SUR LES SOMMES DE CARACTÈRES LIÉES AUX COURBES ELLIPTIQUES À MULTIPLICATION COMPLEXE

A. JOUX ET F. MORAIN

17 mars 1994

RÉSUMÉ. Nous évaluons les sommes de caractères liées aux courbes elliptiques à multiplication complexe par l'anneau des entiers d'un corps quadratique imaginaire de discriminant -43, -67 ou -163, en simplifiant la méthode due à Rajwade *et alii*.

1. Introduction

Soit d un entier strictement positif tel que le corps quadratique $K_d = \mathbb{Q}(\sqrt{-d})$ ait pour nombre de classes 1. D'après [31], d fait partie des neuf valeurs : $1, 2, 3, 7, 11, 19, 43, 67, 163$. Soit E une courbe elliptique à multiplication complexe par l'anneau des entiers $\mathcal{O}_d$ de K_d. L'invariant de E, noté j_d, est un entier rationnel et par suite E est définie sur $\mathbb{Q}$. On trouve dans [10] les équations les plus générales de ces courbes, sous la forme d'une famille indexée par un nombre rationnel non nul c. La courbe $E_{d,c}$ est définie par l'équation $y^2 = f_{d,c}(x)$ où $f_{d,c}$ est un polynôme du troisième degré à coefficients entiers. Nous rappellons les différentes expressions possibles de $f_{d,c}(x)$ dans la table 1.

d	$f_{d,c}$
1	$x^3 + cx$
2	$x(x^2 + 4cx + 2c^2)$
3	$x^3 + c$
7	$x(x^2 + 3.7cx + 2^4.7c^2)$
11	$x^3 - 2^5.3.11c^2x + 2^4.7.11^2c^3$
19	$x^3 - 2^3.19c^2x + 2.19^2c^3$
43	$x^3 - 2^4.5.43c^2x + 2.3.7.43^2c^3$
67	$x^3 - 2^3.5.11.67c^2x + 2.7.31.67^2c^3$
163	$x^3 - 2^4.5.23.29.163c^2x + 2.7.11.19.127.163^2c^3$

TABLEAU 1. Équations des courbes $y^2 = f_{d,c}(x)$ des courbes à multiplication complexe par $\mathcal{O}_d$.

Soient p un nombre premier ($p > 3$) et (a/p) le symbole de Legendre. On pose

$$S_{d,c}(p) = \sum_{x=0}^{p-1} \left(\frac{f_{d,c}(x)}{p} \right).$$

Le nombre de points sur la courbe $E_{d,c}$ modulo p est égal à $p + 1 + S_{d,c}(p)$. Pour cette raison, les sommes $S_{d,c}(p)$, sont utilisées de façon critique dans l'implantation du test de primalité ECPP [1], et nous désirons les évaluer.

Le second auteur est mis à disposition du LIX par la Délégation Générale pour l'Armement.

Il est aisé de voir que pour $d > 3$, on a $S_{d,c}(p) = (c/p)S_{d,1}$, aussi nous contenterons-nous de travailler avec les courbes $E_d = E_{d,1}$ d'équation $y^2 = x^3+a_dx+b_d$ et évaluerons-nous $S_d(p) = S_{d,1}(p)$. D'après la théorie de la multiplication complexe (voir [3]), on sait que si $(-d/p) = -1$, alors $S_d(p) = 0$. Dans le cas où $(-d/p) = 1$, ces sommes sont connues au signe près (cf. section 3) et nous devons lever l'ambiguité du signe.

Notons que le cas $d = 1$ a été traité dans [8, 18, 26, 30] ; $d = 3$ dans [24, 25, 19, 33]; $d = 2$ dans [4, 32, 9, 27, 15] ; les cas $d = 7$ dans [28], $d = 11$ dans [22] et $d = 19$ dans [20]. Ces trois derniers cas ont été étudiés en s'appuyant sur une méthode qui utilise les propriétés des points de $\sqrt{-d}$ division de la courbe E_d.

Notre travail s'inscrit dans la continuation des idées de Rajwade *et al.*. Par une méthode plus simple que celle de Rajwade, nous déterminons les abscisses des points de $\sqrt{-d}$ division. Cela nous permet de prouver que ces abscisses sont en fait des entiers du corps cyclotomique $\mathbb{Q}(\exp(2i\pi/d))$, résultat utilisé empiriquement dans [28, 22, 20]. Nous en déduisons alors les coordonnées des points de $\sqrt{-d}$ division sur la courbe E_d. Nous décrivons ensuite l'idée de Rajwade et expliquons les modifications apportées à celle-ci pour pouvoir traiter les trois cas $d = 43$, $d = 67$, $d = 163$. En particulier, nous remplaçons la résolution délicate d'équations diophantiennes par une utilisation judicieuse de l'algorithme LLL. Le théorème final est le suivant.

Théorème 1.1. *Soit $d \in \{43, 67, 163\}$. Soit p un nombre premier tel que $(-d/p) = +1$ et donc $4p = u^2 + dv^2$, u et v entiers relatifs. Alors*

$$S_d(p) = (2/p)(u/d)u.$$

Corollaire 1.1. *Avec les notations précédentes, le nombre de points sur E_d modulo p vaut $p+1+(2/p)(u/d)u$.*

Dans [22], il est fait mention des résultats pour les trois cas 43, 67 et 163, attribués à Stark. À notre connaissance, la preuve de ceux-ci n'a pas été publiée.

Notons enfin qu'il existe quatre courbes à multiplication complexe par un ordre non principal d'un corps quadratique imaginaire. Les sommes de caractères associées ont été évaluées dans [23, 21].

2. Points de $\sqrt{-d}$ division

Dans la suite de l'article, nous supposons que d est un nombre premier impair ($d > 7$) et que E_d est une courbe elliptique à multiplication complexe par $\mathcal{O}_d$, d'équation donnée dans la table 1.

