[8] A. N. Parshin, *Local class field theory*, Proc. Steklov Inst. Math. 165 (1985), Issue 3, 157–185; Translation from Trudy Mat. Inst. Steklov. 165 (1984), 143–170 (Russian).
[9] S. Saito, *Class field theory for curves over local fields*, J. Number Theory 21 (1985), 44–80.

INSTITUT HENRI POINCARÉ
PROBLÈMES DIOPHANTIENS
11, rue P. et M. Curie
75231 Paris Cedex 05, France

Reçu le 21.5.1987
et dans la forme modifiée le 23.9.1988 (1724)

ACTA ARITHMETICA
LIV (1990)

Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers

par

JEAN COUGNARD (Besançon)

1. Introduction. Etant donné un corps de nombres K, on note $\boldsymbol{Z}_k$ son anneau des entiers; si L/K est une extension algébrique de degré fini de corps de nombres, on dit que $\boldsymbol{Z}_L$ est $\boldsymbol{Z}_K$-monogène s'il existe θ tel que $\boldsymbol{Z}_L = \boldsymbol{Z}_K[\theta]$.

Si $K = \boldsymbol{Q}$ et $L/\boldsymbol{Q}$ cyclique de degré premier $l \geqslant 5$, M.-N. Gras a montré [9] qu'une condition nécessaire de monogénéité est que L soit un corps de rayon. On peut voir à travers les résultats de [1] que ce lien entre monogénéité et corps de rayons ne se limite pas à $k = \boldsymbol{Q}$. Des travaux récents ([2], [4], [6], [7]) montrent que les conditions nécessaires sont aussi parfois suffisantes. Dans le même ordre d'idées on se propose de démontrer:

THÉORÈME 1.1. *Si k est un corps quadratique imaginaire de discriminant $d_k < -4$, $\mathfrak{f}$ un idéal entier impair de $\boldsymbol{Z}_k$, $k^{(\mathfrak{f})}$ (resp. $k^{(2)}$) le corps de classes de k de rayon $\mathfrak{f}$ (resp. 2) alors l'anneau des entiers $k^{(\mathfrak{f})}k^{(2)}$ est monogène sur celui de $k^{(2)}$.*

En particulier, si 2 est décomposé dans $k/\boldsymbol{Q}$, on retrouve le résultat de [4].

Lorsque $k = \boldsymbol{Q}(\sqrt{-d})$ avec $d \equiv 2 \bmod 4$ on peut améliorer le théorème 1.1 en démontrant qu'alors l'anneau des entiers de $k^{(\mathfrak{f})}$ est monogène sur celui du corps de classes de Hilbert H_k de k (cf. paragraphe 12).

La méthode utilisée suit le canevas établi dans [3], le paramétrage de la courbe elliptique $\boldsymbol{C}/\boldsymbol{Z}_k$ conduit au modèle de Legendre. Les résultats dépendent essentiellement des propriétés de divisibilité de la fonction de Legendre pour certains entiers quadratiques imaginaires, et des congruences satisfaites par les coordonnées des points de division d'ordre impair aux places de mauvaise réduction.

La méthode est effective car nous donnons une formule de récurrence qui permet de calculer des polynômes annulés par la première coordonnée des points de n-division (celle qui permet de construire l'élément θ tel que $\boldsymbol{Z}_{k^{(2)}k^{(\mathfrak{f})}} = \boldsymbol{Z}_{k^{(2)}}[\theta]$). Pour être tout à fait complet il aurait fallu prolonger ces formules à tous les points de $\boldsymbol{Z}_k$ premiers à 2.

Des résultats analogues à ceux démontrés ici viennent d'être annoncés par M. Taylor et Ph. Cassou-Noguès [5].

2. Modèle de Legendre. Soient $\mathscr{H}$ le demi-plan de Poincaré et $\tau\in\mathscr{H}$. On associe à τ le réseau Λ_τ de base 1, τ et la courbe elliptique $E_\tau = C/\Lambda_\tau$. On peut tout d'abord paramétrer E_τ par la fonction $\wp$ de Weierstrass et sa dérivée $\wp'$. Lorsque c'est nécessaire on indique la dépendance des fonctions par rapport au réseau: $\wp(z;\tau,1)$.

Nous construisons la fonction

$$T(z)=\frac{\wp(1/2)-\wp((1+\tau)/2)}{\wp(z)-\wp((1+\tau)/2)}$$

et la fonction

$$T_1=\frac{1}{2}\cdot\frac{T'}{(\wp(\tau/2)-\wp((1+\tau)/2))^{1/2}},$$

le choix de la racine carrée étant fait une fois pour toute. Nous sommes également amenés à utiliser la fonction de Legendre:

$$\lambda(\tau)=\frac{\wp(1/2;\tau,1)-\wp((1+\tau)/2;\tau,1)}{\wp(\tau/2;\tau,1)-\wp((1+\tau)/2;\tau,1)}$$

qui est une fonction modulaire pour le groupe $\Gamma(2)$, noyau de la réduction de $\mathrm{SL}_2(\mathbf{Z})$ modulo 2.

Les fonctions T, T_1 ont mêmes diviseurs que les fonctions de Fueter utilisées dans [3], il n'est donc pas étonnant de retrouver un formulaire voisin de celui qui y est exposé. Pour les démonstrations très voisines de celles de Fueter nous renvoyons à cet ouvrage. Les fonctions T et T_1 ont pour diviseur respectivement

$$2(0)-2\left(\frac{1+\tau}{2}\right)\quad\text{et}\quad(0)+\left(\frac{1}{2}\right)+\left(\frac{\tau}{2}\right)-3\left(\frac{1+\tau}{2}\right);$$

elles paramètrent E_τ en donnant le modèle de Legendre:

$$T_1^2=T(T-1)(T-\lambda(\tau)). \tag{1}$$

De plus la fonction T satisfait une formule d'inversion:

$$T(z+(1+\tau)/2)=\frac{\lambda(\tau)}{T(z)}. \tag{2}$$

Si on introduit la fonction D définie par $D(z)=T_1(z)/T(z)$, on peut énoncer:

THÉORÈME 2.1 (formule d'addition). *Pour u et v dans E_τ on a l'égalité*

$$T(u+v)=\lambda(\tau)\frac{[D(u)+D(v)]^2\,T(u)\,T(v)}{(\lambda(\tau)-T(u)\,T(v))^2}. \tag{3}$$

On en déduit aisément deux corollaires:

COROLLAIRE 2.2 (formule de duplication). *Pour $u\in E_\tau$ on a:*

$$T(2u)=4\lambda(\tau)\frac{T(u)(T(u)-1)(T(u)-\lambda(\tau))}{(\lambda(\tau)-T(u)^2)^2}. \tag{4}$$

COROLLAIRE 2.3 (formule de soustraction). *Pour u et $v\in E_\tau$ on a l'égalité:*

$$(T(u)-T(v))^2(T(u+v)-T(u-v))=\frac{4}{\lambda(\tau)}T(u+v)\,T(u-v)\,T_1(u)\,T_1(v). \tag{5}$$

3. Choix de τ et conséquences. L'objet de ce travail étant l'étude de l'anneau des entiers de certaines extensions abéliennes d'un corps quadratique imaginaire $k=\mathbf{Q}(\sqrt{-d})$, nous supposons que Λ_τ est l'anneau des entiers d'un tel corps. Rappelons que le discriminant d_k de ce corps est supposé <-4.

Les fonctions λ et T étant des fonctions homographiques de $\wp$, on peut remplacer cette dernière par la première fonction de Weber ([3], ch. VII):

$$h^{(1)}_{\Lambda_\tau}(z)=-\frac{2^7\cdot3^5\,g_2(\Lambda_\tau)\,g_3(\Lambda_\tau)}{\Delta(\Lambda_\tau)}\wp(z;\tau,1).$$

La théorie de la multiplication complexe nous montre que le modèle de Legendre est défini sur $k^{(2)}$ et que étant donnés $\mathfrak{f}$ idéal entier impair de $\mathbf{Z}_k$, α un point primitif de $\mathfrak{f}$-division de E_τ, le nombre algébrique $T(\alpha)$ engendre sur $k^{(2)}$ le corps $k^{(\mathfrak{f})}k^{(2)}$.

Rappelons qu'étant donné l'idéal entier $\mathfrak{L}$, le degré $[k^{(\mathfrak{L})}:H_k]$ est égal à $\varphi(\mathfrak{L})$ et $\varphi(\mathfrak{L})/2$ si $\mathfrak{L}\not\mid 2$ (d'après [3], ch. II, Th. 2.5).

Les points de 2-division de E_τ n'ayant pas le même annulateur dans $\mathbf{Z}_k$ et ne jouant pas un rôle symétrique dans la définition de T et de λ nous sommes amenés à préciser le choix de τ. Nous utiliserons plusieurs fois la formule liant les fonctions λ et j (cf. [10], ch. 18, §6) $\lambda^2(\lambda-1)^2j=2^8(\lambda^2-\lambda+1)^3$. Notons encore que les propriétés de la fonction $\wp$ impliquent que λ est définie sur $\mathscr{H}$, ne s'annule ni ne prend la valeur 1. Précisons maintenant le choix des points de 2-division suivant la décomposition de l'idéal $2\mathbf{Z}_k$.

(a) Supposons 2 décomposé dans $k/\mathbf{Q}$. L'entier d définissant le corps $k=\mathbf{Q}(\sqrt{-d})$ vérifie $d\equiv 7 \bmod 8$. On choisit $\tau=(1+\sqrt{-d})/2$. Des calculs élémentaires montrent que $(1+\tau)/2$ (resp. $\tau/2$, $1/2$) a pour annulateur l'idéal $\mathscr{P}=(2,\tau)$ (resp. $\mathscr{P}'=(2,1-\tau,(2))$. Puisque 2 est décomposé, on a $k^{(2)}=H_k=k(j)=k(\lambda(\tau))$. On a de même $k^{(2\mathscr{P})}=H_k$. On en déduit que si α est un point primitif de $2\mathscr{P}$-division $T(\alpha)\in H_k$. Mais $2\alpha=(1+\tau)/2$, donc α est un pôle de $z\mapsto T(2z)$. La formule de duplication montre que $T(\alpha)^2=\lambda(\tau)$. On peut alors énoncer:

PROPOSITION 3.1. *Si 2 est décomposé dans $k/\mathbf{Q}$ les nombres $\lambda(\tau)$ et $1-\lambda(\tau)$ sont des carrés dans H_k.*

Démonstration. La conjugaison complexe opère non trivialement sur le sous-corps H_k de C; de plus elle laisse globalement invariant le réseau Λ_τ.

On a donc $\overline{\wp(1/2)} = \wp(1/2)$, $\overline{\wp(\tau/2)} = \wp(\bar{\tau}/2) = \wp((1+\tau)/2)$ et $\overline{\lambda(\tau)} = 1-\lambda(\tau)$. La proposition résulte donc de la discussion précédente.

