THÉORIE DES NOMBRES

BESANÇON

Année 1983 - 1984

COMPATIBILITÉ AVEC LE SPIEGELUNGSSATZ DE PROBABILITÉS CONJECTURALES SUR LE p-RANG DU GROUPE DES CLASSES

Philippe DUTARTE

COMPATIBILITÉ AVEC LE SPIEGELUNGSSATZ DE PROBABILITÉS CONJECTURALES SUR LE p- RANG DU GROUPE DES CLASSES

par Philippe Dutarte (*)

Cette étude a été effectuée au sein de l'équipe de Théorie des Nombres de Besançon au titre du stage de D.E.A. 1983/84 .

INTRODUCTION .

A partir d'un principe heuristique général , H. Cohen et H.W. Lenstra Jr. ont proposé un certain nombre d'énoncés conjecturaux sur le comportement asymptotique des groupes de classes des corps de nombres, notamment à propos des p-rangs des groupes de classes des corps quadratiques ([1]) . Or le Spiegelungssatz de Leopoldt ([6] , voir aussi [7]) relie , par ailleurs , pour tout premier p impair , le p-rang du groupe des classes d'un corps quadratique au p-rang d'un certain sous-groupe du groupe des classes d'une extension cyclique de degré p-1 du corps des rationnels .

L'objectif de cette note est d'étudier la cohérence des énoncés probabilistes de Cohen et Lenstra concernant ces p-rangs , compte-tenu des contraintes précédentes . Nous limiterons notre étude à p = 3 , cas où les corps mis en jeu sont des corps quadratiques dont les groupes des classes se correspondent globalement par le Spiegelungssatz . Il s'agit d'un théorème antérieur au Spiegelungssatz , dû à A. Scholz ([8]) .

1.- A PROPOS DU THEOREME DE SCHOLZ .

Nous considérons une extension quadratique réelle de $\mathbb{Q}$, notée $k = \mathbb{Q}(\sqrt{m})$, et l'extension quadratique imaginaire , notée $k' = \mathbb{Q}(\sqrt{-3m})$, qui lui est associée par adjonction à $\mathbb{Q}$ des racines cubiques de l'unité , ceci en vue d'appliquer la théorie de Kummer . Soit K le composé de k et de k' et $G = \mathrm{Gal}(K/\mathbb{Q})$.

(*) 58 rue sous-bois , F-25400 TAILLECOURT .

Pour tout corps L , nous désignons par Z_L l'anneau des entiers de L , par H_L l'extension abélienne maximale non ramifiée d'exposant 3 de L et par Cl_L le 3-sous-groupe élémentaire maximal du groupe des classes de L . Nous notons $\dim_3 A$ le 3-rang d'un groupe abélien fini A , c'est-à-dire $\dim_{\mathbb{F}_3} \{a \in A \ ; a^3 = 1\}$.

Soit S l'ensemble des places de L au-dessus de 3 , nous notons $\mathcal{O}_L = \prod_{\mathfrak{p} \in S} \mathcal{O}_{\mathfrak{p}}$, où $\mathcal{O}_{\mathfrak{p}}$ est l'anneau des entiers du complété en $\mathfrak{p}$ de L. Nous notons de même $U_L = \prod_{\mathfrak{p} \in S} U_{\mathfrak{p}}$, où $U_{\mathfrak{p}} = 1 + \bar{\mathfrak{p}}$ est le groupe des unités locales principales en $\mathfrak{p}$ de L . Nous désignons par U_L^3 le groupe des cubes de U_L et par $U_L^{(\nu)}$, $\nu \geq 1$, le produit , pour $\mathfrak{p}$ parcourant S , des groupes $U_{\mathfrak{p}}^{(\nu)} = 1 + \bar{\mathfrak{p}}^{\nu}$.

Nous notons enfin s l'automorphisme de $Gal(K/\mathbb{Q})$ qui fixe k , s' celui qui fixe k' et t celui qui fixe $\mathbb{Q}(\sqrt{-3})$.

