ACTA ARITHMETICA
LII (1989)

Relations congruentielles linéaires entre nombres de classes de corps quadratiques

par

GEORGES GRAS (Besançon)

0. Introduction. Il existe un certain nombre de congruences, entre nombres de classes de corps quadratiques imaginaires, de la forme

$$\sum_i \alpha_i h(-e_i) \equiv \alpha \bmod 2^r,$$

où α_i, e_i, α, r se définissent de façon élémentaire à partir de la donnée d'un nombre premier ou d'un ensemble U convenable de nombres premiers impairs. Celles de A. Pizer [P] proviennent de la théorie des algèbres de quaternions sur Q (via le dénombrement des classes d'isomorphie des ordres d'Eichler) et elles utilisent essentiellement des e_i diviseurs de $2pq$ (i.e. $U = \{p, q\}$, p, q premiers). Celles de M. A. Kenku [K] sont obtenues dans le cadre de la théorie des courbes elliptiques, via la formule de Riemann–Hurwitz, et conduisent à des congruences semblables(1). L'article plus récent de K. Hardy et K. S. Williams [HW] donne une congruence générale (i.e. U arbitraire) contenant les précédentes. Rappelons enfin qu'un certain nombre de congruences générales de H. Lang et R. Schertz [LS] (voir également [L]) procèdent à la fois de congruences de la forme précédente, et de congruences, d'une autre nature, qui traduisent en fait des propriétés du module de continuité des fonctions L p-adiques: ce dernier point a été abordé par Desnoux [D] puis Hikita [Hi], à la suite des résultats de Kaplan, Kaplan–Williams et Williams (cf. [K], [KW1], [KW2], [KW3], [W1], [W2]); dans ces travaux, on a en général $|U| \leqslant 2$, le cas d'un ensemble U arbitraire ayant été donné dans [G1], en ce qui concerne l'aspect module de continuité.

Les congruences générales de Hardy–Williams, Lang–Schertz et Hikita ainsi que celles de Kaplan–Williams–Desnoux, sont de type analytique et sont obtenues par des transformations élémentaires complexes des formules analytiques classiques pour les corps quadratiques, sans que soit dégagée l'origine commune de ces congruences; cependant, celles de Desnoux sont directement issues de la théorie des fonctions L p-adiques.

(1) Voir [HW] au sujet de l'inexactitude de certaines congruences dans [K].

Nous montrons dans cet article que les aspects structurels développés dans [G1], pour la théorie des fonctions L p-adiques de $\boldsymbol{Q}$ (avec ici $p=2$), permettent de résoudre systématiquement et complètement ce type de problème; en outre l'intérêt majeur des fonctions L_p est de conduire, sans apports techniques supplémentaires, à des relations congruentielles mettant aussi en jeu des nombres de classes et unités de corps quadratiques réels. De façon précise, nous obtenons d'abord un système maximal de 7 congruences indépendantes, avec lesquelles nous décrivons et classifions l'ensemble des relations linéaires qui s'en déduisent (cf. théorème (1.3)), et nous obtenons alors, comme conséquence essentielle, une famille de congruences modulo 2^{n+5}, où $n=|U|$, U étant arbitraire (cf. théorème (1.4)); l'existence de congruences générales modulo 2^{n+5} a été rendu crédible par Desnoux qui a établi une telle congruence dans le cas $n=1$ (i.e. modulo 64) [D, th. C], et excepté cet exemple, toutes les congruences citées ont pour module 2^{n+2} pour les plus générales et 2^{n+3} pour les autres dans les meilleurs cas.

1. Enoncé des résultats principaux (théorèmes (1.3) et (1.4)).

(1.1) NOTATIONS. Pour tout entier $e>0$ sans facteur carré on désigne par:

$h(\pm e)$ le nombre de classes d'idéaux de $\boldsymbol{Q}(\sqrt{\pm e})$, excepté pour $-e\in\{-1,-3\}$, où l'on pose $h(-1)=1/2$, $h(-3)=1/3$ (donc $h(\pm e)$ est dans tous les cas le produit du nombre de classes par le facteur $2/w(\pm e)$, où $w(\pm e)$ désigne le nombre de racines de l'unité contenues dans $\boldsymbol{Q}(\sqrt{\pm e})$),

$\varepsilon(e)$ et $\dfrac{\log\varepsilon(e)}{\sqrt{D(e)}}$ l'unité fondamentale (>1) de $\boldsymbol{Q}(\sqrt{e})$ et le quotient de son logarithme 2-adique par la racine carrée (positive) du discriminant du corps,

$\left(\dfrac{\pm e}{p}\right)$ le symbole de Legendre de reste quadratique modulo le nombre premier p impair, $p\nmid e$,

$\left(\dfrac{\pm e}{2}\right)$ le symbole de Kronecker (nul si $\pm e\equiv 2, 3(4)$, égal à -1 si $\pm e\equiv 5(8)$, égal à 1 si $\pm e\equiv 1(8)$).

(1.2) DÉFINITIONS. Soit $m\geqslant 1$ un entier impair sans facteur carré.

(i) Pour $\lambda\in\{1,2\}$, $\mu\in\{-1,+1\}$, on considère les sommations:

$$S(-\lambda,\mu)=\sum_{\substack{d|m\\ d\equiv\mu(4)}}(-1)^{n_d}\left(1-\left(\frac{-\lambda d}{2}\right)\right)h(-\lambda d)\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{-\lambda d}{l}\right)\right),$$

$$S(\lambda,\mu)=\sum_{\substack{d|m\\ d\equiv\mu(4)\\ (d\neq 1\text{ si }\lambda=\mu=1)}}(-1)^{n_d}\left(2-\left(\frac{\lambda d}{2}\right)\right)h(\lambda d)\frac{\log\varepsilon(\lambda d)}{\sqrt{D(\lambda d)}}\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{\lambda d}{l}\right)l^{-1}\right),$$

où d est toujours pris positif et où n_d désigne le nombre de diviseurs premiers de d.

(ii) On obtient ainsi les 8 sommes fondamentales suivantes:

$$A=S(-1,1)=\sum_{\substack{d|m\\ d\equiv 1(4)}}(-1)^{n_d}h(-d)\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{-d}{l}\right)\right),$$

$$\bar{A}=S(-1,-1)=2\sum_{\substack{d|m\\ d\equiv -5(8)}}(-1)^{n_d}h(-d)\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{-d}{l}\right)\right),$$

$$B=S(-2,1)=\sum_{\substack{d|m\\ d\equiv 1(4)}}(-1)^{n_d}h(-2d)\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{-2d}{l}\right)\right),$$

$$\bar{B}=S(-2,-1)=\sum_{\substack{d|m\\ d\equiv -1(4)}}(-1)^{n_d}h(-2d)\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{-2d}{l}\right)\right),$$

$$X=S(1,1)=\sum_{\substack{d|m\\ d\equiv 1(4), d\neq 1}}(-1)^{n_d}\left(2-\left(\frac{d}{2}\right)\right)h(d)\frac{\log\varepsilon(d)}{\sqrt{d}}\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{d}{l}\right)l^{-1}\right),$$

$$\bar{X}=S(1,-1)=\sum_{\substack{d|m\\ d\equiv -1(4)}}(-1)^{n_d}h(d)\frac{\log\varepsilon(d)}{\sqrt{d}}\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{d}{l}\right)l^{-1}\right),$$

$$Y=S(2,1)=\sum_{\substack{d|m\\ d\equiv 1(4)}}(-1)^{n_d}h(2d)\frac{\log\varepsilon(2d)}{\sqrt{2d}}\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{2d}{l}\right)l^{-1}\right),$$

$$\bar{Y}=S(2,-1)=\sum_{\substack{d|m\\ d\equiv -1(4)}}(-1)^{n_d}h(2d)\frac{\log\varepsilon(2d)}{\sqrt{2d}}\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{2d}{l}\right)l^{-1}\right).$$

(iii) On définit également

$$S^*(-1,-1)=\sum_{\substack{d|m\\ d\equiv -1(4)}}(-1)^{n_d}h(-d)\prod_{\substack{l|m\\ l\nmid d}}\left(1-\left(\frac{-d}{l}\right)\right)\quad\text{si } m>1,$$

$S^*(-1,-1)=1/2$ si $m=1$.

