Astérisque

DON ZAGIER

Nombres de classes et fractions continues

Astérisque, tome 24-25 (1975), p. 81-97
<http://www.numdam.org/item?id=AST_1975__24-25__81_0>

Société Mathématique de France
Astérisque 24-25 (1975)

NOMBRES DE CLASSES ET FRACTIONS CONTINUES

par

Don ZAGIER

-:-:-:-

La partie originale de ce papier (§. V) représente un travail fait en collaboration avec F. Hirzebruch.

§. I. - SOMMES DE DEDEKIND. - Nous allons associer à chaque matrice $A \in SL(2, \mathbb{Z})$ un entier. n_A qui ne dépendra que de la classe de conjugaison de A, c'est-à-dire tel que

(1) $$n_{BAB^{-1}} = n_A \qquad (A, B \in SL(2, \mathbb{Z})).$$

On note par

$$H = \{ z \in \mathbb{C} \mid \operatorname{Im} z > 0 \}$$

le demi-plan supérieur et par

$$\operatorname{Log} \; : \; \mathbb{C} \setminus [-\infty, 0] \to \mathbb{C}$$

la branche de la fonction logarithme qui prend des valeurs réelles sur $\mathbb{R}_+$.

Posons :

$$(2) \qquad \delta(z) = 2\pi iz + 24 \sum_{n=1}^{\infty} \operatorname{Log}(1-e^{2\pi inz}) \quad ; \quad (z \in H)$$

cette fonction est continue (et même holomorphe) sur H. Mais il est clair que

$$e^{\delta(z)} = \Delta(z) = e^{2\pi iz} \prod (1-e^{2\pi inz})^{24}$$

et on sait que $\Delta(z)$ est une forme modulaire de poids 12, donc satisfait à l'équation

$$\Delta(A\,z) = (c\,z+d)^{12}\,\Delta(z) \qquad (z \in H)$$

pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$ (ici $A\,z = \frac{a\,z+b}{c\,z+d}$). En prenant les logarithmes des deux côtés, on trouve

$$(3) \qquad \delta(A\,z) = \delta(z) + 12\operatorname{Log}(c\,z+d) + 2\pi i\,n_A \qquad (z \in H)$$

pour quelque entier $n_A \in \mathbb{Z}$ (le fait que n_A soit indépendant de z provient de la continuité de $\delta(z)$ et de $\operatorname{Log}(c\,z+d)$ dans H).

La propriété d'invariance (1) est claire, ainsi que l'équation

$$(4) \qquad n_{-A} = n_A + 6\operatorname{sign}(c) \qquad (c \neq 0)\ .$$

Par exemple, si $A = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ $(\lambda \in \mathbb{Z})$ est une translation, on a évidemment $\delta(A\,z) = \delta(z+\lambda) = \delta(z) + 2\pi i\lambda$, d'où

$$(5) \qquad n_{\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}} = \lambda \qquad (\lambda \in \mathbb{Z})\ .$$

De même, de $\delta(A\,z+\lambda) = \delta(A\,z) + 2\pi i\lambda$ il suit que

$$n_{\begin{pmatrix} a+\lambda c & b+\lambda d \\ c & d \end{pmatrix}} = n_{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} + \lambda\ ,$$

c'est-à-dire que $n_{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} - \frac{a}{c}$ ne dépend que de la deuxième ligne $(c \;\; d)$ de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
On a

THÉORÈME (Dedekind). - <u>Soit</u> $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$, $c > 0$. <u>Alors</u> :

$$(6) \qquad n_A = \frac{a+d}{c} - 3 - 12\, s(d,c) \; ,$$

<u>où le nombre rationel</u> $s(d,c)$ <u>est défini par la somme</u> (<u>dite</u> "<u>somme de Dedekind</u>")

$$(7) \qquad s(d,c) = \sum_{k=1}^{c-1} \frac{k}{c} \left(\frac{kd}{c} - \left[\frac{kd}{c}\right] - \frac{1}{2}\right) \qquad ((d,c) = 1) \; .$$

