Groupe de travail
d'analyse ultramétrique

Pierre Jean Desnoux

Congruences dyadiques entre nombres de classes de corps quadratiques

Groupe de travail d'analyse ultramétrique, tome 13 (1985-1986), p. 31-45

<http://www.numdam.org/item?id=GAU_1985-1986__13__31_0>

CONGRUENCES DYADIQUES ENTRE NOMBRES DE CLASSES DE CORPS QUADRATIQUES

Pierre Jean Desnoux

1. NOTATIONS ET PRINCIPE DE LA PREUVE

Dans les généralités p-adiques, qui seront ensuite spécifiées à p = 2, nous utilisons les notations traditionnelles (cf. [A], [W], [Bar]...). ω est le caractère de Teichmüller; $\langle\ \rangle$ est le caractère défini sur $\mathbb{Z}_p^*$ par $\langle a\rangle = (\omega(a))^{-1}a$.

*Nous utilisons les fonctions L_p (fonctions L p-adiques) (cf. [K-L], [W] p.56, [Bar] p 13)...): Nous fixons le choix d'un plongement de $\overline{\mathbb{Q}}$ dans $\mathbb{C}_p$; soit χ un caractère de Dirichlet primitif, dont les valeurs sont vues dans $\mathbb{C}_p$. Soit $\rho_p = qp^{-1/(p-1)}$. Les $B_{n,\chi}$ sont les nombres de Bernoulli généralisés. Alors :

Théorème 0 : a) Il existe une unique fonction $L_p(s,\chi)$, méromorphe (analytique si $\chi \neq 1$) sur $D(1,\rho_p^-)$ telle que $\forall n\in\mathbb{N}^*$, $L_p(1-n,\chi) = -(1-(\chi\omega^{-n})(p).p^{n-1})(B_{n,\chi\omega^{-n}}/n)$

b) pour tout multiple entier non nul F de q et du conducteur f de χ,

$$L_p(s,\chi) = (1/F)(1/(s-1))\ {\sum_{1\leqslant a\leqslant f}}'\ \chi(a)\langle a\rangle^{1-s}\ \sum_{j\geqslant 0}\binom{1-s}{j}.B_j.\left(\frac{F}{a}\right)^j \quad ([W])$$

c) $sL_p(1+s,\chi) = \lim_{h\to\infty}(1/fp^h)\ {\sum_{0\leqslant a\leqslant fp^h}}'\ \chi(a)\langle a\rangle^{-s}$ ([K-L]; [Bar])

Remarques: 1) $\chi\omega^{-n}$ est le produit (primitif) des deux caractères χ et ω^{-n}; 2) Σ' désigne une sommation sur les entiers premiers à p; 3) Pour $x\in\mathbb{C}_p$, $\binom{x}{j} = x(x-1)...(x-j+1)/j!$; 4) La formule c) est imprimée par erreur dans [Bar] avec un signe moins.

d désignera un entier libre de carrés positif. $K_+ = \mathbb{Q}(\sqrt{d})$, $K_- = \mathbb{Q}(\sqrt{-d})$. χ_+ (respectivement χ_-) est le caractère quadratique associé à K_+ (respectivement K_-). $h(K_+)$ (respectivement $h(K_-)$) est le nombre de classes de K_+ (respectivement K_-). D_+ et D_- sont leurs discriminants.

Nous noterons ε (respectivement u, respectivement η) l'unité fondamentale (> 1) de K_+ (respectivement le générateur du sous-groupe des unités positives de $\mathbb{Z}[\sqrt{d}]$, respectivement le générateur de norme 1 du sous-groupe des unités positives de $\mathbb{Z}[\sqrt{d}])$). C'est-à-dire qu'on a $u=\alpha+\beta\sqrt{d}$, avec α et $\beta > 0$, et $\alpha^2-d\beta^2=\pm 1$, tous les autres éléments de $\mathbb{Z}[\sqrt{d}]$ vérifiant des conditions analogues étant une puissance de u, tandis que $\eta = R + S\sqrt{d}$, avec R et $S > 0$, et $R^2-dS^2 = 1$, tous les autres éléments de $\mathbb{Z}[\sqrt{d}]$ vérifiant des conditions analogues étant une

puissance de η; $\eta = u$ ou u^2 suivant que $\alpha^2 - d\beta^2 = 1$ ou $\alpha^2 - d\beta^2 = -1$. Classiquement (cf. [S] p.78), $u = \varepsilon$, sauf si $d \equiv 1\ [4]$ et $\varepsilon = (a + b\sqrt{d})/2$ avec $a \equiv b \equiv 1\ [2]$, où $u = \varepsilon^3$. Nous poserons $u = \varepsilon^S$.

On dispose alors, pour l'évaluation des deux nombres de classes, de deux formules:

*Une formule valable dans les corps abéliens totalement complexes L, cf.[W] p.42:

$$(I)\quad h^-(L) = w(L).Q(L).\Pi[\,(-1/2)B_{1,\chi}\,]$$

où: $h^-(L)$ est le quotient (entier) de $h(L)$ par $h^+(L)$ ($h^+(L)$ est le nombre de classes du sous-corps réel maximal L^+ de L);

$w(L)$ est le cardinal de $W(L)$, groupe des racines de l'unité contenues dans L ;

$E(K)$ désignant le groupe des unités d'un corps K, $Q(L)$ est l'indice $[E(L):W(L)E(L^+)]$;

le produit $\Pi[\,(-1/2)B_{1,\chi}\,]$ est étendu aux caractères impairs χ de L.

*La formule analytique p-adique du nombre de classes pour les corps abéliens totalement réels M (cf. [W] p.71):

$$(II)\quad 2^{n-1}h(M)(R_p(M)/\sqrt{d(M)}\,) = \Pi[\,1 - (\chi(p)/p)\,]^{-1}L_p(1,\chi)$$

où : n est le degré de M, $d(M)$ est son discriminant;

le produit $\Pi[\,1 - (\chi(p)/p)\,]^{-1}L_p(1,\chi)$ est étendu aux caractères non triviaux de M ;

$R_p(M)$ est le régulateur p-adique de M; la définition en général de ce régulateur dépend d'un certain nombre de choix de plongements du corps dans $\mathbb{C}$ ou $\mathbb{C}_p$, cf. [W] p.70; le régulateur, et la racine, sont en fait déterminés au signe près; la formule signifie qu'on peut faire un choix donnant l'égalité. Toutefois, un résultat d'Amice et Fresnel (cf. [A-F]) indique comment faire ce choix: dans le cas qui nous intéresse, le quotient $(R_p(K_+)/\sqrt{D_+}\,)$ désigne $\log(\varepsilon)/\sqrt{D_+}$ (où la racine de D_+ et celle qui figure dans ε ont été plongées de la même façon dans $\mathbb{C}_p^*$).

Nous calculerons les différents facteurs qui interviennent dans (I) et (II) . Ainsi, (I) ramènera $h(K_-)$ à $L_2(0,\chi_+)$. On aura alors une relation entre $h(K_+)$ et $h(K_-)$, affectés de certains coefficients, exprimée à l'aide de la différence $\Delta = L_2(1,\chi_+) - L_2(0,\chi_+)$.

Cette idée de ramener la comparaison de nombres de classes à celle de valeurs prises par une fonction L_p en 0 et en 1 figure dans Washington (pour retrouver un résultat de divisibilité par 3 des nombres de classes de $\mathbb{Q}(\sqrt{3m}\,)$ et $\mathbb{Q}(\sqrt{-m}\,)$, cf. [W] p.83).

Ici, il faudra aller plus loin dans l'étude de Δ. Nous utiliserons la description des fonctions L_p par les séries l_θ due à Iwasawa, (cf.[Iw]), et une explicitation de ces séries due à Barsky (cf.[Bar]). Δ pourra être alors calculé mod 16. En comparant les différents Δ obtenus pour d et 2d (d impair), on peut obtenir une relation mod 64, où la contribution des fonctions L_2 est exprimée en termes de congruences des diviseurs de d. Nous renvoyons à [D], où l'on trouvera aussi tous les détails des calculs et des preuves.