(1.3) THÉORÈME. *Soient* $l_1,\ldots,l_n$, $n\geqslant 0$, *des nombres premiers impairs distincts et soit* $m=\prod_{i=1}^{n} l_i$; *soient*

$$\pi=\prod_{i=1}^{n}(1-l_i^{-1}),\qquad \eta=(\pi/2)\left(2a_0+\sum_{i=1}^{n}\frac{\log l_i}{l_i-1}\right)\quad et\quad \xi=\frac{\log 5}{4}\equiv 31 \bmod 64$$

(*où la fonction* log *désigne le logarithme 2-adique, et où* a_0 *est une constante universelle congrue à* 8 mod 32 (cf. (3.2))).

(i) *On a la congruence suivante*:

$$(c_0)\qquad S^*(-1,\,-1)\equiv \pi/2 \bmod 2^n;$$

(ii) *On a les 7 congruences indépendantes suivantes* (cf. (1.2), (ii)):

$$(c_1)\qquad \bar{A}-A+X-\bar{X}\equiv -\eta+\xi\pi/2 \bmod 2^{n+3},$$

$$(c_2)\qquad \bar{A}-B+Y-\bar{X}\equiv (4/3)\,\xi\pi/2 \bmod 2^{n+3},$$

$$(c_3)\qquad \bar{A}-A-\bar{B}+B\equiv (5/3)\,\xi\pi/2 \bmod 2^{n+2},$$

$$(c_4)\qquad \bar{A}-B+X-\bar{Y}\equiv -\eta-(2/3)\,\xi\pi/2 \bmod 2^{n+2},$$

$$(c_5)\qquad \bar{A}-\bar{X}\equiv 0 \bmod 2^{n+2},$$

$$(c_6)\qquad \bar{A}-A\equiv \xi\pi/2 \bmod 2^{n+1},$$

$$(c_7)\qquad \bar{B}-A\equiv \xi\pi/2 \bmod 2^{n+1};$$

(iii) *L'ensemble de toutes les congruences, dont le 1er membre est combinaison* $\mathbf{Z}_2$*-linéaire de ceux des* c_i, $1\leqslant i\leqslant 7$, *est décrit par la congruence générale suivante*:

$$aA+\bar{a}\bar{A}+bB+\bar{b}\bar{B}+xX+\bar{x}\bar{X}+yY+\bar{y}\bar{Y}\equiv \alpha\eta+\beta\xi\pi/2 \bmod 2^{n+1+\gamma},$$

$a,\ \bar{a},\ b,\ \bar{b},\ x,\ \bar{x},\ y,\ \bar{y}\in\mathbf{Z}_2$, $a+\bar{a}+b+\bar{b}+x+\bar{x}+y+\bar{y}=0$, *où* $\alpha=-x$, $\beta=-a+(2/3)\,b+2y$, *où* 2^γ *est le* p.g.c.d, *dans* $\mathbf{Z}_2$, *des 7 nombres*

$\bar{a}+\bar{b}+\bar{x}+\bar{y}$,
$b+\bar{b}+2(x+\bar{x})-(y+\bar{y})$,
$2(\bar{b}+\bar{y})-4(x-y)$,
$4(x+\bar{x}+y+\bar{y})$,
$8(x+y)$,
$8(x+\bar{x})$,
16.

(1.4) Théorème. (i) *Les hypothèses et notations étant les mêmes qu'en* (1.3), *on a la congruence générale suivante*:

$$a_1A+\bar{a}_1\bar{A}+b_1B+\bar{b}_1\bar{B}+x_1X+\bar{x}_1\bar{X}+y_1Y+\bar{y}_1\bar{Y}$$

$$\equiv -x_1\eta+(-a_1+(2/3)\,b_1+2y_1)\,\xi\pi/2 \bmod 2^{n+5},$$

où $a_1=1-4f-8e-8h+16j-16i$, $\bar{a}_1=1-2e+4f-8g-8h-16j$, $b_1=1+2f+8e+8h+16i$, $\bar{b}_1=1+2e-2f+4g$, $x_1=-1$, $\bar{x}_1=-1+2e$, $y_1=-1+2f$, $\bar{y}_1=-1-2e-2f+4g+8h$, $e,\ f,\ g,\ h,\ i,\ j$ *arbitraires dans* $\mathbf{Z}_2$;

(ii) *En particulier on a la congruence suivante*:

$$A+\bar{A}+B+\bar{B}-X-\bar{X}-Y-\bar{Y}\equiv \eta-(7/3)\,\xi\pi/2 \bmod 2^{n+5}.$$

(1.5) Remarques. (i) On constatera que, par rapport aux congruences déjà connues, les congruences (1.3), (iii), et (1.4), ont une forme canonique; en particulier, les constantes a_0 et ξ sont universelles.

(ii) La théorie des genres analytique fournit les congruences suivantes:

$$A\equiv \pi/2 \bmod 2^n,$$

$$\bar{A}\equiv B\equiv \bar{B}\equiv X\equiv \bar{X}\equiv Y\equiv \bar{Y}\equiv 0 \bmod 2^n;$$

en effet, on verra au § 4 que chaque terme de chaque somme S est de la forme $L_2(\theta,s)$, θ caractère quadratique, $s\in\{0,1\}$, auquel cas [G1, (0.2)] conduit au résultat dès que $\theta\neq 1$; le cas $\theta=1$ concerne le terme de $A=S(-1,1)$, relatif à $d=1$, et c'est

$$(1/2)\prod_{l\mid m}\left(1-\left(\frac{-1}{l}\right)\right)\equiv \pi/2 \bmod 2^n.$$

(iii) La nouvelle famille de congruences (1.4) donne toutes les congruences générales, de la forme (1.3), (iii), selon le module 2^{n+5}.

(iv) Les résultats des §§ 4, 5 permettent de vérifier que les congruences de Kenku, Pizer, Lang–Schertz, Kaplan, Williams, Hardy–Williams et Desnoux (cf. § 0) sont des conséquences de (1.3), (1.4). On peut alors obtenir, à partir de (1.3), (iii), et (1.4), un nombre considérable de congruences particulières, selon les modules 2^{n+1} à 2^{n+5} (par exemple en imposant que certains des coefficients $a,\ \bar{a},\ b,\ \bar{b},\ x,\ \bar{x},\ y,\ \bar{y}$ soient nuls); nous laissons au lecteur le soin d'écrire celles qu'il souhaite: les données numériques citées en (1.3), (1.4), (3.3), (4.5) sont suffisantes pour conduire ces calculs élémentaires.

(v) Voir le point (4.6) en complément aux résultats précédents.

2. Congruences entre fonctions L_2. Des relations linéaires générales entre les fonctions L p-adiques des différentes composantes d'un caractère de Dirichlet χ ont été obtenues dans [G2] comme conséquence des propriétés standard des $\mathbf{Z}_p$-distributions de Stickelberger (cf. [G1]). Dans le cas qui nous occupe ($p=2$, χ quadratique), ces congruences se simplifient et nous en donnons un peu plus loin l'énoncé correspondant.

