit que

$$u \in K_{nr}. \tag{3}$$

Lemme 3. *Il existe deux éléments $\alpha \in \mu_{3(r-1)}$ et $\alpha' \in \mu_{3(r-1)} \cup \{0\}$ tels que*

$$u \equiv \alpha + 2\alpha' \text{ mod. } 4.$$

Démonstration : Il existe deux éléments $\zeta \in \mu_{r-1}$ et $\zeta' \in \mu_{r-1} \cup \big\{0\big\}$ tels que

$$j' \equiv \zeta + 2\zeta' \text{ mod. } 4.$$

Par conséquent, il existe une racine cubique $\zeta^{1/3}$ de ζ dans K_{nr} telle que

$$u \equiv \zeta^{1/3}\left(1 + 2\frac{\zeta'}{\zeta}\right) \text{ mod. } 4.$$

Les éléments $\alpha = \zeta^{1/3}$ et $\alpha' = \zeta'\zeta^{-2/3}$ satisfont alors les conditions du lemme.

3.2. L'assertion 2 du théorème

Par hypothèse, on a

$$v(j) \in \{1, 2, 5, 7, 10, 11\}.$$

L'égalité $3v(c_4) - v(\Delta) = v(j)$ entraîne que 3 ne divise pas $v(\Delta)$; par conséquent, on a $|\Phi| \in \{3, 6, 24\}$ ([Kr2], th. 3).

On a

$$\frac{B}{c_4^2} = 1 + 12j^{-1/3} + 144j^{-2/3} \in K_{nr}(\theta). \tag{4}$$

Il s'agit de démontrer que B n'est pas un carré dans $K_{nr}(\theta)$, qui est l'unique extension de degré 3 de K_{nr} (*loc. cit.*). Pour cela, on va procéder par l'absurde en supposant que B est un carré dans $K_{nr}(\theta)$.

3.2.1. Cas où $v(j) \in \{1, 2, 5\}$

D'après l'hypothèse faite, il existe trois éléments a, b et c de K_{nr} tels que l'on ait

$$\frac{B}{c_4^2} = (a + b\theta + c\theta^2)^2,$$

c'est à dire

$$\frac{B}{c_4^2} = (a^2 + 4bc) + 2(c^2 + ab)\theta + (b^2 + 2ac)\theta^2. \tag{5}$$

Il résulte de la formule (4) que B/c_4^2 est une unité de $K_{nr}(\theta)$. Par ailleurs, on a

$$v\left(\frac{B}{c_4^2}\right) = 2v(a + b\theta + c\theta^2).$$

Puisque $v(\theta) = 1/3$, et donc que $v(a)$, $v(b\theta)$ et $v(c\theta^2)$ sont distincts deux à deux, on obtient

$$v(a) = 0,\ v(b) \geqslant 0 \quad \text{et} \quad v(c) \geqslant 0. \tag{6}$$

Cas où $v(j) = 1$

On a

$$\frac{B}{c_4^2} = 1 + 72\ u^{-2}\theta + 6\ u^{-1}\theta^2.$$

D'après la condition (3), l'égalité (5) et le fait que $(1, \theta, \theta^2)$ soit une base de $K_{nr}(\theta)/K_{nr}$, on a donc

$$c^2 + ab = 36u^{-2}, \tag{7}$$

$$b^2 + 2ac = 6u^{-1}. \tag{8}$$

D'après la condition (8), on a $v(b) > 0$ puis $v(c) = 0$. La condition (7) conduit alors à une contradiction, ce qui prouve le résultat dans ce cas.

Cas où $v(j) = 2$

On a

$$\frac{B}{c_4^2} = 1 + 6\ u^{-1}\theta + 36\ u^{-2}\theta^2.$$

Il en résulte que l'on a

$$c^2 + ab = 3u^{-1}, \tag{9}$$

$$b^2 + 2ac = 36u^{-2}. \tag{10}$$

D'après (6), on a $v(a) = 0$. Si $v(c) > 0$, la condition (9) entraîne $v(ab) = 0$, d'où $v(b) = 0$, ce qui contredit (10). Par suite on a $v(c) = 0$; d'après (10), on a donc $v(b^2) = 1$, ce qui conduit de nouveau à une contradiction.

Cas où $v(j) = 5$

On a

$$\frac{B}{c_4^2} = 1 + 3\ u^{-1}\theta + 9\ u^{-2}\theta^2.$$

On a dans ce cas

$$2(c^2 + ab) = 3u^{-1},$$

ce qui implique $v(c^2 + ab) = -1$ et contredit (6).

3.2.2. Cas où $v(j) \in \{7, 10, 11\}$

Dans ce cas, on vérifie que l'élément

$$\frac{\theta^{2v(j)}u^2 B}{12^2 c_4^2}$$

est une unité de $K_{nr}(\theta)$ (cf. (7)). On en déduit, comme ci-dessus, l'existence d'éléments a, b et c de K_{nr} de tels que $v(a) = 0$, $v(b) \geqslant 0$, $v(c) \geqslant 0$ et que

$$\frac{\theta^{2v(j)}u^2B}{12^2c_4^2} = (a^2 + 4bc) + 2(c^2 + ab)\theta + (b^2 + 2ac)\theta^2,$$

Cas où $v(j) = 7$

On a

$$\frac{\theta^{14}u^2B}{12^2c_4^2} = 1 + \frac{u}{3}\theta + \frac{u^2}{9}\theta^2,$$

d'où

$$2(c^2 + ab) = \frac{u}{3},$$

puis $v(c^2 + ab) = -1$, ce qui conduit à une contradiction.

Cas où $v(j) = 10$

On a

$$\frac{\theta^{20}u^2B}{12^2c_4^2} = 1 + \frac{2u}{3}\theta + \frac{4u^2}{9}\theta^2.$$

On en déduit les égalités

$$c^2 + ab = \frac{u}{3}, \tag{11}$$

$$b^2 + 2ac = \frac{4u^2}{9}. \tag{12}$$

On a $v(a) = 0$. Si $v(c) > 0$, la condition (11) entraîne $v(ab) = 0$, d'où $v(b) = 0$, ce qui contredit (12). Donc $v(c) = 0$; d'après (12), on a ainsi $v(b^2) = 1$, ce qui est impossible.

Cas où $v(j) = 11$

On a

$$\frac{\theta^{22}u^2B}{12^2c_4^2} = 1 + \frac{8}{9}u^2\theta + \frac{2}{3}u\theta^2.$$

On a donc

$$c^2 + ab = \frac{4}{9}u^2, \tag{13}$$

$$b^2 + 2ac = \frac{2}{3}u. \tag{14}$$

D'après (14), on a $v(b) > 0$ et $v(c) = 0$, ce qui contredit (13).

Cela termine la démonstration de l'assertion 2 du théorème.

3.3. Un lemme préliminaire

Nous utiliserons dans la suite à plusieurs reprises le résultat suivant :

Proposition 1. *Supposons $v(c_4)$ pair, $c_6 \neq 0$ et $v(j) \equiv 0 \bmod 3$. Alors, si pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr}, on a $|\Phi| = 8$.*

Démonstration : On a $c_4 \neq 0$. Posons

$$\pi = 1 + \frac{B^{1/2}}{c_4}.$$

On va démontrer que C n'est pas un carré dans $K_{nr}\big(\sqrt{B}\big)$, ce qui prouvera le résultat ([Kr2], th. 3 (i) b)). On vérifie que l'on a

$$\frac{C}{2^{v(c_4)}} = c_4'\big(12j^{-1/3} + 2\pi\big).$$

Supposons que C soit un carré dans $K_{nr}\big(\sqrt{B}\big)$. Puisque $v(c_4)$ est pair, il existe deux éléments a et b de K_{nr} tels que l'on ait

$$(a + b\pi)^2 = c_4'\big(12j^{-1/3} + 2\pi\big).$$

En utilisant les définitions de π et B, on vérifie que l'on a

$$\pi^2 = 2\pi + 12j^{-1/3} + 144j^{-2/3}.$$

Par hypothèse, 3 divise $v(j)$; d'après l'assertion 6 du lemme 1, il en résulte que

$$j^{1/3} \in K_{nr}.$$

Puisque $(1, \pi)$ est une base de $K_{nr}\big(\sqrt{B}\big)$ sur K_{nr}, on obtient ainsi

$$ab + b^2 = c_4', \tag{15}$$

$$a^2 - 12ab\ j^{-1/3} + 144b^2\ j^{-2/3} = 0. \tag{16}$$

Il résulte de (16) l'existence d'un élément $t \in \mu_3$ tel que l'on ait

$$a = -12tb\ j^{-1/3}. \tag{17}$$

Les égalités (15) et (17) entraînent alors $b^2\big(1-12t\ j^{-1/3}\big)=c_4'$. Puisque $v(c_4)$ est pair, l'élément

$$A_t=2^{v(c_4)}c_4'\big(1-12t\ j^{-1/3}\big)$$

est donc un carré dans K_{nr}. L'égalité (2) et le fait que et c_6 soit non nul entraînent alors que B_t est un carré dans K_{nr}. On obtient ainsi une contradiction, ce qui prouve que C n'est pas un carré dans $K_{nr}\big(\sqrt{B}\big)$. Cela entraîne le résultat ([Kr2], th. 3).

3.4. L'assertion 3 du théorème

Par hypothèse, on a

$$v(j)\in\big\{3,9\big\}.$$

Puisque 3 divise $v(\Delta)$, on a $|\Phi|\in\big\{2,4,8\big\}$ ([Kr2], th. 3). Rappelons que l'on a

$$1-\frac{c_6^2}{c_4^3}=\frac{1728}{j}. \tag{18}$$

3.4.1. Cas où $v(j)=3$

Prouvons l'énoncé suivant :

Lemme 4. *L'entier $v(c_4)$ est pair et pour tout $t\in\mu_3$, A_t n'est pas un carré dans K_{nr}.*

Démonstration : D'après (18), on a

$$v\left(1-\frac{c_6^2}{c_4^3}\right)=3.$$

En particulier, c_6^2/c_4^3 est un carré dans K_{nr} ; il en est de même de c_4 et donc $v(c_4)$ est pair.

Par ailleurs, on a $A_t=c_4\big(1-12tj^{-1/3}\big)$. Par conséquent $v\Big(1-\frac{A_t}{c_4}\Big)=1$, et donc A_t/c_4 n'est pas un carré dans K_{nr} (lemme 1, assertion 3). D'où le lemme.

L'égalité (2) et le fait que $c_6\neq 0$ entraînent alors que pour tout $t\in\mu_3$, B_t n'est pas un carré dans K_{nr} (lemme 4). Puisque $v(c_4)$ est pair (*loc. cit.*), il résulte de la proposition 1 que l'on a $|\Phi|=8$.

3.4.2. Cas où $v(j)=9$

Soit t un élément de μ_3. On vérifie que l'on a

$$\frac{4u^2B_t}{9c_4^2t^2}=1+\frac{2}{3}t^2u+\frac{4}{9}tu^2.$$

Par conséquent, on a

$$v\left(\frac{4u^2B_t}{9c_4^2t^2}-1\right)=1.$$

D'après (3) et l'assertion 3 du lemme 1, B_t n'est donc pas un carré dans K_{nr}.

Supposons que C soit un carré dans $K_{nr}\big(B^{1/2}\big)$. On a :

$$\frac{C}{2^{v(c_4)-1}} = \left(4 + 24j^{-1/3} + \frac{4B^{1/2}}{c_4}\right)c_4'.$$

Puisque $v(c_4)$ est impair (cf. (18)), il existe donc a et b dans K_{nr} tels que :

$$\big(a + 2bB^{1/2}\big)^2 = \left(4 + 3u^{-1} + \frac{4B^{1/2}}{c_4}\right)c_4'.$$

On en déduit que l'on a

$$ab = \frac{c_4'}{c_4} \quad \text{et} \quad a^2 + 4b^2B = \big(4 + 3u^{-1}\big)c_4'. \tag{19}$$

Par ailleurs, on a

$$\frac{4B}{c_4^2} = 4 + 6u^{-1} + 9u^{-2}.$$

On obtient ainsi l'égalité $a^2 - a\big(4+3u^{-1}\big)c_4b + b^2c_4^2\big(4+6u^{-1}+9u^{-2}\big) = 0$. On vérifie alors qu'il existe $t \in \mu_3$, $t \neq 1$, tel que l'on ait

$$a = bc_4\big(2 - 3tu^{-1}\big).$$

En utilisant la première égalité de (19), on obtient ainsi

$$b^2c_4^2\big(2 - 3tu^{-1}\big) = c_4'.$$

Il en résulte que $c_4'\big(2 - 3tu^{-1}\big)$ est un carré dans K_{nr}. Par ailleurs, on vérifie que l'on a $\frac{2A_t}{c_4} = 2 - 3tu^{-1}$. Autrement dit, on a

$$\frac{A_t}{2^{v(c_4)-1}} = c_4'\big(2 - 3tu^{-1}\big).$$

Puisque $v(c_4)$ est impair, A_t est donc un carré dans K_{nr}. L'égalité (2) entraîne que B_t est un carré dans K_{nr}, ce qui conduit à une contradiction. Ainsi, C n'est pas un carré dans $K_{nr}\big(B^{1/2}\big)$ et on a $|\Phi| = 8$ ([Kr2], th.3).

3.5. L'assertion 4 du théorème

Par hypothèse, on a $v(j) = 4$. L'ordre de Φ est donc 3, 6 ou 24.

On a

$$\frac{B}{c_4^2} = 1 + 18u^{-2}\theta + 3u^{-1}\theta^2. \tag{20}$$

Proposition 2. *L'élément B est un carré dans $K_{nr}(\theta)$ si et seulement si il existe deux éléments ζ et ζ' dans μ_{r-1} tels que l'on ait*

$$j' \equiv \zeta + 2\zeta' \text{ mod. } 4 \quad \textit{et} \quad \zeta^5 = \zeta'^4. \tag{21}$$

Démonstration : Soient α et α' deux éléments réalisant l'énoncé du lemme 3.

Supposons que B soit un carré dans $K_{nr}(\theta)$. On va démontrer que l'on a l'égalité

$$\alpha^7 = \alpha'^4. \tag{22}$$

Par hypothèse, il existe a, b et c dans K_{nr} tels que l'on ait

$$\frac{B}{c_4^2} = (a + b\theta + c\theta^2)^2,$$

autrement dit,

$$\frac{B}{c_4^2} = (a^2 + 4bc) + 2(c^2 + ab)\theta + (b^2 + 2ac)\theta^2. \tag{23}$$

D'après l'égalité (20), B/c_4^2 est une unité de $K_{nr}(\theta)$, donc on a

$$v(a) = 0, \quad v(b) \geqslant 0 \quad \text{et} \quad v(c) \geqslant 0.$$

On déduit alors de (20) et (23) les égalités

$$a^2 + 4bc = 1, \tag{24}$$

$$c^2 + ab = 9u^{-2}, \tag{25}$$

$$b^2 + 2ac = 3u^{-1}. \tag{26}$$

D'après la condition (24), on a

$$a \equiv 1 \text{ mod. } 2. \tag{27}$$

D'après le lemme 4 et l'égalité (26), on a

$$b^2 \equiv \alpha^{-1} \text{ mod. } 2.$$

L'élément α^{-1} est un carré dans K_{nr} car c'est une racine de l'unité d'ordre impair. D'après l'assertion 3 de *loc. cit.*, on a donc

$$b^2 \equiv \alpha^{-1} \text{ mod. } 4. \tag{28}$$

Les conditions (26) à (28) entraînent alors la congruence

$$\alpha^{-1} + 2c \equiv -u^{-1} \text{ mod. } 4.$$

Par ailleurs, on a

$$u^{-1} \equiv \alpha^{-1}\big(1 + 2\alpha'\alpha^{-1}\big) \text{ mod. } 4,$$

d'où l'on déduit que

$$c \equiv \alpha^{-1} + \alpha'\alpha^{-2} \text{ mod. } 2. \tag{29}$$

D'après (25), on a $c^4 + a^2b^2 \equiv u^{-4}$ mod. 2. Les conditions (27) à (29) impliquent la congruence $\big(\alpha^{-1} + \alpha'\alpha^{-2}\big)^4 + \alpha^{-1} \equiv \alpha^{-4}$ mod 2. On en déduit que l'on a

$$\alpha^7 \equiv \alpha'^4 \text{ mod. } 2.$$

L'assertion 1 du lemme 1 entraîne alors l'égalité (22).

Par ailleurs, il existe $\zeta \in \mu_{r-1}$ et $\zeta' \in \mu_{r-1} \cup \{0\}$ tels que

$$j' \equiv \zeta + 2\zeta' \text{ mod. } 4.$$

On a $j' = u^3$, d'où $j' \equiv \alpha^3 + 2\alpha^2\alpha'$ mod. 4. Il en résulte que l'on a (lemme 1, assertion 1)

$$\zeta = \alpha^3 \quad \text{et} \quad \zeta' = \alpha^2\alpha'.$$

Par suite, la condition (21) est satisfaite (cf. (22)).

Inversement, supposons que la condition (21) soit réalisée. On vérifie d'abord que l'on a $\alpha^7 = \alpha'^4$, et donc que

$$\big(\alpha^{-1} + \alpha'\alpha^{-2}\big)^4 + \alpha^{-1} \equiv \alpha^{-4} \text{ mod } 2.$$

Par ailleurs, puisque α appartient à $\mu_{3(r-1)}$, on a

$$\alpha^{-4} + \alpha^{-1} \equiv \left(\alpha^{-2} + \alpha^{\frac{-(3r-2)}{2}}\right)^2 \text{ mod. } 2.$$

Il en résulte que l'on a

$$\big(\alpha^{-1} + \alpha'\alpha^{-2}\big)^2 \equiv \alpha^{-2} + \alpha^{\frac{-(3r-2)}{2}} \text{ mod. } 2. \tag{30}$$

Par ailleurs, d'après (20), on a

$$\frac{B}{c_4^2} \equiv 1 + 2\alpha^{-2}\theta + 3\alpha^{-1}\big(1 + 2\alpha'\alpha^{-1}\big)\theta^2 \text{ mod. } 4. \tag{31}$$

On vérifie alors que les conditions (30) et (31) entraînent la congruence

$$\frac{B}{c_4^2} \equiv \left(1 + \alpha^{\frac{-(3r-2)}{2}}\theta + \left(\alpha^{-1} + \alpha'\alpha^{-2}\right)\theta^2\right)^2 \text{ mod. } 4.$$

Cela montre que B est un carré dans $K_{nr}(\theta)$ (cf. [Kr2], lemme 7). D'où la proposition.

L'assertion 4 du théorème se déduit comme suit : on remarque d'abord que la condition (C_1) de l'énoncé est équivalente à la condition (21). En effet, il est immédiat de constater que la condition (C_1) implique (21). Inversement, l'application de μ_{r-1} dans μ_{r-1} qui à x associe x^4 est un isomorphisme de groupes. Il existe donc $\gamma \in \mu_{r-1}$ tel que $\zeta = \gamma^4$. On a ainsi $\zeta'^4 = \gamma^{20}$. Puisque ζ' est une racine de l'unité d'ordre impair, on a $\zeta' = \gamma^5$, et la condition (C_1) est donc réalisée. Les assertions (i) du théorème 2 et (ii) du théorème 3 de [Kr2] entraînent alors le résultat.

3.6. L'assertion 6 du théorème

La démonstration de cette assertion est analogue à celle de l'alinéa précédent.

Par hypothèse, on a $v(j) = 8$. L'ordre de Φ est donc 2, 4 ou 8. On vérifie que l'on a

$$\frac{\theta^4 u^2 B}{c_4^2} = 9 + 2u^2\theta + 3u\theta^2. \tag{32}$$

Proposition 3. *L'élément B est un carré dans $K_{nr}(\theta)$ si et seulement si il existe deux éléments ζ et ζ' dans μ_{r-1} tels que l'on ait*

$$j' \equiv \zeta + 2\zeta' \text{ mod. } 4 \quad \textit{et} \quad \zeta^3 = \zeta'^4. \tag{33}$$

Démonstration : Soient α et α' deux éléments satisfaisant l'énoncé du lemme 3.

Supposons que B soit un carré dans $K_{nr}(\theta)$. Vérifions que l'on a

$$\alpha = \alpha'^4. \tag{34}$$

Il existe trois éléments a, b et c de K_{nr}, de valuations positives, tels que

$$\frac{\theta^4 u^2 B}{c_4^2} = (a^2 + 4bc) + 2(c^2 + ab)\theta + (b^2 + 2ac)\theta^2. \tag{35}$$

D'après (32) et (35), on a donc

$$a^2 + 4bc = 9, \tag{36}$$

$$c^2 + ab = u^2, \tag{37}$$

(38) $$b^2 + 2ac = 3u.$$

D'après la condition (36), on a $a \equiv 1$ mod. 2. Par ailleurs, on a $b^2 \equiv \alpha$ mod. 2 (cf. (38)), d'où (assertion 3 du lemme 1)

$$b^2 \equiv \alpha \text{ mod. } 4.$$

On en déduit que $c \equiv \alpha + \alpha'$ mod. 2. D'après (37), on a ainsi $(\alpha + \alpha')^4 + \alpha \equiv \alpha^4$ mod. 2, d'où $\alpha \equiv \alpha'^4$ mod. 2, puis l'égalité (34).

Il existe $\zeta \in \mu_{r-1}$ et $\zeta' \in \mu_{r-1} \cup \{0\}$ tels que $j' \equiv \zeta + 2\zeta'$ mod. 4. La congruence $j' \equiv \alpha^3 + 2\alpha^2\alpha'$ mod. 4 entraîne $\zeta = \alpha^3$ et $\zeta' = \alpha^2\alpha'$. L'égalité (34) implique alors la condition (33).

Inversement, supposons la condition (33) réalisée. On vérifie que $\alpha = \alpha'^4$, puis que

$$(\alpha + \alpha')^2 \equiv \alpha^2 + \alpha^{\frac{3r-2}{2}} \text{ mod. } 2.$$

Par ailleurs, on a

$$\frac{\theta^4 u^2 B}{c_4^2} \equiv 1 + 2\alpha^2\theta + 3(\alpha + 2\alpha')\theta^2 \text{ mod. } 4.$$

Il en résulte que l'on a

$$\frac{\theta^4 u^2 B}{c_4^2} \equiv \left(1 + \alpha^{\frac{3r-2}{2}}\theta + \big(\alpha + \alpha'\big)\theta^2\right)^2 \text{ mod. } 4,$$

ce qui entraîne que B est un carré dans $K_{nr}(\theta)$. D'où la proposition.

On vérifie ensuite que la condition (C_3) de l'énoncé est équivalente à la condition (33). Les assertions (i) du théorème 2 et (ii) du théorème 3 de [Kr2] impliquent alors de nouveau le résultat.

3.7. L'assertion 5 du théorème

Par hypothèse, on a $v(j) = 6$. L'ordre de Φ est donc 2, 4 ou 8. D'après l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on a $2v(c_6) \geqslant 3v(c_4)$. On est ainsi dans l'un des cas envisagés dans l'énoncé de l'assertion 5 du théorème.

3.7.1. Cas où $2v(c_6) = 3v(c_4)$

Pour tout $t \in \mu_3$, on a

(39) $$\frac{B_t}{c_4^2} = 1 + 3tu^{-1} + 9t^2u^{-2} \in K_{nr}.$$

Proposition 4. *L'élément B_t est un carré dans K_{nr} si et seulement si il existe un élément γ dans μ_{r-1}, qui n'est pas dans μ_3, tel que l'on ait*

$$t^2u \equiv \gamma^2 + 2\gamma\big(1+\gamma^2\big) \text{ mod. } 4. \tag{40}$$

Démonstration : Supposons la condition (40) satisfaite. On a

$$tu^{-1} \equiv \gamma^{-2}\big(1 + 2\gamma^{-1}(1+\gamma^2)\big) \text{ mod. } 4.$$

Par suite, on a $t^2u^{-2} \equiv \gamma^{-4}$ mod. 4. Compte tenu de (39), on vérifie que l'on a

$$\frac{B_t}{c_4^2} \equiv \big(1+\gamma^{-1}+\gamma^{-2}\big)^2 \text{ mod. } 4.$$

Puisque γ n'est pas dans μ_3, l'élément $1+\gamma^{-1}+\gamma^{-2}$ est une unité de K_{nr} (lemme 1, assertion 2). Il en résulte que B_t est un carré dans K_{nr} ([Kr2], lemme 7).

Inversement, supposons que B_t soit un carré dans K_{nr}. Soient α et α' deux éléments réalisant l'énoncé du lemme 3. Vérifions que l'on a

$$\alpha^3 \neq 1. \tag{41}$$

On remarque pour cela que l'on a $1 - \frac{c_6^2}{c_4^3} = \frac{27}{j'}$, d'où

$$\frac{1}{j'} - 1 \equiv \frac{c_6^2}{c_4^3} \text{ mod. } 2.$$

De l'égalité $3v(c_4) = 2v(c_6)$, on déduit que $j' \not\equiv 1$ mod. 2. La congruence $j' \equiv \alpha^3$ mod. 2 entraîne alors (41).

Par ailleurs, on a

$$\frac{\alpha^2 B_t}{t^2c_4^2} \equiv 1 + 3t^2\alpha + 2t^2\alpha' + t\alpha^2 \text{ mod. } 4.$$

On en déduit que

$$\frac{\alpha^2 B_t}{t^2c_4^2} \equiv \left(1 + t\alpha^{\frac{3r-2}{2}} + t^2\alpha\right)^2 + 2\left(t^2\alpha' - t\alpha^{\frac{3r-2}{2}} - \alpha^{\frac{3r}{2}}\right) \text{ mod. } 4.$$

D'après l'assertion 3 du lemme 1, puisque B_t est un carré, on a donc

$$t^2\alpha' \equiv t\alpha^{\frac{3r-2}{2}} + \alpha^{\frac{3r}{2}} \text{ mod. } 2. \tag{42}$$

Posons

$$\gamma = t\alpha^{\frac{3r-2}{2}}.$$

On a les égalités

$$\gamma^2 = t^2\alpha \quad \text{et} \quad \gamma^3 = \alpha^{\frac{3r}{2}}. \tag{43}$$

Il résulte alors de (42) et (43) que l'on a

$$t^2 u \equiv \gamma^2 + 2\gamma(1+\gamma^2) \text{ mod. } 4. \tag{44}$$

L'élément γ appartient à $\mu_{3(r-1)}$ et n'est pas dans μ_3 : si γ était dans μ_3, d'après la première égalité de (43) α serait aussi dans μ_3, ce qui contredit la condition (41).

Il reste à démontrer que l'on a

$$\gamma \in \mu_{r-1}. \tag{45}$$

L'égalité $j' = u^3$ et la congruence (44) entraînent

$$j' \equiv \gamma^6 + 2\gamma^5(1+\gamma^2) \text{ mod. } 4.$$

Par ailleurs, il existe $\zeta \in \mu_{r-1}$ et $\zeta' \in \mu_{r-1} \cup \{0\}$ tels que

$$j' \equiv \zeta + 2\zeta' \text{ mod. } 4.$$

D'après l'assertion 1 du lemme 1, on a donc $\zeta = \gamma^6$. On a ainsi $\zeta' \equiv \gamma^6\big(\gamma + \gamma^{-1}\big)$ mod. 2, puis

$$\zeta'\zeta^{-1} \equiv \gamma + \gamma^{-1} \text{ mod. } 2. \tag{46}$$

Puisque γ n'est pas dans μ_3, on a $\gamma \neq 1$, donc $\gamma \not\equiv \gamma^{-1}$ mod. 2, et on a ainsi

$$\zeta' \neq 0. \tag{47}$$

D'après (46), on a $\zeta'^r\zeta^{-r} \equiv \big(\gamma+\gamma^{-1}\big)^r$ mod. 2. On a $\zeta^{r-1} = 1$ et d'après (47) on a $\zeta'^{r-1} = 1$. L'entier r étant une puissance de 2, on en déduit que

$$\zeta'\zeta^{-1} \equiv \gamma^r + \gamma^{-r} \text{ mod. } 2. \tag{48}$$

Par ailleurs, γ appartenant à $\mu_{3(r-1)}$, on a $\gamma^{3r} = \gamma^3$, et il existe $s \in \mu_3$ tel que

$$\gamma^r = s\gamma. \tag{49}$$

D'après les conditions (46), (48) et (49), on obtient ainsi $\gamma + \gamma^{-1} \equiv s\gamma + s^{-1}\gamma^{-1}$ mod. 2, autrement dit, on a

$$\gamma(1+s) \equiv \gamma^{-1}(1+s^{-1}) \text{ mod. } 2. \tag{50}$$

Supposons que l'on ait $s \neq 1$. On déduit alors de (50) que l'on a $\gamma^2 \equiv s^2$ mod. 2, ce qui, d'après l'assertion 1 du lemme 1, implique $\gamma^2 = s^2$. Ainsi $\gamma = s$ et γ est dans μ_3, ce qui conduit à une contradiction. On a donc $s = 1$, ce qui démontre la condition (45). D'où la proposition 4.

On en déduit le résultat suivant :

Proposition 5. *Si pout tout $t \in \mu_3$, B_t n'est pas un carré dans K_{nr}, on a $|\Phi| = 8$. Sinon, on a $|\Phi| = 4$.*

Démonstration : D'après l'égalité $3v(c_4) = 2v(c_6)$, $v(c_4)$ est pair. Par ailleurs, c_6 est non nul et 3 divise $v(j)$. D'après la proposition 1, si pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr}, on a donc $|\Phi| = 8$.

Supposons qu'il existe $t \in \mu_3$ tel que B_t soit un carré dans K_{nr}. D'après la proposition 4, il existe $\gamma \in \mu_{r-1}$, qui n'est pas dans μ_3, tel que

$$t^2 u \equiv \gamma^2 + 2\gamma\big(1 + \gamma^2\big) \text{ mod. } 4.$$

Considérons un élément $t' \in \mu_3$ distinct de t. Démontrons que $B_{t'}$ n'est pas un carré dans K_{nr}. On procède par l'absurde en supposant que $B_{t'}$ est un carré dans K_{nr}. Il existe alors $\gamma' \in \mu_{r-1}$ tel que (prop. 4)

$$t'^2 u \equiv \gamma'^2 + 2\gamma'\big(1 + \gamma'^2\big) \text{ mod. } 4.$$

On a $t\gamma^2 \equiv t'\gamma'^2$ mod. 2, d'où $t\gamma^2 = t'\gamma'^2$ (lemme 1, assertion 1). On a ainsi

$$t\gamma(1 + \gamma^2) \equiv t'\gamma'(1 + \gamma'^2) \text{ mod. } 2. \tag{51}$$

Posons $s = t/t'$. C'est un élément de μ_3 distinct de 1. En élevant les deux membres de la congruence (51) au carré, on vérifie que l'on a $\gamma^4 \equiv s^2$ mod. 2. On en déduit que $\gamma^4 = s^2$, puis que $\gamma^2 = s$. En particulier, γ est dans μ_3, d'où une contradiction et notre assertion.

Puisque B_t est un carré dans K_{nr}, l'ordre de Φ est 2 ou 4 ([Kr2], th. 3). Par ailleurs, $B_{t'}$ n'étant pas un carré dans K_{nr}, Φ est d'ordre 4 ou 8 (*loc. cit.*). On a donc $|\Phi| = 4$. D'où la proposition.

On en déduit l'assertion 5 (a) du théorème de la façon suivante : supposons que la condition (C_2) soit satisfaite. Il existe $\gamma \in \mu_{r-1}$ qui n'est pas dans μ_3 tel que

$$j' \equiv \gamma^6\big(1 + 2\gamma^{-1}(1 + \gamma^2)\big) \text{ mod. } 4.$$

De l'égalité $j' = u^3$, on déduit alors l'existence d'un élément $t \in \mu_3$ tel que

$$tu \equiv \gamma^2 + 2\gamma(1 + \gamma^2) \text{ mod. } 4.$$

La proposition 4 entraîne que B_{t^2} est un carré dans K_{nr}. D'après la proposition 5 on a alors $|\Phi| = 4$.

Supposons que la condition (C_2) ne soit pas réalisée. Dans ce cas, pour tout $t \in \mu_3$, la condition (40) n'est pas satisfaite, et B_t n'est pas un carré dans K_{nr}. On a donc $|\Phi| = 8$ (prop. 5). D'où le résultat.

3.7.2. Cas où $2v(c_6) > 3v(c_4)$

Posons

$$\lambda = \frac{c_6^2}{c_4^3}.$$

On a $v(\lambda) \geqslant 1$. Démontrons l'énoncé suivant :

Proposition 6.

1. *Supposons* $v(\lambda) \geqslant 2$.

   (i) Supposons $v(c_4)$ *pair. On a* $|\Phi| = 4$ *s'il existe* $t \in \mu_3$, $t \neq 1$, *et* $b \in \mu_{r-1}$ *tels que*

   $$c_4' \equiv b(t+2) \text{ mod. } 4.$$

   On a $|\Phi| = 8$ *sinon.*

   (ii) Si $v(c_4)$ *est impair, on a* $|\Phi| = 8$.

2. *Supposons* $v(\lambda) = 1$.

   (i) Si $\lambda \equiv 2$ mod. 4, *on a* $|\Phi| = 4$.

   (ii) Si $\lambda \not\equiv 2$ mod. 4, *on a* $|\Phi| = 8$.

Démonstration : Soit ν la racine cubique de $1 - \lambda$ qui est congrue à 1 modulo 2. Il existe $s \in \mu_3$ tel que l'on ait (cf. (18))

$$\nu = \frac{12s}{j^{1/3}}. \tag{52}$$

On a les congruences

$$\nu \equiv 1 - \frac{\lambda}{3} - \frac{\lambda^2}{9} \text{ mod. } 8, \tag{53}$$

$$\nu^2 \equiv 1 - \frac{2\lambda}{3} - \frac{\lambda^2}{9} \text{ mod. } 8.$$

On a $\frac{B_s}{c_4^2} = 1 + \nu + \nu^2$, d'où il résulte que

$$\frac{B_s}{c_4^2} \equiv 3 - \lambda \text{ mod. } 8. \tag{54}$$

Choisissons une racine carrée $B_s^{1/2}$ de B_s dans $\overline{\mathbb{Q}_2}$ et posons

$$C_s = 2\big(c_4 + 6s\Delta^{1/3} + B_s^{1/2}\big).$$

1) Supposons que l'on ait $v(\lambda) \geqslant 2$. D'après (54), on a $\frac{B_s}{c_4^2} \equiv 3$ mod. 4. Puisque 3 n'est pas un carré dans K_{nr}, B_s n'est donc pas un carré dans K_{nr}. Par suite, on a

$$\frac{B_s^{1/2}}{c_4} \equiv \sqrt{3} \text{ mod. } 2. \tag{55}$$

Il résulte alors de (52) et des congruences (53) et (55), que l'on a

$$\frac{C_s}{c_4} \equiv 3 + 2\sqrt{3} \text{ mod. } 4. \tag{56}$$

Il s'agit alors de décider si C_s est un carré dans $K_{nr}\big(\sqrt{3}\big)$ (cf. [Kr2], th. 3).

1.1) Supposons que $v(c_4)$ est pair.

On utilise dans ce cas le résultat suivant :

Lemme 5. *Pour que C_s soit un carré dans $K_{nr}\big(\sqrt{3}\big)$ il faut et il suffit qu'il existe $t \in \mu_3$, $t \neq 1$, et $b \in \mu_{r-1}$ tels que l'on ait*

$$c_4' \equiv b(t+2) \text{ mod. } 4. \tag{57}$$

Démonstration : Posons $\pi = 1 + \sqrt{3}$. Supposons que C_s soit un carré dans $K_{nr}\big(\sqrt{3}\big)$. Puisque $v(c_4)$ est pair, $c_4'(1+2\pi)$ est alors un carré dans $K_{nr}\big(\sqrt{3}\big)$ (cf. (56) et le lemme 7 de [Kr2]). D'après le lemme 2, il existe donc $\gamma \in \mu_{r-1}$ et $\gamma' \in \mu_{r-1} \cup \big\{0\big\}$ tels que l'on ait

$$c_4'(1+2\pi) \equiv \gamma + \gamma'^2\pi^2 + \gamma^{\frac{r}{2}}\gamma'\pi^3 \text{ mod. } 4.$$

Par ailleurs, il existe deux éléments $a \in \mu_{r-1}$ et $b \in \mu_{r-1} \cup \{0\}$ tels que $c_4' \equiv a + 2b$ mod. 4. On a $2 \equiv \pi^2 - \pi^3$ mod. 4, d'où

$$c_4'(1+2\pi) \equiv a + b\pi^2 + (a+b)\pi^3 \text{ mod. } 4.$$

Il résulte de l'assertion 1 du lemme 1 que $a = \gamma$, $b = \gamma'^2$, puis $a + b \equiv \gamma^{\frac{r}{2}}\gamma'$ mod. 2. On en déduit que

$$(a+b)^2 \equiv ab \text{ mod. } 2.$$

Cela entraîne l'existence d'un élément $t \in \mu_3$, $t \neq 1$, tel que l'on ait

$$a \equiv tb \text{ mod. } 2.$$

Puisque a et tb sont des racines de l'unité d'ordre impair, on a donc $a = tb$. En particulier, b est non nul et la condition (57) est satisfaite.

