Canad. J. Math. Vol. **56** (4), 2004 pp. 673–698

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

Élie Cali

Abstract. Let $\overline{\mathbb{Q}_2}$ be an algebraic closure of $\mathbb{Q}_2$ and K be an unramified finite extension of $\mathbb{Q}_2$ included in $\overline{\mathbb{Q}_2}$. Let E be an elliptic curve defined over K with additive reduction over K, and having an integral modular invariant. Let us denote by K_{nr} the maximal unramified extension of K contained in $\overline{\mathbb{Q}_2}$. There exists a smallest finite extension L of K_{nr} over which E has good reduction. We determine in this paper the degree of the extension L/K_{nr}.

Introduction

Étant donné un nombre premier p, soient $\overline{\mathbb{Q}_p}$ une clôture algébrique de $\mathbb{Q}_p$ et K une extension finie de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}_p}$. Soit E une courbe elliptique définie sur K ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire j est entier, *i.e.* j appartient à l'anneau de valuation de K. Soit K_{nr} l'extension non ramifiée maximale de K contenue dans $\overline{\mathbb{Q}_p}$. Il existe une plus petite extension finie L de K_{nr} sur laquelle E acquiert bonne réduction. Si E_n désigne le sous-groupe des points de n-torsion de $E(\overline{\mathbb{Q}_p})$, on a $L = K_{nr}(E_n)$ pour tout entier $n \geq 3$ non divisible par p ([4], 2, corollaire 3). Le groupe de Galois Φ de L sur K_{nr} est connu dans le cas où $p \geq 3$ (*cf.* [2]). Si $p = 2$, le groupe Φ n'est connu que dans certains cas particuliers, par exemple si $K = \mathbb{Q}_2$ (*loc. cit.*). Dans ce travail, on détermine Φ dans le cas où K est une extension finie *non ramifiée* de $\mathbb{Q}_2$. Les résultats que l'on obtient permettent de calculer directement l'ordre de Φ en fonction des coefficients d'une équation de Weierstrass minimale de E sur K.

Signalons par ailleurs que ces résultats permettent de compléter, dans le cas non ramifié, ceux obtenus dans le théorème 4 de [1] sur la détermination de la différente du corps des points de ℓ-torsion des courbes elliptiques dans le cas où $\ell \neq 2$.

Je remercie A. Kraus pour les conseils qu'il m'a donnés au cours de ce travail.

1 Énoncé des résultats

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

Reçu par la rédaction le October 9, 2002; revu le March 4, 2003.
Classification (AMS) par sujet: 11G07.

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

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

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

(C_1) : il existe $\gamma \in \mu_{r-1}$ tel que l'on ait $j' \equiv \gamma^4 + 2\gamma^5 \bmod 4$.
(C_2) : il existe un élément γ de μ_{r-1} qui n'appartient pas à μ_3 tel que l'on ait $j' \equiv \gamma^6 + 2\gamma^5(1+\gamma^2) \bmod 4$.
(C_3) : il existe $\gamma \in \mu_{r-1}$ tel que l'on ait $j' \equiv \gamma^4 + 2\gamma^3 \bmod 4$.

Le groupe $\Phi = \mathrm{Gal}(L/K_{nr})$ est soit cyclique d'ordre 2, 3, 4 ou 6, soit d'ordre 8 et isomorphe au groupe quarternionien, soit d'ordre 24 et isomorphe à $\mathrm{SL}_2(\mathbb{F}_3)$. Son ordre est donné par l'énoncé suivant :