2. LE THEOREME ET SES APPLICATIONS

La quantité $\mathbf{1}_{x \equiv a\,[n]}$ vaut 1 si $x \equiv a\,[n]$, et 0 sinon.

THEOREME : Soit d un entier libre de carrés, $d \geqslant 5$; soient $h(d)$ et $h(-d)$ les nombres de classes au sens restreint (deux idéaux sont équivalents s'ils diffèrent d'un idéal principal engendré par un élément du corps de norme strictement positive) de $\mathbb{Q}(\sqrt{d})$ et $\mathbb{Q}(\sqrt{-d})$ respectivement. Alors, modulo 16 :

$$c_1 h(-d) + c_2 (RS/2)(-1)^R h(d) \equiv \begin{cases} 8.\mathbf{1}_{p \equiv \pm 3 \pm 7\,[16]} & \text{si } d = p \text{ ou } 2p \\ & (p \text{ premier impair}) \\ 8.\mathbf{1}_{p \equiv \pm 3\,[8]}.\mathbf{1}_{q \equiv \pm 3\,[8]} & \text{si } d = pq \text{ ou } 2pq \\ & (p, q \text{ premiers impairs}) \\ 0 & \text{sinon} \end{cases}$$

où $c_1 = 1$ si $d \equiv 1, 2\,[4]$; $c_1 = 0$ si $d \equiv 7\,[8]$; $c_1 = 2$ si $d \equiv 3\,[8]$.

$c_2 = 1$, sauf si $d \equiv 5\,[8]$ et si l'unité fondamentale ε de $\mathbb{Q}(\sqrt{d})$ vérifie $\varepsilon \in \mathbb{Z}[\sqrt{d}]$ où $c_2 = 3$.

(R,S) est la solution minimale en nombres entiers de $R^2 - dS^2 = 1$.

En détaillant suivant les valeurs de d, on peut obtenir de nombreux résultats prouvés séparément et par divers auteurs dans la littérature, notamment pour $d = p \equiv 1\,[8]$ (Williams), $d = p \equiv 5\,[8]$ (Kaplan et Williams), $d = 2p$, $p \equiv 1\,[4]$ (Kaplan et Williams), $d = pq$, p et $q \equiv 1\,[4]$ (Kaplan et Williams)... On obtient aussi des résultats nouveaux, pour $d = 2p$, $p \equiv 3\,[4]$, $d = pq$, $p \equiv q \equiv 3\,[4]$, ou pour $l(d) \geqslant 3$. Nous renvoyons à [D] où figure une comparaison systématique des résultats contenus dans le Théorème et des résultats antérieurs ou démontrés simultanément.

Georges Gras nous a adressé, après l'achèvement de ces travaux, un papier où il étudie les valeurs des $L_p(s,\chi)$ pour χ pair associé à une quelconque extension abélienne finie de $\mathbb{Q}$ (cf. [G]). Il y donne notamment une congruence générale pour $L_p(s,\chi) - L_p(t,\chi)$ modulo une puissance de p variable mais, dans le cas d'un corps quadratique par exemple, grosso modo d'autant plus élevée qu'il y a de diviseurs du discriminant. Ces résultats sont évidemment trop

généraux pour paraître vraiment explicites. Par ailleurs, quand il y a peu de diviseurs, ces énoncés ne fournissent pas dans tous les cas une congruence suffisamment élevée. Mais l'auteur explique également comment on peut raffiner dans certains cas, et traite en exemple celui où χ est quadratique pair de conducteur 8p, p premier , $p \equiv 1\ [4]$, suivant des techniques susceptibles d'être généralisées. Tous ces résultats fournissent en tout cas un guide précieux pour des recherches ultérieures qui exploiteraient les méthodes que nous avons utilisées.

3. PREMIERES EXPLICITATIONS

Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique de discriminant D; χ associé à K est un caractère primitif, d'ordre 2, de conducteur $|D|$ (valeur absolue réelle de D), explicitement: $\chi = (\frac{D}{\cdot})$

(Soit $m \in \mathbb{Z}$; si $m \wedge D \neq 1$, $(\frac{D}{m}) = 0$;

si $m \wedge D = 1$, $(\frac{D}{m}) = {}_{v_p(m)} \sqcap \equiv 1\ [2]\ (\frac{D}{p})$ ($= {}_{p\ \text{premier}} \sqcap (\frac{D}{p})^{v_p(m)}$),

où $v_p(m)$ est la valuation p-adique de m, $(\frac{D}{p})$ est le symbole de Legendre si p est impair,

$(\frac{D}{2})$ vaut $(-1)^{((D^2-1)/8)}$ si $D \wedge 2 = 1$, et 0 sinon.)

On vérifie alors, si ω le caractère de Teichmüller 2-adique:

Proposition 1 : $\chi_- = \chi_+ \omega$. Si $d \equiv 1, 2\ [4]$: $\chi_-(2) = 0$; si $d \equiv 3\ [4]$: $\chi_-(2) = (-1)^{((d^2-1)/8)}$. Si $d \equiv 1\ [4]$: $\chi_+(2) = (-1)^{((d^2-1)/8)}$; si $d \equiv 2, 3\ [4]$: $\chi_+(2) = 0$.

Les notations se simplifient dans un corps quadratique imaginaire, (I) s'écrit $h(-d) = -B_{1,\chi_-}$

Puis, par définition des fonctions L_2 , avec n = 1 :

$L_2(0,\chi_+) = -(1 - (\chi_+\omega^{-1})(2))\, B_{1,\chi_+\omega^{-1}} = -(1 - \chi_-(2))\, B_{1,\chi_-}$ (ici $\omega^{-1} = \omega$).

Ainsi (I) s'écrit encore : $L_2(0,\chi_+) = (1 - \chi_-(2))\, h(-d)$, ou, par la Proposition 1:

Proposition 2 : $L_2(0,\chi_+) = c_1\, h(-d)$, avec $c_1 = 1$, sauf si $d \equiv 3\ [8]$: $c_1 = 2$ ou si $d \equiv 7\ [8]$: $c_1 = 0$

Nous exprimons ensuite $\log(\varepsilon)$ en fonction de $\log(\eta)$, pour unifier les notations ($x^2 - dy^2 = 1$ a toujours des solutions) et surtout pour pouvoir approximer le terme $\log(\varepsilon)/\sqrt{D_+}$.

En partant de: $2h(K_+)\log(\varepsilon) = h(d)\log(\eta)s^{-1}$, de la valeur de $1 - (\chi_+(2)/2)$ (Proposition 1) et en distinguant suivant $d \equiv 1\ [8]$, $d \equiv 5\ [8]$, $d \not\equiv 1\ [4]$, il vient:

Lemme 3 : $(1 - (\chi_+(2)/2))\, 2h(K_+)\, (\log(\varepsilon)/\sqrt{D_+}) = c_2\, T\, h(d)$

où $c_2 = 1$, sauf si $d \equiv 5\ [8]$ et si $\varepsilon = u$ (i.e. $s = 1$), où $c_2 = 3$, et $T = \log(R + S\sqrt{d})/2\sqrt{d}$.

Lemme 4. : On a l'un des deux cas suivants (dans les deux cas, $T \in \mathbb{Z}_2$):

1) R est impair, S est pair, et

$$T = \frac{S}{2R} \sum_{k \geq 0} \frac{1}{2k+1} \left(\frac{S}{R}\right)^{2k} d^k$$

2) R est pair, S est impair, et

$$T = \frac{R}{2dS} \sum_{k \geq 0} \frac{1}{2k+1} \left(\frac{R}{S}\right)^{2k} d^{-k}$$

Démonstration : $R^2 - dS^2 = 1 \Rightarrow$ R ou S est impair; mais ils ne le sont pas tous les deux, sinon, mod 8, $1-d \equiv 1$, absurde. Si R est impair et S pair, écrivons $\log(R+S\sqrt{d}) = \log(R) + \log(1+(S/R)\sqrt{d})$; on a ici $|(S/R)\sqrt{d}| < 1$: $\log(R+S\sqrt{d}) = \log(R) + \sum_{n \geq 1} ((-1)^{n+1}/n)((S/R)\sqrt{d})^n$; de même: $\log(R-S\sqrt{d}) = \log(R) + \sum_{n \geq 1} ((-1)^{n+1}/n)(-(S/R)\sqrt{d})^n$.