(2.1) Définitions. (i) Pour tout ensemble I de nombres premiers, on désigne par $\mathbf{Q}_I$ l'extension abélienne maximale de $\mathbf{Q}$, non ramifiée en dehors de $I\cup\{\infty\}$; si $I\cap I'=\emptyset$, alors $\mathbf{Q}_{I\cup I'}$ est le composé direct sur $\mathbf{Q}$ de $\mathbf{Q}_I$ et $\mathbf{Q}_{I'}$.

(ii) Soit U un ensemble de $n\geqslant 0$ nombres premiers impairs et soit $S=U\cup\{2\}$. On sait que $\mathbf{Q}_{\{2\}}$ est le composé direct sur $\mathbf{Q}$ de $\mathbf{Q}_0$ et $\mathbf{Q}_\infty$, où $\mathbf{Q}_0=\mathbf{Q}(\sqrt{-1})$ où $\mathbf{Q}(\sqrt{-2})$, et $\mathbf{Q}_\infty$ la $\mathbf{Z}_2$-extension cyclotomique de $\mathbf{Q}$; donc pour tout $J\subseteq U$, $\mathbf{Q}_{J\cup\{2\}}$ est le composé direct sur $\mathbf{Q}$ de $\mathbf{Q}_J$, $\mathbf{Q}_0$ et $\mathbf{Q}_\infty$.

(iii) On pose $G_S=\mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q})$; on sait qu'il existe un isomorphisme canonique qui permet d'identifier G_S à $\prod_{q\in S}\mathbf{Z}_q^*$ et donc de décrire tous les groupes de Galois des sous-extensions de Q_S/Q, ce que nous faisons systématiquement.

(iv) Pour tout $I \subseteq S$, soit X_I le groupe des caractères d'ordre fini de Q_I; le point (ii) précédent montre en particulier que pour tout $J \subseteq U$ on a

$$X_{J\cup\{2\}} = X_0 \oplus X_\infty \oplus X_J,$$

où X_0, X_∞, X_J sont les groupes des caractères des corps Q_0, Q_∞, Q_J (on a $X_0 \oplus X_\infty = X_{Q_{\{2\}}}$). Si $\chi \in X_{J\cup\{2\}}$, on désigne par χ_0, χ_∞, χ_J ses composantes sur X_0, X_∞, X_J.

(v) On désigne par ω le caractère d'ordre 2 de $Q(\sqrt{-1})$ et par ψ celui de $Q(\sqrt{2})$, par $\langle\ \rangle$ le caractère d'ordre infini de Q_∞ défini par $\langle a \rangle = a\omega^{-1}(a)$, pour tout a de Z_2^* considéré comme sous-groupe de G_S. On désigne par ω_0 le caractère d'ordre 2 de Q_0; on a $\omega_0 = \omega$ si $Q_0 = Q(\sqrt{-1})$, $\omega_0 = \omega\psi$ si $Q_0 = Q(\sqrt{-2})$.

(vi) Pour tout $l \in U$ on appelle h_l un progénérateur de $\mathrm{Gal}(Q_S/Q_{S-\{l\}})$; on désigne par h_{-1} le générateur de $\mathrm{Gal}(Q_S/Q_U Q_\infty)$ et par h_0 un progénérateur de $\mathrm{Gal}(Q_S/Q_U Q_0)$; enfin σ désigne l'unique élément de G_S qui fixe $Q_U(\sqrt{-1})$ et est tel que $\langle\sigma\rangle = 5$ (on a $h_0 = \sigma$ ou σh_{-1} selon que $Q_0 = Q(\sqrt{-1})$ ou $Q(\sqrt{-2})$).

(vii) On pose $\pi = \prod_{l\in U}(1-l^{-1})$ et $\xi = (\log 5)/4$.

Nous pouvons maintenant écrire les congruences fondamentales, issues des théorèmes (0.2) et (0.3) de [G2], avec les données suivantes (cf. [G2, (0.1)]):

χ est un caractère quadratique dont l'ensemble des diviseurs premiers du conducteur est U ou $U\cup\{2\}$,

$$E = U, \quad U\cup\{0\}, \quad U\cup\{-1\} \quad \text{ou } U\cup\{-1, 0\};$$

en outre, si $\chi_0 \neq 1$ nous supposerons que $-1 \notin E$ (cf. [G2, lemme, p. 17]).

Désignons par v la valuation 2-adique sur Q.

(2.2) Proposition ([G2, (0.2), $E = U$). *Pour tout caractère quadratique χ dont l'ensemble des diviseurs premiers du conducteur est U ($|U| = n$, U ne contenant pas 2), on a la congruence*

$$-\sum_{J\subseteq U}(-1)^{|J|}B_1(\chi_J)\prod_{l\in U-J}(1-\chi_J(l)) \equiv \pi/2 \mod 2^n.$$

(2.3) Proposition ([G2, (0.3)]). *Soit χ un caractère quadratique dont l'ensemble des diviseurs premiers du conducteur est U ou $U\cup\{2\}$ ($|U| = n$):*

(i) *Si $\chi_0 = \omega_0$ et $E = U\cup\{0\}$, on a la congruence:*

$$-\sum_{J\subseteq U}(-1)^{|J|}L_2(\omega_0\chi_\infty\chi_J, s)\prod_{l\in U-J}(1-\omega\omega_0\chi_\infty\chi_J(l)\langle l\rangle^{-s})$$
$$-\sum_{J\subseteq U}(-1)^{|J|}B_1(\chi_J)(1-\chi_J(2))\prod_{l\in U-J}(1-\chi_J(l)) \equiv 0 \mod 2^{n_\chi},$$

où $n_\chi = n+1$ (resp. $n+2+v(s)$) si $\omega_0\chi_\infty = \omega\psi$ (resp. ω);

(ii) *si $\chi_0 = 1$ et $E = U\cup\{-1\}$, on a la congruence:*

$$-\sum_{J\subseteq U}(-1)^{|J|}L_2(\chi_\infty\chi_J, s)\prod_{l\in U-J}(1-\omega\chi_\infty\chi_J(l)\langle l\rangle^{-s})$$
$$+\sum_{J\subseteq U}(-1)^{|J|}L_2(\omega_0\chi_\infty\chi_J, s)\prod_{l\in U-J}(1-\omega\omega_0\chi_\infty\chi_J(l)\langle l\rangle^{-s})$$
$$\equiv -2\xi(1-\chi_\infty(5)5^{1-s})^{-1}\pi \mod 2^{n+1};$$

(iii) *si $\chi_0 = 1$ et $E = U\cup\{0\}$, on a la congruence:*

$$-\sum_{J\subseteq U}(-1)^{|J|}L_2(\chi_\infty\chi_J, s)\prod_{l\in U-J}(1-\omega\chi_\infty\chi_J(l)\langle l\rangle^{-s})$$
$$-\sum_{J\subseteq U}(-1)^{|J|}B_1(\omega_0\chi_J)\prod_{l\in U-J}(1-\omega_0\chi_J(l))$$
$$\equiv -2\xi\left((1-\chi_\infty(5)5^{1-s})^{-1}-(1-5\omega_0(5))^{-1}\right)\pi \mod 2^{n_\chi},$$

où $n_\chi = n+1$ (resp. $n+2+v(s)$) si $\omega_0\chi_\infty = \omega\psi$ (resp. ω);

(iv) *si $\chi_0 = 1$ et $E = U\cup\{-1, 0\}$, on a la congruence:*

$$\sum_{J\subseteq U}(-1)^{|J|}L_2(\chi_\infty\chi_J, s)\prod_{l\in U-J}(1-\omega\chi_\infty\chi_J(l)\langle l\rangle^{-s})$$
$$-\sum_{J\subseteq U}(-1)^{|J|}L_2(\omega_0\chi_\infty\chi_J, s)\prod_{l\in U-J}(1-\omega\omega_0\chi_\infty\chi_J(l)\langle l\rangle^{-s})$$
$$+\sum_{J\subseteq U}(-1)^{|J|}B_1(\omega_0\chi_J)\prod_{l\in U-J}(1-\omega_0\chi_J(l))$$
$$-\sum_{J\subseteq U}(-1)^{|J|}B_1(\chi_J)(1-\chi_J(2))\prod_{l\in U-J}(1-\chi_J(l))$$
$$\equiv 2\xi\left((1-\chi_\infty(5)5^{1-s})^{-1}-(1-5\omega_0(5))^{-1}\right)\pi \mod 2^{n_\chi},$$

où $n_\chi = n+2$ (resp. $n+3+v(s)$) si $\omega_0\chi_\infty = \omega\psi$ (resp. ω).