Théorème

1. *Si* $v(j) = 0$, *on a* $|\Phi| = 2$.
2. *Si* $v(j) \in \{1, 2, 5, 7, 10, 11\}$, *on a* $|\Phi| = 24$.
3. *Si* $v(j) \in \{3, 9\}$, *on a* $|\Phi| = 8$.
4. *Supposons* $v(j) = 4$.
   (a) *Si la condition* (C_1) *est satisfaite, on a*
   $$|\Phi| = \begin{cases} 3 & \text{si le type de réduction de } E \text{ est } IV^* \\ 6 & \text{sinon.} \end{cases}$$
   (b) *Si la condition* (C_1) *n'est pas satisfaite, on a* $|\Phi| = 24$.
5. *Supposons* $v(j) = 6$.
   (a) *Si* $2v(c_6) = 3v(c_4)$, *on a*
   $$|\Phi| = \begin{cases} 4 & \text{si la condition } (C_2) \text{ est vérifiée} \\ 8 & \text{sinon.} \end{cases}$$
   (b) *Si* $2v(c_6) = 3v(c_4) + 1$, *on a*
   $$|\Phi| = \begin{cases} 4 & \text{si } j' \equiv 1 \bmod 4 \\ 8 & \text{sinon.} \end{cases}$$
   (c) *Supposons* $2v(c_6) > 3v(c_4) + 1$.
      (c.1) *Supposons* $v(c_4)$ *pair. On a* $|\Phi| = 4$ *s'il existe* $t \in \mu_3$, $t \neq 1$, *et* $\zeta \in \mu_{r-1}$ *tels que*
      $$c_4' \equiv \zeta(t+2) \bmod 4.$$
      On a $|\Phi| = 8$ *sinon.*

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

6. *Supposons $v(j) = 8$.*
   (a) *Si la condition (C_3) est satisfaite, on a*

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

   (b) *Si la condition (C_3) n'est pas satisfaite, on a $|\Phi| = 24$.*
7. *Supposons $v(j) \geq 12$.*
   (a) *Si 3 divise $v(\Delta)$, on a $|\Phi| = 2$.*
   (b) *Si 3 ne divise pas $v(\Delta)$, on a*

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

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

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

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

(i) on a $v(\Delta) = 4$ ou bien $v(\Delta) = 8$;
(ii) il existe $\zeta \in \mu_{r-1}$ tel que $c_6' \equiv \zeta \bmod 4$.

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

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

1. *Si $v(j) = 0$, on a $|\Phi| = 2$.*
2. *Si $v(j) \in \{1, 2, 5, 7, 10, 11\}$, on a $|\Phi| = 24$.*
3. *Si $v(j) \in \{3, 9\}$, on a $|\Phi| = 8$.*
4. *Supposons $v(j) = 4$.*
   (a) *Supposons qu'il existe $\gamma \in \mu_3$ tel que $j' \equiv \gamma + 2\gamma^2 \bmod 4$. On a $|\Phi| \in \{3, 6\}$. Soit $\zeta \in \mu_3$ tel que $c_6' \equiv \zeta \bmod 2$. On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont réalisées :*
      (i) *on a $v(\Delta) = 8$;*
      (ii) *on a ($\gamma = 1$ et $c_6' \equiv -\zeta \bmod 4$) ou bien ($\gamma \neq 1$ et $c_6' \equiv \zeta \bmod 4$).*
   (b) *On a $|\Phi| = 24$ sinon.*

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

5. *Supposons* $v(j) = 6$.
   (a) *Si* $2v(c_6) = 3v(c_4)$, *on a* $|\Phi| = 8$.
   (b) *Si* $2v(c_6) = 3v(c_4) + 1$, *on a*

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

   (c) *Supposons* $2v(c_6) > 3v(c_4) + 1$.
      (c.1) *Supposons* $v(c_4)$ *pair. On a* $|\Phi| = 4$ *s'il existe* $t \in \mu_3$, $t \neq 1$, *et* $\zeta \in \mu_3$ *tels que*

