JOURNAL OF ALGEBRA **179,** 145–190 (1996)
ARTICLE NO. 0008

# Sommes arithmétiques et éléments de Stickelberger

A. Bayad et W. Bley*

*Institut für Mathematik der Universität Augsburg, Universitätsstr. 8, D-86159 Augsburg, Germany*

et

Ph. Cassou-Noguès

*U.F.R. de Mathématiques et d'Informatique, Université Bordeaux I, F-33405, Talence Cedex, France*

*Communicated by Walter Feit*

Received June 14, 1994

## 1. INTRODUCTION ET RÉSULTATS

Le célèbre théorème de Stickelberger fournit des annulateurs du groupe des classes d'idéaux des corps cyclotomiques. La démonstration de ce théorème repose de manière essentielle sur la factorisation en produit d'idéaux premiers des sommes de Gauss [2, 9].

L'étude d'une situation relative, lorsqu'on remplace $\mathbb{Q}$ par un corps de nombres $F$, est introduite dans [4]. On étudie pour cela la factorisation de certaines résolvantes, introduites par Abel et Jacobi, construites à partir d'une courbe elliptique munie d'un point d'ordre premier rationnel sur $F$. Cette factorisation est analogue à celle des sommes de Gauss.

On s'intéresse ici aux propriétés de nouvelles résolvantes introduites dans le cas de la multiplication complexe par S. P. Chan [5] qui généralisent les fonctions considérées dans [4].

Le but de cet article est notamment d'étudier leur factorisation en produit d'idéaux premiers et ses conséquences arithmétiques. Les théorèmes 1.1, 1.2 et 1.3 que nous obtenons généralisent les théorèmes 1 et 2 de [4], qui en sont des cas particuliers, et les théorèmes A et B de [1]. Ils les améliorent également en donnant la valuation en des premiers que

* Les auteurs tiennent à remercier la DFG pour son soutien financier à l'aboutissement de ce travail.



0021-8693/96 $12.00

l'étude de [4] excluait. On sait que l'étude de la structure galoisienne des anneaux d'entiers de corps de nombres dépend de manière cruciale du comportement arithmétique de ce type de résolvantes de Lagrange [3, 5, 7].

Il est à noter que les résolvantes considérées ici sont à une constante multiplicative non nulle près celles de [7].

Si $n$ est un entier, $n \geq 2$, on note $\zeta_n$ une racine primitive $n$-ième de 1. Pour tout entier $t$, $1 \leq t \leq n$, $(t, n) = 1$, on note $\sigma_t$ l'automorphisme de $\mathbb{Q}(\zeta_n)$ induit par $\zeta_n \mapsto \zeta_n^t$; par abus de notation, $\sigma_t$ désigne également toute restriction ou prolongement "naturel" de cet automorphisme. Si $E$ est une courbe elliptique définie sur un corps de nombres on pose $E[n]$ le groupe des points de $n$-division de $E$.

On fixe un nombre premier $l$, $l \geq 5$, et un corps de nombres $F$. On suppose que $F \cap \mathbb{Q}(\zeta_l) = \mathbb{Q}$. On pose $N = F(\zeta_l + \zeta_l^{-1})$ et $\Gamma = \mathrm{Gal}(N/F)$ où $\Gamma = \{\sigma_t, 1 \leq t \leq (l-1)/2\}$. Soit $(E, P)$ une courbe elliptique $E$ définie sur $F$ munie d'un point rationnel sur $F$ d'ordre $l$. A tout nombre premier $p$ tel que $(l, p(p+1)) = 1$ et à tout point $Q \in E[l] \setminus \mathbb{Z}P$ nous associons une "somme de Gauss elliptique", $\tilde{T}_p(P, Q)$ dont la définition précise est donnée en (2.3). On vérifie que $\tilde{T}_p(P, Q) \in F(E[l])$ et que $\tilde{T}_p^l(P, Q) \in N$.

DÉFINITION. On définit l'élément de Stickelberger quadratique $\theta_2(p)$ de $\mathbb{Q}[\Gamma]$ par:

$$\theta_2(p) = (p^3 - p^2) \sum_{t=1}^{(l-1)/2} \gamma(t)\sigma_t^{-1}, \qquad \sigma_t \in \Gamma$$

avec

$$\gamma(t) = (p^2 - p)\beta(t) + \sum_{s=1}^{p-1} \alpha(t, s)$$

où $\beta(t)$ et $\alpha(t, s)$ sont les rationnels définis par:

$$\beta(t) = \frac{l}{p}\left(\frac{t}{l}\left\{\frac{tp}{l}\right\} + \inf\left(0, 1 - \frac{t}{l} - \left\{\frac{tp}{l}\right\}\right)\right)$$

$$\alpha(t, s) = -tp\left\{\frac{a}{lp}\right\} + lp \inf\left(\frac{t}{l}, \left\{\frac{a}{lp}\right\}\right)$$

et

$$a = lsx + pty,$$

où $x, y \in \mathbb{Z}$ sont choisis tels que $lx - py = 1$.

On pose $\{z\}$ la partie fractionnaire du nombre réel $z$.

*Remarques.* (i) La définition de $\alpha(t, s)$ ne dépend pas du choix de $x$ et $y$.

(ii) L'élément $\theta_2(p)$ de $\mathbb{Q}[\Gamma]$ est dit quadratique car il satisfait la congruence suivante:

$$\theta_2(p) \equiv \frac{12n_p}{l} \sum_{t=1}^{(l-1)/2} t^2\sigma_t^{-1} \qquad (\mathrm{mod}\, \mathbb{Z}[\Gamma])$$

où

$$n_p = \frac{p^2(p-1)^2(p+1)}{12}.$$

Lorsqu'on choisit $p \equiv 1 \pmod{l}$ on montre dans l'appendice 2 l'égalité

$$\theta_2(p) = \frac{6n_p}{l} \sum_{t=1}^{(l-1)/2} (tl - t^2)\sigma_t^{-1}.$$

Pour tout idéal premier $\mathfrak{p}$ de $F$ on note $r_\mathfrak{p}$ la valuation $\mathfrak{p}$-adique du discriminant minimal $\mathfrak{D}_{E/F}$ de la courbe $E/F$.

On désigne par $\mathfrak{R}(E, P)$ l'ensemble des diviseurs premiers $\mathfrak{p}$ de $\mathfrak{D}_{E/F}$, premier à $l$, pour lesquels la réduction de $P$ modulo $\mathfrak{p}$ est un point régulier de la courbe réduite.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux fractionnaires de $N$, on écrit:

$$\mathfrak{a} \equiv \mathfrak{b} \qquad (\mathrm{mod}\, l)$$

lorsque les diviseurs de $\mathfrak{a}\mathfrak{b}^{-1}$ divisent $l$.

Maintenant on peut énoncer les principaux résultats de cet article.

THÉORÈME 1.1. *Tout idéal premier $\mathfrak{p}$ de $\mathfrak{R}(E, P)$ possède un relèvement $\mathfrak{P}$ dans $N$ tel que*:

$$\left(\tilde{T}_p(P, Q)\right)^l \mathfrak{D}_{E/F}^{ln_p} \equiv \left(\prod_{\mathfrak{p} \in \mathfrak{R}(E,P)} \mathfrak{P}^{r_\mathfrak{p}}\right)^{l\theta_2(p)} \qquad (\mathrm{mod}\, l).$$

THÉORÈME 1.2. *On suppose que tout diviseur premier de $\mathfrak{D}_{E/F}$, premier à $l$, appartient à $\mathfrak{R}(E, P)$. Alors on a*:

$$\left(\prod_{t=1}^{(l-1)/2} \tilde{T}_p(P, tQ)\right) \equiv \mathfrak{D}_{E/F}^{(l(l-1)/2)n_p} \qquad (\mathrm{mod}\, l).$$

Il est à remarquer que le théorème 1.2 se déduit immédiatement du théorème 1.1 et de l'évaluation des sommes suivantes:

$$\sum_{n=1}^{l-1} \beta(n) \qquad \text{et} \qquad \sum_{n=1}^{l-1} \sum_{s=1}^{p-1} \alpha(n,s)$$

qui sont riches en propriétés analytiques et arithmétiques.

THÉORÈME 1.3. *Soient $l$ et $p$ des entiers tels que $(l, p(p+1)) = 1$. Alors on a les égalités*:

$$\text{(i)} \quad \sum_{n=1}^{l-1} \beta(n) = \frac{l^2-1}{12p}$$

$$\text{(ii)} \quad \sum_{n=1}^{l-1} \sum_{s=1}^{p-1} \alpha(n,s) = \frac{p(p-1)(l^2-1)}{12}.$$

*Remarque*. Lorsque les hypothèses du théorème 1.2 ne sont pas remplies on pose

$$\mathfrak{D}_{E/F,reg} = \prod_{\mathfrak{p} \in \mathfrak{R}(E,P)} \mathfrak{p}^{r_{\mathfrak{p}}}.$$

Le théorème 1.2 doit être remplacé par

$$\left( \prod_{t=1}^{(l-1)/2} \tilde{T}_p(P, tQ) \right) \equiv \left( \mathfrak{D}_{E/F,reg}^{l+1} \mathfrak{D}_{E/F}^{-1} \right)^{((l-1)/2)n_p} \pmod{l}.$$

Le plan de cet article est le suivant: le paragraphe 2 contient la définition de nos résolvantes et leurs propriétés. Ces propriétés se démontrent comme dans [4, paragraphe 2]. Le lecteur peut aussi se reporter à [1]. Les paragraphes 3 et 4 sont consacrés à l'étude complexe et $p$-adique de ces sommes. Le point crucial est leur expression comme produit de fonctions $\theta$ complexes, théorème 3.9, et $p$-adique, théorème 4.6.

Les démonstrations techniques du paragraphe 4 sont données en appendice 1. Dans le paragraphe 5 nous donnons une démonstration analytique du théorème 1.3. Une démonstration de ces égalités reposant sur la théorie des sommes de Dedekind nous a été communiquée par C. Meyer.

Le théorème 1.1 est démontré dans le paragraphe 6. Enfin dans le paragraphe 7 nous donnons une application du théorème 1.1 à l'annulation de certains groupes de classes d'idéaux ainsi que quelques exemples. Nous indiquons notamment une méthode de calcul de l'idéal $\prod_{\mathfrak{p} \in \mathfrak{R}(E,P)} \mathfrak{P}^{r_{\mathfrak{p}}}$.

Lorsque $l = 5$ nous déterminons explicitement cet idéal dans plusieurs cas. Les calculs de ce paragraphe ont été effectués avec le système Pari.
Les auteurs remercient H. Cohen, A. Jehanne et M. Olivier de leur aide. Ils remercient également J. Cougnard pour ses nombreuses suggestions.

Une partie de ce travail a été realisé lors d'un sejours de l'un des auteurs au Fields Institute. Il le remercie de son hospitalité.

## 2. RÉSOLVANTES ELLIPTIQUES

Ce paragraphe contient la définition et quelques propriétés de nos "sommes de Gauss elliptiques". Les démonstrations données dans [1] sont essentiellement celles de [4, paragraphe 2].

On fixe deux nombres premiers $l$ et $p$ distincts, $l \geq 5$, et un corps de nombres $F$ qu'on suppose linéairement disjoint de $\mathbb{Q}(\zeta_l)$.

Soit $E$ une courbe elliptique définie sur $F$, munie d'un point $P$ rationnel sur $F$, d'ordre $l$.

Soit $\{S, R\}$ un couple de points de $E[p]$ qui forment une base de $E[p]$ sur $\mathbb{F}_p$.

DÉFINITION 2.1. On désigne par $D(\cdot, S, R)$ une fonction appartenant à $M(E)$, $M = F(E[p])$, telle que:

$$(D) = \sum_{k=0}^{p-1} ((S + kR) - (kR)).$$

*Remarque* 2.2. L'existence d'une telle fonction est assurée par le théorème d'Abel-Jacobi [8, III, remarque 3.5.1].

DÉFINITION 2.3. Soient $S$ et $T$ deux points primitifs respectivement de $p$-division et $p^2$-division de la courbe $E$ tels que $\{S, R = pT\}$ forment une base de $E[p]$ sur $\mathbb{F}_p$. Si $Q$ est un point d'ordre $l$ de $E$, n'appartenant pas à $\langle P \rangle_{\mathbb{Z}}$, alors on associe à $(P, Q, S, T)$ la somme de Gauss elliptique:

$$\mathscr{R}(P, Q, S, T) = \sum_{u \in \mathbb{F}_l} \frac{D(Q + uP, S, R)}{D(T, S, R)} e_l(Q, uP)^{-1}$$

où $e_l$ désigne l'accouplement de Weil sur les points de $l$-division de $E$.

On déduit de la définition de $D$ que $\mathscr{R}(P, Q, S, T)$ ne dépend que de la classe de $S$ modulo $\langle R \rangle_{\mathbb{Z}}$. On définit une nouvelle somme indépendante du choix de $S$ et $T$ en posant:

$$\tilde{T}_p(P, Q) = p^{-(p^4 - p^3)} \prod_{T \in E'[p^2]} \prod_{S \in E''[p]} \mathscr{R}(P, Q, S, T)$$

où $E'[p^2]$ désigne l'ensemble des points primitifs de $p^2$-division de la courbe $E$ et $E''[p]$ désigne un système de représentants des points non nuls de $E[p]/\langle R\rangle_{\mathbb{Z}}$. Par raison de simplicité on note désormais $\tilde{T}$ la somme $\tilde{T}_p$. Les propriétés de ces sommes sont rappelées ci-dessous.

PROPOSITION 2.4. (i) *$\tilde{T}(P,Q)$ ne dépend pas du choix de modèle de la courbe $E$ sur $F$.*

(ii) *$\tilde{T}(P,Q) \in F(E[l])$ pour toute $\mathbb{F}_l$-base $\{P,Q\}$ de $E[l]$.*

(iii) *Soit $\omega \in \mathrm{Gal}(F(E[l]/F))$ défini par*

$$Q^{\omega} = a_{\omega}Q + b_{\omega}P \qquad \text{avec } a_{\omega} \in \mathbb{F}_l^*,\ b_{\omega} \in \mathbb{F}_l,$$
$$P^{\omega} = P.$$

*On a alors*:

$$\tilde{T}(P,Q)^{\omega} = e_l(P,Q)^{p^2(p-1)^2(p+1)a_{\omega}b_{\omega}}\tilde{T}(P,a_{\omega}Q).$$

(iv) *$\tilde{T}(P,Q)^l \in N$ et $\tilde{T}(P,Q) = \tilde{T}(P,-Q)$.*

(v) *L'idéal $(\tilde{T}(P,Q))$ est un idéal ambige pour $(F(E[l])/N)$.*

Puisque l'idéal $(\tilde{T}(P,Q))$ est ambige pour $F(E[l])/N$ nous aurons

$$\left(\tilde{T}(P,Q)^l\right) \equiv I^l \prod_{\mathfrak{P}} \mathfrak{P}^{s_{\mathfrak{P}}} \qquad (\mathrm{mod}\, l),$$

où $I$ est un idéal de $N$ et $\mathfrak{P}$ parcourt les idéaux premiers de $N$, ramifiés dans $F(E[l])$, qui ne divisent pas $l$. Les idéaux $\mathfrak{P}$ sont nécessairement des relèvements dans $N$ d'idéaux premiers de $F$ où la courbe $E$ possède mauvaise réduction, Il est à noter que l'existence d'un point rationnel sur $F$ d'ordre $l$, $l \geq 5$, implique qu'en de tels premiers la réduction de $E$ est semi-stable, [4, paragraphe 1]. Le but des paragraphes 3 et 4 est de préciser la factorisation de $(\tilde{T}(P,Q))^l$ en produit d'idéaux premiers.

## 3. RÉSOLVANTES COMPLEXES

Dans ce paragraphe $l$ et $p$ désignent des entiers tels que $(l,p) = 1$, qu'on ne suppose pas nécessairement premiers. On donne le lien entre nos résolvantes et les résolvantes considérées dans [7], puis on les factorise en produit de fonctions de Klein.

Pour cela, on fixe un réseau $\Omega$ de $\mathbb{C}$ et une base $\{\omega_1, \omega_2\}$ de $\Omega$ telle que $\mathrm{Im}(\omega_1/\omega_2) > 0$. On note $E[n]$ le groupe des points de $\mathbb{C}/\Omega$ annulés par $n$, $n \in \mathbb{N}$. On fixe un système de générateurs $\{\varphi, \psi\}$ de $E[p]$ sur $\mathbb{Z}$, $\lambda \in E[p^2]$ tel que $p\lambda = \psi$ et un système de générateurs $\{\alpha, \gamma\}$ de $E[l]$ sur $\mathbb{Z}$.

DÉFINITION 3.1. Soit $D(\cdot, \varphi, \psi)$ une fonction elliptique pour $\Omega$ qui a pour diviseur:

$$(D(\cdot, \varphi, \psi)) = \sum_{k=0}^{p-1} ((\varphi + k\psi) - (k\psi)).$$

On définit la résolvante elliptique

$$\mathscr{R}(\alpha, \gamma, \varphi, \lambda) = \sum_{u=0}^{l-1} \frac{D(\gamma + u\alpha, \varphi, \psi)}{D(\lambda, \varphi, \psi)} e_l(\gamma, u\alpha)^{-1}, \tag{1}$$

où $e_l$ désigne l'accouplement de Weil sur les points de $l$-division de $\mathbb{C}/\Omega$.