(b) Lorsque 2 est inerte dans $k = \boldsymbol{Q}(\sqrt{-d})$ c'est que $d \equiv 3 \bmod 8$. On choisit $\tau = (1+\sqrt{-d})/2$. On sait que $\lambda(\tau) \in k^{(2)}$ et que $[k^{(2)}: H_k] = 3$ puisque $d_K < -4$. Déterminons l'action de $\mathrm{Gal}(k^{(2)}/H_k)$ sur $\lambda(\tau)$. Pour cela on considère l'idèle unité égal à 1 pour toute place première à 2 et égal à τ en 2. A cet idèle correspond, par la loi de réciprocité de Shimura ([3], ch. IX, Th. 3.1, cor. 3.2) un automorphisme σ de $k^{(2)}/H_k$ défini, sur les points P de 2-division de la façon suivante: $h^{(1)}_{\Lambda_\tau}(P) = h^{(1)}_{\Lambda_\tau}(\tau P)^\sigma$. On en déduit la proposition suivante:

PROPOSITION 3.2. *Si 2 est inerte dans $k/\boldsymbol{Q}$ et $d_k < -4$, on a $k^{(2)} = k(\lambda(\tau))$, les nombres algébriques $\lambda(\tau)$, $1-1/\lambda(\tau)$ sont conjugués sur H_k.*

Démonstration. Un calcul immédiat montre que l'idèle défini plus haut induit sur les points de 2-division la permutation circulaire qui envoie 1/2 sur $\tau/2$. L'image de $\lambda(\tau)$ par l'automorphisme σ^{-1} est $1-1/\lambda(\tau)$; comme $d \neq 3$, ces deux nombres sont distincts, ce qui donne la proposition (si $d = 3$ $\lambda(\tau) = 1-1/\lambda(\tau)$ car $j((1+\sqrt{-3})/2) = 0$, mais alors $k^{(2)} = \boldsymbol{Q}(\sqrt{-3})$).

(c) Lorsque 2 est ramifié dans $k/\boldsymbol{Q}$, on a soit $d \equiv 0 \bmod 2$, soit $d \equiv 1 \bmod 4$. Notons $\mathfrak{P}$ l'unique idéal premier de $\boldsymbol{Z}_k$ divisant 2. L'anneau $\boldsymbol{Z}_k$ a pour base 1, $\sqrt{-d}$. Si $d \equiv 2 \bmod 4$ l'idéal $\wp$ est engendré par 2 et $\sqrt{-d}$. On en déduit que l'unique point de $\mathfrak{P}$-division de $\boldsymbol{C}/\boldsymbol{Z}_k$ est l'image de $\sqrt{-d}/2$. Posons $\tau = \sqrt{-d}-1$. Si $d \equiv 1 \bmod 4$ l'idéal $\wp$ est engendré par 2 et $1+\sqrt{-d}$. On choisit $\tau = \sqrt{-d}$.

Dans les deux cas l'unique point non nul de $\mathfrak{P}$-division est $(1+\tau)/2$. Nous pouvons établir les résultats suivants:

PROPOSITION 3.3. *Si 2 est ramifié dans $k/\boldsymbol{Q}$ et $d \neq 1$, $k^{(2)} = k(\lambda(\tau))$, les nombres algébriques $\lambda(\tau)$ et $1/\lambda(\tau)$ sont H_k-conjugués.*

Démonstration. Le degré de $k^{(2)}/H_k$ est égal à 2. Soit σ l'automorphisme non trivial de $k^{(2)}/H_k$; il lui correspond un idèle unité qui permute les 2 points primitifs de 2-division. Le conjugué de $\lambda(\tau)$ est $1/\lambda(\tau)$.

Ces deux nombres sont égaux si et seulement si $\lambda(\tau) = -1$ (puisque λ ne peut prendre la valeur 1). La formule liant λ et j implique qu'alors $j(\tau) = 1728$ ce qui équivaut à $\boldsymbol{Z}_k = \boldsymbol{Z}[i]$.

PROPOSITION 3.4. *Si 2 est ramifié dans $k/\boldsymbol{Q}$, $\lambda(\tau)$ est un carré dans $k^{(2)}$.*

Démonstration. Si $\boldsymbol{Z}_k = \boldsymbol{Z}[i]$, $\tau = i$, on a $\lambda(\tau) = -1$, sinon utilisons le fait que $k^{(2)} = k^{(\mathfrak{P}^3)}$. Soit α un point primitif de $\mathfrak{P}^3$-division de E_τ, $2\alpha = (1+\tau)/2$. Le point α est tel que $T(\alpha) \in k^{(2)}$ et est un pôle de la fonction $T(2z)$. On conclut comme dans la proposition 3.1.

4. Conséquences de quelques théorèmes classiques de la théorie du corps de classes. Nous regroupons ici divers résultats utilisés ultérieurement.

PROPOSITION 4.1. *Si 2 est inerte ou ramifié dans $k/\boldsymbol{Q}$, le produit des idéaux premiers au-dessus de 2 dans $k^{(2)}$ est principal.*

Démonstration. Dans l'extension abélienne $k^{(2)}/k$ les idéaux premiers au-dessus de 2 ont même groupe d'inertie cyclique d'ordre premier. On peut considérer $k^{(2)}/k$ comme le composé d'extensions cycliques de k. L'une de ces extensions, notons-la L/k, est ramifiée en 2, le produit des idéaux premiers au-dessus de 2 est ambige dans L/k et $k^{(2)}/L$ est non ramifiée. Le théorème de Tannaka–Terada (cf. [12]) nous dit alors que cet idéal ambige devient principal dans le corps des genres de L/k. Des considérations de degré montrent aisément que ce corps est $k^{(2)}$.

PROPOSITION 4.2. *Supposons 2 inerte ou ramifié dans $k/\boldsymbol{Q}$ et soit $\mathfrak{P}$ un idéal premier de k divisant 3. Alors les idéaux premiers de H_k divisant 2 sont décomposés dans $k^{(\mathfrak{P})}/H_k$.*

Démonstration. Si 3 est ramifié ou décomposé dans $k/\boldsymbol{Q}$, il n'y a rien à démontrer. Si 3 et 2 sont inertes dans $k/\boldsymbol{Q}$, 2 appartient au rayon modulo 3 et est donc décomposé dans $k^{(3)}/k$. Si 3 est inerte et $2 = Q^2$ ramifié dans $k/\boldsymbol{Q}$, Q n'est pas principal ($d_K < -4$) mais Q^2 est dans le rayon modulo 3, il en résulte que Q a un degré résiduel égal à 2 à la fois dans $k^{(3)}/k$ et dans H_k/k, d'où le résultat.

PROPOSITION 4.3. *Si $d_k < -4$ le groupe de Galois de $k^{(4)}/H_k$ est cyclique d'ordre 4 si $d \equiv 2 \bmod 4$ et isomorphe à $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$ si $d \equiv 1 \bmod 4$.*

Démonstration. Le groupe de Galois de $k^{(4)}/H_k$ est isomorphe à $(\boldsymbol{Z}_k/4\boldsymbol{Z}_k)^*/(\pm 1)$, il est donc d'ordre 4 et peut donc se déterminer en faisant les calculs dans le complété de k pour la place divisant 2. On se ramène donc aux six extensions qudratiques ramifiées de $\boldsymbol{Q}_2$: $\boldsymbol{Q}_2(\sqrt{-1})$, $\boldsymbol{Q}_2(\sqrt{3})$, $\boldsymbol{Q}_2(\sqrt{2})$, $\boldsymbol{Q}_2(\sqrt{-2})$, $\boldsymbol{Q}_2(\sqrt{6})$, $\boldsymbol{Q}_2(\sqrt{-6})$. Un calcul immédiat permet de conclure.

Remarque. Si 2 est ramifié dans $k/\boldsymbol{Q}$ et $d \equiv 1 \bmod 4$ le corps $\boldsymbol{Q}(i)$ est inclus dans H_k, il ne l'est pas si $d \equiv 2 \bmod 4$. Un calcul rapide de discriminant montre qu'alors $k^{(2)} = H_k(i)$.

5. Formules du produit pour les fonctions T, T_1. Rappelons que l'on suppose que Λ_τ est l'anneau des entiers d'un corps quadratique imaginaire $\boldsymbol{Q}(\sqrt{-d})$. On note $\mathrm{rad}(2)$ l'idéal égal à $\wp$ si $(2) = \wp^2$ et égal à (2) sinon.

On choisit $\nu \in \boldsymbol{Z}_k$, $\nu \equiv 1 \bmod \mathrm{rad}(2)$. Le choix de τ implique que le point $(1+\tau)/2$ de E_τ est invariant par ν.

PROPOSITION 5.1. *Si $\nu \equiv 1 \bmod \mathrm{rad}(2)$ on a la relation:*

$$\pm\lambda(\tau)^{(N(\nu)-1)/2}\, T(\nu z) = \prod_{\substack{\alpha \in E_\tau \\ \nu\alpha = 0}} T(z+\alpha). \tag{6}$$

Démonstration. On considère les diviseurs des fonctions elliptiques de chaque membre. Ils sont égaux. Le quotient des deux membres est une constante que l'on évalue en choisissant $z = 1/2$ ou $z = \tau/2$. Les deux points

pouvant être permutés par v on fait le produit des deux relations obtenues. La formule d'inversion montre que le carré de la constante est égal à 1.

Remarque. Lorsque la courbe n'admet pas de multiplication complexe, on a la même relation avec $n \in \mathbf{Z}$, $n \equiv 1 \bmod 2$.

COROLLAIRE 5.2. *Si $v \in \mathbf{Z}_k$, $v \equiv 1 \bmod \mathrm{rad}(2)$ les valeurs de T aux points de v-division de E_τ non nuls satisfont à la relation:*

$$\pm v^2 \lambda(\tau)^{(N(v)-1)/2} = \prod_{\substack{\alpha \in E_\tau - \{0\} \\ v\alpha = 0}} T(\alpha). \tag{7}$$

Démonstration. On divise les deux membres de la formule (6) par $T(z)$ puis on fait tendre z vers 0.

On va maintenant établir un résultat analogue pour les fonctions T_1.

Si on note $\sigma_1, \sigma_2, \sigma_3$ les points de 2-division de E_τ, on obtient, en dérivant l'équation vérifiée par les fonctions de Weierstrass:

$$\wp''(\sigma_i) = 2\big(\wp(\sigma_i)-\wp(\sigma_j)\big)\big(\wp(\sigma_i)-\wp(\sigma_k)\big), \quad i, j, k \text{ deux à deux distincts.}$$

Cette relation permet d'obtenir des équivalents pour la fonction T_1 au voisinage des points de 2-division. Par construction, au voisinage de 0

$$T_1(z) \sim -\frac{\wp(1/2)-\wp\big((1+\tau)/2\big)}{\big(\wp(\tau/2)-\wp\big((1+\tau)/2\big)\big)^{1/2}} z.$$

En $z = 1/2$, $z = \tau/2$ la fonction T_1 s'annulle; le calcul de $\wp''(\sigma_i)$ permet d'écrire

$$T_1\left(z+\frac{1}{2}\right) \sim \frac{\wp(1/2)-\wp(\tau/2)}{\big(\wp(\tau/2)-\wp\big((1+\tau)/2\big)\big)^{1/2}} z$$

et

$$T_1\left(z+\frac{\tau}{2}\right) \sim -\frac{\big(\wp(1/2)-\wp\big((1+\tau)/2\big)\big)\big(\wp(\tau/2)-\wp(1/2)\big)}{\big(\wp(\tau/2)-\wp\big((1+\tau)/2\big)\big)^{3/2}} z.$$

Pour obtenir un équivalent de T_1 au voisinage de $(1+\tau)/2$, on dérive la formule d'inversion et on obtient:

$$T_1\left(z+\frac{1+\tau}{2}\right) \sim \frac{\lambda(\tau)}{\big(\wp(\tau/2)-\wp\big((1+\tau)/2\big)\big)^{1/2}\big(\wp(1/2)-\wp\big((1+\tau)/2\big)\big)} \cdot \frac{1}{z^3}.$$

On peut alors démontrer le résultat suivant:

LEMME 5.3. *Les fonctions translatées de la fonction T_1 par les points de 2-division satisfont à la relation:*

$$T_1(z)\,T_1\left(z+\frac{1}{2}\right)T_1\left(z+\frac{\tau}{2}\right)T_1\left(z+\frac{1+\tau}{2}\right) = \lambda(\tau)^2\big(1-\lambda(\tau)\big)^2. \tag{8}$$

Démonstration. Le membre de gauche est une fonction elliptique de diviseur nul; c'est donc une constante que l'on évalue en faisant tendre z vers 0 et en utilisant les équivalents pour T_1 rappelés ci-dessus.

