JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

VINCENT FLECKINGER

Étude de la courbe elliptique $y^2 = 4x^3 - 27((3+\sqrt{-19})/2)^2$ et monogénéité de certains anneaux d'entiers

Journal de Théorie des Nombres de Bordeaux, tome 1, n° 1 (1989), p. 103-116

<http://www.numdam.org/item?id=JTNB_1989__1_1_103_0>

Séminaire de Théorie des Nombres,
Bordeaux, **1**, *103–116(1989)*

Etude de la courbe elliptique $y^2 = 4x^3 - 27((3+\sqrt{-19})/2)^2$ et monogénéité de certains anneaux d'entiers.

par VINCENT FLECKINGER

Le sujet de cet exposé est une étude de la courbe elliptique $E : y^2 = 4x^3 - 27(\frac{3+\sqrt{-19}}{2})^2$, concernant sa fonction $L(E/k, s)$ et le calcul du rang $E(k)$ sous la conjecture de Birch et Swinnerton Dyer, où $k = \mathbb{Q}(\sqrt{-19})$. On justifie ainsi la méthode utilisée dans le travail en commun avec J. Cougnard sur la non existence de point entier sur $E(k)$. Rappelons brièvement les motivations de ce travail. Soient k un corps quadratique imaginaire, H_k son corps de classes de Hilbert, $\mathcal{F}$ un idéal de $\mathbf{Z}_k$ l'anneau des entiers de k et $k^{(\mathcal{F})}$ le corps de classes de k de rayon $\mathcal{F}$. Les résultats de Cassou-Noguès et Taylor ([C.-N., T]) sur l'existence d'une base de puissances pour les anneaux d'entiers dans les extensions $k^{(4\mathcal{F})}/k^{(4)}$ et $k^{(4)}k^{(\mathcal{F})}/k^{(4)}$ lorsque $\mathcal{F}$ est premier à (2) et que (2) est décomposé dans k, ont conduit plusieurs auteurs à s'intéresser à ce problème. C'est ainsi que des améliorations et des généralisations ont été apportées par ces auteurs J. Cougnard , moi-même et finalement par R. Schertz ([Sc]), qui donne les meilleurs résultats possibles et chez qui on peut trouver une bibliographie complète.

Si on étudie les résultats obtenus on constate que le cas le plus défavorable est le cas où (2) et (3) sont inertes dans k. En effet il n'existe pas de points de torsion de la courbe C/A_k, pour lequel la valeur de la fonction de Weber correspondante soit dans H_k, car on sait que ses valeurs engendrent des corps de rayons distincts de H_k. On est donc amené considérer des corps de la forme $k = \mathbb{Q}(\sqrt{-d})$ avec $d \equiv 19 \bmod 24$. Le premier exemple abordable expérimentalement se trouve être d=19, car le nombre de classe est alors égal à 1. C'est donc ce corps que nous allons considérer, et nous notons $\omega = \frac{1+\sqrt{-19}}{2}$. Dans le corps $k = \mathbb{Q}(\omega)$, l'idéal (7) se décompose $(7) = \mathfrak{p}_7\mathfrak{p}_7'$ avec $\mathfrak{p}_7 = (1+\omega)$. Nous pouvons alors citer le théorème suivant [C,F] :

THÉORÈME 1. *Pour que l'anneau $A_{k(\mathfrak{p}_7)}$ possède une base de puissances sur A_k il faut et il suffit que l'équation diophantienne $Y^2 + 27 = 4(1+\omega)X^3$ possède une solution première à 3 dans A_k .*

D'où l'étude de la courbe E ; le résultat démontré avec J. Cougnard s'énonce alors sous la forme :

Manuscrit reçu le 10 avril 1989

THÉORÈME 2. *L'anneau des entiers du corps des classes de rayon* $k^{(\mathfrak{p}_7)}$ *n'admet pas de base de puissance sur l'anneau des entiers de* k.

Ce qui fournit ainsi une obstruction à la généralisation des résultats obtenus sur la monogénéité.

Plan de l'exposé :

- Dans la première partie on détermine la fonction $L(E/k, s)$
- Dans la deuxième partie on détermine l'équation fonctionnelle de la fonction $L(E/k, s)$.
- Dans la troisième partie on fait une 3-descente pour calculer le rang de cette courbe elliptique sur k. On montre que, sous la conjecture de Birch et Swinnerton Dyer, ce rang est 1 .

