ACTA ARITHMETICA
104.1 (2002)

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

par

Élie Cali (Boulogne) et Alain Kraus (Paris)

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

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

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

L'article [2] est consacré au cas où $\ell = p$. On se préoccupera ici du cas où ℓ et p sont *distincts*, ce que l'on supposera dans toute la suite.

I. Énoncé des résultats. Considérons un corps K comme ci-dessus. Soit v la valuation de K qui prolonge celle de $\mathbb{Q}_p$; on suppose que v est normée : on a $v(p) = 1$. Soient E une courbe elliptique définie sur K et j son invariant modulaire. On note c_4, c_6 et Δ les invariants standard associés à un modèle minimal de E sur K ([10, 1.]). Les entiers $v(c_4)$, $v(c_6)$ et $v(\Delta)$ sont indépendants du modèle minimal choisi (cf. *loc. cit.*, 2.).

I.1. *Cas où E a bonne réduction sur K.* Rappelons pour mémoire l'énoncé suivant :

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

C'est une conséquence directe du critère de Néron–Ogg–Shafarevich (cf. [9, p. 184, th. 7.1]).

2000 *Mathematics Subject Classification*: Primary 11G07.

I.2. *Cas où* $v(j) < 0$

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

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

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

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

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

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

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

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

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

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

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

I.3.1. *Cas où* $p \geq 5$

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

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

I.3.2. *Cas où* $p = 3$

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

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

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

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

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

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

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

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

$v(\Delta)$	3	4	5	6	7
$v(c_6)=3$	$D=1$ *ou* 7 $(*)$	$D=4$	$D=7$	$D=0$	
$v(c_6)=4$	$D=7$		$D=11$		
$v(c_6)=5$	$D=1$			$D=4$	$D=11$
$v(c_6)\geq 6$	$D=1$			$D=0$	

$(*)$ *On a* $D=1$ *si et seulement si la congruence* $4x^3-(c_4/3)x-c_6/27\equiv 0 \bmod 9$ *a une solution dans l'anneau des entiers de* K.
Si $K=\mathbb{Q}_3$, *on a* $D=1$ *si et seulement si* $\Delta/27$ *est congru à* 2 *ou* 4 *modulo* 9.

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

$(**)$ *On a* $D=1$ *si et seulement si la congruence* $4x^3-(c_4/27)x-c_6/729\equiv 0 \bmod 9$ *a une solution dans l'anneau des entiers de* K.
Si $K=\mathbb{Q}_3$, *on a* $D=1$ *si et seulement si* $\Delta/3^9$ *est congru à* 2 *ou* 4 *modulo* 9.

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

I.3.3. *Cas où $p = 2$.* On suppose dans ce paragraphe que $K = \mathbb{Q}_2$. On notera $c_4' = c_4/2^{v(c_4)}$, $c_6' = c_6/2^{v(c_6)}$, $\Delta' = \Delta/2^{v(\Delta)}$. On désignera respectivement par $\overline{c_4'}$, $\overline{c_6'}$ et $\overline{\Delta'}$ les classes modulo $4\mathbb{Z}_2$ de c_4', c_6' et Δ'.

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

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

$v(\Delta)$	7	8	9	10
$v(c_4) = 4$	$D = 68$	$\begin{cases} \overline{\Delta'} = -1 \\ \overline{c_6'} = 1 \end{cases} \Rightarrow D = 8$ $\begin{cases} \overline{\Delta'} = -1 \\ \overline{c_6'} = -1 \end{cases} \Rightarrow D = 2$ $\begin{cases} \overline{\Delta'} = 1 \\ \overline{c_6'} = 1 \end{cases} \Rightarrow D = 32$ $\begin{cases} \overline{\Delta'} = 1 \\ \overline{c_6'} = -1 \end{cases} \Rightarrow D = 38$	$D = 16$	$\overline{c_6'} = 1 \Rightarrow D = 38$ $\overline{c_6'} = -1 \Rightarrow D = 32$
$v(c_4) = 5$		$D = 68$	$v(c_6) = 8 \Rightarrow D = 11$ $v(c_6) > 8 \Rightarrow D = 24$	
$v(c_4) = 6$		$\overline{c_6'} = 1 \Rightarrow D = 32$ $\overline{c_6'} = -1 \Rightarrow D = 38$		$\overline{c_4'} = -1 \Rightarrow D = 11$ $\overline{c_4'} = 1 \Rightarrow D = 50$
$v(c_4) = 7$		$\overline{c_6'} = 1 \Rightarrow D = 2$ $\overline{c_6'} = -1 \Rightarrow D = 8$		$D = 50$
$v(c_4) \geq 8$		$\overline{c_6'} = 1 \Rightarrow D = 2$ $\overline{c_6'} = -1 \Rightarrow D = 8$		$D = 11$

