JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

J. BOXALL
E. BAVENCOFFE

Quelques propriétés arithmétiques des points de 3-division de la jacobienne de $y^2 = x^5 - 1$

Journal de Théorie des Nombres de Bordeaux, tome 4, n° 1 (1992), p. 113-128

<http://www.numdam.org/item?id=JTNB_1992__4_1_113_0>

Séminaire de Théorie des Nombres,
Bordeaux 4 (1992), 113-128

Quelques propriétés arithmétiques des points de 3-division de la jacobienne de $y^2 = x^5 - 1$.

par J. BOXALL ET E. BAVENCOFFE

RÉSUMÉ – Soit C la courbe projective lisse et irréductible, définie sur $\mathbf{Q}$, et dont un modèle affine est donné par $y^2 = x^5 - 1$. On désigne par ∞ l'unique point de C qui n'est pas contenu dans cette partie affine. Soit J la jacobienne de C et soit $\phi : C^2 \longrightarrow J$ le morphisme associant à chaque couple (ξ, η) de points de C la classe du diviseur $[\xi] + [\eta] - 2[\infty]$ dans $\mathrm{Pic}_0 C$. Soient u, v, f les trois fonctions rationnelles sur J définies par

$$u \circ \phi(\xi, \eta) = x(\xi) + x(\eta),$$
$$v \circ \phi(\xi, \eta) = x(\xi)x(\eta),$$
$$f = -u + v + 1.$$

Le but de cet article est de montrer que pour tout point P de 3-division non nul de J, $u(P)$ et $v(P)$ sont des entiers algébriques et $f(P)/\sqrt{5}$ est une unité. Nous expliciterons le corps engendré par ces valeurs ainsi que le polynôme minimal des $f(P)$.

1. Généralités.

Posons $C_1 = \mathrm{spec}\ \mathbf{Q}[x, y]/(y^2 - x^5 + 1)$, $C_2 = \mathrm{spec}\ \mathbf{Q}[X, Y]/(Y^2 - X + X^6)$. En identifiant X avec $1/x$ et Y avec y/x^3, on obtient une courbe C, projective, lisse, irréductible et définie sur $\mathbf{Q}$, qui est la réunion de C_1 et de C_2. Soit ∞ le point de C qui correspond à l'origine de la partie affine C_2; alors $C(F) = C_1(F) \cup \{\infty\}$ pour toute extension finie F de $\mathbf{Q}$. On désigne par J la jacobienne de C et par ϕ le morphisme de C^2 dans J qui associe à tout point (ξ, η) de C^2 la classe du diviseur $[\xi] + [\eta] - 2[\infty]$ de $\mathrm{Pic}_0 C$. Alors ϕ est de degré 2 et induit une équivalence birationnelle entre le carré symétrique $C^{(2)}$ de C et J. Soit ι l'involution de C définie par $\iota(x, y) = (x, -y)$ et soit E l'image dans $C^{(2)}$ de l'ensemble des points de C^2 de la forme $(\xi, \iota(\xi))$ avec ξ dans C. D'après le théorème d'Abel-Jacobi, ϕ induit un isomorphisme de $C^{(2)} \setminus E$ sur $J \setminus (0)$, et $\phi(E) = 0$; autrement dit $C^{(2)}$ est l'éclatement de J à l'origine et le diviseur exceptionnel est E. Pour tout point P non nul de J désignons par ξ_P, η_P les deux points de

Manuscrit reçu le 10 avril 1992.

C tels que $\phi(\xi_P, \eta_P) = P$. Remarquons que la variété abelienne J est à multiplications complexes par l'anneau des entiers du corps $\mathbf{Q}(\zeta)$, où la racine cinquième primitive de l'unité ζ opère sur C par $[\zeta](x, y) = (\zeta x, y)$.

Définissons trois fonctions u, v et f, rationnelles sur J, par

$$\begin{aligned} u(P) &= x(\xi_P) + x(\eta_P), \\ v(P) &= x(\xi_P)x(\eta_P), \\ f(P) &= -u(P) + v(P) + 1 \\ &= \big(x(\xi_P) - 1\big)\big(x(\eta_P) - 1\big). \end{aligned}$$

Soit J_3 l'ensemble des points de 3–division de J différents de l'origine; nous nous intéressons aux propriétés arithmétiques des valeurs de u, v et f en ces points. Ces trois fonctions étant paires, il y a quarante valeurs de chacune; puisque $u(\zeta.P) = \zeta u(P)$ et $v(\zeta.P) = \zeta^2 v(P)$ il y a huit valeurs de $u(P)^5$ et de $v(P)^5$. Dans le §2 nous montrerons que ces nombres sont des entiers algébriques appartenant au sous-corps maximal réel du corps des racines quinzièmes de l'unité; le but des §3 et 4 est d'étudier les valeurs de f et de calculer explicitement le polynôme dont elles sont les racines.

Remarque 1. Les calculs des §3 et 4 ont été faits par le deuxième auteur *avant* que les calculs décrits au §2 n'aient été faits par le premier. Les coefficients du polynôme satisfait par les $f(P)$ étaient ainsi conjecturales (i.e. ils n'étaient que des entiers à 10^{-10} près). En effet, les $f(P)$ ont été calculés en utilisant les formules de Thomaë exprimant f à l'aide de la fonction thêta de Riemann asociée à la matrice des périodes de C, considérée comme surface de Riemann et les coefficients obtenus comme fonctions symétriques de ces valeurs. Le but principal du calcul du §2 est de *démontrer* que les $f(P)$ sont bien des entiers algébriques et de justifier ainsi les valeurs des coefficients suggérées par les calculs effectués auparavant.