On peut démontrer l'analogue, pour la fonction T_1, de la formule de la proposition 5.1.

PROPOSITION 5.4. *Soit $v \equiv 1 \bmod \mathrm{rad}(2)$ un élément de $\mathbf{Z}_k$. On a la relation:*

$$\eta_v\big(\lambda(\tau)\big(1-\lambda(\tau)\big)\big)^{(N(v)-1)/2} T_1(vz) = \prod_{\substack{\alpha \in E_\tau \\ v\alpha = 0}} T_1(z \mp \alpha) \quad \text{avec } \eta_v^4 = 1. \tag{9}$$

Démonstration. Les deux membres de la relation sont des fonctions elliptiques de z qui ont même diviseur, leur quotient est une constante. On divise les deux membres par $T_1(z)$ puis on fait successivement tendre z vers 0, $1/2$, $\tau/2$, $(1+\tau)/2$. On fait alors le produit des quatre relations obtenues et on conclut en utilisant le lemme 5.3.

COROLLAIRE 5.5. *Si $v \in \mathbf{Z}_k$, $v \equiv 1 \bmod \mathrm{rad}(2)$ les valeurs de T_1 aux points de v-division de E_τ satisfont à la formule du produit:*

$$\eta_v\, v\big(\lambda(\tau)\big(1-\lambda(\tau)\big)\big)^{(N(v)-1)/2} = \prod_{\substack{\alpha \in E_\tau - \{0\} \\ v\alpha = 0}} T_1(\alpha) \quad \text{avec } \eta_v^4 = 1. \tag{10}$$

6. Multiplication sur E_τ. Soit $\mathfrak{f}$ un idéal entier impair de $\mathbf{Z}_k$ de norme n. Si α est un point primitif de $\mathfrak{f}$-division de E_τ c'est également un point de n-division. α est un zéro de la fonction $T(nz)$. On sait également que $T(\alpha)$ engendre le corps $k^{(\mathfrak{f})}k^{(2)}$ sur $k^{(2)}$. On construit par récurrence des polynômes dont les $T(\alpha)$ sont racines lorsque n varie. L'étude de ces polynômes nous permet dans le paragraphe 8 de mettre en évidence des congruences satisfaites par les $T(\alpha)$.

La fonction qui à z associe $T(nz)$ est une fonction paire. Comme T est une fonction homographique de $\wp$ il existe deux polynômes P et Q tels que $T(nz) = P\big(T(z)\big)/Q\big(T(z)\big)$.

Posons

$$Z_1 = N_1 = 1, \quad Z_n = \prod_\alpha{}'\big(X - T(\alpha)\big), \quad N_n = n\prod_\alpha{}'\left(X - T\left(\alpha+\frac{1+\tau}{2}\right)\right)$$

où $\prod'_\alpha$ désigne le produit sur un demi-système de points de n-division non nuls de E_τ.

LEMME 6.1. *La fonction $T(nz)$ est égale à $T(z)\dfrac{Z_n\big(T(z)\big)^2}{N_n\big(T(z)\big)^2}$.*

Démonstration. Les deux fonctions ont même diviseur, leur quotient est une constante c. On a donc

$$n^2 \frac{T(nz)}{T(z)} = c\prod_\alpha{}'\left(\frac{T(z)-T(\alpha)}{T(z)-T\big(\alpha+(1+\tau)/2\big)}\right)^2.$$

On fait alors tendre z vers 0 puis on utilise la formule d'inversion (2) et la formule du produit (7) pour obtenir l'égalité annoncée.

Le théorème suivant est la première étape pour déterminer les polynômes Z_n et N_n.

THÉORÈME 6.2. *Le polynôme Z_3 est égal à*

$$X^4-6\lambda(\tau)X^2+4\lambda(\tau)(\lambda(\tau)+1)X-3\lambda(\tau)^2$$

et les polynômes Z_{n-4}, Z_{n-2}, N_{n-2}, Z_n sont liés par la relation:

$$(11)\qquad (X^2-\lambda(\tau))^2 Z_{n-2}^2-4\lambda(\tau)(X-1)(X-\lambda(\tau))N_{n-2}^2 = Z_n Z_{n-4}.$$

Démonstration. La démonstration est analogue à celle de [3], chapitre 4; les seules différences proviennent des formules de duplication utilisées.

La proposition suivante donne le lien entre les polynômes Z_n et N_n.

PROPOSITION 6.3. *Le polynôme N_n se déduit du polynôme Z_n au moyen de la formule*

$$(12)\qquad N_n(X) = (-1)^{(n-1)/2}\lambda(\tau)^{(1-n^2)/4} X^{(n^2-1)/2} Z_n\left(\frac{\lambda(\tau)}{X}\right).$$

Démonstration. On utilise le fait que N_n, Z_n sont premiers entre eux par construction et de degré $(n^2-1)/2$. Si on remplace z par $z+(1+\tau)/2$ dans $T(nz)$ on obtient

$$\frac{1}{T(nz)} = \frac{1}{T(z)}\cdot\frac{U_n^2(T(z))}{V_n^2(T(z))} = \frac{1}{T(z)}\cdot\frac{N_n(T(z))^2}{Z_n(T(z))^2}$$

où l'on a posé

$$U_n = X^{(n^2-1)/2} Z_n\left(\frac{\lambda(\tau)}{X}\right), \qquad V_n = X^{(n^2-1)/2} N_n\left(\frac{\lambda(\tau)}{X}\right).$$

On en déduit l'existence d'une constante c_n telle que $Z_n = c_n V_n$, $N_n = \varepsilon c_n U_n$, avec $\varepsilon = \pm 1$. Déterminons c_n et ε. Si on évalue en 0 les relations ci-dessus on obtient $Z_n(0) = c_n n\lambda(\tau)^{(n^2-1)/2}$, $N_n(0) = \varepsilon c_n \lambda(\tau)^{(n^2-1)/2}$. On en déduit une expression de $Z_n(0)N_n(0)$ que l'on compare à ce que l'on obtient par construction des polynômes Z_n, N_n et application de la formule d'inversion:

$$\varepsilon n c_n^2 \lambda(\tau)^{n^2-1} = n\lambda(\tau)^{(n^2-1)/2}$$

c_n est donc de la forme $i^r \lambda(\tau)^{(1-n^2)/4}$.

On peut constater en utilisant les formules de récurrence qu'en fait

$$c_n = (-1)^{(n-1)/2}\lambda(\tau)^{(1-n^2)/4} \quad \text{et} \quad \varepsilon = +1.$$

Ceci nous permet donc, par récurrence, de construire tous les polynômes Z_n et N_n. On en déduit que les polynômes N_{n-4}, N_{n-2}, Z_{n-2}, N_n vérifient une formule de récurrence analogue à celle démontrée dans le théorème 6.2.

COROLLAIRE 6.4. *Les polynômes N_{n-4}, N_{n-2}, Z_{n-2}, N_n sont liés par la relation:*

$$(13)\qquad (X^2-\lambda(\tau))^2 N_{n-2}^2-4X^2(X-1)(X-\lambda(\tau))Z_{n-2}^2 = N_n N_{n-4}.$$

COROLLAIRE 6.5. *Les polynômes Z_n, N_n appartiennent à $\boldsymbol{Z}[\lambda(\tau), X]$.*

COROLLAIRE 6.6. *Les polynômes Z_n évalués en 1 valent $(\lambda(\tau)-1)^{(n^2-1)/4}$.*

Les deux derniers corollaires résultent de l'application des formules de récurrence.

On avait remarqué au paragraphe 5 que la formule du produit reste vraie pour $\nu = n$ impair, même quand la courbe E_τ n'admet pas de multiplication complexe. Les résultats de ce paragraphe restent donc valables dans ce contexte.

Toutes les formules démontrées font apparaître le rôle joué par les nombres $\lambda(\tau)$, $\lambda(\tau)(1-\lambda(\tau))$, $\sqrt{\lambda(\tau)}$, ... Le but du paragraphe suivant est d'étudier les propriétés arithmétiques de ces nombres.

7. Propriétés arithmétiques de certaines valeurs de la fonction de Legendre. On a déjà remarqué que la fonction λ est une fonction modulaire de niveau 2. Le calcul de ses images par $\mathrm{SL}_2(\boldsymbol{Z})$ est classique et montre que $\lambda(1-\lambda)$ est une fonction modulaire pour $\Gamma_0(2)$ (voir [3], ch.VII). Cette fonction n'ayant ni zéro ni pôle sur $\mathscr{H}$ ceux-ci sont concentrés aux pointes 0 et ∞ du compactifié de $X_0(2) = \Gamma_0(2)\backslash\mathscr{H}$. Si Δ est la forme modulaire classique de poids 12, on a:

THÉORÈME 7.1. *La fonction $\lambda(1-\lambda)$ associe à τ le nombre $-2^{-8}\dfrac{\Delta(\tau)}{\Delta(2\tau)}$. Si 2 est inerte dans $k/\boldsymbol{Q}$, $\lambda(\tau)$ et $1-\lambda(\tau)$ sont des unités de $k^{(2)}$, si 2 est ramifié dans $k/\boldsymbol{Q}$, $\lambda(\tau)$ est une unité de $k^{(2)}$ et $\lambda(\tau)-1$ est associé à 2, si 2 est décomposé dans $k/\boldsymbol{Q}$, $\lambda(\tau)(1-\lambda(\tau))$ est associé à 2^4.*

Démonstration. On calcule le premier terme du développement en série de Fourier de $\lambda(1-\lambda)$ aux pointes de $X_0(2)$. En utilisant les formules de [3], p. 115 on trouve $-2^{-8}e^{2i\pi\tau}$ à l'infini et $-2^4 e^{i\pi\tau}$ en zéro. On compare ce développement avec celui de $\Delta(2\tau)/\Delta(\tau)$ (cf. [3], p. 111) ce qui donne la première partie du théorème.

Le théorème IX, 5.10 de [3] prouve que si 2 est inerte (resp. ramifié, resp. décomposé) $\Delta(2\tau)/\Delta(\tau)$ est associé à 2^8 (resp. 2^9, resp. 2^{12}): ceci montre que $\lambda(\tau)$ est un entier algébrique dans tous les cas. Si 2 est inerte, $\lambda(\tau)(\lambda(\tau)-1)$ est une unité, il en est donc de même de $\lambda(\tau)$ et $\lambda(\tau)-1$ pris séparément. Il reste à voir ce qu'il en est lorsque 2 est ramifié dans $k/\boldsymbol{Q}$. On a vu (cf. proposition 3.3) que le conjugué de $\lambda(\tau)$ dans $k^{(2)}/H_k$ est alors $1/\lambda(\tau)$ donc $\lambda(\tau)$ est une unité.

COROLLAIRE 7.2. *Soit ν un entier de $\boldsymbol{Z}_k$, premier à 2 et α un point de ν-division de E_τ, $T(\alpha)$ et $T_1(\alpha)$ sont des entiers algébriques et si 2 est inerte dans $k/\boldsymbol{Q}$, $T(\alpha)-1$ est une unité.*

Démonstration. $n = N_{k/\mathbf{Q}}(v)$ est un entier impair, α est donc un point de n-division de E_τ, $T(\alpha)$ est racine de Z_n polynôme unitaire à coefficients entiers dans $k^{(2)}$, c'est donc un entier algébrique. $Y = T(\alpha)-1$ est racine de $Z_n(X+1)$ dont le coefficient constant $Z_n(1) = (1-\lambda(\tau))^{(n^2-1)/4}$ est une unité si 2 est inerte dans $k/\mathbf{Q}$.