Mais $R^2 - dS^2 = 1$, donc la somme de ces deux lignes est nulle; par différence, il vient:

$2\log(R+S\sqrt{d}) = \sum_{n \geq 1} ((-1)^{n+1}/n)((S/R)\sqrt{d})^n (1-(-1)^n)$; d'où le résultat pour T.

On sait la série écrite convergente a priori (on le revérifie sans peine), sa somme est donc dans $\mathbb{Q}_2$ (complet) et en fait dans $\mathbb{Z}_2$ (car S/2R est 2-entier ainsi que tous les termes de la série). Preuve analogue si R est pair et S impair.

Proposition 5 : $L_2(1,\chi_+) \equiv c_2 (RS/2)(-1)^{R+1} h(d)$ [16]

Démonstration : On a $L_2(1,\chi_+) = c_2 T h(d)$ (formule (1) plus Lemme 3). Si R impair, $R^2 \equiv 1$ [8], d'où $dS^2 \equiv 0$ [8] $\Rightarrow S \equiv 0$ [4], et alors $R^2 \equiv 1$[16]. Dans 1), on a 2 en facteur de la série, dont le terme général est de valuation au moins 4k; pour une évaluation mod 16, on peut donc s'arrêter au premier terme. Il vient: $T \equiv (S/2R) \equiv (RS/2)$ [16]. Si R est pair, d est impair; de plus $N(u)=1$ donc $2 \mid h(d) = 2h(K_+)$: il suffit de connaître T mod 8. Dans 2) le terme général est de valuation au moins 2k, et dépasse donc 3 pour $k \geq 2$. On garde donc ici deux termes. En remplaçant dS^2 par $R^2 - 1$, il vient $T \equiv (RS/2)(1/(R^2-1))(1+R^2/3(R^2-1)) \equiv -(RS/2)$ [8].

Proposition 6 : Notons $\Delta(d)$ la quantité $L_2(1,\chi_+) - L_2(0,\chi_+)$, χ_+ étant le caractère associé à $\mathbb{Q}(\sqrt{d})$. Alors: $c_1 h(-d) + c_2(RS/2)(-1)^R h(d) \equiv -\Delta(d)$ [16].

Démonstration : Il suffit de recoller les morceaux. Il reste à évaluer $\Delta(d)$ mod 16.

4. FACTORISATION DES CARACTERES

On obtient sans difficulté les deux lemmes suivants ([Bar]):

Lemme 7 : On a un isomorphisme: $\ell : (1 + q\mathbb{Z}_p, \times) \longrightarrow (\mathbb{Z}_p, +)$

$$u \quad \rightsquigarrow -\log(u)/\log(1+q)$$

de réciproque : $e : (\mathbb{Z}_p, +) \longrightarrow (1 + q\mathbb{Z}_p, \times)$

$$v \quad \rightsquigarrow \exp(-\log(1+q)\,v).$$

ℓ vérifie : $|\ell(a) - \ell(b)| = |a-b|/|q|$ et transforme $1+qp^h\mathbb{Z}_p$ en $p^h\mathbb{Z}_p$; en particulier:

$$\mathbb{Z}_p/p^h\mathbb{Z}_p \cong (1 + q\mathbb{Z}_p)/(1 + qp^h\mathbb{Z}_p) \text{ (noté } G_h).$$

Lemme 8 : on a un deux isomorphismes: $\theta_h : (\mathbb{Z}_p/qp^h\mathbb{Z}_p)^* \cong \mu_{\varphi(q)}(1) \times G_h$

et $\Theta : (\mathbb{Z}/_{mqp^h\mathbb{Z}})^* \cong (\mathbb{Z}/_{mq\mathbb{Z}})^* \times G_h$ (par l'application naturelle).

Ceci permet d'obtenir une factorisation des caractères.

Un caractère de Dirichlet χ est dit "de première espèce" (sous-entendu : par rapport à p) s'il est de conducteur f_χ tel que $f_\chi = m$ ou mq (avec $m \wedge p = 1$)

Pour définir les caractères "de deuxième espèce", reprenons l'isomorphisme θ_h du lemme 8, et notons encore: $\theta_h : (\mathbb{Z}/qp^h\mathbb{Z})^* \cong \mu_{\varphi(q)}(1) \times G_h$, d'où $\langle\theta_h\rangle : \langle(\mathbb{Z}/qp^h\mathbb{Z})^*\rangle \cong \langle\mu_{\varphi(q)}(1)\rangle \times \langle G_h\rangle$

(Pour G un groupe commutatif, $\langle G\rangle$ est mis pour le traditionnel $\hat{G}$, groupe des caractères de G).

Tout élément de $\langle G_h\rangle$ peut donc se voir comme un caractère modulo qp^h, trivial sur l'image réciproque par θ_h de $\mu_{\varphi(q)}(1) \times \{1\}$: un tel caractère de Dirichlet sera pour nous, par définition, un caractère de deuxième espèce mod qp^h. Il est de la forme $x \mapsto \varphi(\overline{\langle x\rangle})$ pour un $\varphi \in \langle G_h\rangle$. Et:

Proposition 9 : Soit χ primitif, supposons $f_\chi = mqp^h$; alors $\langle(\mathbb{Z}/_{mqp^h\mathbb{Z}})^*\rangle \cong \langle(\mathbb{Z}/_{mq\mathbb{Z}})^*\rangle \times \langle G_h\rangle$ fournit une décomposition $\chi = \chi_1\,\chi_2$ où χ_i est de i^{e} espèce. On a unicité au sens que χ_1^* et χ_2^* (caractères primitifs induits) sont uniques ; $\chi = \chi_1^*\,\chi_2^*$. Si $f_\chi = mq$, $\chi_1^* = \chi$ (conducteur mq) et $\chi_1^* = \mathbf{1}$ (conducteur 1). Si $f_\chi = mqp^h$, $h \geqslant 1$, $f_{\chi_1^*} = m$ ou mq, et $f_{\chi_2^*} = qp^h$.

On peut préciser les caractères de deuxième espèce. Il suffit d'étudier les caractères sur G_h. Un caractère sur G_h est défini par sa valeur sur un générateur de G_h (on peut prendre par exemple 1 + q, ou 1 + mq, ...) pourvu que cette valeur soit dans $\mu_{p^h}(1)$.

Pour simplifier les calculs finals, nous prendrons 1 + q comme générateur. Nous signalerons les modifications que cela entraîne par rapport au papier de Barsky ([Bar]) (où c'est 1+mq qui a été choisi).

Ainsi, pour tout $h \geqslant 0$, pour tout choix de $\zeta \in \mu_{p^h}(1)$, il existe un unique caractère χ sur G_h tel que $\chi(\overline{1+q}) = \zeta^{-1}$; nous le notons ϖ_ζ. $\zeta \mapsto \varpi_\zeta$ est une réalisation d'un isomorphisme $\mu_{p^h}(1) \cong \langle G_h\rangle$.

Proposition 10 : pour tout a de $1+q\mathbb{Z}_p$, on a $\varpi_\zeta(\overline{a}) = \zeta^{\ell(a)}$ où ℓ est l'isomorphisme du lemme 7.