Inversement, supposons la condition (57) réalisée. Dans ce cas, μ_3 est contenu dans μ_{r-1} : en effet, d'après l'assertion 1 du lemme 1, bt, puis t appartient à μ_{r-1}. Il s'agit de vérifier que $c_4'(1+2\pi)$ est un carré dans $K_{nr}\big(\sqrt{3}\big)$. D'après (57), on a

$$c_4'(1+2\pi) \equiv bt + b\pi^2 + t^2 b\pi^3 \text{ mod. } 4.$$

Posons

$$\gamma = bt \quad \text{et} \quad \gamma' = b^{\frac{r}{2}}.$$

Les éléments γ et γ' sont dans μ_{r-1}. Puisque 3 divise $r-1$, on a $t^{\frac{r}{2}} = t^2$. On constate alors que l'on a la congruence

$$c_4'(1+2\pi) \equiv \gamma + \gamma'^2\pi^2 + \gamma^{\frac{r}{2}}\gamma'\pi^3 \text{ mod. } 4,$$

ce qui, d'après le lemme 2, prouve notre assertion. D'où le lemme.

Le lemme 5 et le théorème 3 de [Kr2] entraînent l'assertion (i) de la proposition.

1.2) Supposons que $v(c_4)$ est impair.

Dans ce cas, C_s n'est pas un carré dans $K_{nr}\big(\sqrt{3}\big)$. En effet, d'après (56), on a la congruence

$$\frac{C_s}{2^{v(c_4)-1}} \equiv 2c_4' \text{ mod. } 4,$$

et l'assertion 5 du lemme 1 entraîne notre assertion. D'où l'assertion (ii) de la proposition (cf. [Kr2], th. 3).

2) Supposons que l'on ait $v(\lambda) = 1$. On a $2v(c_6) = 3v(c_4) + 1$, de sorte que

$$v(c_4) \equiv 1 \text{ mod. } 2. \tag{58}$$

2.1) Supposons $\lambda \equiv 2$ mod. 4.

D'après la congruence (54), on a $\frac{B_s}{c_4^2} \equiv 1$ mod. 4, ce qui montre que B_s est un carré dans K_{nr}. L'ordre de Φ est donc 2 ou 4. La condition (58) et l'assertion (iii) du théorème 2 de [Kr2] impliquent alors $|\Phi| = 4$.

2.2) Supposons $\lambda \not\equiv 2$ mod. 4. Il existe alors $\gamma \in \mu_{r-1}$, $\gamma \neq 1$ tel que l'on ait

$$\lambda \equiv 2\gamma \text{ mod. } 4.$$

D'après la formule (54), on a donc

$$\frac{B_s}{c_4^2} \equiv 3 + 2\gamma \text{ mod. } 4.$$

Puisque γ est distinct de 1, on a $\gamma + 1 \not\equiv 0$ mod. 2 et donc $v\Big(\frac{B_s}{c_4^2} - 1\Big) = 1$. Par conséquent, B_s n'est pas un carré dans K_{nr}. Par ailleurs, on a

$$\frac{C_s}{c_4} = 2 + \nu + 2\frac{B_s^{1/2}}{c_4}.$$

Il en résulte que

$$\frac{C_s}{2^{v(c_4)-1}} \equiv 2c_4' \text{ mod. } 4.$$

La condition (58) et l'assertion 5 du lemme 1 entraînent alors que C_s n'est pas un carré dans $K_{nr}\big(B_s^{1/2}\big)$. On a donc $|\Phi| = 8$. D'où l'assertion 2) (ii) de la proposition et le résultat.

On en déduit ensuite l'assertion 5 (b) du théorème : on a l'égalité $1 - \lambda = \frac{27}{j'}$. Ainsi, on a $\lambda \equiv 2$ mod. 4 si et seulement si $j' \equiv 1$ mod. 4 ; cela entraîne le résultat (prop. 6). En ce qui concerne l'assertion 5 (c) du théorème, elle résulte directement l'assertion 1 de la proposition 6.

Cela termine la démonstration du théorème.

4. Démonstration du corollaire

Les assertions 1, 2 et 3 sont des conséquences directes du théorème. Il en est de même de l'assertion 5, en remarquant que la condition (C_2) ne peut être satisfaite si $K = \mathbb{Q}_2(\mu_3)$.

Pour la démonstration des assertions 4, 6 et 7, on utilisera l'article [Pa] de Papadopoulos et l'on suivra ses notations.

4.1. L'assertion 4 du corollaire

On a $v(j) = 4$.

Démontrons l'assertion 4 (a). Supposons que la condition (C_1) soit vérifiée, autrement dit, qu'il existe $\gamma \in \mu_3$ tel que l'on ait la congruence

$$j' \equiv \gamma + 2\gamma^2 \text{ mod. } 4. \tag{59}$$

D'après le théorème, l'ordre de Φ est 3 ou 6.

Soit ζ un élément de μ_3 tel que $c_6' \equiv \zeta$ mod. 2. Prouvons le lemme suivant :

Lemme 6. *Supposons que l'on ait* $\big(v(c_4), v(c_6), v(\Delta)\big) = (4, 6, 8)$.

1. *Si* $\gamma \neq 1$, *le type de réduction de* E *est* IV^* *si et seulement si* $c_6' \equiv \zeta$ mod. 4.

2. *Si $\gamma = 1$, le type de réduction de E est IV^* si et seulement si $c'_6 \equiv -\zeta$ mod. 4.*

Démonstration : D'après le tableau IV de [Pa], le type de réduction de E est I_0^*, I_1^* ou IV^*. Par ailleurs, la courbe elliptique E admet un modèle minimal sur K de la forme

$$y^2 = x^3 - \frac{c'_4}{3}x - \frac{2c'_6}{27}.$$

Les invariants standard associés à E sont (cf. [Ta])

$$a_1 = 0, \quad a_2 = 0, \quad a_3 = 0, \quad a_4 = -\frac{c'_4}{3}, \quad a_6 = -\frac{2c'_6}{27},$$

$$b_2 = 0, \quad b_4 = -\frac{2c'_4}{3}, \quad b_6 = -\frac{8c'_6}{27}, \quad b_8 = -\frac{{c'_4}^2}{9}.$$

De l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on déduit que l'on a ${c'_4}^3 \equiv {c'_6}^2$ mod. 4. Cela implique que c'_4 est un carré dans K_{nr}. D'après le lemme 1, il existe donc $\nu \in \mu_3$ tel que l'on ait

$$c'_4 \equiv \nu \text{ mod. } 4.$$

1. Supposons $\gamma \neq 1$. On utilise les propositions 3 et 4 de [Pa]. Posons

$$r = -\frac{c'_6}{c'_4}.$$

On vérifie que l'on a

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

Posons

$$t = 2\gamma^2\zeta^2.$$

En utilisant la congruence

$$\frac{{c'_6}^2}{{c'_4}^3} \equiv 1 - \frac{12}{j'} \text{ mod. } 16,$$

on vérifie que 8 divise $a_6 + ra_4 + r^3 - t^2$.

Si l'on a $c'_6 \not\equiv \zeta$ mod. 4, on a $v(a_6 + ra_4 + r^3 - t^2) = 3$ et dans ce cas le type de réduction de E est I_0^* ([Pa], prop. 3).

Supposons que l'on ait $c'_6 \equiv \zeta$ mod. 4. On a alors $v(a_6 + ra_4 + r^3 - t^2) \geqslant 4$, d'où il résulte que le type de réduction de E est I_1^* ou IV^*. Posons

$$s = \frac{\nu}{\zeta}.$$

On a alors la congruence $3r \equiv s^2$ mod. 4. D'après la proposition 4 de [Pa], le type de réduction de E est donc IV^*. D'où l'assertion 1 du lemme.

2. Supposons $\gamma = 1$. On pose dans ce cas

$$r = \frac{c'_6}{c'_4}.$$

On a la congruence $b_8 + 3rb_6 + 3r^2b_4 + 3r^4 \equiv 0$ mod. 32. En posant

$$t = 2\zeta^2,$$

on constate que 8 divise $a_6 + ra_4 + r^3 - t^2$.

Si $c'_6 \not\equiv -\zeta$ mod. 4, on a $v(a_6 + ra_4 + r^3 - t^2) = 3$ et le type de réduction de E est I_0^*.

Si $c'_6 \equiv -\zeta$ mod. 4, on a $v(a_6 + ra_4 + r^3 - t^2) \geqslant 4$. Avec $s = \nu/\zeta$, on vérifie que l'on a $3r \equiv s^2$ mod. 4, et donc le type de réduction de E est IV^*. D'où le lemme.

Supposons que l'on ait $|\Phi| = 3$. L'égalité $v(j) = 4$ et l'assertion (i) du théorème 2 de [Kr2] entraînent que le type de réduction de E est IV^*, et que

$$\big(v(c_4), v(c_6), v(\Delta)\big) = (4, 6, 8). \tag{60}$$

D'après le lemme 6, la condition (ii) de l'énoncé est réalisée. Inversement, si la condition (i) est satisfaite, on a l'égalité (60), et si la condition (ii) est réalisée, le lemme 6 montre que le type de réduction de E est IV^*. On a ainsi $|\Phi| = 3$ ([Kr2], th. 2). D'où l'assertion 4 (a) du corollaire.

En ce qui concerne l'assertion 4 (b), elle résulte directement du théorème.

4.2. L'assertion 6 du corollaire

On a $v(j) = 8$.

Prouvons l'assertion 6 (a). Supposons la condition (C_3) vérifiée, i.e. qu'il existe $\gamma \in \mu_3$ tel que l'on ait

$$j' \equiv \gamma + 2 \text{ mod. } 4. \tag{61}$$

D'après le théorème, l'ordre de Φ est 3 ou 6.

Soient α_1, β_1 des éléments de μ_3 et α_2, β_2 des éléments de $\mu_3 \cup \{0\}$ tels que

$$c'_4 \equiv \alpha_1 + 2\alpha_2 \text{ mod. } 4 \quad \text{et} \quad c'_6 \equiv \beta_1 + 2\beta_2 \text{ mod. } 4.$$

On a le lemme suivant :

Lemme 7. *Supposons que l'on ait* $\big(v(c_4), v(c_6), v(\Delta)\big) = (4, 5, 4)$. *Alors, le type de réduction de E est IV si et seulement si on a*

$$\alpha_2 = \alpha_1\beta_1^2 \quad \textit{et} \quad \beta_2 \equiv 1 + \beta_1^2 \text{ mod. } 2. \tag{62}$$

Démonstration : D'après le tableau IV de [Pa], le type de réduction de E est II, III ou IV. La courbe elliptique E admet un modèle minimal sur K de la forme

$$y^2 = x^3 - \frac{c'_4}{3}x - \frac{c'_6}{27}.$$

Les invariants standard associés à E sont

$$a_1 = 0, \quad a_2 = 0, \quad a_3 = 0, \quad a_4 = -\frac{c'_4}{3}, \quad a_6 = -\frac{c'_6}{27},$$

$$b_2 = 0, \quad b_4 = -\frac{2c'_4}{3}, \quad b_6 = -\frac{4c'_6}{27}, \quad b_8 = -\frac{{c'_4}^2}{9}.$$

On utilise la proposition 1 de *loc. cit.* avec

$$r = \alpha_1^2 \quad \text{et} \quad t = \beta_1^2.$$

On constate que le type de réduction de E est III ou IV si et seulement si on a

$$\beta_2 + \alpha_2\alpha_1^2 \equiv 1 \text{ mod. } 2. \tag{63}$$

Supposons la condition (63) réalisée. On a $v(b_8 + 3rb_6 + 3r^2b_4 + 3r^4) \geqslant 3$ si et seulement si 2 divise $\alpha_2^2 + \beta_1\alpha_1^2$, i.e. si l'on a

$$\alpha_2^2 = \beta_1\alpha_1^2. \tag{64}$$

Il en résulte que le type de réduction de E est IV si et seulement si les conditions (63) et (64) sont satisfaites, i.e. si la condition (62) est réalisée. D'où le lemme.

Supposons que l'on ait $|\Phi| = 3$. L'égalité $v(j) = 8$ et l'assertion (i) du théorème 2 de [Kr2] entraînent que le type de réduction de E est IV, et que

$$\big(v(c_4), v(c_6), v(\Delta)\big) = (4, 5, 4). \tag{65}$$

De l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on déduit que l'on a la congruence $j' \equiv \frac{{c'_4}^3}{{c'_6}^2}$ mod. 4. Par ailleurs, on a

$${c'_4}^3 \equiv 1 + 2\alpha_1^2\alpha_2 \text{ mod. } 4 \quad \text{et} \quad {c'_6}^2 \equiv \beta_1^2 \text{ mod. } 4,$$

d'où il résulte que

$$j' \equiv \beta_1\big(1 + 2\alpha_1^2\alpha_2\big) \text{ mod. } 4. \tag{66}$$

D'après le lemme 7 et la congruence (66), on obtient ainsi $j' \equiv \beta_1 + 2$ mod. 4. D'après la condition (61), on a donc

$$\gamma = \beta_1. \tag{67}$$

Si $\gamma = 1$, on déduit de (67) et (62) que $\beta_2 = 0$, d'où $c_6' \equiv 1 \bmod. 4$. Si $\gamma \neq 1$, on a $\beta_2 \equiv -\gamma \bmod. 2$ (cf. (62)), puis $c_6' \equiv -\gamma \bmod. 4$. La condition (ii) de l'assertion 6 (a) est donc satisfaite.

Inversement, supposons les conditions (i) et (ii) de l'énoncé réalisées. L'égalité (65) est alors vérifiée.

Supposons que l'on ait $\gamma = 1$ et $c_6' \equiv 1 \bmod. 4$. Dans ce cas, on a $\beta_1 = 1$ et $\beta_2 = 0$. Par ailleurs, on a $j' \equiv -1 \bmod. 4$, et l'on déduit de (66) la congruence $\alpha_1^2\alpha_2 \equiv 1 \bmod. 2$. On a donc $\alpha_1 = \alpha_2$ et la condition (62) est vérifiée.

Supposons que l'on ait $\gamma \neq 1$ et $c_6' \equiv -\gamma \bmod. 4$. On a alors $\beta_1 = \beta_2 = \gamma$. D'après (61) et (66), on obtient $\alpha_1 \equiv \gamma\alpha_2 \bmod. 2$. Par suite, on a $\alpha_2 = \gamma^2\alpha_1$, et la condition (62) est de nouveau vérifiée.

D'après le lemme 7, le type de réduction de E est IV, ce qui entraîne que $|\Phi| = 3$. Cela prouve l'assertion 6 (a) du corollaire.

L'assertion 6 (b) résulte directement du théorème.

4.3. L'assertion 7 du corollaire

On a $v(j) \geqslant 12$.

Démontrons la remarque qui suit l'énoncé du théorème. C'est une conséquence du lemme suivant :

Lemme 8.

1. *Supposons que l'on ait $v(c_4) \geqslant 6$, $v(c_6) = 5$ et $v(\Delta) = 4$. Alors, le type de réduction de E est IV si et seulement si il existe $\zeta \in \mu_{r-1}$ tel que $c_6' \equiv \zeta \bmod. 4$.*
2. *Supposons que l'on ait $v(c_4) \geqslant 7$, $v(c_6) = 7$ et $v(\Delta) = 8$. Alors, le type de réduction de E est IV^* si et seulement si il existe $\zeta \in \mu_{r-1}$ tel que $c_6' \equiv \zeta \bmod. 4$.*

Démonstration : La courbe elliptique E possède un modèle minimal sur K de la forme

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}.$$

Soit ζ un élément de μ_{r-1} tel que $c_6' \equiv \zeta \bmod. 2$.

1. Le type de réduction de E est II ou IV. En utilisant la proposition 1 de [Pa] avec $r = 0$ et $t = \zeta^{\frac{r}{2}}$, on constate que le type de réduction de E est IV si et seulement si $c_6' \equiv \zeta \bmod. 4$.

2. Le type de réduction de E est I_0^* ou IV^*. On applique dans ce cas la proposition 3 de *loc. cit.* avec $r = 0$ et $t = 2\zeta^{\frac{r}{2}}$ pour obtenir le résultat.

L'assertion 7 (a) résulte du théorème. Prouvons l'assertion 7 (b). Supposons que l'on ait $|\Phi| = 3$. Dans ce cas le type de réduction de E est IV ou IV^*. On a alors $v(\Delta) = 4$

ou $v(\Delta) = 8$. D'après l'inégalité $v(j) \geqslant 12$, le triplet $\big(v(c_4), v(c_6), v(\Delta)\big)$ vérifient ainsi les hypothèses faites dans le lemme 8. Les conditions (i) et (ii) de l'énoncé sont donc satisfaites. Inversement, si ces conditions sont réalisées, le type de réduction de E est IV ou IV^* (lemme 8) et on a $|\Phi| = 3$. Le théorème entraîne alors le résultat.

Cela termine la démonstration du corollaire.

Chapitre III

Sur le discriminant des corps des points de ℓ-torsion des courbes elliptiques

Considérons une courbe elliptique $E/\mathbb{Q}$ définie par une équation de Weierstrass, et un nombre premier ℓ. Notons $\mathbb{Q}(E_\ell)$ le corps des points de ℓ-torsion de E. C'est le sous-corps de $\mathbb{C}$ engendré par les coordonnées des points de ℓ-torsion de E. L'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$ est galoisienne et son groupe de Galois, qui est isomorphe à un sous-groupe de $\mathbb{G}L_2(\mathbb{F}_\ell)$, est essentiellement connu (cf. [Se1]). L'objectif de ce chapitre est de préciser dans quelle mesure les résultats obtenus dans le chapitre I, ainsi que dans [Kr4], permettent d'obtenir des informations sur le discriminant de $\mathbb{Q}(E_\ell)$ et parfois de le déterminer. En application, on l'explicitera si l'invariant modulaire de $E/\mathbb{Q}$ est 1728. On étudiera par ailleurs le cas où E est la courbe elliptique de conducteur 11 d'équation $y^2 - y = x^3 - x^2$.

1. Lien entre la différente et le discriminant

Soient K une extension galoisienne de $\mathbb{Q}$ de degré d et D_K le discriminant de K. Rappelons que la différente de l'extension $K/\mathbb{Q}$ est un idéal de l'anneau d'entiers O_K de K, dont la norme sur $\mathbb{Q}$ est la valeur absolue de D_K. Le signe de D_K est $(-1)^{r_2}$, où r_2 est le nombre de places complexes de K. Pour tout nombre premier p, on note e_p l'indice de ramification de p dans K et n_p l'exposant d'un idéal premier de O_K divisant p dans la différente de $K/\mathbb{Q}$. Puisque $K/\mathbb{Q}$ est galoisienne, il est le même pour tous les idéaux premiers divisant p.

Lemme. *On a l'égalité*

$$|D_K|^{\frac{1}{d}} = \prod_p p^{\frac{n_p}{e_p}}. \tag{1}$$

Démonstration : Ce produit est fini car $n_p = 0$ si p est non ramifié dans K. Soient p un nombre premier, g_p le nombre d'idéaux premiers de O_K divisant p et f_p leur degré résiduel commun. Leur norme est p^{f_p} et leur contribution à la norme de la différente est donc

$$(p^{f_p})^{g_p n_p}.$$

L'égalité $d = e_p f_p g_p$ entraîne alors le résultat.

Prenons pour K le corps $\mathbb{Q}(E_\ell)$ des points de ℓ-torsion d'une courbe elliptique $E/\mathbb{Q}$. L'étude faite dans [Se1] permet généralement de calculer le degré de $\mathbb{Q}(E_\ell)$ sur $\mathbb{Q}$. Par ailleurs, les résultats obtenus dans *loc. cit.* ainsi que dans [Kr3] permettent de déterminer les indices de ramification e_p dans l'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$. En ce qui concerne les exposants

n_p, ils ont été déterminés dans le chapitre I dans tous les cas où $p \neq \ell$, et dans [Kr4] il se trouve la détermination de n_ℓ. Il convient de remarquer, notamment si E a bonne réduction ordinaire en ℓ, que la connaissance de n_ℓ et e_ℓ nécessite de déterminer si l'inertie en ℓ dans $\mathbb{Q}(E_\ell)/\mathbb{Q}$ est modérée ou non, i.e. si le degré des sous-groupes d'inertie en ℓ de $\mathrm{Gal}\big(\mathbb{Q}(E_\ell)/\mathbb{Q}\big)$ est d'ordre premier à ℓ ou non. Il est facile de le décider si par exemple E a des multiplications complexes, ou bien si l'invariant modulaire de la courbe elliptique $\widetilde{E}(\ell)$ sur $\mathbb{F}_\ell$ déduite de E par réduction est 0 ou 1728. Il n'en va pas de même dans le cas général. On est alors amené à déterminer la congruence modulo ℓ^2 de l'invariant modulaire du relèvement canonique de $\widetilde{E}(\ell)$ ([Kr4]). En fonction de cette congruence, il y a deux valeurs possibles pour n_ℓ (*loc. cit.*). On illustrera cette situation dans le paragraphe 3 avec la courbe de conducteur 11 signalée prédemment.

2. Courbes elliptiques d'invariant modulaire 1728

Considérons une courbe elliptique E définie sur $\mathbb{Q}$ d'invariant modulaire $j = 1728$. Il existe un entier $a \in \mathbb{Z}$ non nul et sans puissances quatrièmes, tel que E admette une équation de Weierstrass de la forme

$$y^2 = x^3 + ax. \tag{2}$$

La courbe est à multiplications complexes et son anneau d'endomorphismes est isomorphe à $\mathbb{Z}[i]$ où $i^2 = -1$ (cf. [Si2], p. 74). Pour tout nombre premier ℓ, on va calculer le discriminant $D(\ell)$ du corps $\mathbb{Q}(E_\ell)$ des points de ℓ-torsion de E. Remarquons que l'on a

$$\mathbb{Q}(E_2) = \mathbb{Q}\big(\sqrt{-a}\big),$$

dont le discriminant est connu. On supposera donc dans toute la suite que l'on a $\ell \geqslant 3$.

Les invariants standard c_4, c_6 et Δ associés à l'équation (2) sont (cf. [Ta]) :

$$c_4 = -2^4.3.a, \quad c_6 = 0 \quad \text{et} \quad \Delta = -2^6.a^3. \tag{3}$$

Pour tout nombre premier p, notons v_p la valuation p-adique de $\mathbb{Q}$. Puisque que l'on a $v_p(a) < 4$ pour tout p, l'équation (2) est un modèle minimal de E (cf. par exemple le lemme 1 du chap. V). Posons

$$m_p = \text{dénominateur}\left(\frac{v_p(a)}{4}\right) \quad \text{si} \quad p \geqslant 3, \tag{4}$$

$$m_2 = \begin{cases} 4 & \text{si } \ a \equiv 3 \bmod. 4 \text{ ou } a \equiv 4 \bmod. 16 \\ 9/2 & \text{si } \ a \equiv 1 \bmod. 4 \text{ ou } a \equiv 12 \bmod. 16 \\ 6 & \text{si } \ v_2(a) \in \big\{1, 3\big\}. \end{cases} \tag{5}$$

On va démontrer le résultat suivant :

Theorème 1.

1) Supposons $\ell \equiv 1$ mod. 4. *On a*

$$D(\ell) = 2^{m_2(\ell-1)^2}\ \ell^{2(\ell-1)(\ell-2)} \prod_{p\geqslant 3,\ p\neq\ell,\ p|a} p^{\frac{2(\ell-1)^2(m_p-1)}{m_p}}.$$

2) Supposons $\ell \equiv 3$ mod. 4. *On a*

$$D(\ell) = 2^{m_2(\ell^2-1)}\ \ell^{2(\ell^2-2)} \prod_{p\geqslant 3,\ p\neq\ell,\ p|a} p^{\frac{2(\ell^2-1)(m_p-1)}{m_p}}.$$

Démonstration : Conformément à l'égalité (1), il s'agit de déterminer le degré d de l'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$. Soit $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. Notons

$$\rho_\ell : \mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big) \to \mathrm{Aut}(E_\ell),$$

la représentation donnant l'action de $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ sur E_ℓ. Le groupe $\mathrm{Aut}(E_\ell)$ s'identifie à $\mathbb{G}L_2(\mathbb{F}_\ell)$ via le choix d'une base de E_ℓ sur $\mathbb{F}_\ell$.

Proposition. *L'image de* ρ_ℓ *est le normalisateur d'un sous-groupe de Cartan de* $\mathrm{Aut}(E_\ell)$. *Il est déployé si* $\ell \equiv 1$ mod. 4 *et non déployé si* $\ell \equiv 3$ mod. 4. *En particulier, on a*

$$d = \begin{cases} 2(\ell-1)^2 & \text{si } \ell \equiv 1 \text{ mod. } 4 \\ 2(\ell^2-1) & \text{si } \ell \equiv 3 \text{ mod. } 4. \end{cases}$$

Rappelons qu'un élément de $\mathrm{Aut}(E_\ell)$ est dit semi-simple si son polynôme minimal de $\mathbb{F}_\ell[X]$ est séparable. Un sous-groupe de Cartan de $\mathrm{Aut}(E_\ell)$ est le centralisateur d'un élément semi-simple de $\mathrm{Aut}(E_\ell)$ qui n'est pas une homothétie. On dit qu'un tel sous-groupe est déployé si le polynôme minimal de l'élément centralisé associé est réductible sur $\mathbb{F}_\ell$, et non déployé dans le cas contraire. Un sous-groupe de Cartan déployé est d'ordre $(\ell-1)^2$ isomorphe à $\mathbb{F}_\ell^* \times \mathbb{F}_\ell^*$, et un sous-groupe de Cartan non déployé est cyclique d'ordre ℓ^2-1. Par ailleurs, un sous-groupe de Cartan de $\mathrm{Aut}(E_\ell)$ est d'indice 2 dans son normalisateur (cf. [Se1]).

2.1. Démonstration de la proposition

On note M l'image de ρ_ℓ et M_0 l'image du sous-groupe $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}(i)\big)$.

1) Prouvons d'abord que M est contenu dans le normalisateur d'un sous-groupe de Cartan de $\mathrm{Aut}(E_\ell)$. On dispose de l'endomorphisme $\psi : E \to E$ défini pour tout point $P = (x, y) \in E\big(\overline{\mathbb{Q}}\big)$ par l'égalité

$$\psi\big((x,y)\big) = (-x, iy). \tag{6}$$

Il induit un endomorphisme du $\mathbb{F}_\ell$-espace vectoriel E_ℓ, que l'on notera encore ψ. On a $\psi\big(\psi(P)\big) = -P$ i.e. ψ^2 est moins l'identité de E_ℓ. Le déterminant de ψ est donc non nul et ψ est un automorphisme de E_ℓ. Ce n'est pas une homothétie de E_ℓ (cf. [Si-Ta], démonstration du lemme 1 p. 206). Le polynôme minimal de ψ est donc $X^2+1 \in \mathbb{F}_\ell[X]$ qui est séparable : si $\ell \equiv 3$ mod. 4 il est irréductible sur $\mathbb{F}_\ell$, et si $\ell \equiv 1$ mod. 4 il possède deux racines distinctes dans $\mathbb{F}_\ell$. Par suite, ψ est semi-simple. Soit C le centralisateur de ψ dans $\mathrm{Aut}(E_\ell)$. C'est un sous-groupe de Cartan de $\mathrm{Aut}(E_\ell)$. Il est déployé si $\ell \equiv 1$ mod. 4 et non déployé sinon.
Soit N le normalisateur de C dans $\mathrm{Aut}(E_\ell)$. On va démontrer que M est contenu dans N. Puisque ψ est défini sur $\mathbb{Q}(i)$, l'image M_0 centralise ψ, autrement dit, M_0 est contenu dans C. Considérons alors un élément $g \in M - M_0$. Il existe $\sigma \in \mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ tel que $\sigma(i) \neq i$ et que $g = \rho_\ell(\sigma)$. On a ${}^\sigma\psi = -\psi$ et pour tout point $P \in E_\ell$, on a donc

$$ {}^\sigma\big(\psi(P)\big) = -\psi\big({}^\sigma P\big). \tag{7}$$

On déduit alors de (7) que pour tout $P \in E_\ell$, on a l'égalité

$$ g\psi g^{-1}(P) = -\psi(P). \tag{8}$$

Il résulte de (8) que pour tout $\alpha \in C$, l'élément $g\alpha g^{-1}$ appartient à C, autrement dit, g appartient à N, d'où l'assertion.

2) Démontrons que le corps $\mathbb{Q}(i)$ est contenu dans $\mathbb{Q}(E_\ell)$. Considérons pour cela un élément $\sigma \in \mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ et prouvons l'équivalence

$$ \rho_\ell(\sigma) \in C \Longleftrightarrow \sigma(i) = i. \tag{9}$$

Cela entraînera en particulier notre assertion (si σ fixe E_ℓ, on a $\rho_\ell(\sigma) = 1 \in C$). Supposons que $\rho_\ell(\sigma)$ soit dans C. Puisque C est le centralisateur de ψ, on a $\rho_\ell(\sigma)\psi = \psi\rho_\ell(\sigma)$. Soit $P = (x, y)$ un point de E_ℓ. On a ${}^\sigma(\psi(P)) = \psi({}^\sigma(P))$, ce qui, d'après (6), se traduit par l'égalité

$$\big(-\sigma(x), \sigma(i)\sigma(y)\big) = \big(-\sigma(x), i\sigma(y)\big).$$

Puisque l'on a $\ell \geqslant 3$, on a $y \neq 0$, d'où $\sigma(i) = i$. Inversement, supposons que l'on ait $\sigma(i) = i$. Soit $P = (x, y)$ un point de E_ℓ. On a les égalités

$$\rho_\ell(\sigma)\psi\big((x,y)\big) = \big(-\sigma(x), \sigma(i)\sigma(y)\big) = \big(-\sigma(x), i\sigma(y)\big) = \psi\big(\rho_\ell(\sigma)\big((x,y)\big)\big).$$

Par suite, $\rho_\ell(\sigma)$ commute avec ψ, d'où $\rho_\ell(\sigma) \in C$ et l'équivalence (9).

Notons encore ρ_ℓ la représentation fidèle passée au quotient de $\mathrm{Gal}\big(\mathbb{Q}(E_\ell)/\mathbb{Q}\big)$ dans $\mathrm{Aut}(E_\ell)$. On a $M_0 = \rho_\ell\big(\mathrm{Gal}\big(\mathbb{Q}(E_\ell)/\mathbb{Q}(i)\big)\big)$. On déduit de l'alinéa 2 que ρ_ℓ induit un isomorphisme de $\mathrm{Gal}\big(\mathbb{Q}(E_\ell)/\mathbb{Q}(i)\big)$ sur $C \cap M$, autrement dit, que $M_0 = C \cap M$. On va démontrer que ρ_ℓ induit en fait un isomorphisme de $\mathrm{Gal}\big(\mathbb{Q}(E_\ell)/\mathbb{Q}(i)\big)$ sur C, soit encore que l'on a

$$ M_0 = C. \tag{10}$$

Cela entraînera la proposition. En effet, C étant d'indice 2 dans N, l'égalité (10) implique que ρ est un isomorphisme de $\mathrm{Gal}\big(\mathbb{Q}(E_\ell)/\mathbb{Q}\big)$ sur N. Par ailleurs, l'ordre de C est $(\ell-1)^2$ si $\ell \equiv 1$ mod. 4 et est ℓ^2-1 sinon.

3) Considérons l'anneau d'entiers A de $\mathbb{Q}(E_\ell)$ et $\mathfrak{L}$ un idéal premier de A au-dessus de ℓ. Soit $I_\mathfrak{L}$ le sous-groupe d'inertie de $\mathfrak{L}$ sur ℓ. Vérifions que $I_\mathfrak{L}$ est un sous-groupe de $\mathrm{Gal}\big(\mathbb{Q}(E_\ell)/\mathbb{Q}(i)\big)$. Cela prouvera que $\rho_\ell(I_\mathfrak{L})$ est contenu dans M_0. Soit σ un élément de $I_\mathfrak{L}$. Pour tout $x \in A$, $\sigma(x)-x$ appartient à $\mathfrak{L}$. Il en résulte que pour tout $x \in \mathbb{Z}[i]$, $\sigma(x)-x$ appartient à $\mathfrak{L}_1 := \mathfrak{L}\cap\mathbb{Z}[i]$, autrement dit, la restriction de σ à $\mathbb{Q}(i)$ appartient au sous-groupe d'inertie de $\mathfrak{L}_1$ de $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. Puisque $\mathbb{Q}(i)/\mathbb{Q}$ est non ramifié en ℓ, ce sous-groupe d'inertie est trivial, et σ fixe donc $\mathbb{Q}(i)$, d'où l'assertion.

4) Supposons $\ell \equiv 1$ mod. 4 et démontrons l'égalité (10).

4.1) Vérifions que M_0 contient le sous-groupe de $\mathrm{Aut}(E_\ell)$ formé des homothéties. On choisit pour cela un nombre premier vérifiant les conditions suivantes :

(i) q est inerte dans $\mathbb{Q}(i)$.

(ii) q ne divise pas a.

(iii) $-q$ mod. ℓ est un générateur de $\mathbb{F}_\ell^*$.

Le théorème chinois et le théorème de Dirichlet entraînent l'existence d'un tel nombre premier q. On a $q \neq 2, \ell$ et la condition (ii) entraîne que E a bonne réduction en q. D'après le critère de Néron-Ogg-Shafarevitch, l'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$ est donc non ramifiée en q ([Si2], p. 184). La substitution de Frobenius en q dans $\mathrm{Gal}\big(\mathbb{Q}(E_\ell)/\mathbb{Q}\big)$, notons la σ_q, qui est bien définie à conjugaison près, ne fixe pas $\mathbb{Q}(i)$ (condition (i)) et d'après l'équivalence (9), $\rho_\ell(\sigma_q)$ n'appartient pas à C. Puisque que $\rho_\ell(\sigma_q)$ est dans le normalisateur N de C, sa trace est donc nulle. Par ailleurs, le déterminant de $\rho_\ell(\sigma_q)$ est q mod. ℓ (cf. [Se1], p. 303). On en déduit que $\rho_\ell(\sigma_q)^2$ est l'homothétie de rapport $-q$ mod. ℓ. La condition (iii) implique alors notre assertion.

On est alors amené à considérer deux cas selon que ℓ divise a ou non.

4.2) Supposons que ℓ ne divise pas a. Dans ce cas, ℓ étant congru à 1 modulo 4, la courbe E a bonne réduction ordinaire en ℓ. Puisque l'ordre de N est premier à ℓ, il en est de même du degré de $\mathbb{Q}(E_\ell)$ sur $\mathbb{Q}$ d'après l'alinéa 1. On déduit alors du corollaire p. 274 de [Se1] que $\rho(I_\mathfrak{L})$ est d'ordre $\ell-1$ et que la restriction de ρ_ℓ à $I_\mathfrak{L}$ est représentable matriciellement sous la forme

$$\begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix},$$

où $\chi : I_\mathfrak{L} \to \mathbb{F}_\ell^*$ est le caractère cyclotomique donnant l'action de $I_\mathfrak{L}$ sur le groupe des racines ℓ-ièmes de l'unité. Soit H le sous-groupe des homothéties de $\mathrm{Aut}(E_\ell)$. L'intersection $\rho_\ell(I_\mathfrak{L}) \cap H$ est triviale. Compte tenu des alinéas 3 et 4.1, $\rho_\ell(I_\mathfrak{L})H$ est donc un sous-groupe de M_0 d'ordre $(\ell-1)^2$. Puisque C est d'ordre $(\ell-1)^2$ et que M_0 est contenu dans C, on a donc $M_0 = C$.

