Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères

F. Leprévost et F. Morain

F. Leprévost
Université Paris 7
Département de Mathmatiques
Tour 45-55, 5ème Étage
2 Place Jussieu
F-75252 Paris Cedex 05
FRANCE

F. Morain
Laboratoire de l'École Polytechnique (LIX)
F-91128 Palaiseau Cedex
FRANCE

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn
GERMANY

MPI/95-124

REVÊTEMENTS DE COURBES ELLIPTIQUES À MULTIPLICATION COMPLEXE PAR DES COURBES HYPERELLIPTIQUES ET SOMMES DE CARACTÈRES

F. LEPRÉVOST et F. MORAIN

RÉSUMÉ. Soit p un nombre premier impair et $\chi(x)$ le symbole de Legendre. Nous considérons les sommes de caractères $\Gamma_{p,n}(A,B) = \sum_x \chi(x(x^{2n} - Ax^n + B))$ et $\Delta_{p,n}(A,B) = \sum_x \chi((x^{2n} - Ax^n + B))$ pour A, B et n entiers. Nous étudions les propriétés de ces sommes et en donnons quelques valeurs particulières. Dans le cas $n = 2$, nous utilisons des revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques pour évaluer $\Gamma_{p,2}(\theta, 1)$. Nous appliquons ces résultats à l'algorithme ECPP.

1. INTRODUCTION

Dans cet article, p désigne un nombre premier impair et $\chi(x)$ le symbole de Legendre. Soit $P(X) = \sum_{r=0}^{m} a_r X^r$ un polynôme à coefficients dans $\mathbf{Z}$, de degré m, i.e. $a_m \neq 0$. On pose

$$S_p(P) = \sum_{x=0}^{p-1} \chi(P(x)) = \sum_{x=0}^{p-1} \left(\frac{P(x)}{p}\right).$$

Pour les valeurs de $m \leq 2$, les résultats sont connus. Pour $m = 0$, $S_p(P) = p\chi(a_0)$; pour $m = 1$, $S_p(P) = 0$; pour $m = 2$, $S_p(P) = -\chi(a_2)$ si $p \nmid a_1^2 - 4a_2a_0$, et $(p-1)\chi(a_2)$ sinon.

Quand $m = 3$ ou $m = 4$, les calculs sont intimement liés aux propriétés des courbes elliptiques et en particulier aux propriétés liées à la multiplication complexe. Dans le cas des courbes elliptiques à multiplication complexe définies sur $\mathbf{Q}$, il est possible d'évaluer ces sommes en fonction de la représentation de p par des formes quadratiques (voir par exemple [16] et les références citées).

Quand $m > 3$, les résultats sont partiels. Les cas les plus étudiés sont ceux des sommes de Jacobsthal

$$\Phi_{p,k}(a) = \sum_{x=0}^{p-1} \chi(x(x^k + a))$$

et les sommes reliées :

$$\Psi_{p,k}(a) = \sum_{x=0}^{p-1} \chi(x^k + a).$$

Nous renvoyons à [4, 13, 14, 20] (et les références qui y sont données) pour cela. Des sommes analogues aux sommes de Jacobsthal ont été calculées dans $\mathbf{F}_{p^2}$ par Berndt et Evans [3]. Brewer a considéré des sommes reliées à la suite des polynômes de Dickson (voir section 2).

Dans ce travail, nous introduisons les sommes de caractères

$$\Gamma_{p,n}(A,B) = S_p(X(X^{2n} - AX^n + B)), \quad \Delta_{p,n}(A,B) = S_p(X^{2n} - AX^n + B)$$

où A et B sont deux entiers et n un entier positif (nous nous autoriserons aussi dans la suite à considérer les sommes $\Gamma_{p,n}(A,B)$ avec A et B rationnels, du moment que les nombres premiers p considérés ne divisent pas les dénominateurs de A et B).

Date: 27 octobre 1995.

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

Dans la section suivante, outre la démonstration d'un lemme sur les sommes de caractères, que nous utilisons pour établir des résultats concernant les sommes $\Gamma_{p,n}$ et $\Delta_{p,n}$, nous rappelons un résultat de Brewer donnant une formule close pour $\Gamma_{p,2}(5Q, 5Q^2)$ dans le cas où p admet la décomposition $p = a^2+b^2 = u^2+5v^2$, avec a, b, u, v des nombres entiers relatifs. Il y est également rappelé quelques-unes des propriétés importantes de la théorie de la multiplication complexe et celle des fonctions de Weber. En particulier, si E est une courbe elliptique à multiplication complexe par un ordre $\mathcal{O}_z$ de conducteur m d'un corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-D})$ de discriminant $-D$, et d'équation $y^2 = f(x)$, on peut évaluer $S_p(f)$ en fonction de la représentation de p sous la forme $4p = U^2 + m^2DV^2$, où U et V sont des entiers vérifiant des conditions de normalisation. La recherche de ces conditions de normalisation est l'un des buts de ce travail.

La décomposition $p = a^2 + b^2 = u^2 + 5v^2$ traduit le fait que p se décompose dans le corps biquadratique $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$, qui est le corps de classe du corps quadratique $\mathbb{Q}(\sqrt{-20})$. Il est donc naturel de chercher un lien entre la courbe d'équation $y^2 = x(x^4 - 5Qx^2 + 5Q^2)$ et une courbe à multiplication complexe par l'anneau des entiers de $\mathbb{Q}(\sqrt{-20})$.

Dans cet esprit, nous nous concentrons ensuite sur le cas $\Gamma_{p,2}(\theta, 1)$. Dans la section 3, nous montrons, lorsque $\theta \neq \pm 2$, que la courbe C_θ d'équation $y^2 = x(x^4 - \theta x^2 + 1)$ est de genre 2, et que sa jacobienne est isogène au produit de deux courbes elliptiques E_θ et E'_θ, d'équations respectives $y^2 = P_\theta(x) = x(x^2 + 4x + 2 - \theta)$ et $y^2 = x(x^2 - 4x + 2 - \theta)$. Nous montrons que si θ prend des valeurs particulières s'exprimant comme fraction rationnelle en une des fonctions de Weber pour un nombre complexe z donné, alors E_θ a pour invariant $j(z)$. Nous en déduisons, dans la section 4 le résultat suivant :

Théorème 1. *Soit p un nombre premier impair et θ un élément de $\mathbb{F}_p$, différent de 2. Alors*

$$\Gamma_{p,2}(\theta, 1) = (1 + \chi(-1))S_p(P_\theta).$$

La section 5 applique ce théorème aux courbes E_θ à multiplication complexe, quand le nombre de classes de $\mathcal{O}_z$ est égal à 1 ou 2. En particulier, nous obtenons des formules closes pour certaines valeurs rationnelles de θ des quantités $\Gamma_{p,2}(\theta, 1)$ en fonction de la représentation de p par une forme quadratique de discriminant $-m^2D$. Nous en tirons également une nouvelle démonstration de formules connues pour $\Phi_{p,4}(a)$. Dans le cas où $D = 20$ (avec $\mathcal{O}_z = \mathcal{O}$, l'ordre principal de nombre de classes $h_z = 2$), on a $\theta = \sqrt{5}$, et les travaux de Brewer permettent de donner une formule close pour la somme de caractères $S_p(X(X^2+4X+2-\sqrt{5}))$. Nous concluons cet article par des remarques sur les cas D impair ou $h_z > 2$, et les applications à l'algorithme de primalité ECPP [1].