Proposition 2.1. *Soient ω_1 et ω_2 des périodes de E_d, avec $\omega_1 \in \mathbb{R}$, $\tau = \omega_2/\omega_1$ tel que $\Im(\tau) > 0$ et $\tau \in K_d$. Alors*

$$\tau = \frac{-d + \sqrt{-d}}{2d}.$$

Preuve : Posons $T = (1 + \sqrt{-d})/2$. Soit $j_d = j(T)$ l'invariant des courbes à multiplication complexe par $\mathcal{O}_d$. Il est facile de voir que la courbe d'équation

$$Y^2 = X^3 + \frac{3j_d}{1728 - j_d}X + \frac{2j_d}{1728 - j_d} \tag{1}$$

a pour invariant j_d. Cette courbe est isomorphe à $\mathbb{C}/(\mathbb{Z} + T\mathbb{Z})$ et a pour périodes Ω_1 et Ω_2 telles que $\Omega_1 \in \mathbb{R}$ et $\Omega_2/\Omega_1 = T$ (voir [6, Chapitre 7, §4] par exemple). On remarque alors que

$$\begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix} \frac{1 + \sqrt{-d}}{2} = \frac{-d + \sqrt{-d}}{2d}$$

d	j_d
19	$(-2^5.3)^3$
43	$(-2^6.3.5)^3$
67	$(-2^5.3.5.11)^3$
163	$(-2^6.3.5.23.29)^3$

TABLEAU 2. Invariants des courbes à multiplication complexe par $\mathcal{O}_d$ pour $d \in \{19, 43, 67, 163\}$.

donc les coefficients de (1) se transforment par multiplication par $(2T-1)^4 = d^2$ et d^3 respectivement.

Notant alors que les invariants des courbes E_d sont donnés dans la table 2, on conclut la preuve de la proposition. □

Soit L le réseau $\mathbb{Z}[\omega_1, \omega_2]$. La courbe E_d est naturellement isomorphe à $\mathbb{C}/L$. Soit $\wp$ la fonction de Weierstrass associée à E_d. La fonction $\wp$ fournit un paramétrage de la courbe E_d : quand $z \notin L$, $(\wp(z), \wp'(z)/2, 1)$ est un point de $E_d : y^2 = x^3 + a_d x + b_d$.

Pour utiliser l'idée de Rajwade, il est nécessaire de connaître les points de $\sqrt{-d}$ division de la courbe. Un tel point $P = (\wp(z), \wp'(z)/2, 1) \neq O_{E_d}$ vérifie $\sqrt{-d}P = O_{E_d}$, autrement dit, z est un pôle de la fonction $\wp_d : z \mapsto \wp(\sqrt{-d}z)$. On a le résultat suivant [7, §10, C].

Théorème 2.1. *La fonction $\wp_d$ s'exprime comme une fonction rationnelle de $\wp$:*

$$\wp(\sqrt{-d}z) = \frac{F_d(\wp(z))}{G_d(\wp(z))},$$

avec $F_d(X)$ et $G_d(X)$ des polynômes à coefficients dans $\mathbb{C}$, de degré respectif d et $d-1$.

En fait, si l'on développe en série les fonctions $\wp_d$ et $F_d(\wp)/G_d(\wp)$, on constate que ces coefficients doivent être des rationnels car les coefficients de E_d le sont. On pourra toujours supposer que $F_d(X) = \sum_{i=0}^{d} f_i X^i$ et $G_d(X) = \sum_{i=0}^{d-1} g_i X^i$ sont à coefficients dans $\mathbb{Z}$ et premiers entre eux. De plus, en comparant les développements en fonction de z, on voit que

$$\wp_d(z) = \frac{-1}{dz^2} + \cdots$$

et donc $f_d/g_{d-1} = -1/d$.

On trouve le résultat suivant dans [13, Chapitre II].

Théorème 2.2. *Soit $P = (X, Y, 1)$ un point de E_d. Alors*

$$dP = \left(\frac{\varphi_d(X)}{\psi_d^2(X)}, Y\frac{\omega_d(X)}{\psi_d^3(X)}\right)$$

où $\varphi_d(X)$, $\psi_d(X)$ et $Y\omega_d(X)$ sont des polynômes à coefficients dans $\mathbb{Z}[a,b]$. Si l'on affecte les poids 4 à a, 6 à b, 2 à X et 3 à Y, ces polynômes sont homogènes en a, b, X, Y. De plus, le polynôme ψ_d est de la forme :

$$\psi_d(X) = dX^{(d^2-1)/2} + \sum_{k=0}^{(d^2-3)/2} c_k(a,b)X^k. \tag{2}$$

On en déduit la propriété clef suivante.

Corollaire 2.1. *Les abscisses des points de d division de E_d sont des entiers algébriques.*

Preuve : On remarque que a_d et b_d sont multiples de d. Par suite, on tire de (2) que $\psi_d(X) = d\tilde{\psi}(X)$ avec $\tilde{\psi}$ unitaire à coefficients entiers. □

Proposition 2.2. *On a*

$$G_d(X) \mid \psi_d^2(X)$$

et $G_d(X)$ est le carré d'un polynôme de $\mathbb{Z}[X]$.

Preuve : On écrit

$$\wp(dz) = \wp(-dz) = \wp(\sqrt{-d}(\sqrt{-d}z)) = \frac{F_d(F_d(\wp(z))/G_d(\wp(z)))}{G_d(F_d(\wp(z))/G_d(\wp(z)))}. \square$$

On en déduit alors les résultats suivant.

Corollaire 2.2. (1) *On a $f_d = -d$ et $g_{d-1} = d^2$.*
(2) *Soit x une racine de $G_d(X)$. Alors x est un entier algébrique.*

Intéressons-nous maintenant au calcul des racines de $G_d(X)$.

Proposition 2.3. *Les racines de $G_d(X)$ sont les $\wp(r\omega_2/\sqrt{-d})$ où r est un entier compris entre 1 et $d-1$:*

$$G_d(X) = d^2 \prod_{r=1}^{d-1} (X - \wp(r\omega_2/\sqrt{-d}))$$

et même $G_d(X) = d^2 H_d(X)^2$ avec

$$H_d(X) = \prod_{r=1}^{(d-1)/2} (X - \wp(r\omega_2/\sqrt{-d}))$$

un polynôme unitaire à coefficients dans $\mathbb{Z}$, que nous appellerons polynôme de $\sqrt{-d}$-division.