COROLLAIRE 7.3. *Si α est un point de n-division de E_τ, n impair, $T(\alpha)$ a une valuation nulle aux places ne divisant pas $2n$.*

Démonstration. Les $T(\alpha)$ étant entiers le résultat se déduit immédiatement de la formule (7).

On a vu (proposition 3.4) que si 2 est ramifié dans $k/\mathbf{Q}$, $\lambda(\tau)$ admet une racine carrée dans $k^{(2)}$. Le conjugué de $\lambda(\tau)$ dans $k^{(2)}/H_k$ étant $1/\lambda(\tau)$, celui de $\sqrt{\lambda(\tau)}$ est $\pm 1/\sqrt{\lambda(\tau)}$. La fin de ce paragraphe est consacrée à la détermination de ce signe.

Rappelons tout d'abord des formules dont on peut trouver la démonstration dans [9], chapitre 18. En notant $q = e^{2i\pi\tau}$, la fonction λ admet un développement en produit infini

$$\lambda(\tau) = -2^{-4} q^{-1/2} \prod_{n=1}^{\infty} \left(\frac{1-q^{n-1/2}}{1+q^n}\right)^8;$$

on peut de même exprimer la fonction λ au moyen de la fonction σ de Weierstrass et des quasi périodes $\eta(1)$, $\eta(\tau)$ de la fonction ζ de Weierstrass associée au réseau de base 1, τ:

$$\lambda(\tau) = e^{\{\eta(1;\tau,1) - \eta(\tau;\tau,1)\}(1+\tau)/2} \frac{\sigma^4(\tau/2;\tau,1)}{\sigma^4(1/2;\tau,1)}.$$

Ces formules montrent que l'on peut définir sur $\mathscr{H}$ une fonction holomorphe dont le carré est égal à λ:

$$\sqrt{\lambda(\tau)} = e^{\frac{\{\eta(1;\tau,1) - \eta(\tau;\tau,1)\}}{2} \cdot \frac{1+\tau}{2}} \frac{\sigma^2(\tau/2;\tau,1)}{\sigma^2(1/2;\tau,1)}.$$

Compte-tenu des relations fonctionnelles et des propriétés d'homogénéité il est aisé de voir que $\sqrt{\lambda}$ est une fonction modulaire de niveau 4 invariante par la matrice $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ de $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})/\{\pm 1\}$. Le développement en produit infini montre que la fonction $i\sqrt{\lambda}$ a un développement en série de Fourier au voisinage de l'infini dont les coefficients sont rationnels. Il s'ensuit (cf. [10], ch.6, § 3, Th.3) que l'image de $\sqrt{\lambda}$ par l'élément $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ de $\mathrm{GL}_2(\mathbf{Z}/4\mathbf{Z})/\{\pm 1\}$ est $-\sqrt{\lambda}$.

Si on considère un idèle unité u dont les composantes sont égales à 1 pour les places premières à 2, la multiplication par u dans l'anneau des adèles de k définit un élément de $\mathrm{GL}_2(\mathbf{Z}/4\mathbf{Z})/\{\pm 1\}$. La loi de réciprocité de Shimura associe à cette matrice l'automorphisme $(u^{-1}, k) \in \mathrm{Gal}(k^{(4)}/H_k)$ de la théorie du corps de classes (cf. [10], ch.11).

PROPOSITION 7.4. *Le conjugué de $\sqrt{\lambda(\tau)}$ dans $k^{(2)}/H_k$, lorsque $k/\mathbf{Q}$ est ramifiée en 2 est égal à $-1/\sqrt{\lambda(\tau)}$.*

Démonstration. Supposons d'abord $d \equiv 2 \bmod 4$, $(\mathbf{Z}_k/4\mathbf{Z}_k)^*/\{\pm 1\}$ est cyclique d'ordre 4 (cf. proposition 4.3). Localement, $\sqrt{-d}$ se comporte comme une uniformisante en 2. Prenons pour idèle unité de la discussion précédente l'idèle égal à $1+\sqrt{-d}$ pour la place au-dessus de 2. Rappelons que nous avons choisi pour base de $\mathbf{Z}_k$ (cf. paragraphe 2) $\tau = \sqrt{-d}-1$, 1. La matrice de la multiplication par $1+\sqrt{-d}$ dans cette base est

$$\begin{bmatrix} 0 & 1 \\ -d-1 & 2 \end{bmatrix} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix} \bmod 4$$

dont l'inverse dans $\mathrm{GL}_2(\mathbf{Z}/4\mathbf{Z})/(\pm 1)$ est $\begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Le conjugué de $\sqrt{\lambda(\tau)}$ est donc $-\sqrt{\lambda((2\tau-1)/\tau)}$. En utilisant l'expression de $\sqrt{\lambda}$ au moyen des fonctions σ on trouve $-1/\sqrt{\lambda(\tau)}$.

Supposons maintenant $d \equiv 1 \bmod 4$. L'élément $\sqrt{-d}$ est une unité en 2, la base de $\mathbf{Z}_k$ que nous avons choisie est $\tau = \sqrt{-d}$, 1. La matrice de la multiplication par τ suivant cette base est $\begin{bmatrix} 0 & 1 \\ -d & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \bmod 4$. Cette matrice étant dans $\mathrm{SL}_2(\mathbf{Z}/4\mathbf{Z})/(\pm 1)$ le conjugué de $\sqrt{\lambda(\tau)}$ est $\sqrt{\lambda(-1/\tau)}$. L'utilisation de l'expression de $\sqrt{\lambda}$ au moyen de la fonction σ nous donne également $-1/\sqrt{\lambda(\tau)}$.

8. Congruences pour $T(\alpha)$, $T_1(\alpha)$ lorsque 2 n'est pas inerte dans $k/\mathbf{Q}$. On a remarqué que les formules du produit pour les fonctions T, T_1 font apparaître, via $\lambda(\tau)$, $1-\lambda(\tau)$, des idéaux premiers au-dessus de 2. Nous allons montrer que ces idéaux se répartissent également entre les différents facteurs du produit.

PROPOSITION 8.1. *Si 2 est décomposé dans $k/\mathbf{Q}$ et α un point de division d'ordre n impair de E_τ alors $T(\alpha)/\sqrt{\lambda(\tau)}$ est un entier algébrique premier à 2.*

Démonstration. Soit $\mathfrak{P}$ un idéal premier de H_k divisant $\lambda(\tau)$, d'après le théorème 7.1 on sait que $\lambda(\tau) \equiv 0 \bmod \mathfrak{P}^4$ et $\lambda(\tau) \not\equiv 0 \bmod \mathfrak{P}^5$. Dans les polynômes Z_n et N_n posons $X = \sqrt{\lambda(\tau)}\, Y$. On constate, lorsque $n = 1$, $n = 3$ que les coefficients sont des entiers algébriques congrus à 0 modulo $\mathfrak{P}^{n^2-1}$. Ceci étant vrai pour tous les $\mathfrak{P}$ divisant $\sqrt{\lambda(\tau)}$, on peut diviser les polynômes obtenus par $\lambda(\tau)^{(n^2-1)/4}$, Z_n devient unitaire à coefficients entiers, N_n devient

un polynôme à coefficients entiers. Utilisons les formules de récurrence pour montrer que ces propriétés sont valables pour tout n. Avec ce changement de variable la formule 11 devient:

$$\lambda(\tau)^2(1-Y^2)^2 Z_{n-2}^2\left(\sqrt{\lambda(\tau)}\,Y\right)-4\lambda(\tau)\sqrt{\lambda(\tau)}\left(\sqrt{\lambda(\tau)}\,Y-1\right)\left(Y-\sqrt{\lambda(\tau)}\right)$$
$$\times N_{n-2}^2\left(\sqrt{\lambda(\tau)}\,Y\right)=Z_n\left(\sqrt{\lambda(\tau)}\,Y\right)Z_{n-4}\left(\sqrt{\lambda(\tau)}\,Y\right).$$

Dans le membre de gauche, on peut mettre $\lambda(\tau)^{((n-2)^2+3)/2}$ facteur d'un polynôme unitaire à coefficients entiers (le terme de plus haut degré provenant de $\lambda(\tau)^2(1-Y^2)^2 Z_{n-2}^2\left(\sqrt{\lambda(\tau)}\,Y\right)$).

Dans le membre de droite $\lambda(\tau)^{((n-4)^2-1)/4}$ est facteur d'un polynôme unitaire à coefficients entiers. Il s'ensuit que les coefficients de $Z_n\left(\sqrt{\lambda(\tau)}\,Y\right)$ sont divisibles par $\lambda(\tau)^{(n^2-1)/4}$ et qu'après division on obtient un polynôme unitaire. Le même procédé est valable pour la formule (13). On en déduit que les $T(\alpha)/\sqrt{\lambda(\tau)}$ sont des entiers algébriques. Le terme constant de Z_n étant $(-1)^{(n-1)/2}n\lambda^{(n^2-1)/4}$ la seconde propriété est immédiate.

COROLLAIRE 8.2. *Si 2 est décomposé dans $k/\mathbf{Q}$ et α un point d'ordre impair de E_τ, $T_1(\alpha)/\sqrt{\lambda(\tau)}$ est un entier algébrique premier avec les idéaux divisant $\lambda(\tau)$.*

Démonstration. On écrit l'équation de la courbe sous la forme

$$\left(\frac{T_1}{\sqrt{\lambda(\tau)}}\right)^2=\frac{T}{\sqrt{\lambda(\tau)}}(T-1)\left(\frac{T}{\sqrt{\lambda(\tau)}}-\sqrt{\lambda(\tau)}\right);$$

quand on évalue en α, les termes du produit sont tous premiers à $\lambda(\tau)$.

Intéressons nous maintenant aux idéaux premiers qui divisent $1-\lambda(\tau)$. Lorsque 2 est décomposé dans $k/\mathbf{Q}$ on pose $\pi=\sqrt{1-\lambda(\tau)}$. Si 2 est ramifié dans $k/\mathbf{Q}$ on sait (cf. théorème 7.1) que $\lambda(\tau)-1$ est associé à 2. Comme $\lambda(\tau)-1=\left(\sqrt{\lambda(\tau)}-1\right)\left(\sqrt{\lambda(\tau)}+1\right)$ les éléments $\sqrt{\lambda(\tau)}-1$ et $\sqrt{\lambda(\tau)}+1$ sont associés au produit des idéaux premiers au-dessus de 2 dans H_k. On pose $\pi=\sqrt{\lambda(\tau)}-1$. Dans les deux cas $\lambda(\tau)-1$ est associé à π^2. Nous pouvons alors énoncer la proposition:

PROPOSITION 8.3. *Avec les notations ci-dessus, si 2 n'est pas inerte dans $k/\mathbf{Q}$ et si α est un point de division d'ordre n impair de E_τ alors $(T(\alpha)-1)/\pi$ est une unité.*

Démonstration. Posons $X=1+\pi Y$. On fait ce changement de variable pour $n=1$, $n=3$. Pour $n=3$ on obtient:

Z_3 se transforme en

$$\pi^4 Y^4+4\pi^3 Y^3+6\pi^2(1-\lambda(\tau))Y^2+4\pi(1-\lambda(\tau))^2 Y+(\lambda(\tau)-1)^2,$$

N_3 se transforme en

$$3\pi^4 Y^4+4\pi^3(2-\lambda(\tau))Y^3+6\pi^2(1-\lambda(\tau))Y^2-(\lambda(\tau)-1)^2.$$

On constate qu'après division par π^4 on obtient des polynômes à coefficients entiers et que les racines du transformé de Z_3 sont des unités. On remarque (cf. démonstration du corollaire 7.2) qu'après le changement de variable $X=1+\pi Y$ puis division par $\pi^{(n^2-1)/2}$ le terme constant est une unité. Il est évident que le polynôme obtenu est unitaire, il ne reste donc qu'à vérifier que les autres coefficients sont des entiers algébriques.