Remarque 2. Les fonctions u et v sont les analogues de la fonction $\wp$ de Weierstrass associée à une courbe elliptique $y^2 = x^3 + ax + b$ et la fonction f est un analogue des fonctions $\wp - e_r$, les e_r étant les racines de $x^3 + ax + b = 0$. J étant à multiplication complexe, on peut se demander si la théorie des courbes elliptiques à multiplication complexe peut être étendue à J. La théorie des corps de classes a été traitée par Shimura, Tanayama et Weil ([Sh-Ta], [We]) mais la théorie arithmétique (unités de Ramachandra et de Robert, structure de module galoisien, calcul explicite des anneaux des entiers ...) reste très peu développée. Le seul travail dans cette direction que nous connaissons est celui de Grant [G2], où des S-unités

(avec un ensemble fini explicite de nombres premiers S) sont construites à partir de points d'ordre *infini* de J.

Les calculs décrits au §2 ont été faits en utilisant le système PARI (version 1.35.04) par le premier auteur alors que les autres calculs, et notamment celui des valeurs de la fonction f à partir des fonctions thêta de deux variables, ont été faits en UBASIC par le deuxième auteur.

2. Les valeurs de u.

Soit $P \in J_3$ et soit ξ_P et η_P les deux points de C tels que $\phi(\xi_P, \eta_P) = P$. Il existe donc une fonction ψ, rationnelle sur C, de diviseur $3\big([\xi_P] + [\eta_P] - 2[\infty]\big)$, alors que $[\xi_P] + [\eta_P] - 2[\infty]$ n'est pas principal. Par conséquent ψ a un unique pôle situé au point ∞ et d'ordre 6; quitte à le multiplier par une constante on peut écrire

$$\psi = x^3 + ax^2 + bx + c + \alpha y,$$

où a, b, c et $\alpha \in \overline{\mathbf{Q}}$ dépendent de P. La fonction

$$\psi\,\psi\circ\iota = (x^3 + ax^2 + bx + c)^2 - \alpha^2(x^5 - 1)$$

a comme diviseur $3\big([\xi_P] + [\iota(\xi_P)]\big) + 3\big([\eta_P] + [\iota(\eta_P)]\big) - 12[\infty]$, d'où

$$\begin{aligned}\psi\,\psi\circ\iota &= \big(x - x(\xi_P)\big)^3\big(x - x(\eta_P)\big)^3 \\ &= (x^2 - ux + v)^3,\end{aligned}$$

où l'on a écrit $u = u(P)$ et $v = v(P)$ pour abréger. La comparaison des coefficients de x^5, x^4, ..., 1 fournit six équations entre les six inconnues a, b, c, α, u et v :

$$\begin{aligned}\alpha^2 &= 2a + 3u, \\ 0 &= a^2 + 2b - 3u^2 - 3v, \\ 0 &= 2ab + 2c + 6uv + u^3, \\ 0 &= b^2 + 2ac - 3u^2v - 3v^2, \\ 0 &= 2bc + 3uv^2, \\ -\alpha^2 &= c^2 - v^3.\end{aligned}$$

Si $\alpha = 0$, alors $x^3 + ax^2 + bx + c = (x - \beta)^3$, où $\beta = x(\xi_P) = x(\eta_P)$ et ψ est donc le cube d'une fonction sur C en contradiction avec l'hypothèse que $P \neq 0$.

Ecrivons $s = \alpha^2$ afin de simplifier la notation et posons $v = t + \frac{1}{4}u^2$. Substituons les valeurs de a, b et c obtenues en fonction de s, t et u à partir des trois premières équations dans les trois dernières :

$$(2,1)\quad -\tfrac{3}{4}t^2 + \tfrac{3}{8}(-3s^2 + 10us)t + \tfrac{1}{64}(5s^4 - 60us^3 + 180u^2s^2 - 80u^3s) = 0,$$

$$(2,2)\quad \tfrac{3}{4}(-3s + u)t^2 + \tfrac{3}{8}(s^3 - 7us^2)t + \tfrac{1}{64}(-s^5 + 15us^4 - 60u^2s^3 + 20u^3s^2 + 60u^4s) = 0,$$

$$(2,3)\quad -t^3 + \tfrac{3}{16}(3s^2 + 6us - u^2)t^2 - \tfrac{3}{32}(s^4 - 8us^3 + 3u^2s^2 + 10u^3s)t + \tfrac{1}{256}(s^6 - 18us^5 + 105u^2s^4 - 220u^3s^3 + 180u^4s^2 - 48u^5s) = -s.$$

En multipliant (2,1) par $-3s + u$ et en le rajoutant à (2,2), on obtient, après multiplication par le dénominateur commun :

$$(2,4)\quad 60(s^2 - 4us + u^2)t + (-4s^4 + 50us^3 - 165u^2s^2 + 110u^3s - 5u^4) = 0.$$

De même, en multipliant (2,1) par $\frac{4}{3}t$ et en soustrayant (2,3) on obtient

$$(2,5)\quad 48(-33s^2 + 62us + 3u^2)t^2 + 8(19s^4 - 192us^3 + 387u^2s^2 - 70u^3s) + 3(-s^6 + 18us^5 - 105u^2s^4 + 220u^3s^3 - 180u^4s^2 + 48u^5s) = 768s.$$

Substituons la valeur de t en fonction de u et s obtenue à partir de (2,4) dans (2,1). On obtient l'équation $u^8F(s/u) = 0$, où

$$(2,6)\quad F(X) = X^8 - 40X^7 + 580X^6 - 3880X^5 + 11790X^4 - 11000X^3 - 8300X^2 + 3400X + 25.$$

