ACTA ARITHMETICA
LV (1990)

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

par

JEAN COUGNARD et VINCENT FLECKINGER (Besançon)

1. Introduction. Pour tout corps de nombres K on note $\mathbf{Z}_K$ son anneau des entiers. Si L/K est une extension algébrique de degré fini de corps de nombres, on dit que $\mathbf{Z}_L$ est $\mathbf{Z}_K$-monogène s'il existe θ tel que $\mathbf{Z}_L = \mathbf{Z}_K[\theta]$. Des résultats antérieurs [1] ont conduit à conjecturer:

CONJECTURE. *Si K est un corps quadratique imaginaire, H_K son corps de classes de Hilbert, $\mathfrak{F}$ un idéal de $\mathbf{Z}_K$ alors l'anneau des entiers de $K^{(\mathfrak{F})}$ est monogène sur celui de H_K.*

Des résultats récents ([2], [3], [5], [6], [7], [8], [9]) rendent cette conjecture plausible. Tous sont basés sur l'étude des valeurs de fonctions elliptiques ad-hoc évaluées en des points de division de la courbe elliptique $E = C/\mathbf{Z}_K$. La conjecture est en particulier démontrée avec $\mathfrak{F}$ premier à 2, 2 décomposé dans $K/\mathbf{Q}$ ([6]), ou $K = \mathbf{Q}(\sqrt{-d})$ avec $d \equiv 2 \bmod 4$ ([3]). On se propose, à partir des méthodes de ([3]), de compléter ces résultats en prouvant ceux annoncés dans [4]:

THÉORÈME 1. *Soit K un corps quadratique imaginaire dans lequel 2 est ramifié et $\mathfrak{F}$ un idéal de $\mathbf{Z}_K$ premier à 2 alors l'anneau des entiers de $K^{(\mathfrak{F})}$ est monogène sur celui de H_K.*

THÉORÈME 2. *Soit K un corps quadratique imaginaire dans lequel 2 est inerte, $\mathfrak{F}$ un idéal de $\mathbf{Z}_K$ premier à 2 qui n'est pas une puissance d'un idéal premier, alors l'anneau des entiers de $K^{(\mathfrak{F})}$ est monogène sur celui de H_K.*

D'autres résultats sont annoncés d'une part par M. Vérant, d'autre part par V. Fleckinger. Le premier reprend l'article [2] et démontre la monogénéité pour les corps de rayon de $\mathbf{Q}(i)$ dont le conducteur n'est pas une puissance de $1+i$. Le second démontre des résultats analogues aux théorèmes 1 et 2 en utilisant le modèle de Deuring et en faisant jouer à l'idéal 3 le rôle que joue l'idéal 2 dans les énoncés ci-dessus.

Il semble au vu de ces différents travaux que le cas où la conjecture résiste est celui où les idéaux 2 et 3 sont inertes dans $K/\mathbf{Q}$ et le conducteur une puissance d'un idéal premier.

Notons encore que les méthodes utilisées permettent dans de nombreux cas d'aboutir à des calculs explicites ([2], [4], [9]).

Notons que dans [7] la méthode suivie est à priori différente puisque les auteurs cherchent d'abord des générateurs pour certains sous anneaux de corps de fonctions modulaires et spécialisent ensuite pour trouver des résultats similaires aux notres.

Au moment de terminer la rédaction de ce travail nous avons eu connaissance des résultats de R. Schertz [11] qui travaille essentiellement avec des conducteurs $\mathfrak{J}$ qui ne sont pas puissance d'un idéal premier (cf. [11], Th. 5, Th. 6) et qui n'ont pas à être premiers avec (2). Ces divers travaux confirment la remarque précédente sur le cas qui reste à résoudre.

2. Rappels et notations (cf. [3]). Dans ce qui suit K est un corps quadratique imaginaire dans lequel 2 est inerte ou ramifié. Soit $\mathfrak{P}$ l'idéal premier de $\boldsymbol{Z}_K$ divisant 2. On choisit une base 1, τ de $\boldsymbol{Z}_K$ de telle sorte que $\mathrm{Im}(\tau) > 0$ et que $\mathfrak{P}$ soit l'annulateur de $(1+\tau)/2$ (cf. [3], § 3). Soit $\wp$ la fonction de Weierstrass associée au réseau $\boldsymbol{Z}_K$ de base 1, τ. On pose:

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

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

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

La fonction λ est la fonction de Legendre et les fonctions T et T_1 sont liées par la relation:

$$T_1^2 = T(T-1)(T-\lambda)$$

qui est le modèle de Legendre de la courbe $E = C/\boldsymbol{Z}_K$. Ce modèle est défini sur le corps $K^{(2)}$.