Supposons donc que dans les polynômes Z_{n-4}, N_{n-4} (resp. Z_{n-2}, N_{n-2}) le changement de variable $X=1+\pi Y$ suivi de la division par $\pi^{((n-4)^2-1)/2}$ (resp. $\pi^{((n-2)^2-1)/2}$) donne des polynômes à coefficients entiers. Voyons ce qu'il en est pour Z_n et N_n (on n'explique que pour Z_n, la démarche étant similaire pour N_n). Le changement de variable $X=1+\pi Y$ transforme $(X^2-\lambda(\tau))^2$ en

$$\pi^4 Y^4+4\pi^3 Y^2+2\pi^2(3-\lambda(\tau))+4\pi(1-\lambda(\tau))Y+(\lambda(\tau)-1)^2$$

et $4\lambda(\tau)\left(X^2-(\lambda(\tau)+1)X+\lambda(\tau)\right)$ en

$$4\lambda(\tau)\pi^2 Y^2+4\pi\lambda(\tau)(1-\lambda(\tau))Y.$$

On constate que les coefficients de ces deux polynômes sont congrus à 0 mod π^4. On reporte ceci dans la formule de récurrence (11) et l'on constate que les coefficients de $Z_n(1+\pi Y)$ sont divisibles par $\pi^{(n^2-1)/2}$, ce qui termine la démonstration.

On en déduit:

COROLLAIRE 8.4. *En conservant les notations de la proposition précédente, si 2 n'est pas inerte dans $k/\mathbf{Q}$ et si α est un point de division d'ordre impair de E_τ, $T_1(\alpha)/\pi$ est un entier algébrique premier à π.*

Démonstration. On écrit l'équation de la courbe sous la forme

$$\left(\frac{T_1}{\pi}\right)^2=T\left(\frac{T-1}{\pi}\right)\left(\frac{T-1+1-\lambda(\tau)}{\pi}\right)$$

et on remarque que pour $z=\alpha$, $T(\alpha)$, $(T(\alpha)-1)/\pi$ sont des entiers premiers à π, et $(1-\lambda(\tau))/\pi\equiv 0 \bmod(\pi)$, ce qui suffit pour démontrer le corollaire.

On peut résumer les deux corollaires en énonçant:

COROLLAIRE 8.5. *Si 2 est ramifié (resp. décomposé) dans $k/\mathbf{Q}$, et α un point d'ordre impair de E_τ, $T_1(\alpha)^2/2$ (resp. $T_1(\alpha)/2^2$) est un entier algébrique premier à 2.*

L'utilisation de l'équation de E_τ et les formules du produit permettent également d'énoncer la proposition suivante:

PROPOSITION 8.6. *Soit α un point d'ordre n impair de E_τ, alors:*

(i) *Si 2 est inerte dans $k/\mathbf{Q}$, $T_1(\alpha)^2$ est associé à $T(\alpha)$.*

(ii) *Si 2 est ramifié dans $k/\mathbf{Q}$, $T_1(\alpha)^2$ est associé à $2T(\alpha)$.*

(iii) *Si 2 est décomposé dans $k/\mathbf{Q}$, $T_1(\alpha)^2/2^4$ est associé à $T(\alpha)/\sqrt{\lambda(\tau)}$.*

Démonstration. (i) Si 2 est inerte dans $k/\mathbf{Q}$, α d'ordre n, l'élément $T_1(\alpha)^2/T(\alpha)=(T(\alpha)-1)(T(\alpha)-\lambda(\tau))$ est un entier algébrique. Faisons le

produit de ces égalités lorsque α parcourt l'ensemble des points de n-division non nuls de E_τ:

$$\lambda(\tau)^{(N(v)-1)/2}(1-\lambda(\tau))^{N(v)-1} = \prod_{\substack{\alpha\in E_\tau-\{0\}\\ n\alpha=0}} (T(\alpha)-1)(T(\alpha)-\lambda(\tau))$$

il en résulte que les $T(\alpha)-\lambda(\tau)$ et $T(\alpha)-1$ sont des unités ce qui donne le résultat dans ce cas.

(ii) Si 2 est ramifié dans $k/\boldsymbol{Q}$, la formule du produit peut s'écrire pour $v \equiv 1 \bmod \mathrm{rad}\,(2)$:

$$n_v v\lambda(\tau)^{(N(v)-1)/2} = \prod_{\substack{\alpha\in E_\tau-\{0\}\\ v\alpha=0}} \frac{T_1(\alpha)}{\sqrt{\lambda(\tau)-1}}$$

avec $\eta_v^4 = 1$, $\lambda(\tau)$ une unité, $T_1(\alpha)/\sqrt{\lambda(\tau)-1}$ entier.

On transforme l'équation de E_τ en:

$$\left(\frac{T_1}{\sqrt{1-\lambda(\tau)}}\right)^2 = T\left(\frac{T-1}{\sqrt{1-\lambda(\tau)}}\right)\left(\frac{T-\lambda(\tau)}{\sqrt{1-\lambda(\tau)}}\right)$$

les facteurs du produit de droite étant des entiers. On évalue les deux membres aux points de v-division non nuls; les facteurs, à droite, sont des entiers. On fait le produit

$$\pm v^2\lambda(\tau)^{N(v)-1} = \pm v^2\lambda(\tau)^{(N(v)-1)/2} \prod_{\substack{\alpha\in E_\tau-\{0\}\\ v\alpha=0}} \frac{T(\alpha)-1}{\sqrt{1-\lambda(\tau)}}\cdot\frac{T(\alpha)-\lambda(\tau)}{\sqrt{1-\lambda(\tau)}}.$$

Il en résulte que les $(T(\alpha)-\lambda(\tau))/\sqrt{1-\lambda(\tau)}$ sont des unités et donc que $T_1(\alpha)^2$ est associé à $2T(\alpha)$.

(iii) Si 2 est décomposé dans $k/\boldsymbol{Q}$, on peut réécrire les formules du produit:

$$\pm v^2 = \prod_{\substack{\alpha\in E_\tau-\{0\}\\ v\alpha=0}} \frac{T(\alpha)}{\sqrt{\lambda(\tau)}}, \qquad \eta_v v = \prod_{\substack{\alpha\in E_\tau-\{0\}\\ v\alpha=0}} \frac{T_1(\alpha)}{\sqrt{\lambda(\tau)}\sqrt{1-\lambda(\tau)}}.$$

On transforme également l'équation de E_τ:

$$\left(\frac{T_1}{\sqrt{\lambda(\tau)}\sqrt{1-\lambda(\tau)}}\right)^2 = \frac{T}{\sqrt{\lambda(\tau)}}\cdot\frac{T-1}{\sqrt{1-\lambda(\tau)}}\cdot\frac{T-\lambda(\tau)}{\sqrt{\lambda(\tau)}\sqrt{1-\lambda(\tau)}}.$$

Comme précédemment on évalue aux points de v-division non nuls de E_τ et on fait le produit de ces relations pour obtenir (iii).

9. Divisibilité de $T(u)-T(v)$ par les idéaux au-dessus de 2, u et v d'ordre impair. Utilisons les propriétés démontrées dans le paragraphe précédent pour transformer le second membre de la formule de différence, en faisant apparaître au maximum les entiers premiers à 2:

Si 2 est décomposé:

$$2^6\frac{T(u+v)}{\sqrt{\lambda(\tau)}}\cdot\frac{T(u-v)}{\sqrt{\lambda(\tau)}}\cdot\frac{T_1(u)}{2^2}\cdot\frac{T_1(v)}{2^2},$$

si 2 est ramifié:

$$\frac{2^3}{\lambda(\tau)}T(u+v)\,T(u-v)\frac{T_1(u)\,T_1(v)}{2},$$

si 2 est inerte:

$$\frac{2^2}{\lambda(\tau)}T(u+v)\,T(u-v)\,T_1(u)\,T_1(v).$$

Dans les deux premiers cas l'exposant de 2 est multiple de 3. Si 2 est inerte dans $k/\boldsymbol{Q}$, l'extension $k^{(2)}/H_k$ est de degré 3 et le produit $\mathfrak{J}$ des idéaux premiers au-dessus de 2 dans $k^{(2)}$ est principal (proposition 4.1).

Notation. On pose, si 2 est décomposé (resp. ramifié, resp. inerte) dans $k/\boldsymbol{Q}$, $\varrho = 2^2$ (resp. 2, resp. un générateur de $\mathfrak{J}^2$).

On peut alors énoncer le théorème suivant qui s'inspire du Théorème 208 de [8].

THÉORÈME 9.1. *Soient u et v deux points d'ordre impair de E_τ, $u \neq \pm v$; $u \neq 0$, $v \neq 0$ alors $(T(u)-T(v))/\varrho$ est un entier algébrique premier à 2.*

Démonstration. L'ordre de u et v est impair, $u \neq \pm v$, donc les points $u+v$ et $u-v$ sont distincts et différents de l'élément neutre. Avec les notations ci-dessus et les résultats du paragraphe précédent on peut écrire la formule de différence:

$$(T(u)-T(v))^2(T(u+v)-T(u-v)) = \varrho^3 X(u, v)$$

où $X(u, v)$ est premier à 2. Si on remplace u par $u+v$, v par $u-v$:

$$(T(u+v)-T(u-v))^2(T(2u)-T(2v)) = \varrho^3 X(u+v, u-v).$$

On élève la première relation au carré, on la divise par la seconde, ce qui donne:

$$\frac{(T(u)-T(v))^4}{T(2u)-T(2v)} = \varrho^3 Y_1(u, v) \quad \text{avec } Y_1(u, v) \text{ premier à } 2.$$

Par une récurrence élémentaire on obtient:

$$\frac{(T(u)-T(v))^{2^{2s}}}{T(2^s u)-T(2^s v)} = \varrho^{2^{2s}-1} Y_s(u, v) \quad \text{avec } Y_s(u, v) \text{ premier à } 2,$$

u et v étant d'ordre impair, il existe s tel que $2^s u = u$, $2^s v = v$, ce qui montre bien que $T(u)-T(v) \equiv 0 \pmod{\varrho}$ et que l'entier quotient $(T(u)-T(v))/\varrho$ est premier à 2.

Lorsque u et v sont d'ordre impair on écrit donc la formule de différence de la manière suivante:

2 décomposé:

$$\text{(14a)}\quad \left(\frac{T(u)-T(v)}{\varrho}\right)^2\left(\frac{T(u+v)-T(u-v)}{\varrho}\right)=\frac{T(u+v)}{\sqrt{\lambda(\tau)}}\cdot\frac{T(u-v)}{\sqrt{\lambda(\tau)}}\cdot\frac{T_1(u)}{\varrho}\cdot\frac{T_1(v)}{\varrho},$$

2 ramifié:

$$\text{(14b)}\quad \left(\frac{T(u)-T(v)}{\varrho}\right)^2\left(\frac{T(u+v)-T(u-v)}{\varrho}\right)=\frac{1}{\lambda(\tau)}T(u+v)\,T(u-v)\frac{T_1(u)\,T_1(v)}{\varrho},$$

2 inerte:

$$\text{(14c)}\quad \left(\frac{T(u)-T(v)}{\varrho}\right)^2\left(\frac{T(u+v)-T(u-v)}{\varrho}\right)=\frac{1}{\lambda(\tau)}T(u+v)\,T(u-v)\,T_1(u)\,T_1(v),$$

les facteurs intervenant dans les produits étant premiers à 2.