Le théorème de Scholz nait de la confrontation de la théorie de Kummer et de la théorie du corps de classes .

(i) Selon la théorie du corps de classes, $Gal(H_{k'}/k')$ est isomorphe à $Cl_{k'}$. Par composition de $H_{k'}$ et de K , on a :

$$Gal(KH_{k'}/K) \simeq Cl_{k'} \ .$$

De façon symétrique ,

$$Gal(KH_k/K) \simeq Cl_k \ .$$

(ii) D'après la théorie de Kummer , comme K contient les racines cubiques de l'unité , la 3-extension composée KH_k (resp. $KH_{k'}$) de K est de la forme :

$$KH_k = K(\sqrt[3]{R'_o}) \qquad (\text{resp. } KH_{k'} = K(\sqrt[3]{R_o})) \ ,$$

où les radicaux R'_o et R_o sont des sous-groupes de $K^{\times}$ contenant $K^{\times 3}$. De plus , comme l'extension KH_k/k est abélienne et décomposée sur k , on peut choisir R'_o inclus dans k' (resp. R_o inclus dans k) .

(iii) Par l'isomorphisme , qui à $\alpha k^{\times 3}$ de $R_o/k^{\times 3}$ associe l'élément du dual $Gal(KH_{k'}/K)^*$ défini par :

$$\tau \in Gal(KH_{k'}/K) \mapsto (\sqrt[3]{\alpha})^{\tau - 1} \ ,$$

nous avons $R_o/k^{\times 3} \simeq \mathrm{Gal}(KH_{k'}/K)^*$. De façon analogue ,

$$R'_o/k'^{\times 3} \simeq \mathrm{Gal}(KH_k/K)^* .$$

En confrontant ceci aux résultats du point (i) et en notant respectivement r et r' les 3-rangs de Cl_k et de $Cl_{k'}$, on obtient :

$$r' = \dim_3(R_o/k^{\times 3}) \quad \text{et} \quad r = \dim_3(R'_o/k'^{\times 3}) .$$

(iv) Posons $R = \langle \alpha_1, \dots, \alpha_r, \varepsilon \rangle k^{\times 3}$ où les α_i sont éléments de $k^\times$, choisis indépendants modulo les cubes, tels que $\alpha_i Z_k = a_i^3$ où $cl(a_1), \dots, cl(a_r)$ constituent une $\mathbb{F}_3$-base de Cl_k et où ε est l'unité de k . Notons de même $R' = \langle \alpha'_1, \dots, \alpha'_{r'} \rangle k'^{\times 3}$ dans le cas imaginaire.

Introduisons l'application φ qui envoie diagonalement $R/k^{\times 3}$ dans $U_K/U_K^3 U_K^{(3)}$. D'après la théorie de la ramification dans les extensions de Kummer ([4]) , le fait que l'extension $KH_{k'}$ soit maximale non ramifiée sur K se traduit par le fait que $R_o/k^{\times 3}$ est le noyau de φ .
De façon analogue , $R'_o/k'^{\times 3}$ est le noyau de l'application φ' définie de même de $R'/k'^{\times 3}$ dans $U_K/U_K^3 U_K^{(3)}$.

Nous pouvons alors poser :

$$\dim_3(R_o/k^{\times 3}) = r + 1 - \delta$$

$$\text{et} \quad \dim_3(R'_o/k'^{\times 3}) = r' - \delta' ,$$

où δ et δ' mesurent les défauts de 3-primarité . Nous considérons donc les suites exactes suivantes (avec les 3-rangs correspondants) :

$$1 \longrightarrow \underset{r'=r+1-\delta}{R_o/k^{\times 3}} \longrightarrow \underset{r+1}{R/k^{\times 3}} \xrightarrow{\varphi} U_K/U_K^3 U_K^{(3)} ,$$

$$1 \longrightarrow \underset{r=r'-\delta'}{R'_o/k'^{\times 3}} \longrightarrow \underset{r'}{R'/k'^{\times 3}} \xrightarrow{\varphi'} U_K/U_K^3 U_K^{(3)} .$$