2. Préliminaires

Le but de cette section est d'abord de faire des rappels sur les sommes de Brewer, la multiplication complexe et les fonctions de Weber. Ensuite, nous donnons un lemme très général sur les sommes de caractères que nous utiliserons ensuite pour prouver des résultats sur les sommes $\Gamma_{p,n}$ et $\Delta_{p,n}$. Nous donnons également quelques propriétés élémentaires des sommes $\Gamma_{p,n}$.

2.1. Les sommes de Brewer.

2.1.1. *Définition et propriétés.* Soit Q un entier non nul. Les polynômes de Dickson $V_n(X, Q)$ sont définis par (cf. [19]) $V_0(X, Q) = 2$, $V_1(X, Q) = X$ et pour $n \geq 2$:

$$V_n(X, Q) = XV_{n-1}(X, Q) - QV_{n-2}(X, Q).$$

Les premières valeurs de cette suite sont :

$$V_2(X, Q) = X^2 - 2Q, V_3(X, Q) = X^3 - 3QX,$$

$$V_4(X, Q) = X^4 - 4QX^2 + 2Q^2, \quad V_5(X, Q) = X^5 - 5QX^3 + 5Q^2X.$$

Ces polynômes jouissent de propriétés particulières dans de multiples domaines (voir la référence citée). On pose $\Lambda_{p,n}(Q) = S_p(V_n(X,Q))$. Les valeurs de $\Lambda_{p,n}(1)$ pour $1 \leq n \leq 5$ sont calculées dans [7] et $\Lambda_{p,5}(Q)$ dans [8] ; un lien entre $\Lambda_{p,n}(Q)$ et $\Lambda_{p,2n}(Q)$ a été donné dans [24] et appliqué à la détermination de $\Lambda_{p,n}(Q)$ pour $n = 6$ et $n = 10$. On consultera [12] et [4] pour des extensions de ces travaux à certaines valeurs de $n \leq 18$.

2.1.2. *La somme* $\Lambda_{p,5}(Q)$. Notons que $\Lambda_{p,5}(Q) = \Gamma_{p,2}(5Q, 5Q^2)$. On rappelle alors les résultats suivants [7, 8] :

Théorème 2. *Soit p un nombre premier s'écrivant $p = a^2 + b^2 = u^2 + 5v^2$ avec a, b, u, v entiers relatifs (le signe de u sera fixé ci-dessous). Cela équivaut à $p \equiv r \bmod 20$, avec $r \in \{1, 9\}$. On suppose $a \equiv 1 \bmod 4$ et on pose $\varepsilon_{20}(p) = +1$ si $p \equiv 1 \bmod 20$ et -1 si $p \equiv 9 \bmod 20$. Soit Q un entier.*
Si $\chi(Q) = +1$, soit m une racine carrée de Q modulo p ; on a

$$\Lambda_{p,5}(Q) = \begin{cases} 0 & \text{si } a \equiv 0 \bmod 5; \\ -4u\chi(m)\varepsilon_{20}(p) & \text{si } u \equiv a \bmod 5, a \not\equiv 0 \bmod 5. \end{cases}$$

Si $\chi(Q) = -1$, on suppose que $b \equiv aQ^{(p-1)/4} \bmod p$; on a

$$\Lambda_{p,5}(Q) = \begin{cases} 0 & \text{si } a \not\equiv 0 \bmod 5; \\ -4u\varepsilon_{20}(p) & \text{si } u \equiv b \bmod 5, a \equiv 0 \bmod 5. \end{cases}$$

2.2. **Rappels sur la multiplication complexe.** On pourra consulter [11] (et éventuellement [6] et [10]) pour les résultats qui suivent.

Soient D un entier positif, $\mathbf{K} = \mathbb{Q}(\sqrt{-D})$ le corps quadratique imaginaire de discriminant $-D$ (ce qui veut dire que $D \equiv 0 \bmod 4$ ou $D \equiv 3 \bmod 4$ avec $D/4$ ou D sans facteur carré), $\mathcal{O}$ l'ordre principal de $\mathbf{K}$, et m un entier. On s'intéresse aux nombres complexes z vérifiant une des équations

$$z^2 + z + \frac{m^2 D + 1}{4} = 0$$

(avec dans ce cas $m^2 D \equiv 3 \bmod 4$) ou

$$z^2 + \frac{m^2 D}{4} = 0$$

(avec ici $m^2 D \equiv 0 \bmod 4$). On note $\mathcal{O}_z$ l'ordre de conducteur m ainsi engendré et h_z son nombre de classes (notons que si $m = 1$, alors $\mathcal{O}_z = \mathcal{O}$). Le corps de classe de $\mathcal{O}_z$ est le corps $\mathbf{K}_z = \mathbb{Q}(z, j(z))$ où j est l'invariant modulaire. Le nombre $j(z)$ est algébrique de degré h_z, de polynôme minimal sur $\mathbb{Q}$ noté $H_z(X)$. Si $m = 1$, on notera $H_z = \mathcal{W}_D$.

Notons $\mathcal{Q}$ la forme quadratique $(1, 1, (m^2 D + 1)/4)$ dans le premier cas et $(1, 0, m^2 D/4)$ dans le second, à laquelle z est naturellement associé. Alors $p > 3$ est représentable par $\mathcal{Q}$ si et seulement si p se décompose dans $\mathbf{K}_z$, ou encore $H_z(X)$ a une racine modulo p.