4.2) Supposons que ℓ divise a. Dans ce cas, E a réduction additive en ℓ. On a $\ell \geqslant 5$. D'après le lemme 1 et la proposition 1 de [Kr3], la restriction de ρ_ℓ à $I_{\mathfrak{L}}$ est représentable matriciellement sous la forme

$$\begin{pmatrix} \chi^{1-\alpha} & * \\ 0 & \chi^{\alpha} \end{pmatrix} \quad \text{avec} \quad \alpha = \frac{(\ell-1)v_\ell(a)}{4}.$$

Vérifions que $H \cap \rho_\ell\big(I_{\mathfrak{L}}\big)$ est réduit à l'identité. Considérons pour cela un élément σ de $I_{\mathfrak{L}}$ tel que $\chi^{1-\alpha}(\sigma) = \chi^{\alpha}(\sigma)$ i.e. tel que $\chi^{2\alpha-1}(\sigma) = 1$. On a

$$\chi^{2\alpha-1}(\sigma) = \Big(\chi^{(\ell-1)/2}(\sigma)\Big)^{v_\ell(a)}\chi(\sigma)^{-1}.$$

Puisque $\ell \equiv 1$ mod. 4, $(\ell-1)/2$ est pair, d'où $\chi^{(\ell-1)/2}(\sigma) = 1$ puis $\chi(\sigma) = 1$ et l'assertion. En particulier, le groupe $\rho(I_{\mathfrak{L}})$, qui n'est pas trivial, n'est pas contenu dans H. Par ailleurs, $\rho(I_{\mathfrak{L}})$ est contenu dans C, qui est un sous-groupe de Cartan déployé. Il existe donc exactement deux droites de E_ℓ stables sous l'action de $I_{\mathfrak{L}}$. Il en résulte que la restriction de ρ_ℓ à $I_{\mathfrak{L}}$ est représentable matriciellement sous la forme

$$\begin{pmatrix} \chi^{1-\alpha} & 0 \\ 0 & \chi^{\alpha} \end{pmatrix}.$$

L'ordre de χ est $\ell - 1$. Par suite, $\rho_\ell(I_{\mathfrak{L}})$ est aussi d'ordre $\ell - 1$. Puisque $H \cap \rho_\ell\big(I_{\mathfrak{L}}\big)$ est réduit à l'identité, $\rho_\ell(I_{\mathfrak{L}})H$ est donc un sous-groupe de M_0 d'ordre $(\ell-1)^2$, ce qui entraîne comme ci-dessus que $M_0 = C$.

5) Supposons $\ell \equiv 3$ mod. 4.

5.1) Supposons que ℓ ne divise pas a. Dans ce cas, E a bonne réduction supersingulière en ℓ. D'après la proposition 12 de [Se1], $\rho_\ell\big(I_{\mathfrak{L}}\big)$ est cyclique d'ordre $\ell^2 - 1$. Par ailleurs, C est aussi d'ordre $\ell^2 - 1$. Il en résulte que $C = M_0$. [En fait, l'image par ρ_ℓ du sous-groupe de décomposition en $\mathfrak{L}$ de $\mathrm{Gal}\big(\mathbb{Q}(E_\ell)/\mathbb{Q}\big)$ est le normalisateur N (*loc. cit.*).]

5.2) Supposons que ℓ divise a.

5.2.1) Supposons $\ell \geqslant 5$. D'après les lemmes 1 et 2 ainsi que la proposition 2 de [Kr3], la représentation de $I_{\mathfrak{L}}$ dans $E_\ell \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}_\ell}$, que l'on déduit de la restriction de ρ_ℓ à $I_{\mathfrak{L}}$ par extension des scalaires, est représentable sous la forme

$$\begin{pmatrix} \psi^{\alpha}\psi'^{\ell-\alpha} & 0 \\ 0 & \psi'^{\alpha}\psi^{\ell-\alpha} \end{pmatrix} \quad \text{avec} \quad \alpha = \frac{(\ell+1)v_\ell(a)}{4},$$

où ψ et ψ' sont appelés par Serre dans [Se1] les deux caractères fondamentaux de niveau 2. On a $\psi' = \psi^\ell$ et ψ est un caractère d'ordre $\ell^2 - 1$. Posons $\varphi = \psi^{\alpha}\psi'^{\ell-\alpha}$. On a

$$\varphi = \begin{cases} \psi^{\frac{3\ell^2+1}{4}} & \text{si} \quad v_\ell(a) = 1 \\ \psi^{\frac{\ell^2+1}{2}} & \text{si} \quad v_\ell(a) = 2 \\ \psi^{\frac{\ell^2+3}{4}} & \text{si} \quad v_\ell(a) = 3. \end{cases}$$

On en déduit que l'ordre de φ est ℓ^2-1. Par suite, $I_{\mathfrak{L}}$ est un groupe d'ordre ℓ^2-1, et il en est de même de $\rho_\ell(I_{\mathfrak{L}})$. Il en résulte que $C=M_0$.

5.2.2) Supposons $\ell=3$. D'après la proposition 7 de [Kr3], la représentation de $I_{\mathfrak{L}}$ dans $E_3\otimes_{\mathbb{F}_3}\overline{\mathbb{F}_3}$ que l'on déduit par extension des scalaires est représentable matriciellement sous la forme

$$\begin{pmatrix}\psi^2\psi' & 0\\ 0 & \psi'^2\psi\end{pmatrix}\quad\text{si}\quad v_\ell(a)\in\Big\{1,2\Big\}\quad\text{et}\quad\begin{pmatrix}\psi & 0\\ 0 & \psi'\end{pmatrix}\quad\text{si}\quad v_\ell(a)=3,$$

où $\psi,\psi' : I_{\mathfrak{L}}\to\mathbb{F}_9^*$ sont les caractères fondamentaux de niveau 2. On a $\psi^2\psi'=\psi^5$ qui est d'ordre 8 i.e. l'ordre de ψ. Comme ci-dessus, $I_{\mathfrak{L}}$ et $\rho_\ell(I_{\mathfrak{L}})$ sont donc d'ordre 8, ce qui entraîne de nouveau que $C=M_0$. Cela termine la démonstration de la proposition.

2.2. Fin de la démonstration du théorème

L'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$ étant totalement imaginaire de degré d multiple de 4, le nombre de places complexes de $\mathbb{Q}(E_\ell)$ est pair et $D(\ell)$ est un entier naturel. Pour tout nombre premier p, on note e_p l'indice de ramification de p dans $\mathbb{Q}(E_\ell)$ et n_p l'exposant d'un idéal premier au-dessus de p de la différente de l'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$. D'après la formule (1), on a

$$D(\ell)=\prod_p p^{\frac{dn_p}{e_p}}. \tag{11}$$

Tout revient ainsi à déterminer pour tout nombre premier p les entiers n_p et e_p. Notons que le degré de l'extension $\mathbb{Q}(E_\ell)/\mathbb{Q}$ étant premier à ℓ, l'inertie en ℓ est en particulier modérée, ce qui entraîne l'égalité ([Se2], chap. IV) :

$$n_\ell=e_\ell-1. \tag{12}$$

D'après le critère de Néron-Ogg-Shafarevitch, pour tout nombre premier p impair ne divisant pas ℓa, on a $e_p=1$, $n_p=0$ et $v_p\big(D(\ell)\big)=0$. Par ailleurs, si p divise $2a$, la courbe E a potentiellement bonne réduction en p (formules (3)) ; si de plus p est distinct de ℓ, alors e_p est l'ordre du groupe Φ_p mesurant le défaut de semi-stabilité de E en p (cf. [Se1] p. 311 et [Se-Ta], 2. cor. 3).

1) Si $p=2$: posons $c_4'=c_4/2^{v_2(c_4)}$. La valeur de n_2 est déterminée dans le théorème 4 du chapitre I.
Si $v_2(a)=0$, on a $\big(v_2(c_4),v_2(\Delta)\big)=(4,6)$ et $c_4'=-3a\equiv a \bmod 4$. On a ainsi

$$n_2=\begin{cases}18 & \text{si } a\equiv 1 \bmod 4\\ 16 & \text{si } a\equiv 3 \bmod 4.\end{cases}$$

Si $v_2(a)=1$, on a $\big(v_2(c_4),v_2(\Delta)\big)=(5,9)$ et $c_6=0$, d'où $n_2=24$.

Si $v_2(a) = 2$, on a $\big(v_2(c_4), v_2(\Delta)\big) = (6, 12)$ et $c_4' = -3a/4$. Par suite, on a

$$n_2 = \begin{cases} 16 & \text{si } a \equiv 4 \bmod. 16 \\ 18 & \text{si } a \equiv 12 \bmod. 16. \end{cases}$$

Si $v_2(a) = 3$, on a $\big(v_2(c_4), v_2(\Delta)\big) = (7, 15)$ et $c_6 = 0$, d'où $n_2 = 24$.
D'après la formule (5), on a donc

$$m_2 = \frac{n_2}{4}.$$

Par ailleurs, on constate dans chacun des cas précédents que l'on a $|\Phi_2| = 8$ ([Kr2], cor. p. 357), d'où $e_2 = 8$. D'après la proposition, on obtient ainsi

$$\frac{dn_2}{e_2} = \begin{cases} (\ell-1)^2 m_2 & \text{si } \ell \equiv 1 \bmod. 4 \\ (\ell^2-1) m_2 & \text{si } \ell \equiv 3 \bmod. 4, \end{cases}$$

qui, d'après la formule (11), est l'exposant de 2 annoncé dans $D(\ell)$.

2) Supposons $p = \ell$. En utilisant les théorèmes 2, 3 et 4 de [Kr4], suivant que ℓ divise a ou non, et que $\ell = 3$ ou $\ell \geqslant 5$, on constate que l'on a

$$n_\ell = \begin{cases} \ell - 2 & \text{si } \ell \equiv 1 \bmod. 4 \\ \ell^2 - 2 & \text{si } \ell \equiv 3 \bmod. 4, \end{cases}$$

Compte tenu de la formule (12), et de la proposition, on obtient l'exposant de ℓ annoncé.

3) Supposons désormais $p \neq \ell$ et $p \geqslant 3$.

3.1) Supposons $p = 3$. Si $v_3(a) = 0$, on a $n_3 = 0$. Si $v_3(a) = 1$, on a $v_3(\Delta) = 3$. Cela conduit à $n_3 = 3$ et $e_3 = 4$ (chap. I, th. 3 et [Kr2], cor. du th. 1). Si $v_3(a) = 2$, on a $v_3(\Delta) = 6$, d'où $n_3 = 1$ et $e_3 = 2$. Si $v_3(a) = 3$, on a $v_3(\Delta) = 9$ et l'on obtient $n_3 = 3$ et $e_3 = 4$. On vérifie que l'on a

$$\frac{n_3}{e_3} = \frac{m_3 - 1}{m_3}, \quad \text{d'où} \quad v_3\big(D(\ell)\big) = d\left(\frac{m_3 - 1}{m_3}\right),$$

et le résultat dans ce cas.

3.2) Supposons $p \geqslant 5$. Si p ne divise pas a, E a bonne réduction en p et $n_p = 0$. Si $v_p(a) \neq 0$, on a $n_p = m_p - 1$ (chap. I, th. 2) et $e_p = m_p$ ([Kr2], prop. 1), ce qui entraîne de nouveau le résultat.

Cela termine la démonstration du théorème.

3. La courbe elliptique d'équation $y^2 - y = x^3 - x^2$

Désignons par E cette courbe elliptique, qui est celle notée 11A dans les tables de [Cr]. Les invariants standard c_4, c_6, Δ et j associés à cette équation sont

$$c_4 = 2^4, \quad c_6 = -2^3.19, \quad \Delta = -11 \quad \text{et} \quad j = -\frac{2^{12}}{11}. \tag{13}$$

La courbe E a réduction multiplicative en 11 et bonne réduction en tout nombre premier $\ell \neq 11$. Elle a réduction supersingulière en 2 et réduction ordinaire en 3. Notons $\widetilde{E(\ell)}$ la courbe elliptique sur $\mathbb{F}_\ell$ déduite de E par réduction. Si l'on a $\ell \geqslant 5$, rappelons que E a bonne réduction ordinaire en ℓ si et seulement si l'ordre du groupe des points de $\widetilde{E(\ell)}$ rationnels sur $\mathbb{F}_\ell$ est distinct de $\ell + 1$ (cf. [Si2], p. 145).

Soit ℓ un nombre premier en lequel E a bonne réduction ordinaire. Notons $j_{can}^{(\ell)}$ l'invariant modulaire du relèvement canonique de $E(\ell)$ (cf. par exemple [Kr3] et les références y figurant à ce sujet). C'est un élément de $\mathbb{Z}_\ell$ qui possède les deux propriétés suivantes :

$$j_{can}^{(\ell)} \equiv j \text{ mod. } \ell. \tag{14}$$

Par ailleurs, avec la notation standard, si $\Phi_\ell(X, X) \in \mathbb{Z}[X]$ est le polynôme modulaire de niveau ℓ, qui est de degré 2ℓ (cf. par exemple [Co], p. 231), on a

$$\Phi_\ell\Big(j_{can}^{(\ell)}, j_{can}^{(\ell)}\Big) = 0. \tag{15}$$

Soit $D(\ell)$ le discriminant du corps $\mathbb{Q}(E_\ell)$.

Théorème 2.

1) Soit ℓ un nombre premier distinct de 2, 5 et 11. On a

$$D(\ell) = 11^{(\ell-1)^3(\ell+1)}\ell^n,$$

où n est l'entier défini comme suit :

1.1) si E a bonne réduction ordinaire en ℓ, on a

$$n = \begin{cases} \ell(\ell^2-1)(\ell-2) & \text{si } j \equiv j_{can}^{(\ell)} \text{ mod. } \ell^2 \\ (\ell^2-1)(\ell^2-2) & \text{si } j \not\equiv j_{can}^{(\ell)} \text{ mod. } \ell^2. \end{cases}$$

1.2) Si E a bonne réduction supersingulière en ℓ, on a

$$n = (\ell^2-2)(\ell^2-\ell).$$

2) On a $D(2) = -2^4.5^3$, $D(5) = 5^{15}.11^{16}$ et $D(11) = 11^{26280}$.

Démonstration : La représentation ρ_ℓ de $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ dans $\mathrm{Aut}(E_\ell)$ donnant l'action de Galois sur E_ℓ est surjective pour tout $\ell \neq 5$ ([Se1], p. 309). Dans ce cas, le degré de $\mathbb{Q}(E_\ell)/\mathbb{Q}$ est l'ordre de $\mathbb{G}L_2(\mathbb{F}_\ell)$, autrement dit, on a

$$[\mathbb{Q}(E_\ell) : \mathbb{Q}] = (\ell^2-1)(\ell^2-\ell) \quad \text{si} \quad \ell \neq 5. \tag{16}$$

Par ailleurs, on vérifie que $(0, 0)$ est un point d'ordre 5 de E. En utilisant le fait que $v_{11}(j)$ n'est pas multiple de 5, il en résulte que (*loc. cit.* et chap I, cor. 1) :

$$[\mathbb{Q}(E_5) : \mathbb{Q}] = 20. \tag{17}$$

En particulier, $D(2)$ est négatif et $D(\ell)$ est positif si $\ell \geqslant 3$. Comme dans le paragraphe 2, on note, pour tout nombre premier p, n_p l'exposant d'un idéal premier au-dessus de p de l'anneau d'entiers de $\mathbb{Q}(E_\ell)$ dans la différente de $\mathbb{Q}(E_\ell)/\mathbb{Q}$, et e_p son indice de ramification. Pour tout p distinct de 11 et ℓ, on a $e_p = 1$ et $v_p\big(D(\ell)\big) = 0$.

1) Supposons ℓ distinct de 5 et 11.

1.1) Le nombre premier ℓ ne divise pas $v_{11}(j)$. D'après le théorème 1 et le corollaire 1 du chapitre I a donc $n_{11} = \ell - 1$ et $e_{11} = \ell$ (la notation n_ℓ du cor. 1 du chap. I n'est pas celle utilisée ici). Cela conduit à l'exposant de 11 annoncé dans $D(\ell)$.

1.2) Démontrons l'assertion concernant l'exposant de ℓ dans $D(\ell)$. Supposons que E ait bonne réduction ordinaire en ℓ. En particulier, on a $\ell \neq 2, 19$, ce qui entraîne que l'invariant modulaire de $\widetilde{E(\ell)}$ est différent de 0 et 1728. Il résulte alors du lemme 1 et de la proposition 2 de [Kr4] que l'image par ρ_ℓ d'un sous-groupe d'inertie en ℓ de $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ est d'ordre premier à ℓ si et seulement si on a $j \equiv j_{can}^{(\ell)}$ mod. ℓ^2. Le théorème 2 de [Kr4] et le corollaire p. 274 de [Se1] entraînent alors que l'on a

$$e_\ell = \ell - 1, \quad n_\ell = \ell - 2 \quad \text{si} \quad j \equiv j_{can}^{(\ell)} \text{ mod. } \ell^2,$$

$$e_\ell = (\ell - 1)\ell, \quad n_\ell = \ell^2 - 2 \quad \text{si} \quad j \not\equiv j_{can}^{(\ell)} \text{ mod. } \ell^2.$$

Si E a bonne réduction supersingulière en ℓ, on a $e_\ell = \ell^2 - 1$ et $n_\ell = \ell^2 - 2$ ([Se1], prop. 12). Compte tenu de l'égalité (16), on obtient l'exposant annoncé.
Cela entraîne le résultat si $\ell \neq 5, 11$.

2) Supposons $\ell = 5$. On vérifie que E a bonne réduction ordinaire en 5. On a la congruence $j \equiv 4$ mod. 5. Par ailleurs, on a

$$\Phi_5(X, X) = (X - 287496)^2(X + 32768)^2(X - 1728)^2(X + 884736)^2$$

$$\times(X^2 - 1264000X - 681472000).$$

On déduit alors des conditions (14) et (15) que l'on a

$$j_{can}^{(5)} = -2^{15}.3^3 = -884736.$$

On constate que l'on a $j \equiv j_{can}^{(5)}$ mod. 5^2. L'image par ρ_5 d'un sous-groupe d'inertie en 5 de $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}\big)$ est donc d'ordre 4 et l'on a $n_5 = 3$. Par ailleurs, on a $e_{11} = 5$ et $n_{11} = 4$. Compte tenu de l'égalité (17), cela conduit à la valeur de $D(5)$ annoncée.

3) Supposons $\ell = 11$. La courbe E a réduction de type multiplicatif en 11. Puisque $v_{11}(j)$ n'est pas multiple de 11, on a ([Kr4], th. 1 et sa démonstration)

$$e_{11} = 11 \times 10 = 110 \quad \text{et} \quad n_{11} = 219,$$

d'où $D(11) = 11^{\frac{219}{110} \times 120 \times 110}$ et le résultat.

À titre indicatif, déterminons $D(3)$ et $D(7)$.

Corollaire. *On a les égalités*

$$D(3) = 3^{56}.11^{32} \quad et \quad D(7) = 7^{2256}.11^{1728}.$$

Démonstration : La courbe E a bonne réduction ordinaire en 3 et 7. On a

$$j \equiv 4 \text{ mod. } 3^2 \quad \text{et} \quad j \equiv 33 \text{ mod. } 7^2.$$

Par ailleurs, on a

$$\Phi_3(X, X) = -X(X - 54000)(X - 8000)^2(X + 32768)^2,$$

$$\Phi_7(X, X) = -(X - 16581375)(X - 54000)^2X^2(X + 3375)(X + 884736)^2(X + 12288000)^2$$
$$\times(X^2 - 4834944X + 14670139392)^2.$$

On en déduit que

$$j_{can}^{(3)} = -32768,$$

et que $j_{can}^{(7)}$ est une racine dans $\mathbb{Z}_7$ du polynôme

$$X^2 - 4834944X + 14670139392 \in \mathbb{Z}[X].$$

Il possède deux racines dans $\mathbb{Z}_7$ congrues respectivement à 19 et 46 modulo 7^2. D'après la congruence (14), on a donc

$$j_{can}^{(7)} \equiv 19 \text{ mod. } 7^2.$$

Dans les deux cas j n'est pas congru à $j_{can}^{(\ell)}$ modulo ℓ^2. Le théorème 2 entraîne alors le résultat.

Chapitre IV

Obstructions locales des quartiques

$$x^4 + y^4 = bz^4$$

Introduction

Soit K un corps de nombres. Étant donné un élément b de K^*, on note C_b la courbe définie sur K d'équation

$$x^4 + y^4 = bz^4.$$

C'est une courbe lisse de genre 3. D'après les travaux de Faltings, l'ensemble $C_b(K)$ des points de C_b rationnels sur K est fini.

Le problème de la détermination de $C_b(K)$, ou seulement celui de décider si cet ensemble est vide ou non, est en général très difficile, sauf dans des cas particuliers. Une méthode permettant d'établir que $C_b(K)$ est vide, si tel est le cas, consiste à démontrer que C_b n'a pas de points rationnels sur un de ses complétés. On se propose dans ce chapitre d'expliciter des conditions nécessaires et suffisantes simples pour qu'il en soit ainsi. Si c'est le cas, on dit que C_b a une obstruction locale. S'il existe un complété non archimédien de K sur lequel C_b n'a pas de points rationnels, on dira que C_b a une obstruction locale en l'idéal premier de l'anneau d'entiers O_K de K qui correspond à ce complété.

Étant donnée une place archimédienne v de K, en notant K_v le complété de K en v, il est facile de décider si $C_b(K_v)$ est vide ou non. Si v est complexe, $C_b(K_v)$ est non vide. Si v est réelle et si $\sigma : K \to \mathbb{R}$ est le plongement de K dans $\mathbb{R}$ associé à v, alors $C_b(K_v)$ est vide si et seulement si la courbe d'équation $x^4 + y^4 = \sigma(b)z^4$ n'a pas de points rationnels sur $\mathbb{R}$. Par suite, pour que C_b n'ait pas d'obstructions locales archimédiennes, il faut et il suffit que pour tout plongement σ de K dans $\mathbb{R}$, on ait $\sigma(b) > 0$. On se préoccupera donc dans la suite des obstructions locales éventuelles de C_b sur les complétés non archimédiens de K.

Si $K = \mathbb{Q}$, il est très fréquent que C_b possède des obstructions locales (cf. par exemple [Br-Mo]). Au vu des résultats obtenus, on constate que ce phénomène s'étend à de nombreux corps de nombres. Plus précisément, on démontrera qu'il existe une infinité d'éléments b de K^* modulo K^{*4} tels que C_b ait une obstruction locale en un idéal premier de O_K si et seulement si K ne contient pas le corps $\mathbb{Q}(\mu_8)$ des racines huitièmes de l'unité. On peut ainsi souvent conclure que $C_b(K)$ est vide par des arguments locaux, en faisant l'économie de techniques globales plus longues à mettre en œuvre (cf. le chapitre suivant). On présentera à ce sujet, dans les paragraphes 3 à 5 de ce chapitre, des applications numériques pour illustrer ce phénomène, notamment si b est dans $\mathbb{Q}$. Par exemple, supposons que b soit un

entier naturel, sans puissances quatrièmes et congru à 3 ou 6 modulo 8. Alors, si K est un corps quadratique ou une extension de degré impair de $\mathbb{Q}$, la courbe C_b a toujours une obstruction locale en un idéal premier de O_K. En particulier, $C_b(K)$ est vide. Par ailleurs, pour tout entier $n \geqslant 1$, on explicitera un corps de nombres K de degré n sur $\mathbb{Q}$ et un élément b de O_K tels que C_b ait une obstruction locale en un idéal premier de O_K.

On fera par ailleurs une remarque concernant une famille infinie de courbes C_b avec b dans $\mathbb{N}$, deux à deux non $\mathbb{Q}$-isomorphes, qui possèdent des points rationnels sur tous les complétés de $\mathbb{Q}$ et pour lesquelles $C_b(\mathbb{Q})$ est vide. Une telle courbe C_b contredit ainsi le principe de Hasse. Signalons qu'il était connu que tel est le cas, par exemple, des courbes C_{146} et C_{226}. L'entier $b = 146$ est le plus petit entier naturel réalisant cette condition.

On pourra trouver en annexe un programme, fonctionnant sous le logiciel de calculs Pari (cf. [Pari]), permettant de tester si C_b a ou non une obstruction locale avec des corps K dont le degré sur $\mathbb{Q}$ est relativement grand, disons de l'ordre de 100, la limite essentielle étant la mémoire nécessaire pour l'initialisation du corps considéré (instruction nfinit dans Pari). Dans la mesure où le logiciel Pari initialise le corps considéré, ce programme fournit un idéal premier de O_K en lequel C_b a une éventuelle obstruction. Son temps d'exécution peut alors être de quelques secondes pour détecter une obstruction locale en dehors d'un idéal premier au-dessus de 2. En revanche, le temps est beaucoup plus long, en pratique souvent plusieurs minutes, pour expliciter une obstruction en un idéal premier au-dessus de 2 ou pour annoncer qu'il n'y en a pas. Par exemple, si $K = \mathbb{Q}(\alpha)$ où α est une racine du polynôme $X^5 - 2 \in \mathbb{Z}[X]$ et $b = 1 + 6\alpha^2 + \alpha^4$, la courbe C_b a une unique obstruction locale, qui est en l'idéal premier de O_K au-dessus de 2. Sur un processeur Athlon 2400, le temps est de deux minutes vingt secondes pour la détecter. Si $K = \mathbb{Q}(\alpha)$ où α est une racine de $X^{100} - 2 \in \mathbb{Z}[X]$ et

$$b = \sum_{i=0}^{97} \alpha^i + 2\alpha^{98},$$

le temps est de l'ordre de treize secondes pour expliciter une obstruction locale en l'idéal premier de O_K au-dessus de 1232351 qui est de degré résiduel 1. Si l'on prend pour K le corps $\mathbb{Q}\big(\sqrt{2}\big)$ et $b = 17 + 4\sqrt{2}$, on constate qu'il n'y a pas d'obstructions locales, le temps d'exécution étant de l'ordre de la seconde. On dispose d'un autre exemple avec le corps $\mathbb{Q}\big(\alpha\big)$ où $\alpha^4 = 2$ et $b = 1 + 102\alpha^2$, pour lequel C_b n'a pas d'obstruction locale, le temps de calcul étant d'une dizaine de secondes.

1. Énoncé du théorème principal

Considérons un corps de nombres K, d'anneau d'entiers O_K. Soit $\mathfrak{P}$ un idéal premier de O_K de caractéristique résiduelle p : on a $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$. Notons :

. $\widehat{K}$ le complété de K en $\mathfrak{P}$,

. v la valuation $\mathfrak{P}$-adique normalisée de $\widehat{K}$: on a $v\big(\widehat{K}^*\big) = \mathbb{Z}$,

. A l'anneau de valuation de $\widehat{K}$,

. U le groupe des unités de A,

. π une uniformisante de A,

. e l'indice de ramification de $\widehat{K}$; c'est l'indice de ramification en $\mathfrak{P}$ de l'extension $K/\mathbb{Q}$.

. f le degré résiduel de $\widehat{K}$; c'est le degré de $O_K/\mathfrak{P}$ sur $\mathbb{F}_p$.

Étant donné un élément non nul b de $\widehat{K}$, afin de décider si l'ensemble $C_b\big(\widehat{K}\big)$ des points de C_b rationnels sur $\widehat{K}$ est vide ou non, on se ramène au cas où b appartient à A. Par ailleurs, on peut supposer, sans perte de généralité, que l'on a $v(b) < 4$. En effet, supposons que l'on ait $v(b) \geqslant 4$. Il existe un entier $m \geqslant 0$ et un élément b' de A tels que l'on ait $b = b'\pi^{4m}$ et $v(b') < 4$. Les courbes C_b et $C_{b'}$ sont alors isomorphes sur $\widehat{K}$ (appendice 1), d'où notre assertion.

Le résultat que l'on a en vue est le suivant :

Théorème 1. *Soit b un élément de A tel que $v(b) < 4$. On est dans l'un des cinq cas ci-dessous.*

1) Supposons $p = 2$. Alors, $C_b\big(\widehat{K}\big)$ est non vide si et seulement si l'une des conditions suivantes est satisfaite :

1.1) il existe $u \in U$ tel que $u^4 \equiv -1$ mod. π^{4e}, autrement dit, -1 est une puissance quatrième dans $\widehat{K}$.

1.2) Il existe un entier m tel que $0 \leqslant m < e$ et deux éléments $w_1 \in U$ et $w_2 \in A$ tels que l'on ait

$$b\pi^{4m} \equiv w_1^4 + w_2^4 \text{ mod. } \pi^{4e}.$$

2) Supposons p impair et $v(b) > 0$. Alors, $C_b\big(\widehat{K}\big)$ est non vide si et seulement si l'on a $p^f \equiv 1$ mod. 8.

3) Supposons p impair et $v(b) = 0$. Si l'on a $p \equiv 3$ mod. 4 ou bien $p^f \geqslant 37$, alors $C_b\big(\widehat{K}\big)$ est non vide.

4) Si $p = 17$, alors $C_b\big(\widehat{K}\big)$ est non vide.

5) Supposons $v(b) = 0$ et $p \in \Big\{5, 13, 29\Big\}$.

5.1) Si l'on a $f \neq 1$, alors $C_b\big(\widehat{K}\big)$ est non vide.

5.2) Si $f = 1$, alors $C_b\big(\widehat{K}\big)$ est non vide si et seulement si l'une des conditions suivantes est satisfaite :

$$p = 5 \quad et \quad b \not\equiv 3 \text{ ou } 4 \text{ mod. } \pi,$$

$$p = 13 \quad et \quad b \not\equiv 7, 8 \text{ ou } 11 \text{ mod. } \pi,$$

$$p = 29 \quad et \quad b \not\equiv 4, 5, 6, 9, 13, 22 \text{ ou } 28 \text{ mod. } \pi.$$

Si $K = \mathbb{Q}$, on en déduit l'énoncé suivant (cf. [Br-Mo]) :

Corollaire 1. *Supposons $K = \mathbb{Q}$. Soit b un entier naturel non nul sans puissances quatrièmes.*

1) *L'ensemble $C_b(\mathbb{Q}_2)$ est non vide si et seulement si l'on a $b \equiv 1$ ou 2 mod. 16.*
2) *Si p est un diviseur impair de b, alors $C_b(\mathbb{Q}_p)$ est non vide si et seulement si l'on a $p \equiv 1$ mod. 8.*
3) *Supposons que p ne divise pas b. Si l'on a $p \equiv 3$ mod. 4 ou bien $p \geqslant 37$, alors $C_b(\mathbb{Q}_p)$ est non vide.*
4) *L'ensemble $C_b(\mathbb{Q}_{17})$ est non vide.*
5) *Supposons que p ne divise pas b et que l'on ait $p \in \Big\{5, 13, 29\Big\}$. Alors, $C_b(\mathbb{Q}_p)$ est non vide si et seulement si l'une des conditions suivantes est satisfaite :*

$$p = 5 \quad et \quad b \not\equiv 3 \text{ ou } 4 \text{ mod. } 5,$$

$$p = 13 \quad et \quad b \not\equiv 7, 8 \text{ ou } 11 \text{ mod. } 13,$$

$$p = 29 \quad et \quad b \not\equiv 4, 5, 6, 9, 13, 22 \text{ ou } 28 \text{ mod. } 29.$$

2. Démonstration du théorème 1

Remarquons que si $C_b\big(\widehat{K}\big)$ est non vide, il existe un point $[x, y, z] \in C_b\big(\widehat{K}\big)$ tel que

$$\mathrm{Inf}\big(v(x), v(y), v(z)\big) = 0. \tag{1}$$

2.1. L'assertion 1

On suppose que l'on a $p = 2$. Vérifions le lemme suivant :

Lemme 1. *Un élément $c \in U$ est une puissance quatrième dans $\widehat{K}$ si et seulement si il existe $\alpha \in A$ tel que l'on ait*

$$c \equiv \alpha^4 \text{ mod. } \pi^{4e}.$$

Démonstration : Considérons un élément $\alpha \in A$ tel que $c \equiv \alpha^4$ mod. π^{4e}. Il existe deux éléments θ et ξ dans U tels que l'on ait

$$2 = \theta\pi^e \quad \text{et} \quad c \equiv \alpha^4 + \xi\pi^{4e} \text{ mod. } \pi^{4e+1}.$$

Posons

$$\alpha' = \alpha + \frac{4\xi}{\alpha^3\theta^4}.$$

Puisque α et θ sont des unités, α' appartient à A. On vérifie que l'on a

$$\alpha'^4 \equiv \alpha^4 + \xi\pi^{4e} \text{ mod. } \pi^{4e+1}.$$

Par suite, on a $c \equiv \alpha'^4 \bmod. \pi^{4e+1}$. Posons $F = X^4 - c \in A[X]$. On a $v\big(F(\alpha')\big) \geqslant 4e+1$ et $v\big(F'(\alpha')\big) = 2e$ (car α' est dans U). D'après le lemme de Hensel, F a donc une racine dans A, et c est donc une puissance quatrième dans $\widehat{K}$.
L'implication réciproque est immédiate, d'où le lemme.

Supposons que $C_b\big(\widehat{K}\big)$ soit non vide. Soit $[x, y, z]$ un point de $C_b\big(\widehat{K}\big)$ vérifiant l'égalité (1). Démontrons que l'une des conditions 1.1 et 1.2 de l'énoncé est satisfaite. On distingue pour cela deux cas suivant que $v(z)$ est nul ou non.

Si $v(z) = 0$, puisque $v(b) \leqslant 3$, x ou y est une unité de A. On a ainsi

$$b = \Big(\frac{x}{z}\Big)^4 + \Big(\frac{y}{z}\Big)^4,$$

et l'on obtient la condition 1.2 avec $m = 0$.

Supposons $v(z) \neq 0$. Si $z = 0$, alors -1 est une puissance quatrième dans $\widehat{K}$. Si z n'est pas nul, il existe $m \geqslant 1$ et $z' \in U$ tel que $z = \pi^m z'$. On a dans ce cas

$$b\pi^{4m} = \alpha^4 + \beta^4 \quad \text{avec} \quad \alpha = \frac{x}{z'} \quad \text{et} \quad \beta = \frac{y}{z'}.$$

D'après l'égalité (1), on a $v(\alpha) = v(\beta) = 0$. Si l'on a $m \geqslant e$, on obtient la congruence $\alpha^4 + \beta^4 \equiv 0 \bmod. \pi^{4e}$, autrement dit,

$$-1 \equiv \Big(\frac{\alpha}{\beta}\Big)^4 \bmod. \pi^{4e}.$$

On déduit alors du lemme 1 que -1 est dans $\widehat{K}^4$. Si l'on a $m < e$, on obtient la condition 1.2. D'où l'assertion.

Inversement, si -1 est une puissance quatrième dans K, on a $\alpha^4 + 1 = 0$ et le point $[\alpha, 1, 0]$ est dans $C_b\big(\widehat{K}\big)$.
Supposons la condition 1.2 réalisée. D'après le lemme 1, $b\pi^{4m} - w_2^4$ est une puissance quatrième dans K, autrement dit, il existe $\beta \in A$ tel que $b\pi^{4m} - w_2^4 = \beta^4$ et le point $[\beta, w_2, \pi^m]$ appartient à $C_b\big(\widehat{K}\big)$. Par suite, $C_b\big(\widehat{K}\big)$ est non vide.

Cela prouve l'assertion 1.

2.2. Les assertions 2 à 5

Notons k le corps résiduel de $\widehat{K}$. Son cardinal est p^f. Soit $\widetilde{C_b}$ la courbe définie sur k déduite de C_b par réduction.

Lemme 2. *Supposons p impair.*

1) On a l'équivalence

$$-1 \in k^4 \Longleftrightarrow p^f \equiv 1 \bmod. 8.$$

2) Si -1 appartient à k^4, alors $C_b\big(\widehat{K}\big)$ n'est pas vide.

Démonstration : 1) Soit $\alpha \in k$ tel que $\alpha^4 = -1$. L'élément α est d'ordre 8 dans k^* (car $p \neq 2$) et donc 8 divise $p^f - 1$. Inversement, si $p^f \equiv 1$ mod. 8, le groupe k^* étant cyclique, il possède un élément α d'ordre 8 et l'on a $\alpha^4 = -1$.

2) Soit $\alpha \in k$ tel que $\alpha^4 = -1$. Posons $F = X^4 + 1 \in A[X]$. Si x_0 est un relèvement dans A de α, on a $v\big(F(x_0)\big) \geqslant 1$ et $v\big(F'(x_0)\big) = 0$ (car $p \neq 2$). D'après le lemme de Hensel, F a une racine t dans $\widehat{K}$ et le point $[t, 1, 0]$ appartient à $C_b\big(\widehat{K}\big)$. D'où le lemme.