Pour étudier (1) on introduit une fonction elliptique pour $\Omega$, définie par:

$$\mathscr{R}(z, \alpha, \gamma, \varphi, \lambda) = \sum_{u=0}^{l-1} \frac{D(z + u\alpha, \varphi, \psi)}{D(\lambda, \varphi, \psi)} e_l(\gamma, u\alpha)^{-1}. \tag{2}$$

Dans la suite on note $\mathscr{R}(z)$ cette fonction. Elle a les propriétés suivantes:

PROPOSITION 3.2. (i) $\mathscr{R}(z + \psi) = \omega_\Omega(\varphi, \psi)\mathscr{R}(z)$, *où* $\omega_\Omega(\varphi, \psi)$ *est une racine p-ième de l'unité.*

(ii) $\mathscr{R}(z + \alpha) = e_l(\gamma, \alpha)\mathscr{R}(z)$.

Si l'on définit $D_\psi(\cdot, \varphi, \psi)$ par

$$D_\psi(z, \varphi, \psi) = D(z + \psi, \varphi, \psi)$$

on note que les fonctions $D$ et $D_\psi$ ont le même diviseur. Elles sont donc égales à une constante $\omega_\Omega(\varphi, \psi)$ près. Puisque $\psi$ est d'ordre $p$ on en déduit que $\omega_\Omega(\varphi, \psi)^p = 1$ ce qui démontre (i). La démonstration de (ii) se déduit de la définition (2).

On considère la fonction thêta définie par

$$\vartheta\left(z \middle| \begin{matrix}\omega_1 \\ \omega_2\end{matrix}\right) = 2\pi i e^{-(1/2)(\eta_2/\omega_2)z^2} \sigma\left(z \middle| \begin{matrix}\omega_1 \\ \omega_2\end{matrix}\right) \eta^2\left(\frac{\omega_1}{\omega_2}\right) \omega_2^{-1},$$

où $\eta$ désigne la fonction $\eta$ de Dedekind, $\eta_1$ et $\eta_2$ les quasi-périodes de la fonction $\zeta$ de Weierstrass et $\sigma$ la fonction sigma de Weierstrass pour le réseau $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. La fonction thêta vérifie les propriétés suivantes, que l'on déduit de celles de la fonction $\sigma$, [3, III, proposition 3.10].

PROPOSITION 3.3.

(i) $\vartheta\left(z \middle| \begin{matrix}\omega_1\\ \omega_2\end{matrix}\right)$ *est une fonction holomorphe sur* $\mathbb{C}$ *dont les zéros sont simples et sont les éléments de* $\Omega$.

(ii) $$\vartheta\left(z+\omega_1 \middle| \begin{matrix}\omega_1\\ \omega_2\end{matrix}\right) = -e^{-(2\pi i/\omega_2)(z+(1/2)\omega_1)}\vartheta\left(z \middle| \begin{matrix}\omega_1\\ \omega_2\end{matrix}\right).$$

(iii) $$\vartheta\left(z+\omega_2 \middle| \begin{matrix}\omega_1\\ \omega_2\end{matrix}\right) = -\vartheta\left(z \middle| \begin{matrix}\omega_1\\ \omega_2\end{matrix}\right).$$

Soit $\Omega$ un réseau de $\mathbb{C}$, $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\mathrm{Im}(\omega_1/\omega_2) > 0$, et $x$ en point d'ordre $n$ de $\mathbb{C}/\Omega$. On définit le réseau $\Omega + \mathbb{Z}x$ en posant $\Omega + \mathbb{Z}x = \Omega + \mathbb{Z}u$ où $u$ est un représentant quelconque de $x$ dans $\mathbb{C}$. On utilise souvent le lemme suivant

LEMME 3.4. *Il existe un représentant* $\gamma$ *de* $x$ *dans* $\mathbb{C}$ *et* $\beta \in \Omega$ *tels que*

$$\Omega + \mathbb{Z}x = \mathbb{Z}\beta + \mathbb{Z}\gamma \qquad \textit{avec } \mathrm{Im}\frac{\beta}{\gamma} > 0,$$

$$\Omega = \mathbb{Z}\beta + \mathbb{Z}n\gamma.$$

Montrons qu'il existe un représentant $\gamma$ de $x$ tel que $n\gamma = n_1\omega_1 + n_2\omega_2$ avec $(n_1, n_2) = 1$. Soit $u$ un représentant de $x$. On a

$$nu = a_1\omega_1 + a_2\omega_2.$$

On suppose que $a_1a_2 = 0$, par exemple $a_1 = 0$. Puisque $x$ est d'ordre $n$ alors $(a_2, n) = 1$. On pose $\gamma = \omega_1 + u$. On suppose dorénavant $a_1a_2 \neq 0$. On pose $d = (a_1, a_2)$ et $a_1 = dm_1$, $a_2 = dm_2$. Soit $m_2'$ le plus grand diviseur de $m_2$ premier à $n$ et $m_2''$ tel que $m_2 = m_2'm_2''$. Puisque $(n, dm_2') = 1$ il existe $b_1, b_2 \in \mathbb{Z}$ tels que

$$1 - dm_1 = b_1n + b_2(dm_2').$$

On pose $\gamma = u + b_1\omega_1$. On obtient

$$n\gamma = (dm_1 + nb_1)\omega_1 + (dm_2)\omega_2.$$

On note $n_1 = dm_1 + nb_1$ et $n_2 = dm_2$. Soit $l$ un nombre premier. Si $l|dm_2'$ alors $l$ ne divise pas $n_1 = dm_1 + b_1n$. Si $l \nmid dm_2'$ et $l|m_2''$ alors $l|n$, mais $l \nmid dm_1$, donc $l \nmid n_1$. On a donc montré que $(n_1, n_2) = 1$. Soit $(u_0, v_0) \in \mathbb{Z}^2$ tel que

$$u_0n_2 - v_0n_1 = 1.$$

On note $\beta = u_0\omega_1 + v_0\omega_2$. Puisque

$$M = \begin{pmatrix} u_0 & v_0 \\ n_1 & n_2 \end{pmatrix} \in Sl_2(\mathbb{Z})$$

les égalités du lemme sont immédiates.

Soit $\Lambda = \Omega + \mathbb{Z}\psi$. On choisit un représentant de $\psi$ qu'on note aussi $\psi$ et un élément $\beta_1$ de $\Omega$ tels que $\{\psi, \beta_1\}$ (resp. $\{p\psi, \beta_1\}$) soit une base sur $\mathbb{Z}$ de $\Lambda$ (resp. $\Omega$) et $\mathrm{Im}(\psi/\beta_1) > 0$.

DÉFINITION 3.5. (i) On désigne par $m_0$ et $n_0$ des éléments de $\mathbb{Z}$ tels que

$$\varphi = m_0\psi - n_0\frac{\beta_1}{p}.$$

(ii) On définit la fonction $h$ par

$$h(z) = \frac{\vartheta\left(z + n_0(\beta_1/p)\middle|\begin{matrix}\psi\\ \beta_1\end{matrix}\right)}{\vartheta\left(z\middle|\begin{matrix}\psi\\ \beta_1\end{matrix}\right)}.$$

D'après la proposition (3.3), on sait que $h$ est une fonction elliptique pour $\Omega$. Son diviseur est donné par

$$\begin{aligned}(h) &= \sum_{k=0}^{p-1}\left(\left(-n_0\frac{\beta_1}{p} + k\psi\right) - (k\psi)\right)\\ &= \sum_{k=0}^{p-1}((\varphi + k\psi) - (k\psi)).\end{aligned}$$

Donc, d'après le théorème d'Abel-Jacobi, la fonction $h(z)$ est égale à $D(z, \varphi, \psi)$ à une constante multiplicative non nulle près.

On considère le réseau $\Sigma = \Lambda + \mathbb{Z}\alpha$. Puisque $(l, p) = 1$, $\Sigma/\Lambda$ est un groupe cyclique d'ordre $l$.

DÉFINITION 3.6. On désigne par $\chi$ le caractère de $\Sigma/\Lambda$ défini par

$$\chi(u\alpha) = e_l(\gamma, u\alpha).$$

Alors on obtient

$$\mathscr{R}(z) = \frac{1}{h(\lambda)} \sum_{u=0}^{l-1} h(z + u\alpha)\,\bar{\chi}(u\alpha).$$

*Remarque*. La quantité $\sum_{u=0}^{l-1} h(z + u\alpha)\bar{\chi}(u\alpha)$ est la résolvante considérée par Schertz dans [7]. Il est à noter que cette résolvante dépend du modèle choisi de la courbe $E$, tandis que $\mathscr{R}(z)$ ne dépend pas de ce modèle.

Grâce au lemme 3.4 on peut choisir un représentant de $\alpha$ modulo $\Lambda$ qu'on note aussi $\alpha$ de façon que $l\alpha = n_1\psi + n_2\beta$ avec $(n_1, n_2) = 1$. On fixe $(u_0, v_0) \in \mathbb{Z} \times \mathbb{Z}$ tel que $u_0 n_2 - v_0 n_1 = 1$ et l'on pose $\beta_2 = u_0\psi + v_0\beta_1$. On sait que $\{\beta_2, \alpha\}$ (resp. $\{\beta_2, l\alpha\}$) est une base de $\Sigma$ (resp. $\Lambda$).

On désigne par $a$ et $b$ des entiers tels que:

$$e_l(\gamma, \alpha) = e^{2\pi i a/l},$$
$$\omega_\Omega(\varphi, \psi) = e^{2\pi i b/p}.$$

On déduit alors de la proposition 3.2:

$$\begin{aligned} \mathscr{R}(z + \alpha) &= e^{2\pi i a/l}\mathscr{R}(z) \\ \mathscr{R}(z + \beta_2) &= e^{2\pi i b u_0/p}\mathscr{R}(z). \end{aligned} \tag{3}$$

On considère une nouvelle fonction qu'on définit par

$$T(z) = e^{2\pi i(a/\alpha l)z} \frac{\vartheta\left(lz + \delta \middle| \begin{matrix} l\beta_2 \\ l\alpha \end{matrix}\right)}{\vartheta\left(lz \middle| \begin{matrix} l\beta_2 \\ l\alpha \end{matrix}\right)} \tag{4}$$

où $\delta = -bu_0(\alpha l/p) + a\beta_2$.

On remarque que $T$ satisfait les propriétés (3), donc la fonction $\mathscr{R}/T$ est elliptique pour $\Sigma$ et ne peut avoir qu'un pôle en $z \equiv -(\delta/l) \pmod{\Sigma}$ qui est simple. Cette fonction est donc une constante. Soit $C \in \mathbb{C}^*$ tel que

$$\mathscr{R} = CT. \tag{5}$$

On pose $z_0 = -\delta/l$, $w_0 = lpz_0$. La condition $(l, p) = 1$ implique que la fonction $\mathscr{R}$ elliptique pour $\Omega$ est de valence $lp$. On déduit de (4) le diviseur de $T$ qui est aussi grâce à (5) celui de $\mathscr{R}$.

PROPOSITION 3.7.

$$(\mathscr{R}) = \sum_{\substack{0\le i\le p-1\\ 0\le u\le l-1}} \left(\left(-\frac{\delta}{l} + i\psi + u\alpha\right) - (i\psi + u\alpha)\right)$$

*avec* $\delta = -bu_0(\alpha l/p) + a\beta_2$.

On exprime maintenant la fonction $\mathscr{R}$ à l'aide de la fonction $\sigma(z) = \sigma(z|_{\omega_2}^{\omega_1})$.

PROPOSITION 3.8. *La fonction $\mathscr{R}$ s'exprime comme le produit*:

$$\mathscr{R}(z) = e^{z\eta(w_0) - \lambda\eta(p\varphi)} \prod_{i=0}^{p-1} \frac{\sigma(\lambda + i\psi)\sigma(-\varphi + i\psi)}{\sigma(\lambda - \varphi + i\psi)\sigma(i\psi)}$$
$$\times \prod_{\substack{0\le i\le p-1\\ 0\le u\le l-1}} \frac{\sigma(i\psi + u\alpha)\sigma(z - z_0 + i\psi + u\alpha)}{\sigma(-z_0 + i\psi + u\alpha)\sigma(z + i\psi + u\alpha)},$$

*où, par convention, chaque facteur du produit qui donne $\sigma(0)$ est remplacé par* 1.

De la proposition 3.7 on déduit la décomposition de $\mathscr{R}$ en produit de fonctions $\sigma$ pour le réseau $\Omega$

$$\mathscr{R}(z) = A\frac{\sigma(z - z_0)}{\sigma(z - w_0)} \prod_{i,u} \frac{\sigma(z - z_0 + i\psi + u\alpha)}{\sigma(z + i\psi + u\alpha)}, \tag{6}$$

où $(i, u)$ parcourt l'ensemble

$$\{0, 1, \ldots, p-1\} \times \{0, 1, \ldots, l-1\} \setminus \{0, 0\}$$

et $A$ est une constante à déterminer. Pour cela nous étudions la limite de $\sigma(z - w_0)\mathscr{R}(z)$ lorsque $z \to w_0$. On déduit immédiatement des propriétés des fonctions $\sigma$ et $\eta$, [3, III], l'égalité

$$\lim_{z\to w_0} \sigma(z - w_0)\mathscr{R}(z) = Ae^{-(w_0/2)\eta(w_0)}\sigma(-z_0) \prod \frac{\sigma(i\psi + u\alpha - z_0)}{\sigma(i\psi + u\alpha)}. \tag{7}$$

On veut maintenant calculer cette limite en revenant à la définition de $\mathscr{R}$. Puisque $\mathscr{R}$ ne dépend pas du choix de la fonction $D$ satisfaisant (3.1), nous choisissons

$$D(z, \varphi, \psi) = \frac{\sigma(z - \varphi)}{\sigma(z - p\varphi)} \prod_{i=1}^{p-1} \frac{\sigma(z - \varphi + i\psi)}{\sigma(z + i\psi)}.$$

On obtient alors

$$\lim_{z\to w_0}\sigma(z-w_0)\mathscr{R}(z)=\lim_{z\to w_0}\sigma(z-w_0)\frac{D(z)}{D(\lambda)},$$

d'où l'on déduit

$$\lim_{z\to w_0}\sigma(z-w_0)\mathscr{R}(z)=e^{-(p\varphi/2)\eta(p\varphi)}\frac{\sigma(-\varphi)}{D(\lambda)}\prod_{i=1}^{p-1}\frac{\sigma(-\varphi+i\psi)}{\sigma(i\psi)}. \quad (8)$$

La proposition 3.8 est alors une conséquence de (6), (7) et (8).

Comme la fonction $\varphi$ de Klein fournit par une spécialisation "convenable" des entiers algébriques, il est naturel d'exprimer $\mathscr{R}(\alpha,\gamma,\varphi,\lambda)$ comme produit de fonctions de Klein. On rappelle qu'on définit la fonction de Klein par:

$$\varphi\left(z\middle|\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right)=2\pi i e^{-(1/2)zz^*}\sigma\left(z\middle|\begin{matrix}\omega_1\\ \omega_2\end{matrix}\right)\eta^2\left(\frac{\omega_1}{\omega_2}\right)\omega_2^{-1},\qquad \operatorname{Im}\frac{\omega_1}{\omega_2}>0,$$

où

$$z^*=a_1\eta_1+a_2\eta_2 \qquad \text{avec } a_1,a_2\in\mathbb{R} \text{ tels que}$$
$$z=a_1\omega_1+a_2\omega_2.$$

De la définition de $\varphi$ et la proposition 3.8, on déduit le résultat suivant:

THÉORÈME 3.9. *On a l'égalité*:

$$\mathscr{R}(z)^{2lp^2}=F(z)^{2lp^2},$$

*où*

$$F(z)=\prod_{i=0}^{p-1}\frac{\varphi(\lambda+i\psi)\varphi(-\varphi+i\psi)}{\varphi(\lambda-\varphi+i\psi)\varphi(i\psi)}\times\prod_{\substack{0\le i\le p-1\\ 0\le u\le l-1}}\frac{\varphi(i\psi+u\alpha)\varphi(z-z_0+i\psi+u\alpha)}{\varphi(-z_0+i\psi+u\alpha)\varphi(z+i\psi+u\alpha)}.$$

*Par convention, chaque facteur du produit qui donne* $\varphi(0)$ *est remplacé par* 1.

## 4. RÉSOLVANTES LOCALES

Nous nous proposons dans ce paragraphe d'introduire l'analogue $p$-adique des résolvantes considérées dans le paragraphe 2. La décomposi-

tion de ces résolvantes en produits de fonctions thêta qu'on obtient dans le théorème 4.6 est l'analogue $p$-adique de la proposition 3.8. Soient $K$ une extension finie d'un corps $p$-adique et $\overline{K}$ une clôture algébrique de $K$. On note $v_K$ la valuation discrète normalisée de $K$. On considère $q$ un élément de $K$ de valuation strictement positive. Nos références pour ce paragraphe sont chap. III, VI et App. I de [1].

