THEORIE DES NOMBRES
BESANCON

Années 1986/87-1987/88
Fascicule 1

GENERATION DE BASES D'ENTIERS A PARTIR DE LA COURBE $y^2 = 4x^3+1$

Vincent FLECKINGER

Génération de bases d'entiers à partir de la courbe $y^2 = 4x^3 + 1$

par Vincent FLECKINGER

Soit $k = \mathbb{Q}[j]$, où j désigne la racine cubique de l'unité $e^{\frac{2i\pi}{3}}$. L'anneau des entiers de k, $\mathbb{Z}[j]$, est un réseau de $\mathbb{C}$. On notera $\wp$ la fonction de Weierstrass associée, et E la courbe elliptique $\mathbb{C}/\mathbb{Z}[j]$. En utilisant le modèle $y^2 = 4x^3 + 1$ de cette courbe, on montre le théorème suivant :

Théorème principal :

Soit $\mathfrak{A}$ un idéal propre de $\mathbb{Z}[j]$, premier avec $1 - j$. Si β désigne un point de E, primitif de $\mathfrak{A}$-division, et $F(\beta) = x^{-1}(\beta)$, alors on a l'égalité suivante :

$$A_{k(\mathfrak{A})} = \mathbb{Z}[j]\left[\frac{F^3(\beta) + 4}{3(1 - j)}\right]$$

où $A_{k(\mathfrak{A})}$ désigne l'anneau des entiers du corps de classes de rayon $\mathfrak{A}$ sur k.

Ces résultats sont dans la lignée de ceux obtenus par Ph. Cassou-Noguès et M. Taylor [C.-N, T], J. Cougnard [Cou2], et l'auteur [Fl]. Dans une première partie, on établit les formules de récurrences permettant d'obtenir les abscisses des points de division de E, pour le modèle considéré, en vue de la programmation sur micro-ordinateur. Dans la deuxième partie on étudie les propriétés algébriques des valeurs des coordonnées x et y aux points de division d'ordre premier à 3.

Enfin on démontre le théorème principal dans la troisième partie , et on donne quelques exemples numériques .

1.- Les points de division du modèle $y^2 = 4x^3 + 1$.

Soit f un point primitif de $(1 - j)$-division de E , $f \in \{\frac{2+j}{3}, -\frac{2+j}{3}\}$. On désigne par $\wp'(f)^{1/3}$ une racine cubique de $\wp'(f)$ fixée une fois pour toute .

On pose :

$$x(z) = \frac{\wp(z) - \wp(f)}{\wp'(f)^{2/3}} = \frac{\wp(z)}{\wp'(f)^{2/3}} \quad \text{et} \quad y(z) = \frac{\wp'(z)}{\wp'(f)} .$$

Alors les fonctions elliptiques x et y sont liées par l'équation :

$$y^2(z) = 4x^3(z) + 1 . \tag{1}$$

Le diviseur de x étant $(f) + (-f) - 2(0)$, on vérifie aisément que :

$$x(z)\, x(z+f)\, x(z-f) = -1 \tag{2}$$

de même le diviseur de y étant $(\frac{1}{2}) + (\frac{j}{2}) + (\frac{j^2}{2}) - 3(0)$, on obtient :

$$y(z)\, y(z+\tfrac{1}{2})\, y(z+\tfrac{j}{2})\, y(z+\tfrac{j^2}{2}) = -27 \tag{3}$$

$\frac{1}{2}$, $\frac{j}{2}$ et $\frac{j^2}{2}$ représentant les points non nuls de 2-division de E .

Soit maintenant un idéal entier $\mathfrak{J}$ de $\mathbb{Z}[j]$, il existe un entier algébrique ν engendrant $\mathfrak{J}$. Pour obtenir les points de ν-division , on utilise la fonction $x(\nu z)$.

Proposition 1 :

Soit ν un élément de $\mathbb{Z}[j]$ premier avec $1-j$.

Alors on a l'égalité :

$$x(\nu z) = c_\nu \prod_{\nu\beta = 0} x(z + \beta) \qquad (4)$$

où $c_\nu^3 = (-1)^{N(\nu)} - 1$ et $N(\nu) = \nu\bar{\nu}$.

Pour la démonstration on renvoie le lecteur à [FI] .

Posons alors :

$$Z_\nu(X) = \nu \prod_{\substack{\nu\beta = 0 \\ \beta \neq 0}}' (X - x(\beta)) \quad \text{si } (\nu, 2) = 1$$

$$Z_\nu(X) = \frac{\nu}{2} \prod_{\substack{\nu\beta = 0 \\ 2\beta \neq 0}}' (X - x(\beta)) \quad \text{si } 2 \mid \nu$$

le produit étant indexé par un système de représentants des classes non nulles des points de ν-division modulo ± 1 .

Proposition 2 :

Soit ν un élément de $\mathbb{Z}[j]$ premier avec $(1 - j)$.

$$Z_\nu(0) = c_\nu \chi(\nu) \qquad (5)$$

où χ désigne le caractère non trivial modulo $1 - j$.

Démonstration :

De l'égalité (4) on déduit :

$$\frac{x(\nu z)}{x(z)} = c_\nu \prod_{\substack{\nu\beta = 0 \\ \beta \neq 0}} x(z + \beta) \qquad (6)$$

La règle de l' Hopital permet d'écrire :

$$\lim_{z \to f} \frac{x(\nu z)}{x(z)} = \nu \frac{x'(\nu f)}{x'(f)}$$

Or $\nu f = \chi(\nu) f$ dans E , d'où $\dfrac{x'(\nu f)}{x'(f)} = \chi(\nu)$.

