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

F. LEPRÉVOST ET F. MORAIN

26 octobre 1994

RÉSUMÉ. Nous utilisons des revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques pour évaluer certaines sommes de caractères.

1. INTRODUCTION

Soit $P(X) = \sum_{r=0}^{m} a_r X^r$ un polynôme à coefficients dans $\mathbb{Z}$. Pour p premier, soit $\chi(x)$ le symbole de Legendre. 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. Le cas des courbes elliptiques à multiplication complexe par un anneau d'entiers de nombre de classes 1 a été complètement traité (voir [17] 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, 14, 15, 20] (et les références qui y sont données) pour cela.

Brewer a considéré des sommes reliées à une suite de polynômes particulière (voir section 2). Des sommes analogues aux sommes de Jacobsthal ont été calculées dans $\mathbb{F}_{p^2}$ par Berndt et Evans [3].

Dans ce travail, nous introduisons les sommes de caractères

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

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

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).

Après avoir donné quelques propriétés élémentaires des sommes $\Gamma_{p,n}$, nous rappelons quelques-uns des résultats de Brewer. Puis nous décrivons brièvement quelques-unes des propriétés importantes de la théorie de la multiplication complexe et celles des fonctions de Weber. Dans la section 3, nous montrons que les courbes de genre 2 d'équation $y^2 = x(x^4 - Ax^2 + B)$ sont décomposables. À partir de la section 4, nous nous concentrons plus particulièrement sur les sommes $\Gamma_{p,2}(A,B)$. Après avoir démontré le théorème fondamental, nous donnons dans la section 5 quelques valeurs particulières des sommes $\Gamma_{p,2}(A,B)$. En particulier, nous montrons que certaines courbes elliptiques à multiplication complexe par un ordre d'un corps quadratique $K = \mathbb{Q}(\sqrt{-d})$, $d > 0$, ont comme revêtement une courbe de genre 2 d'équation $y^2 = x(x^4 - Ax^2 + B)$ de paramètres A et B qui s'expriment comme fractions rationnelles en les fonctions de Weber. Nous déduisons de cela plusieurs résultats. Le premier est une nouvelle démonstration de formules connues pour $\Phi_{p,4}(a)$. Puis, nous montrons comment relier des sommes de caractères liées à certaines courbes elliptiques à multiplication complexe par un ordre d'un corps quadratique imaginaire $\mathbb{Q}(\sqrt{-d})$ de nombre de classes 2 à des sommes $\Gamma_{p,2}(A,B)$ bien choisies. Dans le cas $d = 5$, nous utilisons les travaux de Brewer qui nous permettent de calculer précisément la somme de caractères.

Nous concluons par des remarques sur les autres cas et les applications à l'algorithme de primalité ECPP [1].

2. Préliminaires

2.1. Quelques résultats sur les sommes de caractères. Commençons par des résultats élémentaires.

Proposition 1. *Pour $p > 2$, on a*

$$\Gamma_{p,0}(A,B) = 0, \quad \Gamma_{p,n}(A, A^2/4) = 0,$$

$$\Gamma_{p,n}(0,B) = \Phi_{2n,p}(B),$$

$$\Gamma_{p,n}(A,0) = \begin{cases} \Psi_{p,n}(-A) & \textit{si } n \textit{ est impair} \\ \Phi_{p,n}(-A) & \textit{sinon;} \end{cases}$$

$$\Gamma_{p,n}(Am^n, Bm^{2n}) = \chi(m)^{2n+1}\Gamma_{p,n}(A,B).$$

Si $p \equiv 3 \bmod 4$, alors $\Gamma_{p,2n}(A,B) = 0$. Quand $p \equiv 1 \bmod 4$, soit i une racine carrée de -1 modulo p. Alors $\Gamma_{p,2}(-A,B) = \chi(i)\Gamma_{p,2}(A,B)$.

Les valeurs de $\Gamma_{p,1}$ sont moins connues. Quand la courbe elliptique $E : y^2 = x(x^2 - Ax + B)$ est à multiplication complexe par un anneau d'entiers de corps quadratique imaginaire de nombre de classes 1, les résultats sont connus (voir [17] et les références citées).

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 et soit $P^*(X) = X^m P(1/X)$ son polynôme réciproque. Alors*

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

Si P est de degré impair, on a

$$S_p(XP(X)) = S_p(P^*(X)).$$

Démonstration : Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. On écrit d'abord :

$$S_p(P(X^2)) = \chi(P(0)) + \sum_{i=0}^{p-1} \chi(P(g^{2i})) = \chi(P(0)) + 2\sum_{i=0}^{(p-1)/2} \chi(P(g^{2i})) = \chi(P(0)) + 2\sum_{(x/p)=+1} \chi(P(x))$$
$$= \sum_{x=0}^{p-1} (1+\chi(x))\chi(P(x)),$$

ce qui prouve la première formule.

Supposons $m = 2n+1$. Alors la courbe d'équation $y^2 = xP(x)$ est birationnellement équivalente à la courbe $Y^2 = P^*(X)$ via les formules $x = 1/X$, $yX^{n+1} = Y$. La seconde formule s'en déduit. □

Le corollaire suivant généralise des propriétés connues des sommes de Jacobsthal.

