Défaut de semi-stabilité des courbes elliptiques

Nicolas Billerey

Résumé

Let K be a finite extension of $\mathbf{Q}_2$ complete with a discrete valuation v, $\overline{K}$ an algebraic closure of K and K_{nr} its maximal unramified subextension. Let E be an elliptic curve defined over K with additive reduction over K and having an integral modular invariant j. There exits a smallest extension L of K_{nr} over which E has good reduction. For some congruences modulo 12 of the valuation $v(j)$ of j, we give the degree of the extension L/K_{nr}. When K is a quadratic ramified extension of $\mathbf{Q}_2$, we determine explicitly this degree in term of the coefficients of a Weierstrass equation of E.

Introduction

Étant donnés un nombre premier p, une clôture algébrique $\overline{\mathbf{Q}_p}$ de $\mathbf{Q}_p$ et une extension finie K de $\mathbf{Q}_p$ contenue dans $\overline{\mathbf{Q}_p}$, on considère une courbe elliptique E définie sur K ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire j est entier. Il existe alors une plus petite extension L de la clôture non ramifiée K_{nr} de K dans $\overline{\mathbf{Q}_p}$ où E acquiert bonne réduction. Si E_n désigne le groupe des points de n-torsion de E, on a $L = K_{nr}(E_n)$ pour tout entier $n \geq 3$ non divisible par p ([4, 2.cor.3.]). Le groupe $\Phi = \mathrm{Gal}(L/K_{nr})$ est connu dans le cas où $p \geq 3$ ([2]). Lorsque $p = 2$, il est soit cyclique d'ordre 2, 3, 4 ou 6, soit d'ordre 8 et isomorphe à un groupe quaternionien, soit d'ordre 24 et isomorphe à $\mathrm{SL}_2(\mathbf{F}_3)$. La détermination précise du groupe Φ lorsque $p = 2$ n'a été menée que dans deux cas : par A. Kraus pour $K = \mathbf{Q}_2$ ([2]) et par É. Cali pour toutes les extensions finies $K/\mathbf{Q}_2$ non ramifiées ([1]).

Le présent travail a deux objectifs : d'une part, établir en fonction de la valuation de j modulo 12 plusieurs résultats généraux sur le groupe Φ, valables pour toute extension finie $K/\mathbf{Q}_2$ et, d'autre part, le déterminer explicitement en fonction des coefficients d'une équation de Weierstrass de E dans le cas des extensions quadratiques ramifiées de $\mathbf{Q}_2$. Combiné avec les travaux de Cali et Kraus, ce dernier résultat achève le calcul du groupe Φ pour toutes les extensions de $\mathbf{Q}_2$ de degré ≤ 2.

Remerciements. Je remercie vivement Alain Kraus pour les nombreuses discussions que j'ai eues avec lui durant la préparation de ce travail ainsi que pour sa relecture minutieuse du document.

Table des matières

1 Énoncés des résultats

Soient K une extension finie de $\mathbf{Q}_2$ d'indice de ramification e, π une uniformisante de K et v la valuation de K normalisée par $v(\pi) = 1$. Soit E une courbe elliptique définie sur K d'invariant modulaire j ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire est de valuation ≥ 0.

L'article se compose de deux parties. Dans la première on établit l'ordre du groupe Φ pour certaines valeurs de la congruence de $v(j)$ modulo 12. Les seuls résultats généraux connus sont les suivants ([2, th.2]) :

1. si $v(j) = 0$, alors on a $|\Phi| = 2$.
2. supposons $v(j) \geq 12e$.
   (a) Si $v(j)$ est divisible par 3, on a $|\Phi| = 2$;
   (b) Si $v(j)$ n'est pas divisible par 3, on a $|\Phi| = 3$ si le type de Néron de E est IV ou IV^* et $|\Phi| = 6$ sinon.

En particulier, aucun résultat n'a été démontré si l'on a $0 < v(j) < 12e$. Dans ce cas, on obtient l'énoncé suivant.

Théorème 1 *Supposons* $0 < v(j) < 12e$.

1. *Supposons* $v(j) \equiv \pm 3 \pmod{12}$*, alors* $|\Phi| = 8$*.*
2. *Supposons* $v(j) \equiv \pm 1 \pmod{12}$ *ou* $v(j) \equiv \pm 5 \pmod{12}$*, alors* $|\Phi| = 24$*.*
3. *Supposons* $v(j) \equiv \pm 2 \pmod{12}$ *et* $|6e - v(j)| > 2e$*, alors* $|\Phi| = 24$*.*

Dans tous les autres cas, la valuation de j ne suffit pas à déterminer l'ordre du groupe Φ (*cf.* [1] et le Théorème 2 ci-dessous).

Dans la seconde partie de ce travail, on détermine le groupe Φ lorsque K est une extension quadratique ramifiée de $\mathbf{Q}_2$. Il y a exactement six telles extensions que l'on regroupe en deux ensembles de la façon suivante :

$$\Omega_1 = \{\mathbf{Q}_2(\sqrt{-1}), \mathbf{Q}_2(\sqrt{3})\}$$

et

$$\Omega_2 = \{\mathbf{Q}_2(\sqrt{2}), \mathbf{Q}_2(\sqrt{-2}), \mathbf{Q}_2(\sqrt{6}), \mathbf{Q}_2(\sqrt{-6})\}.$$

On suppose E donnée par une équation de Weierstrass entière, non nécessairement minimale, et dont (c_4, c_6, Δ) sont les invariants standard ([5]) qui lui sont associés. On a $j = c_4^3/\Delta$. Dans le cas où jc_6 est non nul, on pose

$$c_4 = \pi^{v(c_4)} c_4', \quad c_6 = \pi^{v(c_6)} c_6',$$

$$\Delta = \pi^{v(\Delta)} \Delta' \quad \text{et} \quad j' = c_4'^3/\Delta'.$$

On désigne par (C1), (C1'), (C2), et (C3) les conditions suivantes :

$$\Delta' \equiv 1 + \pi \pmod{2} \tag{C1}$$

$$c_4' \equiv 1 + \pi \pmod{2} \tag{C1'}$$

$$j' \equiv 1 + \pi^2 \pmod{\pi^3} \tag{C2}$$

$$c_4' \equiv 1 + \pi^2 \pmod{4} \quad \text{ou} \quad c_4' \equiv 1 + \pi^3 \pmod{4}. \tag{C3}$$

Remarques.

1. Les conditions ci-dessus sont indépendantes du modèle choisi pour représenter la courbe E. En particulier, il n'est pas nécessaire qu'il soit minimal.
2. Elles ne dépendent pas non plus du choix de l'uniformisante de K.

Notations. On note ε l'unité de l'anneau des entiers de K définie par

$$\varepsilon = 3 \cdot \left(\frac{2}{\pi^2}\right)^2.$$

On définit alors les ensembles suivants de couples d'unités de l'anneau des entiers de K :

$$\mathcal{L}_1 = \big\{(-\varepsilon^2 + 6 + \pi^6 + \pi^7, -\varepsilon), (-\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7, -\varepsilon + \pi^4)$$

$$(-\varepsilon^2+6+\pi^6,-\varepsilon+\pi^5),(-\varepsilon^2+2\pi^4+6+\pi^6,-\varepsilon+\pi^4+\pi^5),$$
$$(-\varepsilon^2+2\varepsilon\pi^2+6-\pi^4+\pi^6,-\varepsilon+\pi^2),(-\varepsilon^2+2\varepsilon\pi^2+6+\pi^4+\pi^6,-\varepsilon+\pi^2+\pi^4),$$
$$(-\varepsilon^2+2\varepsilon\pi^2+6-\pi^4+\pi^6+\pi^7,-\varepsilon+\pi^2+\pi^5),(-\varepsilon^2+2\varepsilon\pi^2+6+\pi^4+\pi^6+\pi^7,$$
$$-\varepsilon+\pi^2+\pi^4+\pi^5),(-\varepsilon^2+2\varepsilon\pi^3+6,-\varepsilon+\pi^3),(-\varepsilon^2+2\varepsilon\pi^3+6+2\pi^4,$$
$$-\varepsilon+\pi^3+\pi^4),(-\varepsilon^2+2\varepsilon\pi^3+6+\pi^7,-\varepsilon+\pi^3+\pi^5),(-\varepsilon^2+2\varepsilon\pi^3+6+2\pi^4+\pi^7,$$
$$-\varepsilon+\pi^3+\pi^4+\pi^5),(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3-\pi^4+6,-\varepsilon+\pi^2+\pi^3),$$
$$(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3+\pi^4+6,-\varepsilon+\pi^2+\pi^3+\pi^4),$$
$$(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3-\pi^4+6+\pi^7,-\varepsilon+\pi^2+\pi^3+\pi^5),$$
$$(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3+\pi^4+6+\pi^7,-\varepsilon+\pi^2+\pi^3+\pi^4+\pi^5)\big\}\,;$$

$$\mathcal{L}_2=\left\{\left(-1,\frac{2}{\pi^2}\right),\left(-1+\pi^2+\pi^3,\frac{2}{\pi^2}\right),\left(1,\frac{2}{\pi^2}+\pi^2\right),\right.$$
$$\left(1+\pi^2+\pi^3,\frac{2}{\pi^2}+\pi^2\right),\left(-1+\pi^3,\frac{2}{\pi^2}+\pi^3\right),\left(-1+\pi^2,\frac{2}{\pi^2}+\pi^3\right),$$
$$\left.\left(1+\pi^3,\frac{2}{\pi^2}+\pi^2+\pi^3\right),\left(1+\pi^2,\frac{2}{\pi^2}+\pi^2+\pi^3\right)\right\}.$$

Théorème 2 *On suppose que l'extension $K/\mathbf{Q}_2$ est quadratique ramifiée. On est dans l'un des cas suivants.*

1. *Si $v(j)=0$, on a $|\Phi|=2$.*
2. *Si $v(j)\in\{1,2,5,7,10,11,13,14,17,19,22,23\}$, on a $|\Phi|=24$.*
3. *Si $v(j)\in\{3,9,15,21\}$, on a $|\Phi|=8$.*
4. *Supposons $v(j)=4$.*
   (a) *Supposons que la condition* (C1) *soit satisfaite.*
   On a $|\Phi|=3$ si les conditions suivantes sont satisfaites :
      i. *on a $v(\Delta)\equiv 8 \pmod{12}$;*
      ii. *Si $K\in\Omega_1$, on a $c_6'\equiv 1+\pi^2 \pmod 4$ ou $c_6'\equiv 1+\pi^3 \pmod 4$;*
      iii. *Si $K\in\Omega_2$, on a $c_6'\equiv 1 \pmod 4$ ou $c_6'\equiv 1+\pi^2+\pi^3 \pmod 4$.*

   On a $|\Phi|=6$ sinon.
   (b) *Si la condition* (C1) *n'est pas satisfaite, on a $|\Phi|=24$.*
5. *Supposons $v(j)=6$. On a*
$$|\Phi|=\begin{cases}4 & \text{si la condition (C1) est satisfaite,}\\ 8 & \text{sinon.}\end{cases}$$
6. *Supposons $v(j)=8$.*
   (a) *Supposons que la condition* (C2) *soit satisfaite.*
   On a $|\Phi|=3$ si les deux conditions suivantes sont satisfaites :

i. on a $v(\Delta) \equiv 4 \pmod{12}$ *;*

ii. il existe $(a, b) \in \mathcal{L}_1$ *tel que* $c'_4 \equiv a \pmod{\pi^8}$ *et* $c'_6 \equiv b \pmod{\pi^6}$.

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

(b) Si la condition (C2) *n'est pas satisfaite, on a* $|\Phi| = 24$.

7. Supposons $v(j) = 12$.

(a) Si $2v(c_6) = 3v(c_4) + 1$, *on a* $|\Phi| = 8$.

(b) Si $2v(c_6) = 3v(c_4) + 2$.

i. Si $K \in \Omega_1$, *on a*

$$|\Phi| = \begin{cases} 4 & \text{si la condition (C1') est satisfaite,} \\ 8 & \text{sinon.} \end{cases}$$

ii. Si $K \in \Omega_2$, *on a*

$$|\Phi| = \begin{cases} 8 & \text{si la condition (C1') est satisfaite,} \\ 2 & \text{si la condition (C3) est satisfaite,} \\ 4 & \text{sinon.} \end{cases}$$

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

$$|\Phi| = \begin{cases} 8 & \text{si } K \in \Omega_1, \\ 4 & \text{si } K \in \Omega_2. \end{cases}$$

(d) Si $2v(c_6) - 3v(c_4) \geq 4$.

i. Si $K \in \Omega_1$, *on a*

$$|\Phi| = \begin{cases} 2 & \text{si la condition (C3) est satisfaite et } v(c_4) \text{ est pair,} \\ 4 & \text{sinon.} \end{cases}$$

ii. Si $K \in \Omega_2$, *on a* $|\Phi| = 8$.

8. Supposons $v(j) = 16$.

(a) Supposons que la condition (C2) *soit satisfaite.*

On a $|\Phi| = 3$ *si les deux conditions suivantes sont satisfaites :*

i. on a $v(\Delta) \equiv 8 \pmod{12}$ *;*

ii. il existe $(a, b) \in \mathcal{L}_2$ *tel que* $c'_4 \equiv a \pmod{4}$ *et* $c'_6 \equiv b \pmod{4}$.

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

(b) Si la condition (C2) *n'est pas satisfaite, on a* $|\Phi| = 24$.

9. Supposons $v(j) = 18$. *On a*

$$|\Phi| = \begin{cases} 4 & \text{si la condition (C1') est satisfaite,} \\ 8 & \text{sinon.} \end{cases}$$

10. Supposons $v(j) = 20$.

(a) *Supposons que la condition* (C1') *soit satisfaite.*
On a $|\Phi| = 3$ *si les deux conditions suivantes sont satisfaites :*
i. on a $v(\Delta) \equiv 4 \pmod{12}$ *;*
ii. on a $c_6' \equiv \frac{\pi^2}{2} + 2 \pmod 4$ *ou* $c_6' \equiv \frac{\pi^2}{2} + \pi^3 \pmod 4$.
On a $|\Phi| = 6$ *sinon.*

(b) *Si la condition* (C1') *n'est pas satisfaite, on a* $|\Phi| = 24$.

11. *Supposons* $v(j) \geq 24$.
(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 deux conditions suivantes sont satisfaites :*
i. on a $v(\Delta) \equiv 4 \pmod{12}$ *ou* $v(\Delta) \equiv 8 \pmod{12}$ *;*
ii. on a $c_6' \equiv \frac{\pi^2}{2} \pmod 4$ *ou* $c_6' \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.
On a $|\Phi| = 6$ *sinon.*

Dans l'Appendice A, on montre que chacun des cas ci-dessus se réalise.

2 Le cas des extensions quelconques

2.1 Lemmes sur les carrés

On reprend les notations de la section 1. Il existe une unique extension quadratique non ramifiée de K dans $\overline{K}$. On la note N. Lorsque l'extension $K/\mathbf{Q}_2$ est totalement ramifiée, le corps résiduel de N est de cardinal 4 et un système de représentants est $\mu_3 \cup \{0\}$, où μ_3 est l'ensemble des racines cubiques de l'unité. On note $\mathcal{O}_K$ (resp. $\mathcal{O}_N$) l'anneau des entiers de K (resp. de N) et $\mathcal{U}_K$ (resp. $\mathcal{U}_N$) ses unités.

Par commodité, on rappelle le résultat suivant ([2, lem.7]).

Lemme 1 *Soit* x *un élément de* $\mathcal{U}_K$ *congru à* 1 *modulo* $4\mathcal{O}_K$. *Alors,* x *est un carré dans* K_{nr}.

On en déduit le résultat suivant.

Lemme 2 *Soit* x *un élément de* $\mathcal{U}_K$. *Alors,* x *est un carré dans* K_{nr} *si et seulement si il existe un élément* y *de* $\mathcal{U}_N$ *tel que*

$$x \equiv y^2 \pmod{4\mathcal{O}_N}.$$

Démonstration : La condition est nécessaire car si x est un carré dans K_{nr}, c'est un carré dans une extension quadratique non ramifiée de K, donc dans N. Réciproquement, s'il existe un élément y de N tel que $x \equiv y^2 \pmod{4\mathcal{O}_N}$, alors, d'après le lemme 1, x est un carré dans la clôture non ramifiée de N dans $\overline{K}$. Or $N_{nr} = K_{nr}$ car N/K est non ramifiée. D'où le lemme.

Lorsque l'extension $K/\mathbf{Q}_2$ est totalement ramifiée, on a le résultat plus précis suivant.

Lemme 3 *Supposons l'extension $K/\mathbf{Q}_2$ totalement ramifiée. Soit x un élément de $\mathcal{U}_K$. Alors, x est un carré dans K_{nr} si et seulement si il existe un élément $y \in \mathcal{U}_K$ tel que $x \equiv y^2 \pmod{4\mathcal{O}_K}$. Autrement dit, x est un carré dans K_{nr} si et seulement si il existe des éléments $a_0, a_1, \ldots, a_{e-1}$ tels que les deux conditions suivantes soient satisfaites :*

1. *on a $a_0 = 1$ et $a_j = 0$ ou 1 pour $1 \leq j \leq e-1$;*
2. *on a*
$$x \equiv \left(a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1}\right)^2 \pmod{4\mathcal{O}_K}. \tag{1}$$

Démonstration : La condition est suffisante d'après le lemme précédent.

Réciproquement, supposons que x soit un carré dans K_{nr}. Il existe alors y dans $\mathcal{O}_N$ tel que $x = y^2$. On choisit comme système de représentants du corps résiduel de N l'ensemble μ_3 des racines cubiques de l'unité. On écrit le développement de Hensel de y modulo 2 :

$$y \equiv a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1} \pmod{2\mathcal{O}_N}, \quad \text{où } a_j \in \mu_3 \cup \{0\}.$$

Soit i un entier ≥ 0 et $P(i)$ la proposition de récurrence suivante :

$$\ll a_0, \ldots, a_i = 0 \text{ ou } 1 \gg.$$

Montrons $P(0)$. L'extension $K/\mathbf{Q}_2$ étant totalement ramifiée, x est congru à 1 modulo $\pi\mathcal{O}_K$, d'où $y^2 \equiv 1 \pmod{\pi\mathcal{O}_K}$. Or π est une uniformisante de N, donc $\pi\mathcal{O}_N$ est un idéal premier de $\mathcal{O}_N$. On en déduit $y \equiv \pm 1 \pmod{\pi\mathcal{O}_N}$. Puis, comme $-1 \equiv 1 \pmod{\pi}$, il vient $y \equiv 1 \pmod{\pi\mathcal{O}_N}$. Cela démontre $P(0)$ et on a $a_0 = 1$. Si $e = 1$, cela démontre le résultat.

Supposons $e > 1$. Soit $i \geq 0$ tel que $i < e-1$ et $P(i)$ vraie. Montrons $P(i+1)$. Posons

$$z = \frac{1}{\pi^{i+1}}\left(y - (1 + a_1\pi + \cdots + a_i\pi^i)\right).$$

L'élément z est dans $\mathcal{O}_N$. Calculons $z^2 \pmod{\pi\mathcal{O}_N}$ de deux façons différentes.

D'une part, on a

$$z^2 = \frac{1}{\pi^{2(i+1)}}\left(y^2 - 2y(1 + a_1\pi + \cdots + a_i\pi^i) + (1 + a_1\pi + \cdots + a_i\pi^i)^2\right).$$

Or

$$2y(1 + a_1\pi + \cdots + a_i\pi^i) \equiv 2(1 + a_1\pi + \cdots + a_i\pi^i)^2 \pmod{\pi^{e+i+1}\mathcal{O}_N}.$$

Comme $x = y^2$, on en déduit donc,

$$z^2 \equiv \frac{1}{\pi^{2(i+1)}}\left(x - (1 + a_1\pi + \cdots + a_i\pi^i)^2\right) \pmod{\pi^{e-1-i}\mathcal{O}_N}.$$

Posons

$$\alpha = \frac{1}{\pi^{2(i+1)}}\left(x - (1 + a_1\pi + \cdots + a_i\pi^i)^2\right).$$

Alors, par hypothèse de récurrence, $\alpha \in \mathcal{O}_N \cap K = \mathcal{O}_K$ et on a, en particulier,

$$\alpha \equiv 0 \text{ ou } 1 \pmod{\pi\mathcal{O}_N}.$$

On en déduit alors

$$z^2 \equiv 0 \text{ ou } 1 \pmod{\pi\mathcal{O}_N}.$$

D'autre part, on a

$$z \equiv a_{i+1} \pmod{\pi\mathcal{O}_N}, \quad \text{puis } z^2 \equiv a_{i+1}^2 \pmod{\pi\mathcal{O}_N}.$$

On en déduit $a_{i+1} = 0$ ou 1. D'où le résultat par récurrence. On a donc, $x \equiv (1 + a_1\pi + \cdots + a_{e-1}\pi^{e-1})^2 \pmod{4\mathcal{O}_N}$ avec $a_1, \ldots, a_{e-1} = 0$ ou 1. D'où

$$\frac{1}{4}\left(x - (1 + a_1\pi + \cdots + a_{e-1}\pi^{e-1})^2\right) \in \mathcal{O}_N \cap K = \mathcal{O}_K.$$

D'où la congruence annoncée.

Lemme 4 *Soit x un élément de K_{nr} de valuation 0. Alors, toutes les racines cubiques de x dans $\overline{K}$ sont dans K_{nr}.*

Démonstration : L'élément x est une unité des entiers de $K(x)$. Elle s'écrit en particulier, $x = \xi \cdot b$, où ξ est une racine de l'unité d'ordre impair et b une unité principale des entiers de $K(x)$, i.e. $b \equiv 1 \pmod{\pi\mathcal{O}_{K(x)}}$. Or, ξ est un cube dans K_{nr} et le lemme de Hensel appliqué au polynôme $X^3 - b$ de $\mathcal{O}_{K(x)}[X]$ montre qu'il en va de même pour b. D'où le résultat.

On rappelle que e désigne l'indice de ramification de l'extension $K/\mathbf{Q}_2$.

Lemme 5 *Soient K'/K_{nr} une extension finie de degré n impair, x et y deux éléments de K' de valuation ≥ 0 et ρ un rationnel positif. On suppose que les conditions suivantes sont satisfaites.*

1. *$v(x - y) = \rho$;*
2. *$\rho = r/s$, avec r et s entiers premiers entre eux et r impair ;*
3. *$\rho \leq 2e$.*

Alors, l'un au-moins des éléments x et y n'est pas un carré dans K'.

Démonstration : Supposons que $x = a^2$ et $y = b^2$ soient des carrés dans K'. On a $v(2b) = e + v(b) = e + v(y)/2 \geq \rho/2$ par hypothèse.

Supposons $v(a - b) < \rho/2$. Alors, d'après l'égalité $a + b = a - b + 2b$, on en déduit $v(a + b) = v(a - b) < \rho/2$. Or, c'est absurde car $v(a - b) + v(a + b) = v(a^2 - b^2) = \rho$. On a donc $v(a - b) \geq \rho/2$ et de même, $v(a + b) \geq \rho/2$. D'où, $v(a - b) = v(a + b) = \rho/2$. Mais, r et n étant impairs, $\rho/2 \notin v(K') \subset \frac{1}{n}\mathbf{Z}$. D'où une contradiction et le lemme.

2.2 La courbe $\widetilde{E}$

On reprend les notations de la section 1. En particulier, e désigne l'indice de ramification de $K/\mathbf{Q}_2$ et on note encore v le prolongement de la valuation normalisée v de K à une clôture algébrique $\overline{K}$ de K . On choisit une racine cubique $\Delta^{1/3}$ de Δ dans $\overline{K}$. On note M l'extension de K_{nr} engendrée par $\Delta^{1/3}$. D'après le lemme 4, si $v(\Delta)$ est divisible par 3, alors $\Delta^{1/3}$ est dans K_{nr}, i.e. l'extension M/K_{nr} est triviale. Réciproquement, si $\Delta^{1/3}$ est dans K_{nr}, alors $v(\Delta)$ est divisible par 3 car $v(K_{nr}) \subset \mathbf{Z}$.

On pose, pour t dans l'ensemble μ_3 des racines cubiques de l'unité :

$$A_t = c_4 - 12t\Delta^{1/3} \quad \text{et} \quad B_t = c_4^2 + 12tc_4\Delta^{1/3} + (12t\Delta^{1/3})^2.$$

Lorsque $t = 1$, on retrouve les éléments $A_1 = A$ et $B_1 = B$ de [2, th.3]. On a également $A_tB_t = c_6^2$. De plus, d'après le lemme 4, A_t et B_t sont dans K_{nr} si et seulement si 3 divise $v(\Delta)$, i.e. si et seulement si 3 divise $v(j)$. On désigne par $j^{1/3}$ la racine cubique de j dans $\overline{K}$ définie par l'égalité

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

On fait l'hypothèse $v(j) > 6e$. L'équation suivante définit alors un modèle entier d'une courbe elliptique, notée $\widetilde{E}$, sur K :

$$y^2 + 2xy = x^3 + \frac{j}{3(j-1728)}x + \frac{j}{3^3(j-1728)}. \tag{2}$$

Les coefficients standard $(\widetilde{c_4}, \widetilde{c_6}, \widetilde{\Delta})$ de $\widetilde{E}$ sont donnés par les égalités suivantes :

$$\widetilde{c_4} = -2^4\frac{1728}{j-1728} = -2^{10}\cdot 3^3\frac{\Delta}{c_6^2}, \quad \widetilde{c_6} = 2^6\frac{1728}{j-1728} = 2^{12}\cdot 3^3\frac{\Delta}{c_6^2} \tag{3}$$

et

$$\widetilde{\Delta} = -2^{12}\frac{1728j}{(j-1728)^3} = -2^{18}\cdot 3^3\frac{c_4^3\Delta^2}{c_6^6}. \tag{4}$$

On vérifie que l'on a $v(\widetilde{\Delta}) = v(j)$. De plus, on a $\widetilde{j} = \widetilde{c_4}^3/\widetilde{\Delta} = 1728^2/j$, d'où en particulier, $v(\widetilde{j}) = 12e - v(j)$.