Preuve : Si $\omega \in L$ et $\varpi = \omega/\sqrt{-d} \notin L$, alors ϖ est un pôle de $\wp_d$. Les pôles de $\wp_d$ sont donc à prendre parmi les $z_{s,r} = (s\omega_1 + r\omega_2)/\sqrt{-d}$, avec s et r entiers. Or

$$\frac{\omega_1}{\sqrt{-d}} = -2\omega_2 - \omega_1,$$

donc il suffit de considérer le cas où $s = 0$.

À cause de la parité de $\wp$, il suffit de prendre r compris entre 1 et $(d-1)/2$. □

Montrons maintenant le résultat suivant.

Proposition 2.4. *Les racines de $H_d(X)$ sont réelles.*

Preuve : Il suffit de montrer que $\wp(\omega_2/\sqrt{-d})$ est réel. Utilisant la relation

$$\overline{\omega}_2 = -\omega_2 - \omega_1$$

on trouve que

$$\overline{\left(\frac{\omega_2}{\sqrt{-d}}\right)} \equiv \frac{\omega_2}{\sqrt{-d}} \bmod L$$

et on a bien le résultat cherché. □

Le dernier résultat dont nous aurons besoin est le suivant.

Théorème 2.3. *Le polynôme $H_d(X)$ se décompose sur $\mathbb{Q}(\zeta)$ avec ζ une racine primitive d-ième de l'unité.*

Preuve : Notons F l'isogénie multiplication par $\sqrt{-d}$ et $\hat{F}$ l'isogénie duale. Soit e_F l'accouplement de Weil associé à F. Il est défini sur $\mathrm{Ker}F \times \mathrm{Ker}\hat{F}$. Comme $\hat{F} = -d/F = -F$, e_F est une forme bilinéaire symétrique non dégénérée sur $(\mathrm{Ker}F)^2$. Soit $P = (X, Y)$ un générateur de $\mathrm{Ker}F$. Alors $e_F(P, P)$ est une racine primitive d-ième de 1 car e_F est non dégénéré.

Soit maintenant σ un automorphisme de $\overline{\mathbb{Q}}$ qui stabilise ζ. Alors

$$\sigma(e_F(P, P)) = e_F(P, P).$$

Le Théorème 3.8 (pp. 229) de [11] entraîne :

$$\sigma(e_F(P, P)) = e_{\sigma\circ F}(\sigma(P), \sigma(P)).$$

Comme F est définie sur $\mathbb{Q}(\sqrt{-d}) \subset \mathbb{Q}(\zeta)$, on a

$$e_{\sigma\circ F}(\sigma(P), \sigma(P)) = e_F(\sigma(P), \sigma(P)).$$

On a $\sigma(P) \in \mathrm{Ker}F$; il existe donc un entier r tel que $\sigma(P) = rP$. On en déduit :

$$e_F(P, P) = e_F(rP, rP) = e_F(P, P)^{r^2}.$$

Donc, puisque $e_F(P, P)$ est une racine primitive de 1, $r^2 = 1 \bmod d$, soit $r \equiv \pm 1 \bmod d$. Par suite, $\sigma(P) = \pm P$ et donc $\sigma(X) = X$ et donc X est dans $\mathbb{Q}(\zeta)$. □

Remarque. Ce théorème se généralise à certains cas où $h(-d) > 1$ et la courbe E_d est définie sur $\mathbb{Q}(j_d)$ avec j_d un entier algébrique de degré $h(-d)$. L'étude des sommes de caractères dans le cas $h(-d) > 1$ sera reprise dans un article ultérieur.

Utilisant les deux théorèmes précédents, on en déduit le résultat suivant.

Corollaire 2.3. *Le polynôme $H_d(X)$ se décompose dans $\mathbb{Q}(\theta)$ où $\theta = \zeta + \zeta^{-1}$.*

Remarque. Notons que notre approche diffère de celle de Rajwade dans le calcul des points de $\sqrt{-d}$ division. Rajwade commence par expliciter la multiplication complexe par $(1 + \sqrt{-d})/2$ et trouve des formules du type

$$Q = (X, Y, 1) = (R_1(x), R_2(x, y))$$

où $(x, y, 1)$ sont les coordonnées d'un point P de E_d et les R_i des fractions rationnelles à coefficients dans $\mathbb{Q}(\sqrt{-d})$. Le point Q est un point de $\sqrt{-d}$ division si et seulement si $Q = \overline{Q}$ (conjugaison dans $\mathbb{Q}(\sqrt{-d})$), ce qui conduit à résoudre $X = \overline{X}$, qui se ramène à une équation polynomiale en x, $H_d(x) = 0$. Nous préferons pour notre part déterminer directement $H_d(x)$.

3. La méthode de Rajwade

3.1. Théorie. On se propose d'évaluer

$$S_d(p) = \sum_{x=0}^{p-1} \left(\frac{f_d(x)}{p}\right)$$

pour $d \in \{19, 43, 67, 163\}$.

Soit p un nombre premier plus grand que 3. D'après la théorie de la multiplication complexe (cf. [3], par exemple), on sait que si $(-d/p) = -1$, alors p reste inerte dans $\mathbb{Q}(\sqrt{-d})$ et par suite

$$S_d(p) = 0.$$

Par contre, si $(-d/p) = +1$, le nombre premier p se décompose dans $\mathbb{Q}(\sqrt{-d})$: il existe un entier algébrique $\pi = (u + v\sqrt{-d})/2 \in \mathcal{O}_d$, u et v entiers relatifs, tel que $p = \mathrm{N}(\pi) = (u^2 + dv^2)/4$. D'autre part, soit π_p le Frobenius de E_d, c'est-à-dire l'application de E_d dans E_d, définie sur $\mathbb{F}_p$, qui au point $(x, y, 1)$ associe $(x^p, y^p, 1)$. On sait que π_p satisfait également à $p = \mathrm{N}(\pi_p)$, par suite, u et v étant fixés, $\pi_p = (\pm u \pm v\sqrt{-d})/2$. Finalement, on a

$$S_d(p) = -\mathrm{Tr}(\pi_p) = \pm u.$$

Il y a ambiguité sur le signe dans la dernière égalité. Le travail qu'il nous reste à accomplir est la levée de cette ambiguité.