Si 2 est ramifié dans $K/\boldsymbol{Q}$ le degré de $K^{(2)}/H_K$ est égal à 2 et on pose $\varrho = 2$. Si 2 est inerte dans $K/\boldsymbol{Q}$ le degré de $K^{(2)}/H_K$ est égal à 3. Le produit $\mathfrak{J}$ des idéaux premiers de $K^{(2)}$ divisant 2 est principal et on note ϱ un générateur de $\mathfrak{J}^2$.

On démontre que si α et β sont des points de E d'ordre premier à 2 les nombres $T(\alpha)$ et $T(\beta)$ sont des entiers algébriques et $T(\alpha)-T(\beta) \equiv 0 \bmod \varrho$ (cf. [3], Th. 9.1). On a également prouvé qu'il existe un élément entier $a \in K^{(2)}$ tel que $T(\alpha) \equiv a \bmod \varrho$ (lorsque 3 est décomposé ou inerte dans $K/\boldsymbol{Q}$ il suffit de prendre a égal à $T(\beta)$ où β est un point de E dont l'annulateur divise strictement 3). Avec ces notations, on a pu énoncer:

THÉORÈME 3. *Si $\mathfrak{F}$ est un idéal de K premier à 2, α un point primitif de $\mathfrak{F}$-division de E, alors $0 = (T(\alpha)-a)/\varrho$ engendre l'anneau des entiers de $K^{(2)}K^{(\mathfrak{F})}$ sur celui de $K^{(2)}$.*

3. Le cas 2 ramifié

Remarque. Le cas où $K = \boldsymbol{Q}(i)$ ayant été traité dans [2] on suppose dans ce paragraphe que le discriminant de K est strictement plus petit que 4.

Rappelons tout d'abord que dans ce cas $\lambda(\tau)$ est une unité de $K^{(2)}$, que $\sqrt{\lambda(\tau)}$ est dans $K^{(2)}$ et que le conjugué de cet élément sur H_K est $-1/\sqrt{\lambda(\tau)}$.

PROPOSITION 4. *Si 2 est ramifié dans $K/\boldsymbol{Q}$ il existe une unité ε de H_K telle que $K^{(2)} = H_K(\sqrt{\varepsilon})$.*

Démonstration. Dans l'extension $K^{(2)}/H_K$ le groupe de ramification est cyclique d'ordre 2. Il existe donc une extension cyclique L_1/K avec L_1 extension quadratique ramifiée en 2 d'une extension cyclique non ramifiée L_0/K telle que $K^{(2)}/L_1$ soit non ramifiée.

Soit $x \in L_1$ tel que $L_1 = L_0(\sqrt{x})$ (et donc $K^{(2)} = H_K(\sqrt{x})$). Les discriminants de $K^{(2)}/H_K$ et L_1/L_0 étant égaux à 2 l'idéal de L_0 engendré par x est le carré d'un idéal $\mathfrak{B}$ de L_0. L'extension L_1/K étant galoisienne la classe de $\mathfrak{B}$ est ambige dans L_0/K. Le théorème de Tannaka–Terrada [12] montre que $\mathfrak{B}$ devient principal dans le corps des genres de L_0/K qui est H_K; d'où le résultat annoncé.