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

      On a $|\Phi| = 8$ *sinon.*
      (c.2) *Si* $v(c_4)$ *est impair, on a* $|\Phi| = 8$.
6. *Supposons* $v(j) = 8$.
   (a) *Supposons qu'il existe* $\gamma \in \mu_3$ *tel que* $j' \equiv \gamma + 2 \bmod 4$. *On a* $|\Phi| \in \{3, 6\}$. *On a* $|\Phi| = 3$ *si et seulement si les conditions suivantes sont réalisées :*
      (i) *on a* $v(\Delta) = 4$ *;*
      (ii) *on a* ($\gamma = 1$ *et* $c_6' \equiv 1 \bmod 4$) *ou bien* ($\gamma \neq 1$ *et* $c_6' \equiv -\gamma \bmod 4$).
   (b) *On a* $|\Phi| = 24$ *sinon.*
7. *Supposons* $v(j) \geq 12$.
   (a) *Si* 3 *divise* $v(\Delta)$, *on a* $|\Phi| = 2$.
   (b) *Supposons que* 3 *ne divise pas* $v(\Delta)$. *On a* $|\Phi| = 3$ *si les conditions suivantes sont réalisées :*
      (i) *on a* $v(\Delta) = 4$ *ou bien* $v(\Delta) = 8$ *;*
      (ii) *il existe* $\zeta \in \mu_3$ *tel que* $c_6' \equiv \zeta \bmod 4$.

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

2 Préliminaires

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

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

5. *Soit d un élément de K_{nr} tel que $v(d-1)=1$. Soit x un élément de $K_{nr}(\sqrt{d})$ tel que l'on ait $x \equiv 2y \bmod 4$, où y est un élément de K_{nr} de valuation 0. Alors, x n'est pas un carré dans $K_{nr}(\sqrt{d})$.*
6. *Soit x une unité de K_{nr}. Alors, les trois racines cubiques de x sont dans K_{nr}.*

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

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

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

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

$$(\xi^{(n+1)/2})^2 = \xi,$$

ce qui montre que ξ est un carré dans K_{nr}. D'après le lemme 7 de [2], x est donc un carré dans K_{nr}.

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

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

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

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

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

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

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

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

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

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

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

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

3 Démonstration du théorème

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

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

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

3.1 Notations

On choisit, *pour toute la suite*, une racine cubique $\Delta^{1/3}$ de Δ dans $\overline{\mathbb{Q}_2}$. Notons, à l'instar de [2] :

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

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

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

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

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

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

Les éléments A_t et B_t appartiennent à K_{nr} si et seulement si 3 divise $v(\Delta)$, autrement dit, si et seulement si 3 divise $v(j)$ (lemme 1, assertion 6).

On désigne par $j^{1/3}$ la racine cubique de j dans $\overline{\mathbb{Q}_2}$ définie par l'égalité

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

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

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

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

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

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

$$u \equiv \alpha + 2\alpha' \bmod 4.$$

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

$$j' \equiv \zeta + 2\zeta' \bmod 4.$$

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

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

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

3.2 L'assertion 2 du théorème

Par hypothèse, on a

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

L'égalité $3v(c_4) - v(\Delta) = v(j)$ entraîne que 3 ne divise pas $v(\Delta)$; par conséquent, on a $|\Phi| \in \{3, 6, 24\}$ ([2], théorème 3).

On a

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

3.2.1 Cas où $v(j) \in \{1, 2, 5\}$

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

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

c'est à dire

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

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

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

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

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

Cas où $v(j) = 1$ On a

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

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

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

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

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

Cas où $v(j) = 2$ On a

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

Il en résulte que l'on a

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

Cas où $v(j) = 5$ On a

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

On a dans ce cas

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

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

3.2.2 Cas où $v(j) \in \{7, 10, 11\}$

Dans ce cas, on vérifie que l'élément

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

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

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

Cas où $v(j) = 7$ On a

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

d'où

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

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

Cas où $v(j) = 10$ On a

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

On en déduit les égalités

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

Cas où $v(j) = 11$ On a

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

On a donc

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

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

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

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

3.3 Un lemme préliminaire

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

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

Démonstration On a $c_4 \neq 0$. Posons

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

On va démontrer que C n'est pas un carré dans $K_{nr}(\sqrt{B})$, ce qui prouvera le résultat ([2], théorème 3(i)b)). On vérifie que l'on a

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

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

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

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

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

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

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

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

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

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

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

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

3.4 L'assertion 3 du théorème

Par hypothèse, on a

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

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

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

3.4.1 Cas où $v(j) = 3$

Prouvons l'énoncé suivant :