<u>La somme</u> $s(d,c)$ <u>a les propriétés suivantes</u> :

i) $s(d,c)$ <u>ne dépend qu</u> d c)

ii) $6c\, s(d,c) \in \mathbb{Z}$

i) (<u>loi de réciprocité</u>) $s(d,c) + s(c,d) = \frac{c^2 + d^2 + 1}{12\, c\, d} - \frac{1}{4}$ $(c, d > 0 \; , \; (c,d) = 1)$.

Remarquons que $s(d,c)$ est tout à fait défini par les propriétés i) et iii), comme on voit en appliquant l'algorithme d'Euler. Il est d'ailleurs amusant que (pour c impair), le symbole de Legendre-Jacobi est déterminé par la formule

$$\left(\frac{d}{c}\right) = (-1)^{\frac{1}{2}\left(\frac{c-1}{2} - 6c\, s(d,c)\right)}$$

et que la loi de réciprocité quadratique est une conséquence de iii).

Les propriétés i) et iii) se démontrent facilement avec l'aide de l'équation (1) avec les matrices B convenables.

§. II. - FORMULE LIMITE DE KRONECKER. - Etant donné une forme quadratique définie positive

$$Q(m,n) = am^2 + 2bmn + cn^2 \qquad (a, c > 0 \ , \ b^2 - ac < 0) \ ,$$

il est important de connaître le comportement de la fonction zêta associée

$$\sum_{m,n}{}' \frac{1}{Q(m,n)^s}$$

(où Σ' indique une sommation sur $(m,n) \in \mathbb{Z}^2 - (0,0)$), au voisinage du point $s = 1$. Puisque cette fonction ne change que par un facteur trivial λ^{-s} quand on remplace Q par λQ $(\lambda \in \mathbb{R}_+)$, on peut supposer que Q est normalisée de façon que son discriminant $b^2 - ac$ est égal à -1 ; dans ce cas, on a :

$$Q(m,n) = \frac{1}{Y} |m + nz|^2$$

pour quelque $z \in H$, $z = X + iY$, et on est ramené à étudier la fonction

$$f(s,z) = \sum_{m,n}{}' \frac{Y^s}{|m+nz|^{2s}} \qquad (z \in H \ , \ \mathrm{Im}(s) > 1) \ . \tag{8}$$

Il se trouve que f, en tant que fonction de s, peut être prolongée comme fonction méromorphe dans tout le plan complexe avec un pôle simple pour $s = 1$ comme unique singularité, et en plus que le résidu de f pour $s = 1$ est égal à π, donc indépendant de z (ce fait a été démontré par Dirichlet, qui l'utilisait pour évaluer le nombre de classes d'un corps quadratique imaginaire). La "formule-limite de Kronecker" est donnée par

THÉORÈME (Kronecker). - Pour $z \in H$, on a :

$$\lim_{s \to 1} \left(f(s,z) - \frac{\pi}{s-1} \right) = 2\pi \left(\gamma - \log 2 - \frac{1}{2} \log Y - 2 \,\mathrm{Re}\, \delta(z) \right)$$

(γ = constante d'Euler, $Y = \mathrm{Im}\, z$, $\delta(z)$ comme ci-dessus).

Le fait évident que

(9) $f(s, A z) = f(s, z) \qquad (\forall z \in H, \ A \in SL(2, \mathbb{Z}))$

entraîne maintenant l'équation fonctionnelle (3) pour $\eth(z)$ (avec quelque constante $n_A \in \mathbb{C}$).