Corollaire 1. *Pour toutes valeurs de A et B, on a*

$$\Delta_{p,2n}(A,B) = \Delta_{p,n}(A,B) + \Gamma_{p,n}(A,B),$$

2.2. Les sommes de Brewer.

2.2.1. *Définition et propriétés.* Soit Q un entier non nul. On considère la suite de polynômes $V_n(X,Q)$ définie par $V_1(X,Q) = X$, $V_2(X,Q) = X^2 - 2Q$ et pour $n > 2$:

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

Les premières valeurs de cette suite sont :

$$V_3(X,Q) = X^3 - 3QX, \quad V_4(X,Q) = X^4 - 4QX^2 + 2Q^2, \quad V_5(X,Q) = X(X^4 - 5QX^2 + 5Q^2).$$

On pose alors $\Lambda_{p,n}(Q) = S_p(V_n(X,Q))$. Les valeurs de $\Lambda_{p,n}(1)$ pour $1 \le n \le 5$ 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 $n = 10$. Ces travaux ont été étendus aux cas $n \in \{7, 8, 9, 12, 14, 18\}$ dans [13] et une nouvelle expression pour $n = 10$ donnée. Voir aussi [4].

2.2.2. *La somme $\Lambda_{p,5}(Q)$.* Notons tout de suite que $\Lambda_{p,5}(Q) = \Gamma_{p,2}(5Q, 5Q^2)$. Soit p un nombre premier qui s'écrit $p = a^2+b^2 = u^2+5v^2$ avec a, b, u, v entiers relatifs. Cela équivaut à $p \equiv r \bmod 20$, avec $r \in \{1, 9\}$. On suppose dans la suite que $a \equiv 1 \bmod 4$ et on pose $\varepsilon_{20}(p) = +1$ si $p \equiv 1 \bmod 20$ et -1 si $p \equiv 9 \bmod 20$. On rappelle alors les théorèmes suivants [7, 8] :

Théorème 1. *Soit Q tel que $\chi(Q) = +1$ et soit m une racine carrée de Q modulo p. On a*

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

Théorème 2. *Soit Q tel que $\chi(Q) = -1$. On suppose que $p = u^2+5v^2 = a^2+b^2$ avec $a \equiv 1 \bmod 4$, $b \equiv aQ^{(p-1)/4} \bmod p$. On a*

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

Remarque. Les résultats précédents sont à l'origine de notre travail. En effet, la décomposition de p sous la forme $p = a^2+b^2 = u^2+5v^2$ traduit le fait que p se décompose dans le corps biquadratique $\mathbb{Q}(i, \sqrt{5})$, qui se trouve être le corps de classe du corps quadratique $\mathbb{Q}(\sqrt{-5})$. La recherche du lien entre la courbe d'équation $y^2 = x(x^4 - 5Qx^2 + 5Q^2)$ et une courbe elliptique à multiplication complexe par l'anneau des entiers de $\mathbb{Q}(\sqrt{-5})$ a été le moteur de nos travaux. La section qui suit donne quelques propriétés de la multiplication complexe.

2.3. Rappels sur la multiplication complexe. On pourra consulter [12] (et éventuellement [6] et [11]) pour les résultats qui suivent.

Soit d un entier positif sans facteur carré. Soit $K = \mathbb{Q}(\sqrt{-d})$ un corps quadratique imaginaire de discriminant $\mathcal{D}$ (avec $\mathcal{D} = -d$ si $d \equiv 3 \bmod 4$ et $\mathcal{D} = -4d$ sinon), et soit $\mathcal{O}$ l'ordre principal de K. Soient a, b, c trois entiers premiers entre eux tels que $b^2 - 4ac = m^2\mathcal{D}$, m entier positif. On considère la forme quadratique $\mathcal{Q}(u, v)$ associée au triplet (a, b, c). Pour cette forme, on note z la racine de partie imaginaire positive de l'équation

$$az^2 + bz + c = 0.$$

On associe à z l'ordre $\mathcal{O}_m = \mathbb{Z} + az\mathbb{Z}$ de K. Soit $h(\mathcal{O}_m)$ le nombre de classes de $\mathcal{O}_m$. On sait que le corps de classe de $\mathcal{O}_m$ est le corps $K_z = \mathbb{Q}(z, j(z))$ où $j(z)$ est l'invariant modulaire. De plus $j(z)$ est alors algébrique de degré $h(\mathcal{O}_m)$, de polynôme minimal sur $\mathbb{Q}$ noté $H_z(X)$.

Dans la suite, nous nous limiterons aux cas des nombres z vérifiant soit

$$z^2 + z + (d + 1)/4 = 0$$

(avec dans ce cas $d \equiv 3 \bmod 4$), soit

$$z^2 + m^2 d = 0$$

avec $m \geq 1$ (sans restriction sur d). Autrement dit, z est associée à l'une des formes quadratiques $\mathcal{Q}_0 = (1, 1, (d + 1)/4)$ ou $\mathcal{Q}_m = (1, 0, m^2 d)$.