$v(\Delta)$	11	12	13	14
$v(c_4)=4$	$\overline{c_6'}=1 \Rightarrow D=38$ $\overline{c_6'}=-1 \Rightarrow D=32$	$D=2$		
$v(c_4)=6$		$\overline{c_4'}=1 \Rightarrow D=16$ $\overline{c_4'}=-1 \Rightarrow D=18$	$D=68$	$\overline{\Delta'}=-1 \Rightarrow D=11$ $\overline{\Delta'}=1 \Rightarrow D=50$
$v(c_4)=7$		$D=16$		$D=68$
$v(c_4)=8$		$D=2$		$D=50$
$v(c_4)\geq 9$		$D=2$		$D=11$

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

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

Rappel ([2, p. 411]). Soient N une extension finie de K_{nr} et M une extension galoisienne finie de N. La différente de l'extension M/N s'obtient de la façon suivante : soit $(G_i)_{i\geq 0}$ la suite des sous-groupes de ramification de l'extension M/N. Si π est une uniformisante de M, le groupe G_i est le sous-groupe du groupe de Galois $\mathrm{Gal}(M/N)$ formé des éléments σ tels que

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

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

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

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

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

II.1. *Le théorème 1.* On a par hypothèse $v(j)<0$. Il existe donc une unique extension minimale L de K, de degré au plus 2 sur K, sur laquelle E est isomorphe à la courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$, où q est l'élément entier de K^*

défini par l'égalité (cf. [8, IV, pp. 29–30], ou [9, pp. 355–357]) :

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

Rappelons le lemme suivant (cf. [6, p. 276], si E a réduction multiplicative) :

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

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

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

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

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

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

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

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

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

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

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

PROPOSITION 2. 1) *Supposons que E ait réduction de type multiplicatif sur K. Alors, on a* $K_{\mathrm{nr}}(E_\ell) = K_{\mathrm{nr}}(q^{1/\ell})$.

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

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

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

(La preuve de la formule (5) est la même que celle de l'égalité (4), p. 413 de [2] ; le fait que, dans notre situation, ℓ soit distinct de p n'intervient pas.)

Supposons que E ait réduction multiplicative sur K. Alors, L est une extension non ramifiée de K (cf. [9, th. 14.1]). D'après (5), on a donc $K_{\mathrm{nr}}(E_\ell) = K_{\mathrm{nr}}(\mu_\ell, q^{1/\ell})$. Puisque ℓ est distinct de p, le groupe μ_ℓ est contenu dans K_{nr} ; d'où l'assertion 1).

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

que $K_{\mathrm{nr}}(E_\ell)$ est contenu dans $K_{\mathrm{nr}}(\sqrt{-c_6}, q^{1/\ell})$. Inversement, démontrons l'inclusion

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

Considérons pour cela le caractère quadratique ε associé à l'extension $K_{\mathrm{nr}}(\sqrt{-c_6})/K_{\mathrm{nr}}$. La courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$ possède un point d'ordre ℓ rationnel sur K_{nr} (cf. [8, IV, p. 31], en tenant compte du fait que μ_ℓ est contenu dans K_{nr}). Puisque les courbes elliptiques E et $\mathbb{G}_m/q^{\mathbb{Z}}$ sont isomorphes sur $K_{\mathrm{nr}}(\sqrt{-c_6})$, elles se déduisent l'une de l'autre par torsion par le caractère ε. On déduit de là qu'il existe une base de E_ℓ dans laquelle la représentation donnant l'action de $\mathrm{Gal}(\overline{K}/K_{\mathrm{nr}})$ sur E_ℓ s'écrit matriciellement sous la forme $\left(\begin{smallmatrix}\varepsilon & * \\ 0 & \varepsilon\end{smallmatrix}\right)$. Par conséquent, si σ est un élément de $\mathrm{Gal}(\overline{K}/K_{\mathrm{nr}}(E_\ell))$, on a $\varepsilon(\sigma) = 1$, autrement dit, σ fixe $\sqrt{-c_6}$. D'après (5), σ fixe aussi $q^{1/\ell}$, ce qui prouve l'inclusion (6), puis l'assertion 2). D'où la proposition.