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

Démonstration D'après (18), on a

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

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

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

3.4.2 Cas où $v(j) = 9$

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

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

Par conséquent, on a

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

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

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

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

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

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

On en déduit que l'on a

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

Par ailleurs, on a

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

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

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

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

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

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

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

3.5 L'assertion 4 du théorème

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

On a

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

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

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

Démonstration Soient α et α' deux éléments réalisant l'énoncé du lemme 3. Supposons que B soit un carré dans $K_{nr}(\theta)$. On va démontrer que l'on a l'égalité

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

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

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

autrement dit,

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

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

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

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

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

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

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

D'après la condition (24), on a

$$a \equiv 1 \bmod 2. \tag{27}$$

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

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

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

Par ailleurs, on a

$$u^{-1} \equiv \alpha^{-1}(1 + 2\alpha'\alpha^{-1}) \bmod 4,$$

d'où l'on déduit que

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

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

$$\alpha^7 \equiv \alpha'^4 \bmod 2.$$

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

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

$$j' \equiv \zeta + 2\zeta' \bmod 4.$$

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

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

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

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

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

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

$$\alpha^{-4} + \alpha^{-1} \equiv (\alpha^{-2} + \alpha^{-(3r-2)/2})^2 \bmod 2.$$

Il en résulte que l'on a

$$(\alpha^{-1} + \alpha'\alpha^{-2})^2 \equiv \alpha^{-2} + \alpha^{-(3r-2)/2} \bmod 2. \tag{30}$$

Par ailleurs, d'après (20), on a

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

Cela montre que B est un carré dans $K_{nr}(\theta)$ (*cf.* [2], lemme 7). D'où la proposition.

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

3.6 L'assertion 6 du théorème

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

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

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

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

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

Démonstration Soient α et α' deux éléments satisfaisant l'énoncé du lemme 3. Supposons que B soit un carré dans $K_{nr}(\theta)$. Vérifions que l'on a

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

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

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

D'après (32) et (35), on a donc

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

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

$$b^2 + 2ac = 3u. \tag{38}$$

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

$$b^2 \equiv \alpha \bmod 4.$$

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

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

$$(\alpha + \alpha')^2 \equiv \alpha^2 + \alpha^{(3r-2)/2} \bmod 2.$$

Par ailleurs, on a

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

Il en résulte que l'on a

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

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

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

3.7 L'assertion 5 du théorème

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

3.7.1 Cas où $2v(c_6) = 3v(c_4)$

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

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

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

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

Démonstration Supposons la condition (40) satisfaite. On a

$$tu^{-1} \equiv \gamma^{-2}\left(1 + 2\gamma^{-1}(1 + \gamma^2)\right) \bmod 4.$$

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

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

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

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

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

Par ailleurs, on a

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

On en déduit que

$$\frac{\alpha^2 B_t}{t^2 c_4^2} \equiv (1+t\alpha^{(3r-2)/2}+t^2\alpha)^2+2(t^2\alpha'-t\alpha^{(3r-2)/2}-\alpha^{3r/2}) \bmod 4.$$

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

$$t^2\alpha' \equiv t\alpha^{(3r-2)/2}+\alpha^{3r/2} \bmod 2. \tag{42}$$

Posons

$$\gamma = t\alpha^{(3r-2)/2}.$$

On a les égalités

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

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

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

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

Il reste à démontrer que l'on a

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

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

$$j' \equiv \gamma^6+2\gamma^5(1+\gamma^2) \bmod 4.$$

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

Par ailleurs, il existe $\zeta \in \mu_{r-1}$ et $\zeta' \in \mu_{r-1} \cup \{0\}$ tels que $j' \equiv \zeta + 2\zeta' \bmod 4$. D'après l'assertion 1 du lemme 1, on a donc $\zeta = \gamma^6$. On a ainsi $\zeta' \equiv \gamma^6(\gamma + \gamma^{-1}) \bmod 2$, puis

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

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

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

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

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

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

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

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

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

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

On en déduit le résultat suivant :

