THEORIE DES NOMBRES
BESANCON

Années 1981-1982
et 1982-1983

CALCUL DU RESIDU EN s = 1 DE LA FONCTION DZETA p-ADIQUE DE CORPS CUBIQUES CYCLIQUES

Jean-Noël MARTIN

Calcul du résidu en $s = 1$ de la fonction dzéta p-adique de corps cubiques cycliques

par J.-N. MARTIN

Ce travail a été effectué, dans l'équipe de Théorie des Nombres de Besançon, au titre du rapport de stage du D.E.A.

Introduction

Nous nous proposons de déterminer, pour quelques nombres premiers p, des exemples de corps cubiques cycliques dont le nombre de classes h et le régulateur p-adique R_p vérifient :

$$h \frac{R_p}{p^u} \equiv 0(p),$$

où p^u est une puissance de p canonique qui divise tout régulateur dans ce cas ; nous calculerons même la valuation p-adique de $h \frac{R_p}{p^u}$.

Nous rappellerons comment le produit $h \frac{R_p}{p^u}$ est lié d'une part aux fonctions L p-adiques en $s = 1$ et d'autre part à l'ordre de p-groupes finis issus du corps de classes. Puis nous approcherons p-adiquement la quantité voulue par une expression qui se prêtera, en particularisant, au calcul par ordinateur de ces valeurs de fonctions L_p. Après avoir précisé l'algorithme, nous produisons une table dans laquelle sont consignés les cas favorables.

Rappels et notations

(1) Pour k abélien sur $\mathbb{Q}$, de conducteur f, nous noterons $\left(\frac{k/\mathbb{Q}}{c}\right)$ l'automorphisme d'Artin relatif à c (c premier à f).

(2) Nous noterons θ le caractère de Leopoldt défini, pour $a \in \mathbb{Z}_p^*$, de la façon suivante :

si $p \neq 2$, $\theta(a)$ est l'unique racine $(p-1)$-ième de l'unité de $\mathbb{Z}_p$ congrue à a modulo p ;

si $p = 2$, $\theta(a) = \pm 1$, de telle sorte que $a\theta^{-1}(a) \equiv 1 \ (4)$.

Nous noterons $\langle b \rangle = b\,\theta^{-1}(b)$ pour $b \in \mathbb{Z}_p^*$.

(3) Soit χ un caractère de Dirichlet modulo f ; la fonction L p-adique, notée $L_p(\chi, s)$, est l'unique fonction continue de $\mathbb{Z}_p$ dans $\mathbb{C}_p$ vérifiant :

$$L_p(\chi, 1-n) = L\left(\chi\theta^{-n}, 1-n\right), \text{ quel que soit } n \in \mathbb{N}, n \geq 1,$$

où L est la série de Dirichlet usuelle ([3], [4]).

(4) Formule de Coates [1]

Si k est une extension abélienne réelle de $\mathbb{Q}$, X l'ensemble des caractères de Dirichlet associés, on a :

$$\frac{h R_p}{p^{\frac{n}{e}-1} \sqrt{D}} = \prod_{\substack{\chi \in X \\ \chi \neq 1}} \frac{1}{2} L_p(\chi, 1),$$

où h est le nombre de classes de k, R_p son régulateur p-adique, D son discriminant,

où $n = [k : \mathbb{Q}]$ et e est l'indice de ramification de p dans $k/\mathbb{Q}$.

<u>Remarque</u> :

Cette formule est la formule analytique p-adique du nombre de classes donnée par Leopoldt ([1], [4]).