Soit p un nombre premier ($p > 3$). Soit $\mathcal{Q}$ une des formes $\mathcal{Q}_0$ ou $\mathcal{Q}_m$ suivant les cas. On sait que p est représentable par $\mathcal{Q}$ si et seulement si p se décompose dans K_z, ou encore $H_z(X)$ a une racine modulo p.

Soit E une courbe elliptique à multiplication complexe par $\mathcal{O}_m$, définie sur $\mathbb{Q}(j(z))$. Si p se décompose dans K_z, on peut écrire

$$4p = U^2 + (m^2 d)V^2$$

avec U et V entiers rationnels, c'est-à-dire p s'écrit comme le produit de deux entiers algébriques π et π' dans $\mathcal{O}$. On peut alors réduire E modulo p, obtenant une courbe définie sur $\mathbb{F}_p$, d'équation $y^2 \equiv x^3 + rx + s$. Le Frobenius de la courbe $E \bmod p$ s'identifie à $\zeta\pi$ (où ζ est une racine de l'unité dans K, $\zeta = \pm 1$ dès que $d \notin \{1, 3\}$) et le nombre de points de $E(\mathbb{F}_p)$ vérifie

$$4\#E(\mathbb{F}_p) = (\zeta U - 2)^2 + (m^2 d)V^2 = 4(p + 1) - 4(\zeta U).$$

Comme le nombre de points s'écrit aussi

$$\#E(\mathbb{F}_p) = p + 1 + S_p(x^3 + rx + s)$$

on en déduit que

$$S_p(x^3 + rx + s) = -(\zeta U).$$

Il reste un problème difficile à résoudre, celui de la détermination de ζ. L'un des buts de ce travail est de lever l'indétermination dans certains cas. On posera

$$\Sigma_{p,z} = S_p(x^3 + rx + s).$$

2.4. Les fonctions de Weber. Rappelons quelques définitions. La fonction de Dedekind est

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

et on pose

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

Soit $\gamma_2(z)$ la racine cubique de $j(z)$ (on prend comme détermination de la racine cubique celle qui envoie $i\mathbb{R}$ sur $\mathbb{R}$). On a [28, §54, p. 179]

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

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

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

Le résultat suivant sera crucial dans la suite.

Proposition 2. *Les solutions de l'équation*

$$\frac{64\,(3\,\theta+10)^3}{(\theta-2)^2\,(\theta+2)} = j(z)$$

pour $j \neq 1728$ *sont*

$$2\frac{\mathfrak{f}(z)^{24}+2^6}{\mathfrak{f}(z)^{24}-2^6}, \quad 2\frac{\mathfrak{f}_1(z)^{24}-2^6}{\mathfrak{f}_1(z)^{24}+2^6}, \quad 2\frac{\mathfrak{f}_2(z)^{24}-2^6}{\mathfrak{f}_2(z)^{24}+2^6}.$$

Pour $j = 1728$, *la racine double de l'équation est* $-14/9 = 2(\mathfrak{f}_1(i)^{24}-2^6)/(\mathfrak{f}_1(i)^{24}+2^6) = 2(\mathfrak{f}_2(i)^{24}-2^6)/(\mathfrak{f}_2(i)^{24}+2^6)$.

Démonstration : Le résultat du théorème se vérifie aisément. Indiquons comment il a été trouvé. On commence par chercher à quelle condition $(\theta-2)^2(\theta+2)$ est un cube. Cela est possible si $\theta = 2(x^3+1)/(x^3-1)$, auquel cas la quantité qui nous intéresse vaut $4x/(x^3-1)$. Injectant cette valeur de θ, on trouve que :

$$(4x)^3 - \gamma_2(z)(4x) - 16 = 0$$

et le résultat en découle par application du théorème précédent. □

3. Courbes de genre 2 décomposables

Le but de cette section est de prouver le résultat suivant.

Théorème 5. *Soient A et B deux nombres complexes tels que la courbe C, d'équation*

$$y^2 = x(x^4 - Ax^2 + B),$$

soit de genre 2. Alors la jacobienne de C est isogène au produit de deux courbes elliptiques E et E' d'équations

$$E : V^2 = (U-1)((2-\theta)U^2 + (12+2\theta)U + 2 - \theta),$$
$$E' : V^2 = (1-U)((2-\theta)U^2 + (12+2\theta)U + 2 - \theta),$$

où $\theta = A/\sqrt{B}$.

Démonstration : Outre l'involution hyperelliptique, la courbe C possède un automorphisme non trivial donné par

$$(x, y) \longrightarrow (-x, iy).$$

Les courbes de genre 2 munies d'un automorphisme différent de l'involution hyperelliptique ont été classifiées par Bolza [5].