1. Détermination de la fonction $L(E/k, s)$

Il nous faut donc calculer le nombre de points de la courbe réduite $E_\nu(k_\nu)$, en chaque place finie ν de k. Soit $\mathfrak{p}$ un idéal premier de k, Il y a plusieurs cas à considérer :

- Si $\mathfrak{p}$ est un idéal premier ne divisant pas $6(1+\omega)$, alors la courbe réduite admet pour modèle :

$$y^2 = 4x^3 - 27(1+\omega)^2.$$

- Si $\mathfrak{p}$ divise $3(1+\omega)$ alors le changement de variable $y = 2y' + 9(1+w)$, $x = x'$ donne :

$$y'^2 + 9(1+w)y' = x'^3 - 27(1+w)^2$$

Ce qui permet de calculer la valuation du conducteur de cette courbe en 3 et $1+\omega$ en utilisant les résultats de ([N]). On retrouve aussi que la réduction $y'^2 = x'^3$ est additive pour chacune de ces deux places, ce qui n'est pas étonnant puisque la courbe est à multiplication complexe ([Si]).

- Enfin si $\mathfrak{p} = 2$, le changement de variable précédent montre que la courbe admet une bonne réduction en 2, le modèle réduit étant:

$$y'^2 + (1+w)y' = x'^3 + (1+\omega)^2$$

Ces considérations permettent d'affirmer que le conducteur de la courbe est $9(1+\omega)^2$. Soit alors $q = N_{k/Q}(\mathfrak{p})$, un calcul classique sur les corps finis donne les résultats suivant :

$\mathfrak{p}$	$L_{\mathfrak{p}}(T)$
3	1
$(1+\omega)$	1
$q \not\equiv 1 \mod 3$	$(1+qT^2)$
$q \equiv 1 \mod 3$	$(1-\pi_{\mathfrak{p}}T)(1-\overline{\pi}_{\mathfrak{p}}T))$

avec

$$\pi_{\mathfrak{p}} = -\chi_3(4(1+\omega))^2 \sum_{x \in k_{\mathfrak{p}}} \chi_2(x)\chi_3(1-x)$$

où χ_2 et χ_3 désigne des caractères non triviaux de $k_{\mathfrak{p}}^*$ d'ordre respectifs 2 et 3, prolongés en 0 par 0.
On obtient ainsi une première expression pour la fonction L :

$$L(E/k,s) = \prod_{N(\mathfrak{p})\equiv 1 \ (3)} \left(\frac{1}{1-\pi_{\mathfrak{p}}N(\mathfrak{p})^{-s}}\right)\left(\frac{1}{1-\overline{\pi}_{\mathfrak{p}}N(\mathfrak{p})^{-s}}\right) \prod_{N(\mathfrak{p})\equiv 2 \ (3)} \left(\frac{1}{1+N(\mathfrak{p})^{1-2s}}\right)$$

Pour mettre en évidence le großencharacter associé à cette fonction, on considère les quantités suivantes définies pour tout idéal premier $\mathfrak{p}$ de $\mathbf{Z}[j]$, premier avec 3 :

- χ_3 est le caractère cubique défini pour tout élément de $\mathbf{Q}[j]$ premier à p par

$$\chi_3(x) \equiv x^{(q-1)/3} \pmod{\mathfrak{p}}$$

- La fonction $J(\chi_3,\chi_3)(\mathfrak{p}) = -\sum_{x \bmod \mathfrak{p}} \chi_3(x)\chi_3(1-x)$, prolongée par multiplicativité à l'ensemble des idéaux premier avec 3 . On remarque que l'on a l'identité :

$$\sum_{x \in \mathbf{F}_q} \chi_2(x)\chi_3(1-x) = \chi_3(-4)J(\chi_3,\chi_3)(\mathfrak{p})$$

On pose $K = k(j)$. Le großencharacter φ est alors défini pour les idéaux de K premier à $3(1+\omega)$ par

$$\varphi(\mathfrak{A}) = \left(\frac{1+\omega}{\mathfrak{A}}\right)^2 J(\chi_3, \chi_3)(N_{K/\mathbb{Q}[j]}(\mathfrak{A}))$$

où $\left(\frac{\cdot}{\mathfrak{A}}\right)$ désigne le symbole de puissance 3 ième sur K. On obtient ainsi une autre expression pour la fonction $L(E/k, s)$

$$L(E/k, s) = \prod_{(\mathfrak{p},\ 3(1+\omega))=1} \left(\frac{1}{1-\varphi(\mathfrak{p})N(\mathfrak{p})^{-s}}\right)$$

Mais $k(j)$ est principal et l'unité principale $\epsilon = 3 + 10j + 4\omega$ est de norme relative 1 sur $Q(j)$. Si $\lambda_{\mathfrak{A}}$ est un générateur de $\mathfrak{A}$ alors on a :

$$\varphi(\lambda_{\mathfrak{A}}) = \left(\frac{1+\omega}{\lambda_{\mathfrak{A}}}\right)^2 N_{K/\mathbb{Q}(j)}(\lambda_{\mathfrak{A}})\chi\left(N_{K/\mathbb{Q}(j)}(\lambda_{\mathfrak{A}})\right)$$

où $\chi(x)$ est la racine de l'unité définie par $\chi(x) \equiv x^{-1} \bmod 3$.

