ANNALES DE L'INSTITUT FOURIER

DOMINIQUE BERNARDI

Résidus de puissances et formes quadratiques

Annales de l'institut Fourier, tome 30, n° 4 (1980), p. 7-17

<http://www.numdam.org/item?id=AIF_1980__30_4_7_0>

Ann. Inst. Fourier, Grenoble
30, 4 (1980), 7-17.

RÉSIDUS DE PUISSANCES ET FORMES QUADRATIQUES

par Dominique BERNARDI

Introduction.

Le but de ce travail est de donner une méthode générale dont découlent des résultats épars dans la littérature, reliant d'une part la décomposition des nombres premiers p congrus à 1 modulo n dans l'extension kummérienne $\mathbf{Q}(\sqrt[n]{q},\zeta_n)/\mathbf{Q}(\zeta_n)$ ou, ce qui revient au même, l'existence de solutions en nombres entiers à la congruence

$$x^n \equiv q \quad \text{modulo} \quad p$$

et d'autre part la représentation de p par certaines formes quadratiques binaires à coefficients dans l'anneau $\mathbf{Z}[\zeta_n+\zeta_n^{-1}]$ des entiers du sous-corps réel maximal du n-ième corps cyclotomique. Le premier, et le plus célèbre, de ces résultats est dû à Gauss et affirme que 2 est résidu cubique modulo $p = 3k + 1$ si et seulement si p peut s'écrire sous la forme $A^2 + 27B^2$. Un résultat typique est dû à E. Lehmer : si $p = 5k + 1$ est un nombre premier, 2 est résidu de puissance cinquième modulo p si et seulement si le système

$$\begin{aligned} p &= x^2 + 25u^2 + 25v^2 + 125w^2 \\ 0 &= u^2 + uv - v^2 - xw \end{aligned}$$

a une solution en nombres entiers. Pour une recension complète, voir [1].

L'idée de départ est d'utiliser les résultats de P. Satgé [7] qui portent sur des formes de degré $\varphi(n)$ à $\varphi(n)$ variables sur $\mathbf{Z}$. En transposant sa méthode par le choix, comme anneau de base, de $\mathbf{Z}[\zeta_n+\zeta_n^{-1}]$ au lieu de $\mathbf{Z}$, on obtient bien des formes quadratiques. On est amené pour ce faire à poser les hypothèses techniques suivantes :

1° l'anneau $\mathbf{Z}[\zeta_n+\zeta_n^{-1}]$ est principal ;

2° le nombre de classes d'idéaux de $\mathbf{Z}[\zeta_n]$ est impair.

Autrement dit, si $h = h^+ . h^-$ désigne la décomposition classique du nombre de classes d'idéaux du n-ième corps cyclotomique, h^+ doit être égal à 1 et h^- doit être impair.

1. Préliminaires.

On désigne par :

ℓ un nombre premier ;

$n = \ell^\alpha$ une puissance de ℓ ;

$K = \mathbf{Q}(\zeta_n)$ le corps des racines n-ièmes de l'unité ;

$A = \mathbf{Z}[\zeta_n]$ son anneau d'entiers ;

$K^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1}) = K \cap \mathbf{R}$ son sous-corps réel maximal ;

$B = \mathbf{Z}[\zeta_n + \zeta_n^{-1}]$ l'anneau des entiers de K^+ ;

q un nombre entier dont la racine ℓ-ième n'est pas entière ;

$L = K(\sqrt[n]{q})$;

Δ le groupe de Galois de K sur $\mathbf{Q}$, canoniquement isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$;

H le groupe de Galois de L sur K isomorphe (non canoniquement) à $\mathbf{Z}/n\mathbf{Z}$;

G le groupe de Galois de L sur K^+, diédral d'ordre $2n$; ses éléments sont des couples $(a,b) \in \{\pm 1\} \times \mathbf{Z}/n\mathbf{Z}$ avec la loi

$$(a,b) * (c,d) = (ac, ad+b) ;$$

p un nombre premier congru à 1 modulo n.