Démonstration : Soit $\zeta \in \mu_{p^h}(1)$; $\zeta^{\ell(a)}$ est défini par la série $\sum_{k\geq 0}(\zeta-1)^k \binom{\ell(a)}{k}$ où, pour $x \in \mathbb{C}_p$, $\binom{x}{k} = (x(x-1)\ldots(x-k+1))/k!$. ($\ell(a) \in \mathbb{Z}_p$, donc $|\binom{\ell(a)}{k}| \leq 1$; de plus, pour $\zeta \in \mu_{p^h}(1)$ d'ordre $o(\zeta)$, on a classiquement $|\zeta-1|<1$, car $|\zeta-1| = p^{-1/(p-1)\,p^{\alpha(\zeta)-1}}$; la série est donc convergente.)

Pour a et b dans $1+q\mathbb{Z}_p$, tels que $a \equiv b \bmod 1+qp^h\mathbb{Z}_p$, on a $\ell(a) \equiv \ell(b) \bmod p^h\mathbb{Z}_p$ donc $\zeta^{\ell(a)} = \zeta^{\ell(b)}$. C'est dire que $a \longmapsto \zeta^{\ell(a)}$ est définie sur G_h ; de plus, c'est un caractère de G_h, puisque ℓ est un morphisme. Enfin $\zeta^{\ell(1+q)} = \zeta^{-1}$: par unicité, on a le résultat attendu.

Corollaire 11 : tout caractère de deuxième espèce χ_2 vérifie: $\forall \bar{a} \in (\mathbb{Z}/qp^h\mathbb{Z})^*$ $\chi_2(\bar{a}) = \zeta^{\psi(a)}$

ou encore $\forall a \in \mathbb{Z}\backslash p\mathbb{Z}$, $\chi_2(a) = \zeta^{\psi(a)}$

où $\psi(a) = -\log(\langle a\rangle) / \log(1+q)$, pour un unique $\zeta \in \mu_{p^h}(1)$ $(h>0)$.

Définition 12 : pour $h>0$ et $\zeta \in \mu_{p^h}(1)$, nous notons π_ζ le caractère de deuxième espèce vérifiant les propriétés du corollaire 11.

5. CALCUL DE Δ PAR LES SERIES l_θ

Soit θ un caractère de Dirichlet primitif de première espèce, de conducteur m ou mq (m premier à p), K_θ l'extension de $\mathbb{Q}_p$ engendrée par les valeurs de θ, $\mathcal{O}_\theta$ son anneau d'entiers.

Une construction des séries l_θ d'Iwasawa est détaillée dans le papier de Barsky ([Bar], p.16 et suiv.). Toutefois, le choix de 1+q et non 1+mq comme générateur conduit à modifier les différentes fonctions intervenant aux différentes étapes de la construction. On obtient de façon analogue une série l_θ (de $\mathcal{O}_\theta[[T]]$) telle que:

$$l_\theta((1+q)^s\zeta - 1) = L_p(s, \theta\pi_\zeta),$$

où π_ζ vérifie : $\forall a \in \mathbb{Z}\backslash p\mathbb{Z}$, $\pi_\zeta(a) = \zeta^{\psi(a)}$ avec $\psi(a) = -\log(\langle a\rangle)/\log(1+q)$.

On trouve dans [Bar] le lemme suivant (lemme 8, p.21):

Lemme 13 : $\forall h>0$, $\forall k/\ 0\leq k\leq p^h-1$, les nombres entiers a satisfaisant aux deux conditions:

$$(1)\ 0\leq a\leq mqp^h-1 \text{ et } a\wedge mp = 1 \quad (2)\ |\psi(a)-k| \leq p^{-h}$$

constituent un $\varphi(mq)$-uplet, qui est un système complet de représentants de $(\mathbb{Z}/mq\mathbb{Z})^*$.

On a: $\{a;(1)\} = \bigcup_{0\leq k\leq p^h-1} \{a;(1),(2)\}$, l'union étant disjointe.

Démonstration : Soit $b = (1+q)^{-k} \in \mathbb{Z}_p$ ($\psi(b) = k$). Alors: $|\psi(a)-\psi(b)| \leq p^{-h} \Leftrightarrow |\ell(\langle a\rangle)-\ell(\langle b\rangle)| \leq p^{-h} \Leftrightarrow |\langle a\rangle-\langle b\rangle| \leq |qp^h| \Leftrightarrow \overline{\langle a\rangle} = \overline{\langle b\rangle}$ dans G_h. On conclut en considérant l'isomorphisme $\Theta: (\mathbb{Z}/mqp^h\mathbb{Z})^* \cong (\mathbb{Z}/mq\mathbb{Z})^* \times G_h$, $x \longmapsto (\bar{x}, \overline{\langle x\rangle})$.

Définition : $\Sigma_a^{(m,k,h)}$ désigne une somme étendue aux a tels que (1) et (2).

Remarque : $\Sigma_a^{(m,k,h)}\ \theta(a) = 0$ vu la preuve du lemme13.

Nous choisissons alors pour I_θ la description de la proposition 9 de [Bar] :

Proposition 14 : pour tout $h \geqslant 0$, il existe $I^*_{\theta,h}(T) \in \mathcal{O}_\theta[[T]]$ et $J_{\theta,h}(T) \in \mathcal{O}_\theta[[T]]$ telles que :

$$I_\theta(T) = I^*_{\theta,h}(T) + [(1+T)^{p^h} - 1]\, J_{\theta,h}(T).$$ On a :

$$I^*_{\theta,h}(T) = -\sum_{k=0}^{p^h-1} (1+T)^k \sum_a^{(m,k,h)} \theta(a)\ \frac{\langle a\rangle - (1+q)^{-k}}{mqp^h}$$

Lemme 15 : Soit χ un caractère de Dirichlet primitif de conducteur $f = m$ premier à p (auquel cas nous noterons $h_0 = 0$) ou de la forme mqp^{h_0} ($m \wedge p = 1$), différent de ω. Alors

$$L_p(0,\chi) = \lim_{h\to\infty} -(1/mqp^h) \sum'_{0 \leqslant a \leqslant mqp^{h-1}} \chi(a)\langle a\rangle$$

et en fait, dès que $h \geqslant h_0$: $L_p(0,\chi) = -(1/mqp^h) \sum'_{0 \leqslant a \leqslant mqp^{h-1}} \chi(a)\langle a\rangle$

Démonstration : La première égalité résulte du Théorème 0, c) avec $s = -1$. La deuxième vient de b) avec $s = 0$.

Démonstration de la proposition : Définissons pour $h \geqslant 0$ $I^*_{\theta,h}(T)$ comme dans la proposition; il s'agit d'une série à coefficients dans $\mathcal{O}_\theta$ par définition d'une somme $\Sigma_a^{(m,k,h)}$.

Soit $h_0 \geqslant 0$ fixé et $\zeta \in \boldsymbol{\mu}_{p^{h_0}}(\mathbf{1})$. $\chi = \theta\pi_\zeta$ satisfait aux conditions du lemme.

Pour $h \geqslant h_0$, soit
$$\begin{aligned} L_p(0,\chi) &= -(1/mqp^h) \sum'_{0 \leqslant a \leqslant mqp^{h-1}} \chi(a)\langle a\rangle \\ &= -(1/mqp^h) \sum_{0 \leqslant a \leqslant mqp^{h-1}} \theta(a)\zeta^{\psi(a)}\langle a\rangle \\ &= -\sum_{0 \leqslant k \leqslant p^{h-1}} \Sigma_a^{(m,k,h)} (\theta(a)\zeta^{\psi(a)}\langle a\rangle / mqp^h) \end{aligned}$$

Mais $|\psi(a) - k| \leqslant p^h$ puisqu'on somme sur des a tels que (1) et (2); or, $h \geqslant h_0 \Rightarrow \zeta^{p^h} = 1$, donc $\zeta^{\psi(a)} = \zeta^k$. Ainsi:

$$L_p(0,\chi) = -\sum_{0 \leqslant k \leqslant p^{h-1}} \zeta^k \Sigma_a^{(m,k,h)} (\theta(a)\langle a\rangle / mqp^h).$$

Pour utiliser ce résultat, il nous faut une série à coefficients entiers, ce qui n'est pas le cas. Mais on a remarqué: $\Sigma_a^{(m,k,h)}\ \theta(a) = 0$, donc $\Sigma_a^{(m,k,h)}\ \theta(a)(1+q)^{-k} = 0$. D'où:

$$L_p(0,\chi) = -\sum_{0 \leqslant k \leqslant p^{h-1}} \zeta^k \Sigma_a^{(m,k,h)} \theta(a)(\langle a\rangle - (1+q)^{-k}) / mqp^h).$$

Ainsi, pour $h \geqslant h_0$: $I^*_{\theta,h}(\zeta - 1) = L_p(0, \theta\pi_\zeta) = I_\theta(\zeta - 1)$; en particulier $I^*_{\theta,h_0}(\zeta - 1) = I_\theta(\zeta - 1)$.

