BULL. AUSTRAL. MATH. SOC.
VOL. 60 (1999) [407–428]

11G05

SUR LA p-DIFFÉRENTE DU CORPS DES POINTS DE p-TORSION DES COURBES ELLIPTIQUES

ALAIN KRAUS

Let p be a prime number, K be a finite non-ramified extension of $\mathbb{Q}_p$ and E be an elliptic curve defined over K. Let $K(E_p)$ be the field of the p-division points of E. In this paper we determine the valuation of the different of the extension $K(E_p)/K$.

INTRODUCTION

Soit K une extension finie *non ramifiée* de $\mathbb{Q}_p$ munie de la valuation v qui prolonge celle de $\mathbb{Q}_p$. On suppose que v est normée (c'est-à-dire, on a $v(p) = 1$). Soient $\overline{K}$ une clôture algébrique de K, E une courbe elliptique définie sur K et E_p le sous-groupe des points de p-torsion de $E(\overline{K})$. Soit $K(E_p)$ l'extension de K obtenue en adjoignant à K les coordonnées des points de E_p. On note encore v le prolongement à $\overline{K}$ de la valuation de K. On se propose dans ce travail de déterminer l'entier D, caractérisé par les propriétés équivalentes suivantes:

(a) la différente de l'extension $K(E_p)/K$ est la puissance D-ième de l'idéal de valuation de $K(E_p)$;

(b) l'idéal discriminant de l'extension $K(E_p)/K$ est engendré par $p^{nD/e}$, où n est le degré et e l'indice de ramification de l'extension $K(E_p)/K$.

I. ÉNONCÉ DES RÉSULTATS

Soient K un corps comme ci-dessus, et r le cardinal de son corps résiduel. Soient E une courbe elliptique définie sur K et $j = j(E)$ son invariant modulaire; on note c_4, c_6, Δ les invariants standards associés à un modèle minimal de E sur K [**8**, 1.]. On rappelle que les invariants relatifs à un autre modèle minimal sont c_4u^4, c_6u^6, Δu^{12}, où u est un élément de K de valuation 0; ainsi $v(c_4)$, $v(c_6)$ et $v(\Delta)$ sont indépendants du modèle choisi.

I.1. Lorsque l'invariant modulaire j est de valuation < 0, l'entier D défini au début est donné par l'énoncé suivant:

Received 16th February, 1999
Je remercie J. Oesterlé pour les conversations que nous avons eues au cours de ce travail.

THÉORÈME 1. *Supposons* $v(j) < 0$. *Posons* $j = p^{v(j)}j'$. *On a*

$$D = \begin{cases} 2p^2 - 2p - 1 & \text{si } v(j) \not\equiv 0 \bmod p \\ p - 2 & \text{si } v(j) \equiv 0 \bmod p \text{ et } j'^{r-1} \equiv 1 \bmod p^2 \\ p^2 - 2 & \text{si } v(j) \equiv 0 \bmod p \text{ et } j'^{r-1} \not\equiv 1 \bmod p^2. \end{cases}$$

I.2. Supposons que E ait bonne réduction sur K. Soit h la hauteur de la réduction de E sur K. On a $h = 1$ si E a une réduction ordinaire et $h = 2$ si E a une réduction supersingulière [**4**, 1.11.]. Soient $\widetilde{E}$ la courbe elliptique déduite de E par réduction modulo l'idéal de valuation de K et $j\left(\widetilde{E}\right)$ son invariant modulaire. Si h est égal à 1, on note $j_{can}\left(\widetilde{E}\right)$ l'invariant modulaire du relèvement canonique de E; puisque K est absolument non ramifié, $j_{can}\left(\widetilde{E}\right)$ est un élément de l'anneau de valuation de K qui relève $j\left(\widetilde{E}\right)$ (cf. [**3**, **5**]).

THÉORÈME 2. *Supposons que* E *ait bonne réduction sur* K. *On est dans l'un des cas suivants:*

(i) $j\left(\widetilde{E}\right) = 0$ *(c'est-à-dire,* $v(c_4) \geq 1$*) et* $h = 1$ *(c'est-à-dire,* $p \equiv 1 \bmod 3$*).*

$$D = \begin{cases} p^2 - 2 & \text{si } v(c_4) = 1 \\ p - 2 & \text{si } v(c_4) \neq 1. \end{cases}$$

(ii) $j\left(\widetilde{E}\right) = 1728$ *(c'est-à-dire,* $v(c_6) \geq 1$*) et* $h = 1$ *(c'est-à-dire,* $p \equiv 1 \bmod 4$*).*

$$D = \begin{cases} p^2 - 2 & \text{si } v(c_6) = 1 \\ p - 2 & \text{si } v(c_6) \neq 1. \end{cases}$$

(iii) $j\left(\widetilde{E}\right) \notin \{0, 1728\}$ *et* $h = 1$.

$$D = \begin{cases} p^2 - 2 & \text{si } v\left(j - j_{can}\left(\widetilde{E}\right)\right) = 1 \\ p - 2 & \text{si } v\left(j - j_{can}\left(\widetilde{E}\right)\right) \neq 1. \end{cases}$$

(iv) $h = 2$.

$$D = p^2 - 2.$$

https://doi.org/10.1017/S0004972700036595 Published online by Cambridge University Press

I.3. Supposons que l'invariant modulaire j soit de valuation ≥ 0 et que E ait mauvaise réduction (nécessairement de type additif) sur K.

Supposons $p \geq 5$. Posons $u = p^{v(\Delta)/12}$. Notons L le corps $K(u)$; ce corps est une extension totalement ramifiée de K dont le degré est égal au dénominateur de $v(\Delta)/12$. Soit E_L la courbe elliptique déduite de E par extension des scalaires à L; la courbe E_L a bonne réduction sur L (cf. par exemple [**1**, Proposition 1]). Soient $\widetilde{E_L}$ la courbe déduite de E_L par réduction modulo l'idéal de valuation de L et $j\left(\widetilde{E_L}\right)$ son invariant modulaire. Notons h la hauteur de réduction de E_L sur L. On a $h = 1$ si E_L a une réduction ordinaire et $h = 2$ si E_L a une réduction supersingulière. Lorsque h est égal à 1, on note $j_{can}\left(\widetilde{E_L}\right)$ l'invariant modulaire du relèvement canonique de $\widetilde{E_L}$. Parce que $j\left(\widetilde{E_L}\right)$ est un élément du corps résiduel de K, $j_{can}\left(\widetilde{E_L}\right)$ est un élément de l'anneau de valuation de K qui relève $j\left(\widetilde{E_L}\right)$ (cf. [**3**, **5**]).

THÉORÈME 3. *Supposons que E ait mauvaise réduction de type additif sur K, et que l'on ait $v(j) \geq 0$ et $p \geq 5$.*

On est alors dans l'un des cas suivants:

(i) $v(\Delta) = 2$

$$D = \begin{cases} (5p^2 - 4p - 4)/3 & \text{si } p \equiv 1 \bmod 3,\ v(c_4) = 1 \\ p - 2 & \text{si } p \equiv 1 \bmod 3,\ v(c_4) \neq 1 \\ (5p^2 - 6p - 2)/3 & \text{si } p \equiv 2 \bmod 3,\ v(c_4) = 1 \\ (p^2 - 4)/3 & \text{si } p \equiv 5 \bmod 9,\ v(c_4) \neq 1 \\ p^2 - 2 & \text{si } p \equiv 2 \bmod 3,\ p \not\equiv 5 \bmod 9,\ v(c_4) \neq 1. \end{cases}$$

(ii) $v(\Delta) = 3$

$$D = \begin{cases} (3p^2 - 2p - 3)/2 & \text{si } p \equiv 1 \bmod 4, v(c_6) = 2 \\ p - 2 & \text{si } p \equiv 1 \bmod 4,\ v(c_6) \neq 2 \\ (3p^2 - 4p - 1)/2 & \text{si } p \equiv 3 \bmod 4,\ v(c_6) = 2 \\ p^2 - 2 & \text{si } p \equiv 3 \bmod 4,\ v(c_6) \neq 2. \end{cases}$$

(iii) $v(\Delta) = 4$

$$D = \begin{cases} (4p^2 - 2p - 5)/3 & \text{si } p \equiv 1 \bmod 3,\ v(c_4) = 2 \\ p - 2 & \text{si } p \equiv 1 \bmod 3,\ v(c_4) \neq 2 \\ (4p^2 - 6p - 1)/3 & \text{si } p \equiv 2 \bmod 3,\ v(c_4) = 2 \\ (p^2 - 4)/3 & \text{si } p \equiv 2 \bmod 9,\ v(c_4) \neq 2 \\ p^2 - 2 & \text{si } p \equiv 2 \bmod 3,\ p \not\equiv 2 \bmod 9,\ v(c_4) \neq 2. \end{cases}$$

https://doi.org/10.1017/S0004972700036595 Published online by Cambridge University Press

(iv) $v(\Delta) = 6$

On a $D = p - 2$ *si l'une des conditions suivantes est satisfaite:*

(a) *on a* $p \equiv 1 \bmod. 3$ *et* $v(c_4) \geq 4$;

(b) *on a* $p \equiv 1 \bmod. 4$ *et* $v(c_6) \geq 5$;

(c) *on a* $\big(v(c_4), v(c_6)\big) = (2,3)$, $h = 1$ *et* $v\Big(j - j_{can}\Big(\tilde{E}_L\Big)\Big) \neq 1$.