Réunissant les résultats des points (iii) et (iv) , il vient que $r' = r + 1 - \delta$ et $r = r' - \delta'$ d'où $r' - r = \delta' = 1 - \delta$ et ainsi δ et δ' ne prennent que les valeurs 1 ou 0 . On peut alors énoncer le théorème de Scholz ([8]) sous la forme suivante ([3]) :

Les 3-rangs r et r' des groupes des classes des corps quadratiques $k = \mathbb{Q}(\sqrt{m})$, $m > 0$, et $k' = \mathbb{Q}(\sqrt{-3m})$ sont tels que :

- $r' = r + 1$, si l'image par φ de tout élément de $R/k^{\times 3}$ est triviale,
- $r' = r$, sinon .

Pour l'exploitation probabiliste de ce résultat, il convient de préciser l'application φ et en particulier d'étudier la structure de $U_K / U_K^3 \, U_K^{(3)}$.

2.- STRUCTURE DES GROUPES D'UNITES LOCALES EN 3 .

Nous étudions la structure du groupe $U_K / U_K^3 \, U_K^{(3)}$ où l'on rappelle que U_K est le produit pour les places $\mathfrak{p}$ au-dessus de 3 des groupes d'unités locales en 3 et où $U_K^{(3)}$ est le produit des groupes d'unités locales congrues à 1 modulo $\bar{\mathfrak{p}}^3$.

(i) <u>Inclusion de U_K^3 dans $U_K^{(3)}$</u> .

Soit π_K une S-uniformisante et $x \in \mathcal{O}_K$, le développement de $(1 + \pi_K x)^3$, en tenant compte du fait que l'indice de ramification de 3 dans $K/\mathbb{Q}$ est 2 dans tous les cas , montre le résultat annoncé .

(ii) <u>Filtration de $U_K^{(1)} / U_K^{(3)}$</u> .

En notant e l'indice de ramification de 3 dans $K/\mathbb{Q}$, f le degré résiduel et g le cardinal de S , on a :

$$U_K^{(\nu)} / U_K^{(\nu+1)} \simeq (\mathbb{F}_{3^f})^g \quad \text{pour} \quad \nu \geq 1 \ .$$

D'où , puisque $4 = efg$ et $e = 2$, $|U_K^{(\nu)} / U_K^{(\nu+1)}| = 9$.
On en déduit que $|U_K^{(1)} / U_K^{(3)}| = 81$.

(iii) <u>Décomposition en somme directe</u> .

Puisque 3 est premier avec l'ordre de $G = \mathrm{Gal}(K/\mathbb{Q})$ (situation semi-simple) , on peut décomposer $U_K^{(1)} / U_K^{(3)}$, considéré comme $\mathbb{Z}_3[G]$-module , en somme directe suivant les idempotents de $\mathbb{Z}_3[G]$.

Si l'on note $\mathcal{U}_K = U_K^{(1)} / U_K^{(3)}$ et $\mathcal{U}_{K/F} = N_{K/F} \, \mathcal{U}_K$ pour toute sous-extension K/F de K , on obtient :

$$\mathcal{U}_K = \mathcal{U}_{K/k}^{1-t} \oplus \mathcal{U}_{K/k'}^{1-t} \oplus \mathcal{U}_{K/\mathbb{Q}(j)}^{1-s} \oplus \mathcal{U}_{K/\mathbb{Q}} \ .$$

On peut montrer que chacun des termes de cette somme est , dans tous les cas de ramification de 3 dans $K/\mathbb{Q}$, d'ordre 3 .

(iv) <u>Où l'on montre que φ applique $R/k^{\times 3}$ dans un groupe d'ordre</u> 3 .