(2.4) Remarques. (i) Dans chacune des sommations des congruences (2.3), nous avons posé systématiquement $I = J\cup K$, $K \subseteq \{-1, 0\}$, et décomposé le caractère χ_I sur $X_0 \oplus X_\infty \oplus X_J$;

(ii) Les signes des premiers membres sont tels que le module correspondant de la congruence est toujours de la forme $\langle\omega\chi\langle\ \rangle^s, v\prod_{l\in E}(1-h_l)\rangle$ (cf.

(2.1), (v), (vi)), où ν est une $\boldsymbol{Z}_p$-mesure sur G_S qui ne dépend que du choix de la décomposition de G_S en somme directe et de celui de E, et non du caractère χ (i.e. qui ne dépend pas des valeurs de χ_0 et χ_∞);

(iii) On ne fait aucune hypothèse sur la parité de χ; on rappelle que $L_2(\theta) = 0$ si θ est impair, que $B_1(\theta) = 0$ si $\theta \neq 1$ est pair et que $B_1(1) = 1/2$.

Avant d'utiliser les congruences précédentes, en vue de la démonstration de (1.3), on remarque que pour $\chi_\infty = 1$, les congruences (2.3), (ii), (iii) et (iv) sont indéterminées en $s = 1$ (présence d'un pôle simple dans chacun des 2 membres).

3. Suppression des parties polaires. On est dans le cas où $\chi_0 = \chi_\infty = 1$; il suffit, par différence, de calculer la limite (notée η) de

(3.1) $$\eta(s) = L_2(1, s)\prod_{l\in U}\left(1-\omega(l)\langle l\rangle^{-s}\right) - 2\xi(1-5^{1-s})^{-1}\pi,$$

lorsque $s \to 1$.

(3.2) Lemme. *On a*

$$\lim_{s\to 1}\eta(s) = \eta = \left(2a_0 + \sum_{l\in U}\frac{\log l}{l-1}\right)\pi/2,$$

où

$$a_0 = \lim_{s\to 1}\left(L_2(1, s) - 2\xi(1-5^{1-s})^{-1}\right)\in \boldsymbol{Z}_2.$$

D'après [S], on sait que la pseudo-mesure λ telle que $L_2(1, s) = \langle\langle\ \rangle^{1-s}, \lambda\rangle$, est de la forme

$$\lambda = c\alpha_A T^{-1} + \sum_{i\geq 0}\alpha_i T^i, \qquad T = 1-\sigma,$$

où

α_A est la $\boldsymbol{Z}_2$-mesure de Haar sur $A = \mathrm{Gal}(\boldsymbol{Q}_{(2)}/\boldsymbol{Q}_\infty)$ égale ici à $1+\tau$ où τ engendre A,

$\alpha_i \in \boldsymbol{Z}_2[A]$,

$c = \xi$ (cf. [G2, (3.8)]; la constante c se détermine en écrivant que $\mathrm{Rés}_{s=1} L_2(1, s) = 1/2$).

Posons $T(s) = \langle\langle\ \rangle^{1-s}, T\rangle = 1-5^{1-s}$; l'égalité (3.1) devient

$$\eta(s) = \left(2\xi T(s)^{-1} + \sum_{i\geq 0} a_i T(s)^i\right)\prod_{l\in U}\left(1-\langle l\rangle^{1-s}l^{-1}\right) - 2\xi\pi T(s)^{-1},$$

où $a_i \in \boldsymbol{Z}_2$ pour tout $i \geq 0$. Comme $T(1) = 0$, il suffit d'étudier

$$\eta_1(s) = \left(2\xi T(s)^{-1} + a_0\right)\prod_{l\in U}\left(1-\langle l\rangle^{1-s}l^{-1}\right) - 2\xi\pi T(s)^{-1}$$

ou encore

$$\eta_2(s) = 2\xi T(s)^{-1}\left(\prod_{l\in U}\left(1-\langle l\rangle^{1-s}l^{-1}\right)-\pi\right) + a_0\pi.$$

Ecrivons $\langle l\rangle^{1-s} = \sum_{i\geq 0}\left((1-s)\log l\right)^i/i!$ (série convergente dans $\boldsymbol{Z}_2$); on a alors

$$\prod_{l\in U}\left(1-\langle l\rangle^{1-s}l^{-1}\right) = \prod_{l\in U}\left(1-l^{-1}-l^{-1}\sum_{i\geq 1}\left((1-s)\log l\right)^i/i!\right)$$
$$= \pi - (1-s)\pi\sum_{l\in U}\frac{\log l}{l-1} + (1-s)^2 f(1-s),$$

où $f(1-s)$ est une série convergente en $s = 1$.

Comme $(1-s)^2 f(1-s)\,T(s)^{-1} \to 0$ si $s \to 1$, on est amené à étudier, au voisinage de 1,

$$\eta_3(s) = -2\xi(1-s)\,T(s)^{-1}\pi\sum_{l\in U}\frac{\log l}{l-1} + a_0\pi$$

dont la limite est (puisque $T(s)/(s-1) \to \log 5$)

$$\eta = \pi\left(a_0 + (1/2)\sum_{l\in U}\frac{\log l}{l-1}\right).$$

Comme $\pi \equiv 0 \bmod 2^n$, il suffit en pratique de connaître a_0 modulo 32:

(3.3) Lemme. *On a* $\xi \equiv -97 \bmod 2^9$ *et* $a_0 \equiv 8 \bmod 2^5$.

On a $L_2(1, s) = 2\xi(1-5^{1-s})^{-1} + \sum_{i\geq 0} a_i(1-5^{1-s})^i$, et pour $s = -7$, on obtient

$$L_2(1, -7) \equiv -2\xi/(5^8-1) + a_0 \bmod 2^5$$

$$\text{or}\quad L_2(1, -7) = -(1-2^7)B_8/8 = (1-2^7)/240,$$

et il suffit de connaître ξ modulo 2^9; un calcul élémentaire de $\log 5$ modulo 2^{11} donne alors le résultat annoncé.

4. Démonstration du théorème principal. Rappelons brièvement les formules analytiques p-adiques classiques de Hasse [H] (cas imaginaire) et Leopoldt [L] (cas réel):

(4.1) Lemme. (i) *Pour tout caractère quadratique impair θ, de conducteur f, on a* $B_1(\theta) = -h(-f)$ (cf. (1.1));

(ii) *pour tout caractère quadratique pair $\theta \neq 1$, de conducteur f, on a*

$$L_2(\theta, 1) = \left(2-\theta(2)\right)h(f)\frac{\log\varepsilon(f)}{\sqrt{f}} \quad \text{(cf. (1.1))};$$

(iii) *on a également, pour tout* θ:

$$\dot{L}_2(\theta, 0) = -(1-\omega\theta(2))\,B_1(\omega\theta).$$

On considère désormais $U = \{l_1, \ldots, l_n\}$ (cf. (1.3)) auquel on va appliquer les résultats du § 2.