On obtient donc :

$$\nu\,\chi(\nu) = c_\nu \prod_{\substack{\nu\beta = 0 \\ \beta \neq 0}} x(f+\beta)\ .$$

L'utilisation de (2) permet d'écrire :

si $(\nu, 2) = 1$ $\quad \displaystyle\prod_{\substack{\nu\beta = 0 \\ \beta \neq 0}} x(f+\beta) = \frac{(-1)^{\frac{N(\nu)-1}{2}}}{\prod' x(\beta)} = \frac{\nu}{Z_\nu(0)}$

si $2 \mid \nu$ $\quad \displaystyle\prod_{\substack{\nu\beta = 0 \\ 2\beta \neq 0}} x(f+\beta) = \frac{(-1)^{\frac{N(\nu)-4}{2}}}{\prod' x(\beta)} = \frac{\nu}{2\,Z_\nu(0)}$

Il reste à calculer le produit $x(\frac{1}{2}+f)\,x(\frac{j}{2}+f)\,x(\frac{j^2}{2}+f)$.

Pour cela on constate que les solutions dans E de :

$$(1-j)Z = \frac{1}{2}$$

sont $\frac{j}{2}$, $\frac{j}{2}+f$ et $\frac{j}{2}-f$.

Et on calcule $x((1-j)z)$ en utilisant la formule d'addition de la fonction $\wp$, soit :

$$x((1-j)z) = -\frac{x(z)^3+1}{3j\,x(z)^2} \qquad (7)$$

$x(\frac{j}{2})$, $x(\frac{j}{2}+f)$ et $x(\frac{j}{2}-f) = x(\frac{j}{2}+f)$ sont les racines du polynôme

$$X^3 + 3j\,x(\tfrac{1}{2})X + 1$$

d'où $x(\frac{j}{2}+f)$ est la racine double de ce polynôme , soit :

$$x(\tfrac{j}{2}+f) = -2j\,x(\tfrac{1}{2}) = -2x(\tfrac{j}{2})$$

puis $\quad x(\frac{j^2}{2}+f) = -2j\,x(\frac{j}{2}) = -2x(\frac{j^2}{2})$

et $\quad x(\frac{1}{2}+f) = -2j\,x(\frac{j^2}{2}) = -2x(\frac{j}{2})$.

Enfin, l'égalité $4(X - x(\frac{1}{2}))(X - x(\frac{j}{2}))(X - x(\frac{j^2}{2})) = 4X^3 + 1$

donne :

$$(X - x(\tfrac{1}{2} + f))(X - x(\tfrac{j}{2} + f))(X - x(\tfrac{j^2}{2} + f)) = X^3 - 2 \qquad (8)$$

et $$x(\tfrac{1}{2} + f)\, x(\tfrac{j}{2} + f)\, x(\tfrac{j^2}{2} + f) = 2$$

ce qui achève la démonstration de la proposition 2 .

Exprimons maintenant $x(\nu z)$ à l'aide du polynôme Z_ν .

Proposition 3 :

Soit ν un élément de $\mathbb{Z}[j]$, premier avec $1 - j$.

Si $(\nu, 2) = 1$ alors :

$$x(\nu z) = c_\nu\, x(z)^{N(\nu)}\, \frac{Z_\nu(x(z+f))\, Z_\nu(x(z-f))}{Z_\nu(x(z))^2} \qquad (9)$$

Si $2 \mid \nu$ alors :

$$x(\nu z) = c_\nu\, x(z)^{N(\nu)-3}\, \frac{Z_\nu(x(z+f))\, Z_\nu(x(z-f))\,(2 - x(z)^3)}{Z_\nu(x(z))^2\,(4x(z)^3 + 1)}$$

Démonstration :

Le diviseur de $x(\nu z)$ est :

$$\sum_{\nu\beta = 0} (\beta + f) + (\beta - f) - 2(\beta) .$$

Le diviseur de $x(z + f)$ est $(f) + (0) - 2(-f)$

et celui de $x(z - f)$ est $(-f) + (0) - 2(f)$.

D'après (8) celui de $2 - x(z)^3$ est :

$$(\tfrac{1}{2} + f) + (\tfrac{j}{2} + f) + (\tfrac{j^2}{2} + f) + (\tfrac{1}{2} - f) + (\tfrac{j}{2} - f) + (\tfrac{j^2}{2} - f) - 6(0)$$

et celui de $Z_\nu(x(z))$ est :

$$\sum_{\substack{\nu\beta = 0 \\ 2\beta \neq 0}} [(\beta) + (-\beta) - 2(0)]$$

On en déduit l'égalité des diviseurs des deux membres de chaque égalité citée en (9) , il reste donc à calculer le coefficient de proportionnalité . Pour cela , on calcule la limite du rapport quand z tend vers 0 .

Pour obtenir des relations de récurrences , on calcule :

$$x(\nu z) - x((1-j)z) \ .$$

Proposition 4 :

Soit ν un élément de $\mathbb{Z}[j]$ premier avec $1-j$.

Si $\nu \equiv 0 \bmod 2$:

$$x(\nu z) - x((1-j)z) = \frac{1}{3j} \frac{Z_{\nu-1+j}(x(z))\, Z_{\nu+1-j}(x(z))}{Z_{\nu}(x(z))^2\, x(z)^2\, (4x^3(z)+1)}$$

Si $\nu \equiv 1 , j \bmod 2$:

$$x(\nu z) - x((1-j)z) = \frac{1}{3j} \frac{Z_{\nu-1+j}(x(z))\, Z_{\nu+1-j}(x(z))}{Z_{\nu}(x(z))^2\, x(z)^2} \qquad (10)$$

Si $\nu \equiv j^2 \bmod 2$:

$$x(\nu z) - x(1-j)z) = \frac{1}{3j} \frac{Z_{\nu-1+j}(x(z))\, Z_{\nu+1-j}(x(z))\, (4x^3(z)+1)}{Z_{\nu}(x(z))^2\, x(z)^2}$$

La démonstration est de même nature que celle de la proposition 3 .