On définit la fonction $\theta$ fondamentale par

$$\theta(w) = (1-w)\prod_{n\geq 1}(1-q^n w)(1-q^n w^{-1}), \qquad w \in \overline{K}^*.$$

Pour tout $m \in \mathbb{Z}$ elle satisfait l'équation

$$\theta(q^m w) = (-1)^m q^{-m(m-1)/2} w^{-m}\theta(w). \tag{9}$$

Si $n$ est un entier, $n > 0$, on note $E[n]$ le groupe des points $x$ dans $\overline{K}^*/q^{\mathbb{Z}}$ tels que $x^n = 1$. On fixe un entier $p$, $p > 0$ et $\{\varphi, \psi\}$ une base de $E[p]$ sur $\mathbb{Z}/p\mathbb{Z}$. On considère une fonction $q$-périodique $D$ de diviseur

$$(D(\cdot, \varphi, \psi)) = \sum_{i=0}^{p-1}\big((\varphi\psi^i) - (\psi^i)\big). \tag{10}$$

Si l'on fixe de représentants dans $\overline{K}^*$ de cette base, qu'on note encore $\{\varphi, \psi\}$, on sait qu'à constante multiplicative non nulle près on a l'égalité

$$D(z, \varphi, \psi) = \frac{\theta(z\varphi^{-1})}{\theta(z\varphi^{-p})}\prod_{i=1}^{p-1}\frac{\theta(z\psi^i\varphi^{-1})}{\theta(z\psi^i)}. \tag{11}$$

Soit $l$ un entier, $l > 0$ tel que $(l, p) = 1$. On suppose $l$ premier à la caractéristique résiduelle de $K$. On fixe une base $\{\alpha, \gamma\}$ de $E[l]$ sur $\mathbb{Z}/l\mathbb{Z}$ et $\lambda \in E[p^2]$ tel que $\lambda^p = \psi$.

DÉFINITION 4.1. On définit la résolvante

$$\mathscr{R}(\alpha, \gamma, \varphi, \lambda) = D(\lambda, \varphi, \psi)^{-1}\sum_{u=0}^{l-1} D(\gamma\alpha^u, \varphi, \psi)e_l(\gamma, \alpha^u)^{-1},$$

où $e_l$ est l'accouplement de Weil sur les points de $l$-division de $\overline{K}^*/q^{\mathbb{Z}}$.

Pour étudier cette quantité on introduit la fonction $q$-périodique $\mathscr{R}$ où

$$\mathscr{R}(z) = \mathscr{R}(z, \alpha, \gamma, \varphi, \lambda) = D(\lambda, \varphi, \psi)^{-1}\sum_{u=0}^{l-1} D(z\alpha^u, \varphi, \psi)e_l(\gamma, \alpha^u)^{-1}.$$

De la définition de la fonction $\mathscr{R}$ et de (9) on déduit

PROPOSITION 4.2. (i) *Soit* $s$ (*resp.* $t$) *l'entier défini par* $\varphi^p = q^s$ (*resp.* $\psi^p = q^t$), *on a alors*:

$$\mathscr{R}(z\psi) = \varphi^t \psi^{-s} \mathscr{R}(z).$$

(ii)

$$\mathscr{R}(z\alpha) = e_l(\gamma, \alpha)\mathscr{R}(z).$$

*Remarque* 4.3. Soit $n$ un entier, $n \geq 1$, et $q^{1/n}$ (resp. $\zeta_n$) une racine $n$-ième de $q$ dans $\overline{K}$ (resp. primitive $n$-ième de 1) fixée. Soient $x$ et $y$ des éléments de $E[n]$ respectivements représentés par $q^{a/n}\zeta_n^b, q^{c/n}\zeta_n^d$. On peut vérifier l'égalité suivante [1, Chap. II, lemme 3.1]

$$e_n(x, y) = \zeta_n^{ad-bc}.$$

C'est une généralisation de [3, lemme 3-18].

On veut factoriser la fonction $\mathscr{R}(z)$ en produit de fonctions thêta. On introduit pour cela des fonctions auxilliaires. On fixe des représentants de la base $\{\alpha, \gamma\}$ de $E[l]$ qu'on note encore $\alpha$ et $\gamma$. A tout point non nul de $lp$-division, $z_0$, on associe la fonction

$$T_{z_0}(z) = \frac{\theta\left(zz_0^{-1}\right)}{\theta\left(zz_0^{-lp}\right)} \prod_{j,i}{}' \frac{\theta\left(zz_0^{-1}\psi^i\alpha^j\right)}{\theta\left(z\psi^i\alpha^j\right)}$$

où le couple $(j, i)$ parcourt $\{0, \ldots, l-1\} \times \{0, \ldots, p-1\} \setminus \{(0,0)\}$.

On fixe $\zeta_l$ (resp. $\zeta_p$) une racine primitive $l$-ième (resp. $p$-ième) de 1 et $q^{1/l}$ (resp. $q^{1/p}$) une racine $P$-ième (resp. $p$-ième) de $q$ dans $\overline{K}$. On peut écrire $\alpha = q^{m_1/l}\zeta_l^{m_2}$ et $\psi = q^{s_1/p}\zeta_p^{s_2}$ où $s_1 = t$ et $m_1$ et $m_2$ (resp. $s_1$ et $s_2$) sont des entiers non tous deux divisibles par $l$ (resp. $p$).

DÉFINITION 4.4. On associe à $\{\alpha, \gamma\}$ et $\{\varphi, \psi\}$ les entiers $a = a(\alpha, \gamma)$ et $b = b(\varphi, \psi)$ définis par

$$e_l(\gamma, \alpha) = \zeta_l^a, \qquad 0 \leq a \leq l-1,$$
$$\varphi^t\psi^{-s} = \zeta_p^b, \qquad 0 \leq b \leq p-1.$$

Il existe des entiers $a_1$ et $a_2$ qui satisfont le système d'équations suivant:

$$\begin{aligned} -m_2a_1 + m_1a_2 &\equiv a(\alpha, \gamma) \pmod{l} \\ -s_2a_1 + s_1a_2 &\equiv b(\varphi, \psi) \pmod{p}. \end{aligned} \tag{12}$$

Puisque $(l, p) = 1$ on peut choisir une racine primitive $lp$-ième de 1 et une racine $lp$-ième de $q$ de façon que

$$\zeta_{lp}^p = \zeta_l, \qquad \zeta_{lp}^l = \zeta_p, \qquad \left(q^{1/lp}\right)^l = q^{1/p}, \qquad \left(q^{1/lp}\right)^p = q^{1/l}.$$

On pose

$$z_0 = q^{a_1/lp}\zeta_{lp}^{a_2}, \qquad a_1, a_2 \in \mathbb{Z}.$$

PROPOSITION 4.5. (i) $T_{z_0}(z\alpha) = \varphi^t\psi^{-s}T_{z_0}(z)$

(ii) $T_{z_0}(z\psi) = e_l(\gamma, \alpha)T_{z_0}(z)$.

Ces égalités se déduisent immédiatement de (9) et de la remarque (4.3).

THÉORÈME 4.6. *La fonction $\mathscr{R}$ satisfait l'égalité*

$$\mathscr{R}(z) = \lambda^s z^{-a_1} \prod_{i=0}^{p-1} \frac{\theta(\lambda\psi^i)\theta(\psi^i\varphi^{-1})}{\theta(\lambda\psi^i\varphi^{-1})\theta(\psi^i)} \times \prod_{\substack{0\le i\le p-1\\ 0\le u\le l-1}} \frac{\theta(\psi^i\alpha^u)\theta(zz_0^{-1}\psi^i\alpha^u)}{\theta(z_0^{-1}\psi^i\alpha^u)\theta(z\psi^i\alpha^u)},$$

*où, par convention, chaque facteur du produit qui donne $\theta(1)$ est remplacé par* 1.

On déduit des propositions 4.2 et 4.5 que $\mathscr{R}/T_{z_0}$ est une fonction méromorphe sur $\overline{K}^*$ de valence inférieure ou égale à 1 comme fonction de $\overline{K}^*/q^{\mathbb{Z}}\alpha^{\mathbb{Z}}\psi^{\mathbb{Z}}$. Comme dans le cas complexe on déduit de [1, lemme 3-14] que

$$\mathscr{R} = C \cdot T_{z_0}.$$

Pour calculer $C$ on multiplie les deux membres de cette égalité par $\theta(zz_0^{-lp})$ et on fait tendre $z$ vers $z_0^{lp}$. Le calcul, analogue à celui de la proposition 3.8, est laissé au lecteur.

*Remarque* 4.7. Il est important pour la suite de notre étude de remarquer qu'on ne change pas la valeur de $\mathscr{R}(\alpha, \gamma, \varphi, \lambda)$ en remplaçant $\alpha$ ou $\psi$ par tout autre générateur du sous-groupe qu'il engendre dans $\overline{K}^*/q^{\mathbb{Z}}$. On remarque également les égalités

$$\mathscr{R}(\alpha, \gamma\alpha^u, \varphi\psi^v, \lambda) = \mathscr{R}(\alpha, \gamma, \varphi, \lambda) \qquad \forall u, v \in \mathbb{Z}.$$

Ainsi l'étude dans le cas général de la valuation de $\mathscr{R}(\alpha, \gamma, \varphi, \lambda)$ se ramène lorsque $l$ et $p$ seront premiers à l'étude des cas considérés dans les théorèmes 4.8 et 4.9.

Dans ce paragraphe si $x$ et $y \in \overline{K}^*$ on note $x \sim y$ si $xy^{-1}$ est une unité de $\overline{K}^*$

THÉORÈME 4.8. (i) *Soit $u$ un entier tel que $1 \le u < p^2$ et $(u, p) = 1$. Alors on a*

$$\mathscr{R}\left(q^{1/l}, \zeta_l, \zeta_p, q^{u/p^2}\right) \sim (1 - \zeta_p).$$

(ii) *Soient $s$ et $u$ des nombres entiers tels que* $1 \le s \le p-1$, $(s,p)=1$, $0 \le u < p^2$ *et* $u \equiv 0 \pmod p$. *Alors on a*

$$\mathscr{R}\left(q^{1/l}, \zeta_l, q^{s/p}, \zeta_{p^2} q^{u/p^2}\right) \sim M(u,s) q^{su/p^2 - \inf(s,u/p)}$$

*avec*

$$M(u,s) = \begin{cases} 1 & \text{si } u \neq 0,\ u \neq ps, \\ (1-\zeta_p) & \text{si } u = 0, \\ (1-\zeta_p)^{-1} & \text{si } u = ps. \end{cases}$$

On s'intéresse maintenant au cas où $\alpha$ est une unité. Si $x \in \mathbb{Q}$ on note $\{x\}$ sa partie fractionnaire. Enfin on rappelle que l'entier $n_p$ et les rationnels $\beta(n)$, $\gamma(n)$ et $\alpha(n,s)$ sont définis dans l'introduction.

THÉORÈME 4.9. (i) *Soient $n$ et $u$ des nombres entiers tels que* $1 \le n \le l-1$, $(n,1)=1$, $1 \le u < p^2$ *et* $(u,p)=1$. *Alors on a*:

$$\mathscr{R}\left(\zeta_l, q^{n/l}, \zeta_p, q^{u/p^2}\right) \sim (1-\zeta_p) q^{\beta(n)}$$

(ii) *Soient $n$, $s$ et $u$ des nombres entiers tels que* $1 \le n \le l-1$, $(n,l)=1$, $1 \le s \le p-1$, $(s,p)=1$, $0 \le u < p^2$ *et* $u \equiv 0 \pmod p$. *Alors on a*:

$$\mathscr{R}\left(\zeta_l, q^{n/l}, q^{s/p}, \zeta_{p^2} q^{u/p^2}\right) \sim M(u,s) q^{su/p^2 - \inf(s,u/p) + \alpha(n,s)}$$

*où $M(u,s)$ est défini dans le théorème* 4.8.

Les démonstrations de ces théorèmes sont données dans l'appendice. On suppose dorénavant que $l$ et $p$ sont des nombres premiers distincts.

DÉFINITION 4.10.

$$\tilde{T}(\alpha,\gamma) = p^{-(p^4-p^3)} \prod_{\lambda \in E'[p^2]} \prod_{\varphi_\lambda \in E''_\lambda[p]} \mathscr{R}(\alpha, \gamma, \varphi_\lambda, \lambda)$$

où $E'[p^2]$ est l'ensemble des points primitifs de $p^2$-division de $\overline{K}^*/q^{\mathbb{Z}}$ et $E''_\lambda[p]$ désigne un système de représentants non nuls de $E[p]/\langle p\lambda \rangle$.

PROPOSITION 4.11. (i) *Pour tout entier $m$,* $1 \le m \le l-1$, *on a*

$$\tilde{T}\left(q^{m/l}, \zeta_l\right) \sim q^{-n_p},$$

(ii) *Soit $n$ un entier, $1 \le n \le l-1$, alors on a*

$$\tilde{T}\left(\zeta_l, q^{n/l}\right) \sim q^{-n_p+(p^3-p^2)\gamma(n)}.$$

On désigne par $E_1'[p^2]$ (resp. $E_2'[p^2]$) l'ensemble des $\lambda \in E'[p^2]$ tels que $\lambda^{p^2} = q^u$ avec $0 \le u \le p^2-1$ et $u \equiv 0 \pmod p$ (resp. $u \not\equiv 0 \pmod p$). On associe à cette partition de $E'[p^2]$ une décomposition de $p^{(p^4-p^3)}\tilde{T}(\alpha,\gamma)$ en produit

$$T_1(\alpha,\gamma)\cdot T_2(\alpha,\gamma)$$

avec

$$T_1(\alpha,\gamma) = \prod_{\substack{0\le u<p\\ 0\le x<p^2\\ (x,p)=1}} \prod_{1\le s\le p-1} \mathscr{R}\left(\alpha,\gamma,q^{s/p},\zeta_{p^2}^x q^{u/p}\right)$$

$$T_2(\alpha,\gamma) = \prod_{\substack{0\le u<p^2\\ 0\le x<p^2\\ (u,p)=1}} \prod_{1\le s\le p-1} \mathscr{R}\left(\alpha,\gamma,\zeta_p^s,\zeta_{p^2}^x q^{u/p^2}\right).$$

On déduit du théorème 4.8(i) et (ii)

$$T_2\left(q^{m/l},\zeta_l\right) \sim p^{(p^4-p^3)}$$

$$T_1\left(q^{m/l},\zeta_l\right) \sim q^{(p^2-p)v}$$

où

$$v = \sum_{\substack{1\le s<p\\ 1\le u<p}} \left(s\frac{u}{p} - \inf(s,u)\right)$$

on vérifie immédiatement les égalités

$$\begin{aligned} \sum_{\substack{1\le s<p\\ 1\le u<p}} s\frac{u}{p} &= \frac{p(p-1)^2}{4}, \\ \sum_{\substack{1\le s<p\\ 1\le u<p}} \inf(s,u) &= \frac{1}{6}p(p-1)(2p-1), \end{aligned} \tag{13}$$

d'où l'on déduit $v = -p(p-1)(p+1)/12$, ce qui démontre (i). On déduit (ii) du théorème 4.9(i) et (ii) et de (13).

## 5. SOMMES ARITHMÉTIQUES

Ce paragraphe contient la démonstration du théorème 1.3. Pour cela on fixe deux entiers $l$ et $p$ qui vérifient $(l, p(p+1)) = 1$. Il s'agit de déterminer les sommes

$$\sum_{n=1}^{l-1} \beta(n) \qquad \text{et} \qquad \sum_{n=1}^{l-1} \sum_{s=1}^{p-1} \alpha(n, s)$$

qui proviennent des valuations des résolvantes $\mathscr{R}(\alpha, \gamma, \varphi, \lambda)$ dans le cas local. La stratégie de la démonstration est d'utiliser d'une part le théorème 3.9 qui est l'analogue complexe du théorème 4.6 et d'autre part les propriétés des fonctions $\varphi$ de Siegel. Notre référence pour ce paragraphe est [6, chap. 2, paragraphe 4].

Pour $\tau \in \mathbb{C}$, $\operatorname{Im} \tau > 0$, nous notons $\Omega_\tau$ le réseau $\mathbb{Z}\tau + \mathbb{Z}$. Soit $n$ un entier, $n \geq 1$, on note $S_n$ l'anneau des séries formelles de Laurent $\mathbb{Q}(\zeta_n)((q_\tau^{1/n}))$ où $q_\tau = e^{2\pi i \tau}$. Si $f$ et $g$ sont des éléments de cet anneau on note $f \sim g$ lorsque $f = gh$ où $h = \sum_{k=0}^{\infty} c_k q_\tau^{k/n}$ avec $c_k \in \mathbb{Q}(\zeta_n)$ $\forall k \geq 0$ et $c_0 \neq 0$.