(4.2) Lemme. *Soit* χ *un caractère quadratique de conducteur* m, $4m$ *ou* $8m$, *de parité quelconque*:

(i) *dans les congruences* (2.2), (2.3), *le caractère* χ_J, $J \subseteq U$, *est le caractère non trivial du corps* $\boldsymbol{Q}(\sqrt{(-1)^k d})$, $k = (d-1)/2$, *où* $d = \prod_{j \in J} l_j$; *on a alors la correspondance suivante* ($J \subseteq U$, $d \mid m$):

$$\begin{array}{llll}
\chi_J \leftrightarrow \boldsymbol{Q}(\sqrt{d}) & \text{si } d \equiv 1\,(4), & \boldsymbol{Q}(\sqrt{-d}) & \text{si } d \equiv -1\,(4),\\
\omega\chi_J \leftrightarrow \boldsymbol{Q}(\sqrt{-d}) & \text{si } d \equiv 1\,(4), & \boldsymbol{Q}(\sqrt{d}) & \text{si } d \equiv -1\,(4),\\
\psi\chi_J \leftrightarrow \boldsymbol{Q}(\sqrt{2d}) & \text{si } d \equiv 1\,(4), & \boldsymbol{Q}(\sqrt{-2d}) & \text{si } d \equiv -1\,(4),\\
\omega\psi\chi_J \leftrightarrow \boldsymbol{Q}(\sqrt{-2d}) & \text{si } d \equiv 1\,(4), & \boldsymbol{Q}(\sqrt{2d}) & \text{si } d \equiv -1\,(4);
\end{array}$$

(ii) *on a* (cf. (1.1)):

$$\chi_J = \left(\frac{\pm d}{\cdot}\right), \quad \omega\chi_J = \left(\frac{\mp d}{\cdot}\right), \quad \psi\chi_J = \left(\frac{\pm 2d}{\cdot}\right), \quad \omega\psi\chi_J = \left(\frac{\mp 2d}{\cdot}\right),$$

les signes convenables étant définis en (i) *ci-dessus.*

Il suffit maintenant de considérer les congruences (2.2) et (2.3), et de faire varier χ_0, χ_∞ respectivement dans $\{1, \omega_0\}$, $\{1, \psi\}$, avec les 2 choix possibles pour $\omega_0 \in \{\omega, \omega\psi\}$; on en déduit alors toutes les congruences possibles, d'une part en $s = 0$ et d'autre part en $s = 1$, en utilisant les formules analytiques (4.1) et la correspondance (4.2).

Lorsque l'on est dans le cas $s = 1$, on tient compte du calcul effectué au § 3. On remarque enfin que si $s = 0$ et $\omega_0\chi_\infty = \omega$, alors les congruences (2.3), (i), (iii) et (iv) se réduisent à $0 \equiv 0 \bmod 2^{n_\chi}$.

On obtient alors la liste suivante:

congruence issue de (2.2) (pour $U \neq \emptyset$, le terme en $J = \emptyset$ est nul):

$$(c_0) \qquad S^*(-1, -1) \equiv \pi/2 \bmod 2^n.$$

congruences issues de (2.3) (on rappelle que $\chi_0 = 1$ sauf dans le cas (i)):

$$\begin{array}{lll}
(r_1) & ((\mathrm{i}),\ s = 0,\ \omega_0\chi_\infty = \omega\psi) & \bar{A} - \bar{B} \equiv 0 \bmod 2^{n+1}\\
(r_2) & ((\mathrm{i}),\ s = 1,\ \omega_0\chi_\infty = \omega) & \bar{A} - \bar{X} \equiv 0 \bmod 2^{n+2}\\
(r_3) & ((\mathrm{i}),\ s = 1,\ \omega_0\chi_\infty = \omega\psi) & \bar{A} - \bar{Y} \equiv 0 \bmod 2^{n+1}\\
(r_4) & ((\mathrm{ii}),\ s = 0,\ \chi_\infty = 1,\ \omega_0 = \omega) & \bar{A} - A \equiv \xi\pi/2 \bmod 2^{n+1}
\end{array}$$

$$\begin{array}{lll}
(r_5) & ((\mathrm{ii}),\ s = 0,\ \chi_\infty = 1,\ \omega_0 = \omega\psi) & \bar{B} - A \equiv \xi\pi/2 \bmod 2^{n+1}\\
(r_6) & ((\mathrm{ii}),\ s = 0,\ \chi_\infty = \psi,\ \omega_0 = \omega) & \bar{B} - B \equiv -(\xi/3)\pi \bmod 2^{n+1}\\
(r_7) & ((\mathrm{ii}),\ s = 0,\ \chi_\infty = \psi,\ \omega_0 \equiv \omega\psi) & \bar{A} - B \equiv -(\xi/3)\pi \bmod 2^{n+1}\\
(r_8) & ((\mathrm{ii}),\ s = 1,\ \chi_\infty = 1,\ \omega_0 = \omega) & \bar{X} - X \equiv \eta \bmod 2^{n+1}\\
(r_9) & ((\mathrm{ii}),\ s = 1,\ \chi_\infty = 1,\ \omega_0 = \omega\psi) & \bar{Y} - X \equiv \eta \bmod 2^{n+1}\\
(r_{10}) & ((\mathrm{ii}),\ s = 1,\ \chi_\infty = \psi,\ \omega_0 = \omega) & \bar{Y} - Y \equiv -\xi\pi \bmod 2^{n+1}\\
(r_{11}) & ((\mathrm{ii}),\ s = 1,\ \chi_\infty = \psi,\ \omega_0 = \omega\psi) & \bar{X} - Y \equiv -\xi\pi \bmod 2^{n+1}\\
(r_{12}) & ((\mathrm{iii}),\ s = 0,\ \chi_\infty = 1,\ \omega_0 = \omega\psi) & B - A \equiv (5/3)\,\xi\pi/2 \bmod 2^{n+1}\\
(r'_{12}) & ((\mathrm{iii}),\ s = 0,\ \chi_\infty = \psi,\ \omega_0 = \omega) & A - B \equiv -(5/3)\,\xi\pi/2 \bmod 2^{n+1}\\
(r_{13}) & ((\mathrm{iii}),\ s = 1,\ \chi_\infty = 1,\ \omega_0 = \omega) & A - X \equiv \eta - \xi\pi/2 \bmod 2^{n+2}\\
(r_{14}) & ((\mathrm{iii}),\ s = 1,\ \chi_\infty = 1,\ \omega_0 = \omega\psi) & B - X \equiv \eta + (\xi/3)\pi \bmod 2^{n+1}\\
(r_{15}) & ((\mathrm{iii}),\ s = 1,\ \chi_\infty = \psi,\ \omega_0 = \omega) & A - Y \equiv -3\xi\pi/2 \bmod 2^{n+1}\\
(r_{16}) & ((\mathrm{iii}),\ s = 1,\ \chi_\infty = \psi,\ \omega_0 = \omega\psi) & B - Y \equiv -2(\xi/3)\pi \bmod 2^{n+2}\\
(r_{17}) & ((\mathrm{iv}),\ s = 0,\ \chi_\infty = 1,\ \omega_0 = \omega\psi) & A + \bar{A} - B - \bar{B} \equiv -5(\xi/3)\pi/2 \bmod 2^{n+2}\\
(r_{18}) & ((\mathrm{iv}),\ s = 0,\ \chi_\infty = \psi,\ \omega_0 = \omega) & \bar{A} - A - \bar{B} + B \equiv 5(\xi/3)\pi/2 \bmod 2^{n+2}\\
(r_{19}) & ((\mathrm{iv}),\ s = 1,\ \chi_\infty = 1,\ \omega_0 = \omega) & \bar{A} - A + X - \bar{X} \equiv -\eta + \xi\pi/2 \bmod 2^{n+3}\\
(r_{20}) & ((\mathrm{iv}),\ s = 1,\ \chi_\infty = 1,\ \omega_0 = \omega\psi) & \bar{A} - B + X - \bar{Y} \equiv -\eta - (\xi/3)\pi \bmod 2^{n+2}\\
(r_{21}) & ((\mathrm{iv}),\ s = 1,\ \chi_\infty = \psi,\ \omega_0 = \omega) & \bar{A} - A + Y - \bar{Y} \equiv 3\xi\pi/2 \bmod 2^{n+2}\\
(r_{22}) & ((\mathrm{iv}),\ s = 1,\ \chi_\infty = \psi,\ \omega_0 = \omega\psi) & \bar{A} - B + Y - \bar{X} \equiv 2(\xi/3)\pi \bmod 2^{n+3}.
\end{array}$$