L'ordre du p-groupe de torsion T du groupe de Galois de la p-extension abélienne p-ramifiée maximale de k est donné par la formule analytique suivante (Coates [1]) :

$$|T| = [\mathbb{Q}_\infty \cap k : \mathbb{Q}] \prod_{\substack{\chi \in X \\ \chi \neq 1}} \frac{1}{2} L_p(\chi, 1),$$

où $\mathbb{Q}_\infty$ est la $\mathbb{Z}_p$-extension cyclotomique de $\mathbb{Q}$. Dans nos exemples, nous aurons $\mathbb{Q}_\infty \cap k = \mathbb{Q}$, ce qui fait que sous cette hypothèse la formule devient :

$$|T| = \prod_{\substack{\chi \in X \\ \chi \neq 1}} \frac{1}{2} L_p(\chi, 1).$$

Remarque 1 :
Dans [1], l'expression de T est d'abord obtenue via le corps de classes ; elle est donnée par la relation suivante :

$$|T| = \frac{[\mathbb{Q}_\infty \cap k : \mathbb{Q}]\ h\ R_p}{p^{\frac{n}{e} - 1} \sqrt{D}} .$$

Il ne reste alors qu'à utiliser la formule analytique de Leopoldt pour avoir l'expression analytique de $|T|$.

Remarque 2 :
Il s'agira bien de calculer le résidu de la fonction dzéta p-adique de k en $s = 1$ puisqu'on a la relation ([3], [4]) :

$$\text{Rés}_{s=1}\ \zeta_p(k, s) = \frac{p-1}{p} \prod_{\substack{\chi \in X \\ \chi \neq 1}} L_p(\chi, 1).$$

Tout revient donc à calculer les $L_p(\chi, 1)$. Or, on connait une expression des $L_p(\chi, 1)$ qui est ([3], [4]) :

$$L_p(\chi, 1) = -\left(1 - \frac{\chi(p)}{p}\right) \frac{\tau(\chi)}{f_\chi} \sum_{\substack{a=1 \\ (a, f_\chi)=1}}^{f_\chi} \chi^{-1}(a) \log_p\left(1 - \xi_{f_\chi}^a\right)$$

où f_χ est le conducteur de χ, $\xi_{f_\chi} = \exp\left(2 i\pi/f_\chi\right)$, et $\tau(\chi) = \sum_{a=1}^{f_\chi} \chi(a)\ \xi_{f_\chi}^a$.

Mais le calcul numérique des $L_p(\chi, 1)$ ainsi donnés n'est pas praticable car lié à des logarithmes p-adiques de nombres algébriques.

Nous utiliserons une formule entièrement rationnelle obtenue dans [2] qui permettra le calcul effectif.

I - Obtention de la congruence fondamentale

I-1 Elément de Stickelberger :

Soit p un nombre premier fixé ; on pose $q = p$ si $p \neq 2$, $q = 4$ sinon. Considérons un corps K abélien sur $\mathbb{Q}$ contenant les racines q-ièmes de l'unité, de conducteur f ; nous appelons (premier) élément de Stickelberger, l'élément de $\mathbb{Q}[G]$ (où G désigne $\mathrm{Gal}(K/\mathbb{Q})$) défini par :

$$\alpha(K) = \sum_{a=1}^{f}{}^{*} \left(\frac{K/\mathbb{Q}}{a}\right)^{-1} \left(\frac{1}{2} - \frac{a}{f}\right),$$

où Σ^* signifie ici, et pour la suite, que la sommation est étendue aux a premiers à f.

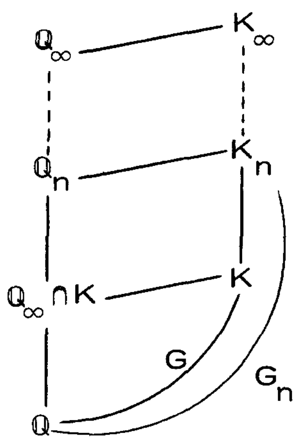
Pour c premier à f nous noterons $\alpha^c(K) = \left(1 - c\left(\frac{K/\mathbb{Q}}{c}\right)^{-1}\right)\alpha(K)$, soit :

$$\alpha^c(K) = \left(1 - c\left(\frac{K/\mathbb{Q}}{c}\right)^{-1}\right) \sum_{a=1}^{f}{}^{*} \left(\frac{K/\mathbb{Q}}{a}\right)^{-1} \left(\frac{1}{2} - \frac{a}{f}\right).$$