On choisit de noter $\widetilde{\Delta}^{1/3}$ la racine cubique de $\widetilde{\Delta}$ définie par l'égalité :

$$\widetilde{\Delta}^{1/3} = -2^6\cdot 3\frac{j^{1/3}}{j-1728} = -2^6\cdot 3\frac{c_4\Delta^{2/3}}{c_6^2}.$$

Pour $t \in \mu_3$, on définit, comme pour E ci-dessus, le coefficient

$$\widetilde{B}_t = \widetilde{c_4}^2 + 12t\widetilde{c_4}\widetilde{\Delta}^{1/3} + (12t\widetilde{\Delta}^{1/3})^2.$$

À nouveau, $\widetilde{B}_t$ est dans K_{nr} si et seulement si 3 divise $v(j)$. Posons à présent

$$w_t = 2^4\cdot 3\cdot t^2\frac{\Delta^{1/3}}{c_6}.$$

Proposition 1 *On est dans l'un des cas suivants :*

1. *supposons $v(j)$ divisible par 3, alors w_t appartient à K_{nr} ;*
2. *supposons $v(j)$ non divisible par 3, alors w_t n'appartient pas à K_{nr} et w_t appartient à M qui est l'unique extension de degré 3 de K_{nr}.*

De plus, on a, pour $t \in \mu_3$,

$$\widetilde{B}_t = w_t^4 B_{t^2}.$$

Démonstration : Les deux premières assertions résultent du lemme 4. On a

$$12 \cdot \frac{\widetilde{\Delta}^{1/3}}{\widetilde{c_4}} = \frac{1}{12} \cdot \frac{c_4}{\Delta^{1/3}}.$$

D'où

$$\begin{aligned}\frac{\widetilde{B}_t}{\widetilde{c_4}^2} &= 1 + 12t\frac{\widetilde{\Delta}^{1/3}}{\widetilde{c_4}} + \left(12t\frac{\widetilde{\Delta}^{1/3}}{\widetilde{c_4}}\right)^2 = 1 + \frac{t}{12} \cdot \frac{c_4}{\Delta^{1/3}} + \left(\frac{t}{12} \cdot \frac{c_4}{\Delta^{1/3}}\right)^2 \\ &= \left(t\frac{c_4}{12\Delta^{1/3}}\right)^2 \left(1 + 12t^2\frac{\Delta^{1/3}}{c_4} + \left(12t^2\frac{\Delta^{1/3}}{c_4}\right)^2\right) = \left(t\frac{c_4}{12\Delta^{1/3}}\right)^2 \cdot \frac{B_{t^2}}{c_4^2}.\end{aligned}$$

D'où, comme $\widetilde{c_4} = -2^{10} \cdot 3^3\Delta/c_6^2$, on a

$$\widetilde{B}_t = 2^{16} \cdot 3^4 \cdot t^2\frac{\Delta^{4/3}}{c_6^4}B_{t^2} = w_t^4 B_{t^2}$$

et la proposition.

On note, comme $\widetilde{j} \neq 0$, $\widetilde{c_4} = \pi^{v(\widetilde{c_4})}\widetilde{c_4}'$, $\widetilde{\Delta} = \pi^{v(\widetilde{\Delta})}\widetilde{\Delta}'$ et $\widetilde{j} = \pi^{v(\widetilde{j})}\widetilde{j}'$. On vérifie alors d'après les formules (3) et (4) que l'on a le résultat suivant.

Lemme 6 *On a*

$$\widetilde{\Delta}' = -3^3 \cdot \left(\frac{2}{\pi^e}\right)^{18} \frac{c_4'^3\Delta'^2}{c_6'^6} \quad \textit{et} \quad j'\widetilde{j}' = 3^6 \cdot \left(\frac{2}{\pi^e}\right)^{12}.$$

2.3 Démonstration du théorème 1

On suppose que l'on a $0 < v(j) < 12e$. On reprend les notations introduites à la section 2.2 et on choisit une racine carrée $B^{1/2}$ de B dans $\overline{K}$. On pose alors :

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

La proposition suivante est à peu de choses près [1, prop.1].

Proposition 2 *Supposons $c_6 \neq 0$ et $v(j) \equiv 0 \pmod 3$. Alors, si pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr}, on a $|\Phi| = 8$.*

DÉMONSTRATION : D'après [2, th.3], il s'agit de montrer que C n'est pas un carré dans $K_{nr}(B^{1/2})$. On a $A_tB_t = c_6^2$ qui est non nul par hypothèse. Donc A_t est un carré dans K_{nr} si et seulement si B_t l'est. De plus, on a $c_4 \neq 0$ (car B_t n'est pas un carré dans K_{nr}). Posons

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

Alors, $(1, \nu)$ est une base de $K_{nr}(B^{1/2})$ sur K_{nr}. Supposons que C soit un carré dans $K_{nr}(B^{1/2})$. Il existe deux éléments a et b de K_{nr} tels que

$$C = c_4(12j^{-1/3} + 2\nu) = (a + b\nu)^2. \tag{5}$$

Or, on vérifie que l'on a $\nu^2 = 2\nu + 12j^{-1/3} + 144j^{-2/3}$. Mais, $j^{1/3} \in K_{nr}$ car $v(j) \equiv 0 \pmod 3$, donc d'après (5), il vient

$$\begin{cases} c_4 = b(a+b) \\ 12c_4j^{-1/3} = a^2 + b^2(12j^{-1/3} + 144j^{-2/3}), \end{cases}$$

puis, $a^2 - 12abj^{-1/3} + 144b^2j^{-2/3} = 0$. Autrement dit, il existe $t \neq 1$ dans μ_3 tel que $a = -12tbj^{-1/3}$. D'où, $c_4 = b^2(1 - 12tj^{-1/3})$. Or, $A_t = c_4(1 - 12tj^{-1/3})$, donc $A_t = b^2(1 - 12tj^{-1/3})^2$ est un carré dans K_{nr} et B_t l'est aussi et ceci contredit l'hypothèse. D'où le résultat.

2.3.1 Démonstration de l'assertion 1

On fait l'hypothèse $v(j) \equiv \pm 3 \pmod{12}$. On a en particulier, $v(j) \equiv 0 \pmod 3$, donc $j^{1/3} \in K_{nr}$.

Supposons dans un premier temps, $v(j) < 6e$ de sorte que $v(12j^{-1/3}) = 2e - v(j)/3$ est impair et vérifie l'inégalité $0 < v(12j^{-1/3}) \leq 2e$. Alors, pour $t \in \mu_3$,

$$\frac{B_t}{c_4^2} = 1 + 12tj^{-1/3} + (12tj^{-1/3})^2$$

est une unité de K_{nr} et

$$v\left(\frac{B_t}{c_4^2} - 1\right) = v(12tj^{-1/3}) = 2e - \frac{v(j)}{3}.$$

D'après le lemme 5 appliqué à $K' = K_{nr}$, $x = B_t/c_4^2$, $y = 1$ et $\rho = 2e - v(j)/3$, B_t n'est pas un carré dans K_{nr}. D'après la proposition 2, on a donc $|\Phi| = 8$.

Par ailleurs, si $v(j) > 6e$, alors la courbe $\widetilde{E}$ d'équation (2) a un invariant modulaire $\widetilde{j}$ de valuation $12e - v(j)$. Autrement dit, $\widetilde{E}$ satisfait aux hypothèses précédentes. Donc, pour tout $t \in \mu_3$, $\widetilde{B}_t$ n'est pas un carré dans K_{nr}. Or, d'après la proposition 1, cela vaut aussi pour B_{t^2}. Ainsi, pour tout t dans μ_3, B_{t^2} n'est pas un carré dans K_{nr}. D'après la proposition 2, cela implique $|\Phi| = 8$.

Cela démontre l'assertion 1 du théorème 1.

2.3.2 Démonstration de l'assertion 2

On fait l'hypothèse $v(j) \equiv \pm 1 \pmod{12}$ ou $v(j) \equiv \pm 5 \pmod{12}$. En particulier, $v(j)$ est impair et n'est pas divisible par 3.

Supposons dans un premier temps, $v(j) < 6e$ de sorte que $v(12j^{-1/3}) = 2e - v(j)/3$ est > 0. On a alors,

$$v\left(\frac{B}{c_4^2} - 1\right) = v(12j^{-1/3}) = 2e - \frac{v(j)}{3} = \frac{6e - v(j)}{3} \leq 2e.$$

Or, par hypothèse, $6e - v(j)$ est impair et n'est pas divisible par 3. D'après le lemme 5 appliqué à $K' = K_{nr}(\Delta^{1/3}) = M$, $x = B/c_4^2$, $y = 1$ et $\rho = (6e - v(j))/3$, B n'est pas un carré dans M.

Par ailleurs, si $v(j) > 6e$, alors la courbe $\widetilde{E}$ d'équation (2) a un invariant modulaire $\widetilde{j}$ de valuation $12e - v(j)$. Autrement dit, $\widetilde{E}$ satisfait aux hypothèses précédentes. Donc, $\widetilde{B}$ n'est pas un carré dans M. Or, d'après la proposition 1, cela vaut aussi pour B.

D'après [2, th.3], cela implique $|\Phi| = 24$ et l'assertion 2 du théorème 1.

2.3.3 Démonstration de l'assertion 3

On a $v(j) \equiv \pm 2 \pmod{12}$ de sorte que $v(j)$ n'est pas divisible par 3. Supposons tout d'abord $v(j) < 6e$. Alors,

$$\frac{B}{c_4^2} = 1 + 12j^{-1/3} + 144j^{-2/3}$$

est une unité de M. Notons π_0 une racine cubique de π dans $\overline{K}$ et supposons que B soit un carré dans M. Il existe alors a, b et c dans K_{nr} tels que

$$\begin{aligned} \frac{B}{c_4^2} &= (a + b\pi_0 + c\pi_0^2)^2 \\ &= (a^2 + 2bc\pi) + (c^2\pi + 2ab)\pi_0 + (b^2 + 2ac)\pi_0^2. \end{aligned} \tag{6}$$

Or, $v(\pi_0) = 1/3$, donc $v(a)$, $v(b\pi_0)$ et $v(c\pi_0^2)$ sont distincts puis, d'après l'égalité

$$0 = v\left(\frac{B}{c_4^2}\right) = 2v(a + b\pi_0 + c\pi_0^2),$$

il vient, $v(a) = 0$, $v(b) \geq 0$ et $v(c) \geq 0$. Posons par ailleurs

$$u = \frac{j^{1/3}}{\pi_0^{v(j)}}.$$

On a $u^3 = j'$ et $v(j') = 0$, donc $u \in K_{nr}$ en vertu du lemme 4.

On distingue à présent deux cas selon la congruence de $v(j)$ modulo 12.

Supposons $v(j) \equiv 2 \pmod{12}$**.** Écrivons $v(j) = 12k+2$, $k \geq 0$. On a alors,

$$j^{-1/3} = u^{-1}\pi_0^{-12k-2} = \frac{u^{-1}}{\pi^{4k+1}}\pi_0 \quad \text{et} \quad j^{-2/3} = \frac{u^{-2}}{\pi^{8k+2}}\pi_0^2,$$

puis,

$$\frac{B}{c_4^2} = 1 + 12\frac{u^{-1}}{\pi^{4k+1}}\pi_0 + 144\frac{u^{-2}}{\pi^{8k+2}}\pi_0^2$$

et l'on peut identifier dans (6) les coefficients de la décomposition dans la base $(1, \pi_0, \pi_0^2)$. Il vient en particulier (comme $u \in K_{nr}$) :

$$\begin{cases} c^2\pi + 2ab = 12 \cdot u^{-1}/\pi^{4k+1} \\ b^2 + 2ac = 144 \cdot u^{-2}/\pi^{8k+2}. \end{cases} \tag{7}$$

Supposons $2v(b) \geq 4e - 8k - 2 = v(144u^{-2}/\pi^{8k+2})$. Alors, d'après (7), on a $v(2ac) = e + v(c) \geq 4e - 8k - 2$. Puis, comme $e + v(b) > 2e - 4k - 1$, on a $v(c^2\pi) = 2v(c) + 1 = 2e - 4k - 1$, i.e. $v(c) = e - 2k - 1$. Or,

$$e - 2k - 1 \geq 3e - 8k - 2 \Longrightarrow v(j) \geq 4e.$$

Si $v(j) < 4e$, on a une contradiction et l'hypothèse $2v(b) \geq v(144u^{-2}/\pi^{8k+2})$ est absurde.

Supposons que tel soit le cas, i.e. $v(j) < 4e$. On a alors $2v(b) < 4e - 8k - 2$, puis d'après (7), $e + v(c) = 2v(b)$, d'où $2v(c) + 1 = 4v(b) - 2e + 1$. On distingue à présent trois cas.

1. Supposons $2v(c) + 1 = e + v(b)$. Alors, $3(v(b) - e) + 1 = 0$, d'où une contradiction en réduisant cette égalité modulo 3.
2. Supposons $2v(c) + 1 > e + v(b)$, i.e. $4v(b) - 2e + 1 > e + v(b)$. Alors, d'après (7), $e + v(b) = 2e - 4k - 1$, i.e. $v(b) = e - 4k - 1$. Or, $4v(b) - 2e + 1 > e + v(b)$ par hypothèse. Donc $v(j) < 0$. C'est une contradiction.
3. Supposons $2v(c) + 1 < e + v(b)$. Alors, d'après (7), $2v(c) + 1 = 2e - 4k - 1$, puis $v(c) = e - 2k - 1$. Or, $2v(b) = v(c) + e$, donc $2v(b) = 2e - 2k - 1$. On en déduit une contradiction en réduisant cette égalité modulo 2.

Après examen de tous les cas possibles, on a finalement montré que l'hypothèse B est un carré dans M est absurde si $v(j) \equiv 2 \pmod{12}$ et $v(j) < 4e$.

Supposons $v(j) \equiv -2 \pmod{12}$**.** Écrivons $v(j) = 12k+10$, $k \geq 0$. On a alors,

$$j^{-1/3} = u^{-1}\pi_0^{-12k-10} = \frac{u^{-1}}{\pi^{4k+4}}\pi_0^2 \quad \text{et} \quad j^{-2/3} = \frac{u^{-2}}{\pi^{8k+7}}\pi_0,$$

puis,

$$\frac{B}{c_4^2} = 1 + 144\frac{u^{-2}}{\pi^{8k+7}}\pi_0 + 12\frac{u^{-1}}{\pi^{4k+1}}\pi_0^2$$

et l'on peut identifier dans (6) les coefficients de la décomposition dans la base $(1, \pi_0, \pi_0^2)$. Il vient en particulier (comme $u \in K_{nr}$) :

$$\left\{ \begin{array}{l} c^2\pi + 2ab = 144 \cdot u^{-2}/\pi^{8k+7} \\ b^2 + 2ac = 12 \cdot u^{-1}/\pi^{4k+4}. \end{array} \right. \tag{8}$$

On distingue trois cas.

1. Supposons $2v(b) > 2e-4k-4$, i.e. $v(b) > e-2k-2$. Alors, d'après (8), on a $e+v(c) = 2e-4k-4$, i.e. $v(c) = e-4k-4$. Donc $2v(c)+1 = 2e-8k-7$, puis $2v(c)+1 < 4e-8k-7 = v(144u^{-2}/\pi^{8k+7})$. Alors, d'après (8), $v(2ab) = e+v(b) = 2v(c)+1 = 2e-8k-7$. Autrement dit, $v(b) = e-8k-7$, d'où $e-8k-7 > e-2k-2$. Or cela équivaut à $v(j) < 0$. D'où une contradiction.
2. Supposons $2v(b) < 2e-4k-4$, i.e. $v(b) < e-2k-2$. Alors, d'après (8), on a $e+v(c) = 2v(b)$, puis $2v(c)+1 = 4v(b)-2e+1$. En réduisant en modulo 3, on constate que l'égalité $e+v(b) = 4v(b)-2e+1$ est impossible. De plus,

   $$2v(c)+1 = 4v(b)-2e+1 > e+v(b) \Longleftrightarrow v(b) > e-\frac{1}{3} \Longleftrightarrow v(b) \geq e,$$

   car e et $v(b)$ sont entiers. Or, l'hypothèse faite entraîne $v(b) < e$. On a alors $2v(c)+1 = 4v(b)-2e+1 = 4e-8k-7$, puis $2v(b) = 3e-4k-4$. Comme $2v(b) < 2e-4k-4$, on en déduit $e < 0$. C'est donc une contradiction et l'hypothèse $2v(b) < 2e-4k-4$ était absurde.
3. On a donc finalement $2v(b) = 2e-4k-4$, i.e. $v(b) = e-2k-2$. Donc

   $$e+v(b) = 2e-2k-2 < 4e-8k-7 \Longleftrightarrow v(j) < 4e.$$

   Autrement dit, si $v(j) < 4e$, il vient, d'après (8), $2v(c)+1 = e+v(b) = 2e-2k-2$. D'où une contradiction en réduisant cette égalité modulo 2.

Après examen de tous les cas possibles, on a finalement montré que l'hypothèse B est un carré dans M est absurde si $v(j) \equiv -2 \pmod{12}$ et $v(j) < 4e$.

Il reste donc à voir que si $v(j) \equiv \pm 2 \pmod{12}$ et $v(j) > 8e$, alors B n'est pas un carré dans M. On considère pour ce faire, la courbe $\widetilde{E}$ d'équation (2). On a

$$v(\widetilde{j}) = 12e - v(j) \equiv -v(j) \equiv \pm 2 \pmod{12} \quad \text{et} \quad v(\widetilde{j}) < 4e.$$

Autrement dit, la courbe $\widetilde{E}$ satisfait aux hypothèses précédentes, donc $\widetilde{B}$ n'est pas un carré dans M et B non plus, d'après la proposition 1.

D'après [2, th.3], on a donc $|\Phi| = 24$. Cela démontre bien l'assertion 3 du théorème 1 et achève sa démonstration.

3 Le cas des extensions quadratiques

On reprend les notations ds sections 1 et 2.1 et l'on suppose l'extension $K/\mathbf{Q}_2$ quadratique ramifiée. Désignons par π_0 une racine cubique de π dans $\overline{K}$. C'est une uniformisante de l'extension $K_{nr}(\pi_0)/K_{nr}$.

3.1 Lemmes généraux

Lemme 7 *Soit x un élément de $\mathcal{U}_K$. Alors,*

$$x^2 \equiv \begin{cases} 1 \pmod{4\pi} & \text{si } x \equiv 1 \pmod 2 \\ 1+\pi^2+\pi^3 \pmod 4 & \text{si } x \equiv 1+\pi \pmod 2. \end{cases}$$

En particulier, on a $x^2 \equiv 1 \pmod 2$.

Démonstration : Si $x \equiv 1 \pmod 2$, alors il existe a dans $\mathcal{O}_K$ tel que $x = 1+2a$. Puis $x^2 = 1+4a(a+1)$. Or, $a(a+1) \equiv 0 \pmod \pi$, donc $x^2 \equiv 1 \pmod 4$. De même, si $x \equiv 1+\pi \pmod 2$, alors il existe a dans $\mathcal{O}_K$ tel que $x = 1+\pi+2a$. Puis $x^2 \equiv 1+\pi^2+2\pi \pmod 4$. Or, 2 est associé à π^2, d'où $2\pi \equiv \pi^3 \pmod 4$ et la congruence annoncée. Dans les deux cas, on a $x^2 \equiv 1 \pmod 2$. D'où le résultat.

Lemme 8 *Soit x un élément de $\mathcal{U}_K$. Alors, x est un carré dans K_{nr} si et seulement si $x \equiv 1$ ou $1+\pi^2+\pi^3 \pmod 4$.*

Démonstration : D'après le lemme 3, x est un carré dans K_{nr} si et seulement si x est un carré modulo $4\mathcal{O}_K$. On conclut alors avec le lemme précédent.

Lemme 9 *Soient x un élément de $\mathcal{U}_K$ congru à 1 modulo 4 et $\sqrt{x}$ une racine carrée de x dans $\overline{K}$. Alors, on a $\sqrt{x} \equiv 1 \pmod{2\mathcal{O}_{K_{nr}}}$.*

Démonstration : D'après le lemme 8, $\sqrt{x} \in K_{nr}$. Supposons $v(\sqrt{x}-1) < 2$. Alors, d'après l'égalité, $\sqrt{x}+1 = \sqrt{x}-1+2$, il vient, $v(\sqrt{x}+1) = v(\sqrt{x}-1) < 2$. Donc $v(x-1) < 4$ ce qui est contraire aux hypothèses. D'où le lemme.

Pour chacune des six extensions quadratiques ramifiées de $\mathbf{Q}_2$, on indique dans le tableau ci-dessous un choix d'uniformisante.

K	$\mathbf{Q}_2(\sqrt{-1})$	$\mathbf{Q}_2(\sqrt{3})$	$\mathbf{Q}_2(\sqrt{2})$	$\mathbf{Q}_2(\sqrt{-2})$	$\mathbf{Q}_2(\sqrt{6})$	$\mathbf{Q}_2(\sqrt{-6})$
π	$1+\sqrt{-1}$	$1+\sqrt{3}$	$\sqrt{2}$	$\sqrt{-2}$	$\sqrt{6}$	$\sqrt{-6}$

Avec ces choix d'uniformisantes, si K est dans Ω_1, on vérifie que l'on a

$$2 \equiv \pi^2+\pi^3 \pmod 4 \quad \text{et} \quad -1 \equiv 1+\pi^2+\pi^3 \pmod 4. \tag{9}$$

De même, si K est dans Ω_2, on a

$$2 \equiv \pi^2 \pmod 4 \quad \text{et} \quad -1 \equiv 1+\pi^2 \pmod 4. \tag{10}$$

Remarque. On vérifie que le développement de Hensel de 2 modulo 4 est indépendant du choix de l'uniformisante de K.

On rappelle que l'on a posé

$$\varepsilon = 3 \cdot \left(\frac{2}{\pi^2}\right)^2. \tag{11}$$

Lemme 10 *On a*

$$\varepsilon \equiv \begin{cases} 1 \pmod 4 & \text{si } K \in \Omega_1 \\ -1 \equiv 1+\pi^2 \pmod 4 & \text{si } K \in \Omega_2. \end{cases}$$

En particulier, $\varepsilon \equiv 1 \pmod 2$.

Démonstration : D'après les congruences (9) et (10), on a

$$\frac{2}{\pi^2} \equiv \begin{cases} 1+\pi \pmod 2 & \text{si } K \in \Omega_1 \\ 1 \pmod 2 & \text{si } K \in \Omega_2. \end{cases}$$

D'où le résultat en élevant au carré.

3.2 Carrés dans l'extension quadratique non ramifiée de K

Par unicité d'une extension quadratique non ramifiée de K dans $\overline{K}$, on a $N = K(\zeta)$ où ζ est une racine primitive cubique de l'unité dans $\overline{K}$.

Lemme 11 *Soit x une unité de l'anneau d'entiers de $K(\zeta)$ congrue modulo 4 à l'un des éléments suivants :*

$$1+\zeta\pi^2, \quad 1+\zeta^2\pi^2, \quad 1+\zeta\pi^2+\zeta\pi^3, \quad 1+\zeta^2\pi^2+\zeta^2\pi^3.$$

Alors, x n'est pas un carré dans K_{nr}.

Démonstration : On raisonne par l'absurde. D'après le lemme 2, il existe un élément y dans l'unique extension quadratique non ramifiée N' de $K(\zeta)$ tel que

$$x \equiv y^2 \pmod{4\mathcal{O}_{N'}}.$$

Notons $\mathcal{R}$ un système de représentants du corps résiduel de N' contenant l'ensemble $\{0, 1, \zeta, \zeta^2\}$. Le développement de Hensel de y modulo 2 s'écrit :

$$y \equiv a_0 + a_1\pi \pmod{2\mathcal{O}_{N'}},$$

avec $a_0 \in \mathcal{R} \setminus \{0\}$ et $a_1 \in \mathcal{R}$. Les éléments 2 et π^2 de K étant associés, on en déduit

$$x \equiv y^2 \equiv a_0^2 + a_1^2\pi^2 + a_0a_1\pi^3 \pmod{4\mathcal{O}_{N'}}. \tag{12}$$

Par unicité du développement de Hensel, on a,

$$a_0^2 = 1 \quad \text{et} \quad a_1^2 = \zeta \text{ ou } \zeta^2.$$

Or, les polynômes X^2-1, $X^2-\zeta$ et $X^2-\zeta^2$ de $\mathcal{O}_{K(\zeta)}[X]$ ont toutes leurs racines dans $\mathcal{O}_{K(\zeta)}$. On en déduit donc :

$$a_0 = 1 \quad \text{et} \quad a_1 = \zeta \text{ ou } \zeta^2.$$

En substituant ces valeurs dans l'équation (12), on obtient $x \equiv 1+\zeta\pi^2+\zeta^2\pi^3 \pmod 4$ ou $x \equiv 1+\zeta^2\pi^2+\zeta\pi^3 \pmod 4$. D'où une contradiction et le lemme.