Il sera toujours supposé que n satisfait aux conditions indiquées dans l'introduction, c'est-à-dire que B est un anneau principal et que le groupe des classes d'idéaux de A est d'ordre impair. Ceci est le cas si A est principal, c'est-à-dire pour $n = 3, 4, 5, 7, 8, 9, 11, 13, 16, 19, 25, 27$ et 32 (cf. [5]) mais aussi dans d'autres cas, par exemple $n = 23$ $(h^+ = 1, h^- = 3)$ et $n = 31$ $(h^+ = 1, h^- = 9)$ (cf. [4]).

2. L'anneau B.

Plaçons-nous tout d'abord dans un cadre un peu plus général : K est un corps abélien imaginaire de degré $2r$, K^+ son sous-corps réel maximal,

$h = h^+ . h^-$ le nombre de classes d'idéaux de K, h^+ étant celui de K^+, E le groupe des unités de K^+, $\mathrm{Sgn}(E) \subset (\mathbf{Z}/2\mathbf{Z})^r$ son image par l'homomorphisme de signature et E^2 le sous-groupe des carrés d'éléments de E.

PROPOSITION 1. — *Si* 2^s *désigne le cardinal de* $\mathrm{Sgn}\,E$, h^- *est divisible par* 2^{r-s-1}. *Si de plus l'extension* K/K^+ *est ramifiée en au moins une place finie,* h^- *est divisible par* 2^{r-s}.

Démonstration. — On sait (cf. [6], th. 3.7 cor. 1) que le groupe des classes d'idéaux au sens strict de K^+ a $2^{r-s}h^+$ éléments. Le corps de classes correspondant, noté M, est la plus grande extension abélienne de K^+ non ramifiée aux places finies. L'extension MK/K est abélienne non ramifiée, elle est contenue dans le corps de classes de Hilbert de K : son degré divise donc h. Or ce degré vaut $2^{r-s-1}h^+$ ou $2^{r-s}h^+$ selon que K est ou non contenu dans M. On en conclut que $2^{r-s-1}.h^+$ divise h (ou encore 2^{r-s-1} divise h^-) et que si K/K^+ est ramifiée en une place finie, M ne contient pas K et 2^{r-s} divise h^-.

On voit donc que si h^- est impair et K/K^+ ramifiée en au moins une place finie, on a $2^r = 2^s$. Or le théorème de Dirichlet montre que 2^r est l'indice dans E du sous-groupe des carrés ; d'autre part il est clair que 2^s est l'indice dans E du sous-groupe des unités totalement positives. On en déduit la

PROPOSITION 2. — *Si* h^- *est impair et si* K/K^+ *est ramifiée en au moins une place finie, toute unité totalement positive est le carré d'une unité de* K^+.

Enfin on a la

PROPOSITION 3. — *Si de plus* $h^+ = 1$, *tout idéal de* K^+ *possède un générateur totalement positif. Ce générateur est unique au carré d'une unité près.*

Revenons au cadre défini en 1.: Si $K = \mathbf{Q}(\zeta_n)$, le nombre ℓ, étant totalement ramifié dans $K/\mathbf{Q}$, se ramifie dans K/K^+ ; de plus, $h^+ = 1$ et h^- est impair : les unités de $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ prennent donc toutes les signatures possibles et tout idéal de l'anneau $B = \mathbf{Z}[\zeta_n + \zeta_n^{-1}]$ admet un générateur totalement positif, ce dernier étant unique au carré d'une unité près.