En utilisant (7) , (9) et (10) on obtient les formules suivantes :

Si $\nu \equiv 0 \bmod 2$:

$$Z_{\nu+1-j}(x(z))\, Z_{\nu-1+j}(x(z)) =$$

$$3j c_{\nu} x(z)^{N(\nu)-1} Z_{\nu}(x(z+f))\, Z_{\nu}(x(z-f))\, (2-x^3(z)) + (4x^6(z)+5x^3(z)+1)\, Z_{\nu}(x)$$

Si $\nu \equiv 1$, j mod 2 :

$$Z_{\nu+1-j}(x(z))\, Z_{\nu-1+j}(x(z)) =$$

$$3jc_\nu\, x(z)^{N(\nu)+2}\, Z_\nu(x(z+f))\, Z_\nu(x(z-f)) + (x(z)^3+1)\, Z_\nu(x(z))^2$$

Si $\nu \equiv j^2$ mod 2 :

$$Z_{\nu+1-j}(x(z))\, Z_{\nu-1+j}(x(z))(4x^3(z)+1) =$$

$$3jc_\nu\, x(z)^{N(\nu)+2}\, Z_\nu(x(z+f))\, Z_\nu(x(z-f)) + (x(z)^3+1)\, Z_\nu(x(z))^2 \ .$$

Il nous reste à exprimer $x(z+f)$ et $x(z-f)$ en fonction de $x(z)$ et $y(z)$.

z , $z+f$ et $z-f$ sont les solutions de $(1-j)Z = (1-j)z$ dans E , on en déduit que $x(z)$, $x(z+f)$ et $x(z-f)$ sont les racines du polynôme :

$$X^3 + 3jx((1-j)z)\,X^2 + 1 = X^3 - \frac{x^3(z)+1}{x^2(z)}\,X^2 + 1 \ .$$

On en déduit :

$$x(z+f) + x(z-f) = \frac{1}{x^2(z)} \quad \text{et} \quad x(z+f)\,x(z-f) = \frac{-1}{x(z)} \ .$$

$x(z+f)$ et $x(z-f)$ sont donc les racines du polynôme :

$$X^2 - \frac{1}{x^2(z)}\,X - \frac{1}{x(z)} \ ,$$

dont le discriminant est :

$$\left(\frac{y(z)}{x^2(z)}\right)^2 \ .$$

On en déduit , puisque $x(2f) = 0$:

$$x(z+f) = \frac{1}{2}\,\frac{1-y(z)}{x^2(z)} \quad \text{et} \quad x(z-f) = \frac{1}{2}\,\frac{1+y(z)}{x^2(z)} \qquad (11)$$

Puisque $x(jz) = j\,x(z)$, il est clair que les $Z_\nu(X)$ sont en fait des polynômes en X^3 . On pose donc :

$$P_\nu(X^3) = Z_\nu(X) ,$$

ce qui précède permet alors d'écrire les formules de récurrences liant les P_ν .

Si $\nu \equiv 0 \bmod 2$:

$$P_{\nu+1-j}(X)\,P_{\nu-1+j}(X) = 3jc_\nu X^{\frac{N(\nu)-1}{3}}(2-X)Q_\nu(X) + (4X^2+5X+1)P_\nu(X)^2$$

Si $\nu \equiv 1, j \bmod 2$:

$$P_{\nu+1-j}(X)\,P_{\nu-1+j}(X) = 3jc_\nu X^{\frac{N(\nu)+2}{3}} Q_\nu(X) + (X+1)\,P_\nu(X)^2$$

Si $\nu \equiv j^2 \bmod 2$:

$$P_{\nu+1-j}(X)\,P_{\nu-1+j}(X)(4X+1) = 3jc_\nu X^{\frac{N(\nu)+2}{3}} Q_\nu(X) + (X+1)P_\nu(X)^2$$

où $Q_\nu(X)$ désigne $P_\nu\left(\frac{3X+1-(X+1)\sqrt{4X+1}}{2X^2}\right)P_\nu\left(\frac{3X+1+(X+1)\sqrt{4X+1}}{2X^2}\right)$

Notons ensuite :

$$T_\nu(X) = (c_\nu\,\chi(\nu))^{-1} X^{\frac{N(\nu)-4}{6}} P_\nu\left(\frac{1}{X}\right) \qquad \text{si } 2 \mid \nu$$

$$T_\nu(X) = (c_\nu\,\chi(\nu))^{-1} X^{\frac{N(\nu)-1}{6}} P_\nu\left(\frac{1}{X}\right) \qquad \text{si } 2 \nmid \nu$$

Les relations de récurrences deviennent : (12)

Pour $\nu \equiv 1, j \bmod 2$:

$$T_{\nu+1-j}(X)\,T_{\nu+j-1}(X) = 3jc_\nu(-X)^{\frac{N(\nu)-1}{6}} U_\nu(X) + (X+1)\,T_\nu(X)^2$$

Si $\nu \equiv j^2 \bmod 2$:

$$T_{\nu+1-j}(X)\,T_{\nu+j-1}(X)(4+X) = 3jc_\nu(-X)^{\frac{N(\nu)-1}{6}}\,U_\nu(X) + (X+1)T_\nu(X)^2$$

Si $\nu \equiv 0 \bmod 2$:

$$T_{\nu+1-j}(X)\,T_{\nu+j-1}(X) = -3jc_\nu(2X-1)(-X)^{\frac{N(\nu)-4}{6}}\,U_\nu(X)+(X^2+5X+4)T_\nu(X)^2$$

avec $U_\nu(X) = T_\nu\left(\frac{3X + X^2 +(X+1)\sqrt{4X+X^2}}{-2X}\right)T_\nu\left(\frac{3X+X^2-(X+1)\sqrt{4X+X^2}}{-2X}\right)$

On obtient alors la proposition suivante :

Proposition 5 :

Soit ν un élément de $\mathbb{Z}[j]$, premier avec $(1-j)$.