Lemme 3. *Supposons $v(2b) = 0$. On a l'équivalence*

$$C_b\big(\widehat{K}\big) \neq \emptyset \Longleftrightarrow \widetilde{C_b}(k) \neq \emptyset.$$

En particulier, si -1 n'est pas une puissance quatrième dans k, on a l'équivalence

$$C_b\big(\widehat{K}\big) \neq \emptyset \Longleftrightarrow b \text{ mod. } \pi \in k^4 + k^{*4}.$$

Démonstration : Supposons $\widetilde{C_b}(k)$ non vide. Il existe un élément (x_0, y_0, z_0) de A^3, non nul modulo π, tel que l'on ait $x_0^4 + y_0^4 \equiv bz_0^4$ mod. π. Puisque $v(b) = 0$, on a l'égalité $\mathrm{Inf}\big(v(x_0), v(y_0)\big) = 0$. Supposons par exemple $v(x_0) = 0$. Posons $F = X^4 + y_0^4 - bz_0^4$. On a $v\big(F(x_0)\big) \geqslant 1$ et $v\big(F'(x_0)\big) = 0$ (car $v(2) = 0$). D'après le lemme de Hensel, F a donc une racine t dans $\widehat{K}$ et le point $[t, y_0, z_0]$ appartient à $C_b\big(\widehat{K}\big)$. Inversement, si $C_b\big(\widehat{K}\big)$ est non vide, il existe un point $[x, y, z] \in C_b\big(\widehat{K}\big)$ vérifiant la condition (1). Ce point réduit modulo π appartient alors à $\widetilde{C_b}(k)$. Cela démontre la première équivalence.

Supposons maintenant que -1 ne soit pas une puissance quatrième dans k. Supposons de plus $C_b\big(\widehat{K}\big)$ non vide. Tel est alors le cas de $\widetilde{C_b}(k)$. Soit $[\alpha, \beta, \gamma]$ un point de $\widetilde{C_b}(k)$. On a $\gamma \neq 0$, sinon, $\alpha\beta$ est non nul et l'on a $\alpha^4 + \beta^4 = 0$, ce qui entraîne que $-1 \in k^4$ et une contradiction. Par suite, on a

$$b \text{ mod. } \pi = \Big(\frac{\alpha}{\gamma}\Big)^4 + \Big(\frac{\beta}{\gamma}\Big)^4.$$

Puisque $v(b) = 0$, l'un des éléments α et β est non nul, d'où l'implication. Inversement, si l'on a b mod. $\pi = \alpha^4 + \beta^4$ avec $\beta \neq 0$, alors $\widetilde{C_b}(k)$ n'est pas vide et il en est de même de $C_b\big(\widehat{K}\big)$. D'où le résultat.

Démontrons l'assertion 2 du théorème. Si l'on a $p^f \equiv 1$ mod. 8, le lemme 2 entraîne que $C_b\big(\widehat{K}\big)$ n'est pas vide (on notera que l'on n'utilise pas ici le fait que $v(b) > 0$). Inversement, supposons $C_b\big(\widehat{K}\big)$ non vide. Soit $[x, y, z]$ un point de $C_b\big(\widehat{K}\big)$ vérifiant la condition (1). L'inégalité $v(b) \leqslant 3$ entraîne alors $v(x) = 0$ ou $v(y) = 0$. Puisque l'on a $v(b) > 0$, on en déduit que $v(x) = v(y) = 0$ et donc -1 appartient à k^4, d'où $p^f \equiv 1$ mod. 8 (lemme 2) et l'assertion.

Démontrons l'assertion 3.

a) Supposons $p \equiv 3$ mod. 4. Si l'on a $p^f \equiv 1$ mod. 8, l'assertion résulte du lemme 2. Supposons $p^f \not\equiv 1$ mod. 8. D'après les lemmes 2 et 3, il s'agit de prouver que b mod. π appartient à $k^4 + k^{*4}$. Tout élément d'un corps fini étant somme de deux carrés, il existe $\alpha \in k$ et $\beta \in k^*$ tels que b mod. $\pi = \alpha^2 + \beta^2$. Par ailleurs, p^f n'étant pas congru à 1 modulo 8, f est impair, autrement dit le degré de k sur $\mathbb{F}_p$ est impair. Il en résulte que -1 n'est pas un carré dans k. En considérant le morphisme $x \mapsto x^4$ de k^* dans k^*, on en déduit alors que $k^{*2} = k^{*4}$, d'où l'assertion.

b) Supposons $p^f \geqslant 37$. Puisque l'on a $v(2b) = 0$, la courbe $\widetilde{C_b}$ est lisse et absolument irréductible. Notons N_b le cardinal de $\widetilde{C_b}(k)$. En utilisant les bornes obtenues par A. Weil sur le nombre de points rationnels des courbes sur les corps finis (cf. [We], cor. 3 p. 70), on obtient l'inégalité

$$|N_b - (p^f + 1)| \leqslant 6\sqrt{p^f}.$$

Par suite, si l'on a $p^f \geqslant 37$ alors N_b est non nul, autrement dit, $\widetilde{C_b}(k)$ est non vide. D'après le lemme 3, $C_b\big(\widehat{K}\big)$ est donc non vide. D'où l'assertion 3.

En ce qui concerne l'assertion 4, on a $17^f \equiv 1$ mod. 8 et le lemme 2 entraîne le résultat.

Il reste à démontrer l'assertion 5. Compte tenu des cas déjà envisagés, les hypothèses faites dans cette assertion sont les dernières que l'on doit considérer.

Supposons $f \neq 1$. Si $p = 13$ ou $p = 29$, l'assertion 3 entraîne que $C_b\big(\widehat{K}\big)$ est non vide. Si $p = 5$, on a $p^f = 25$ qui est congru à 1 modulo 8, ou bien $p^f \geqslant 37$. Les assertions 2 et 4 impliquent alors le résultat.

Supposons $f = 1$. On a dans ce cas $k = \mathbb{F}_p$ et l'on vérifie que -1 n'est pas une puissance quatrième dans k. Les équivalences annoncés se déduisent alors directement du lemme 3.

Cela termine la démonstration du théorème. Le corollaire 1 en est une conséquence directe.

3. Obstructions locales quadratiques

On considère dans ce paragraphe un corps quadratique K et un idéal premier $\mathfrak{P}$ de O_K au-dessus de 2. Étant donné un entier naturel $b \geqslant 1$, on se propose d'examiner les obstructions locales éventuelles de C_b en $\mathfrak{P}$. Afin de simplifier la présentation du résultat obtenu et de ne pas alourdir sa démonstration, on se limitera au cas où b n'est pas multiple de 4. Posons $K = \mathbb{Q}\big(\sqrt{d}\big)$ où d est un entier sans facteurs carrés et notons $\widehat{K}$ le complété de K en $\mathfrak{P}$. On va démontrer le résultat suivant :

Théorème 2. *Soit b un entier naturel.*

1) Si $b \equiv 1$ ou 2 mod. 16, alors $C_b\big(\widehat{K}\big)$ est non vide.

2) Si $b \equiv 3$ ou 6 mod. 8, alors $C_b\big(\widehat{K}\big)$ est vide.

On a les équivalences suivantes :

3) *Si* $b \equiv 5$ mod. 16, *alors* $C_b(\widehat{K}) = \emptyset \iff d \not\equiv 2, 3$ *ou* 6 mod. 8.
4) *Si* $b \equiv 7$ mod. 8, *alors,* $C_b(\widehat{K}) = \emptyset \iff d \not\equiv 5$ mod. 8.
5) *Si* $b \equiv 9$ *ou* 10 mod. 16, *alors* $C_b(\widehat{K}) = \emptyset \iff d \not\equiv 3$ *ou* 5 mod. 8.
6) *Si* $b \equiv 13$ mod. 16, *alors* $C_b(\widehat{K}) = \emptyset \iff d \not\equiv 3$ *ou* 7 mod. 8.

On en déduit en particulier le résultat suivant :

Corollaire 2. *Soit* b *un entier naturel congru à* 3 *ou* 6 *modulo* 8. *Alors, l'ensemble* $C_b(K)$ *est vide. Autrement dit, la courbe* C_b *n'a pas de points quadratiques.*

Démonstration du théorème 2

Remarquons que si v est la valuation $\mathfrak{P}$-adique normalisée de $\widehat{K}$, on a $v(b) < 4$ et l'hypothèse faite dans l'énoncé du théorème 1 est donc satisfaite par b. On identifie dans la suite $\widehat{K}$ à une extension de $\mathbb{Q}_2$ de degré $\leqslant 2$ contenue dans une clôture algébrique implicitement choisie de $\mathbb{Q}_2$. Rappelons qu'il existe huit telles extensions. Mis à part $\mathbb{Q}_2$, il s'agit des corps

$$\mathbb{Q}_2(\sqrt{2}),\ \mathbb{Q}_2(\sqrt{3}),\ \mathbb{Q}_2(\sqrt{6}),\ \mathbb{Q}_2(\sqrt{-1}),\ \mathbb{Q}_2(\sqrt{-2}),\ \ \mathbb{Q}_2(\sqrt{-3})\ \text{ et }\ \mathbb{Q}_2(\sqrt{-6}).$$

Démontrons l'énoncé ci-dessous :

Proposition 1. *On a les équivalences suivantes :*

1) *si* $\widehat{K} = \mathbb{Q}_2$, *alors* $C_b(\widehat{K}) \neq \emptyset \iff b \equiv 1$ *ou* 2 mod. 16.
2) *Si* $\widehat{K}$ *est l'un des corps* $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{-2})$, $\mathbb{Q}_2(\sqrt{6})$ *et* $\mathbb{Q}_2(\sqrt{-6})$ *alors*

$$C_b(\widehat{K}) \neq \emptyset \iff b \equiv 1, 2 \ \ \textit{ou} \ \ 5 \text{ mod. } 16.$$

3) *Si* $\widehat{K} = \mathbb{Q}_2(\sqrt{3})$, *alors* $C_b(\widehat{K}) \neq \emptyset \iff b \equiv 1, 2, 5, 9, 10$ *ou* 13 mod. 16.
4) *Si* $\widehat{K} = \mathbb{Q}_2(\sqrt{-1})$, *alors* $C_b(\widehat{K}) \neq \emptyset \iff b \equiv 1, 2$ *ou* 13 mod. 16.
5) *Si* $\widehat{K} = \mathbb{Q}_2(\sqrt{-3})$, *alors* $C_b(\widehat{K}) \neq \emptyset \iff b \equiv 1, 2, 7, 9, 10$ *ou* 15 mod. 16.

Démonstration : Les notations A, U, e et π du paragraphe précédent sont conservées sans autre précision. On a $e = 1$ ou $e = 2$.

Remarquons d'abord que -1 n'est pas une puissance quatrième dans $\widehat{K}$, car l'extension de $\mathbb{Q}_2$ engendrée par les racines huitièmes de l'unité est de degré 4 sur $\mathbb{Q}_2$. Par suite, $C_b(\widehat{K})$ n'est pas vide si et seulement si la condition 1.2 de l'énoncé du théorème 1 est satisfaite. Par ailleurs, si la condition 1.2 est réalisée, elle ne peut l'être qu'avec $m = 0$. En effet, c'est immédiat si $e = 1$; si $e = 2$, des éléments w_1 et w_2 de A vérifiant la congruence

$b\pi^4 \equiv w_1^4 + w_2^4$ mod. 16 doivent être tous les deux dans U (car $w_1 \in U$). Le corps résiduel de $\widehat{K}$ étant isomorphe à $\mathbb{F}_2$, w_1 et w_2 sont donc congrus à 1 modulo π. Il en résulte que $w_1^4 + w_2^4 \equiv 2$ mod. π^4, ce qui entraîne que $v(w_1^4 + w_2^4) = 2$ et conduit à une contradiction. Ainsi, $C_b\big(\widehat{K}\big)$ est non vide si et seulement si il existe $w_1 \in U$ et $w_2 \in A$ tels que

$$b \equiv w_1^4 + w_2^4 \text{ mod. } 16. \tag{2}$$

1) L'assertion 1 est une conséquence directe de cette condition : si $\widehat{K} = \mathbb{Q}_2$, on peut prendre $\pi = 2$ et pour tout $u \in U$, on a $u^4 \equiv 1$ mod. 16 (cet argument entraîne l'assertion 1 du corollaire 1).

En ce qui concerne les autres assertions, déterminons pour tout $\alpha \in A$ la congruence de α^4 modulo 16, en fonction des coefficients du développement de Hensel de α. On distingue pour cela deux cas, selon que $e = 1$ ou $e = 2$.
Supposons $e = 1$, auquel cas $\widehat{K} = \mathbb{Q}_2\big(\sqrt{-3}\big)$. Soit μ_3 le groupe des racines cubiques de l'unité. Pour tout $i \geqslant 0$, il existe a_i dans $\mu_3 \cup \big\{0\big\}$ tel que l'on ait

$$\alpha = \sum_{i \geqslant 0} a_i 2^i.$$

On vérifie alors que l'on a

$$\alpha^4 \equiv a_0^4 + 8a_0^2 a_1\big(a_0 + a_1\big) \text{ mod. } 16. \tag{3}$$

Si $e = 2$, pour tout $i \geqslant 0$, il existe $a_i = 0$ ou 1 tel que l'on ait

$$\alpha = \sum_{i \geqslant 0} a_i \pi^i.$$

Dans ce cas, en tenant compte du fait que $a_i^2 = a_i$, on obtient la congruence

$$\alpha^4 \equiv a_0 + a_1\pi^4 + 2\big(a_0a_1\pi^2 + a_0a_2\pi^4\big) +$$

$$4\big(a_0a_1\pi^2 + a_0a_1\pi + a_0a_2\pi^2 + a_0a_3\pi^3 + a_0a_1a_2\pi^3 + a_0a_1\pi^3\big) \text{ mod. } 16.$$

En particulier, si α est dans U, on a $a_0 = 1$, d'où

$$\alpha^4 \equiv 1 + a_1(\pi^4 + 6\pi^2) + 4a_1\pi + 2a_2\pi^4 + 4a_2\pi^2 + 4\pi^3(a_1 + a_3 + a_1a_2) \text{ mod. } 16, \tag{4}$$

et si α appartient à l'idéal maximal de A, on a $a_0 = 0$, d'où

$$\alpha^4 \equiv 0 \ \text{ ou } \ \pi^4 \text{ mod. } 16. \tag{5}$$

2) Démontrons l'assertion 2.

2.1) Supposons $\widehat{K} = \mathbb{Q}_2\big(\sqrt{-2}\big)$ ou $\widehat{K} = \mathbb{Q}_2\big(\sqrt{6}\big)$. On a $e = 2$ et l'on peut prendre respectivement $\pi = \sqrt{-2}$ et $\pi = \sqrt{6}$. Pour tout $\alpha \in U$, on vérifie alors que la congruence (4) entraîne dans les deux cas

$$\alpha^4 \equiv 1,\ 1+\pi^5+\pi^6,\ 1+\pi^7 \text{ ou } 1+\pi^5+\pi^6+\pi^7 \text{ mod. } 16.$$

Compte tenu des conditions (2) et (5), on en déduit que $C_b\big(\widehat{K}\big)$ est non vide si et seulement si b vérifie l'une des congruences suivantes :

$$b \equiv 1,\ 1+\pi^5+\pi^6,\ 1+\pi^7,\ 1+\pi^5+\pi^6+\pi^7,\ 1+\pi^4,\ 1+\pi^4+\pi^5+\pi^6,\ 1+\pi^4+\pi^7,$$

$$1+\pi^4+\pi^5+\pi^6+\pi^7,\ 2,\ 2+\pi^5+\pi^6,\ 2+\pi^7 \text{ ou } 2+\pi^5+\pi^6+\pi^7 \text{ mod. } 16.$$

Dans le cas particulier où b est un entier naturel, il en résulte que $C_b\big(\widehat{K}\big)$ est non vide si et seulement si $b \equiv 1, 2$ ou 5 mod. 16. D'où l'assertion dans ce cas.

2.2) Supposons $\widehat{K} = \mathbb{Q}_2\big(\sqrt{2}\big)$ ou $\widehat{K} = \mathbb{Q}_2\big(\sqrt{-6}\big)$. On peut prendre respectivement $\pi = \sqrt{2}$ et $\pi = \sqrt{-6}$. Pour tout $\alpha \in U$, on déduit de la congruence (4) que l'on a

$$\alpha^4 \equiv 1,\ 1+\pi^5,\ 1+\pi^7 \text{ ou } 1+\pi^5+\pi^7 \text{ mod. } 16.$$

Il en résulte que $C_b\big(\widehat{K}\big)$ est non vide si et seulement si b vérifie l'une des congruences :

$$b \equiv 1,\ 1+\pi^5,\ 1+\pi^7,\ 1+\pi^5+\pi^7,\ 1+\pi^4,\ 1+\pi^4+\pi^5,\ 1+\pi^4+\pi^7,\ 1+\pi^4+\pi^5+\pi^7,$$

$$2,\ 2+\pi^5,\ 2+\pi^7,\ 2+\pi^5+\pi^7 \text{ mod. } 16,$$

et l'on aboutit à la même conclusion. D'où l'assertion 2.

3) Démontrons l'assertion 3. On suppose $\widehat{K} = \mathbb{Q}_2\big(\sqrt{3}\big)$. On peut prendre $\pi = \sqrt{3} - 1$ et l'on vérifie que pour tout $\alpha \in U$, on a

$$\alpha^4 \equiv 1,\ 1+\pi^6,\ 1+\pi^7 \text{ ou } 1+\pi^6+\pi^7 \text{ mod. } 16.$$

Par suite, $C_b\big(\widehat{K}\big)$ est non vide si et seulement si on a

$$b \equiv 1,\ 1+\pi^4,\ 1+\pi^6,\ 1+\pi^4+\pi^6,\ 1+\pi^7,\ 1+\pi^4+\pi^7,\ 1+\pi^6+\pi^7,$$

$$1+\pi^4+\pi^6+\pi^7,\ 2,\ 2+\pi^6,\ 2+\pi^7 \text{ ou } 2+\pi^6+\pi^7 \text{ mod. } 16,$$

et l'on vérifie que cela entraîne le résultat.

4) Supposons $\widehat{K} = \mathbb{Q}_2\big(\sqrt{-1}\big)$. On peut prendre $\pi = 1 + \sqrt{-1}$ et l'on vérifie que pour tout $\alpha \in U$, on a

$$\alpha^4 \equiv 1 \text{ ou } 1+\pi^7 \text{ mod. } 16,$$

de sorte que $C_b(\widehat{K})$ est non vide si et seulement si on a

$$b \equiv 1,\ 2,\ 1+\pi^4,\ 1+\pi^7,\ 1+\pi^4+\pi^7 \text{ ou } 2+\pi^7 \text{ mod. } 16,$$

d'où l'on déduit l'assertion.

5) Supposons $\widehat{K} = \mathbb{Q}_2(\sqrt{-3})$. D'après la congruence (3), pour tout $\alpha \in U$, il existe $\zeta \in \mu_3$ tel que

$$\alpha^4 \equiv \zeta \text{ ou } 9\zeta \text{ mod. } 16.$$

Il en résulte que $C_b(\widehat{K})$ est non vide si et seulement si il existe ζ et $\zeta' \in \mu_3$, avec $\zeta' \neq 1$, tels que

$$b \equiv \zeta,\ 2\zeta,\ 7\zeta,\ 9\zeta,\ 10\zeta,\ 15\zeta,\ 7\zeta + 8\zeta'\zeta \text{ mod. } 16,$$

d'où l'assertion.

Cela termine la démonstration de la proposition.

Les assertions 1 et 2 du théorème 2 sont des conséquences directes de la proposition 1. Par ailleurs, un entier congru à 1 modulo 8 est un carré dans $\mathbb{Q}_2$. Il en résulte que l'on a $\widehat{K} = \mathbb{Q}_2(\sqrt{-1})$ si $d \equiv 7$ mod. 8, $\widehat{K} = \mathbb{Q}_2(\sqrt{\pm 2})$ si $d \equiv \pm 2$ mod. 16, $\widehat{K} = \mathbb{Q}_2(\sqrt{\pm 6})$ si $d \equiv \pm 6$ mod. 16, et $\widehat{K} = \mathbb{Q}_2(\sqrt{\pm 3})$ si $d \equiv \pm 3$ mod. 8. La proposition 1 entraîne alors le résultat. D'où le théorème 2.

4. Existence d'obstructions locales

Soit K un corps de nombres d'anneau d'entiers O_K. À travers la question ci-dessous, on se propose ici d'illustrer le fait que les obstructions locales pour les courbes C_b sont très fréquentes en pratique, comme on l'a d'ailleurs constaté si K est le corps $\mathbb{Q}$ ou un corps quadratique.

Question. *Existe-t-il $b \in K^*$ tel que C_b ait une obstruction locale en un idéal premier de O_K ? Si tel est le cas, existe-t-il une infinité de tels éléments b modulo K^{*4} ?*

Bien entendu, la réponse n'est pas toujours positive. En effet, soient μ_8 le sous-groupe des racines huitièmes de l'unité de $\mathbb{C}^*$ et ζ un de ses générateurs. Si K contient le corps $\mathbb{Q}(\mu_8)$, alors pour tout $b \in K^*$, le point $[\zeta, 1, 0]$ appartient à $C_b(K)$. L'existence de ce point interdit ainsi la présence d'obstructions locales pour les courbes C_b. Cela étant, c'est la seule situation où ce phénomène se produit, comme le montre le résultat qui suit :

Théorème 3. *Les conditions suivantes sont équivalentes :*

1) *Le corps $\mathbb{Q}(\mu_8)$ n'est pas contenu dans K.*
2) *Il existe une infinité d'éléments $b \in K^*/K^{*4}$ tels que C_b ait une obstruction locale en un idéal premier de O_K.*
3) *Il existe $b \in K^*$ tel que C_b ait une obstruction locale en un idéal premier de O_K.*

On en déduit l'énoncé suivant (cf. l'appendice 1) :

Corollaire 3. *Si $\mathbb{Q}(\mu_8)$ n'est pas contenu dans K, il existe une infinité de classes de K-isomorphisme de courbes C_b ($b \in O_K$) ayant une obstruction locale en un idéal premier de O_K.*

4.1. Démonstration du théorème 3

Il est conséquence du théorème 1 et du théorème de densité de Chebotarev ([Se3], I-7). Plus précisément, il se déduit du résultat suivant (cf. [Co], p. 171) :

Lemme 4. *Soient L et M deux corps de nombres tels que L soit une extension galoisienne de $\mathbb{Q}$. Soit S_L l'ensemble des nombres premiers totalement décomposés dans L. Soit $\widetilde{S_M}$ l'ensemble des nombres premiers p non ramifiés dans M, pour lesquels il existe un idéal premier $\mathfrak{P}$ de O_M au-dessus de p de degré résiduel 1 sur p. Les deux conditions suivantes sont équivalentes :*

1) le corps L est contenu dans M.

2) Pour tout nombre premier p sauf un nombre fini, on a l'implication

$$p \in \widetilde{S_M} \Longrightarrow p \in S_L.$$

Démonstration : Supposons L contenu dans M. Soit p un nombre premier de $\widetilde{S_M}$. Il existe un idéal premier $\mathfrak{P}$ de O_M au-dessus de p qui est non ramifié et de degré résiduel 1 sur p. Posons $\mathfrak{p} = \mathfrak{P} \cap O_L$. C'est un idéal premier de O_L qui est non ramifié et de degré résiduel 1 sur p. Puisque $L/\mathbb{Q}$ est galoisienne, tel est aussi le cas de tous les idéaux premiers de O_L au-dessus de p, d'où il résulte que p est dans S_L.

Inversement, supposons la condition 2 réalisée. Considérons une extension galoisienne N de $\mathbb{Q}$ contenant L et M. Il s'agit de montrer que le groupe de Galois $\mathrm{Gal}(N/M)$ est contenu dans $\mathrm{Gal}(N/L)$. Soit σ un élément de $\mathrm{Gal}(N/M)$. D'après le théorème de densité de Chebotarev, il existe un idéal premier $\mathfrak{P}$ de O_N, non ramifié sur $\mathbb{Q}$, tel que

$$(\mathfrak{P}, N/\mathbb{Q}) = \sigma, \tag{6}$$

où $(\mathfrak{P}, N/\mathbb{Q})$ est la substitution de Frobenius de l'extension $N/\mathbb{Q}$. Soit p le nombre premier tel que $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$. Vérifions que

$$p \in \widetilde{S_M}. \tag{7}$$

Posons $\mathfrak{P}' = \mathfrak{P} \cap O_M$. C'est un idéal premier de O_M au-dessus de p. Pour tout $\alpha \in O_M$, on a $\sigma(\alpha) = \alpha$ et $\sigma(\alpha) \equiv \alpha^p$ mod. $\mathfrak{P}$. On en déduit la congruence

$$\alpha \equiv \alpha^p \text{ mod. } \mathfrak{P}'.$$

Il en résulte que $O_M/\mathfrak{P}'$ est isomorphe à $\mathbb{F}_p$, autrement dit, que le degré résiduel de $\mathfrak{P}'$ sur p est 1. Puisque p est non ramifié dans M, cela prouve l'assertion (7). Par ailleurs, d'après le théorème de densité de Chebotarev, il existe une infinité d'idéaux premiers de O_N vérifiant l'égalité (6). D'après l'hypothèse faite, on peut donc supposer que p appartient à S_L. L'extension $L/\mathbb{Q}$ étant galoisienne, la restriction de σ à L est $(\mathfrak{P} \cap O_L, L/\mathbb{Q})$. Puisque p appartient à S_L, la substitution de Frobenius $(\mathfrak{P} \cap O_L, L/\mathbb{Q})$ est donc l'identité de L, autrement dit, σ fixe L, d'où le lemme.

Le théorème 3 se déduit comme suit.

Démontrons l'implication 1) $\Longrightarrow$ 2). On applique le lemme avec $L = \mathbb{Q}(\mu_8)$ et $M = K$. Il existe ainsi une infinité de nombres premiers p non ramifiés dans K, pour lesquels il existe un idéal premier $\mathfrak{P}$ de O_K au-dessus de p de degré résiduel 1 sur p, qui n'est pas congru à 1 modulo 8. D'après l'assertion 2 du théorème 1, pour chacun de ces nombres premiers p la courbe C_p a une obstruction locale en $\mathfrak{P}$. Par ailleurs, deux tels nombres premiers distincts p et p' ne sont pas congrus multiplicativement modulo K^{*4}. En effet, supposons qu'il existe $a \in K$ tel que l'on ait par exemple $p = p'a^4$. Puisque p et p' sont non ramifiés dans K, on a $pO_K = p'O_K$, d'où une contradiction. L'implication 2) $\Longrightarrow$ 3) est immédiate. Quant à l'implication 3) $\Longrightarrow$ 1), elle résulte du fait, comme on l'a déjà constaté, que si K contient $\mathbb{Q}(\mu_8)$, il n'existe pas de courbes C_b ayant une obstruction locale. D'où le théorème.

Il résulte directement de la démonstration du théorème 3 l'énoncé suivant :

Corollaire 4. *Supposons que $\mathbb{Q}(\mu_8)$ ne soit pas contenu dans K. Il existe une infinité de nombres premiers p non congrus à 1 modulo 8 tels que C_p ait une obstruction locale en un idéal premier de O_K au-dessus de p.*

4.2. Effectivité

Si K ne contient pas $\mathbb{Q}(\mu_8)$, l'énoncé du théorème 3 ne fournit pas un élément b de O_K spécifique pour lequel C_b a une obstruction locale. Il se pose ainsi le problème de l'effectivité de cet énoncé. Si K est le corps $\mathbb{Q}$ ou un corps quadratique, on dispose dans les paragraphes précédents de familles infinies explicites de tels éléments b. Dans le cas particulier où le degré de K sur $\mathbb{Q}$ est impair, on a le résultat effectif suivant :

Proposition 2. *Supposons que le degré de K sur $\mathbb{Q}$ soit impair. Soit b un entier naturel non nul, sans puissances quatrièmes, divisible par un nombre premier impair p non congru à 1 modulo 8. Alors, C_b a une obstruction locale en un idéal premier de O_K au-dessus de p. En particulier, $C_b(K)$ est vide.*

Démonstration : Considérons la décomposition de pO_K en produit d'idéaux premiers de O_K :

$$pO_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_t^{e_t}.$$

Notons d le degré de K sur $\mathbb{Q}$ et f_i le degré résiduel de $\mathfrak{P}_i$ sur p. On a l'égalité

$$d = \sum_{i=1}^{t} e_i f_i.$$

Puisque d est impair il existe un indice i tel que $e_i f_i \equiv 1$ mod. 2. On a l'égalité (v_p étant la valuation p-adique de b)

$$v_{\mathfrak{P}_i}(b) = v_p(b) e_i,$$

L'entier b étant divisible par p et sans puissances quatrièmes, on a $1 \leqslant v_p(b) \leqslant 3$, et e_i étant impair, on a

$$v_{\mathfrak{P}_i}(b) \not\equiv 0 \text{ mod. } 4.$$

Vérifions que C_b a une obstruction locale en $\mathfrak{P}_i$. Considérons pour cela une uniformisante π du complété $\widehat{K}$ de K en $\mathfrak{P}_i$. Posons

$$b = \pi^{N+4\lambda} u,$$

où $1 \leqslant N \leqslant 3$ et où u est une unité de l'anneau de valuation de $\widehat{K}$. Les courbes C_b et $C_{\pi^N u}$ sont isomorphes sur $\widehat{K}$. Le corps résiduel de $\widehat{K}$ est de cardinal p^{f_i} qui n'est pas congru à 1 modulo 8 car f_i est impair. L'assertion 2 du théorème 1 entraîne alors que $C_{\pi^N u}\big(\widehat{K}\big)$ est vide, d'où l'assertion et le résultat.

Il semble beaucoup plus difficile d'obtenir un énoncé explicite analoque en ce qui concerne les corps de nombres de degré pair sur $\mathbb{Q}$ qui ne contiennent pas $\mathbb{Q}(\mu_8)$. À titre d'exemple, on va expliciter ci-dessous, pour tout entier $n \geqslant 2$, un corps de nombres K de degré n sur $\mathbb{Q}$ et un élément $b \in O_K$ tels que C_b ait une obstruction locale en un idéal premier de O_K et n'ait pas d'obstructions locales aux places à l'infini.

Soit K le corps $\mathbb{Q}(\alpha)$ où α est une racine du polynôme $P = X^n - X - 1 \in \mathbb{Z}[X]$. Selmer à démontré que P est un polynôme irréductible sur $\mathbb{Q}$ ([Sel]), de sorte que K est une extension de degré n de $\mathbb{Q}$. Posons $b = \alpha + 4$. On vérifie directement que C_b n'a pas d'obstructions locales à l'infini. Cela étant, C_b a une obstruction locale en un idéal premier de O_K . En effet, on vérifie que la norme de K sur $\mathbb{Q}$ de b est $4^n + 3(-1)^n$ (on utilise le fait que b est racine du polynôme $P(X-4)$). Pour tout idéal premier $\mathfrak{P}_i$ de O_K divisant bO_K, soit p_i le nombre premier tel que $\mathfrak{P}_i \cap \mathbb{Z} = p_i\mathbb{Z}$. Notons e_i et f_i l'indice de ramification et le degré résiduel de $\mathfrak{P}_i$ sur p_i. On a ainsi

$$\prod_i p_i^{e_i f_i} = 4^n + 3(-1)^n.$$

Il existe donc un indice i tel que $p_i^{e_i f_i} \not\equiv 1$ mod. 8. En particulier, $e_i f_i$ est impair et l'on a donc $v_{\mathfrak{P}_i}(b) \not\equiv 0$ mod. 4. Le même argument que celui utilisé dans la proposition ci-dessus entraîne alors que C_b a une obstruction locale en $\mathfrak{P}_i$.

5. Contre-exemples au principe de Hasse

On se limitera dans ce paragraphe au cas où $K = \mathbb{Q}$. Rappelons qu'une courbe sur $\mathbb{Q}$ contredit le principe de Hasse si elle ne possède pas d'obstructions locales (y compris à l'infini) et si elle n'a pas de points rationnels sur $\mathbb{Q}$. Il est en général difficile d'expliciter de tels exemples. Comme on va le constater les quartiques de Fermat en fournissent de nombreux.

5.1. Infinités de contre-exemples

Compte tenu du corollaire 1, il est tout d'abord facile d'expliciter des familles infinies d'entiers naturels b sans obstructions locales. En effet, comme conséquence immédiate de ce corollaire, on obtient :

Proposition 3. *Soit b un entier naturel non nul sans puissances quatrièmes. Pour que la courbe C_b possède des points rationnels sur tous les complétés de $\mathbb{Q}$, il faut et il suffit que les conditions suivantes soient réalisées :*

1) on a $b \equiv 1$ ou 2 mod. 16.

2) Tout diviseur premier impair de b est congru à 1 modulo 8.

3) On a $b \not\equiv 3$ ou 4 mod. 5.

4) On a $b \not\equiv 7, 8$ ou 11 mod. 13.

5) On a $b \not\equiv 4, 5, 6, 9, 13, 22$ ou 28 mod. 29.

On a le résultat suivant :

Proposition 4. *Soit b un entier naturel $\geqslant 2$ sans facteurs carrés. Si la courbe C_{b^2} n'a pas d'obstructions locales, elle contredit le principe de Hasse.*

En particulier, on obtient une infinité de classes d'isomorphisme de quartiques de Fermat contredisant le principe de Hasse :

Corollaire 5. *Si p est un nombre premier congru à 1 modulo 1160, la courbe C_{p^2} contredit le principe de Hasse.*

C'est une conséquence directe de la proposition 4, compte tenu du fait que l'on a $1160 = 5 \times 8 \times 29$ et que 7, 8 et 11 ne sont pas résidus quadratiques modulo 13.

Quant à la proposition 4, elle se déduit du lemme qui suit :

Lemme 5. *Pour tout entier $b \geqslant 2$ qui n'est pas un carré dans $\mathbb{Z}$, l'ensemble $C_{b^2}(\mathbb{Q})$ est vide.*

Démonstration : Considérons la courbe elliptique E définie sur $\mathbb{Q}$ d'équation

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

On dispose d'un morphisme sur $\mathbb{Q}$, $\nu : C_{b^2} \to E$, défini pour tout point $[x, y, z]$ de C_{b^2} par l'égalité

$$\nu\big([x, y, z]\big) = [x^2y, bxz^2, y^3].$$

La courbe elliptique E est celle noté $64A4$ dans les tables de Cremona ([Cr], p. 115). D'après *loc. cit.*, on a $E(\mathbb{Q}) = \big\{[0, 1, 0], [0, 0, 1]\big\}$. Supposons qu'il existe un point $[x, y, z] \in C_{b^2}(\mathbb{Q})$. On est alors dans l'un des deux cas suivants :

1) on a $[x^2y, bxz^2, y^3] = [0, 1, 0]$. Cela conduit à $y = 0$ et $xz \neq 0$, puis à l'égalité $x^4 = b^2z^4$, ce qui contredit l'hypothèse faite sur b.

2) On a $[x^2y, bxz^2, y^3] = [0, 0, 1]$. On a dans ce cas $xy = 0$ et l'on aboutit à la même contradiction. D'où le lemme.

Comme me l'a fait remarquer Henri Cohen, l'énoncé du lemme 5 se déduit directement des travaux de Fermat sur l'équation $x^4 + y^4 = z^2$.

5.2. Quelques remarques

Afin d'expliciter des quartiques de Fermat qui contredisent le principe de Hasse, on est ainsi confronté au problème suivant :

Problème. *Étant donné un entier naturel $b \geqslant 2$ sans puissances quatrièmes vérifiant les cinq conditions de la proposition 3 (i.e. C_b est sans obstructions locales), comment démontrer, si tel est le cas, que $C_b(\mathbb{Q})$ est vide ?*

Une méthode d'attaque possible pour aborder ce problème consiste à remarquer que la courbe C_b possède deux quotients elliptiques sur $\mathbb{Q}$, qui sont en fait uniques à $\mathbb{Q}$-isogénies près. Plus précisément, notons E_b et F_b les courbes elliptiques sur $\mathbb{Q}$ d'équations

$$E_b : \ Y^2Z = X^3 - bXZ^2 \quad \text{et} \quad F_b : \ Y^2Z = X^3 + b^2XZ^2.$$

On dispose alors de deux morphismes sur $\mathbb{Q}$, $\varphi : C_b \to E_b$ et $\psi : C_b \to F_b$ définis pour tout point $[x, y, z]$ de C_b par les égalités

$$\varphi\big([x, y, z]\big) = [-x^2z, xy^2, z^3] \quad \text{et} \quad \psi([x, y, z]\big) = [bx^2y, b^2xz^2, y^3].$$

Si l'un des deux groupes $E_b(\mathbb{Q})$ et $F_b(\mathbb{Q})$ est fini, i.e. si l'une des deux courbes E_b et F_b est de rang 0 sur $\mathbb{Q}$, il est alors facile de déterminer $C_b(\mathbb{Q})$. Bien entendu, cette remarque est aussi valable si le corps de base est un corps de nombres.