La loi de réciprocité cubique permet encore d'écrire pour $(\lambda, 3(1+\omega)) = 1$:

$$\left(\frac{1+\omega}{\lambda}\right)^2 = \left(\frac{\lambda}{1+\omega}\right)^2 (\lambda,\ 1+\omega)^2_{\mathfrak{P}_3}$$

où $\mathfrak{P}_3$ est l'idéal engendré par $(1-j)$ dans K, et $(\ .\ ,\ .\ )_{\mathfrak{P}_3}$ le symbole local de reste normique associé.

2. Equation fonctionnelle de la fonction L(E/k,s)

On vient de voir que $L(E/k, s) = L(s, \varphi)$ où φ est un caractère de Hecke de K, de conducteur $\mathfrak{F}$ divisant $9(1+\omega)$. Nous utilisons maintenant les travaux de J. Tate [T] pour déterminer l'équation fonctionnelle.

Soit $S = \{\infty_1, \infty_2, \mathfrak{P}_3, \mathfrak{P}_7, \mathfrak{P}_7'\}$ l'ensemble des places infinies et des places divisant $\mathfrak{F}$ dans K, la place ∞_1 correspondant au plongements $\{id, \overline{id}\}$, la place ∞_2 correspondant aux générateurs respectifs $\tau, \overline{\tau}$ de $Gal(K/\mathbb{Q}(j))$ et $Gal(K/k)$. Déterminons les caractères locaux associés au caractère de Hecke φ d'exposant 1/2. Pour cela, on pose pour $\mathfrak{A}$ premier avec $3(1+\omega)$ dans K :

$$\phi(\mathfrak{A}) = \frac{\varphi(\mathfrak{A})}{N(\mathfrak{A})^{1/2}}$$

ϕ est alors un caractère d'exposant 0. La formule du produit donne, si c désigne le caractère sur le groupe des idèles de K associé à ϕ et $\mathfrak{P}_7 = (2j+\omega)$, $\mathfrak{P}_7' = (2j^2+\omega)$

$$c_{\infty_1}(\alpha)c_{\infty_2}(\alpha)c_{(1-j)}(\alpha)c_{\mathfrak{P}_7}(\alpha)c_{\mathfrak{P}_7'}(\alpha) = \phi^{-1}((\alpha)_S)$$

où $(\alpha)_S$ désigne l'idéal de K engendré par la partie de α première avec $3(1+\omega)$.

Posons $\psi = \chi^{-1}$, soit pour $x \in \mathbb{Q}(j)$, $(x,3) = 1$: $\psi(x) \equiv x$ modulo 3. On obtient alors les caractères aux places de S:

$$c_{\infty_1}(\alpha) = \left(\frac{\alpha}{|\alpha|^{1/2}}\right)^{-1}$$

$$c_{\infty_2}(\alpha) = \left(\frac{\tau(\alpha)}{|\tau(\alpha)|^{1/2}}\right)^{-1}$$

$$c_{\mathfrak{P}_7}(\alpha) = \left(\frac{\alpha(2j+\omega)^{-\nu(\alpha)}}{\mathfrak{P}_7}\right)|\alpha|_{\mathfrak{P}_7}^{it_1}$$

$$c_{\mathfrak{P}_7'}(\alpha) = \left(\frac{\alpha(2j^2+\omega)^{-\nu(\alpha)}}{\mathfrak{P}_7'}\right)|\alpha|_{\mathfrak{P}_7'}^{it_2}$$

$$c_{\mathfrak{P}_3}(\alpha) = \left(\alpha(1-j)^{-\nu(\alpha)}, 1+w\right)_{\mathfrak{P}_3} \psi(N_{K/\mathbb{Q}(j)}(\alpha(1-j)^{-\nu(\alpha)}))|\alpha|_{\mathfrak{P}_3}^{it_3}$$

La détermination du symbole local $(\ ,\ 1+\omega)_{\mathfrak{P}_3}$ est faite dans l'appendice 1. On obtient qu'il est de conducteur 3, donc déterminé par les valeurs

$$(a+b(1-j),\ 1+\omega)_{\mathfrak{P}_3},\ a,\ b \in \{\pm 1,\ \pm\omega,\ \pm(\omega+1),\ \pm(1-\omega)\}$$
$$= \{\omega^k, 0 \le k \le 7\}$$

Sachant que $(\omega^k,\ 1+\omega)_{\mathfrak{P}_3} = (-\omega,\ 1+\omega)_{\mathfrak{P}_3}^k = 1$, il suffit en fait de connaître ce symbole pour les unités principales locales $\epsilon_k = 1+\omega^k(1-j)$. De même on a $\psi\left(N_{K/\mathbb{Q}(j)}(\omega^k)\right) = (-1)^k$, il suffit donc de connaître les valeurs du caractère ψ sur les unités principales.