Alors $T_\nu(X)$ est un polynôme unitaire de $\mathbb{Z}[j][X]$ vérifiant :

$$T_\nu(0) = \frac{\nu}{c_\nu\,\chi(\nu)}\ .$$

Remarque :

$$T_\nu(X) = \prod_{\substack{\nu\beta=0\\ 2\beta\neq 0}}{}''\ (X - x^{-3}(\beta))$$

le produit portant sur des représentants des orbites des points non nuls de ν-divisions, non annulés par 2, sous l'action du groupe d'automorphisme de E engendré par $-j$.

II.- Propriétés arithmétiques des coordonnées x et y aux points de division d'ordre premier à 3 .

Dans la suite $\mathfrak{A}$ désigne un idéal propre de $\mathbb{Z}[j]$, premier avec $1-j$, et $k(\mathfrak{A})$ le corps des classes de rayon $\mathfrak{A}$ sur $k = \mathbb{Q}[j]$.

Soit $h(z) = -\frac{2^9 3^6 g_3}{\Delta} \wp^3(z)$ la troisième fonction de Weber associée à $\mathbb{Z}[j]$.

Si on pose $F(z) = \frac{1}{x(z)}$, alors $F^3(z) = \frac{2^9 3^6}{h(z)}$ (13)

Un résultat classique de multiplication complexe ([Sh], Chap.6, § 6-8) permet d'affirmer que pour tout point β primitif de $\mathfrak{A}$-division, c'est-à-dire d'annulateur égal à $\mathfrak{A}$, $k(F^3(\beta)) = k(\mathfrak{A})$.

Proposition 1 :

Soit β un point primitif de $\mathfrak{A}$-division.

Alors $F^3(\beta)$ est un entier algébrique.

Cela résulte de I, proposition 5.

La loi de réciprocité de Shimura permet de décrire explicitement les conjugués de $F^3(\beta)$: si u est un idèle unité de k, et si α est un élément de $\mathbb{Z}[j]$ vérifiant $\alpha \equiv u \bmod^* \mathfrak{A}$, alors :

$$F^3(\beta)^{(u^{-1},k)} = F^3(\alpha\beta)$$

où $(.,k)$ désigne le symbole d'Artin.

Les conjugués de $F^3(\beta)$ sont donc les éléments de la forme :

$F^3(\beta')$, avec annulateur (β') = annulateur (β).

Posons, pour tout idéal $\mathfrak{A}$ premier avec $1-j$:

$$S_{\mathfrak{A}}(X) = \begin{cases} 1 \ , \ \text{si} \ \mathfrak{A} = (2) \\ \prod_{\text{Ann}(\beta) = \mathfrak{A}}'' (X - F^3(\beta)) \ \text{sinon} \end{cases}$$

le produit portant sur les orbites des points primitifs de $\mathfrak{A}$-division , sous l'action du groupe des automorphismes de E .

Soit ν un élément de $\mathbb{Z}[j]$, premier avec $1 - j$, la décomposition en facteurs irréductibles de $T_\nu(X)$ est donc :

$$T_\nu(X) = \prod_{\mathfrak{A} \mid \nu} S_{\mathfrak{A}}(X)$$

Sachant que $(T_\nu(0)) = (\nu)(\nu, 2)^{-1}$ où $(\nu, 2)$ désigne le pgcd de (ν) et (2) , on obtient :

Proposition 2 :

Si $\mathfrak{A} = (2)^n$ $n > 1$ $(S_{\mathfrak{A}}(0)) = (2)$.

Si $\mathfrak{A} = \mathfrak{p}^n$ $n \geq 1$, $\mathfrak{p}$ premier distinct de 2 et $1 - j$, alors : $(S_{\mathfrak{A}}(0)) = \mathfrak{p}$.

Si $\mathfrak{A}$ est divisible par deux idéaux premiers distincts , $(\mathfrak{A}, 3) = 1$, alors $S_{\mathfrak{A}}(0)$ est une unité .

Corollaire 3 :

Soient $\mathfrak{A}$ un idéal propre de $\mathbb{Z}[j]$, premier avec $1 - j$ et β un point primitif de $\mathfrak{A}$-division .

Si $\mathfrak{A} = (2)$ $F^3(\beta) = -4$.

Si $\mathfrak{A} = (2^n)$ $n > 1$, (ou $\mathfrak{A} = \mathfrak{p}^n$ $n \geq 1$, $\mathfrak{p}$ premier) , alors :

$$(F^3(\beta))^{[k(\mathfrak{A}) : k]} = (2) \ , \ ((F^3(\beta))^{[k(\mathfrak{A}) : k]} = \mathfrak{p})$$

Si $\mathfrak{A}$ est divisible par deux idéaux premiers distincts :

$F^3(\beta)$ est une unité .

Intéressons nous maintenant à la deuxième coordonnée .