Par cette méthode, on constate par exemple que les entiers $b < 500$ pour lesquels C_b contredit le principe de Hasse sont 146, 226 et 482. Pour les autres entiers $b < 500$, la courbe C_b a une obstruction locale ou bien b est de la forme $x^4 + y^4$ avec $x, y \in \mathbb{Z}$. En ce qui concerne les trois entiers b précédents, la courbe C_b n'a pas d'obstructions locales (prop.

3). Par ailleurs, les groupes $F_b(\mathbb{Q})$ sont finis. Pour le démontrer, il suffit de vérifier que les valeurs des fonctions L de Hasse-Weil en 1 associées aux trois courbes F_b sont non nulles ([Co-Wi]). Tel est le cas : des valeurs approchées à 10^{-3} près sont

$$L(F_{146}, 1) \sim 1,227, \quad L(F_{226}, 1) \sim 3,946 \quad \text{et} \quad L(F_{482}, 1) \sim 0,675.$$

On vérifie ensuite directement, que les groupes $F_b(\mathbb{Q})$ sont d'ordre 2, engendrés par le point de coordonnées affines $(0, 0)$, ce qui entraîne que $C_b(\mathbb{Q})$ est vide.

Lorsque l'on ne peut pas conclure par la méthode précédente i.e. si les groupes $E_b(\mathbb{Q})$ et $F_b(\mathbb{Q})$ sont infinis, il existe d'autres méthodes qui parfois permettent de démontrer que $C_b(\mathbb{Q})$ est éventuellement vide. Tel est le cas des méthodes de factorisation utilisées dans [Br-Mo]. Signalons que les techniques de *loc. cit.* permettent de démontrer que la courbe C_{577} contredit le principe de Hasse et que la méthode décrite ci-dessus ne s'applique pas : on peut démontrer que les groupes $E_b(\mathbb{Q})$ et $F_b(\mathbb{Q})$ sont de rang 2. Par ailleurs, Dem'janenko a démontré en 1968, que pour tout $b \geqslant 3$ sans puissances quatrièmes, si le rang de $E_b(\mathbb{Q})$ est 1 alors $C_b(\mathbb{Q})$ est vide ([De]). Il en est ainsi par exemple des entiers naturels $b = 2642$ et $b = 7762$ pour lesquels C_b contredit le principe de Hasse et $F_b(\mathbb{Q})$ est infini. Le chapitre V est principalement consacré aux généralisations du résultat de Dem'janenko si $\mathbb{Q}$ est remplacé par un corps de nombres.

Appendice 1 - Classes d'isomorphisme des quartiques

Soit K un corps parfait. On se propose ici de démontrer le résultat suivant :

Proposition. *Soient b et b' deux éléments non nuls de K. Alors, les courbes C_b et $C_{b'}$ sont K-isomorphes si et seulement si b et b' diffèrent multiplicativement par une puissance quatrième dans K.*

Démonstration : Supposons qu'il existe $\alpha \in K$ tel que $b = \alpha^4 b'$. Les courbes C_b et $C_{b'}$ sont alors K-isomorphes via le morphisme $\nu : C_b \to C_{b'}$ défini pour tout $[x, y, z]$ de C_b par

$$\nu\big([x, y, z]\big) = [x, y, \alpha z].$$

Inversement, supposons que C_b et $C_{b'}$ soient isomorphes sur K. Notons C la courbe d'équation $x^4 + y^4 + z^4 = 0$. Les courbes C_b et $C_{b'}$ sont des tordues galoisiennes de C i.e. sont isomorphes à C sur une clôture algébrique $\overline{K}$ de K. Plus précisément, soient β et β' des racines quatrièmes respectivement de $-b$ et $-b'$ dans $\overline{K}$. Les courbes C_b et $C_{b'}$ sont isomorphes à C via les morphismes $\varphi : C_b \to C$ et $\varphi' : C_{b'} \to C$ définis par

$$\varphi\Big([x, y, z]\Big) = [x, y, \beta z] \quad \text{et} \quad \varphi'\Big([x, y, z]\Big) = [x, y, \beta' z].$$

Soient $\mathrm{Aut}(C)$ le groupe des automorphismes de C et G_K le groupe de Galois de $\overline{K}$ sur K. Les classes de K-isomorphisme de C_b et C'_b correspondent à deux classes de cocycle de l'ensemble de cohomologie $H^1\big(G_K, \mathrm{Aut}(C)\big)$ ([Si2], p. 284-286). En fait, pour tout $\sigma \in G_K$, ${}^\sigma\varphi\varphi^{-1}$ et ${}^\sigma\varphi'\varphi'^{-1}$ sont dans $\mathrm{Aut}(C)$, et les applications Ψ et Ψ' de G_K à valeurs dans $\mathrm{Aut}(C)$ définies par

$$\Psi(\sigma) = {}^\sigma\varphi\varphi^{-1} \quad \text{et} \quad \Psi'(\sigma) = {}^\sigma\varphi'\varphi'^{-1},$$

sont deux 1-cocycles, dont les classes correspondent respectivement à celles de C_b et $C_{b'}$ (cf. *loc. cit.*). Pour tout $\sigma \in G_K$, on a

$$\Psi(\sigma)\Big([x, y, z]\Big) = \left[x, y, \frac{\sigma\beta}{\beta} z\right] \quad \text{et} \quad \Psi'(\sigma)\Big([x, y, z]\Big) = \left[x, y, \frac{\sigma\beta'}{\beta'} z\right].$$

D'après l'hypothèse faite, Ψ et Ψ' sont cohomologues. Autrement dit, il existe $\alpha \in \mathrm{Aut}(C)$ tel que l'on ait pour tout $\sigma \in G_K$

$$\Psi(\sigma)\ \alpha = {}^\sigma\alpha\ \Psi'(\sigma). \tag{1}$$

Il s'agit de montrer que b/b' appartient à K^4. Soit ζ un générateur du groupe μ_4 des racines quatrièmes de l'unité. Le groupe $\mathrm{Aut}(C)$ est d'ordre 96. Il est formé des seize éléments

$$\alpha_{j,j'} : [x, y, z] \mapsto [\zeta^j x, \zeta^{j'} y, z],$$

où $0 \leqslant j, j' \leqslant 3$ et de leurs composés avec les automorphismes de permutations, qui est un groupe isomorphe à $\mathbb{S}_3$ (cf. [Ku-Ko], p. 274). On va alors vérifier que l'égalité (1) entraîne notre assertion.

Notons $\chi : G_K \to \{\pm 1\}$ le caractère cyclotomique donnant l'action de G_K sur μ_4. On a $\chi(\sigma) = 1$ si $\sigma(\zeta) = \zeta$ et $\chi(\sigma) = -1$ sinon. Soient j et j' deux indices tels que $0 \leqslant j, j' \leqslant 3$.

1) Supposons $\alpha = \alpha_{j,j'}$. Pour tout $\sigma \in G_K$, on a

$$\Psi(\sigma)\ \alpha\big([x,y,z]\big) = \left[x, \zeta^{j'-j} y, \zeta^{-j}\frac{\sigma\beta}{\beta} z\right],$$

$$^{\sigma}\alpha\ \Psi'(\sigma)\big([x,y,z]\big) = \left[x, \zeta^{\chi(\sigma)(j'-j)} y, \zeta^{-j\chi(\sigma)}\frac{\sigma\beta'}{\beta'} z\right].$$

On en déduit que

$$\zeta^{-j}\frac{\sigma\beta}{\beta} = \zeta^{-j\chi(\sigma)}\frac{\sigma\beta'}{\beta'} \quad \text{i.e.} \quad \sigma\Big(\frac{\beta\zeta^j}{\beta'}\Big) = \frac{\beta\zeta^j}{\beta'}.$$

Par suite, $\beta\zeta^j/\beta'$ appartient à K, d'où le résultat dans ce cas. On aboutit visiblement à la même conclusion si l'on remplace α par $\alpha \circ r$, où $r\big([x,y,z]\big) = [y,x,z]$.

2) Supposons $\alpha = \alpha_{j,j'} \circ s$ où $s\big([x,y,z]\big) = [z,x,y]$. On a dans ce cas

$$\Psi(\sigma)\ \alpha\big([x,y,z]\big) = \left[\zeta^j\frac{\beta}{\sigma\beta} z, \zeta^{j'}\frac{\beta}{\sigma\beta} x, y\right],$$

$$^{\sigma}\alpha\ \Psi'(\sigma)\big([x,y,z]\big) = \left[\zeta^{j\chi(\sigma)}\frac{\sigma\beta'}{\beta'} z, \zeta^{\chi(\sigma)j'} x, y\right].$$

Cela entraîne dans ce cas que $-b$ et $-b'$ sont dans K^4, par suite $b/b' \in K^4$. Il en est de même avec l'automorphisme $\alpha = \alpha_{j,j'} \circ t$ où $t\big([x,y,z]\big) = [z,y,x]$.

3) Supposons $\alpha = \alpha_{j,j'} \circ s^2$. On a $s^2\big([x,y,z]\big) = [y,z,x]$. On a

$$\Psi(\sigma)\ \alpha\big([x,y,z]\big) = \left[\zeta^j\frac{\beta}{\sigma\beta} y, \zeta^{j'}\frac{\beta}{\sigma\beta} z, x\right],$$

$$^{\sigma}\alpha\ \Psi'(\sigma)\big([x,y,z]\big) = \left[\zeta^{j\chi(\sigma)} y, \zeta^{\chi(\sigma)j'}\frac{\sigma\beta'}{\beta'} z, x\right],$$

ce qui implique de nouveau que $-b$ et $-b'$ sont dans K^4. On a la même conclusion si $\alpha = \alpha_{j,j'} \circ u$ où $u\big([x,y,z]\big) = [x,z,y]$.

Cela termine la démonstration de la proposition.

Appendice 2 - Programme de calcul des obstructions locales

Obstructions Locales

```
 1 : \\*************************************************************
 2 : \\*                                                           *
 3 : \\* Programme de calcul des obstructions locales de la courbe : *
 4 : \\*                          x^4 + y^4 = bz^4                 *
 5 : \\*                       sur un corps de nombres             *
 6 : \\*                                                           *
 7 : \\*                            16/02/2005                     *
 8 : \\*                                                           *
 9 : \\*     Paramètres :                                          *
10 : \\*                                                           *
11 : \\*         nf : corps de nombres                             *
12 : \\*         b : entier de nf sans puissances quatrièmes       *
13 : \\*                                                           *
14 : \\*                                                           *
15 : \\*    Utilisation :                                          *
16 : \\*                                                           *
17 : \\*    obsloc(nf, b)                                          *
18 : \\*    nf doit être initialisé par nfinit avec un polynôme en y *
19 : \\*    b est donné dans la base nf[7][7] et se termine par ~  *
20 : \\*                                                           *
21 : \\*    Résultat :                                             *
22 : \\*                                                           *
23 : \\*    [1, 0] s'il n'y a pas d'obstruction locale             *
24 : \\*    [0, x] s'il y a une obstruction locale sur R en x      *
25 : \\*    [0, idprem] s'il y a une obst locale en l'idéal idprem *
26 : \\*    [0, 0] si b comporte une puissance quatrième           *
27 : \\*    S'il y a plusieurs obst locales, le pgme en donne une  *
28 : \\*                                                           *
29 : \\*    Exemple :                                              *
30 : \\*                                                           *
31 : \\*    nf = nfinit(y^2-2)                                     *
32 : \\*    b = [1,1]~                                             *
33 : \\*    obsloc(nf,b) trouve les obst locales sur Q(sqrt(2))    *
34 : \\*    de la courbe : x^4 + y^4 = (1+sqrt(2))z^4              *
35 : \\*                                                           *
36 : \\*                                                           *
37 : \\*************************************************************
38 :
```

```
39 : {recurs2(w2, ind2)=
40 : local(i2, w, ind, w24, w4, flag, flag2, i0, coeftotal, m, pi4m);
41 : if (ind2<2*ep+1,
42 : for (i2=1, 2^fp,
43 : w=w2+nfeltmul(nf,elt_Fp[i2],unif[ind2]);
44 : ind = ind2+1;
45 : flag2 = recurs2(w, ind);
46 : if (flag2 == 1, return(1),);
47 : );
48 : return(0),
49 :
50 : flag=0;
51 : w24=nfeltpow(nf,w2,4);
52 : w4=w14+w24;
53 : if (debug>5,print("w4 = "w4),);
54 :
55 : for (m=0, ep-1,
56 : pi4m=nfeltpow(nf,unif[1], 4*m);
57 : for (i0=1,2^fp-1,
58 : coeftotal=nfeltmul(nf,c,pi4m)-nfeltmul(nf,w4,elt_Fp[i0]);
59 : if (debug>4, print(coeftotal),);
60 : if (nfeltval(nf,coeftotal,id_prem)>4*ep-1,flag=1,);
61 : )
62 : );
63 : return(flag);
64 : );
65 : }
66 :
67 : {recurs1(w1, ind1)=
68 : local(i1, w, ind, w2, ind2, flag, flag2);
69 : if (ind1<2*ep,
70 : for (i1=1, 2^fp,
71 : w=w1+nfeltmul(nf,elt_Fp[i1],unif[ind1]);
72 : ind = ind1+1;
73 : flag2 = recurs1(w, ind);
74 : if (flag2==1, return(1),);
75 : );
76 : return(0),
77 :
```

```
 78 : w14=nfeltpow(nf,w1,4);
 79 : w2=0;
 80 : ind2=1;
 81 : flag = recurs2(w2, ind2);
 82 : return(flag);
 83 : );
 84 : }
 85 :
 86 : \\programme principal
 87 : {obsloc(nf, c)=
 88 : debug=0;
 89 : resultat=vector(2);
 90 : obs=0;
 91 :
 92 : \\degré du corps K
 93 : degk=poldegree(nf.pol);
 94 : if (debug>5,print("deg K = "degk),);
 95 :
 96 : \\verification : c est-il sans puissance quatrième
 97 : liste_factorc=idealfactor(nf, c);
 98 : longfactorc=matsize(liste_factorc)[1];
 99 : for (i=1, longfactorc,
100 : if (liste_factorc[i,1].e>3,
101 : print("b a une puissance quatrieme en l'ideal :",
102 : liste_factorc[i,1]);
103 : return([0,0]);
104 : ,);
105 : );
106 :
107 : \\initialisation des idéaux premiers au-dessus de 2, 5, 13,et 29
108 : liste_idprem2=idealprimedec(nf,2);
109 : longprem2=matsize(liste_idprem2)[2];
110 : liste_idprem5=idealprimedec(nf,5);
111 : longprem5=matsize(liste_idprem5)[2];
112 : liste_idprem13=idealprimedec(nf,13);
113 : longprem13=matsize(liste_idprem13)[2];
114 : liste_idprem29=idealprimedec(nf,29);
115 : longprem29=matsize(liste_idprem29)[2];
116 :
```

```
117 : \\recherche des obstructions locales sur R
118 : \\on prend chaque racine réelle du polynôme nf.pol
119 : flag_r=1;
120 : for (i=1, degk,
121 : t=polroots(nf.pol)[i];
122 : if (imag(t)==0,
123 :
124 : \\ on calcule sigma(c)
125 : t=real(t);
126 : monpol = Pol(0,y);
127 : for (j=1, poldegree(nf.pol),
128 : monpol=monpol+nf[7][j]*c[j];
129 : );
130 : result=subst(monpol,y,t);
131 : \\ si sigma(c)<0, il y a obtruction locale
132 : if (result<0, flag_r=0;obs=result,);
133 : ,);
134 : );
135 :
136 : if (flag_r == 0, return([flag_r, obs]);,);
137 :
138 : \\pour chacun des idéaux premiers au-dessus de c ne divisant pas 2
139 : flag3=1;
140 : fact=idealfactor(nf,c);
141 : if (debug>4,print(fact),);
142 : longfact=matsize(fact)[1];
143 : if (longfact >0,
144 : for (l=1,longfact,
145 : idprem=fact[l,1];
146 : if (idprem[1]<>2,
147 :
148 : \\vérification de la condition du théorème
149 : if (Mod(idprem[1]^idprem[4],8)<>Mod(1,8),flag3=0;
150 : obs=idprem,)
151 : ,);
152 : );
153 : ,);
154 :
```

```
155 : \\si condition vérifiée, flag3=1
156 : if (flag3==0,
157 : return([0,obs]),
158 : if (debug>4, print(idealnorm(nf,c)," OK3 ",c),);
159 : );
160 :
161 : \\pour chaque idéal premier au-dessus de 5 ne divisant pas c
162 : flag5=1;
163 : for (i_prem=1,longprem5,
164 : id_prem=liste_idprem5[i_prem];
165 : if (idealval(nf,c,id_prem)<>0, next(),);
166 :
167 : \\si le degré résiduel est supérieur à 1, c'est OK
168 : if (id_prem[4]>1, next(),);
169 :
170 : \\sinon : test de la condition du théorème
171 : nffact = nffactormod(nf,x+c,id_prem);
172 : modgen=if(type(nffact)=="t_VEC",nffact[1][1],nffact[1,1]);
173 : \\           modgen=nffactormod(nf,x+c,id_prem)[1,1];
174 : if (polcoeff(modgen,0)<>1,
175 : if (polcoeff(modgen,0)<>2,
176 : flag5=0; obs=id_prem
177 : ,)
178 : ,);
179 :
180 : \\idéal suivant
181 : );
182 :
183 : \\si KO, flag5=0
184 : if (flag5==0, return([0,obs]),);
185 :
186 : \\pour chaque idéal premier au-dessus de 13 ne divisant pas c
187 : flag13=1;
188 : for (i_prem=1,longprem13,
189 : id_prem=liste_idprem13[i_prem];
190 : if (idealval(nf,c,id_prem)<>0, next(),);
191 :
192 : \\si le degré résiduel est supérieur à 1, c'est OK
193 : if (id_prem[4]>1, next(),);
194 :
```

```
\\sinon : test de la condition du théorème
nffact = nffactormod(nf,x+c,id_prem);
modgen=if(type(nffact)=="t_VEC",nffact[1][1],nffact[1,1]);
\\           modgen=nffactormod(nf,x+c,id_prem)[1,1];
if (polcoeff(modgen,0)<>1
&polcoeff(modgen,0)<>2
&polcoeff(modgen,0)<>3
&polcoeff(modgen,0)<>4
&polcoeff(modgen,0)<>5
&polcoeff(modgen,0)<>6
&polcoeff(modgen,0)<>9
&polcoeff(modgen,0)<>10
&polcoeff(modgen,0)<>12,
flag13=0; obs=id_prem,);

\\idéal suivant
);

\\si KO, flag13 = 0
if (flag13==0, return([0,obs]),);

\\pour chaque idéal premier au-dessus de 29 ne divisant pas c
flag29=1;
for (i_prem=1,longprem29,
id_prem=liste_idprem29[i_prem];
if (idealval(nf,c,id_prem)<>0, next(),);

\\si le degré résiduel est supérieur à 1, c'est OK
if (id_prem[4]>1, next(),);

```

```
225 : \\sinon : test de la condition du théorème
226 : nffact = nffactormod(nf,x+c,id_prem);
227 : modgen=if(type(nffact)=="t_VEC",nffact[1][1],nffact[1,1]);
228 : \\           modgen=nffactormod(nf,x+c,id_prem)[1,1];
229 : if (polcoeff(modgen,0)<>1
230 : &polcoeff(modgen,0)<>2
231 : &polcoeff(modgen,0)<>3
232 : &polcoeff(modgen,0)<>7
233 : &polcoeff(modgen,0)<>8
234 : &polcoeff(modgen,0)<>9
235 : &polcoeff(modgen,0)<>10
236 : &polcoeff(modgen,0)<>11
237 : &polcoeff(modgen,0)<>12
238 : &polcoeff(modgen,0)<>14
239 : &polcoeff(modgen,0)<>15
240 : &polcoeff(modgen,0)<>16
241 : &polcoeff(modgen,0)<>17
242 : &polcoeff(modgen,0)<>18
243 : &polcoeff(modgen,0)<>19
244 : &polcoeff(modgen,0)<>20
245 : &polcoeff(modgen,0)<>21
246 : &polcoeff(modgen,0)<>23
247 : &polcoeff(modgen,0)<>24
248 : &polcoeff(modgen,0)<>25
249 : &polcoeff(modgen,0)<>26
250 : &polcoeff(modgen,0)<>27,
251 : flag29=0; obs=id_prem,);
252 :
253 : \\idéal suivant
254 : );
255 :
256 : \\si KO, flag29=0
257 : if (flag29==0, return([0,obs]),);
258 :
259 : flag2 = 0;
260 : flag2_final=1;
261 : \\en 2 : on vérifie d'abord que -1 n'est pas une puissance 4ieme
262 : if (nfisincl(y^4+1, nf), flag2_final=1,
263 :
```

```
264 : \\SINON, pour chaque ideal premier P au-dessus de 2
265 : for (i_prem=1,longprem2,
266 : id_prem=liste_idprem2[i_prem];
267 :
268 : \\uniformisante, indice de ramification et degré résiduel en P
269 : uniform=id_prem[2];
270 : fp=id_prem[4];
271 : ep=id_prem[3];
272 : if (debug>5,print("id2 = "uniform" ep="ep" fp="fp"
273 : longprem2="longprem2),);
274 :
275 : \\soit zeta_0 une racine primitive du corps résiduel
276 : kresiduel=nfrootsof1(nf);
277 : puiss=factor(kresiduel[1])[1,2];
278 : zeta_0=nfeltpow(nf,kresiduel[2],2^puiss);
279 : elt_Fp=vector(2^fp);
280 : for (i_zeta=1,2^fp-1,elt_Fp[i_zeta]=nfeltpow(nf,zeta_0,i_zeta));
281 : elt_Fp[2^fp]=0;
282 :
283 : \\on construit 1 dans K
284 : un=c;
285 : un[1]=1;
286 : for (i=2, degk, un[i]=0);
287 :
288 : \\on construit W1 selon les puissances de pi jusqu'à pi^(2e-1)
289 : unif=vector(2*ep);
290 : unif[2*ep]=un;
291 : unif[1]=uniform;
292 : for (i=2, 2*ep-1,
293 : unif[i]=nfeltpow(nf,unif[1],i));
294 :
295 : \\w1 est de valuation nulle.
296 : \\On multipliera w4 par toutes les racines de l'unité à la fin
297 : w1=un;
298 : ind1=1;
299 : if (debug>5,print("debut recurs", un),);
300 : flag2=recurs1(w1,ind1);
301 : if (flag2==0, obs=id_prem; return([0, obs]),);
302 : flag2_final=flag2_final*flag2;
303 : );
304 :
```

```
305 : \\fin du SINON (-1 n'est pas une puisance quatrieme)
306 : );
307 :
308 : \\résultat
309 : flag = flag2_final*flag3*flag5*flag13*flag29;
310 : resultat = [flag, obs];
311 : return(resultat);
312 : }
313 :
314 :
315 :
```

Chapitre V

Étude globale des quartiques

$$x^4 + y^4 = bz^4$$

Introduction

Soit K un corps de nombres. Pour tout b dans K^*, notons comme au chapitre précédent, C_b la courbe d'équation

$$x^4 + y^4 = bz^4.$$

On s'intéresse ici au problème de l'effectivité de certaines méthodes globales concernant l'étude de l'ensemble $C_b(K)$. Plus précisément, soit E_b ou E_b/K la courbe elliptique définie sur K d'équation

$$Y^2Z = X^3 - bXZ^2.$$

Rappelons qu'il existe un morphisme défini sur K de C_b sur E_b (chap. IV). On dispose aussi d'une autre courbe elliptique sur K, qui est un quotient de C_b sur K, celle notée F_b dans le paragraphe 5.2 du chapitre IV, mais elle n'interviendra pas dans la suite. Mis à part la situation où C_b possède une obstruction locale ou bien si l'un des groupes $E_b(K)$ et $F_b(K)$ est fini, il est en général très difficile de déterminer $C_b(K)$. Ce chapitre concerne principalement l'étude de $C_b(K)$ dans le cas où $E_b(K)$ est de rang 1.

Les classes de K-isomorphisme de E_b et de C_b ne dépendent que de celle de b modulo K^{*4}. Comme conséquence d'une étude des points rationnels de certaines tordues galoisiennes de courbes sur des corps de nombres, J. Silverman a démontré en 1986 le résultat suivant ([Si3]) :

Théorème (Silverman). *Il existe une constante absolue c_0, dépendant seulement du degré de K sur $\mathbb{Q}$, telle que la condition suivante soit satisfaite :*

soient b un élément de K^* qui ne soit pas dans K^{*4} et L une extension de K obtenue en adjoignant à K une racine quatrième de b. Alors, si $E_b(K)$ est de rang 1 et si la norme de K sur $\mathbb{Q}$ du discriminant relatif de l'extension L/K est plus grande que c_0, l'ensemble $C_b(K)$ est vide.

En particulier, pour toute classe d'élément b dans K^*/K^{*4} sauf un nombre fini, si le rang de $E_b(K)$ est 1, alors $C_b(K)$ est vide.

Silverman a obtenu une constante c_0 dépendant exponentiellement du degré de K sur $\mathbb{Q}$. On va se préoccuper du problème de l'effectivité de cet énoncé en explicitant une telle constante c_0. La démonstration du théorème précédent repose sur le fait qu'il existe deux morphismes indépendants définis sur K de C_b dans E_b et sur la mise en œuvre d'une méthode de Dem'janenko et Manin faisant intervenir des arguments de hauteurs (cf. [Se4],

p. 62). Du point de vue de l'effectivité, on sera confronté au problème de rendre effectif le théorème des zéros de Hilbert dans un cas particulier. Comme conséquence du résultat que l'on obtient à ce sujet (théorème 1), en notant n le degré de K sur $\mathbb{Q}$, on constate que

$$c_0 = \exp\Big(169 + 6\ n\Big),$$

convient. Bien que dans certains cas particuliers, par exemple si b est un carré dans K, on puissse abaisser notablement cette constante, le résultat obtenu s'avère inefficace d'un point de vue pratique.

Néanmoins, si K est un corps totalement réel, on démontre dans cette direction un énoncé plus exploitable du point de vue de l'effectivité. On s'est inspiré pour cela d'une méthode de G. Grigorov et J. Rizov qui permet d'obtenir, si $K = \mathbb{Q}$, des estimations uniformes pour la différence entre la hauteur de Weil et la hauteur de Néron-Tate sur la courbe elliptique E_b ([Gr-Ri]). Ils en déduisent en application une nouvelle démontration du théorème suivant démontré par Dem'janenko en 1968 ([De]) :

Théorème (Dem'janenko). *Soit b un entier $\geqslant 3$ sans puissances quatrièmes. Si $E_b(\mathbb{Q})$ est de rang $\leqslant 1$, alors l'ensemble $C_b(\mathbb{Q})$ est vide.*

On a généralisé, dans le théorème 2, l'énoncé de Dem'janenko aux corps totalement réels avec une constante effective qui reste « pratiquable » dans certaines situations. Indiquons un cas particulier de ce théorème. Le corps K étant un corps totalement réel, notons :

- n son degré sur $\mathbb{Q}$.
- O_K son anneau d'entiers.
- $\mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ l'application norme de K sur $\mathbb{Q}$.
- $v_{\mathfrak{P}} : K^* \to \mathbb{Z}$ la valuation sur K standard normalisée associée à un idéal premier $\mathfrak{P}$ de O_K.

Proposition 1. *Soit b un élément non nul de O_K. Supposons les conditions suivantes réalisées :*

1) pour tout idéal premier $\mathfrak{P}$ de O_K, on a $v_{\mathfrak{P}}(b) < 4$.

2) Pour tout plongement σ de K dans $\mathbb{R}$, on a $\sigma(b) \geqslant 1$.

3) Le groupe $E_b(K)$ est de rang $\leqslant 1$.

Alors, si l'on a

$$\mathrm{N}_{K/\mathbb{Q}}(b) > 2^{\frac{11n}{2}},$$

l'ensemble $C_b(K)$ est vide.

En particulier, supposons que b soit un entier naturel sans puissances quatrièmes, dont tous les diviseurs premiers sont non ramifiés dans K. Il résulte directement de la proposition 1 que si l'on a $b \geqslant 46$ et si $E_b(K)$ est de rang au plus 1, alors $C_b(K)$ est vide ; cette remarque

n'a en fait d'intérêt que si le degré de K sur $\mathbb{Q}$ est pair, compte tenu des résultats obtenus par A. Bremner dans [Br], dans le cas où b est un entier naturel.

Notons que la condition 2 de la proposition 1 n'est pas très restrictive pour les corps K de petit degré sur $\mathbb{Q}$. À titre indicatif, supposons que K soit un corps quadratique réel. Posons $K = \mathbb{Q}\big(\sqrt{u}\big)$ et considérons un entier s fixé ainsi que les éléments $b \in O_K$ de la forme

$$b = \frac{r + s\sqrt{u}}{2} \quad \text{avec} \quad r \in \mathbb{Z} \quad \text{et} \quad r \equiv s \text{ mod. } 2.$$

Alors, il existe au plus quatre valeurs de r telles que l'on ait

$$0 < b < 1 \quad \text{ou bien} \quad 0 < \sigma(b) < 1,$$

où σ est l'élément non trivial de $\mathrm{Gal}(K/\mathbb{Q})$. En choisissant $r \geqslant 2 + |s|\sqrt{u}$, on obtient ainsi une infinité d'éléments b satisfaisant la condition 2.

Dans le paragraphe 5 en se limitant au cas où $K = \mathbb{Q}$, on fait quelques remarques sur le théorème de Dem'janenko ainsi que sur d'éventuelles généralisations. On s'intéresse plus précisément au problème suivant :

Problème. *Dans quelle mesure la conclusion de ce théorème reste-t-elle vraie si l'on ne suppose plus que le rang de $E_b(\mathbb{Q})$ est au plus* 1 *?*

On démontre dans cette direction l'énoncé ci-dessous. Rappelons que la conjecture de parité pour la courbe elliptique $E_b/\mathbb{Q}$ affirme que le signe de l'équation fonctionnelle de la fonction L de Hasse-Weil associée à E_b vaut 1 si et seulement si le rang de $E_b(\mathbb{Q})$ est pair.

Proposition 2. *Soit b un entier naturel non nul sans puissances quatrièmes. Supposons que la conjecture de parité pour $E_b/\mathbb{Q}$ soit vraie ou bien que la partie 2-primaire du groupe de Tate-Shafarevitch de $E_b/\mathbb{Q}$ soit finie. Supposons de plus que l'on soit dans l'un des cas suivants :*

1) le rang de $E_b(\mathbb{Q})$ est impair et $b \equiv 1$ mod. 16.

2) Le rang de $E_b(\mathbb{Q})$ est pair et $b \equiv 2$ mod. 16.

Alors, b est divisible par un nombre premier impair p qui n'est pas congru à 1 *modulo* 8. *En particulier, C_b a une obstruction locale en p et $C_b(\mathbb{Q})$ est vide.*

Rappelons que C_b n'a pas d'obstruction locale en 2 si b est congru à 1 ou 2 modulo 16. Remarquons par ailleurs que la conclusion de cet énoncé entraîne que C_b possède des obstructions locales sur toute extension de degré impair de $\mathbb{Q}$ (chap. IV, prop. 2). Sous l'hypothèse que la partie 2-primaire du groupe de Tate-Shafarevitch de $E_b/\mathbb{Q}$ soit finie, Grigorov et Rizov avaient déjà remarqué que la condition 1 ci-dessus entraîne le résultat annoncé (cf. [Gr-Ri], prop. 3.1). Si l'on a $b \equiv 1$ mod. 16 et si $E_b(\mathbb{Q})$ est de rang 1, alors conjecturalement, $C_b(\mathbb{Q})$ est donc vide pour des raisons locales, ce qui précise dans ce cas

le résultat de Dem'janenko. Cela étant, il n'en va pas de même si $b \equiv 2$ mod. 16, comme on le constate par exemple avec $b = 562$, pour lequel C_b n'a pas d'obstructions locales, $E_b(\mathbb{Q})$ est de rang 1 et $C_b(\mathbb{Q})$ est vide.

1. Énoncé des résultats effectifs

Soit $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$. Tous les corps de nombres intervenant dans la suite sont supposés contenus dans $\overline{\mathbb{Q}}$.

1.1. Effectivité du théorème de Silverman

Soient K un corps de nombres et b un élément non nul de K qui n'est pas dans K^4. Choisissons une racine quatrième α de b dans $\overline{\mathbb{Q}}$. Notons :

- L le corps $K(\alpha)$.
- d le degré de L sur K ; on a $d = 4$ si et seulement si b n'est pas un carré dans K et b n'est pas dans $-4K^4$. On a $d = 2$ sinon.
- $D_{L/K}$ le discriminant relatif de l'extension L/K ; c'est un idéal de l'anneau d'entiers de K.
- $\mathrm{N}_{K/\mathbb{Q}}\big(D_{L/K}\big)$ la norme de K sur $\mathbb{Q}$ de $D_{L/K}$.
- δ_K le nombre de places archimédiennes de K. Si r_1 (resp. $2r_2$) est le nombre de plongements réels (resp. complexes) de K, on a $\delta_K = r_1 + r_2$.

L'énoncé que l'on obtient est le suivant :

Théorème 1. *Supposons que le rang de $E_b(K)$ soit 1. Alors, si l'on a*

$$\log \mathrm{N}_{K/\mathbb{Q}}\big(D_{L/K}\big) \geqslant \Big(14,08\ (d-1) + \delta_K\ \log d\Big)d, \tag{1}$$

l'ensemble $C_b(K)$ est vide.

En notant D_L le discriminant de L et D_K celui de K, on a l'égalité

$$|D_L| = \mathrm{N}_{K/\mathbb{Q}}\big(D_{L/K}\big)|D_K|^d,$$

de sorte que l'égalité (1) peut aussi s'écrire

$$\log |D_L| \geqslant \Big(14,08\ (d-1) + \delta_K\ \log d + \log |D_K|\Big)d. \tag{2}$$

1.2. Cas des corps totalement réels

Soit K un corps de nombres totalement réel, de degré n sur $\mathbb{Q}$, d'anneau d'entiers O_K. Pour tout x de O_K, notons $H(x)$ la hauteur de x relative à K. On a

$$H(x) = \prod_{\sigma} \mathrm{Max}\big(1, |\sigma(x)|\big), \tag{3}$$

où σ parcourt les n plongements de K dans $\mathbb{R}$. Le groupe des unités de O_K modulo $\{\pm 1\}$ est un $\mathbb{Z}$-module libre de rang $n-1$. Soit $(u_1, \cdots, u_{n-1})$ un système d'unités fondamentales de O_K. On a l'énoncé suivant :

Théorème 2. *Soit b un élément non nul de O_K. Supposons que les conditions suivantes soient satisfaites :*

1) pour tout idéal premier $\mathfrak{P}$ de O_K, on a $v_{\mathfrak{P}}(b) < 4$.

2) Le groupe $E_b(K)$ est de rang $\leqslant 1$.

3) On a les inégalités

$$\mathrm{N}_{K/\mathbb{Q}}(b) > 2^{\frac{11n}{2}} \quad et \quad \mathrm{N}_{K/\mathbb{Q}}(b) \geqslant \left(\prod_{i=1}^{n-1} H(u_i)\right)^4. \tag{4}$$

Alors, l'ensemble $C_b(K)$ est vide.

Il convient de signaler que si O_K est principal, il n'y a qu'un nombre fini d'éléments de K^*/K^{*4} pour lesquels il n'existe pas de représentants satisfaisant les conditions 1 et 3 du théorème 2. Il n'en va pas de même si O_K n'est pas principal. On montrera à ce sujet dans le paragraphe 4 que si par exemple le nombre de classes de K est 3, il existe une infinité d'éléments de K^*/K^{*4} pour lesquels il n'existe pas de représentants $b \in O_K$ qui satisfont la condition 1 de ce théorème.