Soit E une courbe elliptique à multiplication complexe par $\mathcal{O}_z$, définie sur $\mathbb{Q}(j(z)) \subset \mathbf{K}_z$. Soit $\mathcal{O}_H$ l'anneau des entiers de $\mathbf{K}_z$. Supposons que p se décompose dans $\mathbf{K}_z$ et soit $\mathfrak{P}$ un idéal au-dessus de (p) dans $\mathbf{K}_z$, et donc $\mathcal{O}_H/\mathfrak{P} \simeq \mathbb{F}_p$. On a alors (voir par exemple [10, Theorem 14.16])

Théorème 3. *On suppose que E a bonne réduction modulo $\mathfrak{P}$ et on note $\overline{E}$ la courbe réduite. Alors il existe π dans $\mathcal{O}_z$ tel que $p = \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\pi)$ et $\#\overline{E}(\mathbf{F}_p) = \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\pi - 1)$. En outre, $\overline{E}$ est à multiplication complexe par $\mathcal{O}_z$. Réciproquement, toute courbe elliptique définie sur $\mathbb{F}_p$ à multiplication complexe par $\mathcal{O}_z$ est obtenue de cette façon.*

Quand ce théorème s'applique, on peut écrire $\pi = (U + mV\sqrt{-D})/2$ avec U et V éléments de $\mathbf{Z}$. On a alors $p = \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\pi) = (U^2 + m^2 D V^2)/4$ et $\#\overline{E}(\mathbb{F}_p) = p + 1 - U$. On en déduit facilement

que si l'équation de $\overline{E}$ est $y^2 = f(x)$, alors

$$S_p(f) = -U.$$

En normalisant $\mathfrak{P}$, il est possible de calculer une équation de $\overline{E}$. Ces calculs ont été explicités dans le cas où $h_z = 1$ (cf. [16] pour une bibliographie des travaux dans ce domaine), et nous verrons à la section 5.2 comment nos résultats fournissent la normalisation cherchée quand $D = 20$. Ce résultat sera appliqué à l'algorithme ECPP dans la section 6.1.

2.3. **Les fonctions de Weber.** Notons η la fonction de Dedekind

$$\eta(z) = \exp(2i\pi z/24) \prod_{n=1}^{\infty} (1 - \exp(2i\pi nz))$$

et

$$\mathfrak{f}(z) = e^{-i\pi/24} \frac{\eta((z+1)/2)}{\eta(z)}, \mathfrak{f}_1(z) = \frac{\eta(z/2)}{\eta(z)}, \mathfrak{f}_2(z) = \sqrt{2}\frac{\eta(2z)}{\eta(z)}$$

les fonctions de Weber. Elles vérifient entre autres l'identité

$$\mathfrak{f}(z)\,\mathfrak{f}_1(z)\,\mathfrak{f}_2(z) = \sqrt{2}.$$

Soit $\gamma_2(z)$ la racine cubique de $j(z)$, qui est réelle sur $i\mathbf{R}_+$. On a [28, §54, p. 179]

Théorème 4. *Les racines de l'équation* $x^3 - \gamma_2(z)x - 16 = 0$ *sont* $\mathfrak{f}(z)^8$, $-\mathfrak{f}_1(z)^8$, $-\mathfrak{f}_2(z)^8$.

Soit f une des fonctions de Weber. D'après le théorème précédent, $f(z)^{24}$ appartient à une extension cubique de $\mathbb{Q}(j(z))$. Dans certains cas, on a un résultat meilleur [28] (voir aussi [26]) :

Théorème 5. *Soit z un nombre algébrique vérifiant $az^2+bz+c = 0$, avec a entier, $-\mathcal{D} = b^2-4ac$, et $-\mathcal{D}$ différent de -3, -4, -7, -12, -15, -16. Si $\mathcal{D} \equiv 0 \bmod 4$, alors*

$$\begin{aligned}
\mathbb{Q}(\mathfrak{f}(z)^{24}) &= \mathbb{Q}(j(z)) \quad \text{si } a+b+c \equiv 0 \bmod 2, b \equiv 0 \bmod 2,\\
\mathbb{Q}(\mathfrak{f}_1(z)^{24}) &= \mathbb{Q}(j(z)) \quad \text{si } c \equiv 0 \bmod 2, b \equiv 0 \bmod 2,\\
\mathbb{Q}(\mathfrak{f}_2(z)^{24}) &= \mathbb{Q}(j(z)) \quad \text{si } a \equiv 0 \bmod 2, b \equiv 0 \bmod 2.
\end{aligned}$$

Si $\mathcal{D} \not\equiv 0 \bmod 4$, les fonctions de Weber engendrent le corps $\mathbb{Q}(z, j(z))$.

2.4. **Un lemme général sur les sommes de caractères.** Le lemme qui suit est implicite dans plusieurs des références citées dans l'introduction.

Lemme 1. *Soit $P(X) = \sum_{r=0}^{m} a_r X^r$ un polynôme à coefficients entiers ($a_m \neq 0$). Alors*

$$S_p(P(X^2)) = S_p(P(X)) + S_p(XP(X)).$$

Soit $P^*(X) = X^m P(1/X)$ le polynôme réciproque de P. Si m est impair, on a

$$S_p(XP(X)) = S_p(P^*(X)) - \chi(a_m).$$

Si m est pair, on a

$$S_p(P(X)) = S_p(P^*(X)) + \chi(a_0) - \chi(a_m).$$

Démonstration : On écrit

$$S_p(P(X^2)) = \sum_{x=0}^{p-1} \chi(P(x^2)) = \sum_{x=0}^{p-1} \sum_{y=x^2 \bmod p} \chi(P(y)) = \sum_{x=0}^{p-1} (1+\chi(x))\chi(P(x)) = S_p(P(X)) + S_p(XP(X)),$$

ce qui prouve la première formule.
Supposons $m = 2n+1$. Alors

$$S_p(XP(X)) = \sum_{x=1}^{p-1} \chi(xP(x)) = \sum_{x=1}^{p-1} \chi(x^{2n+2}P^*(1/x)) = S_p(P^*(X)) - \chi(a_m).$$

Si $m = 2n$, on a

$$S_p(P(X)) = \chi(a_0) + \sum_{x=1}^{p-1} \chi(x^{2n} P^*(1/x)) = S_p(P^*(X)) + \chi(a_0) - \chi(a_m).\square$$

2.5. **Quelques résultats sur les sommes $\Gamma_{p,n}$ et $\Delta_{p,n}$.** Notons (a, b) le pgcd de deux entiers naturels a et b. L'objet de cette section est de démontrer les résultats suivants :

Proposition 1. *Pour $p > 2$, A et B entiers, on a*
(i) $\Gamma_{p,0}(A, B) = 0$;
(ii) $\Gamma_{p,n}(0, B) = \Phi_{p,2n}(B)$;
(iii) $\Delta_{p,2n}(A, B) = \Delta_{p,n}(A, B) + \Gamma_{p,n}(A, B)$;
(iv) si $(p-1)/(p-1, n)$ est impair, on a $\Gamma_{p,n}(A, B) = 0$;
(v) pour tout a, $\Gamma_{p,n}(2a, a^2) = -\sum_{x^n=a} \chi(x)$.