I-2 Définition de $m(s)$ et $\beta^c(K_n, s)$:

Considérons alors la tour cyclotomique de K ; notons f_n le conducteur de $K_n = K\mathbb{Q}_n$ où $\mathbb{Q}_n$ est le sous-corps de $\mathbb{Q}^{(qp^n)}$ de degré p^n sur $\mathbb{Q}$ (on a $f_n \equiv 0 \bmod qp^n$, pour tout $n \geq 0$).

Soit $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$. Notons $G_\infty = \mathrm{Gal}(K_\infty/\mathbb{Q}) = \varprojlim G_n$ et $K_\infty = \bigcup_{n\geq 0} K_n$; nous avons donc le schéma suivant :



Soit $m(s) : \mathbb{Z}_p[G_\infty] \longrightarrow \mathbb{Z}_p[G_\infty]$ définie comme suit :

pour $\sigma \in G_\infty$ on peut écrire $\sigma = (\sigma_n)_n = \left(\left(\frac{K_n/\mathbb{Q}}{a_n}\right)\right)_n$ comme élément de $\varprojlim G_n$; mais pour $m \geq n$, on a $a_m \equiv a_n \bmod qp^n$, car $\mathbb{Q}^{(qp^n)} \subset K_n$; ainsi la suite $\left(a_n\right)_n$ admet une limite p-adique ne dépendant que de σ, notée par conséquent a_σ ; de plus $a_\sigma \in \mathbb{Z}_p^*$;

à σ on associe $\theta(a_\sigma) \langle a_\sigma \rangle^{-1} \sigma^{-1}$.

Posons alors $\beta^c\left(K_n, s\right) = m(s)\alpha^c\left(K_n\right)$, pour tout $n \geq 0$.

I-3 Résultats :

I-3-1 Approximation de $\beta^c\left(K_n, s\right)$.

Soit K abélien sur $\mathbb{Q}$ contenant les racines q-ièmes de l'unité. Alors on démontre que pour tout $s \neq 1$, tout $n \in \mathbb{N}$, on a ([2]) :

$$\beta^c\left(K_n, s\right) \equiv \left(1 - \langle c \rangle^{1-s}\left(\frac{K_n/\mathbb{Q}}{c}\right)\right) \frac{1}{(1-s)f_n} \sum_{a=1}^{f_n}{}^{*} \left(\frac{K_n/\mathbb{Q}}{a}\right) a^{-1}\left(\frac{1-s}{2} f_n - a\right) \langle a \rangle^{1-s} \bmod\left(p^{n+1}\right)$$

I-3-2 Lien avec les fonctions L_p.

. Définition de la p-admissibilité :

Soit χ un caractère de Dirichlet modulo f pair ($f \equiv 0 \bmod q$),

Soit K un corps tel que :

χ soit un caractère de K,

K contienne les racines q-ièmes de l'unité,

f_K et f aient les mêmes diviseurs premiers ;

alors K est dit p-admissible pour χ.

. Expression des fonctions L_p :

Soit χ un caractère de Dirichlet modulo f distinct du caractère unité et soit K un corps abélien p-admissible pour χ ; soit c premier à p et f, $\chi(c) \neq 1$; alors, pour $s \neq 1$, on a :

$$L_p(\chi, s) = \frac{1}{1 - \langle c \rangle^{1-s} \chi(c)} \lim_{n \to \infty} \chi\left(\beta^c\left(K_n, s\right)\right).$$

Plus précisément, on a la congruence :

$$L_p(\chi, s)\left(1 - \langle c \rangle^{1-s} \chi(c)\right) \equiv \chi\left(\beta^c\left(K_n, s\right)\right) \bmod \left(p^{n+1}\right)$$

pour tout $n \in \mathbb{N}$.