3.3 Carrés dans l'extension cubique $K(\pi_0)$

Lemme 12 *Soit x une unité des entiers de $K(\pi_0)$ congrue modulo 4 à l'un des éléments suivants*

$$1+\pi_0^8, \quad 1+\pi_0^4+\pi_0^7+\pi_0^8, \quad 1+\pi_0^4+\pi_0^7+\pi_0^8+\pi_0^{10}, \quad 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k,$$

où h et k sont, soit nuls, soit des sommes de puissances >0 de π_0^3. Alors, x n'est pas un carré dans $K_{nr}(\pi_0)$.

Démonstration : On raisonne par l'absurde. L'extension $K(\pi_0)/\mathbf{Q}_2$ étant totalement ramifiée, il existe, d'après le lemme 3, un élément y de $\mathcal{U}_{K(\pi_0)}$ tel que $x \equiv y^2 \pmod{4\mathcal{O}_{K(\pi_0)}}$. Notons $1+a_1\pi_0+a_2\pi_0^2+a_3\pi_0^3+a_4\pi_0^4+a_5\pi_0^5$, avec $a_i=0$ ou 1, le développement de Hensel de y modulo 2. On a

$$x \equiv y^2 \equiv 1+a_1^2\pi_0^2+a_2^2\pi_0^4+a_3^2\pi_0^6+a_4^2\pi_0^8+a_5^2\pi_0^{10}+2a_1\pi_0+2a_2\pi_0^2+2a_3\pi_0^3$$
$$+2a_4\pi_0^4+2a_5\pi_0^5+2a_1a_2\pi_0^3+2a_1a_3\pi_0^4+2a_1a_4\pi_0^5+2a_2a_3\pi_0^5 \pmod{4\mathcal{O}_{K(\pi_0)}}.$$

Si $x \equiv 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k \pmod 4$, alors, par unicité du développement de Hensel, on a $a_1=a_2=1$. Si $a_3=1$, le coefficient devant π_0^6 dans le membre de droite de la congruence ci-dessus est non nul, ce qui est absurde. On a donc $a_3=0$. Or, $2 \equiv \pi_0^6 \pmod{\pi_0^9}$ car $2 \equiv \pi^2 \pmod{\pi^3}$· D'où

$$x \equiv 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k \equiv 1+\pi_0^2+\pi_0^4+\pi_0^7+(a_4+1)\pi_0^8+\pi_0^9+a_5\pi_0^{10} \pmod 4$$

ce qui est à nouveau absurde car le coefficient devant π_0^9 est nul dans le membre de gauche et non nul dans celui de droite.

Donc nécessairement, $x \not\equiv 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k \pmod 4$ et $a_1=0$. Autrement dit, le coefficient de π_0^7 dans le développement de x est nul. On en déduit $x \equiv 1+\pi_0^8 \pmod 4$, i.e. $a_1=a_2=a_3=0$. Comme 2 est associé à π_0^6, il vient alors :

$$x \equiv 1+a_4\pi_0^8+a_5^2\pi_0^{10}+2a_4\pi_0^4+2a_5\pi_0^5 \pmod 4 \quad \text{et} \quad a_4=a_5=1.$$

Puis, comme $2 \equiv \pi_0^6 \pmod{\pi_0^9}$, on a $x \equiv 1+\pi_0^8+\pi_0^{11} \pmod 4$. D'où la contradiction et le lemme.

Lemme 13 *L'unité $1+\pi_0^8+\pi_0^{11}$ est un carré dans $K_{nr}(\pi_0)$. On a les équivalences suivantes :*

$$1+\pi_0^4+\pi_0^8+\pi_0^{10} \text{ est un carré dans } K_{nr}(\pi_0) \Longleftrightarrow K \in \Omega_1$$

et

$$1+\pi_0^4+\pi_0^8 \text{ est un carré dans } K_{nr}(\pi_0) \Longleftrightarrow K \in \Omega_2.$$

Démonstration : D'après la relation $2 \equiv \pi^2 \pmod{\pi^3}$, on a $2 \equiv \pi_0^6 \pmod{\pi_0^9}$, d'où

$$1+\pi_0^8+\pi_0^{11} \equiv (1+\pi_0^4+\pi_0^5)^2 \pmod 4$$

et le fait que $1+\pi_0^8+\pi_0^{11}$ est un carré dans $K_{nr}(\pi_0)$ (lemme 2). Par ailleurs, on a

$$(1+\pi_0^4+\pi_0^8+\pi_0^{10})(1+\pi_0^4+\pi_0^8) \equiv 1+\pi_0^8 \pmod 4$$

et $1+\pi_0^8$ n'est pas un carré dans $K_{nr}(\pi_0)$ d'après le lemme précédent. Autrement dit, si l'un des éléments $1+\pi_0^4+\pi_0^8+\pi_0^{10}$ et $1+\pi_0^4+\pi_0^8$ est un carré dans $K_{nr}(\pi_0)$, alors l'autre ne l'est pas.

Si $K \in \Omega_1$, d'après la relation (9), on a

$$1+\pi_0^4+\pi_0^8+\pi_0^{10} \equiv (1+\pi_0^2+\pi_0^5)^2 \pmod 4.$$

Donc $1+\pi_0^4+\pi_0^8+\pi_0^{10}$ est un carré dans $K_{nr}(\pi_0)$ et $1+\pi_0^4+\pi_0^8$ ne l'est pas.

Si $K \in \Omega_2$, d'après la relation (10), on a

$$1+\pi_0^4+\pi_0^8 \equiv (1+\pi_0^2)^2 \pmod 4.$$

Donc $1+\pi_0^4+\pi_0^8$ est un carré dans $K_{nr}(\pi_0)$ et $1+\pi_0^4+\pi_0^8+\pi_0^{10}$ ne l'est pas.

D'où les équivalences annoncées.

3.4 Carrés dans une extension quadratique ramifiée de K

D'après le lemme 8, l'unité $1+\pi^3$ de K n'est pas un carré dans K_{nr}. Notons γ une solution dans $\overline{K}$ de l'équation à coefficients dans $\mathcal{O}_K$

$$X^2 - \frac{2}{\pi}X - \pi = 0. \tag{13}$$

Lemme 14 *L'élément γ est une uniformisante de l'extension $K(\sqrt{1+\pi^3})/K$ et on a*

$$\pi \equiv \gamma^2+\gamma^3 \pmod 2.$$

Démonstration : D'après l'équation (13), on a $v(\gamma)=1/2$ et $\gamma \in K(\sqrt{1+\pi^3})$. Donc γ est bien une uniformisante de l'extension $K(\sqrt{1+\pi^3})/K$. Par ailleurs, on a $\gamma^2 = (2/\pi)\gamma+\pi$, donc $\gamma^3 = (4/\pi^2)\gamma+2+\pi\gamma$. D'où

$$\gamma^2+\gamma^3 \equiv \frac{2}{\pi}\gamma+\pi+\pi\gamma \equiv \pi \pmod 2,$$

car $4/\pi^2 \equiv 2/\pi+\pi \equiv 0 \pmod 2$. D'où le lemme.

Lemme 15 *Soient x un élément de $\mathcal{U}_K$ et $\sqrt{x}$ une racine carrée de x dans $\overline{K}$. On suppose $x \equiv 1+\pi^3 \pmod 4$. Alors, $K_{nr}(\sqrt{x}) = K_{nr}(\sqrt{1+\pi^3})$ et $\sqrt{x} \equiv 1+\gamma^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{x})}}$.*

Démonstration : La première assertion résulte du lemme 1. D'après le lemme 14, γ est une uniformisante de $K(\sqrt{1+\pi^3})/K$. Notons $a_0+a_1\gamma+a_2\gamma^2+a_3\gamma^3$, avec $a_i = 0$ ou 1, le développement de Hensel de $\sqrt{x}$ modulo 2 (il est indépendant du choix de la racine carrée). Alors, d'après le lemme 14, on a $\pi^2 \equiv \gamma^4+\gamma^6$

(mod 4), $\pi^3 \equiv \gamma^6+\gamma^7 \pmod 4$ puis, comme 2 est associé à π^2, $2 \equiv \gamma^4 \pmod{\gamma^6}$. Donc

$$\begin{aligned} 1+\gamma^6 \equiv x &\equiv a_0^2 + a_1^2\gamma^2 + a_2^2\gamma^4 + a_3^2\gamma^6 + 2a_0a_1\gamma + 2a_0a_2\gamma^2 \pmod{\gamma^7} \\ &\equiv a_0^2 + a_1^2\gamma^2 + a_2^2\gamma^4 + a_0a_1\gamma^5 + (a_3^2 + a_0a_2)\gamma^6 \pmod{\gamma^7}. \end{aligned}$$

Par unicité du développement de Hensel, on en déduit :

$$a_0 = 1, \quad a_1 = a_2 = 0 \quad \text{et} \quad a_3 = 1.$$

D'où le lemme.

Lemme 16 *Soit x une unité des entiers de $K(\sqrt{1+\pi^3})$. On suppose que x vérifie l'une des deux conditions suivantes :*

1. *l'unité x est congrue modulo 4 à l'un des quatre éléments*

$$1+\gamma^4+\gamma^6+\gamma^7, \quad 1+\gamma^4, \quad 1+\gamma^6, \quad 1+\gamma^7;$$

2. *on a $x \equiv 1+\gamma^2+\gamma^3 \pmod 2$.*

Alors, x n'est pas un carré dans $K_{nr}(\sqrt{1+\pi^3})$.

Démonstration : On raisonne par l'absurde. L'extension $K(\sqrt{1+\pi^3})/\mathbf{Q}_2$ étant totalement ramifiée, il existe, d'après le lemme 3, une unité y des entiers de $K(\sqrt{1+\pi^3})$ telle que $x \equiv y^2 \pmod 4$. Notons $1+a_1\gamma+a_2\gamma^2+a_3\gamma^3$, avec $a_i = 0$ ou 1, le développement de Hensel de y modulo 2. On a alors

$$x \equiv y^2 \equiv 1 + a_1^2\gamma^2 + a_2^2\gamma^4 + 2a_1\gamma + a_3^2\gamma^6 + 2a_2\gamma^2 + 2a_3\gamma^3 \pmod 4.$$

Par unicité du développement de Hensel, x ne vérifie pas la seconde condition (le coefficient de γ^3 est nul). Il vient alors $a_1 = 0$, puis

$$x \equiv 1 + a_2^2\gamma^4 + a_3^2\gamma^6 + 2a_2\gamma^2 + 2a_3\gamma^3 \pmod 4.$$

Or, on a $2 \equiv \gamma^4 \pmod{\gamma^6}$ car $2 \equiv \pi^2 \pmod{\pi^3}$. Donc

$$x \equiv \begin{cases} 1 \pmod 4 & \text{si } (a_2,a_3) = (0,0) \\ 1+\gamma^4+\gamma^6 \pmod 4 & \text{si } (a_2,a_3) = (1,0) \\ 1+\gamma^6+\gamma^7 \pmod 4 & \text{si } (a_2,a_3) = (0,1) \\ 1+\gamma^4+\gamma^7 \pmod 4 & \text{si } (a_2,a_3) = (1,1). \end{cases}$$

D'où la contradiction et le résultat.

3.5 Carrés dans $K_{nr}(\sqrt{3})$

D'après le lemme 8 et les relations (9) et (10), 3 est un carré dans K_{nr} si et seulement si K est dans Ω_1. Notons $\sqrt{3}$ une racine carrée de 3 dans $\overline{K}$. Soient x un élément de $\mathcal{U}_K$ et $\sqrt{x}$ une racine carrée de x dans $\overline{K}$.

Lemme 17 *Supposons $K \in \Omega_1$ et $x \equiv 3 \pmod 4$. Alors, on a*

$$\sqrt{3} \equiv \sqrt{x} \equiv 1 + \pi \pmod{2\mathcal{O}_{K_{nr}}}.$$

Démonstration : Supposons $v(\sqrt{3} - \sqrt{x}) < 2$. Alors, d'après l'égalité, $\sqrt{3} + \sqrt{x} = \sqrt{3} - \sqrt{x} + 2\sqrt{x}$, on a $v(\sqrt{3} - \sqrt{x}) = v(\sqrt{3} + \sqrt{x}) < 2$ puis $v(3 - x) < 4$ ce qui est absurde. D'où, $v(\sqrt{3} - \sqrt{x}) \geq 2$ ou, autrement dit, $\sqrt{3} \equiv \sqrt{x} \pmod{2\mathcal{O}_{K_{nr}}}$. L'extension $K(\sqrt{x})/K$ est non ramifiée (elle est même éventuellement triviale). En particulier, on peut choisir un système de représentants $\mathcal{R}$ du corps résiduel de $K(\sqrt{x})$ contenu dans $\{0, 1, \zeta, \zeta^2\}$. Notons alors $a_0 + a_1\pi$ le développement de Hensel modulo $2\mathcal{O}_{K_{nr}}$ de $\sqrt{x}$. On a $a_0, a_1 \in \mathcal{R} \subset \{0, 1, \zeta, \zeta^2\}$. Puis, d'après la relation (9),

$$3 \equiv 1 + \pi^2 + \pi^3 \equiv a_0^2 + a_1^2\pi^2 + a_0a_1\pi^3 \pmod{4\mathcal{O}_{K_{nr}}}.$$

Par unicité du développement de Hensel, on en déduit, $a_0 = a_1 = 1$. D'où le lemme.

On suppose désormais $K \in \Omega_2$ de sorte que 3 n'est pas un carré dans K_{nr}.

Lemme 18 *Supposons $K \in \Omega_2$. L'unité x est un carré dans $K_{nr}(\sqrt{3})$ si et seulement si $x \equiv 1 \pmod 2$.*

Démonstration : Supposons que x soit un carré dans $K_{nr}(\sqrt{3})$. Il existe alors a et b deux éléments de K_{nr} tels que $x = (a + b\sqrt{3})^2$. Puis, comme $(1, \sqrt{3})$ est une base de l'extension $K_{nr}(\sqrt{3})/K_{nr}$, on a $x = a^2 + 3b^2$ et $ab = 0$. Si $b = 0$, on en déduit que x est un carré dans K_{nr} et si $a = 0$ que $x/3$ est un carré dans K_{nr}. Réciproquement, si x ou $x/3$ est un carré dans K_{nr}, alors x est un carré dans $K_{nr}(\sqrt{3})$. Par ailleurs, d'après le lemme 8, x est un carré dans K_{nr} si et seulement si $x \equiv 1 \pmod 4$ ou $x \equiv 1 + \pi^2 + \pi^3 \pmod 4$. De plus, d'après la relation (10), on a $3 \equiv 1 + \pi^2 \pmod 4$. Donc, d'après le lemme 8, $x/3$ est un carré dans K_{nr} si et seulement si $x \equiv 1 + \pi^2 \pmod 4$ ou $x \equiv 1 + \pi^3 \pmod 4$. On en déduit le résultat avec l'équivalence précédente.

Notons η une uniformisante de $K(\sqrt{3})$. C'est une extension quadratique de K.

Lemme 19 *Supposons $K \in \Omega_2$ et $x \equiv 3 \pmod 4$. Alors, $K_{nr}(\sqrt{x}) = K_{nr}(\sqrt{3})$ et on a*

$$\pi \equiv \eta^2 + \eta^3 \pmod{2\mathcal{O}_{K(\sqrt{3})}} \quad \textit{et} \quad \sqrt{x} \equiv \sqrt{3} \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}$$

Démonstration : L'égalité résulte du lemme 1. L'extension $K(\sqrt{3})/K$ étant totalement ramifiée, π est associé à η^2 et on a

$$\pi \equiv \eta^2 \pmod{2\mathcal{O}_{K(\sqrt{3})}} \quad \text{ou} \quad \pi \equiv \eta^2 + \eta^3 \pmod{2\mathcal{O}_{K(\sqrt{3})}}.$$

Dans les deux cas, on a, d'après la relation (10), $2 \equiv \eta^4 \pmod{\eta^6}$. Notons $a_0 + a_1\eta + a_2\eta^2 + a_3\eta^3$, avec $a_i = 0$ ou 1, le développement de Hensel de $\sqrt{3}$

modulo 2. D'après la relation (10), on a alors :

$$3 \equiv 1 + \pi^2 \equiv a_0^2 + a_1^2\eta^2 + a_2^2\eta^4 + a_3^2\eta^6 + 2a_0a_1\eta + 2a_0a_2\eta^2 + 2a_0a_3\eta^3 + 2a_1a_2\eta^3 \pmod 4.$$

Par unicité du développement de Hensel, comme π^2 est associé à η^4, il vient $a_0 = 1$, $a_1 = 0$ et $a_2 = 1$. D'où, comme $2 \equiv \eta^4 \pmod{\eta^6}$,

$$\begin{aligned} 3 &\equiv 1 + \eta^4 + (a_3^2 + 1)\eta^6 + a_3\eta^7 \pmod 4 \\ &\equiv \begin{cases} 1 + \eta^4 + \eta^6 \pmod 4 & \text{si } a_3 = 0, \\ 1 + \eta^4 + \eta^7 \pmod 4 & \text{si } a_3 = 1. \end{cases} \end{aligned} \tag{14}$$

Supposons $\pi \equiv \eta^2 \pmod 2$. Alors, d'après la relation (10), on a $2 \equiv \pi^2 \equiv \eta^4 \pmod 4$ et donc, $3 \equiv 1 + \eta^4 \pmod 4$. D'après (14), c'est une contradiction. On a donc nécessairement,

$$\pi \equiv \eta^2 + \eta^3 \pmod{2\mathcal{O}_{K(\sqrt{3})}}.$$

D'où, $2 \equiv \eta^4 + \eta^6 \pmod{4\mathcal{O}_{K(\sqrt{3})}}$ et, en remplacant dans (14),

$$1 + \eta^4 + \eta^6 \equiv 1 + \eta^4 + (a_3^2 + 1)\eta^6 + a_3\eta^7 \pmod 4.$$

On en déduit $a_3 = 0$. D'où $\sqrt{3} \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K(\sqrt{3})}}$.

Supposons $v(\sqrt{3} - \sqrt{x}) < 2$. Alors, d'après l'égalité, $\sqrt{3} + \sqrt{x} = \sqrt{3} - \sqrt{x} + 2\sqrt{x}$, on a $v(\sqrt{3} - \sqrt{x}) = v(\sqrt{3} + \sqrt{x}) < 2$ puis $v(3 - x) < 4 = v(4)$ ce qui est absurde. D'où, $v(\sqrt{3} - \sqrt{x}) \geq 2$ ou, autrement dit, $\sqrt{3} \equiv \sqrt{x} \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}$. D'où le lemme.

Lemme 20 *Supposons $K \in \Omega_2$. L'unité $3+2\sqrt{3}$ de l'anneau d'entiers de $K(\sqrt{3})$ n'est pas un carré dans $K_{nr}(\sqrt{3})$.*

Démonstration : L'extension $K(\sqrt{3})/\mathbf{Q}_2$ est totalement ramifiée. Supposons que $3 + 2\sqrt{3}$ soit un carré dans $K_{nr}(\sqrt{3})$. Alors, d'après le lemme 3, il existe une unité y des entiers de $K(\sqrt{3})$ telle que $3 + 2\sqrt{3} \equiv y^2 \pmod{4\mathcal{O}_{K(\sqrt{3})}}$. Or, d'après le lemme 19, on a $3 + 2\sqrt{3} \equiv 1 + 2\eta^2 \equiv 1 + \eta^6 \pmod 4$. Notons $a_0 + a_1\eta + a_2\eta^2 + a_3\eta^3$, avec $a_i = 0$ ou 1, le développement de Hensel de y modulo 2. En utilsant la relation $2 \equiv 1 + \eta^4 + \eta^6 \pmod 4$ déduite du lemme 19 et de la relation (10), on a

$$3 + 2\sqrt{3} \equiv 1 + \eta^6 \equiv a_0^2 + a_1^2\eta^2 + a_2^2\eta^4 + a_0a_1\eta^5 + (a_3^2 + a_0a_2)\eta^6 + (a_0a_1 + a_0a_3 + a_1a_2)\eta^7 \pmod{4\mathcal{O}_{K(\sqrt{3})}}.$$

Par unicité du développement de Hensel, il vient $a_0 = 1$, $a_1 = 0$ et $a_2 = 0$. On a donc

$$1 + \eta^6 \equiv 1 + a_3^2\eta^6 + a_3\eta^7 \pmod{4\mathcal{O}_{K(\sqrt{3})}}.$$

D'où une contradiction car $a_3 = 0$ ou 1. D'où le lemme.

Lemme 21 *Soit y une unité des entiers de $K(\sqrt{3})$. On suppose que y est un carré dans $K_{nr}(\sqrt{3})$. Alors,*

$$y \equiv 1 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}} \quad ou \quad y \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$

DÉMONSTRATION : L'extension $K(\sqrt{3})/\mathbf{Q}_2$ est totalement ramifiée. Comme y est un carré dans $K_{nr}(\sqrt{3})$, il existe d'après le lemme 3, une unité z des entiers de $K(\sqrt{3})$ telle que $y \equiv z^2 \pmod 4$. Notons $1 + a_1\eta$, avec $a_1 = 0$ ou 1, le développement de Hensel de z modulo η^2. Alors,

$$y \equiv z^2 \equiv 1 + a_1^2\eta^2 \pmod{2\mathcal{O}_{K(\sqrt{3})}}.$$

D'où le lemme car $a_1 = 0$ ou 1.

3.6 Notations et préliminaires aux démonstrations

On reprend les notations introduites aux sections précédentes en explicitant le choix de la racine cubique $\Delta^{1/3}$ de Δ. D'après le lemme de Hensel appliqué au polynôme $X^3 - \Delta'$ de $\mathcal{O}_K[X]$, Δ' possède une unique racine cubique dans K. On la note δ. On choisit alors de prendre

$$\Delta^{1/3} = \pi_0^{v(\Delta)}\delta$$

de sorte que si $v(\Delta) \equiv 0 \pmod 3$, on a $\Delta^{1/3} \in K$. Notons θ l'unité de K définie par

$$\theta = \varepsilon\frac{\delta}{c_4'}. \tag{15}$$

On choisit une racine $B^{1/2}$ de B dans $\overline{K}$ et on pose

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

Alors,

$$\frac{C}{\pi^{v(c_4)}} = c_4'\left[2\left(1 + \frac{B^{1/2}}{c_4}\right) + \theta\pi_0^{12-v(j)}\right] \tag{16}$$

est une unité de $K(B^{1/2})$.

3.6.1 Cas où $v(j) < 12$

On a, pour t dans μ_3,

$$\frac{B_t}{c_4^2} = 1 + 12tj^{-1/3} + 144t^2j^{-2/3} = 1 + t\theta\pi_0^{12-v(j)} + (t\theta\pi_0^{12-v(j)})^2, \tag{17}$$

car $12j^{-1/3} = 3(2/\pi^2)^2\pi_0^{12-v(j)}\delta/c_4' = \theta\pi_0^{12-v(j)}$.

Par ailleurs, l'égalité $c_4^3 - c_6^2 = 1728\Delta$ s'écrit

$$\pi^{3v(c_4)}c_4'^3 - \pi^{2v(c_6)}c_6'^2 = 3^3 \cdot 2^6\pi^{v(\Delta)}\Delta',$$

puis

$$c_4'^3 - c_6'^2 = \varepsilon^3 \pi^{12-v(j)} \Delta', \tag{18}$$

car $2v(c_6) = 3v(c_4)$. D'où

$$1 - \frac{c_6'^2}{c_4'^3} = \left(\theta \pi_0^{12-v(j)}\right)^3. \tag{19}$$

Lemme 22 *Supposons $v(j) \leq 8$. Alors,*

$$c_4' \equiv c_4'^3 \equiv c_6'^2 \pmod 4.$$

Démonstration : En réduisant l'égalité (19) modulo 2, on en déduit avec le lemme 7, $c_4' \equiv 1 \pmod 2$, puis $c_4' \equiv c_4'^3 \pmod 4$. Les congruences annoncées résultent alors de la même égalité réduite modulo 4, car $v(j) \leq 8$.

3.6.2 Cas où $v(j) = 12$

Pour t dans μ_3, on a

$$\frac{B_t}{c_4^2} = 1 + 12tj^{-1/3} + 144t^2 j^{-2/3} = 1 + t\theta + (t\theta)^2. \tag{20}$$

Le corps K étant totalement ramifié, pour $t = 1$, B/c_4^2 est une unité de $\mathcal{O}_K$.