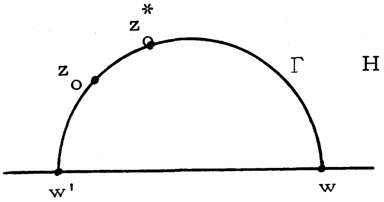
§. III. - <u>LE THÉORÈME DE MEYER.</u> - Soit :

$$A \in SL(2, \mathbb{Z}), \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad c > 0, \quad |a+d| > 2$$

une matrice hyperbolique, et soient w et w' les deux racines de $AX = X$, avec $w > w'$, c'est-à-dire

$$w = \frac{a-d+\sqrt{(a+d)^2-4}}{2c}, \qquad w' = \frac{a-d-\sqrt{(a+d)^2-4}}{2c}$$

On note avec Γ le demi-cercle de H d'extrémités w et w' ; la transformation $z \to A z$ laisse Γ fixe. Soit $z_o \in \Gamma$ quelconque et $z_o^* = A z_o$; alors l'intégrale



(10) $$I(A, s) = \int_{z_o}^{z_o^*} \frac{\partial}{\partial z}(f(s, z))\, dz$$

(prise le long de l'arc de Γ liant z_o et z_o^*) ne dépend pas du choix de z_o^*, parce qu'il suit de (9) que $\frac{\partial}{\partial z} f(s, z)\, dz$ est invariant sous l'action de A. De même, l'équation (9) entraîne la propriété d'invariance

(11) $$I(BAB^{-1}, s) = I(A, s) \qquad (A, B \in SL(2, \mathbb{Z})).$$

Puisque la fonction $f(s, z)$ en (10) peut être remplacée par la fonction partout holomorphe $f(s, z) - \frac{\pi}{s-1}$ sans changer la valeur de l'intégrale, on voit que $I(A, s)$ est une fonction holomorphe en s. Pour $s \to 1$ on peut substituer à $f(s, z)$ l'expression qui apparaît dans la formule-limite de Kronecker, et maintenant l'intégrale peut être évaluée avec l'aide de l'équation (6) de Dedekind. Ceci donne :

THÉORÈME (C. Meyer). - Soit $A \in SL(2, \mathbb{Z})$ comme ci-dessus, alors :

$$I(A, 1) = \frac{\pi^2}{6i} n_A \quad (12)$$

Ce théorème est intéressant pour la raison suivante. Il y a une correspondance biunivoque entre les classes de conjugaison de matrices hyperboliques $A \in SL(2, \mathbb{Z})$ et les classes de similitude de tous les couples (M, V), où M est un module complet (c'est-à-dire un $\mathbb{Z}$-module libre de rang 2) dans un corps quadratique réel et V est un groupe abélien de rang 1 d'unités totalement positives ε telles que $\varepsilon M = M$ (deux couples (M, V) et (M', V') sont dits semblables si $M' = \alpha M$ pour un $\alpha \neq 0$ du corps et $V' = V$). A savoir, si (M, V) est un tel couple, $\{\beta_1, \beta_2\}$ une base orientée de M (c'est-à-dire $\beta_2 > 0$, $\beta_1 \beta_2' - \beta_1' \beta_2 > 0$) et $\varepsilon > 1$ un générateur du groupe V, on définit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ par

$$\begin{aligned} \varepsilon \beta_1 &= a\beta_1 + b\beta_2 , \\ \varepsilon \beta_2 &= c\beta_1 + d\beta_2 , \end{aligned} \quad (13)$$

(ça existe, puisque $\varepsilon M = M$) ; si $A \in SL(2, \mathbb{Z})$ est donnée, on pose $\beta_1 = w$, $\beta_2 = 1$ (w comme ci-dessus), M = module engendré par $1, w$, et $\varepsilon > 1 > \varepsilon' > 0$ les valeurs propres de A (ε est défini par (13)).

A une paire (M, V) on associe une fonction L comme il suit :

$$L_{M,V}(s) = \sum_{\beta \in M/V}' \frac{\text{sign } N(\beta)}{|N(\beta)|^s} , \quad (14)$$

où le Σ' signifie que la valeur $\beta = 0$ doit être omise ; la sommation s'étend sur toutes les orbites de $M - \{0\}$ modulo l'opération du groupe V.