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

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

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

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

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

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

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

2) Supposons que E ait réduction additive sur K.

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

2.2) Supposons $p = 2$. Il résulte de l'inégalité $v(j) < 0$, que l'on a (cf. [4, p. 129])

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

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

Lemme 2. *On a*

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

Démonstration. Posons $c_6' = c_6 2^{-v(c_6)}$. Soient $(H_i)_{i\geq 0}$ la suite des sous-groupes de ramification de l'extension $K_{\mathrm{nr}}(\sqrt{-c_6})/K_{\mathrm{nr}}$ et σ l'élément non trivial du groupe de Galois de $K_{\mathrm{nr}}(\sqrt{-c_6})$ sur K_{nr}. L'indice de ramification absolu de K étant égal à 1, le groupe H_3 est trivial (cf. [7, p. 79, 3) alinéa c)]).

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

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

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

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

Cela termine la démonstration du théorème 1.

II.2. *Le théorème 2.* 1) Supposons $\ell \neq 2$. Puisque ℓ est distinct de p, $K_{\mathrm{nr}}(E_\ell)$ est l'extension minimale de K_{nr} sur laquelle E acquiert bonne réduction ([3, p. 6, prop.]). Par ailleurs, p étant supérieur ou égal à 5, l'extension $K_{\mathrm{nr}}(E_\ell)/K_{\mathrm{nr}}$ est modérément ramifiée de degré m ([1, prop. 1]). D'après la formule (2), on a donc $D = m - 1$.

2) Supposons $\ell = 2$. Notons d le degré de l'extension $K_{\mathrm{nr}}(E_2)/K_{\mathrm{nr}}$. D'après la proposition de [3, p. 6], on a

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

2.1) Supposons que $v(\Delta)$ soit impair. On a alors $v(\Delta) \in \{3, 9\}$ (cf. [10, p. 46]), puis $m = 4$. Puisque d divise 6, on a donc $d = 2$, et d'après la formule (2), on a $D = 1$.

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

II.3. *Les théorèmes 3 et 4*

II.3.1. *Préliminaires.* Soit r un nombre premier impair et distinct de p. On désignera désormais par

• L l'extension minimale de K_{nr} sur laquelle E acquiert bonne réduction. On a l'égalité $L = K_{\mathrm{nr}}(E_r)$ ([3, p. 6, prop.]) ;

• Φ le groupe de Galois $\mathrm{Gal}(L/K_{\mathrm{nr}})$ (cf. [6, pp. 311–312] et [1]) ;

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

• I l'ensemble des entiers $i \geq 1$ tels que G_i ne soit pas le groupe réduit à l'élément neutre. C'est un ensemble fini ; plus précisément, on a (cf. [7, p. 79, 3) alinéa c)])

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

• δ l'invariant sauvage du $\mathrm{Gal}(\overline{K}/K_{\mathrm{nr}})$-module E_r (cf. [3, pp. 2–4]). On a

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

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

Lemme 3. *On a l'égalité*

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

Démonstration. Les deux membres de l'égalité à démontrer étant indépendants de r, on peut supposer que $r \geq 5$. Soit i un élément de I. Montrons que $E_r^{G_i}$ est le groupe trivial. Supposons pour cela qu'il existe un point P non nul de E_r fixé par G_i. D'après la proposition de [3, p. 6], on a $L = K_{\mathrm{nr}}(P)$. On déduit de là que G_i est réduit à l'élément neutre, ce qui conduit à une contradiction et prouve notre assertion. Le fait que $G_0 = \Phi$, et que E_r soit de dimension 2 sur $\mathbb{Z}/r\mathbb{Z}$, entraînent alors le lemme.

L'invariant δ peut se calculer en utilisant la formule de Ogg (cf. [3, th. 2]) : soit n le nombre de composantes connexes géométriques de la fibre spéciale du modèle de Néron de E. Alors, on a

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

Cette formule a été démontrée par Ogg dans *loc. cit.* si p est distinct de 2. Le cas général a par la suite été prouvé par Saito [5].

II.3.2. *Démonstration du théorème 3.* Les invariants c_4, c_6 et Δ étant ceux associés à un modèle minimal de E sur K, $(v(\Delta), v(c_6))$ est l'un des couples intervenant dans les tableaux figurant dans l'énoncé du théorème 3 (cf. [1, p. 365]).