Ainsi, le calcul montre que, si $A \neq 0$ et $B \neq 9A^2/100$, la forme sextique $F(X,Y) = XY(X^4 - AX^2Y^2 + BY^4)$ associée à l'équation de C est isomorphe à la forme canonique de type III de Bolza [5, p. 70]. De même, on constate que, si $A = 0$ (resp. $B = 9A^2/100$), la forme sextique $F(X,Y)$ est isomorphe à la forme canonique de type VI (resp. V) de Bolza [5, p. 70]. Dans chacun de ces cas, la jacobienne de C est isogène à un produit de courbes elliptiques. Explicitons simplement le cas où $A \neq 0$ et $B \neq 9A^2/100$, les deux autres se traitant de manière similaire. La courbe C est isomorphe à la courbe C_θ d'équation

$$C_\theta : y_1^2 = f_1(x_1) = x_1(x_1^4 - \theta x_1^2 + 1)$$

via les formules

$$x = \alpha x_1, \quad y = \sqrt{\alpha B}\, y_1$$

où on a posé $\alpha^4 = B$ et $\theta = A/\sqrt{B}$. Effectuant maintenant le changement

$$x_1 = \frac{x_2+1}{x_2-1}, \quad y_1 = \frac{y_2}{(x_2-1)^3}, \tag{1}$$

on trouve que C_θ est isomorphe à la courbe C' d'équation

$$C' : y_2^2 = f_2(x_2^2) = (x_2^2 - 1)((2-\theta)x_2^4 + (12+2\theta)x_2^2 + 2 - \theta)$$

d'où des revêtements sur des courbes elliptiques. Ainsi, notons E la courbe elliptique d'équation

$$E : V^2 = (U-1)((2-\theta)U^2 + (12+2\theta)U + 2 - \theta),$$

et E' la courbe elliptique d'équation

$$E' : V^2 = (1-U)((2-\theta)U^2 + (12+2\theta)U + 2 - \theta),$$

on a alors des morphismes φ_1 et φ_2 de C' sur, respectivement, E et E' donnés par

$$\begin{aligned} \varphi_1(x_2, y_2) &= (x_2^2, y_2), \\ \varphi_2(x_2, y_2) &= \left(\frac{1}{x_2^2}, \frac{y_2}{x_2^3}\right). \end{aligned}$$

Les images réciproques des différentielles de première espèce de E et E', $\omega_1 = \frac{dU}{V}$ et $\omega_2 = \frac{dU}{V}$, par les morphismes φ_1 et φ_2 sont $\varphi_1{}^*(\omega_1) = \frac{2x_2dx_2}{y_2}$ et $\varphi_2{}^*(\omega_2) = -\frac{2dx_2}{y_2}$, qui sont indépendantes et engendrent $\Omega^{1,0}(C)$, l'espace des formes différentielles de première espèce de C. Par conséquent la jacobienne de C est isogène au produit $E \times E'$. Remarquons que E et E' sont isomorphes *via*

$$(U, V) \longrightarrow (U, iV).\square$$

Corollaire 2. *Si E est à multiplication complexe, la jacobienne de C est en réalité isomorphe à un produit de courbes elliptiques.*

Démonstration : ce corollaire est une application directe du théorème de Shioda-Mitani ([27], p. 271 ou [25], p. 296). $\square$

Il est plus simple, pour notre propos, de mettre la courbe E sous forme de Weierstraß. Posons pour ce faire $\kappa = \theta - 2$ et effectuons dans E le changement de variable

$$(L, M) = (-U/\kappa, V/\kappa^2).$$

On obtient

$$M^2 = L^3 + (3/\kappa + 16/\kappa^2)L^2 + (3/\kappa^2 + 16/\kappa^3)L + 1/\kappa^3$$

et une dernière transformation

$$N = L + 16/(3\kappa^2) + 1/\kappa$$

donne

$$M^2 = N^3 - \left(\frac{256}{3\,\kappa^4} + \frac{16}{\kappa^3}\right) N + \left(\frac{8192}{27\,\kappa^6} + \frac{256}{3\,\kappa^5}\right)$$

ou encore, en fonction de θ :

$$E_\theta : M^2 = P_\theta(N) = N^3 + r(\theta)N + s(\theta) = N^3 - \left(\frac{256}{3\,(\theta-2)^4} + \frac{16}{(\theta-2)^3}\right) N + \left(\frac{8192}{27\,(\theta-2)^6} + \frac{256}{3\,(\theta-2)^5}\right)$$

qui se factorise comme

$$M^2 = \left(N - \frac{16}{3(\theta-2)^2}\right)\left(N^2 + \frac{16N}{3(\theta-2)^2} - \frac{144\theta + 224}{9(\theta-2)^4}\right). \tag{2}$$

L'invariant de cette courbe est

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

4. Le théorème fondamental

On utilise les notations de la section précédente. On se place dans le cas où A et B sont entiers. Soit p un nombre premier ne divisant pas B et supposons qu'il existe β dans $\mathbb{Z}/p\mathbb{Z}$ tel que $\beta^8 \equiv B \bmod p$ (ce sera par exemple le cas quand $B = 1$). *A fortiori*, $\theta \equiv A/\beta^4 \in \mathbb{Z}/p\mathbb{Z}$. Par suite, E_θ, tout comme C, est définie modulo p.