Les équations (2,1), (2,2) et (2,3) montrent que si $u = 0$, alors $s = t = 0$, ce qui est impossible. On en tire que $F(s/u) = 0$. Or, F est le produit des deux polynômes F_1 et F_2 donnés par

$$(2,7)\quad F_1(X) = X^4 - 10X^3 + 20X^2 + 10X - 5,$$

$$(2,8)\quad \text{et}\quad F_2(X) = X^4 - 30X^3 + 260X^2 - 690X - 5.$$

On voit facilement que F_1 et F_2 se décomposent en facteurs de degré deux sur $\mathbf{Q}(\sqrt{5})$ et que le corps de rupture de F_1 et de F_2 est le corps $\mathbf{K} = \mathbf{Q}(\sqrt{5}, \theta)$, où

$$\theta^2 = 3\sqrt{5}\left(\frac{1+\sqrt{5}}{2}\right).$$

En outre, **K** est une extension galoisienne de **Q** dont le groupe de Galois est cyclique d'ordre 4.

Le discriminant de F_1 (resp F_2) est $2^{12}3^25^3$ (resp $2^{12}3^25^359^2$). Pour toute racine β de F, $(\beta+1)/2$ est un entier algébrique, et on conclut que le discriminant de **K** n'est divisible que par 3 et 5; **K** étant modérément ramifié et totalement réel, le théorème de Kronecker et Weber montre qu'il n'y a qu'une seule possibilité : **K** est le sous-corps réel maximal du corps des racines quinzièmes de l'unité.

En substituant la valeur de t de (2,4) dans (2,5), on trouve qu'à chaque racine β de F il correspond 5 valeurs de u satisfaisant à

$$u^5 = \frac{2^8 3^2 5^2 \beta(\beta^2 - 4\beta + 1)^2}{H(\beta)}, \tag{2,9}$$

H étant le polynôme de degré 10 donné par

$$H(X) = 7X^{10} - 178X^9 + 1423X^8 - 120X^7 - 58690X^6 + 325940X^5 - 670330X^4 + 406600X^3 - 44325X^2 + 5550X + 75.$$

Notre premier but est de démontrer la proposition suivante :

PROPOSITION 1. *Les valeurs des $u(P)$, $v(P)$ et $f(P)$, P étant un point de trois-division non nul de J, sont des entiers algébriques.*

Démonstration. Montrons d'abord que les $u(P)$ sont des entiers algébriques. On considère séparément les deux cas $F_1(\beta) = 0$ et $F_2(\beta) = 0$ dans (2,9).

a) Si $F_1(\beta) = 0$, alors (2,9) se simplifie en

$$u^5 = \frac{3^2\beta(\beta^2 - 4\beta + 1)^2}{(6\beta^3 - 46\beta^2 + 32\beta - 5)}.$$

Désignons par $N\alpha$ la norme d'un élément α de **K**. On a alors $N\beta = -5$, $N(\beta^2 - 4\beta + 1) = 4$ et $N(\beta^3 - 46\beta^2 + 32\beta - 5) = 3^25$; 2 étant inerte dans **K**, 3 étant ramifié dans $\mathbf{K}/\mathbf{Q}(\sqrt{5})$ et 5 étant ramifié dans **K**/**Q** on conclut que u est un entier algébrique avec $N(u^5) = -2^83^6$.

b) Si $F_2(\beta) = 0$, (2,9) devient $u^5 = 2.3^2\beta(\beta^2 - 4\beta + 1)^2/\gamma$, où $\gamma = 346127\beta^3 - 4415427\beta^2 + 13856189\beta + 100365$. Cette fois $N\beta = -5$, $N(\beta^2 - 4\beta + 1) = 2^459^2$ et $N\gamma = 2^43^25.59^4$. On vérifie que la trace et la norme

de u^5 sur $\mathbf{Q}(\sqrt{5})$ sont des entiers de ce corps et donc que u^5 est un entier algébrique (avec encore $N(u^5) = -2^8 3^6$).

Montrons enfin que les $v(P)$ et les $f(P)$ sont des entiers algébriques. Puisque $v = t + \frac{1}{4}u^2$ et $\beta = s/u$ on trouve, grâce à (2,4) :

$$v = \frac{(2\beta^4 - 25\beta^3 + 90\beta^2 - 85\beta + 10)}{30(\beta^2 - 4\beta + 1)}u^2. \tag{2,10}$$

En considérant séparément les cas selon que $F_1(\beta) = 0$ ou $F_2(\beta) = 0$, on conclut que v est bien un entier algébrique (et dans les deux cas on a $N(v^5) = -2^{16}3^2$). Comme $f = -u + v + 1$, on conlut que f est également un entier algébrique.

3. Calcul des fonctions thêta.

Soit $g \geq 1$ un entier et soit X une courbe propre et lisse de genre g sur $\mathbf{C}$. Si $\sigma = {}^t(\sigma_1, \sigma_2, \ldots \sigma_g)$ (où ${}^tA$ désigne le transposé de la matrice ou du vecteur A), avec $\sigma_1, \sigma_2, \ldots, \sigma_g$ une base de $\Omega^1_{X/\mathbf{C}}$, alors

$$\Lambda = \left\{ \int_\gamma \sigma \mid \gamma \in \mathrm{H}_1(X, \mathbf{Z}) \right\}$$

est un réseau dans $\mathbf{C}^g$; c'est-à-dire un sous-groupe discret de rang $2g$ de $\mathbf{C}^g$. Si en plus $A_1, A_2, \ldots, A_g, B_1, \ldots B_g$ est une base symplectique de $\mathrm{H}_1(X, \mathbf{Z})$ (i. e. $A_i.A_j = B_i.B_j = 0$ et $A_i.B_j = \delta_{ij}$, le symbole de Kronecker, pour tout i, j) et si Ω (resp Ω') est la matrice des périodes

$$\Omega_{ij} = \int_{A_j} \sigma_i \quad (\text{resp } \Omega'_{ij} = \int_{B_j} \sigma_i)$$

alors Ω est inversible, la matrice $T = \Omega^{-1}\Omega'$ est symétrique et sa partie imaginaire est définie positive.