Démonstration : Les deux premiers points sont évidents. Le point (iii) est une application du lemme 1. Pour démontrer le point (iv), posons $d = (p-1)/(p-1, n)$ et $k = (p-1)/d$. Soit g un générateur de $\mathbb{F}_p$. On écrit :

$$\Gamma_{p,n}(A, B) = \sum_{i=1}^{p-1} \chi(g^i((g^{2n})^i - A(g^n)^i + B)).$$

Comme l'ordre de g^n est d, il vient

$$\Gamma_{p,n}(A, B) = \left(1 + \chi(g^d) + \chi(g^{2d}) + \cdots + \chi(g^{(k-1)d})\right) \sum_{i=1}^{d} \chi(g^{2ni} - Ag^{ni} + B).$$

Si d est impair, k est pair et il y a autant de termes égaux à 1 et à -1 dans la première somme, donc elle est nulle et le résultat en découle.
Pour le point (v), on a

$$\Gamma_{p,n}(2a, a^2) = \sum_{x=0}^{p-1} \chi(x(x^n - a)^2) = \sum_{x^n \neq a} \chi(x) = -\sum_{x^n = a} \chi(x).\square$$

Nous utiliserons souvent le résultat suivant :

Proposition 2. *Pour tout A et B, on a*

$$\Gamma_{p,n}(Am^n, Bm^{2n}) = \chi(m)\Gamma_{p,n}(A, B).$$

et son corollaire :

Corollaire 1. *Si $B = \beta^{2n} \bmod p$ avec $\beta \in \mathbb{F}_p$, alors* $\Gamma_{p,n}(A, B) = \chi(\beta^n)\Gamma_{p,n}(A/\beta^n, 1)$.

Les valeurs de $\Gamma_{p,1}$ ne sont pas toutes connues. Il est clair que $p + 1 - \Gamma_{p,1}(A, B)$ compte le nombre de points sur la réduction modulo p de la courbe $E : y^2 = x(x^2 - Ax + B)$. Quand E est à multiplication complexe par un anneau d'entiers de corps quadratique imaginaire de nombre de classes 1, on peut évaluer ces sommes en fonctions de la représentation de p par une forme quadratique (voir [16] et les références citées ; voir aussi la section 2.2).

Le reste de l'article traite essentiellement des sommes $\Gamma_{p,2}(\theta, 1)$ avec θ dans $\mathbb{F}_p$. Notons que l'application du corollaire 1 permet d'en déduire les valeurs de $\Gamma_{p,2}(A, B)$ avec $A/\sqrt{B} = \theta$. En outre, nous supposerons dans la suite que $\theta \neq 2$ car l'application de la proposition 1 nous fournit $\Gamma_{p,2}(2, 1) = -1 - \chi(-1)$.

3. La courbe C_θ

Notons, pour $\theta \in \mathbb{C}$, $F_\theta(x) = x(x^4 - \theta x^2 + 1)$ et $P_\theta(X) = X(X^2 + 4X + 2 - \theta)$. Nous montrons ici le

Théorème 6. *Soit $\theta \neq \pm 2$ un nombre complexe. Alors la courbe C_θ d'équation*

$$y^2 = F_\theta(x)$$

est de genre 2. De plus, soient E_θ et E'_θ les courbes elliptiques d'équations

$$\begin{array}{rcl} E_\theta & : & Y^2 = X(X^2 + 4X + 2 - \theta), \\ E'_\theta & : & Y^2 = X(X^2 - 4X + 2 - \theta). \end{array}$$

Alors la jacobienne de C_θ est isogène à $E_\theta \times E'_\theta$ sur $\mathbb{Q}(\theta)$, et à E_θ^2 sur $\mathbb{Q}(i, \theta)$.

Notons en effet $\omega_1 = \frac{dx}{y}$ et $\omega_2 = \frac{x dx}{y}$ une base de $\Omega^{1,0}(C_\theta)$, l'espace des formes différentielles de première espèce de C_θ. Le calcul montre que les images réciproques des différentielles de première espèce, $\omega = \frac{dX}{Y}$ et $\omega' = \frac{dX}{Y}$, des courbes E_θ et E'_θ par les morphismes φ et ψ de C_θ sur, respectivement, E_θ et E'_θ, définis par :

$$\varphi(x, y) = \left((2 - \theta)\frac{x}{(x-1)^2}, (2 - \theta)\frac{y}{(x-1)^3} \right),$$

et

$$\psi(x, y) = \left((2 - \theta)\frac{x}{(x+1)^2}, (2 - \theta)\frac{y}{(x+1)^3} \right),$$

sont

$$\varphi^*(\omega) = -\omega_1 - \omega_2 \qquad \text{et} \qquad \psi^*(\omega') = \omega_1 - \omega_2.$$

Elles sont indépendantes et engendrent $\Omega^{1,0}(C_\theta)$. Par conséquent, la jacobienne de C_θ est $\mathbb{Q}(\theta)$-isogène à $E_\theta \times E'_\theta$. Comme E_θ et E'_θ sont isomorphes *via* l'application $(X, Y) \longrightarrow (-X, iY)$, la jacobienne de C_θ est $\mathbb{Q}(i, \theta)$-isogène à E_θ^2. □

Une application directe d'un théorème de Shioda et Mitani ([25, p. 296] ou [27, p. 271]) établit le

Corollaire 2. *Si E_θ est à multiplication complexe, la jacobienne de C_θ est isomorphe à un produit de courbes elliptiques.*

Remarque : Les courbes de genre 2 munies d'un automorphisme différent de l'involution hyperelliptique, comme c'est ici le cas pour C_θ, cet automorphisme étant $(x, y) \longrightarrow (-x, iy)$, ont été classifiées par Bolza (*cf.* [5]).

On en déduit alors le résultat annoncé dans l'introduction :

Théorème 7. *Soit $E = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ une courbe elliptique d'invariant $j(\tau)$. Alors E admet un revêtement par la courbe de genre 2 d'équation $y^2 = x(x^4 - \theta x^2 + 1)$ où θ est l'un des nombres*

$$\Theta(\tau) = 2\frac{\mathfrak{f}(\tau)^{24} + 2^6}{\mathfrak{f}(\tau)^{24} - 2^6},\ \Theta_1(\tau) = 2\frac{\mathfrak{f}_1(\tau)^{24} - 2^6}{\mathfrak{f}_1(\tau)^{24} + 2^6},\ \Theta_2(\tau) = 2\frac{\mathfrak{f}_2(\tau)^{24} - 2^6}{\mathfrak{f}_2(\tau)^{24} + 2^6}$$

si $j \neq 1728$, et

$$-\frac{14}{9} = \Theta_1(i) 2\frac{\mathfrak{f}_1(i)^{24} - 2^6}{\mathfrak{f}_1(i)^{24} + 2^6} = \Theta_2(i) = 2\frac{\mathfrak{f}_2(i)^{24} - 2^6}{\mathfrak{f}_2(i)^{24} + 2^6}$$

sinon.