Soit P_d un point de $\sqrt{-d}$ division de E_d. D'après la section précédente, l'abscisse de $P_d = (X, Y, 1)$ est un entier de $\mathbb{Q}(\theta)$ avec $\theta = \zeta + \zeta^{-1}$. Posant $\theta_1 = \theta$ et $\theta_r = \zeta^r + \zeta^{-r}$ pour r entier, on en déduit que

$$X = \sum_{r=1}^{(d-1)/2} a_r \theta_r$$

où les a_i sont des entiers naturels. L'ordonnée Y de P_d est donnée par $y^2 = x^3 + a_d x + b_d$ et appartient à une extension de degré au plus 2 de $\mathbb{Q}(\theta)$. Soit $Q = \pi_p(P_d)$. Le point Q est également un point de $\sqrt{-d}$ division. Par suite, il existe un entier k tel que $Q = kP_d$. On déduit que $(\pi_p - k)P_d = O_{E_d}$, ce qui conduit à

$$\pi_p - k \equiv 0 \bmod \sqrt{-d}.$$

Écrivons $\pi_p = (u_p + v_p\sqrt{-d})/2$ avec $|u_p| = |u|$, $|v_p| = |v|$. Nous déduisons de cela que $u_p \equiv 2k \bmod d$. Reste à vérifier que $(2k/d) = -(2/p)$ pour arriver à la preuve du théorème 1.1.

3.2. Pratique.

3.2.1. *Le cas $d = 19$ revisité.* Nous utiliserons le cas $d = 19$ à des fins de comparaison avec l'article [20].

Posons $\delta = (d-1)/2$. Soit X_1 une racine de $H_d(X)$:

$$X_1 = \sum_{r=1}^{\delta} a_r \theta_r$$

avec les a_r des entiers relatifs. On notera pour simplifier $X_1 = [a_1, a_2, \ldots, a_\delta]$. Grâce au logiciel `PARI-gp`, on calcule les périodes de la courbe donnée dans la table 1 :

$$\omega_1 = 2.9631663359, \quad \omega_2 = -1.4815831679 + 0.3398984897i$$

et il est rassurant de constater que $\omega_2/\omega_1 \approx (-19 + \sqrt{-19})/38$.

Pour des raisons pratiques (expliquées à la section suivante), on préfère utiliser une racine de petit module de H_d. Avec les notations habituelles, on choisit :

$$X_1 = \wp(5\omega_2/\sqrt{-19}) \approx 4.9186942326.$$

Grâce à l'algorithme LLL (voir section suivante), on trouve :

$$X_1 = -2[6, 4, 2, 5, 4, 4, 7, 2, 4].$$

Cette valeur correspond bien à une de celles trouvées dans [20]. Après essais et erreurs, on trouve que l'ordonnée du point P_1 d'abscisse Y_1 est (toujours en utilisant LLL) :

$$Y_1 = -\sqrt{2}[25, 23, 3, 39, 7, 11, 35, -1, 29].$$

Notons que ces valeurs de X et Y peuvent être vérifiées par substitution dans le polynôme H_d pour X_1 et simple élévation au carré pour Y_1.

On trouve dans le tableau suivant les points $kP = (X_k, Y_k)$ pour $1 \le k \le \delta = 9$ (le détail des calculs se trouve à la section suivante).

k	X_k	$Y_k/\sqrt{2}$
1	$[-12,-8,-4,-10,-8,-8,-14,-4,-8]$	$-[25,23,3,39,7,11,35,-1,29]$
2	$[-8,-8,-10,-12,-8,-4,-4,-8,-14]$	$[7,29,39,25,11,-1,3,23,35]$
3	$[-8,-10,-8,-4,-8,-14,-8,-4,-12]$	$[23,39,11,-1,29,35,7,3,25]$
4	$[-8,-14,-12,-8,-4,-8,-10,-8,-4]$	$[-11,-35,-25,-7,1,-23,-39,-29,-3]$
5	$[-4,-8,-8,-14,-10,-12,-8,-8,-4]$	$[-3,-11,-29,-35,-39,-25,-23,-7,1]$
6	$[-8,-12,-4,-8,-14,-4,-8,-10,-8]$	$[-29,-25,1,-23,-35,-3,-11,-39,-7]$
7	$[-14,-8,-8,-8,-4,-10,-4,-12,-8]$	$[-35,-7,-23,-29,-3,-39,1,-25,-11]$
8	$[-4,-4,-8,-8,-8,-8,-12,-14,-10]$	$[-1,3,7,11,23,29,25,35,39]$
9	$[-10,-4,-14,-4,-12,-8,-8,-8,-8]$	$[-39,1,-35,-3,-25,-7,-29,-11,-23]$

Passons maintenant à la détermination de la valeur propre du Frobenius π_p en fonction du nombre premier p. Soit p un nombre premier tel que $(-19/p) = +1$: p s'écrit $r + 19n$, avec $r \in \{1,4,5,6,7,9,11,16,17\}$. L'action du Frobenius π_p correspond à l'action $\zeta_d \mapsto \zeta_d^r$ sur x_1 et sur y_1, combinée à la transformation $\sqrt{2} \mapsto (2/p)\sqrt{2}$. Pour chaque valeur de r, on trouve dans le tableau ci-dessous l'entier k tel que $\pi_p(P) = k(2/p)P$ et donc $u \equiv 2k(2/p) \bmod d$.

r	k	r	k	r	k	r	k	r	k	r	k	r	k	r	k	r	k
1	1	4	-2	5	9	6	5	7	-8	9	-3	11	7	16	4	17	6

On vérifie que pour toutes les valeurs de r, on a bien $(2k/d) = -1$ et que par conséquent, la condition de normalisation de u est alors $(u/d) = -(2/p)$.