Quitte à les remplacer par une puissance étrangère à 3 , on peut supposer les éléments α_i et ϵ , qui engendrent $R/k^{\times 3}$, congrus à 1 modulo S et ainsi prendre $U_K^{(1)} / U_K^{(3)}$ comme arrivée de φ .

Puisque R est inclus dans k , $\varphi(R/k^{\times 3})$ est inclus dans $\mathcal{U}_{K/k}$. Considérons alors la suite exacte :

$$1 \longrightarrow \mathcal{U}_{K/k}^{1-t} \longrightarrow \mathcal{U}_{K/k} \xrightarrow{1+t} \mathcal{U}_{K/k}^{1+t} \longrightarrow 1 \ .$$

Soit $\overline{\alpha}$ un élément de $R/k^{\times 3}$. D'après la théorie de Kummer , $K(\sqrt[3]{\overline{\alpha}})/\mathbb{Q}(j)$ est galoisienne si et seulement si $\overline{\alpha}^t = \overline{\alpha}^\mu$, avec $(\mu, 3) = 1$.

Mais , par ailleurs , $\mathbb{Q}(j)$ étant principal , pour toute 3-classe h de K , on a $h^{1+t} = 1$, donc $h^t = h^{-1}$; ce qui fait que $\langle t \rangle$ opère sur Cl_K, et donc (par l'isomorphisme d'Artin) sur $Gal(H_K/K)$, de telle sorte que $K(\sqrt[3]{\overline{\alpha}})/\mathbb{Q}(j)$ est une extension galoisienne de type diédral . Ainsi , $\mu = -1$ et $\overline{\alpha}^t = \alpha^{-1}$.

On en déduit que $\varphi(R/k^{\times 3})$ est inclus dans $\mathcal{U}_{K/k}^{1-t}$ que l'on sait être d'ordre 3 et que l'on identifiera à $\mathbb{Z}/3\mathbb{Z}$.

L'analyse du théorème de Scholz ainsi faite , considérons maintenant les résultats de Cohen et Lenstra à sa lumière .

3.- COMPATIBILITE DES CONJECTURES DE H. COHEN ET H.W. LENSTRA AVEC LE THEOREME DE SCHOLZ .

Nous considérons l'ensemble Ω (resp. Ω') des 3-sous-groupes élémentaires des groupes de classes des extensions quadratiques réelles (resp. imaginaires) de $\mathbb{Q}$. Les ensembles Ω et Ω' sont liés par la bijection ψ définie par :

$$\psi \begin{cases} \Omega \to \Omega' \\ Cl_k \mapsto Cl_{k'} \end{cases}$$

où k' est tel que si $k = \mathbb{Q}(\sqrt{m})$, $m > 0$, alors $k' = \mathbb{Q}(\sqrt{-3m})$.
Nous évaluons les 3-rangs par les applications :

$$r \begin{cases} \Omega \to \mathbb{N} \\ Cl_k \mapsto 3\text{-rg}(Cl_k) \end{cases} , \quad r' \begin{cases} \Omega' \to \mathbb{N} \\ Cl_{k'} \mapsto 3\text{-rg}(Cl_{k'}) \end{cases} .$$

Enfin , le théorème de Scholz permet de définir l'application :

$$\delta \begin{cases} \Omega \to \{0, 1\} \\ Cl_k \mapsto \begin{cases} 0 & \text{si } 3\text{-rg}(\psi(Cl_k)) = 3\text{-rg}(Cl_k) + 1 \\ 1 & \text{si } 3\text{-rg}(\psi(Cl_k)) = 3\text{-rg}(Cl_k) \end{cases} \end{cases}$$

3.1. Enoncés de H. Cohen et H.W. Lenstra.

Rappelons ce qu'entendent par " probabilité " Cohen et Lenstra dans leur article ([1]).