On a $D = p^2 - 2$ *sinon.*

(v) $v(\Delta) = 8$

$$D = \begin{cases} (5p^2 - 4p - 4)/3 & si\ p \equiv 1 \bmod. 3,\ v(c_4) = 3 \\ p - 2 & si\ p \equiv 1 \bmod. 3,\ v(c_4) \neq 3 \\ (5p^2 - 6p - 2)/3 & si\ p \equiv 2 \bmod. 3,\ v(c_4) = 3 \\ (p^2 - 4)/3 & si\ p \equiv 5 \bmod. 9,\ v(c_4) \neq 3 \\ p^2 - 2 & si\ p \equiv 2 \bmod. 3,\ p \not\equiv 5 \bmod. 9, v(c_4) \neq 3. \end{cases}$$

(vi) $v(\Delta) = 9$

$$D = \begin{cases} (3p^2 - 2p - 3)/2 & si\ p \equiv 1 \bmod. 4,\ v(c_6) = 5 \\ p - 2 & si\ p \equiv 1 \bmod. 4,\ v(c_6) \neq 5 \\ (3p^2 - 4p - 1)/2 & si\ p \equiv 3 \bmod. 4,\ v(c_6) = 5 \\ p^2 - 2 & si\ p \equiv 3 \bmod. 4,\ v(c_6) \neq 5. \end{cases}$$

(vii) $v(\Delta) = 10$

$$D = \begin{cases} (4p^2 - 2p - 5)/3 & si\ p \equiv 1 \bmod. 3,\ v(c_4) = 4 \\ p - 2 & si\ p \equiv 1 \bmod. 3,\ v(c_4) \neq 4 \\ (4p^2 - 6p - 1)/3 & si\ p \equiv 2 \bmod. 3,\ v(c_4) = 4 \\ (p^2 - 4)/3 & si\ p \equiv 2 \bmod. 9,\ v(c_4) \neq 4 \\ p^2 - 2 & si\ p \equiv 2 \bmod. 3,\ p \not\equiv 2 \bmod. 9,\ v(c_4) \neq 4. \end{cases}$$

Lorsque l'on a $p = 2$ ou $p = 3$, l'entier D est donné par les deux énoncés suivants:

THÉORÈME 4. *Supposons que* E *ait mauvaise réduction de type additif sur* K, *et que l'on ait* $v(j) \geq 0$ *et* $p = 3$. *Posons* $\Delta = 3^{v(\Delta)}\Delta'$.

(a) *Supposons* $v(\Delta) \equiv 0 \bmod. 3$. *On a* $D = 1$ *si l'on a* $2v(c_6) \leq 4 + v(\Delta)$ *et* $\Delta'^{r-1} \equiv 1 \bmod. 9$. *On a* $D = 7$ *dans le cas contraire.*

(b) *Si* $v(\Delta)$ *n'est pas divisible par* 3, *on a* $D = 11$.

THÉORÈME 5. *Supposons que* E *ait mauvaise réduction de type additif sur* K, *et que l'on ait* $v(j) \geq 0$ *et* $p = 2$. *Posons* $\Delta = 2^{v(\Delta)}\Delta'$.

(a) *Si* $v(\Delta)$ *est impair, on a* $D = 3$.

https://doi.org/10.1017/S0004972700036595 Published online by Cambridge University Press

(b) *Supposons que* $v(\Delta)$ *soit pair. On a* $D = 2$ *si l'une des deux conditions suivantes est satisfaite:*

(i) *on a* $\Delta'^{r-1} \equiv -1 \bmod. 4$;

(ii) *on a* $v(\Delta) \in \{6, 8, 12, 14\}$ *et* $3v(c_4) \geq 8 + v(\Delta)$.

On a $D = 0$ *dans le cas contraire.*

II. Démonstrations

On désigne par K_{nr} la clôture non ramifiée de K dans $\overline{K}$.

Remarque 1. Soient N une extension finie de K_{nr}, M une extension galoisienne finie de N, et $\widehat{M}$, $\widehat{N}$ les complétés de M et N. Si π est une uniformisante de M, notons G_i, pour $i \geq 0$, le sous-groupe du groupe de Galois $\mathrm{Gal}(M/N)$ formé des éléments s satisfaisant à l'inégalité

$$v(s\pi - \pi) \geq \frac{i+1}{[M : K_{nr}]}.$$

Le groupe G_i est isomorphe au i-ème sous-groupe de ramification de l'extension $\widehat{M}/\widehat{N}$, au sens de [**5**, Chapitre IV]. Par suite, G_1 est le p-sous-groupe de Sylow de $\mathrm{Gal}(M/N)$ et la différente de l'extension M/N est la puissance δ-ième de l'idéal de valuation de M, où

$$\delta = \sum_{i \geq 0} (|G_i| - 1),$$

(cf. [**5**, p.61, Proposition 10 et p.72, Proposition 4]). Par définition, on dira que G_i est le i-ème sous-groupe de ramification de l'extension M/N.

Soit μ_n le groupe des racines n-ièmes de l'unité de $\overline{K}$. Le corps $K_{nr}(E_p)$ contient $K_{nr}(\mu_p)$. On notera dans toute la suite

- D' l'entier tel que la différente de l'extension $K_{nr}(E_p)/K_{nr}(\mu_p)$ soit la puissance D'-ième de l'idéal de valuation de $K_{nr}(E_p)$;
- $(H_i)_{i \geq 0}$ la suite des sous-groupes de ramification de l'extension $K_{nr}(E_p)/K_{nr}(\mu_p)$. Le groupe H_i est donc le sous-groupe des éléments s de $\mathrm{Gal}\big(K_{nr}(E_p)/K_{nr}(\mu_p)\big)$ pour lesquels on a

$$v(s\pi - \pi) \geq \frac{i+1}{[K_{nr}(E_p) : K_{nr}]},$$

(où π est une uniformisante de $K_{nr}(E_p)$). D'après la remarque 1, on a

$$D' = \sum_{i \geq 0} (|H_i| - 1). \tag{1}$$

https://doi.org/10.1017/S0004972700036595 Published online by Cambridge University Press

Le groupe $\mathrm{Gal}\big(K_{nr}(\mu_p)/K_{nr}\big)$ est cyclique d'ordre $p-1$. L'extension $K_{nr}(\mu_p)/K_{nr}$ est modérément ramifiée, sa différente est la puissance $(p-2)$-ième de l'idéal de valuation de $K_{nr}(\mu_p)$. On a ainsi, par transitivité des différentes [**5**, p.60, Proposition 8]

$$D = D' + (p-2)[K_{nr}(E_p) : K_{nr}(\mu_p)]. \tag{2}$$

II. 1. PRÉLIMINAIRES.

LEMME 1. *Soit u un élément de K de valuation 0. Pour que u soit une puissance p-ième dans K_{nr}, il faut et il suffit que l'on ait $u^{r-1} \equiv 1 \bmod. p^2$.*

DÉMONSTRATION: On peut écrire $u = z'u'$ où z' appartient à μ_{r-1}, et où u' est un élément de K congru à 1 modulo p. Rappelons d'abord l'équivalence des deux assertions suivantes:

(i) u' est une puissance p-ième dans K_{nr};
(ii) on a $u' \equiv 1 \bmod. p^2$.

Lorsque $p \geq 3$, cela résulte de [**5**, p.219, Proposition 9]. Si $p = 2$, l'implication (i) $\Longrightarrow$ (ii) est immédiate et la réciproque résulte de [**1**, Lemme 7].

Supposons que u soit une puissance p-ième dans K_{nr}. L'égalité $z'^r = z'$ montre que z' est une puissance p-ième, donc que u' est une puissance p-ième dans K_{nr} ; on a ainsi $u' \equiv 1 \bmod. p^2$, et cela entraîne $u^{r-1} \equiv 1 \bmod. p^2$.

Inversement, supposons $u^{r-1} \equiv 1 \bmod. p^2$. On a l'égalité

$$u^{r-1} - 1 = u'^{r-1} - 1 = (u'-1)\big(u'^{r-2} + \ldots + 1\big).$$

Comme on a $u' \equiv 1 \bmod. p$, l'élément $1 + \ldots + u'^{r-2}$ est congru à $r-1$ modulo p, et sa valuation est égale à 0. On a donc $u' \equiv 1 \bmod. p^2$ et u' est une puissance p-ième dans K_{nr}. Il en est alors de même de u, d'où le lemme. □

LEMME 2. *Soit u un élément de $\overline{K}$ de valuation 0 satisfaisant à l'inégalité $v(u-1) \leq 1$. On a $pv\big(u^{1/p} - 1\big) = v(u-1)$.*

DÉMONSTRATION: Posons $a = u^{1/p} - 1$. On a

$$u - 1 = (1+a)^p - 1 = a^p + \sum_{1 \leq k \leq p-1} C_p^k a^k.$$

Si on a $v(a) = 0$, on a $v(u-1) = 0$; si on a $v(a) > 0$, chacun des termes $C_p^k a^k$, pour $1 \leq k \leq p-1$, est de valuation > 1, donc on a $v(u-1) = v(a^p) = pv(a)$. Cela prouve le lemme. □

II.2. Le Théorème 1.

Par hypothèse on a $v(j) < 0$. Il existe une unique extension T de degré ≤ 2 de K sur laquelle E est isomorphe à la courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$, où q est l'élément de K^* défini par l'identité [**6**, Theorem 14.1] :

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

Proposition 1. *On a* $K_{nr}(E_p) = K_{nr}\left(\mu_p, q^{1/p}\right)$.