Par exemple, en prenant pour K le corps $\mathbb{Q}(\sqrt{2})$, la condition 3 concerne les éléments $b \in O_K$ tels que $\mathrm{N}_{K/\mathbb{Q}}(b) > 2048$. En utilisant les résultats du chapitre IV, on obtient alors la conclusion du théorème pour les éléments $b \in O_K$ vérifiant les conditions 1 et 2 tels que $\mathrm{N}_{K/\mathbb{Q}}(b) > 1889$. Signalons que ce résultat permet d'obtenir des contre-exemples au principe de Hasse. On vérifie que tel est par exemple le cas avec $b = 82 + 8\sqrt{2}$ (cf. [Sim]).

2. Démonstration du théorème 1

2.1. Notations

Étant donné un corps de nombres k, on introduit les notations suivantes :

. O_k son anneau d'entiers.

. $v_{\mathfrak{P}} : k^* \to \mathbb{Z}$ la valuation normalisée standard associée à un idéal premier $\mathfrak{P}$ de O_k.

. M_k l'ensemble des places de k i.e. l'ensemble des classes d'équivalences de valeurs absolues usuelles sur k.

. M_k^∞ l'ensemble des places archimédiennes de k. Si $v \in M_k^\infty$ correspond à un plongement $\sigma : k \to \mathbb{C}$, la valeur absolue normalisée associée à v est définie pour tout $x \in k$ par la formule

$$|x|_v = |\sigma(x)|.$$

. M_k^0 l'ensemble des places non archimédiennes de k. Soit v une telle place correspondant à un idéal premier $\mathfrak{P}$ de O_k de caractéristique résiduelle p. La place v est représentée par la valeur absolue qui est définie pour tout $x \in k^*$ par la formule

$$|x|_v = p^{-v_{\mathfrak{P}}(x)/e_{\mathfrak{P}}},$$

où $e_{\mathfrak{P}} = v_{\mathfrak{P}}(p)$ est l'indice de ramification de $\mathfrak{P}$ sur p.

. Pour tout $v \in M_k$, on note n_v le degré local de v. Si $v \in M_k^\infty$, on a $n_v = 1$ ou $n_v = 2$. On a $n_v = 1$ si et seulement si v correspond à un plongement de k dans $\mathbb{R}$. Si $v \in M_k^0$ est associée à un idéal premier $\mathfrak{P}$ de O_k au-dessus d'un nombre premier p, on a $n_v = e_{\mathfrak{P}} f_{\mathfrak{P}}$ où $f_{\mathfrak{P}}$ est le degré de $O_k/\mathfrak{P}$ sur $\mathbb{F}_p$.

2.2. Les hauteurs h_C, h_E^X et $\widehat{h_E}$

Rappelons la définition de l'application hauteur absolue logarithmique $h : \mathbb{P}^2\big(\overline{\mathbb{Q}}\big) \to \mathbb{R}$ définie sur l'ensemble des points du plan projectif $\mathbb{P}^2$ à valeurs dans $\overline{\mathbb{Q}}$. Soient $P = [x, y, z]$ un point de $\mathbb{P}^2\big(\overline{\mathbb{Q}}\big)$ et k un corps de nombres contenant x, y et z. La hauteur absolue logarithmique $h(P)$ de P est définie par la formule ([Si2], p. 215) :

$$h(P) = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} n_v \ \log \mathrm{Max}\Big(|x|_v, |y|_v, |z|_v\Big), \tag{5}$$

où $[k : \mathbb{Q}]$ est le degré de k sur $\mathbb{Q}$. La définition de $h(P)$ ne dépend pas du choix des coordonnées de P choisies ni du corps de nombres k les contenant.

Afin de simplifier les notations, on désigne dans la suite par C et E les courbes sur $\mathbb{Q}$ d'équations

$$C : \ x^4 + y^4 = z^4 \quad \text{et} \quad E : \ Y^2Z = X^3 - XZ^2.$$

On notera :

. h_C la restriction de la hauteur h à $C\big(\overline{\mathbb{Q}}\big)$.

. h_E^X la hauteur sur E relative à la fonction X/Z (*loc. cit.*). En posant $O = [0, 1, 0]$, on a $h_E^X(O) = 0$. Pour tout point $M = [X, Y, Z] \in E\big(\overline{\mathbb{Q}}\big)$ distinct de O et tout corps k contenant X et Z, on a l'égalité :

$$h_E^X(M) = \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} n_v \ \log \mathrm{Max}\Big(|X|_v, |Z|_v\Big), \tag{6}$$

Cette définition ne dépend pas du choix des coordonnées de M.

. $\widehat{h_E} : E\big(\overline{\mathbb{Q}}\big) \to \mathbb{R}$ la hauteur de Néron-Tate sur E ([Si2], p. 228). On a $2\widehat{h_E} = h_E^X + O(1)$ (cf. *loc. cit.*, th. 9.3 p. 229). Silverman dans [Si4] a effectivisé cette égalité. Pour tout point $M \in E\big(\overline{\mathbb{Q}}\big)$, on a en fait ([Si4], p. 727) :

$$\Big|\widehat{h_E}(M) - \frac{1}{2} h_E^X(M)\Big| \leqslant 2,252. \tag{7}$$

2.3. Une majoration de hauteur

On dispose de deux morphismes ϕ et ψ sur $\mathbb{Q}$ de C sur E définis pour tout point $[x,y,z]$ de C par les formules

$$\phi\big([x,y,z]\big) = [-x^2z, xy^2, z^3] \quad \text{et} \quad \psi\big([x,y,z]\big) = [-y^2z, x^2y, z^3]. \tag{8}$$

On va démontrer le résultat suivant :

Théorème 3. *Soit P un point de $C\big(\overline{\mathbb{Q}}\big)$. Supposons que $\phi(P)$ et $\psi(P)$ dans $E\big(\overline{\mathbb{Q}}\big)$ soient linéairement dépendants sur $\mathbb{Z}$. Alors, on a*

$$h_C(P) < 7,04. \tag{9}$$

Démonstration : Indiquons d'abord le principe de la démonstration. Soit $\phi+\psi : C \to E$ le morphisme somme de ϕ et ψ relatif à loi de groupe sur E. On fournit des majorations explicites des quantités

$$\big|h_C(P) - \widehat{h_E}\big(\phi(P)\big)\big|, \quad \big|h_C(P) - \widehat{h_E}\big(\psi(P)\big)\big| \quad \text{et} \quad \Big|2h_C(P) - \widehat{h_E}\Big(\big(\phi+\psi\big)(P)\Big)\Big|.$$

Notons $<\ ,\ >:\ E\big(\overline{\mathbb{Q}}\big) \times E\big(\overline{\mathbb{Q}}\big) \to \mathbb{R}$ l'accouplement de Néron-Tate sur E (cf. [Si2], p. 232). On a

$$< \phi(P), \phi(P) >= 2\widehat{h_E}\big(\phi(P)\big), \quad < \psi(P), \psi(P) >= 2\widehat{h_E}\big(\psi(P)\big),$$
$$< \phi(P), \psi(P) >= \widehat{h_E}\Big(\big(\phi+\psi\big)(P)\Big) - \widehat{h_E}\big(\phi(P)\big) - \widehat{h_E}\big(\psi(P)\big).$$

Les points $\phi(P)$ et $\psi(P)$ étant linéairement dépendants dans $E\big(\overline{\mathbb{Q}}\big)$, le déterminant de la matrice

$$\begin{pmatrix} < \phi(P), \phi(P) > & < \phi(P), \psi(P) > \\ < \phi(P), \psi(P) > & < \psi(P), \psi(P) > \end{pmatrix}$$

est nul. Les majorations obtenues ci-dessus permettent alors d'obtenir le résultat annoncé.

Posons $P = [x,y,z] \in C\big(\overline{\mathbb{Q}}\big)$. Pour toute la suite de la démonstration, on considère un corps de nombres k contenant x, y et z. On supposera, ce qui n'est pas restrictif, que x, y et z sont dans O_k.

Proposition 3. *On a l'inégalité*

$$\Big|4h_C(P) - h_E^X\Big(\big(\phi+\psi\big)(P)\Big)\Big| \leqslant \log 69. \tag{10}$$

Démonstration : On vérifie que l'on a

$$\big(\phi+\psi\big)\big([x,y,z]\big) = [U,V,W],$$

$$\text{avec} \quad U = (x+y)z(x^2+xy+y^2)^2, \quad V = -xy(x^2+xy+y^2)(2x^2+3yx+2y^2),$$
$$W = (x+y)^3z^3.$$

Vérifions l'égalité (10) si $(x+y)z = 0$. On a dans ce cas $U = W = 0$ et $\big(\phi+\psi\big)(P) = O$, d'où $h_E^X\Big(\big(\phi+\psi\big)(P)\Big) = 0$.
Si $z = 0$, on a $xy \neq 0$ et pour tout $v \in M_k$ on a $|x|_v = |y|_v$, ce qui conduit d'après la formule du produit à $h_C(P) = 0$ (formule (5)).
Supposons $x + y = 0$. On a alors $2x^4 = z^4$, $xyz \neq 0$ et $P = [1, -1, \alpha]$, où $\alpha \in \overline{\mathbb{Q}}$ vérifie l'égalité $\alpha^4 = 2$. Prenons pour k le corps $\mathbb{Q}(\alpha)$ qui est bien défini à isomorphisme près. On a alors $r_1 = 2$, $r_2 = 1$. Pour toute place $v \in M_k^\infty$, on a $|\alpha|_v = 2^{1/4}$ où $2^{1/4}$ est la racine quatrième positive de 2 dans $\mathbb{R}$. Par ailleurs, α étant dans O_k, on a $|\alpha|_v \leqslant 1$ pour toute place finie $v \in M_k^0$. Il en résulte que l'on a

$$h_C(P) = \frac{1}{4}\Big(4\ \log 2^{1/4}\Big) = \frac{\log 2}{4}.$$

Puisque $4h_C(P) = \log 2$ est plus petit que $\log 41$, l'égalité (10) est donc vraie si $x + y = 0$. D'où notre assertion.

Supposons désormais $(x + y)z$ non nul. Dans ce cas, on a (formule (6))

$$h_E^X\Big(\big(\phi+\psi\big)(P)\Big) = \frac{1}{[k:\mathbb{Q}]}\sum_{v\in M_k} n_v\ \log \mathrm{Max}\Big(\big|x^2+xy+y^2\big|_v^2, \big|(x+y)z\big|_v^2\Big). \tag{11}$$

Pour tout $v \in M_k^0$ on a

$$\big|x^2+xy+y^2\big|_v \leqslant\ \mathrm{Max}\big(|x|_v,|y|_v,|z|_v\big)^2 \quad \text{et} \quad |(x+y)z|_v \leqslant\ \mathrm{Max}\big(|x|_v,|y|_v,|z|_v\big)^2.$$

Par ailleurs, pour tout $v \in M_k^\infty$ on a

$$\big|x^2+xy+y^2\big|_v \leqslant 3\ \mathrm{Max}\big(|x|_v,|y|_v,|z|_v\big)^2 \quad \text{et} \quad |(x+y)z|_v \leqslant 2\ \mathrm{Max}\big(|x|_v,|y|_v,|z|_v\big)^2.$$

On en déduit l'inégalité

$$h_E^X\Big(\big(\phi+\psi\big)(P)\Big) \leqslant \frac{1}{[k:\mathbb{Q}]}\sum_{v\in M_k^0} n_v\ \log \mathrm{Max}\big(|x|_v,|y|_v,|z|_v\big)^4$$

$$+\frac{1}{[k:\mathbb{Q}]}\sum_{v\in M_k^\infty} n_v\ \log\Big(9\ \mathrm{Max}\big(|x|_v,|y|_v,|z|_v\big)^4\Big)$$

Compte tenu du fait que

$$[k:\mathbb{Q}] = \sum_{v\in M_k^\infty} n_v,$$

il en résulte que l'on a

$$h_E^X\Big(\big(\phi+\psi\big)(P)\Big) \leqslant \log 9 + 4h_C(P). \tag{12}$$

Inversement, démontrons que l'on a

$$4h_C(P) \leqslant \log 69 + h_E^X\Big(\big(\phi+\psi\big)(P)\Big). \tag{13}$$

On utilise pour cela la proposition de l'appendice 1. Posons

$$g = (x^2+xy+y^2)^2 \quad \text{et} \quad h = (x+y)^2z^2.$$

Le point $[x,y,z]$ appartenant à $C\big(\overline{\mathbb{Q}}\big)$ on a $x^4+y^4=z^4$. Par suite, les égalités (1) et (2) de cette proposition entraînent, avec ses notations,

$$x^{12} = Q(x,y,z)g + R(x,y,z)h, \quad y^{12} = Q(y,x,z)g + R(y,x,z)h$$

$$z^{12} = 2z^8g - z^6(x+y)^2h.$$

Pour toute place finie $v \in M_k^0$, les éléments x, y et z étant dans O_k, les valeurs absolues v-adiques des éléments $Q(x,y,z)$, $R(x,y,z)$, $Q(y,x,z)$ et $R(y,x,z)$ sont inférieures à $\mathrm{Max}\big(|x|_v,|y|_v,|z|_v\big)^8$. Il en résulte que l'on a

$$\mathrm{Max}\big(|x|_v,|y|_v,|z|_v\big)^4 \leqslant \mathrm{Max}\big(|g|_v,|h|_v\big).$$

Pour toute place $v \in M_k^\infty$ on obtient dans ce cas l'inégalité (cf. les coefficients des polynômes Q et R de la proposition de l'appendice 1)

$$\mathrm{Max}\big(|x|_v,|y|_v,|z|_v\big)^4 \leqslant 69\,\mathrm{Max}\big(|g|_v,|h|_v\big),$$

L'égalité (11) entraîne alors l'inégalité (13). La proposition 3 se déduit alors des conditions (12) et (13). D'où le résultat.

Proposition 4. *On a les inégalités*

$$\big|2h_C(P) - h_E^X\big(\phi(P)\big)\big| \leqslant \frac{\log 2}{2} \quad \textit{et} \quad \big|2h_C(P) - h_E^X\big(\psi(P)\big)\big| \leqslant \frac{\log 2}{2}. \tag{14}$$

Démonstration : Par symétrie par rapport à x et y, il suffit de démontrer la première inégalité de (14). Supposons $z=0$. On a $\phi(P)=[0,1,0]$ et $h_E^X\big(\phi(P)\big)=0$. Par ailleurs, on a $h_C(P)=0$ comme on l'a déjà constaté dans la démonstration de la proposition 3. D'où le résultat dans ce cas.

Supposons z non nul. D'après la condition (8) on a alors

$$h_E^X\big(\phi(P)\big) = \frac{1}{[k:\mathbb{Q}]}\sum_{v\in M_k} n_v \log \mathrm{Max}\big(|x|_v^2,|z|_v^2\big).$$

Posons $a = x^2$ et $b = z^2$. On a $x^4 + y^4 = z^4$. On en déduit pour tout $v \in M_k^0$ l'inégalité $|y|_v^2 \leqslant \mathrm{Max}\big(|a|_v, |b|_v\big)$. Par suite, on a dans ce cas

$$\mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^2 \leqslant \mathrm{Max}\big(|a|_v, |b|_v\big).$$

Par ailleurs, pour tout $v \in M_k^\infty$ on a $|y|_v^2 \leqslant \sqrt{2}\,\mathrm{Max}\big(|a|_v, |b|_v\big)$ et l'on obtient ainsi

$$\mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^2 \leqslant \sqrt{2}\,\mathrm{Max}\big(|a|_v, |b|_v\big).$$

Il en résulte l'inégalité

$$2h_C(P) \leqslant \frac{\log 2}{2} + h_E^X\big(\phi(P)\big).$$

Inversement, pour tout $v \in M_k$ on a

$$|a|_v, |b|_v \leqslant \mathrm{Max}\big(|x|_v, |y|_v, |z|_v\big)^2,$$

d'où $h_E^X\big(\phi(P)\big) \leqslant 2h_C(P)$ et le résultat.

Corollaire 1. *On a les inégalités*

$$\big|h_C(P) - \widehat{h_E}\big(\phi(P)\big)\big| \leqslant 2,426, \quad \big|h_C(P) - \widehat{h_E}\big(\psi(P)\big)\big| \leqslant 2,426,$$

$$\Big|2h_C(P) - \widehat{h_E}\Big(\big(\phi+\psi\big)(P)\Big)\Big| \leqslant 4,37.$$

Démonstration : C'est une conséquence directe de l'inégalité (7) ainsi que des propositions 3 et 4.

Terminons maintenant la démonstration du théorème 3. Posons pour cela

$$\widehat{h_E}\big(\phi(P)\big) = h_C(P) + \delta, \quad \widehat{h_E}\big(\psi(P)\big) = h_C(P) + \beta \quad \text{et} \quad \widehat{h_E}\Big(\big(\phi+\psi\big)(P)\Big) = 2h_C(P) + \gamma.$$

En exprimant le fait que le déterminant de la matrice

$$\begin{pmatrix} 2\big(h_C(P)+\delta\big) & \gamma - (\delta+\beta) \\ \gamma - (\delta+\beta) & 2\big(h_C(P)+\beta\big) \end{pmatrix}$$

est nul, on obtient l'égalité

$$h_C(P)^2 + (\delta+\beta)h_C(P) + \delta\beta - \frac{\big(\gamma - (\delta+\beta)\big)^2}{4} = 0.$$

Le discriminant de cette équation est $2\delta^2 + 2\beta^2 + \gamma^2 - 2\gamma(\delta+\beta)$. Il est donc majoré en valeur absolue par

$$2\delta^2 + 2\beta^2 + \gamma^2 + 2\big|\gamma\big|\big|\delta\big| + 2\big|\gamma\big|\big|\beta\big|,$$

donc d'après le corollaire par $85,046$. Il en résulte que l'on a

$$h_C(P) < \frac{|\delta| + |\beta| + \sqrt{85,046}}{2} < 7,04.$$

Cela termine la démonstration du théorème 3.

2.4. Fin de la démonstration du théorème 1

Rappelons que α désigne une racine quatrième de b dans $\overline{\mathbb{Q}}$. Les courbes C_b et C sont isomorphes sur $L = K(\alpha)$ via le morphisme $f_b : C_b \to C$ défini pour tout point $[x, y, z]$ de C_b par l'égalité

$$f_b\big([x, y, z]\big) = [x, y, \alpha z].$$

Le corps L est un corps minimal, au sens de l'appendice 2, sur lequel les courbes C_b et C sont isomorphes. En effet, par hypothèse b n'est pas une puissance quatrième dans K, ainsi C et C_b ne sont pas isomorphes sur K (chap. IV, appendice 1). L'assertion est donc immédiate si $d = 2$. Supposons $d = 4$ et C_b isomorphe à C sur une extension quadratique H de K contenue dans L. D'après l'appendice 1 du chapitre IV, b est alors une puissance quatrième dans H, ce qui contredit le fait que l'extension $K(\alpha)/K$ soit de degré 4. D'où l'assertion.

Supposons que $C_b(K)$ ne soit pas vide. Considérons un point $P \in C_b(K)$. Posons $P = [x, y, z]$ (où x, y et z sont dans O_K) et $Q = f_b(P) \in C(L)$. On est dans l'un des deux cas intervenant dans l'énoncé du théorème de l'appendice 2.

Supposons que l'on soit dans le premier cas de ce théorème, i.e. qu'il existe σ dans le groupe de Galois de $\overline{\mathbb{Q}}$ sur K tel que ${}^{\sigma}f_b \circ f_b^{-1} \in \mathrm{Aut}(C)$ ne soit pas l'identité et fixe le point Q. On a

$${}^{\sigma}f_b \circ f_b^{-1}(Q) = \big[x, y, \sigma(\alpha)z\big],$$

ce qui conduit à l'égalité $z\big(\sigma(\alpha) - \alpha\big) = 0$. On a $\sigma(\alpha) \neq \alpha$ car ${}^{\sigma}f_b$ est distinct de f_b. Il en résulte que $z = 0$. On en déduit que $xy \neq 0$ puis que $P = [x/y, 1, 0]$ où x/y est une racine primitive huitième de l'unité. En particulier, le groupe μ_4 des racines quatrièmes de l'unité est contenu dans K. Soient i un générateur de μ_4 et $[i]$ l'automorphisme de E_b défini par

$$[i]\big(X, Y, Z\big) = [-X, iY, Z].$$

Le groupe $E_b(K)$ est alors muni de la structure de $\mathbb{Z}[i]$-module définie pour tout $a, b \in \mathbb{Z}$ et $P \in E_b(K)$ par l'égalité

$$(a + ib).P = aP + b[i](P).$$

Ainsi $E_b(K)$ modulo son sous-groupe de torsion est un $\mathbb{Z}[i]$-module libre de rang $r/2$ où r est le rang usuel de $E_b(K)$. L'entier r est donc pair ce qui contredit le fait que $r = 1$.

La condition 2 du théorème de l'appendice 2 est donc satisfaite, autrement dit on a

$$\log \mathrm{N}_{K/\mathbb{Q}}\, D_{L/K} \leqslant \Big(2(d-1)h_C(Q) + \delta_K \log d\Big)d. \tag{15}$$

Les morphismes ϕ et ψ étant définis par les formules (8), vérifions que les points

$$\phi\big(f_b(P)\big) \quad \text{et} \quad \psi\big(f_b(P)\big) \in E(L),$$

sont $\mathbb{Z}$-linérairement dépendants dans $E(L)$. Les courbes elliptiques E_b et E sont isomorphes sur L via le morphisme $g_b : E_b \to E$ défini pour tout point $[X, Y, Z]$ de E_b par l'égalité

$$g_b\big([X, Y, Z]\big) = \left[\frac{X}{\alpha^2}, \frac{Y}{\alpha^3}, Z\right].$$

Par ailleurs, on dispose de deux morphismes $\phi_b : C_b \to E_b$ et $\psi_b : C_b \to E_b$ définis sur K par les égalités

$$\phi_b\big([x, y, z]\big) = [-x^2 z, xy^2, z^3] \quad \text{et} \quad \psi_b\big([x, y, z]\big) = [-y^2 z, yx^2, z^3].$$

On vérifie directement que l'on a

$$g_b^{-1} \circ \phi \circ f_b = \phi_b \quad \text{et} \quad g_b^{-1} \circ \psi \circ f_b = \psi_b.$$

Il en résulte que les points

$$g_b^{-1} \circ \phi \circ f_b(P) \quad \text{et} \quad g_b^{-1} \circ \psi \circ f_b(P),$$

appartiennent à $E_b(K)$. Puisque le rang de $E_b(K)$ est 1, ces points sont donc $\mathbb{Z}$-dépendants sur $E_b(K)$. Le fait que g_b soit un isomorphisme défini sur L de E_b sur E entraîne alors notre assertion. D'après le théorème 3 on a donc l'inégalité

$$h_C\big(f_b(P)\big) < 7,04.$$

On déduit alors de (15) l'inégalité

$$\log \mathrm{N}_{K/\mathbb{Q}}\, D_{L/K} < \Big(14.08\ (d-1) + \delta_K \log d\Big)d,$$

ce qui contredit l'inégalité (1) du théorème 1. Cela termine sa démonstration.

3. Démonstration du théorème 2

Rappelons que dans cette partie K désigne un corps totalement réel de degré n sur $\mathbb{Q}$. On reprend les notations du paragraphe 2.1, à ceci près que pour toute place finie $v \in M_K^0$, on note ici $v : K^* \to \mathbb{Z}$ la valuation standard normalisée associée à l'idéal premier de O_K

qui lui correspond. Avec cette notation, si v est de caractéristique résiduelle p, on a pour tout $x \in K^*$

$$|x|_v = p^{-v(x)/e_v}, \tag{16}$$

où e_v est l'indice de ramification de v sur p.

Soit b un élément de O_K vérifiant les deux premières conditions du théorème 2. Il s'agit de montrer que si la norme de K sur $\mathbb{Q}$ de b est assez grande, comme il est précisé dans l'énoncé de ce théorème, l'ensemble $C_b(K)$ est vide.

3.1. Réduction sur b

S'il existe un plongement σ de K dans $\mathbb{R}$ tel que $\sigma(b) < 0$, il est immédiat que $C_b(K)$ est vide et le théorème est démontré dans ce cas. On peut donc supposer que b est totalement positif, autrement dit que pour tout plongement $\sigma : K \to \mathbb{R}$, on a $\sigma(b) > 0$. Compte tenu de l'appendice 3 et de la deuxième inégalité de la condition (4), il existe donc une unité u de O_K telle que pour tout plongement de K dans $\mathbb{R}$ on ait $\sigma(bu^4) \geqslant 1$. Par ailleurs, les courbes C_b et C_{bu^4} sont K-isomorphes et si l'on remplace b par bu^4 les trois conditions intervenant dans l'énoncé du théorème ne changent pas. Quitte à remplacer b par bu^4, on peut donc supposer, ce que l'on fera dans toute la suite, que la condition suivante est satisfaite :

$$\text{pour tout plongement } \sigma : K \to \mathbb{R}, \text{ on a } \sigma(b) \geqslant 1. \tag{17}$$

3.2. La courbe elliptique E_b

Afin de simplifier les notations, on notera dans la suite E_b la courbe affine d'équation de Weierstrass

$$y^2 = x^3 - bx. \tag{18}$$

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

$$c_4 = 2^4.3.b, \quad c_6 = 0 \quad \text{et} \quad \Delta = 2^6.b^3. \tag{19}$$

La courbe E_b a bonne réduction en toutes les places finies $v \in M_K^0$ pour lesquelles on a $v(2b) = 0$. Son invariant modulaire est 1728, il est entier, donc E_b a partout potentiellement bonne réduction.

Lemme 1. *Soit v une place finie de K telle que $v(b) > 0$. Alors, le modèle* (18) *est minimal en v et E_b a mauvaise réduction de type additif en v.*

Démonstration : Posons $m = v(b)$ et $e = v(2)$. D'après la condition 1 du théorème, on a $m = 1, 2$ ou 3. Cela entraîne l'assertion si $e = 0$. Supposons $e \geqslant 1$. D'après (19), on a

$$v(c_4) = 4e + m \quad \text{et} \quad v(\Delta) = 6e + 3m. \tag{20}$$

Supposons que le modèle (18) ne soit pas minimal en v, autrement dit qu'il ne soit pas minimal sur le complété K_v de K en v. Dans ce cas, il existe un élément $u \in K_v$ de valuation > 0 tel que

$$\frac{c_4}{u^4}, \quad \frac{c_6}{u^6} \ (=0) \quad \text{et} \quad \frac{\Delta}{u^{12}},$$

appartiennent à l'anneau de valuation de K_v et soient les invariants standard associés à une courbe elliptique sur K_v. En notant encore v le prolongement de v à K_v, on déduit de (20) les inégalités

$$0 < v\Big(\frac{c_4}{u^4}\Big) < 4e \quad \text{et} \quad v\Big(\frac{c_4}{u^4}\Big) \not\equiv 0 \text{ mod. } 4.$$

Cela contredit le théorème 2 de [Kr1] et la remarque qui le suit. D'où le résultat.

Considérons une place finie v de K telle que $v(b) > 0$. Soient K_v le complété de K en v et k_v le corps résiduel. On déduit du lemme 1 que la courbe sur k_v déduite de la courbe elliptique E_b par réduction possède un unique point singulier qui est $(0,0)$ (cf. [Si2], p.173). On désigne par $E_b^0(K_v)$ le sous-groupe de $E_b(K_v)$ formé des points de réduction non singulière sur k_v.

Lemme 2. *Supposons $v(b) > 0$. Soit $P = (x,y)$ un point de $E_b(K_v)$. Alors, P appartient à $E_b^0(K_v)$ si et seulement si $v(x) \leqslant 0$.*

Démonstration : Le modèle (18) étant minimal sur K_v, la condition annoncée est clairement nécessaire car si $v(x) > 0$ on a aussi $v(y) > 0$. Inversement, supposons $v(x) \leqslant 0$. Posons $x = \pi^n a$, où π est une uniformisante de K_v, $n \leqslant 0$ et $v(a) = 0$. Si $n = 0$, on a $v(y) \geqslant 0$ et P ne se réduit pas en $(0,0)$. Si $n < 0$, on a $2v(y) = 3v(x)$ et P se réduit en le point $[0,1,0]$ sur la courbe projective réduite $Y^2Z = X^3$, en particulier $P \in E_b^0(K_v)$. D'où le lemme.

Pour tout point $P = (x,y) \in E_b(K)$ à distance finie, on notera désormais

$$H_x(P) = \prod_{v \in M_K} \mathrm{Max}\big(1, |x|_v\big)^{n_v/n} \quad \text{et} \quad h_x(P) = \log H_x(P), \tag{21}$$

où, comme dans le paragraphe 2.1, n_v est le degré local en v. On pose $H_x(O) = 1$, où O est le point à l'infini de E_b.

3.3. Le sous-groupe Γ de $E_b(K)$

On va maintenant définir un sous-groupe Γ d'indice fini de $E_b(K)$. Considérons pour cela le sous-ensemble G de $E_b(K)$ formé des points qui appartiennent à $E_b^0(K_v)$ pour toute place finie $v \in M_K^0$ telle que $v(b) > 0$. D'après le lemme 2, étant donné $P = (x,y) \in E_b(K)$, on a l'équivalence

$$P \in G \Longleftrightarrow v(x) \leqslant 0 \quad \text{pour toute place } v \in M_K^0 \text{ telle que } v(b) > 0. \tag{22}$$

C'est un sous-groupe d'indice fini de $E_b(K)$ car $E_b^0(K_v)$ est lui-même un sous-groupe d'indice fini de $E_b(K_v)$ ([Si2], p. 359).

Pour tout plongement $\sigma : K \to \mathbb{R}$ notons $E_{\sigma(b)}$ la courbe elliptique définie sur $\mathbb{R}$ d'équation

$$y^2 = x^3 - \sigma(b)x.$$

Puisque les trois abscisses des points d'ordre 2 de $E_{\sigma(b)}$ sont réelles, l'ensemble $E_{\sigma(b)}(\mathbb{R})$ possède deux composantes connexes. On désigne par I_σ la composante connexe de l'élément neutre. Compte tenu du fait que l'on a $\sigma(b) > 0$, pour tout point $M = (x, y) \in E_{\sigma(b)}(\mathbb{R})$, on a l'équivalence (en prenant la racine carrée positive)

$$M \in I_\sigma \iff x \geqslant \sqrt{\sigma(b)}. \tag{23}$$

Par ailleurs, pour tout $M \in E_{\sigma(b)}(\mathbb{R})$, le point $2M$ appartient à I_σ.

On définit alors Γ comme étant le sous-ensemble de G formé des points $P \in G$ tels que $\sigma(P)$ appartienne à I_σ pour tout plongement $\sigma : K \to \mathbb{R}$. C'est une sous-groupe de G et d'après l'assertion précédente, il est d'indice 2 dans G. En particulier, Γ est un sous-groupe d'indice fini de $E_b(K)$.

3.4. Hauteurs sur Γ

Pour tout idéal $\mathscr{I}$ de O_K, on notera dans toute la suite $\mathrm{N}(\mathscr{I})$ la norme de K sur $\mathbb{Q}$ de $\mathscr{I}$.

Lemme 3. *Soit $Q = (x, y)$ un point de $E_b(K)$. Supposons que pour tout plongement $\sigma : K \to \mathbb{R}$, le point $\sigma(Q)$ appartienne à I_σ. On a l'égalité*

$$H_x(Q)^n = \prod_{\{\mathfrak{p}\ ;\ v_\mathfrak{p}(x)>0\}} \mathrm{N}(\mathfrak{p})^{v_\mathfrak{p}(x)},$$

le produit étant indexé par l'ensemble des idéaux premiers $\mathfrak{p}$ de O_K tels que $v_\mathfrak{p}(x) > 0$.

Démonstration : D'après (21), on a

$$H_x(P)^n = \prod_{v \in M_K^0} \mathrm{Max}\big(1, |x|_v\big)^{n_v} \prod_{v \in M_K^\infty} \mathrm{Max}\big(1, |x|_v\big)^{n_v}.$$

Soit v une place finie. La formule (16) entraîne l'égalité

$$|x|_v^{n_v} = q_v^{-v(x)},$$

où q_v est le cardinal du corps résiduel de v. Si $\mathfrak{p}$ est l'idéal premier de O_K correspondant à v, on a donc

$$|x|_v = \mathrm{N}(\mathfrak{p})^{-v_\mathfrak{p}(x)}.$$

Il en résulte que l'on a

$$\prod_{v \in M_K^0} \mathrm{Max}\big(1, |x|_v\big)^{n_v} = \prod_{\{\mathfrak{p}\ ;\ v_\mathfrak{p}(x)<0\}} \mathrm{N}(\mathfrak{p})^{-v_\mathfrak{p}(x)}. \tag{24}$$

Par ailleurs, l'hypothèse faite et les conditions (23) et (17) entraînent que pour tout plongement $\sigma : K \to \mathbb{R}$, on a $\sigma(x) \geqslant \sqrt{\sigma(b)} \geqslant 1$. Les dégrés locaux n_v étant égaux à 1 pour les places infinies, on obtient

$$\prod_{v \in M_K^\infty} \mathrm{Max}\big(1, |x|_v\big)^{n_v} = \big|N_{K/\mathbb{Q}}(x)\big| = \prod_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{v_{\mathfrak{p}}(x)}. \tag{25}$$

Les égalités (24) et (25) entraînent alors le lemme.