3. Formes normes.

Rappelons que si L_1 et L_2 sont deux réseaux d'un espace vectoriel de dimension finie sur le corps des fractions d'un anneau de Dedekind B, on

désigne par $[L_1 : L_2]_B$ l'idéal engendré par les déterminants des endomorphismes de cet espace tels que $U(L_1) \subset L_2$ (dans le cas où B est principal, il existe un U tel que $U(L_1) = L_2$ et $[L_1 : L_2]_B = (\det U)$). Considérons maintenant un ordre $\mathfrak{O}$ du corps K, dont on suppose qu'il contient l'anneau B, et un $\mathfrak{O}$-idéal fractionnaire $\mathfrak{a}$; $\mathfrak{O}$ et $\mathfrak{a}$ sont alors des B-modules, donc des réseaux de l'extension K de K^+. L'idéal $[\mathfrak{O} : \mathfrak{a}]_B$ est donc bien défini et possède, d'après la proposition 3, un générateur totalement positif noté c. L'anneau B étant principal, $\mathfrak{a}$ admet une base sur B, soit $\{a_1, a_2\}$. Posons alors

$$F_{\mathfrak{a}}(X,Y) = c^{-1}N_{K/K^+}(Xa_1 + Ya_2)$$
$$= c^{-1}[a_1\bar{a}_1X^2 + (a_1\bar{a}_2 + \bar{a}_1a_2)XY + a_2\bar{a}_2Y^2]$$

$F_{\mathfrak{a}}$ est une forme quadratique binaire à coefficients dans B. Si la base de $\mathfrak{a}$ utilisée pour définir $F_{\mathfrak{a}}$ est remplacée par une autre, $F_{\mathfrak{a}}$ est modifiée par un changement de variables dans $GL_2(B)$. De même, si c est remplacé par un autre générateur totalement positif, ce dernier s'écrit cu^2 où u est une unité de B et

$$G(X,Y) = u^{-2}F_{\mathfrak{a}}(X,Y) = F_{\mathfrak{a}}(u^{-1}X, u^{-1}Y).$$

La forme $F_{\mathfrak{a}}$ est donc déterminée par $\mathfrak{a}$ à équivalence près sur B. De plus si x est un élément non nul de K, les formes associées à $\mathfrak{a}$ et $x.\mathfrak{a}$ sont les mêmes. On peut donc parler de la forme norme associée à une classe d'idéaux de $\mathfrak{O}$. On désignera par $C1(\mathfrak{O})$ le groupe des classes d'idéaux inversibles de $\mathfrak{O}$. On dira que $F_{\mathfrak{a}}$ représente un élément z de B s'il existe des éléments x et y de B tels que $F_{\mathfrak{a}}(x,y) = z$.

PROPOSITION 4. — *La forme norme associée à une classe de $\mathfrak{O}$-idéaux inversibles représente un élément totalement positif non nul z de B si et seulement si l'inverse de cette classe contient un idéal entier $\mathfrak{b}$ tel que* $[\mathfrak{O} : \mathfrak{b}]_B = (z)$.

Démonstration. — Si $F_{\mathfrak{a}}(x,y) = z$, posons $t = xa_1 + ya_2$ et $\mathfrak{b} = \mathfrak{a}^{-1}.t$. Comme t est dans $\mathfrak{a}$, $\mathfrak{b}$ est un $\mathfrak{O}$-idéal entier de la classe inverse de celle de $\mathfrak{a}$; de plus, on a

$$[\mathfrak{O} : \mathfrak{b}]_B = [\mathfrak{O} : \mathfrak{a}^{-1}.t]_B = [\mathfrak{O} : t\mathfrak{O}]_B[\mathfrak{O} : \mathfrak{a}^{-1}]_B = (F_{\mathfrak{a}}(x,y)) = (z).$$