Soit P l'application de l'ensemble des parties de Ω dans $[0, 1]$ définie par :

$$\text{Pour } A \in \mathcal{P}(\Omega) \text{ , } P(A) = \lim_{x \to \infty} \frac{\Sigma\, 1_A(Cl_k)}{\Sigma\, 1} \text{ ,}$$

où chaque sommation est étendue aux corps quadratiques réels k de discriminants inférieurs à x et où 1_A désigne la fonction caractéristique de l'ensemble A. L'expression P(A) n'existe que si la limite est finie.

L'application P possède les propriétés suivantes :

(i) $P(\phi) = 0$.

(ii) Pour $A_1, \dots, A_n$, n ensembles deux à deux disjoints de $\mathcal{P}(\Omega)$ tels que $P(A_i)$ existe, on a :

$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i) \text{ .}$$

Cette propriété d'additivité ne s'étendant pas nécessairement aux unions infinies d'ensembles deux à deux disjoints, il ne s'agit pas d'une mesure sur $\mathcal{P}(\Omega)$. Pourtant, comme de plus, $P(\Omega) = 1$, nous parlons tout de même de probabilité sur $(\Omega, \mathcal{P}(\Omega))$. Nous considérons de même comme variables aléatoires les applications r et δ définies précédemment.

Au sens de cette probabilité, Cohen et Lenstra obtiennent le résultat suivant :

$$\boxed{P(r = a) = 3^{-a(a+1)}\, \eta_\infty\, \eta_a^{-2}\, (1 - 3^{-(a+1)})^{-1} \qquad (1)}$$

avec $\eta_a = \prod_{k=1}^{a} (1 - 3^{-k})$.

De même, on définit une probabilité P' sur Ω' par :

$$\text{Pour } A' \subset \Omega' \text{ , } P'(A') = \lim_{x \to \infty} \frac{\Sigma\, 1_{A'}(Cl_{k'})}{\Sigma\, 1} \text{ ,}$$

où chaque sommation est étendue aux corps quadratiques imaginaires k' dont la valeur absolue du discriminant est inférieure à x.

Cohen et Lenstra obtiennent alors :

$$\boxed{P'(r' = a) = 3^{-a^2}\ \eta_\infty \eta_a^{-2} \qquad (2)}$$

3.2. Compatibilité avec le théorème de Scholz .

La bijection ψ permet de traduire des informations concernant Ω en des informations concernant Ω' (et réciproquement) :

• En effet , r , sur Ω , et r' , sur Ω' , sont liées par la relation de Scholz :

Pour $Cl_k \in \Omega$, $\quad r' \circ \psi(Cl_k) = r(Cl_k) + 1 - \delta(Cl_k)$,

i.e. $$\boxed{r' \circ \psi = r - \delta + 1 \qquad (*)}$$

• Quant aux probabilités P , sur Ω , et P' , sur Ω' , elles sont liées par ψ selon la formule :

$$\boxed{P \circ \psi^{-1} = P' \qquad (**)}$$

En effet , pour tout sous-ensemble A' de Ω' , on a :

$$P \circ \psi^{-1}(A') = P[\psi^{-1}(A')] = \lim_{x \to \infty} \frac{\sum 1_{\psi^{-1}(A')}(Cl_k)}{\sum 1} = \lim_{x \to \infty} \frac{\sum 1_{A'}(\psi(Cl_k))}{\sum 1}$$

$$= \lim_{x \to \infty} \frac{\sum 1_{A'}(Cl_{k'})}{\sum 1} = P'(A') .$$

• A partir de l'expression de $P(r = a)$, donnée par (1) , cherchons maintenant , à l'aide des formules (*) et (**) , à déterminer $P'(r' = a)$. Nous comparerons ensuite avec l'expression (2) donnée indépendamment par Cohen et Lenstra .

La valeur de r' étant complètement déterminée à partir de celles de r et de δ , cherchons au préalable la probabilité pour que δ prenne la valeur 0 sachant que r prend la valeur a . Il s'agit de la probabilité pour que $|R_o/k^{\times 3}|$ vaille 3^{a+1} sachant que $r = a$.

