POLSKA AKADEMIA NAUK, INSTYTUT MATEMATYCZNY

DISSERTATIONES MATHEMATICAE

(ROZPRAWY MATEMATYCZNE)

CCCLXIV

ALAIN KRAUS

Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique

WARSZAWA 1997

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

Published by the Institute of Mathematics, Polish Academy of Sciences
Typeset in TEX at the Institute
Printed and bound by

drukarnia
herman & herman
02-240 Warszawa, ul. Jakobinów 23, tel: 846-79-66, tel/fax: 49-89-95

PRINTED IN POLAND

ISSN 0012-3862

TABLE DES MATIÈRES

Résumé

Étant donnés un nombre premier p et une courbe elliptique E définie sur $\mathbb{Q}$, le groupe de Galois $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ agit sur le groupe des points de p-torsion de $E(\overline{\mathbb{Q}})$ suivant un homomorphisme continu $\varrho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. J.-P. Serre associe à ϱ deux entiers, un poids et un conducteur, qu'il a déterminés dans des cas particuliers. L'objet de ce travail est de les calculer dans tous les cas.

1991 *Mathematics Subject Classification*: Primary 11G.
Received 28.9.1994; revised version 20.6.1996.

Introduction

Considérons un nombre premier p et une courbe elliptique E définie sur $\mathbb{Q}$. Soient $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$, et $E_p(\overline{\mathbb{Q}})$ le sous-groupe des points de p-torsion de $E(\overline{\mathbb{Q}})$.

L'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $E_p(\overline{\mathbb{Q}})$ définit une représentation continue ϱ_p de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ dans un espace vectoriel de dimension 2 sur $\mathbb{Z}/p\mathbb{Z}$. A une représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ dans un espace vectoriel de dimension 2 sur un corps de caractéristique p, J.-P. Serre ([8], §1 et §2) associe un poids qui est un entier ≥ 2, un conducteur $N(\varrho_p)$ qui est un entier ≥ 1 premier à p, et un caractère de Dirichlet. Le caractère de Dirichlet associé de la sorte à ϱ_p est le caractère trivial. Le but de cet article est de calculer le poids k associé à ϱ_p et de comparer le conducteur $N(\varrho_p)$ associé à ϱ_p au conducteur de la courbe elliptique. Nous rappellerons pour mémoire les cas particuliers dans lesquels le couple $(N(\varrho_p), k)$ est déjà connu.

Je remercie J. Oesterlé pour les conseils qu'il a bien voulu me donner au cours de ce travail, ainsi que J.-P. Serre qui m'a adressé une lettre qui me fut très utile.

I. Détermination du poids

La définition du poids k ne dépend que de la restriction de la représentation ϱ_p au sous-groupe d'inertie de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ d'une place de $\overline{\mathbb{Q}}$ prolongeant la valuation p-adique de $\mathbb{Q}$. C'est pourquoi nous changeons de notations par rapport à l'introduction et nous nous plaçons dans la situation locale suivante :

Nous considérons une courbe elliptique E définie sur $\mathbb{Q}_p$. Nous notons $\overline{\mathbb{Q}}_p$ une clôture algébrique de $\mathbb{Q}_p$, E_p le groupe des points de p-torsion de $E(\overline{\mathbb{Q}}_p)$, G_p le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, v la valuation de $\overline{\mathbb{Q}}_p$ normalisée par $v(p) = 1$, ϱ la représentation continue de G_p dans le groupe E_p et k le poids qui lui est associé par Serre. Il résulte de la prop. 2 de [8], et du fait que le déterminant de ϱ est le caractère donnant l'action de G_p sur les racines p-ièmes de l'unité de $\overline{\mathbb{Q}}_p$, que l'on a $k \equiv 2 \bmod p-1$. J.-P. Serre détermine k lorsque E est à réduction semi-stable : si E a bonne réduction, on a $k = 2$; si E a mauvaise réduction de type multiplicatif et si $j = j(E)$ est son invariant modulaire, on a

$$k = \begin{cases} 2 & \text{si } p \text{ divise } v(j), \\ p+1 & \text{si } p \text{ ne divise pas } v(j) \text{ et } p \neq 2, \\ 4 & \text{si } p \text{ ne divise pas } v(j) \text{ et } p = 2 \end{cases}$$

(cf. *loc. cit.*, 2.9, prop. 5; noter que, à cet endroit, si p ne divise pas $v(j)$ et si p est égal à 2, la valeur de k est donnée par la définition (2.4.9)). J.-P. Serre indique également la valeur de k dans un cas particulier où E a une réduction de type additif (*loc. cit.*, 2.9, remarque 2, et [9]). L'objet de cette partie est de calculer k dans tous les cas où E a mauvaise réduction de type additif. La méthode suivie est directement inspirée de celle de [9].

A. Énoncé des résultats. Supposons que la courbe elliptique E (définie sur $\mathbb{Q}_p$) ait mauvaise réduction de type additif et soit j son invariant modulaire; notons c_4, c_6, Δ les invariants standards associés à un modèle minimal de E ([13], 1). Les invariants relatifs à un autre modèle minimal sont c_4u^4, c_6u^6, Δu^{12}, où u est une unité p-adique; ainsi $v(c_4)$, $v(c_6)$ et $v(\Delta)$ sont indépendants du modèle choisi.

THÉORÈME 1. *Supposons $p \geq 5$ (et E à réduction additive).*

(a) *Supposons $v(j) < 0$. On a*

$$k = \begin{cases} (p^2+3)/2 & \text{si } v(j) \equiv 0 \bmod p; \\ (p+1)^2/2 & \text{si } v(j) \not\equiv 0 \bmod p. \end{cases}$$

(b) *Supposons $v(j) \geq 0$. On est alors dans l'un des cas suivants :*

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

$$k = \begin{cases} 14 & \text{si } p = 7,\ v(c_4) = 1; \\ 2 & \text{si } p = 7,\ v(c_4) \neq 1; \\ (p^2+4p+7)/6 & \text{si } p \equiv 1 \bmod 3,\ p \neq 7; \\ (p^2+6p+5)/6 & \text{si } p \equiv 2 \bmod 3. \end{cases}$$

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

$$k = \begin{cases} 10 & \text{si } p = 5,\ v(c_6) = 2; \\ 2 & \text{si } p = 5,\ v(c_6) \neq 2; \\ (p^2+2p+5)/4 & \text{si } p \equiv 1 \bmod 4,\ p \neq 5; \\ (p^2+4p+3)/4 & \text{si } p \equiv 3 \bmod 4. \end{cases}$$

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

$$k = \begin{cases} (p^2+p+4)/3 & \text{si } p \equiv 1 \bmod 3; \\ (p^2+3p+2)/3 & \text{si } p \equiv 2 \bmod 3. \end{cases}$$

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

$$k = (p^2+3)/2.$$

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

$$k = \begin{cases} (p^2+4p+1)/3 & \text{si } p \equiv 1 \bmod 3; \\ (p^2+3p+2)/3 & \text{si } p \equiv 2 \bmod 3,\ v(c_4) = 3; \\ (p^2+5)/3 & \text{si } p \equiv 2 \bmod 3,\ v(c_4) \neq 3. \end{cases}$$

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

$$k = \begin{cases} (p^2+6p+1)/4 & \text{si } p \equiv 1 \bmod 4; \\ (p^2+4p+3)/4 & \text{si } p \equiv 3 \bmod 4,\ v(c_6) = 5; \\ (p^2+7)/4 & \text{si } p \equiv 3 \bmod 4,\ v(c_6) \neq 5. \end{cases}$$

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

$$k = \begin{cases} 2 & si\ p = 5; \\ (p^2+10p+1)/6 & si\ p \equiv 1 \bmod 3; \\ (p^2+6p+5)/6 & si\ p \equiv 2 \bmod 3,\ p \neq 5,\ v(c_4) = 4; \\ (p^2+11)/6 & si\ p \equiv 2 \bmod 3,\ p \neq 5,\ v(c_4) \neq 4. \end{cases}$$

THÉORÈME 2. *Supposons $p = 3$ (et E à réduction additive). Posons $\Delta = 3^{v(\Delta)}\Delta'$.*

(a) *Supposons $v(j) < 0$. On a*

$$k = \begin{cases} 8 & si\ v(\Delta) \not\equiv 0 \bmod 3; \\ 6 & si\ v(\Delta) \equiv 0 \bmod 3\ et\ \Delta' \not\equiv \pm 1 \bmod 9; \\ 2 & si\ v(\Delta) \equiv 0 \bmod 3\ et\ \Delta' \equiv \pm 1 \bmod 9. \end{cases}$$

(b) *Supposons $v(j) \geq 0$. On est alors dans l'un des cas du tableau suivant* :

$v(\Delta)$	3		4	5		6		7	9	10	11		12	13
$v(c_6)$	3	≥ 4	3	3	4	3	≥ 5	5	≥ 6	6	6	7	8	8
k	2 *ou* 6 (*)	6	8	8	4	2 *ou* 6 (*)	6	8	2	4	4	8	2	4

(*) *On a $k = 2$ si $\Delta' \equiv \pm 1 \bmod 9$ et $k = 6$ sinon.*

THÉORÈME 3. *Supposons $p = 2$ (et E à réduction additive). On a*

$$k = \begin{cases} 4 & si\ v(\Delta)\ est\ impair; \\ 2 & si\ v(\Delta)\ est\ pair. \end{cases}$$

B. Démonstrations. On introduit les notations suivantes :

• $\mathbb{F}_p$ le corps à p éléments;
• $\overline{\mathbb{F}}_p$ le corps résiduel de $\overline{\mathbb{Q}}_p$;
• $\mathbb{Q}_{p,\mathrm{nr}}$ l'extension non ramifiée maximale de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}}_p$;
• $I = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{nr}})$ le groupe d'inertie de $\overline{\mathbb{Q}}_p$ sur $\mathbb{Q}_p$;
• I_p le plus grand pro-p-sous-groupe de I, c'est-à-dire le groupe d'inertie sauvage de $\overline{\mathbb{Q}}_p$ sur $\mathbb{Q}_p$;
• μ_p le groupe des racines p-ièmes de l'unité de $\overline{\mathbb{Q}}_p$;
• χ le caractère à valeurs dans $\mathbb{F}_p^*$ donnant l'action de I sur μ_p;
• conformément à ([6], 1.7), on définit pour tout $\alpha \in \mathbb{Q}$ un caractère continu $\chi_\alpha : I \to \overline{\mathbb{F}}_p^*$ de la façon suivante : si $s \in I$, les éléments sx/x de $\overline{\mathbb{Q}}_p$, où x décrit l'ensemble des éléments de $\overline{\mathbb{Q}}_p$ de valuation α, sont congrus modulo l'idéal de v à un même élément de $\overline{\mathbb{F}}_p^*$, qui est par définition $\chi_\alpha(s)$. Le noyau de χ_α contient I_p. Tout caractère continu $I \to \overline{\mathbb{F}}_p^*$ est de la forme χ_α pour au moins un $\alpha \in \mathbb{Q}$. On a $\chi_{\alpha+\alpha'} = \chi_\alpha\chi_{\alpha'}$; on a χ_α=1 si et seulement si $\alpha \in \mathbb{Z}[1/p]$. Les caractères $\psi = \chi_{1/(p^2-1)}$ et $\psi' = \psi^p$ de I sont appelés par Serre les *caractères fondamentaux de niveau* 2. On a $\chi = \chi_{1/(p-1)}$ et $\psi\psi' = \chi$.

B.1. *Le cas $p \geq 5$, $v(j) \geq 0$*

1. ***Préliminaires.*** Le discriminant Δ étant celui d'un modèle minimal de E, on a $v(\Delta) \leq 12$ parce que $p \geq 5$ et $v(j) \geq 0$ ([13], 3, remarque 4). L'égalité $c_4^3 - c_6^2 = 1728\Delta$

et les inégalités $3v(c_4) \geq v(\Delta) > 0$ impliquent alors que $(v(\Delta), v(c_4), v(c_6))$ est l'un des triplets 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

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

est une équation minimale de E sur $\mathbb{Q}_p$ (cf. [13], 1).

Notons L le corps $\mathbb{Q}_p(p^{v(\Delta)/12})$. En effectuant le changement de variables

$$(1) \qquad \begin{cases} x = u^2X, \\ y = u^3Y \end{cases} \quad \text{avec } u = p^{v(\Delta)/12},$$

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

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

Cette équation est à coefficients entiers et son discriminant est de valuation 0, donc E_L a bonne réduction sur L et (W_L) est une équation minimale de E_L sur L.

Les fonctions $t = -x/y$ et $T = -X/Y$ sont des uniformisantes locales au voisinage du point à l'infini O et sont liées par l'égalité

$$(2) \qquad T = p^{v(\Delta)/12}t.$$

Notons h la hauteur de la réduction de E_L sur L (cf. [6], 1.11); par définition, on a $h = 1$ si E_L est à réduction ordinaire et $h = 2$ si E_L est à réduction supersingulière.

Lemme 1. (a) *Supposons que l'on ait* $v(\Delta) \in \{2, 4, 8, 10\}$ *ou que* $(v(\Delta), v(c_4), v(c_6))$ *soit de la forme* $(6, n, 3)$ *avec* $n \geq 3$. *L'invariant modulaire* $j(\widetilde{E_L})$ *de la courbe elliptique* $\widetilde{E_L}$ *déduite de* E_L *par réduction modulo l'idéal de la valuation de* L *est* 0. *On a* $h = 1$ *si* $p \equiv 1 \bmod 3$, *et* $h = 2$ *si* $p \equiv 2 \bmod 3$.

(b) *Supposons que l'on ait* $v(\Delta) \in \{3, 9\}$ *ou que* $(v(\Delta), v(c_4), v(c_6))$ *soit de la forme* $(6, 2, n)$ *avec* $n \geq 4$. *On a* $j(\widetilde{E_L}) = 1728$. *On a* $h = 1$ *si* $p \equiv 1 \bmod 4$, *et* $h = 2$ *si* $p \equiv 3 \bmod 4$.

Démonstration. Sous l'hypothèse de (a), on a $3v(c_4) > v(\Delta)$, donc $j(E) = j(E_L)$ est de valuation > 0 et on a $j(\widetilde{E_L}) = 0$. Sous l'hypothèse de (b), on a $2v(c_4) > v(\Delta)$, donc $j(E) - 1728 = j(E_L) - 1728$ est de valuation > 0 et on a $j(\widetilde{E_L}) = 1728$. Les assertions (a) et (b) en résultent ([1], p. 252, §4).

2. *Description de l'action de* I *sur* E_p

2.1. *Rappels*. Soient X, Y les fonctions coordonnées de Weierstrass de E_L dans le modèle (W_L). La fonction $T = -X/Y$ est une uniformisante locale de E_L au voisinage du point à l'infini O ([12], 3). Le complété formel en O du modèle (W_L) de E_L est muni

d'une loi de groupe formel sur l'anneau de valuation de L. La multiplication par p dans ce groupe formel est donnée par une série entière

$$[p](T) = \sum_{n=1}^{\infty} \tau_n T^n$$

à coefficients dans l'anneau de valuation de L (*loc. cit.*). La hauteur de ce groupe formel (cf. [6], 1.9) est égale à h (*loc. cit.*, 1.11).

2.2. *Notations*. Soient

• N_p le groupe des points de p-torsion du groupe formel associé à E_L, c'est-à-dire l'ensemble des éléments a de $\overline{\mathbb{Q}}_p$ tels que $v(a) > 0$ et $[p](a) = 0$;

• E_p le groupe des points de p-torsion de $E(\overline{\mathbb{Q}}_p) = E_L(\overline{\mathbb{Q}}_p)$;

• $\widetilde{E_L}$ la courbe elliptique déduite de E_L par réduction modulo l'idéal de la valuation de L;

• $\widetilde{E_{L,p}}$ le groupe des points de p-torsion de $\widetilde{E_L}(\overline{\mathbb{F}}_p)$;

Enfin, si $\alpha \in \mathbb{Q}$, m_α (resp. m_α^+) désignera l'ensemble des éléments a de $\overline{\mathbb{Q}}_p$ tels que $v(a) \geq \alpha$ (resp. $v(a) > \alpha$). Le quotient m_α/m_α^+ est un espace vectoriel de dimension 1 sur $m_0/m_0^+ = \overline{\mathbb{F}}_p$ ([6], 1.8). Le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ opère sur le groupe m_α/m_α^+. L'action du groupe d'inertie I sur m_α/m_α^+ est $\overline{\mathbb{F}}_p$-linéaire, et donnée par $s \mapsto \chi_\alpha(s)$, où χ_α est le caractère défini au début de B; cela découle de la définition même de ce caractère.

2.3. *L'action de I sur E_p*

2.3.1. *Cas où $h = 1$*

Proposition 1. *Lorsque $h = 1$, le nombre $\alpha = (p-1)v(\Delta)/12$ est entier et la représentation de I dans E_p s'écrit matriciellement*

$$\begin{pmatrix} \chi^{1-\alpha} & * \\ 0 & \chi^{\alpha} \end{pmatrix}$$

dans une base convenable de E_p sur $\mathbb{F}_p$.

Démonstration. Si $h = 1$, le groupe $\widetilde{E_{L,p}}$ est d'ordre p; on dispose d'une application de réduction $E_p \to \widetilde{E_{L,p}}$ qui est un homomorphisme surjectif de groupes ([6], 1.11). Soit C_p son noyau. Il est d'ordre p.

Considérons un point $P \in E_p$ non nul. On a $P \in C_p$ si et seulement si $v(Y(P)) < 0$, c'est-à-dire si et seulement si $v(y(P)) < v(\Delta)/4$ (formule (1)). Le sous-groupe C_p de E_p est stable par $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ puisque l'on a les égalités $v(y({}^\sigma P)) = v({}^\sigma(y(P))) = v(y(P))$ pour tout $\sigma \in G_p$.

Si $P \neq O$ est un élément de C_p, posons $T(P) = -X(P)/Y(P)$ et $t(P) = -x(P)/y(P)$. Posons par ailleurs $T(O) = t(O) = 0$. On a $v(T(P)) > 0$ pour tout $P \in C_p$, et l'application $P \mapsto T(P)$ est un isomorphisme du groupe C_p sur le groupe N_p. L'étude du polygône de Newton de la série formelle $[p]$ permet de montrer que pour tout $P \neq O$ dans C_p, on a $v(T(P)) = 1/(p-1)$ ([6], 1.10). Cela s'écrit aussi $v(t(P)) = \mu$, avec

$$\mu = \frac{1}{p-1} - \frac{v(\Delta)}{12}$$

d'après la formule (2).