. Passage à la limite en s :

Notons log le logarithme p-adique. En passant à la limite en s dans l'expression de $\beta^c\left(K_n, s\right)$ donnée en I-3-1, nous obtenons finalement, pour tout $n \geq 0$:

$$\chi\left(\beta^c\left(K_n, 1\right)\right) \equiv (1 - \chi(c)) \sum_{a=1}^{f_n}{}^{*} \chi(a) \left(\frac{1}{2a} - \frac{\log a}{f_n}\right) \bmod \left(p^{n+1}\right),$$

puisque $\lim\limits_{s \to 1} \dfrac{\langle a \rangle^{1-s}}{1-s} = \log \langle a \rangle = \log a$. Si χ n'est pas d'ordre puissance de p, on peut choisir c tel que $1 - \chi(c)$ soit inversible, sinon on peut le choisir de sorte que $1 - \chi(c)$ soit une uniformisante π_χ de $\mathbb{Q}_p(\chi)$ (corps des valeurs de χ).

Nous posons alors $\omega_\chi = \pi_\chi$ (respectivement 1) si χ est (respectivement n'est pas) d'ordre puissance de p ; alors :

$$L_p(\chi, 1) \equiv \sum_{a=1}^{f_n}{}^{*} \chi(a) \left(\frac{1}{2a} - \frac{\log a}{f_n}\right) \bmod \left(\frac{p^{n+1}}{\omega_\chi}\right), \; n \geq 0.$$

. Simplification de la sommation :

Posons $S = \frac{1}{2} \sum\limits_{a=1}^{f_n}{}^{*} \frac{\chi(a)}{a}$; il vient, en posant $a = f_n - b$ (b décrit alors le même ensemble que a),

$$S = \frac{1}{2} \sum_{b=1}^{f_n}{}^{*} \frac{\chi(b)}{f_n - b}, \text{ car } \chi \text{ est pair, soit}$$

$$S = -\frac{1}{2}\sum_{b=1}^{f_n}{}^{*} \frac{\chi(b)}{b}\left(1-\frac{f_n}{b}\right)^{-1}$$

$$S \equiv -\frac{1}{2}\sum_{b=1}^{f_n}{}^{*} \frac{\chi(b)}{b}\left(1+\frac{f_n}{b}\right) \bmod \frac{(qp^n)^2}{2}$$

$$S \equiv -S - \frac{f_n}{2}\sum_{b=1}^{f_n}{}^{*} \frac{\chi(b)}{b^2} \bmod \frac{(qp^n)^2}{2}\ , \text{ d'où}$$

$$2S \equiv -\frac{f_n}{2}\sum_{b=1}^{f_n}{}^{*} \frac{\chi(b)}{b^2} \bmod \frac{(qp^n)^2}{2}\ , \text{ et}$$

$$S \equiv -\frac{f_n}{4}\sum_{b=1}^{f_n}{}^{*} \frac{\chi(b)}{b^2} \bmod \frac{(qp^n)^2}{4}\ .$$

Si $p \neq 2$, on a $S \equiv 0 \bmod qp^n$; si $p = 2$, on vérifie facilement que $\sum_{b=1}^{f_n}{}^{*} \frac{\chi(b)}{b^2} \equiv 0 \bmod 4$, pour $\chi \neq 1$.

Donc $S \equiv 0 \bmod qp^n$.

En conséquence la sommation initiale se ramène à l'étude de l'expression

$$-\frac{1}{f_n}\sum_{a=1}^{f_n}{}^{*} \chi(a) \log a \ \text{modulo} \left(\frac{p^{n+1}}{\omega_\chi}\right)$$

(C) $$\boxed{L_p(\chi, 1) \equiv -\frac{1}{f_n}\sum_{a=1}^{f_n}{}^{*} \chi(a) \log a \mod \left(\frac{p^{n+1}}{\omega_\chi}\right),\ n \geq 0\ ,\ \chi \neq 1}$$

Remarque 1 :

Comme signalé plus haut, Σ^* signifie que la sommation est étendue aux a premiers à f_n.