3.2.2. *Le cas $d = 43$.* On trouve

$$\omega_1 = 2.043921192, \quad \omega_2 = -1.021960596 + 0.1558475298i$$

avec $\omega_2/\omega_1 \approx (-43 + \sqrt{-43})/86$. On choisit

$$X_1 = \wp(5\omega_2/\sqrt{-43}) \approx 2.7583672875$$

et on trouve

$$X_1 = -2[17,21,32,36,31,28,22,18,12,23,26,34,30,35,23,18,12,20,19,26,33].$$

De même

$$Y_1 = -\sqrt{2}[13,-281,-399,-587,-491,-375,-103,37,35,-67,-305,-463,\\ -571,-407,-275,-23,37,37,-193,-377,-531].$$

On trouve dans le tableau ci-dessous les valeurs propres du frobenius π_p pour les $p = 43n + r$ qui se scindent dans $\mathbb{Q}(\sqrt{-43})$.

r	k	r	k	r	k	r	k	r	k	r	k	r	k
1	1	9	-3	13	-20	16	4	23	-18	31	17	38	9
4	-2	10	15	14	10	17	-19	24	14	35	11	40	13
6	-7	11	21	15	-12	21	-8	25	-5	36	6	41	16

La condition de normalisation est encore $(u/43) = -(2/p)$.

3.2.3. *Le cas $d = 67$.* On trouve dans ce cas :

$$\omega_1 = 1.491162900, \quad \omega_2 = -0.7455814504 + 0.09108727122i$$

avec $\omega_2/\omega_1 \approx (-67 + \sqrt{-67})/134$. On choisit

$$X_1 = \wp(7\omega_2/\sqrt{-67}) \approx 28.1133288468$$

et on trouve

$$X_1 = -2[93, 62, 98, 66, 67, 88, 62, 110, 38, 109, 50, 103, 70, 77, 78, 72, \\ 102, 56, 95, 52, 108, 62, 88, 71, 60, 104, 52, 103, 38, 100, 61, 84, 67],$$

$$Y_1 = \sqrt{2}[3477, -69, 2529, 1349, 1611, 2383, 47, 3123, -173, 3719, -291, 2607, \\ 589, 1997, 2019, 419, 2745, -329, 3583, -157, 2883, 227, 2135, 1835, \\ 847, 2547, -139, 3543, -129, 3325, -65, 2381, 1491].$$

Le tableau des valeurs propres pour les $p = 67n + r$ est donné ci-dessous.

r	k	r	k	r	k	r	k	r	k	r	k	r	k
1	1	14	9	21	17	26	19	37	29	54	−11	62	14
4	−2	15	22	22	25	29	−30	39	21	55	16	64	−8
6	26	16	4	23	−31	33	10	40	24	56	−18	65	−20
9	−3	17	33	24	15	35	−13	47	−28	59	−27		
10	−12	19	−32	25	−5	36	6	49	−7	60	23		

La condition de normalisation est aussi $(u/67) = -(2/p)$.

3.2.4. *Le cas $d = 163$.* Après avoir calculé

$$\omega_1 = 0.5611934280, \quad \omega_2 = -0.2805967140 + 0.02197802718i$$

et $\omega_2/\omega_1 \approx (-163 + \sqrt{-163})/326$, on sélectionne

$$X_1 = \wp(9\omega_2/\sqrt{-163}) \approx -110.7585949142$$

que l'on peut récrire comme

$$X_1 = -2[1002, 1179, 1337, 1240, 1271, 1613, 1862, 2040, 1876, 1964, 1896, 2010, 1904, \\ 1584, 1433, 1292, 1353, 1146, 1063, 878, 860, 1025, 1180, 1258, 1266, 1522, 1684, \\ 1952, 1942, 1858, 1804, 1841, 1975, 1638, 1531, 1253, 1267, 1193, 1057, 878, 724, \\ 976, 1104, 1252, 1260, 1381, 1542, 1816, 1958, 1809, 1810, 1824, 2022, 1822, \\ 1629, 1317, 1170, 1305, 1088, 960, 724, 979, 1137, 1247, 1280, 1262, 1522, 1792, \\ 1963, 1864, 1894, 1938, 1995, 1910, 1675, 1445, 1212, 1335, 1140, 1078, 924].$$

On trouve alors

$$Y_1 = \sqrt{2}[27189, 9317, -23555, -108727, -194051, -241243, -284899, -310837, \\ -381771, -408975, -400275, -339493, -289001, -257153, -213889, \\ -155635, -50575, 1197, 29067, 5109, 14717, 21829, -6707, -65521, \\ -177831, -228535, -275099, -292027, -358117, -410095, -408319, \\ -366103, -296027, -272997, -237685, -187221, -82617, -8579, 15723, \\ 12627, 6725, 30273, 2749, -42037, -146741, -206727, -251233, \\ -289245, -333867, -397813, -401815, -393449, -325559, -288023, \\ -249559, -202523, -128831, -35691, 7831, 29809, 4913, 14799, 11733, \\ -16373, -98411, -193979, -237867, -282545, -301811, -377579, \\ -410375, -410107, -348315, -289287, -268159, -219629, -165239, \\ -59939, -3291, 24231, 6905].$$

Le tableau des valeurs propres est le suivant.

r	k	r	k	r	k	r	k	r	k	r	k	r	k	r	k
1	1	25	−5	46	−32	61	77	85	−30	111	33	135	61	156	51
4	−2	26	−29	47	−79	62	15	87	24	113	−73	136	25	158	22
6	−13	33	14	49	−7	64	−8	88	−67	115	21	140	38	160	46
9	−3	34	69	51	41	65	−37	90	47	118	−66	143	−44	161	−18
10	−70	35	−19	53	−78	69	−45	91	55	119	49	144	−12		
14	60	36	6	54	39	71	−76	93	16	121	−11	145	54		
15	34	38	53	55	−50	74	−20	95	62	126	−17	146	−31		
16	4	39	56	56	43	77	−27	96	−52	131	−72	150	65		
21	64	40	−23	57	−63	81	9	97	74	132	−28	151	71		
22	−48	41	81	58	−59	83	−75	100	10	133	40	152	57		
24	26	43	−80	60	−68	84	35	104	58	134	−42	155	36		

La condition de normalisation est encore $(u/163) = -(2/p)$.

4. Quelques détails des calculs

Notons pour commencer que les calculs des périodes de E_d ainsi que les calculs sur la fonction $\wp$ ont été faits en `PARI-gp` [2] d'après les algorithmes décrits dans [6]. Les calculs sur les points, ainsi que les calculs finaux, ont été faits en `Maple` [5].