COROLLAIRE. *Si τ est tel que 1, τ est une base de l'anneau des entiers d'un corps quadratique imaginaire, alors $j(\tau)-12^3$ engendre le carré d'un idéal principal de H_K, et c'est un carré de H_K si $\boldsymbol{Q}(\tau)/\boldsymbol{Q}$ n'est pas ramifiée en 2.*

Démonstration. On sait (cf. [10], ch. 18) que $(j-12^3)^{1/2}$ est une fonction modulaire de niveau 2 et qu'elle engendre l'unique sous-corps, de degré 2 sur $\boldsymbol{Q}(j)$, du corps des fonctions modulaires de niveau 2 définies sur $\boldsymbol{Q}$. Pour des τ tels que ceux de l'énoncé la loi de réciprocité de Shimura montre que $(j(\tau)-12^3)^{1/2}$ appartient au corps $K^{(2)}$ et est quadratique sur H_K ce qui donne le résultat lorsque 2 n'est pas ramifié dans $\boldsymbol{Q}(\tau)/\boldsymbol{Q}$. Lorsque 2 est ramifié dans $\boldsymbol{Q}(\tau)/\boldsymbol{Q}$ on a $[K^{(2)}:H_K] = 2$ donc $K^{(2)}/H_K$ est engendrée par $(j(\tau)-12^3)^{1/2}$; cette extension peut également être engendrée par la racine carrée d'une unité de H_K ce qui termine la démonstration.

Démonstration du Théorème 1. Soit s l'automorphisme non trivial de $K^{(2)}K^{(\mathfrak{F})}/K^{(\mathfrak{F})}$ on sait que si α est un point de E d'ordre premier à 2 on a: $s(T(\alpha)) = T(\alpha)/\lambda(\tau)$ (cf. [3], lemme 12.1). Puisque $\sqrt{\lambda(\tau)}$ est dans $K^{(2)}$ et a $-1/\sqrt{\lambda(\tau)}$ comme conjugué sur H_K, il s'ensuit qu'avec l'unité ε de la proposition 4, l'élément $\sqrt{\varepsilon}T(\alpha)/\sqrt{\lambda(\tau)}$ appartient à $K^{(\mathfrak{F})}$. D'après le théorème 3 l'application qui à σ associe

$$\left(\sigma\left(\sqrt{\varepsilon}T(\alpha)/\sqrt{\lambda(\tau)}\right)-\sqrt{\varepsilon}T(\alpha)/\sqrt{\lambda(\tau)}\right)/\varrho$$

est un un-cocycle de $\mathrm{Gal}(K^{(\mathfrak{F})}/H_K)$ à valeurs dans $\boldsymbol{Z}_{K(\mathfrak{F})}$. Supposons tout d'abord que $\mathfrak{F}$ soit un idéal premier, premier à 2, et μ un point primitif de $\mathfrak{F}$-division de E. L'extension $K^{(\mathfrak{F})}/H_K$ est modérément ramifiée donc son

anneau des entiers est cohomologiquement trivial pour $\mathrm{Gal}(K^{(\mathfrak{F})}/H_K)$; il existe donc un élément $b \in Z_{K^{(\mathfrak{F})}}$ tel que:

$$\frac{\sigma\left(\sqrt{\varepsilon T(\mu)}/\sqrt{\lambda(\tau)}\right)-\sqrt{\varepsilon T(\mu)}/\sqrt{\lambda(\tau)}}{\varrho} = \sigma(b)-b$$

mais alors $a = \sqrt{\varepsilon T(\mu)}/(\varrho\sqrt{\lambda(\tau)})-b$ est un élément de H_K. Revenons maintenant à $\mathfrak{F}$ premier à 2 sans plus de précision; les résultats rappelés dans le §2 permettent d'écrire que:

$$\frac{\sqrt{\varepsilon T(\alpha)}}{\varrho\sqrt{\lambda(\tau)}}-a-b$$

est un entier algébrique et donc que

$$\theta = \frac{\sqrt{\varepsilon T(\alpha)}}{\varrho\sqrt{\lambda(\tau)}}-a$$

est un entier algébrique de $K^{(\mathfrak{F})}$ quel que soit α point primitif de $\mathfrak{F}$-division de E avec $\mathfrak{F}$ premier à 2. Les discriminants de $K^{(\mathfrak{F})}K^{(2)}/K^{(2)}$ et $K^{(\mathfrak{F})}/H_K$ étant les mêmes on peut reprendre la démonstration du §11 de [3] pour terminer la preuve du théorème 1.

4. Le cas 2 inerte

Remarque. Le cas K corps des racines cubiques de l'unité ayant été traité dans [9] on suppose dans ce qui suit que le discriminant de $K/\boldsymbol{Q}$ est inférieur strictement à 3.