Démonstration: D'après le théorème précédent, si $\theta \neq \pm 2$, la courbe elliptique E_θ admet un revêtement par la courbe C_θ, qui est de genre 2. Or E est isomorphe à E_θ si et seulement si leurs invariants modulaires sont égaux, *i.e.*

$$j(\tau) = j(E_\theta) = \frac{64(3\theta+10)^3}{(\theta-2)^2(\theta+2)}.$$

Comme $\theta \neq \pm 2$, il existe $\lambda \neq 0$ tel que $\theta = 2(\lambda^3+1)/(\lambda^3-1)$. Écrivant $j(\tau) = \gamma_2(\tau)^3$, on doit résoudre :

$$\gamma_2(\tau)^3 = \frac{64\,(4\,\lambda^3-1)^3}{\lambda^3}$$

ou encore

$$(4\lambda)^3 - \gamma_2(\tau)(4\lambda) - 16 = 0$$

et on utilise alors le théorème 4. □

Corollaire 3. *Soit z un nombre complexe associé à un ordre $\mathcal{O}_z$ de $\mathbf{K}$. Alors la courbe d'équation $y^2 = P_\theta(x)$ où θ est l'un des nombres $\Theta(z)$, $\Theta_1(z)$ ou $\Theta_2(z)$, est à multiplication complexe par $\mathcal{O}_z$.*

4. Démonstration du théorème 1

Soit θ un élément de $\mathbf{F}_p$, différent de 2. On a

$$S_p(F_\theta) = \sum_{x=0}^{p-1} \chi(F_\theta(x)) = \chi(F_\theta(1)) + \sum_{x\neq 1} \chi(F_\theta(x)).$$

Notons $G(x) = (x-1)[(2-\theta)x^2 + 2(6+\theta)x + 2 - \theta]$. Pour $x \neq 1$, on a :

$$G\left(\left(\frac{x+1}{x-1}\right)^2\right) = \frac{64}{(x-1)^6} F_\theta(x),$$

si bien que

$$S_p(F_\theta) = \chi(F_\theta(1)) + \sum_{x\neq 1} \chi(G(x^2)) = \chi(F_\theta(1)) + \chi(G(0)) + \sum_{x=1}^{p-1} \chi(G(x^2)),$$

en remarquant que $G(1) = 0$. D'après le lemme 1, on a

$$\sum_{x=1}^{p-1} \chi(G(x^2)) = \sum_{x=1}^{p-1} \chi(G(x)) + \sum_{x=1}^{p-1} \chi(xG(x)).$$

De plus, $G^* = -G$, et le lemme 1 implique également

$$\sum_{x=1}^{p-1} \chi(xG(x)) = \chi(-1) \sum_{x=1}^{p-1} \chi(G(x)).$$

Par conséquent,

$$\sum_{x=1}^{p-1} \chi(G(x^2)) = (1+\chi(-1)) \sum_{x=1}^{p-1} \chi(G(x)),$$

donc, comme $G(0) = -F_\theta(1)$, on a

$$S_p(F_\theta) = (1+\chi(-1))S_p(G) = (1+\chi(-1))S_p(P_\theta). \square$$

Le théorème 1 permet de connecter deux sommes de caractères. Les résultats que nous allons en déduire sont de deux types. Le premier est celui où nous savons évaluer la somme «elliptique» $S_p(P_\theta)$ et donc nous en déduisons la somme «hyperelliptique» $\Gamma_{p,2}(\theta, 1)$. L'autre type correspond au calcul en sens inverse.

5. Applications aux cas des courbes à multiplication complexe

Dans la suite, E_θ sera toujours à multiplication complexe par un ordre $\mathcal{O}_z$ d'un corps quadratique imaginaire $\mathbf{K}$, z le nombre complexe associé à $\mathcal{O}_z$. La courbe E_θ est donc définie sur $\mathbb{Q}(j(z))$. Remarquons que E_θ a nécessairement un point d'ordre 2 dont l'abscisse est dans le corps de définition. À chaque fois que l'on peut appliquer le théorème 5, on sait que E_θ et C_θ sont définies sur $\mathbb{Q}(j(z))$. Nous nous limitons au cas $h_z \leq 2$.

5.1. **Cas où $h(\mathcal{O}_z) = 1$.** Il y a 9 ordres principaux de nombre de classe 1 et 4 non principaux. Les courbes elliptiques associées sont définies sur $\mathbb{Q}(j(z)) = \mathbb{Q}$. Dans 7 cas, une des fonctions de Weber, f, est telle que $f(z)^{24} \in \mathbb{Q}$. Le théorème 5 ne s'applique pas directement, mais on trouve [28, Tabelle VI] les valeurs qui nous intéressent [1]. Dans certains cas, on a utilisé la formule

$$\mathfrak{f}(z)\mathfrak{f}_2((z+1)/2) = e^{i\pi/24}\sqrt{2}.$$

On donne dans la table 1 les valeurs des discriminants, conducteurs des ordres ainsi que les valeurs correspondantes de θ.

D	m	z	f	$f(z)^{24}$	θ
3	1	$(-1+\sqrt{-3})/2$	$\mathfrak{f}_2$	-2^4	$-10/3$
3	2	$\sqrt{-3}$	$\mathfrak{f}$	2^8	$10/3$
4	1	i	$\mathfrak{f}$	2^6	$-14/9$
4	2	$2i$	$\mathfrak{f}_1$	2^9	$14/9$
7	1	$(-1+\sqrt{-7})/2$	$\mathfrak{f}_2$	-1	$-130/63$
7	2	$\sqrt{-7}$	$\mathfrak{f}$	2^{12}	$130/63$
8	1	$\sqrt{-2}$	$\mathfrak{f}_1$	2^6	0

Table 1 -

On peut en déduire des résultats sur les sommes $\Gamma_{p,2}(\theta, 1)$. Notons que le calcul de $\Gamma_{p,2}(-\theta, 1)$ se fait à l'aide de la proposition 1, une fois connue la valeur de $\Gamma_{p,2}(\theta, 1)$.