En oubliant l'indice 0, nous avons obtenu $I^*_{\theta,h}(\zeta - 1) = I_\theta(\zeta - 1)\ \forall h \geqslant 0$; la proposition en résulte par un Lemme de continuité de la division euclidienne (cf. [A], Lemme 4.4.2. p.128.)

Désormais, $p = 2$ (donc $q = 4$) (ce qui pourra nous autoriser à utiliser la lettre p ailleurs que devant -adique).

Soit d un entier positif libre de carrés, $d \geq 5$; $K_+ = \mathbb{Q}(\sqrt{d})$ est associé au caractère χ_+, de conducteur D. χ_+ est primitif et d'ordre 2. Deux cas se présentent:

* d est impair: alors $D = d$ ou $4d$: χ_+ est de première espèce; sa factorisation est $\chi_+ = \chi_+ \mathbf{1} = \chi_+ \pi_1$. Nous poserons $\theta = \chi_+$ et $m = d$, et on a $\chi_+ = \theta\pi_1$.

* d est pair: alors $D = 4d = 8m$ en posant $m = d/2$ (impair). Ici $f_{\chi_+} = m.4.2^1$. On a une factorisation $\chi_+ = \chi_1 \chi_2$ donc aussi $\chi_+ = \chi_1^* \chi_2^*$; posons $\theta = \chi_1^*$ (caractère primitif de première espèce, de conducteur m ou 4m); $\chi_2(a) = \varphi(\langle a \rangle)$, où φ est un caractère sur $G_1 \cong \boldsymbol{\mu}_2(\mathbf{1}) = \{1, -1\}$. φ, ne pouvant être trivial, correspond à -1, i.e. $\chi_2 = \pi_{-1}$ (qui est primitif): on a $\chi_+ = \theta\pi_{-1}$.

Pour les deux cas, on peut donc noter: $\chi_+ = \theta\pi_\zeta$, où θ est un caractère primitif pair de conducteur m ou 4m, avec $m = d$ (resp $d/2$) et $\zeta = 1$ (resp -1) si d est impair (resp pair).

Nous disposons alors de la série I_θ telle que: $I_\theta(5^s\zeta - 1) = L_2(s, \chi_+)$

En application de la Proposition 14, nous pouvons énoncer:

Proposition 15 : $\forall h \geq 1$, $L_2(s, \chi_+) \equiv I^*_{\theta,h}(5^s\zeta - 1)\ [2^{h+2}]$.

Démonstration : $I_\theta(T) = I^*_{\theta,h}(T) + [(1+T)^{2^h} - 1]\, J_{\theta,h}(T)$, où $J_{\theta,h}(T) \in \mathcal{O}_\theta[[T]]$ ($= \mathbb{Z}_2[[T]]$ ici).

Substituons à T: $5^s\zeta - 1$, et regardons le terme $\alpha = (5^s\zeta)^{2^h} - 1$: $\zeta^{2^h} = 1$ puisque $h \geq 1$; si $s = 0$, $\alpha = 0$; si $s = 1$, $\alpha = \binom{2^h}{1}.4 + \binom{2^h}{2}.4^2 + \ldots$; or $v_2\left(\binom{2^h}{k}4^k\right) \geq h+2$ pour $k \geq 1$. Comme $J_{\theta,h}(5^s\zeta - 1)$ est entier, on a le résultat annoncé.

Corollaire 16 : $\Delta = L_2(1, \chi_+) - L_2(0, \chi_+) \equiv I^*_{\theta,h}(5\zeta - 1) - I^*_{\theta,h}(\zeta - 1)\ [2^{h+2}]$.

6. PRINCIPE DU CALCUL

On a ainsi:

$$-\Delta \equiv \sum_{k=0}^{2^h-1} \zeta^k (5^k - 1) \sum_a^{(m,k,h)} \theta(a)\ \frac{\langle a \rangle - 5^{-k}}{m2^{h+2}}\ [2^{h+2}]$$

L'idée du calcul est de traiter séparément la contribution de θ et celle de $(\langle a \rangle - 5^{-k})/m2^{h+2}$ dans la somme $\sum_a^{(m,k,h)}$. Pour cela, nous scindons cette quantité Δ en deux parties:

$$U \equiv \sum_{k=0}^{2^h-1} \zeta^k (5^k - 1) \sum_a^{(m,k,h)} \frac{\langle a \rangle - 5^{-k}}{2^{h+2}}\ [2^{h+2}]$$

$$V \equiv \sum_{k=0}^{2^h-1} \zeta^k (5^k - 1) \sum_a^{(m,k,h)} (\theta(a) - 1)\ \frac{\langle a \rangle - 5^{-k}}{2^{h+2}}\ [2^{h+2}]$$

On a alors : $-\ m\Delta \equiv U + V\ [2^{h+2}]$.

On voit que U ne contient que des choses connues, ou au moins connaissables. Il suffira d'étudier l'ensemble des a sur lequel on somme, puis de faire apparaître d'une part la somme des a sur cet ensemble, d'autre part son cardinal. Nous obtiendrons alors une expression générale en h. Nous expliciterons pour h=2. Pour V, on pourrait penser qu'on n'a rien gagné par rapport à Δ. En fait, on a gagné seulement quantitativement: comme c'est une $\Sigma_a^{(m,k,h)}$ qui intervient, $\theta(a) \neq 0$, donc $\theta(a) \in \{1, -1\}$, d'où $2 \mid \theta(a) - 1$. Grâce au 4 qui apparaît dans 5^k-1, nous avons déjà $8 = 2^3$ en facteur. Nous allons alors découper la $\Sigma_a^{(m,k,h)}$ en explicitant $(\langle a\rangle - 5^{-k})/2^{h+2}$ mod 2^{h+2-3} : il va apparaître des $\Sigma\,(\theta(a) - 1\,)$ étendues à certaines classes d'entiers, avec des coefficients connus. Nous constaterons que, pour h = 2, la somme se duplique: nous gagnons un 2 supplémentaire, et $V \equiv 0\ [16]$.

7. ETUDE DE U

$$U \equiv \sum_{k=0}^{2^h-1} \zeta^k\,(5^k-1) \sum_{(1)\,(2)} \frac{\langle a\rangle - 5^{-k}}{2^{h+2}}\ [2^{h+2}]$$

où (1) est mis pour ($0 \leqslant a < 2^{h+2}m$ et $a \wedge 2m = 1$), et (2) pour $\langle a\rangle \equiv 5^{-k}\ [2^{h+2}]$. Cette dernière condition se scinde en ($a \equiv 5^{-k}\ [2^{h+2}]$) et ($a \equiv -\,5^{-k}\ [2^{h+2}]$). Nous allons donc étudier l'ensemble $A^{(u)}$, en général seulement noté A :

$A^{(u)} := \{\ a;\ 0 \leqslant a < 2^{h+2}m,\ a \wedge m = 1,\ a \equiv u\ [2^{h+2}]\ \}$ (où u est une 2-unité).