4.1. Quelques lemmes utiles. Soit d un nombre premier impair. On pose $\delta = (d-1)/2$, $\zeta = \exp(2i\pi/d)$ et $\theta_r = \zeta^r + \zeta^{-r}$ (avec $\theta_1 = \theta$).

Lemme 4.1. *Les relations suivantes sont satisfaites :*

$$\sum_{r=1}^{\delta} \theta_r = -1, \tag{3}$$

$$\sum_{r=1}^{\delta} \theta_r^2 = d-2, \tag{4}$$

et

$$\sum_{1\leq r<s\leq\delta} \theta_r\theta_s = -2. \tag{5}$$

Preuve : L'équation (3) est immédiate en utilisant les propriétés des racines primitives de l'unité. Ensuite, remarquons que

$$\theta_r\theta_s = \theta_{r+s \bmod \delta} + \theta_{r-s \bmod \delta}$$

pour toutes valeurs de r et s. On en déduit

$$\sum_{r=1}^{\delta}\theta_r^2 = \sum_{r=1}^{\delta}(\theta_{2r \bmod \delta}+2) = (\sum_{r=1}^{\delta}\theta_r) + 2\delta = d-1-1 = d-2.$$

De même

$$\sum_{1\leq r<s\leq\delta}\theta_r\theta_s = \sum_{1\leq r<s\leq\delta}(\theta_{r+s \bmod \delta}+\theta_{r-s \bmod \delta}) = 2\sum_{r=1}^{\delta}\theta_r = -2.\square$$

Soit g une racine primitive modulo d et σ l'automorphisme de $\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q})$ qui envoie θ sur θ_g. Les racines du polynôme $H_d(X)$ sont les

$$x_k = \sum_{r=1}^{\delta} a_r \sigma^{k-1}(\theta_r)$$

avec les a_i des entiers relatifs. Nous sommes maintenant en mesure de prouver :

Proposition 4.1. *Soit*

$$\xi_1 = \sum_{k=1}^{\delta} x_k, \xi_2 = \sum_{1\leq k<\ell\leq\delta} x_k x_\ell.$$

Alors

$$\sum_{r=1}^{\delta} a_r = -\xi_1, \tag{6}$$

$$\sum_{r=1}^{\delta} a_r^2 = \frac{3\xi_1^2 - 2\xi_2}{d}. \tag{7}$$

Preuve : On a

$$\xi_1 = \sum_{k=1}^{\delta} x_k = (\sum_r a_r)(\sum_k \theta_k) = -\sum_r a_r.$$

Pour la deuxième relation

$$\sum_{k=1}^{\delta} x_k^2 = \sum_k (\sum_r a_r^2 \sigma^{k-1}(\theta_r)^2) + 2 \sum_{1\leq r<s\leq\delta} a_r a_s \sigma^{k-1}(\theta_r\theta_s)$$

ce que l'on peut réorganiser comme

$$(\sum_k a_k^2)(\sum_{r=1}^{\delta} \theta_r^2) + 2(\sum_{1\leq r<s\leq\delta} a_r a_s)(\sum_{1\leq k<\ell\leq\delta} \theta_k\theta_\ell)$$

pour trouver finalement

$$(d-2)(\sum_k a_k^2) - 4\sum_{r,s} a_r a_s$$

en utilisant le lemme précédent et deux fois l'identité

$$\sum z_r^2 = (\sum z_r)^2 - 2\sum_{r,s} z_r z_s. \square$$

On trouve dans le tableau 4.1 les valeurs des deux sommes pour les valeurs de d considérées. Ces valeurs ont été calculées en `PARI-gp`, en flottants, le résultat fournissant un entier avec une grande précision.

d	ξ_1	ξ_2	$\sum a_r^2$
19	76	1748	728
43	1032	414520	55024
67	5092	10596988	844648
163	−236024	23884912904	732221840

TABLEAU 3.

4.2. Détermination de P_d : l'algorithme LLL.

4.2.1. *Détermination de l'abscisse de P_d.* La solution utilisée dans [20] consiste à rechercher les coefficients a_i par résolution d'équations diophantiennes. Cette méthode paraît trop lourde pour traiter les cas qui nous intéressent. Une première alternative consiste à utiliser un système de calcul formel du type de `Maple` ou `Axiom`, dans lequel existent des procédures de factorisation de polynômes sur les corps de nombres. Cette méthode a l'avantage de la simplicité (pour le programmeur), mais nécessite le calcul du polynôme $H_d(X)$ qui a des coefficients entiers très grands. Le temps de calcul et la place mémoire nécessaires sont prohibitifs. Par exemple, sur un RS6000 avec 64 Moctets de mémoire centrale, `Axiom` met 4275 secondes pour factoriser H_{19} et la factorisation de H_{43} est impossible. Pour pallier ce problème, nous avons utilisé une méthode, qui si elle n'est pas simple conceptuellement, est très efficace. Elle utilise l'algorithme LLL.

L'algorithme de Lenstra, Lenstra et Lovász [14], généralement appelé LLL, est un algorithme de réduction de réseaux entiers, qui transforme une base d'un réseau entier $(b_1, b_2, \dots, b_n)$ en une base réduite $(b'_1, b'_2, \dots, b'_n)$ du même réseau. Informellement, une base réduite est formée de vecteurs assez courts et presque orthogonaux entre eux. En particulier, soit L_1 le premier minimum du réseau. Alors

$$\|b'_1\| \leq 2^{n/2} L_1. \tag{8}$$

L'une des applications classiques de cet algorithme consiste à rechercher des relations de dépendances linéaires à coefficients entiers (ou rationnels) entre nombres réels ou complexes, de telle sorte que le vecteur formé des coefficients de la combinaison soit de poids faible, lorsque l'on sait à l'avance qu'une telle combinaison existe. Pour cela on utilise le réseau engendré par les vecteurs colonnes de la matrice suivante :

$$R = \begin{pmatrix} N_1 & N_2 & \cdots & N_n \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

où les N_i sont les nombres dont on cherche une combinaison linéaire “courte”. Le résultat attendu pour le premier vecteur de la base réduite est :

$$e = \begin{pmatrix} 0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

où les α vérifient $\sum_{i=1}^{n} \alpha_i N_i = 0$.