10. Divisibilité de $T(\alpha)$, α d'ordre impair aux places premières à 2. On va d'abord établir le résultat suivant:

PROPOSITION 10.1. *Soit $\mathfrak{f}$ un idéal entier impair de $\mathbf{Z}_k$, γ et δ deux points primitifs de $\mathfrak{f}$-division de E_τ, les nombres $T(\gamma)$ et $T(\delta)$ sont associés.*

Démonstration. Il suffit de démontrer le résultat localement. Traitons séparément les places au-dessus de 2 et les autres.

La formule du produit montre que les seules places au-dessus de 2 divisant les entiers $T(\alpha)$, α d'ordre premier à 2, sont celles qui apparaissent dans l'entier $\lambda(\tau)$. Le théorème 7.1 et la proposition 8.1 nous assurent que $T(\gamma)$ et $T(\delta)$ ont même valuation pour les idéaux au-dessus de (2) dans $k^{(2)}k^{(\mathfrak{f})}$.

Considérons maintenant une place $\mathfrak{P}$ première à 2 dans $k^{(2)}k^{(\mathfrak{f})}$. Puisque γ et δ sont primitifs de $\mathfrak{f}$-division avec $\mathfrak{f}$ impair on peut trouver ν premier à $\mathfrak{f}$, $\nu\equiv 1 \bmod \mathrm{rad}\,(2)$ tel que $\nu\gamma=\delta$. La formule (6) avec $z=\gamma$ donne

$$\pm\lambda(\tau)^{(N(\nu)-1)/2}\,T(\delta)=T(\gamma)\prod_{\substack{\alpha\in E_\tau-\{0\}\\ \nu\alpha=0}}T(\gamma+\alpha).$$

Les points $\gamma+\alpha$ ont pour annulateur $\nu\mathfrak{f}$ qui est un idéal premier à 2, les nombres $T(\gamma+\alpha)$ sont des entiers algébriques, par conséquent la valuation en $\mathfrak{P}$ de $T(\gamma)$ est inférieure à celle de $T(\delta)$. On échange ensuite les rôles de γ et δ pour terminer la démonstration.

De cette proposition et de la proposition 8.6 on déduit immédiatement:

COROLLAIRE 10.2. *Soit $\mathfrak{f}$ un idéal entier impair de $\mathbf{Z}_k$, γ et δ deux points primitifs de $\mathfrak{f}$-division de E_τ, alors $T_1(\gamma)$ et $T_1(\delta)$ sont associés.*

De plus si 2 est inerte (resp. ramifié, resp. décomposé) dans $k/\mathbf{Q}$, $T_1(\gamma)\,T_1(\delta)$ (resp. $T_1(\gamma)\,T_1(\delta)/2$, resp. $T_1(\gamma)\,T_1(\delta)/2^4$) est associé à $T(\alpha)$.

Le lemme suivant est essentiel pour déterminer la valuation de $T(\alpha)$ pour les idéaux premiers à (2) dans $k^{(\mathfrak{f})}k^{(2)}$.

LEMME 10.3. *Soient $\mathfrak{f}$ un idéal entier impair de $\mathbf{Z}_k$, $\mathfrak{f}=\mathfrak{p}^r\mathfrak{q}$ où $\mathfrak{p}$ est un idéal premier qui divise $\mathfrak{f}$ et $\mathfrak{p}+\mathfrak{q}=\mathbf{Z}_k$, et $m\geqslant r$ tel que $\mathfrak{p}^m$ soit principal ($\mathfrak{p}^m=a\mathbf{Z}_k$); alors si γ est un point primitif de $\mathfrak{f}$-division de E_τ, 2 non décomposé (resp. 2 décomposé) alors $T(\gamma)$ (resp. $T(\gamma)/\sqrt{\lambda(\tau)}$) divise a.*

Démonstration. Soit $\nu\in\mathbf{Z}_k$, $\nu\equiv 1 \bmod \mathfrak{p}\,\mathrm{rad}(2)$, $\nu\equiv 0 \bmod \mathfrak{q}$. Le point $\nu\gamma$ est un point primitif de $\mathfrak{p}^r$-division, donc en particulier un point de $\mathfrak{p}^m$-division. D'après la formule (7) (et la proposition 8.1 si 2 est décomposé dans $k/\mathbf{Q}$) $T(\nu\gamma)$ (resp. $T(\nu\gamma)/\sqrt{\lambda(\tau)}$ si 2 est décomposé dans $k/\mathbf{Q}$) divise a. L'entier ν étant impair le même raisonnement montre que $T(\gamma)$ (resp. $T(\gamma)/\sqrt{\lambda(\tau)}$ si 2 est décomposé dans $k/\mathbf{Q}$) divise $T(\nu\gamma)$ (resp. $T(\nu\gamma)/\sqrt{\lambda(\tau)}$).

On en déduit immédiatement le corollaire suivant:

COROLLAIRE 10.4. *Soit $\mathfrak{f}$ un idéal entier impair de $\mathbf{Z}_k$ divisible par deux idéaux premiers distincts et γ un point primitif de $\mathfrak{f}$-division de E_τ; alors si 2 est non décomposé (resp. décomposé) dans $k/\mathbf{Q}$ $T(\gamma)$ (resp. $T(\gamma)/\sqrt{\lambda(\tau)}$) est une unité.*

On peut alors énoncer:

PROPOSITION 10.5. *Soit $\mathfrak{f}$ un idéal entier impair de $\mathbf{Z}_k$ si 2 n'est pas décomposé (resp. est décomposé) dans $k/\mathbf{Q}$*

$$\prod_{\substack{\alpha\in E_\tau\\ \mathrm{Ann}(\alpha)=\mathfrak{f}}}{}'\,T(\alpha)=\mathfrak{f}\mathbf{Z}_{k^{(2)}}\quad\left(\text{resp. }\prod_{\substack{\alpha\in E_\tau\\ \mathrm{Ann}(\alpha)=\mathfrak{f}}}{}'\frac{T(\alpha)}{\sqrt{\lambda(\tau)}}=\mathfrak{f}\mathbf{Z}_{k^{(2)}}\right).$$

Démonstration. Soient ν_1 et $\nu_2\in\mathfrak{f}$, $\nu_1\equiv\nu_2\equiv 1 \bmod \mathrm{rad}(2)$ tels que $\mathfrak{f}=(\nu_1,\nu_2)$.

Remarquons que les produits cités dans l'énoncé sont invariants par $\mathrm{Gal}(k^{(\mathfrak{f})}k^{(2)}/k^{(2)})$. Donnons la démonstration lorsque 2 n'est pas décomposé.

La formule (7) montre que $\prod'_{\substack{\alpha\in E_\tau-\{0\}\\ \nu_1\alpha=0}}T(\alpha)$ engendre l'idéal $\nu_1\mathbf{Z}_{k^{(2)}}$, de même avec ν_2, or ces deux produits contiennent $\prod'_{\substack{\alpha\in E_\tau\\ \mathrm{Ann}(\alpha)=\mathfrak{f}}}T(\alpha)$. Ce produit divise ν_1 et ν_2 donc il divise $\mathfrak{f}\mathbf{Z}_{k^{(2)}}$.

Soit maintenant $\mathfrak{q}$ un idéal premier à $\mathfrak{f}$ dans la classe de $\mathfrak{f}^{-1}$ tel que $\mathfrak{q}\mathfrak{f}=(a)$ avec $a\equiv 1 \bmod \mathrm{rad}(2)$. Dans la formule (7) on sépare les termes de la façon suivante:

$$\pm a^2\,\lambda(\tau)^{(N(a)-1)/2}=\Big(\prod_{\substack{\alpha\in E_\tau\\ \mathrm{Ann}(\alpha)=\mathfrak{f}}}{}'T(\alpha)\Big)^2\prod_{\substack{\beta\in E_\tau-\{0\}\\ \mathrm{Ann}(\beta)\neq\mathfrak{f}}}T(\beta).$$

Les points β ont pour annulateur $\mathfrak{q}$ ou un produit d'au moins deux idéaux premiers, le second produit est donc premier à $\mathfrak{f}$ et donc $\mathfrak{f}$ divise $\prod'_{\substack{\alpha\in E_\tau\\ \mathrm{Ann}(\alpha)=\mathfrak{f}}}T(\alpha)$ ce qui démontre le résultat.

Outre l'aspect constructif d'une forme faible du théorème des idéaux principaux cette proposition permet de trouver des générateurs de certains idéaux ambiges principaux:

COROLLAIRE 10.6. *Soit* $\mathfrak{f} = \mathfrak{p}^r$ *où* $\mathfrak{p}$ *est un idéal premier de* $\boldsymbol{Z}_k$, *premier à* 2, *si* 2 *n'est pas décomposé (resp. est décomposé) dans* $k/\boldsymbol{Q}$ *le produit des idéaux premiers au-dessus de* $\mathfrak{p}$ *dans* $k^{(2)}k^{(\mathfrak{p}^r)}$ *est engendré par* $T(\alpha)$ *(resp.* $T(\alpha)/\sqrt{\lambda(\tau)}$*) où* α *est un point primitif de* $\mathfrak{p}^r$*-division de* E_τ.

Démonstration. Lorsque 2 n'est pas décomposé dans $k/\boldsymbol{Q}$, on peut écrire que

$$\prod_{\substack{\beta\in E_\tau \\ \mathrm{Ann}(\beta)\mid \mathfrak{p}^r}}{}' T(\beta) = \prod_{\substack{\beta\in E_\tau \\ \mathrm{Ann}(\beta)\mid \mathfrak{p}^{r-1}}}{}' T(\beta) \prod_{\substack{\beta\in E_\tau \\ \mathrm{Ann}(\beta)=\mathfrak{p}^r}}{}' T(\beta)$$

engendre $(\mathfrak{p}\boldsymbol{Z}_{k^{(2)}})^r$ et $\prod_{\substack{\beta\in E_\tau \\ \mathrm{Ann}(\beta)\mid \mathfrak{p}^{r-1}}}{}' T(\beta)$ engendre $(\mathfrak{p}\boldsymbol{Z}_{k^{(2)}})^{r-1}$. Il s'ensuit que

$$\prod_{\substack{\beta\in E_\tau \\ \mathrm{Ann}(\beta)=\mathfrak{p}^r}}{}' T(\beta) = \mathfrak{p}\boldsymbol{Z}_{k^{(2)}}.$$

Les $T(\beta)$ avec $\mathrm{Ann}(\beta) = \mathfrak{p}^r$ étant 2 à 2 conjugués dans $k^{(2)}k^{(\mathfrak{p}^r)}/k^{(2)}$, chacun d'eux engendre donc le produit des idéaux premiers de $k^{(2)}k^{(\mathfrak{p}^r)}$ divisant $\mathfrak{p}$.

11. Démonstration du théorème 1.1. Soit $\mathfrak{f}$ un idéal entier impair de k, α un point primitif de $\mathfrak{f}$-division de E_τ. On sait que $k^{(2)}k^{(\mathfrak{f})}$ est engendré par $T(\alpha)$ sur $k^{(2)}$. Construisons l'élément dont les puissances forment une base de $\boldsymbol{Z}_{k^{(2)}k^{(\mathfrak{f})}}/\boldsymbol{Z}_{k^{(2)}}$. Supposons tout d'abord 3 décomposé ou ramifié dans $k/\boldsymbol{Q}$ et notons $\mathfrak{L}$ un idéal premier de $\boldsymbol{Z}_k$ divisant 3. Le corps $k^{(\mathfrak{L})}$ est égal à H_k, si β est un point primitif de $\mathfrak{L}$-division de E_τ alors $T(\beta)\in k^{(2)}$.

Notation. Si 3 n'est pas inerte dans $k/\boldsymbol{Q}$ on pose $\theta = (T(\alpha)-T(\beta))/\varrho$ (où ϱ est défini au début du paragraphe 9).