Considérons alors l'application $f : C_p \to m_\mu/m_\mu^+$ définie par $f(P) = t(P) \bmod m_\mu^+$. Démontrons que t est un homomorphisme injectif de groupes compatible à l'action de G_p. Soient P, P' deux points de C_p. On a $v(T(P+P')-T(P)-T(P')) > 1/(p-1)$ ([12], 3, formule (16)), d'où $v(t(P+P')-t(P)-t(P')) > \mu$ (formule (2)), et cela prouve que f est un homomorphisme. Le fait que f commute à l'action de G_p résulte de ce que l'on a $t({}^\sigma P) = {}^\sigma(t(P))$ pour $\sigma \in G_p$ et $P \in C_p$.

Posons $\alpha = (p-1)v(\Delta)/12$. Le nombre α est entier : c'est clair si $v(\Delta) = 6$; si $v(\Delta) \neq 6$, on a $v(\Delta) \in \{2,3,4,8,9,10\}$ et cela résulte du lemme 1 et de l'hypothèse $h = 1$. On a $\mu = (1-\alpha)/(p-1)$, et le groupe d'inertie I opère sur m_μ/m_μ^+ via le caractère $\chi_\mu = \chi^{1-\alpha}$. Il opère donc aussi sur C_p suivant ce caractère. D'autre part, le déterminant de la représentation de I dans E_p est le caractère cyclotomique χ ([6], 1.11). Par conséquent, I opère sur E_p/C_p par le caractère χ^α, d'où la proposition.

2.3.2. *Cas où $h = 2$.* Soit τ_p le coefficient de T^p dans le développement de $[p](T)$.

Proposition 2. *Supposons $h = 2$. Posons $\alpha = (p+1)v(\Delta)/12$. Le nombre α est entier.*

(a) *Supposons $v(\tau_p) < p/(p+1)$. Dans une base convenable de E_p sur $\mathbb{F}_p$ la représentation de I dans E_p s'écrit matriciellement*

$$\begin{pmatrix} \chi^{1-\alpha} & * \\ 0 & \chi^\alpha \end{pmatrix} \quad \text{si } v(\Delta) < 6, \qquad \begin{pmatrix} \chi^{2-\alpha} & * \\ 0 & \chi^{\alpha-1} \end{pmatrix} \quad \text{si } v(\Delta) > 6.$$

(b) *Supposons $v(\tau_p) \geq p/(p+1)$. La représentation de I dans E_p est irréductible. La représentation de I dans $E_p \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ qu'on en déduit par extension des scalaires est diagonalisable et représentable matriciellement dans une base convenable par*

$$\begin{pmatrix} \psi^\alpha \psi'^{p-\alpha} & 0 \\ 0 & \psi'^\alpha \psi^{p-\alpha} \end{pmatrix},$$

où ψ et ψ' désignent les caractères $\chi_{1/(p^2-1)}$ et $\chi_{p/(p^2-1)}$ (appelés caractères fondamentaux de niveau 2 dans [6]*).*

Lemme 2. *Supposons $h = 2$. Si $(v(\Delta), v(c_4), v(c_6))$ est l'un des triplets $(2,1,1)$, $(3,1,2)$, $(4,2,2)$, $(8,3,4)$, $(9,3,5)$, $(10,4,5)$, on a*

$$v(\tau_p) = \begin{cases} v(\Delta)/6 & \text{si } v(\Delta) < 6, \\ (v(\Delta)/6) - 1 & \text{si } v(\Delta) > 6; \end{cases}$$

on a $v(\tau_p) \geq 1$ lorsque $(v(\Delta), v(c_4), v(c_6))$ n'est pas l'un des triplets ci-dessus.

Démonstration. Soit $u = p^{v(\Delta)/12}$, et $\tau(c_4, c_6)$ le coefficient de X^{p-1} dans l'expression

$$\left(X^3 - \frac{c_4}{48u^4}X - \frac{c_6}{864u^6}\right)^{(p-1)/2};$$

on a $v(\tau(c_4,c_6) - \tau_p) \geq 1$ (cf. appendice sur l'invariant de Hasse, théorème et lemme 1). On en déduit que l'on a

$$\begin{cases} v(\tau_p) = v(\tau(c_4,c_6)) & \text{si } v(\tau(c_4,c_6)) < 1, \\ v(\tau_p) \geq 1 & \text{si } v(\tau(c_4,c_6)) \geq 1. \end{cases} \tag{3}$$

On a

$$\tau(c_4,c_6)=\sum\frac{((p-1)/2)!(-1)^{l+m}}{k!l!m!(48)^l(864)^m}\left(\frac{c_4}{u^4}\right)^l\left(\frac{c_6}{u^6}\right)^m,$$

où la somme est étendue aux triplets (k,l,m) d'entiers ≥ 0 tels que $k+l+m=(p-1)/2$ et $3k+l=p-1$. Notons que les coefficients

$$\frac{((p-1)/2)!(-1)^{l+m}}{k!l!m!(48)^l(864)^m}$$

sont des unités p-adiques.

Si $v(\Delta)\in\{2,4,8,10\}$ (resp.$\{3,9\}$), on a $v(c_6)=v(\Delta)/2=v(u^6)$ (resp. $v(c_4)=v(\Delta)/3=v(u^4)$). Parce que $h=2$, on a $p\equiv 2 \bmod 3$ (resp. $p\equiv 3 \bmod 4$) (lemme 1). Ainsi les triplets (k,l,m) sur lesquels on somme sont tels que $l\neq 0$ (resp. $m\neq 0$) et il y en a un seul pour lequel $l=1$ (resp. $m=1$). Le terme de la somme correspondant a une valuation égale à $v(c_4)-(v(\Delta)/3)$ (resp. $v(c_6)-(v(\Delta)/2)$) et cette valuation est strictement inférieure à celle des autres termes. Par suite, on a $v(\tau(c_4,c_6))=v(c_4)-(v(\Delta)/3)$ (resp. $v(\tau(c_4,c_6))=v(c_6)-(v(\Delta)/2)$); le lemme résulte alors de (3). Lorsque $v(\Delta)=6$, u^2 est égal à p et appartient à $\mathbb{Q}_p$, donc $\tau(c_4,c_6)\in\mathbb{Z}_p$. D'après (3) on a $v(\tau_p)=0$ ou bien $v(\tau_p)\geq 1$. L'hypothèse $h=2$ entraîne que $v(\tau_p)\neq 0$ ([6], 1.10) d'où $v(\tau_p)\geq 1$.

Démonstration de la proposition 2. Si $h=2$, le groupe $\widetilde{E_{L,p}}$ est réduit à l'élément neutre et l'application $P\mapsto T(P)$ (où $T(P)=-X(P)/Y(P)$ si $P\neq 0$ et où $T(O)=0$) est un isomorphisme du groupe E_p sur le groupe N_p. Par ailleurs, $\alpha=(p+1)v(\Delta)/12$ est entier : c'est clair si $v(\Delta)=6$; si $v(\Delta)\neq 6$, on a $v(\Delta)\in\{2,3,4,8,9,10\}$ et cela résulte du lemme 1.

Supposons $v(\tau_p)<p/(p+1)$. L'étude du polygône de Newton de la série formelle $[p]$ montre que les éléments non nuls de N_p ont pour valuation $\alpha_1=(1-v(\tau_p))/(p-1)$ ou $\alpha_2=v(\tau_p)/(p^2-p)$ (cf. [6], 1.10). On a $\alpha_1>\alpha_2$ et l'ensemble A des éléments P de E_p pour lesquels $v(T(P))\geq\alpha_1$ est un sous-groupe d'ordre p de E_p. Si P est un point non nul de E_p, on a $v(t(P))=\alpha_1-v(\Delta)/12$ ou $v(t(P))=\alpha_2-v(\Delta)/12$ suivant que P appartient ou non à A (formule (1)); ainsi A est stable sous l'action de $G_p=\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Posons $\mu_1=\alpha_1-v(\Delta)/12$. Par une démonstration analogue à celle de la prop. 1, on vérifie que l'on définit un homomorphisme injectif de groupes $f_1: A\to m_{\mu_1}/m_{\mu_1}^+$ par $P\mapsto t(P) \bmod m_{\mu_1}^+$, compatible à l'action de G_p, puis que la représentation de I dans E_p s'écrit

$$\begin{pmatrix}\chi_{\mu_1} & * \\ 0 & \chi/\chi_{\mu_1}\end{pmatrix}$$

dans une base convenable de E_p. D'après le lemme 2, on a soit

$$v(\Delta)<6,\quad \mu_1=\frac{1}{p-1}-\frac{v(\Delta)}{6(p-1)}-\frac{v(\Delta)}{12}=\frac{1-\alpha}{p-1}\quad\text{et}\quad\chi_{\mu_1}=\chi^{1-\alpha},$$

soit

$$v(\Delta)>6,\quad \mu_1=\frac{2}{p-1}-\frac{v(\Delta)}{6(p-1)}-\frac{v(\Delta)}{12}=\frac{2-\alpha}{p-1}\quad\text{et}\quad\chi_{\mu_1}=\chi^{2-\alpha}.$$

Cela démontre l'assertion (a) de la prop. 2.

Supposons désormais $v(\tau_p) \geq p/(p+1)$. L'étude du polygône de Newton de la série formelle $[p]$ montre que les éléments non nuls de N_p ont pour valuation $1/(p^2-1)$ (cf. [6], 1.10). Si P est un point non nul de E_p, on a donc $v(t(P)) = \mu$ avec

$$\mu = \frac{1}{p^2-1} - \frac{v(\Delta)}{12}$$

(formule (2)). Par une démonstration analogue à celle de la prop. 1, on vérifie que l'application $f : E_p \to m_\mu/m_\mu^+$ définie par $f(P) = t(P) \bmod m_\mu^+$ est un homomorphisme injectif de groupes compatible à l'action de $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Si $\sigma \in I$, on a donc $f({}^\sigma P) = \chi_\mu(\sigma) f(P)$ pour $P \in E_p$, et $f(E_p)$ est un sous-groupe du $\overline{\mathbb{F}}_p$-espace vectoriel m_μ/m_μ^+, stable par l'homothétie de rapport $\chi_\mu(\sigma)$.

Soit $\mathbb{F}_{p^2}$ l'unique extension quadratique de $\mathbb{F}_p$ contenue dans $\overline{\mathbb{F}}_p$. Si $\sigma \in I$, on a $\chi_\mu(\sigma) \in \mathbb{F}_{p^2}$, car l'ordre de χ_μ divise p^2-1. Démontrons que χ_μ n'est pas d'ordre $p-1$. Si c'était le cas, on aurait $(p-1)\mu \in \mathbb{Z}[1/p]$, i.e.

$$\frac{1}{p+1} - \frac{(p-1)v(\Delta)}{12} \in \mathbb{Z}\left[\frac{1}{p}\right].$$

Cela entraîne que $p+1$ divise 6, d'où $p = 5$. Or $\frac{1}{6} - \frac{v(\Delta)}{3}$ n'appartient pas à $\mathbb{Z}[1/5]$. Puisque χ_μ n'est pas d'ordre $p-1$, le sous-anneau de $\overline{\mathbb{F}}_p$ engendré par les $\chi_\mu(\sigma)$, avec $\sigma \in I$, est $\mathbb{F}_{p^2}$; ainsi, $f(E_p)$ est stable par multiplication par les éléments de $\mathbb{F}_{p^2}$, et est un sous-$\mathbb{F}_{p^2}$-espace vectoriel de m_μ/m_μ^+. Comme f est injective, par transport de structure, on déduit une unique structure de $\mathbb{F}_{p^2}$-espace vectoriel sur E_p pour laquelle f est $\mathbb{F}_{p^2}$-linéaire. L'opération du groupe I sur E_p est alors donnée par

$${}^\sigma P = \chi_\mu(\sigma) P \quad (\sigma \in I,\ P \in E_p).$$

La représentation de I dans E_p est irréductible sur $\mathbb{F}_p$. Par contre, en tant que I-module, $E_p \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ est somme directe de deux $\overline{\mathbb{F}}_p$-espaces vectoriels de dimension 1 sur lesquels I agit suivant $\gamma_1 \circ \chi_\mu$ et $\gamma_2 \circ \chi_\mu$, où γ_1 et γ_2 sont les deux plongements de $\mathbb{F}_{p^2}$ dans $\overline{\mathbb{F}}_p$ (cf. [6], 1.9, dém. du cor. 3); autrement dit, après extension des scalaires à $\overline{\mathbb{F}}_p$, l'action de I est représentable matriciellement dans une base convenable par

$$\begin{pmatrix} \chi_\mu & 0 \\ 0 & \chi_{p\mu} \end{pmatrix}.$$

Si α est l'entier $(p+1)v(\Delta)/12$, on a

$$\mu = \frac{1}{p^2-1} - \frac{v(\Delta)}{12} = \frac{\alpha}{p^2-1} + \frac{(p-\alpha)p}{p^2-1} - 1,$$

d'où $\chi_\mu = \psi^\alpha \psi'^{p-\alpha}$ et $\chi_{p\mu} = \psi^{p-\alpha}\psi'^\alpha$. Cela démontre l'assertion (b) de la prop. 2.

2.4. *Le groupe E_p en tant que I_p-module.* Rappelons que l'on a posé $u = p^{v(\Delta)/12}$ et désigné par L le corps $\mathbb{Q}_p(u)$. Notons L_{nr} l'extension non ramifiée maximale de L dans $\overline{\mathbb{Q}}_p$. On a $L_{\mathrm{nr}} = \mathbb{Q}_{p,\mathrm{nr}}(u)$. L'extension L de $\mathbb{Q}_p$ est totalement ramifiée; son degré e est le dénominateur de $v(\Delta)/12$. L'entier e est aussi l'indice de ramification absolu de L_{nr}. Posons

$$C_4 = \frac{c_4}{u^4}, \quad C_6 = \frac{c_6}{u^6}. \tag{4}$$

Rappelons que l'équation

$$(W_L) \qquad Y^2 = X^3 - \frac{C_4}{48}X - \frac{C_6}{864}$$

est une équation minimale de E_L sur L, et que E_L a bonne réduction sur L.

Soit $\widetilde{E_L}$ la courbe déduite de E_L par réduction modulo l'idéal de la valuation de L, et $j(\widetilde{E_L})$ son invariant modulaire. Lorsque E_L a bonne réduction ordinaire, i.e. lorsque $h = 1$, on note $j_{\mathrm{can}}(\widetilde{E_L})$ l'invariant modulaire du relèvement canonique de $\widetilde{E_L}$ (cf. [5], 5); comme le corps résiduel de L est $\mathbb{F}_p$, on a $j(\widetilde{E_L}) \in \mathbb{F}_p$, et $j_{\mathrm{can}}(\widetilde{E_L})$ est un élément de $\mathbb{Z}_p$ qui relève $j(\widetilde{E_L})$ (*loc. cit.*).

Dans ce paragraphe, nous nous intéressons à la restriction au groupe d'inertie sauvage I_p de la représentation de G_p dans E_p. Comme le degré de L sur $\mathbb{Q}_p$ divise 12, il est premier à p, l'extension L de $\mathbb{Q}_p$ est modérément ramifiée et I_p est contenu dans $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L_{\mathrm{nr}})$. Plus précisément, I_p est le plus grand pro-p-sous-groupe de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L_{\mathrm{nr}})$.

2.4.1. *Cas où $h = 1$.* Soit $\widehat{L_{\mathrm{nr}}}$ le complété du corps L_{nr}. Le groupe d'inertie sauvage d'une extension galoisienne M de L_{nr} est égal au groupe d'inertie sauvage de l'extension $\widehat{M}$ de $\widehat{L_{\mathrm{nr}}}$, où $\widehat{M}$ désigne le complété de M (qui n'est autre que le composé de M et $\widehat{L_{\mathrm{nr}}}$). Il résulte alors de l'appendice sur les courbes elliptiques à réduction ordinaire que l'on peut associer à E_L un élément λ de $\widehat{L_{\mathrm{nr}}}$ possédant les propriétés suivantes :

Proposition 3. (a) *Le groupe I_p opère trivialement sur E_p si et seulement si λ est une puissance p-ième dans $\widehat{L_{\mathrm{nr}}}$.*

(b) *On a, en notant encore v la valuation de $\widehat{L_{\mathrm{nr}}}$ prolongeant celle de L_{nr},*

$$v(\lambda - 1) = \begin{cases} v(C_4)\ (= v(c_4) - v(\Delta)/3) & \text{si } j(\widetilde{E_L}) = 0, \\ v(C_6)\ (= v(c_6) - v(\Delta)/2) & \text{si } j(\widetilde{E_L}) = 1728, \\ v(j(E) - j_{\mathrm{can}}(\widetilde{E_L})) & \text{si } j(\widetilde{E_L}) \neq 0, 1728. \end{cases}$$

Pour savoir si λ est une puissance p-ième dans $\widehat{L_{\mathrm{nr}}}$, nous utiliserons le lemme suivant :

Lemme 3. *Soit u un élément de $\widehat{L_{\mathrm{nr}}}$ tel que l'on ait $v(u-1) > 0$.*

(i) *Si u est une puissance p-ième dans $\widehat{L_{\mathrm{nr}}}$, on a $v(u-1) \geq \inf(p/e, 1 + (1/e))$;*

(ii) *si on a $v(u-1) > p/(p-1)$, u est une puissance p-ième dans $\widehat{L_{\mathrm{nr}}}$.*

Démonstration. Supposons que u soit une puissance p-ième dans $\widehat{L_{\mathrm{nr}}}$. Dans ce cas u s'écrit $(1+z)^p$, avec z un élément de $\widehat{L_{\mathrm{nr}}}$ de valuation > 0. On a

$$u - 1 = \sum_{k=1}^{p-1} \binom{k}{p} z^k + z^p.$$

Pour chaque indice k, $1 \leq k \leq p-1$, p divise $\binom{k}{p}$ et on a $v\big(\binom{k}{p} z^k\big) \geq v(pz) \geq 1 + (1/e)$. Par ailleurs on a $v(z^p) \geq p/e$. L'assertion (i) en résulte.

Supposons que l'on ait $v(u-1) > p/(p-1)$. On a $v(u-1) - 1 > 1/(p-1)$ et u est la puissance p-ième d'un élément z de $\widehat{L_{\mathrm{nr}}}$ satisfaisant à l'inégalité $v(z-1) \geq v(u-1) - 1$ (cf. [7], p. 219, prop. 9). Cela démontre le lemme.

2.4.2. *Cas où $h = 2$.* On rappelle que τ_p est le coefficient de T^p dans le développement de $[p](T)$.

Lemme 4. *Supposons que E_L ait bonne réduction supersingulière. L'action de I_p sur E_p est triviale si et seulement si on a $v(\tau_p) \geq 1$.*

Démonstration. Si on a $v(\tau_p) \geq 1$, la représentation de I dans E_p est irréductible (prop. 2(b)) et I_p agit donc trivialement sur E_p ([6], prop. 4). Inversement, si on a $v(\tau_p) < 1$, $v(\tau_p)$ est égal à 1/3, 1/2 ou 2/3 (lemme 2) et il existe des éléments de N_p de valuation $v(\tau_p)/(p^2-p)$ (cf. dém. de la prop. 2). En particulier, p divise le degré de $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$ sur $\mathbb{Q}_{p,\mathrm{nr}}$ et l'action de I sur E_p n'est pas modérée, d'où le lemme.