Théorème 6. *Avec les notations qui précèdent :*

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

Démonstration : Il est clair que si $B \equiv \beta^8 \bmod p$, on a $\Gamma_{p,2}(A,B) = S_p(f_1)$. On écrit ensuite :

$$S_p(f_1) = \sum_{x_1=0}^{p-1} \chi(f_1(x_1)) = \chi(f_1(1)) + \sum_{x_1 \neq 1} \chi(f_1(x_1)),$$

d'où en utilisant le changement de variable (1) :

$$S_p(f_1) = \chi(f_1(1)) + \sum_{x_2 \neq 1} \chi(f_2(x_2^2)) = \chi(f_1(1)) + \chi(f_2(0)) + \sum_{x_2=1}^{p-1} \chi(f_2(x_2^2))$$

en remarquant que $f_2(1) = 0$. En imitant la démonstration du lemme 1, et en utilisant le fait que $f_2^* = -f_2$, on a

$$\sum_{x_2=1}^{p-1} \chi(f_2(x_2^2)) = (1 + \chi(-1)) \sum_{x_2=1}^{p-1} \chi(f_2(x_2)),$$

et parce que $f_2(0) = \theta - 2 = -f_1(1)$, nous obtenons finalement

$$S_p(f_1) = (1 + \chi(-1)) S_p(P_\theta). \square$$

Remarque. On retrouve immédiatement le fait que si $p \equiv 3 \bmod 4$ (et B résidu octique), alors $\Gamma_{p,2}(A,B) = 0$, puisque $\chi(-1) = -1$ dans ce cas.

5. Applications aux cas des courbes à multiplication complexe

Le théorème précédent 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" $\Gamma_{p,2}(A,B)$. L'autre type correspond au calcul en sens inverse.

Dans la suite, E_θ sera toujours à multiplication complexe par un ordre $\mathcal{O}_m$ d'un corps quadratique imaginaire K, z le nombre complexe associé à $\mathcal{O}_m$. La courbe E 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 4, on sait que E_θ et C sont définies sur le même corps, et dans certains cas, C est définie dans un sous-corps du corps de définition de E_θ. Nous nous limiterons au cas où au moins l'une de ces courbes est définie sur $\mathbb{Q}$.

5.1. Cas où $h(\mathcal{O}_m) = 1$. Il y a 9 ordres principaux de nombre de classes 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 4 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

$$f(z) f_2((z+1)/2) = e^{i\pi/24}\sqrt{2}.$$

On donne dans le tableau 1 les valeurs des discriminants, conducteurs des ordres ainsi que les valeurs correspondantes de θ et les coefficients $r(\theta)$ et $s(\theta)$ de E_θ.

On peut en déduire des résultats sur des sommes de caractères bien choisies, en choisissant $A = \theta$, $B = 1$, dans chacun des cas qui nous intéressent. 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 $\Gamma_{p,2}(\theta, 1)$.

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

5.1.1. *Le cas $d = 3$.* On utilise [16, Théorème 4 p. 304].

Théorème 7. *Soit $p \equiv 1 \bmod 3$. 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

$$S_p(X^3 - (3/16)^3) = \overline{\xi}\pi + \xi\overline{\pi}.$$

De cela on déduit

Corollaire 3. *Si $p \equiv 1 \bmod 12$, avec les notations du théorème précédent*

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

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 $\Gamma_{p,2}(-10/3, 1) = -52$.

5.1.2. *Le cas $d = 1$.* En utilisant par exemple [16, Théorème 5 p. 307], on a d'abord :

Théorème 8. *Soit $p \equiv 1 \bmod 4$. Alors*

$$S_p(X^3 - (3/4)^6 X) = -2\chi(3)u$$

avec $p = u^2 + v^2$, $u \equiv 1 \bmod 2$, $v \equiv 0 \bmod 2$ et $u - v \equiv 1 \bmod 4$.

On a alors

Corollaire 4. *Avec les notations précédentes :*

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

5.1.3. *Le cas $d = 7$.* La courbe E est isomorphe à la courbe

$$M^2 = L'^3 + \frac{3969}{4096}L'^2 + \frac{250047}{1048576}L$$

ou encore

$$M^2 = L'^3 + 21cL'^2 + 112c^2L'$$

avec $c = 189/4096$. On applique alors le théorème suivant [23].

Théorème 9. *On écrit $p = u^2 + 7v^2$, avec $u \equiv 1, 4, 2 \bmod 7$ si $p \equiv 1, 9, 11 \bmod 14$. Alors*

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

D'où l'on déduit

Corollaire 5. *Avec les notations du théorème précédent et dans le cas où $p \equiv 1 \bmod 4$, $p \nmid 63$, on a*

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

5.1.4. *Le cas $d = 2$.*

Théorème 10. *Soit $p = 8F + 1 = c^2 + 2\delta^2$, $c \equiv -1 \bmod 4$. 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 $\mathbb{Z}[\sqrt{-2}]$ [21] est

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

pour laquelle la somme de caractères correspondante a été évaluée dans [22] et vaut :

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

Il suffit de constater que la courbe E_{-2} est isomorphe à la courbe précédente avec $\vartheta = -1$.