Supposons maintenant 3 inerte dans $k/\boldsymbol{Q}$; on choisit β élément primitif de 3-division de E_τ.

Si 2 est décomposé dans $k/\boldsymbol{Q}$, on sait que $T(\beta)\equiv 0 \bmod (\sqrt{\lambda(\tau)})$, $T(\beta)\equiv 1 \bmod (\sqrt{1-\lambda(\tau)})$, il existe donc $a\in k^{(2)}$ tel que $T(\beta)\equiv a \bmod (\varrho)$.

Si 2 est inerte ou ramifié, l'extension $k^{(2)}k^{(3)}/k^{(3)}$ est cyclique de degré 4 donc modérément ramifiée; il s'ensuit que $H^1(\mathrm{Gal}(k^{(2)}k^{(3)}/k^{(2)}), \boldsymbol{Z}_{k^{(2)}k^{(3)}}) = 0$. L'application

$$\sigma \mapsto \frac{\sigma(T(\beta))-T(\beta)}{\varrho}$$

étant un un-cocycle de $\mathrm{Gal}(k^{(2)}k^{(3)}/k^{(2)})$ à valeurs dans $\boldsymbol{Z}_{k^{(2)}k^{(3)}}$, c'est un un-cobord et l'on peut trouver b dans $\boldsymbol{Z}_{k^{(2)}k^{(3)}}$ tel que

$$\frac{\sigma(T(\beta))-T(\beta)}{\varrho} = \sigma(b)-b.$$

Il existe donc $a\in\boldsymbol{Z}_{k^{(2)}}$ tel que $T(\beta)\equiv a \bmod (\varrho)$.

Notation. Si 3 est inerte dans $k/\boldsymbol{Q}$ on pose $\theta = (T(\alpha)-a)/\varrho$ où a est un élément de $k^{(2)}$ congru à $T(\beta)$ modulo ϱ.

L'élément θ construit ci-dessus est un entier algébrique (théorème 9.1). La démonstration du théorème 1.1 se fait en calculant le discriminant du réseau engendré par les puissances de θ (par l'utilisation des formules (14)) et en montrant qu'il est égal au discriminant de $k^{(2)}k^{(\mathfrak{f})}/k^{(2)}$ calculé au moyen de la formule de Hasse [11].

(a) Etant donnée une extension L/K, on note $\delta(L/K)$ son discriminant. Calculons $\delta(k^{(2)}k^{(\mathfrak{f})}/k^{(2)})$; l'étude de la ramification montre que ceci est égal à $\delta(k^{(\mathfrak{f})}/H_k)$. On sait que

$$\delta(k^{(\mathfrak{f})}/k) = \delta(k^{(\mathfrak{f})}/H_k)^{[H_k:k]},$$

on peut donc se contenter de calculer ce dernier. Ce discriminant n'est divisible que par les idéaux premiers de k divisant $\mathfrak{f}$. Soit $\mathfrak{p}$ l'un de ces idéaux, calculons son exposant dans $\delta(k^{(\mathfrak{f})}/k)$; on écrit $\mathfrak{f} = \mathfrak{p}^r\mathfrak{b}$ avec $\mathfrak{b}$ premier à $\mathfrak{f}$ et on utilise le fait que $\delta(k^{(\mathfrak{f})}/k)$ est le produit des conducteurs des caractères de $k^{(\mathfrak{f})}/k$; le nombre de ceux d'entre eux dont le conducteur est divisible par $\mathfrak{p}^s$ $(1\leqslant s\leqslant r)$ est égal à:

$$[k^{(\mathfrak{b}\mathfrak{p}^s)}:k]-[k^{(\mathfrak{b}\mathfrak{p}^{s-1})}:k].$$

Ce nombre est déterminé au moyen du calcul du degré relatif d'un corps de rayon et vaut:

si $s>1$,

$$\mathfrak{b}\neq\boldsymbol{Z}_k \quad [k^{(\mathfrak{b})}:k](N(\mathfrak{p})-1)(N(\mathfrak{p})^{s-1}-N(\mathfrak{p})^{s-2}),$$

$$\mathfrak{b}=\boldsymbol{Z}_k \quad [H_k:k]\frac{N(\mathfrak{p})-1}{2}(N(\mathfrak{p})^{s-1}-N(\mathfrak{p})^{s-2});$$

si $s=1$,

$$\mathfrak{b}\neq\boldsymbol{Z}_k \quad [k^{(\mathfrak{b})}:k](N(\mathfrak{p})-2),$$

$$\mathfrak{b}=\boldsymbol{Z}_k \quad [H_k:k]\left(\frac{N(\mathfrak{p})-1}{2}-1\right).$$

On montre donc que la p-valuation de $\delta(k^{(\mathfrak{f})}/k)$ est égale à

$$[k^{(\mathfrak{b})}:k]\Big(N(\mathfrak{p})-2+\sum_{s=2}^{r} s(N(\mathfrak{p})-1)(N(\mathfrak{p})^{s-1}-N(\mathfrak{p})^{s-2})\Big)$$
$$= [k^{(\mathfrak{b})}:k]\big(rN(\mathfrak{p})^r-(r+1)N(\mathfrak{p})^{r-1}\big) \quad \text{si } \mathfrak{b}\neq\boldsymbol{Z}_k$$

et à

$$[H_k:k]\left(\frac{N(\mathfrak{p})-1}{2}-1+\sum_{s=2}^{r} s\frac{N(\mathfrak{p})-1}{2}(N(\mathfrak{p})^{s-1}-N(\mathfrak{p})^{s-2})\right)$$
$$= [H_k:k]\left(\frac{rN(\mathfrak{p})^r-(r+1)N(\mathfrak{p})^{r-1}-1}{2}\right) \quad \text{sinon.}$$

(b) Calculons maintenant le discriminant du réseau $1, \theta, \theta^2, \ldots, \theta^{n-1}$ où $n = [k^{(\mathfrak{f})}:H_k]$ dans l'extension $k^{(\mathfrak{f})}k^{(2)}/k^{(2)}$. La formule d'Euler nous dit que ce discriminant est égal à

$$\prod_{\sigma\in \mathrm{Gal}(k^{(2)}k^{(\mathfrak{f})}/k^{(2)})-\{\mathrm{id}\}} N_{k^{(\mathfrak{f})}k^{(2)}/k^{(2)}}(\theta-\sigma(\theta)).$$

Et donc, par construction des éléments θ à:

$$\prod_{\sigma\in \mathrm{Gal}(k^{(2)}k^{(\mathfrak{f})}/k^{(2)})-\{\mathrm{id}\}} N_{k^{(\mathfrak{f})}k^{(2)}/k^{(2)}}\left(\frac{T(\alpha)-\sigma(T(\alpha))}{\varrho}\right).$$

Soit alors U (resp. $U_{\mathfrak{f}}$) le groupe des idèles unités (resp. des idèles unités congrus à 1 mod* $\mathfrak{f}$) du corps k. Le groupe de Galois de $k^{(2)}k^{(\mathfrak{f})}/k^{(2)}$ est canoniquement isomorphe à $\mathrm{Gal}(k^{(\mathfrak{f})}/H_k)$ lui-même isomorphe à $U/U_{\mathfrak{f}}\langle\pm 1\rangle$ au moyen de la loi de réciprocité d'Artin (cf. [3]). La théorie de la multiplication complexe associe à $u^{-1}\in U$ l'automorphisme $\sigma_u\in \mathrm{Gal}(k^{(2)}k^{(\mathfrak{f})}/k^{(2)})$ défini par $\sigma_u(T(\alpha)) = T(u\alpha)$. Le discriminant du réseau est donc égal à:

$$\prod_{u\in U/U_{\mathfrak{f}}\langle\pm 1\rangle-\{1\}} N_{k^{(2)}k^{(\mathfrak{f})}/k^{(2)}}\left(\frac{T(\alpha)-T(u\alpha)}{\varrho}\right).$$

La formule de différence et les corollaires 10.2, 10.4, 10.6 montrent que les seuls idéaux premiers de $\boldsymbol{Z}_{k^{(2)}}$ qui divisent ces normes sont ceux qui relèvent les facteurs premiers de $\mathfrak{f}$. Soit $\mathfrak{p}$ idéal premier de $\boldsymbol{Z}_k$ divisant $\mathfrak{f}$ et $\mathfrak{P}$ un idéal premier de $\boldsymbol{Z}_{k^{(2)}}$ divisant $\mathfrak{p}\boldsymbol{Z}_{k^{(2)}}$. Pour un idèle $u\in U-U_{\mathfrak{f}}\langle\pm 1\rangle$, on note $s_u = N_{k^{(2)}k^{(\mathfrak{f})}/k^{(2)}}\left(\frac{T(\alpha)-T(u\alpha)}{\varrho}\right)$, on se propose de déterminer la valuation en $\mathfrak{P}$ de s_u. Traitons le cas où $\mathfrak{f} = \mathfrak{p}^r$, $r\geqslant 1$.

L'idéal $\mathfrak{P}$ est totalement ramifié dans $k^{(\mathfrak{p}^r)}k^{(2)}/k^{(2)}$; pour chaque s, $1\leqslant s\leqslant r$, on note $\mathfrak{P}_s$ l'unique idéal premier de $k^{(\mathfrak{p}^s)}k^{(2)}$ relevant $\mathfrak{P}$.

Les formules (14) font intervenir les points α, $u\alpha$, $\alpha+u\alpha$, $\alpha-u\alpha$; ou bien les points $\alpha+u\alpha$, $\alpha-u\alpha$ ont pour annulateur $\mathfrak{p}^r$ ou bien un et un seul d'entre eux a pour annulateur $\mathfrak{p}^s$, $1\leqslant s\leqslant r$.

Si $\alpha+u\alpha$ et $\alpha-u\alpha$ ont pour annulateur $\mathfrak{p}^r$, $T(\alpha)-T(u\alpha)$, $T(\alpha+u)-T(\alpha-u)$ appartiennent à $\mathfrak{P}_r$, la valuation de $T(\alpha+u)T(\alpha-u)T_1(\alpha)T_1(u\alpha)$ en $\mathfrak{P}_r$ est égale à 3 (corollaires 10.2 et 10.6) donc celle de $T(\alpha)-T(u\alpha)$ est égale à 1. En prenant la norme dans $k^{(2)}k^{(\mathfrak{f})}/k^{(2)}$ la valuation en $\mathfrak{P}$ de s_u est égale à 1.

Si l'un des points $\alpha+u\alpha$, $\alpha-u\alpha$ a pour annulateur $\mathfrak{p}^s$ avec $1\leqslant s\leqslant r$, on peut supposer que c'est $\alpha-u\alpha$ (on travaille modulo $U_{\mathfrak{f}}\langle\pm 1\rangle$). La différence $\left(\frac{T(\alpha+u\alpha)-T(\alpha-u\alpha)}{\varrho}\right)$ est donc associée en $\mathfrak{P}_r$ à $T(\alpha+u\alpha)$ et $\left(\frac{T(\alpha)-T(u\alpha)}{\varrho}\right)^2$ est associé en $\mathfrak{P}_r$ à $T(\alpha-u\alpha)T_1(\alpha)T_1(u\alpha)$ et donc à $T(\alpha-u\alpha)T(\alpha)$ (corollaire 10.2).

La valuation en $\mathfrak{P}_r$ de $T(\alpha-u\alpha)T(\alpha)$ est égale à

$$[k^{(2)}k^{(\mathfrak{p}^r)}:k^{(2)}k^{(\mathfrak{p}^s)}]+1 = N(\mathfrak{p})^{r-s}+1$$

et donc la valuation en $\mathfrak{P}_r$ de $T(\alpha)-T(u\alpha)$ est $(N(\mathfrak{p})^{r-s}+1)/2$. Pour $r = s$ on retrouve la valeur précédente.