II.3.2.1. *Cas où $\ell \geq 5$.* Notons O_K l'anneau des entiers de K.

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

• $(v(\Delta), v(c_6)) = (3,3)$ et la congruence $4x^3 - (c_4/3)x - c_6/27 \equiv 0 \bmod 9$ a une solution dans O_K ;

• $(v(\Delta), v(c_6)) = (9,6)$ et la congruence $4x^3 - (c_4/27)x - c_6/729 \equiv 0 \bmod 9$ a une solution dans O_K ;

• $(v(\Delta), v(c_6)) \in \{(3, \geq 5), (9, \geq 8)\}$.

On a $|\Phi| = 4$ ([1, cor., pp. 355–356]) et donc G_1 est trivial ; d'où $D = 3$ (formule (2)).

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

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

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

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

Si $(v(\Delta), v(c_6)) \in \{(3,3), (3,4)\}$ le type de Néron de E est II ([4, p. 126] et [1, p. 356]), et l'on a ainsi $n = 1$ ([10, p. 46]) ; si $(v(\Delta), v(c_6)) \in \{(9,6), (9,7)\}$, E de type est IV* et $n = 7$; si $(v(\Delta), v(c_6)) = (5,3)$, E est de type IV et $n = 3$; si $(v(\Delta), v(c_6)) = (11,6)$, E est de type II* et $n = 9$. D'après la formule (11), on constate que sous l'hypothèse (B), l'on a $\delta = 1$.

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

(C) Supposons que l'on ait

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

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

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

(D) Supposons que l'on ait

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

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

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

(E) Supposons que l'on ait :

• $(v(\Delta), v(c_6)) \in \{(6,3), (6, \geq 6)\}$.

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

(F) Supposons que l'on ait

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

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

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

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

II.3.2.2. *Cas où $\ell = 2$.* Soit $\Delta^{1/4}$ une racine quatrième de Δ dans $\overline{K}$. On a l'égalité ([1, p. 362, cor.])

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

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

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

Démonstration. Si 4 divise $v(\Delta)$, alors Δ est une puissance quatrième dans K_{nr}, et d'après l'égalité (12), on a $L = K_{\mathrm{nr}}(E_2)$, i.e. on a $s = 1$. Supposons $v(\Delta) \not\equiv 0 \bmod 4$. D'après la proposition de [3, p. 6], on a $s \leq 2$. Il suffit donc de prouver que les corps L et $K_{\mathrm{nr}}(E_2)$ sont distincts. Supposons le contraire, autrement dit que $\Delta^{1/4}$ appartienne à $K_{\mathrm{nr}}(E_2)$. Puisque 4 ne divise pas $v(\Delta)$, $\Delta^{1/4}$ n'est pas dans K_{nr}, et donc 2 divise le degré $[K_{\mathrm{nr}}(\Delta^{1/4}) : K_{\mathrm{nr}}]$. D'après l'hypothèse faite, 2 divise donc $[K_{\mathrm{nr}}(E_2) : K_{\mathrm{nr}}]$, et Δ n'est pas un carré dans K_{nr}. Il en résulte que $[K_{\mathrm{nr}}(\Delta^{1/4}) : K_{\mathrm{nr}}] = 4$, puis que 4 divise $[K_{\mathrm{nr}}(E_2) : K_{\mathrm{nr}}]$. Cela conduit à une contradiction car $[K_{\mathrm{nr}}(E_2) : K_{\mathrm{nr}}]$ divise 6. D'où le lemme.

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

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

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

II.3.3. *Démonstration du théorème 4.* On suppose désormais $K = \mathbb{Q}_2$. Le groupe Φ est isomorphe à un sous-groupe de $\mathrm{SL}_2(\mathbb{F}_3)$ ([6, p. 312]). On utilisera à plusieurs reprises le lemme suivant :

LEMME 5. *Le groupe* $\mathrm{SL}_2(\mathbb{F}_3)$ *ne possède pas de sous-groupe distingué d'ordre* 4.