2.4.3. *Liste des cas où l'action de I_p n'est pas triviale.* On conserve les notations des numéros 2.4.1 et 2.4.2.

Proposition 4. *Pour que I_p n'opère pas trivialement sur E_p, il faut et il suffit que l'une des conditions suivantes soit réalisée* :

(i) *on a* $(v(\Delta), v(c_4)) \in \{(2,1),(4,2),(8,3),(10,4)\}$;
(ii) *on a* $(v(\Delta), v(c_6)) \in \{(3,2),(9,5)\}$;
(iii) *on a* $(v(\Delta), v(c_4)) = (6,3)$ *et* $p \equiv 1 \bmod 3$;
(iv) *on a* $(v(\Delta), v(c_6)) = (6,4)$ *et* $p \equiv 1 \bmod 4$;
(v) *on a* $(v(\Delta), v(c_4), v(c_6)) = (6,2,3)$, $h = 1$ *et* $v(j(E) - j_{\mathrm{can}}(\widetilde{E_L})) = 1$.

Démonstration. 1) Supposons $v(\Delta) \geq 8$. On a $v(c_4) \geq 3$ et $v(c_6) \geq 4$. Il existe une courbe elliptique E' sur $\mathbb{Q}_p$ dont les invariants sont $c_4(E') = c_4/p^2$, $c_6(E') = c_6/p^3$ et $\Delta(E') = \Delta/p^6$. Les courbes E et E' se déduisent l'une de l'autre par torsion quadratique par $\sqrt{p}$. Ainsi, I_p agit trivialement sur E_p si et seulement si il en est de même sur E'_p. Il suffit donc de démontrer la prop. 4 sous l'hypothèse $v(\Delta) < 8$, hypothèse que nous faisons désormais.

2) *Cas où* $(v(\Delta), v(c_4), v(c_6)) \neq (6,2,3)$ *et* $h = 1$. Supposons $h = 1$. La prop. 3, les lemmes 1 et 3 permettent de vérifier les résultats indiqués dans le tableau ci-dessous :

$v(\Delta)$	2		3		4		6			
e	6		4		3		2			
$v(c_4)$	1	≥ 2	1		2	≥ 3	2		3	≥ 4
$v(c_6)$	1	1	2	≥ 3	2	2	4	≥ 5	3	3
$v(\lambda-1)$	1/3	$\geq 4/3$	1/2	$\geq 3/2$	2/3	$\geq 5/3$	1	≥ 2	1	≥ 2
$\inf(p/e, 1+1/e)$	7/6		5/4		4/3		3/2		3/2	
$p/(p-1)$		$\leq 7/6$		$\leq 5/4$		$\leq 7/6$		$\leq 5/4$		$\leq 7/6$
λ	$\notin (\widehat{L_{\mathrm{nr}}})^p$	$\in (\widehat{L_{\mathrm{nr}}})^p$	$\notin (\widehat{L_{\mathrm{nr}}})^p$	$\in (\widehat{L_{\mathrm{nr}}})^p$	$\notin (\widehat{L_{\mathrm{nr}}})^p$	$\in (\widehat{L_{\mathrm{nr}}})^p$	$\notin (\widehat{L_{\mathrm{nr}}})^p$	$\in (\widehat{L_{\mathrm{nr}}})^p$	$\notin (\widehat{L_{\mathrm{nr}}})^p$	$\in (\widehat{L_{\mathrm{nr}}})^p$

Dans le cas où nous sommes, la prop. 4 résulte alors de la prop. 3 et du lemme 1.

3) *Cas où* $h = 2$. Lorsque $h = 2$, on a d'après le lemme 2 le tableau suivant :

$v(\Delta)$	2		3		4		6
$v(c_4)$	1	≥ 2	1	1	2	≥ 3	≥ 2
$v(c_6)$	1	1	2	≥ 3	2	2	≥ 3
$v(\tau_p)$	1/3	≥ 1	1/2	≥ 1	2/3	≥ 1	≥ 1

Dans le cas où nous sommes, la prop. 4 résulte des lemmes 1 et 4.

4) *Cas où* $(v(\Delta), v(c_4), v(c_6)) = (6, 2, 3)$ *et* $h = 1$. D'après l'égalité $c_4^3 - c_6^2 = 1728\Delta$, on a $j(\widetilde{E_L}) \neq 0, 1728$. D'après la prop. 3, on a $v(\lambda - 1) = v(j(E) - j_{\mathrm{can}}(\widetilde{E_L}))$. L'élément $j_{\mathrm{can}}(\widetilde{E_L})$ appartient à $\mathbb{Z}_p$ (cf. [5], 5). Si $v(\lambda - 1) \geq 2$, on a $v(\lambda - 1) > p/(p-1)$, donc λ est une puissance p-ième dans $\widehat{L_{\mathrm{nr}}}$ (lemme 3) et I_p opère trivialement sur E_p (prop. 3). Par contre, si $v(\lambda - 1) = 1$, on a $v(\lambda - 1) < \inf(p/e, 1 + (1/e)) = 3/2$, donc λ n'est pas une puissance p-ième dans $\widehat{L_{\mathrm{nr}}}$ (lemme 3) et I_p n'opère pas trivialement sur E_p. Cela démontre la prop. 4 dans le cas où nous sommes, et qui est le dernier cas que nous avions à considérer.

3. *Ramification sauvage.* Dans ce numéro, exceptionnellement, p désigne un nombre premier quelconque (pas nécessairement ≥ 5).

Supposons que I_p n'opère pas trivialement sur E_p et que la représentation de I dans E_p s'écrive matriciellement sous la forme

$$\begin{pmatrix} \chi^{\beta} & * \\ 0 & \chi^{\alpha} \end{pmatrix},$$

α et β étant normalisés de telle sorte que $0 \leq \alpha \leq p-2$, $1 \leq \beta \leq p-1$. Si β est égal à $\alpha + 1$, il existe $x \in \mathbb{Q}_{p,\mathrm{nr}}^*$ tel que l'on ait $\mathbb{Q}_{p,\mathrm{nr}}(E_p) = \mathbb{Q}_{p,\mathrm{nr}}(\mu_p, x^{1/p})$ ([8], 2.4, (ii)). Dans cette situation, Serre dit que l'extension $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$ est *peu ramifiée* si x peut être choisi parmi les unités de $\mathbb{Q}_{p,\mathrm{nr}}$, et *très ramifiée* dans le cas contraire.

L'extension $\mathbb{Q}_{p,\mathrm{nr}}(E_p)/\mathbb{Q}_{p,\mathrm{nr}}(\mu_p)$ est par hypothèse cyclique de degré p. Notons w la valuation normalisée de $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$ (égale à $p(p-1)v$). Si π est une uniformisante de $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$, notons, pour $i \geq 0$, G_i le sous-groupe de $\mathrm{Gal}(\mathbb{Q}_{p,\mathrm{nr}}(E_p)/\mathbb{Q}_{p,\mathrm{nr}}(\mu_p))$ formé des éléments s satisfaisant à l'inégalité

$$w(s\pi - \pi) \geq i + 1.$$

Le groupe G_i est réduit à l'élément neutre pour i assez grand. Posons $\delta = w(D)$, où D est la différente de l'extension $\mathbb{Q}_{p,\mathrm{nr}}(E_p)/\mathbb{Q}_{p,\mathrm{nr}}(\mu_p)$. On a

$$\delta = \sum_{i \geq 0} (|G_i| - 1). \tag{5}$$

(Voir [7], p. 61, prop. 10. On prendra garde que dans cette référence, les corps locaux considérés sont supposés complets, ce qui n'est pas le cas ici. Cependant, on peut appliquer cette référence en remarquant que les groupes G_i et la valuation de la différente sont inchangés par passage au complété.)

Proposition 5. *Si l'extension* $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$ *est très ramifiée, on a* $\delta = p^2 - 1$; *on a* $\delta \leq p^2 - p$ *sinon.*

Démonstration. 1) Supposons que $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$ soit très ramifiée. Il existe alors un élément x de $\mathbb{Q}_{p,\mathrm{nr}}$ tel que p ne divise pas $v(x)$ et que $\mathbb{Q}_{p,\mathrm{nr}}(E_p) = \mathbb{Q}_{p,\mathrm{nr}}(\mu_p, x^{1/p})$. Quitte à remplacer x par $x^m p^{rp}$ avec m et r des entiers convenables, on se ramène au cas où $v(x) = 1$. On a $[\mathbb{Q}_{p,\mathrm{nr}}(E_p) : \mathbb{Q}_{p,\mathrm{nr}}] = p(p-1)$. Soit ζ une racine primitive p-ième de l'unité. Posons $\pi = (\zeta - 1)/x^{1/p}$. On a

$$v(\pi) = \frac{1}{p-1} - \frac{1}{p} = \frac{1}{p(p-1)};$$

par suite, π est une uniformisante de $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$. Si σ est un élément distinct de l'identité de $\mathrm{Gal}(\mathbb{Q}_{p,\mathrm{nr}}(E_p)/\mathbb{Q}_{p,\mathrm{nr}}(\mu_p))$, on a $\sigma(\zeta)=\zeta$ et il existe $z\in\mu_p$, $z\neq 1$ tel que $\sigma(x^1/p)=x^{1/p}/z$; on a donc $\sigma\pi-\pi=(z-1)\pi$ et $v(\sigma\pi-\pi)$ est égal à

$$\frac{1}{p-1}+\frac{1}{p(p-1)}=\frac{p+1}{p(p-1)}.$$

Alors $w(\sigma\pi-\pi)=p+1$, d'où $|G_i|=p$ pour $i\leq p$ et $G_i=(1)$ pour $i>p$. D'après la formule (5), on a $\delta=(p-1)(p+1)=p^2-1$. Cela prouve la première assertion de la proposition.

2) Supposons $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$ peu ramifiée. On a l'égalité $\mathbb{Q}_{p,\mathrm{nr}}(E_p)=\mathbb{Q}_{p,\mathrm{nr}}(\mu_p,u^{1/p})$, où u est un élément de $\mathbb{Q}_{p,\mathrm{nr}}$ de valuation 0. Soit $\sigma\in\mathrm{Gal}(\mathbb{Q}_{p,\mathrm{nr}}(E_p)/\mathbb{Q}_{p,\mathrm{nr}}(\mu_p))$, $\sigma\neq 1$. Il existe $z\in\mu_p$, $z\neq 1$, tel que l'on ait $\sigma u^{1/p}-u^{1/p}=(z-1)u^{1/p}$, et $v(\sigma u^{1/p}-u^{1/p})$ est égal à $1/(p-1)$. Si π est une uniformisante de $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$, on a donc $v(\sigma\pi-\pi)\leq 1/(p-1)$ (cf. [7], p. 69, lemme 1), d'où $w(\sigma\pi-\pi)\leq p$ et, par définition, G_p est trivial. Cela entraîne l'inégalité $\delta\leq(p-1)p=p^2-p$ d'après la formule (5); d'où la proposition.

4. *Démonstration de l'assertion* (b) *du théorème* 1. Rappelons que, sauf lorsque $(v(\Delta),v(c_4),v(c_6))=(6,2,3))$, la valeur de h est donnée dans le lemme 1.

4.1. *Cas où* $h=1$. La représentation de I dans E_p s'écrit matriciellement sous la forme

$$\begin{pmatrix}\chi^{1-\alpha} & *\\ 0 & \chi^{\alpha}\end{pmatrix}$$

avec $\alpha=(p-1)v(\Delta)/12$ (prop. 1). Posons $\beta=p-\alpha$. Le caractère $\chi^{1-\alpha}$ est égal à χ^{β}.

1) Supposons $v(\Delta)=2$. On a alors $p\equiv 1 \bmod 3$ (lemme 1). On a $\alpha=(p-1)/6$ et $\beta=(5p+1)/6$. Les entiers α et β satisfont aux inégalités $0\leq\alpha\leq p-2$ et $\alpha+1<\beta\leq p-2$, sauf si $p=7$.

Si on a $p\neq 7$, les définitions (2.3.2) et (2.4.5) de [8] montrent que l'on a $k=1+p\alpha+\beta$, i.e. $k=(p^2+4p+7)/6$.

Supposons $p=7$. On a $\alpha=1$ et $\beta=6$. Si $v(c_4)=1$, le groupe I_7 n'opère pas trivialement sur E_7 (prop. 4), d'où $k=14$ (cf. [8], (2.4.5)). Si $v(c_4)\neq 1$, I_7 opère trivialement sur E_7 (prop. 4); la représentation de I dans E_7 s'écrit matriciellement

$$\begin{pmatrix}1 & 0\\ 0 & \chi\end{pmatrix}$$

et l'on a $k=2$ (cf. [8], (2.3.2)).

2) Supposons $v(\Delta)=3$. On a alors $p\equiv 1 \bmod 4$ (lemme 1). On a $\alpha=(p-1)/4$ et $\beta=(3p+1)/4$; α et β satisfont aux inégalités $0\leq\alpha\leq p-2$ et $\alpha+1<\beta\leq p-2$, sauf si $p=5$.

Si $p\neq 5$, on a $k=1+p\alpha+\beta$, i.e. $k=(p^2+2p+5)/4$ (*loc. cit.*, (2.3.2) et (2.4.5)).

Supposons $p=5$. On a $\alpha=1$ et $\beta=4$. Si $v(c_6)=2$, d'après la prop. 4, I_5 n'opère pas trivialement sur E_5, d'où $k=10$ (*loc. cit.*, (2.4.5)). Si $v(c_6)\neq 2$, I_5 opère trivialement sur E_5 (prop. 4); la représentation de I dans E_5 s'écrit matriciellement

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

d'où $k=2$ (cf. [8], (2.3.2)).

3) Supposons $v(\Delta) = 6$. On a $\alpha = (p-1)/2$ et $\beta = (p+1)/2$. Les entiers α et β sont compris entre 1 et $p-2$ et satisfont à l'égalité $\beta = \alpha + 1$. Déterminons la ramification de l'extension $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$ (cf. n° 3). Les inégalités $v(c_4) \geq 2$, $v(c_6) \geq 3$ impliquent l'existence d'une courbe elliptique E' sur $\mathbb{Q}_p$, dont les invariants standards associés sont $\Delta(E') = \Delta/p^6$, $c_4(E') = c_4/p^2$ et $c_6(E') = c_6/p^3$. La courbe E' a bonne réduction sur $\mathbb{Q}_p$. La représentation de I définie par les points de p-torsion de E' est de poids 2 (cf. [8], prop. 5). La courbe E' est isomorphe à E sur $\mathbb{Q}_p(\sqrt{p})$. Le groupe $\mathrm{Gal}(\mathbb{Q}_{p,\mathrm{nr}}(\mu_p)/\mathbb{Q}_{p,\mathrm{nr}})$ est cyclique d'ordre $p-1$ et $\mathbb{Q}_{p,\mathrm{nr}}(\sqrt{p})$ est l'unique extension quadratique de $\mathbb{Q}_{p,\mathrm{nr}}$. Par suite, $\mathbb{Q}_{p,\mathrm{nr}}(\sqrt{p})$ est contenu dans $\mathbb{Q}_{p,\mathrm{nr}}(\mu_p)$ et en particulier dans $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$. Elle est de même contenue dans $\mathbb{Q}_{p,\mathrm{nr}}(E'_p)$. L'extension de $\mathbb{Q}_{p,\mathrm{nr}}$ engendrée par les points de p-torsion de E' est donc égale à $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$. D'après la prop. 3 de [8], l'action de I_p sur E'_p est soit triviale, soit peu ramifiée, et il en est donc de même de l'action de I_p sur E_p. Les définitions (2.3.2) et (2.4.8) de *loc. cit.* montrent alors que l'on a $k = 1 + p\alpha + \beta = (p^2+3)/2$.

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

(a) $v(\Delta) \in \{4, 8, 10\}$ (ce qui entraîne $p \equiv 1 \bmod 3$ d'après le lemme 1);
(b) $v(\Delta) = 9$ (ce qui entraîne $p \equiv 1 \bmod 4$ d'après le lemme 1).

On a le tableau suivant :

$v(\Delta)$	4	8	9	10
α	$(p-1)/3$	$2(p-1)/3$	$3(p-1)/4$	$5(p-1)/6$
β	$(2p+1)/3$	$(p+2)/3$	$(p+3)/4$	$(p+5)/6$

Si $v(\Delta) = 4$ et $p \equiv 1 \bmod 3$, on a $1 \leq \alpha \leq p-2$ et $\alpha + 1 < \beta \leq p-2$; d'où $k = 1 + p\alpha + \beta = (p^2+p+4)/3$ (cf. [8], (2.3.2) et (2.4.5)).

Dans les autres cas ci-dessus, les entiers α et β satisfont aux égalités $1 \leq \beta \leq \alpha \leq p-2$. D'où $k = 1+p\beta+\alpha$ (*loc. cit.*), ce qui conduit aux valeurs de k annoncées dans le théorème.

4.2. *Cas où $h = 2$.* 1) Supposons que l'on soit dans l'un des cas suivants :

(a) $(v(\Delta), v(c_4), v(c_6)) = (2, 1, 1)$ (et donc $p \equiv 2 \bmod 3$, d'après le lemme 1)
(b) $(v(\Delta), v(c_4), v(c_6)) = (3, 1, 2)$ (et donc $p \equiv 3 \bmod 4$, d'après le lemme 1)
(c) $(v(\Delta), v(c_4), v(c_6)) = (4, 2, 2)$ (et donc $p \equiv 2 \bmod 3$, d'après le lemme 1).

La représentation de I dans E_p s'écrit matriciellement

$$\begin{pmatrix} \chi^{1-\alpha} & * \\ 0 & \chi^{\alpha} \end{pmatrix}$$

avec $\alpha = (p+1)v(\Delta)/12$ (lemme 2 et prop. 2(a)). Le groupe I_p n'opère pas trivialement sur E_p (prop. 4). Le caractère $\chi^{1-\alpha}$ est égal à χ^{β} où $\beta = p - \alpha$. On a pour α et β les valeurs indiquées ci-dessous :

$v(\Delta)$	2	3	4
α	$(p+1)/6$	$(p+1)/4$	$(p+1)/3$
β	$(5p-1)/6$	$(3p-1)/4$	$(2p-1)/3$

Dans les cas (a) et (b), on a les inégalités $0 \leq \alpha < \beta \leq p-1$ et $\beta \neq \alpha+1$. Cela conduit à $k = 1 + p\alpha + \beta$ (cf. [8], (2.4.5)), ce qui donne les valeurs de k indiquées dans l'énoncé du théorème.

Supposons maintenant que l'on soit dans le cas (c) ci-dessus, i.e. que l'on ait $p \equiv 2 \bmod 3$ et $(v(\Delta), v(c_4), v(c_6)) = (4, 2, 2)$. On a $1 \leq \alpha < \beta \leq p-1$ et $\beta \neq \alpha+1$ sauf pour $p = 5$.