D'après (2) et (11) , on a les égalités suivantes :

$$y(z) = 1 - 2x(z)^2\, x(z+f)$$
$$= 1 + 2\,\frac{x(z)}{x(z-f)}$$

d'où :

$$(y(z)-1)^3 = 8\,\frac{x(z)^3}{x(z-f)^3}$$

puis :

$$y(z)(y(z)^2+3) - 3y^2(z) - 1 = 8\,\frac{x^3(z)}{x^3(z-f)}$$

soit :

$$y(z)\,(1+F^3(z)) = 2F^3(z-f) + F^3(z) + 3$$

En particulier si β est primitif de $\mathfrak{A}$-division :

$$k(y(\beta)) = k((1-j)\mathfrak{A}) \quad \text{et} \quad k(y^2(\beta)) = k(\mathfrak{A})$$

D'après (7) on a :

$$x((1-j)z) = -\,\frac{x^3(z)+1}{3jx^2(z)}$$

d'où :

$$F^3(z) + 1 = -3j\,\frac{F(z)}{F((1-j)z)} \qquad (14)$$

Soit β un point primitif de $\mathfrak{A}$-division , alors il en est de même pour $(1-j)\beta$, et $\dfrac{F(\beta)}{F((1-j)\beta)}$ est une unité (II, corollaire 3) . Puisque $y^2(\beta) = \dfrac{F^3(\beta)+4}{F^3(\beta)}$, si ν est une place de $k(\mathfrak{A})$ divisant $1-j$, on a :

$$\nu(y^2(\beta)) \geq \nu(3) = 2\nu(1-j)$$

Or l'extension $k(y^2(\beta))/k$ est non ramifiée en $1-j$, et l'extension $k(y(\beta))/k(y^2(\beta))$ est ramifiée en toute place divisant $1-j$, la valuation $\nu(y^2(\beta))$ ne peut donc pas être paire , d'où :

$$\nu(y^2(\beta)) \geq 3\nu(1-j)) \ .$$

L'égalité (3) donne alors :

$$\nu(y^2(\beta)) = 3\nu(1-j) \ .$$

Proposition 4 :

Soient $\mathfrak{A}$ un idéal propre de $\mathbb{Z}[j]$, premier avec $1-j$ et β un point primitif de $\mathfrak{A}$-division .

Si $\mathfrak{A} = \mathfrak{p}^n$ $n>0$ $\mathfrak{p}$ premier distinct de 2 $(y^2(\beta)) = (1-j)^3 (F^3(\beta))^{-1}$.

Si $\mathfrak{A} = 2\mathfrak{p}^n$ $n>0$ $\mathfrak{p}$ premier distinct de 2 $(y^2(\beta)) = ((1-j)^3)(F(2\beta))$.

Dans les autres cas , $(y^2(\beta)) = (1-j)^3$ si $\mathfrak{A} \neq (2)$.

Démonstration :

Le calcul concernant la valuation de $y^2(\beta)$ en une place divisant $1-j$ vient d'être fait .

D'après la formule (3) :

$$x(2z) = x(z)\ \frac{x^3(z)-2}{4x^3(z)+1}$$

d'où :

$$(F^3(\beta)+4)\,F(\beta) = F(2\beta)\,(1-2F^3(\beta)) \ .$$

Chaque facteur de cette égalité est un entier algébrique , ce qui permet d'affirmer que :

$$1-2F^3(\beta) \text{ divise } F^3(\beta)+4$$

mais :

$$1-2F^3(\beta) = 9-2(F^3(\beta)+4)$$

donc :

$$1-2F^3(\beta) \text{ divise } 9 \ , \text{ puis l'égalité}$$

$$y^2(\beta)\,F^3(\beta) = F^3(\beta) + 4$$

et la valuation de $y^2(\beta)$ aux places divisant $1 - j$ donne :

$$(1 - 2F^3(\beta)) = ((1 - j)^3) \qquad (15)$$

Enfin $y^2(\beta)$ est associé à $\frac{F(2\beta)}{F^4(\beta)}(1 - j)^3$ d'où la proposition .

III.- Démonstration du théorème principal .

Soit $\mathfrak{A}$ un idéal propre de $\mathbb{Z}[j]$, distinct de 2 et premier avec $1 - j$. Si β est un point primitif de $\mathfrak{A}$-division , alors

$\frac{F^3(\beta) + 4}{3(1 - j)}$ est un entier algébrique engendrant $k(\mathfrak{A})$ sur k .

Pour démontrer que $\mathbb{Z}[j]\left[\frac{F^3(\beta) + 4}{3(1 - j)}\right] = A_{k(\mathfrak{A})}$ il suffit de montrer l'égalité des discriminants :

$$d_1 = \mathcal{D}(A_{k(\mathfrak{A})}/\mathbb{Z}[j]) \qquad d_2 = \mathcal{D}(\mathbb{Z}[j]\left[\frac{F^3(\beta)+4}{3(1 - j)}\right]/\mathbb{Z}[j])$$

Calcul de d_1 :

Soit $\mathfrak{p}$ un idéal premier de $\mathbb{Z}[j]$ divisant $\mathfrak{A}$, posons :

$$\mathfrak{A} = \mathfrak{p}^r\,\mathfrak{A}' \text{ avec } (\mathfrak{A}', \mathfrak{p}) = 1 , \quad q = N_{\mathbb{Q}[j]/\mathbb{Q}}(\mathfrak{p}) .$$

On calcule la valuation de d_1 en $\mathfrak{p}$ en utilisant la théorie du corps de classes .