Démonstration. Il existe un unique 2-sous-groupe de Sylow dans $\mathrm{SL}_2(\mathbb{F}_3)$. Il est d'ordre 8 isomorphe au groupe quaternionien. Il en résulte que $\mathrm{SL}_2(\mathbb{F}_3)$ a exactement trois sous-groupes d'ordre 4, qui sont cycliques. Ces trois sous-groupes sont engendrés respectivement par $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & -1 \\ -1 & -1 \end{smallmatrix}\right)$. On vérifie ensuite qu'ils ne sont pas distingués dans $\mathrm{SL}_2(\mathbb{F}_3)$. D'où le lemme.

Démontrons maintenant le théorème 4. Les invariants c_4, c_6 et Δ étant ceux associés à un modèle minimal de E sur $\mathbb{Q}_2$, $(v(c_4), v(\Delta))$ est l'un des couples intervenant dans l'énoncé du théorème 4 (cf. [1, p. 374]).

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

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

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

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

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

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

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

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

Le groupe Φ est d'ordre 24 et est isomorphe au groupe $\mathrm{SL}_2(\mathbb{F}_3)$. Par ailleurs, on a $\delta = 1$. On a ainsi l'égalité $\sum_{i \in I} |G_i| = 12$. Le groupe G_1 est

d'ordre 8. Puisque les sous-groupes G_i sont distingués dans $G_0 = \Phi$, on déduit alors du lemme 5 que $|G_2| = |G_3| = 2$, puis que $|G_i| = 1$ si $i \geq 4$. Cela conduit à $D = 32$.

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

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

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

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

Prouvons que l'on a

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

Remarquons d'abord que l'on a l'égalité $G_2 = G_3$ (cf. [7, p. 79, 3) alinéa e)]). Puisque G_1 est d'ordre 8, l'ordre de G_2 divise 8. Supposons que $|G_2| = 8$. On a alors $G_1 = G_2 = G_3$, et l'égalité (13) implique $|G_4| = 1$. Par ailleurs, G_1 est isomorphe au 2-sous-groupe de Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$, qui est quaternionien d'ordre 8. Ainsi G_2 possède un élément s d'ordre 4. D'après *loc. cit.*, s^2 appartient à G_4, et en particulier, G_4 n'est pas trivial. On obtient ainsi une contradiction et donc $|G_2| \neq 8$. D'après le lemme 5 le groupe G_2 n'est pas d'ordre 4, et la formule (13) entraîne $|G_2| \neq 1$. D'où l'égalité (14).

On déduit alors de (13) et (14) que $|G_i| = 2$ pour $2 \leq i \leq 9$, et $|G_i| = 1$ si $i \geq 10$. On obtient ainsi $D = 38$.

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

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

On a $|\Phi| = 8$ et $\delta = 3$, de sorte que $\sum_{i \in I} |G_i| = 12$. Le groupe G_1 est d'ordre 8. Par ailleurs, on a $|G_2/G_3| \leq 2$ ([7, p. 79, 3) alinéa e)]). On déduit de là que $|G_2| = |G_3| = 2$ et $|G_i| = 1$ si $i \geq 4$. D'où $D = 16$.

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

- $(v(c_4), v(\Delta)) = (4, 6)$ et $\overline{c'_4} = 1$;
- $(v(c_4), v(\Delta)) = (6, 12)$ et $\overline{c'_4} = -1$;
- $(v(c_4), v(\Delta)) \in \{(5, 6), (6, 15)\}$.

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

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

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

(G) Supposons que l'on ait

- $(v(c_4), v(\Delta)) \in \{(\geq 6, 6), (6, 18)\}$.

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

(H) Supposons que l'on ait

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

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

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

Prouvons que l'on a

$$|G_i| = \begin{cases} 8 & \text{si } 1 \leq i \leq 5, \\ 2 & \text{si } 6 \leq i \leq 15, \\ 1 & \text{si } i \geq 16. \end{cases} \tag{17}$$

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

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

En effet, supposons $G_1 \neq G_2$. Puisque G_1 est d'ordre 8, il résulte du lemme 5 que $|G_2| = 2$. Cela entraîne les inégalités $|G_i| \leq 2$ si $i \geq 2$; le fait que G_i soit trivial si $i \geq 25$ (formule (9)) contredit alors (16) : d'où $G_1 = G_2$. Par ailleurs, l'alinéa 3) e) p. 79 de [7] entraîne $G_2 = G_3$ et $G_4 = G_5$. D'où les égalités (18).