On rappelle les $q_\tau$-développements des fonctions $\varphi$ et $\Delta$:

$$\Delta\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \left(\frac{2\pi i}{\omega_2}\right)^{12} q_\omega \prod_{n=1}^{\infty} (1 - q_\omega^n)^{24}, \qquad q_\omega = e^{2\pi i \omega}, \tag{14}$$

où $\omega = \omega_1/\omega_2$ tel que $\operatorname{Im} \omega > 0$. Pour tout $a_1, a_2 \in \mathbb{Q}$ on a:

$$\varphi\left(a_1\tau + a_2 \middle|_1^\tau\right) = -q_\tau^{(1/2)B_2(a_1)} e^{2\pi i a_2 (a_1 - 1)/2} \left(1 - q_\tau^{a_1} e^{2\pi i a_2}\right) \prod_{n=1}^{\infty} \left(1 - q_\tau^{n + a_1} e^{2\pi i a_2}\right)\left(1 - q_\tau^{n - a_1} e^{-2\pi i a_2}\right) \tag{15}$$

où $B_2(X) = X^2 - X + 1/6$ et $q_\tau = e^{2\pi i \tau}$. On vérifie facilement que

$$\varphi^{12n}\left(a_1\tau + a_2 \middle| \begin{matrix} \tau \\ 1 \end{matrix}\right) \sim \varphi^{12n}\left(a_1\tau \middle| \begin{matrix} \tau \\ 1 \end{matrix}\right) \tag{16}$$

pour tout $(a_1, a_2) \in (1/n)\mathbb{Z}^2$, $a_1 \neq 0$, $n \in \mathbb{N}$.

Démontrons (i). On suppose les éléments $\alpha$, $\gamma$, $\varphi$, $\psi$ et $\lambda$ respectivement représentés modulo $\Omega_\tau$ par

$$\alpha = \frac{1}{l}, \gamma = \frac{n}{l}\tau, \varphi = \frac{1}{p}, \psi = \frac{1}{p}\tau, \lambda = \frac{1}{p^2}\tau.$$

On vérifie que dans ce cas l'élément $z_0$ introduit au paragraphe 3 est égal à

$$z_0 = -\frac{n}{lp}\tau + \frac{1}{lp}.$$

D'après le théorème (3.9) on a

$$\mathscr{R}\left(\frac{1}{l}, \frac{n}{l}\tau, \frac{1}{p}, \frac{1}{p^2}\tau\right)^{12lp^2}$$

$$= \left( \prod_{i=0}^{p-1} \frac{\varphi(\tau/p^2 + (i/p)\tau)\varphi(-1/p + (i/p)\tau)}{\varphi(\tau/p^2 + (i/p)\tau - 1/p)\varphi((i/p)\tau)} \right.$$

$$\left. \times \prod_{\substack{0 \le i \le p-1 \\ 0 \le u \le l-1}} \frac{\varphi((i/p)\tau + u/l) \times \varphi((n/l)\tau + (i/p)\tau + u/l + (n/lp)\tau - 1/lp)}{\varphi((i/p)\tau + u/l + (n/lp)\tau - 1/lp) \times \varphi((n/l)\tau + (i/p)\tau + u/l)} \right)^{12lp^2}. \tag{17}$$

On va appliquer plusieurs fois le théorème 4.1 de [6, chap. 2, paragraphe 4] pour simplifier le produit (17). On a les résultats suivants qui découlent immédiatement de ce théorème:

$$\prod_{i=1}^{p-1} \varphi^{12lp^2}\left(\frac{i}{p}\tau \middle| \begin{matrix}\tau \\ 1\end{matrix}\right) = \left(\frac{\Delta\left(\begin{matrix}\tau/p \\ 1\end{matrix}\right)}{\Delta\left(\begin{matrix}\tau \\ 1\end{matrix}\right)}\right)^{lp^2}, \tag{18}$$

$$\prod_{i=0}^{p-1} \varphi^{12lp^2}\left(\xi + \frac{i}{p}\tau \middle| \begin{matrix}\tau \\ 1\end{matrix}\right) = \varphi^{12lp^2}\left(\xi \middle| \begin{matrix}\tau/p \\ 1\end{matrix}\right) \tag{19}$$

pour tout $\xi \in \mathbb{C} \setminus \Omega_{(1/p)\tau}$ et tel que $lp^2\xi \in \Omega_\tau$,

$$\prod_{(i,u) \neq (0,0)} \varphi^{12lp^2}\left(\frac{i}{p}\tau + \frac{u}{l} \middle| \begin{matrix}\tau \\ 1\end{matrix}\right) = \left(\frac{\Delta\left(\begin{matrix}\tau/p \\ 1/l\end{matrix}\right)}{\Delta\left(\begin{matrix}\tau \\ 1\end{matrix}\right)}\right)^{lp^2}, \tag{20}$$

$$\prod_{\substack{0 \le i \le p-1 \\ 0 \le u \le l-1}} \varphi^{12lp^2}\left(\xi + \frac{i}{p}\tau + \frac{u}{l} \middle| \begin{matrix}\tau \\ 1\end{matrix}\right) = \varphi^{12lp^2}\left(\xi \middle| \begin{matrix}\tau/p \\ 1/l\end{matrix}\right) \tag{21}$$

pour tout $\xi \in \mathbb{C} \setminus (\mathbb{Z}(1/p)\tau + \mathbb{Z}(1/l))$ et tel que $lp^2\xi \in \Omega_\tau$.

De (16), (18), (19), (20) et (21) on obtient:

$$\mathscr{R}\left(\frac{1}{l}, \frac{n}{l}\tau, \frac{1}{p}, \frac{1}{p^2}\tau\right)^{12lp^2}$$

$$\sim \left(\frac{\varphi\left(-1/p \middle| \begin{matrix}\tau/p\\1\end{matrix}\right)\varphi\left((n/l)\tau + (n/lp)\tau \middle| \begin{matrix}\tau/p\\1/l\end{matrix}\right)}{\varphi\left((n/lp)\tau \middle| \begin{matrix}\tau/p\\1/l\end{matrix}\right)\rho\left((n/l)\tau \middle| \begin{matrix}\tau/p\\1/l\end{matrix}\right)}\right)^{12lp^2}$$

$$\times \left(\frac{\Delta\left(\begin{matrix}\tau/p\\1/l\end{matrix}\right)}{\Delta\left(\begin{matrix}\tau/p\\1\end{matrix}\right)}\right)^{lp^2}.$$

Les propriétés d'homogéneité des fonctions $\varphi$ permettent d'écrire l'équivalence suivante

$$\mathscr{R}\left(\frac{1}{l}, \frac{n}{l}\tau, \frac{1}{p}, \frac{1}{p^2}\tau\right)^{12lp^2}$$

$$\sim \left(\frac{\varphi\left(-1/p \middle| \begin{matrix}\tau/p\\1\end{matrix}\right)\varphi\left((p+1)(n/p)\tau \middle| \begin{matrix}l\tau/p\\1\end{matrix}\right)}{\varphi\left((n/p)\tau \middle| \begin{matrix}l\tau/p\\1\end{matrix}\right)\varphi\left(n\tau \middle| \begin{matrix}l\tau/p\\1\end{matrix}\right)}\right)^{12lp^2} \times \left(\frac{\Delta\left(\begin{matrix}\tau/p\\1/l\end{matrix}\right)}{\Delta\left(\begin{matrix}\tau/p\\1\end{matrix}\right)}\right)^{lp^2}.$$

En utilisant le $q_\tau$-développement à l'infini (14) et (15) de $\varphi$ et $\Delta$ on obtient

$$\mathscr{R}\left(\frac{1}{l}, \frac{n}{l}\tau, \frac{1}{p}, \frac{1}{p^2}\tau\right)^{12lp^2} \sim q_\tau^{12lp^2\delta(n)+lp(l-1)}, \tag{22}$$

où

$$\delta(n) = \frac{l}{2p}\left(\frac{1}{6l} + B_2\left(\left\{\frac{np}{l} + \frac{n}{l}\right\}\right) - B_2\left(\left\{\frac{n}{l}\right\}\right) - B_2\left(\left\{\frac{np}{l}\right\}\right)\right).$$

On vérifie que $12lp^2\delta(n) + lp(l-1) = 12lp^2\beta(n)$.

Comme $(p+1)$ et $p$ sont premiers avec $l$ l'ensemble des éléments $(p+1)(n/p)\tau$ (resp. $(n/p)\tau$, resp. $n\tau$), $1 \le n \le l-1$ constitue un système de représentants non triviaux de $\Omega_{(1/p)\tau}/\Omega_{(l/p)\tau}$. On en déduit que

$$\prod_{n=1}^{l-1} \mathscr{R}\left(\frac{1}{l}, \frac{n}{l}\tau, \frac{1}{p}, \frac{1}{p^2}\tau\right)^{12lp^2}$$

$$\sim \varphi\left(-\frac{1}{p}\,\middle|\,\begin{matrix}\tau/p\\ 1\end{matrix}\right)^{12lp^2(l-1)} \left(\frac{\Delta\begin{pmatrix}\tau/p\\ 1/l\end{pmatrix}}{\Delta\begin{pmatrix}\tau/p\\ 1\end{pmatrix}}\right)^{lp^2(l-1)} \left(\frac{\Delta\begin{pmatrix}l\tau/p\\ 1\end{pmatrix}}{\Delta\begin{pmatrix}\tau/p\\ 1\end{pmatrix}}\right)^{lp^2}.$$

On utilise maintenant les $q_\tau$-développements de $\varphi$ et $\Delta$. Un calcul élémentaire nous donne:

$$\prod_{n=1}^{l-1} \mathscr{R}\left(\frac{1}{l}, \frac{n}{l}\tau, \frac{1}{p}, \frac{1}{p^2}\tau\right)^{12lp^2} \sim q_\tau^{lp(l^2-1)}. \tag{23}$$

Le théorème 1.3 (i) se déduit donc de (22) et (23).

Démontrons maintenant (ii). On suppose $\alpha$, $\gamma$, $\varphi$, $\psi$ et $\lambda$ respectivement représentés par

$$\alpha = \frac{1}{l}, \gamma = \frac{n}{l}\tau, \varphi = \frac{s}{p}\tau, \psi = \frac{1}{p}, \lambda = \frac{1}{p^2}.$$

On vérifie que dans ce cas

$$z_0 = \frac{z_1}{lp}\tau \qquad \text{avec } z_1 = lsx + pyn$$

où $x$ et $y$ vérifient $lx - py = 1$. On considère la fonction

$$\mathscr{R}\left(\frac{1}{l}, \frac{n}{l}\tau, \frac{s}{p}\tau, \frac{1}{p^2}\right)^{12lp^2}$$

$$= \left(\prod_{i=0}^{p-1} \frac{\varphi(1/p^2 + i/p)\varphi(-(s/p)\tau + i/p)}{\varphi(1/p^2 + i/p - (s/p)\tau)\varphi(i/p)}\right.$$

$$\left.\times \prod_{\substack{0\le i\le p-1\\ 0\le u\le l-1}} \frac{\varphi(i/p + u/l)\varphi((n/l)\tau + i/p + u/l - (z_1/lp)\tau)}{\varphi(i/p + u/l - z_1/lp)\varphi((n/l)\tau + i/p + u/l)}\right)^{12lp^2}. \tag{24}$$

Comme dans le cas précédent en appliquant plusieurs fois le théorème 4.1 de [6, (2), paragraphe 4] on obtient:

$$\prod_{i=1}^{p-1} \varphi^{12lp^2}\left(\frac{i}{p}\,\middle|\,\tau\right) = \left(\frac{\Delta\begin{pmatrix}\tau\\ 1/p\end{pmatrix}}{\Delta\begin{pmatrix}\tau\\ 1\end{pmatrix}}\right)^{lp^2}, \tag{25}$$

$$\prod_{i=0}^{p-1} \varphi^{12lp^2}\left(\xi+\frac{i}{p}\,\middle|\,\tau\right) = \varphi^{12lp^2}\left(\xi\,\middle|\,\begin{matrix}\tau\\ 1/p\end{matrix}\right) \tag{26}$$

pour tout $\xi \in \mathbb{C} \setminus (\mathbb{Z}\tau + \mathbb{Z}(1/p))$ et tel que $lp^2\xi \in \Omega_\tau$,

$$\prod_{(i,u)\neq(0,0)} \varphi^{12lp^2}\left(\frac{i}{p}+\frac{u}{l}\,\middle|\,\tau\right) = \left(\frac{\Delta\begin{pmatrix}\tau\\ 1/lp\end{pmatrix}}{\Delta\begin{pmatrix}\tau\\ 1\end{pmatrix}}\right)^{lp^2}, \tag{27}$$

$$\prod_{\substack{0\le i\le p-1\\ 0\le u\le l-1}} \varphi^{12lp^2}\left(\xi+\frac{i}{p}+\frac{u}{l}\,\middle|\,\tau\right) = \varphi^{12lp^2}\left(\xi\,\middle|\,\begin{matrix}\tau\\ 1/lp\end{matrix}\right) \tag{28}$$

pour tout $\xi \in \mathbb{C} \setminus (\mathbb{Z}\tau + \mathbb{Z}(1/lp))$ et tel que $lp^2\xi \in \Omega_\tau$.

De (16), (25), (26), (27) et (28) on déduit:

$$\begin{aligned}\mathscr{R}\left(\frac{1}{l},\frac{n}{l}\tau,\frac{s}{p}\tau,\frac{1}{p^2}\right)^{12lp^2} &\sim \left(\frac{\Delta\begin{pmatrix}\tau\\ 1/pl\end{pmatrix}}{\Delta\begin{pmatrix}\tau\\ 1/p\end{pmatrix}}\right)^{lp^2}\\ &\quad\times\left(\frac{\varphi\left(1/p^2\,\middle|\,\begin{matrix}\tau\\ 1/p\end{matrix}\right)\varphi\left((n/l)\tau-(z_1/lp)\tau\,\middle|\,\begin{matrix}\tau\\ 1/lp\end{matrix}\right)}{\varphi\left(-(z_1/lp)\tau\,\middle|\,\begin{matrix}\tau\\ 1/lp\end{matrix}\right)\varphi\left((n/l)\tau\,\middle|\,\begin{matrix}\tau\\ 1/lp\end{matrix}\right)}\right)^{12lp^2}.\end{aligned}$$

Des $q_\tau$-développements de $\varphi$ et $\Delta$ on déduit l'équivalence:

$$\mathscr{R}\left(\frac{1}{l},\frac{n}{l}\tau,\frac{s}{p}\tau,\frac{1}{p^2}\right)^{12lp^2} \sim q_\tau^{12lp^2\omega(n,s)+lp^3(l-1)} \tag{29}$$

où

$$\omega(n,s) = \frac{lp}{2}\left(\frac{1}{6l} + B_2\left(\left\{\frac{n}{l} - \frac{z_1}{pl}\right\}\right) - B_2\left(\left\{-\frac{z_1}{pl}\right\}\right) - B_2\left(\frac{n}{l}\right)\right)$$

et l'on vérifie que $12lp^2\omega(n,s) + lp^3(l-1) = 12lp^2\alpha(n,s)$.

On est donc ramené à démontrer que:

$$\prod_{s=1}^{p-1}\prod_{n=1}^{l-1}\mathscr{R}\left(\frac{1}{l}, \frac{n}{l}\tau, \frac{s}{p}\tau, \frac{1}{p^2}\right)^{12lp^2} \sim q_\tau^{lp^3(p-1)(l^2-1)}.$$

On applique de nouveau le théorème 4.1 de [6]. Compte-tenu de l'homogéneité de la fonction $\varphi$, on trouve:

$$\prod_{s=1}^{p-1}\prod_{n=1}^{l-1}\mathscr{R}\left(\frac{1}{l}, \frac{n}{l}\tau, \frac{s}{p}\tau, \frac{1}{p^2}\right)^{12lp^2}$$

$$\sim \left(\frac{\Delta\begin{pmatrix}\tau\\ 1/lp\end{pmatrix}}{\Delta\begin{pmatrix}\tau\\ 1/p\end{pmatrix}}\right)^{lp^2(l-1)(p-1)} \left(\frac{\Delta\begin{pmatrix}lp\tau\\ 1\end{pmatrix}}{\Delta\begin{pmatrix}p\tau\\ 1\end{pmatrix}}\right)^{lp^2(p-1)} \varphi\left(\frac{1}{p}\middle|\begin{matrix}p\tau\\ 1\end{matrix}\right)^{12lp^2(l-1)(p-1)}$$

$$\times \underbrace{\prod_{s=1}^{p-1}\prod_{n=1}^{l-1}\left(\frac{\varphi\left(pn\tau - z_1\tau\middle|\begin{matrix}lp\tau\\ 1\end{matrix}\right)}{\varphi\left(-z_1\tau\middle|\begin{matrix}lp\tau\\ 1\end{matrix}\right)}\right)^{12lp^2}}_{A(s)}.$$

Nous démontrons que $\prod_{s=1}^{p-1}A(s) \sim 1$. D'après la définition de $z_1$ on a:

$$A(s) = \prod_{n=1}^{l-1}\left(\frac{\varphi\left(n(1-y)p\tau - lxs\tau\middle|\begin{matrix}lp\tau\\ 1\end{matrix}\right)}{\varphi\left(-ynp\tau - lxs\tau\middle|\begin{matrix}lp\tau\\ 1\end{matrix}\right)}\right)^{12lp^2}.$$

Comme $lx - py = 1$ et $(l, p(p+1)) = 1$, on déduit que $(l, y) = (1-y, l) = 1$. Par conséquent, les éléments $n(1-y)$ (resp. $-yn$) parcourent un système de représentants non nuls de $\mathbb{Z}/l\mathbb{Z}$. On conclut que $A(s) = 1$.