Réciproquement, si $\mathfrak{b}$ satisfait aux conditions de l'énoncé, on a $\mathfrak{a}\mathfrak{b} = t\mathfrak{O}$; t appartient à $\mathfrak{a}$, $t = xa_1 + ya_2$ et

$$(F_{\mathfrak{a}}(x,y)) = (z);$$

$F_a(x,y)$ et z sont alors deux générateurs totalement positifs du même idéal fractionnaire de B donc on a, pour une unité u de B,

$$z = u^2 F_a(x,y) = F_a(ux,uy).$$

4. Le corps $L = K(\sqrt[n]{q})$.

Notons $\mathfrak{f}$ le conducteur de l'extension abélienne L/K, $\mathfrak{O}_\mathfrak{f}$ l'ordre $B + \mathfrak{f}$ de K, $I(\mathfrak{f})$ le groupe des idéaux de K premiers à $\mathfrak{f}$ et $N(\mathfrak{f})$ le sous-groupe de $I(\mathfrak{f})$ engendré par les idéaux de la forme (x), où x appartient à $\mathfrak{O}_\mathfrak{f}$ et est premier à $\mathfrak{f}$.

PROPOSITION 5. — *L'application :* $\mathfrak{a} \longmapsto \mathfrak{a} \cap \mathfrak{O}_\mathfrak{f}$ *induit un isomorphisme de* $I(\mathfrak{f})/N(\mathfrak{f})$ *sur* $C1(\mathfrak{O}_\mathfrak{f})$.

Démonstration. — L'idéal $\mathfrak{f}$ étant un multiple du conducteur de l'anneau A dans $\mathfrak{O}_\mathfrak{f}$, l'application en question définit un isomorphisme entre les monoïdes des idéaux entiers premiers à $\mathfrak{f}$ dans A et dans $\mathfrak{O}_\mathfrak{f}$, dont la réciproque est : $\mathfrak{a} \longmapsto \mathfrak{a}.A$. On voit donc que les idéaux entiers de $N(\mathfrak{f})$ correspondent aux idéaux principaux étrangers à $\mathfrak{f}$ de $\mathfrak{O}_\mathfrak{f}$. Les quotients respectifs sont alors isomorphes, et $I(\mathfrak{f})/N(\mathfrak{f})$ est isomorphe au groupe des classes d'idéaux étrangers à $\mathfrak{f}$ de $\mathfrak{O}_\mathfrak{f}$. Tout idéal inversible de $\mathfrak{O}_\mathfrak{f}$ contenant dans sa classe un idéal étranger à $\mathfrak{f}$, ce dernier groupe est $C1(\mathfrak{O}_\mathfrak{f})$.

L'extension L/**Q** étant galoisienne, l'idéal $\mathfrak{f}$ est stable sous l'action de Δ. Les groupes $I(\mathfrak{f})/N(\mathfrak{f})$ et $C1(\mathfrak{O}_\mathfrak{f})$ sont alors des Δ-modules et l'isomorphisme de la proposition 5 est un isomorphisme de Δ-modules. Passons maintenant à la décomposition des idéaux premiers dans L/K.

LEMME. — *Le transfert :* $G^{ab} \longmapsto H$ *est nul.*

Démonstration. — Si $\ell \neq 2$, H est le sous-groupe des commutateurs de G. Le groupe G^{ab} est donc d'ordre 2 et H d'ordre impair, d'où le résultat (qui est un cas particulier évident du théorème de Furtwängler).

Si $\ell = 2$, le groupe des commutateurs de G est le sous-groupe d'indice 2 de H. Le groupe G est produit semi-direct de $\{\pm 1\}$ par $\mathbf{Z}/n\mathbf{Z}$. Un système de représentants dans G de G^{ab} est formé par (1,0), (1,1), (−1,0) et (−1,1) tandis que (1,0) et (−1,0) forment un système de représentants dans G de G/H. Les formules explicites de calcul du transfert

(cf. [3]) donnent alors :

$$\left.\begin{array}{l}(1,1) * (1,0) = (1,0) * (1,1)\\ (1,1) * (-1,0) = (-1,0) * (1,-1)\end{array}\right\} \quad \text{donc} \quad \begin{array}{l}\mathrm{Ver}(1,1)\\ = (1,1) * (1,-1) = (1,0)\end{array}$$

$$\left.\begin{array}{l}(-1,0) * (1,0) = (-1,0) * (1,0)\\ (-1,0) * (-1,0) = (1,0) * (1,0)\end{array}\right\} \quad \text{donc} \quad \begin{array}{l}\mathrm{Ver}(-1,0)\\ = (1,0) * (1,0) = (1,0)\end{array}$$

enfin $(-1,1) = (1,1) * (-1,0)$ donc

$$\mathrm{Ver}(-1,1) = \mathrm{Ver}(1,1) * \mathrm{Ver}(-1,0) = (1,0),$$

d'où le résultat.