5.1.1. *Le cas $D = 3$.*

Théorème 8. *Soit $p \equiv 1 \bmod 12$. On pose $\omega = (-1+\sqrt{-3})/2$. Le nombre p se décompose sous la forme $\pi\overline{\pi}$ avec $\pi = a + b\omega$, ou encore $p = a^2 - ab + b^2$. On suppose que $a \equiv 2 \bmod 3$, $b \equiv 0 \bmod 3$. On pose*

$$\xi = 2^{(p-1)/3} \bmod \pi.$$

(On remarque que $\xi \in \{1, \omega, \omega^2\}$.) Alors

$$\Gamma_{p,2}(-10/3, 1) = 2(\overline{\xi}\pi + \xi\overline{\pi}).$$

Démonstration : Le changement de variable $(x = 4X - 4/3, y = 8Y)$ montre que $E_{-10/3}$ est isomorphe à la courbe d'équation $Y^2 = X^3 - 1/3^3$. On utilise alors [15, Théorème 4 p. 304], qui nous donne

$$S_p(X^3 - 1/3^3) = \overline{\xi}\pi + \xi\overline{\pi}.$$

Le résultat en découle. □

Exemple. Prenons $p = 181 = 11^2 - 11 \times 15 + 15^2$. On trouve $2^{(p-1)/3} \equiv 48 \bmod p$, ce qui conduit à $\xi = \omega^2$ et $\Gamma_{p,2}(-10/3, 1) = -52$.

1. Notons que la valeur de $\mathfrak{f}_1(2i)$ est erronée : la valeur correcte est $8^{1/8}$ et non $8^{1/3}$.

5.1.2. *Le cas $D = 4$.*

Théorème 9. *Soit $p \equiv 1 \bmod 4$. On peut écrire $p = u^2 + v^2$, avec $u \equiv 1 \bmod 2$, $v \equiv 0 \bmod 2$ et $u - v \equiv 1 \bmod 4$. Alors*

$$\Gamma_{p,2}(-14/9, 1) = -4\chi(3)u.$$

Démonstration : La courbe $E_{-14/9}$ est isomorphe à la courbe $Y^2 = X^3 - 1/3^6 X$ via $(x = 36X - 4/3, y = 6^3 Y)$. On utilise par exemple [15, Théorème 5 p. 307] pour évaluer d'abord :

$$S_p(X^3 - 1/3^6 X) = -2\chi(3)u$$

et le résultat en découle. □

5.1.3. *Le cas $D = 7$.*

Théorème 10. *On écrit $p = u^2 + 7v^2$, avec $u \equiv 1, 4, 2 \bmod 7$ si $p \equiv 1, 9, 11 \bmod 14$. Dans le cas où $p \equiv 1 \bmod 4$, $p \nmid 63$, on a*

$$\Gamma_{p,2}(-130/63, 1) = -4\chi(21)u.$$

Démonstration : L'équation de $E_{-130/63}$ est :

$$y^2 = x\left(x^2 + 4x + \frac{256}{63}\right)$$

ou encore

$$y^2 = x(x^2 + 21cx + 112c^2)$$

avec $c = 4/21$. On applique alors le théorème de [23] qui nous donne directement

$$S_p(P_{-130/63}) = -2\chi(c)u = -2\chi(21)u$$

et le résultat suit. □

5.1.4. *Le cas $D = 8$.*

Théorème 11. *Soit $p = 8F + 1 = c^2 + 2d^2$, $c \equiv -1 \bmod 4$. Si B est un résidu octique modulo p, alors*

$$\Phi_{p,4}(B) = \Gamma_{p,2}(0, B) = 4(-1)^F c.$$

Si B est un résidu quartique, mais pas un résidu octique, alors

$$\Phi_{p,4}(B) = \Gamma_{p,2}(0, B) = -4(-1)^F c.$$

Démonstration : L'équation la plus générale d'une courbe à multiplication complexe par $\mathbf{Z}[\sqrt{-2}]$ (voir [21]) est

$$y^2 = x(x^2 - 4\vartheta x + 2\vartheta^2)$$

pour laquelle la somme de caractères correspondante vaut (cf. [22])

$$S_p(X(X^2 - 4\vartheta X + 2\vartheta^2)) = -2\chi(\vartheta)(-1)^F c.$$

Il suffit de constater que la courbe E_0 est isomorphe à la courbe précédente avec $\vartheta = -1$.
Si B est un résidu octique, le corollaire 1 s'applique et le résultat du théorème est vrai. Si B est un résidu quartique, sans être un résidu octique, on peut trouver m tel que Bm^4 soit un résidu octique (et $\chi(m) = -1$). On applique alors le résultat précédent à Bm^4 et on conclut en appliquant la formule [17, p. 104] :

$$\Phi_{p,4}(Bm^4) = \chi(m)^3 \Phi_{p,4}(B). \square$$

Notons que notre approche ne nous donne pas de résultat dans les cas où B n'est pas au moins un résidu quartique. Pour ces résultats, voir [4, Théorème 4.6].

5.2. **Le cas $h(\mathcal{O}_z) = 2$.**

5.2.1. *Résultats généraux.* Il y a 19 ordres principaux et 11 non principaux. Dans chacun des cas, $j(z)$ est algébrique de degré 2. En fait, $j(z)$ appartient à un corps quadratique réel $\mathbb{Q}(\varpi)$. La table 2 donne les valeurs de D, m, $\xi(z)$ où $\xi(z)$ est tel que $\mathbb{Q}(\xi(z)) = \mathbb{Q}(j(z))$ (valeurs[2] prises dans [28]) et les valeurs correspondantes de θ dans chacun des cas où le théorème 5 s'applique et où la courbe elliptique d'invariant $j(z)$ a un point d'ordre 2. Remarquons que dans tous les cas $z = \sqrt{-m^2 D/4}$.

D	m	ϖ	$\xi(z)$	θ
3	4	$\sqrt{3}$	$\mathfrak{f}_1^{24} = 2^7(1+\varpi)^6$	$(170+320\varpi)/3$
4	3	$\sqrt{3}$	$\mathfrak{f}^{12} = 2(1+\varpi)^4$	$7\varpi/6$
4	4	$\sqrt{2}$	$\mathfrak{f}_1^8 = 2^3\varpi(1+\varpi)^2$	$(-114+704\varpi)/441$
4	5	$\sqrt{5}$	$8\mathfrak{f}^4 = (1+\varpi)^4$	$161\varpi/180$
7	4	$\sqrt{7}$	$\mathfrak{f}_1^8 = 2^3(3+\varpi)^2$	$(910+21760\varpi)/29241$
8	2	$\sqrt{2}$	$\mathfrak{f}_1^8 = 8+8\varpi$	$(-130+160\varpi)/49$
8	3	$\sqrt{6}$	$\mathfrak{f}_1^{12} = 2(2+\varpi)^4$	$40\varpi/49$
15	2	$\sqrt{5}$	$\mathfrak{f}^6 = 2(1+\varpi)^2$	$(2730-896\varpi)/363$
20	1	$\sqrt{5}$	$\mathfrak{f}^4 = 1+\varpi$	ϖ
24	1	$\sqrt{2}$	$\mathfrak{f}_1^6 = 4+2\varpi$	$4\varpi/3$
40	1	$\sqrt{5}$	$\sqrt{2}\mathfrak{f}_1^2 = 1+\varpi$	$8\varpi/9$
52	1	$\sqrt{13}$	$\mathfrak{f}^4 = 3+\varpi$	$5\varpi/9$
88	1	$\sqrt{2}$	$\mathfrak{f}_1^2 = \varpi(1+\varpi)$	$140\varpi/99$
148	1	$\sqrt{37}$	$\mathfrak{f}^4 = 2(6+\varpi)$	$145\varpi/441$
232	1	$\sqrt{29}$	$\sqrt{2}\mathfrak{f}_1^2 = 5+\varpi$	$3640\varpi/9801$