On obtient alors tableau suivant :

k	0	1	2	3	4	5	6	7
$(\epsilon_k,\ (1+\omega))\mathfrak{p}_3$	j	j	j^2	1	j^2	j^2	j	1
$\psi(N_{K/\mathbb{Q}(j)}(\epsilon_k))$	j	j^2	1	j^2	j^2	j	1	j

Il reste à déterminer les réels t_1, t_2 et t_3, cela se fait en utilisant la formule du produit pour les éléments $2j+\omega$, $2j^2+\omega$ et $1-j$.

$$|2j+\omega|_{\mathfrak{P}_7}^{-it_1} = \left(\frac{2j+\omega}{\mathfrak{P}_7'}\right)\frac{\sqrt{7}(2j+\omega,1+\omega)\mathfrak{p}_3}{N_{K/\mathbb{Q}[j]}(2j+\omega)}\psi(N_{K/\mathbb{Q}[j]}(2j+\omega))$$

$$|2j^2+\omega|_{\mathfrak{P}_7'}^{-it_2} = \left(\frac{2j^2+\omega}{\mathfrak{P}_7}\right)\frac{\sqrt{7}(2j^2+\omega,1+\omega)\mathfrak{p}_3}{N_{K/\mathbb{Q}[j]}(2j^2+\omega)}\psi(N_{K/\mathbb{Q}[j]}(2j^2+\omega))$$

$$|1-j|_{\mathfrak{p}_3}^{-it_3} = \left(\frac{1-j}{\mathfrak{P}_7\mathfrak{P}_7'}\right)\left(\frac{\sqrt{3}}{1-j}\right)^2$$

soit encore :

$$|2j+\omega|_{\mathfrak{P}_7}^{-it_1} = \frac{2-j}{\sqrt{7}} \qquad |2j^2+\omega|_{\mathfrak{P}_7}^{-it_2} = \frac{2-j^2}{\sqrt{7}} \qquad |1-j|_{\mathfrak{p}_3}^{-it_3} = -j$$

Les facteurs locaux provenant des places à l'infini dans l'équation fonctionnelle sont alors avec les notations de [T] :

- Le facteur provenant des places ramifiées de K, ne divisant pas le conducteur $\mathfrak{F}$, c'est à dire des deux places $\mathfrak{P}_{19}$, $\mathfrak{P}_{19}'$ au dessus de $\sqrt{-19}$, soit :

$$\phi(\mathfrak{P}_{19}^{-1})19^{s-1/2} \qquad 19^{s-1/2}\phi(\mathfrak{P}_{19}'^{-1})$$

ou

$$\phi(\mathfrak{P}_{19}^{-1}) = \sqrt{19}/(-5-3j) \quad \phi(\mathfrak{P}_{19}'^{-1}) = \sqrt{19}/(-5-3j^2)$$

d'où une contribution totale de 19^{2s-1}.

- Le facteur provenant des places infinies :

$$\rho(c_{\infty_1}\|^s) = \rho(c_{\infty_1}\|^s) = (-i)\frac{(2\pi)^{1-s}\Gamma(s+\frac{1}{2})}{(2\pi)^s\Gamma(1-s+\frac{1}{2})}$$

d'où une contribution totale de

$$-\frac{(2\pi)^{2-2s}\Gamma(s+\frac{1}{2})^2}{(2\pi)^{2s}\Gamma(1-s+\frac{1}{2})^2}$$

- Le facteur provenant des deux places $\mathfrak{P}_7$, $\mathfrak{P}_7'$:

$$\rho(c_{\mathfrak{P}_7}\|^{s+it_1}) = 7^{s+it_1-1}\sum_{a \bmod \mathfrak{P}_7} c_{\mathfrak{P}_7}(a)\exp\left(2i\pi Tr_{K/\mathbb{Q}}(\frac{a}{2j+\omega})\right)$$

$$\rho(c_{\mathfrak{P}_7'}\|^{s+it_2}) = 7^{s+it_2-1}\sum_{a \bmod \mathfrak{P}_7'} c_{\mathfrak{P}_7'}(a)\exp\left(2i\pi Tr_{K/\mathbb{Q}}(\frac{a}{2j^2+\omega})\right)$$

On remarque que l'on peut prendre a entier modulo 7 dans les deux cas, et donc que le facteur exponentiel est le même et est égal $\exp(10i\pi a/7)$. Les sommes de gauss intervenant correspondent à des caractères conjugués, leur produit vaut donc $7c_{\mathfrak{P}_7'}(-1) = 7$, de plus $7^{i(t_1+t_2)} = 1$, d'où une contribution totale : 7^{2s-1}.