Par ailleurs, l'égalité $c_4^3 - c_6^2 = 1728\Delta$ s'écrit comme à la relation (19),

$$1 - \pi^{2v(c_6)-3v(c_4)} \frac{c_6'^2}{c_4'^3} = \theta^3. \tag{21}$$

La somme de deux unités n'en étant pas une, on a $2v(c_6) - 3v(c_4) > 0$.

3.6.3 Cas où $v(j) > 12$

On considère alors la courbe $\widetilde{E}$ d'équation (2). Son invariant modulaire $\widetilde{j}$ est de valuation $v(\widetilde{j}) = 24 - v(j) < 12$.

Lemme 23 *On a*

$$\widetilde{\Delta}' \equiv c_4' \pmod 2 \quad \textit{et} \quad j' \cdot \widetilde{j}' \equiv 1 \pmod 4.$$

Démonstration : Cela résulte des lemmes 6 et 7.

3.7 Démonstration du théorème 2

L'assertion 1 du théorème 2 résulte de l'assertion (i) de [2, th.2]. L'assertion 11 résulte de l'assertion (iv) de [2, th.2] et de la proposition 13. On suppose donc désormais que l'on a $1 \leq v(j) \leq 23$. D'où en particulier, $j \neq 0$.

L' assertion 2 lorsque $v(j) \neq 10$ et $v(j) \neq 14$ ainsi que l'assertion 3 résultent directement du théorème 1.

Démontrons à présent les autres assertions du théorème 2 (la détermination des types de Néron est reportée à la section 3.8).

3.7.1 Démonstration de l'assertion 2 lorsque $v(j) = 10$ ou 14

Supposons $v(j) = 10$. On vérifie, avec la relation (17) que l'on a

$$\frac{B}{c_4^2} = 1 + \theta\pi_0^2 + (\theta\pi_0^2)^2.$$

Or, $\varepsilon \equiv \pm 1 \pmod 4$ (lemme 10), donc, d'après la relation (15), $\theta \equiv \pm\delta/c_4' \pmod 4$. D'après les relations (9) et (10), on a alors

$$\frac{B}{c_4^2} \equiv 1 + \pi_0^2 + \pi_0^4 + \pi_0^2 h + \pi_0^4 k \pmod 4,$$

où h et k sont, soit nuls, soit des sommes de puissances > 0 de π_0^3. D'après le lemme 12, B n'est pas un carré dans M. D'où $|\Phi| = 24$ dans ce cas d'après [2, th.3(ii)].

Supposons $v(j) = 14$. Alors, la courbe $\widetilde{E}$ d'équation (2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 10$. Autrement dit, $\widetilde{B}$ n'est pas un carré dans M. D'après la proposition 1, il en va de même pour B et donc $|\Phi| = 24$ d'après [2, th.3(ii)].

3.7.2 Démonstration de l'assertion 4

On suppose $v(j) = 4$.

Lemme 24 *On a*

$$\frac{B}{c_4^2} \equiv 1 + \pi_0^8\Delta' \pmod 4.$$

De plus, B est un carré dans M si et seulement si $\Delta' \equiv 1 + \pi \pmod 2$.

Démonstration : D'après les lemmes 7 et 10, on a

$$\varepsilon \equiv 1 \pmod 2 \quad \text{et} \quad \delta \equiv \Delta' \pmod 2.$$

De plus, d'après les lemmes 7 et 22, on a $c_4' \equiv c_6'^2 \equiv 1 \pmod 2$. D'où, $\theta \equiv \Delta' \pmod 2$, puis $\theta\pi_0^8 \equiv \pi_0^8\Delta' \pmod 4$. La congruence annoncée résulte alors de l'égalité (17) appliquée à $t = 1$. On en déduit que B est un carré dans M si et seulement si l'unité $1 + \pi_0^8\Delta'$ de l'anneau des entiers de $K(\pi_0)$ l'est (lemme 1). Or,

$$1 + \pi_0^8\Delta' \equiv \begin{cases} 1 + \pi_0^8 \pmod 4 & \text{si } \Delta' \equiv 1 \pmod 2 \\ 1 + \pi_0^8 + \pi_0^{11} \pmod 4 & \text{si } \Delta' \equiv 1 + \pi \pmod 2. \end{cases}$$

On conclut à l'équivalence annoncée avec les lemmes 12 et 13.

Lorsque la condition (C1) n'est pas satisfaite, l'assertion 4 résulte du lemme précédent et de [2, th.3(*ii*)]. Lorsque la condition (C1) est satisfaite, l'assertion 4 se déduit alors du lemme précédent, de l'assertion (*ii*) de [2, th.3] et des propositions 4 et 5.

3.7.3 Démonstration de l'assertion 10

On suppose $v(j) = 20$. La courbe $\widetilde{E}$ d'équation (2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 4$. D'après la proposition 1, B est un carré dans M si seulement si $\widetilde{B}$ l'est. Or, d'après le lemme 24, c'est le cas si et seulement si $\widetilde{\Delta}' \equiv 1 + \pi \pmod 2$. D'après le lemme 23, c'est équivalent à dire $c_4' \equiv 1 + \pi \pmod 2$.

Lorsque la condition (C1') n'est pas satisfaite, l'assertion 10 résulte de l'équivalence ci-dessus et de l'assertion (ii) de [2, th.3]. Lorsque la condition (C1') est satisfaite, l'assertion 10 se déduit alors de l'équivalence ci-dessus, de l'assertion (ii) de [2, th.3] et de la proposition 11.

3.7.4 Démonstration de l'assertion 5

On suppose $v(j) = 6$.

Lemme 25 *On a, pour tout $t \in \mu_3$,*

$$\frac{B_t}{c_4^2} \equiv 1 + t\Delta'\pi^2 \pmod 4.$$

De plus, B_t est un carré dans K_{nr} si seulement si

$$t = 1 \quad et \quad \Delta' \equiv 1 + \pi \pmod 2.$$

Démonstration : D'après le lemme 10, on a $\varepsilon \equiv 1 \pmod 2$ et d'après le lemme 7, $\delta \equiv \Delta' \pmod 2$. Puis d'après le lemme 22, $c_4' \equiv c_6'^2 \equiv 1 \pmod 2$. On en déduit $\theta \equiv \Delta' \pmod 2$. D'où la congruence annoncée avec la relation (17). De plus, B_t est un carré dans K_{nr} si et seulement si l'unité $1+t\Delta'\pi^2$ de N l'est. Supposons que tel soit le cas. Alors, comme $\Delta' \equiv 1$ ou $1 + \pi \pmod 2$, on a, d'après le lemme 11, $t = 1$, puis $\Delta' \equiv 1 + \pi \pmod 2$. Réciproquement, si $t = 1$ et $\Delta' \equiv 1 + \pi \pmod 2$, alors $1 + t\Delta'\pi^2 \equiv (1 + \pi)^2 \pmod 4$ et $B = B_1$ est un carré dans K_{nr}. D'où le lemme.

Supposons $\Delta' \equiv 1 + \pi \pmod 2$. Alors, d'une part, d'après le lemme précédent, $B = B_1$ est un carré dans K_{nr}, donc $|\Phi| = 2$ ou 4, d'après [2, th.3(i)]. D'autre part, B_t pour $t \neq 1$, n'est pas un carré dans K_{nr}, donc $|\Phi| = 4$ ou 8 (*loc. cit.*). On en déduit que nécessairement, $|\Phi| = 4$.

Supposons $\Delta' \not\equiv 1 + \pi \pmod 2$. Alors, d'après le lemme précédent, pour tout $t \in \mu_3$, B_t n'est pas un carré dans K_{nr}. Donc d'après la proposition 2, on a $|\Phi| = 8$ (on a $c_6 \neq 0$ car $v(j) \neq 12$).

3.7.5 Démonstration de l'assertion 9

Supposons $v(j) = 18$. La courbe $\widetilde{E}$ d'équation (2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 6$. D'après la proposition 1, si $t \in \mu_3$, B_t est un carré dans K_{nr} si seulement si $\widetilde{B}_{t^2}$ l'est. Or, d'après le lemme 25, on a

$$\widetilde{B}_{t^2} \in {K_{nr}}^2 \Longleftrightarrow t = 1 \quad \text{et} \quad \widetilde{\Delta}' \equiv 1 + \pi \pmod 2.$$

D'après le lemme 23, on en déduit l'équivalence

$$B_t \in {K_{nr}}^2 \Longleftrightarrow t = 1 \quad \text{et} \quad c'_4 \equiv 1 + \pi \pmod 2.$$

L'assertion 9 résulte alors, comme au paragraphe précédent, de l'équivalence ci-dessus et de l'assertion (i) de [2, th.3].

3.7.6 Démonstration de l'assertion 6

Supposons $v(j) = 8$.

Lemme 26 *On a*

$$\frac{B}{c_4^2} \equiv 1 + \varepsilon j' \pi_0^4 + \pi_0^8 \pmod 4.$$

De plus, B est un carré dans M si et seulement si $j' \equiv 1 + \pi^2 \pmod{\pi^3}$.

Démonstration : L'élément c'_4/δ est une unité de K, donc d'après le lemme 7, on a

$$\left(\frac{c'_4}{\delta}\right)^4 \equiv 1 \pmod 4, \quad \text{d'où } j' = \frac{{c'_4}^3}{\delta^3} \equiv \frac{\delta}{c'_4} \pmod 4.$$

D'après les lemmes 10 et 7, on a

$$\varepsilon^2 {j'}^2 \pi_0^8 \equiv \pi_0^8 \pmod 4.$$

D'où la congruence annoncée d'après (17).

Supposons $K \in \Omega_1$. Alors, d'après le lemme 10, $\varepsilon \equiv 1 \pmod 4$. Donc

$$\frac{B}{c_4^2} \equiv \begin{cases} 1 + \pi_0^4 + \pi_0^8 \pmod 4 & \text{si } j' \equiv 1 \pmod{\pi^3}, \\ 1 + \pi_0^4 + \pi_0^7 + \pi_0^8 \pmod 4 & \text{si } j' \equiv 1 + \pi \pmod{\pi^3}, \\ 1 + \pi_0^4 + \pi_0^8 + \pi_0^{10} \pmod 4 & \text{si } j' \equiv 1 + \pi^2 \pmod{\pi^3}, \\ 1 + \pi_0^4 + \pi_0^7 + \pi_0^8 + \pi_0^{10} \pmod 4 & \text{si } j' \equiv 1 + \pi + \pi^2 \pmod{\pi^3}. \end{cases}$$

On vérifie alors avec les lemmes 12 et 13 que B est un carré dans M si et seulement si $j' \equiv 1 + \pi^2 \pmod{\pi^3}$.

Supposons $K \in \Omega_2$. Alors, d'après le lemme 10, $\varepsilon \equiv -1 \equiv 1 + \pi^2 \pmod 4$. Donc

$$\frac{B}{c_4^2} \equiv \begin{cases} 1 + \pi_0^4 + \pi_0^8 + \pi_0^{10} \pmod 4 & \text{si } j' \equiv 1 \pmod{\pi^3}, \\ 1 + \pi_0^4 + \pi_0^7 + \pi_0^8 + \pi_0^{10} \pmod 4 & \text{si } j' \equiv 1 + \pi \pmod{\pi^3}, \\ 1 + \pi_0^4 + \pi_0^8 \pmod 4 & \text{si } j' \equiv 1 + \pi^2 \pmod{\pi^3}, \\ 1 + \pi_0^4 + \pi_0^7 + \pi_0^8 \pmod 4 & \text{si } j' \equiv 1 + \pi + \pi^2 \pmod{\pi^3}. \end{cases}$$

On vérifie alors avec les lemmes 12 et 13 que B est un carré dans M si et seulement si $j' \equiv 1 + \pi^2 \pmod{\pi^3}$. D'où le lemme.

Lorsque la condition (C2) n'est pas satisfaite, l'assertion 6 résulte du lemme ci-dessus et de l'assertion (ii) de [2, th.3]. Lorsque la condition (C2) est satisfaite, l'assertion 6 résulte alors du lemme ci-dessus, de l'assertion (ii) de [2, th.3] et de la proposition 7.

3.7.7 Démonstration de l'assertion 8

Supposons $v(j) = 16$. La courbe $\widetilde{E}$ d'équation (2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 8$. D'après la proposition 1, B est un carré dans M si seulement si $\widetilde{B}$ l'est. Or, d'après l'assertion 6 du théorème 2, c'est le cas si et seulement si $\widetilde{j}' \equiv 1 + \pi^2 \pmod{\pi^3}$. D'après le lemme 23, c'est équivalent à dire $j' \equiv 1 + \pi^2 \pmod{\pi^3}$ car on a $j' \equiv 1/\widetilde{j}' \pmod{\pi^3}$.

Lorsque la condition (C2) n'est pas satisfaite, l'assertion 8 résulte de l'équivalence ci-dessus et de l'assertion (ii) de [2, th.3]. Lorsque la condition (C2) est satisfaite, l'assertion 8 résulte alors de l'équivalence ci-dessus, de l'assertion (ii) de [2, th.3] et de la proposition 9.

3.7.8 Démonstration de l'assertion 7a

On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) = 1$.

Lemme 27 *On a, pour t dans μ_3,*

$$\theta \equiv 1 + \pi \pmod 2 \quad et \quad \frac{B_t}{c_4^2} \equiv 1 + t + t^2 + t\pi \pmod 2.$$

Démonstration : D'après la relation (21), on a $\theta^3 \equiv 1 + \pi \pmod 2$. Puis, d'après le lemme 7, on a $\theta^2 \equiv 1 \pmod 2$, d'où $\theta \equiv \theta^3 \equiv 1 + \pi \pmod 2$. La seconde congruence résulte alors de la première et de la relation (20). D'où le lemme.

Supposons $t = 1$. Alors, $B/c_4^2 \equiv 1 + \pi \pmod 2$. Donc, d'après le lemme 8, B n'est pas un carré dans K_{nr}.

Supposons $t \neq 1$. Alors, $v(B_t) = 1$ est impair. Donc, B_t n'est pas un carré dans K_{nr}.

Autrement dit, pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr} . D'après la proposition 2, on a $|\Phi| = 8$.

Cela démontre l'assertion 7a du théorème 2.

3.7.9 Démonstration de l'assertion 7b

On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) = 2$. En particulier, $v(c_4)$ est pair.

Lemme 28 *On a,*

$$\theta \equiv 1 + \pi^2 c_4' \pmod 4 \quad et \quad \frac{B}{c_4^2} \equiv 3 + \pi^2 c_4' \pmod 4.$$

Démonstration : D'après la relation (21), on a $\theta^3 \equiv 1 \pmod 2$. Donc, d'après le lemme 7, on a $\theta \equiv \theta^3 \equiv 1 + \pi^2 c_4' \pmod 4$. La seconde congruence résulte alors de la première et de l'égalité (20) appliquée à $t = 1$. D'où le lemme.

Lemme 29 *Supposons que l'une des deux conditions suivantes soit satisfaite :*

1. *on a* $K \in \Omega_1$ *et* $c_4' \equiv 1 + \pi \pmod 2$ *;*
2. *on a* $K \in \Omega_2$ *et* $c_4' \equiv 1 \pmod 2$.

Alors, $K_{nr}(B^{1/2}) = K_{nr}$*, puis*

$$\frac{B^{1/2}}{c_4} \equiv 1 \pmod{2\mathcal{O}_{K_{nr}}} \quad \textit{et} \quad \frac{C}{\pi^{v(c_4)}} \equiv c_4' + \pi^2 \pmod{4\mathcal{O}_{K_{nr}}}.$$

Démonstration : Sous ces hypothèses, on a, d'après les relations (9) et (10) et le lemme 28,

$$\frac{B}{c_4^2} \equiv 1 \pmod 4.$$

D'après le lemme 9, il vient $B^{1/2}/c_4 \equiv 1 \pmod{2\mathcal{O}_{K_{nr}}}$. En particulier,

$$\frac{B^{1/2}}{c_4} + 1 \equiv 0 \pmod{2\mathcal{O}_{K_{nr}}}.$$

Donc, d'après l'égalité (16), on a

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4'\theta \pmod{4\mathcal{O}_{K_{nr}}}.$$

Puis, d'après le lemme 28, $c_4'\theta \equiv c_4' + \pi^2 \pmod 4$. D'où le résultat annoncé.

On reprend les notations du §3.4. En particulier, γ est une uniformisante de $K(\sqrt{1+\pi^3})$.

Lemme 30 *Supposons que l'une des deux conditions suivantes soit satisfaite :*

1. *on a* $K \in \Omega_1$ *et* $c_4' \equiv 1 \pmod 2$ *;*
2. *on a* $K \in \Omega_2$ *et* $c_4' \equiv 1 + \pi \pmod 2$.

Alors, $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{1+\pi^3})$ *est une extension quadratique de* K_{nr}*, puis*

$$\frac{B^{1/2}}{c_4} \equiv 1 + \gamma^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{1+\pi^3})}}$$

et

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4' + \gamma^4 + \gamma^6 + \gamma^7 \pmod{4\mathcal{O}_{K_{nr}(\sqrt{1+\pi^3})}}.$$

Démonstration : Sous ces hypothèses, on a, d'après les relations (9) et (10) et le lemme 28,

$$\frac{B}{c_4^2} \equiv 1 + \pi^3 \pmod 4.$$

D'après le lemme 15, on a donc $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{1+\pi^3})$ et $B^{1/2}/c_4 \equiv 1+\gamma^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{1+\pi^3})}}$, d'où la première congruence. Puis, d'après l'égalité (16), on a

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4'(2\gamma^3 + \theta) \pmod{4\mathcal{O}_{K_{nr}}}.$$

Or, 2 est associé à γ^4, donc $2c'_4\gamma^3 \equiv \gamma^7 \pmod 4$. Et, d'après le lemme 14, on a $\pi^2 \equiv \gamma^4 + \gamma^6 \pmod 4$. Donc, d'après le lemme 28, on a $c'_4\theta \equiv c'_4 + \pi^2 \equiv c'_4 + \gamma^4 + \gamma^6 \pmod 4$. D'où le lemme.

On procède comme suit pour la fin de la démonstration de l'assertion 7b.

1. Supposons $K \in \Omega_1$. Si la condition (C1') est satisfaite, on est alors dans un cas d'application du lemme 29. En particulier, B est un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans K_{nr} si et seulement si l'unité $c'_4 + \pi^2$ de $\mathcal{O}_K$ l'est. Or, d'après le lemme 8, ce n'est jamais le cas car $c'_4 + \pi^2 \equiv 1 + \pi \pmod 2$ (condition (C1')). On en déduit que $|\Phi| = 4$ dans ce cas ([2, th.3(i)]).
   Si la condition (C1') n'est pas satisfaite, on est alors dans un cas d'application du lemme 30. En particulier, B n'est pas un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans $K_{nr}(B^{1/2})$ si et seulement si l'unité $c'_4 + \gamma^4 + \gamma^6 + \gamma^7$ des entiers de $K(\sqrt{1+\pi^3})$ l'est. Or, d'après le lemme 14, on a
$$c'_4+\gamma^4+\gamma^6+\gamma^7 \equiv \begin{cases} 1+\gamma^4+\gamma^6+\gamma^7 \pmod 4 & \text{si } c'_4 \equiv 1 \pmod 4, \\ 1+\gamma^7 \pmod 4 & \text{si } c'_4 \equiv 1+\pi^2 \pmod 4, \\ 1+\gamma^4 \pmod 4 & \text{si } c'_4 \equiv 1+\pi^3 \pmod 4, \\ 1+\gamma^6 \pmod 4 & \text{si } c'_4 \equiv 1+\pi^2+\pi^3 \pmod 4. \end{cases}$$
   D'après le lemme 16, C n'est donc pas un carré dans $K_{nr}(B^{1/2})$ et $|\Phi| = 8$ dans ce cas ([2, th.3(i)]).
2. Supposons $K \in \Omega_2$. Si la condition (C1') est satisfaite, on est alors dans un cas d'application du lemme 30. En particulier, B n'est pas un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans $K_{nr}(B^{1/2})$ si et seulement si l'unité $c'_4 + \gamma^4 + \gamma^6 + \gamma^7$ des entiers de $K(\sqrt{1+\pi^3})$ l'est. Or, $c'_4 + \gamma^4 + \gamma^6 + \gamma^7 \equiv c'_4 \equiv 1 + \gamma^2 + \gamma^3 \pmod 2$. Donc, d'après le lemme 16, C n'est pas un carré dans $K_{nr}(B^{1/2})$ et $|\Phi| = 8$ dans ce cas ([2, th.3(i)]).
   Si la condition (C1') n'est pas satisfaite, on est alors dans un cas d'application du lemme 29. En particulier, B est un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans K_{nr} si et seulement si l'unité $c'_4 + \pi^2$ de $\mathcal{O}_K$ l'est. Autrement dit, d'après le lemme 8, C est un carré dans K_{nr} si et seulement si $c'_4 \equiv 1 + \pi^2 \pmod 4$ ou $c'_4 \equiv 1 + \pi^3 \pmod 4$. D'après [2, th.3(i)], on a donc dans ce cas :
$$|\Phi| = \begin{cases} 2 & \text{si la condition (C3) est satisfaite,} \\ 4 & \text{sinon.} \end{cases}$$

Cela achève de démontrer l'assertion 7b du théorème 2.

3.7.10 Démonstration de l'assertion 7c

On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) = 3$.

Lemme 31 *On a, pour tout t dans μ_3,*

$$\theta \equiv 1 + \pi^3 \pmod 4 \quad et \quad \frac{B_t}{c_4^2} \equiv 1 + t + t^2 + t\pi^3 \pmod 4.$$

DÉMONSTRATION : D'après la relation (21), on a $\theta^3 \equiv 1 \pmod 2$ et d'après le lemme 7, $\theta^2 \equiv 1 \pmod 2$, d'où, $\theta \equiv 1 \pmod 2$. D'après *loc. cit.* et la relation (21) on a alors, $\theta \equiv \theta^3 \equiv 1 + \pi^3 \pmod 4$. La seconde congruence résulte alors de la première et de l'égalité (20). D'où le lemme.

On déduit du lemme 31 que pour $t \neq 1$ dans μ_3, $v(B_t) = 1$ est impair. En particulier, B_t n'est pas un carré dans K_{nr}.

On procède comme suit pour la fin de la démonstration de l'assertion 7c.

1. Supposons $K \in \Omega_1$. Alors, d'après le lemme 31 et la relation (9), on a

$$\frac{B}{c_4^2} \equiv 3 + \pi^3 \equiv 1 + \pi^2 \pmod 4.$$

   Autrement dit, d'après le lemme 8, B n'est pas un carré dans K_{nr}. Par suite, pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr}. D'après la proposition 2, cela implique $|\Phi| = 8$.

2. Supposons $K \in \Omega_2$. Alors, d'après le lemme 31 et la relation (10), on a

$$\frac{B}{c_4^2} \equiv 3 + \pi^3 \equiv 1 + \pi^2 + \pi^3 \pmod 4.$$

   Autrement dit, d'après le lemme 8, B est un carré dans K_{nr}. D'après [2, th.3(i)], on a donc $|\Phi| = 2$ ou 4. Or, pour $t \neq 1$ dans μ_3, B_t n'est pas un carré dans K_{nr}, donc $|\Phi| = 4$ ou 8 (*loc. cit.*). Cela implique que l'on a nécessairement $|\Phi| = 4$ dans ce cas.

Cela achève la démonstration de l'assertion 7c du théorème 2.

3.7.11 Démonstration de l'assertion 7d

On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) \geq 4$.

Lemme 32 *On a,*

$$\theta \equiv 1 \pmod 4 \quad et \quad \frac{B}{c_4^2} \equiv 3 \pmod 4.$$

DÉMONSTRATION : D'après la relation (21), on a $\theta^3 \equiv 1 \pmod 2$ et d'après le lemme 7, $\theta^2 \equiv 1 \pmod 2$, d'où, $\theta \equiv 1 \pmod 2$. D'après *loc. cit.* et la relation (21) on a alors, $\theta \equiv \theta^3 \equiv 1 \pmod 4$. La seconde congruence résulte alors de l'égalité (20). D'où le lemme.

Lemme 33 *Supposons $K \in \Omega_1$. Alors, $K_{nr}(B^{1/2}) = K_{nr}$ et on a*

$$\frac{B^{1/2}}{c_4} \equiv 1 + \pi \pmod{2\mathcal{O}_{K_{nr}}} \quad et \quad \frac{C}{\pi^{v(c_4)}} \equiv c_4' + \pi^3 \pmod{4\mathcal{O}_{K_{nr}}}.$$

DÉMONSTRATION : D'après le lemme 32, on a $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$. Or, 3 est un carré dans K_{nr} car K est dans Ω_1. D'où l'égalité annoncée. La première congruence résulte du lemme 17 et de la congruence $B/c_4^2 \equiv 3 \pmod 4$ du lemme 32. D'après l'égalité (16), le lemme 32 et la première congruence ci-dessus, on a

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4'(2\pi + 1) \pmod{4\mathcal{O}_{K_{nr}}}.$$

D'où le résultat car $2c_4'\pi \equiv \pi^3 \pmod 4$.