Si B est un résidu octique, le théorème 6 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 [18, 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 $h(\mathcal{O}_m) = 2$. Décrivons le principe général des calculs (qui se généralise facilement au cas où $h(\mathcal{O}_m) > 2$). Soit E une courbe elliptique à multiplication complexe par un ordre $\mathcal{O}_m$ de nombre de classes 2. Cette courbe est définie sur $\mathbb{Q}(j(z))$ où z est associé à $\mathcal{O}_m$. Si E a un point de Weierstrass d'ordre 2 rationnel sur son corps de définition, on peut l'identifier avec une courbe E_θ où θ est donné par la proposition 2. Si le théorème 4 s'applique, la courbe E_θ est aussi définie sur $\mathbb{Q}(j(z))$. Si p est un nombre premier qui se décompose dans K_z, alors E tout comme E_θ (et C_θ) sera définie dans $\mathbb{F}_p$ et on pourra utiliser le théorème 6 pour identifier les deux sommes de caractères. Dans certains cas, on verra même comment remonter directement à la somme $\Gamma_{p,2}(A, B)$ avec A et B entiers rationnels.

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, $j(z)$ est réel et appartient à un corps $\mathbb{Q}(\varpi)$. À partir de $j(z)$, on construit une courbe elliptique $E_z : y^2 = x^3 + R_z x + S_z$, à multiplication complexe par $\mathcal{O}_m$ en calculant les coefficients R_z et S_z par

$$R_z = 3j(z)/(1728 - j(z)), \quad S_z = 2j(z)/(1728 - j(z)).$$

Le tableau 2 donne les valeurs de (d, m) et ξ_0^t où t est le plus petit entier pour lequel $\mathbb{Q}(\xi_0^t) = \mathbb{Q}(j(z))$ (valeurs prises dans [28]) et les valeurs correspondantes de θ dans chacun des cas où E_z a un point de Weierstrass d'ordre 2 et où le théorème 4 s'applique. L'examen de cette table 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 $A/\sqrt{B} = \theta$ dans chacun de ces cas.

Soit p un nombre premier qui se décompose dans K_z. L'idée est alors de nous servir de la section précédente, en liant la somme $\Sigma_{p,z}$ à une somme $\Gamma_{p,2}(A, B)$ avec $A/\sqrt{B} = \theta$. Nous avons ainsi trouvé une courbe E_θ de même invariant modulaire que E_z, et qui est un des facteurs de la jacobienne d'une courbe hyperelliptique C_θ. Mais il n'est pas sûr que E_z et E_θ soient $\mathbb{F}_p$-isomorphes. Dans chacun des cas, on peut écrire $R(z)c_z^2 = r(\theta)$ (resp. $S(z)c_z^3 = s(\theta)$) avec c_z un élément de $\mathbb{Q}(\varpi)$. Les deux courbes E_z et E_θ seront $\mathbb{F}_p$-isomorphes si et seulement si c_z est un carré modulo p. Dans le cas contraire, E_θ est $\mathbb{F}_p$-isomorphe à la tordue de E_z. Par suite, en utilisant le théorème 6 :

Théorème 11. *Avec les notations précédentes :*

$$\Sigma_{p,z} = \chi(c_z)\Gamma_{p,2}(A,B)/2.$$

On trouve dans le tableau 3 les nombres c_z.

5.2.2. *Le cas $d = 5$.* Le corps K_z est ici $\mathbb{Q}(\sqrt{-1}, \sqrt{5})$. Un nombre premier p se décompose dans K_z si et seulement s'il s'écrit sous la forme $p = a^2 + b^2 = u^2 + 5v^2$.

D'après ce qui précède, on prend $\theta = \sqrt{5}$, et par exemple, $A = B = 5$ convient. La somme $\Gamma_{p,2}(5,5)$ est justement la somme $\Lambda_{p,5}(1)$ étudiée par Brewer et dont on a rappelé les propriétés dans la section 2.

Le résultat suivant va nous permettre de terminer les calculs.

Proposition 3. *Pour tout p, il existe un entier Q tel que $5Q^2$ soit un résidu octique modulo p, avec $\chi(Q) = (5/p)_4$.*

Démonstration : Nous allons exhiber un tel Q pour tous les cas possibles. Notons m une racine carrée de 5 modulo p.

Dans un premier temps, supposons que $(5/p)_4 = +1$. Si $p = 8n + 5$, tout résidu quartique est une puissance huitième. On prend donc $Q = 1$. Si $p = 8n + 1$ et $(5/p)_8 = +1$, on prend $Q = 1$; si $(5/p)_8 = -1$, on prend $Q = m$, car $(m/p)_4 = (5/p)_8$. Notons que $\chi(Q) = +1$ dans tous ces cas.