(4.3) Définition. Nous considérons maintenant le $\boldsymbol{Z}_2$-module libre $\mathscr{C}$ engendré par les lettres A, $\bar{A}$, B, $\bar{B}$, X, $\bar{X}$, Y, $\bar{Y}$ et nous appelons par abus congruence toute écriture de la forme

$$C \equiv \alpha\eta + \beta\xi\pi/2 \bmod 2^{n+1+\gamma}, \qquad C \in \mathscr{C},$$

où α, $\beta \in \boldsymbol{Z}_2$, $\gamma \in \boldsymbol{N}$ sont fonction des coefficients de C; tout argument d'algèbre linéaire attribué, par abus de langage, au mot "congruence" concerne en fait le 1er membre $C \in \mathscr{C}$.

(4.4) Lemme. *Parmi les 22 congruences précédentes*, $c_1 = r_{19}$, $c_2 = r_{22}$, $c_3 = r_{18}$, $c_4 = r_{20}$, $c_5 = r_7$, $c_6 = r_4$, $c_7 = r_5$, *engendrent un sous-module de dimension 7 de* $\mathscr{C}$, *facteur direct dans* $\mathscr{C}$; *les autres congruences* r_i *s'expriment sur la base des* c_i, $1 \leqslant i \leqslant 7$, *de la façon suivante*:

$$\begin{array}{llll}
r_1 = (\ 0 & 0 & 0 & 0\ 0\ \ 1\ -1)\\
r_3 = (-1 & 0 & 1 & 1\ 1\ -1\ \ 1)\\
r_6 = (\ 0 & 0 & -1 & 0\ 0\ \ 1\ \ 0)\\
r_7 = (\ 0 & 0 & -1 & 0\ 0\ \ 2\ -1)\\
r_8 = (-1 & 0 & 0 & 0\ 0\ \ 1\ \ 0)\\
r_9 = (\ 0 & 0 & -1 & -1\ 0\ \ 2\ -1)\\
r_{10} = (\ 1 & -1 & -2 & -1\ 0\ \ 3\ -2)\\
r_{11} = (\ 0 & -1 & -1 & 0\ 0\ \ 2\ -1)
\end{array}
\qquad
\begin{array}{llll}
r_{12} = (\ 0 & 0 & 1 & 0\ 0\ -1\ \ 1)\\
r_{13} = (-1 & 0 & 0 & 0\ 1\ \ 0\ \ 0)\\
r_{14} = (-1 & 0 & 1 & 0\ 1\ -1\ \ 1)\\
r_{15} = (\ 0 & -1 & -1 & 0\ 1\ \ 1\ -1)\\
r_{16} = (\ 0 & -1 & 0 & 0\ 1\ \ 0\ \ 0)\\
r_{17} = (\ 0 & 0 & -1 & 0\ 0\ \ 2\ -2)\\
r_{21} = (-1 & 1 & 2 & 1\ 0\ -2\ \ 2)
\end{array}$$

(4.5) LEMME. *Il existe une congruence (à coefficients dans $\mathbf{Z}_2$) de la forme*

$$C = aA+\bar{a}\bar{A}+bB+\bar{b}\bar{B}+xX+\bar{x}\bar{X}+yY+\bar{y}\bar{Y} \equiv \alpha\eta+\beta\xi\pi/2 \mod 2^{n+1+\gamma},$$

qui soit combinaison $\mathbf{Z}_2$-linéaire des congruences c_i, $1 \leqslant i \leqslant 7$, si et seulement si $a+\bar{a}+b+\bar{b}+x+\bar{x}+y+\bar{y}=0$; on a alors

$$C = \sum_{i=1}^{7} \lambda_i c_i \equiv \alpha\eta+\beta\xi\pi/2 \mod 2^{n+1+\gamma},$$

où

$$\lambda_1 = x+\bar{y}, \quad \lambda_2 = y, \quad \lambda_3 = b+y-\bar{y}, \quad \lambda_4 = -\bar{y},$$

$$\lambda_5 = a+\bar{a}+b+\bar{b}, \quad \lambda_6 = \bar{a}-b+\bar{x}-y+2\bar{y}, \quad \lambda_7 = b+\bar{b}+y-\bar{y},$$

$$\alpha = -x, \quad \beta = -a+(2/3)b+2y.$$

Les lemmes (4.4) et (4.5) résultent de l'étude (élémentaire) du système linéaire qui se déduit de l'écriture

$$\sum_{i=1}^{7} \lambda_i c_i = aA+\bar{a}\bar{A}+bB+\bar{b}\bar{B}+xX+\bar{x}\bar{X}+yY+\bar{y}\bar{Y}.$$

Ceci termine la démonstration du théorème (1.3), hormis le calcul du module ($2^{n+1+\gamma}$) en fonction des coefficients, ce qui va être effectué au § 5.

Le résultat suivant complète (1.3) dans la mesure où il montre qu'il n'existe pas de "8-ième congruence" selon le module 2^{n+1}:

(4.6) PROPOSITION. *Il n'existe pas de congruence c_8 (au sens de (4.3)), de la forme $C \equiv u \bmod 2^{n+1}$, telle que $(c_i)_{1 \leqslant i \leqslant 8}$ constitue une $\mathbf{Z}_2$-base de $\mathcal{C}$, et telle que $u = u(l_1, \ldots, l_n)$ soit continue 2-adiquement (comme application de $\mathbf{Z}_2^n$ dans $\mathbf{Q}_2$).*

D'après (4.4) et (4.5), l'existence de c_8 équivaut à l'existence d'une congruence de la forme

$$\bar{A} \equiv u+\alpha\eta+\beta\xi\pi/2 \mod 2^{n+1}, \quad \alpha, \beta \in \mathbf{Z}_2,$$
$$\equiv v \mod 2^{n+1},$$

où $v = v(l_1, \ldots, l_n)$ est aussi continue 2-adiquement, puisque η et π ont cette propriété.

Prenons alors $n = 1$ et $m = 3l$, $l \equiv -1\,(8)$; on obtient

$$-2h(-3)\left(1-\left(\frac{-3}{l}\right)\right) \equiv v(l)\,(8)$$

soit

$$-(2/3)\left(1-\left(\frac{l}{3}\right)\right) \equiv v(l)\,(8);$$

or si $l \equiv 7\,(24)$, $v(l) \equiv 0\,(8)$ et si $l \equiv -1\,(24)$, $v(l) \equiv 4\,(8)$, ce qui prouve que v n'est pas continue (en particulier elle ne peut être de la forme $\alpha\eta+\beta\xi\pi/2$), d'où le résultat.

Abordons maintenant le calcul de 2^{γ} en fonction des coefficients de C.