Puisque $r = a$, on a $R = \langle \varepsilon , \alpha_1 , \ldots , \alpha_a \rangle k^{\times 3}$. Donc $|R_o/k^{\times 3}|$ vaut 3^{a+1} si et seulement si ε et les α_i , pour $i = 1 , \ldots , a$, ont pour image par φ dans $\mathcal{U}_k^{1-t} \simeq \mathbb{Z}/3\mathbb{Z}$ l'élément neutre $\overline{0}$. Si l'on considère que les images des générateurs de $R_o/k^{\times 3}$ sont déterminées de façon indépendante les unes des autres et selon une loi d'équiprobabilité , on peut alors poser :

$$\boxed{P(\delta = 0 \mid r = a) = 3^{-(a+1)} \qquad (3)}$$

En appliquant (**), on peut écrire :

$$P'(r' = a) = P \circ \psi^{-1}(r' = a) = P[\psi^{-1} \circ r'^{-1}(\{a\})]$$
$$= P[(r' \circ \psi)^{-1}(\{a\})].$$

En appliquant (*) , on a alors :

$$P'(r' = a) = P(r - \delta + 1 = a) = P(r - \delta = a - 1).$$

Or on a l'égalité $r - \delta = a - 1$ si $\delta = 0$ et $r = a - 1$,ou bien si $\delta = 1$ et $r = a$, donc :

$$P'(r' = a) = P(\delta = 0, r = a - 1) + P(\delta = 1, r = a)$$
$$= P(r = a - 1) P(\delta = 0 \mid r = a - 1) + P(r = a) P(\delta = 1 \mid r = a).$$

En utilisant (1) et (3) , on obtient donc :

$$P(r' = a) = 3^{-a(a-1)} \eta_\infty \eta_{a-1}^{-2} (1 - 3^{-a})^{-1} 3^{-a}$$
$$+ 3^{-a(a+1)} \eta_\infty \eta_a^{-2} (1 - 3^{-(a+1)})^{-1} (1 - 3^{-(a+1)})$$
$$P(r' = a) = \eta_\infty \eta_a^{-2} [3^{-a(a-1)} (1 - 3^{-a}) 3^{-a} + 3^{-a(a+1)}]$$
$$= \eta_\infty \eta_a^{-2} 3^{-a^2}.$$

Ce qu'obtiennent indépendamment de (1) Cohen et Lenstra .

On pourrait de façon analogue retrouver l'expression $P(r = a)$ donnée par (1) à partir de celle de $P'(r' = a)$ donnée par (2) . Les lois (1) et (2) sont donc compatibles avec l'énoncé du théorème de Scholz . Toutefois, en supposant l'indépendance et l'équiprobabilité , nous avons implicitement supposé que la probabilité pour que $\varphi(\varepsilon)$ vaille $\overline{0}$ (i.e. ε 3-primaire) est , comme pour les α_i , de 1/3 . Cette question présente l'intérêt d'être accessible au calcul donc à une vérification expérimentale , mais nous la traitons du point de vue de la compatibilité avec les lois de Cohen et Lenstra .

4.- REPARTITION DES UNITES FONDAMENTALES 3- PRIMAIRES .

4.1. Compatibilité théorique .

Rappelons que nous considérons la suite exacte (§ 2 , (iv)) :

$$1 \longrightarrow R_0/k^{\times 3} \longrightarrow R/k^{\times 3} \xrightarrow{\varphi} \mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$$

avec $\dim_3(R_0/k^{\times 3}) = r + 1 - \delta = r'$ et $\dim_3(R/k^{\times 3}) = r + 1$.