Vérifions que l'on a l'égalité

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

On considère pour cela un élément s d'ordre 3 de Φ et un élément t d'ordre 4 de G_3 (un tel élément t existe, car d'après (18), G_3 est quaternionien d'ordre 8). Le corollaire 1, p. 77 de [7], appliqué avec $i = 3$, implique que $sts^{-1}t^{-1}$ appartient à G_4. En identifiant Φ et $\mathrm{SL}_2(\mathbb{F}_3)$, on constate que quel

que soit le choix de s et t, l'élément $sts^{-1}t^{-1}$ est d'ordre 4. On déduit de là que l'ordre de G_4 est divisible par 4, ce qui implique $|G_4| = 8$ (lemme 5) et l'égalité (19).

On remarque ensuite que

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

En effet, si $G_6 \neq G_7$, les entiers $i \geq 1$ tels que $G_i \neq G_{i+1}$ sont pairs ([7, p. 77, prop. 11]), et le groupe G_1 devrait alors être cyclique, ce qui n'est pas (cf. *loc. cit.*, p. 79, alinéa f)).

On déduit de là que

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

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

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

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

- $(v(c_4), v(\Delta)) = (5, 9)$ et $v(c_6) = 8$;
- $(v(c_4), v(\Delta)) = (7, 15)$ et $v(c_6) = 11$.

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

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

- $(v(c_4), v(\Delta)) = (5, 9)$ et $v(c_6) > 8$;
- $(v(c_4), v(\Delta)) = (7, 15)$ et $v(c_6) > 11$.

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

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

On a $G_1 = \Phi$. Prouvons que

$$|G_i| = \begin{cases} 4 & \text{si } i = 2, 3, \\ 2 & \text{si } 4 \leq i \leq 7, \\ 1 & \text{si } i \geq 8. \end{cases} \tag{23}$$

Puisque G_1 n'est pas cyclique, on a $G_{2i} = G_{2i+1}$ pour tout $i \geq 1$ (cf. [7, p. 77, prop. 11 et p. 79 alinéa f)]). On déduit de là que $G_1 \neq G_2$: en effet, si

$G_1 = G_2$, le groupe G_4 est trivial (cf. (22) et le fait que $G_2 = G_3$), et G_2 possède un élément d'ordre 4, ce qui conduit à une contradiction. D'après la formule (9) on a $|G_9| = 1$; l'égalité (22) implique alors $|G_2| = 4$. Il en résulte que G_8 est trivial, puis que $|G_4| \neq 4$: si $|G_4| = 4$, G_4 est cyclique d'ordre 4, ce qui entraîne de nouveau une contradiction. On a ainsi $|G_4| = 2$. D'où les formules (23) et le fait que $D = 24$.

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

- $(v(c_4), v(\Delta)) = (6, 10)$ et $\overline{c'_4} = -1$;
- $(v(c_4), v(\Delta)) = (6, 14)$ et $\overline{\Delta'} = -1$;
- $(v(c_4), v(\Delta)) \in \{(\geq 8, 10), (\geq 9, 14)\}$.

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

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

- $(v(c_4), v(\Delta)) = (6, 10)$ et $\overline{c'_4} = 1$;
- $(v(c_4), v(\Delta)) = (6, 14)$ et $\overline{\Delta'} = 1$;
- $(v(c_4), v(\Delta)) \in \{(7, 10), (8, 14), (6, 16), (6, 17)\}$.

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

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

Vérifions que

$$|G_i| = \begin{cases} 8 & \text{si } i = 1, \\ 2 & \text{si } 2 \leq i \leq 21, \\ 1 & \text{si } i \geq 22. \end{cases} \tag{25}$$

Tout revient à démontrer que G_2 est d'ordre 2. Puisque G_1 est d'ordre 8 et non cyclique, on a $G_{2i} = G_{2i+1}$ pour tout $i \geq 1$. Supposons $|G_2| = 8$. Dans ce cas, on a $G_1 = G_2$, et G_2 possède un élément t d'ordre 4. Si s est un élément d'ordre 3 de Φ, l'élément $sts^{-1}t^{-1}$ est d'ordre 4 et appartient à G_4 (cf. l'alinéa, (H) ci-dessus). D'après le lemme 5, on a alors $|G_4| = 8$. On a donc aussi $|G_5| = 8$ et l'on déduit de (24) que le groupe G_{10} est trivial. Cela conduit à une contradiction, car G_5 a un élément d'ordre 4, et G_{11} ne peut donc être trivial. D'où $|G_2| \neq 8$. Puisque $|G_2| \neq 4$ (lemme 5), on a donc $|G_2| = 2$. D'où (25) et le fait que $D = 50$.