- Le facteur provenant de la place $\mathfrak{P}_3$:

$$\rho(c_{\mathfrak{P}_3}\|^{s+it_3}) = N_{K/\mathbb{Q}}((1-j)^3)^{s+it_3-1/2}\rho_o(c_{\mathfrak{P}_3})$$

avec

$$\rho_o(c_{\mathfrak{P}_3}) = N_{K/\mathbb{Q}}((1-j)^2)^{-1/2}$$
$$\sum_{\epsilon \bmod 1+(1-j)^2} c_{\mathfrak{P}_3}(\epsilon)\exp\left(2i\pi Tr_{K/\mathbb{Q}}(\frac{\epsilon}{(1-j)^3})\right)$$

Pour calculer cette somme on la paramètre à l'aide des unités locales ω^k, $\omega^k\epsilon_l$ pour $0 \leq k < 8$, $0 \leq l < 8$. On vérifie alors les égalités :

$$\exp\left(2i\pi Tr_{K/\mathbb{Q}}(\frac{\omega^k\epsilon_l}{(1-j)^3})\right) = \begin{cases} 1 & \text{si } l+k = 2, 6 \\ j & \text{si } l+k = 1, 3, 4 \\ j^2 & \text{si } l+k = 0, 5, 7 \end{cases}$$

$$\exp\left(2i\pi Tr_{K/\mathbb{Q}}(\frac{\omega^k}{(1-j)^3})\right) = 1$$

$$\sum_k c_{\mathfrak{P}_3}(\omega^k + \omega^\ell(1-j)) = 3(-1)^{\ell+1}$$

ce qui permet d'affirmer que la somme de Gauss vaut -9. La contribution finale de la place $\mathfrak{P}_3$ est donc : $9^{3s+3it_3-3/2} = 9^{3s-3/2}$.

Ceci nous donne l'équation fonctionnelle suivante :

$$L(1-s,\phi) = -\frac{(2\pi)^{2-2s}\Gamma(s+\frac{1}{2})^2}{(2\pi)^{2s}\Gamma(1-s+\frac{1}{2})^2} 19^{2s-1}7^{2s-1}9^{3s-3/2}L(s,\phi)$$

On peut donc obtenir le prolongement analytique de la fonction

$$L(E/k,s) = L(s,\varphi) = L(s-\frac{1}{2},\phi)$$

en posant

$$\Lambda(E,s) = \frac{3591^s\Gamma(s)^2}{\sqrt{3591}(2\pi)^{2s}}L(E/k,s)$$

et l'on obtient l'équation fonctionnelle de la fonction L :

$$\Lambda(E,2-s) = -\Lambda(E,s).$$

3. La descente

Remarquons d'abord que les points d'ordre 2 ou 3 de E ne sont pas rationnels sur k. Une conséquence du tableau donnant les fonctions $L_{\mathfrak{P}}$ est que le nombre de points de la courbe réduite en 2 est 3. Ce qui permet d'affirmer que le sous groupe de torsion de $E(k)$ est trivial. Le même raisonnement montre que la torsion de $E(k(j))$ est d'ordre 3 engendrée par le point $T = (0, 3j(1-j)(1+\omega))$ dont l'annulateur est $1-j$.

Pour majorer le rang de $E(k)$, on utilise la multiplication par $1-j$, définie sur le corps $K = k(j)$. Le groupe $E(K)$ est un $\mathbb{Z}[j]$-module, et nous avons l'égalité suivante :

$$\text{rang}_{\mathbb{Z}} E(k) = \text{rang}_{\mathbb{Z}[j]} E(K).$$

Or le sous-groupe de torsion par $[1-j]$ de E, $E[1-j]$ est contenu dans $E(K)$, ce qui permet d'écrire :

$$\text{rang}_{\mathbb{Z}[j]} E(K) = \text{rang}_{F_3} (E(K)/[1-j]E(K)) - 1.$$

De la suite exacte

$$1 \to E[1-j] \to E \xrightarrow{[1-j]} E \to 1$$

on déduit la suite exacte de 3-descente :

$$1 \to E(K)/[1-j]E(K) \xrightarrow{\delta} S^{[1-j]}(E/K) \xrightarrow{\phi} W(E/K)[1-j] \to 1$$