Si U désigne le groupe des idèles unités de $\mathbb{Q}[j]$, $U_{\mathfrak{A}}$ le groupe des idèles unités de $\mathbb{Q}[j]$ congrus à 1 mod* $\mathfrak{A}$, et $\langle -j \rangle$ le groupe des unités de $\mathbb{Z}[j]$, alors le groupe de Galois $Gal(k(\mathfrak{A})/k)$ est isomorphe à $U/\langle -j \rangle U_{\mathfrak{A}}$. Il y a exactement $[k(\mathfrak{p}^s\mathfrak{A}') : k] - [k(\mathfrak{p}^{s-1}\mathfrak{A}') : k]$ caractères de $Gal(k(\mathfrak{A})/k)$ dont

le conducteur est de valuation $0 < s \leq r$ en $\mathfrak{p}$, d'où en utilisant la formule de Hasse :

$$v_{\mathfrak{p}}(d_1) = [k(\mathfrak{A}') : k] \sum_{s=1}^{r} s([k(\mathfrak{p}^s \mathfrak{A}') : k(\mathfrak{A}')] - [k(\mathfrak{p}^{s-1} \mathfrak{A}') : k(\mathfrak{A}')])$$

La fonction d'Euler définie par $\varphi(\mathfrak{A}) = \#(\mathbb{Z}[j]/\mathfrak{A})^*$ permet le calcul de $[k(\mathfrak{A}) : k]$:

Si $\mathfrak{A} \neq 2, 3$ $\quad [k(\mathfrak{A}) : k] = \frac{1}{6} \varphi(\mathfrak{A})$

$$[k(2) : k] = [k(3) : k] = 1$$

d'où :

$$v_{\mathfrak{p}}(d_1) = \begin{cases} \frac{1}{6}(r q^r - (r+1) q^{r-1} - 5) & \text{si } \mathfrak{A}' = 1 \quad \mathfrak{p} \neq 2 \\ \frac{1}{6}(r q^r - (r+1) q^{r-1} - 8) & \text{si } \mathfrak{A} = (2^r)\ r > 1 \\ \frac{1}{2}(r q^r - (r+1) q^{r-1} - 1) & \text{si } \mathfrak{A}' = (2) \\ [k(\mathfrak{A}') : k](r q^r - (r+1) q^{r-1}) & \text{sinon} \end{cases}$$

Calcul de d_2 :

On utilise la formule d'Euler :

$$d_2 = N_{k(\mathfrak{A})/k}\left(\prod_{\sigma \neq id} \left(\frac{F^3(\beta) - F^3(\beta)^{\sigma}}{3(1-j)} \right) \right)$$

Il faut donc évaluer les différences :

$F^3(\beta) - F^3(\beta)^{\sigma}$ pour $\sigma \in Gal(k(\mathfrak{A})/k) \setminus \{id\}$

Soit u un idèle unité de k, dont la classe modulo $\langle -j \rangle U_{\mathfrak{A}}$ est non triviale, la loi de réciprocité de Shimura donne :

$$F^3(\beta) = F^3(\beta)^{(u^{-1}, \beta)} = F^3(\beta) - F^3(u\beta) \qquad (16)$$

où $u\beta$ est le point de $\mathfrak{A}$-division défini par $\alpha\beta$ pour α appartenant à $\mathbb{Z}[j]$ et vérifiant $\alpha \equiv u \mod^* \mathfrak{A}$.

Lemme 1 :

On a l'identité suivante :

$$\frac{(F^3(z) - F^3(\beta))^2}{F^3(z)F^3(\beta)(F^3(z) + F^3(\beta)+3) - 1} = - \prod_{i=0}^{5} F((-j)^i z - \beta)$$

Démonstration :

On montre d'abord que :

$$F^3(z)\, F^3(\beta)(F^3(z) + F^3(\beta) + 3) - 1 =$$

$$(F^3(z) - F^3(\beta - f))\,(F^3(z) - F^3(\beta+f))\, F^3(\beta) \qquad (17)$$

En effet , d'après le calcul conduisant à (11) , les racines du polynôme

$$X^2 - F^2(\beta)X - F(\beta)$$

sont $F^{-1}(\beta + f)$ et $F^{-1}(\beta - f)$. On obtient alors le polynôme dont les racines sont $F^3(\beta + f)$ et $F^3(\beta - f)$, et de coefficient dominant $F^3(\beta)$, d'où (17) .

Le lemme résulte alors de l'égalité des diviseurs des deux membres de l'identité , et de l'évaluation en 0 .

Lemme 2 :

Soit $\mathfrak{A}$ un idéal propre de $\mathbb{Z}[j]$ distincts de 2 et premier avec $1 - j$. Si β et β' sont deux points primitifs de $\mathfrak{A}$-division , et d'orbites distinctes sous l'action de $\langle -j \rangle$, alors :

$$(F^3(\beta)F^3(\beta')(F^3(\beta) + F^3(\beta') + 3) - 1) = (27)$$

Démonstration :

On a l'égalité polynomiale suivante :

$$XY(X + Y + 3) - 1 = (X - Y)(Y(X - Y) + 3Y(Y + 1)) + (2Y - 1)(Y + 1)^2$$

Posons $F^3(\beta) = X$ $F^3(\beta') = Y$ $A = XY(X + Y + 3) - 1$.

D'après (13) et (14) $((2Y - 1)(Y + 1)^2) = (27(1 - j))$.

Le pgcd de A et $X - Y$ divise donc $27(1 - j)$.

D'après le lemme 1 , A divise $(X - Y)^2$ et le quotient est premier avec $1 - j$. A est donc une unité en dehors des places divisant $1 - j$.