On reprend les notations du §3.5. En particulier, η désigne, lorsque $K \in \Omega_2$, une uniformisante de $K(\sqrt{3})$.

Lemme 34 *Supposons $K \in \Omega_2$. Alors, $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$ et on a*

$$\frac{B^{1/2}}{c_4} \equiv \sqrt{3} \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}$$

et

$$\frac{C}{\pi^{v(c_4)}} \equiv c_4'(3 + 2\sqrt{3}) \pmod{4\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$

DÉMONSTRATION : L'égalité et la première congruence résultent des lemmes 32 et 19. La seconde résulte de la première congruence, du lemme 32 et de l'égalité (16).

On procède comme suit pour la fin de la démonstration de l'assertion 7d.

1. Supposons $K \in \Omega_1$. Si $v(c_4) = v(C)$ est impair, alors C n'est pas un carré dans $K_{nr}(B^{1/2}) = K_{nr}$. Donc $|\Phi| = 4$ d'après [2, th.3(i)]. Si $v(c_4)$ est pair. Alors, d'après le lemme 33, B est un carré dans K_{nr}. De plus, C est un carré dans K_{nr} si et seulement si l'unité $c_4' + \pi^3$ de $\mathcal{O}_K$ l'est. Or, d'après le lemme 8, c'est le cas si et seulement si la condition (C3) est satisfaite. D'où le résultat d'après [2, th.3(i)].
2. Supposons $K \in \Omega_2$. Alors, d'après le lemme 34, B n'est pas un carré dans K_{nr}. Si $v(c_4)$ est impair, on a

   $$\frac{C}{\pi^{v(c_4)-1}\eta^2} \equiv c_4'\beta(3 + 2\sqrt{3}) \pmod{4\mathcal{O}_{K_{nr}(\sqrt{3})}},$$

   où β est une unité des entiers de $K(\sqrt{3})$ telle que $\pi = \eta^2\beta$. On en déduit que C est un carré dans $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$ si et seulement si l'unité $c_4'\beta(3+2\sqrt{3})$ de $K(\sqrt{3})$ est un carré dans $K_{nr}(\sqrt{3})$. Or, d'après le lemme 19, on a $\beta \equiv 1+\eta \pmod{\eta^2}$. D'où $c_4'\beta(3+2\sqrt{3}) \equiv 1+\eta \pmod{\eta^2}$. On en déduit, avec le lemme 21 que C n'est pas un carré dans $K_{nr}(\sqrt{3})$. D'où $|\Phi| = 8$ dans ce cas d'après [2, th.3(i)].

   Supposons $v(c_4)$ pair. Alors, C est un carré dans $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$ si et seulement si l'unité $c_4'(3 + 2\sqrt{3})$ de $K(\sqrt{3})$ l'est. Si c_4' est un carré dans $K_{nr}(\sqrt{3})$, alors C n'est pas un carré dans $K_{nr}(\sqrt{3})$, car d'après le

lemme 20, $3+2\sqrt{3}$ ne l'est pas. Si c'_4 n'est pas un carré dans $K_{nr}(\sqrt{3})$, alors d'après le lemme 18, on a $c'_4 \equiv 1+\pi \pmod 2$. D'après le lemme 19, on a alors

$$c'_4(3+2\sqrt{3}) \equiv 1+\pi \equiv 1+\eta^2+\eta^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$

Donc, d'après le lemme 21, $c'_4(3+2\sqrt{3})$ n'est pas un carré dans $K_{nr}(\sqrt{3})$ et il en va de même pour C d'après l'équivalence ci-dessus. D'où $|\Phi| = 8$ dans ce cas d'après [2, th.3(i)].

Cela achève la démonstration de l'assertion 7d du théorème 2.

3.8 Calculs des types de Néron

D'après [5], la courbe E admet un modèle de Weierstrass de la forme

$$Y^2 = X^3 - \frac{c_4}{48}X - \frac{c_6}{864}. \qquad (W_0)$$

Ce modèle est entier si et seulement si on a $v(c_4) \geq 8$ et $v(c_6) \geq 10$. Dans toute cette section, on note Δ_m le discriminant minimal de E.

3.8.1 Cas où $v(j) = 4$

On suppose que le modèle de Weierstrass de E vérifie $v(j) = 4$ et la condition (C1), i.e. $\Delta' \equiv 1+\pi \pmod 2$. D'après la formule (18), on a

$$c'^3_4 - c'^2_6 = \varepsilon^3\pi^8\Delta', \qquad (22)$$

où l'on a posé $\varepsilon = 3\left(\frac{2}{\pi^2}\right)^2$.

Lemme 35 *La courbe E n'est pas de type IV. Supposons qu'elle soit de type IV^*. Alors, on a $v(\Delta_m) = 8$.*

Démonstration : D'après [2, th.2(i)], si E est de type IV, on a $v(\Delta_m) = 4$. C'est en contradiction avec la condition $v(j) = 4$. Par ailleurs, si E est de type IV^*, on a alors $v(\Delta_m) = 8$. D'où le lemme.

Lemme 36 *Supposons $v(\Delta) \equiv 8 \pmod{12}$. Alors, $v(\Delta_m) = 8$ si et seulement si $c'_6 \equiv 1 \pmod 2$.*

Démonstration : Supposons $v(\Delta) \equiv 8 \pmod{12}$. D'après l'appendice B, quitte à faire un changement de variables, on peut supposer que l'on a

$$(v(c_4), v(c_6), v(\Delta)) = (8, 12, 20).$$

La courbe E correspond alors à un cas 7 de Tate ou à un cas non minimal. Le modèle (W_0) de E est entier et, avec les notations de [5], on a

$$b_2 = 0; \quad b_4 = -2\frac{c_4}{48} = -6\frac{c'_4}{\varepsilon^2}; \quad b_6 = -4\frac{c_6}{864} = -2^3\frac{c'_6}{\varepsilon^3};$$

$$b_8 = -\left(\frac{c_4}{48}\right)^2 = -3^2\frac{c_4'^2}{\varepsilon^4}.$$

Examinons à présent à quelle condition le système suivant de congruences admet une solution (r,s) dans $\mathcal{O}_K$:

$$\begin{cases} b_8 + 3r^2 b_4 + 3r^4 \equiv 0 \pmod{4\pi} \\ r \equiv s^2 \pmod 2. \end{cases}$$

Comme $v(b_8) = 0$, si (r,s) est une solution, on a nécessairement $r \in \mathcal{U}_K$, donc s est également une unité et, d'après la seconde congruence, $r \equiv 1 \pmod 2$ (et on peut choisir $s = 1$). On a alors, $r^2 \equiv r^4 \equiv 1 \pmod{4\pi}$ et de même, $\varepsilon^2 \equiv \varepsilon^4 \equiv 1 \pmod{4\pi}$. Donc

$$-9c_4'^2 - 18c_4' + 3 \equiv 0 \pmod{4\pi}.$$

Autrement dit, le système précédent admet une solution si et seulement si $c_4'^2 + 2c_4' \equiv 3 \pmod{4\pi}$. Or, d'après la relation (22) et le lemme 7, on a $c_4' \equiv 1 \pmod 2$, puis $c_4'^2 \equiv 1 \pmod{4\pi}$ et $c_4' \equiv c_6'^2 \pmod{4\pi}$. Donc, on a $3 \equiv c_4'^2 + 2c_4' \equiv 1 + 2c_6'^2 \pmod{4\pi}$. Mais, par ailleurs, on a

$$1 + 2c_6'^2 \equiv \begin{cases} 3 \pmod{4\pi} & \text{si } c_6' \equiv 1 \pmod 2 \\ 3 + \pi^4 \pmod{4\pi} & \text{si } c_6' \equiv 1 + \pi \pmod 2. \end{cases}$$

On en déduit qu'il existe une solution (r,s) au système de congruences ci-dessus si et seulement si $c_6' \equiv 1 \pmod 2$. On conclut alors au lemme avec [3, prop.4].

Lemme 37 *Supposons $c_6' \equiv 1 \pmod 2$. Alors, on a*

$$c_4' \equiv (1+\pi^4)(1-c_6'^2) + 1 + \pi^8 + \pi^9 \pmod{\pi^{10}}.$$

Démonstration : On a $\varepsilon \equiv \pm 1 \pmod 4$, d'où, $\varepsilon^2 \equiv 1 \pmod{\pi^6}$, puis $\varepsilon^4 \equiv 1 \pmod{\pi^8}$ (lemme 10). En réduisant l'égalité (22) modulo 2, on obtient $c_4' \equiv 1 \pmod 2$. Puis, d'après le lemme 7, on a $c_4' \equiv c_4'^3 \pmod{4\pi}$ et, comme $c_6' \equiv 1 \pmod 2$, $c_6'^2 \equiv 1 \pmod{4\pi}$. Comme d'après la relation (22), on a $c_4'^3 \equiv c_6'^2 \pmod{4\pi}$, il vient $c_4' \equiv 1 \pmod{4\pi}$. On en déduit $c_4'^2 \equiv 1 \pmod{\pi^7}$, puis $c_4'^3 \equiv c_4' \pmod{\pi^7}$. D'où $c_4' \equiv c_6'^2 \pmod{\pi^7}$ avec la relation (22) réduite modulo π^7. Posons donc $c_4' = c_6'^2 + \pi^7 a$, avec $a \in \mathcal{O}_K$. On a

$$c_4'^3 \equiv c_6'^6 + 3\pi^7 c_6'^4 a \pmod{\pi^{10}}.$$

Or, $c_6'^4 \equiv 1 \pmod{\pi^3}$ et $3 \equiv 1 + \pi^2 \pmod{\pi^3}$, donc $c_4'^3 \equiv c_6'^6 + \pi^7 a + \pi^9 a \pmod{\pi^{10}}$, puis

$$c_4'^3 - c_6'^2 \equiv c_6'^6 - c_6'^2 + \pi^7 a + \pi^9 a \pmod{\pi^{10}}.$$

Mais, comme $c_6'^2 \equiv 1 \pmod{\pi^5}$ car $c_6' \equiv 1 \pmod 2$, on a $c_6'^2 + 1 \equiv 2 \pmod{\pi^5}$ et

$$c_6'^6 - c_6'^2 = c_6'^2(c_6'^2+1)(c_6'^2-1) \equiv 2(c_6'^2 - 1) \equiv 2(c_4' - \pi^7 a - 1) \pmod{\pi^{10}}.$$

Autrement dit, on a $c_4'^3-c_6'^2 \equiv 2c_4'-2-\pi^7 a+\pi^9 a \pmod{\pi^{10}}$ et $c_4'^3-c_6'^2 \equiv c_4'+c_6'^2-2+\pi^9 a \pmod{\pi^{10}}$. Par ailleurs, d'après l'hypothèse (C1), on a $c_4'^3-c_6'^2 \equiv \pi^8+\pi^9 \pmod{\pi^{10}}$. On en déduit donc

$$c_4' \equiv -c_6'^2 + 2 + \pi^8 + \pi^9(a+1) \pmod{\pi^{10}}.$$

Or, on a $\pi^9(a+1) = \pi^2(c_4'-c_6'^2+\pi^7)$. Donc $(1-\pi^2)c_4' \equiv -(1+\pi^2)c_6'^2+2+\pi^8+\pi^9 \pmod{\pi^{10}}$. D'où

$$c_4' \equiv \frac{1+\pi^2}{1-\pi^2}(1-c_6'^2) + 1 + \pi^8 + \pi^9 \pmod{\pi^{10}}.$$

Enfin, on a $(1+\pi^2)/(1-\pi^2) \equiv 1+\pi^4 \pmod{\pi^5}$ et donc le résultat car $c_6'^2-1 \equiv 0 \pmod{\pi^5}$. Cela démontre le lemme.

Posons

$$a_2 = \frac{1}{\pi^2}\left(\frac{3}{\varepsilon}c_6' - 1\right); \quad a_4 = \frac{1}{\pi^4}\left(\frac{3}{\varepsilon^2}\left(c_6'^2 - c_4'\right) - 4\right);$$

$$a_6 = \frac{1}{\pi^6}\left(\frac{c_6'}{\varepsilon^3}\left(c_6'^2 - 3c_4' - 2\right) - 4\right).$$

Proposition 3 *Supposons $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. Alors, l'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + a_2x^2 + a_4x + a_6, \tag{W}$$

définit un modèle de Weierstrass entier de E pour lequel on a

$$a_4 \equiv \frac{1}{\pi^2}\left(c_6'^2 - 1\right) + \varepsilon \pmod 4, \quad a_6 \equiv \frac{\varepsilon}{\pi^2}\left(\frac{c_6'}{\varepsilon} + 1\right) + \pi^2 + \pi^3 \pmod 4$$

et

$$a_6 + \varepsilon a_2 \equiv \pi^3 \pmod 4, \quad \pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right) \equiv a_4 - \varepsilon \pmod 4.$$

Démonstration : Le changement de variables

$$X = x + \frac{1}{\pi^2}\frac{c_6'}{\varepsilon}; \qquad Y = y + \frac{x}{\pi} + \frac{2}{\pi^3}$$

transforme le modèle (W_0) de E en le modèle de la proposition.

Les éléments $2/\pi$ et $4/\pi^3$ sont entiers. D'après le lemme 36, on a $c_6' \equiv 1 \pmod 2$. Donc, d'après le lemme 10, le coefficient a_2 est entier. Vérifions que les coefficients a_4 et a_6 le sont aussi et qu'ils satisfont aux congruences annoncées. D'après le lemme 37, on a

$$\begin{aligned}\pi^4 a_4 &\equiv \frac{3}{\varepsilon^2}\left(c_6'^2 - (1+\pi^4)(1-c_6'^2) - 1\right) - 4 \pmod{\pi^8} \\ &\equiv \frac{3}{\varepsilon^2}(2+\pi^4)(c_6'^2-1) - 4 \pmod{\pi^8}.\end{aligned}$$

Or, $c_6'^2 - 1 \equiv 0 \pmod{\pi^5}$, donc $v(a_4) = 0$ et a_4 est une unité de $\mathcal{O}_K$. Puis, on a $\pi^4 a_4 \equiv 2(c_6'^2 - 1) - 4 \pmod{\pi^8}$ et

$$a_4 \equiv \left(\frac{2}{\pi^2}\right) \frac{1}{\pi^2}(c_6'^2 - 1) - \left(\frac{2}{\pi^2}\right)^2 \pmod 4.$$

On en déduit la congruence annoncée pour a_4 car $v(c_6'^2 - 1) \geq 5$ et $2/\pi^2$ est une unité.

Examinons à présent le coefficient a_6. On a, d'après le lemme 37,

$$\begin{aligned}
\pi^6 a_6 &= \frac{c_6'}{\varepsilon^3}\left(c_6'^2 - 3c_4' - 2\right) - 4 \\
&\equiv \frac{c_6'}{\varepsilon^3}\left(c_6'^2 - 3(1+\pi^4)(1-c_6'^2) - 5\right) + \pi^8 + \pi^9 - 4 \pmod{\pi^{10}} \\
&\equiv \frac{c_6'}{\varepsilon^3}\left((4+3\pi^4)(c_6'^2 - 1) - 4\right) + \pi^8 + \pi^9 - 4 \pmod{\pi^{10}}.
\end{aligned}$$

Or, $4 + 3\pi^4 \equiv 0 \pmod{\pi^5}$ et $c_6'^2 - 1 \equiv 0 \pmod{\pi^5}$, donc $\pi^6 a_6 \equiv -4c_6'/\varepsilon^3 - 4 + \pi^8 + \pi^9 \pmod{\pi^{10}}$. Puis, comme $\varepsilon^2 \equiv 1 \pmod{\pi^6}$, on a

$$\pi^6 a_6 \equiv -4\left(\frac{c_6'}{\varepsilon} + 1\right) + \pi^8 + \pi^9 \pmod{\pi^{10}}.$$

D'où $v(a_6) \geq 0$ car $c_6'/\varepsilon + 1 \equiv 0 \pmod 2$ et on a

$$a_6 \equiv -\left(\frac{2}{\pi^2}\right)^2 \frac{1}{\pi^2}\left(\frac{c_6'}{\varepsilon} + 1\right) + \pi^2 + \pi^3 \pmod 4.$$

D'où la congruence annoncée pour a_6 par définition de ε.

On en déduit que l'on a

$$3a_6 \equiv \frac{\varepsilon}{\pi^2}\left(\frac{3}{\varepsilon}c_6' + 3\right) + \pi^2 + \pi^3 \pmod 4.$$

Or, $3 \equiv -5 \equiv -1 - 4 \pmod{\pi^6}$, donc

$$3a_6 \equiv \frac{\varepsilon}{\pi^2}\left(\frac{3}{\varepsilon}c_6' - 1\right) - \frac{4}{\pi^2}\varepsilon + \pi^2 + \pi^3 \pmod 4.$$

Or, $4 \equiv \pi^4 \pmod{\pi^6}$, donc, par définition du coefficient a_2, on a $3a_6 \equiv \varepsilon a_2 + \pi^3 \pmod 4$. C'est la congruence voulue.

Enfin, on a, par définition du coefficient a_2,

$$\begin{aligned}
\pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right) &= \frac{1}{\pi^2}\left(\frac{3}{\varepsilon}c_6' - 1\right)\left(\frac{3}{\varepsilon}c_6' + 1\right) \equiv \frac{1}{\pi^2}\left(\frac{9}{\varepsilon^2}c_6'^2 - 1\right) \pmod 4 \\
&\equiv \frac{1}{\pi^2}(c_6'^2 - 1) \pmod 4 \quad \text{car } 9/\varepsilon^2 \equiv 1 \pmod{\pi^6} \\
&\equiv a_4 - \varepsilon \pmod 4
\end{aligned}$$

d'après la première congruence. Cela achève la démonstration de la proposition 3.

Posons

$$r = \frac{2}{\pi^2} + \pi \quad \text{et} \quad t = \pi.$$

Notons b_2, b_4, b_6 et b_8 les invariants standard associés au modèle (W) de E.

Lemme 38 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. *Alors, on a*

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \pmod{\pi^5}.$$

De plus, la courbe E correspond à un cas ≥ 7 de Tate si et seulement si on a $(a_2 + 1)(\pi^3 + 2a_2) + 2 \equiv \pi^2 + \pi^3 \pmod 4$.

Démonstration : On considère le modèle (W) de E de la proposition 3. On a

$$b_2 = \left(\frac{2}{\pi}\right)^2 + 4a_2; \quad b_4 = \frac{2^3}{\pi^4} + 2a_4; \quad b_6 = \left(\frac{4}{\pi^3}\right)^2 + 4a_6;$$

et

$$b_8 = \left(\frac{2}{\pi}\right)^2 a_6 - \frac{2^3}{\pi^4}a_4 + 4a_2a_6 + \frac{2^4}{\pi^6}a_2 - a_4^2.$$

On en déduit que l'on a les congruences suivantes :

$$b_2 \equiv -\varepsilon\pi^2 + 4a_2 \pmod{4\pi}, \qquad b_4 \equiv 2(a_4 - \varepsilon) \equiv 0 \pmod{4\pi},$$

$$b_6 \equiv \pi^2 + 4a_2 \pmod{4\pi}, \qquad b_8 \equiv \pi^2(a_2 - \varepsilon a_6) + 1 + 4a_2 \equiv 1 \pmod{4\pi}$$

car $a_2 - \varepsilon a_6 \equiv 2a_2 \pmod{\pi^3}$.

L'entier r de $\mathcal{O}_K$ est une unité de $\mathcal{O}_K$ et on a

$$\begin{aligned} b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 &\equiv 1 + 3r\pi^2 + 4a_2 - \varepsilon r^3\pi^2 + 4a_2 + 3 \pmod{4\pi} \\ &\equiv 4 + \pi^2(3 - \varepsilon r^2) \pmod{4\pi} \\ &\equiv 4 + \pi^2\left(\left(\frac{2}{\pi^2}\right)^2 - r^2\right) \pmod{4\pi}. \end{aligned}$$

Or, $r^2 \equiv (2/\pi^2)^2 + \pi^2 \pmod{\pi^3}$. Donc $4 + \pi^2((2/\pi^2)^2 - r^2) \equiv 0 \pmod{4\pi}$. Autrement dit, $r = 2/\pi^2 + \pi$ vérifie la condition (a) de [3, prop. 3]. On a alors,

d'après les congruences de la proposition 3,

$$\begin{aligned}
a_6 + ra_4 + r^2a_2 + r^3 &= a_6 + \left(\frac{2}{\pi^2} + \pi\right) a_4 + \left(\frac{2}{\pi^2} + \pi\right)^2 a_2 + \left(\frac{2}{\pi^2} + \pi\right)^3 \\
&\equiv \pi^3 - \varepsilon a_2 + \left(\frac{2}{\pi^2} + \pi\right)\left(\varepsilon + \pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right)\right) \\
&\quad + \left(\frac{2}{\pi^2} + \pi\right)^2 a_2 + \left(\frac{2}{\pi^2} + \pi\right)^3 \pmod 4 \qquad (23) \\
&\equiv \pi^3 - \varepsilon a_2 + \varepsilon\left(\frac{2}{\pi^2}\right) + \pi\varepsilon + 2a_2\left(a_2 + \frac{2}{\pi^2}\right) - \varepsilon a_2 + \frac{4}{\pi}a_2 + \pi^2 a_2 \\
&\quad - \varepsilon\left(\frac{2}{\pi^2}\right) + \pi\varepsilon + 2 + \pi^3 \pmod 4 \\
&\equiv \pi^3(a_2+1) + 2a_2(a_2+1) + 2 \equiv (a_2+1)(\pi^3 + 2a_2) + 2 \pmod 4.
\end{aligned}$$

Par ailleurs, on a $v((a_2+1)(\pi^3+2a_2)) \geq 3$, donc en particulier,

$$a_6 + ra_4 + r^2a_2 + r^3 \equiv 2 \equiv \pi^2 \pmod{\pi^3}.$$

On a alors, avec $t = \pi$,

$$\begin{aligned}
t\left(\frac{4}{\pi^3}\right) + t^2 + rt\left(\frac{2}{\pi}\right) &\equiv \pi^2\left(\frac{2}{\pi^2}\right)^2 + \pi^2 + 2\left(\frac{2}{\pi^2} + \pi\right) \pmod 4 \\
&\equiv \pi^2 + \pi^2 + \pi^2 + \pi^3 \pmod 4 \qquad (24) \\
&\equiv \pi^2 + \pi^3 \pmod 4.
\end{aligned}$$

Donc, en particulier, $t(4/\pi^3) + t^2 + rt(2/\pi) \equiv \pi^2 \pmod{\pi^3}$. On déduit alors de [3, prop. 3] appliqué à r et t et des congruences (23) et (24) que l'on est dans un cas ≥ 7 de Tate si et seulement si $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2 + \pi^3 \pmod 4$. D'où le lemme.

Lemme 39 *Supposons $c_6' \equiv 1 \pmod 2$. Alors, $v((a_2+1)(\pi^3+2a_2)) \geq 3$. De plus, on a $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$ si et seulement si $a_2 \equiv 0$ ou $1+\pi \pmod 2$.*

Démonstration : D'après l'hypothèse faite, le coefficient a_2 est entier. On a $v((a_2+1)(\pi^3+2a_2)) \geq 3$. De plus, $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$ si et seulement si $v((a_2+1)(\pi^3+2a_2)) = 3$. Or, $v((a_2+1)(\pi^3+2a_2)) = 3$ si et seulement si $v(a_2) \geq 2$ ou $v(a_2+1) = 1$. D'où le résultat.

Proposition 4 *Supposons $K \in \Omega_1$. On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites*

1. *on a $v(\Delta) \equiv 8 \pmod{12}$;*
2. *on a $c_6' \equiv 1 + \pi^2 \pmod 4$ ou $c_6' \equiv 1 + \pi^3 \pmod 4$.*

DÉMONSTRATION : Supposons $|\Phi| = 3$. D'après [2, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 35, E est de type IV^* (cas 8 de Tate) et $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut de plus supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. Puis, d'après le lemme 36, on a $c'_6 \equiv 1 \pmod 2$. Comme on est dans un cas ≥ 7 de Tate, on a, d'après le lemme 38, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Donc, comme K est dans Ω_1, il vient $(a_2+1)(\pi^3+2a_2) \equiv 0 \pmod 4$. Autrement dit, d'après le lemme 39, on a $a_2 \equiv 1$ ou $\pi \pmod 2$. Or, par définition du coefficient a_2, lorsque K est dans Ω_1, on a, d'après le lemme 10,

$$\begin{aligned} \pi^2 a_2 \equiv -c'_6 - 1 \pmod 4, \text{ d'où } c'_6 &\equiv \pi^2 a_2 - 1 \\ &\equiv \pi^2 a_2 + 1 + \pi^2 + \pi^3 \pmod 4. \end{aligned}$$

On en déduit que l'on a $c'_6 \equiv 1 + \pi^2 \pmod 4$ ou $c'_6 \equiv 1 + \pi^3 \pmod 4$.