Démonstration: Démontrons d'abord que l'on a

$$T(E_p) = T\left(\mu_p, q^{1/p}\right). \tag{4}$$

Le groupe E_p s'identifie à $\left(\mu_p q^{\mathbb{Z}/p}\right)/q^{\mathbb{Z}}$ en tant que $\mathrm{Gal}\left(\overline{K}/T\right)$-module (cf. *loc. cit.*). On en déduit que $T(E_p)$ est contenu dans $T\left(\mu_p, q^{1/p}\right)$. Par ailleurs, si $s \in \mathrm{Gal}\left(\overline{K}/T(E_p)\right)$, on a $s\left(q^{1/p}\right) \equiv q^{1/p} \bmod. q^{\mathbb{Z}}$, d'où $s\left(q^{1/p}\right) = q^{(1/p)+n}$ avec $n \in \mathbb{Z}$, et en prenant la valuation des deux membres, on voit que $n = 0$, donc que s fixe $q^{1/p}$. Cela prouve que $q^{1/p}$ appartient à $T(E_p)$. Par ailleurs, μ_p est contenu dans $T(E_p)$. Nous avons ainsi démontré l'égalité (4).

Supposons que E soit à réduction multiplicative sur K. L'extension T/K est alors non ramifiée (*loc. cit.*) et la Proposition 1 résulte de l'égalité (4).

Supposons que E soit à réduction additive sur K et que l'on ait $p \neq 2$. L'extension T/K est ramifiée (*loc. cit.*). Comme $p \neq 2$, TK_{nr} est l'unique extension quadratique de K_{nr}, c'est-à-dire est le sous-corps de $K_{nr}(\mu_p)$ fixé par le sous-groupe d'indice 2 de $\mathrm{Gal}\left(K_{nr}(\mu_p)/K_{nr}\right)$, qui est un groupe cyclique d'ordre $p-1$. On déduit de là que l'on a $T.K_{nr}(\mu_p) = K_{nr}(\mu_p)$; comme μ_p est contenu dans $K_{nr}(E_p)$, la Proposition 1 résulte de la formule (4).

Supposons maintenant $p = 2$. Démontrons que c_4 est un carré dans K_{nr}. Pour cela, posons $c_4 = 2^{v(c_4)}c_4'$, $c_6 = 2^{v(c_6)}c_6'$. On a $j\Delta = c_4^3$ et $v(j) < 0$, d'où $3v(c_4) < v(\Delta)$. De l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on déduit alors $3v(c_4) = 2v(c_6)$; $v(c_4)$ est donc pair et l'égalité $c_4^3 - c_6^2 = 1728\Delta$ s'écrit aussi ${c_4'}^3 - {c_6'}^2 = 1728\Delta\, 2^{-3v(c_4)}$. Comme on a $3v(c_4) < v(\Delta)$, on a en particulier ${c_4'}^3 \equiv {c_6'}^2 \equiv 1 \bmod. 4$. Or, un élément de K de valuation 0 qui est congru à 1 modulo 4 est un carré dans K_{nr} (Lemme 1); c_4' est donc un carré dans K_{nr} et cela démontre notre assertion.

Puisque c_4 est un carré dans K_{nr} et que $j\Delta = c_4^3$, on a l'égalité $K_{nr}\left(\sqrt{\Delta}\right) = K_{nr}\left(\sqrt{j}\right)$. L'élément jq est aussi un carré dans K_{nr} car il est congru à 1 modulo 4 (formule (3)), d'où $K_{nr}\left(\sqrt{j}\right) = K_{nr}\left(\sqrt{q}\right)$ et on obtient finalement l'égalité $K_{nr}\left(\sqrt{\Delta}\right) = K_{nr}\left(\sqrt{q}\right)$. Le groupe $\mathrm{Gal}\left(K_{nr}(E_2)/K_{nr}\right)$ est un sous-groupe de $\mathbf{GL}_2(\mathbb{F}_2)$ et $\mathbf{GL}_2(\mathbb{F}_2)$

est d'ordrer 6. Par ailleurs, $K_{nr}(E_2)/K_{nr}$ est une extension de degré divisant 4 d'après (4); on a donc $\left[K_{nr}(E_2) : K_{nr}\right] \leq 2$. Il résulte de [**4**, 5.3. (a)] que $K_{nr}\left(\sqrt{\Delta}\right)$ est contenu dans $K_{nr}(E_2)$ et que $\left[K_{nr}(E_2) : K_{nr}\right]$ est impair ou pair suivant que Δ est ou non un carré dans K_{nr}; on en déduit l'égalité $K_{nr}(E_2) = K_{nr}\left(\sqrt{\Delta}\right)$. On a ainsi $K_{nr}(E_2) = K_{nr}\left(\sqrt{q}\right)$, d'où la proposition. □

DÉMONSTRATION DU THÉORÈME 1. (1) Supposons $v(j) \not\equiv 0 \bmod. p$. On a $v(j) = -v(q)$ (formule (3)). Le corps $K_{nr}(E_p)$ est donc de la forme $K_{nr}\left(\mu_p, (p^n q')^{1/p}\right)$, où $1 \leq n \leq p-1$ et où q' est une unité de K. Comme p ne divise pas n, q' est la puissance n-ième d'une unité u de K_{nr}, et l'on a l'égalité

$$K_{nr}(E_p) = K_{nr}\left(\mu_p, (pu)^{1/p}\right).$$

En particulier, l'extension $K_{nr}(E_p)/K_{nr}$ est de degré $p(p-1)$. Soit z un générateur de μ_p. L'élément $\pi = (z-1)/(pu)^{1/p}$ est de valuation $1/(p-1) - (1/p) = 1/p(p-1)$; c'est donc une uniformisante de $K_{nr}(E_p)$. Soit σ un générateur du groupe de Galois $\mathrm{Gal}\left(K_{nr}(E_p)/K_{nr}(\mu_p)\right)$ (qui est cyclique d'ordre p). Posons $t = \sigma\left((pu)^{1/p}\right)/(pu)^{1/p}$; c'est une racine primitive p-ième de l'unité. On a $\sigma(\pi) - \pi = (z-1)(1-t)/\sigma\left((pu)^{1/p}\right)$; d'où $v\left(\sigma(\pi) - \pi\right) = 2/(p-1) - 1/p = (p+1)/p(p-1)$. On en déduit, avec les notations introduites au début du paragraphe II, que l'on a

$$|H_i| = \begin{cases} p & \text{si } 0 \leq i \leq p \\ 1 & \text{si } i > p+1. \end{cases}$$

Il en résulte les égalités $D' = (p+1)(p-1)$ (formule (1)) et $D = 2p^2 - 2p - 1$ d'après la formule (2).

(2) Supposons $v(j) \equiv 0 \bmod. p$. D'après le Lemme 1 et la formule (3), jq est une puissance p-ième dans K_{nr}. D'après la Proposition 1, on a donc $K_{nr}(E_p) = K_{nr}\left(\mu_p, j^{1/p}\right)$. Posons $j = p^{v(j)} j'$.

Si on a $j'^{r-1} \equiv 1 \bmod. p^2$, j est une puissance p-ième dans K_{nr} (Lemme 1). D'où $K_{nr}(E_p) = K_{nr}(\mu_p)$ et $D = p-2$ (formule (2)).

Supposons $j'^{r-1} \not\equiv 1 \bmod. p^2$; posons $j' = z't$, où $z' \in \mu_{r-1}$ et où t est un élément de K de valuation 0 congru à 1 modulo p. On a $z' \in K_{nr}^p$, car $z'^r = z'$, ce qui entraîne l'égalité $K_{nr}(E_p) = K_{nr}\left(\mu_p, t^{1/p}\right)$. Par ailleurs, on a $j'^{r-1} = t^{r-1}$; t n'est donc pas une puissance p-ième dans K_{nr} (Lemme 1) et $v(t-1)$ est égal à 1. En particulier, le degré $\left[K_{nr}(E_p) : K_{nr}\right]$ est égal à $p(p-1)$. D'après le Lemme 2 on a $pv\left(t^{1/p} - 1\right) = 1$. Notons z une racine primitive p-ième de l'unité et posons $\pi = (z-1)/\left(t^{1/p} - 1\right)$; on a $v(\pi) = 1/(p-1) - 1/p = 1/p(p-1)$, de sorte que π est une uniformisante de $K_{nr}(E_p)$.

Notons σ un générateur de $\mathrm{Gal}\big(K_{nr}(E_p)/K_{nr}(\mu_p)\big)$ et posons $t' = \sigma\big(t^{1/p}\big)/t^{1/p}$; t' est une racine primitive p-ième de l'unité. On a

$$\sigma(\pi) - \pi = (z-1)\frac{t^{1/p} - \sigma\big(t^{1/p}\big)}{\big(t^{1/p}-1\big)\sigma\big(t^{1/p}-1\big)} = (z-1)t^{1/p}\frac{1-t'}{\big(t^{1/p}-1\big)\sigma\big(t^{1/p}-1\big)}.$$

On a ainsi $v\big(\sigma(\pi)-\pi\big) = 2/(p-1) - 2/p = 2/p(p-1)$. On déduit de là les égalités $|H_0| = |H_1| = p$ et $|H_i| = 1$ si $i \geq p-2$, d'où $D' = 2(p-1)$ (formule (1)) et $D = p^2-2$ (formule (2)). Cela termine la démonstration du Théorème 1.

II.3. Le Théorème 2.