Remarque 2 :

Lorsque χ est d'ordre puissance de p ($\chi \neq 1$), $\frac{p}{\omega_\chi}$ est encore non inversible pour $p \neq 2$ (ce qui permet le test d'inversibilité pour $L_p(\chi, 1)$ (ceci se rencontrera dans nos exemples numériques pour $p = 3$) ; pour $p = 2$ ce n'est plus le cas (car $\omega_\chi = 2$), mais alors le test avec $n=0$ est sans intérêt car on sait ([2]) que $L_2(\chi, 1) \equiv 0 \bmod 2$, au moins lorsque χ n'est pas caractère de $\mathbb{Q}_\infty$, cas que l'on écarte de toutes façons.

Remarque 3 :

Cette approximation de $L_p(\chi, 1)$ permet un calcul effectif puisque la somme qui intervient dans (C) ne met en jeu que des nombres p-adiques rationnels dans les coefficients de $\chi(a)$. De plus, la valuation exacte de $L_p(\chi, 1)$ est obtenue dès que n considéré est assez grand.

II - Application

Dans cette partie on fixe le nombre premier p.

Considérons un nombre premier ℓ, distinct de p, et appliquons la relation (C) précédente aux caractères de Dirichlet modulo ℓ d'ordre 3 ; ceci introduit donc un corps cubique cyclique k : nécessairement $\ell - 1 \equiv 0 \bmod 3$.

Nous avons la situation suivante :

$$\begin{array}{cc} & \mathbb{Q}^{(\ell)} \\ & | \\ & k \\ 3 & | \\ & \mathbb{Q} \end{array}$$

II-1 Procédé de sommation :

Considérons g, une racine primitive modulo ℓ ; alors $\mathrm{Gal}\left(\mathbb{Q}^{(\ell)}/\mathbb{Q}\right)$ est engendré par $\bar{g}$ dans l'isomorphisme $\mathrm{Gal}\left(\mathbb{Q}^{(\ell)}/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/\ell\mathbb{Z}\right)^*$. Donc $\mathrm{Gal}\left(\mathbb{Q}^{(\ell)}/k\right)$ est engendré par $\bar{g}^3$. Le caractère χ d'ordre 3 est trivial sur $\mathrm{Gal}\left(\mathbb{Q}^{(\ell)}/k\right)$.

Cas où $p \neq 2$

La sommation considérée dans la relation (C) va s'effectuer sur $\left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^* \times \left(\mathbb{Z}/\ell\mathbb{Z}\right)^*$ identifié à $\mathrm{Gal}\left(\mathbb{Q}^{(p^{n+1}\ell)}/\mathbb{Q}\right)$; nous sommes amenés à considérer pour le calcul, des générateurs de ces deux groupes :

$$\begin{tikzcd}
\mathbb{Q}^{(\ell)} \arrow[r, dash, "\langle \bar{\gamma}_{n+1} \rangle"] \arrow[d, dash] & \mathbb{Q}^{(p^{n+1}\ell)} \arrow[d, dash] \arrow[dd, dash, bend left=60, "\langle \bar{g}_{n+1} \rangle"] \\
k \arrow[r, dash] \arrow[d, dash] & K_n \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & \mathbb{Q}^{(p^{n+1})}
\end{tikzcd}$$

A l'étage n, nous avons $f_n = p^{n+1}\ell$: en effet ici $K = k\,\mathbb{Q}^{(p)}$ d'où $K_n = k\mathbb{Q}^{(p^{n+1})}$.

Nous considérons γ_{n+1} racine primitive mod p^{n+1}, et $\gamma_{n+1} \equiv 1 (\ell)$ pour engendrer l'image canonique de $\left(\mathbb{Z}/_{p^{n+1}\mathbb{Z}}\right)^*$ dans le produit cartésien précité.