Si $p \neq 5$, on a $k = 1 + p\alpha + \beta$, i.e. $k = (p^2+3p+2)/3$ (*loc. cit.*).

Supposons $p = 5$. On a $\alpha = 2$ et $\beta = 3$. Pour déterminer k, il nous faut étudier la ramification sauvage de $\mathbb{Q}_{5,\mathrm{nr}}(E_5)$. Calculons pour cela la valuation normalisée δ sur $\mathbb{Q}_{5,\mathrm{nr}}(E_5)$ de la différente D de l'extension $\mathbb{Q}_{5,\mathrm{nr}}(E_5)/\mathbb{Q}_{5,\mathrm{nr}}(\mu_5)$ (cf. n° 3). Dans une base convenable (P_1, P_2) de E_5 sur $\mathbb{F}_5$, le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}_5/L_{\mathrm{nr}}(\mu_5))$ opère matriciellement par

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

en particulier, il existe $\sigma \in \mathrm{Gal}(L_{\mathrm{nr}}(E_5)/L_{\mathrm{nr}}(\mu_5))$ tel que l'on ait ${}^{\sigma}P_1 = P_1$ et ${}^{\sigma}P_2 = P_1+P_2$. On a $v(T(P_1)) = 1/12$ et $v(T(P_2)) = 1/30$ (cf. dém. de la prop. 2(b) et lemme 2). Le degré de L_{nr} sur $\mathbb{Q}_{5,\mathrm{nr}}$ (qui est le dénominateur de $v(\Delta)/12$) est égal à 3 et, de l'écriture matricielle de la représentation de I dans E_5, on déduit que $\mathbb{Q}_{5,\mathrm{nr}}(E_5)$ est une extension de degré 20 de $\mathbb{Q}_{5,\mathrm{nr}}$. Par suite, le degré de $L_{\mathrm{nr}}(E_5)$ sur $\mathbb{Q}_{5,\mathrm{nr}}$ est égal à 60 et l'élément $\pi = T(P_1)/T(P_2)^2$ est une uniformisante de $L_{\mathrm{nr}}(E_5)$. Posons $P_3 = P_1 + P_2$. On a

$$\sigma\pi - \pi = T(P_1)\left(\frac{1}{T(P_3)^2} - \frac{1}{T(P_2)^2}\right).$$

Par ailleurs, on a $T(P_3) = T(P_1) + T(P_2)$ + des termes de valuation $> 1/12$ (cf. [12], formule (16)), d'où $v(T(P_3) - T(P_2)) = v(T(P_1)) = 1/12$, et $v(T(P_3)) = v(T(P_3) + T(P_2)) = 1/30$. Il en résulte l'égalité $v(\sigma\pi - \pi) = 1/15$. Si v' est la valuation normalisée de $L_{\mathrm{nr}}(E_5)$, égale à $60v$, on a $v'(\sigma\pi - \pi) = 4$, donc les groupes de ramification supérieurs G_i de l'extension $L_{\mathrm{nr}}(E_5)/L_{\mathrm{nr}}(\mu_5)$ sont d'ordre 5 pour $i \leq 3$ et d'ordre 1 pour $i \geq 4$. D'après la formule (5) (ou plus correctement, par son analogue relatif à l'extension considérée ici), la différente de l'extension $L_{\mathrm{nr}}(E_5)/L_{\mathrm{nr}}(\mu_5)$ est (π^{16}). Puisque $L_{\mathrm{nr}}(\mu_5)/\mathbb{Q}_{5,\mathrm{nr}}(\mu_5)$ est une extension modérément ramifiée de degré 3, sa différente est (π'^2), où π' est une uniformisante de $L_{\mathrm{nr}}(\mu_5)$ et engendre l'idéal (π^{10}) de $L_{\mathrm{nr}}(E_5)$. Par suite, la différente de l'extension $L_{\mathrm{nr}}(E_5)/\mathbb{Q}_{5,\mathrm{nr}}(\mu_5)$ est (π^{26}). Comme $L_{\mathrm{nr}}(E_5)/\mathbb{Q}_{5,\mathrm{nr}}(E_5)$ est une extension modérément ramifiée de degré 3, sa différente est (π^2) et la différente D de l'extension $\mathbb{Q}_{5,\mathrm{nr}}(E_5)/\mathbb{Q}_{5,\mathrm{nr}}(\mu_5)$ engendre l'idéal (π^{24}) de $L_{\mathrm{nr}}(E_5)$. Si w désigne la valuation normalisée de $\mathbb{Q}_{5,\mathrm{nr}}(E_5)$ et δ l'entier $w(D)$, on a $\delta = 24/3 = 8$. D'après la prop. 5, $\mathbb{Q}_{5,\mathrm{nr}}(E_5)$ est peu ramifiée, et cela implique que l'on a $k = 14$ (cf. [8], (2.4.8)). La valeur de k calculée pour $p \neq 5$, à savoir $k = (p^2+3p+2)/3$, est donc valable si $p = 5$.

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

(a) $(v(\Delta), v(c_4), v(c_6)) = (8, 3, 4)$ (et donc $p \equiv 2 \bmod 3$, d'après le lemme 1);

(b) $(v(\Delta), v(c_4), v(c_6)) = (9, 3, 5)$ (et donc $p \equiv 3 \bmod 4$, d'après le lemme 1);

(c) $(v(\Delta), v(c_4), v(c_6)) = (10, 4, 5)$ (et donc $p \equiv 2 \bmod 3$, d'après le lemme 1).

La représentation de I dans E_p s'écrit matriciellement

$$\begin{pmatrix} \chi^{2-\alpha} & * \\ 0 & \chi^{\alpha-1} \end{pmatrix}$$

avec $\alpha = (p+1)v(\Delta)/12$ (lemme 2 et prop. 2(a)). Le groupe I_p n'opère pas trivialement sur E_p (prop. 4). Posons $\beta = p-(\alpha-1)$; on a $\chi^\beta = \chi^{2-\alpha}$. Les valeurs de $\alpha-1$ et β sont calculées ci-dessous :

$v(\Delta)$	8	9	10
α	$(2p-1)/3$	$(3p-1)/4$	$(5p-1)/6$
β	$(p+1)/3$	$(p+1)/4$	$(p+1)/6$

Considérons les cas (a) et (b). Les entiers $\alpha-1$ et β vérifient les inégalités $1 \leq \beta < \alpha - 1 \leq p-2$; d'où $k = 1+p\beta+\alpha-1$ (cf. [8], (2.4.5)), ce qui donne les valeurs de k annoncées.

Supposons que l'on soit dans le cas (c), i.e. que l'on ait $(v(\Delta), v(c_4), v(c_6)) = (10,4,5)$ et $p \equiv 2 \bmod 3$. On a $1 \leq \beta < \alpha - 1 \leq p-2$, sauf pour $p=5$.

Si $p \neq 5$, on a $k = 1+p\beta+\alpha-1$, i.e. $k = (p^2+6p+5)/6$ (*loc. cit.*).

Si p est égal à 5, l'image de I dans $\mathrm{Aut}(E_5)$ est représentable matriciellement sous la forme

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

et pour déterminer k, on est amené à étudier la ramification sauvage de $\mathbb{Q}_{5,\mathrm{nr}}(E_5)$. Soit E' la courbe elliptique déduite de E par torsion quadratique par $\sqrt{5}$; l'extension engendrée par les points de 5-torsion de E' est égale à $\mathbb{Q}_{5,\mathrm{nr}}(E_5)$ (la démonstration est la même que celle du n° 3). On a les égalités $v(\Delta(E')) = 4$, $v(c_4(E')) = 2$ et $v(c_6(E')) = 2$. Il résulte alors de l'étude du cas 1)(c) du n° 4.2 que $\mathbb{Q}_{5,\mathrm{nr}}(E_5)$ est peu ramifiée, d'où $k=2$ (*loc. cit.*, (2.4.8)).

3) Supposons que $(v(\Delta), v(c_4), v(c_6))$ ne soit pas l'un des triplets $(2,1,1)$, $(3,1,2)$, $(4,2,2)$, $(8,3,4)$, $(9,3,5)$, $(10,4,5)$. La représentation de I dans $E_p \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ que l'on déduit par extension des scalaires de celle de I dans E_p s'écrit matriciellement

$$\begin{pmatrix} \psi^\alpha \psi'^{p-\alpha} & 0 \\ 0 & \psi'^\alpha \psi^{p-\alpha} \end{pmatrix}$$

où ψ et ψ' sont les caractères fondamentaux de niveau 2 et où α est égal à $(p+1)v(\Delta)/12$ (lemme 2 et prop. 2(b)). Dans cette situation on est dans l'un des cas suivants :

- $v(\Delta) \in \{2,4,8,10\}$ et $p \equiv 2 \bmod 3$;
- $v(\Delta) \in \{4,9\}$ et $p \equiv 3 \bmod 4$;
- $v(\Delta) = 6$.

Les valeurs de α et $p-\alpha$ sont indiquées ci-dessous :

$v(\Delta)$	2	3	4	6	8	9	10
α	$(p+1)/6$	$(p+1)/4$	$(p+1)/3$	$(p-1)/2$	$2(p+1)/3$	$3(p+1)/4$	$5(p+1)/6$
β	$(5p-1)/6$	$(3p-1)/4$	$(2p-1)/3$	$(p+1)/2$	$(p-2)/3$	$(p-3)/4$	$(p-5)/6$

Si $v(\Delta) \in \{2,3,4,6\}$, les entiers α et $p-\alpha$ satisfont aux inégalités $1 \leq \alpha < p-\alpha \leq p-1$. D'après la définition de (2.2.4) de [8], on a $k = 1 + p\alpha + p - \alpha$ et l'on obtient les valeurs de k annoncées.

Si $v(\Delta) \in \{8,9\}$, on a les inégalités $1 \leq p-\alpha < \alpha \leq p-1$; d'où $k = 1 + p(p-\alpha) + \alpha$ (cf. [8], (2.2.4)) et l'on obtient encore les valeurs de k annoncées.

Si enfin $v(\Delta) = 10$, on a les inégalités $1 \leq p-\alpha < \alpha \leq p-1$ sauf si p est égal à 5. Si $p \neq 5$, on trouve $k = (p^2+11)/6$ (*loc.cit.*). Si $p = 5$, la représentation de I dans $E_5 \otimes_{\mathbb{F}_5} \overline{\mathbb{F}}_5$ s'écrit matriciellement

$$\begin{pmatrix} \psi & 0 \\ 0 & \psi' \end{pmatrix};$$

d'où $k = 2$ (*loc. cit.*). Cela termine la démonstration de l'assertion (b) du théorème 1.

B.2. *Le cas* $p = 3$, $v(j) \geq 0$

1. *Préliminaires.* Les invariants Δ et c_6 étant relatifs à un modèle minimal de E, le couple $(v(\Delta), v(c_6))$ ne peut être égal à $(12,6)$ ni être de la forme (m,n) avec $m \geq 12$ et $n \geq 9$ ([3], th. 1 et 3(1)). L'égalité $c_4^3 - c_6^2 = 1728\Delta$, les inégalités $2v(c_6) \geq v(\Delta) > 0$ et le corollaire du th. 1 de [3] impliquent alors que $(v(\Delta), v(c_6))$ est l'un des couples intervenant dans le tableau ci-dessous :

$v(\Delta)$	3		4	5		6		7	9	10	11		12	13
$v(c_6)$	3	≥ 4	3	3	4	3	≥ 5	5	≥ 6	6	6	7	8	8

L'équation

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

est une équation minimale de E sur $\mathbb{Q}_3$ (cf. [13], 1).

Puisque l'on a $v(j) \geq 0$, il y a potentiellement bonne réduction, autrement dit, il existe une extension finie de $\mathbb{Q}_3$ sur laquelle E acquiert bonne réduction ([11], p. 181, prop. 5.5). La lettre L désignera une telle extension. On note E_L la courbe déduite de E par extension des scalaires à L; E_L a bonne réduction sur L.

Rappelons pour mémoire le résultat suivant :

Lemme 5. *Soit K une extension finie de $\mathbb{Q}_3$; la courbe elliptique E a bonne réduction sur K si et seulement si il existe $u \in K$ avec $v(u) = v(\Delta)/12$ tel que c_4/u^4 et c_6/u^6 soient les invariants $c_4(W_K)$ et $c_6(W_K)$ d'une équation de Weierstrass*

$$(W_K) \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

définie sur K à coefficients entiers.

Démonstration. Si la condition de l'énoncé est satisfaite, le discriminant de (W_K), égal à Δ/u^{12}, est une unité et (W_K) est l'équation d'une courbe elliptique isomorphe à E sur K, donc E a bonne réduction sur K. La réciproque est immédiate.

Lemme 6. *Il existe des éléments entiers u et z de L avec $v(u) = v(\Delta)/12$ tels que la cubique (W_L) d'équation*

$$(W_L) \qquad Y^2 = X^3 + \frac{z}{4u^2}X^2 + \frac{z^2 - c_4}{48u^4}X + \frac{z^3 - 3zc_4 - 2c_6}{1728u^6}$$

soit une équation minimale de E_L sur L. L'élément z est tel que l'on ait $v(z) = v(c_6)/3$ si $v(\Delta) \leq 2v(c_6) < 6 + v(\Delta)$ et peut être choisi égal à 0 si $2v(c_6) \geq 6 + v(\Delta)$.

Démonstration. La courbe E a bonne réduction sur L. Considérons un élément u satisfaisant à l'énoncé du lemme 5. Il existe alors un élément Z de L de valuation ≥ 0, tel que l'on ait

$$\begin{cases} Z^3 - 3Zc_4/u^4 - 2c_6/u^6 \equiv 0 \bmod 27, \\ c_4/u^4 \equiv Z^2 \bmod 3 \end{cases} \qquad \text{(cf. [3], dém. du th. 1).}$$

Les éléments u et $z = Zu^2$ satisfont à l'énoncé du lemme. En effet, le système précédent s'écrit

$$\begin{cases} z^3 - 3zc_4 - 2c_6 \equiv 0 \bmod 27u^6, \\ c_4 - z^2 \equiv 0 \bmod 3u^4. \end{cases}$$

Par suite, la cubique (W_L) est à coefficients entiers; les invariants standards associés à (W_L) sont $c_4(W_L) = c_4/u^4$, $c_6(W_L) = c_6/u^6$ et $\Delta(W_L) = \Delta/u^{12}$; son discriminant est donc de valuation 0. Cela montre que (W_L) est une équation minimale de E_L sur L.

Si $2v(c_6) = v(\Delta)$, on a $v(c_6) = 3$ et $v(c_4) = 2$, comme on peut le constater dans le tableau préliminaire, et cela entraîne $v(z) = 1$. Si $v(\Delta) < 2v(c_6) < 6 + v(\Delta)$, on a $0 < v(c_6(W_L)) < 3$ et la remarque qui suit le th. 1 de [3] entraîne l'égalité $3v(z) = v(c_6)$. Si enfin on a $2v(c_6) \geq 6+v(\Delta)$, l'égalité $c_4^3 - c_6^2 = 1728\Delta$ montre que l'on a $3v(c_4) \geq 3+v(\Delta)$ et l'élément u défini ci-dessus, avec $z = 0$, satisfait à l'énoncé du lemme; cela termine la démonstration.

Remarque. Les formules de transformation entre les modèles (W) et (W_L) sont de la forme

$$(6) \qquad \begin{cases} x = u^2X + z/12, \\ y = u^3Y \end{cases} \qquad \text{(cf. [13], 1, 2).}$$

Soit h la hauteur de réduction de E_L sur L.

Lemme 7. *On a $h = 1$ si et seulement si $2v(c_6) = v(\Delta)$.*

Démonstration. Une courbe elliptique définie sur un corps de caractéristique 3 est supersingulière si et seulement si son invariant modulaire est nul. Pour que l'on ait $h = 2$, il faut et il suffit que l'invariant modulaire $j(\widetilde{E_L})$ de la courbe elliptique $\widetilde{E_L}$ déduite de E_L par réduction modulo l'idéal de valuation de L soit nul, c'est-à-dire que la valuation de $j(E_L) = j(E)$ soit > 0, ou encore que celle de $j(E) - 1728 = c_6^2\Delta$ soit > 0. Comme on a par hypothèse $2v(c_6) \geq v(\Delta)$, le lemme en résulte.

2. *Description de l'action de I sur E_3.* Soient X, Y (resp. x, y) les fonctions coordonnées de Weierstrass de E_L dans le modèle (W_L) (resp. dans le modèle (W)). Les

fonctions $T = -X/Y$ et $t = -x/y$ sont des uniformisantes locales au voisinage du point à l'infini O. On conserve avec $p = 3$ les notations de la partie B.1, 2. En particulier, on désigne par :

• [3] la série entière $\sum_{n=1}^{\infty} \tau_n T^n$ donnant la multiplication par 3 dans le groupe formel associé à E_L;

• N_3 le groupe des points de 3-torsion du groupe formel associé à E_L;

• E_3 le groupe des points de 3-torsion de $E(\overline{\mathbb{Q}}_3) = E_L(\overline{\mathbb{Q}}_3)$;

• $\widetilde{E_L}$ la courbe elliptique déduite de E_L par réduction modulo l'idéal de la valuation de L;

• $\widetilde{E_{L,3}}$ le groupe des points de 3-torsion de $\widetilde{E_L}(\overline{\mathbb{F}}_3)$.

Lemme 8. *Supposons $v(\Delta) \leq 2v(c_6) \leq 4 + v(\Delta)$. Il existe un sous-groupe H de E_3 d'ordre 3, stable sous l'action de G_3, tel que si P est un point non nul de H, on ait $v(y(P)) = (v(c_6) - 3)/2$.*

Démonstration. 1) Supposons $2v(c_6) = v(\Delta)$. D'après le tableau préliminaire, $v(\Delta)$ est égal à 6. On a $h = 1$ (lemme 7) et le groupe $\widetilde{E_{L,3}}$ est d'ordre 3. L'application de réduction $E_3 \to \widetilde{E_{L,3}}$ est un homomorphisme surjectif de groupes. Son noyau C_3 est d'ordre 3. Si P est un point non nul de E_3, on a $P \in C_3$ si et seulement si $v(Y(P)) < 0$, c'est-à-dire si et seulement si $v(y(P)) < 3/2$ (formule (6)). Le sous-groupe C_3 de E_3 est donc stable par G_3.

L'application $P \mapsto T(P)$ (où $T(P) = -X(P)/Y(P)$ si $P \neq 0$ et où $T(O) = 0$) est un isomorphisme du groupe C_3 sur le groupe N_3. Soit P un point de C_3 non nul; l'étude du polygone de Newton de la série formelle [3] montre que $v(T(P))$ est égal à $1/2$ ([6], 1.10). On a $v(Y(P)) = -3v(T(P)) = -3/2$. L'égalité $y(P) = u^3 Y(P)$ où $v(u) = 1/2$ (car $v(\Delta) = 6$) implique alors $v(y(P)) = 0$; comme on a $v(c_6) = 3$, le groupe C_3 vérifie l'assertion du lemme.