Proposition 2. *Supposons que E ait bonne réduction ordinaire sur K. Il existe $\lambda \in K_{nr}$ satisfaisant à l'égalité $K_{nr}(E_p) = K_{nr}\big(\mu_p, \lambda^{1/p}\big)$ tel que la valuation de $\lambda - 1$ soit donnée par*

$$v(\lambda-1) = \begin{cases} v(c_4) & \text{si } j\Big(\widetilde{E}\Big) = 0 \\ v(c_6) & \text{si } j\Big(\widetilde{E}\Big) = 1728 \\ v\Big(j(E) - j_{can}\Big(\widetilde{E}\Big)\Big) & \text{si } j\Big(\widetilde{E}\Big) \neq 0, 1728. \end{cases}$$

Démonstration: Soit $\widehat{K}_{nr}$ le complété du corps K_{nr}; notons encore v la valuation de $\widehat{K}_{nr}$ prolongeant celle de K_{nr} par continuité. Il résulte de l'Appendice de [2], sur les courbes elliptiques à réduction ordinaire, l'existence d'un élément λ dans $\widehat{K}_{nr}$ tel que $\widehat{K}_{nr}(E_p) = \widehat{K}_{nr}\big(\mu_p, \lambda^{1/p}\big)$ et que $v(\lambda-1)$ satisfasse les conditions énoncées à la fin de la Proposition 2. Quitte à remplacer λ par un élément de K_{nr} suffisamment voisin, on se ramène au cas où λ appartient à K_{nr}. Mais alors l'égalité $\widehat{K}_{nr}(E_p) = \widehat{K}_{nr}\big(\mu_p, \lambda^{1/p}\big)$ entraîne l'égalité $K_{nr}(E_p) = K_{nr}\big(\mu_p, \lambda^{1/p}\big)$: cela résulte de l'égalité $[M : K_{nr}] = [\widehat{M} : \widehat{K}_{nr}]$ appliquée en prenant pour M les extensions $K_{nr}\big(\lambda^{1/p}\big)$ et $K_{nr}(\mu_p)$ de K_{nr} ainsi que le composé de ces extensions. □

Démonstration du Théorème 2. Supposons $h = 1$ et $j\Big(\widetilde{E}\Big) = 0$. D'après la Proposition 2, il existe $\lambda \in K_{nr}$ tel que l'on ait $K_{nr}(E_p) = K_{nr}\big(\mu_p, \lambda^{1/p}\big)$ avec $v(\lambda-1) = v(c_4)$. Supposons $v(c_4) = 1$. Une démonstration analogue à celle du dernier alinéa du paragraphe II.2 montre que l'on a alors $D = p^2-2$. Supposons $v(c_4) \geq 2$; λ est alors une puissance p-ième dans K_{nr} (Proposition 2) et on a $K_{nr}(E_p) = K_{nr}(\mu_p)$, d'où $D = p-2$. Cela démontre l'assertion (i) du théorème.
La démonstration des assertions (ii) et (iii) est analogue.

Supposons $h = 2$. L'extension $K_{nr}(E_p)/K_{nr}$ est modérément ramifiée de degré p^2-1 [**4**, Proposition 12]; on en déduit $D = p^2-2$ (formule (1)), d'où le Théorème 2. □

II.4. Le Théorème 3.

On suppose que E a une réduction de type additif sur K, et que l'on a $v(j) \geq 0$ et $p \geq 5$.

On reprend les notations du paragraphe I.3. Notons L_{nr} la clôture non ramifiée de L dans $\overline{K}$. On a $L_{nr} = K_{nr}(u)$, où $u = p^{v(\Delta)/12}$.

Remarque 2. Par hypothèse, K est un corps absolument non ramifié, c'est-à-dire, p est une uniformisante de K. La description de l'action de $\mathrm{Gal}\left(\overline{K}/K_{nr}\right)$ sur E_p, qui est faite dans [2], dans le cas où $K = \mathbb{Q}_p$, ne dépend en fait que de l'indice de ramification absolu de K. Les résultats obtenus à propos de cette description ne changent donc pas si l'on remplace $\mathbb{Q}_p$ par K ; à ceci près que dans la situation où E_L a bonne réduction ordinaire sur L, l'invariant modulaire $j_{can}\left(\widetilde{E}_L\right)$ du relèvement canonique de $\widetilde{E}_L$ est un élément de l'anneau de valuation de K. Nous utiliserons donc les résultats de [2] en les appliquant au couple (E, K) sans les redémontrer. Cette remarque est aussi valable pour $p = 2$ ou $p = 3$.

Le triplet $\left(v(\Delta), v(c_4), v(c_6)\right)$ est l'un de ceux intervenant dans le tableau ci-dessous:

$v(\Delta)$	2	3	4	6		8	9	10
$v(c_4)$	≥ 1	1	≥ 2	2	≥ 3	≥ 3	3	≥ 4
$v(c_6)$	1	≥ 2	2	≥ 3	3	4	≥ 5	5

L'équation

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

est une équation minimale de E sur K (cf. [8, 1]).

En effectuant le changement de variables

$$\begin{cases} x = u^2 X \\ y = u^3 Y, \end{cases}$$

on obtient une équation sur L de la courbe elliptique E_L déduite de E par extension des scalaires

$$(W_L) \qquad Y^2 = X^3 - \left(\frac{c_4}{48u^4}\right)X - \left(\frac{c_6}{864u^6}\right) \quad .$$

Cette équation est à coefficients entiers et son discriminant est de valuation 0; on retrouve le fait que E_L a bonne réduction sur L.

REMARQUE 3. Supposons toujours $p \geq 5$ et de plus $v(\Delta) \geq 8$. Il existe alors une courbe elliptique E' dont un modèle minimal a pour invariants associés $c_4(E') = c_4/p^2$, $c_6(E') = c_6/p^3$ et $\Delta(E') = \Delta/p^6$. Les courbes E et E' se déduisent l'une de l'autre par torsion quadratique par $\sqrt{p}$. L'extension $K_{nr}(\mu_p)/K_{nr}$ est une extension cyclique de degré $p-1$, donc $K_{nr}(\sqrt{p})$, qui est l'unique extension quadratique de K_{nr}, est contenue dans $K_{nr}(\mu_p)$. Le corps $K_{nr}(E_p)$ contient $K_{nr}(\mu_p)$, et il en est de même de $K_{nr}(E'_p)$, où E'_p est le sous-groupe des points de p-torsion de $E'(\overline{K})$. On en déduit l'égalité $K_{nr}(E_p) = K_{nr}(E'_p)$. Il suffit donc de vérifier le Théorème 3 sous l'hypothèse $v(\Delta) < 8$. Le même argument montre que le Théorème 3, lorsque $v(\Delta) = 6$, est conséquence du Théorème 2. Dans la suite, nous supposerons donc que $v(\Delta)$ est égal à 2, 3 ou 4.

II.4.1. CAS OÙ E_L A BONNE RÉDUCTION ORDINAIRE SUR L, C'EST-À-DIRE, CAS OÙ $h = 1$.

LEMME 3. *Supposons $h = 1$. Le corps $K_{nr}(\mu_p)$ contient L_{nr}.*

DÉMONSTRATION: Comme h est égal à 1, le dénominateur d de $v(\Delta)/12$ divise $p-1$ (cf. [**2**, Lemme 1]). Par ailleurs, l'extension $K_{nr}(\mu_p)/K_{nr}$ est cyclique de degré $p-1$ et le corps L_{nr} est l'unique extension de degré d de K_{nr}. Il est donc contenu dans $K_{nr}(\mu_p)$, d'où le lemme. □

PROPOSITION 3. *Supposons $h = 1$. Il existe alors λ dans $K_{nr}(\mu_p)$ satisfaisant à l'égalité $K_{nr}(E_p) = K_{nr}(\mu_p, \lambda^{1/p})$ tel que la valuation de $\lambda - 1$ soit donnée par*

$$v(\lambda-1) = \begin{cases} v(c_4) - v(\Delta)/3 & \text{si } j(\widetilde{E}_L) = 0 \\ v(c_6) - v(\Delta)/2 & \text{si } j(\widetilde{E}_L) = 1728 \\ v\left(j(E) - j_{can}(\widetilde{E}_L)\right) & \text{si } j(\widetilde{E}_L) \neq 0, 1728. \end{cases}$$

DÉMONSTRATION: D'après le Lemme 3, la courbe déduite de E par extension des scalaires à $K_{nr}(\mu_p)$ a bonne réduction ordinaire et (W_L) en est une équation minimale, avec pour invariants standards associés $c_4(W_L) = c_4/u^4$ et $c_6(W_L) = c_6/u^6$. Par ailleurs, $K_{nr}(\mu_p)$ est contenu dans $K_{nr}(E_p)$. Il suffit alors de récrire la démonstration de la Proposition 2 en remplacant K_{nr} par $K_{nr}(\mu_p)$, pour obtenir la Proposition 3. □

DÉMONSTRATION DU THÉORÈME 3 LORSQUE h EST ÉGAL À 1. Nous supposons $h = 1$; la lettre λ désignera un élément de $K_{nr}(\mu_p)$ satisfaisant à l'énoncé de la Proposition 3. Posons $a = \lambda^{1/p}$.

(1) Cas où $v(\Delta) = 2$

L'hypothèse $h = 1$ implique dans ce cas que l'on a $p \equiv 1 \bmod 3$ [**2**, Lemme 1]).

https://doi.org/10.1017/S0004972700036595 Published online by Cambridge University Press

Supposons $v(c_4) = 1$. On a $j\left(\widetilde{E}_L\right) = 0$, d'où $v(\lambda - 1) = 1/3$ (Proposition 3). Il résulte de [**2**, Proposition 4] que l'on a $\left[K_{nr}(E_p) : K_{nr}\right] = p(p-1)$. Soit z une racine primitive p-ième de l'unité. Posons $\pi = (z-1)/(a-1)^3$. On a $v(a-1) = 1/3p$ (Lemme 2) et $v(\pi)$ est égal à $1/(p-1) - 3/3p = 1/p(p-1)$; π est donc une uniformisante de $K_{nr}(E_p)$. Soit σ un générateur de $\mathrm{Gal}\big(K_{nr}(E_p)/K_{nr}(\mu_p)\big)$. On a $\sigma(a) = ta$, avec t une racine primitive p-ième de l'unité. Calculons la valuation de $\sigma(\pi) - \pi$. On a

$$\sigma(\pi) - \pi = (z-1)\frac{S_a}{(a-1)^3\sigma(a-1)^3},$$

où $S_a = (a-1)^3 - \sigma(a-1)^3 = a(1-t)\big(a^2(1+t+t^2) - 3a(t+1) + 3\big)$. Comme on a $v(t-1) = 1/(p-1)$, on peut écrire $t = 1 + \pi^p t_0$, où t_0 est un élément de $K_{nr}(E_p)$ de valuation 0. On a alors

$$S_a = -a\pi^p t_0\big(a^2\pi^{2p}t_0^2 + 3a\pi^p t_0(a-1) + 3(a-1)^2\big).$$

Or on a $v(a-1) = 1/3p$, d'où $v(S_a) = 1/(p-1) + 2/3p = (5p-2)/3p(p-1)$ et on a donc $v(\sigma(\pi) - \pi) = 1/(p-1) + (5p-2)/3p(p-1) - 6/3p = (2p+4)/3p(p-1)$. On en déduit les égalités

$$|H_i| = \begin{cases} p & \text{si } 0 \le i \le (2p+1)/3 \\ 1 & \text{si } i \ge (2p+4)/3, \end{cases}$$

d'où $D' = (p-1)(2p+4)/3$ (formule (1)) et $D = \big(5p^2 - 4p - 4\big)/3$ (formule (2)).