Cherchons une matrice T associée à la courbe de genre 2 C du §1.

Posons $\zeta = \exp(\frac{2\pi i}{5})$.

PROPOSITION 2. *Soit C, la courbe définie au §1. Il existe un choix de σ, A_1, A_2, B_1 et B_2* (qui sera précisé pendant la démonstration) *pour lequel*

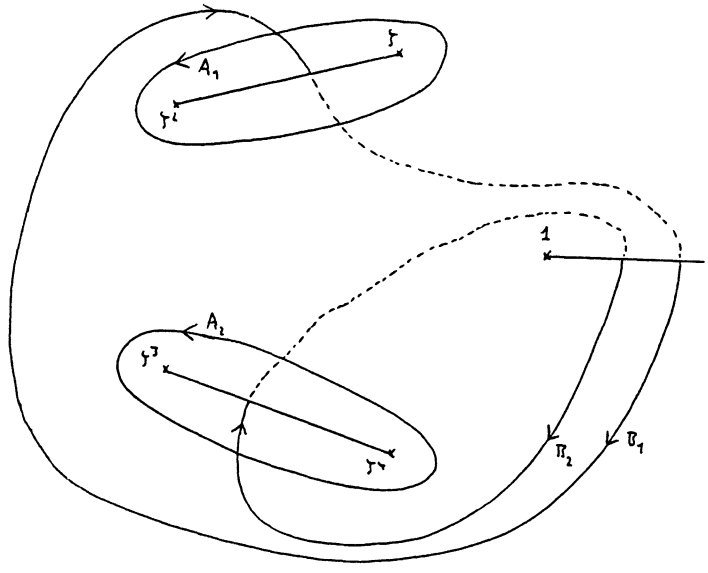
$$T = \begin{pmatrix} -1+\zeta & \zeta+\zeta^3 \\ \zeta+\zeta^3 & -\zeta^4 \end{pmatrix}. \tag{3,1}$$

Si en outre

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},\ e_1' = \begin{pmatrix} -1+\zeta \\ \zeta+\zeta^3 \end{pmatrix},\ e_2' = \begin{pmatrix} \zeta+\zeta^3 \\ -\zeta^4 \end{pmatrix},$$

est la base standard du réseau $\mathbf{Z}^2 + T.\mathbf{Z}^2$, *alors l'opération de* ζ *sur* e_1, e_2, e_1' *et* e_2' *est donnée par* $[\zeta]e_1 = e_1' - e_2'$, $[\zeta]e_2 = e_2'$, $[\zeta]e_1' = -(e_1 + e_1')$ *et* $[\zeta]e_2' = -(e_1 + e_2 + e_1')$.

Remarque. Une matrice de périodes différente a été obtenue par Bost, Mestre et Moret-Bailly [BMMB].



Démonstration. On fixe une racine carrée holomorphe y de $x^5 - 1$ dans $\mathbf{C}$ dépourvu des segments joignant ζ à ζ^2 et ζ^3 à ζ^4 et de l'intervalle réel $[1, \infty[$. La surface de Riemann de C peut être representée par deux copies du plan complexe avec ses segments identifiés. Un choix possible de la base A_1, A_2, B_1 et B_2 est celui indiqué dans la figure; en outre dx/y et $x\,dx/y$ forment une base de $\Omega^1_{C/\mathbf{C}}$. En remplaçant x par ζx, on voit que $\int_{A_2}(dx/y) = \zeta \int_{A_1}(dx/y)$, et on trouve de la même manière en écrivant $\Omega = \begin{pmatrix} \Omega_{11} & \Omega_{12} \\ \Omega_{21} & \Omega_{22} \end{pmatrix}$ et $\Omega' = \begin{pmatrix} \Omega'_{11} & \Omega'_{12} \\ \Omega'_{21} & \Omega'_{22} \end{pmatrix}$:

$$\Omega_{11} = \int_{A_1} \frac{dx}{y} \qquad \Omega_{12} = \int_{A_2} \frac{dx}{y} = \zeta^2\Omega_{11}$$

$$\Omega_{21} = \int_{A_1} \frac{x\,dx}{y} \qquad \Omega_{22} = \int_{A_2} \frac{x\,dx}{y} = \zeta^4\Omega_{21}$$

$$\Omega'_{11} = \int_{B_1} \frac{dx}{y} = -(\zeta + \zeta^3)\Omega_{11} \qquad \Omega'_{12} = \int_{B_2} \frac{dx}{y} = -\zeta^3\Omega_{11}$$

$$\Omega'_{21} = \int_{B_1} \frac{x\,dx}{y} = -(\zeta^2 + \zeta)\Omega_{21} \qquad \Omega'_{22} = \int_{B_2} \frac{x\,dx}{y} = -\zeta\Omega_{21}.$$

Il s'ensuit que

$$\Omega = \begin{pmatrix} \Omega_{11} & \zeta^2\Omega_{11} \\ \Omega_{21} & \zeta^4\Omega_{21} \end{pmatrix} \text{ et } \Omega' = \begin{pmatrix} -(\zeta + \zeta^3)\Omega_{11} & -\zeta^3\Omega_{11} \\ -(\zeta^2 + \zeta)\Omega_{21} & -\zeta\Omega_{21} \end{pmatrix}$$

d'où $T = \Omega^{-1}\Omega' = \begin{pmatrix} -1+\zeta & \zeta+\zeta^3 \\ \zeta+\zeta^3 & -\zeta^4 \end{pmatrix}$.