2) Supposons maintenant $v(\Delta) < 2v(c_6) \leq 4 + v(\Delta)$. On a $h = 2$ (lemme 7). Le groupe $\widetilde{E_{L,3}}$ est trivial et l'application $P \mapsto T(P)$ est un isomorphisme du groupe E_3 sur le groupe N_3. Par ailleurs, τ_3 est égal à $-2z/u^2$ (cf. [11], p. 121, 4.5) et sa valuation est $v(\tau_3) = v(z) - 2v(u) = (2v(c_6) - v(\Delta))/6$ d'après le lemme 6. De l'inégalité $2v(c_6) \leq 4 + v(\Delta)$ on déduit $v(\tau_3) \leq 2/3$. L'étude du polygone de Newton de la série formelle [3] montre que les éléments non nuls de N_3 ont pour valuation $\alpha_1 = (1 - v(\tau_3))/2$ ou $\alpha_2 = v(\tau_3)/6$ (cf. [6], 1.10). On a $\alpha_1 > \alpha_2$ et l'ensemble H des éléments P de E_3 pour lesquels $v(T(P)) \geq \alpha_1$ est un sous-groupe d'ordre 3 de E_3. Soit P un point non nul de E_3; puisque l'on a $v(Y(P)) = -3v(T(P))$ et $y(P) = u^3 Y(P)$ où $v(u) = v(\Delta)/12$, le point P appartient à H si et seulement si $v(y(P))$ est égal à $(v(c_6) - 3)/2$; en particulier, le sous-groupe H de E_3 est stable sous l'action de G_3 et il satisfait à l'énoncé du lemme.

Proposition 6. *Supposons $v(\Delta) \leq 2v(c_6) \leq 4 + v(\Delta)$. Dans une base convenable de E_3 sur $\mathbb{F}_3$, la représentation de I dans E_3 s'écrit matriciellement $\left(\begin{smallmatrix} 1 & * \\ 0 & \chi \end{smallmatrix}\right)$ si $v(c_6)$ est impair, et $\left(\begin{smallmatrix} \chi & * \\ 0 & 1 \end{smallmatrix}\right)$ si $v(c_6)$ est pair.*

Démonstration. Considérons un sous-groupe H de E_3 satisfaisant à l'énoncé du lemme 8. Puisque le déterminant de la représentation de I dans E_3 est égal au caractère

χ, il suffit de démontrer que I agit trivialement sur H si $v(c_6)$ est impair et que I agit sur H suivant χ si $v(c_6)$ est pair.

Soit P un point non nul de H. Posons $\alpha = (v(c_6) - 3)/2$. On a $v(y(P)) = \alpha$ (lemme 8). Le groupe H étant d'ordre 3, on a ${}^{\sigma}P = \varepsilon(\sigma)P$ pour tout $\sigma \in I$ avec $\varepsilon(\sigma) \in \{-1, 1\}$ et $\sigma(y(P))/y(P)$ est donc égal à $\varepsilon(\sigma)$. Par définition du caractère χ_α, $\chi_\alpha(\sigma)$ est l'image de $\varepsilon(\sigma)$ dans $\overline{\mathbb{F}}_3$. Par suite, I opère sur H par la formule

$$ {}^{\sigma}P = \chi_\alpha(\sigma)P \quad (\sigma \in I,\ P \in H).$$

Si $v(c_6)$ est impair, α appartient à $\mathbb{Z}$ et χ_α est égal au caractère trivial. Si $v(c_6)$ est pair, α appartient à $(1/2) + \mathbb{Z}$ et χ_α est égal au caractère cyclotomique χ.

Rappelons que ψ et ψ' désignent les caractères fondamentaux de niveau 2; on a $\psi = \chi_{1/8}$ et $\psi' = \chi_{3/8}$.

Proposition 7. *Supposons $2v(c_6) > 4 + v(\Delta)$. La représentation de I dans E_3 est irréductible. La représentation de I dans $E_3 \otimes_{\mathbb{F}_3} \overline{\mathbb{F}}_3$ qu'on en déduit par extension des scalaires est diagonalisable et représentable matriciellement dans une base convenable par $\left(\begin{smallmatrix} \psi & 0 \\ 0 & \psi' \end{smallmatrix}\right)$ si $v(\Delta) \equiv 1 \bmod 4$, et par $\left(\begin{smallmatrix} \psi^2\psi' & 0 \\ 0 & \psi'^2\psi \end{smallmatrix}\right)$ si $v(\Delta) \not\equiv 1 \bmod 4$.*

Démonstration. On a $h = 2$ (lemme 7). L'application $P \mapsto T(P)$ est un isomorphisme du groupe E_3 sur le groupe N_3. Puisque l'on a $v(\tau_3) = (v(c_6) - (v(\Delta))/2)/3$, l'inégalité $2v(c_6) > 4 + v(\Delta)$ implique que l'on a $2v(c_6) \geq 5 + v(\Delta)$, d'où $v(\tau_3) \geq 5/6 > 3/4$. L'étude du polygone de Newton de la série formelle [3] montre que les éléments non nuls de N_3 ont pour valuation $1/8$ (cf. [6], 1.10).

Soit P un point non nul de E_3; on a $v(T(P)) = 1/8$. D'après les formules de transformation (6), on a

$$ t(P) = \frac{T(P)}{u} - \frac{z}{12u^3Y(P)}, \tag{7}$$

où u est de valuation $v(\Delta)/12$ et où $v(z) \geq 0$.

1) Supposons $v(c_6) < 6 + v(\Delta)$. Par hypothèse cela entraîne $2v(c_6) = 5 + v(\Delta)$, c'est-à-dire $(v(\Delta), v(c_6)) \in \{(3, 4), (9, 7)\}$ (cf. le tableau préliminaire). Des égalités $3v(z) = v(c_6)$ (lemme 6) et $3v(T(P)) = -v(Y(P))$, on déduit les égalités

$$ v\left(\frac{T(P)}{u}\right) - v\left(\frac{z}{12u^3Y(P)}\right) = \frac{v(\Delta) - 2v(c_6) + (9/2)}{6} = -\frac{1}{12}.$$

Par suite, on a

$$ v\left(\frac{T(P)}{u}\right) < v\left(\frac{z}{12u^3Y(P)}\right) \tag{8}$$

et $v(t(P)) = \mu$ avec

$$ \mu = \frac{v(T(P))}{u} = \frac{1}{8} - \frac{v(\Delta)}{12}.$$

Considérons l'application $f : E_3 \to m_\mu/m_\mu^+$ définie par $f(P) = t(P) \bmod m_\mu^+$. Démontrons que f est un homomorphisme injectif de groupes compatible à l'action de G_3. Soient P, P' deux points de E_3. On a $v(T(P + P') - T(P) - T(P')) > 1/8$ (cf. [12],

formule (16)),

$$v\left(\frac{T(P+P')}{u}-\frac{T(P)}{u}-\frac{T(P')}{u}\right)>\frac{1}{8}-\frac{v(\Delta)}{12}=\mu.$$

L'inégalité (8) et la formule (7) entraînent alors $v(t(P+P')-t(P)-t(P'))>\mu$; cela prouve que f est un homomorphisme; f est injectif car $v(t(P))$ est égal à μ pour tout P non nul de E_3 et il commute à l'action de G_3 puisque l'on a $t({}^\sigma P)={}^\sigma t(P)$ pour $\sigma\in G_3$ et $P\in E_3$. L'action du groupe I sur $f(E_3)$ est donc donnée par la formule

$$f({}^\sigma P)=\chi_\mu(\sigma)f(P)\quad(P\in E_3,\ \sigma\in I).$$

Si $v(\Delta)=3$, on a $\mu=-1/8\equiv 7/8 \bmod \mathbb{Z}$, d'où $\chi_\mu=\psi\psi'^2$. Si $v(\Delta)=9$, on a $\mu=-5/8\equiv 3/8 \bmod \mathbb{Z}$, d'où $\chi_\mu=\psi'$. Dans chacun des deux cas, $\chi_\mu(I)$ est égal à $\mathbb{F}_9^*$; ainsi $f(E_3)$ est stable par multiplication par les éléments de $\mathbb{F}_9$ et est un sous-$\mathbb{F}_9$-espace vectoriel de m_μ/m_μ^+ (où $\mathbb{F}_9$ est l'extension quadratique de $\mathbb{F}_3$ contenue dans $\overline{\mathbb{F}}_3$). Puisque f est injectif, on en déduit une unique structure de $\mathbb{F}_9$-espace vectoriel sur E_3 pour laquelle f est $\mathbb{F}_9$-linéaire. Le groupe I opère donc sur E_3 par la formule

$${}^\sigma P=\chi_\mu(\sigma)P\quad(P\in E_3,\ \sigma\in I).$$

En particulier, la représentation de I dans E_3 est irréductible, et après extension des scalaires à $\overline{\mathbb{F}}_3$, l'action de I dans $E_3\otimes_{\mathbb{F}_3}\overline{\mathbb{F}}_3$ est représentable matriciellement dans une base convenable par

$$\begin{pmatrix}\chi_\mu & 0\\ 0 & \chi_{3\mu}\end{pmatrix}$$

(cf. [6], 1.9, dém. du cor. 3).

2) Supposons $2v(c_6)\geq 6+v(\Delta)$. On peut prendre $z=0$ (lemme 6) et alors $v(t(P))$ est égal à μ, avec $\mu=1/8-(v(\Delta)/12)$. L'application $f: E_3\to m_\mu/m_\mu^+$ définie par $f(P)=t(P) \bmod m_\mu^+$ est un homomorphisme de groupes injectif compatible avec l'action de G_3 (cf. dém. de la prop. 1). Si $\sigma\in I$ et $P\in E_3$, on a donc $f({}^\sigma P)=\chi_\mu(\sigma)f(P)$. On a

$$\mu=\frac{1}{8}+\frac{v(\Delta)}{4}-\frac{v(\Delta)}{3}\equiv\frac{1}{8}+\frac{v(\Delta)}{4} \bmod \mathbb{Z}\left[\frac{1}{3}\right],$$

donc le caractère χ_μ est égal à $\psi^{1+2v(\Delta)}$ et l'on a

$$\chi_\mu=\begin{cases}\psi' & \text{si } v(\Delta)\equiv 1 \bmod 4,\\ \psi^2\psi' & \text{si } v(\Delta)\equiv 2 \bmod 4,\\ \psi'^2\psi & \text{si } v(\Delta)\equiv 3 \bmod 4\end{cases}$$

(sous l'hypothèse $2v(c_6)\geq 6+v(\Delta)$, 4 ne divise pas $v(\Delta)$ comme on peut le constater dans le tableau préliminaire). On a ainsi $\chi_\mu(I)=\mathbb{F}_9^*$ et par une démonstration analogue à celle du cas 1) ci-dessus, on en déduit que la représentation de I dans E_3 est irréductible, et que la représentation de I dans $E_3\otimes_{\mathbb{F}_3}\overline{\mathbb{F}}_3$ est diagonalisable et donnée par les caractères χ_μ et $\chi_{3\mu}$. Cela démontre la proposition.

3. *Démonstration de l'assertion* (b) *du théorème* 2. On note ϱ la représentation de I dans E_3.

Lemme 9. *Δ est un cube dans $\mathbb{Q}_{3,\mathrm{nr}}$ si et seulement si on a $v(\Delta)\equiv 0 \bmod 3$ et $\Delta'\equiv\pm 1 \bmod 9$.*

Démonstration. Toute unité de $\mathbb{Q}_{3,\mathrm{nr}}$ congrue à $\pm 1 \bmod 9$ est un cube dans $\mathbb{Q}_{3,\mathrm{nr}}$ (cf. [7], p. 219, prop. 9). Donc la condition est suffisante. Montrons qu'elle est nécessaire. Supposons que Δ soit un cube de $\mathbb{Q}_{3,\mathrm{nr}}$. On a alors $v(\Delta) \equiv 0 \bmod 3$ et Δ' est le cube d'un élément x de $\mathbb{Q}_{3,\mathrm{nr}}$. Puisque l'on a $\Delta' \equiv \pm 1 \bmod 3$, on a $x \equiv \pm 1 \bmod 3$, d'où $x^3 \equiv \pm 1 \bmod 9$. Cela prouve le lemme.

Proposition 8. *Si la représentation ϱ s'écrit matriciellement $\left(\begin{smallmatrix} 1 & * \\ 0 & \chi \end{smallmatrix}\right)$, on a*

$$k = \begin{cases} 8 & \text{si } v(\Delta) \not\equiv 0 \bmod 3, \\ 6 & \text{si } v(\Delta) \equiv 0 \bmod 3 \text{ et } \Delta' \not\equiv \pm 1 \bmod 9, \\ 2 & \text{si } v(\Delta) \equiv 0 \bmod 3 \text{ et } \Delta' \equiv \pm 1 \bmod 9. \end{cases}$$

Démonstration. L'ordre de $\varrho(I)$ est égal à 2 ou 6. On a $\mathbb{Q}_{3,\mathrm{nr}}(E_3) = \mathbb{Q}_{3,\mathrm{nr}}(\mu_3, \Delta^{1/3})$ (cf. [6], 5.3.b)).

Supposons que Δ ne soit pas un cube dans $\mathbb{Q}_{3,\mathrm{nr}}$. On a $|\varrho(I)| = 6$ et I_3 n'opère pas trivialement sur E_3. On est dans l'un des deux cas suivants :

(a) $v(\Delta) \not\equiv 0 \bmod 3$;
(b) $v(\Delta) \equiv 0 \bmod 3$ et $\Delta' \not\equiv \pm 1 \bmod 9$.

Dans le cas (a), $\mathbb{Q}_{3,\mathrm{nr}}(E_3)$ est très ramifiée et, par définition, on a $k = 8$ (cf. [8], (2.4.9)). Dans le cas (b), $\mathbb{Q}_{3,\mathrm{nr}}(E_3)$ est peu ramifiée et l'on a $k = 6$ (*loc. cit.*, (2.4.8)).

Lorsque Δ est un cube dans $\mathbb{Q}_{3,\mathrm{nr}}$, i.e. lorsque l'on a $v(\Delta) \equiv 0 \bmod 3$ et $\Delta' \equiv \pm 1 \bmod 9$, l'action de I_3 sur E_3 est triviale, et l'on a $k = 2$ (*loc. cit.*, (2.9.2)). Cela prouve la proposition.

Proposition 9. *Si la représentation de I dans E_3 s'écrit matriciellement $\left(\begin{smallmatrix} \chi & * \\ 0 & 1 \end{smallmatrix}\right)$, on a*

$$k = \begin{cases} 4 & \text{si } v(\Delta) \not\equiv 0 \bmod 3, \\ 2 & \text{si } v(\Delta) \equiv 0 \bmod 3. \end{cases}$$

Démonstration. Elle est identique à celle de la prop. 8. Si on a $v(\Delta) \not\equiv 0 \bmod 3$, l'égalité $\mathbb{Q}_{3,\mathrm{nr}}(E_3) = \mathbb{Q}_{3,\mathrm{nr}}(\mu_3, \Delta^{1/3})$ montre que $\mathbb{Q}_{3,\mathrm{nr}}(E_3)$ est très ramifiée, d'où $k = 4$ (cf. [8], (2.4.9)). Si on a $v(\Delta) \equiv 0 \bmod 3$, $\mathbb{Q}_{3,\mathrm{nr}}(E_3)$ est modérément ramifiée ou peu ramifiée, auquel cas on a $k = 2$ (*loc. cit.*, (2.4.8)). Cela prouve la proposition.

Considérons alors un couple $(v(\Delta), v(c_6)) \neq (6, 5)$ intervenant dans le tableau préliminaire. Si on a $v(\Delta) \leq 2v(c_6) \leq 4 + v(\Delta)$, la valeur de k indiquée dans le théorème s'obtient en appliquant les prop. 6, 8 et 9. Si $2v(c_6) > 4 + v(\Delta)$, la valeur de k s'obtient en appliquant la prop. 7 et la définition (2.2.4) de [8]. Supposons $(v(\Delta), v(c_6)) = (6, 5)$. L'égalité $c_4^3 - c_6^2 = 1728\Delta$ implique $\Delta' \equiv c_4'^3 - 3c_6'^2 \equiv \pm 1 - 3 \bmod 9$; d'après les prop. 6 et 8, on a $k = 6$. Cela termine la démonstration de l'assertion (b) du théorème 2.

B.3. *Le cas $p \geq 3$, $v(j) < 0$*

1. *Description de l'action de I sur E_p.* On suppose $v(j) < 0$. Il existe une unique extension quadratique ramifiée L de $\mathbb{Q}_p$ sur laquelle E devient isomorphe à la courbe de Tate $G_m/q^{\mathbb{Z}}$, où q est l'élément de $\mathbb{Q}_p^*$ déterminé par l'égalité $j(E) = (1/q) + 744 + 196884q + \ldots$ ([11], p. 355, 14). On a $v(q) = -v(j(E))$. Notons $\mathrm{Tate}(q)$ la courbe $G_m/q^{\mathbb{Z}}$. Le G_p-module $\mathrm{Tate}(q)(\overline{\mathbb{Q}}_p)$ est canoniquement isomorphe à $\overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$ (*loc. cit.*).

LEMME 10. *Il existe un isomorphisme de groupes θ de $E(\overline{\mathbb{Q}}_p)$ sur $\overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$ tel que pour tout $\sigma \in G_p$ on ait*

$$\theta({}^\sigma P) = \begin{cases} {}^\sigma(\theta(P)) & \text{si la restriction de } \sigma \text{ à } L \text{ est l'identité,} \\ ({}^\sigma\theta(P))^{-1} & \text{si la restriction de } \sigma \text{ à } L \\ & \text{est l'élément non trivial de } \mathrm{Gal}(L/\mathbb{Q}_p). \end{cases}$$

Démonstration. Les courbes E et $\mathrm{Tate}(q)$ sont définies sur $\mathbb{Q}_p$, non isomorphes sur $\mathbb{Q}_p$ et isomorphes sur l'extension quadratique L de $\mathbb{Q}_p$; elles se déduisent donc l'une de l'autre par torsion quadratique par l'extension $L/\mathbb{Q}_p$. Soit $d \in \mathbb{Q}_p^*$ tel que $L = \mathbb{Q}_p(\sqrt{d})$. Soit F un polynôme séparable de degré 3 à coefficients dans $\mathbb{Q}_p$ tel que

$$y^2 = F(x) \tag{W}$$

soit une équation de E sur $\mathbb{Q}_p$; alors $dy^2 = F(x)$ est une équation de $\mathrm{Tate}(q)$ sur $\mathbb{Q}_p$. Soient x, y les fonctions coordonnées de Weierstrass de E dans le modèle (W). L'application $f : E(\overline{\mathbb{Q}}_p) \to \mathrm{Tate}(q)(\overline{\mathbb{Q}}_p)$ donnée dans les modèles de E et $\mathrm{Tate}(q)$ définie par les équations ci-dessus par $f(P) = \big(x(P), y(P)/\sqrt{d}\big)$ est un isomorphisme de groupes. Pour $P \in E(\overline{\mathbb{Q}}_p)$ et $\sigma \in G_p$, on a $f({}^\sigma P) = \big(\sigma(\sqrt{d})/\sqrt{d}\big){}^\sigma f(P)$. L'homomorphisme θ, obtenu en composant l'isomorphisme canonique de $\mathrm{Tate}(q)(\overline{\mathbb{Q}}_p)$ sur $\overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$ avec f, satisfait alors à l'énoncé du lemme.