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

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

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

$$t^2u \equiv \gamma^2 + 2\gamma(1 + \gamma^2) \bmod 4.$$

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

$$t'^2u \equiv \gamma'^2 + 2\gamma'(1 + \gamma'^2) \bmod 4.$$

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

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

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

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

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

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

$$tu \equiv \gamma^2 + 2\gamma(1+\gamma^2) \bmod 4.$$

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

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

3.7.2 Cas où $2v(c_6) > 3v(c_4)$

Posons

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

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

Proposition 6

1. *Supposons* $v(\lambda) \geq 2$.
   (i) *Supposons* $v(c_4)$ *pair. On a* $|\Phi| = 4$ *s'il existe* $t \in \mu_3$, $t \neq 1$, *et* $b \in \mu_{r-1}$ *tels que* $c_4' \equiv b(t+2) \bmod 4$. *On a* $|\Phi| = 8$ *sinon.*
   (ii) *Si* $v(c_4)$ *est impair, on a* $|\Phi| = 8$.
2. *Supposons* $v(\lambda) = 1$.
   (i) *Si* $\lambda \equiv 2 \bmod 4$, *on a* $|\Phi| = 4$.
   (ii) *Si* $\lambda \not\equiv 2 \bmod 4$, *on a* $|\Phi| = 8$.

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

On a les congruences

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

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

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

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

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

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

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

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

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

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

Il s'agit alors de décider si C_s est un carré dans $K_{nr}(\sqrt{3})$ (*cf.* [2, théoréme 3]).

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

On utilise dans ce cas le résultat suivant :

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

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

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

$$c_4'(1+2\pi) \equiv \gamma + \gamma'^2\pi^2 + \gamma^{r/2}\gamma'\pi^3 \bmod 4.$$

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

$$c_4'(1+2\pi) \equiv a + b\pi^2 + (a+b)\pi^3 \bmod 4.$$

Il résulte de l'assertion 1 du lemme 1 que $a = \gamma$, $b = \gamma'^2$, puis $a + b \equiv \gamma^{r/2}\gamma' \bmod 2$. On en déduit que $(a+b)^2 \equiv ab \bmod 2$. Cela entraîne l'existence d'un élément $t \in \mu_3$, $t \neq 1$, tel que l'on ait $a \equiv tb \bmod 2$. Puisque a et tb sont des racines de l'unité d'ordre impair, on a donc $a = tb$. En particulier, b est non nul et la condition (57) est satisfaite.

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

$$c_4'(1+2\pi) \equiv bt + b\pi^2 + t^2 b\pi^3 \bmod 4.$$

Posons

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

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

$$c_4'(1+2\pi) \equiv \gamma + \gamma'^2\pi^2 + \gamma^{r/2}\gamma'\pi^3 \bmod 4,$$

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

Le lemme 5 et le théorème 3 de [2] entraînent l'assertion (i) de la proposition.

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

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

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

et l'assertion 5 du lemme 1 entraîne notre assertion. D'où l'assertion (ii) de la proposition (*cf.* [2], théorème 3).

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

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

(2.1) Supposons $\lambda \equiv 2 \bmod 4$.

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

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

$$\lambda \equiv 2\gamma \bmod 4.$$

D'après la formule (54), on a donc

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

Il en résulte que

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

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

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

Cela termine la démonstration du théorème.

4 Démonstration du corollaire

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

Pour la démonstration des assertions 4, 6 et 7, on utilisera l'article [3] de Papadopoulos et l'on suivra ses notations.

4.1 L'assertion 4 du corollaire

On a $v(j) = 4$.