On remarque que $S^{[1-j]}(E/K)$ est un sous-groupe de $H^1(G_K, E[1-j])$, et que l'action de G_K sur $E[1-j]$) étant triviale, on peut identifier

$$H^1(G_K, E[1-j]) \text{ et } K^*/K^{*3}$$

Déterminons maintenant les applications δ et ϕ. De la formule de multiplication par $[1-j]$ on déduit :

$$(1) \quad \begin{aligned} 4(1-j)^3 (y((1-j)z) - 3j(1-j)(1+\omega)) &= \left(\frac{y(z) - 9(1+\omega)}{x(z)}\right)^3 \\ 4(1-j)^3 (y((1-j)z) + 3j(1-j)(1+\omega)) &= \left(\frac{y(z) + 9(1+\omega)}{x(z)}\right)^3 \end{aligned}$$

de plus la translation par le point d'ordre 3, $T = (0, 3j(1-j)(1+\omega))$ s'écrit:

$$x(z+T) = y(T)\frac{y(T)-y(z)}{2x^2(z)}$$
$$y(z+T) = y(T)\frac{x^3(z)+y^2(T)-y(z)y(T)}{x^3(z)}$$

on déduit l'identité suivante :

$$\frac{y(z+T)-y(T_1)}{x(z+T)} = j^2\frac{y(z)-y(T_1)}{x(z)}$$
$$\frac{y(z+T)+y(T_1)}{x(z+T)} = j\frac{y(z)+y(T_1)}{x(z)}$$

où $T_1 = (3(1+\omega)^{2/3}, 9(1+\omega))$ vérifie $[1-j]T_1 = T$. L'application δ est alors définie par :

$$\delta(X,Y,Z) = \begin{cases} 4(y+3j(1-j)(1+\omega)), & \text{si } [X,Y,Z] = [x,y,1], \\ 1, & \text{si } [X,Y,Z] = [0,1,0] \end{cases}$$

Pour l'application ϕ il faut associer à tout $\lambda \in K^*/K^{*3}$ un espace homogène pour la courbe E. En utilisant les équations (1) on associe à tout élément λ de K^*/K^{*3} la courbe :

$$6^3.\lambda^2.(1+\omega)U^3 = V^3 - \lambda W^3$$

avec :

$$U = X,\ V = \lambda^{2/3}(Y + 9(1+\omega)Z) \text{ et } W = \lambda^{1/3}(Y - 9(1+\omega)Z)$$

D'où la définition de l'application ϕ :

$$\phi(\lambda) : 6^3.\lambda^2.(1+\omega)U^3 = V^3 - \lambda W^3$$

L'étude du groupe de Selmer $S^{[1-j]}(E/K)$:

On sait que le groupe de Selmer correspond à des extensions non ramifiées en dehors des places qui ne divisent pas $3(1+\omega)$ donc en fait

$S^{[1-j]}(E/K) \subset \langle -j,\ \epsilon,\ 1-j,\ 2j+\omega,\ 2j^2+\omega\rangle$ dans K^*/K^{*3}. De plus si λ est un élément du groupe de Selmer, alors l'espace homogène correspondant

$$6^3.\lambda^2.(1+\omega)U^3 = V^3 - \lambda W^3$$

avec :

$$U = X,\ V = \lambda^{2/3}(Y + 9(1+\omega)Z) \text{ et } W = \lambda^{1/3}(Y - 9(1+\omega)Z)$$

admet des points rationnels dans en toute place de K. Un raisonnement élémentaire sur les valuations, montre que λ doit être premier avec $1-j$. De plus le symbole local de reste normique $(\ .\ ,\ .\ )_\nu$ associé aux extensions cubiques est trivial sur les couples dont la somme est un cube soit ici, puisque U et W ne peuvent être nuls :

$$1 = (\lambda W^3,\ 6^3\lambda^2(1+\omega)U^3)_\nu = (\lambda,\ \lambda^2(1+\omega))_\nu = (\lambda, 1+\omega)_\nu$$

pour toute place de K. Posons $\lambda = j^a\epsilon^b(2j+\omega)^c(2j^2+\omega)^d$ alors on obtient en utilisant respectivement les symboles en $\mathfrak{P}_3, \mathfrak{P}_7$ et $\mathfrak{P}_7'$ le système suivant (voir appendice 2):

$$\begin{cases} -a-b+c-d \equiv 0 \\ -a-b+c-d \equiv 0 \\ -a-b+c-d \equiv 0 \end{cases} \quad \text{modulo}(3)$$

qui admet pour ensemble de solutions un espace vectoriel de dimension 3 sur $\mathbf{F}_3$ correspondant au sous-groupe

$$\langle 1+\omega,\ j^2\epsilon,\ j(2j+\omega)\rangle K^{*3}/K^{*3}$$

Mais on sait que $1+\omega = \delta(T)$ est un élément du groupe de Selmer, donc il suffit d'examiner les éléments du groupe

$$\langle\ j^2\epsilon,\ j(2j+\omega)\rangle K^{*3}/K^{*3},$$

ou plus simplement $j^2\epsilon,\ j(2j+\omega),\ \epsilon(2j+\omega)$, et $j^2\epsilon^2(2j+\omega)$. Ces calculs sont fait dans l'appendice 2. On obtient finalement $S^{[1-j]}(E/K) = \langle 1+\omega, j^2\epsilon^2(2j+\omega)\rangle$.

Remarque : Sous la conjecture de Birch et Swinnerton Dyer, le rang de cette courbe détermine le signe de l'équation fonctionnelle de $L(E/K, s)$.