Nous considérons de même g_{n+1} racine primitive mod ℓ et $g_{n+1} \equiv 1 \ (p^{n+1})$ pour engendrer l'image canonique de $\left(\mathbb{Z}/_{\ell\,\mathbb{Z}}\right)^*$ dans le même produit cartésien.

Cas où p = 2

$\left(\mathbb{Z}/_{2\ell\,\mathbb{Z}}\right)^*$ est cyclique.

Pour un entier $n \geq 1$, les nombres b premiers à $2^{n+1}\ell$ se déduisent des nombres a premiers à 2ℓ par 2ℓ-translation. Le procédé de sommation reste très proche du précédent, par conséquent, puisque a et ses 2ℓ-translatés ont même caractère modulo $2^{n+1}\ell$.

II-2 Détermination de $L_p(\chi, 1)$:

. Dans la relation de Coates $\dfrac{hR_p}{p^{\frac{n}{e}-1}\sqrt{D}} = \prod\limits_{\substack{\chi\in X \\ \chi\neq 1}} \frac{1}{2} L_p(\chi, 1) = |T|$, nous avons

$D = \ell^2$ et $e = 1$ puisqu'on a supposé $\ell \neq p$; ainsi cette formule se simplifie dans notre cas ; nous obtenons ici :

$$\frac{hR_p}{p^2} = \prod_{\substack{\chi\in X \\ \chi\neq 1}} \frac{1}{2} L_p(\chi, 1),$$

à une constante multiplicative près dans $\mathbb{Z}_p^*$.

Remarque :

Le terme p^2 qui subsiste ($n = 3$ et $e = 1$ ici) est en fait le diviseur canonique de R_p (appelé p^u dans l'introduction) : en effet, pour un corps cubique cyclique on sait que le groupe des unités est de la forme $E = \langle \pm 1, \varepsilon, \varepsilon^\sigma \rangle$, où ε est unité fondamentale et ε^σ un conjugué de ε ; on a donc

$R_p = \begin{vmatrix} \log \varepsilon & \log \varepsilon^{\sigma} \\ \log \varepsilon^{\sigma} & \log \varepsilon^{\sigma^2} \end{vmatrix}$. Mais comme p est non ramifié dans $k/\mathbb{Q}$, l'uniformisante en p est encore p et, comme ε est entier, on a $\log \varepsilon = p\,\alpha$, avec α p-entier ; d'où $R_p = \begin{vmatrix} p\alpha & p\alpha^{\sigma} \\ p\alpha^{\sigma} & p\alpha^{\sigma^2} \end{vmatrix} = p^2 \beta$, avec β p-entier.

Il y a alors deux choix possibles pour χ ; le deuxième correspond au conjugué du premier.

. Avec les notations du paragraphe précédent, nous poserons $\chi(\bar{g}) = \chi(\bar{g}_{n+1}) = j$ et implicitement $\chi\left(\bar{\gamma}_{n+1}\right) = 1$. Tous les termes de la sommation ($\mathbb{C}$) sont alors connus.
La somme qui apparaît dans ($\mathbb{C}$) est a priori élément de $\mathbb{Z}_p[j]$; elle s'écrira $A_1 + A_2 j + A_3 j^2$ avec $A_i \in \mathbb{Z}_p$. Nous l'écrirons sous la forme $A + Bj$, $(A, B) \in \mathbb{Z}_p^2$; nous étudierons son inversibilité modulo p.

. L'étude de l'inversibilité de $A+Bj$ modulo p dépend de la décomposition de p modulo 3 :

si $\left(\frac{p}{3}\right) = 1$, $A+Bj$ non inversible équivaut à $N(A+Bj) = A^2+B^2-AB \equiv 0(p)$;

si $\left(\frac{p}{3}\right) = -1$, $A+Bj$ non inversible équivaut à $A \equiv 0(p)$ et $B \equiv 0(p)$;

si $p = 3$, $A+Bj$ non inversible équivaut à $A + B \equiv 0(p)$.