PROPOSITION 10. *Supposons $p \geq 3$ et $v(j) < 0$; dans une base convenable de E_p sur $\mathbb{F}_p$, la représentation de I dans E_p s'écrit matriciellement*

$$\begin{pmatrix} \chi^{p-\alpha} & * \\ 0 & \chi^\alpha \end{pmatrix}$$

avec $\alpha = (p-1)/2$.

Démonstration. Soit θ un isomorphisme de groupes de $E(\overline{\mathbb{Q}}_p)$ sur $\overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$, comme indiqué dans le lemme 10. Par définition, $\theta(E_p)$ est le noyau de la multiplication par p dans $\overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$. L'image réciproque de $\mu_p q^{\mathbb{Z}}/q^{\mathbb{Z}}$ par θ est un sous-groupe C_p d'ordre p de E_p. Parce que l'on a $p \geq 3$, $\mathbb{Q}_{p,\mathrm{nr}}(\sqrt{p})$ est l'unique extension quadratique de $\mathbb{Q}_{p,\mathrm{nr}}$; c'est donc le composé de L et $\mathbb{Q}_{p,\mathrm{nr}}$. Le groupe I agit par le caractère cyclotomique χ sur le groupe $\mu_p q^{\mathbb{Z}}/q^{\mathbb{Z}}$, et il résulte du lemme 10 que l'on a, pour $P \in C_p$ et $\sigma \in I$,

$$\theta({}^\sigma P) = \begin{cases} \theta(P)^{\chi(\sigma)} & \text{si } \sigma(\sqrt{p}) = \sqrt{p}, \\ \theta(P)^{-\chi(\sigma)} & \text{si } \sigma(\sqrt{p}) = -\sqrt{p}. \end{cases}$$

L'application θ restreinte à E_p étant $\mathbb{F}_p$-linéaire injective, on en déduit que l'on a ${}^\sigma P = \chi(\sigma)P$ si $\sigma(\sqrt{p}) = \sqrt{p}$ et ${}^\sigma P = -\chi(\sigma)P$ si $\sigma(\sqrt{p}) = -\sqrt{p}$. En particulier, C_p est stable sous l'action de I. On a en fait $\sigma(\sqrt{p}) = \chi(\sigma)^{(p-1)/2}\sqrt{p}$, donc I agit sur C_p suivant le caractère $\chi^{(p+1)/2} = \chi^{p-\alpha}$; le déterminant de la représentation de I dans E_p étant le caractère $\chi = \chi^p$, I opère sur E_p/C_p par le caractère χ^α; cela démontre la proposition.

2. *Démonstration des assertions* (a) *des théorèmes* 1 *et* 2

LEMME 11. *Supposons $p \geq 3$ et $v(j) < 0$; on a $\mathbb{Q}_{p,\mathrm{nr}}(E_p) = \mathbb{Q}_{p,\mathrm{nr}}(\mu_p, q^{1/p})$.*

Démonstration. Puisque $p \geq 3$, on voit que $\mathbb{Q}_{p,\mathrm{nr}}(\sqrt{p})$, qui est l'unique extension quadratique de $\mathbb{Q}_{p,\mathrm{nr}}$, est contenu dans $\mathbb{Q}_{p,\mathrm{nr}}(\mu_p)$, donc dans $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$ et $\mathbb{Q}_{p,\mathrm{nr}}(\mathrm{Tate}(q)_p)$.

Comme E et $\mathrm{Tate}(q)$ sont isomorphes sur $\mathbb{Q}_p(\sqrt{p})$, on a $\mathbb{Q}_{p,\mathrm{nr}}(E_p) = \mathbb{Q}_{p,\mathrm{nr}}(\mathrm{Tate}(q)_p) = \mathbb{Q}_{p,\mathrm{nr}}(\mu_p, q^{1/p})$.

Rappelons que l'on a $v(j) = -v(q)$. Posons $\alpha = (p-1)/2$ et $\beta = p - \alpha$. La représentation de I dans E_p s'écrit matriciellement

$$\begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix}$$

(prop. 10). On a $\beta = \alpha + 1$.

Supposons $p \geq 5$. Si p divise $v(j)$, d'après le lemme 11, l'action de I_p sur E_p est soit triviale, soit peu ramifiée. Les entiers α et β sont compris entre 1 et $p-2$; d'où $k = 1 + p\alpha + \beta = (p^2+3)/2$ (cf. [8], (2.3.2) ou (2.4.8)). Si p ne divise pas $v(j)$, l'extension $\mathbb{Q}_{p,\mathrm{nr}}(E_p)$ est très ramifiée et cela conduit à $k = (p+1)^2/2$ (*loc. cit.*, (2.4.9)). Cela démontre l'assertion (a) du théorème 1.

Si p est égal à 3, la représentation de I dans E_3 s'écrit matriciellement sous la forme

$$\begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}.$$

La valeur de k s'obtient alors en appliquant la prop. 8 (qui est valable si $v(j) < 0$); cela prouve l'assertion (a) du théorème 2.

B.4. *Le cas $p = 2$.* On rappelle que ϱ est la représentation de I dans E_2. D'après [8], n° 2, trois cas sont possibles :

(a) La représentation ϱ est irréductible. Dans ce cas, la représentation déduite de ϱ par extension des scalaires à $\overline{\mathbb{F}}_2$ est représentable matriciellement dans une base convenable par

$$\begin{pmatrix} \psi & 0 \\ 0 & \psi' \end{pmatrix},$$

où ψ et ψ' sont les caractères fondamentaux de niveau 2. On a $|\varrho(I)| = 3$ et $k = 2$ (*loc. cit.*, (2.2.4)).

(b) On a $|\varrho(I)| = 1$. Dans ce cas, on a $k = 2$ (*loc. cit.*, (2.3.2)).

(c) La représentation ϱ est représentable matriciellement dans une base convenable de E_2 sur $\mathbb{F}_2$ par

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

où $\lambda : I \to \mathbb{F}_2$ est un homomorphisme non nul. On a alors $|\varrho(I)| = 2$. On a $k = 2$ si l'extension $\mathbb{Q}_{2,\mathrm{nr}}(E_2)$ de $\mathbb{Q}_{2,\mathrm{nr}}$ est peu ramifiée, et $k = 4$ si elle est très ramifiée.

Si $v(\Delta)$ est impair, Δ n'est pas un carré dans $\mathbb{Q}_{2,\mathrm{nr}}$, donc $\varrho(I)$ est pair ([6], 5.3, a)). On est alors dans le cas (c), et on a $[\mathbb{Q}_{2,\mathrm{nr}}(E_2) : \mathbb{Q}_{2,\mathrm{nr}}] = 2$. Comme $\mathbb{Q}_{2,\mathrm{nr}}(E_2)$ contient le corps $\mathbb{Q}_{2,\mathrm{nr}}\big(\sqrt{\Delta}\big)$, il est égal à ce corps, et est une extension très ramifiée de $\mathbb{Q}_{2,\mathrm{nr}}$. On a donc $k = 4$.

Supposons $v(\Delta)$ pair. Si on est dans le cas (a) ou le cas (b), on a $k = 2$. Si on est dans le cas (c), les mêmes arguments que ceux de l'alinéa précédent permettent de prouver que le corps $\mathbb{Q}_{2,\mathrm{nr}}(E_2)$ est égal à $\mathbb{Q}_{2,\mathrm{nr}}\big(\sqrt{\Delta}\big)$ et est une extension peu ramifiée de $\mathbb{Q}_{2,\mathrm{nr}}$, de sorte que l'on a encore $k = 2$. Cela démontre le théorème 3.

II. Détermination du conducteur

Considérons comme dans l'introduction une courbe elliptique E définie sur $\mathbb{Q}$ et un nombre premier p. Notons $N(E)$ le conducteur de E et E_p le groupe des points de p-torsion de $E(\overline{\mathbb{Q}})$ (où $\overline{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$); E_p est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension 2. Si l est un nombre premier $\neq p$, on note $\mathbb{Q}_{l,\mathrm{nr}}$ l'extension non ramifiée maximale de $\mathbb{Q}_l$ dans une clôture algébrique $\overline{\mathbb{Q}}_l$ et f_l l'exposant de l dans $N(E)$. Rappelon que l'on a

$$f_l = \begin{cases} 0 & \text{si } E \text{ a bonne réduction en } l, \\ 1 & \text{si } E \text{ a une réduction multiplicative en } l, \\ 2+\delta_l & \text{si } E \text{ a une réduction additive en } l, \end{cases}$$

où δ_l est l'invariant sauvage du $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_{l,\mathrm{nr}})$-module E_p (cf. [11], p. 361 et [4]); δ_l est égal à 0 si et seulement si l'extension $\mathbb{Q}_{l,\mathrm{nr}}(E_p)/\mathbb{Q}_{l,\mathrm{nr}}$ est de degré premier à l. Nous nous intéressons à comparer $N(E)$ au conducteur $N(\varrho_p)$ associé par Serre ([8], 1.2) à la représentation $\varrho_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(E_p)$ définie par les points de p-torsion de E.

A. Énoncé du résultat. Soient Δ le discriminant minimal de E et $v_l(\Delta)$ l'exposant de l dans Δ.

Proposition. *Le conducteur $N(\varrho_p)$ divise $N(E)$. Plus précisément, on a*

$$N(\varrho_p) = \prod_{l \neq p} l^{f_l - f_l(p)},$$

où $f_l(p)$ est donné dans la table ci-dessous :

(a) *Si E a bonne réduction en l, alors $f_l(p) = 0$.*

(b) *Si E a mauvaise réduction de type multiplicatif en l, alors*

$$f_l(p) = \begin{cases} 0 & \textit{si } p \textit{ ne divise pas } v_l(\Delta), \\ 1 & \textit{si } p \textit{ divise } v_l(\Delta). \end{cases}$$

(c) *Supposons que E ait mauvaise réduction de type additif en l.*

(i) *Si $p \geq 5$, on a $f_l(p) = 0$.*

(ii) *On a*

$$f_l(3) = \begin{cases} 1 & \textit{si } E \textit{ a en } l \textit{ une réduction de type IV ou } IV^*, \\ 0 & \textit{sinon.} \end{cases}$$

(iii) *On a*

$$f_l(2) = \begin{cases} 2 & \textit{si } E \textit{ a en } l \textit{ une réduction de type } I_\nu^* \textit{ avec } \nu \textit{ entier pair} \geq 0, \\ 1 & \textit{si } E \textit{ a en } l \textit{ une réduction de type III, } III^* \textit{ ou } I_\nu^* \textit{ avec } \nu \textit{ impair}, \\ 0 & \textit{si } E \textit{ a en } l \textit{ une réduction de type II, IV, } IV^*, \textit{ ou } II^*. \end{cases}$$

B. Démonstration. Dans toute la suite, la lettre l désignera un nombre premier différent de p. On note $E(\mathbb{Q}_{l,\mathrm{nr}})$ le groupe des points de E définis sur $\mathbb{Q}_{l,\mathrm{nr}}$ et par $E(\mathbb{Q}_{l,\mathrm{nr}})[p]$ le noyau de la multiplication par p dans $E(\mathbb{Q}_{l,\mathrm{nr}})$. Si $n(l, \varrho_p)$ est l'exposant de $N(\varrho_p)$ en un nombre premier $l \neq p$, on a par définition ([8], (1.2.2) et (1.2.3))

$$n(l, \varrho_p) = 2 + \delta_l - \dim_{\mathbb{Z}/p\mathbb{Z}} E(\mathbb{Q}_{l,\mathrm{nr}})[p]. \tag{1}$$

1. *Préliminaires.* Rappelons d'abord le résultat suivant :

LEMME 1. *Si E a mauvaise réduction de type multiplicatif en l, on a*

$$\dim_{\mathbb{Z}/p\mathbb{Z}} E(\mathbb{Q}_{l,\mathrm{nr}})[p] = \begin{cases} 2 & \textit{si } p \textit{ divise } v_l(\Delta), \\ 1 & \textit{si } p \textit{ ne divise pas } v_l(\Delta), \end{cases}$$

et

$$[\mathbb{Q}_{l,\mathrm{nr}}(E_p) : \mathbb{Q}_{l,\mathrm{nr}}] = \begin{cases} 1 & \textit{si } p \textit{ divise } v_l(\Delta), \\ p & \textit{si } p \textit{ ne divise pas } v_l(\Delta). \end{cases}$$

Démonstration. Soit μ_p le groupe des racines p-ièmes de l'unité de $\overline{\mathbb{Q}}_l$. La courbe E est isomorphe sur $\mathbb{Q}_{l,\mathrm{nr}}$ à une courbe de Tate $G_m/q^{\mathbb{Z}}$, où q est un élément de $\mathbb{Q}_l^*$ dont la valuation $v_l(q)$ est égale à $v_l(\Delta)$ (cf. [11], p. 357, th. 14.1). Le groupe E_p s'identifie à $(\mu_p q^{\mathbb{Z}/p})/q^{\mathbb{Z}}$ comme $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_{l,\mathrm{nr}})$-module; μ_p est contenu dans $\mathbb{Q}_{l,\mathrm{nr}}$, et q est une puissance p-ième dans $\mathbb{Q}_{l,\mathrm{nr}}$ si et seulement si p divise $v_l(q)$; cela démontre le lemme.

Supposons maintenant que E ait mauvaise réduction de type additif en l. La cubique $\widetilde{E}$ déduite de E par réduction modulo l a un unique point singulier P. Posons $\widetilde{E_{\mathrm{ns}}} = \widetilde{E} - \{P\}$; rappelons que l'on dispose d'une application de réduction $E(\mathbb{Q}_{l,\mathrm{nr}}) \to \widetilde{E}(\overline{\mathbb{F}}_l)$ (où $\overline{\mathbb{F}}_l$ est le corps résiduel de $\mathbb{Q}_{l,\mathrm{nr}}$). L'ensemble $E_0(\mathbb{Q}_{l,\mathrm{nr}})$ des points de $E(\mathbb{Q}_{l,\mathrm{nr}})$ dont la réduction est différente de P est un sous-groupe de $E(\mathbb{Q}_{l,\mathrm{nr}})$; l'application de réduction $E_0(\mathbb{Q}_{l,\mathrm{nr}}) \to \widetilde{E_{\mathrm{ns}}}(\overline{\mathbb{F}}_l)$ est un homomorphisme surjectif de groupes dont le noyau $E_1(\mathbb{Q}_{l,\mathrm{nr}})$ s'identifie à l'ensemble des points du groupe formel associé à E, à valeurs dans l'idéal de valuation de $\mathbb{Q}_{l,\mathrm{nr}}$.

LEMME 2. *Supposons E à réduction additive en l. Le noyau de la multiplication par p dans $E(\mathbb{Q}_{l,\mathrm{nr}})/E_0(\mathbb{Q}_{l,\mathrm{nr}})$ est isomorphe à $E(\mathbb{Q}_{l,\mathrm{nr}})[p]$.*

Démonstration. On écrit la suite exacte (cf. [11], prop. 2.1, p. 174) :

$$0 \to E_1(\mathbb{Q}_{l,\mathrm{nr}}) \to E_0(\mathbb{Q}_{l,\mathrm{nr}}) \to \widetilde{E_{\mathrm{ns}}}(\overline{\mathbb{F}}_l) \to 0;$$

le groupe $E_1(\mathbb{Q}_{l,\mathrm{nr}})$ est la limite inductive d'une suite de pro-l-groupes. Il est donc p-divisible sans p-torsion; comme par hypothèse E a réduction de type additif, le groupe $\widetilde{E_{\mathrm{ns}}}(\overline{\mathbb{F}}_l)$ est isomorphe au groupe additif $\overline{\mathbb{F}}_l$, donc p-divisible sans p-torsion; d'après le lemme du serpent, $E_0(\mathbb{Q}_{l,\mathrm{nr}})[p]$ et $E_0(\mathbb{Q}_{l,\mathrm{nr}})/pE_0(\mathbb{Q}_{l,\mathrm{nr}})$ sont réduits à 0. Il suffit ensuite de réappliquer le lemme du serpent, de nouveau avec la multiplication par p, à la suite exacte

$$0 \to E_0(\mathbb{Q}_{l,\mathrm{nr}}) \to E(\mathbb{Q}_{l,\mathrm{nr}}) \to E(\mathbb{Q}_{l,\mathrm{nr}})/E_0(\mathbb{Q}_{l,\mathrm{nr}}) \to 0$$

pour obtenir le lemme.

2. *Démonstration de la proposition.* 1) Si E a bonne réduction en l, on a $\mathbb{Q}_{l,\mathrm{nr}}(E_p) = \mathbb{Q}_{l,\mathrm{nr}}$ d'après le critère de Néron–Ogg–Shafarevitch ([11], p. 184, th. 7.1); δ_l est égal à 0, d'où $n(l, \varrho_p) = 0$ (formule (1)). Comme on a $f_l = 0$, cela montre l'assertion (a).

2) Supposons que E ait mauvaise réduction de type multiplicatif en l. D'après le lemme 1, on a

$$\dim_{\mathbb{Z}/p\mathbb{Z}} E(\mathbb{Q}_{l,\mathrm{nr}})[p] = \begin{cases} 1 & \text{si } p \text{ ne divise pas } v_l(\Delta), \\ 2 & \text{sinon}, \end{cases}$$

et l'extension $\mathbb{Q}_{l,\mathrm{nr}}(E_p)/\mathbb{Q}_{l,\mathrm{nr}}$ est de degré premier à l, de sorte que $\delta_l = 0$. D'où

$$n(l,\varrho_p) = \begin{cases} 1 & \text{si } p \text{ ne divise pas } v_l(\Delta), \\ 0 & \text{sinon} \end{cases}$$

(formule (1)). Comme f_l est égal à 1, on en déduit l'assertion (b) de la proposition.