Considérons maintenant un point $P = (x, y) \in E_b(K)$ tel que $2P \neq O$. L'abscisse de $2P$ est donnée par l'égalité

$$x(2P) = \frac{(x^2 + b)^2}{4x(x^2 - b)}. \tag{26}$$

Pour tout idéal premier $\mathfrak{p}$ de O_K posons $\alpha(\mathfrak{p}) = v_{\mathfrak{p}}(x)$. Notons A l'ensemble des idéaux premiers $\mathfrak{p}$ tels que $\alpha(\mathfrak{p}) > 0$ et B l'ensemble des idéaux premiers $\mathfrak{p}$ tels que $\alpha(\mathfrak{p}) < 0$. Les décompositions des idéaux fractionnaires xO_K, $(x^2 + b)O_K$ et $(x^2 - b)O_K$ en produit d'idéaux premiers sont de la forme :

$$xO_K = \prod_{\mathfrak{p} \in A} \mathfrak{p}^{\alpha(\mathfrak{p})} \prod_{\mathfrak{p} \in B} \mathfrak{p}^{\alpha(\mathfrak{p})}, \tag{27}$$

$$(x^2 + b)O_K = \prod_{\mathfrak{p} \in B} \mathfrak{p}^{2\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q}) > 0\}} \mathfrak{q}^{\beta(\mathfrak{q})}, \tag{28}$$

$$(x^2 - b)O_K = \prod_{\mathfrak{p} \in B} \mathfrak{p}^{2\alpha(\mathfrak{p})} \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r}) > 0\}} \mathfrak{r}^{\gamma(\mathfrak{r})}, \tag{29}$$

où pour tous idéaux premiers $\mathfrak{q}$ et $\mathfrak{r}$, on pose $\beta(\mathfrak{q}) = v_{\mathfrak{q}}(x^2 + b)$ et $\gamma(\mathfrak{r}) = v_{\mathfrak{r}}(x^2 - b)$. Démontrons le lemme suivant :

Lemme 4. *Supposons que P appartienne à G. Il existe un idéal I de O_K qui divise $8O_K$ tel que l'on ait*

$$H_x(2P)^n = \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q}) > 0\}} \mathrm{N}(\mathfrak{q})^{2\beta(\mathfrak{q})} \times \frac{1}{\mathrm{N}(I)}.$$

Démonstration : D'après l'égalité (26), on a

$$x(2P)O_K = \prod_{\mathfrak{p} \in B} \mathfrak{p}^{\alpha(\mathfrak{p})} \prod_{\mathfrak{p} \in A} \mathfrak{p}^{-\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q}) > 0\}} \mathfrak{q}^{2\beta(\mathfrak{q})} \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r}) > 0\}} \mathfrak{r}^{-\gamma(\mathfrak{r})}\ (4O_K)^{-1}. \tag{30}$$

Soit I le plus grand commun diviseur des deux idéaux entiers

$$\prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathfrak{q}^{2\beta(\mathfrak{q})} \quad \text{et} \quad \prod_{\mathfrak{p}\in A} \mathfrak{p}^{\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in B} \mathfrak{p}^{-\alpha(\mathfrak{p})} \prod_{\{\mathfrak{r}\ :\ \gamma(\mathfrak{r})>0\}} \mathfrak{r}^{\gamma(\mathfrak{r})}\ (4O_K).$$

Le point $2P$ vérifie l'hypothèse faite dans l'énoncé du lemme 3. L'égalité (30) et le lemme 3 entraînent alors l'égalité

$$H_x(2P)^n = \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{2\beta(\mathfrak{q})} \times \frac{1}{\mathrm{N}(I)}.$$

Tout revient donc à prouver que

$$I \text{ divise } 8O_K. \tag{31}$$

Considérons pour cela un idéal premier $\mathfrak{P}$ de O_K qui divise I. Puisque $\mathfrak{P}$ divise le produit des idéaux $\mathfrak{q}^{2\beta(\mathfrak{q})}$ où $\beta(\mathfrak{q})>0$, on déduit de (28) que

$$\mathfrak{P} \text{ ne divise pas } \prod_{\mathfrak{p}\in B} \mathfrak{p}^{-\alpha(\mathfrak{p})}.$$

Par suite, on a $v_{\mathfrak{P}}(x) \geqslant 0$. Il en résulte que

$$v_{\mathfrak{P}}(x) = 0. \tag{32}$$

En effet, dans le cas contraire, on aurait $v_{\mathfrak{P}}(x) > 0$ et $v_{\mathfrak{P}}(x^2+b) > 0$, d'où $v_{\mathfrak{P}}(b) > 0$, ce qui, d'après le lemme 2, contredit le fait que P soit dans G. On en déduit que

$$I \text{ divise } \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r})>0\}} \mathfrak{r}^{\gamma(\mathfrak{r})}\ (4O_K). \tag{33}$$

En particulier, on a l'inégalité

$$v_{\mathfrak{P}}\big(4(x^2-b)\big) > 0. \tag{34}$$

Par ailleurs, on a

$$v_{\mathfrak{P}}(x^2+b) > 0. \tag{35}$$

Les conditions (32), (34) et (35) entraînent alors que $\mathfrak{P}$ est l'un des idéaux premiers de O_K au-dessus de 2. Il reste à démontrer que l'on a, $v_{\mathfrak{P}}(I)$ étant l'exposant de $\mathfrak{P}$ dans I,

$$v_{\mathfrak{P}}(I) \leqslant 3v_{\mathfrak{P}}(2). \tag{36}$$

Supposons pour cela que l'on ait $v_{\mathfrak{P}}(I) \geqslant 3v_{\mathfrak{P}}(2)+1$. D'après la condition (33) et le fait que I divise le produit des idéaux $\mathfrak{q}^{2\beta(\mathfrak{q})}$ où $\beta(\mathfrak{q})>0$, on a

$$2v_{\mathfrak{P}}(x^2+b) \geqslant v_{\mathfrak{P}}(I) \quad \text{et} \quad v_{\mathfrak{P}}\big(4(x^2-b)\big) \geqslant v_{\mathfrak{P}}(I).$$

On obtient alors

$$v_{\mathfrak{P}}(x^2+b) \geqslant \frac{3v_{\mathfrak{P}}(2)+1}{2} \quad \text{et} \quad v_{\mathfrak{P}}(\big(4(x^2-b)\big) \geqslant 3v_{\mathfrak{P}}(2)+1,$$

ce qui conduit aux inégalités

$$v_{\mathfrak{P}}(x^2+b) \geqslant v_{\mathfrak{P}}(2)+1 \quad \text{et} \quad v_{\mathfrak{P}}(x^2-b) \geqslant v_{\mathfrak{P}}(2)+1.$$

On en déduit que $2v_{\mathfrak{P}}(x) \geqslant 1$ et la condition (32) implique alors une contradiction. Cela prouve l'inégalité (36), puis la condition (31). D'où le résultat.

3.5. Comparaison entre les hauteurs $\widehat{h}$ et h_x sur Γ

Notons $\widehat{h}$ la hauteur de Néron-Tate sur E_b. On a une égalité de la forme $2\widehat{h} = h_x + O(1)$ où h_x est définie par la formule (6) déshomogénisée ([Si2], p. 229). On va maintenant effectiviser cette égalité uniformément, i.e. indépendamment de b, sur le groupe Γ. Démontrons le résultat suivant :

Proposition 5. *Soit P un point de Γ. On a*

$$\big|2\widehat{h}(P) - h_x(P)\big| \leqslant \log 2.$$

Prouvons pour cela l'énoncé ci-dessous :

Lemme 5. *On a $\big|h_x(2P) - 4h_x(P)\big| \leqslant 3\log 2$.*

Démonstration : Vérifions d'abord que cette inégalité est vraie si $2P = O$. Tel est le cas si $P = O$, car alors $h_x(P) = h_x(2P) = 0$. Supposons $P \neq O$. Soit $a \in \overline{\mathbb{Q}}$ tel que $b = a^2$. On a alors $P = (0,0)$ ou bien $P = \big(\pm a, 0\big)$, cette dernière éventualité ne pouvant se produire que si a est dans K. Pour tout plongement $\sigma : K \to \mathbb{R}$, le point $\sigma(P)$ étant dans I_σ, on a $P \neq (0,0)$, d'où $P = \big(\pm a, 0\big)$. Par ailleurs, P appartient à G. D'après l'équivalence (22), l'élément a est donc une unité de O_K. On obtient $H_x(P) = \big|N_{K/\mathbb{Q}}(a)\big| = 1$, d'où $h_x(P) = 0$ et notre assertion (car $h_x(2P) = 0$).

Supposons désormais $2P \neq O$ et que les décompositions des idéaux fractionnaires xO_K et $(x^2+b)O_K$ soient données par les formules (27) et (28).
Pour tout plongement $\sigma : K \to \mathbb{R}$, le point $\sigma(P)$ étant dans I_σ, on déduit de l'équivalence (23) que l'on a

$$\mathrm{N}_{K/\mathbb{Q}}(x^2+b) = \prod_{\sigma} \big(\sigma(x^2) + \sigma(b)\big) \leqslant \mathrm{N}_{K/\mathbb{Q}}(2x^2).$$

Il en résulte que

$$\prod_{\mathfrak{p}\in B} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{\beta(\mathfrak{q})} \leqslant 2^n \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in B} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})},$$

d'où l'inégalité

$$\prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{\beta(\mathfrak{q})} \leqslant 2^n \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})}.$$

On déduit alors des lemmes 3 et 4 que l'on a

$$H_x(2P)^n \leqslant 2^{2n} \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{4\alpha(\mathfrak{p})} = 2^{2n} H_x(P)^{4n}. \tag{37}$$

Par ailleurs, b étant totalement positif, on a

$$\mathrm{N}_{K/\mathbb{Q}}(x^2+b) \geqslant \mathrm{N}_{K/\mathbb{Q}}(x^2).$$

On déduit alors de (28) que l'on a

$$\prod_{\mathfrak{p}\in B} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{\beta(\mathfrak{q})} \geqslant \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in B} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})},$$

autrement dit,

$$\prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{\beta(\mathfrak{q})} \geqslant \prod_{\mathfrak{p}\in A} \mathrm{N}(\mathfrak{p})^{2\alpha(\mathfrak{p})}.$$

Puisque l'on a $\mathrm{N}(8O_K) = 8^n$, on déduit alors des lemmes 3 et 4 l'inégalité

$$H_x(2P)^n \geqslant \frac{1}{8^n} H_x(P)^{4n}. \tag{38}$$

D'où le lemme en prenant les logarithmes des inégalités (37) et (38).

La proposition 5 est alors une conséquence directe du lemme 5 et du résultat qui suit (cf. [Si2], p. 228-229) :

Lemme 6. *Soit S un sous-ensemble de $E_b(K)$ stable par multiplication par 2. Supposons qu'il existe une constante $c > 0$ telle que pour tout $Q \in S$ l'on ait $\left|h_x(2Q) - 4h_x(Q)\right| \leqslant c$. Alors, pour tout $Q \in S$, on a $\left|2\widehat{h}(Q) - h_x(Q)\right| \leqslant c/3$.*

Démonstration : Rappelons que pour tout point $M \in E_b(K)$, on a (*loc. cit.*) :

$$\widehat{h}(M) = \frac{1}{2} \lim_{n\to+\infty} \frac{h_x(2^n M)}{4^n}.$$

Considérons un point $Q \in S$. Pour tout entier $n \geqslant 1$ on a

$$\frac{1}{4^n} h_x(2^n Q) - h_x(Q) = \sum_{j=0}^{n-1} \left(\frac{1}{4^{j+1}} h_x(2^{j+1} Q) - \frac{1}{4^j} h_x(2^j Q) \right).$$

On en déduit l'inégalité

$$\Big| \frac{1}{4^n} h_x(2^n Q) - h_x(Q) \Big| \leqslant \sum_{j=0}^{n-1} \frac{1}{4^{j+1}} \big| h_x(2^{j+1} Q) - 4 h_x(2^j Q) \big|.$$

Par hypothèse, $2^j Q$ appartient à S. Il en résulte que l'on a

$$\Big| \frac{1}{4^n} h_x(2^n Q) - h_x(Q) \Big| \leqslant c \sum_{j=0}^{n-1} \frac{1}{4^{j+1}}.$$

On obtient ainsi

$$\lim_{n \to +\infty} \Big| \frac{1}{4^n} h_x(2^n Q) - h_x(Q) \Big| \leqslant \frac{c}{3},$$

ce qui entraîne le lemme.

Cela termine la démonstration de la proposition 5.

3.6. Hauteurs sur les images de $C_b(K)$ dans $E_b(K)$

Rappelons que l'on dispose de deux morphismes $\phi_b : C_b \to E_b$ et $\psi_b : C_b \to E_b$ définis sur K par les égalités

$$\phi_b\big([x, y, z]\big) = [-x^2 z, xy^2, z^3] \quad \text{et} \quad \psi_b\big([x, y, z]\big) = [-y^2 z, yx^2, z^3].$$

Considérons dans tout ce paragraphe un point $Q = [x, y, z] \in C_b(K)$. On a $z \neq 0$, car sinon -1 est une puissance quatrième dans K, ce qui contredit le fait que K soit totalement réel. On peut donc supposer que l'on a $z = 1$. On a ainsi l'égalité

$$x^4 + y^4 = b. \tag{39}$$

Posons $P_1 = \varphi_b(Q)$ et $P_2 = \psi_b(Q)$ dans $E_b(K)$. On a dans le modèle affine (18)

$$P_1 = (-x^2, xy^2) \quad \text{et} \quad P_2 = (-y^2, yx^2). \tag{40}$$

Lemme 7. *Les points P_1 et P_2 appartiennent à G.*

Démonstration : Soit v une place finie de K telle que $v(b) > 0$. D'après l'équivalence (22) et les égalités (40), il s'agit de démontrer que l'on a $v(x) \leqslant 0$. Supposons $v(x) > 0$.

L'égalité (39) entraîne alors $v(y) > 0$ puis $v(b) \geqslant 4$, ce qui contredit la condition 1 de l'énoncé du théorème 2. D'où notre assertion et le résultat.

Proposition 6. *On a les inégalités*

$$\big|h_x(2P_1) - h_x(2P_2)\big| \leqslant 5\log 2 \qquad \textit{et} \qquad \big|\widehat{h}(P_1) - \widehat{h}(P_2)\big| \leqslant \frac{7}{8}\log 2.$$

Démonstration : 1) Prouvons la première inégalité. Elle est vraie si $xy = 0$, car dans ce cas, compte tenu de l'égalité (39), les points P_1 et P_2 sont d'ordre 2 dans $E_b(K)$.

Supposons désormais xy non nul. Dans ce cas, P_1 et P_2 ne sont pas d'ordre 2 et les abscisses de $2P_1$ et $2P_2$ sont données par les égalités

$$x(2P_1) = \frac{(x^4+b)^2}{4x^2(b-x^4)} \quad \text{et} \quad x(2P_2) = \frac{(y^4+b)^2}{4y^2(b-y^4)}. \tag{41}$$

Pour tout idéal premier $\mathfrak{p}$ de O_K, posons, comme précédemment, $\alpha_\mathfrak{p} = v_\mathfrak{p}(x)$ et notons A l'ensemble des idéaux premiers $\mathfrak{p}$ tels que $v_\mathfrak{p}(x) > 0$ et B l'ensemble des idéaux premiers tels que $v_\mathfrak{p}(x) < 0$. Les décompositions des idéaux fractionnaires xO_K et $(x^4+b)O_K$ en produit d'idéaux premiers sont de la forme :

$$xO_K = \prod_{\mathfrak{p}\in A} \mathfrak{p}^{\alpha(\mathfrak{p})} \prod_{\mathfrak{p}\in B} \mathfrak{p}^{\alpha(\mathfrak{p})},$$

$$(x^4+b)O_K = \prod_{\mathfrak{p}\in B} \mathfrak{p}^{4\alpha(\mathfrak{p})} \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathfrak{q}^{\beta(\mathfrak{q})}. \tag{42}$$

Par ailleurs, pour tout idéal premier $\mathfrak{p}$ de O_K, compte tenu de (39), on a $v_\mathfrak{p}(x) < 0$ si et seulement si $v_\mathfrak{p}(y) < 0$ et dans ce cas $v_\mathfrak{p}(x) = v_\mathfrak{p}(y)$. Il en résulte que la décomposition de $(y^4+b)O_K$ en produit d'idéaux premiers est de la forme suivante :

$$(y^4+b)O_K = \prod_{\mathfrak{p}\in B} \mathfrak{p}^{4\alpha(\mathfrak{p})} \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r}))>0\}} \mathfrak{r}^{\gamma(\mathfrak{r})}. \tag{43}$$

D'après les lemmes 4 et 7 et les égalités (40), il existe ainsi deux idéaux J_1 et J_2 de O_K qui divisent $8O_K$ tels que l'on ait

$$H_x(2P_1)^n = \prod_{\{\mathfrak{q}\ ;\ \beta(\mathfrak{q})>0\}} \mathrm{N}(\mathfrak{q})^{2\beta(\mathfrak{q})} \times \frac{1}{\mathrm{N}(J_1)},$$

$$H_x(2P_2)^n = \prod_{\{\mathfrak{r}\ ;\ \gamma(\mathfrak{r})>0\}} \mathrm{N}(\mathfrak{r})^{2\gamma(\mathfrak{r})} \times \frac{1}{\mathrm{N}(J_2)}.$$

D'après (42) et (43) on obtient donc l'égalité

$$\frac{H_x(2P_1)^n}{H_x(2P_2)^n} = \frac{\mathrm{N}_{K/\mathbb{Q}}(x^4+b)^2}{\mathrm{N}_{K/\mathbb{Q}}(y^4+b)^2} \times \frac{N(J_2)}{N(J_1)}.$$

L'égalité (39) entraîne alors

$$\frac{H_x(2P_1)^n}{H_x(2P_2)^n} = \frac{\mathrm{N}_{K/\mathbb{Q}}(2x^4+y^4)^2}{\mathrm{N}_{K/\mathbb{Q}}(2y^4+x^4)^2} \times \frac{N(J_2)}{N(J_1)}.$$

Posons

$$t = \frac{x^4}{y^4}.$$

On obtient

$$\frac{H_x(2P_1)^n}{H_x(2P_2)^n} = \frac{\mathrm{N}_{K/\mathbb{Q}}(2t+1)^2}{\mathrm{N}_{K/\mathbb{Q}}(t+2)^2} \times \frac{N(J_2)}{N(J_1)},$$

ce qui conduit à

$$\frac{H_x(2P_1)^n}{H_x(2P_2)^n} = \mathrm{N}_{K/\mathbb{Q}}\Big(2 - \frac{3}{t+2}\Big)^2 \times \frac{N(J_2)}{N(J_1)}. \tag{44}$$

Pour tout plongement $\sigma : K \to \mathbb{R}$, on a $\sigma(t) \geqslant 0$, d'où il résulte que l'on a

$$\frac{1}{2} \leqslant 2 - \frac{3}{\sigma(t)+2} \leqslant 2.$$

On en déduit les inégalités

$$\frac{1}{2^n} \leqslant \mathrm{N}_{K/\mathbb{Q}}\Big(2 - \frac{3}{t+2}\Big) \leqslant 2^n. \tag{45}$$

On déduit alors de (44) et (45) que l'on a

$$\frac{1}{2^{2n}} \times \frac{1}{8^n} = \frac{1}{2^{5n}} \leqslant \frac{H_x(2P_1)^n}{H_x(2P_2)^n} \leqslant 2^{2n} \times 8^n = 2^{5n}.$$

D'où la première inégalité de la proposition.

2) En ce qui concerne la deuxième inégalité, on a

$$\big|\widehat{h}(P_1) - \widehat{h}(P_2)\big| = \frac{1}{4}\big|\widehat{h}(2P_1) - \widehat{h}(2P_2)\big|.$$

Il en résulte que

$$\big|\widehat{h}(P_1) - \widehat{h}(P_2)\big| \leqslant \frac{1}{4}\Big(\big|\widehat{h}(2P_1) - \frac{1}{2}h_x(2P_1)\big| + \frac{1}{2}\big|h_x(2P_1) - h_x(2P_2)\big| + \big|\frac{1}{2}h_x(2P_2) - \widehat{h}(2P_2)\big|\Big).$$

Par ailleurs, on déduit du lemme 7 que $2P_1$ et $2P_2$ appartiennent au sous-groupe Γ de $E_b(K)$. L'inégalité déjà prouvée et la proposition 5 entraînent alors le résultat. D'où la proposition.

3.7. Fin de la démonstration du théorème 2

On suppose que l'ensemble $C_b(K)$ est non vide. Il s'agit d'obtenir une contradiction. Comme on l'a constaté au début du paragraphe 3.6, il existe alors $Q = (x, y) \in C_b(K)$ dans l'ouvert affine $z = 1$, l'égalité (39) étant ainsi satisfaite. On pose comme précédemment

$$P_1 = \varphi_b(Q) \quad \text{et} \quad P_2 = \psi_b(Q).$$

Vérifions que l'on a

$$P_1 + P_2 \neq O \quad \text{et} \quad P_1 - P_2 \neq O. \tag{46}$$

Supposons $P_1 = \pm P_2$. D'après (40), on a $P_1 = (-x^2, xy^2)$ et $P_2 = (-y^2, yx^2)$, d'où $x^2 = y^2$, puis $b = 2x^4$. Soit v une place finie de K telle que $v(x) \neq 0$. On a $v(2) > 0$: en effet, dans le cas contraire, on aurait $v(b) = 4v(x) > 0$ (car $b \in O_K$) ce qui contredit la condition 1 de l'énoncé du théorème 2. Par suite, on a

$$xO_K = \prod_{\mathfrak{p}|2} \mathfrak{p}^{\alpha(\mathfrak{p})},$$

où $\mathfrak{p}$ parcourt l'ensemble des idéaux premiers de O_K au-dessus de 2 et où $\alpha(\mathfrak{p}) \in \mathbb{Z}$. Pour la même raison, l'égalité $b = 2x^4$ entraîne $\alpha(\mathfrak{p}) \leqslant 0$ pour tout $\mathfrak{p}$. On en déduit que

$$\mathrm{N}_{K/\mathbb{Q}}(b) \leqslant 2^n,$$

ce qui contredit l'inégalité $\mathrm{N}_{K/\mathbb{Q}}(b) \geqslant 2^{\frac{11n}{2}}$ intervenant dans la condition 3 de l'énoncé du théorème. D'où l'assertion (46).

On désigne par R un point de $E_b(K)$ vérifiant la condition suivante : si $E_b(K)$ est de rang 0 on a $R = O$, et si $E_b(K)$ est de rang 1 alors R est un générateur de $E_b(K)$ modulo son sous-groupe de torsion. Il existe ainsi des entiers m, n et des points de torsion T_1, T_2 de $E_b(K)$ tels que l'on ait

$$P_1 = mR + T_1 \quad \text{et} \quad P_2 = nR + T_2.$$

Soit N un multiple des ordres de T_1 et T_2. On a $NP_1 = NmR$ et $NP_2 = NnR$. On en déduit les égalités

$$\widehat{h}(P_1) = m^2\widehat{h}(R) \quad \text{et} \quad \widehat{h}(P_2) = n^2\widehat{h}(R). \tag{47}$$

De même, on a

$$\widehat{h}(P_1+P_2)=(m+n)^2\widehat{h}(R)\quad\text{et}\quad\widehat{h}(P_1-P_2)=(m-n)^2\widehat{h}(R).$$

On en déduit que

$$\widehat{h}(P_1+P_2)\leqslant|m^2-n^2|\widehat{h}(R)\quad\text{si}\quad mn\leqslant 0, \tag{48}$$

$$\widehat{h}(P_1-P_2)\leqslant|m^2-n^2|\widehat{h}(R)\quad\text{si}\quad mn\geqslant 0. \tag{49}$$

Considérons alors un plongement $\sigma : K\to\mathbb{R}$. D'après (40), on a

$$\sigma\big(x(P_1)\big)\leqslant 0\quad\text{et}\quad\sigma\big(x(P_2)\big)\leqslant 0,$$

par suite $\sigma(P_1)$ et $\sigma(P_2)$ n'appartiennent pas à la composante neutre I_σ. Par définition de la loi de groupe sur $E_{\sigma(b)}$, les points $\sigma(P_1+P_2)$ et $\sigma(P_1-P_2)$ sont donc dans I_σ. D'après le lemme 7, il en résulte que

$$P_1+P_2\in\Gamma\quad\text{et}\quad P_1-P_2\in\Gamma.$$

D'après la proposition 5, on obtient alors

$$h_x(P_1+P_2)\leqslant 2\widehat{h}(P_1+P_2)+\log 2\quad\text{et}\quad h_x(P_1-P_2)\leqslant 2\widehat{h}(P_1-P_2)+\log 2. \tag{50}$$

Compte tenu des conditions (48), (49) et (50), on a donc les inégalités

$$h_x(P_1+P_2)\leqslant 2|m^2-n^2|\widehat{h}(R)+\log 2\quad\text{si}\quad mn\leqslant 0,$$

$$h_x(P_1-P_2)\leqslant 2|m^2-n^2|\widehat{h}(R)+\log 2\quad\text{si}\quad mn\geqslant 0.$$

Supposons $mn\leqslant 0$. Dans ce cas, les égalités (47) entraînent

$$h_x(P_1+P_2)\leqslant 2|\widehat{h}(P_1)-\widehat{h}(P_2)|+\log 2.$$

D'après la proposition 6, on en déduit que

$$h_x(P_1+P_2)\leqslant\frac{11}{4}\log 2. \tag{51}$$

De même, si $mn\geqslant 0$, on obtient

$$h_x(P_1-P_2)\leqslant\frac{11}{4}\log 2. \tag{52}$$

Démontrons maintenant que l'on a

$$nh_x(P_1+P_2) \geqslant \frac{\log \mathrm{N}_{K/\mathbb{Q}}(b)}{2} \quad \text{et} \quad nh_x(P_1-P_2) \geqslant \frac{\log \mathrm{N}_{K/\mathbb{Q}}(b)}{2}. \tag{53}$$

D'après (46), le point P_1+P_2 est non nul. Posons $P_1+P_2=(u,w)\in E_b(K)$. On a

$$H_x(P_1+P_2)^n = \prod_{v\in M_K} \mathrm{Max}\big(1,|u|_v\big)^{n_v} \geqslant \prod_{v\in M_K^\infty} \mathrm{Max}\big(1,|u|_v\big).$$

Par ailleurs, puisque P_1+P_2 appartient à Γ, on a $|\sigma(u)|=\sigma(u)\geqslant\sqrt{\sigma(b)}$ pour tout plongement $\sigma : K\to\mathbb{R}$. On a ainsi

$$H_x(P_1+P_2)^n \geqslant \prod_{\sigma} \mathrm{Max}\Big(1,\sqrt{\sigma(b)}\Big),$$

D'après la condition (17), pour tout σ on a $\sigma(b)\geqslant 1$. On en déduit que

$$H_x(P_1+P_2)^n \geqslant \sqrt{\mathrm{N}_{K/\mathbb{Q}}(b)}.$$

d'où la première inégalité de (53). La démonstration de la deuxième inégalité de (53) est la même. Les conditions (51) et (52) impliquent alors

$$\log \mathrm{N}_{K/\mathbb{Q}}(b) \leqslant \frac{11n}{2}\log 2,$$

d'où

$$\mathrm{N}_{K/\mathbb{Q}}(b) \leqslant 2^{\frac{11n}{2}}.$$

La première inégalité de la condition 3 de l'énoncé du théorème conduit alors à une contradiction.

Cela termine la démonstration du théorème 2.

4. Remarque sur le théorème 2

Le théorème de Silverman affirme que pour toute classe d'élément b dans K^*/K^{*4}, sauf un nombre fini, si le rang de $E_b(K)$ est 1, alors $C_b(K)$ est vide. Si K est totalement réel et si O_K est principal, le théorème 2 entraîne aussi cette assertion. En effet, si O_K est principal tout élément de K^*/K^{*4} est représenté par un élément de O_K vérifiant la condition 1 du théorème 2 et il n'y a donc qu'un nombre fini de classes dans K^*/K^{*4} qui ne sont pas représentées par un élément vérifiant les conditions 1 et 3. L'objectif de ce paragraphe est de montrer qu'il n'en vas pas de même, en général, si O_K n'est pas principal.

Considérons un corps de nombres K, pas nécessairement totalement réel, d'anneau d'entiers O_K, dont le nombre de classes vaut 3. Soit S l'ensemble des éléments $x\in O_K$ tels

que pour tout idéal premier $\mathfrak{p}$ de O_K, on ait $v_{\mathfrak{p}}(x) < 4$. Soit H le sous-ensemble de K^*/K^{*4} formé des classes qui ne sont pas représentées par un élément de S.

Lemme 8. *L'ensemble H est infini.*

Démonstration : Il existe un idéal premier $\mathfrak{P}$ de O_K qui n'est pas principal. Soit a un générateur de $\mathfrak{P}^3$. Soit p un nombre premier non ramifié dans K. Démontrons que a^2pK^{*4} appartient à H. Supposons que ce ne soit pas le cas. Il existe alors $\lambda \in K^*$ tel que

$$\mu := a^2p\lambda^4 \in S.$$

Il existe deux éléments α et β de O_K tels que $\lambda = \alpha/\beta$. Par définition de S, μ appartient à O_K. On a l'égalité

$$\mu\beta^4 = a^2p\alpha^4. \tag{54}$$

Considérons alors les décompositions en produit d'idéaux premiers des idéaux engendrés respectivement par μ, p, α et β :

$$\mu O_K = \prod \mathfrak{M}_i{}^{m_i}, \quad pO_K = \prod \mathfrak{P}_j, \quad \alpha O_K = \prod \mathfrak{p}_k^{a_k} \quad \text{et} \quad \beta O_K = \prod \mathfrak{B}_\ell^{b_\ell},$$

les exposants intervenant dans ces égalités étant strictement positifs. On a l'égalité

$$\prod \mathfrak{M}_i{}^{m_i} \prod \mathfrak{B}_\ell^{4b_\ell} = \mathfrak{P}^6 \prod \mathfrak{P}_j \prod \mathfrak{p}_k^{4a_k}.$$

Il existe donc deux idéaux J_1 et J_2 de O_K tels que l'on ait

$$\prod \mathfrak{M}_i{}^{m_i} J_1^4 = \mathfrak{P}^2 \prod \mathfrak{P}_j J_2^4.$$

Pour tout idéal premier $\mathfrak{q}$ de O_K, on a

$$4\big(v_{\mathfrak{q}}(J_2) - v_{\mathfrak{q}}(J_1)\big) = v_{\mathfrak{q}}\Big(\prod \mathfrak{M}_i{}^{m_i}\Big) - v_{\mathfrak{q}}\Big(\mathfrak{P}^2 \prod \mathfrak{P}_j\Big).$$

Puisque μ est dans S, les entiers m_i sont compris entre 1 et 3. Il en résulte que l'on a $v_{\mathfrak{q}}(J_2) = v_{\mathfrak{q}}(J_1)$. On a donc $J_1 = J_2$, puis

$$\prod \mathfrak{M}_i{}^{m_i} = \mathfrak{P}^2 \prod \mathfrak{P}_j.$$

On obtient ainsi l'égalité

$$\mu O_K = \mathfrak{P}^2 \, pO_K,$$

ce qui entraîne que $\mathfrak{P}^2$ est principal et conduit à une contradiction. Par suite, a^2pK^{*4} est dans H.

Par ailleurs, si p et q sont deux nombres premiers distincts non ramifiés dans K, les classes de a^2p et a^2q modulo K^{*4} sont distinctes. En effet, dans le cas contraire, il existerait $x \in K^*$ tel que $p = qx^4$, d'où $pO_K = qO_K(xO_K)^4$, puis $pO_K = qO_K$, ce qui contredit le fait que p et q soient distincts. D'où le lemme.

5. Démonstration de la proposition 2

Rappelons que G. Shimura a démontré que la courbe elliptique $E_b/\mathbb{Q}$, qui est à multiplications complexes, est modulaire. Sa fonction L de Hasse-Weil se prolonge analytiquement à tout le plan complexe, et vérifie l'équation fonctionnelle

$$\Lambda(2-s) = \varepsilon\Lambda(s) \quad \text{avec} \quad \Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s) \quad \text{et} \quad \varepsilon = \pm 1,$$

où N est le conducteur de E_b ([Si2], p. 360). Le signe ε est un produit de signes locaux qui sont presque tous égaux à 1 :

$$\varepsilon = -\prod_{p \ premier} W_p(E_b). \tag{55}$$

La détermination complète des signes locaux, pour toute courbe elliptique sur $\mathbb{Q}$, se trouve dans [Ha1].

1) Démontrons que la conjecture de parité entraîne la conclusion de la proposition 2. En utilisant les résultats de *loc. cit.*, on démontre le résultat suivant :

Lemme 9. *Supposons que tous les diviseurs premiers impairs de b soient congrus à 1 modulo 8.*

1) Si $b \equiv 1$ mod. 16 on a $\varepsilon = 1$.

2) Si $b \equiv 2$ mod. 16 on a $\varepsilon = -1$.

Démonstration : Rappelons que l'équation (18) du paragraphe 3.2 de E_b est minimale et que les invariants standard c_4, c_6 et Δ associés à cette équation sont

$$c_4 = 2^4.3.b, \quad c_6 = 0 \quad \text{et} \quad \Delta = 2^6.b^3.$$

Pour tout nombre premier p, la courbe E_b a potentiellement bonne réduction en p.

Calculons $W_2(E_b)$. En le nombre premier 2, E_b a réduction de type additif. Supposons $b \equiv 1$ mod. 16. On a

$$v_2(c_4) = 4, \quad v_2(\Delta) = 6 \quad \text{et} \quad \frac{c_4}{2^4} \equiv 3 \text{ mod. } 16.$$

D'après le tableau 1 de [Ha1], on déduit alors que $W_2(E_b) = -1$. Supposons $b \equiv 2$ mod. 16. On a

$$v_2(c_4) = 5, \quad v_2(\Delta) = 9 \quad \text{et} \quad \frac{c_4}{2^5} \equiv 3 \text{ mod. } 8.$$

Il résulte de nouveau directement de *loc. cit.* que l'on a $W_2(E_b) = 1$ dans ce cas.

Puisque 3 ne divise pas b, la courbe E_b a bonne réduction en 3 et l'on a $W_3(E_b) = 1$.

Il reste à déterminer $W_p(E_b)$ si $p \geqslant 5$. Si p ne divise pas b, on a $W_p(E_b) = 1$. Supposons que p divise b. La courbe E_b a alors réduction de type additif en p, et b étant sans puissances quatrièmes, on a $v_p(\Delta) = 3, 6$ ou 9. Posons

$$e = \frac{12}{\mathrm{pgcd}(12, v_p(\Delta))}.$$

Si $v_p(\Delta) = 3$ ou 9, on a $e = 4$ auquel cas $W_p(E_b) = \left(\frac{-2}{p}\right)$. Si $v_p(\Delta) = 6$, on a $e = 2$ et $W_p(E_b) = \left(\frac{-1}{p}\right)$. Par hypothèse on a $p \equiv 1$ mod. 8, et dans les deux cas on obtient $W_p(E_b) = 1$. L'égalité (55) entraîne alors le lemme.

La conjecture de parité affirme que le rang de $E_b(\mathbb{Q})$ est pair si $\varepsilon = 1$ et est impair si $\varepsilon = -1$. Si l'une des deux conditions 1 et 2 de la proposition 2 est satisfaite, il résulte ainsi du lemme que b est divisible par un nombre premier qui n'est pas congru à 1 modulo 8. D'où la conclusion annoncée.

2) Supposons maintenant que les deux conditions suivantes soient satisfaites :

(i) la partie 2-primaire du groupe de Tate-Shafarevitch de $E_b/\mathbb{Q}$ est finie.

(ii) Tous les diviseurs premiers impairs de b sont congrus à 1 modulo 8.

On va alors démontrer que le rang de $E_b(\mathbb{Q})$ est pair si $b \equiv 1$ mod. 16 et qu'il est impair si $b \equiv 2$ mod. 16, ce qui prouvera le résultat.

On effectue pour cela une 2-descente, via une 2-isogénie, sur E_b. Le principe d'une telle 2-descente est exposé par exemple dans [Si2], p. 301-302. Notons E'_b la courbe elliptique d'équation

$$E'_b : \ Y^2 = X^3 + 4bX.$$

La courbe E_b est liée à E'_b via une isogénie $\phi : E_b \to E'_b$ sur $\mathbb{Q}$ de degré 2 (*loc. cit.*) Soient $p_1, \cdots, p_n$ les diviseurs premiers impairs de b et S l'ensemble des places de $\mathbb{Q}$ formé de la place archimédienne et de celles associées à 2 et aux nombres premiers p_i :

$$S = \Big\{\infty, 2, p_1, \cdots, p_n\Big\}.$$

Soit $\mathbb{Q}(S, 2)$ l'ensemble des $x \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ tels que $v(x) \equiv 0$ mod. 2 pour toute place v de $\mathbb{Q}$ en dehors de S. Un système de représentants de $\mathbb{Q}(S, 2)$ est l'ensemble

$$\Big\{ \pm a, \pm 2a\Big\},$$

où a parcourt les produits $\geqslant 1$ sans facteurs carrés des p_i, étant entendu que $a = 1$ pour le produit vide. On l'identifiera à $\mathbb{Q}(S, 2)$. Pour chaque $d \in \mathbb{Q}(S, 2)$, soit H_d l'espace homogène pour $E_b/\mathbb{Q}$:

$$H_d : \ dw^2 = (4b)z^4 + d^2.$$

Pour toute place v de $\mathbb{Q}$ notons $\mathbb{Q}_v$ le complété de $\mathbb{Q}$ en cette place. Rappelons que le groupe de Selmer $S^{\phi}(E_b/\mathbb{Q})$, de $E_b/\mathbb{Q}$ relatif à ϕ, est l'ensemble des éléments $d \in \mathbb{Q}(S,2)$ tels que $H_d(\mathbb{Q}_v)$ soit non vide pour toute place $v \in S$.
On dispose par ailleurs de l'isogénie duale $\widehat{\phi} : E'_b \to E_b$. Pour tout $d \in \mathbb{Q}(S,2)$, on note H'_d l'espace homogène pour $E'_b/\mathbb{Q}$:

$$H'_d : \ dW^2 = -bZ^4 + d^2.$$

C'est, à l'isomorphisme $Z \mapsto 2Z$ près, celui intervenant dans la prop. 4.9 de *loc. cit.*. Le groupe de Selmer $S^{\widehat{\phi}}(E'_b/\mathbb{Q})$, de $E'_b/\mathbb{Q}$ relatif à $\widehat{\phi}$, est l'ensemble des $d \in \mathbb{Q}(S,2)$ tels que $H'_d(\mathbb{Q}_v)$ soit non vide pour toute place $v \in S$. Les groupes $S^{\phi}(E_b/\mathbb{Q})$ et $S^{\widehat{\phi}}(E'_b/\mathbb{Q})$ sont des espaces vectoriels de dimensions finies sur $\mathbb{F}_2$.

On va démontrer le résultat suivant :

Proposition 7.

1) Si $b \equiv 1$ mod. 16, les dimensions de $S^{\phi}(E_b/\mathbb{Q})$ et $S^{\widehat{\phi}}(E'_b/\mathbb{Q})$ sont égales.