Soit A la matrice carrée d'ordre 2 donnant l'action de ζ sur $\mathbf{C}^2/(\mathbf{Z}^2 + T.\mathbf{Z}^2)$. Puisque $[\zeta]^*(dx/y) = \zeta(dx/y)$ et $[\zeta]^*(x\,dx/y) = \zeta^2(x\,dx/y)$ on trouve A à partir du diagramme commutatif

$$\begin{array}{ccc} \mathbf{C}^2/(\Omega.\mathbf{Z}^2 + \Omega'.\mathbf{Z}^2) & \xrightarrow{\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}} & \mathbf{C}^2/(\Omega.\mathbf{Z}^2 + \Omega'.\mathbf{Z}^2) \\ \Omega\uparrow & & \uparrow\Omega \\ \mathbf{C}^2/(\mathbf{Z}^2 + T.\mathbf{Z}^2) & \xrightarrow[A]{} & \mathbf{C}^2/(\mathbf{Z}^2 + T.\mathbf{Z}^2) \end{array}$$

On a donc $A = \Omega^{-1}\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}\Omega = \begin{pmatrix} -(1+\zeta^3) & \zeta+\zeta^3 \\ -(1+\zeta^4) & -\zeta^4 \end{pmatrix}$ ce qui donne $[\zeta]e_1 = Ae_1 = e'_1 - e'_2$, etc.

Soit $z : J(\mathbf{C}) \longrightarrow \mathbf{C}^2/(\mathbf{Z}^2 + T.\mathbf{Z}^2)$ l'application définie par

$$z(P) = \int_\infty^{\xi_P} \sigma' + \int_\infty^{\eta_P} \sigma',$$

σ' étant la base de $\Omega^1_{C/\mathbf{C}}$ dont le réseau des périodes est égal à $\mathbf{Z}^2 + T.\mathbf{Z}^2$. Soit $\theta_{a,b}$ la fonction thêta de Riemann avec caractéristiques $a,\ b \in \mathbf{R}^2$ définie par

$$\theta_{a,b}(z) = \theta_{a,b}(z,T) = \sum_{n\in\mathbf{Z}^2} e^{\pi i\,{}^t(n+a)T(n+a)+2\pi i\,{}^t(n+a)(z+b)}.$$

La formule qui suit est un cas spécial d'une formule de Riemann et Thomaë. On trouvera des exposés modernes dans [M] et [F]. (Voir aussi [G1]). Rappelons que C est plongée dans J par $\xi \mapsto$ la classe de $[\xi]-[\infty]$ dans $\mathrm{Pic}_0 C$.

THÉORÈME 1. *Pour tout $P \notin C$ on a la formule suivante*

$$f(P) = \sqrt{5}\left(\frac{\theta_{a,b}(z(P))}{\theta_{a,c}(z(P))}\right)^2, \tag{3,2}$$

où $a = \frac{1}{2}\binom{1}{1}$, $b = \frac{1}{2}\binom{3}{2}$ *et* $c = \frac{1}{2}\binom{2}{1}$.

Remarque. L'équation (3,2) est une conséquence, à multiplication par une racine quatrième de l'unité ε près, du théorème 7.6 de [M] et de la proposition 3.6 de [F]. Nous n'avons pas trouvé de discussion de la valeur exacte de ε dans la littérature. Nous avons obtenu la valeur $\varepsilon = 1$ en comparant les valeurs des deux côtés de (3,2) aux points de deux-division de J : f est définie et différente de 0 et ∞ aux dix points de deux-division représentés par les diviseurs de la forme $[\zeta^r]+[\zeta^s]-2[\infty]$ avec $0 \leq r < s \leq 4$.

La série définissant $\theta_{a,b}$ converge très rapidement et permet un calcul relativement aisé des valeurs de f à 10^{-40} près et ces valeurs (avec $P \in J_3$) sont données dans la table 1. Les valeurs propres de la partie imaginaire de T étant $\frac{1}{4}\sqrt{10-2\sqrt{5}} = 0,58778\ldots$ et $\frac{1}{4}\sqrt{5}\sqrt{10-2\sqrt{5}} = 1,31439\ldots$, il suffit de prendre les termes où $n = (n_1, n_2)$ avec $|n_1| \leq 9$ et $|n_2| \leq 9$.

4. Le polynôme p.

Rappelons (§1) que p est le polynôme de degré 40 défini par

$$p(T) = \prod_{P \in J_3/\pm 1} (T - f(P)).$$

Les $f(P)$ étant des entiers algébriques (§2), on en déduit que $p(T) \in \mathbf{Z}[T]$, ses coefficients sont calculés comme des fonctions symétriques des $f(P)$.

Reprenons les notations du §2. On désigne par β_r, $1 \leq r \leq 8$ les racines du polynôme F (2,6). Pour chaque $r \in \{1,2,\ldots,8\}$, soit $P_{r,0}$ l'élément de J_3 tel que $u(P_{r,0})$ soit réel et satisfasse à (2,9) avec $\beta = \beta_r$; $P_{r,0}$ est alors unique modulo ± 1. D'après (2,10), $v(P_{r,0})$ et donc $f(P_{r,0})$ sont également réels. Pour tout $k \in \{0,1,2,3,4\}$, désignons par $P_{r,k}$ l'un des deux représentants de $[\zeta^k](P_{r,0})$ modulo ± 1, les points $\{P_{r,k} \mid 1 \leq r \leq$

$8,\ 0 \leq k \leq 4\}$ forment alors un système complet de représentants de $J_3/\pm 1$ et la table 2 donne les valeurs des $f(P_{r,k})$. Puisque

$$f(P_{r,k}) = \zeta^k u(P_{r,0}) + \zeta^{2k} v(P_{r,0}) + 1, \tag{4,1}$$

on voit que $f(P_{r,k})$ est réel si et seulement si $k = 0$. Ecrivons :

$$p_r(T) = \prod_{k=0}^{4} (T - f(P_{r,k})); \tag{4,2}$$

les résultats du §2 montrent que $p_r(T)$ appartient à $\mathbf{K}[T]$, $\mathbf{K}$ étant le sous-corps réel maximal du corps des racines quinzièmes de l'unité.