Si $v(c_4) \neq 1$, λ est une puissance p-ième dans $K_{nr}(\mu_p)$ (cf. [**2**, Proposition 4]) et l'on a $K_{nr}(E_p) = K_{nr}(\mu_p)$, d'où $D = p - 2$.

(2) Cas où $v(\Delta) = 3$

L'hypothèse $h = 1$ implique dans ce cas que l'on a $p \equiv 1 \bmod. 4$ [**2**, Lemme 1]).

Supposons $v(c_6) = 2$. On a $j\left(\widetilde{E}_L\right) = 1728$, d'où $v(\lambda - 1) = 1/2$ (Proposition 3). On a $\left[K_{nr}(E_p) : K_{nr}\right] = p(p-1)$ (cf. [**2**, Proposition 4]). D'après le Lemme 2, $v(a-1)$ est égal à $1/2p$, et l'élément $\pi = (z-1)/(a-1)^2$, où z est une racine primitive p-ième de l'unité, est une uniformisante de $K_{nr}(E_p)$. Soit σ un générateur de $\mathrm{Gal}\big(K_{nr}(E_p)/K_{nr}(\mu_p)\big)$. On a $\sigma(a) = ta$, avec t une racine primitive p-ième de l'unité. On a

$$\sigma(\pi) - \pi = (z-1)\frac{S_a}{(a-1)^2\sigma(a-1)^2},$$

où $S_a = (a-1)^2 - \sigma(a-1)^2 = a(1-t)\big(a(1+t) - 2\big)$. Comme on a $v(t-1) = 1/(p-1)$, on peut écrire $t = 1 + \pi^p t_0$, où t_0 est un élément de $K_{nr}(E_p)$ de valuation 0. On a alors

$$S_a = -a\pi^p t_0\big(2(a-1) + a\pi^p t_0\big),$$

d'où $v(S_a) = 1/(p-1) + 1/2p = (3p-1)/2p(p-1)$ et on déduit de là que l'on a les égalités $v\big(\sigma(\pi) - \pi\big) = 1/(p-1) + (3p-1)/2p(p-1) - 4/2p = (p+3)/2p(p-1)$. On a donc

$$|H_i| = \begin{cases} p & \text{si } 0 \le i \le (p+1)/2 \\ 1 & \text{si } i \ge (p+3)/2, \end{cases}$$

d'où $D' = (p-1)(p+3)/2$ (formule (1)) et $D = \big(3p^2 - 2p - 3\big)/2$ (formule (2)).

Si $v(c_6) \neq 2$, λ est une puissance p-ième dans $K_{nr}(\mu_p)$ (cf. [**2**, Proposition 4]) et l'on a $K_{nr}(E_p) = K_{nr}(\mu_p)$, d'où $D = p-2$.

(3) Cas où $v(\Delta) = 4$

L'hypothèse $h = 1$ implique dans ce cas que l'on a $p \equiv 1 \bmod. 3$ [**2**, Lemme 1].

Supposons $v(c_4) = 2$. On a $j\Big(\widetilde{E}_L\Big) = 0$, d'où $v(\lambda - 1) = 2/3$ (Proposition 3). Le degré $\big[K_{nr}(E_p) : K_{nr}\big]$ est $p(p-1)$ et $v(a-1) = 2/3p$ (Lemme 2). Soit z une racine primitive p-ième de l'unité. L'élément $\pi' = (z-1)^2/(a-1)^3$ est de valuation $2/(p-1) - 2/p = 2/p(p-1)$. Cette valuation normalisée sur $K_{nr}(E_p)$ est donc pair égale à 2; comme on a $p \neq 2$, π' est le carré d'une uniformisante π de $K_{nr}(E_p)$. On a

$$\sigma(\pi') - \pi' = (z-1)^2 \frac{S_a}{(a-1)^3 \sigma(a-1)^3},$$

où $S_a = (a-1)^3 - \sigma(a-1)^3$. Soit σ un générateur de $\mathrm{Gal}\big(K_{nr}(E_p)/K_{nr}(\mu_p)\big)$. Par une démonstration analogue à celle du cas **(1)**, on prouve que l'on a $v(S_a) = (7p-4)/3p(p-1)$ et $v\big(\sigma(\pi') - \pi'\big) = 2/(p-1) + (7p-4)/3p(p-1) - 4/p = (p+8)/3p(p-1)$. Comme σ appartient au groupe d'inertie sauvage, on a $\sigma(\pi)/\pi \equiv 1 \bmod. \pi$, d'où $\sigma(\pi) + \pi \equiv 2\pi \bmod. \pi^2$ et $v\big(\sigma(\pi) + \pi\big) = 1/p(p-1)$. De l'égalité $\sigma(\pi') - \pi' = \sigma(\pi)^2 - \pi^2 = \big(\sigma(\pi) - \pi\big)\big(\sigma(\pi) + \pi\big)$ on déduit alors $v\big(\sigma(\pi) - \pi\big) = (p+5)/3p(p-1)$. On a par conséquent

$$|H_i| = \begin{cases} p & \text{si } 0 \le i \le (p+2)/3 \\ 1 & \text{si } i \ge (p+5)/3, \end{cases}$$

d'où $D' = (p-1)(p+5)/3$ (formule (1)) et $D = \big(4p^2 - 2p - 5\big)/3$ (formule (2)).

Si $v(c_4) \neq 2$, λ est une puissance p-ième dans $K_{nr}(\mu_p)$ (cf. [**2**, Proposition 4]) et l'on a $K_{nr}(E_p) = K_{nr}(\mu_p)$, d'où $D = p-2$. □

II.4.2. Cas où E_L a une réduction supersingulière sur L, c'est-à-dire, cas où $h = 2$.

Notons $\mathbb{F}_p$ le corps à p éléments, $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$ et $\mathbb{F}_{p^2}$ l'unique extension quadratique de $\mathbb{F}_p$ contenue dans $\overline{\mathbb{F}_p}$. Rappelons que la représentation donnant l'action de $\mathrm{Gal}\big(\overline{K}/K_{nr}\big)$ sur E_p satisfait l'une des conditions suivantes [**2**, Proposition 1 et 2]):

(a) son image est contenue dans un sous-groupe de Borel de $\mathbf{GL}_2(\mathbb{F}_p)$;

(b) après extension des scalaires à $\overline{\mathbb{F}_p}$, elle est diagonalisable et représentable matriciellement sous la forme

$$\begin{pmatrix} \varphi & 0 \\ 0 & \varphi^p \end{pmatrix},$$

où φ est un caractère à valeurs dans $\mathbb{F}_{p^2}$, dont l'image n'est pas contenue dans $\mathbb{F}_p$ [**2**, Proposition 2].

LEMME 4. *Supposons que la condition (b) soit satisfaite. L'ordre du caractère φ est égal à $D+1$.*

DÉMONSTRATION: Sur $\overline{\mathbb{F}_p}$, la représentation s'écrit matriciellement $\begin{pmatrix} \varphi & 0 \\ 0 & \varphi^p \end{pmatrix}$; l'ordre de φ est donc égal au degré de l'extension $K_{nr}(E_p)/K_{nr}$ qui n'est pas divisible par p (*loc. cit.* et [**4**, Proposition 4]). L'extension $K_{nr}(E_p)/K_{nr}$ étant modérément ramifiée, on a donc $D = \big[K_{nr}(E_p) : K_{nr}\big] - 1$, (Remarque 1), d'où le lemme. □

Soient X, Y les fonctions coordonnées de Weierstrass de E_L dans le modèle (W_L). Posons $T = -X/Y$; c'est une uniformisante locale de E_L au voisinage de l'origine 0.

LEMME 5. *Supposons que l'on ait $h = 2$ et que $\big(v(\Delta), v(c_4), v(c_6)\big)$ soit l'un des triplets $(2,1,1)$, $(3,1,2)$, $(4,2,2)$. Soient α_1 et α_2 les nombres définis dans le tableau ci-dessous:*

$v(\Delta)$	2	3	4
$v(c_4)$	1	1	2
$v(c_6)$	1	2	2
α_1	$2/\big(3(p-1)\big)$	$1/\big(2(p-1)\big)$	$1/\big(3(p-1)\big)$
α_2	$1/\big(3p(p-1)\big)$	$1/\big(2p(p-1)\big)$	$1/\big(3p(p-1)\big)$

Il existe une base (P_1, P_2) de E_p sur $\mathbb{F}_p$ telle que l'on ait $v\big(T(P_1)\big) = \alpha_1$ et $v\big(T(P_2)\big) = \alpha_2$. L'extension $L_{nr}(E_p)/L_{nr}(\mu_p)$ est de degré p et il existe un élément s du groupe de Galois $\mathrm{Gal}\big(L_{nr}(E_p)/L_{nr}(\mu_p)\big)$ satisfaisant à $s(P_1) = P_1$ et $s(P_2) = P_1 + P_2$.