La fonction $L_{M,V}(s)$ est difficile à étudier à cause du fait qu'on est obligé de diviser par l'action des unités au lieu d'étendre la somme sur tout le module comme on pouvait le faire dans le cas des corps quadratiques imaginaires étudié par Kronecker. Meyer a cependant pu évaluer $L_{M,V}(s)$ en employant une astuce célèbre de Hecke (voir Hecke [1], p. 201) pour démontrer la formule

$$(15) \qquad D_M^{s/2}\, L_{M,V}(s) = 2i \frac{\Gamma(s)}{\Gamma(\frac{s+1}{2})^2}\, I(A,s) ,$$

où $A \in SL(2,\mathbb{Z})$ est la matrice hyperbolique correspondante à (M,V) dans la façon qu'on vient de décrire et $D_M = N(M)^2 D$ ($N(M)$ = norme , D = discriminant du corps) est le discriminant de M. En combinant avec le théorème précédant, on obtient :

THÉORÈME (Meyer [3]). - Soient K un corps quadratique, $M \subset K$ un module complet, et V un groupe d'unités totalement positives engendré par une unité $\varepsilon > 1$ telle que $\varepsilon M = M$; alors :

$$(16) \qquad L_{M,V}(1) = \frac{\pi^2}{3\sqrt{D_M}}\, n_A ,$$

où $A \in SL(2,\mathbb{Z})$ est la matrice qui décrit l'opération de ε sur M (par rapport à quelque base orientée).

Avec l'aide de l'équation fonctionnelle de $L_{M,V}$, on peut écrire ce résultat sous la forme :

$$(17) \qquad L_{M,V}(0) = n_A/3 .$$

§. IV. - VALEURS DE NOMBRES DE CLASSES. - Jusqu'à maintenant on n'a parlé ni de fractions continues, ni de nombres de classes.

Soit K un corps quadratique réel dont l'unité fondamentale est totalement positive (par exemple, tel que le discriminant D n'est pas somme de deux carrés). Soit χ un caractère sur les idéaux de K tel que l'on a

$$\chi((\alpha)) = \operatorname{sign}\,(N(\alpha)) \tag{18}$$

pour un idéal principal (α) ("norm signature character"), c'est-à-dire, χ est un caractère sur le groupe des classes d'idéaux au sens restreint qui n'est pas induit par un caractère sur le groupe des classes d'idéaux au sens large. On décompose la fonction $L(s,\chi)$ associée à χ :

$$L(s,\chi) = \sum_{C} \sum_{\mathfrak{A}\in C} \frac{\chi(\mathfrak{A})}{N(\mathfrak{A})^s}, \tag{19}$$

où la première sommation (finie !) s'étend sur toutes les classes d'idéaux au sens large. Fixons une telle classe C et choisissons un idéal entier $\mathfrak{A}_o \in C^{-1}$. Alors

$$\sum_{\mathfrak{A}\in C} \frac{\chi(\mathfrak{A})}{N(\mathfrak{A})^s} = \overline{\chi(\mathfrak{A}_o)}\, N(\mathfrak{A}_o)^s \sum_{\mathfrak{A}\in C} \frac{\chi(\mathfrak{A}\cdot\mathfrak{A}_o)}{N(\mathfrak{A}\mathfrak{A}_o)^s},$$

et $\mathfrak{A}\mathfrak{A}_o$ $(\mathfrak{A}\in C)$ parcourent tous les idéaux principaux (β) avec (β) divisible par $\mathfrak{A}_o$, c'est-à-dire $\beta\in\mathfrak{A}_o$. Deux éléments $\beta\in K$ définissent le même idéal (β) s'ils diffèrent par $\pm\varepsilon$ (ε une unité positive). Donc :