PROPOSITION 6. — *Le sous-groupe* $H(\mathfrak{f})$ *de* $I(\mathfrak{f})$ *attaché par la théorie du corps de classes à l'extension* L/K *contient* $N(\mathfrak{f})$.

Démonstration. — Le groupe $N(\mathfrak{f})$ est engendré par les idéaux de la forme (x) de deux types : soit x est congru à 1 modulo $\mathfrak{f}$, soit x appartient à B et x premier à $\mathfrak{f}$. Par définition du conducteur, les idéaux du premier type sont dans $H(\mathfrak{f})$. D'autre part, si y est un élément de B premier au discriminant de L et $F_{L/K^+}(y.B) \in G^{ab}$, l'image de l'idéal $y.B$ par l'isomorphisme de réciprocité, on sait que $F_{L/K}(y.A)$ est le transfert dans H de $F_{L/K^+}(y.B)$. C'est donc 1 d'après le lemme, ce qui signifie que l'idéal (y) est dans $H(\mathfrak{f})$. Enfin si x est dans B et étranger à $\mathfrak{f}$, il existe un élément y de B étranger au discriminant de L et tel que $x.y^{-1}$ soit congru à 1 modulo $\mathfrak{f}$. D'après ce qui précède, (y) et $(x.y^{-1})$ sont dans $H(\mathfrak{f})$, donc aussi (x), d'où la proposition.

Le type de décomposition dans L d'un idéal premier de K ne divisant pas $\mathfrak{f}$ ne dépend donc que de sa classe dans $I(\mathfrak{f})/N(\mathfrak{f})$, ou encore de son image dans $C1(\mathfrak{O}_{\mathfrak{f}})$.

PROPOSITION 7. — *Soit* p *un nombre premier congru à* 1 *modulo* n *et ne divisant pas* q. *Les propositions suivantes sont équivalentes :*

(i) *tout idéal entier* $\mathfrak{a}$ *de* A *tel que* $\mathfrak{a}\bar{\mathfrak{a}} = (p)$ *est dans* $H(\mathfrak{f})$;

(ii) *si* 8 *ne divise pas* n, p *est totalement décomposé dans* $L/\mathbf{Q}$ *et, si* 8 *divise* n, *le degré résiduel des idéaux de* L *au-dessus de* p *est* 1 *ou* 2.

Démonstration. — Le nombre premier p est décomposé dans K. Soit $\mathfrak{p}$ un de ses diviseurs premiers dans K. Dire que $\mathfrak{a}$ est entier et vérifie

$\mathfrak{a}\bar{\mathfrak{a}} = (p)$, c'est dire que $\mathfrak{a}$ est produit de la moitié des conjugués, un dans chaque paire $\{\mathfrak{p},\bar{\mathfrak{p}}\}$; il est donc clair que (i) signifie qu'un tel $\mathfrak{a}$ existe dans $H(\mathfrak{f})$ et que $\mathfrak{p}$ est congru à $\bar{\mathfrak{p}}$ modulo $H(\mathfrak{f})$. Si n est égal à 4, cela signifie seulement que $\mathfrak{p}$ est dans $H(\mathfrak{f})$, c'est-à-dire décomposé dans L/K, d'où le résultat dans le cas $n = 4$. D'autre part le Δ-module $I(\mathfrak{f})/N(\mathfrak{f})$ est isomorphe au Δ-module H, ou encore au $(\mathbf{Z}/n\mathbf{Z})^*$-module $\mathbf{Z}/n\mathbf{Z}$, la conjugaison complexe correspondant à la multiplication par -1. Dire que $\mathfrak{p}$ et $\bar{\mathfrak{p}}$ sont congrus modulo $H(\mathfrak{f})$ équivaut à ce que l'image x de $\bar{\mathfrak{p}}$ dans $I(\mathfrak{f})/N(\mathfrak{f})$ (isomorphe à $\mathbf{Z}/n\mathbf{Z}$) vérifie $x = -x$.