DÉMONSTRATION: L'application $P \mapsto T(P)$ (où $T(P) = -X(P)/Y(P)$ et où $T(0) = 0$) est un isomorphisme du groupe E_p sur le groupe N_p des points de p-torsion du groupe formel associé à E_L. On a $\alpha_1 > \alpha_2$; les éléments non nuls de N_p ont pour valuation α_1 ou α_2 et l'ensemble des éléments P de E_p pour lesquels on a $v\big(T(P)\big) \geq \alpha_1$ est un sous-groupe d'ordre p de E_p (cf. [**2**, Lemme 2 et démonstration de la Proposition 2 (a)]). Il existe donc deux éléments P_1 et P_2 de E_p indépendants sur $\mathbb{F}_p$ tels que l'on ait $v\big(T(P_1)\big) = \alpha_1$ et $v\big(T(P_2)\big) = \alpha_2$.

Le corps $L_{nr}(E_p)$ contient $L_{nr}(\mu_p)$. Le degré de l'extension $K_{nr}(E_p)/K_{nr}(\mu_p)$ est égal à p (cf. *loc. cit.*, Proposition 4).

Comme le degré de L_{nr}/K_{nr} est égal au dénominateur de $v(\Delta)/12$, il est premier à p; le degré de $L_{nr}(\mu_p)/K_{nr}(\mu_p)$ est donc aussi premier à p. L'égalité $K_{nr}(E_p).L_{nr}(\mu_p) = L_{nr}(E_p)$ montre alors que $L_{nr}(E_p)/L_{nr}(\mu_p)$ est une extension de degré p. Par ailleurs, dans la base (P_1, P_2) l'homomorphisme $\mathrm{Gal}\big(\overline{K}/L_{nr}(\mu_p)\big) \to \mathrm{Aut}(E_p)$ donnant l'action de $\mathrm{Gal}\big(\overline{K}/L_{nr}(\mu_p)\big)$ sur E_p est représentable matriciellement sous la forme

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix},$$

(cf. *loc. cit.*, Proposition 2 (a)); le lemme en résulte. □

Lemme 6. *Supposons toujours $h = 2$. Posons $n = \big[L_{nr} : K_{nr}(\mu_p) \cap L_{nr}\big]$.*

(a) *On a*

$$n = \begin{cases} 3 & \text{si } v(\Delta) = 2 \\ 2 & \text{si } v(\Delta) = 3 \\ 3 & \text{si } v(\Delta) = 4. \end{cases}$$

(b) *Supposons de plus que $\big(v(\Delta), v(c_4), v(c_6)\big)$ soit l'un des triplets $(2,1,1)$, $(3,1,2)$, $(4,2,2)$.*

(i) *On a $\big[L_{nr}(E_p) : K_{nr}\big] = np(p-1)$;*

(ii) *la différente de l'extension $L_{nr}(E_p)/L_{nr}(\mu_p)$ est la puissance D''-ième de l'idéal de valuation de $L_{nr}(E_p)$, où D'' est un entier satisfaisant l'égalité*

$$nD = D'' + (n-1)(p-1) + np(p-2).$$

Démonstration: Soit T l'unique extension quadratique de K_{nr}. Si $v(\Delta) = 2$, le groupe $\mathrm{Gal}\,(L_{nr}/K_{nr})$ est cyclique d'ordre 6; T est donc contenu dans L_{nr}. L'extension $K_{nr}(\mu_p)/K_{nr}$ étant cyclique de degré $p-1$, T est aussi contenu dans $K_{nr}(\mu_p)$. Comme $p-1$ n'est pas divisible par 3 (cf. [**2**, Lemme 1]), on a l'égalité $T = L_{nr} \cap K_{nr}(\mu_p)$; on a donc $n = 3$. Si $v(\Delta) = 3$, $\mathrm{Gal}\,(L_{nr}/K_{nr})$ est d'ordre 4. Comme $p-1$ n'est pas divisible par 4 (*loc. cit.*), on a encore $T = L_{nr} \cap K_{nr}(\mu_p)$; d'où $n = 2$. Si $v(\Delta) = 4$, $\mathrm{Gal}\,(L_{nr}/K_{nr})$ est d'ordre 3. Comme $p-1$ n'est pas divisible par 3 (*loc. cit.*), on a $n = 3$; cela démontre l'assertion (a).

Démontrons l'assertion (b). On a $\big[K_{nr}(E_p) : K_{nr}(\mu_p)\big] = p$ (cf. [**2**, Proposition 2 (a), et Proposition 4]), et $\big[L_{nr}(E_p) : L_{nr}(\mu_p)\big] = p$ (Lemme 5). Puisque l'on a $K_{nr}(E_p).L_{nr}(\mu_p) = L_{nr}(E_p)$, les extensions $L_{nr}(\mu_p)$ et $K_{nr}(E_p)$ sont donc linéairement disjointes sur $K_{nr}(\mu_p)$. De même, l'égalité $L_{nr}.K_{nr}(\mu_p) = L_{nr}(\mu_p)$ montre que n est égal à $\big[L_{nr}(\mu_p) : K_{nr}(\mu_p)\big]$; on a donc $n = \big[L_{nr}(E_p) : K_{nr}(E_p)\big]$.

L'assertion (i) en résulte: on a

$$\big[L_{nr}(E_p) : K_{nr}\big] = n\big[K_{nr}(E_p) : K_{nr}(\mu_p)\big]\big[K_{nr}(\mu_p) : K_{nr}\big] = np(p-1).$$

L'extension $L_{nr}(\mu_p)/K_{nr}(\mu_p)$ est de degré n, donc est modérément ramifiée. Sa différente est la puissance $n-1$-ième de l'idéal de valuation de $L_{nr}(\mu_p)$; elle engendre la puissance $p(n-1)$-ième de l'idéal de valuation de $L_{nr}(E_p)$. D'après la propriété de transitivité des différentes [**5**, p.60, Proposition 8], la différente de l'extension $L_{nr}(E_p)/K_{nr}(\mu_p)$ est la puissance $\big(D'' + (n-1)p\big)$-ième de l'idéal de valuation de $L_{nr}(E_p)$. Calculons-la d'une autre façon. L'extension $L_{nr}(E_p)/K_{nr}(E_p)$ est de degré n, donc modérément ramifiée. Sa différente est la puissance $(n-1)$-ième de l'idéal de valuation de $L_{nr}(E_p)$. Par ailleurs, la différente de l'extension $K_{nr}(E_p)/K_{nr}(\mu_p)$ est la puissance $\big(D - p(p-2)\big)$-ième de l'idéal de valuation de $K_{nr}(E_p)$ (formule (2)). Par transitivité des différentes, la différente de $L_{nr}(E_p)/K_{nr}(\mu_p)$ est la puissance $\big((n-1) + n\big(D - p(p-2)\big)\big)$-ième de l'idéal de valuation de $L_{nr}(E_p)$. En conclusion, on a $D'' + (n-1)p = (n-1) + n\big(D - p(p-2)\big)$, d'où l'assertion (b). □

DÉMONSTRATION DU THÉORÈME 3 LORSQUE h EST ÉGAL À 2. On introduit les notations suivantes:

- ψ désigne le caractère fondamental de niveau 2, égal à $\chi_{1/(p^2-1)}$ (cf. par exemple [**2**, p.7 pour sa définition]);
- $(G_i)_{i\geq 0}$ est la suite des sous-groupes de ramification de l'extension $L_{nr}(E_p)/L_{nr}(\mu_p)$;
- D'' est l'entier défini de la façon suivante: la différente de l'extension $L_{nr}(E_p)/L_{nr}(\mu_p)$ est la puissance D''-ième de l'idéal de valuation de $L_{nr}(E_p)$. On a

$$D'' = \sum_{i\geq 0}\big(|G_i| - 1\big) \quad \text{(Remarque 1)}. \tag{5}$$

(1) Cas où $v(\Delta) = 2$

L'hypothèse $h = 2$ implique que l'on a dans ce cas $p \equiv 2 \bmod 3$ [**2**, Lemme 1].

Supposons $v(c_4) = 1$. Soient P_1, P_2 et s comme dans le Lemme 5. L'élément $\pi = T(P_2)$ est une uniformisante de $L_{nr}(E_p)$ (Lemme 5 et Lemme 6 (b) (i)). On a

$$s\big(T(P_2)\big) = T(P_1 + P_2) = T(P_1) + T(P_2) + \text{des termes de valuation} > v\big(T(P_1)\big),$$

(cf. [**7**, formule (16)]), d'où $v(s(\pi) - \pi) = v\big(T(P_1)\big) = 2/3(p-1)$. On a donc les égalités (cf. Lemme 6 (b) (i)):

$$|G_i| = \begin{cases} p & \text{si } 0 \leq i \leq 2p-1 \\ 1 & \text{si } i \geq 2p. \end{cases}$$

https://doi.org/10.1017/S0004972700036595 Published online by Cambridge University Press

On en déduit $D'' = 2p(p-1)$ (formule (5)) et $D = (5p^2 - 6p - 2)/3$ (Lemme 6 (b) (ii)).