On utilise maintenant les $q_\tau$-développements de $\varphi$ et $\Delta$ pour démontrer que

$$\prod_{s=1}^{p-1}\prod_{n=1}^{l-1}\mathscr{R}\left(\frac{1}{l},\frac{n}{l}\tau,\frac{s}{p}\tau,\frac{1}{p^2}\right)^{12lp^2} \sim q_\tau^{lp^3(p-1)(l^2-1)},$$

ce qui termine la démonstration du théorème 1.3.

## 6. DÉMONSTRATION DU THÉORÈME 1.1

On désigne par $\mathscr{S}$ l'ensemble des idéaux premiers de $F$ pour lesquels la courbe $(E/F)$ a mauvaise réduction ou qui divisent $l$. Pour démontrer le théorème 1.1 on doit déterminer la valuation des résolvantes $\tilde{T}(P,Q)$ en tout idéal premier. Cette étude se décompose en deux parties suivant que l'idéal considéré relève ou ne relève pas un élément de $\mathscr{S}$.

### A. *Etude aux places de bonne réduction*

On exprime $\tilde{T}(P,Q)$ comme valeur de fonction modulaire et on utilise le principe du "$q$-développement". On fixe un modèle de Weierstrass de $E$, défini sur $F$, associé à un réseau $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ de $\mathbb{C}$ où $\tau = \omega_1/\omega_2 \in \mathscr{H}$. Si $\wp$ désigne la fonction de Weierstrass de $\Omega$ on considère l'isomorphisme de variétés complexes:

$$\begin{aligned} \mathbb{C}/\Omega &\mapsto E(\mathbb{C}) \\ z &\mapsto (\wp(z),\wp'(z)) \qquad \text{si } z \notin \Omega \\ z &\mapsto 0 \qquad \text{si } z \in \Omega. \end{aligned} \tag{30}$$

Le point $M$ de $E(\mathbb{C})$ de coordonnées $(\wp(z),\wp'(z))$ est dit de paramètre $z$. Pour tout entier $n$, $n \geq 1$, on identifie via (30) les groupes $E[n]$ et $(1/n)\Omega/\Omega$. Soit $\alpha$ (resp. $\gamma$) un paramètre de $P$ (resp. $Q$). Alors $\tilde{T}(P,Q)$ s'exprime à l'aide des résolvantes introduites en (1), paragraphe 3, par l'égalité

$$\tilde{T}(\alpha,\gamma) = p^{-(p^4-p^3)} \prod_{\lambda \in E'[p^2]} \prod_{\varphi_\lambda \in E''_\lambda[p]} \mathscr{R}(\alpha,\gamma,\varphi_\lambda,\lambda). \tag{31}$$

Les notations et les choix des éléments $\alpha, \gamma, \varphi, \psi, \lambda$ sont dorénavant ceux précisés au paragraphe 3. Nous utilisons le lemme suivant

LEMME 6.1. *Pour tout couple* $(i,u)$, $0 \leq i \leq p-1$, $0 \leq u \leq l-1$, *les nombres complexes* $\gamma - z_0 + i\psi + u\alpha$ *et* $-z_0 + i\psi + u\alpha$ *sont des paramètres de points de* $E[pl] \setminus E[p]$.

On rappelle les définitions et les choix du paragraphe 3.

On a $\Lambda = \Omega + \mathbb{Z}\psi$, $\Sigma = \Lambda + \mathbb{Z}\alpha$. En outre $\psi$, $\alpha$, $\beta_1$, $\beta_2$ ont été choisis de manière que:

$$\Omega = \mathbb{Z}\beta_1 + \mathbb{Z}(p\psi),\ \Lambda = \mathbb{Z}\beta_1 + \mathbb{Z}\psi = \mathbb{Z}\beta_2 + \mathbb{Z}(l\alpha),\ \Sigma = \mathbb{Z}\beta_2 + \mathbb{Z}\alpha. \tag{32}$$

Puisque $\beta_2 \in \Lambda - \Omega$ on peut écrire $\beta_2 = v_0\beta_1 + u_0\psi$, avec $(p, u_o) = 1$. On déduit facilement des égalités précédentes

$$\Omega = \mathbb{Z}(p\beta_2) + \mathbb{Z}(l\alpha). \tag{33}$$

On a posé

$$z_0 = bu_0\frac{\alpha}{p} - a\frac{\beta_2}{l}, \tag{34}$$

où $a$ et $b$ satisfont

$$e_l(\gamma, \alpha) = e^{2i\pi(a/l)}, \qquad \omega_\Omega(\varphi, \psi) = e^{2i\pi(b/l)}, \qquad (a, l) = (b, p) = 1.$$

Puisque $(bu_0, p) = (a, l) = 1$ on déduit de (33) et de (34) que $z_0$ est le paramètre d'un point primitif de $lp$-division. Puisque $\{p(\beta_2/l), \alpha\}$ est une base sur $\mathbb{F}_l$ de $E[l]$ on peut écrire

$$\gamma = x_0\frac{p\beta_2}{l} + y_0\alpha, \tag{35}$$

où $x_0, y_0 \in \mathbb{Z}$ et $(x_0, l) = 1$. On obtient alors l'égalité $e_l(\gamma, \alpha) = e^{(2i\pi/l)x_0}$, [1, I, proposition 1-3], d'où l'on déduit que $a \equiv x_0 \pmod{l}$. Supposons qu'il existe $u$, $0 \le u \le l - 1$, tel que

$$p(\gamma - z_0) - u\alpha \equiv 0 \qquad (\mathrm{mod}\ \Omega).$$

On déduit de (34) et (35) que

$$\left(\frac{a + x_0p}{l}\right)(p\beta_2) + \left(\frac{py_0 - bu_0 - u}{l}\right)(l\alpha) \in \Omega,$$

i.e., $(a + x_0p) \equiv 0 \pmod{l}$ et $(py_0 - bu_0 - u) \equiv 0 \pmod{l}$.

La première congruence est équivalente à

$$x_0(p + 1) \equiv 0 \qquad (\mathrm{mod}\ l).$$

Ce qui est impossible puisque $(l, p) = (l, p + 1) = 1$. On démontre ainsi que $\gamma - z_0 + i\psi + u\alpha$ définit un élément de $E[pl] \setminus E[p]$. On démontre de la même manière la propriété souhaitée pour $-z_0 + i\psi + u\alpha$.

On veut maintenant exprimer $\mathscr{R}(\alpha, \gamma, \varphi, \lambda)$ comme valeur de fonction modulaire. On fixe $a$ (resp. $c$, resp. $d$, resp. $r$, resp. $s$, resp. $t$) appartenant à $(1/l)\mathbb{Z}^2$ (resp. $(1/l)\mathbb{Z}^2$, resp. $(1/pl)\mathbb{Z}^2$, resp. $(1/p)\mathbb{Z}^2$, resp. $(1/p)\mathbb{Z}^2$, resp. $(1/p^2)\mathbb{Z}^2$) tels que $\alpha/\omega_2 = a\tau$ (resp. $\gamma/\omega_2 = c\tau$, resp. $z_0/\omega_2 = d\tau$, resp. $\varphi/\omega_2 = r\tau$, resp. $\psi/\omega_2 = s\tau$, resp. $\lambda/\omega_2 = t\tau$) où, lorsque $x = (x_1, x_2) \in \mathbb{Q}^2$ on note $x\tau$ l'élément $x_1\tau + x_2$ de $\mathbb{C}$. Pour tout $x \in \mathbb{Q}^2 - \mathbb{Z}^2$ on définit la fonction $\varphi(x)$ par

$$\begin{aligned} \mathscr{H} &\mapsto \mathbb{C} \\ \omega &\mapsto \varphi\left(x\omega \middle| \begin{matrix}\omega \\ 1\end{matrix}\right). \end{aligned}$$

On rappelle la convention $\varphi(x) = 1$ si $x \in \mathbb{Z}^2$. On pose

$$G(a,c,r,t) = \prod_{i=0}^{p-1} \frac{\varphi(t+is)\,\varphi(-r+is)}{\varphi(t-r+is)\,\varphi(is)} \prod_{\substack{0\le i\le p-1 \\ 0\le u\le l-1}} \frac{\varphi(is+ua)\,\varphi(c-d+is+ua)}{\varphi(-d+is+ua)\,\varphi(c+is+ua)}. \quad (36)$$

Le théorème 3.9 fournit l'égalité

$$\mathscr{R}^m(\alpha,\gamma,\varphi,\lambda) = G^m(a,c,r,t)(\tau), \qquad m = 12lp^2. \quad (37)$$

On utilise maintenant la terminologie et les résultats de [6, II, paragraphe 2]. Si $n$ est un entier, $n \geq 1$, on désigne par $F_n$ le corps des fonctions modulaires de niveau $n$ dont les coefficients de Fourier aux pointes appartiennent à $\mathbb{Q}(\xi_n)$. On désigne par $R_n$ la clôture intégrale de $\mathbb{Z}[j]$ dans $F_n$. Le théorème 2.2 de [6, II] implique que $G(a,c,r,t)$ est une unité de $R_{lp^2}[1/l, 1/p]$.

DÉFINITION 6.2. Soient $f$ et $g$ des éléments de $F_{lp^2}$ on note $f \sim g$ lorsque $fg^{-1}$ est une unité de $R_{lp^2}[1/l]$.

PROPOSITION 6.3. *On a l'équivalence*

$$G^m(a,c,r,t) \sim \prod_{i=0}^{p-1} \left(\frac{\varphi(t+is)\,\varphi(-r+is)}{\varphi(t-r+is)}\right)^m.$$

On sait grâce au lemme 6.1 que pour tout couple $(i,u)$, les éléments de $(1/p^2l)\mathbb{Z}^2$, $c-d+is+ua$, $-d+is+ua$ et $c+is+ua$ sont d'ordre composite ou égal à $l$ modulo $\mathbb{Z}^2$. Le théorème 2.2, de [6, II], affirme alors

que les fonctions $\varphi$ associées sont des unités de $R_{lp^2}[1/l]$. Ce même théorème implique

$$\prod_{\substack{0\le i\le p-1\\ 0\le u\le l-1}} \varphi(is+ua) \sim \prod_{i=0}^{p-1} \varphi(is).$$

Ce qui permet de conclure.

Soit $\mathscr{E}'[p^2]$ un système de représentants dans $(1/p^2)\mathbb{Z}^2$ des points d'ordre $p^2$ du groupe $(\mathbb{Q}/\mathbb{Z})^2$. Pour tout $t \in \mathscr{E}'[p^2]$ on considère le quotient du groupe $(1/p)\mathbb{Z}^2/\mathbb{Z}^2$ par le sous-groupe engendré par l'image de $pt$. On note $\mathscr{E}_t''[p]$ un système de représentants des éléments non nuls de ce groupe.

PROPOSITION 6.4. *On a l'équivalence*

$$\prod_{t\in\mathscr{E}'[p^2]} \prod_{r\in\mathscr{E}_t''[p]} G^m(a,c,r,t) \sim p^{m(p^4-p^3)}.$$

Désignons par $F$ le membre de gauche. La proposition 6.3 nous donne l'équivalence

$$F \sim \prod_{t\in\mathscr{E}'[p^2]} \prod_{r\in\mathscr{E}_t''[p]} \prod_{i=0}^{p-1} \left( \frac{\varphi(t+is)\,\varphi(-r+is)}{\varphi(t-r+is)} \right)^m. \tag{38}$$

On vérifie facilement les égalités

$$\prod_{t\in\mathscr{E}'[p^2]} \prod_{r\in\mathscr{E}_t''[p]} \prod_{i=0}^{p-1} \varphi(t+is) = \prod_{t\in\mathscr{E}'[p^2]} \prod_{r\in\mathscr{E}_t''[p]} \prod_{i=0}^{p-1} \varphi(t-r+is) \tag{39}$$

$$\sim \prod_{t\in\mathscr{E}'[p^2]} \varphi^{p^2}(t). \tag{40}$$

On déduit de (39) et (40)

$$F \sim \prod_{t\in\mathscr{E}'[p^2]} \prod_{r\in\mathscr{E}_t''[p]} \prod_{i=0}^{p-1} \varphi^m(-r+is). \tag{41}$$

Si $\mathscr{E}'[p]$ désigne un système de représentants dans $(1/p)\mathbb{Z}^2$ des points d'ordre $p$ de $(\mathbb{Q}/\mathbb{Z})^2$, on obtient de (41)

$$F \sim \left( \prod_{v\in\mathscr{E}'[p]} \varphi^m(v) \right)^{(p^4-p^3)}. \tag{42}$$

Pour tout $\omega$ de $\mathscr{H}$ notons $\Omega_\omega$ le réseau $\mathbb{Z}\omega + \mathbb{Z}$. Le théorème 4.1 de [6, II] nous fournit l'égalité

$$\prod_{v \in \mathscr{E}'[p]} \varphi^{12p}(v) = \left( \frac{\Delta((1/p)\Omega_\omega)}{\Delta(\Omega_\omega)} \right)^p = p^{12p}. \tag{43}$$

La proposition s'obtient alors à partir de (41) et (42).

PROPOSITION 6.5. *$\tilde{T}(P, Q)$ est une $\mathscr{S}$-unité.*

Grâce à (37) et la proposition 6.4 on sait qu'il existe une unité $H$ de $R_{lp^2}[1/l]$ telle que

$$\tilde{T}^m(P, Q) = H(\tau).$$

Soit $\mathfrak{P}$ un relèvement premier dans $N$ d'un idéal premier $\mathfrak{p}$ de $F$, $\mathfrak{p} \notin \mathscr{S}$. Puisque $v_\mathfrak{p}(j(\tau)) \geq 0$, le principe du $q$-développement implique que

$$v_\mathfrak{P}\left(\tilde{T}^m(P, Q)\right) = 0.$$

B. *Etude aux places de mauvaise réduction*

Soit $\mathfrak{p}$ un idéal premier de $F$, de caractéristique résduelle $t \neq l$, en lequel la courbe $E/F$ a mauvaise réduction. On pose $r_\mathfrak{p} = -v_\mathfrak{p}(j(E))$. On rappelle que $N = F(\xi_l + \xi_l^{-1})$.

PROPOSITION 6.6. (i) *Si $\mathfrak{p} \notin \mathfrak{N}(E, P)$, on a*

$$v_\mathfrak{P}\left(\tilde{T}^l(P, Q)\right) = -ln_p r_\mathfrak{p}.$$

*pour tout relèvement premier $\mathfrak{P}$ de $\mathfrak{p}$ dans $N$.*

(ii) *Si $\mathfrak{p} \in \mathfrak{N}(E, P)$ il existe un relèvement premier $\mathfrak{P}$ de $\mathfrak{p}$ dans $N$ tel qu'on ait*

$$v_{\mathfrak{P}\sigma_t^{-1}}\left(\tilde{T}^l(P, Q)\right) = lr_\mathfrak{p}\left((p^3 - p^2)\gamma(t) - n_p\right), \qquad 1 \leq t \leq \frac{l-1}{2}.$$

Les résultats de cette proposition se déduisent de la proposition 4.11 suivant la méthode développée dans [4, paragraphe V, démonstration du théorème 6.1].

Nous la rappelons brièvement. On fixe un plongement $h$ de $\overline{\mathbb{Q}}$ dans $\overline{\mathbb{Q}}_t$ qui par restriction à $F$ (resp. $N$) définit le premier $\mathfrak{p}$ (resp. $\mathfrak{q}$). La courbe $E/F$ devient via $h$ une courbe elliptique sur le corps local $F_\mathfrak{p}$. Puisque $E$ possède un point rationnel sur $F_\mathfrak{p}$ d'ordre $l \geq 5$, la réduction de $E$ en $\mathfrak{p}$ est nécéssairement semi-stable, [4, proposition 1.1]. On sait qu'il existe alors

un unique élément $q$ de $F_{\mathfrak{p}}^*$, de valuation $r_{\mathfrak{p}}$, une extension non ramifiée $(L/F_{\mathfrak{p}})$, $[L:F_{\mathfrak{p}}] \leq 2$ en un isomorphisme défini sur $L$ de $E_q$, la courbe de Tate associée à $q$, sur $E$, [4, paragraphe 1]. On déduit un isomorphisme de modules galoisiens

$$\xi : \overline{F_{\mathfrak{p}}}^*/q^{\mathbb{Z}} \simeq E\big(\overline{F_{\mathfrak{p}}}\big).$$

Soit $M \in E(\overline{F_{\mathfrak{p}}})$, on appelle paramètre de $M$ tout élément de $\overline{F_{\mathfrak{p}}}^*$ dont l'image par $\xi$ de la classe modulo $q^{\mathbb{Z}}$ est égale à $M$. Soit $\alpha$ (resp. $\gamma$) un paramètre de $P$ (resp. $Q$). On a

$$h\big(\tilde{T}^l(P,Q)\big) = \tilde{T}^l(\alpha,\gamma),$$

où $\tilde{T}^l(\alpha,\gamma)$ est défini au paragraphe 4.