Pour δ un diviseur positif de m, soit $A_\delta^{(u)}$ (ou A_δ) l'ensemble: $\{\ a;\ 0 \leqslant a < 2^{h+2}m,\ \delta \mid a,\ a \equiv u\ [2^{h+2}]\}$. A et les A_δ sont tous dans $A_1 = \{\ a\ ;\ 0 \leqslant a < 2^{h+2}m,\ \ a \equiv u\ [2^{h+2}]\ \}$, que nous prenons comme ensemble de référence. Alors $A = (\bigcup_{p \mid m} A_p\ )^c$.

Soit l(m) = n (longueur de m), soient $p_1,\ldots,p_n$ les diviseurs de m ($m = p_1 \ldots p_n$). On s'assure que ($\mathbf{1}_B$ désignant la fonction caractéristique de l'ensemble B):

$$\mathbf{1}_A = \sum_{0 \leqslant k \leqslant n} (-1)^k \sum_{\delta \mid m,\ l(\delta) = k} \mathbf{1}_{A_\delta} = \sum_{\delta \mid m} (-1)^{l(\delta)}\ \mathbf{1}_{A_\delta}.$$

A_δ est, lui, facile à décrire: introduisons $b(\delta)$ tel que $b(\delta)\,\delta \equiv 1\ [2^{h+2}]$. Par Bezout, les deux conditions ($a \equiv u\ [2^{h+2}]$) et ($a \equiv 0\ [\delta]$) équivalent à ($a \equiv b(\delta)\delta u\ \ [2^{h+2}\delta]$). On doit donc chercher les entiers v tels que les entiers $a = b(\delta)\delta u + 2^{h+2}\delta v$ satisfassent $0 \leqslant a < 2^{h+2}m$, ce qui donne : $(-b(\delta)\delta u/2^{h+2}\delta) \leqslant v < (-b(\delta)\delta u/2^{h+2}\delta) + (m/\delta)$.

Comme (m/δ) est entier, on obtient (m/δ) solutions en v :

$v = -E(b(\delta)\delta u/2^{h+2}) + j$, avec $0 \leqslant j < (m/\delta)$,

et (m/δ) solutions en a correspondantes. (E désigne la partie entière).

En particulier, $|A_\delta^{(u)}| = (m/\delta)$ (indépendant de u).

Comme $|A^{(u)}| = \sum_{\delta|m} (-1)^{l(\delta)} |A_\delta^{(u)}|$, $|A^{(u)}|$ ne dépend pas de u non plus et vaut :

$$|A| = \sum_{\delta|m} (-1)^{l(\delta)} (m/\delta) = (-1)^{l(m)} \sum_{\delta|m} (-1)^{l(\delta)} \delta.$$

Or pour $\alpha \in \mathbb{N}$: $\prod_{1\leq i\leq n}(1-p_i^\alpha) = \sum_{0\leq k\leq n}(-1)^k \left(\sum_{1\leq i_1<\ldots<i_k\leq n} p_{i_1}^\alpha \ldots p_{i_k}^\alpha\right) = \sum_{0\leq k\leq n}(-1)^k \sum_{\delta|m, l(\delta)=k} \delta^\alpha$

$= \sum_{\delta|m}(-1)^{l(\delta)} \delta^\alpha$. Ainsi : $|A| = (-1)^{l(m)} \prod_{1\leq i\leq n}(1-p_i) = \prod_{1\leq i\leq n}(p_i - 1)$ que nous noterons D(m).

Nous cassons le terme $\langle a\rangle - 5^{-k}$ en deux, ce qui donne $U = U' - U''$, avec

$U' = \sum_{0\leq k\leq 2^{h-1}} \zeta^k (5^k-1) \Sigma(\langle a\rangle/2^{h+2})$ et $U'' = \sum_{0\leq k\leq 2^{h-1}} \zeta^k (5^k-1) \Sigma(5^{-k}/2^{h+2})$,

où les sommes sont étendues à $a \in A^{(5^{-k})} \cup A^{(-5^{-k})}$ (l'union est disjointe).

U'' est immédiatement calculé, puisque ce qu'on somme ne dépend pas de a:

$$U'' = \sum_{0\leq k\leq 2^{h-1}} \zeta^k (5^k-1)(5^{-k}/2^{h+2}) \mid A^{(5^{-k})} \cup A^{(-5^{-k})}$$
$$= \sum_{0\leq k\leq 2^{h-1}} \zeta^k (5^k-1)(5^{-k}/2^{h+2})(2D(m))$$

Il reste à sommer deux progressions géométriques, de raisons ζ et $\zeta/5$: en supposant $h \geq 1$, la première est de somme nulle (resp. 2^h) si $\zeta = -1$ (resp. $\zeta = 1$); on peut donc noter sa somme $2^h.\mathbf{1}_{\zeta=1}$ et on a:

$$U'' = -\frac{D(m)}{2^{h+1}} \left(2^h.\mathbf{1}_{\zeta=1} - \frac{5^{-2h}-1}{(\zeta/5)-1}\right) \quad (16)$$

Lemme 17 : $\Sigma\langle a\rangle = \sum_{\delta|m}(-1)^{l(\delta)} m(2[b(\delta)5^{-k}] - 2^{h+2})$, où la première somme est étendue aux $a \in A^{(5^{-k})} \cup A^{(-5^{-k})}$, et où le crochet [n] désigne le reste de la division de n par 2^{h+2}.

Démonstration : La somme se casse en deux: $\Sigma\langle a\rangle = \Sigma_+ a - \Sigma_- a$, si $\Sigma_\pm$ désigne la somme étendue aux $a \in A^{(\pm 5^{-k})}$. Elle vaut donc $\sum_{\delta|m}(-1)^{l(\delta)}(\sum_\delta{}_+ a - \sum_\delta{}_- a)$, si $\sum_\delta{}_\pm$ désigne la somme étendue aux $a \in A_\delta^{(\pm 5^{-k})}$. En revenant à l'étude de $A_\delta^{(u)}$, on a :

$$\sum_{a\in A_\delta^{(u)}} a = \sum_{0\leq j\leq (m/\delta)-1} \{b(\delta)\delta u + 2^{h+2}\delta(-E(b(\delta)u/2^{h+2}) + j)\}$$
$$= m\{b(\delta)u - 2^{h+2}E(b(\delta)u/2^{h+2})\} + 2^{h+1}\delta(m/\delta)((m/\delta)-1).$$

Or pour c entier, $n - cE(n/c)$ est le reste de la division euclidienne de n par c, soit [n]; de plus, $[n] - [-n] = 2[n] - c$, quand $[n] \neq 0$. Ici $b(\delta)u$ est impair, donc son reste par 2^{h+2}, soit $[b(\delta)u]$, est non nul, et: $\sum_{a\in A_\delta^{(u)}} a = m[b(\delta)u] + 2^{h+1}\delta(m/\delta)((m/\delta)-1)$, puis

$\sum_{a\in A_\delta^{(u)}} a - \sum_{a\in A_\delta^{(-u)}} a = m(2[b(\delta)u] - 2^{h+2})$, et le lemme est prouvé.