TABLE 2 -

Soit z associé à un couple (D, m) de la table 2 et θ le nombre associé. Soit p un nombre premier qui se décompose dans $\mathbf{K}_z$. Alors $\theta \in \mathbb{F}_p$ et par suite, on obtient une identité entre deux sommes de caractères définies sur $\mathbb{F}_p$.

Remarque. L'examen de la table 2 montre que dans certains cas, θ est de trace nulle dans $\mathbb{Q}(\varpi)$. Il existe donc deux entiers rationnels A et B tels que $A/\sqrt{B} = \theta$ et on peut donc évaluer les sommes $\Gamma_{p,2}(A, B)$ en utilisant le théorème 1 et le corollaire 1.

5.2.2. *Le cas $D = 20$.* Le corps $\mathbf{K}_z$ est ici $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$. Un nombre premier p se décompose dans $\mathbf{K}_z$ si et seulement s'il s'écrit sous la forme $p = a^2 + b^2 = u^2 + 5v^2$. D'après la table 2, la valeur correspondante de θ est $\sqrt{5}$, ce qui permet de connecter la somme de caractère liée à $E_{\sqrt{5}}$ à $\Lambda_{p,5}(1/\sqrt{5})$:

Théorème 12. *Soit $\varpi = \sqrt{5} \bmod p$ et $Q = 1/\varpi \bmod p$. Avec les normalisations du théorème 2, on obtient :*

$$\Sigma_p = S_p(X(X^2 + 4X + 2 - \varpi)) = -\varepsilon_{20}(p)\,\varepsilon(Q)\,(2u)$$

où $\varepsilon(Q)$ vaut $(Q/p)_4$ si $\chi(Q) = 1$ et 1 sinon.

2. Noter que la valeur de $\mathfrak{f}_1(\sqrt{-18})^3$ est $2^{1/4}(2+\sqrt{6})$ et non $2^{1/2}(2+\sqrt{6})$.

Démonstration: On remarque que $\chi(Q) = (5/p)_4$. D'après [18], on a $(5/p)_4 = 1$ si et seulement si $b \equiv 0 \bmod 5$. Si $(5/p)_4 = -1$, alors $b \not\equiv 0 \bmod 5$, ce qui implique $a \equiv 0 \bmod 5$. Il suffit alors de combiner le corollaire 1 avec le théorème 2. □

Exemples numériques. Nous allons donner des exemples numériques qui illustrent le théorème 12. Les calculs ont été faits à l'aide de `PARI-gp` [2].

p	$p \bmod 20$	a	$\lvert b\rvert$	$\lvert u\rvert$	ϖ	Q	$\chi(Q)$	$\varepsilon(Q)$	b	u	Σ_p
101	1	1	10	9	45	9	+1	−1	10	−9	−18
401	1	1	20	9	178	196	+1	+1	20	−9	18
521	1	−11	20	21	199	144	+1	−1	20	−21	−42
61	1	5	6	4	26	54	−1	1	6	−4	8
41	1	5	4	6	13	19	−1	1	−4	6	−12
109	9	−3	10	8	21	26	+1	+1	10	−8	−16
409	9	−3	20	2	150	30	+1	+1	20	2	4
929	9	−23	20	18	61	198	+1	−1	−20	−18	36
29	9	5	2	3	11	8	−1	1	−2	3	6
89	9	5	8	3	19	75	−1	1	−8	−3	−6

6. Remarques complémentaires

6.1. **Application à l'algorithme ECPP.** L'algorithme ECPP permet de prouver la primalité d'un entier N en utilisant les courbes elliptiques à multiplication complexe. Exposons de façon simplifiée son mécanisme, les détails se trouvant dans [1]. L'idée est de tout faire comme si N était premier. On commence par chercher à exprimer N comme la norme d'un entier π dans un corps quadratique imaginaire $\mathbf{K} = \mathbb{Q}(\sqrt{-D})$. Si on y parvient, on calcule alors $M = \mathrm{N}_{\mathbf{K}/\mathbb{Q}}(\pi - 1)$ que l'on factorise. Si N est premier, alors M est le nombre de points sur $\mathbf{Z}/N\mathbf{Z}$ d'une courbe elliptique E, à multiplication complexe par $\mathcal{O}$, dont l'invariant j est racine de $\mathcal{W}_D$ modulo N. On calcule une ce des racines et il ne reste plus qu'à trouver une équation de E et à prouver que N est premier en exhibant un élément d'ordre suffisamment grand de $E(\mathbf{Z}/N\mathbf{Z})$. Au cas où l'une des étapes de l'algorithme ne fonctionne pas, c'est que N n'est pas premier.

Dans $\mathbf{F}_p$, on sait que l'invariant modulaire ne suffit pas à classifier complètement les courbes elliptiques. Plus précisément, si $\mathcal{E}$ a pour équation $y^2 = x^3 + a_2x^2 + a_4x + a_6$, toute courbe $\mathcal{E}_c$ d'équation $y^2 = x^3 + a_2cx^2 + a_4c^2x + a_6c^3$, c dans $\mathbf{F}_p$, à même invariant. Si $p + 1 - t$ est le cardinal de $\mathcal{E}$, alors $\mathcal{E}_c$ est isogène à $\mathcal{E}$ si c est un carré dans $\mathbf{F}_p$ et est une tordue de $\mathcal{E}$ sinon, ayant pour cardinal $p + 1 + t$.

Dans ECPP, étant donnés j et M, il faut déterminer une équation de la courbe E. La façon la plus simple de procéder consiste à construire une équation de E sous la forme

$$\mathcal{E} : y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j}.$$

On choisit un point P sur $\mathcal{E}$ et on teste si $MP = O_{\mathcal{E}}$. Si non, on utilise une tordue de $\mathcal{E}$. Si $MP \neq O_{\mathcal{E}_c}$, N n'est pas premier. Sinon on a trouvé une équation de E et on peut poursuivre le reste de l'algorithme. En moyenne, il faut donc essayer 1.5 courbes.