$$\sum_{\mathfrak{A}\in C} \frac{\chi(\mathfrak{A}\mathfrak{A}_o)}{N(\mathfrak{A}\mathfrak{A}_o)^s} = \sum_{\mathfrak{A}_o|(\beta)} \frac{\chi((\beta))}{N((\beta))^s}$$

$$= \sum_{\mathfrak{A}_o|(\beta)} \frac{\operatorname{sign} N(\beta)}{(N(\beta))^s} = \frac{1}{2} L_{M,V}(s),$$

où $M = \mathfrak{A}_o$, V = groupe de toutes les unités totalement positives de K. En substituant la valeur de $L_{M,V}(1)$ donnée par le théorème de Meyer, on trouve alors

$$L(1,\chi) = \frac{\pi^2}{6\sqrt{D}} \sum_{C} \overline{\chi(\mathfrak{A}_o)}\, n(\mathfrak{A}_o) \tag{20}$$

où, pour chaque C , $\mathfrak{A}_o \in C^{-1}$ est un idéal quelconque et $n(\mathfrak{A}_o)$ est donné par n_A avec A la matrice décrivant l'opération de l'unité fondamentale de K sur une base de $\mathfrak{A}_o$. Le théorème de Meyer nous permet alors d'évaluer $L(1, \chi)$ pour les caractères du type "norm signature".

Supposons maintenant que χ est <u>réel</u>, c'est-à-dire ne prend que les valeurs ± 1 . Alors $\chi(\mathfrak{A}^2 \mathfrak{B}) = \chi(\mathfrak{B})$ pour deux idéaux $\mathfrak{A}, \mathfrak{B}$; on appelle un tel caractère un <u>caractère de genre</u>. Il est connu que ces caractères correspondent à toutes les décompositions possibles (à l'ordre près)

$$D = D_1 D_2 \tag{21}$$

du discriminant de K en produit de deux discriminants de corps, et qu'on a alors

$$L(s, \chi) = L_{D_1}(s)\, L_{D_2}(s) \tag{22}$$

(où $L_D(s) = \sum_{n=1}^{\infty} (\frac{D}{n})/n^s$) . Si χ a aussi la propriété (18) , on a $D_1 < 0$, $D_2 < 0$, et dans ce cas on sait que

$$L_{D_i}(1) = \frac{\pi}{\sqrt{|D_i|}}\, h(D_i)$$

(avec les conventions $h(-3) = \frac{1}{3}$, $h(-4) = \frac{1}{2}$) . On a alors :

$$h(D_1)\, h(D_2) = \frac{1}{6} \sum_{C} \chi(\mathfrak{A}_o)\, n(\mathfrak{A}_o) \quad . \tag{23}$$

<u>Exemple</u> : <u>Soit</u> $p \equiv 3 \pmod 4$ <u>un nombre premier</u>, <u>et supposons que</u> $h(p) = 1$. <u>Soient</u> $c, d > 0$ <u>la plus petite solution de l'équation de Pell</u>

$$d^2 - pc^2 = 1 \; .$$

<u>Soit</u>

$$n = \frac{2d}{c} - 3 - 12\, s(d, c) \quad .$$

Alors on a

$$(24) \qquad h(-p) = \frac{1}{3}\, n .$$

En fait, si on pose $D = 4p$, $D_1 = -4$, $D_2 = -p$, $\varepsilon = d+c\sqrt{p}$, et si on choisit pour $\mathfrak{A}_o$ le module $\{\sqrt{p}\ ,\ 1\}$ (il n'y a qu'une classe C) , on voit que $A = \begin{pmatrix} d & cp \\ c & d \end{pmatrix}$; l'entier n n'est autre que n_A .

Evidemment, si $h(p) > 1$ il y a une formule analogue où en (24) n est remplacé par une somme de plusieurs entiers $\pm\, n_A$.

En tant qu'exemple numérique, prenons $p = 7$; alors $c = 3$, $d = 8$, $s(d, c) = \frac{1}{3}\left(\frac{+1}{6}\right) + \frac{2}{3}\left(\frac{-1}{6}\right) = \frac{-1}{18}$, et $n = \frac{16}{3} - 3 + \frac{12}{18} = 3 = 3h(-7)$.