Il vient alors $U' = (m/2^{h+2}) \sum_{\delta | m} (-1)^{l(\delta)} \sum_{0 \leq k \leq 2^{h-1}} \zeta^k (5^k - 1)(2[b(\delta)5^{-k}] - 2^{h+2})$.
Grâce à $\prod_{1 \leq i \leq n}(1-p_i^{\alpha}) = \sum_{\delta | m} (-1)^{l(\delta)} \delta^{\alpha}$ (avec $\alpha = 0$), la contribution du terme constant 2^{h+2} est nulle quand on somme. Finalement, nous avons obtenu:

$$U' = (m/2^{h+1}) \sum_{\delta | m} (-1)^{l(\delta)} \sum_{0 \leq k \leq 2^{h-1}} \zeta^k (5^k - 1)[b(\delta)5^{-k}] \quad (18)$$

Pour U'', avec $\zeta = 1$ et $h = 2$, il vient donc: $U'' = -D(m)(43/125)$. Or $5^{-3} \equiv 1-12\ [16]$, d'où $U'' \equiv -D(m).43.5 \equiv -7D(m) \equiv D(m)\ [16]$. (Ici, et pour la première fois, nous utilisons que $d \neq 2$ (puisque $d \geq 5$), donc m a au moins un diviseur premier (impair): $D(m) = \prod_{p | m}(1-p)$ est donc pair). Si $\zeta = -1$, il vient $(D(m)/8)(624/6.125) \equiv D(m)\ [16]$. Ainsi dans les deux cas:

$$U'' \equiv D(m)\ [16] \quad (19)$$

Pour U', il faut calculer $S = \sum_{1 \leq k \leq 3} \zeta^k (5^k - 1)[b(\delta)5^{-k}]$.
D'une part, on peut remplacer 5^{-k} par $1-4k$ qui lui est congru mod 16 dans le crochet, puisque ce dernier désigne un reste mod 16; d'autre part, il faut évaluer S mod 128, compte tenu du 8 en facteur au dénominateur, pour un résultat mod 16. Il vient

$$S \equiv 4\zeta([13b(\delta)] - [5b(\delta)]) + 24[9b(\delta)]\ [128].$$

Il suffit de calculer S pour les 8 restes impairs b mod 16, de transformer la correspondance $b(\delta) \leftrightarrow S$ en correspondance $\delta \leftrightarrow S$ (par $b(\delta)\delta \equiv 1\ [16]$, qui est la définition de $b(\delta)$). Il vient:

$$S \equiv 4\zeta(8 - 16.\mathbf{1}_{\delta \equiv 9, 11, 13, 15\ [16]}) + 24(\delta + 8.\mathbf{1}_{\delta \equiv 1, 7, 9, 15\ [16]})\ [128]$$
$$\equiv 32\zeta + 24\delta + 64.\mathbf{1}_{\delta \equiv 1, 7, 11, 13\ [16]}\ [128]$$

Par $\sum_{\delta | m} (-1)^{l(\delta)} \delta^{\alpha} = \prod_{\delta | m}(1-p^{\alpha})$, la sommation de la quantité 32ζ (indépendante de δ) sur δ est nulle ; celle de δ fait apparaître $D(m)$; il vient:

$$U' \equiv 3m(-1)^{l(m)} D(m) + 8m \sum_{\delta | m} \mathbf{1}_{\delta \equiv 1, 7, 11, 13\ [16]}\ [16] \quad (20)$$

Nous noterons $f(\delta) = \mathbf{1}_{\delta \equiv 1, 7, 11, 13\ [16]}$. Nous avons obtenu:

Lemme 21 : $U/m \equiv (D(m)/m) + 3(-1)^{l(m)} D(m) + 8 \sum_{\delta | m} f(\delta)\ [16]$

D'où:

Proposition 22 :

*si $m = p$ premier: $U/m \equiv 8.\mathbf{1}_{p \equiv \pm 3, \pm 7\ [16]}\ [16]$

*si $m = pq$ (p, q premiers): $U/m \equiv 8.\mathbf{1}_{p \equiv \pm 3\ [8]\ \text{et}\ q \equiv \pm 3\ [8]}\ [16]$

*si $l(m) \geq 3$: $U/m \equiv 0\ [16]$

Démonstration : a) Puisque m impair, $(1/m) \equiv m\ [8]$; donc $(D(m)/m) \equiv mD(m)\ [16]$.

b) Si $l(m) \geqslant 3$, $8 \mid D(m)$; de plus, $2 \mid m+3(-1)^{K(m)}$; les deux premiers termes de U/m sautent.

c) Si m = pq: les deux premiers termes de U/m fournissent: $(p-1)(q-1)(pq+3)$; si p ou $q \equiv 1\ [4]$, il n'en reste rien; sinon, $pq \equiv 1\ [4]$, et il n'en reste rien non plus.

d) Si m = p: les deux premiers termes de U/m donnent $(p-1)(p-3) \equiv 8.\mathbf{1}_{p \equiv 5,7,13,15\ [16]}\ [16]$.

e) Il reste à étudier la contribution des $f(\delta)$. Nous étudions leur somme mod 2.

Lemme 23 : $1 + f(x) + f(y) + f(xy) = g(x)\,g(y)$, où $g(x) = \mathbf{1}_{x \equiv \pm 3\ [8]}$.

Démonstration : On fait un tableau à double entrée, où x et y prennent les différentes congruences possibles mod 16. Le tableau serait 8x8 a priori, mais la symétrie en x et y et l'invariance de la quantité à étudier par $x \leftrightsquigarrow x+8$ (car $f(x+8) = f(x)+1$, et $f(xy+8y) = f(xy)+1$) ramènent à 10 calculs.

f) On peut alors appliquer le lemme au cas où m = pq, qui s'en trouve réglé.

Le cas où m = p s'obtient en ajoutant au résultat de d) la quantité $8.(f(1) + f(p))$; il vient :

$8 + 8.\mathbf{1}_{p \equiv 1,5,11,15\ [16]}$.

Enfin, si $m = p_1 \ldots p_l$ $(l = l(m) \geqslant 3)$:

$$\sum_{\delta \mid m} f(\delta) = \sum_{\delta \mid p_1 \ldots p_{l-1}} f(\delta) + \sum_{p_l \mid \delta \mid p_1 \ldots p_l} f(\delta) = \sum_{\delta \mid p_1 \ldots p_{l-1}} (f(\delta) + f(p_l \delta))$$

$$= \sum_{\delta \mid p_1 \ldots p_{l-1}} [g(\delta) g(p_l) - (g(p_l)+1)] = g(p_l) \sum_{\delta \mid p_1 \ldots p_{l-1}} g(\delta) \quad (\text{car } \sum_{\delta \mid p_1 \ldots p_{l-1}} 1 = 2^{l-1} = 0).$$

Mais on s'aperçoit (miracle!) que $g(x) + g(y) + g(xy) = 0$ (cette fois-ci, par la symétrie $g(x) = g(-x)$), il ne reste à voir que les couples (1,1), (1,3) et (3,3)).

En recommençant alors la manipulation faite sur la somme initiale avec $\sum_{\delta \mid p_1 \ldots p_{l-1}} g(\delta)$, il vient

$$\sum_{\delta \mid p_1 \ldots p_{l-1}} g(\delta) = \sum_{\delta \mid p_1 \ldots p_{l-2}} g(p_{l-1}) = 2^{l-2} g(p_{l-1}) = 0.$$

8. ETUDE DE V

$$V \equiv \sum_{k=0}^{2^h-1} \zeta^k\,(5^k-1) \sum_{a}^{(m,k,h)} (\theta(a)-1)\ \frac{\langle a \rangle - 5^{-k}}{2^{h+2}}\ [2^{h+2}]$$

$$\equiv \sum_{k=0}^{2^h-1} \zeta^k\,(5^k-1) \sum_{(1)(2)} (\theta(a)-1)\ \frac{\langle a \rangle - 5^{-k}}{2^{h+2}}\ [2^{h+2}]$$

où (1) désigne les a tels que $0 < a < 2^{h+2}m$ et $a \wedge 2m = 1$, et (2) les a tels que $\langle a \rangle \equiv 5^{-k}\ [2^{h+2}]$.

Nous notons $r(a)$ pour $\theta(a) - 1$.