En outre, on tire de (4,1) que les coefficients de T^4 et T^3 de $p_r(T)$ sont respectivement égaux à -5 et 10 pour tout r. La table 2 donne, pour tout $r \in \{1, 2, 3, \ldots, 8\}$, l'une des racines β_r ainsi que les coefficients du p_r qui y correspondent. Les produits $p_1p_2p_3p_4$ et $p_5p_6p_7p_8$ sont alors à coefficients rationnels (et donc entiers), et ils sont tabulés dans la table 3. (Par souci de brièveté, nous ne donnons pas les coefficients de p lui-même). On tire immédiatement de la table 3 que les nombres $f(P_{r,k})/\sqrt{5}$ sont des unités algébriques.

Il nous reste à déterminer le corps de rupture de p. Rappelons (§2) que $\mathbf{K} = \mathbf{Q}(\sqrt{5}, \theta)$ est le sous-corps réel maximal du corps des racines quinzièmes de l'unité, θ étant défini par $\theta^2 = 3\sqrt{5}(1+\sqrt{5})/2$. Le conducteur de $\mathbf{Q}(\sqrt{3})/\mathbf{Q}$ étant égal à 12, on en conclut que le sous-corps maximal réel des racines 60^e de l'unité est

$$\mathbf{Q}(\cos \pi/30) = \mathbf{Q}(\sqrt{3}, \sqrt{5}, \theta). \tag{4,3}$$

Posons donc $\mathbf{F} = \mathbf{Q}(\zeta, \sqrt{3}, \theta, (4/3)^{1/5})$, ζ étant une racine primitive cinquième de l'unité.

THÉORÈME 2. $\mathbf{F}$ *est le corps de rupture de* p *sur* $\mathbf{Q}$.

Démonstration. Pour tout $r \in \{1, 2, \ldots, 8\}$, on pose $u_r = u(P_{r,0})$ et $v_r = v(P_{r,0})$. Nous avons trouvé les valeurs suivantes des u_r et des v_r :

$$u_1 = -(12\sqrt{3})^{1/5}(-1+\sqrt{5})\cos 7\pi/30 \qquad v_1 = (16\sqrt{3})^{1/5}(-1+\sqrt{5})\cos 11\pi/30$$

$$u_2 = -(12\sqrt{3})^{1/5}(-1+\sqrt{5})\cos 17\pi/30 \qquad v_2 = (16\sqrt{3})^{1/5}(-1+\sqrt{5})\cos \pi/30$$

$$u_3 = -(12\sqrt{3})^{1/5}(1+\sqrt{5})\cos 11\pi/30 \qquad v_3 = (16\sqrt{3})^{1/5}(1+\sqrt{5})\cos 17\pi/30$$

$$u_4 = -(12\sqrt{3})^{1/5}(1+\sqrt{5})\cos \pi/30 \qquad v_4 = (16\sqrt{3})^{1/5}(1+\sqrt{5})\cos 7\pi/30$$

$$u_5 = \tfrac{1}{2}\big(3(7-3\sqrt{5}) - (5-3\sqrt{5})\theta'\big)(24)^{-1/5} \qquad v_5 = (4/3)^{1/5}u_5$$

$$u_6 = \tfrac{1}{2}\big(3(7-3\sqrt{5}) + (5-3\sqrt{5})\theta'\big)(24)^{-1/5} \qquad v_6 = (4/3)^{1/5}u_6$$

$$u_7 = \tfrac{1}{2}\big(3(7+3\sqrt{5}) + (5+3\sqrt{5})\theta\big)(24)^{-1/5} \qquad v_7 = (4/3)^{1/5}u_7$$

$$u_8 = \tfrac{1}{2}\big(3(7+3\sqrt{5}) - (5+3\sqrt{5})\theta\big)(24)^{-1/5} \qquad v_8 = (4/3)^{1/5}u_8$$

Considérons d'abord le facteur $p_5p_6p_7p_8$. Puisque u_r^5, v_r^5 et β_r appartiennent à $\mathbf{K}$, on tire de (2,10) que u_r et v_r appartiennent à $\mathbf{F}$ et il en est donc de même pour $f(P_{r,k})$ pour tout $k \in \{0,1,2,3,4\}$. En considérant les degrés des extensions on voit que le corps engendré est nécessairement $\mathbf{F}$ tout entier. Le cas du facteur $p_1p_2p_3p_4$ se traite en utilisant la table ci-dessus; comme $12\sqrt{3} = \frac{4}{3}(\sqrt{3})^5$, on conclut aisément à l'aide de (2,10) et (4,3).

Remarque. $\mathbf{F}$ étant une extension totalement imaginaire de degré 80 de $\mathbf{Q}$, le groupe multiplicatif $\mathcal{O}_F^*$ de ses unités contient un sous-groupe d'indice fini libre de rang 39. Il est alors clair que le groupe engendré par les $f(P_{r,k})/\sqrt{5}$ ne peut être d'indice fini dans $\mathcal{O}_F^*$.

TABLE 1

Les valeurs de f.