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

- $(v(c_4), v(\Delta)) \in \{(4, 12), (\geq 8, 12)\}$.

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

Cela termine la démonstration du théorème 4.

Appendice. Types de Néron des courbes elliptiques sur $\mathbb{Q}_2$ d'invariant modulaire entier. Soit E une courbe elliptique définie sur $\mathbb{Q}_2$ ayant mauvaise réduction de type additif. Soit v la valuation 2-adique de $\mathbb{Q}_2$. On suppose que l'invariant modulaire j de E vérifie $v(j) \geq 0$. Soient c_4, c_6 et Δ les invariants standards associés à un modèle *minimal* de E sur $\mathbb{Q}_2$. Le triplet $(v(c_4), v(c_6), v(\Delta))$ ne dépend pas du modèle minimal choisi. On détermine dans cet Appendice le type de Néron de E sur $\mathbb{Q}_2$ en fonction du triplet (c_4, c_6, Δ), ainsi que la valeur de l'entier

$$\delta = v(\Delta) - 1 - n,$$

où n est le nombre de composantes connexes géométriques de la fibre spéciale du modèle de Néron de E (cf. [10, p. 46]), que l'on a utilisée dans la démonstration du théorème 4.

On note

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

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

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

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

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

$v(\Delta)$	9	9	10		10	11		12	12		12
$v(c_4)$	4	5	4		≥ 6	4		4	6		7
$v(c_6)$	6	≥ 8	6		8	6		6	≥ 10		9
$\overline{c'_4}$									-1	1	
$\overline{c'_6}$			1	-1		1	-1				
Type de Néron	I_0^*	*III*	I_2^*	III^*	I_0^*	I_3^*	II^*	I_4^*	I_2^*	I_3^*	III^*
δ	3	6	2	1	4	2	1	2	4	3	3

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

Démonstration. Le fait que l'on parte d'un modèle minimal de E sur $\mathbb{Q}_2$ implique que le triplet $(v(c_4), v(c_6), v(\Delta))$ est l'un de ceux indiqués dans les tableaux ci-dessus (cf. [1, p. 374]). Dans tous les cas, l'équation de Weierstrass

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

est un modèle entier minimal de E (cf. [10, 1.]). Afin de déterminer le type de Néron de E, nous allons utiliser principalement l'article de Papadopoulos ([4]). Avec les notations de *loc. cit.*, on a

$$a_1 = a_2 = a_3 = 0, \quad a_4 = -2^{v(c_4)-4}\left(\frac{c'_4}{3}\right), \quad a_6 = -2^{v(c_6)-5}\left(\frac{c'_6}{27}\right),$$

$$b_2 = 0, \quad b_4 = -2^{v(c_4)-3}\left(\frac{c'_4}{3}\right),$$

$$b_6 = -2^{v(c_6)-3}\left(\frac{c'_6}{27}\right), \quad b_8 = -2^{2v(c_4)-8}\left(\frac{c'^2_4}{9}\right).$$

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

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

(A) Supposons $(v(c_4), v(c_6), v(\Delta)) = (4, 5, 4)$. Le type de Néron de E est II, III ou IV (*loc. cit.*, p. 129). On utilise la proposition 1 de *loc. cit.* avec $r = 1$ et $t = 1$. On est alors amené à décider si 4 divise $A(1,1)$. On vérifie pour cela que

$$A(1,1) \equiv c'_4 + c'_6 \bmod 4.$$

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

$$B(1) \equiv 2(3 - c'_4) \bmod 8.$$

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

(B) Supposons $(v(c_4), v(c_6), v(\Delta)) = (\geq 5, 5, 4)$. Le type de Néron de E est II, III ou IV. On a

$$A(0, 1) \equiv c'_6 - 1 \bmod 4.$$

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

(C) Supposons $(v(c_4), v(c_6), v(\Delta)) = (4, \geq 7, 6)$. Le type de Néron de E est II ou III. Par ailleurs, on a

$$A(1, 0) = c'_4 + 1 \bmod 4.$$

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

(D) Supposons $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. Le type de Néron de E est I_0^*, I_1^* ou IV^*. Remarquons que l'égalité $c_4^3 - c_6^2 = 1728\Delta$ implique la congruence