Constatons que :

- Si $\delta = 0$ alors $\varphi = 0$ et $\varphi(\varepsilon) = \overline{0}$.
- Si $\delta = 1$ alors $r = r'$. Si $r = a$, dans ce cas , $\dim_3(R/k^{\times 3}) = a + 1$ et $\dim_3 \ker \varphi = a$. Dénombrer les applications φ possibles vérifiant ces conditions revient alors à dénombrer les noyaux possibles c'est-à-dire les sous-groupes isomorphes à C_3^a dans un groupe du type C_3^{a+1} , où C_3 est le groupe cyclique à 3 éléments . Il y en a $\frac{3^{a+1}-1}{2}$.

Pour dénombrer , parmi ces applications φ , celles qui envoyent ε sur $\overline{0}$, observons qu'un sous-groupe donné d'ordre 3 de C_3^{a+1} est contenu dans $\frac{3^a-1}{2}$ sous-groupes de type C_3^a de C_3^{a+1} . Il y a donc $\frac{3^a-1}{2}$ applications φ favorables à $\varphi(\varepsilon) = \overline{0}$.

Introduisons sur Ω , la variable aléatoire Φ définie par :

$$\Phi \begin{cases} \Omega \to \mathbb{Z}/3\mathbb{Z} \\ \\ Cl_k \mapsto \Phi(Cl_k) = \varphi(\varepsilon) \end{cases} ,$$

où ε est l'unité fondamentale de k . La probabilité selon laquelle l'unité fondamentale d'un corps quadratique réel est 3-primaire est alors $P(\Phi = 0)$. Posons :

$$\boxed{\begin{aligned} & P(\Phi = 0 \mid \delta = 0) = 1 \\ & P(\Phi = 0 \mid \delta = 1 , r = a) = \frac{3^a - 1}{3^{a+1} - 1} \end{aligned} \qquad (4)}$$

Ces résultats sont obtenus à partir des observations précédentes en considérant le rapport du nombre de cas favorables par le nombre de cas possibles , c'est-à-dire en présupposant l'équiprobabilité d'occurence des applications φ , c'est-à-dire l'équiprobabilité des images par φ des éléments de base (en particulier que $P(\Phi = 0) = \frac{1}{3}$) . C'est en ce sens que ce qui suit est une étude de compatibilité .

Nous avons par partition ,

$$P(\Phi = 0 , r = a) = P(\Phi = 0 , r = a , \delta = 0) + P(\Phi = 0 , r = a , \delta = 1)$$

$$\begin{aligned} P(\Phi = 0 , r = a) = {} & P(r = a) P(\delta = 0 \mid r = a) P(\Phi = 0 \mid \delta = 0 , r = a) \\ & + P(r = a) P(\delta = 1 \mid r = a) P(\Phi = 0 \mid \delta = 1 , r = a) \end{aligned}$$

Soit , en utilisant (1) , (3) et (4) :

$$P(\Phi = 0\,,\ r = a) = 3^{-a(a+1)}\,\eta_\infty \eta_a^{-2}\,(1 - 3^{-(a+1)})^{-1}$$
$$\times \left[3^{-(a+1)} + (1 - 3^{-(a+1)})\,\frac{3^a - 1}{3^{a+1} - 1} \right]$$

$$P(\Phi = 0\,,\ r = a) = \eta_\infty \eta_a^{-2}(3^{a+1} - 1)^{-1} \left[3^{-a(a+1)}(1 - 3^{-(a+1)})^{-1}\,3^{-(a+1)} (3^{a+1} - 1) + 3^{-a(a+1)}(3^a - 1) \right]$$
$$= \eta_\infty \eta_a^{-2}\,3^{-a^2}\,(3^{a+1} - 1)^{-1}\ .$$

Donc $P\left(\bigcup_{a=0}^{k} (\Phi = 0\,,\ r = a) \right) = \sum_{a=0}^{k} \eta_\infty \eta_a^{-2}\,3^{-a^2}\,(3^{a+1} - 1)^{-1}$.

LEMME (voir [1]) .