La table donne les valeurs de f aux points $P_{r,k}$ (voir §4). Les colonnes présentent : (i) le couple (r,k), (ii) les représentants dans $\mathbf{C}^2$ des points $\pm z(P_{r,k})$ [ils sont donnés sous la forme pqrs avec $0 \leq p, q, r, s, \leq 2$ où pqrs représente $\frac{1}{3}(pe'_1 + qe'_2 + re_1 + se_2)$], (iii) les valeurs de $f(P_{r,k})$.

(r,k) $pqrs$ $p'q'r's'$	$\Re f(P_{r,k})$	$\Im f(P_{r,k})$
(1,0) 1200 2100	3.662243159107971516997965318758858 54	
(1,1) 0001 0002	0.730366180430554394084811619012612 18	2.177029956576261891872651859966208 28
(1,2) 0100 0200	−0.061487759984540152583794278392041 45	0.061388504874776067808567829253531 32
(1,3) 2022 1011	−0.061487759984540152583794278392041 45	−0.061388504874776067808567829253531 32
(1,4) 0010 0020	0.730366180430554394084811619012612 18	−2.177029956576261891872651859966208 28
(2,0) 2111 1222	2.917384793989917577234251118540237 38	
(2,1) 1002 2001	−1.078335274393800516356580336605009 97	0.955732858903265262431407580111213 72
(2,2) 2220 1110	2.119642877398841727739454777334891 28	−2.549085053940723728389173499276777 32
(2,3) 1121 2212	2.119642877398841727739454777334891 28	2.549085053940723728389173499276777 32
(2,4) 0212 0121	−1.078335274393800516356580336605009 97	−0.955732858903265262431407580111213 72
(3,0) 0012 0021	2.107316860277765421629792427200906 87	
(3,1) 1100 2200	2.803978775939644527978298958697245 99	1.528088218186043496285545414860611 95
(3,2) 1012 2021	−1.357637206078527238793195172297699 43	2.662858301054558361332964467060150 26
(3,3) 0120 0210	−1.357637206078527238793195172297699 43	−2.662858301054558361332964467060150 26
(3,4) 1122 2211	2.803978775939644527978298958697245 99	−1.528088218186043496285545414860611 95
(4,0) 1120 2210	11.577800628740852678876162865311431 96	
(4,1) 0112 0221	−0.956230849950026951963472139620133 48	8.362396721897919657068342183092234 80
(4,2) 0122 0211	−2.332669464420399387474609293035582 50	−0.974052890587812512091019059328299 00
(4,3) 1022 2011	−2.332669464420399387474609293035582 50	0.974052890587812512091019059328299 00
(4,4) 1020 2010	−0.956230849950026951963472139620133 48	−8.362396721897919657068342183092234 80
(5,0) 1111 2222	1.068275872731542707349597427044629 58	
(5,1) 2012 1021	−0.344155549785859190211510217910598 64	−0.378663686596168759365489675618057 30
(5,2) 2110 1220	2.310017613420087836536711504388283 85	−1.838979309112262272983405158992758 88

(5,3) 1202 2101	2.3100176134200878365367115043882838 5	1.8389793091122622729834051589927588 8
(5,4) 0201 0102	-0.3441555497858591902115102179105986 4	0.3786636865961687593654896756180573 0
(6,0) 1102 2201	0.9591812491669712370344903072184220 5	
(6,1) 1212 2121	1.8036037954911989773157496568002246 1	0.2263841977305745294988677104252347 6
(6,2) 1101 2202	0.2168055799253154041670051895905643 6	1.0994343272754634362798179789378778 8
(6,3) 1112 2221	0.2168055799253154041670051895905643 6	-1.0994343272754634362798179789378778 8
(6,4) 2112 1221	1.8036037954911989773157496568002246 1	-0.2263841977305745294988677104252347 6
(7,0) 0011 1100	2.2498890928635457945943737223132061 5	
(7,1) 1000 2000	-23.606721138449624039566725490477318 27	-6.9319891903981136379458001899125801 5
(7,2) 2020 1010	24.981776592017851142269538629320715 19	-33.665189304848892148447038390718039 86
(7,3) 0110 0220	24.981776592017851142269538629320715 19	33.665189304848892148447038390718039 86
(7,4) 0222 0111	-23.606721138449624039566725490477318 27	6.9319891903981136379458001899125801 5
(8,0) 1211 2122	1.0400111775830721446347160911442694 5	
(8,1) 1001 2002	0.2122949989490557626081877918811296 3	-0.2219053291084566208170193086383241 6
(8,2) 2120 1210	1.7676994122594081650744541625467356 5	-1.0776827122781400635045536802320936 2
(8,3) 2102 1201	1.7676994122594081650744541625467356 5	1.0776827122781400635045536802320936 2
(8,4) 0202 0101	0.2122949989490557626081877918811296 3	0.2219053291084566208170193086383241 6

TABLE 2

Les racines de F et les coefficients des p_r.

Cette table donne, pour tout entier r avec $1 \leq r \leq 8$, une racine β_r du polynôme F défini par (2,6), ainsi que les coefficients c_r, d_r et e_r du polynôme $p_r(T) = T^5 - 5T^4 + 10T^3 + c_rT^2 + d_rT + e_r$ qui y correspond (voir §4). Les β_r avec $1 \leq r \leq 4$ sont les racines de F_2 et celles où $5 \leq r \leq 8$ sont les racines de F_1, les facteurs F_1 et F_2 de F étant définis par (2,7) et (2,8). En outre θ (resp θ') désigne la racine carrée positive de $3\sqrt{5}(1+\sqrt{5})/2$ (resp $-3\sqrt{5}(1-\sqrt{5})/2$).