Supposons $v(c_4) \neq 1$; la condition (b) du début du paragraphe II.4.2 est alors satisfaite, avec $\varphi = \psi^{(5p^2+1)/6}$ (cf. [**2**, Proposition 2 (b)]). L'ordre de φ est $(p^2-1)/\delta$, où δ est le p.g.c.d de (p^2-1) et $(5p^2+1)/6$; δ divise 6. Il est clair que δ ne peut être égal à 2 ou 6, sinon $5p^2+1$ serait divisible par 4, ce qui est impossible. Par ailleurs, δ est égal à 3 si et seulement si on a $5p^2 + 1 \equiv 0 \bmod. 9$ c'est-à-dire, $p \equiv \pm 4 \bmod. 9$. De l'hypothèse $p \equiv 2 \bmod. 3$, on déduit l'équivalence: $\delta = 3$ si et seulement si $p \equiv 5 \bmod. 9$. Il suffit alors d'appliquer le Lemme 4 pour obtenir l'assertion (i) du Théorème 3.

(2) Cas où $v(\Delta) = 3$

L'hypothèse $h = 2$ implique que l'on a dans ce cas $p \equiv 3 \bmod. 4$ [**2**, Lemme 1].

Supposons $v(c_6) = 2$. Soient P_1, P_2 et s comme dans le Lemme 5. L'élément $\pi = T(P_2)$ est une uniformisante de $L_{nr}(E_p)$ (Lemme 5 et Lemme 6 (b) (i)). On a

$$s\big(T(P_2)\big) = T(P_1 + P_2) = T(P_1) + T(P_2) + \text{des termes de valuation} > v\big(T(P_1)\big),$$

(cf. [**7**, formule (16)]), d'où $v\big(s(\pi) - \pi\big) = v\big(T(P_1)\big) = 1/2(p-1)$. On a donc les égalités (cf. Lemme 6 (b) (i)):

$$|G_i| = \begin{cases} p & \text{si } 0 \leq i \leq p-1 \\ 1 & \text{si } i \geq p. \end{cases}$$

On en déduit $D'' = p(p-1)$ (formule (5)) et $D = (3p^2 - 4p - 1)/3$ (Lemme 6 (b) (ii)).

Supposons $v(c_6) \neq 2$; la condition (b) du début de II.4.2 est alors satisfaite, avec $\varphi = \psi^{(3p^2+1)/4}$ (cf. [**2**, Proposition 2 (b)]). L'ordre de φ est $(p^2-1)/\delta$, où δ est le p.g.c.d de (p^2-1) et $(3p^2+1)/4$. Comme on a $3p^2 + 1 \equiv 4 \bmod. 8$, δ est nécessairement égal à 1. D'après le Lemme 4, on a $D = p^2 - 2$.

(3) Cas où $v(\Delta) = 4$

L'hypothèse $h = 2$ implique que l'on a dans ce cas $p \equiv 2 \bmod. 3$ [**2**, Lemme 1].

Supposons $v(c_4) = 2$. Soient P_1, P_2 et s comme dans le Lemme 5. Posons $m = (p-1)/2$. L'élément

$$\pi = \frac{T(P_1)}{T(P_2)^m}$$

est une uniformisante de $L_{nr}(E_p)$ (Lemme 5 et Lemme 6 (b) (i)). On a $s\big(T(P_1)\big) = T(P_1)$, $s\big(T(P_2)\big) = T(P_3)$ avec $P_3 = P_1 + P_2$ et $s(\pi) - \pi$ est égal à

$$T(P_1)\frac{T(P_2)^m - T(P_3)^m}{T(P_2)^m T(P_3)^m}.$$

Par ailleurs, on a

$$T(P_3) = T(P_1) + T(P_2) + \text{des termes de valuation} > v\big(T(P_1)\big),$$

(cf. [**7**, formule (16)]), d'où $T(P_3)^m - T(P_2)^m = mT(P_1)T(P_2)^{m-1}$+des termes dont la valuation est strictement supérieur à celle de $mT(P_1)T(P_2)^{m-1}$ (car on a $v\big(T(P_1)\big) > v\big(T(P_2)\big)$ et $v(m) = 0$). On en déduit que $v(s(\pi) - \pi)$ est égal à $2v\big(T(P_1)\big) - (m+1)v\big(T(P_2)\big)$, c'est-à-dire, à $1/3p$. On a donc les égalités (cf. Lemme 6 (b) (i)):

$$|G_i| = \begin{cases} p & \text{si } 0 \le i \le p-2 \\ 1 & \text{si } i \ge p-1, \end{cases}$$

$D'' = (p-1)^2$ et $D = \big(4p^2 - 6p - 1\big)/3$ (Lemme 6 (b) (ii)).

Supposons $v(c_4) \neq 2$; la condition (b) du début de II.4.2 est alors satisfaite, avec $\varphi = \psi^{(2p^2+1)/3}$ (cf. [**2**, Proposition 2 (b)]). Soit δ le p.g.c.d de $\big(p^2-1\big)$ et $\big(2p^2+1\big)/3$; δ divise 3. En tenant compte de l'hypothèse $p \equiv 2 \bmod 3$, on voit que l'on a $\delta = 3$ si $p \equiv 2 \bmod 9$ et $\delta = 1$ sinon. L'ordre de φ étant $\big(p^2-1\big)/\delta$, l'assertion (iii) du Théorème se déduit alors du Lemme 4. Cela termine la démonstration du Théorème 3.

II.5. Le Théorème 4.

On suppose que E a mauvaise réduction de type additif sur K, et que l'on a $v(j) \ge 0$ et $p = 3$.

Lemme 7. *Supposons* $2v(c_6) \le 4 + v(\Delta)$. *On a* $K_{nr}(E_3) = K_{nr}\big(\mu_3, \Delta^{1/3}\big)$.

Démonstration: D'après [**2**, Proposition 6] et la Remarque 2, $K_{nr}(E_3)$ est une extension de degré 2 ou 6 de K_{nr}. Le Lemme en résulte d'après [**4**, 5.3. (b)]. □

Démonstration du Théorème 4.

(1) Cas où $v(\Delta) \equiv 0 \bmod 3$

(a) Supposons $2v(c_6) \le 4 + v(\Delta)$. Si on a $\Delta'^{r-1} \equiv 1 \bmod 9$, Δ' est un cube dans K_{nr} (Lemme 1) et donc Δ également; dans ce cas, $K_{nr}(E_3)$ est égal à $K_{nr}(\mu_3)$ (Lemme 7) et est une extension quadratique, modérément ramifiée de K_{nr}, de sorte que $D = 1$. Si on a $\Delta'^{r-1} \not\equiv 1 \bmod 9$, $K_{nr}(E_3)$ est une extension de degré 6 de K_{nr} (*loc. cit.*). On peut écrire $\Delta' = z'\Delta_1$, où z' appartient à μ_{r-1} et où Δ_1 est un élément de K de valuation 0 congru à 1 modulo 3; z' étant un cube dans K (car $z'^r = z'$), on a $K_{nr}(E_3) = K_{nr}\Big(\mu_3, \Delta_1^{1/3}\Big)$. Puisque $\Delta'^{r-1} = \Delta_1^{r-1}$, on a $v(\Delta_1 - 1) = 1$, d'où $v\Big(\Delta_1^{1/3} - 1\Big) = 1/3$ (Lemme 2). Soit z une racine primitive cubique de l'unité; on a $v(z-1) = 1/2$ et l'élément $\pi = (z-1)\Big/\Big(\Delta_1^{1/3} - 1\Big)$ est une uniformisante de $K_{nr}(E_3)$. Notons σ un générateur du groupe $\mathrm{Gal}\big(K_{nr}(E_3)/K_{nr}(\mu_3)\big)$.

On a $\sigma\left(\Delta_1^{1/3}\right) = t\Delta_1^{1/3}$, avec t une racine primitive de l'unité, et l'on a

$$\sigma(\pi) - \pi = (z-1)\Delta_1^{1/3}\frac{1-t}{\left(\Delta_1^{1/3}-1\right)\sigma\left(\Delta_1^{1/3}-1\right)},$$

d'où $v\big(\sigma(\pi)-\pi\big) = (1/2)+(1/2)-(2/3) = 1/3$. Il en résulte que l'on a $|H_0| = |H_1| = 3$ et $|H_i| = 1$ pour $i \geq 2$, d'où $D' = 4$ (formule (1)) et $D = 7$ (formule (2)).

(b) Supposons $2v(c_6) > 4 + v(\Delta)$. Soit ψ le caractère fondamental de niveau 2, égal à $\chi_{1/8}$. La représentation de $\mathrm{Gal}\left(\overline{K}/K_{nr}\right)$ dans E_3 s'écrit matriciellement, après extension des scalaires à $\overline{\mathbb{F}_3}$ sous la forme

$$\begin{pmatrix}\psi & 0\\ 0 & \psi^3\end{pmatrix} \quad \text{ou bien} \quad \begin{pmatrix}\psi^5 & 0\\ 0 & \psi^7\end{pmatrix},$$

(cf. [2, Proposition 7]). Comme ψ et ψ^5 sont des caractères d'ordre 8, on a $D = 7$ (Lemme 4).

(2) Cas où $v(\Delta) \not\equiv 0 \bmod 3$

D'après l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on a nécessairement $v\big(c_6^2\big) \leq v(1728\Delta)$, donc on a $2v(c_6) \leq 4 + v(\Delta)$. Le corps $K_{nr}(E_3)$ est égal à $K_{nr}\big(\mu_3, \Delta^{1/3}\big)$ (Lemme 7). Si $v(\Delta)$ est de la forme $3n+1$, posons $x = \Delta 3^{-3n}$; si $v(\Delta)$ est de la forme $3n+2$, posons $x = \Delta^2 3^{-6n-3}$. On a $v(x) = 1$ et $K_{nr}(E_3) = K_{nr}\big(\mu_3, x^{1/3}\big)$. Soit z une racine cubique primitive de l'unité. On a $v(z-1) = 1/2$. L'élément $\pi = (z-1)/x^{1/3}$ est une uniformisante de K_{nr}. Soit σ un générateur du groupe $\mathrm{Gal}\big(K_{nr}(E_3)/K_{nr}(\mu_3)\big)$. On a $\sigma\big(x^{1/3}\big) = tx^{1/3}$, avec t une racine primitive de l'unité, et

$$\sigma(\pi) - \pi = (z-1)\frac{x^{1/3}(1-t)}{x^{1/3}\sigma\big(x^{1/3}\big)},$$

d'où $v\big(\sigma(\pi)-\pi\big) = 2/3$. Il en résulte que l'on a $|H_i| = 3$ pour $i \leq 3$, et $|H_i| = 1$ pour $i \geq 4$, d'où $D' = 8$ (formule (1)) et $D = 11$ (formule (2)).