> En posant $(q)_k = \prod_{n=1}^{k} (1 - q^n)$, on a :
>
> $$\sum_{s=\alpha}^{\infty} \frac{q^{(s+u)(s-\alpha)}}{(q)_{s-\alpha}(q)_{s+u}} = \frac{1}{(q)_\infty}\ .$$

Donc , en posant $p = \frac{1}{q}$,

$$\eta_\infty \sum_{a=0}^{\infty} \eta_a^{-2}\,p^{-a^2}(p^{a+1} - 1)^{-1} = (q)_\infty \sum_{a=0}^{\infty} (q)_a^{-2}\,\frac{q^{a+1}\,q^{a^2}}{1 - q^{a+1}}$$

$$= (q)_\infty\, q \sum_{a=0}^{\infty} \frac{q^{a(a+1)}}{(q)_a\,(q)_{a+1}} = (q)_\infty\, q\,\frac{1}{(q)_\infty} = q$$

(Ceci en appliquant le lemme pour $\alpha = 0$ et $u = 1$) .

Ainsi , $\lim_{k \to \infty} P\left(\bigcup_{a=0}^{k} (\Phi = 0\,,\ r = a) \right) = \frac{1}{3}$, et l'expression de $P(r = a)$ donnée par Cohen et Lenstra est cohérente avec le comportement estimé des unités fondamentales quant à leur 3-primarité .

4.2. Etude statistique .

Nous avons mis en oeuvre un algorithme permettant , par développement en fraction continue de $\sqrt{m}$, de calculer rapidement modulo 9 l'unité fondamentale du corps quadratique réel $\mathbb{Q}(\sqrt{m})$ et de tester sa 3-

primarité . Nous avons ensuite soumis l'hypothèse " un tiers des unités fondamentales sont 3-primaires " au test statistique du χ^2 . Il s'agit de juger si l'hypothèse concernant la loi de probabilité de la variable aléatoire Φ est compatible avec la réalisation d'un échantillon au hasard de cette variable ([2]) .

Parmi plusieurs tests effectués sur l'ordinateur du centre de calcul de Grenoble , nous avons notamment pour ce faire , fait appel à un générateur machine de nombres pseudo-aléatoires fonctionnant selon la méthode des congruences linéaires ([5]) (ce choix seul nous permettant un échantillon de taille importante) .

La génération au hasard , à deux reprises , de 1000 discriminants compris entre 0 et 10^8 nous permet de donner une réponse positive à l'hypothèse soumise au test , avec un risque d'erreur de 5 % .

RÉFÉRENCES .

[1] H. COHEN and H.W. LENSTRA , Jr.- Heuristics on class groups of number fields , Number Theory , Proc. of the Journées arithmétiques (Noordwijkerhout , 1983) , Lect. Notes in Math. 1068 , Springer-Verlag (1984) , pp. 33-62 .

[2] C. FOURGEAUD et A. FUCHS .- Statistique , Dunod (1967) .

[3] G. GRAS .- Extensions abéliennes non ramifiées de degré premier d'un corps quadratique . Bull. Soc. Math. France , 100 (1972) , pp. 177-193 .

[4] E. HECKE .- Lectures on the Theory of Algebraic Numbers (Translation of : Vorlesung über die Theorie der algebraischen Zahlen , Akad. Verlag. Leipzig , 1923) , Grad. texts in math., 77 (1981) .

[5] D.E. KNUTH .- The art of computer programming , vol. 2 , Addison - Wesley (1969) .

[6] H.W. LEOPOLDT .- Zur Struktur der ℓ-Klassengruppe galoisscher Zahlkörper , J. für reine angew. Math., 199 (1958), pp.165-174.

[7] B. ORIAT .- Spiegelungssatz . Séminaire de Théorie des Nombres , Besançon (1975) .

[8] A. SCHOLZ .- Uber die Beziehung der Klassenzahlen quadratischen Körper zveinander . J. für reine Angew. Math., 166 (1931) , pp. 201-203 .