Réciproquement, supposons les deux conditions de l'énoncé satisfaites. Alors, $c'_6 \equiv 1 \pmod 2$ et, d'après le lemme 36, on a $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. D'après l'appendice B, E correspond alors à un cas 6, 7 ou 8 (type IV^*) de Tate. Par ailleurs, comme K est dans Ω_1, on a $a_2 \equiv (3c'_6 - 1)/\pi^2 \pmod 2$, d'où $a_2 \equiv 1$ ou $\pi \pmod 2$. Donc, d'après le lemme 39, on a $(a_2+1)(\pi^3+2a_2) \equiv 0 \pmod 4$, puis, comme K est dans Ω_1, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Autrement dit, d'après le lemme 38, on est dans un cas ≥ 7 de Tate. Vérifions que l'on est alors dans un cas 8 de Tate. Toujours d'après le lemme 38, comme la condition (a) de [3, prop. 4] est vérifiée, on doit s'assurer qu'il existe un entier s de $\mathcal{O}_K$ tel que

$$a_2 + r \equiv s^2 + s\pi \pmod 2.$$

Or, c'est bien le cas car $a_2 \equiv 1$ ou $\pi \pmod 2$ et $r \equiv 1 \pmod 2$. En effet, on a ou bien $a_2 + 1 \equiv 0 \pmod 2$ et on choisit $s = 0$, ou bien $a_2 + 1 \equiv 1 + \pi \pmod 2$ et on choisit $s = 1$. La condition (b) de [3, prop. 4] est donc vérifiée et on est bien dans un cas 8 de Tate. On conclut alors que $|\Phi| = 3$ avec [2, th.2(i)]. Cela démontre la proposition.

Proposition 5 *Supposons $K \in \Omega_2$. On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites*

1. $v(\Delta) \equiv 8 \pmod{12}$ *;*
2. $c'_6 \equiv 1 \pmod 4$ *ou* $c'_6 \equiv 1 + \pi^2 + \pi^3 \pmod 4$.

DÉMONSTRATION : Supposons $|\Phi| = 3$. D'après [2, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 35, E est de type IV^* (cas 8 de Tate) et $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut de plus supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. Puis, d'après le lemme 36, on a $c'_6 \equiv 1 \pmod 2$. Comme on est dans un cas ≥ 7 de Tate, on a, d'après le lemme 38, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Donc, comme K est dans Ω_2, il vient $(a_2 + 1)(\pi^3 + 2a_2) \equiv \pi^3 \pmod 4$. Autrement dit, d'après le lemme 39, on a

$a_2 \equiv 0$ ou $1+\pi \pmod 2$. Or, par définition du coefficient a_2, lorsque K est dans Ω_2, on a, d'après le lemme 10,

$$\pi^2 a_2 \equiv c_6' - 1 \pmod 4, \text{ d'où } c_6' \equiv \pi^2 a_2 + 1 \pmod 4.$$

On en déduit que l'on a $c_6' \equiv 1 \pmod 4$ ou $c_6' \equiv 1 + \pi^2 + \pi^3 \pmod 4$.

Réciproquement, supposons les deux conditions de l'énoncé satisfaites. Alors, $c_6' \equiv 1 \pmod 2$ et, d'après le lemme 36, on a $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. D'après l'appendice B, E correspond à un cas 6, 7 ou 8 (type IV^*) de Tate. Par ailleurs, comme K est dans Ω_2, on a $a_2 \equiv (c_6' - 1)/\pi^2 \pmod 2$, d'où $a_2 \equiv 0$ ou $1+\pi \pmod 2$. Donc, d'après le lemme 39, on a $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$, puis, comme K est dans Ω_2, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Autrement dit, d'après le lemme 38, on est dans un cas ≥ 7 de Tate. Vérifions que l'on est alors dans un cas 8 de Tate. Toujours d'après le lemme 38, comme la condition (a) de [3, prop. 4] est vérifiée, on doit s'assurer qu'il existe un entier s de $\mathcal{O}_K$ tel que

$$a_2 + r \equiv s^2 + s\pi \pmod 2.$$

Or, c'est bien le cas car $a_2 \equiv 0$ ou $1 + \pi \pmod 2$ et $r \equiv 1 + \pi \pmod 2$. En effet, on a ou bien $a_2 + 1 + \pi \equiv 1 + \pi \pmod 2$ et on choisit $s = 1$, ou bien $a_2 + 1 + \pi \equiv 0 \pmod 2$ et on choisit $s = 0$. La condition (b) de [3, prop. 4] est donc vérifiée et on est bien dans un cas 8 de Tate. On conclut alors que $|\Phi| = 3$ avec [2, th.2(i)]. Cela démontre la proposition.

3.8.2 Cas où $v(j) = 8$

On suppose que le modèle de Weierstrass de E vérifie $v(j) = 8$ et la condition (C2), i.e. $j' \equiv 1 + \pi^2 \pmod{2\pi}$. D'après la formule (18), on a

$$c_4'^3 - c_6'^2 = \varepsilon^3 \pi^4 \Delta'. \tag{25}$$

Lemme 40 *La courbe E n'est pas de type IV^*. Supposons qu'elle soit de type IV. Alors, on a $v(\Delta_m) = 4$.*

Démonstration : D'après [2, th.2(i)], si E est de type IV^*, on a $v(\Delta_m) = 8$. C'est en contradiction avec la condition $v(j) = 8$. Par ailleurs, si E est de type IV, on a $v(\Delta_m) = 4$. D'où le lemme.

Lemme 41 *Supposons $v(\Delta) \equiv 4 \pmod{12}$. Alors, $v(\Delta_m) = 4$ si et seulement si $c_6' \equiv 1 \pmod 2$.*

Démonstration : Supposons $v(\Delta) \equiv 4 \pmod{12}$. D'après l'appendice B, quitte à faire un changement de variables, on peut supposer que l'on a

$$(v(c_4), v(c_6), v(\Delta)) = (8, 12, 16).$$

Le modèle (W_0) de E est alors entier et la courbe E correspond à un cas 7 de Tate ou à un cas non minimal. Exactement comme dans la démonstration du lemme 35, on montre qu'il n'est pas minimal si et seulement si on a $c'_6 \equiv 1 \pmod 2$. D'où le lemme.

Lemme 42 *Supposons* $c'_6 \equiv 1 \pmod 2$. *On a* $c'_4 \equiv c'^2_6 + \varepsilon\pi^4 \pmod{\pi^7}$.

Démonstration : On a $\varepsilon \equiv \pm 1 \pmod 4$, d'où, $\varepsilon^2 \equiv 1 \pmod{\pi^6}$, puis $\varepsilon^4 \equiv 1 \pmod{\pi^8}$ (lemme 10). En réduisant l'égalité (25) modulo 2, on obtient $c'_4 \equiv 1 \pmod 2$. Puis, d'après le lemme 7, on a $c'_4 \equiv c'^3_4 \pmod{4\pi}$ et $c'^2_6 \equiv 1 \pmod{4\pi}$ car $c'_6 \equiv 1 \pmod 2$. Comme d'après la relation (25), on a $c'^3_4 \equiv c'^2_6 + \pi^4 \pmod{4\pi}$, il vient

$$c'_4 \equiv 1 + \pi^4 \pmod{4\pi}. \tag{26}$$

On en déduit $c'^2_4 \equiv 1 + 2\pi^4 \equiv 1 + \pi^6 \pmod{4\pi^3}$, puis

$$c'^3_4 \equiv c'_4 + \pi^6 \pmod{4\pi^3}. \tag{27}$$

Par ailleurs, d'après la relation (26), on a, en particulier, $c'_4 \equiv 1 \pmod{2\pi}$, donc l'hypothèse $j' \equiv 1 + \pi^2 \pmod{2\pi}$ implique

$$\Delta' \equiv 1 + \pi^2 \pmod{2\pi}. \tag{28}$$

Autrement dit, on a, d'après l'égalité (25) et la congruence (27),

$$c'_4 \equiv c'^2_6 + \varepsilon\pi^4 \pmod{\pi^7},$$

car $\varepsilon^2 \equiv 1 \pmod{\pi^6}$ donc, en particulier, $\varepsilon^2 \equiv 1 \pmod{2\pi}$. D'où le résultat.

Posons

$$a_2 = \frac{1}{\pi^2}\left(3\varepsilon c'_6 - 1\right); \quad a_4 = \frac{1}{\pi^4}\frac{3}{\varepsilon^2}\left(\varepsilon^4 c'^2_6 - c'_4\right);.$$

$$a_6 = \frac{1}{\pi^6}\frac{c'_6}{\varepsilon^3}\left(\varepsilon^6 c'^2_6 - 3c'_4\varepsilon^2 - 2\right).$$

Proposition 6 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. *Alors, l'équation*

$$y^2 + \frac{2}{\pi}xy = x^3 + a_2x^2 + a_4x + a_6, \tag{W}$$

définit un modèle de Weierstrass entier de E pour lequel on a $a_4 \equiv 1 \pmod 2$ *et* $a_6 \equiv 1 \pmod \pi$.

Démonstration : Le changement de variables

$$X = x + \frac{\varepsilon c'_6}{\pi^2}; \qquad Y = y + \frac{x}{\pi}$$

transforme le modèle (W_0) de E en le modèle de la proposition.

Le coefficient $2/\pi$ est entier. D'après le lemme 41, on a $c'_6 \equiv 1 \pmod 2$. De plus, d'après le lemme 10, le coefficient a_2 est entier. Vérifions que les coefficients a_4 et a_6 sont entiers et satisfont aux congruences annoncées.

On a

$$\pi^4 a_4 = \frac{3}{\varepsilon^2}(\varepsilon^4 c'^2_6 - c'_4) \equiv \frac{3}{\varepsilon^2}(c'^2_6 - c'_4) \equiv 3\frac{\pi^4}{\varepsilon^2} \equiv \pi^4 \pmod{\pi^6},$$

car $\varepsilon^4 \equiv 1 \pmod{\pi^6}$ et, d'après le lemme 42, $c'_4 \equiv c'^2_6 + \pi^4 \pmod{\pi^6}$. D'où le fait que $a_4 \equiv 1 \pmod 2$.

Examinons à présent le coefficient a_6. On a, d'après le lemme 42,

$$\begin{aligned}\frac{\varepsilon^3}{c'_6}\pi^6 a_6 &\equiv \varepsilon^2 c'^2_6 - 3c'_4\varepsilon^2 - 2\varepsilon^2 \pmod{4\pi^3} \\ &\equiv \varepsilon^2(c'^2_6 - 3c'_4 - 2) \equiv \varepsilon^2(-2c'_4 - 2 - \varepsilon\pi^4) \pmod{4\pi^3},\end{aligned}$$

car $\varepsilon^4 \equiv 1 \pmod{\pi^7}$. Or, $-\varepsilon\pi^4 = -12$ et, d'après le lemme 42 et la congruence $c'_6 \equiv 1 \pmod 2$, on a $c'_4 + 1 \equiv 2 + \pi^4 \pmod{4\pi}$. Donc

$$\frac{\varepsilon^3}{c'_6}\pi^6 a_6 \equiv -2\pi^4 \equiv \pi^6 \pmod{4\pi^3}.$$

Comme ε^3/c'_6 est une unité de $\mathcal{O}_K$, il en résulte $a_6 \equiv 1 \pmod \pi$ et la proposition.

Lemme 43 *Supposons $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. Alors, E ne correspond pas à un cas 4 de Tate.*

Démonstration : D'après l'appendice B, la courbe E correspond à un cas 3 (II), 4 (III) ou 5 (IV) de Tate. Soit (W) le modèle de E de la proposition 6. Supposons qu'il corresponde à un cas ≥ 4 de Tate. D'après la congruence $a_4 \equiv 1 \pmod 2$, $r = 1$ satisfait à la première relation de divisibilité de [3, prop. 2]. On a par ailleurs, avec les notations de [5],

$$b_2 \equiv \pi^2 \pmod{2\pi}; \quad b_4 \equiv \pi^2 \pmod{2\pi}; \quad b_6 \equiv 0 \pmod{2\pi};$$

$$b_8 \equiv \pi^2 a_6 - 1 \pmod{2\pi}.$$

Donc, $b_8 + 3b_6 + 3b_4 + b_2 + 3 \equiv \pi^2 a_6 + 2 \equiv \pi^2(a_6 + 1) \pmod{2\pi}$. D'où le résultat d'après [3, prop. 2] et la congruence $a_6 \equiv 1 \pmod \pi$.

Lemme 44 *Supposons $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. Alors, a_2 et a_6 sont entiers et on a*

$$a_2 \equiv \frac{1}{\pi^2}(\varepsilon c'_6 + 1) \pmod 2, \quad c'_6 \equiv \pi^2 a_2 - \varepsilon \pmod 4.$$

et

$$a_6 \equiv \frac{1}{\pi^6}(c'^2_6 - 3c'_4 - 2) \pmod 2, \quad c'_4 \equiv -c'^2_6 + 6 + \pi^6 a_6 \pmod{\pi^8}.$$

DÉMONSTRATION : Les éléments a_2 et a_6 sont entiers d'après la proposition 6. On a, $3\varepsilon \equiv -\varepsilon \pmod 4$, d'où les deux premières congruences. De plus, on a $\varepsilon^4 \equiv 1 \pmod{\pi^8}$ et $2 \equiv 2\varepsilon^2 \pmod{\pi^8}$. Donc

$$a_6 \equiv \frac{1}{\pi^6}\frac{c_6'}{\varepsilon}\left(c_6'^2 - 3c_4' - 2\right) \pmod 2.$$

D'où la troisième congruence car $c_6'/\varepsilon \equiv 1 \pmod 2$. On en déduit

$$c_4' \equiv \pi^6 a_6 + \frac{1}{3}(c_6'^2 - 2) \pmod{\pi^8}.$$

Or, $1/3 \equiv -1 \pmod{2\pi}$ et $c_6'^2 - 1 \equiv 0 \pmod{4\pi}$ car $c_6' \equiv 1 \pmod 2$. Donc, $(c_6'^2 - 1)/3 \equiv 1 - c_6'^2 \pmod{\pi^8}$. Comme par ailleurs, $-1/3 \equiv 5 \pmod{\pi^8}$, on en déduit la dernière congruence et le lemme.

Proposition 7 *On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites*

1. *on a $v(\Delta) \equiv 4 \pmod{12}$;*
2. *il existe $(a, b) \in \mathcal{L}_1$ tel que $c_4' \equiv a \pmod{\pi^8}$ et $c_6' \equiv b \pmod{\pi^6}$.*

DÉMONSTRATION : Supposons $|\Phi| = 3$. D'après [2, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 40, E est de type IV (cas 5 de Tate) et $v(\Delta_m) = 4$. La première condition est donc satisfaite et d'après le lemme 41, on a $c_6' \equiv 1 \pmod 2$. De plus, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. D'après la proposition 6, le modèle (W) de E est entier. Exprimons à présent le fait que l'on n'est pas dans un cas 3 de Tate. On a $a_4 \equiv 1 \pmod 2$, donc $r = 1$ satisfait à la première relation de divisibilité de [3, prop. 1].

Supposons $a_2 \equiv 1 \pmod \pi$. Alors, $t = 0$ satisfait à la seconde relation. Puis,

$$a_2 + a_6 \equiv a_6 + a_4 + a_2 + 1 \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([3, prop. 1]).

Supposons $a_2 \equiv 0 \pmod \pi$. Alors, $t = 1$ satisfait à la seconde relation. Puis,

$$a_6 + a_4 + a_2 - \frac{2}{\pi} \equiv a_2 + a_6 + 1 + \pi \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([3, prop. 1]). D'où $a_2 + a_6 \equiv 1 + \pi \pmod 2$. Autrement dit, on a $a_2 + a_6 \equiv 0$ ou $1 + \pi \pmod 2$. De plus, d'après le lemme 44, on a

$$c_6' \equiv \pi^2 a_2 - \varepsilon \pmod 4 \quad \text{et} \quad c_4' \equiv -c_6'^2 + 6 + \pi^6 a_6 \pmod{\pi^8}. \tag{29}$$

Par ailleurs, d'après la proposition 6 et les congruences $a_2 + a_6 \equiv 0$ ou $1 + \pi \pmod 2$, on a

$$(a_2 \pmod 2, a_6 \pmod 2) \in \{(0, 1 + \pi), (1, 1), (\pi, 1), (1 + \pi, 1 + \pi)\}.$$

On déduit alors des congruences de la formule (29) les quatre couples ($c_4' + c_6'^2 \pmod{\pi^8}, c_6' \pmod 4$) possibles. À chaque classe $c_6' \pmod 4$ correspond quatre valeurs possibles pour $c_6' \pmod{\pi^6}$. En remplaçant $c_6'^2 \pmod{\pi^8}$ par sa valeur dans la seconde congruence de (29), on obtient ainsi les seize couples ($c_4' \pmod{\pi^8}, c_6' \pmod{\pi^6}$) de l'ensemble $\mathcal{L}_1$.

Réciproquement, supposons les conditions de l'énoncé satisfaites. Alors, on a $c_6' \equiv 1 \pmod 2$ et, d'après le lemme 41, $v(\Delta_m) = 4$. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. Alors, d'après l'appendice B, E correspond à un cas 3, 4 ou 5 de Tate. Montrons que E ne correspond pas à un cas 3 de Tate. Comme a_4 est une unité, $r = 1$ satisfait à la première relation de divisibilité de [3, prop.1]. De plus, d'après le lemme 44, on a

$$a_2 \equiv \frac{1}{\pi^2}(\varepsilon c_6' + 1) \pmod 2 \quad \text{et} \quad a_6 \equiv \frac{1}{\pi^6}(c_6'^2 - 3c_4' - 2) \pmod 2.$$

On vérifie alors que pour chacun des seize couples de l'ensemble $\mathcal{L}_1$, on a $a_2 + a_6 \equiv 0$ ou $1 + \pi \pmod 2$.

Supposons $a_2 + a_6 \equiv 0 \pmod 2$. Alors, $t = 0$ satisfait à la seconde relation de divisilité de [3, prop.1] et $a_6 + a_4 + a_2 + 1 \equiv 0 \pmod 2$, donc on est dans un cas ≥ 4 de Tate. De même, si $a_2 + a_6 \equiv 1 + \pi \pmod 2$, alors, $t = 1$ convient et $a_6 + a_4 + a_2 - 2/\pi \equiv 0 \pmod 2$ et on est encore dans un cas ≥ 4 de Tate. Par ailleurs, d'après le lemme 43, on n'est pas dans un cas 4 de Tate. On est donc dans un cas 5 (type IV) et $|\Phi| = 3$, d'après [2, th.2(i)].

3.8.3 Cas où $v(j) = 16$

On suppose que le modèle de Weierstrass de E vérifie $v(j) = 16$ et la condition (C2), i.e. $j' \equiv 1 + \pi^2 \pmod{2\pi}$.

Lemme 45 *La courbe E n'est pas de type IV. Supposons qu'elle soit de type IV^*. Alors, on a $v(\Delta_m) = 8$.*

Démonstration : D'après [2, th.2(i)], si E est de type IV, on a $v(\Delta_m) = 4$. C'est en contradition avec la condition $v(j) = 16$. Par ailleurs, si E est de type IV^*, alors $v(\Delta_m) = 8$. D'où le lemme.

Posons

$$a_4 = -3\frac{c_4'}{\varepsilon^2} \quad \text{et} \quad a_6 = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3}.$$

Proposition 8 *Supposons $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. Alors, l'équation*

$$y^2 = x^3 + a_4 x + a_6 \qquad (W)$$

définit un modèle de Weierstrass entier de E. De plus, les coefficients a_4 et a_6 sont deux unités de $\mathcal{O}_K$ satisfaisant aux congruences suivantes :

$$a_4 \equiv c_4' \pmod 4, \quad a_6 \equiv \left(\frac{\pi^2}{2}\right) c_6' \pmod 4$$

et

$$a_4 \equiv 1 \pmod 2, \quad a_4 \equiv a_6^2 + \pi^2 \pmod{2\pi}.$$

DÉMONSTRATION : Sous l'hypothèse $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$, le modèle proposé n'est rien d'autre que le modèle (W_0) de E. En effet, on a

$$-\frac{c_4}{48} = -3\frac{c_4'}{\varepsilon^2} = a_4 \quad \text{et} \quad -\frac{c_6}{864} = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3} = a_6.$$

Les coefficients a_4 et a_6 sont deux unités de $\mathcal{O}_K$. De plus,

$$a_4 = -\frac{3}{\varepsilon^2}c_4' \equiv c_4' \pmod 4$$

et

$$a_6 = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3} \equiv \left(\frac{\pi^2}{2}\right)c_6' \pmod 4$$

car $\varepsilon^2 \equiv 1 \pmod 4$. On a enfin

$$j' = \left(\frac{2}{\pi^2}\right)^8 \frac{a_4^3}{a_6^2 + 4(a_4/3)^3} \equiv \frac{a_4^3}{a_6^2} \pmod{2\pi}.$$

D'où $a_4^3 \equiv a_6^2 + \pi^2 \pmod{2\pi}$, d'après la condition (C2). Or, a_6 étant une unité de $\mathcal{O}_K$, on a $a_6^2 \equiv 1 \pmod 2$. D'où $a_4 \equiv 1 \pmod 2$ et $a_4^2 \equiv 1 \pmod 4$. D'où le résultat.

Lemme 46 *Supposons que E soit de type IV^*. Alors, $c_6' \equiv 2/\pi^2 \pmod 2$.*

DÉMONSTRATION : D'après le lemme 45, on a $v(\Delta_m) = 8$. Donc, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. On considère alors le modèle (W) de E de la proposition 8. On a $a_4 \equiv 1 \pmod 2$ et $a_6 \equiv (\pi^2/2)c_6' \pmod 2$. D'après [3, prop.1] appliquée à $r = t = 1$, on a alors, comme E correspond à un cas 8 de Tate,

$$0 \equiv a_6 + a_4 \equiv 1 + \left(\frac{\pi^2}{2}\right)c_6' \pmod 2.$$

D'où le résultat.

Lemme 47 *Supposons que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$ et $c_6' \equiv 2/\pi^2 \pmod 2$. Alors, la courbe E est de type IV^* si et seulement si $a_4 + a_6 \equiv 0$ ou $\pi^2 + \pi^3 \pmod 4$.*

DÉMONSTRATION : D'après l'appendice B, la courbe E correspond à un cas 3, 4, 6, 7 ou 8 (type IV^*) de Tate. Pour le modèle (W) de E de la proposition 8, on a, avec les notations de [5],

$$b_2 = 0; \quad b_4 = 2a_4 = -\frac{6}{\varepsilon^2}c_4'; \quad b_6 = 4a_6 = -4\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3};$$

$$b_8 = -a_4^2 = -9\frac{c_4'^2}{\varepsilon^4}.$$

D'après les hypothèses faites et la proposition 8, on a $a_6 \equiv (\pi^2/2)c_6' \equiv 1 \pmod 2$ et $a_4 \equiv 1 + \pi^2 \pmod{2\pi}$. Donc, d'après [3, prop.1] appliqué à $r = t = 1$, on est dans un cas ≥ 4 de Tate. De plus, comme $\varepsilon \equiv \pm 1 \pmod 4$, on a

$$b_8 + 3b_6 + 3b_4 + b_2 + 3 \equiv -9 - 4 - 18(1 + \pi^2) + 3 \equiv 0 \pmod{4\pi}.$$

Donc d'après [3, prop.2] appliqué à $r = 1$, on est dans un cas ≥ 5 de Tate. Vérifions que l'on n'est jamais dans un cas 7 de Tate. En effet, d'après ce qui précède, $r = 1$ satisfait à la condition (a) de [3, prop. 3] et $s = 1$ satisfait à la condition (b). D'où le fait que l'on n'est jamais dans un cas 7 de Tate. Autrement dit, on est dans un cas 8 de Tate si et seulement si on n'est pas dans un cas 6, c'est-à-dire, d'après [3, prop.3(b)], si et seulement si il existe t dans $\mathcal{O}_K$ tel que $a_6 + a_4 + 1 \equiv t^2 \pmod 4$. Or, $a_6 + a_4 + 1$ étant une unité de $\mathcal{O}_K$, on en déduit que $t \in \mathcal{U}_K$ et on conclut avec le lemme 7.

Proposition 9 *On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites*

1. *on a $v(\Delta) \equiv 8 \pmod{12}$;*
2. *il existe $(a, b) \in \mathcal{L}_2$ tel que $c_4' \equiv a \pmod 4$ et $c_6' \equiv b \pmod 4$.*

Démonstration : Supposons $|\Phi| = 3$. D'après [2, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 45, E est de type IV^* (cas 8 de Tate) et $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. D'après le lemme 46, on a de plus, $c_6' \equiv 2/\pi^2 \pmod 2$. Donc d'après le lemme 47 on a $a_4 + a_6 \equiv 0$ ou $\pi^2 + \pi^3 \pmod 4$. Or, d'après la proposition 8, on a

$$a_4 + a_6 \equiv c_4' + \left(\frac{\pi^2}{2}\right) c_6' \pmod 4$$

On en déduit que l'on a, ou bien $c_4' \equiv -(\pi^2/2)c_6' \pmod 4$, ou bien, $c_4' \equiv -(\pi^2/2)c_6' + \pi^2 + \pi^3 \pmod 4$. En distinguant chaque fois selon les quatre valeurs possibles pour $c_6' \pmod 4$, on obtient les huit couples $(c_4' \pmod 4, c_6' \pmod 4)$ possibles. On vérifie alors qu'il existe $(a, b) \in \mathcal{L}_2$ tel que a (resp. b) soit un représentant de c_4' (resp. c_6') modulo 4.