Conclusion sous la conjecture précédente $\mathrm{rang}_{\mathbb{Z}} E(k) = 1$.

Pour aborder l'existence des points entiers, il faut soit trouver un générateur de $E(k)$, soit utiliser la méthode de Baker. C'est cette dernière solution que nous avons retenue. Les calculs nécessitaient au départ l'emploi d'un système de calcul multiprécision, nous avons utilisé le système PARI que nous ont procuré leurs auteurs H. Cohen, M. Olivier, C. Batut à Bordeaux et D. Bernardi à Paris. Depuis M. Waldschmidt et M.Mignotte ([M,W]) nous ont communiqué des nouvelles constantes pour la méthode de Baker. Ces dernières permettent de travailler avec une précision beaucoup moins importante de l'ordre de 10^{-13} au lieu de 10^{-212}.

Appendice

1. Détermination du symbole local $(\ .\ , 1+\omega)_{\mathfrak{p}_3}$ sur les unités

Pour déterminer ce symbole, on calcul d'abord le conducteur de l'extension locale $K_{\mathfrak{p}_3}(\sqrt[3]{1+\omega})/K_{\mathfrak{p}_3}$. On remarque que $\nu((1+\omega)^8-1) = 2$ ce qui montre que le défaut de l'unité locale $1+\omega$ est 2. On en déduit que le conducteur de l'extension est 3 ([W]). Soit $U^{(i)} = \{x \in K_{\mathfrak{p}_3}\ \nu(x-1) = i\}$ et $U = U^{(0)}$. Puisque ω est un représentant modulo 3 d'un Teichmüller, on peut décrire le groupe $U/U^{(2)} = U/U^{(1)} \times U^{(1)}/U^{(2)}$ sous la forme

$$U/U^{(2)} = \{\omega^k, \omega^k(1+\omega^\ell(1-j)), 0 \le k,\ \ell \le 7\}$$

Mais $(-1, 1+\omega)_{\mathfrak{p}_3} = 1$, donc $(\omega, 1+\omega)^k_{\mathfrak{p}_3} = (-\omega, 1+\omega)^k_{\mathfrak{p}_3} = 1$ Il reste à déterminer les symboles $(1+\omega^\ell(1-j), 1+\omega)_{\mathfrak{p}_3}$. Or $U^{(1)}/U^{(2)}$ est un espace vectoriel sur $\mathbf{F}_3$ de base $((1+(1-j),\ (1+\omega(1-j))$ il suffit donc de calculer les deux symboles correspondants. Les deux calculs sont analogues, nous donnons ici uniquement le premier.

Calcul de $(1+(1-j), 1+\omega)_{\mathfrak{p}_3}$

On a : $1+\omega = -(2j+\omega)(2j^2+\omega)$ et $2-j = -j(2j^2+1-\omega)(2j^2+\omega)$ d'où

$$(1+(1-j), 1+\omega)_{\mathfrak{p}_3} = (2j^2+\omega, 2j+\omega)_{\mathfrak{p}_3}(-j(2j^2+1-\omega, 1+\omega)_{\mathfrak{p}_3}$$

le calcul se ramène donc par utilisation de la loi de réciprocité (voir 1) aux calculs des symboles cubiques .

$$\left(\frac{2j^2+\omega}{2j+\omega}\right),\quad \left(\frac{2j+\omega}{2j^2+\omega}\right),\quad \left(\frac{j\,(2j^2+\omega)}{1+\omega}\right) \text{ et } \left(\frac{1+\omega}{2j^2+\omega}\right)$$

Ce qui donne

$$\left(\frac{2j^2+\omega}{2j+\omega}\right)=j^2 \quad \left(\frac{2j+\omega}{2j^2+\omega}\right)=j$$

soit $(2j^2+\omega, 2j+\omega)_{\mathfrak{P}_3}=j^2$ et

$$\left(\frac{-j(2j^2+1-\omega)}{1+\omega}\right)=j^2; \quad \left(\frac{1+\omega}{-j(2j^2+1-\omega)}\right)=j$$

soit $(-j(2j^2+1-\omega), 1+\omega)_{\mathfrak{P}_3}=j^2$.

On obtient donc$(1+(1-j), 1+\omega)_{\mathfrak{P}_3}=j$.