Soit A la norme euclidienne du vecteur e, le vecteur b'_1 trouvé par LLL vérifie :

$$\|b'_1\| \leq 2^{n/2} A. \tag{9}$$

Par conséquent, si $2^{n/2}A$ est plus petit que les vecteurs courts autres que e (et $-e$ bien sûr), on est sûr que LLL trouvera le vecteur e ou éventuellement $-e$. Comment évaluer la taille des vecteurs courts autres que e? En général, on considère que les autres vecteurs courts ont une norme de l'ordre de celle du vecteur le plus court d'un réseau aléatoire, environ $|\det(R)|^{1/n}$. De plus, comme $|\det(R)| \approx \max_i |N_i|$, on espère donc que LLL trouve e dès lors que:

$$2^{n/2} A \leq N^{1/n} \tag{10}$$

où $N = \max_i |N_i|$. Par conséquent N doit être plus grand que $2^{n^2/2} A^n$ pour que l'algorithme réussisse.

Nous allons appliquer cette technique de recherche de combinaisons linéaires courtes, afin d'exprimer une racine x de $H_d(X)$ sous la forme

$$x = \sum_{r=1}^{\delta} a_r \theta_r$$

avec les a_i entiers relatifs. Pour ce faire, utilisons la variante suivante de R :

$$R' = \begin{pmatrix} \lfloor K\theta_1 \rceil & \lfloor K\theta_2 \rceil & \cdots & \lfloor K\theta_\delta \rceil & \lfloor Kx \rceil \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

où $\lfloor w \rceil$ est l'entier le plus proche de w, et où K est un grand entier bien choisi, servant à préciser le nombre de chiffres nécessaires pour les θ_i et pour x. Le vecteur attendu est:

$$e' = \begin{pmatrix} \epsilon \\ a_1 \\ a_2 \\ \vdots \\ a_n \\ 1 \end{pmatrix}$$

où ϵ n'est pas forcément nul car les θ et x sont représentés de manière approchée seulement. Comme la norme euclidienne de e' vaut approximativement $A = \sqrt{\sum_{r=1}^{\delta} a_r^2}$ et que le determinant de R' est de l'ordre de K (car les θ et x sont tous petits), nous devons choisir K tel que:

$$K \geq 2^{(\delta+1)^2/2} A^{\delta+1} \tag{11}$$

$$\geq 2^{(d+1)^2/8} (\sum_{r=1}^{\delta} a_r^2)^{(d+1)/4} \tag{12}$$

$$\geq 2^{(d+1)^2/8} (\frac{3\xi_1^2 - 2\xi_2}{d})^{(d+1)/4}. \tag{13}$$

Afin de simplifier les notations, nous choisirons toujours pour K une puissance de 10, par exemple $K = 10^{100}$. Nous dirons alors que le calcul est fait avec 100 chiffres. Voici un tableau résumant les valeurs de K à utiliser (pour x) en fonction de d:

d	Nombre de chiffres
19	30
43	125
67	275
163	1376

Cependant, en pratique, l'algorithme LLL donne de meilleurs résultats que ceux annoncés par la borne théorique. C'est pourquoi nous avons pu obtenir tous les résultats présentés dans cet article, en travaillant avec une précision de 1000 chiffres. La réduction de réseau la plus longue à faire n'a duré que quelques heures sur une Sparc-station de type ELC. Il convient toutefois de noter que de telles performances ne sont envisageables qu'en utilisant une version flottante de l'algorithme LLL, comme celle décrite par Schnorr et Euchner dans [29]. De plus, dans ce cas, il convient de mettre en œuvre certaines astuces de calculs, afin de pouvoir mener à bien la réduction de réseau. Nous renvoyons à [12] pour plus de précisions.

4.2.2. *Détermination de l'ordonnée de P_d.* Pour trouver l'ordonnée y correspondant à x sur la courbe (en fait $y/\sqrt{2}$), on a encore le choix entre utiliser la factorisation sur des corps de nombres, en cherchant à factoriser $Y^2 - (x^3 + ax + b)/m$ pour m bien choisi, ou bien utiliser LLL. C'est cette dernière méthode que nous employons là encore.

Le nombre de chiffres à prévoir est environ le double du nombre de chiffres pour x. Les remarques faites précédemment sur le bon comportement de LLL restent valables.

4.3. Calcul des multiples de P_d. L'algorithme de Rajwade nécessite l'identification des multiples de P_d. La méthode la plus simple consiste à calculer kP_d en utilisant les routines d'évaluation des nombres algébriques existant dans un système de calcul formel. Toutefois, l'opération critique consiste à effectuer une division, ce qui est très coûteux.

Une solution, *a priori* moins élégante, consiste à procéder comme suit. On commence par évaluer en flottants tous les conjugués de X, ce qui est facile. On évalue alors les points kP_d *en nombres flottants* et on compare les valeurs numériques des abscisses trouvées à l'évaluation flottante des conjugués de X. Cette méthode, même si elle nécessite des calculs avec plusieurs centaines de chiffres de précision (300 sont nécessaires pour $d = 163$), est beaucoup plus rapide.

4.4. Vérification des résultats. De façon à minimiser les risques d'erreur dans l'écriture du théorème 1.1, nous avons programmé le calcul des sommes de caractères $S_d(p)$ en `gp` et vérifié numériquement la véracité des formules pour tous les nombres premiers $200 \leq p \leq 5000$ tels que $(-d/p) = +1$.

5. Conclusion

Nous avons prouvé dans cet article certains résultats utilisés auparavant par Rajwade *et al.* Cela nous a permis de calculer les sommes $S_d(p)$ pour les cas où $h(-d) = 1$ et $d > 19$. Dans le cas $h(-d) > 1$, le polynôme de $\sqrt{-d}$ division s'obtient cette fois par

$$H_d(X) = \prod_{\substack{1 \leq r \leq d/2 \\ (r,d)=1}} (X - \wp(r\omega_2/\sqrt{-d}))$$

mais le corps de décomposition de $H_d(X)$ n'est plus un corps cyclotomique. La méthode de Rajwade ne s'applique donc plus. Dans certains cas malgré tout, on peut évaluer les sommes $S_d(p)$, mais par une autre méthode [16].