§. V. - NOMBRES DE CLASSES ET FONCTIONS CONTINUES

LEMME. - Pour $b_1, \ldots, b_r \in \mathbb{Z}$ et

$$(25) \qquad A = \begin{pmatrix} b_1 & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} b_r & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$$

on a :

$$(26) \qquad n_A = \sum_{i=1}^{r} (b_i - 3) .$$

Démonstration. - Par induction sur r . Pour $r = 1$,

$$n_A = \frac{a+d}{c} - 3 - 12\, s(d, c) = \frac{b_1 + 0}{1} - 3 - 12 s(0, 1) = b_1 - 3 .$$

Si le lemme est vrai pour r et A est comme en (25), $b_o \in \mathbb{Z}$, $A' = \begin{pmatrix} b_o & -1 \\ 1 & 0 \end{pmatrix} A$, alors

$$A' = \begin{pmatrix} \frac{b_0 a - c}{a} & \frac{b_0 b - d}{b} \end{pmatrix},$$

$$n_{A'} = \frac{b_0 a - c + b}{a} - 3 - 12\, s(b,a)$$

et, puisque $ad-bc = 1$,

$$\begin{aligned} s(b,a) &= s(-c,a) = -s(c,a) \\ &= s(a,c) - \frac{c^2+a^2+1}{12\,ac} + \frac{1}{4} \\ &= s(d,c) - \frac{c^2+a^2+1}{12\,ac} + \frac{1}{4} \end{aligned}$$

(où l'on a utilisé $s(d,c) = s(d',c)$ pour $dd' \equiv 1 \pmod{c}$ et la loi de réciprocité pour $s(d,c)$), ce qui donne

$$\begin{aligned} n_{A'} &= b_0 - 3 + \frac{b-c}{a} - 12\, s(d,c) + \frac{c^2+a^2+1}{ac} - 3 \\ &= b_0 - 3 + \frac{a+d}{c} - 3 - 12\, s(d,c) \\ &= b_0 - 3 + n_A = \sum_{i=0}^{r} (b_i - 3)\ . \end{aligned}$$

C. Q. F. D.

On sait que chaque $A \in SL(2,\mathbb{Z})$ peut s'écrire sous la forme (25) avec $b_1,\ldots,b_r \in \mathbb{Z}$ (parce qu'on sait que $SL(2,\mathbb{Z})$ est engendré par $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$). Mais il y a même une forme standard pour les classes de conjugaison : chaque matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ hyperbolique (et avec $c > 0$) est conjuguée en $SL(2,\mathbb{Z})$ à un produit

$$\begin{pmatrix} b_1 & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} b_r & -1 \\ 1 & 0 \end{pmatrix} \tag{27}$$

avec $b_i \in \mathbb{Z}$, $b_i \geq 2$ (et au moins un $b_i > 2$), et en plus r est unique et $b_1,\ldots,b_r$ sont uniques à permutation cyclique près (une permutation cyclique des b_i ne changeant évidemment pas la classe de conjugaison de (27)). On appelle

$((b_1, \ldots, b_r))$ le cycle associé à la matrice A. Pour trouver les b_i, on définit w comme ci-dessus (c'est-à-dire, w est la solution la plus grande de $Ax = x$) et on le développe en fraction continue

$$w = a_o - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \ddots}} \qquad (a_i \geq 2 \quad \text{pour} \quad i > 0)$$

(remarquez les signes négatifs) ; la suite des quotients partiels $\{a_i\}_{i \in \mathbb{N}}$ sera périodique à partir d'un certain indice i_o et le cycle $((b_1, \ldots, b_r))$ n'est autre que la période de cette suite (ou bien la période primitive ou bien k fois la période primitive, selon que pour le couple (M, V) correspondant à A le groupe V coïncide avec le groupe de toutes les unités totalement positives laissant M invariant ou à un sous-groupe d'indice k de ce groupe).