2. Résolution locale des équations $6^3.d^2.(1+\omega)U^3=V^3-dW^3$ pour $d=j, \epsilon, j^2\epsilon$.

Changeons U en U/6, il vient

$$V^3=dW^3+d^2.(1+\omega)U^3$$

Puisque l'indice de ramification absolu est 2, une unité de $K_{\mathfrak{P}_3}$ est un cube si et seulement c'est un cube modulo 9. D'autre part j, ϵ, $j^2\epsilon$ et $1+\omega$ ne sont pas des cubes dans $K_{\mathfrak{P}_3}$, donc on peut supposer que U et W sont des unités locales. En particulier, on peut supposer $U=1$. L'existence de solution pour cette équation dans le localisé en la place $\mathfrak{P}_3$ de K, est donc équivalente à l'existence de solution modulo 9. Pour faciliter les calculs modulo 9, on choisit un Teichmüller ρ de $K_{\mathfrak{P}_3}$, par exemple $\rho \equiv 4\omega$ modulo 9 alors on obtient le tableau suivant dans $A_K/(9)$:

$1+\rho = \rho^2+\rho\,\pi^2+\rho\,\pi^3$	$1-\rho = \rho^3+\pi^2+\pi^3$	$\rho = \omega -\rho\,\pi^2-\rho\,\pi^3$
$1+\rho^2=-\rho^3+\rho^3\pi^2+\rho^3\pi^3$	$1-\rho^2=-\rho+\rho\pi^2+\rho\pi^3$	$\rho^2=1+\omega+\rho\,\pi^2+\rho\,\pi^3$
$1+\rho^3=-\rho^2+\rho^3\pi^2+\rho^3\pi^3$	$1-\rho^3=\rho+\pi^2+\pi^3$	$\rho^3=1-\omega-\rho^3\pi^2-\rho^3\pi^3$
$1+\rho^4=-1$	$1-\rho^4=-1-\pi^2-\pi^3$	$\rho^4=-1$

Un cube modulo 9 est alors de la forme :

$$V^3=\rho^{3a}(1+(\rho^{3b}-\rho^b)\pi^3), \text{ ou } V^3=\rho^{3a}\pi^3 \text{ avec } a, b\in\{0,\ldots,7\}$$

d'autre part on a :

$$j=1-\pi, \quad 1+\omega=\rho^2-\rho\pi^2-\rho\pi^3, \quad \epsilon=\rho^2-\pi-\rho^3\pi^2-\rho^3\pi^3$$

d'où :

$$\begin{aligned}
j^2\epsilon &= \rho^2+\rho\ \pi-\rho^2\pi^2+\rho^3\pi^3\\
j(2j+\omega) &= -\rho^3-\rho^2\pi+\rho\ \pi^2-\rho^2\pi^3\\
\epsilon(2j+\omega) &= 1-\ \pi+\rho\ \pi^2+\rho^2\pi^3\\
j\epsilon^2(1+\omega) &= -\rho^2+\rho\ \pi+\ \pi^2\\
j^2\epsilon^2(2j+\omega) &= \rho^3\ \ +\rho^2\pi^2-\rho^2\pi^3\\
j^2(2j+\omega)^2(1+\omega) &= 1\ +\rho^3\pi-\ \pi^2-\rho^3\pi^3\\
\epsilon(2j+\omega)(1+\omega) &= -1\ +\rho^3\pi-\rho^2\pi^2-\ \pi^3\\
j^2\epsilon^2(2j+\omega)(1+\omega) &= 1\ \ -\rho^3\pi^2
\end{aligned}$$

On vérifie alors que la seule valeur de d pour laquelle il y a une solution possible est $d = j^2\epsilon^2(2j+\omega)$ avec par exemple

$$(-\rho\pi)^3 = j^2\epsilon^2(2j+\omega)(\rho^3)^3 + j\epsilon^4(2j+\omega)^2(1+\omega)$$

BIBLIOGRAPHIE

[C-F] - J. COUGNARD, V. FLECKINGER *Sur la monogénéité de l'anneau des entiers de certains corps de rayon* A paraître dans Manuscripta Mathematica.

[C-N,T] - Ph. CASSOU-NOGUÈS, M. J. TAYLOR *Elliptic functions and rings of integers.* Progress in Mathematics **66**. Birkhaüser.

[M,W] - M. MIGNOTTE, M. WALDSCHMIDT *Linear forms in two logarithms and Schneider's method (III).* Preprint Université de Strasbourg.

[N] - A. NERON *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux.* IHES Publ. Math.**21** (1964), 361-482.

[Sc] - R. SCHERTZ *Konstruktion von Potenzganzheitsbasen in Strahlklassenkörpern über imaginär quadratischen Zahlkörpern* . A paraître.

[Si] - J. H. SILVERMAN *The Arithmetic of Elliptic Curves.* Springer-Verlag (1986).

[Sh] - G. SHIMURA *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press, (1971).

[T] - J. TATE *Fourier Analysis in number fields and Hecke's Zeta function*, Thesis, Princeton (1950).

[W] - B.F. WYMAN *Widly ramified Gamma Extensions*, American Journal of Mathematics,**91** (1969), 153-152.

U.A. 741 du C.N.R.S.

Laboratoire de Mathématiques

Faculté des Sciences de Besançon

F25030 BESANÇON Cedex