2) Si $b \equiv 2$ mod. 16, on a $\dim_{\mathbb{F}_2} S^{\widehat{\phi}}(E'_b/\mathbb{Q}) = \dim_{\mathbb{F}_2} S^{\phi}(E_b/\mathbb{Q}) + 1$.

5.1. Lemmes préliminaires

On démontre dans ce paragraphe des résultats locaux concernant H_d et H'_d que l'on utilisera pour obtenir la proposition.

Lemme 10. *Soient p_i un nombre premier impair de S et d un élément de $\mathbb{Q}(S,2)$. Les espaces homogènes H_d et H'_d sont isomorphes sur $\mathbb{Q}_{p_i}$.*

Démonstration : Par hypothèse, on a $p_i \equiv 1$ mod. 8. Par suite, 2 est un carré dans $\mathbb{F}_{p_i}$ et -1 est une puissance quatrième dans $\mathbb{F}_{p_i}$. D'après le lemme de Hensel, 2 est donc un carré dans $\mathbb{Q}_{p_i}$ et -1 est une puissance quatrième dans $\mathbb{Q}_{p_i}$. Cela entraîne le résultat.

Lemme 11. *Soit d un élément de $\mathbb{Q}(S,2)$.*

1) Si $d > 0$, alors $H_d(\mathbb{R})$ et $H'_d(\mathbb{R})$ sont non vides.

2) Si $d < 0$, alors $H_d(\mathbb{R})$ est vide et $H'_d(\mathbb{R})$ n'est pas vide.

Sa vérification est immédiate.

Lemme 12. *Soient d un élément de $\mathbb{Q}(S,2)$ et a un produit sans facteurs carrés de nombres premiers p_i : on a $a \geqslant 1$ et $a = 1$ si ce produit est vide.*

1) Si $d = a$ ou bien $d = 2a$, alors $H_d(\mathbb{Q}_2)$ n'est pas vide.

2) Si $d = -a$ ou bien $d = -2a$, alors $H_d(\mathbb{Q}_2)$ est vide.

Démonstration : 1) Si $d = a$, on a $d \equiv 1$ mod. 8 et d est un carré dans $\mathbb{Q}_2$. En posant $d = t^2$ où $t \in \mathbb{Q}_2$, on constate que le point $(z,w) = (0,t)$ appartient à $H_d(\mathbb{Q}_2)$.

Supposons $d = 2a$. On a $d \equiv 2$ mod. 16.

1.1) Supposons $b \equiv 1$ mod. 16. On a alors

$$bd \equiv d \equiv 2, 18 \text{ mod. } 32.$$

Par ailleurs, on a $a^2 \equiv 1$ mod. 16, d'où $2a^2 \equiv 2$ mod. 32 et $2a^3 \equiv d$ mod. 32. On en déduit la congruence

$$bd + 2a^3 \equiv 4 \text{ mod. } 32.$$

Il existe donc $t \in \mathbb{Q}_2$ tel que l'on ait $bd + 2a^3 = 4t^2$. On a donc l'égalité

$$4b + d^2 = d\left(\frac{4t}{d}\right)^2,$$

ce qui montre que le point $(z, w) = (1, 4t/d)$ appartient à $H_d(\mathbb{Q}_2)$, qui est donc non vide.

1.2) Supposons $b \equiv 2$ mod. 16. Dans ce cas, $b/2$ et $d/2$ sont des unités de $\mathbb{Z}_2$ congrues à 1 modulo 8, en particulier b/d est une unité qui est un carré dans $\mathbb{Z}_2$. Il existe donc $t \in \mathbb{Z}_2$ tel que

$$t^2 = \frac{b}{d} + 8\left(\frac{d}{2}\right),$$

Ce qui entraîne que $(z, w) = (1/2, t/2)$ appartient à $H_d(\mathbb{Q}_2)$. D'où l'assertion 1.

2) Supposons $d = -a$ et l'existence d'un point $(z, w) \in H_d(\mathbb{Q}_2)$. On a l'égalité

$$(dw)^2 = (4bd)z^4 + d^3.$$

Notons ici v la valuation 2-adique de $\mathbb{Q}_2$. On a $v(z) < 0$; en effet, si $v(x) \geqslant 0$, on obtient $(dw)^2 \equiv d^3$ mod. 4, d'où $(dw)^2 \equiv d \equiv -1$ mod. 4, ce qui conduit à une contradiction. Posons $z' = 1/z$. On a $v(z') > 0$ et l'égalité

$$(z'^2 dw)^2 = 4bd + d^3 z'^4,$$

d'où $(z'^2 dw)^2 \equiv 4bd$ mod. 16. On en déduit que $(z'^2 dw)^2 \equiv -4b$ mod. 16. Par suite, on a

$$\left(\frac{z'^2 dw}{2}\right)^2 \equiv -1 \text{ ou } 2 \text{ mod. } 4,$$

ce qui n'est pas. D'où le fait que $H_d(\mathbb{Q}_2)$ soit vide.

Supposons $d = -2a$. Soit (z, w) un point de $H_d(\mathbb{Q}_2)$.

2.1) Supposons $b \equiv 1$ mod. 16. On déduit de l'égalité $dw^2 = 4bz^4 + d^2$ que $v(z) = 0$, d'où $z^4 \equiv 1$ mod. 16. Il en résulte que

$$bz^4 \equiv 1 \text{ mod. } 16.$$

On a donc $dw^2 \equiv 8 \bmod. 32$, d'où

$$w^2 \equiv -\frac{4}{a} \equiv -4 \bmod. 16,$$

et une contradiction.

2.2) Supposons $b \equiv 2 \bmod. 16$. L'égalité $dw^2 = 4bz^4 + d^2$ entraîne $v(z) < 0$. Par ailleurs, on a

$$\frac{w^2}{z^4} = \frac{4b}{d} + \frac{d}{z^4},$$

d'où il résulte que l'on a

$$\frac{w^2}{z^4} \equiv \frac{4b}{d} \bmod. 16, \quad \text{puis} \quad \frac{w^2}{z^4} \equiv -\frac{4}{a} \equiv -4 \bmod. 16.$$

On obtient ainsi une contradiction et le lemme.

Lemme 13. *Soient d un élément de $\mathbb{Q}(S,2)$ et a un produit sans facteurs carrés de nombres premiers p_i.*

1) Si $d = a$ ou bien $d = -a$, alors $H'_d(\mathbb{Q}_2)$ n'est pas vide.

2) Si $d = 2a$ ou bien $d = -2a$, alors $H'_d(\mathbb{Q}_2)$ est vide si $b \equiv 1 \bmod. 16$, et est non vide si $b \equiv 2 \bmod. 16$.

Démonstration : 1) Si $d = a$, on a $d \equiv 1 \bmod. 8$, il existe $t \in \mathbb{Q}_2$ tel que $d = t^2$, et le point $(Z, W) = (0, t)$ appartient à $H'_d(\mathbb{Q}_2)$.

Supposons $d = -a$. On a $d \equiv -1 \bmod. 8$.

1.1) Supposons $b \equiv 1 \bmod. 16$. On a $-bd \equiv 1 \bmod. 8$, et il existe donc $t \in \mathbb{Q}_2$ tel que l'on ait $-bd + 16d^3 = t^2$. On obtient

$$-\frac{b}{16} + d^2 = d\left(\frac{t}{4d}\right)^2,$$

et le point $(Z, W) = (1/2, t/4d)$ appartient à $H'_d(\mathbb{Q}_2)$.

1.2) Si $b \equiv 2 \bmod. 16$, on a

$$\frac{-b + d^2}{d} \equiv 1 \bmod. 8,$$

de sorte qu'il existe $u \in \mathbb{Q}_2$ tel que l'on ait

$$du^2 = -b + d^2,$$

et le point $(Z, W) = (1, u)$ appartient à $H'_d(\mathbb{Q}_2)$, d'où l'assertion 1.

2) Supposons $d = 2a$.

2.1) Supposons $b \equiv 1$ mod. 16. Soit (Z, W) un point de $H'_d(\mathbb{Q}_2)$. En considérant la valuation 2-adique des deux membres de l'égalité $dW^2 = -bZ^4 + d^2$, on obtient directement une contradiction.

2.2) Supposons $b \equiv 2$ mod. 16. On a $b/d \equiv 1$ mod. 8 et

$$-\frac{b}{d} + d \equiv -1 + 2 = 1 \text{ mod. } 8.$$

Par suite, on a $du^2 = -b + d^2$ où $u \in \mathbb{Q}_2$, et le point $(Z, W) = (1, u)$ appartient à $H'_d(\mathbb{Q}_2)$, ce qui prouve l'assertion 2 si $d = 2a$.

Supposons $d = -2a$.

2.3) Si $b \equiv 1$ mod. 16, le même argument que celui utilisé dans l'alinéa 2.1 entraîne que $H'_d(\mathbb{Q}_2)$ est vide.

2.4) Supposons $b \equiv 2$ mod. 16. Puisque l'on a $d \equiv -2$ mod. 16, on déduit que

$$-\frac{b}{d} \equiv 1 \text{ mod. } 8.$$

Il existe donc $u \in \mathbb{Q}_2$ tel que l'on ait

$$u^2 = -\frac{b}{d} + 16d.$$

Il en résulte que le point $(Z, W) = (1/2, u/4)$ appartient à $H'_d(\mathbb{Q}_2)$, d'où le lemme.

5.2. Démonstration de la proposition 7

On a l'énoncé suivant :

Lemme 14. *Soit a un produit sans facteurs carrés de nombres premiers p_i.*

1) On a les équivalences

$$a \in S^{\phi}(E_b/\mathbb{Q}) \Longleftrightarrow a \in S^{\widehat{\phi}}(E'_b/\mathbb{Q}), \tag{56}$$

$$2a \in S^{\phi}(E_b/\mathbb{Q}) \Longleftrightarrow -a \in S^{\widehat{\phi}}(E'_b/\mathbb{Q}). \tag{57}$$

2) Supposons $b \equiv 2$ mod. 16. On a les équivalences

$$2a \in S^{\widehat{\phi}}(E'_b/\mathbb{Q}) \Longleftrightarrow -a \in S^{\widehat{\phi}}(E'_b/\mathbb{Q}), \tag{58}$$

$$-2a \in S^{\widehat{\phi}}(E'_b/\mathbb{Q}) \Longleftrightarrow a \in S^{\widehat{\phi}}(E'_b/\mathbb{Q}). \tag{59}$$

Démonstration : 1) D'après les lemmes 11 à 13, les ensembles $H_a(\mathbb{R})$, $H'_a(\mathbb{R})$, $H_a(\mathbb{Q}_2)$ et $H'_a(\mathbb{Q}_2)$ ne sont pas vides. Par ailleurs, pour tout nombre premier p_i, les courbes H_a et H'_a sont isomorphes sur $\mathbb{Q}_{p_i}$, de sorte que $H_a(\mathbb{Q}_{p_i})$ n'est pas vide si et seulement si tel est le cas de $H'_a(\mathbb{Q}_{p_i})$ (lemme 10). Cela entraîne l'équivalence (56).

Démontrons l'équivalence (57). Rappelons que les équations de H_{2a} et H_{-a} sont

$$H_{2a}:\ 2aw^2 = (4b)z^4 + 4a^2 \quad \text{et} \quad H_{-a}:\ -aw^2 = (4b)z^4 + a^2.$$

Soit p_i un diviseur premier impair de b. Puisque 2 est un carré dans $\mathbb{Q}_{p_i}$ et que -1 est une puissance quatrième dans $\mathbb{Q}_{p_i}$, les courbes H_{2a} et H_{-a} sont isomorphes sur $\mathbb{Q}_{p_i}$. Il en résulte que l'on a l'équivalence

$$H_{2a}(\mathbb{Q}_{p_i}) \neq \emptyset \Longleftrightarrow H'_{-a}(\mathbb{Q}_{p_i}) \neq \emptyset.$$

En effet, si $H_{2a}(\mathbb{Q}_{p_i})$ est non vide, il en est de même de $H_{-a}(\mathbb{Q}_{p_i})$, et d'après le lemme 10, $H'_{-a}(\mathbb{Q}_{p_i})$ n'est pas vide. Inversement, si $H'_{-a}(\mathbb{Q}_{p_i})$ n'est pas vide, tel est aussi le cas de $H_{-a}(\mathbb{Q}_{p_i})$ puis de $H_{2a}(\mathbb{Q}_{p_i})$, d'où l'assertion. Par ailleurs, les ensembles $H_{2a}(\mathbb{R})$, $H_{2a}(\mathbb{Q}_2)$, $H'_{-a}(\mathbb{R})$ et $H'_{-a}(\mathbb{Q}_2)$ ne sont pas vides. D'où le résultat.

2) Les ensembles $H'_{2a}(\mathbb{R})$ et $H'_{2a}(\mathbb{Q}_2)$ ne sont pas vides (lemmes 10 et 13). Par suite, $2a$ appartient à $S^{\widehat{\phi}}(E'_b/\mathbb{Q})$ si et seulement si $H_{2a}(\mathbb{Q}_{p_i})$ n'est pas vide pour tout p_i. Les courbes H_{2a} et H_{-a} étant isomorphes sur $\mathbb{Q}_{p_i}$, on déduit alors du lemme 10 que pour tout p_i, $H_{2a}(\mathbb{Q}_{p_i})$ n'est pas vide si et seulement si tel est le cas de $H'_{-a}(\mathbb{Q}_{p_i})$. Puisque $H'_{-a}(\mathbb{R})$ et $H'_{-a}(\mathbb{Q}_2)$ ne sont pas vides, cela prouve l'équivalence (58).

Démontrons l'équivalence (59). Les ensembles $H'_{-2a}(\mathbb{R})$ et $H'_{-2a}(\mathbb{Q}_2)$ ne sont pas vides. Par ailleurs, comme ci-dessus, les courbes H_{-2a} et H_a sont isomorphes sur $\mathbb{Q}_{p_i}$. Il en résulte que pour tout p_i, $H_{-2a}(\mathbb{Q}_{p_i})$ est non vide si et seulement si tel est le cas de $H'_a(\mathbb{Q}_{p_i})$. On en déduit l'équivalence annoncée compte tenu du fait que $H'_a(\mathbb{R})$ et $H'_a(\mathbb{Q}_2)$ ne sont pas vides. D'où le lemme.

Terminons la démonstration de la proposition. Soit a un produit (éventuellement vide) sans facteurs carrés de nombres premiers p_i.

1) Supposons $b \equiv 1$ mod. 16. Soit d un élément de $\mathbb{Q}(S, 2)$. Si l'on a $d < 0$, l'ensemble $H_d(\mathbb{R})$ est vide. Par suite, on a l'implication

$$d \in S^{\phi}(E_b/\mathbb{Q}) \Longrightarrow d = a \quad \text{ou} \quad d = 2a.$$

Par ailleurs, Si $d = 2a$ ou bien $d = -2a$, $H'_d(\mathbb{Q}_2)$ est vide (lemme 13). On en déduit que

$$d \in S^{\widehat{\phi}}(E'_b/\mathbb{Q}) \Longrightarrow d = a \quad \text{ou} \quad d = -a.$$

Les équivalences (56) et (57) du lemme 14 entraînent alors l'assertion 1 de la proposition.

2) Supposons $b \equiv 2$ mod. 16. Les éléments $-a$ et $-2a$ ne sont pas dans $S^{\phi}(E_b/\mathbb{Q})$. D'après le lemme 14, si $a \in S^{\phi}(E_b/\mathbb{Q})$, les éléments a et $-2a$ sont dans $S^{\widehat{\phi}}(E'_b/\mathbb{Q})$. Si $2a \in S^{\phi}(E_b/\mathbb{Q})$, alors $-a$ et $2a$ sont dans $S^{\widehat{\phi}}(E'_b/\mathbb{Q})$. On en déduit que l'ordre de $S^{\widehat{\phi}}(E'_b/\mathbb{Q})$ est égal à deux fois celui de $S^{\phi}(E_b/\mathbb{Q})$. Cela démontre l'assertion 2 de la proposition.

5.3. Fin de la démonstration de la proposition 2

On utilise les résultats de Cassels qui se trouvent dans [Cas]. Avec les notations du théorème 1.1 de cet article, on a

$$T(E_b/E'_b) = \frac{\left|S^{\phi}(E_b/\mathbb{Q})\right|}{\left|S^{\widehat{\phi}}(E'_b/\mathbb{Q})\right|}.$$

Par hypothèse, la 2-partie du groupe de Tate-Shafarevitch de $E_b/\mathbb{Q}$ est finie. Soit r le rang de $E_b(\mathbb{Q})$. D'après le théorème 1.5 de *loc. cit.*, le nombre rationnel

$$2^r T(E_b/E'_b) \quad \text{est un carré.}$$

Si l'on a $b \equiv 1$ mod. 16, d'après la proposition 7 on a $T(E_b/E'_b) = 1$, ce qui entraîne que r est pair. Si l'on a $b \equiv 2$ mod. 16, on a $T(E_b/E'_b) = 1/2$, et dans ce cas r est impair. Cela termine la démonstration de la proposition.

Appendice 1 - Exemple d'effectivité du théorème des zéros de Hilbert

On est confronté dans la démonstration de la proposition 3 au problème de l'effectivité du théorème des zéros de Hilbert dans un cas particulier. Considérons trois indéterminées X, Y et Z. Soit I l'idéal homogène de l'anneau $\mathbb{C}[X,Y,Z]$ engendré par les polynômes F, G et H suivants :

$$F = X^4 + Y^4 - Z^4, \quad G = (X^2 + XY + Y^2)^2 \quad \text{et} \quad H = (X+Y)^2 Z^2.$$

Soit $V_p(I)$ l'ensemble algébrique projectif de $\mathbb{P}^2$ associé à I. Vérifions que $V_p(I)$ est vide. Supposons qu'il existe un point $[x,y,z] \in V_p(I)$. On a $(x+y)z = 0$. Si $z = 0$, alors $xy \neq 0$ et il existe $\alpha \in \mathbb{C}$ tel que $x = \alpha y$ avec $\alpha^4 = -1$. L'égalité $x^2 + xy + y^2 = 0$ conduit alors à $1 + \alpha + \alpha^2 = 0$, d'où $\alpha^3 = 1$ et une contradiction. Si $x + y = 0$, l'égalité $x^2 + xy + y^2 = 0$ entraîne $x = y = 0$, d'où de nouveau une contradiction et notre assertion. D'après le théorème des zéros, il existe donc un entier $n \geqslant 1$ tel que les monômes X^n, Y^n et Z^n appartiennent à I. Il s'agit ici d'effectiviser cette condition. On a l'énoncé suivant :

Proposition. *L'entier $n = 12$ convient. Posons*

$$P = 3X^8 + 4Y^2X^6 + 4Y^4X^4 + 2Y^6X^2 + Y^8,$$

$$Q = -2X^8 + 4YX^7 - 6Y^2X^6 + 4Y^3X^5 + (10Z^4 - 3Y^4)X^4 + 2Y^5X^3$$
$$-3Y^6X^2 + 2Y^7X - Y^8 + 4Z^4Y^4,$$

$$R = -7Z^2X^6 - 6Z^2YX^5 - 7Z^2Y^2X^4 - 3Z^2Y^4X^2 - 2Z^2Y^5X - 3Z^2Y^6.$$

On a les égalités

$$Z^6 = -Z^2F + 2Z^2G - (X+Y)^2H, \tag{1}$$

$$X^{12} = PF + QG + RH \quad \textit{et} \quad Y^{12} = \widetilde{P}F + \widetilde{Q}G + \widetilde{R}H, \tag{2}$$

où $\widetilde{P}(X,Y,Z) = P(Y,X,Z)$, $\widetilde{Q}(X,Y,Z) = Q(Y,X,Z)$ et $\widetilde{H}(X,Y,Z) = H(Y,X,Z)$.

Démonstration : Il est immédiat de vérifier les égalités annoncées à l'aide d'un ordinateur. On est en fait parvenu à ce résultat en partant de l'égalité

$$Z^4 + (X+Y)^4 = 2G - F. \tag{3}$$

L'égalité (1) en résulte. Par ailleurs, on déduit de (3) les deux égalités

$$G = Z^4 + F + 2XY(X+Y)^2 - (XY)^2,$$

$$(XY)^2(X+Y)^4 = -(XY)^2F + (2X^2Y^2 - Z^4)G + Z^2(X^2+Y^2)H.$$

Elles entraînent que $(XY)^4$ appartient à I, puis que

$$(XY)^4 = SF + TG + UH,$$

$$\text{avec} \quad S = -(X^2+Y^2)^2, \quad T = X^4 - 2YX^3 + 3Y^2X^2 - 2Y^3X + Y^4 - 4Z^4,$$
$$U = 3(XZ)^2 + 2XYZ^2 + 3(YZ)^2.$$

En considérant alors l'égalité

$$X^8 + Y^8 = Z^8 + F^2 + 2Z^4F - 2(XY)^4,$$

et en multipliant ses deux membres par X^4 (resp. Y^4) on obtient la première (resp. la deuxième) égalité de (2).

Appendice 2 - Torsion galoisienne

L'objectif de cet appendice est de rappeler un résultat dû à Silverman concernant les tordues galoisiennes de courbes que l'on utilise dans la démonstration du théorème 1 (cf. [Si1]). Les courbes intervenant ci-dessous sont implicitement supposées projectives et lisses et plongées dans un même espace projectif $\mathbb{P}^n$. Tous les corps considérés sont par ailleurs contenus dans $\overline{\mathbb{Q}}$.

Considérons un corps de nombres K et une courbe $\mathscr{C}$ définie sur K. Soit $\mathscr{C}'$ une courbe définie sur K isomorphe à $\mathscr{C}$ sur une extension finie L de K. On suppose que L est *minimale* au sens où si M est un sous-corps strict de L, les courbes $\mathscr{C}$ et $\mathscr{C}'$ ne sont pas isomorphes sur M. Notons :

. G_K le groupe de Galois de $\overline{\mathbb{Q}}$ sur K.

. d le degré de L sur K.

. δ_K le nombre de places archimédiennes de K.

. $D_{L/K}$ le discriminant relatif de l'extension L/K.

. $h : \mathbb{P}^n\big(\overline{\mathbb{Q}}\big) \to \mathbb{R}$ la hauteur absolue logarithmique ([Si2], p. 215) ; elle est définie par une formule analogue à celle si $n = 2$ (paragraphe 2.2).

Soit $f : \mathscr{C}' \to \mathscr{C}$ un isomorphisme défini sur L de $\mathscr{C}'$ sur $\mathscr{C}$. Pour tout $\sigma \in G_K$, on pose

$$\xi(\sigma) = {}^{\sigma}f \circ f^{-1} \in \mathrm{Aut}(\mathscr{C}).$$

Théorème. *Soit Q un point de $f\big(\mathscr{C}'(K)\big)$. On est dans l'un des cas suivants :*

1. *il existe $\sigma \in G_K$ tel que $\xi(\sigma)$ ne soit pas l'identité de $\mathscr{C}$ et que $Q = \xi(\sigma)(Q)$.*
2. *On a l'inégalité*

$$\log \mathrm{N}_{K/\mathbb{Q}}\, D_{L/K} \leqslant \Big(2(d-1)h(Q) + \delta_K \log d\Big)d. \tag{1}$$

Démonstration : On prouve d'abord le lemme suivant :

Lemme. *L'ensemble $f\big(\mathscr{C}'(K)\big)$ est formé des points $A \in \mathscr{C}(L)$ tels que, pour tout σ dans G_K, on ait ${}^{\sigma}A = \xi(\sigma)(A)$.*

Démonstration : Pour tout point $P \in \mathscr{C}'\big(\overline{\mathbb{Q}}\big)$ et tout $\sigma \in G_K$, on a

$${}^{\sigma}\big(f(P)\big) = \xi(\sigma)\big(f({}^{\sigma}P)\big). \tag{2}$$

Cela entraîne que $f\big(\mathscr{C}'(K)\big)$ satisfait la condition du lemme. Inversement, soit $A \in \mathscr{C}(L)$ tel que, pour tout σ dans G_K, on ait ${}^{\sigma}A = \xi(\sigma)(A)$. Posons $P = f^{-1}(A)$. D'après (2), on a les égalités

$$\xi(\sigma)\big(f({}^{\sigma}P)\big) = {}^{\sigma}A = \xi(\sigma)(A) = \xi(\sigma)\big(f(P)\big).$$

On en déduit que $f({}^{\sigma}P) = f(P)$, puis que $P = {}^{\sigma}P$. Il en résulte que P appartient à $\mathscr{C}'(K)$ autrement dit que A est dans $f\big(\mathscr{C}'(K)\big)$. D'où le lemme.

Le théorème se déduit comme suit. Soit $K(Q)$ le sous-corps de $\overline{\mathbb{Q}}$ engendré par K et les coordonnées de Q dans $\mathbb{P}^n\big(\overline{\mathbb{Q}}\big)$. On a l'inclusion

$$K(Q) \subseteq L. \tag{3}$$

Supposons que la condition 1 du théorème ne soit pas réalisée. Soit σ un élément de $\mathrm{Gal}\big(\overline{\mathbb{Q}}/K(Q)\big)$. On a ${}^{\sigma}Q = Q$ et on déduit du lemme l'égalité

$$Q = \xi(\sigma)(Q).$$

D'après l'hypothèse faite, $\xi(\sigma)$ est donc l'automorphisme identité de $\mathscr{C}$, autrement dit f est définie sur $K(Q)$. Les courbes $\mathscr{C}$ et $\mathscr{C}'$ sont donc isomorphes sur $K(Q)$. D'après l'inclusion (3) et le caractère minimal de L, on a donc $L = K(Q)$. Le théorème 2 de [Si1] entraîne alors directement l'inégalité (1). D'où le résultat.

Appendice 3 - Sur les entiers totalement positifs d'un corps totalement réel

Soit K un corps de nombres totalement réel de degré n sur $\mathbb{Q}$, d'anneau d'entiers O_K. Soient $\sigma_1, \cdots, \sigma_n$ les n plongements de K dans $\mathbb{R}$. Pour tout $x \in O_K$ on note $\mathrm{N}_{K/\mathbb{Q}}(x)$ sa norme de K sur $\mathbb{Q}$ et $H(x)$ la hauteur de x relative à K. On a

$$H(x) = \prod_{i=1}^{n} \mathrm{Max}\big(1, |\sigma_i(x)|\big). \tag{1}$$

On utilise dans la démonstration du théorème 2 le résultat suivant concernant les entiers totalement positifs de K. Cet énoncé a été démontré par E. Halberstadt ([Ha2]).

Proposition. *Soit $(u_1, \cdots, u_{n-1})$ un système d'unités fondamentales de O_K. Soit b un élément de O_K tel que l'on ait $\sigma_j(b) > 0$ pour tout $j = 1, \cdots, n$. Supposons que b vérifie la condition suivante :*

$$\mathrm{N}_{K/\mathbb{Q}}(b) \geqslant \left(\prod_{k=1}^{n-1} H(u_k) \right)^4. \tag{2}$$

Alors, il existe une unité u de O_K telle que l'on ait

$$\sigma_j(bu^4) \geqslant 1 \quad \textit{pour} \quad j = 1, \cdots, n.$$

Démonstration : Soit $L : K^* \to \mathbb{R}^n$ le plongement logarithmique de K^* i.e. l'homomorphisme de groupes défini pour tout $x \in K^*$ par

$$L(x) = \Big(\log\big(|\sigma_1(x)|\big), \cdots, \log\big(|\sigma_n(x)|\big) \Big).$$

L'image par L du groupe des unités de O_K est un réseau Λ de l'hyperplan V de $\mathbb{R}^n$ d'équation $x_1 + \cdots + x_n = 0$. Posons

$$e_k = L(u_k) \quad \text{pour} \quad k = 1, \cdots, n-1.$$

Le système $(e_1, \cdots, e_{n-1})$ est une base de Λ sur $\mathbb{Z}$ donc une base de V sur $\mathbb{R}$. Posons par ailleurs

$$\beta = L(b), \quad \beta = (\beta_1, \cdots, \beta_n) \quad \text{et} \quad S = \beta_1 + \cdots + \beta_n.$$

Puisque b est totalement positif, on a donc

$$\beta_j = \log\big(\sigma_j(b)\big) \quad \text{pour} \quad j = 1, \cdots, n. \tag{3}$$

Munissons $\mathbb{R}^n$ de la norme définie pour tout $(x_1, \cdots, x_n) \in \mathbb{R}^n$ par

$$||(x_1, \cdots, x_n)|| = \sum_{h=1}^{n} |x_h|.$$

Vérifions que l'on a

$$S \geqslant 2 \sum_{k=1}^{n-1} ||e_k||. \tag{4}$$

Considérons pour cela une unité a de O_K. Posons

$$P = \prod_i |\sigma_i(a)| \quad \text{et} \quad P' = \prod_j |\sigma_j(a)|,$$

où i parcourt l'ensemble des indices pour lesquels $|\sigma_i(a)| \geqslant 1$ et j parcourt l'ensemble des indices pour lesquels $|\sigma_j(a)| < 1$. On a $PP' = 1$. Il en résulte que

$$\sum_{h=1}^{n} \Big| \log\big(|\sigma_h(a)|\big) \Big| = \sum_i \log\big(|\sigma_h(a)|\big) - \sum_j \log\big(|\sigma_h(a)|\big) = \log(P) - \log(P') = 2\log(P).$$

Par ailleurs, d'après la formule (1), on a $H(a) = P$. D'après le calcul précédent, on a donc

$$||L(a)|| = 2\log\big(H(a)\big).$$

L'inégalité (2) se traduit alors, en prenant les logarithmes, par la condition (4).

Soit M la maille du réseau Λ formée des combinaisons linéaires

$$\sum_{k=1}^{n-1} x_k e_k,$$

où les coefficients x_k décrivent l'intervalle $[-1/2, 1/2]$. Pour tout $i = 1, \cdots, n$, soit $(e_k)_i$ la i-ème coordonnée de e_k dans la base canonique de $\mathbb{R}^n$. Pour tout $z = (z_1, \cdots, z_n) \in M$, on a les inégalités

$$2|z_i| \leqslant \sum_{k=1}^{n-1} \big|(e_k)_i\big| := \ell_i. \tag{5}$$

Pour tout $i = 1, \cdots, n$, le réseau Λ n'étant pas contenu dans l'hyperplan de $\mathbb{R}^n$ d'équation $x_i = 0$, on a $\ell_i > 0$. Posons alors

$$w_i = \frac{\ell_i}{\ell_1 + \cdots + \ell_n} \quad \text{et} \quad w = (w_1, \cdots, w_n) \in \mathbb{R}^n.$$

Considérons le vecteur

$$y = \frac{1}{4}(Sw - \beta).$$

Par définition, y appartient à V. Il existe donc un élément $\lambda = (\lambda_1, \cdots, \lambda_n) \in \Lambda$ tel que $y - \lambda$ soit dans M. On déduit alors de (5) que l'on a

$$\beta_i + 4\lambda_i \geqslant Sw_i - 2\ell_i \quad \text{pour} \quad i = 1, \cdots, n. \tag{6}$$

Il existe des entiers $t_k \in \mathbb{Z}$ tels que l'on ait

$$\lambda = \sum_{k=1}^{n-1} t_k e_k.$$

Posons

$$u = \prod_{k=1}^{n-1} u_k^{t_k}.$$

Vérifions que l'unité u de O_K satisfait la conclusion de la proposition. On a $L(u) = \lambda$, d'où $\lambda_i = \log\big(|\sigma_i(u)|\big)$. Compte tenu de (3), les inégalités (6) s'écrivent donc

$$\log\big(\sigma_i(b)\big) + 4\log\big(|\sigma_i(u)|\big) \geqslant Sw_i - 2\ell_i,$$

autrement dit,

$$\sigma_i(bu^4) \geqslant \exp\big(Sw_i - 2\ell_i\big) \quad \text{pour} \quad i = 1, \cdots, n. \tag{7}$$

Par ailleurs, on a

$$\ell_1 + \cdots + \ell_n = \sum_{k=1}^{n-1} \sum_{i=1}^{n} |(e_k)_i| = \sum_{k=1}^{n-1} ||e_k||.$$

Il résulte alors de la condition (4) que l'on a

$$S \geqslant 2\,\mathrm{Max}\Big(\frac{\ell_1}{w_1}, \cdots, \frac{\ell_n}{w_n}\Big).$$

D'après (7) on obtient ainsi que $\sigma_i(bu^4) \geqslant 1$ pour tout $i = 1, \cdots, n$. D'où la proposition.

Bibliographie

[Br] A. Bremner, Some quartic curves with no points in any cubic fields, *Proc. London Math. Soc.* **52** (1986), 193-214.

[Br-Mo] A. Bremner et P. Morton, A new characterization of the integer 5906, *Manuscripta Math.* **44** (1983), 187-229.

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

[Cal] É. Cali, Défaut de semi-stabilité des courbes elliptiques dans le cas non ramifié, *Canad. J. Math.* **56** (2004), 673-698.

[Cas] J. W. S. Cassels, Arithmetic on curves of genus 1 (VIII). On conjectures of Birch and Swinnerton-Dyer, *J. reine angew. Math.* **217** (1965), 180-199.

[Co-Wi] J. Coates et A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (1977), 223-251.

[Co] D. Cox, Primes of the form $x^2 + ny^2$, Fermat, Class Field Theory, and Complex Multiplication, Wiley-Interscience, 1989.

[Cr] J. E. Cremona, Algorithms for modular elliptic curves, Second edition, Cambridge University Press (1997).

[De] V. A. Dem'janenko, The Indeterminate Equations $x^6 + y^6 = az^2$, $x^6 + y^6 = az^3$, $x^4 + y^4 = az^4$, *Amer. Math. Soc. Transl.* **119** (1983), 27-34.

[Gr-Ri] G. Grigorov et J. Rizov, Heights on elliptic curves and the diophantine equation $x^4 + y^4 = cz^4$, Sophia University, preprint (1998).

[Ha1] E. Halberstadt, Signes locaux des courbes elliptiques en 2 et 3, *C. R. Acad. Sci.* **326** (1998), 1047-1052.

[Ha2] E. Halberstadt, manuscript (2004).

[Ku-Ko] A. Kuribayashi et K. Komiya, On Weierstrass points and automorphisms of curves of genus three, dans Algebraic Geometry, Lecture Notes in Math. **732** (1978), 253-299.

[Kr1] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique, *Acta Arith.* **54** (1989), 75-80.

[Kr2] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, *Manuscripta Math.* **69** (1990), 353-385.

[Kr3] A. Kraus, Détermination du poids et du conducteur associés aux représentations des points de p-torsion des courbes elliptiques, *Dissertationes Math.* **364** (1997).

[Kr4] A. Kraus, Sur la p-différente du corps des points de p-torsion des courbes elliptiques, *Bull. Austral. Math. Soc.* **60** (1999), 407-428.

[Og] Elliptic curves and wild ramification, *Amer. J. of Math.* **89** (1967), 1-21.

[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).

[Sa] T. Saito, Conductor, discriminant, and the Noether formula of arithmetic surfaces, *Duke Math. J.* **57** (1988), 151-173.

[Sel] E. S. Selmer, On the irreducibility of certain trinomials, *Math. Scand.* **4** (1956), 287-302.

[Se-Ta] J.-P. Serre et J. Tate, Good reduction of abelian varieties, *Ann. of Math.* **88** (1968), 492-517.

[Se1] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259-331.

[Se2] J.-P. Serre, Corps Locaux, troisième édition, Hermann, Paris, 1980.

[Se3] J.-P. Serre, Abelian ℓ-Adic Representations and Elliptic Curves, Advanced book classics, Addison-Wesley Publishing Company, 1989, édité en 1968 par W. A. Benjamin.

[Se4] J.-P. Serre, Lectures on the Mordell-Weil Theorem, Aspects of Mathematics, Vieweg, deuxième édition, 1990.

[Si1] J. H. Silverman, Lower bounds for height functions, *Duke Math. J.* **51** (1984), 395-403.

[Si2] J. H. Silverman, The Arithmetic of Elliptic Curves, GTM **106** Springer, 1986.

[Si3] J. H. Silverman, Rational points on certain families of curves of genus at least 2, *Proc. London Math. Soc.* **55** (1987), 465-481.

[Si4] J. H. Silverman, The difference between the Weil height and the canonical height on elliptic curves *Math. Comp.* **192** (1990), 723-743.

[Si-Ta] J. H. Silverman et J. Tate, Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[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/

[Ta] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, dans Modular Functions of One Variable IV, Lecture Notes in Math. **476** (1975), 33-52.

[We] A. Weil, Courbes algébriques et variétés abéliennes, Paris Hermann 1971.