Si n est impair, la condition (i) signifie donc seulement $x = 0$, soit $\mathfrak{p}$ dans $H(\mathfrak{f})$ ou encore $\mathfrak{p}$ décomposé dans $L/\mathbf{Q}$.

Si 8 divise n, cela signifie $x = 0$ ou $n/2$. Les images de tous les conjugués de $\mathfrak{p}$ sont alors égales à x, et $\mathfrak{a}$ qui est produit d'un nombre pair de conjugués de $\mathfrak{p}$ a pour image 0 et est dans $H(\mathfrak{f})$. La condition (i) se résume alors à $x = 0$ ou $n/2$, i.e. $\mathfrak{p}$ d'ordre 1 ou 2 dans $I(\mathfrak{f})/N(\mathfrak{f})$, ce qui veut dire que le degré résiduel des idéaux de L au-dessus de $\mathfrak{p}$ est 1 ou 2. La proposition est complètement démontrée.

THÉORÈME. — *Si* 8 *ne divise pas* n, *il existe un ensemble fini dépendant de* n *et de* q *de formes quadratiques binaires à coefficients dans* B *tel que* q *est un résidu de puissance* n-ième *modulo* p *si et seulement si aucune de ces formes ne représente* p.

Si 8 *divise* n *il existe un ensemble fini de formes quadratiques binaires à coefficients dans* B *tel que* q *est un résidu de puissance* $n/2$-ième *modulo* p *si et seulement si aucune de ces formes ne représente* p.

Démonstration. — La forme associée à une classe de $Cl(\mathfrak{O}_\mathfrak{f})$ n'appartenant pas au noyau de l'homomorphisme

$$Cl(\mathfrak{O}_\mathfrak{f}) \simeq I(\mathfrak{f})/N(\mathfrak{f}) \to I(\mathfrak{f})/H(\mathfrak{f})$$

représente p si et seulement si l'inverse de cette classe contient un idéal entier $\mathfrak{a}$ tel que

$$\mathfrak{a}\bar{\mathfrak{a}} = [\mathfrak{O}_\mathfrak{f} : \mathfrak{a} \cap \mathfrak{O}_\mathfrak{f}]_B = (p).$$

Une de ces formes représente donc p si, et seulement si, il existe un idéal entier $\mathfrak{a}$ tel que $\mathfrak{a}\bar{\mathfrak{a}} = (p)$ qui n'est pas dans $H(\mathfrak{f})$, c'est-à-dire, d'après la proposition précédente, si p n'est pas totalement décomposé dans le cas où

8 ne divise pas n, ou si le degré des diviseurs de p n'excède pas 2 dans le cas où 8 divise n. Enfin la traduction en termes de résidus de puissances est immédiate.

5. Les systèmes diophantiens.

Le fait que p est représenté par une forme quadratique binaire à coefficients dans B se traduit de manière évidente en une réalité palpable, c'est-à-dire qu'on peut expliquer à un ordinateur. Le **Z**-module B est libre de rang $r = (1/2)\varphi(n)$; choisissons-en une base $1 = a_1, \ldots, a_r$. Si F est une forme quadratique binaire à coefficients dans B, l'équation

$$F(x,y) = p$$

s'écrira

$$\begin{aligned} p &= \varphi_1(X_1,\ldots,X_r,Y_1,\ldots,Y_r) \\ 0 &= \varphi_i(X_1,\ldots,X_r,Y_1,\ldots,Y_r) \quad i = 2,\ldots,r \end{aligned}$$

où $x = \Sigma X_i a_i$, $y = \Sigma Y_i a_i$, et $F = \Sigma \varphi_i a_i$; les φ_i sont des formes quadratiques à coefficients entiers. Il est à noter que, si l'on prend $a_i = \zeta_n^i + \zeta_n^{-i}$, l'élément $\varphi_1(x,y)$ de Z est la trace d'un entier totalement positif, divisée par r. On en déduit que φ_1 est définie positive et que l'existence d'une solution en nombres entiers du système quadratique précédent est décidable en un nombre fini de pas.