Soit ν une place de $k(\mathfrak{U})$ divisant $1 - j$. Puisque $1 - j$ ne se ramifie pas dans $k(\mathfrak{U})/k$, on a $\nu(1 - j) = 1$. D'après ce qui précède , $\nu(A) = 2\nu(X - Y)$, donc $\nu(A) \neq (27(1 - j))$ car $\nu(27(1 - j)) = 7$ est impair .

On en déduit :

$$\nu((X - Y)(Y(X - Y) + 3Y(Y + 1)) \leq 7$$

soit :

$$\nu(X - Y) + \nu(Y(X - Y) + 3Y(Y + 1)) \leq 7$$

Or $X - Y = F^3(\beta) + 4 - (F^3(\beta') + 4)$ est divisible par $(1 - j)^3$, d'après le calcul de $y^2(\beta)$ et $y^2(\beta')$.

D'où $\nu(X - Y) \geq 3$ puis :

$$\nu(Y(X - Y) + 3Y(Y + 1)) \leq 4$$

Or $\nu(3(Y + 1)) = 4$ d'après (14)

soit : $\nu(X - Y) \leq 3$.

Conclusion : $\nu(X - Y) = 3$ $\nu(A) = 6$ et $(A) = (27)$.

Soit u un idèle unité de $\mathbb{Q}[j]$ dont la classe modulo $\langle -j \rangle U_{\mathfrak{U}}$ est non triviale . On a :

$$\left(\frac{F^3(\beta) - F^3(u\beta)}{3(1 - j)}\right)^2 \sim \prod_{i=0}^{5} F(((-j)^i u - 1)\beta)$$

d'où :

$$(d_2^6) = \left(\mathop{N}_{\substack{u \in U / \langle -j \rangle U_{\mathfrak{U}} \\ u \neq 1}} \prod_{i=0}^{5} N_{k(\mathfrak{U})/k}(F^3(((-j)^i u - 1)\beta)) \right)$$

On remarque que d_2 ne fait intervenir que les places de k divisant $\mathfrak{U}$. D'après les résultats du paragraphe 2 (prop. 2 , cor. 3) on a le tableau suivant décrivant l'idéal :

$$A_{u,o} = (N_{k(\mathfrak{A})/k}(F^3((u-1)\beta)))$$

Si $\mathfrak{A} = \prod \mathfrak{p}^{r_\mathfrak{p}}$ et $n_{\mathfrak{p},s} = [k(\mathfrak{A}) : k(\mathfrak{p}^s)]$ $\quad 0 < s \leq r_\mathfrak{p}$

Annulateur $((u-1)\beta)$	$\mathfrak{p}^s$ $\mathfrak{p} \neq 2$ $0 < s \leq r_\mathfrak{p}$	2^s $1 < s \leq r_2$	2	autres cas
$A_{u,o}$	$\mathfrak{p}^{r_\mathfrak{p}, s}$	$2^{n_{2,s}}$	$2^{2n_{2,1}}$	(1)

(18)

Posons maintenant :

$$A_{u,i} = (N_{k(\mathfrak{A})/k}(F^3(((-j)^i u - 1)\beta)))$$

et $A_u = \prod_{i=0}^{5} A_{u,i}$.

Fixons un idéal premier $\mathfrak{p}$ divisant $\mathfrak{A}$, et posons :

$$\mathfrak{A} = \mathfrak{p}^{r_\mathfrak{p}} \mathfrak{A}' \qquad (\mathfrak{A}', \mathfrak{p}) = 1 .$$

D'après (18) , un élément u de $U/\langle -j \rangle U_\mathfrak{A}$ donne une contribution A_u divisible par $\mathfrak{p}$, si le conducteur du caractère associé est divisible par $\mathfrak{A}'$.

Il y a exactement $[k(\mathfrak{A}) : k(\mathfrak{p}^{r-s}\mathfrak{A}')] - [k(\mathfrak{A}) : k(\mathfrak{p}^{r-s+1}\mathfrak{A}')]$ caractères de conducteur exactement égal à $\mathfrak{p}^{r-s}\mathfrak{A}'$.

Soit χ un tel caractère , on lui associe un idèle u tel que :

$u \equiv 1 \mod^* \mathfrak{p}^{r-s}\mathfrak{A}'$.

On peut déterminer alors la contribution de $\mathfrak{p}$ en A_u .

$\mathfrak{A}$	$\mathfrak{p}^r$, $\mathfrak{p} \neq 2$	$2\mathfrak{p}^r$, $\mathfrak{p} \neq 2$	2^r $r > 1$ $\mathfrak{p} = 2$	$\mathfrak{p}^r \mathfrak{A}'$ $(\mathfrak{A}', 2) = 1$
$\nu_{\mathfrak{p}}(A_{u,3})$	1	3	4	1
$\nu_{\mathfrak{p}}(A_{u,i})$ $i \neq 0, 3$	1	0	1	1
$\nu_{\mathfrak{p}}(A_u)$	$n_{\mathfrak{p},s} + 5$	$n_{\mathfrak{p},s} + 3$	$s=1 : 2n_{2,1}+8$ $s>1 : n_{2,s}+8$	$n_{\mathfrak{p},s}$

La valuation de d_2 en $\mathfrak{p}$ est alors , si $q = N_{k/\mathbb{Q}}(\mathfrak{p})$:

- $\mathfrak{A} = \mathfrak{p}^r$ $\mathfrak{p} \neq 2$:

$$\nu_{\mathfrak{p}}(d_2) = \frac{1}{6} \sum_{s=1}^{r} (n_{\mathfrak{p},s} + 5)\left([k(\mathfrak{p}^r) : k(\mathfrak{p}^{r-s})] - [k(\mathfrak{p}^r) : k(\mathfrak{p}^{r-s+1})] \right)$$

$$= \frac{1}{6}\left(\sum_{s=1}^{r-1} (q^{r-s} + 5)(q^s - q^{s-1}) + 6\left(\frac{q^r - q^{r-1}}{6} - q^{r-1} \right) \right)$$

$$= \frac{1}{6} (r\,q^r - (r-1)\,q^{r-1} - 5)$$

- $\mathfrak{A} = 2\mathfrak{p}^r$ $\mathfrak{p} \neq 2$:

$$\nu_{\mathfrak{p}}(d_2) = \frac{1}{6} \sum_{s=1}^{r} (n_{\mathfrak{p},s} + 3)\left([k(2\mathfrak{p}^r) : k(2\mathfrak{p}^{r-s})] - [k(2\mathfrak{p}^r) : k(2\mathfrak{p}^{r-s+1})] \right)$$

$$= \frac{1}{6}\left(\sum_{s=1}^{r-1} (3q^{r-s} + 3)(q^s - q^{s-1}) + 6\left(\frac{q^r - q^{r-1}}{2} - q^{r-1} \right) \right)$$

$$= \frac{1}{2} (r\,q^r - (r+1)\,q^{r-1} - 1)$$

De même si $\mathfrak{A} = 2^r$ $r > 1$ $\mathfrak{p} = 2$:

$$\nu_2(d_2) = \frac{1}{6}(r\,4^r - (r+1)\,4^{r-1} - 8)$$

et si $\mathfrak{A} = \mathfrak{p}^r\,\mathfrak{A}'$ $(\mathfrak{A}', 2\mathfrak{p}) = 1$ $\mathfrak{A}' \neq (1)$:

$$\nu_{\mathfrak{p}}(d_2) = \frac{1}{6}(r\,q^r - (r+1)\,q^{r-1})\,[k(\mathfrak{A}') : k]$$

d'où $(d_1) = (d_2)$ dans tous les cas , ce qui achève la démonstration du théorème principal .

Générateurs des anneaux d'entiers des corps de classes de rayon de Q[j], non ramifiés en 3, de dimension ≤ 10

module $(2-j)$: $-1+X$

module et conducteur $(3-j)$: $-1-jX+X^2$

module et conducteur 4 : $(2+2j)-(4+2j)X+X^2$

module et conducteur $(4-2j)$: $(3+2j)-7X+(1-4j)X^2+X^3$

module et conducteur $(3-2j)$: $(-1-j)+(4+j)X+(-3+j)X^2+X^3$

module et conducteur 5 : $-j+(3+6j)X-(7+7j)X^2+(2+j)X^3+X^4$

module et conducteur $(5-j)$: $(1+j)-3X-(4+9j)X^2+(15+11j)X^3-(9+2j)X^4+X^5$

module et conducteur $(4-3j)$:
$j-(1+7j)X+(12+22j)X^2-(31+25j)X^3+(25+4j)X^4+(-6+4j)X^5+X^6$

module et conducteur 7 :
$1+(-5+5j)X-19jX^2+(4+8j)X^3+(17+17j)X^4-(16+8j)X^5+X^6$

module et conducteur $(6-j)$:
$j-6jX+(4+25j)X^2-(32+60j)X^3+(62+60j)X^4-(39+18j)X^5+(5-j)X^6+X^7$

module et conducteur $(5-3j)$:
$(-1-j)+(3+j)X+(13+9j)X^2-(52+8j)X^3+(56-21j)X^4+(-21+28j)X^5+$
$(1-9j)X^6+X^7$

module et conducteur 8 :
$(2+2j)-(16+8j)X+40X^2+(-40+40j)X^3-90jX^4+(52+104j)X^5-(56+56j)X^6+$
$(16+8j)X^7+X^8$

module et conducteur $(5-4j)$:
$(-1-j)+(13+3j)X+(-45+21j)X^2+(67-116j)X^3+(-37+276j)X^4-(89+437j)X^5$
$+(259+429j)X^6-(250+195j)X^7+(92+11j)X^8+(-10+10j)X^9+X^{10}$

Remarque :

Les polynômes correspondant aux conducteurs 6 - j et 5 - 3j apportent une réponse positive pour les extensions cycliques de degré 7 de $\mathbb{Q}[j]$ citées dans le théorème 1 de [Cou 1].

Bibliographie.-

[Cou1] J. Cougnard :
Conditions nécessaires de monogénéité. J. London Math. Soc. (2) 37 (1988) 79-87.

[Cou2] J. Cougnard :
Générateurs de l'anneau des entiers des corps de classes de $\mathbb{Q}[i]$ de rayon impair et points de division de $Y^2 = X^3 - X$. A paraître dans J. of Number Theory .

[C.-N., T] Ph. Cassou-Noguès , M. Taylor :
- Elliptic functions and rings of integers, Birkhäuser , Progree in Mathematics , 66 , 1987 .
- A note on Elliptic Curves and the monogeneity of rings of integers . Proc. L.M.S. à paraître .

[Fl] V. Fleckinger :
- Fonctions elliptiques et génération d'anneaux d'entiers. Thèse , Bordeaux I , 1987 .
- Monogénéité de l'anneau des entiers de certains corps de classes de rayon . A paraître dans Ann. Sci. Inst. Fourier Grenoble (1988) .

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

Vincent FLECKINGER
Laboratoire de Mathématiques
U.A.CNRS 741
Faculté des Sciences
F- 25030 Besançon Cedex