Ceci permet de calculer les n_A à l'aide des fractions continues, et, en combinant cela avec les théorèmes de Meyer déjà énoncés, on obtient des identités assez remarquables exprimant des nombres de classes en termes de fractions continues. Par exemple, on prend un premier $p \equiv 3 \pmod 4$ avec $h(p) = 1$ comme tout à l'heure, on développe :

$$\sqrt{p} = b_o - \cfrac{1}{\underbrace{b_1 - \cfrac{1}{b_2 - \ddots - \cfrac{1}{b_r}}}_{\text{période minimale}} - \cfrac{1}{b_1 - \ddots}}$$

(cette fraction continue est périodique dès b_1), et on a

$$b_1 + \ldots + b_r - 3r = 3h(-p) .$$

Avec $p = 7$, cela donne :

$$\sqrt{7} = 3 - \cfrac{1}{3 - \cfrac{1}{6 - \cfrac{1}{3 - \cfrac{1}{6 - \ddots}}}}$$

$r = 2$, $b_1 = 3$, $b_2 = 6$, $\Sigma\ (b_i - 3) = 0 + 3 = 3 = 3\,h(-7)$.

Pour $h(p) > 1$ on a une formule analogue où il faut considérer toutes les fractions continues des éléments de $\mathbb{Q}(\sqrt{p})$ (il n'y a qu'un nombre fini de périodes distinctes) et sommer les $\Sigma\,(b_i - 3)$ correspondant avec des signes convenables.

§. VI. - UNE FORMULE POUR LE NOMBRE DE CLASSES.(1) - Il se trouve que la formule donnée dans le §. V. pour le nombre de classes d'un corps quadratique imaginaire $\mathbb{Q}(\sqrt{-p})$, $h(p) = 1$, peut être reformulée dans une forme valable pour tout discriminant $-N$ négatif et où l'on n'a pas besoin de connaître ni le nombre de classes d'idéaux de $\mathbb{Q}(\sqrt{N})$ ni les périodes des fractions continues correspondantes. La formule dont il s'agit est la suivante.

THÉORÈME [2]. - Soit $N \equiv 3 \pmod 4$, $N \neq 3$, un nombre positif sans facteurs carrés. Alors on a :

$$3\,h(-N) = \sum_{n=1}^{[2\sqrt{N}]} \chi(n) \sum_{\substack{b=[\sqrt{N}]-n+1 \\ b^2 \equiv N \ (\mathrm{mod}\ n)}}^{[\sqrt{N}]} \left[\frac{b+\sqrt{N}}{n}\right] , \tag{28}$$

où $\chi(n)$ est la fonction multiplicative de période 8 défini par la table

(1) Cette partie n'a pas été traitée dans l'exposé oral

(29)

$n \pmod 8$	0	1	2	3	4	5	6	7
$\chi(n)$	0	1	$(\frac{2}{N})$	-1	0	1	$-(\frac{2}{N})$	-1

(Pour plus de précisions, le lecteur est renvoyé à l'article [2]).

La formule (28) est très amusante, pour la raison suivante. Soit pour $n > 0$

$$a(n) = \sum_{\substack{|b| < \sqrt{N} \\ b > \sqrt{N} - n \\ b^2 \equiv N \pmod n}} \left[\frac{b+\sqrt{N}}{n}\right] . \tag{30}$$