Pour tout entier $t$, $1 \leq t \leq (l-1)/2$, on a:

$$v_{\mathfrak{q}^{\sigma_t^{-1}}}\big(\tilde{T}^l(P,Q)\big) = v_{\mathfrak{q}}\big(\tilde{T}^l(P,Q)^{\sigma_t}\big). \tag{44}$$

Puisque $\sigma_t$ possède un relèvement $\tilde{\sigma}_t$ dans $\mathrm{Gal}(F(E[l])/F)$ tel que $Q^{\tilde{\sigma}_t} = P + tQ$, on déduit de (44), via la proposition 2.4, que

$$v_{\mathfrak{q}^{\sigma_t^{-1}}}\big(\tilde{T}^l(P,Q)\big) = v_{\mathfrak{q}}\big(\tilde{T}^l(P,tQ)\big). \tag{45}$$

On suppose que $\mathfrak{p} \notin \mathfrak{N}(E,P)$. Le point $P$ possède un paramètre $\alpha$ de la forme $q^{n/l}$ avec $1 \leq n \leq l-1$.

Puisque $\tilde{T}^l(P,Q)$ ne dépend que du sons-groupe engendré par $P$, on peut supposer $n = 1$. Le point $Q$ possède un paramètre de la forme $\gamma = q^{m/l}\xi_l$. Puisque

$$\tilde{T}^l(P,tQ) = \tilde{T}^l(P, tQ - mtP),$$

on obtient donc

$$h\big(\tilde{T}^l(P,tQ)\big) = \tilde{T}^l\big(q^{1/l}, \xi_l^t\big). \tag{46}$$

Le point (i) de la proposition se déduit donc de (45), (46) et de la proposition 4.11 (i).

On suppose que $\mathfrak{p} \in \mathfrak{N}(E,P)$. Alors $P$ (resp. $Q$) possède pour paramètre $\alpha = \xi_l$ (resp. $\gamma = q^{n/l}$, $1 \leq n \leq l-1$). Soit $m$, $1 \leq m \leq l-1$, tel que $mn \equiv 1 \pmod{l}$ et $\mathfrak{P} = \mathfrak{q}^{\sigma_m^{-1}}$. On obtient

$$v_{\mathfrak{P}}\big(\tilde{T}^l(P,Q)\big) = v_{\mathfrak{q}}\big(\tilde{T}^l(P,mQ)\big)$$

avec

$$h\big(\tilde{T}^l(P, mQ)\big) = \tilde{T}^l\big(\xi_l, q^{1/l}\big).$$

On déduit que pour tout entier $t$, $1 \le t \le (l-1)/2$,

$$v_{\mathfrak{P}^{\sigma_t^{-1}}}\big(\tilde{T}^l(P, Q)\big) = v_{\mathfrak{q}}\big(\tilde{T}^l(P, mtQ)\big), \tag{47}$$

où $h(\tilde{T}^l(P, mQ)) = \tilde{T}^l(\xi_l, q^{1/l})$. Le point (ii) de la proposition se déduit donc de (47) et de la proposition 4.11 (ii).

Le théorème 1.1 est donc un corollaire immédiat des proposition 6.5 et 6.6.

## 7. ANNULATION DE GROUPES DE CLASSES

Comme dans le cas du théorème de Stickelberger classique le théorème 1.1 nous permet d'introduire un sous-quotient du groupe des classes d'idéaux de $N$ annulé par $l\theta_2(p)$.

On rappelle que $l$ est un nombre fixé, $l \ge 5$. Le nombre premier $p$ peut-être considéré comme auxilliaire, il satisfait $(l, p(p+1)) = 1$.

DÉFINITION 7.1. On appelle $l$-groupe des classes du corps de nombres $L$ et l'on note $Cl'(L)$ le quotient du groupe des classes de $L$ par le sous-groupe engendré par les classes des relèvements premiers de $l$ dans $L$.

Si $M/L$ est une extension de corps de nombres on note $Cl'(M/L)$ le conoyau de l'homomorphisme induit par l'extension des scalaires de $Cl'(L)$ dans $Cl'(M)$.

Soit $F$ tel que $F \cap \mathbb{Q}(\xi_l) = \mathbb{Q}$. A tout couple $(E, P)$ où $E$ est une courbe elliptique définie sur $F$ et $P$ un point rationnel sur $F$ d'ordre $l$ et à tout point $Q \in E[l] \setminus \mathbb{Z}P$ nous associons l'idéal de $N$

$$\mathfrak{M}(E, P, Q) = \prod_{\mathfrak{p} \in \mathfrak{R}(E, P)} \mathfrak{P}^{r_{\mathfrak{p}}} \tag{48}$$

introduit dans le théorème 1.1. On remarque que cet idéal est indépendant de $p$. On déduit de la proposition 2.4 et du paragraphe 6(B) les égalités

$$\mathfrak{M}(E, P, a_\omega P + b_\omega Q) = \mathfrak{M}(E, P, Q)^{\omega}.$$

Pour tout $\omega \in \mathrm{Gal}(F(E[l])/F)$.

DÉFINITION 7.2. On désigne par $\mathscr{E}(N)$ (resp. $\mathscr{E}(N/F)$) le sous-groupe de $Cl'(N)$ (resp. $Cl'(N/F)$) engendré par les images des idéaux $\mathfrak{M}(E, P, Q)$ associés aux couples $(E, P)$ rationnels sur $F$.

On déduit immédiatement du théorème 1.1

THÉORÈME 7.3. (i) *Pour tout nombre premier* $p$, $(l, p(p+1)) = 1$, *alors* $l\theta_2(p)$ *annule le groupe* $\mathscr{E}(N/F)$.

(ii) *On a l'inclusion*:

$$(\mathscr{E}(N))^{\sum_{t=1}^{(l-1)/2} t^2 \sigma_t^{-1}} \subset Cl'(N)^l.$$

*Remarque* 7.4. (1) On peut noter que le théorème 1.1 fournit parfois un résultat meilleur que celui donné en (i). Si la courbe $E/F$ possède un modèle minimal global sur $F$, l'idéal $\mathfrak{M}(E, P, Q)^{l\theta_2(p)}$ définit la classe triviale dans $Cl'(N)$. Si en outre les relèvements premiers de $l$ dans $N$ sont principaux, alors l'idéal $\mathfrak{M}(E, P, Q)^{l\theta_2(p)}$ est principal.

(2) Il faut noter que pour un corps de nombres $F$ la "boundness conjecture"[1] affirme qu'il n'existe qu'un nombre fini de nombres premiers $l$ pour lesquels il existe des couples $(E, P)$ rationnels sur $F$. La liste de ces nombres premiers $l$ est connue lorsque $F = \mathbb{Q}$ grâce à Mazur et lorsque $F/\mathbb{Q}$ est un corps quadratique grâce à Kamieny.

Nous terminons ce paragraphe par des exemples. Nous donnons en particulier une méthode qui permet de déterminer explicitement, à conjugaison près, les idéaux $\mathfrak{M}(E, P, Q)$.

Le couple $(E, P)$ est défini sur le corps de nombres $F$. Soit $\mathfrak{p}$ un idéal premier de $F$ de caractéristique résiduelle $k$ première à $6l$. On suppose que

$$v_{\mathfrak{p}}(j(E)) = -r_{\mathfrak{p}}, \qquad 1 \leq r_{\mathfrak{p}} < l.$$

On sait que $\mathfrak{p} \in \mathfrak{N}(E, P)$, [4, paragraphe 1]. Soit $Q \in E[l] \setminus \mathbb{Z}P$. Nous nous proposons de déterminer le relèvement premier de $\mathfrak{p}$ dans $N$ qui apparait dans l'égalité (48). On dira qu'il s'agit du "bon relèvement de $\mathfrak{p}$".

On fixe un plongement $h$ de $\overline{\mathbb{Q}}$ dans $\overline{\mathbb{Q}}_k$ dont la restriction à $F$ définit $\mathfrak{p}$. On note $\mathfrak{P}$ le relèvement de $\mathfrak{p}$ dans $N$ défini par $h$. Si $L$ est un sous-corps de $\overline{\mathbb{Q}}$ on désigne par $L'$ l'adhérence de $h(L)$ dans $\overline{\mathbb{Q}}_k$.

On suppose la courbe $E$ donnée sur $F$ par une équation de Tate

$$Y^2 + XY = X^3 + a_4 X + a_6, \qquad a_4, a_6 \in F, \tag{49}$$

et l'on suppose que (49) définit via $h$ un modèle minimal de $E/F'$. Puisque $E/F'$ est de mauvaise réduction multiplicative on sait associer à $j(E)$ un unique élément $q$ de $F'$ de valuation $r_{\mathfrak{p}}$ tel que

$$j(E) = \frac{1}{q} + 744 + 196884q + \cdots.$$

[1] La "boundness conjecture" a été démontrée récemment par Merel.

On pose

$$\begin{aligned} a'_4 &= -5 \sum_{n \geq 1} \frac{n^3 q^n}{(1-q^n)}, \\ a'_6 &= -\frac{1}{12} \sum_{n \geq 1} \frac{(7n^5 + 5n^3) q^n}{(1-q^n)}. \end{aligned} \tag{50}$$

On considère la courbe $E_q$ d'équation

$$Y^2 + XY = X^3 + a'_4 X + a'_6. \tag{51}$$

Il existe un isomorphisme de module galoisien

$$\begin{aligned} \theta : \overline{\mathbb{Q}_k}^* &\mapsto E_q\left(\overline{\mathbb{Q}}_k\right) \\ z &\mapsto (X'(z), Y'(z), 1), \qquad \text{si } z \notin q^{\mathbb{Z}}, \\ z &\to 0 \qquad \text{si } z \in q^{\mathbb{Z}}, \end{aligned}$$

où

$$\begin{aligned} X'(z) &= \sum_{n \in \mathbb{Z}} \frac{q^n z}{(1-q^n z)^2} - 2 \sum_{n \leq 1} \frac{n q^n}{(1-q^n)}, \\ Y'(z) &= \sum_{n \in \mathbb{Z}} \frac{q^{2n} z^2}{(1-q^n z)^3} + \sum_{n \geq 1} \frac{n q^n}{(1-q^n)}, \end{aligned} \tag{52}$$

[8, appendice C, paragraphe 14].

On sait en outre qu'il existe un isomorphisme $\varphi$ de $E_q$ sur $E$, d'équation (49), défini sur une extension $F''/F'$ non ramifié où $[F'' : F'] \leq 2$. Cet isomorphisme est explicitement donné par

$$\begin{aligned} X &= v^2 X' + r, \\ Y &= v^3 Y' + s v^2 X' + t, \end{aligned} \tag{53}$$

où $r$, $s$, $t$ et $v \in F''$ et satisfont

$$\begin{aligned} v &= 1 + 2s, \\ 0 &= -s - s^2 + 3r, \\ 0 &= r + 2t, \\ v^4 a'_4 &= a_4 - (t + rs) + 3r^2 - 2st, \\ v^6 a'_6 &= a_6 + r a_4 + r^3 - rt - t^2. \end{aligned} \tag{54}$$

Puisque les modèles sont minimaux $v$ est une unité, puisque $(k, 6) = 1$, on déduit de (54) que $r, s$ et $t$ sont des entiers. Soit $\mathfrak{p}'$ l'idéal de valuation de $F'$. On déduit de (50) que

$$a'_4 \equiv a'_6 \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{p}').$$

Il existe en outre $n_4$ et $n_6 \in O_F$ tels que

$$a_4 \equiv n_4\ (\mathrm{mod}\ \mathfrak{p}'), \qquad a_6 \equiv n_6\ (\mathrm{mod}\ \mathfrak{p}').$$

On déduit facilement de (54), les congruences

$$\begin{aligned} 3r^2 + \frac{r}{2} + n_4 &\equiv 0 \qquad (\mathrm{mod}\ \mathfrak{p}'), \\ r^3 + \frac{r^2}{4} + n_4 r + n_6 &\equiv 0 \qquad (\mathrm{mod}\ \mathfrak{p}'). \end{aligned} \tag{55}$$

Ces congruences nous permettent la détermination explicite de $x_{\mathfrak{p}} \in O_F$ tel que

$$r \equiv x_{\mathfrak{p}} \qquad (\mathrm{mod}\ \mathfrak{p}'). \tag{56}$$

Il est caractérisé modulo $\mathfrak{p}$ par la relation

$$\left(\frac{2}{3}n_4 - \frac{1}{72}\right)x_{\mathfrak{p}} \equiv \left(\frac{n_4}{36} - n_6\right) \qquad (\mathrm{mod}\ \mathfrak{p}'). \tag{57}$$

On rappelle maintenant les conventions du paragraphe 6. On pose $\xi = \varphi o \theta$. On dit que $M \in E(\overline{\mathbb{Q}}_k)$ est de paramètre $z$ en $h$ si l'on a

$$M = \xi\big(z \bmod q^{\mathbb{Z}}\big).$$

LEMME 7.5. *On suppose que $Q$ (resp. $P$) est de paramètre $q^{n/l}$ (resp. $\xi_l$) en $h$. Alors on a*

$$v_{\mathfrak{P}}\left(\prod_{0 \le k \le l-1}\big(X(Q + kP) - x_{\mathfrak{p}}\big)\right) = r_{\mathfrak{p}} \inf(n, l - n).$$

On identifie dans la démonstration tout élément de $\overline{\mathbb{Q}}$ et son image par $h$. On déduit de (52)

$$X'(Q + kP) \sim q^{\inf(n/l,\, 1 - n/l)}, \qquad 0 \le k \le l - 1,$$

d'où, puisque $v$ est une unité,

$$X(Q + kP) - r \sim q^{\inf(n/l,\, 1 - n/l)}.$$

Puisque, $1 \leq r_{\mathfrak{p}} < l$ et que $F'(q^{1/l})/F'$ est totalement ramifée on conclut que

$$X(Q + kP) - x_{\mathfrak{p}} \sim q^{\inf(n/l, 1-n/l)}, \qquad 0 \leq k \leq l-1,$$

d'où l'on déduit le lemme.

On peut maintenant conclure. Soit $(E, P)$ définie sur $F, Q \in E[l] \setminus \mathbb{Z}P$ et $\mathfrak{p} \in \mathfrak{R}(E, P)$ tel que $1 \leq r_{\mathfrak{p}} < l$.

(1) On cherche une équation de Tate de $E/F$ minimale en $\mathfrak{p}$.

(2) On détermine $x_{\mathfrak{p}} \in O_F$ par la congruence (57).

(3) On détermine le polynôme minimal $P(T)$ de $X(Q)$ sur $N$. C'est un polynôme de degré $l$.

On pose

$$R(T) = P(T + x_{\mathfrak{p}}).$$

Alors le bon relèvement de $\mathfrak{p}$ est le relèvement $\mathfrak{P}$ tel que

$$v_{\mathfrak{P}}(R(0)) = r_{\mathfrak{p}}.$$

Pour finir ce paragraphe nous appliquons cette méthode dans le cas où $l = 5$. Soient $F/\mathbb{Q}$ un corps de nombres non ramifié en 5 et $N = F(\sqrt{5})$. On a le lemme suivant

LEMME 7.6. *Soit $u \in F$ tel que $(u-1)(u^2 + 9u - 11) \neq 0$. Alors la courbe $E_u$ d'équation*

$$E_u\colon y^2 + uxy + (u-1)y = x^3 + (u-1)x^2$$

*est une courbe elliptique et $P = (0, 0)$ est un point d'ordre 5 de $E_u$. En outre le discriminant de $E_u$ est donné par*

$$\Delta(u) = (1-u)^5(u^2 + 9u - 11).$$

On suppose dorénavant que $u \in O_F$ et que $E_u$ est un modèle minimal sur $F$. On note que c'est toujours le cas si $F = \mathbb{Q}$ et que c'est souvent le cas si $F$ est une extension quadratique de $\mathbb{Q}$.

On pose $p(u) = u^2 + 9u - 11$. On déduit immédiatement de l'équation de $E_u$ que les éléments de $\mathfrak{R}(E_u, P)$ sont les facteurs premiers dans $F$ de $(p(u))$. Le théorème 1.1 devient alors:

THÉORÈME 7.7. *Tout diviseur premier* $\mathfrak{p}$ *de* $(p(u))$ *possède dans* $N$ *un relèvement premier* $\mathfrak{P}$ *tel qu'on ait*

$$\left(\tilde{T}_p^5(P,Q)\right)\Delta(u)^{5n_p} \equiv \left(\prod_{\mathfrak{p}\mid p(u)} \mathfrak{P}^{r_\mathfrak{p}}\right)^{5\theta(p)} \pmod 5.$$

On sait que l'idéal $\mathfrak{M}(E_u, P, Q)$ est indépendant, à conjugaison près par un élément du groupe de Galois de $(F(\xi_5)/F)$, du choix de $Q$. On note $\mathfrak{M}(u)$ l'un quelconque de ces idéaux. On montre maintenant comment la méthode précédemment décrite permet de déterminer explicitement $\mathfrak{M}(u)$.