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

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

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

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

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

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

Démonstration D'après le tableau IV de [3], le type de réduction de E est I_0^*, I_1^* ou IV^*. Par ailleurs, la courbe elliptique E admet un modèle minimal sur K de la forme

$$y^2 = x^3 - \frac{c_4'}{3}x - \frac{2c_6'}{27}.$$

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

Les invariants standard associés à E sont (*cf.* [5])

$$a_1 = 0, \quad a_2 = 0, \quad a_3 = 0, \quad a_4 = -\frac{c_4'}{3}, \quad a_6 = -\frac{2c_6'}{27},$$
$$b_2 = 0, \quad b_4 = -\frac{2c_4'}{3}, \quad b_6 = -\frac{8c_6'}{27}, \quad b_8 = -\frac{c_4'^2}{9}.$$

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

$$c_4' \equiv \nu \bmod 4.$$

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

$$r = -\frac{c_6'}{c_4'}.$$

On vérifie que l'on a

$$b_8 + 3rb_6 + 3r^2b_4 + 3r^4 \equiv 0 \bmod 32.$$

Posons

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

En utilisant la congruence

$$\frac{c_6'^2}{c_4'^3} \equiv 1 - \frac{12}{j'} \bmod 16,$$

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

Si l'on a $c_6' \not\equiv \zeta \bmod 4$, on a $v(a_6 + ra_4 + r^3 - t^2) = 3$ et dans ce cas le type de réduction de E est I_0^* ([3], proposition 3).

Supposons que l'on ait $c_6' \equiv \zeta \bmod 4$. On a alors $v(a_6 + ra_4 + r^3 - t^2) \geq 4$, d'où il résulte que le type de réduction de E est I_1^* ou IV^*. Posons

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

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

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

$$r = \frac{c_6'}{c_4'}.$$

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

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

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

Si $c_6' \not\equiv -\zeta \bmod 4$, on a $v(a_6 + ra_4 + r^3 - t^2) = 3$ et le type de réduction de E est I_0^*.

Si $c_6' \equiv -\zeta \bmod 4$, on a $v(a_6 + ra_4 + r^3 - t^2) \geq 4$. Avec $s = \nu/\zeta$, on vérifie que l'on a $3r \equiv s^2 \bmod 4$, et donc le type de réduction de E est IV^*. D'où le lemme.

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

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

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

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

4.2 L'assertion 6 du corollaire

On a $v(j) = 8$.

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

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

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

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

$$c_4' \equiv \alpha_1 + 2\alpha_2 \bmod 4 \quad \text{et} \quad c_6' \equiv \beta_1 + 2\beta_2 \bmod 4.$$

On a le lemme suivant :

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

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

Démonstration D'après le tableau IV de [3], le type de réduction de E est II, III ou IV. La courbe elliptique E admet un modèle minimal sur K de la forme

$$y^2 = x^3 - \frac{c_4'}{3}x - \frac{c_6'}{27}.$$

Les invariants standard associés à E sont

$$a_1 = 0, \quad a_2 = 0, \quad a_3 = 0, \quad a_4 = -\frac{c_4'}{3}, \quad a_6 = -\frac{c_6'}{27},$$

$$b_2 = 0, \quad b_4 = -\frac{2c_4'}{3}, \quad b_6 = -\frac{4c_6'}{27}, \quad b_8 = -\frac{c_4'^2}{9}.$$

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

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

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

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

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

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

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

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

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

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

De l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on déduit que l'on a la congruence $j' \equiv c_4'^3/c_6'^2 \bmod 4$. Par ailleurs, on a

$$c_4'^3 \equiv 1 + 2\alpha_1^2\alpha_2 \bmod 4 \quad \text{et} \quad c_6'^2 \equiv \beta_1^2 \bmod 4,$$

d'où il résulte que

$$j' \equiv \beta_1(1 + 2\alpha_1^2\alpha_2) \bmod 4. \tag{66}$$

D'après le lemme 7 et la congruence (66), on obtient ainsi $j' \equiv \beta_1 + 2 \bmod 4$. D'après la condition (61), on a donc

$$\gamma = \beta_1. \tag{67}$$

Si $\gamma = 1$, on déduit de (67) et (62) que $\beta_2 = 0$, d'où $c_6' \equiv 1 \bmod 4$. Si $\gamma \neq 1$, on a $\beta_2 \equiv -\gamma \bmod 2$ (*cf.* (62)), puis $c_6' \equiv -\gamma \bmod 4$. La condition (ii) de l'assertion 6 (a) est donc satisfaite.