PROPOSITION 5. *Si 3 est ramifié dans $K/\boldsymbol{Q}$ il existe une unité v de H_K telle que $K^{(3)} = H_K(\sqrt[3]{v})$.*

Démonstration. On se base comme dans la proposition 4 sur le fait que $K^{(3)}/H_K$ est une extension cyclique de degré 3 et que, 3 étant ramifié dans $K/\boldsymbol{Q}$, H_K contient les racines cubiques de l'unité. Le reste est sans changement.

COROLLAIRE. *Si τ est tel que 1, τ est une base de l'anneau des entiers d'un corps quadratique imaginaire, alors $j(\tau)$ engendre le cube d'un idéal principal de H_K, et c'est un cube de H_K si $\boldsymbol{Q}(\tau)/\boldsymbol{Q}$ n'est pas ramifiée en 3.*

Démonstration. Elle est calquée sur celle du corollaire de la proposition 4, en utilisant cette fois-ci le fait que $j^{1/3}$ est une fonction modulaire de niveau 3, que le degré de $K^{(3)}/H_K$ est premier à 3 lorsque 3 n'est pas ramifié dans $K/\boldsymbol{Q}$ et que le groupe de Galois sur $\boldsymbol{Q}(j)$ du corps des fonctions modulaires de niveau 3 définies sur S est isomorphe à $\mathrm{GL}_2(\boldsymbol{Z}/3\boldsymbol{Z})/\pm 1$ qui est d'ordre 24 (cf. [10], ch. 6).

Dans tout ce qui suit les points α et β de E ont un annulateur qui est premier à 2 et qui n'est pas une puissance d'un idéal premier. Le générateur

dont l'existence est annoncée dans le théorème 2 va être construit au moyen de la première fonction de Weber:

$$h(z) = \frac{-2^7 3^5 g_2(\tau) g_3(\tau)}{\Delta(\tau)}\wp(z;\tau)$$

où g_2, g_3, Δ sont les formes modulaires usuelles (cf. [10], ch. 1). Pour cela commençons par exprimer la différence $T(\alpha)-T(\beta)$ au moyen de h en remarquant pour commencer que dans la définition de T on peut remplacer $\wp$ par h et donc:

$$T(\alpha)-T(\beta) = \frac{h(1/2)-h((1+\tau)/2)}{h(\alpha)-h((1+\tau)/2)}-\frac{h(1/2)-h((1+\tau)/2)}{h(\beta)-h((1+\tau)/2)}$$

ce qui donne:

$$(1)\qquad \frac{T(\alpha)-T(\beta)}{\varrho} = T(\alpha)T(\beta)\frac{h(\beta)-h(\alpha)}{\varrho\left(h(1/2)-h((1+\tau)/2)\right)}.$$

Mais on sait d'après le corollaire 10.4 de [3] que $T(\alpha)$ et $T(\beta)$ sont des unités, donc que:

$$(2)\qquad h(\alpha)-h(\beta) \sim \left(h(1/2)-h((1+\tau)/2)\right)\left(T(\alpha)-T(\beta)\right)$$

où $\sim$ signifie que le quotient des deux membres est une unité. Nous allons maintenant évaluer $\left(h(1/2)-h((1+\tau)/2)\right)$ via le calcul du discriminant du modèle de Weierstrass. En effet, nous avons:

$$16\left[\left(h(\tfrac{1}{2})-h\left(\frac{1+\tau}{2}\right)\right)\left(h(\tfrac{1}{2})-h\left(\frac{\tau}{2}\right)\right)\left(h\left(\frac{\tau}{2}\right)-h\left(\frac{1+\tau}{2}\right)\right)\right]^2 = \Delta(\tau)\left(\frac{2^7 3^5 g_2(\tau) g_3(\tau)}{\Delta(\tau)}\right)^6.$$

De plus d'après le théorème 7.1 de [3] $\lambda(\tau)$ est une unité,

$$j(\tau) = 12^3 g_2^3(\tau)/\Delta(\tau), \quad j(\tau)-12^3 = 2^6 3^6 g_3^2(\tau)/\Delta(\tau).$$

Il en résulte que:

$$\left[h(\tfrac{1}{2})-h\left(\frac{1+\tau}{2}\right)\right]^6 \sim j(\tau)^2\left(j(\tau)-12^3\right)^3 2^8 3^6.$$