On pose

$$S_5 = \{x(R),\ R \in E[5] \setminus \{O\}\}.$$

On sait que $x(P) = 0$ et $x(2P) = 1 - u$ appartiennent à $S_5$.

On définit

$$5f(T) = 5\prod_{a\in S_5} (T-a)/T(T-1+u).$$

On obtient

$$\begin{aligned}
5f(T) = {} & 5x^{10} + (5u^2 + 15u - 15)x^9 \\
& + (u^4 + 3u^3 + 29u^2 - 33u + 1)x^8 \\
& + (-u^5 + 8u^4 + 4u^3 + 77u^2 - 184u + 96)x^7 \\
& + (u^6 - 9u^5 + 49u^4 + 122u^3 - 549u^2 + 575u - 189)x^6 \\
& + (-u^7 + 10u^6 + 32u^5 + 47u^4 - 589u^3 \\
& \qquad + 1036u^2 - 706u + 171)x^5 \\
& + (u^8 + 4u^7 + 38u^6 - 75u^5 - 279u^4 + 910u^3 \\
& \qquad - 988u^2 + 473u - 84)x^4 \\
& + (5u^8 + 10u^7 - 30u^6 - 185u^5 + 675u^4 - 880u^3 \\
& \qquad + 540u^2 - 145u + 10)x^3
\end{aligned}$$

$$+(10u^8 - 15u^7 - 95u^6 + 325u^5 - 375u^4 + 115u^3 + 115u^2 - 105u + 25)x^2$$
$$+(10u^8 - 50u^7 + 70u^6 + 70u^5 - 350u^4 + 490u^3 - 350u^2 + 130u - 20)x$$
$$+(5u^8 - 40u^7 + 140u^6 - 280u^5 + 350u^4 - 280u^3 + 140u^2 - 40u + 5).$$

En examinant l'action de $\mathrm{Gal}(F(E[5])/N)$ sur $S_5$ on vérifie que $f(T)$ se décompose en produit de 2 polynômes irréductibles $f_1(T)f_2(T)$ de $N[T]$.

En effectuant le changement de variables

$$X + \frac{1}{12} = x + \frac{(u^2 + 4u - 4)}{12}, \qquad 2Y + X = 2y + ux + (u - 1), \tag{58}$$

on obtient une équation de Tate de la courbe $E_u$

$$Y^2 + XY = X^3 + a_4(u)X + a_6(u),$$

où

$$a_4(u) = \frac{(u-1)}{48}(-u^3 - 9u^2 + 7u + 15),$$
$$a_6(u) = \frac{(u-1)}{1728}(2u^5 + 26u^4 + 23u^3 - 281u^2 + 487u - 257). \tag{59}$$

Le polynôme $P(T) = f_1(T - (1/12)u^2 - (1/3)u + 5/12)$ est le polynôme minimal de $X(Q)$ où $Q \in E[5] \setminus \mathbb{Z}P$.

Si $\mathfrak{p}$ est un facteur de $(p(u))$, on utilise (59) pour déterminer $x_{\mathfrak{p}}$. Le bon relèvement premier $\mathfrak{P}$ de $\mathfrak{p}$ dans $N$ est caractérisé par l'égalité

$$v_{\mathfrak{P}}\big(P(x_{\mathfrak{p}})\big) = r_{\mathfrak{p}}.$$

Le tableau I regroupe les exemples traités avec le système Pari.

Le corps $F$ est quadratique imaginaire, $F = \mathbb{Q}(\sqrt{-d})$ où $d$ est un entier strictement positif sans facteur carré.

On pose $w = \sqrt{-d}$ (resp. $(1 + \sqrt{-d})/2$) si $d \equiv 1$ ou $2 \pmod 4$ (resp. $d \equiv 3 \pmod 4$).

Lorsqu'un idéal premier de $O_F$ est noté

$$[p, (x, y)],$$

cela signifie qu'il est égal à

$$pO_F + (x + yw)O_F.$$

On note $N$ le corps $F(\sqrt{5})$ et $h_N$ son nombre de classes. On fixe un élément primitif $y$ de $N/\mathbb{Q}$ et l'on note $g(T)$ son polynôme minimal sur $\mathbb{Q}$. Les lignes $w$ et $b$ contiennent respectivement la décomposition de $w$ et d'une $\mathbb{Z}$-base de $O_N$, $(\omega_0, \omega_1, \omega_2, \omega_3)$, sur la base de puissances $\{1, y, y^2, y^3\}$.

On note $[p, (a_0, a_1, a_2, a_3)]$ l'idéal premier de $O_N$

$$pO_N + \alpha O_N, \qquad \alpha = \sum_{k=0}^{3} a_k \omega_k.$$

Le système Pari fournit une famille de générateurs $x_1, x_2, \ldots, x_m$ du groupe des classes $Cl(N)$ de $N$. Nous avons fait suivre chaque facteur premier $\mathfrak{P}$ de $\mathfrak{M}(u)$ d'une suite d'entiers $n_1, \ldots, n_m$ qui traduit l'égalité

$$x = x_1^{n_1} \ldots x_m^{n_m}$$

où $x$ la classe de $\mathfrak{P}$ dans $Cl(N)$. Enfin la ligne $x_{\mathfrak{p}}$ contient un représentant modulo $\mathfrak{p}$ de l'élément considéré en (57).

*Remarque* 7.8. (1) Il est à noter que dans les exemples traités $\mathfrak{M}(u)$ est principal.

Il serait intéressant d'exhiber un tel idéal non principal. C'est certainement difficile. En effet on remarque que le polynôme $p(T) = T^2 + 9T - 11$ étant totalement décomposé dans $\mathbb{Q}(\sqrt{5})$ si l'on a $(p(u)) = \prod \mathfrak{p}^{r_{\mathfrak{p}}}$ dans $O_F$ il existe toujours un produit

$$\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{r_{\mathfrak{p}}}$$

qui est principal dans $O_N$. Ainsi si $(p(u))$ est la puissance d'un idéal premier $\mathfrak{M}(u)$ est principal. On sait en outre, [4, paragraphe 6], que $\mathfrak{M}(u)$ est d'ordre premier à $l$ pour $l < 11$.

(2) Dans les exemples considérés $E_u$ est une équation minimale de Weierstrass. La connaissance de la factorisation de $(u - 1)$, $(p(u))$ et $\mathfrak{M}(u)$ en idéaux premiers rend explicite le théorème 7.3.

TABLE I
Examples $l = 5$

| $d$ | 47 | 47 | 83 | 83 | 41 |
|---|---|---|---|---|---|
| $h_N$ | 5 | 5 | 15 | 15 | $32 = (16, 2)$ |
| $g(T)$ | $T^4 - T^3 + 35T^2 + 12T + 144$ | | $T^4 - T^3 + 62T^2 + 21T + 441$ | | $T^4 + 123T^2 + 1681$ |
| $w$ | $-\frac{1}{13}y^3 + \frac{2}{13}y^2 - \frac{24}{13}y + \frac{12}{13}$ | | $\frac{1}{22}y^3 - \frac{1}{11}y^2 + \frac{21}{11}y + \frac{1}{22}$ | | $-\frac{1}{41}y^3 - 2y$ |
| $b$ | $\left(1, y, y^2, \frac{1}{156}y^3 + \frac{11}{156}y^2 + \frac{11}{156}y + \frac{12}{13}\right)$ | | $\left(1, y, y^2, \frac{1}{462}y^3 + \frac{10}{231}y^2 + \frac{10}{231}y + \frac{21}{22}\right)$ | | $\left(1, y, \frac{1}{41}y^2, \frac{1}{41}y^3\right)$ |
| $u$ | $1 + w$ | $-1 + 3w$ | $-2 + 6w$ | $-5 + 2w$ | $-1 + w$ |
| $(1-u)_F$ | $[2,(0,1)]^2$<br>$[3,(0,1)]$ | $[2,(0,1)]$<br>$[53,(17,1)]$ | $[3,(0,1)]$<br>$[83,(41,1)]$<br>$[3,(-1,1)]$ | $[2,(0,0)]$<br>$[3,(0,1)]^3$ | $[3,(1,1)]$<br>$[5,(-2,1)]$ |
| $p(u)$ | $-13 + 12w$ | $-127 + 30w$ | $-781 + 66w$ | $-115 + 2w$ | $-60 + 7w$ |
| $(p(u))_F$ | $[1741,(144,1)]$ | $[61,(10,1)]$<br>$[379,(160,1)]$ | $[11,(3,1)]$<br>$[11,(-4,1)]$<br>$[41,(-5,1)]$<br>$[131,(10,1)]$ | $[11,(3,1)]$<br>$[29,(-14,1)]$<br>$[41,(4,1)]$ | $[71,(32,1)]$<br>$[79,(14,1)]$ |
| $x_p$ | $x_{1741} = 873$ | $x_{61} = -7$<br>$x_{379} = -19$ | $x_{11} = x'_{11} = 3$<br>$x_{41} = -2$<br>$x_{131} = 32$ | $x_{11} = 3,$<br>$x_{29} = 16,$<br>$x_{41} = -2$ | $x_{71} = -17,$<br>$x_{79} = -7$ |
| $(\mathfrak{M}(u))$ | $[1741,(-814,1,0,0)](1)$ | $[61,(-3,1,1,0,0)](2)$<br>$[379,(168,1,0,0,)](3)$ | $[11,(17,14,12,12)](2)$<br>$[11,(17,14,13,12)](7)$<br>$[41,(17,1,0,0)](12)$<br>$[131,(1,-1,0,0)](9)$ | $[11,(18,18,22,16)](13)$<br>$[29,(-7,1,0,0)](14)$<br>$[41,(6,1,0,0,0)](3)$ | $[71,(4,1,0,0)](15,0)$<br>$[79,(25,0,0)](1,0)$ |

## 8. APPENDICE 1

Les hypothèses sont celles du paragraphe 4. On rappelle que le corps est de caractéristique résiduelle différente de $l$. Le théorème 4.6 nous donne l'égalité

$$\mathscr{R}(\alpha, \gamma, \varphi, \lambda) = A(\varphi, \lambda) B(\alpha, \gamma, \varphi, \psi),$$

où

$$A(\varphi, \lambda) = \lambda^s \prod_{i=0}^{p-1} \frac{\theta(\lambda\psi^i)\theta(\psi^i\varphi^{-1})}{\theta(\lambda\psi^i\varphi^{-1})\theta(\psi^i)},$$

et

$$B(\alpha, \gamma, \varphi, \psi) = \gamma^{-a_1} \prod_{\substack{0 \le i \le p-1 \\ 0 \le u \le l-1}} \frac{\theta(\psi^i\alpha^u)\theta(\gamma z_0^{-1}\psi^i\alpha^u)}{\theta(z_0^{-1}\psi^i\alpha^u)\theta(\gamma\psi^i\alpha^u)},$$

où le choix de $z_0$ et des entiers $a_1$ et $a_2$ est donné dans le paragraphe 4. Pour démontrer les théorèmes 4.8 et 4.9 nous allons déterminer les valuations de $A(\varphi, \lambda)$ et $B(\alpha, \gamma, \varphi, \psi)$ suivant les différents choix de $\alpha$, $\gamma$, $\varphi$, $\psi$ et $\lambda$.

LEMME 8.1. (i) $A(\zeta_p, q^{u/p^2}) \sim (1 - \zeta_p)$ *si* $1 \le u < p^2$ *et* $(u, p) = 1$.

(ii) $A(q^{s/p}, \zeta_{p^2} q^{u/p^2}) \sim (1/p) M(u, s) q^{su/p^2 - \inf(s, u/p)}$ *si* $0 \le u < p^2$ *et* $u \equiv 0 \pmod{p}$.

Puisque dans le cas (i), $\varphi$ est une unité on déduit de la définition de $\theta$

$$\theta(\lambda\psi^i) \sim \theta(\lambda\psi^i\varphi^{-1}), \qquad 0 \le i \le p-1,$$

$$\theta(\psi^i\varphi^{-1}) \sim \theta(\psi^i), \qquad 1 \le i \le p-1,$$

$$\theta(\varphi^{-1}) \sim (1 - \zeta_p),$$

ce qui démontre (i). On suppose maintenant que $\psi$ est une racine primitive $p$-ième de 1, $\psi = \zeta_p$. On obtient alors

$$\theta(\lambda\psi^i) \sim \begin{cases} (1 - \zeta_{p^2}), & \text{si } u = 0, \\ 1, & \text{si } u > 0, \end{cases} \qquad 0 \le i \le p-1.$$

$$\theta(\psi^i\varphi^{-1}) \sim \theta(\varphi^{-1}) \sim q^{-s/p}, \qquad \text{si } 0 \le i \le p-1.$$

$$\theta(\psi^i) \sim (1 - \zeta_p), \qquad \text{si } 1 \le i \le p-1.$$

$$\theta(\lambda\psi^i\varphi^{-1}) \sim \theta(\lambda\varphi^{-1}) \sim \begin{cases} 1, & \text{si } u > ps, \\ (1 - \zeta_{p^2}), & \text{si } u = ps, \\ q^{u/p^2 - s/p}, & \text{si } u < ps. \end{cases}$$

On en déduit l'équivalence de (ii).

LEMME 8.2. *Si $\gamma$ est une unité alors*

$$B(\alpha,\gamma,\varphi,\psi) \sim \begin{cases} 1, & \text{si } \varphi \text{ est une unité,} \\ p, & \text{si } \psi \text{ est une unité.} \end{cases}$$

Puisque $\gamma$ est une unité, on choisit $\zeta_l = \gamma$ et on se ramène à $\alpha = q^{1/l}$. Si $\varphi$ est (resp. n'est pas) une unité, on choisit $\varphi = \zeta_p$, $\psi = q^{1/p}$ (resp. $\varphi = q^{s/p}$, $\psi = \zeta_p$). Ces choix étant faits on déduit de (4.3) et (4.4) les égalités

$$a\left(q^{1/l},\zeta_l\right) = l-1, \qquad b\left(\zeta_p,q^{1/p}\right) = 1, \qquad b\left(q^{s/p},\zeta_p\right) = p-s.$$

Puisque $m_1 = 1$ et $m_2 = 0$, le système (12) devient

$$a_2 \equiv -1 \pmod{l}$$

$$a_2 \equiv 1 \pmod{p} \ (\text{resp. } a_1 \equiv s-p \pmod{p}),$$

si $\varphi$ est (resp. n'est pas) une unité. Dans le premier cas on choisit $a_1 = 0$, $a_2 = lx + py$ où $(x,y)$ vérifient $lx - py = 1$. Dans le second cas on prend $a_1 = s$, $a_2 = -1$. On traite le cas où $\varphi = \xi_p$ et $\psi = q^{1/p}$, $\lambda = q^{u/p^2}$ avec $(u,p) = 1$. On obtient

$$\theta\left(\psi^i\alpha^u\right) \sim \theta\left(\gamma\psi^i\alpha^u\right) \qquad \text{si } (i,u) \neq (0,0),$$

$$\theta(\gamma) \sim 1.$$

Puisque $z_0 = \zeta_p^x\zeta_l^y$, alors

$$\theta\left(\gamma z_0^{-1}\psi^i\alpha^u\right) \sim \theta\left(z_0^{-1}\psi^i\alpha^u\right) \sim \theta\left(\psi^i\alpha^u\right) \qquad \text{si } (i,u) \neq (0,0).$$

En outre

$$\theta\left(z_0^{-1}\right) \sim 1 - \zeta_p^{-x}\zeta_l^{-y}, \qquad \theta\left(\gamma z_0^{-1}\right) \sim 1 - \zeta_p^{-x}\zeta_l^{1-y}.$$

On déduit de la définition de $x$ et $y$ et du fait que $(l, p+1) = 1$, que $x$ et $y$ sont non nuls et $y \not\equiv 1 \pmod{l}$. On a donc $\theta(z_0^{-1}) \sim 1 \sim \theta(\gamma z_0^{-1})$. On déduit des équivalences précédentes que

$$B(\alpha,\gamma,\varphi,\psi) \sim 1$$

dans ce cas.

On suppose maintenant que $\varphi = q^{s/p}$ et $\psi = \zeta_p$. On sait qu'alors $z_0 = q^{s/lp}\zeta_{lp}^{-1}$. Si $u \neq 0$, on a $\theta(\psi^i\alpha^u) \sim \theta(\gamma\psi^i\alpha^u)$. En outre $\theta(\psi^i) \sim (1-\zeta_p)$, $1 \leq i \leq p-1$ et $\theta(\gamma\psi^i) \sim 1$, $0 \leq i \leq p-1$. Comme dans le cas précédent

$$\theta\left(\gamma z_0^{-1}\psi^i\alpha^u\right) \sim \theta\left(z_0^{-1}\psi^i\alpha^u\right) \qquad \text{pour tout } (i,u).$$

On conclut que $B(\alpha,\gamma,\varphi,\psi) \sim (1-\zeta_p)^{p-1} \sim p$.