Dans tous les cas, le test d'inversibilité portera sur la nullité de $N(A+jB)$ modulo p.

. Plus précisément, si dans la congruence $L_p(\chi, 1) \equiv A+Bj \bmod \dfrac{p^{n+1}}{\omega_\chi}$

on a $v_p\left(A^2 - AB + B^2\right) < n+1$ (où v_p est la valuation p-adique),

alors $v_p\left(\prod_{\chi} L_p(\chi, 1)\right) = v_p\left(A^2 - AB + B^2\right)$.

<u>Remarque</u> :
D'après les résultats de Ribet, rappelés dans [2], et pour le cas qui nous intéresse ($p = 3$, caractères d'ordre 3 de conducteur premier $\ell \neq 3$), une C.N.S. pour que $\frac{1}{2}\,L_3(\chi, 1)$ soit de valuation strictement positive est que l'on ait $\ell \equiv 1 \bmod 9$ (ce qui est confirmé par le tableau T 2 du § III).

III - Algorithme et résultats

III-1 Algorithme : remarques générales

Les calculs ont été menés sur micro-ordinateurs sous langage LSE (Langage Spécial Enseignement). Afin de dépasser les limites de la machine en chiffres significatifs, les nombres utilisés ont été considérés si nécessaire comme tableaux, car décomposés dans une base convenable (puissance de p).

La longueur croissante des calculs avec p et ℓ a déterminé les maxima atteints.

III-2 Organigramme sommaire (donné ici pour $p \neq 2$) :

P1

Initialisations

choix de p et ℓ

choix de l'étage n

choix des générateurs g pour $\left(\mathbb{Z}/\ell\mathbb{Z}\right)^*$ choisi tel que $g \equiv 1\,(p^n)$

γ pour $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^*$ choisi tel que $\gamma \equiv 1(\ell)$

Calibrage des calculs : choix des valuations maxima suffisantes en p (en vue de la division par p^n en fin de calcul)

Initialisation à 1 de P_1, P_2, P_3, produits des entiers inférieurs à $p^n\ell$, premiers à $p^n\ell$ de caractères respectifs $1, j, j^2$

Initialisation à 1 de l'entier a variable dans la sommation.

P2

Boucle pour $I = 1$ jusqu'à $\ell - 1$

$a = a * g$; a réduit modulo $p^n\ell$

Boucle pour $J = 1$ jusqu'à $p^{n-1}(p-1)$

$a = a * \gamma$; a réduit modulo $p^n\ell$

$P_{K+1} = P_{K+1} * a$ avec K défini par $K \equiv I\ (3)$

P3

Calcul des logarithmes p-adiques de P_1, P_2, P_3

Calcul de A_1, A_2, A_3 pour $S = A_1 + A_2 j + A_3 j^2 = - \sum_{a=1}^{p^n \ell} \chi(a) \frac{\log(a)}{p^n \ell}$

Ecriture de $S = A + Bj$

Test d'inversibilité de $A+Bj$ par calcul de la norme modulo $\frac{p^n}{\omega_\chi}$

Affichage des résultats et sortie des cas favorables

Remarque :
Les cas favorables (cas de non inversibilité de $A + Bj$) sont alors repris puis étudiés à un étage supérieur.

III-3 Résultats numériques :

Dans chacun des tableaux suivants sont indiqués les conducteurs ℓ, les nombres p pour lesquels $\prod_\chi \frac{1}{2} L_p(\chi, 1)$ est nul modulo $\frac{p^n}{\omega_\chi}$, où $n \geq 1$ désigne l'étage considéré. Ainsi les cas non signalés comme favorables sont ceux pour lesquels le p-groupe T relatif au corps cubique de conducteur ℓ est trivial.