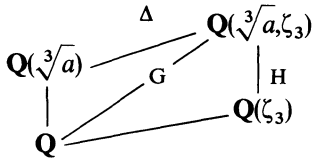
6. Quelques exemples.

Donnons un exemple d'application de ce qui précède. Si p est un nombre premier congru à 1 modulo 9, une condition nécessaire et suffisante pour que 2 soit résidu de puissance neuvième modulo p est qu'aucun des systèmes $\mathbf{Q}_i$, $i \in [1,7]$,

$$\mathbf{Q}_i \begin{cases} p = \varphi_i^1(X_1,\ldots,X_6) \\ 0 = \varphi_i^2(X_1,\ldots,X_6) \\ 0 = \varphi_i^3(X_1,\ldots,X_6) \end{cases}$$

où les φ_i sont des formes quadratiques à coefficients entiers, n'ait de solutions entières. Les valeurs des coefficients des φ_i sont calculées dans [1].

L'exemple précédent souffre de la complication de son écriture détaillée. En voici un autre, dont il est curieux qu'il n'ait pas, apparemment, trouvé sa place dans la littérature (cf. pourtant [2]). Considérons le diagramme



où $a = 6$ ou 12. Si χ est un caractère non trivial de H et 1_Δ le caractère unité de Δ, on a, pour les caractères induits dans G :

$$1_\Delta^* = 1_G + \chi^*.$$

Le conducteur d'Artin de 1_Δ^* est le discriminant de $\mathbf{Q}(\sqrt[3]{a})$ soit $3^5.4$; or on a

$$\mathfrak{F}(\chi^*) = \delta_{\mathbf{Q}(\zeta_3)/\mathbf{Q}} \cdot N_{\mathbf{Q}(\zeta_3)/\mathbf{Q}}(\mathfrak{F}(\chi))$$

et on sait que le discriminant de $\mathbf{Q}(\zeta_3)$ est -3, donc

$$N(\mathfrak{F}(\chi)) = 3^4.4 \qquad \text{et} \qquad \mathfrak{f} = \mathfrak{F}(\chi) = 3^2.2 = 18.$$

Il s'agit donc d'étudier $C1(\mathfrak{O}_{18})$. L'anneau A est ici principal; il est alors clair qu'on a un isomorphisme naturel

$$C1(\mathfrak{O}_{18}) = (A/18A)^*/(B/18B)^*.\tilde{U}$$

où $\tilde{U}$ est l'image modulo 18 des unités de A. Ces dernières étant des racines de l'unité, $\tilde{U}$ peut être remplacé par $\langle\zeta_3\rangle$. Or on a

$$(A/18A)^*/(B/18B)^* = (A/9A)^*/(B/9B)^* \times (A/2A)^*/(B/2B)^*$$

et la composée de l'injection naturelle du premier facteur dans le produit et du passage au quotient par $\langle\zeta_3\rangle$ est un isomorphisme de $(A/9A)^*/(B/9B)^*$ sur $C1(\mathfrak{O}_{18})$. Le groupe $(A/9A)^*/(B/9B)^*$ est de type (3,3), engendré par ζ_3 et $1 + 3\zeta_3$, et la conjugaison y agit comme l'élévation au carré. Il y a donc cinq orbites ayant pour représentants dans $(A/9A)^*/(B/9B)^*$:

$$\tilde{a} = 1, \qquad \tilde{b} = \zeta, \qquad \tilde{c} = 1 + 3\zeta, \qquad \tilde{d} = 3 - \zeta, \qquad \tilde{e} = 1 - 5\zeta.$$