Réciproquement, si les deux conditions de l'énoncé sont satisfaites, alors d'après l'appendice B, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. On vérifie de plus que l'on a nécessairement $c_6' \equiv 2/\pi^2 \pmod 2$. D'après la proposition 8 et la seconde hypothèse, il vient alors :

$$a_4 + a_6 \equiv c_4' + \left(\frac{\pi^2}{2}\right) c_6' \equiv 0 \text{ ou } \pi^2 + \pi^3 \pmod 4$$

Donc d'après le lemme 47, E est de type IV^*. D'où $|\Phi| = 3$ d'après [2, th.2(i)].

3.8.4 Cas où $v(j) = 20$

On suppose que le modèle de Weierstrass de E vérifie $v(j) = 20$ et la condition (C1'), i.e. $c'_4 \equiv 1 + \pi \pmod 2$.

Lemme 48 *La courbe E n'est pas de type IV^*. Supposons qu'elle soit de type IV. Alors, on a $v(\Delta_m) = 4$.*

Démonstration : D'après [2, th.2(i)], si E est de type IV^*, on a $v(\Delta_m) = 8$. C'est en contradiction avec le condition $v(j) = 20$. Par ailleurs, si E est de type IV, alors $v(\Delta_m) = 4$. D'où le lemme.

Lemme 49 *Supposons $v(\Delta) \equiv 4 \pmod{12}$. Alors, on a $v(\Delta_m) = 4$ si et seulement si $c'_6 \equiv \pi^2/2 \pmod 2$.*

Démonstration : Supposons $v(\Delta) \equiv 4 \pmod{12}$. Alors, d'après l'appendice B, quitte à faire un changement de variables, on peut supposer que l'on a

$$(v(c_4), v(c_6), v(\Delta)) = (12, 14, 16).$$

Le modèle (W_0) de E est alors entier. D'après l'appendice B, il correspond à un cas 10 de Tate ou à un cas non minimal. Examinons donc à quelle condition il est minimal. Avec les notations de [5], on a, pour le modèle (W_0) de E :

$$b_6 = -4\frac{c_6}{864} = -2^3\pi^2\frac{c'_6}{\varepsilon^3}; \quad b_8 = -\left(\frac{c_4}{48}\right)^2.$$

En particulier, on a $v(b_8) = 8$, donc $r = 0$ satisfait à la condition de [3, prop.6]. S'il existe un entier x de K tel que

$$b_6 \equiv x^2 \pmod{\pi^{10}},$$

alors on a nécessairement $v(x) = 4$, car $v(b_6) = 8$. Puis, il vient

$$c'_6 \equiv \left(\frac{\pi^2}{2}\right)\left(\frac{x}{2\pi^2}\right)^2 \pmod 2.$$

D'où $c'_6 \equiv \pi^2/2 \pmod 2$ car $x/2\pi^2 \in \mathcal{U}_K$.

Réciproquement, si l'on a $c'_6 \equiv \pi^2/2 \pmod 2$, alors $x = 2\pi^2$ convient. Avec [3, prop.6], cela démontre le lemme.

Posons

$$a_4 = -3\frac{c'_4}{\varepsilon^2}; \qquad a_6 = -\frac{1}{\pi^2}\frac{1}{\varepsilon^3}\left(\left(\frac{2}{\pi^2}\right)c'_6 + \varepsilon^3\left(\frac{2}{\pi^2}\right)^2\right).$$

Proposition 10 *Supposons $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. Alors, l'équation*

$$y^2 + \frac{4}{\pi^3}y = x^3 + a_4x + a_6, \tag{W}$$

définit un modèle de Weierstrass entier de E pour lequel on a $a_4 \equiv 1 + \pi \pmod 2$.

DÉMONSTRATION : Le changement de variables

$$X = x; \qquad Y = y + \frac{2}{\pi^3}$$

transforme le modèle (W_0) de E en le modèle de la proposition.

Le coefficient $4/\pi^3$ est entier. Vérifions que les coefficients a_4 et a_6 sont également entiers et que l'on a $a_4 \equiv 1 + \pi \pmod 2$.

On a

$$a_4 = -3\frac{c'_4}{\varepsilon^2} \equiv -3(1+\pi) \equiv 1 + \pi \pmod 2,$$

car $c'_4 \equiv 1 + \pi \pmod 2$ d'après la condition (C1').

D'après le lemme 49, on a $c'_6 \equiv \pi^2/2 \pmod 2$. D'où

$$\pi^2 a_6 = -\frac{1}{\varepsilon^3}\left(\left(\frac{2}{\pi^2}\right)c'_6 + \varepsilon^3\left(\frac{2}{\pi^2}\right)^2\right) \equiv 0 \pmod 2,$$

car $\varepsilon \equiv 1 \pmod 2$ (lemme 10). D'où la proposition.

Lemme 50 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. *Alors, E ne correspond pas à un cas* 4 *de Tate.*

DÉMONSTRATION : D'après l'appendice B, la courbe E correspond à un cas 3 (II), 4 (III) ou 5 (IV) de Tate. Soit (W) le modèle de E de la proposition 10. Supposons qu'il corresponde à un cas ≥ 4 de Tate. D'après la congruence $a_4 \equiv 1 + \pi \pmod 2$, $r = 1$ satisfait à la première relation de divisibilité de [3, prop. 2]. On a par ailleurs, avec les notations de [5],

$$b_2 = 0; \quad b_4 = -6\frac{c'_4}{\varepsilon^2} \equiv \pi^2 \pmod{2\pi}; \quad b_6 = \left(\frac{4}{\pi^3}\right)^2 + 4a_6 \equiv \pi^2 \pmod{2\pi};$$

$$b_8 = -9\frac{c'^2_4}{\varepsilon^4} \equiv -(1+\pi)^2 \equiv -(1+\pi^2) \pmod{2\pi}.$$

Donc, $b_8 + 3b_6 + 3b_4 + b_2 + 3 \equiv -(1+\pi^2) + 3\pi^2 + 3\pi^2 + 3 \equiv 0 \pmod{2\pi}$. D'où le résultat d'après [3, prop. 2].

Lemme 51 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. *Alors, a_6 est entier et l'on a les congruences*

$$a_6 \equiv \frac{1}{\pi^2}\left(1 - \left(\frac{2}{\pi^2}\right)c'_6\right) \pmod 2 \quad \textit{et} \quad c'_6 \equiv \frac{\pi^2}{2} + 2a_6 \pmod 4.$$

DÉMONSTRATION : Sous l'hypothèse faite, on a on a $c'_6 \equiv \pi^2/2 \pmod 2$ et l'élément a_6 est entier. Comme $\varepsilon \equiv \pm 1 \pmod 4$, on a de plus,

$$-\pi^2 a_6 \equiv \left(\frac{2}{\pi^2}\right)\varepsilon c'_6 + \left(\frac{2}{\pi^2}\right)^2 \equiv \left(\frac{2}{\pi^2}\right)^2\left(1 + 3\left(\frac{2}{\pi^2}\right)c'_6\right) \pmod 4.$$

Or, $(2/\pi^2)^2 \equiv 1 \pmod 2$ et $v(1+3(2/\pi^2)c_6') \geq 2$, d'où

$$\pi^2 a_6 \equiv 1 - \left(\frac{2}{\pi^2}\right) c_6' \pmod 4$$

et la première congruence. On en déduit alors la seconde car $\pi^4 \equiv 4 \pmod{\pi^6}$.

Proposition 11 *On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites*

1. *on a $v(\Delta) \equiv 4 \pmod{12}$;*
2. *on a $c_6' \equiv \frac{\pi^2}{2} + 2 \pmod 4$ ou $c_6' \equiv \frac{\pi^2}{2} + \pi^3 \pmod 4$.*

Démonstration : Supposons $|\Phi| = 3$. D'après [2, th.2(i)], E est de type IV ou IV^*. Donc, d'après le lemme 48, E est de type IV (cas 5 de Tate) et $v(\Delta_m) = 4$. Donc, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. De plus, d'après le lemme 49, on a $c_6' \equiv \pi^2/2 \pmod 2$. Les coefficients a_4 et a_6 sont alors entiers d'après la proposition 10. Exprimons le fait que l'on n'est pas dans le cas 3 de Tate. On a $a_4 \equiv 1 \pmod \pi$, donc $r = 1$ satisfait à la première relation de divisibilité de [3, prop.1].

Supposons $a_6 \equiv 1 \pmod \pi$. Alors, $t = 1$ vérifie $t^2 - a_6 \equiv 0 \pmod \pi$. Puis,

$$a_4 + a_6 - \pi \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([3, prop. 1]). Donc $a_6 \equiv 1 \pmod 2$ car $a_4 \equiv 1 + \pi \pmod 2$ d'après la proposition 10.

Supposons $a_6 \equiv 0 \pmod \pi$. Alors, $t = 0$ vérifie $t^2 - a_6 \equiv 0 \pmod \pi$. Puis,

$$a_4 + a_6 + 1 \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([3, prop. 1]). D'où $a_6 \equiv \pi \pmod 2$ car $a_4 \equiv 1 + \pi \pmod 2$ d'après la proposition 10. La troisième condition est donc satisfaite. Autrement dit, on a $a_6 \equiv 1$ ou $\pi \pmod 2$. Or, d'après le lemme 51, on a

$$c_6' \equiv \frac{\pi^2}{2} + 2a_6 \pmod 4.$$

D'où la seconde condition.

Réciproquement, supposons les deux conditions de l'énoncé satisfaites. Alors, on a $c_6' \equiv \pi^2/2 \pmod 2$. D'après le lemme 49, on a donc $v(\Delta_m) = 4$ et on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. D'après l'appendice B, E correspond à un cas 3, 4 ou 5 de Tate. Montrons que E ne correspond pas à un cas 3 de Tate. On considère le modèle de E de la proposition 10. Comme a_4 est une unité, $r = 1$ satisfait à la première relation de divisibilité de [3, prop.1].

Par ailleurs, d'après le lemme 51, on a

$$a_6 \equiv \frac{1}{\pi^2}\left(1 - \left(\frac{2}{\pi^2}\right) c_6'\right) \pmod 2.$$

D'où, $a_6 \equiv 1$ ou $\pi \pmod 2$.

Supposons $a_6 \equiv 1 \pmod 2$. Alors, $t = 1$ satisfait à la seconde relation de divisilité de [3, prop.1] et $a_4 + a_6 - \pi \equiv 0 \pmod 2$, donc on est dans un cas ≥ 4 de Tate. De même, si $a_6 \equiv \pi \pmod 2$, alors, $t = 0$ convient et $a_4 + a_6 + 1 \equiv 0 \pmod 2$ et on est encore dans un cas ≥ 4 de Tate. Par ailleurs, d'après le lemme 50, on n'est pas dans un cas 4 de Tate. On est donc dans un cas 5 (type IV) et $|\Phi| = 3$, d'après [2, th.2(i)].

3.8.5 Cas où $v(j) \geq 24$

On suppose que le modèle de Weierstrass de E vérifie $v(j) \geq 24$ et que 3 ne divise pas $v(\Delta)$.

Lemme 52 *On suppose $(v(c_4), v(c_6), v(\Delta)) = (\geq 11, 10, 8)$. Alors, E est de type IV^* si et seulement si on a $c'_6 \equiv \frac{\pi^2}{2} \pmod 4$ ou $c'_6 \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.*

Démonstration : On considère le modèle (W_0) de E. Sous l'hypothèse faite, ce modèle est entier et il correspond à un cas 3, 6 ou 8 (type IV^*) de Tate (d'après l'appendice B). De plus, on a

$$-\frac{c_4}{48} = -\frac{3}{\varepsilon^2}\pi^{v(c_4)-8}c'_4 \quad \text{et} \quad -\frac{c_6}{864} = -\left(\frac{2}{\pi^2}\right)\frac{c'_6}{\varepsilon^3}. \tag{30}$$

Les deux premières relations de congruence de [3, prop.1] sont satisfaites par $r = 0$ et $t = 1$, puis

$$-\frac{c_6}{864} - 1 \equiv \left(\frac{2}{\pi^2}\right)c'_6 - 1 \pmod 2.$$

Autrement dit, on est dans un cas ≥ 4 si et seulement si $c'_6 \equiv \pi^2/2 \pmod 2$. Avec les notations de [5], on a $b_8 = -(c_4/48)^2$, donc $v(b_8) \geq 6$ et $r = 0$ satisfait la condition (a) de [3, prop.3]. On conclut alors que E est de type IV^* si et seulement si il existe t dans $\mathcal{O}_K$ tel que $-c_6/864 \equiv t^2 \pmod 4$. D'après le lemme 7 et la seconde égalité (30), c'est le cas si et seulement si $c'_6 \equiv \frac{\pi^2}{2} \pmod 4$ ou $c'_6 \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$. D'où le lemme.

Lemme 53 *On suppose $v(\Delta) \equiv 4 \pmod{12}$. Alors, on a $v(\Delta_m) = 4$ si et seulement si $c'_6 \equiv \frac{\pi^2}{2} \pmod 2$.*

Démonstration : D'après l'appendice B, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 14, 14, 16)$. Le modèle (W_0) de E est alors entier. De plus, on a $v(\Delta_m) = 4$ si et seulement si ce modèle est non minimal, c'est-à-dire, toujours d'après l'appendice B, si et seulement si il ne correspond pas à un cas 10 de Tate. Avec les notations de [5], on a $b_8 = -(c_4/48)^2$ et $v(c_4/48) \geq 6$, donc $v(b_8) \geq 12$. On en déduit que $r = 0$ satisfait la première relation de congruence de [3, prop.6]. Par ailleurs,

pour ce modèle, on a $b_6 = -4c_6/864 = -8\pi^2 c'_6/\varepsilon^3$. Puis, le modèle (W_0) est non minimal si et seulement si il existe x dans $\mathcal{O}_K$ tel que

$$-8\pi^2 \frac{c'_6}{\varepsilon^3} \equiv x^2 \pmod{\pi^{10}}.$$

Autrement dit, si et seulement si il existe x dans $\mathcal{O}_K$ tel que $8\pi^2 c'_6 \equiv x^2 \pmod{\pi^{10}}$. Comme c'_6 est une unité de $\mathcal{O}_K$, si un tel x existe, on a nécessairement $v(x) = 4$ et la congruence ci-dessus équivaut à $c'_6 \equiv (\pi^2/2)(x/2\pi^2)^2 \pmod 2$, puis $c'_6 \equiv \pi^2/2 \pmod 2$ d'après le lemme 7. Réciproquement, si $c'_6 \equiv \pi^2/2 \pmod 2$, alors $x = 2\pi^2$ satisfait à la congruence ci-dessus. Cela démontre le lemme.

Posons

$$a_4 = -3\frac{c'_4}{\varepsilon^2}\pi^{v(c_4)-8}; \qquad a_6 = -\frac{1}{\pi^6}\left(4 + 2\pi^2 \frac{c'_6}{\varepsilon^3}\right).$$

Proposition 12 *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. *Alors, l'équation*

$$y^2 + \frac{4}{\pi^3} y = x^3 + a_4 x + a_6, \tag{W}$$

définit un modèle de Weierstrass entier de E.

Démonstration : Le changement de variables

$$X = x; \qquad Y = y + \frac{2}{\pi^3}$$

transforme le modèle (W_0) de E en le modèle de la proposition. Les coefficients $4/\pi^3$ et a_4 sont entiers. Vérifions que c'est également le cas pour a_6. D'après le lemme 53, on a $c'_6 \equiv \frac{\pi^2}{2} \pmod 2$. Puis,

$$-\pi^6 a_6 = 4 + 2\pi^2 \frac{c'_6}{\varepsilon^3} \equiv 4 + 2\pi^2 c'_6 \pmod{\pi^6}.$$

Comme $4 \equiv \pi^4 \pmod{\pi^6}$, on a donc $-\pi^6 a_6 \equiv 0 \pmod{\pi^6}$ et a_6 est entier. D'où la proposition.

Lemme 54 *On suppose* $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. *Alors, E est de type IV si et seulement si on a* $c'_6 \equiv \frac{\pi^2}{2} \pmod 4$ *ou* $c'_6 \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.

Démonstration : On considère alors le modèle (W) de E de la proposition 12. Il correspond, d'après l'appendice B, à un cas 3 ou 5 (type IV) de Tate. Comme $v(a_4) \geq 2$ (car $v(c_4) \geq 10$), $r = 0$ satisfait à la première relation de congruence de [3, prop.1]. On est donc dans un cas 5 de Tate si et seulement si il existe t dans $\mathcal{O}_K$ tel que $a_6 \equiv t^2 + t\pi \pmod 2$, autrement dit, si et seulement si $a_6 \equiv 0$ ou $1 + \pi \pmod 2$. Or, comme $-\pi^6 a_6 \equiv 4 + 2\pi^2 \varepsilon c'_6 \pmod{\pi^8}$, la congruence $a_6 \equiv 0 \pmod 2$ équivaut à $c'_6 \equiv -\frac{4}{2\pi^2\varepsilon} \equiv \pi^2/2 \pmod 4$. De même, $a_6 \equiv 1 + \pi \pmod 2$ équivaut à $c'_6 \equiv -\frac{4}{2\pi^2\varepsilon} + \frac{\pi^6}{2\pi^2\varepsilon} + \frac{\pi^7}{2\pi^2\varepsilon} \equiv \pi^2/2 + 2 + \pi^3 \pmod 4$. D'où le lemme.

Proposition 13 *On a* $|\Phi| = 3$ *si et seulement si les deux conditions suivantes sont satisfaites*

1. *on a* $v(\Delta) \equiv 4 \pmod{12}$ *ou* $v(\Delta) \equiv 8 \pmod{12}$ *;*
2. *on a* $c_6' \equiv \frac{\pi^2}{2} \pmod 4$ *ou* $c_6' \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.

Démonstration : On suppose que l'on a $|\Phi| = 3$. Alors, d'après [2], E est de type IV ou IV^*. Supposons qu'elle soit de type IV. Dans ce cas, $v(\Delta_m) = 4$ et quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. Puis d'après le lemme 54, on a $c_6' \equiv \frac{\pi^2}{2} \pmod 4$ ou $c_6' \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$. D'où la première condition de l'énoncé. De même, si la courbe E est de type IV^*, alors, d'après [2], on a $v(\Delta_m) = 8$ et quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 11, 10, 8)$. D'après le lemme 52, on a donc $c_6' \equiv \frac{\pi^2}{2} \pmod 4$ ou $c_6' \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4$.

Réciproquement, supposons que les deux conditions de l'énoncé soient satisfaites. Si $v(\Delta) \equiv 4 \pmod{12}$, comme $c_6' \equiv \pi^2/2 \pmod 2$, on a $v(\Delta_m) = 4$ d'après le lemme 53. Quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. On conclut avec le lemme 54 que la courbe E est de type IV. De même, si $v(\Delta) \equiv 8 \pmod{12}$, alors d'après l'appendice B, quitte à faire un changement de variables, on peut supposer que l'on a $(v(c_4), v(c_6), v(\Delta)) = (\geq 11, 10, 8)$ et on conclut que la courbe E est de type IV^* avec le lemme 52. Autrement dit, E est de type IV ou IV^* et $|\Phi| = 3$ d'après [2, th.2]. D'où la proposition.

A Exemples

On montre dans cet appendice que tous les cas du théorème 2 se réalisent. C'est immédiat pour les assertions 1, 2 et 3 en raison de l'existence d'une courbe elliptique sur K d'invariant j donné. On adopte dans toute cette section les notations de [5].

A.1 Cas où $v(j) \geq 24$

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{13}}{48}x - \frac{\pi^{12}}{864}$$

vérifie $v(j) = 27$ et $v(\Delta) = 12$. D'après le théorème 2, on a $|\Phi| = 2$ et le cas $11(a)$ se réalise.

Vérifions qu'il en va de même du cas $11(b)$. La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{11}}{48}x - \frac{\pi^{10}a}{864}, \quad \text{avec } a \in \mathcal{U}_K,$$

vérifie $v(j) = 25$ et $v(\Delta) = 8$. D'après le théorème 2, on a donc

$$|\Phi| = \begin{cases} 3 & \text{si } a \equiv 2/\pi^2 \pmod 4 \text{ ou } a \equiv 2/\pi^2 + 2 + \pi^3 \pmod 4 \\ 6 & \text{sinon.} \end{cases}$$

et le cas $11(b)$ se réalise également.

A.2 Cas où $v(j) = 16$, 18 et 20

Pour $i = 16$, 18 ou 20, l'équation

$$y^2 + \pi^2 xy = x^3 - \frac{36\pi^8}{\pi^i - 1728}x - \frac{\pi^{12}}{\pi^i - 1728} \tag{31}$$

définit un modèle entier d'une courbe elliptique sur K d'invariant modulaire $j = \pi^i$. En particulier, on a $j' = 1$. De plus, on a

$$\begin{aligned} c_4 = \pi^8 + \frac{1728\pi^8}{\pi^i - 1728} &= \pi^8 \left(1 - \frac{1}{1 - \frac{\pi^i}{1728}}\right) \\ &= \frac{\pi^{8+i}}{1728}\left(1 + \sum_{k\geq 1}\left(\frac{\pi^i}{1728}\right)^k\right). \end{aligned}$$

Donc, en particulier, $v(c_4) = 8 + i - 12$ et $c_4' \equiv \frac{\pi^{12}}{3^3.2^6} \equiv 1/\varepsilon^3 \equiv 1 \pmod 2$. Autrement dit, la courbe ci-dessus ne vérifie ni la condition (C1'), ni la condition (C2). Cela démontre que les cas $8(b)$ et $10(b)$ du théorème 2 se réalisent.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{12}(1+\pi)}{48}x - \frac{\pi^{15}}{864} \tag{32}$$

vérifie $v(j) = 18$ et $c_4' = 1 + \pi$. La condition (C1') est donc vérifiée. Avec l'exemple précédent pour $i = 18$, cela montre que le cas 9 se réalise également.

A.2.1 Cas où $v(j) = 16$ et la condition (C2) est vérifiée

On commence par démontrer le résultat suivant.

Proposition 14 *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 = x^3 + a_4 x + a_6,$$

avec a_4 et a_6 deux unités vérifiant $a_4 \equiv a_6^2 + \pi^2 \pmod{2\pi}$. Alors, on a

$$(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8) \quad \textit{et} \quad j' \equiv 1 + \pi^2 \pmod{2\pi}.$$

DÉMONSTRATION : On a $b_2 = 0$, $b_4 = 2a_4$, $b_6 = 4a_6$ et $b_8 = -a_4^2$. Donc,

$$c_4 = -48a_4, \quad c_6 = -864a_6 \quad \text{et} \quad \Delta = -16(4a_4^3 + 27a_6^2).$$

Comme a_4 et a_6 sont deux unités de $\mathcal{O}_K$, on a, en particulier, $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. De plus, on a

$$j' = \frac{a_4^3}{a_6^2 + 4(a_4/3)^3} \equiv \frac{a_4^3}{a_6^2} \pmod{2\pi}.$$

Or, $a_4^2 \equiv 1 \pmod{2\pi}$, car $a_4 \equiv a_6^2 \pmod 2$. D'où, $j' \equiv a_4/a_6^2 \equiv 1 + \pi^2 \pmod{2\pi}$. Cela démontre la proposition.

Exemple 1 *La courbe E d'équation*

$$y^2 = x^3 - x + 1$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$, la condition (C2) et $|\Phi| = 3$.

DÉMONSTRATION : Les deux premières propriétés résultent de la proposition 14. De plus, on a

$$c_4' = \frac{48}{\pi^8} = \frac{1}{3}\varepsilon^2 \equiv -1 \pmod 4 \quad \text{et} \quad c_6' = -\frac{864}{\pi^{10}} = -\frac{2^5 \cdot 3^3}{\pi^{10}} \equiv \frac{2}{\pi^2} \pmod 4.$$

Le couple $(-1, 2/\pi^2) \in \mathcal{L}_2$ est alors un représentant modulo 4 du couple (c_4' (mod 4), c_6' (mod 4)). On conclut que l'on a $|\Phi| = 3$ avec l'assertion 8 du théorème 2.

Exemple 2 *La courbe E d'équation*

$$y^2 = x^3 + x + 1 + \pi$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$, la condition (C2) et $|\Phi| = 6$.

DÉMONSTRATION : Les deux premières propriétés résultent de la proposition 14. De plus, on a

$$c_6' = -\frac{864}{\pi^{10}}(1 + \pi) \equiv \frac{2}{\pi^2} + \pi \pmod 2.$$

En particulier, il n'existe aucun couple (a, b) de $\mathcal{L}_2$ tel que $c_6' \equiv b \pmod 4$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 8 du théorème 2.

Cela démontre que tous les cas de l'assertion 8 se réalisent.

A.2.2 Cas où $v(j) = 20$ et la condition (C1') est vérifiée

On commence par démontrer le résultat suivant.