T 1	$\ell = 7$ fixe ; p variable > 2	Cas favorables	maximum en p étudié
	modulo p	p = 61 ; p = 241	p = 541
	modulo p^2	néant	p = 61

T 2	p = 3 fixe ; ℓ variable	cas favorables	maximum en ℓ étudié
	modulo $\sqrt{-3}$	$\ell = 19, 37, 73, 109, 127,$ $163, 181, 199, 271, 307,$ $379, 397, 433, 487, 523,$ $541, \ldots.$ $\ell \equiv 1 \bmod 9$	
	modulo $3\sqrt{-3}$	$\ell = 199, 271, 487, 523, 541$	541
	modulo $9\sqrt{-3}$	néant	541

T 3	p = 5 fixe ; ℓ variable	cas favorables	maximum en ℓ étudié
	modulo 5 et 5^2	$\ell = 151, 367$	541
	modulo 5^3 et 5^4	néant	367

T 4	p = 2 fixe ; ℓ variable	cas favorables	maximum en ℓ étudié
	modulo 2^3 et 2^4	$\ell = 31, 43, 109, 127,$ $157, 163, 223, 229,$ $277, 283$	283
	modulo 2^5 et 2^6	$\ell = 277$	283
	modulo 2^7 et 2^8	néant	277

Remarque 1 :

Ont aussi été testés deux cas connus comme favorables par le nombre de classes :

$$\ell = 313 \ , \ p = 7$$

$$\ell = 877 \ , \ p = 7$$

A l'étage 1, seul étudié, le phénomène prévu a été confirmé.

Remarque 2 :

Dans le cas $\left(\frac{p}{3}\right) = -1$, le corps $\mathbb{Q}_p(j)$ est de degré 2 sur $\mathbb{Q}_p$ (et 3 est inerte). Donc si l'on écrit $\frac{1}{2}L_p(\chi, 1) = A + Bj$, il est clair que

$$\frac{1}{2}L_p(\chi, 1) \cdot \frac{1}{2}L_p\left(\chi^{-1}, 1\right) = N(A + Bj) = A^2 + B^2 - AB$$

est de la forme $p^{2a}u$, $a \geq 0$, $u \in \mathbb{Z}_p^*$; ainsi les étages où la congruence est favorable se regroupent deux par deux nécessairement (cas de p = 2 et p = 5).

Conclusion : Ordre du groupe T du corps cubique cyclique de conducteur ℓ considéré, dans les cas favorables.

C_1	conducteur $\ell = 7$ fixe		
	valeurs de p	61	241
	ordre de T	61	non obtenu

C_2	p = 3 fixe									
	conducteur ℓ	19	37	73	109	127	163	181	199	271
	ordre de T	3	3	3	3	3	3	3	9	9
	conducteur ℓ	307	379	397	433	487	523	541	577	
	ordre de T	3	3	3	3	9	9	9	3	

C_3	$p = 5$ fixe		
	conducteur ℓ	151	367
	ordre de T	25	25

C_4	$p = 2$ fixe										
	conducteur ℓ	31	43	109	127	157	163	223	229	277	283
	ordre de T	4	4	4	4	4	4	4	4	16	4

Bibliographie

[1] J. COATES
p-adic L-functions and Iwasawa's theory.
Proc. of Durham Symposium 1975, Academic Press, New-York - London (1977), 269-353.

[2] G. GRAS
Formules analytiques p-adiques.
Cours de DEA (Théorie des Nombres), Besançon, (1981-1982).

[3] K. IWASAWA
Lectures on p-adic L-functions
Annals of Math. Studies n°74, Princeton University Press, New Jersey, (1972).

[4] L.-C. WASHINGTON
Introduction to cyclotomic fields.
Springer Verlag, New York, (1982).

Jean-Noël MARTIN
3, rue de Frahier
Chalonvillars
70400 HERICOURT