Les images dans $(A/18A)^*/(B/18B)^*$. $\tilde{U}$ sont :

$$\begin{aligned} a &= 1 & a^{-1} &= 1 \\ b &= -9-8\zeta & 73b^{-1} &= -1+8\zeta \\ c &= 1-6\zeta & 43c^{-1} &= 7+6\zeta \\ d &= 3+2\zeta & 7d^{-1} &= 1-2\zeta \\ e &= 1+4\zeta & 13e^{-1} &= -3-4\zeta. \end{aligned}$$

Si π est dans $\mathfrak{O}_{18} = \mathbf{Z} + 18\zeta\mathbf{Z}$, on peut écrire π sous la forme

$$\pi = (X-9Y)\zeta + (X+9Y)\zeta^2$$

donc $\pi\bar{\pi} = X^2 + 243Y^2$.

Pour que π appartienne à $\mathfrak{a}_i = a_i A \cap \mathfrak{O}_{18}$, il faut et il suffit que $a_i^{-1}\pi$ soit dans A. On trouve donc les conditions :

$$\begin{aligned} \pi \in \mathfrak{a}_b &\Leftrightarrow 73 \text{ divise } X+7Y \\ \pi \in \mathfrak{a}_c &\Leftrightarrow 43 \text{ divise } X+12Y \\ \pi \in \mathfrak{a}_d &\Leftrightarrow 7 \text{ divise } X+3Y \\ \pi \in \mathfrak{a}_e &\Leftrightarrow 13 \text{ divise } X-2Y. \end{aligned}$$

On fait le changement de variable $X = 73X' - 7Y$ et on divise par 73 le résultat obtenu. Après réduction, on obtient les formes suivantes :

$$\begin{aligned} \varphi_1 &= X^2 + 243Y^2 \\ \varphi_2 &= 4X^2 + 2XY + 61Y^2 \\ \varphi_3 &= 9X^2 + 6XY + 28Y^2 \\ \varphi_4 &= 7X^2 + 6XY + 36Y^2 \\ \varphi_5 &= 13X^2 + 4XY + 19Y^2 \end{aligned}$$

Tout nombre premier p congru à 1 modulo 3 est représenté par l'une des cinq formes précédentes et une seule, et l'on a

2 est un cube modulo p si et seulement si φ_1 ou φ_3 représente p;
3 est un cube modulo p si et seulement si φ_1 ou φ_2 représente p;
6 est un cube modulo p si et seulement si φ_1 ou φ_4 représente p;
12 est un cube modulo p si et seulement si φ_1 ou φ_5 représente p.

BIBLIOGRAPHIE

[1] D. BERNARDI, Résidus de puissances, Thèse de 3e cycle, Publications mathématiques d'Orsay, n° 158 (1979).
[2] A. CUNNINGHAM et T. GOSSET, On 4-tic and 3-bic residuacity tables, *Messenger of Math.*, 50 (1920), 1-30.
[3] M. HALL, The theory of Groups, Macmillan, 1959.
[4] J. M. MASLEY, Solutions of small class number problems for Cyclotomic fields, *Compositio Math.*, 33 (1976), 179-186.
[5] J. M. MASLEY et H. L. MONTGOMERY, Cyclotomic fields with unique factorisation, *J. reine angew. Math.*, 286-287 (1976), 248-256.
[6] W. NARKIEWICZ, Elementary and analytic theory of numbers, Warszawa, 1974.
[7] P. SATGÉ, Décomposition des nombres premiers dans des extensions non abéliennes, *Annales de l'Institut Fourier*, 27 (1977), 1-8.

Manuscrit reçu le 7 novembre 1979
révisé le 13 mai 1980.

Dominique BERNARDI,
Université de Paris VI
Mathématiques
4, place Jussieu
75230 Paris Cedex 05.