Expliquons comment faire mieux dans le cas $D = 20$. Dans ce cas, on connait l'équation d'une courbe elliptique $E_{\sqrt{5}}$ à multiplication complexe par $\mathcal{O}$, ainsi que la normalisation permettant de calculer son nombre de points. À l'aide de l'écriture de N sous la forme $N = a^2 + b^2 = u^2 + 5v^2$ avec les conditions de normalisation du théorème 12, on calcule alors $\#E_{\sqrt{5}}(\mathbf{Z}/N\mathbf{Z})$ et on compare cette valeur avec celle de M choisie par ECPP. Si ces deux valeurs coïncident, l'équation de $E_{\sqrt{5}}$ convient, sinon il suffit de considérer l'équation de la tordue. Ce calcul n'est pas couteux, car on calcule $\sqrt{5}$ à partir de $\sqrt{-1} \equiv a/b \bmod N$ et $\sqrt{-5} \equiv u/v \bmod N$.

Plus généralement, pour certaines valeurs de D, on connait des équations de courbes à multiplication complexe par $\mathcal{O}$, ainsi qu'une formule de calcul de leur cardinal en fonction de conditions de normalisation portant sur p. C'est le cas par exemple quand $h(-D) = 1$ (voir par exemple [16] et les articles cités dans sa bibliographie) et pour $D = 15$ (cf. [9]).

6.2. **Les autres où cas $h = 2$.** La démonstration du théorème de Brewer ne se généralise pas aux cas $(A, B) \neq (5, 5)$. Cependant, notre approche montre que les sommes de caractères ainsi construites ont pour valeur $\pm U$ où $p = (U^2 + m^2 DV^2)/4$.
Dans [9] est entrepris le traitement des cas où D est impair avec une méthode analogue à celle développée dans [16].

6.3. **Le cas $h > 2$.** Dans les cas où le théorème 5 s'applique, on peut relier des sommes de caractères de courbes elliptiques à multiplication complexe à des sommes de caractères liées à des courbes de genre 2, mais qui ne sont plus définies sur $\mathbf{Q}$. À notre connaissance, aucun résultat n'est connu pour de telles sommes.

Remerciements. Les auteurs tiennent à remercier Don B. Zagier pour ses nombreuses suggestions qui ont conduit à simplifier l'exposition des résultats contenus dans cet article. Le premier auteur exprime sa gratitude au Max-Planck-Institut für Mathematik pour son hospitalité.

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 paquet gp.
[3] B. C. Berndt et R. J. Evans. Sums of Gauss, Eisenstein, Jacobi, Jacobsthal and Brewer. *Illinois J. Math. 23*, 3 (1979), 374–437.
[4] B. C. Berndt et R. J. Evans. Sums of Gauss, Jacobi and Jacobsthal. *J. Number Theory 11* (1979), 349–398.
[5] O. Bolza. On binary sextics with linear transformations onto themselves. *Amer. J. Math. 10* (1888), 47–70.
[6] 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.
[7] B. W. Brewer. On certain character sums. *Trans. Amer. Math. Soc. 99* (1961), 241–245.
[8] B. W. Brewer. On primes of the form $u^2 + 5v^2$. *Proc. Amer. Math. Soc. 17* (1966), 502–509.
[9] J.-M. Couveignes, A. Joux, et F. Morain. Sur quelques sommes de caractères. En préparation, Fev. 1994.
[10] D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.
[11] M. Deuring. Die Klassenkörper der komplexen Multiplikation. In *Enzyklopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen*, vol. Bd 1, H. 10, T. 2. Teubner, Stuttgart, 1958.
[12] 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.
[13] R. H. Hudson et K. S. Williams. An application of a formula of Western to the evaluation of certain Jacobsthal sums. *Acta Arithmetica XLI*, 3 (1982), 261–276.
[14] R. H. Hudson et K. S. Williams. Resolution of ambiguities in the evaluation of cubic and quartic Jacobsthal sums. *Pacific Journal of Mathematics 99*, 2 (1982), 379–386.
[15] K. Ireland et M. Rosen. *A classical introduction to modern number theory*, vol. 84 des *Graduate Texts in Mathematics*. Springer, 1982.
[16] A. Joux et F. Morain. Évaluation des sommes de caractères liées aux courbes elliptiques à multiplication complexe. Rapport de Recherche LIX/RR/93/11, Laboratoire d'Informatique de l'Ecole Polytechnique (LIX), 1993. À paraître dans *J. Number Theory*.
[17] E. Lehmer. On the number of solutions of $u^k + d \equiv w^2 \bmod p$. *Pacific Journal of Mathematics 5* (1955), 103–18.
[18] E. Lehmer. Criteria for cubic and quartic residuacity. *Mathematika 5* (1958), 20–29.
[19] R. Lidl, G. L. Mullen, et G. Turnwald. *Dickson polynomials*, vol. 65 des *Pitman Monographs and Surveys in Pure and Applied Mathematics*. Longman Scientific & Technical, 1993.
[20] M. G. Monzingo. An elementary evaluation of the Jacobsthal sum. *J. Number Theory 22* (1986), 21–25.
[21] A. R. Rajwade. Arithmetic on curves with complex multiplication by $\sqrt{-2}$. *Proc. Cambridge Philos. Soc. 64* (1968), 659–672.
[22] A. R. Rajwade. Certain classical congruences via elliptic curves. *J. London Math. Soc. 2*, 8 (1974), 60–62.

[23] 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).

[24] S. F. ROBINSON. Theorems on Brewer sums. *Pacific Journal of Mathematics 25*, 3 (1968), 587–596.

[25] W. M. RUPPERT. When is an abelian surface isomorphic or isogeneous to a product of elliptic curves? *Math. Z. 203* (1990), 293–299.

[26] R. SCHERTZ. Die singulären Werte der Weberschen Funktionen f, f_1, f_2, γ_2, γ_3. *J. für die reine und angew. Math. 286-287* (1976), 46–74.

[27] T. SHIODA ET N. MITANI. Singular abelian surfaces and binary quadratic forms. Dans *Classification of algebraic varieties and compact complex manifolds* (1974), H. Popp, Réd., vol. 412 des *Lect. Notes in Math.*, Springer-Verlag, pp. 259–287.

[28] H. WEBER. *Lehrbuch der Algebra*, vol. I, II, III. Chelsea Publishing Company, New York, 1902.

(F. Leprévost) Université Paris 7, Département de Mathématiques, Tour 45-55, 5ème étage, 2 place Jussieu, F-75252 Paris Cedex 05, France

E-mail address, F. Leprévost: leprevot@mathp7.jussieu.fr

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

E-mail address, F. Morain: morain@polytechnique.fr