5. Module de la congruence générale. On revient à la congruence [G2, (3.15)] entre distributions de Stickelberger; elle est caractérisée par la décomposition de G_S en somme directe et par E (une fois σ fixé ainsi que les h_t, $t \in E$ (cf. (2.1), (vi))), et en particulier elle ne dépend ici que du choix de $\mathbf{Q}_0$ et de E (cf. [G2, § 2]).

On a donc 6 congruences distinctes dans la $\mathbf{Z}_2$-algèbre Λ des mesures sur G_S, dont les modules respectifs sont les suivants:

(5.1)

(i) $(E = U \cup \{0\},\ \mathbf{Q}_0 = \mathbf{Q}(\sqrt{-1}))$: $\nu_1(1-h_0)\Delta$, avec $h_0 = \sigma$,

(ii) $(E = U \cup \{0\},\ \mathbf{Q}_0 = \mathbf{Q}(\sqrt{-2}))$: $\nu_2(1-h_0)\Delta$, avec $h_0 = \sigma h_{-1}$,

(iii) $(E = U \cup \{-1\},\ \mathbf{Q}_0 = \mathbf{Q}(\sqrt{-1}))$: $\nu_3(1-h_{-1})\Delta$,

(iv) $(E = U \cup \{-1\},\ \mathbf{Q}_0 = \mathbf{Q}(\sqrt{-2}))$: $\nu_4(1-h_{-1})\Delta$,

(v) $(E = U \cup \{-1, 0\},\ \mathbf{Q}_0 = \mathbf{Q}(\sqrt{-1}))$: $\nu_5(1-h_{-1})(1-h_0)\Delta$, avec $h_0 = \sigma$,

(vi) $(E = U \cup \{-1, 0\},\ \mathbf{Q}_0 = \mathbf{Q}(\sqrt{-2}))$: $\nu_6(1-h_{-1})(1-h_0)\Delta$, avec $h_0 = \sigma h_{-1}$,

où $\Delta = \prod_{l \in U}(1-h_l)$ et $\nu_i \in \Lambda$, $1 \leqslant i \leqslant 6$.

Tout $\nu \in \Lambda$ peut s'écrire (cf. [G1, § 3]):

$$\nu = \sum_{i \geqslant 0} \alpha_i \delta^i, \quad \delta = 1-5\sigma^{-1}, \quad \alpha_i \in \Lambda_A,$$

où Λ_A est l'algèbre des $\mathbf{Z}_2$-mesures sur $A = \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q}_\infty)$. Pour toutes les congruences (2.2) et (2.3), le module s'obtient par intégration de $\omega\chi\langle\ \rangle^s$ par rapport aux mesures (i) à (vi) précédentes (5.1) (cf. [G2, § 4]).

(5.2) LEMME. *On a $\langle \omega\chi\langle\ \rangle^s, \delta \rangle = 1-\chi_0\chi_\infty(\sigma)5^{1-s}$; on a $\langle \omega\chi\langle\ \rangle^s, 1-h_l \rangle = 2$ pour tout $l \in U$; on a $\langle \omega\chi\langle\ \rangle^s, 1-h_{-1} \rangle = 2$ (resp. 0) si $\chi_0 = 1$ (resp. $\chi_0 = \omega_0$); enfin on a $\langle \omega\chi\langle\ \rangle^s, 1-h_0 \rangle = 1-\omega_0\chi_\infty(5)5^s$.*

Les vérifications sont élémentaires.

Posons $T(s) = 1-\chi_0\chi_\infty(5)5^{1-s}$; les 6 modules (5.1) conduisent aux intégrales respectives suivantes:

(5.3)

(i) $2^n(1-\chi_\infty(5)\,5^s)\sum_{i\geqslant 0} u_i\,T(s)^i$;

(ii) $2^n(1+\chi_\infty(5)\,5^s)\sum_{i\geqslant 0} \bar{u}_i\,T(s)^i$;

(iii) $2^{n+1}\sum_{i\geqslant 0} v_i\,T(s)^i$;

(iv) $2^{n+1}\sum_{i\geqslant 0} \bar{v}_i\,T(s)^i$;

(v) $2^{n+1}(1-\chi_\infty(5)\,5^s)\sum_{i\geqslant 0} w_i\,T(s)^i$;

(vi) $2^{n+1}(1+\chi_\infty(5)\,5^s)\sum_{i\geqslant 0} \bar{w}_i\,T(s)^i$. .

Tous les coefficients u_i, $\bar{u}_i$, v_i, $\bar{v}_i$, w_i, $\bar{w}_i$ sont dans $\mathbf{Z}_2$. Seuls les u_i et les $\bar{u}_i$ sont fonction de χ_0 (car d'après (2.3), on a $\chi_0 = 1$ pour les cas (iii) à (vi)); on les notera u_i et $\bar{u}_i$ lorsque $\chi_0 = 1$, puis u_i' et $\bar{u}_i'$ lorsque $\chi_0 = \omega_0$; ainsi précisées, ces 8 suites de coefficients sont indépendantes de s et de χ_∞. Enfin le calcul de $T(s)$ ne dépend de χ_0 que dans les cas (i) et (ii).

On spécialise alors chacun des 8 cas (5.3) pour $\chi_\infty \in \{1, \psi\}$, $\chi_0 \in \{1, \omega_0\}$ et $s \in \{0, 1\}$; en résumé on obtient le tableau suivant, dans lequel on indique successivement la congruence r_i concernée, $1 \leqslant i \leqslant 22$, le module $2^{n+1}m$ correspondant (au facteur 2^{n+1} près, et réduit modulo 16):

(5.4)

r_1	$u_0'+6u_1'+4u_2'+8u_3'$	r_{12}'	$u_0+6u_1+4u_2+8u_3$
r_2	$-2u_0'$	r_{13}	$-2u_0$
r_3	$3u_0'+6u_1'-4u_2'+8u_3'$	r_{14}	$3\bar{u}_0$
r_4	v_0-4v_1	r_{15}	$3u_0+6u_1-4u_2+8u_3$
r_5	$\bar{v}_0-4\bar{v}_1$	r_{16}	$-2\bar{u}_0-4\bar{u}_1-8\bar{u}_2$
r_6	$v_0+6v_1+4v_2+8v_3$	r_{17}	$2\bar{w}_0-8\bar{w}_1$
r_7	$\bar{v}_0+6\bar{v}_1+4\bar{v}_2+8\bar{v}_3$	r_{18}	$2w_0-4w_1+8w_2$
r_8	v_0	r_{19}	$-4w_0$
r_9	$\bar{v}_0$	r_{20}	$6\bar{w}_0$
r_{10}	$v_0+2v_1+4v_2+8v_3$	r_{21}	$6w_0-4w_1+8w_2$
r_{11}	$\bar{v}_0+2\bar{v}_1+4\bar{v}_2+8\bar{v}_3$	r_{22}	$-4\bar{w}_0+8\bar{w}_1$
r_{12}	$\bar{u}_0-4\bar{u}_1$		

Remarque. Pour $\chi_0 = \omega_0 = \omega\psi$, les congruences r_1, r_2, r_3 introduisent aussi les coefficients $\bar{u}_i'$; on peut éliminer l'un des systèmes et conserver par exemple celui des $\bar{u}_i$.