Comptons les $u\in U/U_{\mathfrak{f}}\langle\pm 1\rangle$ tels que $(1\pm u)\alpha$ ait pour annulateur $\mathfrak{p}^s$, $1\leqslant s\leqslant r$; il faut et il suffit que $\mathfrak{p}^s(1\pm u)\subset\mathfrak{p}^r$ et $\mathfrak{p}^{s-1}(1\pm u)\not\subset\mathfrak{p}^r$, donc $\pm u\in U_{\mathfrak{p}^{r-s}}-U_{\mathfrak{p}^{r-s+1}}$. C'est-à-dire que

$$u\in\langle\pm 1\rangle U_{\mathfrak{p}^{r-s}}/\langle\pm 1\rangle U_{\mathfrak{p}^r}-\langle\pm 1\rangle U_{\mathfrak{p}^{r-s+1}}/\langle\pm 1\rangle U_{\mathfrak{p}^r}.$$

Pour $s<r$ le nombre de ces éléments est égal à $N(\mathfrak{p})^s-N(\mathfrak{p})^{s-1}$ et pour $s=r$ à

$$N(\mathfrak{p})^{r-1}\left(\frac{N(\mathfrak{p})-1}{2}-1\right).$$

On en déduit que la valuation en $\mathfrak{P}$ du discriminant du réseau engendré par $1, \theta, \ldots, \theta^{n-1}$ est égale à

$$N(\mathfrak{p})^{r-1}\left(\frac{N(\mathfrak{p})-1}{2}-1\right)+\sum_{s=1}^{r-1}\tfrac{1}{2}(N(\mathfrak{p})^{r-s}+1)(N(\mathfrak{p})^s-N(\mathfrak{p})^{s-1})$$

elle vaut donc $(rN(\mathfrak{p})^r-(r+1)N(\mathfrak{p})^{r-1}-1)/2$.

Il s'ensuit que si $\mathfrak{f} = \mathfrak{p}^r$ le réseau, inclus dans l'anneau des entiers de $k^{(2)}k^{(\mathfrak{f})}$, a même discriminant que cet anneau il lui est donc égal.

Lorsque $\mathfrak{f}$ est divisible par plusieurs idéaux premiers la démonstration est analogue.

12. Monogénéité de l'anneau des entiers de $k^{(\mathfrak{f})}/H_k$ lorsque $d\equiv 2 \bmod 4$. Etablissons tout d'abord le lemme suivant:

LEMME 12.1. *Soit α un point primitif de $\mathfrak{f}$-division de E_τ avec $\mathfrak{f}$ premier à 2. Le conjugué de $T(\alpha)$ dans $k^{(2)}k^{(\mathfrak{f})}/k^{(\mathfrak{f})}$ est égal à $T(\alpha)/\lambda(\tau)$.*

Démonstration. On remarque tout d'abord que $\mathrm{Gal}(k^{(2)}k^{(\mathfrak{f})}/H_k)$ est isomorphe au produit direct $\mathrm{Gal}(k^{(2)}/H_k).\ \mathrm{Gal}(k^{(\mathfrak{f})}/H_k)$ puisque

$$T(\alpha) = \frac{h^{(1)}_{\Lambda_\tau}(1/2)-h^{(1)}_{\Lambda_\tau}((1+\tau)/2)}{h^{(1)}_{\Lambda_\tau}(\alpha)-h^{(1)}_{\Lambda_\tau}((1+\tau)/2)}.$$

Le groupe de Galois de $k^{(2)}k^{(\mathfrak{f})}/k^{(\mathfrak{f})}$ opère trivialement sur $h^{(1)}_{\Lambda_\tau}(\alpha)$, $h^{(1)}_{\Lambda_\tau}((1+\tau)/2)$ (cf. paragraphe 3), par contre son élément $\neq$ id transforme $h^{(1)}_{\Lambda_\tau}(1/2)$ en $h^{(1)}_{\Lambda_\tau}(\tau/2)$, ce qui, compte-tenu de l'écriture de $\lambda(\tau)$ donne le résultat.

THÉORÈME 12.2. *Si $d\equiv 2 \bmod 4$ et $\mathfrak{f}$ un idéal entier de $\boldsymbol{Z}_k$ premier à 2, l'anneau des entiers de $k^{(\mathfrak{f})}$ est monogène sur celui de H_k.*

Démonstration. Il suffit de trouver un générateur de l'anneau des entiers de $k^{(2)}k^{(\mathfrak{f})}/k^{(2)}$ qui appartienne à $k^{(\mathfrak{f})}$.

Supposons d'abord 3 décomposé ou ramifié dans $k/\boldsymbol{Q}$. Avec les notations du paragraphe précédent, l'élément $\theta = (T(\alpha)-T(\beta))/2$ est un générateur de $\boldsymbol{Z}_{k^{(2)}k^{(\mathfrak{f})}}$ sur $\boldsymbol{Z}_{k^{(2)}}$; il conserve cette propriété si on le multiplie par une unité de $\boldsymbol{Z}_{k^{(2)}}$. Considérons donc $\mu = \frac{i}{\sqrt{\lambda(\tau)}}\theta$, on sait (cf. remarque du paragraphe 4)

que $k^{(2)} = H_k(i)$ et que le conjugué de $\sqrt{\lambda(\tau)}$ dans $k^{(2)}/H_k$ est $-1/\sqrt{\lambda(\tau)}$; par conséquent $\mu \in k^{(1)}$; le théorème est démontré dans ce cas.

Supposons maintenant 3 inerte dans $k/\mathbf{Q}$ et soit β un point de 3-division non nul de E_τ. Comme précédemment $iT(\beta)/\sqrt{\lambda(\tau)}$ appartient à $k^{(3)}$. On peut, en procédant comme dans le §11, trouver $b \in H_k$ tel que $iT(\beta)/\sqrt{\lambda(\tau)} \equiv b$ (2). On pose alors

$$\mu = i\frac{1}{2}\left(i\frac{T(\alpha)}{\sqrt{\lambda(\tau)}} - b\right).$$

Il est alors immédiat que μ est un entier de $k^{(1)}$ et qu'il engendre avec ses puissances l'anneau des entiers de $k^{(1)}$ relativement à H_k.

Références

[1] J. Cougnard, *Conditions nécessaires de monogénéité*, J. London Math. Soc. (2) 37 (1988), 73–87.

[2] — *Générateurs de l'anneau des entiers des corps de classes de $Q(i)$ de rayon impair et points de division de $Y^2 = X^3 - X$*, J. Number Theory 30 (1988), 140–155.

[3] Ph. Cassou-Noguès and M. J. Taylor, *Elliptic functions and rings of integers*, Progress in Mathematics n° 66, Birkhäuser, 1987.

[4] —, — *Note on elliptic curves and the monogeneity of rings of integers*, J. London Math. Soc. (2) 37 (1988), 63–72.

[5] —, — *Unités modulaires et monogénéité d'anneaux d'entiers*, Séminaire de Théorie des Nombres de Paris, 1987–1988.

[6] V. Fleckinger, *Monogénéite de l'anneau des entiers de certains corps de rayon*, Ann. Sci. Inst. Fourier Grenoble 38 (1) (1988), 17–57.

[7] — *Génération de base d'entiers à partir de $Y^2 = 4X^3 + 1$*, Publ. Math. Fac. Sci. Besançon 1986-87/1987-88.

[8] R. Fueter, *Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen*, Teubner, 1927.

[9] M.-N. Gras, *Non monogénéité de l'anneau des entiers des extensions cycliques de Q de degré premier $l \geqslant 5$*, J. Number Theory 23 (3) (1986), 347–353.

[10] S. Lang, *Elliptic functions*, Addison-Wesley, 1973.

[11] J.-P. Serre, *Corps locaux*, Hermann, 1968.

[12] F. Terada, *A principal ideal theorem in the genus field*, Tôhoku Math. J. 23 (1971), 697–718.

EQUIPE DE MATHÉMATIQUES DE BESANÇON
C.N.R.S. – U.A. 741
UNIVERSITÉ DE FRANCHE-COMTÉ
25030 Besançon Cedex
France

Reçu le 1.3.1988
et dans la forme modifiée le 3.10.1988 (1797)

ACTA ARITHMETICA
LIV (1990)

Hecke operators on theta series attached to lattices of arbitrary rank

by

LYNNE H. WALLING (Lewiston, Me.)

1. Preliminaries. Let $\boldsymbol{K}$ be a totally real algebraic number field of degree n over $\mathbf{Q}$; let $\mathcal{O}$ denote the ring of integers of $\boldsymbol{K}$ and ∂ the different of $\boldsymbol{K}$. Let V be a quadratic space of dimension m over $\boldsymbol{K}$ with totally positive quadratic form Q and associated bilinear form B where $B(x, x) = Q(x)$. Take L to be a lattice on V (so $\boldsymbol{K}L = V$). Let $\mathcal{H}$ denote the upper half-plane; then for $\tau = (\tau_1, \ldots, \tau_n) \in \mathcal{H}^n$, define

$$\Theta(L, \tau) = \sum_{x \in L} e(Q(x)\tau)$$

where $e(\alpha) = e^{\pi i \mathrm{Tr}(\alpha)}$. Notice that $e(\alpha) = 1$ whenever $\alpha \in 2\partial^{-1}$. For $y \in V$, define

$$\Theta(L, y, \tau) = \sum_{x \in L} e(Q(x+y)\tau).$$

So when $y \in L$, $\Theta(L, y, \tau) = \Theta(L, \tau)$.

As defined in Eichler [6], let $\tilde{L}$ denote the complement of L, $N(L)$ the norm of L, and $\mathcal{N}(L) = N(L)^{-1} N(\tilde{L})^{-1} \partial^2$ the level of L. Notice that $\tilde{L} = \partial^{-1} L^{\#}$ where $L^{\#}$ is the dual of L (as defined in [12]), hence $\mathcal{N}(L) = N(L)^{-1} N(L^{\#})^{-1}$, which is integral (i.e. $\mathcal{N}(L) \subseteq \mathcal{O}$; see [6]). Also, $x \in \tilde{L}$ if and only if $B(x, L) \subseteq \partial^{-1}$. For $\alpha \in \boldsymbol{K}$, let L^α denote L scaled by α; that is, L^α is the lattice L together with the quadratic and bilinear forms Q^α and B^α defined by

$$Q^\alpha(x) = \alpha Q(x) \quad \text{and} \quad B^\alpha(x, y) = \alpha B(x, y)$$

(see §89J of [12]). So $N(L^\alpha) = \alpha N(L)$ and $\mathcal{N}(L^\alpha) = \mathcal{N}(L)$.

For fractional ideals $\mathfrak{I}_1$ and $\mathfrak{I}_2$, define

$$\Gamma_0(\mathfrak{I}_1, \mathfrak{I}_2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, d \in \mathcal{O},\ c \in \mathfrak{I}_1,\ b \in \mathfrak{I}_2,\ ad - bc = 1 \right\}.$$

If $\mathfrak{I}_1 \mathfrak{I}_2$ is integral then $\Gamma_0(\mathfrak{I}_1, \mathfrak{I}_2)$ is a group. If $\mathrm{ord}_{\mathfrak{P}} \mathfrak{I}_2 = 0$ whenever $\mathfrak{P}$ is a prime ideal with $\mathrm{ord}_{\mathfrak{P}} \mathfrak{I}_1 \neq 0$, then we say $\mathfrak{I}_1$ and $\mathfrak{I}_2$ are relatively prime.

The reader is referred to [12], [2] and [10] for details regarding lattices and quadratic forms.