3) Supposons que E ait mauvaise réduction de type additif en l. On a par définition $f_l = 2 + \delta_l$; d'où l'inégalité $n(l,\varrho_p) \leq f_l$ (formule (1)). Si l'on pose $f_l(p) = f_l - n(l,\varrho_p)$, on a (*loc. cit.*)

$$f_l(p) = \dim_{\mathbb{Z}/p\mathbb{Z}} E(\mathbb{Q}_{l,\mathrm{nr}})[p]. \tag{2}$$

3.1. *Cas où $p \geq 5$.* La table de Néron ([13], 6) montre que le groupe $E(\mathbb{Q}_{l,\mathrm{nr}})/E_0(\mathbb{Q}_{l,\mathrm{nr}})$ est d'ordre ≤ 4. D'après le lemme 2, on a donc $E(\mathbb{Q}_{l,\mathrm{nr}})[p] = (0)$. On a ainsi $f_l(p) = 0$ (formule (2)). D'où l'assertion (c)(i) de la proposition.

3.2. *Cas où $p = 3$.* Si E a en l une réduction de type IV ou IV*, $E(\mathbb{Q}_{l,\mathrm{nr}})/E_0(\mathbb{Q}_{l,\mathrm{nr}})$ est un groupe d'ordre 3 ([13], 6). On a ainsi $\dim_{\mathbb{Z}/3\mathbb{Z}} E(\mathbb{Q}_{l,\mathrm{nr}})[3] = 1$ (lemme 2) et $f_l(3) = 1$ (formule (2)). Supposons que E ait en l une réduction différente du type IV ou IV*. Le groupe $E(\mathbb{Q}_{l,\mathrm{nr}})/E_0(\mathbb{Q}_{l,\mathrm{nr}})$ est d'ordre premier à 3 ([13], 6); d'où $E(\mathbb{Q}_{l,\mathrm{nr}})[3] = 0$ (lemme 2) et $f_l(3) = 0$ (formule (2)). Cela démontre l'assertion (c)(ii) de la proposition.

3.3. *Cas où $p = 2$.* Notons $\#E(\mathbb{Q}_{l,\mathrm{nr}})[2]$ le nombre d'éléments de $E(\mathbb{Q}_{l,\mathrm{nr}})[2]$. Il résulte de la table de Néron (cf. [13], 6) et du lemme 2 appliqué avec $p = 2$ que l'on a les résultats indiqués dans les tableaux ci-dessous :

type de réduction de E en l	II	III	IV	I^*_ν, ν pair ≥ 0	I^*_ν, ν impair	IV*	III*	II*
$\#E(\mathbb{Q}_{l,\mathrm{nr}})[2]$	1	2	1	4	2	1	2	1

On déduit alors de la formule (2) l'assertion (c)(iii) de la proposition. Cela termine sa démonstration.

III. Appendice sur l'invariant de Hasse

Soit p un nombre premier. Considérons une courbe elliptique E, définie sur un corps commutatif, d'équation de Weierstrass affine

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

La fonction $t = -x/y$ est une uniformisante locale au voisinage de l'origine O de la courbe elliptique E. Les développements de Laurent de x, y et de la forme différentielle $\omega = dx/(2y + a_1x + a_3)$ en O s'obtiennent en substituant t, a_1, a_2, a_3, a_4, a_6 à T, A_1, A_2 A_3, A_4, A_6 dans les développements formels universels

$$\begin{aligned} X &= \frac{1}{T^2} - A_1\frac{1}{T} - A_2 - A_3T - (A_4 + A_1A_3)T^2 + \ldots, \\ Y &= -\frac{1}{T^3} + A_1\frac{1}{T^2} + A_2\frac{1}{T} + A_3 + (A_4 + A_1A_3)T + \ldots, \\ \Omega &= (1 + A_1T + (A_1^2 + A_2)T^2 + (A_1^3 + 2A_1A_2 + A_3)T^3 + \ldots)\,dT \end{aligned}$$

dont les coefficients appartiennent à l'anneau de polynôme $R = \mathbb{Z}[A_1, A_2, A_3, A_4, A_6]$ (cf. [12], §3). Le développement de Taylor en O de l'endomorphisme de multiplication par p dans E se déduit par les mêmes substitutions d'une série formelle

$$P = pT - \frac{p(p-1)}{2}A_1T^2 + \dots \qquad (\textit{loc. cit.})$$

à coefficients dans R.

Définissons les éléments U_i et V_i de R, pour $i \geq 1$ par

$$\Omega = \Big(1 + \sum_{i\geq 1} U_i T^i\Big)dT, \qquad P = \sum_{i\geq 1} V_i T^i,$$

et notons H le coefficient de $(xyz)^{p-1}$ dans l'expression

$$(y^2z + A_1xyz + A_3yz^2 - x^3 - A_2x^2z - A_4xz^2 - A_6z^3)^{p-1},$$

vue comme polynôme en trois variables x, y, z à coefficients dans R.

Théorème. *On a* $V_p \equiv U_{p-1} \equiv H \bmod pR$.

a) Démontrons la congruence $U_{p-1} \equiv V_p \bmod pR$. Pour E une courbe elliptique comme ci-dessus, la forme différentielle image réciproque de ω par l'endomorphisme de multiplication par p est égal à $p\omega$ ([11], p. 83, cor. 5.3). On a donc l'égalité des développements formels

$$p\Omega = \Big(1 + \sum_{i\geq 1} U_i P^i\Big)dP, \quad \text{où} \quad dP = \sum_{i\geq 1} iV_iT^{i-1}dT.$$

Le coefficient de T^l dans le développement de P, pour $1 \leq l \leq p-1$, est multiple de p (*loc. cit.*, p. 120, cor. 4.4). Le coefficient de $T^{p-1}dT$ dans le développement de

$$\Big(1 + \sum_{i\geq 1} U_i P^i\Big)dP$$

est donc congru à pV_p modulo p^2R; or, par définition, ce coefficient dans le développement de $p\Omega$ est égal à pU_{p-1}; cela démontre la congruence annoncée.

b) Démontrons le lemme suivant :

Lemme 1. *Soit W le coefficient de x^{p-1} dans l'expression $(x^3 + A_4x + A_6)^{(p-1)/2}$, vue comme polynôme en une indéterminée x à coefficients dans R. On a*

$$H(0,0,0,A_4,A_6) = (-1)^{(p-1)/2}\binom{p-1}{(p-1)/2}W.$$

Ce polynôme est congru à W modulo $p\mathbb{Z}[A_4, A_6]$.

Démonstration. Par définition, W est égal à

$$\sum \frac{((p-1)/2)!A_4^lA_6^m}{k!l!m!},$$

où la somme est étendue aux triplets (k,l,m) d'entiers ≥ 0 vérifiant les égalités $k+l+m = (p-1)/2$, $3k + l = p-1$. Par ailleurs, le coefficient $H(0,0,0,A_4,A_6)$ de $(xyz)^{p-1}$ dans

$(y^2z - x^3 - A_4xz^2 - A_6z^3)^{p-1}$ est égal à

$$\sum_{(k,l,m)\in S} \frac{(p-1)!(-1)^{k+l+m}A_4^l A_6^m}{((p-1)/2)!k!l!m!},$$

où S est l'ensemble des triplets (k,l,m) vérifiant les égalités $k+l+m = (p-1)/2$, $3k+l = p-1$, $2l+3m = (p-1)/2$. La troisième de ces égalités étant une conséquence des deux premières, on déduit de ce qui précède la première assertion du lemme.

D'autre part, $\binom{p-1}{(p-1)/2}$ est égal à l'entier

$$\frac{(p-1)(p-2)\dots(p-(p-1)/2)}{1\cdot 2\dots(p-1)/2};$$

la congruence $(p-1)(p-2)\dots(p-(p-1)/2) \equiv (-1)^{(p-1)/2}(1\cdot 2\dots(p-1)/2) \bmod p$ entraîne alors que $\binom{p-1}{(p-1)/2}$ est congru à $(-1)^{(p-1)/2}$ modulo p; d'où le lemme.

c) Démontrons la congruence $H \equiv U_{p-1} \bmod pR$. Si $p=2$, on a $H = U_{p-1} = A_1$. Si $p=3$, on a $H = A_1^2 - 2A_2$ et $U_{p-1} = A_1^2 + A_2$. La congruence ci-dessus est donc vérifiée si $p=2$ ou $p=3$. Nous supposerons désormais $p \geq 5$.

Introduisons les notations suivantes :

$$B_2 = A_1^2 + 4A_2, \quad B_4 = A_1A_3 + 2A_4, \quad B_6 = A_3^2 + 4A_6, \quad C_4 = B_2^2 - 24B_4,$$
$$C_6 = -B_2^3 + 36B_2B_4 - 216B_6, \quad A = -\frac{C_4}{48}, \quad B = -\frac{C_6}{864}.$$

Posons

$$f(x,y,z) = (y^2z + A_1xyz + A_3yz^2 - x^3 - A_2x^2z - A_4xz^2 - A_6z^3)^{p-1},$$
$$g(x,y,z) = (y^2z - x^3 - Axz^2 - Bz^3)^{p-1}.$$

Le polynôme $g(x,y,z)$ est à coefficients dans l'anneau $R[1/2,1/3]$, et l'on a

$$f(x,y,z) = g\left(x + \left(\frac{B_2}{12}\right)z, y + \frac{(A_1x + A_3z)}{2}, z\right). \tag{1}$$

Lemme 2. *Soit W' le coefficient de x^{p-1} dans l'expression $(x^3 + Ax + B)^{(p-1)/2}$, vue comme polynôme en une indéterminée x à coefficients dans $R[1/2,1/3]$. On a $W' \equiv H \bmod pR[1/2,1/3]$.*

Démonstration. Soit H' le coefficient de $(xyz)^{p-1}$ dans le développement de $g(x,y,z)$. Notons ∂_i, pour $i \in \{1,2,3\}$, l'opérateur de dérivation partielle par rapport à la i-ème variable, et D, D' les opérateurs différentiels

$$D = \partial_1^{p-1}\partial_2^{p-1}\partial_3^{p-1},$$
$$D' = (\partial_1 + (A_1/2)\partial_2)^{p-1}(\partial_2)^{p-1}((B_2/12)\partial_1 + (A_3/2)\partial_2 + \partial_3)^{p-1}.$$

On a

$$(Df)(x,y,z) = (D'g)(x + (B_2/12)z, y + (A_1x + A_3z)/2, z)$$

d'après le théorème de dérivation des fonctions composées. L'opérateur D' est la somme de D et de combinaisons linéaires, à coefficients dans $R[1/2,1/3]$, d'opérateurs différentiels de la forme $\partial_1^{n_1}\partial_2^{n_2}\partial_3^{n_3}$, tels que $n_1 \geq p$ ou $n_2 \geq p$. Lorsqu'on applique ces opérateurs à un polynôme dans $R[1/2,1/3][x,y,z]$, on obtient un polynôme appartenant à $pR[1/2,1/3][x,y,z]$. Par suite, on a $(Df)(x,y,z) \equiv (Dg)(x + (B_2/12)z, y + (A_1x +$

$A_3z)/2, z)$ modulo $pR[1/2, 1/3][x, y, z]$. Mais $(Df)(x, y, z)$ et $(Dg)(x, y, z)$ sont les polynômes constants (par rapport à x, y, z) égaux à $(p-1)!^3H$ et à $(p-1)!^3H'$ respectivement. Comme $(p-1)!$ est premier à p, on a $H \equiv H' \bmod pR[1/2, 1/3][x, y, z]$. Par ailleurs, il résulte du lemme 1 que H' est congru modulo $pR[1/2, 1/3]$ au coefficient W'. Cela démontre le lemme 2.

Posons

$$X' = X + \frac{B_2}{12} = \frac{1}{T^2} - A_1\frac{1}{T} - A_2 + \frac{B_2}{12} - A_3T - (A_4 + A_1A_3)T^2 + \dots$$

$$Y' = Y + \frac{(A_1X + A_3)}{2} = -\frac{1}{T^3} + \frac{3A_1}{2}\frac{1}{T^2} + \frac{(A_2 - (A_1^2/2))}{T} + \frac{(3A_3 - A_1A_2)}{2} + \dots$$

On a

$$Y'^2 = X'^3 + AX' + B \quad ([13],\ 1).$$

La série de Laurent X' admet dans l'anneau $R[1/2]((T))$ une unique racine carrée dont le terme de plus bas degré est $-1/T$. Notons la S. On a

$$S = -\frac{1}{T} + \frac{A_1}{2} + \dots, \qquad Y'^2 = S^6\left(1 + \frac{A}{S^4} + \frac{B}{S^6}\right),$$

d'où

$$Y' = S^3\sqrt{1 + \frac{A}{S^4} + \frac{B}{S^6}},$$

où $\sqrt{1 + A/S^4 + B/S^6}$ désigne la racine de la série $1 + A/S^4 + B/S^6$ dont le terme constant est 1. Par ailleurs, Ω est égal à $dX'/2Y'$, c'est-à-dire

$$\Omega = \frac{SdS}{Y} = \frac{1}{S^2\sqrt{1 + \frac{A}{S^4} + \frac{B}{S^6}}}\,dS.$$

Ainsi, Ω admet un développement en série entière de $1/S$ à coefficients dans $R[1/2, 1/3]$ de la forme

$$\Omega = \left(\frac{1}{S^2} + \dots\right)dS.$$

Notons C le coefficient de $(1/S^{p+1})dS$ dans ce développement. Les coefficients de $1/S^n$ dans le développement de $\left(\sqrt{1 + A/S^4 + B/S^6}\right)^p$ sont congrus à 0 modulo $pR[1/2, 1/3]$ pour $0 < n < 4p$. Par suite, si D est le coefficient de $1/S^{p+1}$ dans $1/S^2(1 + A/S^4 + B/S^6)^{(p-1)/2}$ on a

$$D \equiv C \bmod pR[1/2, 1/3]. \tag{2}$$

Vérifions que l'on a $D = W'$. Par définition, on a

$$D = \left(\frac{p-1}{2}\right)! \sum_{(k,l,m)\in S_1} \frac{A^lB^m}{k!l!m!}, \qquad W' = \left(\frac{p-1}{2}\right)! \sum_{(k,l,m)\in S_2} \frac{A^lB^m}{k!l!m!},$$

où $(k, l, m) \in S_1$ (resp. S_2), si et seulement si on a

$$k + l + m = (p-1)/2 \quad \text{et} \quad 4l + 6m = p - 1,$$

$$(\text{resp.} \quad k + l + m = (p-1)/2 \quad \text{et} \quad 3k + l = p - 1).$$

Les ensembles d'indices S_1 et S_2 sont égaux. D'où l'égalité $D = W'$.

Considérons alors une primitive de la forme différentielle formelle $p\Omega$. Elle possède un développement en série entière en $1/S$, qui, à une constante près, s'écrit $-p/S + \ldots$. Les coefficients de $1/S^n$ appartiennent à $p[1/2, 1/3]$ pour $n < p$ et celui de $1/S^p$ est égal à $-C$. En substituant à $1/S$ son développement en série de Taylor en T, on constate que le coefficient de T^p dans la primitive de $p\Omega$ est congru à C modulo $pR[1/2, 1/3]$. Or, par définition, ce coefficient est égal à U_{p-1}; d'où $U_{p-1} \equiv C \bmod pR[1/2, 1/3]$. La congruence (2), l'égalité $D = W'$ et le lemme 2 impliquent alors $H \equiv U_{p-1} \bmod pR[1/2, 1/3]$. Comme H et U_{p-1} sont des éléments de R, et parce que l'on a supposé $p \geq 5$, on a en fait $H \equiv U_{p-1} \bmod pR$; cela termine la démonstration du théorème.

IV. Appendice sur les courbes elliptiques à réduction ordinaire

Les résultats présentés dans cet appendice sont tirés d'une lettre que m'a adressée J.-P. Serre ([10]).

Soient K un corps de caractéristique 0 complet pour une valuation discrète v et $\overline{K}$ une clôture algébrique de K. On suppose que le corps résiduel k de K est algébriquement clos, de caractéristique $p > 0$. Soit E une courbe elliptique définie sur K ayant bonne réduction ordinaire. Si n est un entier ≥ 1, notons E_{p^n} le sous-groupe des points de p^n-torsion de $E(\overline{K})$; c'est un $\mathbb{Z}/p^n\mathbb{Z}$-module libre de rang 2. On se propose de décrire les extensions $K(E_{p^n})$ de K obtenues par adjonction des coordonnées des points de E_{p^n}, et en particulier, de trouver un critère pour que le groupe de Galois $\mathrm{Gal}(\overline{K}/K)$ opère de façon modérée sur E_{p^n}.

Commençons par démontrer le lemme général suivant :

Lemme 1. *Soient A, B deux groupes abéliens et*

$$0 \to A \xrightarrow{i} B \xrightarrow{h} \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

une suite exacte d'homomorphismes de groupes. Supposons que l'homomorphisme canonique $A \to \varprojlim A/p^nA$ soit bijectif (autrement dit, que A soit séparé et complet pour la topologie définie par les sous-groupes p^nA). Alors, il existe un unique homomorphisme $u : \mathbb{Q}_p \to B$ tel que $h \circ u$ soit la surjection canonique de $\mathbb{Q}_p$ sur $\mathbb{Q}_p/\mathbb{Z}_p$.

Démonstration. 1) Démontrons l'existence de u. Soit x un élément de $\mathbb{Q}_p$. Pour tout entier $n \geq 0$, nous pouvons choisir un élément b_n de B tel que $h(b_n) = (x/p^n) + \mathbb{Z}_p$. On a $h(pb_{n+1}) = h(b_n)$ et il existe donc un élément a_n de A tel que $pb_{n+1} - b_n = i(a_n)$. Vu l'hypothèse faite sur A, la série de terme général $p^n a_n$ converge dans A. Posons

$$b = b_0 + i\Big(\sum_{n\geq 0} p^n a_n\Big).$$

Démontrons que b ne dépend que de x et pas de la suite (b_n) choisie. Pour cela considérons $(b'_n)_{n\geq 0}$ une suite d'éléments de B telle que, pour tout $n \geq 0$, on ait $h(b'_n) = (x/p^n) + \mathbb{Z}_p$. D'après ce qui précède, il existe une suite $(a'_n)_{n\geq 0}$ d'éléments de A satisfaisant à $i(a'_n) = pb'_{n+1} - b'_n$ pour $n \geq 0$, et la série de terme général $p^n a'_n$ converge. Posons

$$b' = b'_0 + i\Big(\sum_{n\geq 0} p^n a'_n\Big).$$

Soit k un entier ≥ 0; on a

$$b = p^k b_k + i\Big(\sum_{n\geq k} p^n a_n\Big) \quad \text{et} \quad b' = p^k b'_k + i\Big(\sum_{n\geq k} p^n a'_n\Big),$$

d'où

$$b - b' = p^k\Big(b_k - b'_k + i\Big(\sum_{n\geq k} p^{n-k}(a_n - a'_n)\Big)\Big).$$

Comme $b_k - b'_k$ appartient à $i(A)$, $b - b'$ appartient à $p^k i(A)$, c'est-à-dire à $i(p^k(A))$. Puisque l'on a

$$\bigcap_{k\geq 0} p^k A = \{0\}$$

par hypothèse, b est égal à b'. Cela nous permet de définir une application $u : \mathbb{Q}_p \to B$ en associant à un élément $x \in \mathbb{Q}_p$ l'élément b de B construit par la méthode décrite ci-dessus.