Cela termine la démonstration du Théorème 4. □

II.6. Le Théorème 5.

On suppose que E a mauvaise réduction de type additif sur K, et que l'on a $v(j) \geq 0$ et $p = 2$.

Les invariants c_4, c_6, Δ étant ceux associés à un modèle minimal de E, le triplet $\big(v(\Delta), v(c_4), v(c_6)\big)$ ne peut être de la forme (m,n,t) avec $m \geq 16$, $n \geq 8$ et $t \geq 11$. L'égalité $c_4^3 - c_6^2 = 1728\Delta$, les inégalités $3v(c_4) \geq v(\Delta) > 0$, impliquent alors que $\big(v(\Delta), v(c_4), v(c_6)\big)$ est l'un des triplets indiqués dans le tableau ci-dessous:

$v(\Delta)$	4	6	7	8	9	10	11
$v(c_4)$	≥ 4	$4 \quad \geq 5$	4	$4 \quad \geq 5$	$4 \quad 5$	$4 \quad \geq 6$	4
$v(c_6)$	5	$\geq 6 \quad 6$	6	$6 \quad 7$	$6 \quad \geq 8$	$6 \quad 8$	6

$v(\Delta)$	12	13	14	15	16	17	18
$v(c_4)$	$4 \quad \geq 6 \quad 6$	6	$6 \quad \geq 7$	$6 \quad 7$	6	6	6
$v(c_6)$	$6 \quad 9 \quad \geq 10$	9	$9 \quad 10$	$9 \quad \geq 11$	9	9	9

En particulier l'équation

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

est à coefficients entiers et est une équation minimale de E sur K. Posons

$$P(T) = T^3 - \left(\frac{c_4}{48}\right)T - \left(\frac{c_6}{864}\right).$$

Dans le modèle (W) les abscisses des points de E_2 sont donnés par l'équation $P(x) = 0$.

LEMME 8. *Le degré n de l'extension $K_{nr}(E_2)/K_{nr}$ est égal à 1, 2 ou 3. On a $n = 2$ si et seulement si Δ n'est pas un carré dans K_{nr}; si tel est le cas, on a $K_{nr}(E_2) = K_{nr}(\sqrt{\Delta})$.*

DÉMONSTRATION: Le groupe $\mathrm{Gal}(K_{nr}(E_2)/K_{nr})$ est un sous-groupe de $\mathbb{GL}_2(\mathbb{F}_2)$ et $\mathbb{GL}_2(\mathbb{F}_2)$ est d'ordre 6. D'après [**2**, IV], on ne peut avoir $n = 6$. Le lemme résulte alors de [**4**, 5.3. (a)]. □

DÉMONSTRATION DU THÉORÈME 5.

(I): Supposons que $v(\Delta)$ soit impair: d'après le Lemme 8, on a $K_{nr}(E_2) = K_{nr}(\sqrt{d})$ où d est un élément de K de valuation 1; $\sqrt{d}$ est une uniformisante de $K_{nr}(E_2)$. Notons σ l'élément non trivial de $\mathrm{Gal}(K_{nr}(E_2)/K_{nr})$; on a $\sigma(\sqrt{d}) = -\sqrt{d}$ et $v\left(\sigma(\sqrt{d}) - \sqrt{d}\right) = 3/2$; cela entraîne les égalités $|H_i| = 2$ si $0 \leq i \leq 2$, et $|H_i| = 1$ si $i \geq 3$, d'où $D = 3$ (formule (1)).

(II): Supposons que $v(\Delta)$ soit pair:

(1) si l'on a $\Delta'^{r-1} \equiv -1 \bmod 4$, Δ n'est pas un carré dans K_{nr} (Lemme 1); $K_{nr}(E_2)$ est égal à $K_{nr}(\sqrt{\Delta'})$ (Lemme 8). On a $v\left(\sigma(\sqrt{\Delta'}) - \sqrt{\Delta'}\right) = 1$, d'où $|H_0| = |H_1| = 2$ et $|H_i| = 1$ pour $i \geq 2$, ce qui entraîne que D est égal à 2 (formule (1)).

(2) Supposons que l'on ait $v(\Delta) \in \{6, 8, 12, 14\}$ et $3v(c_4) \geq 8 + v(\Delta)$.

L'égalité $c_4^3 - c_6^2 = 1728\Delta$ et l'inégalité $3v(c_4) \geq 8 + v(\Delta)$ impliquent $2v(c_6) = 6 + v(\Delta)$, et $\Delta' \equiv {c'_6}^2 \bmod. 4$, où $c'_6 = c_6/2^{v(c_6)}$. Une uniformisante de K congrue à 1 modulo 4 est un carré dans K_{nr} (Lemme 1), donc Δ' et Δ sont des carrés dans K_{nr}. On a donc $\left[K_{nr}(E_2) : K_{nr}\right] = 1$ ou 3 (Lemme 8). Sous les hypothèses précédentes, l'étude du polygône de Newton de P permet de vérifier directement que les racines de P sont de valuation non entière (cf. le tableau ci-dessus). En particulier, il n'y a pas de point d'ordre 2 défini sur K_{nr}, et $K_{nr}(E_2)$ est une extension de degré 3 (nécessairement modérément ramifiée) de K_{nr}; cela implique que D est égal à 2 (formule (1)).

(3) Supposons maintenant que nous ne soyons dans aucun des deux cas envisagés précédemment. Il résulte en particulier que l'on a $\Delta'^{r-1} \equiv 1 \bmod. 4$, et Δ est un carré dans K_{nr}. On a encore, d'après le Lemme 8,

$$\left[K_{nr}(E_2) : K_{nr}\right] = 1 \text{ ou } 3. \tag{6}$$

(3.1) Cas où $v(\Delta) \in \{6, 8, 12, 14\}$ et $3v(c_4) < 8 + v(\Delta)$.

L'étude du polygône de Newton de P montre, sous les hypothèses précédentes, que P a une racine dont la valuation est distincte des deux autres. Cette racine appartient donc à K_{nr}, et l'on déduit $K_{nr}(E_2) = K_{nr}$, d'où $D = 0$.

(3.2) Cas où $v(\Delta) \notin \{6, 8, 12, 14\}$.

On a ainsi $v(\Delta) \in \{4, 10, 16, 18\}$.

(a) Supposons $v(\Delta) = 4$. Le discriminant de P est $\Delta/16$; le polynôme $\widetilde{P}$ obtenu en réduisant P modulo 2 est donc séparable, et on peut relever par le Lemme de Hensel, les racines de $\widetilde{P}$ en trois racines de P dans K_{nr}; d'où $K_{nr}(E_2) = K_{nr}$, et $D = 0$.

(b) Supposons $v(\Delta) = 10$.

(b.1) Si $v(c_4) = 4$, l'étude du polygône de Newton de P montre que P a une racine de valuation 1, et deux racines de valuation 0; d'où $K_{nr}(E_2) = K_{nr}$ (formule (6)) et $D = 0$.

(b.2) Supposons $v(c_4) \geq 6$ (et donc $v(c_6) = 8$). Posons $A = -c_4/48$, $B = -c_6/864$, et $A = 2^{v(A)}A'$, $B = 2^{v(B)}B'$. Les racines de P sont de valuation 1 comme le montre l'étude du polygône de Newton de P. Tout revient à voir si le polynôme $Q(Y) = Y^3 + 2^{v(A)-2}A'Y + B'$ a une racine ou non dans K_{nr}. Lorsque $v(A) = 2$, son discriminant est $-\left(4A'^3 + 27B'^2\right)$. Le polynôme $\widetilde{Q}$ déduit de Q par réduction modulo 2 est donc séparable. Si $v(A) \geq 3$, la séparabilité de Q est claire; on en déduit $K_{nr}(E_2) = K_{nr}$, et $D = 0$.

(c) Si $v(\Delta) = 16$ ou $v(\Delta) = 18$, l'étude du polygône de Newton de P montre que P a une racine de valuation 2, et deux racines de valuation 1; d'où $K_{nr}(E_2) = K_{nr}$ (*loc. cit.*), et $D = 0$.

https://doi.org/10.1017/S0004972700036595 Published online by Cambridge University Press

Cela termine la démonstration du Théorème 5. □

Bibliographie

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

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

[3] J.-P. Serre, *Groupes p-divisibles* (d'après J. Tate), (Sém. Bourbaki **318**, 1966/1967).

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

[5] J.-P. Serre, *Corps locaux, 3-ième édition* (Hermann, Paris, 1980).

[6] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Maths. **106** (Springer-Verlag, Berlin, Heidelberg, New York, 1986).

[7] J. Tate, 'The arithmetic of elliptic curves', *Invent. Math.* **23** (1974), 179–206.

[8] J. Tate, 'Algorithm for determining the type of a singular fiber in an elliptic pencil', in *Modular Functions of One Variable IV*, Lecture Notes in Math. **476** (Springer-Verlag, Berlin, Heidelberg, New York, 1975), pp. 33–52.

Université de Paris VI
Institut de Mathématiques, Case 247
4 place Jussieu 75252
Paris Cedex 05
France
e-mail: kraus@math.jussieu.fr