Nous nous proposons de traiter maintenant le cas où $\alpha$ est une unité. Nous posons

$$\alpha = \zeta_l, \qquad \gamma = q^{n/l}, \qquad 1 \le n < l.$$

On détermine les entiers $a_1$ et $a_2$ dans les deux cas que nous avons à étudier. Si $\varphi$ est une unité on choisit $\varphi = \zeta_p$ et $\psi = q^{1/p}$. Ainsi $a_1$ et $a_2$ satisfont

$$\begin{aligned} -a_1 &\equiv n \pmod{l}, \\ a_2 &\equiv 1 \pmod{p}. \end{aligned}$$

On choisit donc $a_1 = -n$, $a_2 = 1$ et $z_0 = q^{-n/lp}\zeta_{lp}$.

Si $\varphi$ n'est pas une unité, on a $\varphi = q^{s/p}$ et $\psi = \zeta_p$.

Le système (12) devient

$$\begin{aligned} -a_1 &\equiv n \pmod{l} \\ a_1 &\equiv s \pmod{p}. \end{aligned}$$

On choisit alors $a_1 = lsx + pyn$ avec $lx - py = 1$ et $a_2 = 0$.

On pose $a = lsx + pyn$ et l'on a $z_0 = q^{a/lp}$.

LEMME 8.3. $B(\zeta_l, q^{n/l}, \zeta_p, q^{1/p}) \sim q^{\beta(n)}$.

On vérifie immédiatement les équivalences suivantes: $\theta(\psi^i\alpha^u) \sim 1$, pour tout couple $(i, u)$. En outre puisque il n'existe pas d'entier $i$, $0 \le i \le p-1$ tel que $n/l + i/p + n/lp$ ou $n/l + i/p$ soient entiers, on obtient

$$\begin{aligned} \theta\left(\gamma z_0^{-1}\alpha^u\psi^i\right) &\sim \theta\left(q^{n/l+i/p+n/lp}\right), \qquad 0 \le u \le l-1, \\ \theta\left(\gamma\alpha^u\psi^i\right) &\sim \theta\left(q^{n/l+i/p}\right), \qquad 0 \le u \le l-1, \\ \theta\left(z_0^{-1}\alpha^u\psi^i\right) &\sim \theta\left(q^{n/lp+i/p}\right), \qquad 0 \le u \le l-1. \end{aligned}$$

On en déduit que

$$B\left(\zeta_l, q^{n/l}, \zeta_p, q^{1/p}\right) \sim q^{n^2/l} \prod_{i=0}^{p-1} \left( \frac{\theta\left(q^{n/l+i/p+n/lp}\right)}{\theta\left(q^{n/l+i/p}\right)} \right)^l.$$

Soit $i_0$ le plus petit entier, $0 \le i_0 \le p-1$, tel que $n/l + i_0/p + n/lp \ge 1$. Puisque $1 \le n \le l-1$ on a les inégalités

$$\frac{n}{l} + \frac{i_0 - 1}{p} < \frac{n}{l} + \frac{i_0 - 1}{p} + \frac{n}{lp} < 1 \le \frac{n}{l} + \frac{n}{lp} + \frac{i_0}{p} < \frac{n}{l} + \frac{i_0 + 1}{p}.$$

On en déduit grâce à (9) les équivalences

$$\prod_{i=0}^{p-1} \frac{\theta\left(q^{n/l+i/p+n/lp}\right)}{\theta\left(q^{n/l+i/p}\right)}$$

$$\sim q^{(-n/lp)(p-i_0-1)} \frac{\theta\left(q^{n/l+i_0/p+n/lp}\right)}{\theta\left(q^{n/l+i_0/p}\right)}$$

$$\sim \begin{cases} q^{(n/l)(i_0/p-1)-(n/l+i_0/p-1)}, & \text{si } \dfrac{n}{l} + \dfrac{i_0}{p} < 1, \\ q^{(n/l)(i_0/p-1)}, & \text{sinon.} \end{cases}$$

On interprète $i_0$ comme l'entier $p - [np/l + n/l]$, où l'on note $[x]$ la partie entière du rationnel $x$. On vérifie alors l'égalité

$$\frac{n}{l} + \frac{i_0}{p} - 1 = \frac{1}{p}\left\{\left\{\frac{np}{l}\right\} + \left\{\frac{n}{l}\right\}\right\} - \frac{1}{p}\left\{\frac{n}{l}\right\}.$$

Ainsi

$$\frac{n}{l} + \frac{i_0}{p} - 1 = \begin{cases} \dfrac{1}{p}\left\{\dfrac{np}{l}\right\} > 0, & \text{si } \left\{\dfrac{np}{l}\right\} + \dfrac{n}{l} < 1, \\ \dfrac{1}{p}\left(\left\{\dfrac{np}{l}\right\} - 1\right) < 0, & \text{sinon.} \end{cases}$$

On conclut que

$$q^{n^2/l} \sum_{i=0}^{p-1} \left( \frac{\theta\left(q^{n/l+i/p+n/lp}\right)}{\theta\left(q^{n/l+i/p}\right)} \right)^l$$

$$\sim \begin{cases} q^{(n/p)\{np/l\}}, & \text{si } \left\{\dfrac{np}{l}\right\} + \dfrac{n}{l} < 1, \\ q^{(n/p)\{np/l\}+(l/p)(1-n/l-\{np/l\})}, & \text{sinon.} \end{cases}$$

Ce qui achève la démonstration du lemme.

LEMME 8.4. $B(\zeta_l, q^{n/l}, q^{s/p}, \zeta_p) \sim pq^{\alpha(n,s)}$.

Si $(i, u) \neq (0, 0)$ on a l'équivalence

$$\theta\left(\zeta_p^i \zeta_l^u\right) \sim \left(1 - \zeta_p^i \zeta_l^u\right),$$

$$\prod_{\substack{0 \le i \le p-1 \\ 0 \le u \le l-1}} \theta\left(\zeta_p^i \zeta_l^u\right) \sim p.$$

Puisque $0 < n \le l - 1$ et que $a/lp$ et $n/l - a/lp$ ne sont pas entiers on obtient que

$$\theta\left(q^{n/l} \zeta_p^i \zeta_l^u\right) \sim 1, \qquad \forall (i, u),$$

$$\theta\left(q^{n/l - a/lp} \zeta_p^i \zeta_l^u\right) \sim \theta\left(q^{n/l - a/lp}\right), \qquad \forall (i, u),$$

$$\theta\left(q^{-a/lp} \zeta_p^i \zeta_l^u\right) \sim \theta\left(q^{-a/lp}\right), \qquad \forall (i, u).$$

On écrit que $a/lp = [a/lp] + \{a/lp\}$ et l'on utilise (9) pour montrer que

$$\frac{\theta\left(q^{n/l - a/lp} \zeta_p^i \zeta_l^u\right)}{\theta\left(q^{-a/lp} \zeta_p^i \zeta_l^u\right)} \sim q^{(n/l)[a/lp]} \cdot \frac{\theta\left(q^{n/l - \{a/lp\}}\right)}{\theta\left(q^{-a/lp}\right)}, \qquad \forall (i, u).$$

Puisque $0 < \{a/lp\} < 1$, $-1 < n/l - \{a/lp\} < 1$ et $n/l \neq \{a/lp\}$, on obtient

$$\theta\left(q^{-\{a/lp\}}\right) \sim q^{-\{a/lp\}},$$

$$\theta\left(q^{n/l - \{a/lp\}}\right) \sim \begin{cases} q^{n/l - \{a/lp\}}, & \text{si } n/l < \{a/lp\}, \\ 1, & \text{sinon.} \end{cases}$$

On conclut que

$$\prod_{\substack{0 \le i \le p-1 \\ 0 \le u \le l-1}} \frac{\theta\left(\psi^i \alpha^u\right) \theta\left(z z_0^{-1} \psi^i \alpha^u\right)}{\theta\left(z_0^{-1} \psi^i \alpha^u\right) \theta\left(\gamma \psi^i \alpha^u\right)} \sim p q^{lp((n/l)[a/lp] + \inf(n/l, \{a/lp\}))}.$$

Puisque $\gamma^{-a_1} = q^{-n(a/l)}$, on obtient l'équivalence souhaitée.

Les théorèmes 4.8 et 4.9 se déduisent maintenant immédiatement des lemmes précédents. Plus précisemment on applique les lemmes 8.3 et 8.4 pour démontrer le théorème 4.9.

## 9. APPENDICE 2

Les théorèmes 1.1 et 1.2 ont été démontrés pour tout couple de nombres premiers $l$ et $p$ tels que $l \ge 5$ et $(l, p(p + 1)) = 1$. Le but de cet

appendice est de démontrer que si l'on suppose $p \equiv 1 \pmod{l}$ l'élément $\theta_2(p)$ prends alors une forme très simple. Puisque, comme nous l'avons déjà remarqué, le groupe de classe $\mathscr{E}(N/F)$ ne dépend pas du choix de $p$, nous utilisons la simplification précédente pour obtenir un annulateur plus simple du $m$-sous-groupe de Sylow de $\mathscr{E}(N/F)$ pour $m \neq l$ et $m > 3$.

THÉORÈME 9.1. *Pour tout nombre premier $p$, tel que $p \equiv 1 \pmod{l}$, on a l'égalité*

$$\theta_2(p) = \frac{6n_p}{l} \sum_{t=1}^{(l-1)/2} (tl - t^2)\sigma_t^{-1}.$$

Si $m$ est un nombre premier on note $\mathscr{E}(N/F)_m$ le $m$-sous-groupe de Sylow de $\mathscr{E}(N/F)$.

COROLLAIRE 9.2. *L'élément $\sum_{t=1}^{(l-1)/2}(tl - t^2)\sigma_t^{-1}$ annule le groupe $\mathscr{E}(N/F)_m$ pour tout nombre premier $m$, $m > 3$ et $m \neq l$.*

*Remarque* 9.3. Si $l = 5$ on note l'égalité $\sum_{t=1}^{(l-1)/2}(tl - t^2)\sigma_t^{-1} = 4(\sigma_1 + \sigma_2) + 2\sigma_2$. Puisque la norme de $N/F$ annule $\mathscr{E}(N/F)$ on déduit, compte tenu de la remarque 7.8, que

$$\mathscr{E}(N/F)_m = \{1\} \qquad \text{si } m \neq 2 \text{ et } 3.$$

*Démonstration du théorème* 9.1 *et du corollaire* 9.2. Les méthodes sont celles du paragraphe 5. On suppose dorénavant la congruence $p \equiv 1 \pmod{l}$. Compte tenu de la définition de $\theta_2(p)$, donnée au paragraphe 1, il suffit de montrer l'égalité:

$$\gamma(t) = \frac{(p^2 - 1)}{2l}(tl - t^2), \qquad 1 \leq t \leq \frac{l-1}{2}. \tag{60}$$

On déduit de la définition les égalités

$$\gamma(t) = (p^2 - p)\beta(t) + \sum_{s=1}^{p-1} \alpha(t, s)$$

avec

$$\beta(t) = \frac{l}{p}\left(\frac{t^2}{l^2} + \inf\left(0, 1 - \frac{2t}{l}\right)\right). \tag{61}$$

On vérifie immédiatement que (60) se déduit de (61) et du lemme suivant que nous allons démontrer.

LEMME 9.4. *Pour tout entier* $t$, $1 \le t \le (l-1)/2$ *on a l'égalité*:

$$\sum_{s=1}^{p-1} \alpha(t,s) = \frac{l(p-1)}{2}\left(\frac{t}{l}(p+1) - \frac{t^2}{l^2}(p+3)\right) - l(p-1)\inf\left(0, 1 - \frac{1-2t}{l}\right).$$

On utilise les notations et les résultats du paragraphe 5. On a les équivalences:

$$\mathscr{R}\left(\frac{1}{l}, \frac{t}{l}\tau, \frac{s}{p}\tau, \frac{1}{p^2}\right)^{12lp^2} \sim q_\tau^{12lp^2\alpha(t,s)} \sim \left(\frac{\Delta\begin{pmatrix}\tau\\ 1/pl\end{pmatrix}}{\Delta\begin{pmatrix}\tau\\ 1/p\end{pmatrix}}\right)^{lp^2} \times \left(\frac{\varphi\left(1/p\middle|\begin{matrix}p\tau\\1\end{matrix}\right)\varphi\left((tp-z_1)\tau\middle|\begin{matrix}lp\tau\\1\end{matrix}\right)}{\varphi\left(pt\tau\middle|\begin{matrix}lp\tau\\1\end{matrix}\right)\varphi\left(-z_1\tau\middle|\begin{matrix}lp\tau\\1\end{matrix}\right)}\right)^{12lp^2}, \tag{62}$$

où $z_1 = lsx + pyt$ et $lx - py = 1$.

Puisque $p \equiv 1 \pmod{l}$ on peut choisir $y = -1$.

On utilise le théorème 4.1 de [6] pour montrer l'égalité

$$\prod_{s=1}^{p-1} \frac{\varphi^{12lp^2}\left((tp-z_1)\tau\middle|\begin{matrix}lp\tau\\1\end{matrix}\right)}{\varphi^{12lp^2}\left((-z_1)\tau\middle|\begin{matrix}lp\tau\\1\end{matrix}\right)} = \left(\frac{\varphi\left(2tp\tau\middle|\begin{matrix}l\tau\\1\end{matrix}\right)\varphi\left(tp\tau\middle|\begin{matrix}lp\tau\\1\end{matrix}\right)}{\varphi\left(2tp\tau\middle|\begin{matrix}lp\tau\\1\end{matrix}\right)\varphi\left(tp\tau\middle|\begin{matrix}l\tau\\1\end{matrix}\right)}\right)^{12lp^2}.$$

On note $H(\tau)$ cette expression. On obtient alors

$$\prod_{s=1}^{p-1} \mathscr{R}\left(\frac{1}{l}, \frac{t}{l}\tau, \frac{s}{p}\tau, \frac{1}{p^2}\right)^{12lp^2} \sim \left(\frac{\Delta\begin{pmatrix}\tau\\ 1/pl\end{pmatrix}}{\Delta\begin{pmatrix}\tau\\ 1/p\end{pmatrix}}\right)^{lp^2(p-1)} \left(\frac{\varphi\left(1/p\middle|\begin{matrix}p\tau\\1\end{matrix}\right)}{\varphi\left(pt\tau\middle|\begin{matrix}lp\tau\\1\end{matrix}\right)}\right)^{12lp^2(p-1)} H(\tau). \tag{63}$$

On sait par (62) que le membre de gauche de l'équivalence (63) est équivalent à

$$q_\tau^{12lp^2\sum_{s=1}^{p-1}\alpha(t,s)}.$$

On détermine par un calcul élémentaire, à partir de (14) et (15), un équivalent du membre de droite de (63). C'est la comparaison de ces équivalents qui fournit l'égalité du lemme 9.4 et achève la démonstration du théorème.

On pose $\theta = \sum_{t=1}^{(l-1)/2}(tl - t^2)\sigma_t^{-1}$. Soit $m$ un nombre premier. On sait que pour tout nombre premier $p$, $p \equiv 1 \pmod{l}$, alors $(6n_p/l)\theta$ annule $\mathscr{E}(N/F)_m$. Si $m > 3$ et $m \neq l$ il existe un nombre premier $p$, tel que $p \equiv 1 \pmod{l}$ et $p \not\equiv 0, \pm 1 \pmod{m}$. On en déduit que $(6n_p/l, m) = 1$ et que par conséquent $\theta$ annule $\mathscr{E}(N/F)_m$, ce qui démontre le corollaire.

## RÉFÉRENCES


1. A. Bayad, "Résolvantes elliptiques et éléments de Stickelberger," Pub.école doctorale de mathématiques de Bordeaux I, 1992.
2. J. Brinkhuis, Gauss sums and their prime factorization, *Enseign. Math.* **36** (1990), 39–51.
3. Ph. Cassou-Noguès et M. J. Taylor, Elliptic functions and rings of integers, *in* "Prog. Math.," Vol. 66, Birkhäuser, Basel/Stuttgart/Boston, 1987.
4. Ph. Cassou-Noguès et M. J. Taylor, Un élément de Stickelberger quadratique, *J. Number Theory* (*3*) **37** (1991), 307–342.
5. Shih-Ping Chan, Modular functions, elliptic functions and Galois module structure, *J. Reine Angew. Math.* (1987), 67–82.
6. D. S. Kubert et S. Lang, Modular units, *in* "Grundlehren Math. Wiss.," Vol. 244, Springer-Verlag, New York/Berlin, 1981.
7. R. Schertz, Galoismodulstruktur und Elliptische Funktionen, *J. Number Theory* **39** (1991), 285–326.
8. J. H. Silverman, The arithmetic of elliptic curves, *in* "Graduate Texts in Mathematics," Vol. 106, Springer-Verlag, New York/Berlin, 1986.
9. L. Washington, Introduction to cyclotomic fields, *in* "Graduate Texts in Mathematics," Vol. 83, Springer-Verlag, New York/Berlin.