Supposons maintenant $(5/p)_4 = -1$. Alors il est facile de voir que $(5m/p)_4 = +1$. Si $p = 8n + 5$, on prend $Q = m$. Si $p = 8n + 1$, on constate que $(5m^2/p)_8 = (5/p)_4 = -1$. On prend alors $Q \equiv 5m \bmod p$. Notons que dans ces cas, on a toujours $\chi(Q) = -1$. □

Finalement, nous obtenons explicitement la quantité $\Sigma_{p,\sqrt{-5}}$:

Théorème 12. *Soit Q un entier tel que $5Q^2$ soit la puissance huitième d'un élément β de $(\mathbb{Z}/p\mathbb{Z})^*$. On choisit $\varpi = \sqrt{5} \equiv \beta^4/Q \bmod p$. Avec les notations précédentes et celles de la section 2.2.2, on obtient :*

$$\Sigma_{p,\sqrt{-5}} = \chi(c_{\sqrt{-5}})\varepsilon_{20}\varepsilon(p)(2u)$$

où $\varepsilon_{20} = 1$ si $p \equiv 1 \bmod 20$ et -1 si $p \equiv 9 \bmod 20$ et $\varepsilon(p)$ est donné dans le tableau suivant :

$(5/p)_4$	$p \bmod 8$	$(5/p)_8$	$\varepsilon(p)$
$+1$	5		-1
	1	$+1$	-1
		-1	$+1$
-1			-1

Les conditions de normalisation sur a, b et u sont celles des théorèmes 1 et 2.

Démonstration : Il suffit de combiner le théorème 6 avec les théorèmes de Brewer rappelés à la section 2. □

Exemples numériques. Nous allons donner un exemple numérique pour chacun des cas du théorème 12. Les calculs ont été faits à l'aide de `PARI-gp` [2].

p	p mod 20	a	$\|b\|$	$(5/p)_4$	p mod 8	$(5/p)_8$	Q	$\varepsilon(p)$	b	u	ϖ	(c_z/p)	Σ_p
101	1	1	10	$+1$	5		1	-1	10	-9	56	$+1$	18
401	1	1	20	$+1$	1	$+1$	1	-1	20	-9	178	-1	-18
521	1	-11	20	$+1$	1	-1	199	$+1$	20	-21	322	-1	42
61	1	5	6	-1	5		26	-1	-6	4	35	-1	8
41	1	5	4	-1	1		24	-1	-4	6	28	$+1$	-12
109	9	-3	10	$+1$	5		1	$+1$	10	-8	21	-1	16
409	9	-3	20	$+1$	1	$+1$	1	$+1$	20	2	259	-1	-4
929	9	-23	20	$+1$	1	-1	61	$+1$	-20	-18	868	$+1$	36
29	9	5	2	-1	5		11	$+1$	2	-3	18	-1	6
89	9	5	8	-1	1		6	-1	-8	-3	70	-1	6

Remarques. On remarque que $b \equiv 0 \bmod 5$ équivaut à $a \not\equiv 0 \bmod 5$ soit encore à 5 résidu quartique modulo p d'après [19].

6. Remarques complémentaires

6.1. Les autres cas $h = 2$. La démonstration des théorèmes 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 $p = (U^2 + m^2dV^2)/4$.

Les cas où m^2d est impair peuvent peut-être être traités avec une méthode analogue à celle développée dans [17]. Cela est entrepris dans [10].

6.2. Le cas $h > 2$. Dans les cas où le théorème 4 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 $\mathbb{Q}$. À notre connaissance, aucun résultat n'est connu pour de telles sommes.

6.3. Cas où θ est de trace nulle. Les cas où θ est de trace nulle peuvent se détecter dans les cas où une des puissances de la fonction de Weber associée est une unité (voir par exemple [28, §141]. Par exemple, si η est une unité d'un corps quadratique, alors $(\eta + 1)/(\eta - 1)$ est de trace nulle.

On remarque aussi par le calcul que dans certains cas, on peut calculer des valeurs de θ qui auront aussi une trace nulle dans leur corps de définition. Par exemple, pour le cas $d = 21$, on a

$$\mathfrak{f}(\sqrt{-21})^{24} = (\sqrt{3} + \sqrt{7})^6(3 + \sqrt{7})^4/2^2$$

et

$$\theta = 12\sqrt{7}/91(4 + \sqrt{3}).$$

6.4. Remarque à propos de ECPP. Dans ECPP [1], la phase finale des calculs consiste justement à lever l'ambiguité sur le signe des sommes de caractères. La réponse fournie dans le cas de 20 est algorithmique, car ECPP a de toute façon besoin de l'écriture de p sous la forme $p = a^2 + b^2 = u^2 + 5v^2$. La détermination de l'ambiguité a donc pour coût celui de quelques symboles de Jacobi (la racine carrée de -5 est également connue, ainsi que $\varpi = \sqrt{5}$), ce qui est plus rapide que la méthode alternative qui consiste à essayer les deux courbes possibles.