Le fait que l'application u soit un homomorphisme résulte de l'assertion que la somme de deux séries convergentes dans A est une série convergente dont la limite est égale à la somme des limites. Par construction, l'application composée $h \circ u$ est la surjection canonique $\mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p$. Cela démontre l'existence de u.

2) Démontrons l'unicité de u. Soit u' un homomorphisme de $\mathbb{Q}_p$ dans B tel que $h \circ u'$ soit la surjection canonique de $\mathbb{Q}_p$ sur $\mathbb{Q}_p/\mathbb{Z}_p$. Pour tout élément x de $\mathbb{Q}_p$, on a $h \circ u'(x) = h \circ u(x)$ et $u - u'$ est un homomorphisme de $\mathbb{Q}_p$ dans $i(A)$. Puisque $\mathbb{Q}_p$ est égal à $p^n\mathbb{Q}_p$, l'image de $u - u'$ est contenue dans $i(p^n A)$ pour tout $n \geq 0$. Or, par hypothèse, l'intersection des sous-groupes $p^n A$ est réduite à l'élément neutre, ce qui entraîne l'égalité $u = u'$, et termine la démonstration du lemme.

Remarque 1. L'application $u|\mathbb{Z}_p$ prend ses valeurs dans $i(A)$. Posons $r = i^{-1} \circ (u|\mathbb{Z}_p)$. L'application $r : \mathbb{Z}_p \to A$ ainsi construite est continue lorsque A est muni de la topologie p-adique. En effet, $r^{-1}(p^n A)$ contient $p^n\mathbb{Z}_p$, qui est un sous-groupe ouvert de $\mathbb{Z}_p$.

Considérons maintenant une courbe elliptique E définie sur K ayant bonne réduction ordinaire. Soient $U^1(K)$ le sous-groupe de K^* formé des éléments x satisfaisant à $v(x - 1) > 0$, et $\widetilde{E}$ la courbe elliptique déduite de E par réduction modulo l'idéal de v. On dispose d'un homomorphisme de réduction de $E(K)$ sur $\widetilde{E}(k)$ dont le noyau $E_1(K)$ s'identifie à l'ensemble des points du groupe formel $\Im$ associé à E, à valeurs dans l'idéal de K (cf. [11], p. 174, prop. 2.1 et prop. 2.2). Puisque E a une réduction ordinaire, $\Im$ est isomorphe au groupe multiplicatif formel (cf. [5], 4), ce qui entraîne que $E_1(K)$ est isomorphe à $U^1(K)$; par ailleurs, le sous-groupe des points de $\widetilde{E}(k)$ d'ordre une puissance de p est isomorphe à $\mathbb{Q}_p/\mathbb{Z}_p$ (cf. *loc. cit.*, p. 137, th. 3.1). On a ainsi, une fois fixés un isomorphisme de groupes $\widetilde{E}(k) \to \mathbb{Q}_p/\mathbb{Z}_p$ et un isomorphisme de groupes formels $\Im \to \widehat{G_m}$, une suite exacte de groupes

$$1 \to U^1(K) \xrightarrow{j} E'(K) \xrightarrow{\pi} \mathbb{Q}_p/\mathbb{Z}_p \to 0, \tag{1}$$

où $E'(K)$ désigne le sous-groupe de $E(K)$ formé des éléments dont l'image dans $\widetilde{E}(k)$ est d'ordre une puissance de p.

Puisque K est complet, $U^1(K)$ est un groupe séparé et complet pour la topologie définie par les sous-groupes $U^1(K)^{p^n}$. D'après le lemme 1, il existe un unique homomorphisme $\psi : \mathbb{Q}_p \to E'(K)$ tel que $\pi \circ \psi$ soit la surjection canonique de $\mathbb{Q}_p$ sur $\mathbb{Q}_p/\mathbb{Z}_p$. On a $\pi \circ \psi(1) = 0$ et il existe un unique élément λ de $U^1(K)$ tel que l'on ait $\psi(1) = j(\lambda^{-1})$. On a ainsi associé à la courbe elliptique E un élément canonique (modulo les choix d'isomorphismes qui ont été faits) λ de $U^1(K)$.

Soit L une extension finie de K. Son corps résiduel est égal à k (car k est supposé algébriquement clos) et la courbe E à une réduction ordinaire sur L. Notons encore v le prolongement à L de la valuation v de K, $\widetilde{E}$ la courbe déduite de E par réduction modulo l'idéal de L et $U^1(L)$ le sous-groupe de L^* formé des éléments x tels que $v(x-1) > 0$. Comme dans l'alinéa précédent, on a une suite exacte de groupes

$$1 \to U^1(L) \xrightarrow{j_L} E'(L) \xrightarrow{\pi_L} \mathbb{Q}_p/\mathbb{Z}_p \to 0,$$

où $E'(L)$ est le sous-groupe des éléments de $E(L)$ dont l'image dans $\widetilde{E}(k)$ est d'ordre une puissance de p. En particulier, il existe un unique homomorphisme ψ_L de $\mathbb{Q}_p$ dans $E'(L)$ tel que $\pi_L \circ \psi_L$ soit la surjection canonique s (lemme 1). Vu l'assertion d'unicité dans le lemme 1, ψ_L coïncide avec ψ; en particulier, $\psi_L(\mathbb{Q}_p)$ est contenu dans $E'(K)$ et $\psi_L(1) = j_L(\lambda^{-1})$. (Autrement dit, la construction de λ est invariante par extension du corps K à L.)

Nous allons maintenant donner, pour chaque extension finie L de K, une description du module galoisien $E'(L)$. Notons $\langle \lambda, 1\rangle$ le sous-groupe fermé de $U^1(L) \times \mathbb{Q}_p$ engendré par le couple $(\lambda, 1)$. C'est le sous-groupe de $U^1(L) \times \mathbb{Q}_p$ formé des couples (λ^x, x), où x appartient à $\mathbb{Z}_p$. La deuxième projection induit un isomorphisme de ce sous-groupe sur $\mathbb{Z}_p$.

Proposition 1. *L'application $f : U^1(L) \times \mathbb{Q}_p \to E'(L)$ définie par*

$$f(a, x) = j_L(a) + \psi_L(x) \qquad (a \in U^1(L),\ x \in \mathbb{Q}_p)$$

est un homomorphisme surjectif de groupes de noyau $\langle \lambda, 1\rangle$. Lorsque L est une extension galoisienne de K, l'isomorphisme de $(U^1(L) \times \mathbb{Q}_p)/\langle \lambda, 1\rangle$ sur $E'(L)$ que l'on déduit de f par passage au quotient est compatible à l'action de $\mathrm{Gal}(L/K)$.

Démonstration. Il est clair que f est un homomorphisme de groupes. Considérons un point P appartenant à $E'(L)$; il existe $x \in \mathbb{Q}_p$ tel que P et x aient même image dans $\mathbb{Q}_p/\mathbb{Z}_p$; par définition de ψ_L, $P - \psi_L(x)$ appartient à $j_L(U^1(L))$, ce qui montre que f est surjectif. Démontrons que le noyau de f est égal à $\langle \lambda, 1\rangle$. Pour cela, remarquons d'abord que pour tout entier relatif n, $\psi_L(n)$ est égal à $j_L(\lambda^{-n})$. Par continuité (cf. remarque 1), on a $\psi_L(x) = j_L(\lambda^{-x})$ pour tout $x \in \mathbb{Z}_p$. Il en résulte que $\langle \lambda, 1\rangle$ est contenu dans le noyau de f. Inversement, soit (a, x) un élément de $U^1(L) \times \mathbb{Q}_p$ satisfaisant à l'égalité $f(a, x) = 0$; on a $\pi_L \circ \psi_L(x) = 0$ et x appartient à $\mathbb{Z}_p$. D'après ce qui précède, on a $j_L(a) = -\psi_L(x) = j_L(\lambda^x)$. Comme j_L est injectif, on a $\lambda^x = a$. Cela prouve que le noyau de f est égal à $\langle \lambda, 1\rangle$.

Supposons L galoisienne sur K. Le groupe de Galois $\mathrm{Gal}(L/K)$ agit trivialement sur $\langle \lambda, 1\rangle$ car $\lambda \in U^1(K)$; son action sur le quotient $(U^1(L) \times \mathbb{Q}_p)/\langle \lambda, 1\rangle$ est donnée par la

formule

$$^{\sigma}(a,x) \bmod \langle\lambda,1\rangle = (^{\sigma}a,x) \bmod \langle\lambda,1\rangle \quad (\sigma \in \mathrm{Gal}(L/K),\ a \in U^1(L),\ x \in \mathbb{Q}_p).$$

Par ailleurs, l'homomorphisme j_L commute à l'action de $\mathrm{Gal}(L/K)$ (car l'isomorphisme de groupes formels $\Im \to \widehat{G_m}$ a été choisi sur K) et $\psi_L(\mathbb{Q}_p)$ est contenu dans $E'(K)$. La proposition en résulte.

Si n est un entier ≥ 1, notons μ_{p^n} le groupe des racines p^n-ièmes de l'unité de $\overline{K}$ et E_{p^n} le sous-groupe des points de p^n-torsion de $E(\overline{K})$.

Proposition 2. *Soit n un entier ≥ 1. On a l'égalité*

$$K(E_{p^n}) = K(\mu_{p^n}, \lambda^{1/p^n}).$$

Démonstration. Soit L une extension galoisienne finie de K contenant les racines p^n-ièmes de λ, ainsi que les coordonnées des points de E_{p^n}. Soit λ^{1/p^n} une racine p^n-ième de λ dans L. Le sous-groupe des points de p^n-torsion de $E'(L)$ est égal à E_{p^n}. De la prop. 1, on déduit alors un isomorphisme de $\mathrm{Gal}(L/K)$-modules de E_{p^n} sur le sous-groupe des points de p^n-torsion du groupe $(U^1(L) \times \mathbb{Q}_p)/\langle\lambda,1\rangle$. Si un élément σ de $\mathrm{Gal}(L/K)$ fixe E_{p^n}, on doit avoir

$$^{\sigma}(\lambda^{1/p^n}, 1/p^n) \equiv (\lambda^{1/p^n}, 1/p^n) \bmod \langle\lambda,1\rangle;$$

autrement dit, le couple $(^{\sigma}\lambda^{1/p^n}/\lambda^{1/p^n}, 0)$ est égal à (λ^x, x) pour un élément $x \in \mathbb{Z}_p$. On a nécessairement $x = 0$ et $^{\sigma}\lambda^{1/p^n} = \lambda^{1/p^n}$. Cela prouve que $K(E_{p^n})$ contient λ^{1/p^n}; par ailleurs, il contient μ_{p^n} comme le montre l'accouplement du Weil. Inversement, soit σ un élément de $\mathrm{Gal}(L/K)$ qui fixe λ^{1/p^n} et μ_{p^n}. Soit $(a,b) \in U^1(L) \times \mathbb{Q}_p$ un point dont l'image dans $(U^1(L) \times \mathbb{Q}_p)/\langle\lambda,1\rangle$ est de p^n-torsion. On a $a^{p^n} = \lambda^x$ et $p^n b = x$ pour un élément x de $\mathbb{Z}_p$; si l'on écrit $x = x' + p^n x''$ avec $x' \in \mathbb{Z}$ et $x'' \in \mathbb{Z}_p$, on a $a = z(\lambda^{1/p^n})^{x'} \lambda^{x''}$ avec $z \in \mu_{p^n}$ et $\lambda^{x''} \in U^1(K)$. Cela implique que l'on a $\sigma(a) = a$. Par ailleurs, on a $\sigma(b) = b$ car $b \in \mathbb{Q}_p$. Cela démontre que $K(\mu_{p^n}, \lambda^{1/p^n})$ contient E_{p^n}. D'où la proposition.

Soit I_p le plus grand pro-p-sous-groupe de $\mathrm{Gal}(\overline{K}/K)$. Le corps laissé fixe par I_p est l'extension modérément ramifiée maximale de K dans $\overline{K}$. Rappelons que l'action de $\mathrm{Gal}(\overline{K}/K)$ sur μ_{p^n} est donnée par un caractère $\chi_n : \mathrm{Gal}(\overline{K}/K) \to (\mathbb{Z}/p^n\mathbb{Z})^*$ dont l'image s'identifie au groupe de Galois $\mathrm{Gal}(K(\mu_{p^n})/K)$ qui est d'ordre premier à p.

Corollaire 1. *Soit n un entier ≥ 1. Les assertions suivantes sont équivalentes* :

(i) *I_p opère trivialement sur E_{p^n}*;

(ii) *λ est une puissance p^n-ième dans $U^1(K)$*;

(iii) *l'action de $\mathrm{Gal}(\overline{K}/K)$ sur E_{p^n} est représentable matriciellement dans une base convenable de E_{p^n} sur $\mathbb{Z}/p^n\mathbb{Z}$ par $\left(\begin{smallmatrix}\chi_n & 0\\ 0 & 1\end{smallmatrix}\right)$.*

Démonstration. Pour que I_p opère trivialement sur E_{p^n}, il faut et il suffit que le degré $[K(E_{p^n}) : K]$ soit premier à p. D'après la prop. 2, c'est le cas si et seulement si λ est une puissance p^n-ième dans K. Soit τ la représentation donnant l'action de $\mathrm{Gal}(\overline{K}/K)$ sur E_{p^n}. Elle est représentable matriciellement dans une base convenable de E_{p^n} sur $\mathbb{Z}/p^n\mathbb{Z}$ par

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

(cf. [6], 1.11). Pour que $[K(E_{p^n}) : K]$ soit premier à p, il faut et il suffit donc que τ soit représentable matriciellement par

$$\begin{pmatrix} \chi_n & 0 \\ 0 & 1 \end{pmatrix}.$$

Cela prouve le corollaire.

Rappelons que $\widetilde{E}$ désigne la courbe elliptique déduite de E par réduction modulo l'idéal de la valuation de K, et que $E'(K)$ est le sous-groupe de $E(K)$ formé des éléments dont l'image dans $\widetilde{E}(k)$ est d'ordre une puissance de p (cf. (1)).

Corollaire 2. *Les assertions suivantes sont équivalentes* :

(i) *on a* $\lambda = 1$;

(ii) *la suite exacte de groupes*

$$(*) \qquad 1 \to U^1(K) \xrightarrow{j} E'(K) \xrightarrow{\pi} \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

est scindée;

(iii) *pour tout* $n \geq 1$, I_p *opère trivialement sur* E_{p^n}.

Démonstration. Supposons $\lambda = 1$. Soit ψ l'homomorphisme de $\mathbb{Q}_p$ dans $E'(K)$ tel que $\pi \circ \psi$ soit la surjection canonique (lemme 1). Puisque l'on a $\psi(x) = j(\lambda^{-x})$, pour tout x appartenant à $\mathbb{Z}_p$ (dém. de la prop. 1), le noyau de ψ contient $\mathbb{Z}_p$. Ainsi, ψ définit par passage au quotient un homomorphisme $t : \mathbb{Q}_p/\mathbb{Z}_p \to E'(K)$. L'homomorphisme composé $\pi \circ t$ est l'identité de $\mathbb{Q}_p/\mathbb{Z}_p$, donc la suite exacte $(*)$ est scindée.

Inversement, si la suite $(*)$ est scindée, il existe un homomorphisme $\varphi : \mathbb{Q}_p/\mathbb{Z}_p \to E'(K)$ tel que $\pi \circ \varphi$ soit l'identité. L'application de $\mathbb{Q}_p$ dans $E'(K)$ definie par $x \mapsto \varphi(x \bmod \mathbb{Z}_p)$ est l'homomorphisme ψ d'après l'assertion d'unicité du lemme 1. On en déduit l'égalité $\psi(1) = 0$, i.e. $\lambda = 1$ (car $\psi(1) = j(\lambda^{-1})$); cela prouve l'équivalence des assertions (i) et (ii).

Par ailleurs, le cor. 1 et le fait que l'intersection des $U^1(K)^{p^n}$ soit triviale entraînent l'équivalence des assertions (i) et (iii); cela termine la démonstration du corollaire.

Remarque 2. On a $\lambda = 1$ si et seulement si E est le relèvement canonique de la courbe $\widetilde{E}$. En effet, d'après [5], 5, il existe une courbe elliptique A définie sur K, unique à un K-isomorphisme près, appelée le *relèvement canonique* de $\widetilde{E}$, telle que :

(a) la réduction de A modulo l'idéal de la valuation de K est égale à $\widetilde{E}$;

(b) pour tout $n \geq 1$, I_p opère trivialement sur les points de p^n-torsion de A.

Nous allons, pour finir, préciser la valuation de $\lambda - 1$. Pour cela, notons c_4, c_6 les invariants standards associés à un modèle minimal de E sur K (cf. [13], 1); $v(c_4)$ et $v(c_6)$ sont indépendants du modèle minimal choisi (cf. *loc. cit.*). Soient $j(E)$ et $j(\widetilde{E})$ les invariants modulaires de E et de $\widetilde{E}$. Notons $j_{\mathrm{can}}(\widetilde{E})$ l'invariant modulaire du relèvement canonique de $\widetilde{E}$; $j_{\mathrm{can}}(\widetilde{E})$ est un élément de l'anneau de valuation de K qui relève $j(\widetilde{E})$ (cf. la remarque ci-dessus).

PROPOSITION 3. *On a les égalités* :

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

Dans [10], Serre indique que λ est l'élément appelé en anglais "Serre–Tate q" où "Dwork q", et que $\widetilde{E}$ et λ suffisent à reconstruire E. Il signale que d'après Katz ([2]), la correspondance $E \leftrightarrow \lambda$ est un isomorphisme de la variété formelle des modules de courbes elliptiques (au voisinage de $\widetilde{E}$) sur le groupe multiplicatif formel. Par ailleurs, j (resp. $j^{1/3}$; resp. $(j-1728)^{1/2}$) paramètre cette variété formelle de modules lorsque $j(\widetilde{E}) \notin \{0, 1728\}$ (resp. $j(\widetilde{E})=0$; resp. $j(\widetilde{E})=1728$), ce qui entraîne la proposition.

Bibliographie

[1] D. Husemöller, *Elliptic Curves*, Grad. Texts in Math. 111, Springer, 1987.

[2] N. Katz, *Serre–Tate local moduli*, dans : Surfaces algébriques, Lecture Notes in Math. 868, Springer, 1981, 138–202.

[3] A. Kraus, *Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique*, Acta Arith. 54 (1989), 75–80.

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

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

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

[7] —, *Corps locaux*, 3ème édition, Hermann, Paris, 1980.

[8] —, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179–230.

[9] —, Lettre à J. Oesterlé, 28 juillet 1987.

[10] —, Lettre à A. Kraus, 4 juillet 1988.

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

[12] J. Tate, *The Arithmetic of Elliptic Curves*, Invent. Math. 23 (1974), 179–206.

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