On dispose alors de 16 relations, obtenues via l'expression des r_i sur la base des c_i, $1 \leqslant i \leqslant 7$ (cf. (4.4)), qui induisent des relations entre les différents coefficients intervenant dans le tableau (5.4) ci-dessus. Les calculs, élémentaires mais fastidieux, conduisent à la paramétrisation suivante des modules (écrits sous la forme $2^{n+1}m_i$) des congruences c_i, $1 \leqslant i \leqslant 7$:

(5.5)
$$\begin{aligned}
m_1 &\equiv 8v_2+4\bar{v}_1+8\bar{v}_2+4\bar{u}_0 \ (16),\\
m_2 &\equiv 4\bar{v}_1 \ (16),\\
m_3 &\equiv -6\bar{v}_1+4\bar{v}_2+8\bar{v}_3+2\bar{u}_0+8u_1' \ (16),\\
m_4 &\equiv 6\bar{v}_1+4\bar{v}_2+8\bar{v}_3 \ (16),\\
m_5 &\equiv -4\bar{v}_1+6\bar{u}_0+8v_2-4u_1' \ (16),\\
m_6 &\equiv \bar{v}_0-2\bar{v}_1-4\bar{v}_2+8\bar{v}_3+\bar{u}_0+4u_1' \ (16),\\
m_7 &\equiv \bar{v}_0-4\bar{v}_1 \ (16).
\end{aligned}$$

On en déduit immédiatement que le module de la congruence générale de (1.3) est donné par $2^{n+1}M$, où

$$\begin{aligned}
M \equiv\ & \bar{v}_0(a+b+x+y)+\bar{u}_0(6a+7\bar{a}+7b+6\bar{b}+4x+\bar{x}+y+4\bar{y})\\
&+\bar{v}_1(-4a-6\bar{a}+4b+8\bar{b}+4x-2\bar{x}-4y+4\bar{y})\\
&+\bar{v}_2(-4\bar{a}+8b+8x-4\bar{x}+8y+8\bar{y})+u_1'(-4a-4\bar{b}+4\bar{x}+4y)\\
&+\bar{v}_3(8\bar{a}+8\bar{x})+v_2(8\bar{x}+8y) \mod 16;
\end{aligned}$$

on exprime alors que M est au moins le p.g.c.d. (dans $\mathbf{Z}_2$) des 7 coefficients ci-dessus et 16, et après transformations élémentaires, on obtient que 2^γ est le p.g.c.d. de l'ensemble formé par 16 et les 6 sommes suivantes:

$$\bar{a}+\bar{b}+\bar{x}+\bar{y}, \quad b+\bar{b}+2x+2\bar{x}-y-\bar{y}, \quad 2\bar{b}+2\bar{y}-4x+4y,$$
$$4(x+\bar{x}+y+\bar{y}), \quad 8(x+y), \quad 8(x+\bar{x}).$$

Ce qui achève la démonstration de (1.3), puis (1.4) facilement.

Bibliografie

[D] P.-J. Desnoux, *Congruences dyadiques entre nombres de classes de corps quadratiques*, thèse, Université Paris 7, 1987.

[G1] G. Gras, *Pseudo-mesures p-adiques associées aux fonctions L de Q*, Manuscripta Math. 57 (1987), 373–415.

[G2] — *Relations congruentielles additives entre fonctions L_p de Q*, Publ. Math. Fac. Sci. Besançon 1984-85/1985-86 (Théorie des Nombres).

[H] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin 1952 (réédition 1985).

[HW] K. Hardy and K. S. Williams, *A congruence relating the class numbers of complex quadratic fields*, Acta Arith. 47 (1986), 263–276.

[Hi] M. Hikita, *On the congruences for the class numbers of the quadratic fields whose discriminants are divisible by 8*, J. Number Theory 23 (1986), 81–101.

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

[Ke] M. A. Kenku, *Atkin–Lehner involutions and class number residuality*, Acta Arith. 33 (1977), 1–9.
[KW1] P. Kaplan and K. S. Williams, *Congruences modulo 16 for the class numbers of $Q(\sqrt{\pm p})$ and $Q(\sqrt{\pm 2p})$ for p a prime congruent to 5 modulo 8*, ibid. 40 (1981/1982), 375–397.
[KW2] – – *On the class number of $Q(\sqrt{\pm 2p})$ modulo 16 for $p \equiv 1\,(8)$ a prime*, ibid. 40 (1981/1982), 289–296.
[KW3] – – *Congruences for the class numbers of the fields $Q(\sqrt{\pm pq})$ with p and q odd primes* (to appear).
[L] H. Lang, *Über die Klassenzahl quadratischer Zahlkörper, deren Diskriminanten nur ungerade Primteiler $p \equiv 1 \bmod 4$ besitzen*, Abh. Math. Sem. Univ. Hamburg 55 (1985), 147–150.
[LS] H. Lang, R. Schertz, *Kongruenzen zwischen Klassenzahlen quadratischer Zahlkörper*, J. Number Theory 8 (1976), 352–365.
[Le] H. W. Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern*, J. Reine Angew. Math. 209, (1962), 54–71.
[P] A. Pizer, *On the 2-part of the class number of imaginary quadratic number fields*, J. Number Theory 8 (1976), 184–192.
[S] J.-P. Serre, *Sur le résidu de la fonction zêta p-adique d'un corps de nombres*, C. R. Acad. Sci. Paris, série A, 287 (1978), 183–188.
[W1] K. S. Williams, *On the class number of $Q(\sqrt{-p})$ modulo 16, for $p \equiv 1$ modulo 8 a prime*, Acta Arith. 39 (1981), 381–398.
[W2] – *Congruences modulo 8 for the class numbers of $Q(\sqrt{\pm p})$, $p \equiv 3 \pmod 4$ a prime*, J. Number Theory 15 (1981), 182–198.

UNIVERSITÉ DE FRANCHE-COMTÉ
FACULTÉ DES SCIENCES
U. A. DE MATHÉMATIQUES 040741
F-25030 Besançon Cedex

Reçu le 2.7.1987
et dans la forme modifiée le 1.10.1987 (1734)

ACTA ARITHMETICA
LII (1989)

An effective order of Hecke–Landau zeta functions near the line $\sigma = 1$, II (some applications)

by

K. M. Bartz (Poznań)

1. The present paper is a sequel to [1] and the notation of that paper is used throughout. Let K be an algebraic number field of finite degree n and absolute value of the discriminant d. Denote by $\mathfrak{f}$ a conductor of a character χ of ideal classes in the "narrow" sense.

We shall show some applications of effective order of Hecke–Landau zeta functions $\zeta_K(\sigma+it, \chi)$ near the line $\sigma = 1$, exactly for $1-1/(n+1) \leqslant \sigma \leqslant 1$, which was given in the preceding note (see [1], th. 1). We first will prove the following

Theorem A (compare [1], th. 2 and [2]). *There exists a positive constant $c_1 > 1$, independent of K and χ such that in the region*

$$\sigma \geqslant 1 - \frac{1}{10^4 \max\left\{\log N\mathfrak{f},\ c_1 n^{3.5} \log^{2/3}(|t|+3)\left(\log\log(|t|+3)\right)^{1/3} \max\left(1, \frac{A_1}{\log\log t}\right)\right\}} \tag{1.1}$$

the function $\zeta_K(\sigma+it, \chi)$ has no zeros except for the hypothetical real simple zero of $\zeta_K(s, \chi_1)$, χ_1 real, where $A_1 = n^{1.5}\sqrt{d}\,D$ and $D = \left(\dfrac{5\log d}{2(n-1)}\right)^{n-1}$ denotes the constant from Siegel's theorem on fundamental system of units (see [5]).

Remark. Putting $\mathfrak{f} = R_K$ we obtain obviously a zero-free region for the Dedekind zeta function (in this case $N\mathfrak{f} = 1$).

Next, as an application of Theorem A we get an effective version of Chebotarev density theorem. Let L be a normal extension of K with Galois group $G = G(L/K)$. Let P denote a prime ideal of K and $\left|\dfrac{L/K}{P}\right|$ denote the conjugacy class of Frobenius automorphisms corresponding to prime ideals