Intéressons nous à h=2. Nous sommons sur $a \wedge 2m = 1$, donc $\theta(a) \neq 0$; comme θ est quadratique, on a donc alors $2 \mid r(a)$. Par ailleurs, $4 \mid 5^k - 1$. Il nous suffit donc de préciser $(\langle a \rangle - 5^{-k})/16$ mod 2 pour avoir V mod 16. Il vient:

$\sum_{(1)\,(2)} r(a)[(\langle a\rangle - 5^{-k})/16\,] \equiv \sum_{(1)\,(2')} r(a).\,0 + \sum_{(1)\,(2'')} r(a).\,1\ [4]$

(si (2') désigne $\langle a\rangle \equiv 5^{-k}\,[32]$ et (2'') $\langle a\rangle \equiv 5^{-k}+16\,[32]$), et finalement

$V \equiv \sum_{1\leqslant k\leqslant 3} \zeta^k(5^k-1) \sum_{(1)\,(2'')} r(a)\,[16]$. Puis:

$5^k - 1 \equiv (1+4)^k - 1 \equiv 4k\,[16]$, et $V \equiv \sum_{1\leqslant k\leqslant 3} 4k \sum_{(1)\,(2)} r(a) \equiv 4 \sum_{(1)\,(2\_1)\,(2\_3)} r(a)\ [16]$

(où (2_i) désigne $\langle a\rangle \equiv 5^{-i}+16\,[32]$).

Nous utilisons alors le lemme suivant:

Lemme 24 : $\sum_{0<a<16m,\,(a,2m)=1,\,\langle a\rangle = u\,[32]} r(a) = \sum_{0<a<4m,\,(a,2m)=1,\,a\,=\,u-12m,\,u-8m,\,\ldots,\,u+16m\,[32]} r(a)$.

Démonstration : Nous omettrons systématiquement la condition $a \wedge 2m = 1$ pour alléger les notations. Alors:

$$\begin{aligned}\sum_{0\leqslant a<16m,\,a\equiv u\,[32]} r(a) &= \sum_{0\leqslant a<4m,\,a\equiv u\,[32]} r(a) + \sum_{4m\leqslant a<8m,\,a\equiv u\,[32]} r(a) + \ldots \\ &= \sum_{0\leqslant a<4m,\,a\equiv u\,[32]} r(a) + \sum_{0\leqslant a<4m,\,a\equiv u-4m\,[32]} r(a) + \ldots \\ &= \sum_{0\leqslant a<4m,\,a\equiv u,\,u-4m,\,u-8m,\,u-12m\,[32]} r(a).\end{aligned}$$

(Ceci grâce à $r(a+4m) = r(a)$). Puis:

$$\begin{aligned}\sum_{0\leqslant a<16m,\,\langle a\rangle = u\,[32]} r(a) &= \sum_{0\leqslant a<16m,\,a\equiv u,\,-u\,[32]} r(a) \\ &= \sum_{0\leqslant a<4m,\,a\equiv u,\,\ldots,\,u-12m;\,-u,\,\ldots,\,-u-12m\,[32]} r(a) \\ &= \sum_{0\leqslant a<4m,\,a\equiv u,\,\ldots,\,u-12m;\,u+4m,\,\ldots,\,u+16m\,[32]} r(a)\end{aligned}$$

(Grâce à $\sum_{0\leqslant a<4m,\,a\equiv u\,[32]} r(a) = \sum_{0\leqslant a<4m,\,a\equiv 4m-u\,[32]} r(a)$ par le changement $a' = 4m-a$ (θ est pair)).

Achevons alors le calcul de V: la sommation écrite au lemme, appliquée à $u = 5^{-i}+16$, est en fait étendue à 8 congruences différentes mod 32 (car $m \equiv 1\,[2]$), et qui se ramènent toutes à 1 mod 4 (car $5^{-i}+16 \equiv 1\,[4]$). Chacune des deux sommes: $\sum_{(1)\,(2\_i)} r(a)$ vaut donc $\sum_{0\leqslant a<4m,\,a\equiv 1\,[4]} r(a)$. Donc $V \equiv 8 \sum_{0\leqslant a<4m,\,a\equiv 1\,[4]} r(a) \equiv 0\ [16]$.

9. CONCLUSION

Pour $d \geqslant 5$, libre de carrés, on réunit

La proposition 6

$-m\,\Delta(d) \equiv U + V\ [16]$ (cf. **5**) (avec $m = d$ si d impair, et $(d/2)$ sinon)

Le calcul de U/m (Proposition 22)

$V \equiv 0\,[16]$ que nous venons d'établir

qui fournissent le Théorème .

Bibliographie

[A] : AMICE, Y. Les nombres p -adiques . Paris, P.U.F., 1975.

[A - F] : AMICE, Y. et FRESNEL, J. Fonctions zêta p-adiques des corps de nombres abéliens réels. Acta Arith., 20 (1972) p. 353-384.

[Bar] : BARSKY, D. Sur la norme de certaines séries d'Iwasawa. Groupe d'étude d'analyse ultramétrique (Amice, Christol, Robba) 10^{e} année, 1982-83, n° 13.

[D] : DESNOUX, P-J. Congruences dyadiques entre nombres de classes de corps quadratiques. Thèse soutenue en 1986 à Paris VII.

[G] : GRAS, G. Pseudo-mesures p-adiques associées aux fonctions L de $\mathbb{Q}$. Preprint, 1986.

[Iw] : IWASAWA, K. Lectures on p-adic L functions. Princeton, Princ. Univ. Press & Univ. of Tokyo Press, 1972 (Annals of Math. Studies, 74).

[K 1] : KAPLAN, P. Sur le 2-groupe des classes d'idéaux des corps quadratiques. J. für die reine und angew. Math., 283/284 (1976), p. 313-363.

[K 2] : KAPLAN, P. Nouvelle démonstration d'une congruence modulo 16 entre les nombres de classes d'idéaux de $\mathbb{Q}(\sqrt{-2p})$ et $\mathbb{Q}(\sqrt{2p})$ pour $p \equiv 1$ [4] . Proc. Japan Acad. (Série A) 57 (1981) 507-509.

[K-W 1] : KAPLAN, P. et WILLIAMS, K.S. Congruences mod 16 for the class numbers of $\mathbb{Q}(\sqrt{\pm p})$ and $\mathbb{Q}(\sqrt{\pm 2p})$ for p a prime congruent to 5 modulo 8. Acta Arith. 40 (1981/1982) , p. 375-397.

[K-W 2] : KAPLAN, P. et WILLIAMS, K.S. On the class numbers of $\mathbb{Q}(\sqrt{\pm 2p})$ modulo 16, for $p \equiv 1$ [8] a prime. Acta Arith. 40 (1981/1982), p. 289-296.

[K-W 3] : KAPLAN, P. et WILLIAMS, K.S. Congruences for the class numbers of the fields $\mathbb{Q}(\sqrt{\pm pq})$ with p and q odd primes. (Preprint).

[K-L] : KUBOTA,T. und LEOPOLDT, H.W. Eine p-adische Theorie der Zetawerte . I : Einführung der p-adischen Dirichletschen L Funktionen. J. für die reine und angew. Math., t. 214-215, (1964), p. 328-339.

[L-S] : LANG, H. und SCHERTZ, R. Kongruenzen zwischen Klassenzahlen quadratischer Zahlkörper. Journal of Number Theory, Vol 8 (1976), p. 352-365.

[S] : SAMUEL, P. Théorie algébrique des nombres. Paris, Hermann, 1967.

[W] : WASHINGTON, L.C. Introduction to Cyclotomic Fields. Springer-Verlag, 1982 (Graduate Texts in Math., 83).

[Will 1] : WILLIAMS, K.S. On the class number of $\mathbb{Q}(\sqrt{-p})$ modulo 16, for $p \equiv 1$ modulo 8 a prime. Acta Arith. 39 (1981), p. 381-398.

[Will 2] : WILLIAMS, K.S. Congruences modulo 8 for the class numbers of $\mathbb{Q}(\sqrt{\pm p})$, $p \equiv 3$ (mod 4) a prime. Journal of Number Theory, Vol 15, n°2, p.182-198.

Pierre-Jean Desnoux

Université PARIS VII
U.E.R DE MATHEMATIQUES ET INFORMATIQUE et U.A. 212
Tour 45-55 5ème Etage
2, Place Jussieu
75251 PARIS CEDEX 05

12, Rue du Faubourg Saint-Denis
75010 PARIS