Proposition 15 *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 + \frac{4}{\pi^3} y = x^3 + a_4 x + a_6,$$

avec $a_4 \equiv 1 + \pi \pmod 2$. Alors, on a

$$(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4) \quad et \quad c'_4 \equiv 1 + \pi \pmod 2.$$

Démonstration : On a $b_4 = 2a_4$ et donc $v(b_4) = 2$. On en déduit que $c_4 = -24b_4$ vérifie $v(c_4) = 8$, puis $c'_4 = -\frac{2^4 \cdot 3}{\pi^8} a_4 = -3 \left(\frac{2}{\pi^2}\right)^4 a_4 \equiv 1 + \pi \pmod 2$. De même, on a $b_6 = (4/\pi^3)^2 + 4a_6$ et donc $v(b_6) = 2$. D'où, $c_6 = -216 b_6$ vérifie $v(c_6) = 8$. Enfin, $\Delta = -8b_4^3 - 27b_6^2$ vérifie $v(\Delta) = 4$. D'où la proposition.

Exemple 3 *La courbe E d'équation*

$$y^2 + \frac{4}{\pi^3} y = x^3 + (1 + \pi)x + 1$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$, la condition (C1') et $|\Phi| = 3$.

Démonstration : Les deux premières propriétés résultent de la proposition 15. De plus, on a

$$c'_6 = -\frac{432}{\pi^8} \left(2 + \frac{8}{\pi^6}\right) \equiv 2 + \frac{8}{\pi^6} \equiv \frac{\pi^2}{2} + 2 \pmod 4.$$

On conclut que l'on a $|\Phi| = 3$ avec l'assertion 10 du théorème 2.

Exemple 4 *La courbe E d'équation*

$$y^2 + \frac{4}{\pi^3} y = x^3 + (1 + \pi)x$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$, la condition (C1') et $|\Phi| = 6$.

Démonstration : Les deux premières propriétés résultent de la proposition 15. De plus, on a

$$c'_6 = -\frac{3456}{\pi^6} \equiv -\frac{1}{3} \left(\frac{\pi^2}{2}\right) \varepsilon^4 \equiv \frac{\pi^2}{2} \pmod 4.$$

On conclut que l'on a $|\Phi| = 6$ avec l'assertion 10 du théorème 2.

Cela démontre que tous les cas de l'assertion 10 se réalisent.

A.3 Cas où $v(j) = 12$

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^9}{48}x - \frac{\pi^{14}}{864}$$

vérifie $v(j) = 12$ et $2v(c_6) = 3v(c_4)+1$. Cela montre que le cas 7a du théorème 2 se réalise.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{10}a}{48}x - \frac{\pi^{16}}{864}, \quad \text{où } a \in \mathcal{U}_K$$

vérifie $v(j) = 12$ et $2v(c_6) = 3v(c_4) + 2$. Elle vérifie la condition (C1') si et seulement si $a \equiv 1 + \pi \pmod 2$. Elle vérifie la condition (C3) si et seulement si on a $a \equiv 1 + \pi^2 \pmod 4$ ou $a \equiv 1 + \pi^3 \pmod 4$. Cela montre que le cas 7b du théorème 2 se réalise.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^9}{48}x - \frac{\pi^{15}}{864}$$

vérifie $v(j) = 12$ et $2v(c_6) = 3v(c_4)+3$. Cela montre que le cas 7c du théorème 2 se réalise.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{10}a}{48}x - \frac{\pi^{17}}{864}, \quad \text{où } a \in \mathcal{U}_K$$

vérifie $v(j) = 12$, $v(c_4) = 10$ et $2v(c_6) - 3v(c_4) = 4$. Elle vérifie la condition (C3) si et seulement si on a $a \equiv 1 + \pi^2 \pmod 4$ ou $a \equiv 1 + \pi^3 \pmod 4$. Cela montre que le cas 7d du théorème 2 se réalise.

Cela démontre que tous les cas de l'assertion 7 se réalisent.

A.4 Cas où $v(j) = 4$, 6 ou 8

On considère la courbe $\widetilde{E}$ d'équation (2) déduite de la courbe d'équation (31). Elle vérifie $v(j) = 24 - i$, où $i = 16$, 18 ou 20, c'est-à-dire $v(j) = 4$, 6 ou 8. Ses invariants standard sont notés $(\widetilde{c_4}, \widetilde{c_6}, \widetilde{\Delta})$ et satisfont d'après le lemme 23 aux congruences suivantes :

$$\widetilde{\Delta} \equiv c_4' \pmod 2 \quad \text{et} \quad \widetilde{j'} \equiv 1 \pmod 4.$$

En particulier, $\widetilde{E}$ ne vérifie ni la condition (C1), ni la condition (C2). Cela démontre que les cas $4(b)$ et $6(b)$ du théorème 2 se réalisent.

De même, la courbe $\widetilde{E}$ d'équation (2) déduite de la courbe d'équation (32) vérifie $v(j) = 6$ et la condition (C1). Avec l'exemple précédent, cela montre que le cas 5 se réalise également.

A.4.1 Cas où $v(j) = 4$ et la condition (C1) est vérifiée

On commence par démontrer le résultat suivant qui est une réciproque partielle à la proposition 3.

Proposition 16 *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$a_6 + \varepsilon a_2 \equiv \pi^3 \pmod 4 \quad \textit{et} \quad \pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right) \equiv a_4 - \varepsilon \pmod 4.$$

Alors, on a

$$(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8), \quad c_6' \equiv 1 \pmod 2 \quad \textit{et} \quad \Delta' \equiv 1 + \pi \pmod 2.$$

Démonstration : On a tout d'abord,

$$b_2 = \left(\frac{2}{\pi}\right)^2 + 4a_2; \quad b_4 = \frac{2^3}{\pi^4} + 2a_4; \quad b_6 = \left(\frac{4}{\pi^3}\right)^2 + 4a_6;$$

$$b_8 = \left(\frac{2}{\pi}\right)^2 a_6 - \frac{2^3}{\pi^4}a_4 + 4a_2a_6 + \frac{2^4}{\pi^6}a_2 - a_4^2$$

On en déduit, avec la définition de ε, que l'on a

$$b_2 = \frac{\pi^2}{3}\varepsilon + 4a_2; \quad b_4 = \frac{2}{3}\varepsilon + 2a_4; \quad b_6 = \frac{\pi^2}{9}\varepsilon^2 + 4a_6$$

et

$$b_8 = \frac{\pi^2}{3}\varepsilon a_6 - \frac{2}{3}\varepsilon a_4 + 4a_2a_6 + \frac{\pi^2}{9}\varepsilon^2 a_2 - a_4^2.$$

En utilisant les congruences $a_2 \equiv a_6 \pmod 2$ et $a_4 \equiv \varepsilon \pmod{2\pi}$, il vient alors

$$v(b_2) = 2, \quad v(b_4) \geq 5, \quad v(b_6) = 2 \quad \text{et} \quad v(b_8) = 0.$$

On en déduit que $c_4 = b_2^2 - 24b_4$ vérifie $v(c_4) = 4$ et $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ vérifie $v(c_6) = 6$. De plus, on a $c_6' \equiv -b_2^3/\pi^6 \pmod 2$, puis, comme $b_2/\pi^2 \equiv 1 \pmod 2$, il vient $c_6' \equiv 1 \pmod 2$.

Il reste donc à montrer que l'on a, d'une part $v(\Delta) = 8$ et, d'autre part $\Delta' \equiv 1 + \pi \pmod 2$. C'est équivalent à montrer $\Delta \equiv \pi^8 + \pi^9 \pmod{\pi^{10}}$. On utilise pour ce faire les congruences suivantes que l'on démontre ci-dessous.

$$b_2^2 \equiv \pi^4 + 2\pi^6 a_2 + \pi^8 a_2^2 \pmod{\pi^{10}} \tag{33}$$

$$-27b_6^2 \equiv \pi^4 + \pi^8 + 2\pi^6 a_6 + \pi^8 a_6^2 \pmod{\pi^{10}} \tag{34}$$

$$b_8 \equiv 1 + \pi^5 + 4a_2^2 + 2\pi^2 a_2 \pmod{\pi^6} \tag{35}$$

$$9b_2b_4b_6 \equiv 2\pi^4(a_4 - \varepsilon) \pmod{\pi^{10}}. \tag{36}$$

D'après les égalités précédentes, on a

$$b_2^2 = \frac{\pi^4}{9}\varepsilon^2 + 16a_2^2 + 8\frac{\pi^2}{3}\varepsilon a_2.$$

Or, on a $\varepsilon^2/9 \equiv 1 \pmod{\pi^6}$, $4 \equiv \pi^4 \pmod{\pi^6}$ et $16 \equiv \pi^8 \pmod{\pi^{10}}$. Cela démontre la congruence (33). Pour les mêmes raisons, on a

$$b_6^2 = \frac{\pi^4}{3^4}\varepsilon^4 + 16a_6^2 + 8\frac{\pi^2}{9}\varepsilon a_6 \equiv \pi^4 + 2\pi^6 a_6 + \pi^8 a_6^2 \pmod{\pi^{10}}.$$

Puis, $-27 \equiv -3 \equiv 1 + \pi^4 \pmod{\pi^6}$. D'où la congruence (34).

Montrons à présent la congruence (35). On a

$$\begin{aligned} b_8 &= \frac{\pi^2}{3}\varepsilon a_6 - \frac{2}{3}\varepsilon a_4 + 4a_2 a_6 + \frac{\pi^2}{9}\varepsilon^2 a_2 - a_4^2 \\ &\equiv -\pi^2\varepsilon a_6 + 2\varepsilon a_4 + 4a_2 a_6 + \pi^2 a_2 - a_4^2 \pmod{\pi^6}. \end{aligned}$$

Or, $a_2 + \varepsilon a_6 \equiv \pi^3 \pmod 4$ et $a_4 \equiv \varepsilon \pmod{2\pi}$. En particulier, $-a_4^2 \equiv 1 - 2\varepsilon a_4 \pmod{\pi^6}$ car $\varepsilon^2 \equiv 1 \pmod{\pi^6}$. On en déduit donc que l'on a

$$b_8 \equiv \pi^2(2a_2 + \pi^3) + 1 + 4a_2^2 \equiv 1 + \pi^5 + 4a_2^2 + 2\pi^2 a_2 \pmod{\pi^6}.$$

Enfin, on a $b_2 \equiv b_6 \equiv \pi^2 \pmod{\pi^6}$ et $b_4 \equiv 2(a_4 - \varepsilon) \pmod{\pi^6}$. On en déduit alors la congruence (36).

Déduisons alors des congruences (33)-(36) celle annoncée pour Δ. On a

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.$$

D'après les congruences (33) et (34) et l'hypothèse $a_2 \equiv a_6 \pmod 2$, on a $-27b_6^2 \equiv b_2^2 + \pi^8 \pmod{\pi^{10}}$. Comme $v(8b_4^3) \geq 10$, on a, d'après la congruence (36) et l'égalité ci-dessus

$$\Delta \equiv b_2^2(1 - b_8) + \pi^8 + 2\pi^4(a_4 - \varepsilon) \pmod{\pi^{10}}.$$

D'après les congruences (33) et (35), il vient alors

$$\Delta \equiv \pi^8 + \pi^9 + 4\pi^4 a_2^2 + 2\pi^6 a_2 + 2\pi^4(a_4 - \varepsilon) \pmod{\pi^{10}}.$$

Or, d'après la congruence de l'énoncé, $a_4 - \varepsilon \equiv \pi^2 a_2^2 + 2a_2 \pmod 4$, on a $+2\pi^4(a_4 - \varepsilon) \equiv 4\pi^4 a_2^2 + 2\pi^6 a_2 \pmod{\pi^{10}}$. En remplaçant dans la congruence ci-dessus, on obtient alors

$$\Delta \equiv \pi^8 + \pi^9 \pmod{\pi^{10}},$$

ce qui était le résultat cherché. Cela achève de démontrer la proposition 16.

Exemple 5 *Supposons K dans Ω_1. La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 - x^2 + (1 + \pi^3)x + 1 + \pi^3$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$, la condition (C1) et $|\Phi| = 3$.

DÉMONSTRATION : Les deux premières propriétés résultent de la proposition 16. De plus, on a

$$c'_6 = -37\frac{2^6}{\pi^{12}} - 3\cdot 5\frac{2^6}{\pi^{10}} + 3\frac{2^5}{\pi^8} \pmod 4.$$

D'où $c'_6 \equiv \varepsilon + 2 + \pi^2 \pmod 4$. Or, comme K est dans Ω_1, on a $c'_6 \equiv 1 + \pi^3 \pmod 4$. On conclut que l'on a $|\Phi| = 3$ avec l'assertion 4 du théorème 2.

Exemple 6 *Supposons K dans Ω_1. La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + x + \pi^3$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$, la condition (C1) et $|\Phi| = 6$.

DÉMONSTRATION : Les deux premières propriétés résultent de la proposition 16. De plus, on a

$$c'_6 = -37\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} \equiv \varepsilon + 2 \pmod 4.$$

Or, comme K est dans Ω_1, on a $c'_6 \equiv 1 + \pi^2 + \pi^3 \pmod 4$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 4 du théorème 2.

Exemple 7 *Supposons K dans Ω_2. La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 - x + \pi^3$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$, la condition (C1) et $|\Phi| = 3$.

DÉMONSTRATION : Les deux premières propriétés résultent de la proposition 16. De plus, on a

$$c'_6 = -37\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} \equiv \varepsilon + 2 \pmod 4.$$

Or, comme K est dans Ω_2, on a $c'_6 \equiv 1 \pmod 4$. On conclut que l'on a $|\Phi| = 3$ avec l'assertion 4 du théorème 2.

Exemple 8 *Supposons K dans Ω_2. La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + x^2 - x + 1 + \pi^3$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$, la condition (C1) et $|\Phi| = 6$.

DÉMONSTRATION : Les deux premières propriétés résultent de la proposition 16. De plus, on a

$$c'_6 = -37\frac{2^6}{\pi^{12}} + 3\cdot 5\frac{2^6}{\pi^{10}} - 3\cdot 5\frac{2^5}{\pi^8} \pmod 4.$$

D'où $c'_6 \equiv \varepsilon + 2 + \pi^2 \pmod 4$. Or, comme K est dans Ω_2, on a $c'_6 \equiv 1 + \pi^2 \pmod 4$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 4 du théorème 2.

Cela démontre que tous les cas de l'assertion 4 se réalisent.

A.4.2 Cas où $v(j) = 8$ et la condition (C2) est vérifiée

On commence par démontrer le résultat suivant.

Proposition 17 *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 + \frac{2}{\pi}xy = x^3 + a_2x^2 + a_4x + a_6,$$

avec $a_4 \equiv 1 \pmod 2$ et $a_6 \equiv 1 \pmod \pi$. Alors, on a

$$(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4), \quad c'_6 \equiv 1 \pmod 2 \quad \textit{et} \quad j' \equiv 1 + \pi^2 \pmod{2\pi}.$$

Démonstration : On a tout d'abord,

$$b_2 = \left(\frac{2}{\pi}\right)^2 + 4a_2; \quad b_4 = 2a_4; \quad b_6 = 4a_6; \quad b_8 = \left(\frac{2}{\pi}\right)^2 a_6 + 4a_2a_6 - a_4^2.$$

En particulier, il vient

$$v(b_2) = 2, \quad v(b_4) = 2, \quad v(b_6) = 4 \quad \text{et} \quad v(b_8) = 0.$$

On en déduit que $c_4 = b_2^2 - 24b_4$ vérifie $v(c_4) = 4$ et $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ vérifie $v(c_6) = 6$. De plus, on a $c'_6 \equiv -b_2^3/\pi^6 \pmod 2$, puis, comme $b_2/\pi^2 \equiv 1 \pmod 2$, il vient $c'_6 \equiv 1 \pmod 2$.

Enfin, on a $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$. Donc, en particulier, $v(\Delta) = 4$ et on a

$$j' = \frac{c_4'^3}{\Delta'} \equiv -\frac{1}{b_8} \equiv -\frac{1}{\pi^2 - a_4^2} \pmod{2\pi}.$$

Or, $a_4 \equiv 1 \pmod 2$, donc $a_4^2 \equiv 1 \pmod{2\pi}$ et $j' \equiv 1 + \pi^2 \pmod{2\pi}$. D'où la proposition 17.

Exemple 9 *La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy = x^3 + x + 1 + \pi$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$, la condition (C2) et $|\Phi| = 3$.

Démonstration : Les deux premières propriétés résultent de la proposition 17. De plus, on a

$$c'_4 = \left(\frac{2}{\pi^2}\right)^4 - 3\left(\frac{2}{\pi}\right)^4 = \frac{1}{9}\varepsilon^2 - \frac{1}{3}\varepsilon^2\pi^4.$$

Donc, en particulier, $c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \pmod{\pi^8}$. De même, on a

$$c'_6 = -\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} - 3^3\frac{2^5}{\pi^6} - 3^3\frac{2^5}{\pi^5}.$$

D'où, $c'_6 \equiv -\varepsilon/3 + 2 + 2\pi^2 + \pi^5 \equiv 5\varepsilon + 2 + 2\pi^2 + \pi^5 \pmod{\pi^6}$.

Supposons à présent $K \in \Omega_1$. Alors, on a

$$c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \equiv -\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7 \pmod{\pi^8}$$

et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 + \pi^5 \equiv -\varepsilon + \pi^4 \pmod{\pi^6}.$$

Autrement dit, le couple $(a, b) = (-\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7, -\varepsilon + \pi^4)$ de l'ensemble $\mathcal{L}_1$ vérifie $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que l'on a $|\Phi| = 3$ avec l'assertion 6 du théorème 2.

Supposons alors $K \in \Omega_2$. Alors, on a

$$c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \equiv -\varepsilon^2 + 6 + 2\pi^4 \equiv -\varepsilon^2 + 6 + \pi^6 \pmod{\pi^8}$$

et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 + \pi^5 \equiv -\varepsilon + \pi^5 \pmod{\pi^6}.$$

Autrement dit, le couple $(a, b) = (-\varepsilon^2 + 6 + \pi^6, -\varepsilon + \pi^5)$ de l'ensemble $\mathcal{L}_1$ vérifie $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que l'on a $|\Phi| = 3$ avec l'assertion 6 du théorème 2 dans ce cas également. D'où le résultat en général.

Exemple 10 *La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy = x^3 + x + 1$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$, la condition (C2) et $|\Phi| = 6$.

Démonstration : Les deux premières propriétés résultent de la proposition 17. De plus, on a

$$c'_4 = \left(\frac{2}{\pi^2}\right)^4 - 3\left(\frac{2}{\pi}\right)^4 = \frac{1}{9}\varepsilon^2 - \frac{1}{3}\varepsilon^2\pi^4.$$

Donc, en particulier, $c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \pmod{\pi^8}$. De même, on a

$$c'_6 = -\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} - 3^3\frac{2^5}{\pi^6}.$$

D'où, $c'_6 \equiv -\varepsilon/3 + 2 + 2\pi^2 \equiv 5\varepsilon + 2 + 2\pi^2 \pmod{\pi^6}$.

Supposons à présent $K \in \Omega_1$. Alors, comme dans l'exemple précédent, on a $c'_4 \equiv -\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7 \pmod{\pi^8}$ et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 \equiv -\varepsilon + \pi^4 + \pi^5 \pmod{\pi^6}.$$

Il n'existe alors aucun couple (a, b) de l'ensemble $\mathcal{L}_1$ vérifiant $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 6 du théorème 2.

Supposons alors $K \in \Omega_2$. Alors, comme dans l'exemple précédent, on a $c'_4 \equiv -\varepsilon^2 + 6 + \pi^6 \pmod{\pi^8}$ et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 \equiv -\varepsilon \pmod{\pi^6}.$$

Il n'existe alors aucun couple (a, b) de l'ensemble $\mathcal{L}_1$ vérifiant $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que l'on a $|\Phi| = 6$ avec l'assertion 6 du théorème 2 dans ce cas également. D'où le résultat en général.

Cela démontre que tous les cas de l'assertion 6 se réalisent.

B Tableaux de Papadopoulos

On explicite dans cet appendice le Tableau V de [3] dans le cas où, avec ses notations, $\lambda = 2$ (i.e. $e = 2$).

Type de Néron	II								
Cas de Tate	3								
$v(c_4)$	4	≥ 8	≥ 8	4	8	8	4	8	≥ 9
$v(c_6)$	6	8	10	6	11	≥ 12	6	12	11
$v(\Delta)$	4	4	8	6	10	12	7	13	10
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$			
$v(N)$	4	4	8	6	10	12	7	13	10

Type de Néron	III									
Cas de Tate	4									
$v(c_4)$	4	8	8	4	8	9	9	9	9	9
$v(c_6)$	6	8	10	6	11	8	10	12	13	≥ 14
$v(\Delta)$	4	4	8	6	10	4	8	12	14	15
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$	$*$			
$v(N)$	3	3	7	5	9	3	7	11	13	14

Type de Néron	IV		
Cas de Tate	5		
$v(c_4)$	4	8	≥ 10
$v(c_6)$	6	8	8
$v(\Delta)$	4	4	4
Conditions sup.	$*$	$*$	$*$
$v(N)$	2	2	2

Type de Néron	I_0^*								
Cas de Tate	6								
$v(c_4)$	8	4	8	8	4	8	≥ 10	≥ 10	≥ 10
$v(c_6)$	10	6	≥ 12	12	6	12	10	12	13
$v(\Delta)$	8	8	12	14	9	15	8	12	14
Conditions sup.	$*$	$*$	$*$	$*$			$*$	$*$	
$v(N)$	4	4	8	10	5	11	4	8	10

Type de Néron	I_1^*			I_3^*		
Cas de Tate	7			7		
$v(c_4)$	4	8	10	4	8	10
$v(c_6)$	6	10	10	6	≥ 12	12
$v(\Delta)$	8	8	8	11	12	12
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	3	3	3	4	5	5

Type de Néron	I_5^*			I_7^*		
Cas de Tate	7			7		
$v(c_4)$	4	8	10	4	8	10
$v(c_6)$	6	12	14	6	12	15
$v(\Delta)$	13	16	16	15	19	20
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	4	7	7	4	8	9

Type de Néron	I_2^*							
Cas de Tate	7							
$v(c_4)$	8	8	8	4	10	10	10	10
$v(c_6)$	≥ 12	12	12	6	12	14	≥ 15	15
$v(\Delta)$	12	14	16	10	12	16	18	19
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	6	8	10	4	6	10	12	13

Type de Néron	I_4^*					
Cas de Tate	7					
$v(c_4)$	8	8	4	10	10	10
$v(c_6)$	12	12	6	14	≥ 15	15
$v(\Delta)$	16	17	12	16	18	20
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	8	9	4	8	10	12

Type de Néron	I_6^*			
Cas de Tate	7			
$v(c_4)$	4	8	10	10
$v(c_6)$	6	12	15	15
$v(\Delta)$	14	18	20	21
Conditions sup.	$*$	$*$	$*$	$*$
$v(N)$	4	8	10	11

Type de Néron	I_ν^*, $\nu \geq 8$		
Cas de Tate	7		
$v(c_4)$	4	8	10
$v(c_6)$	6	12	15
$v(\Delta)$	$8+\nu$	$12+\nu$	$14+\nu$
Conditions sup.	$*$	$*$	$*$
$v(N)$	4	8	10

On notera à cet endroit que si $\big(v(c_4), v(c_6), v(\Delta)\big)$ est le triplet $\big(10, 15, 14+\nu\big)$ et si ν est impair ≥ 9, Papadopoulos ne donne pas de condition supplémentaire $*$, mais il en existe une pour ce triplet si ν est pair ≥ 8.

Type de Néron	IV^*		
Cas de Tate	8		
$v(c_4)$	4	8	≥ 11
$v(c_6)$	6	10	10
$v(\Delta)$	8	8	8
Conditions sup.	$*$	$*$	$*$
$v(N)$	2	2	2

Type de Néron	III*							
Cas de Tate	9							
$v(c_4)$	4	8	8	11	11	11	11	11
$v(c_6)$	6	12	≥ 12	12	14	15	16	≥ 17
$v(\Delta)$	10	14	12	12	16	18	20	21
Conditions sup.	$*$	$*$	$*$	$*$	$*$			
$v(N)$	3	7	5	5	9	11	13	14

Type de Néron	II*						
Cas de Tate	10						
$v(c_4)$	≥ 12	≥ 12	≥ 12	8	4	8	8
$v(c_6)$	15	12	14	≥ 12	6	12	12
$v(\Delta)$	18	12	16	12	11	17	16
Conditions sup.		$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	10	4	8	4	3	9	8

Type de Néron	Équation non minimale						
$v(c_4)$	≥ 12	≥ 12	≥ 12	8	4	8	8
$v(c_6)$	≥ 16	12	14	≥ 12	6	12	12
$v(\Delta)$	≥ 20	12	16	12	≥ 12	16	≥ 18
Conditions sup.		$*$	$*$	$*$	$*$	$*$	$*$

Références

[1] É. Cali. Défaut de semi-stabilité des courbes elliptiques dans le cas non ramifié. *Canad. J. Math.*, 56(4) :673–698, 2004.

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

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

[4] J.-P. Serre et J. Tate. Good reduction of abelian varieties. *Ann. of Math.*, 88 :492–517, 1968.

[5] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. in *Modular functions of one variable, Lect. Notes in Math.*, 273 :33–52, 1975.