Compte-tenu de la définition de ϱ on en déduit que:

$$\varrho\left(h(\tfrac{1}{2})-h\left(\frac{1+\tau}{2}\right)\right) \sim 12 j(\tau)^{1/3}\left(j(\tau)-12^3\right)^{1/2}.$$

Le membre de droite étant un entier, la formule (2) nous dit donc que:

$$h(\alpha)-h(\beta) \equiv 0 \bmod 12 j(\tau)^{1/3}\left(j(\tau)-12^3\right)^{1/2}$$

et, finalement d'après (1) que:

$$\frac{h(\alpha)-h(\beta)}{12j(\tau)^{1/3}\left(j(\tau)-12^3\right)^{1/2}} \sim \frac{T(\alpha)-T(\beta)}{\varrho}.$$

Or on sait d'après les corollaires aux propositions 4 et 5 que $12j(\tau)^{1/3} \times (j(\tau)-12^3)^{1/2}$ est associé à un élément c de H_K. On a donc prouvé, en utilisant à nouveau le §11 de [3], que:

LEMME. *Pour $\mathfrak{F}$ conducteur premier à 2 non puissance d'un idéal premier et α point primitif de $\mathfrak{F}$-division de E le discriminant du polynôme irréductible de $h(\alpha)/c$ dans l'extension $K^{(\mathfrak{F})}/H_K$ est associé à celui de cette extension.*

Le problème qui reste à régler est qu'à priori $h(\alpha)/c$ n'est pas un entier. Nous allons procéder comme dans le paragraphe 3.

Soit $\mathfrak{F}_1$ le produit de deux idéaux premiers distincts de (2): $\mathfrak{F}_1 = \mathfrak{P}_1\mathfrak{P}_2$ et μ un point primitif de $\mathfrak{F}_1$-division de E; l'extension $K^{(\mathfrak{F}_1)}/H_K$ est modérément ramifiée et le un-cocycle de $\mathrm{Gal}(K^{(\mathfrak{F}_1)}/H_K)$ à valeurs dans $\boldsymbol{Z}_{K^{(\mathfrak{F}_1)}}$ qui à σ associe:

$$\frac{\sigma(h(\mu))-h(\mu)}{c}$$

est un un-cobord; il existe donc b dans $\boldsymbol{Z}_{K^{(\mathfrak{F}_1)}}$ tel que:

$$\frac{\sigma(h(\mu))-h(\mu)}{c} = \sigma(b)-b.$$

On pose a l'élément de H_K égal à $(h(\alpha)/c)-b$. On considère maintenant $\mathfrak{F}$ un conducteur premier à (2) qui n'est pas une puissance d'un idéal premier et α un point primitif de $\mathfrak{F}$-division de E on peut alors écrire:

$$\frac{h(\alpha)}{c}-\frac{h(\mu)}{c} = \frac{h(\alpha)}{c}-a-b$$

on constate que $h(\alpha)/c-a$ est un entier de $K^{(\mathfrak{F})}$ et d'après le lemme qu'il est le générateur annoncé dans le théorème 2.

Bibliographie

[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 $\boldsymbol{Q}(i)$ de rayon impair et points de division de $Y^2 = X^3-X$*, J. Number Theory 30 (2) (1988), 140–155.

[3] — *Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers*, Acta Arith. 54 (1990), 191–212.

[4] — *Résultats récents sur la monogénéité de certains anneaux d'entiers*, Séminaire de Théorie des Nombres de Bordeaux 1987–88, à paraître.

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

[6] Ph. Cassou-Noguès et M. J. Taylor, *Note on elliptic curves and the monogeneity of rings of integers*, J. London Math. Soc. (2) 37 (1988), 63–72.

[7] — — *Unités modulaires et monogénéité d'anneaux d'entiers*, Sém. de Théorie des nombres de Paris 1986–87, Progress in Mathematics, Birkhäuser, à paraître.

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

[9] — *Génération de bases d'entiers à partir de $Y^2 = 4X^3+1$*, Publ. Math. Fac. Sci. Besançon, à paraître.

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

[11] R. Schertz, *Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär-quadratischen Zahlkörpern*, à paraître.

[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 29.6.1988
et dans la forme modifiée le 3.10.1988 (1842)