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

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

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

On vérifie que l'on a la congruence

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

Par ailleurs, on a

$$27A(c'_6, 2) \equiv -2c'_6 - 9c'_4c'_6 + 27c_6'^3 + 4 \bmod 16. \tag{3}$$

D'après (1), on a $c_4'^2 \equiv 9 \bmod 16$, et de l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on déduit alors que $9c'_4 \equiv -4\Delta' + c_6'^2 \bmod 16$. La congruence (3) conduit ainsi à

$$27A(c'_6, 2) \equiv 4(3 + \Delta'c'_6) \bmod 16.$$

En particulier, on a $A(c'_6, 2) \equiv 0 \bmod 8$. Si $\Delta' \equiv -c'_6 \bmod 4$, le type de Néron de E est donc I_0^* (*loc. cit.*, prop. 3). Si $\Delta' \equiv c'_6 \bmod 4$, la proposition 4 de *loc. cit.*, utilisée avec $r = c'_6$ (cf. (2)), entraîne alors le résultat.

(E) Supposons $(v(c_4), v(c_6), v(\Delta)) = (6, 7, 8)$. Le type de Néron de E est I_0^* ou I_1^*. On constate que

$$B(2) \equiv 0 \bmod 32.$$

Par ailleurs, on a

$$A(2, 2) \equiv 4(c_6' - 1) \bmod 16.$$

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

(F) Supposons $(v(c_4), v(c_6), v(\Delta)) = (\geq 7, 7, 8)$. Le type de Néron de E est I_0^* ou IV^*. On a

$$B(0) \equiv \bmod\ 32.$$

On vérifie par ailleurs que

$$A(0, 2) \equiv 4(c_6' - 1) \bmod 16,$$

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

(G) Supposons $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 10)$. Le type de Néron de E est I_2^* ou III^*. D'après l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on a les congruences $c_4' \equiv 1 \bmod 8$ et $c_4' \equiv c_6'^2 \bmod 16$. Par ailleurs, on a

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

On déduit de là que

$$B(c_6') \equiv 0 \bmod 32.$$

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

(H) Supposons $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 11)$. Le type de Néron de E est I_3^* ou II^*. L'égalité $c_4^3 - c_6^2 = 1728\Delta$ implique de nouveau $c_4' \equiv c_6'^2 \bmod 16$ et l'on a encore

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

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

(I) Supposons $(v(c_4), v(c_6), v(\Delta)) = (6, \geq 10, 12)$. Le type de Néron de E est I_2^* ou I_3^*. On va utiliser dans ce cas l'algorithme de Tate ([10, pp. 49–51]).

(I.1) Supposons $c_4' \equiv -1 \bmod 4$. Le changement de variables $x = X + 2$, $y = Y$ transforme le modèle initial (W) en l'équation

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

avec

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

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

(I.2) Supposons $c_4' \equiv 1 \bmod 4$. Le changement de variables $x = X + 2$, $y = Y + 4$ transforme le modèle (W) en l'équation

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

avec

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

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

(J) En ce qui concerne les autres cas qui figurent dans les tableaux intervenant dans l'énoncé du théorème, les types de Néron de E se lisent directement dans le tableau IV de [4, p. 129].

Cela termine la démonstration du théorème.

Références

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

[2] —, *Sur la p-différente du corps des points de p-torsion des courbes elliptiques*, Bull. Austral. Math. Soc. 60 (1999), 407–428.

[3] A. Ogg, *Elliptic curves and wild ramification*, Amer. J. Math. 89 (1967), 1–21.

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

[5] T. Saito, *Conductor*, *discriminant*, *and the Noether formula of arithmetic surfaces*, Duke Math. J. 57 (1988), 151–173.

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

[7] —, *Corps Locaux*, 3-ième éd., Hermann, Paris, 1980.

[8] —, *Abelian ℓ-Adic Representations and Elliptic Curves*, Adv. Book Classics, Addison-Wesley, 1989.

[9] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[10] J. Tate, *Algorithm for determining the type of singular fiber in an elliptic pencil*, dans : Modular Functions of One Variable IV, Lecture Notes in Math. 476, Springer, 1975, 33–52.

App. 231
9 rue de Sèvres
92100 Boulogne, France
E-mail: elie.cali@wanadoo.fr

Institut de Mathématiques
Université de Paris VI
UMR 7586 du CNRS
175 rue du Chevaleret
75013 Paris, France
E-mail: kraus@math.jussieu.fr

Reçu le 11.12.2000
et révisé le 20.9.2001 (3926)