Inversement, supposons les conditions (i) et (ii) de l'énoncé réalisées. L'égalité (65) est alors vérifiée.

Supposons que l'on ait $\gamma = 1$ et $c_6' \equiv 1 \bmod 4$. Dans ce cas, on a $\beta_1 = 1$ et $\beta_2 = 0$. Par ailleurs, on a $j' \equiv -1 \bmod 4$, et l'on déduit de (66) la congruence $\alpha_1^2\alpha_2 \equiv 1 \bmod 2$. On a donc $\alpha_1 = \alpha_2$ et la condition (62) est vérifiée.

Supposons que l'on ait $\gamma \neq 1$ et $c_6' \equiv -\gamma \bmod 4$. On a alors $\beta_1 = \beta_2 = \gamma$. D'après (61) et (66), on obtient $\alpha_1 \equiv \gamma\alpha_2 \bmod 2$. Par suite, on a $\alpha_2 = \gamma^2\alpha_1$, et la condition (62) est de nouveau vérifiée.

D'après le lemme 7, le type de réduction de E est IV, ce qui entraîne que $|\Phi| = 3$. Cela prouve l'assertion 6 (a) du corollaire.

L'assertion 6 (b) résulte directement du théorème.

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press

4.3 L'assertion 7 du corollaire

On a $v(j) \geq 12$.

Démontrons la remarque qui suit l'énoncé du théorème. C'est une conséquence du lemme suivant

Lemme 8

1. *Supposons que l'on ait* $v(c_4) \geq 6$, $v(c_6) = 5$ *et* $v(\Delta) = 4$. *Alors, le type de réduction de E est IV si et seulement si il existe* $\zeta \in \mu_{r-1}$ *tel que* $c_6' \equiv \zeta \bmod 4$.
2. *Supposons que l'on ait* $v(c_4) \geq 7$, $v(c_6) = 7$ *et* $v(\Delta) = 8$. *Alors, le type de réduction de E est* IV^* *si et seulement si il existe* $\zeta \in \mu_{r-1}$ *tel que* $c_6' \equiv \zeta \bmod 4$.

Démonstration La courbe elliptique E possède un modèle minimal sur K de la forme

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}.$$

Soit ζ un élément de μ_{r-1} tel que $c_6' \equiv \zeta \bmod 2$.

1. Le type de réduction de E est II ou IV. En utilisant la proposition 1 de [3] avec $r = 0$ et $t = \zeta^{r/2}$, on constate que le type de réduction de E est IV si et seulement si $c_6' \equiv \zeta \bmod 4$.

2. Le type de réduction de E est I_0^* ou IV^*. On applique dans ce cas la proposition 3 de *loc. cit.* avec $r = 0$ et $t = 2\zeta^{r/2}$ pour obtenir le résultat.

L'assertion 7(a) résulte du théorème. Prouvons l'assertion 7(b). Supposons que l'on ait $|\Phi| = 3$. Dans ce cas le type de réduction de E est IV ou IV^*. On a alors $v(\Delta) = 4$ ou $v(\Delta) = 8$. D'après l'inégalité $v(j) \geq 12$, le triplet $(v(c_4), v(c_6), v(\Delta))$ vérifient ainsi les hypothèses faites dans le lemme 8. Les conditions (i) et (ii) de l'énoncé sont donc satisfaites. Inversement, si ces conditions sont réalisées, le type de réduction de E est IV ou IV^* (lemme 8) et on a $|\Phi| = 3$. Le théorème entraîne alors le résultat.

Cela termine la démonstration du corollaire.

Références

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

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

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

[4] J.-P. Serre et J. Tate, *Good reduction of abelian varieties*. Ann. of Math. **88**(1968), 492–517.

[5] J. Tate, *Algorithm for determining the type of singular fiber in an elliptic pencil, dans Modular Functions of One Variable IV*. Lect. Notes in Math. **476**, Springer-Verlag 1975.

App. 231
9 rue de Sèvres
92100 Boulogne
France

e-mail : elie.cali@wanadoo.fr

https://doi.org/10.4153/CJM-2004-031-6 Published online by Cambridge University Press