Remerciements. Les auteurs tiennent à remercier V. Auger pour sa connaissance de `PARI-gp` ; D. Augot pour avoir tenté les calculs de factorisation des polynômes $H_d(X)$ en `Axiom` ; J.-M. Couveignes pour son intérêt constant et ses suggestions concernant ce travail, notamment la preuve du théorème 2.3 ; P. Dumas pour son aide lors du polissage final de l'article ; l'un des referee pour ses commentaires pertinents et la correction de la preuve du théorème 2.3.

Références

1. A. O. L. Atkin et F. Morain. Elliptic curves and primality proving. *Math. Comp. 61*, 203 (Juil. 1993), 29–67.
2. C. Batut, D. Bernardi, H. Cohen, et M. Olivier. *User's Guide to PARI–GP*. Université de Bordeaux I, 1990. Distribué avec le programme gp.
3. A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, et J. P. Serre. *Seminar on complex multiplication*. No. 21 dans Lect. Notes in Math. Springer, 1966.
4. B. W. Brewer. On certain character sums. *Trans. Amer. Math. Soc. 99* (1961), 241–245.
5. B. W. Char, K. O. Geddes, G. H. Gonnet, et S. M. Watt. *MAPLE Reference Manual, Fourth Edition*. Symbolic Computation Group, Department of Computer Science, University of Waterloo, 1985.
6. H. Cohen. *A course in algorithmic algebraic number theory*. Graduate Texts in Mathematics. Springer–Verlag, 1993.
7. D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.
8. H. Davenport et H. Hasse. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. für die reine und angew. Math. 172* (1935), 151–182.
9. R. E. Giudici, J. B. Muskat, et S. F. Robinson. On the evaluation of Brewer's character sums. *Trans. Amer. Math. Soc. 171* (Sept. 1972), 317–347.
10. T. Hadano. Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor. *Proc. Japan Acad. 51* (1975), 92–95.
11. D. Husemöller. *Elliptic curves*, vol. 111 des *Graduate Texts in Mathematics*. Springer, 1987.
12. A. Joux et J. Stern. Lattice reduction: a toolbox for the cryptanalyst. In preparation, 1993.
13. S. Lang. *Elliptic curves, diophantine analysis*. Springer, 1978.
14. A. K. Lenstra, H. W. Lenstra, et L. Lovász. Factoring polynomials with rational coefficients. *Math. Annalen 261* (1982), 515–534.
15. P. A. Leonard et K. S. Williams. Jacobi sums and a theorem of Brewer. *Rocky Mountain Journal of Mathematics 5*, 2 (1975), 301–308. Erratum, 6, 1976, pp. 501.
16. F. Leprévost et F. Morain. Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. En préparation, nov 1993.
17. D. Masser. *Elliptic functions and transcendence*, vol. 437 des *Lect. Notes in Math.* Springer-Verlag, 1975.
18. B. Morlaye. Démonstration élémentaire d'un théorème de Davenport et Hasse. *Enseign. Math. 18* (1972), 269–276.
19. L. D. Olson. Conductors of elliptic curves. *J. of Number Thoery 8* (1976), 397–414.
20. J. Parnami, A. Rajwade, et D. Rishi. Évaluation of a cubic character sum using the $\sqrt{-19}$ division points of the curve $y^2 = x^3 - 2^3.19x + 2.19^2$. *J. Number Theory 19* (1984), 184–194.
21. J. C. Parnami, M. K. Agrawal, et A. R. Rajwade. Some identities involving character sums and their applications. *J. Indian Math. Soc., New. Series 54* (1989), 125–132.
22. J. C. Parnami et A. R. Rajwade. A new cubic character sum. *Acta Arithmetica XL* (1982), 347–356.
23. D. Poulakis. Évaluation d'une somme cubique de caractères. *J. Number Theory 27* (1987), 41–45.
24. A. R. Rajwade. Arithmetic on curves with complex multiplication by the Eisenstein integers. *Proc. Camb. Phil. Soc. 65* (1969), 59–73.
25. A. R. Rajwade. On rational primes congruent to 1 (mod 3 or 5). *Proc. Camb. Phil. Soc. 66* (1969), 61–70.
26. A. R. Rajwade. A note on the number of solutions N_p of the congruence $y^2 \equiv x^3 - dx \pmod{p}$. *Proc. Camb. Phil. Soc. 67* (1970), 603–605.
27. A. R. Rajwade. Certain classical congruences via elliptic curves. *J. London Math. Soc. 2*, 8 (1974), 60–62.
28. A. R. Rajwade. The diophantine equation $y^2 = x(x^2+21dx+112d^2)$ and the conjectures of Birch and Swinnerton-Dyer. *J. Australian Math. Soc. 24* (1977), 286–295. (Series A).
29. C.-P. Schnorr et M. Euchner. Lattice basis reduction: Improved practical algorithms and solving

subset sum problems. Dans *Proceedings of Fundamentals of Computation Theory 91* (New York, 1991), L. Budach, Réd., vol. 529 des *Lect. Notes in Computer Science*, Springer-Verlag, pp. 68–85.

30. S. Singh et A. R. Rajwade. The number of solutions of the congruence $y^2 = x^4 - a \pmod{p}$. *Enseign. Math. 20* (1974), 265–273.
31. H. M. Stark. Class-numbers of complex quadratic fields. Dans *Modular functions of one variable I* (1973), W. Kuyk, Réd., vol. 320 des *Lect. Notes in Math.*, Springer Verlag, pp. 155–174. Proceedings International Summer School University of Antwerp, RUCA, July 17-Agust 3, 1972.
32. A. L. Whiteman. A theorem of Brewer on character sums. *Duke Math. J. 30* (1963), 545–552.
33. K. S. Williams. Note on a cubic character sum. *Aequationes Mathematicae 12* (1975), 229–231.

(A. Joux) DGA/CELAR, Route de Laillé, 35170 Bruz, France

(F. Morain) Laboratoire d'Informatique de l'École polytechnique (LIX), F-91128 Palaiseau Cedex, France