$r = 1$ $\beta_1 = \big((15+\sqrt{5}) - (3+\sqrt{5})\theta\big)/2$ $c_1 = -25(7-3\sqrt{5}) - 10(5-2\sqrt{5})\theta'$

$d_1 = -25(34-15\sqrt{5}) - 25(11-5\sqrt{5})\theta'$ $e_1 = -25(55-24\sqrt{5}) - 25(15-7\sqrt{5})\theta'$

$r = 2$ $\beta_2 = \big((15+\sqrt{5}) + (3+\sqrt{5})\theta\big)/2$ $c_2 = -25(7-3\sqrt{5}) + 10(5-2\sqrt{5})\theta'$

$d_2 = -25(34-15\sqrt{5}) + 25(11-5\sqrt{5})\theta'$ $e_2 = -25(55-24\sqrt{5}) + 25(15-7\sqrt{5})\theta'$

$r = 3$ $\beta_3 = \big((15-\sqrt{5}) - (3-\sqrt{5})\theta'\big)/2$ $c_3 = -25(7+3\sqrt{5}) + 10(5+2\sqrt{5})\theta$

$d_3 = -25(34+15\sqrt{5}) + 25(11+5\sqrt{5})\theta$ $e_3 = -25(55+24\sqrt{5}) + 25(15+7\sqrt{5})\theta$

$r = 4$ $\beta_4 = \big((15-\sqrt{5}) + (3-\sqrt{5})\theta'\big)/2$ $c_4 = -25(7+3\sqrt{5}) - 10(5+2\sqrt{5})\theta$

$d_4 = -25(34+15\sqrt{5}) - 25(11+5\sqrt{5})\theta$ $e_4 = -25(55+24\sqrt{5}) - 25(15+7\sqrt{5})\theta$

$r = 5$ $\beta_5 = \big((5-\sqrt{5}) - 2\theta'\big)/2$ $c_5 = 5(2635 - 1179\sqrt{5}) - 10(400 - 179\sqrt{5})\theta'$

$d_5 = 25(9452 - 4227\sqrt{5}) - 5(14345 - 6415\sqrt{5}))\theta'$

$e_5 = -25(23935 - 10704\sqrt{5}) + 25(7265 - 3249\sqrt{5})\theta'$

$r = 6$ $\beta_6 = \big((5-\sqrt{5}) + 2\theta'\big)/2$ $c_6 = 5(2635 - 1179\sqrt{5}) + 10(400 - 179\sqrt{5})\theta'$

$d_6 = 25(9452 - 4227\sqrt{5}) + 5(14345 - 6415\sqrt{5})\theta'$

$e_6 = -25(23935 - 10704\sqrt{5}) - 25(7265 - 3249\sqrt{5})\theta'$

$r = 7$ $\beta_7 = \big((5+\sqrt{5}) + 2\theta\big)/2$ $c_7 = 5(2635 + 1179\sqrt{5}) + 10(400 + 179\sqrt{5})\theta$

$d_7 = 25(9452 + 4227\sqrt{5}) + 5(14345 + 6415\sqrt{5})\theta$

$e_7 = -25(23935 + 10704\sqrt{5}) - 25(7265 + 3249\sqrt{5})\theta$

$r = 8$ $\beta_8 = \big((5+\sqrt{5}) - 2\theta\big)/2$ $c_8 = 5(2635 + 1179\sqrt{5}) - 10(400 + 179\sqrt{5})\theta$

$d_8 = 25(9452 + 4227\sqrt{5}) - 5(14345 + 6415\sqrt{5})\theta$

$e_8 = -25(23935 + 10704\sqrt{5}) + 25(7265 + 3249\sqrt{5})\theta$

TABLE 3.

Les coefficients de $p_1p_2p_3p_4$ et de $p_5p_6p_7p_8$.

La table donne, pour tout entier r avec $1 \leq r \leq 20$, les coefficients des termes de degré r des facteurs $p_1p_2p_3p_4$ et $p_5p_6p_7p_8$ de p (voir §4).

r	$p_1p_2p_3p_4$	$p_5p_6p_7p_8$
0	9765625	9765625
1	156250000	−78125000
2	1246093750	308593750
3	−398437500	−679687500
4	−198046875	1170703125
5	−84375000	−2503125000
6	176250000	5628750000
7	−103125000	−9901875000
8	23906250	12960656250
9	2875000	−12777125000
10	−1362500	9511337500
11	−650000	−5282600000
12	356250	2138126250
13	−105000	−606195000
14	72000	111636000
15	−39000	−11049000
16	11325	158925
17	−1800	51600
18	190	190
19	−20	−20
20	1	1

Bibliographie

[BMMB] J.-B. BOST, J.-F. MESTRE, L. MORET-BAILLY, *Calcul explicite en genre 2*, dans *Séminaire sur les pinceaux de courbes elliptiques*, édité par L Szpiro. *Astérisque* **183** (1990).

[F] J. D. FAY, *Theta Functions on Riemann Surfaces*, Lecture Notes in Math. **352**, Springer-Verlag (1973).

[G1] D. GRANT, *Formal Groups in Genus Two*, J. Reine und Angew. Math. **441** (1990), 96-121.

[G2] D. GRANT, *A Generalisation of a Formula of Eisenstein*, Proc. London Math. Soc., (3) **62** (1991), 121-132.

[M] D. MUMFORD, *Tata Lectures on Theta II.*, Progress in Math. **43**, Birkhäuser, (1984).

[Sh-Ta] G. SHIMURA, Y. TANAYAMA, *Complex Multiplication of Abelian Varieties and Its Application to Number Theory*, Mathematical Society of Japan (1961).

[We] A. WEIL, *On the Theory of Complex Multiplication*, *Proc. International Symposium on Algebraic Number Theory*, Tokyo-Nikko (1955), 9-12.

Université de Caen
Département de Mathématiques et de Mécanique
Esplanade de la Paix
14032 CAEN Cedex
FRANCE