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 par l'anneau des entiers d'un corps quadratique imaginaire de nombre de classes 1. Rapport de Recherche LIX/RR/93/11, Laboratoire d'Informatique de l'Ecole Polytechnique (LIX), 1993. Soumis au *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. M. G. Monzingo. An elementary evaluation of the Jacobsthal sum. *J. Number Theory 22* (1986), 21–25.
20. A. R. Rajwade. Arithmetic on curves with complex multiplication by $\sqrt{-2}$. *Proc. Cambridge Philos. Soc. 64* (1968), 659–672.
21. A. R. Rajwade. Certain classical congruences via elliptic curves. *J. London Math. Soc. 2*, 8 (1974), 60–62.
22. 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).
23. S. F. Robinson. Theorems on Brewer sums. *Pacific Journal of Mathematics 25*, 3 (1968), 587–596.
24. W. M. Ruppert. When is an abelian surface isomorphic or isogeneous to a product of elliptic curves ? *Math. Z. 203* (1990), 293–299.
25. 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.
26. 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.
27. 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, 75252 Paris Cedex 05

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

d	m	z	f	j	θ	$r(\theta)$	$s(\theta)$
3	1	$(-1+\sqrt{-3})/2$	$\mathfrak{f}_2(z)=-2^4$	0	$-10/3$	0	$(-3/16)^3$
3	2	$\sqrt{-3}$	$\mathfrak{f}(z)=2^8$	$2^4.3^3.5^3$	$10/3$	-11	-14
1	1	i	$\mathfrak{f}(z)=2^6$	12^3	$-14/9$	$-(3/4)^6$	0
1	2	$2i$	$\mathfrak{f}_1(z)=2^9$	66^3	$14/9$	-11	-14
7	1	$(-1+\sqrt{-7})/2$	$\mathfrak{f}_2(z)=-1$	-15^3	$-130/63$	$-3^6.5.7^3/2^{24}$	$-3^9.7^5/2^{35}$
7	2	$\sqrt{-7}$	$\mathfrak{f}(z)=2^{12}$	$(3.5.17)^3$	$130/63$	-595	-5586
2	1	$\sqrt{-2}$	$\mathfrak{f}_1(z)=2^6$	20^3	0	$-10/3$	$56/27$

Tableau 1.

d	m	ϖ	ξ_0^t	$j(z)$	θ
3	4	$\sqrt{3}$	$\mathfrak{f}_1^{24}=2^7(1+\varpi)^6$	$1417905000+818626500\varpi$	$(170+320\varpi)/3$
1	3	$\sqrt{3}$	$\mathfrak{f}^{12}=2(1+\varpi)^4$	$76771008+44330496\varpi$	$7\varpi/6$
1	4	$\sqrt{2}$	$\mathfrak{f}_1^8=2^3\varpi(1+\varpi)^2$	$41113158120+29071392966\varpi$	$(-114+704\varpi)/441$
1	5	$\sqrt{5}$	$8\mathfrak{f}^4=(1+\varpi)^4$	$22015749613248+9845745509376\varpi$	$161\varpi/180$
7	4	$\sqrt{7}$	$\mathfrak{f}_1^8=2^3(3+\varpi)^2$	$137458661985000+51954490735875\varpi$	$(910+21760\varpi)/29241$
2	2	$\sqrt{2}$	$\mathfrak{f}_1^8=8+8\sqrt{2}$	$26125000+18473000\varpi$	$(-130+160\varpi)/49$
2	3	$\sqrt{6}$	$\mathfrak{f}_1^{12}=2(2+\varpi)^4$	$188837384000+77092288000\varpi$	$40\varpi/49$
15	2	$\sqrt{5}$	$\mathfrak{f}^6=2(1+\varpi)^2$	$(37018076625+16554983445\varpi)/2$	$(2730-896\varpi)/363$
5	1	$\sqrt{5}$	$\mathfrak{f}^4=1+\varpi$	$632000+282880\,\varpi$	ϖ
6	1	$\sqrt{8}$	$\mathfrak{f}_1^6=4+\varpi$	$2417472+853632\,\varpi$	$2\varpi/3$
10	1	$\sqrt{5}$	$\sqrt{2}\mathfrak{f}_1^2=1+\varpi$	$212846400+95178240\,\varpi$	$8\varpi/9$
13	1	$\sqrt{13}$	$\mathfrak{f}^4=3+\varpi$	$3448440000+956448000\,\varpi$	$5\varpi/9$
22	1	$\sqrt{8}$	$\mathfrak{f}_1^2=\varpi(2+\varpi)/4$	$3147421320000+1112780592000\,\varpi$	$70\varpi/99$
37	1	$\sqrt{37}$	$\mathfrak{f}^4=2(6+\varpi)$	$19830091900536000+3260047059360000\,\varpi$	$145\varpi/441$
58	1	$\sqrt{29}$	$\sqrt{2}\mathfrak{f}_1^2=5+\varpi$	$302364978924945672000+56147767009798464000\,\varpi$	$3640\varpi/9801$

Tableau 2.

d	m	c_z
1	3	$(-1573600-908544\varpi)/253$
1	5	$(-82556585112960-36920427264000\varpi)/46079$
2	3	$(-354332314574-144655563248\varpi)/23055$
5	1	$(-8040-3616\varpi)/165$
6	1	$(-3426-1212\varpi)/17$
10	1	$(-2518290-1126224\varpi)/145$
13	1	$(-32251608-8944992\varpi)/115$
22	1	$(-892659810042-631205805384\varpi)/3485$
37	1	$(-446362528843706328-73381547712971232\varpi)/276595$
58	1	$(-840424174390775962666602-156062851275664753436016\varpi)/34154525$

Tableau 3.