L'entier $a(n)$ est nul pour $n > 2\sqrt{N}$, puisque l'on a $0 < \frac{b+\sqrt{N}}{n} < \frac{2\sqrt{N}}{n} < 1$ dans ce cas ; donc la formule (28) peut être écrite sous la forme

$$3\, h(-N) = \sum_{n=1}^{\infty} \chi(n)\; a(n) \tag{31}$$

(où la somme est en fait finie). Pour étudier le comportement de cette série pour $N \to \infty$; nous remarquons que, pour $n \ll \sqrt{N}$, on a $b + \sqrt{N} \sim 2\sqrt{N}$ pour chaque b en (30) (puisque $\sqrt{N} - n < b < \sqrt{N}$), donc que $a(n)$ est asymptotique à $\frac{2\sqrt{N}}{n}$ fois le nombre des entiers b satisfaisant aux conditions de la sommation en (30) . D'autre part, dans ce cas la condition $b > -\sqrt{N}$ est comprise dans la condition $b > \sqrt{N} - n$, de telle sorte que

$$\begin{aligned} a(n) &\sim \frac{2\sqrt{N}}{n} \;\#\, \{\, b \mid \sqrt{N} - n < b < \sqrt{N} \;,\;\; b^2 \equiv N \pmod n \,\} \\ &= \frac{2\sqrt{N}}{n}\, b(n) \;, \end{aligned} \tag{32}$$

où

$$b(n) = \sum_{\substack{b \pmod n \\ b^2 \equiv N \pmod n}} 1 \;. \tag{33}$$

Il est donc raisonnable de croire que les deux séries $\sum_{n=1}^{\infty} \chi(n)\, a(n)$ et et $2\sqrt{N} \sum_{n=1}^{\infty} \chi(n) \frac{b(n)}{n}$ sont asymptotiquement égales pour $N \to \infty$. Or, le théorème nous dit qu'elles sont identiques ! Pour le voir, il faut remarquer que $b(n)$ est une fonction multiplicative, donc que $\sum_{n=1}^{\infty} \chi(n) \frac{b(n)}{n^s}$ a un développement en produit d'Euler dont le facteur correspondant à un premier p est (comme on le voit facilement)

$$1 + \frac{(\frac{2}{N})}{2^s} \qquad \text{pour } p = 2 ,$$

$$1 + \frac{(\frac{-1}{p})}{p^s} \qquad \text{pour } p \neq 2 ,\ p \mid N ,$$

$$1 \qquad \text{pour } p \neq 2 ,\ (\tfrac{N}{p}) = -1 ,$$

$$1 + \frac{2(\frac{-1}{p})}{p^s} + \frac{2}{p^{2s}} + \frac{2(\frac{-1}{p})}{p^{3s}} + \dots \qquad \text{pour } p \neq 2 ,\ (\tfrac{N}{p}) = +1 .$$

On vérifie que dans chacun de ces quatre cas, ce facteur peut être écrit comme

$$(1 - (\tfrac{-N}{p})\, p^{-s})^{-1}\, (1 - (\tfrac{-4}{p})\, p^{-s})^{-1}\, (1 - p^{-2s}) .$$

On a donc (pour $Re(s) > 1$)

$$\begin{aligned} \sum_{n=1}^{\infty} \chi(n) \frac{b(n)}{n^s} &= \prod_p (1 - (\tfrac{-N}{p})\, p^{-s})^{-1} \prod_p (1 - (\tfrac{-4}{p}) p^{-s})^{-1} \prod_p (1 - p^{-2s}) \\ &= L_{-N}(s)\, L_{-4}(s) \,/\, \zeta(2s) . \end{aligned} \tag{34}$$

D'autre part, on sait que, pour $N > 0$

$$L_{-N}(1) = \frac{\pi}{\sqrt{N}}\, h(-N)$$

(où $h(-3) = \frac{1}{3}$, $h(-4) = \frac{1}{2}$), donc :

$$\sum_{n=1}^{\infty} b(n) \frac{\chi(n)}{n} = (\frac{\pi}{\sqrt{N}}\, h(-N))\, (\frac{\pi}{4}) \,/\, (\frac{\pi^2}{6}) = \frac{3}{2\sqrt{N}}\, h(-N) ,$$

d'où pour $N > 3$

$$2\sqrt{N} \sum_{n=1}^{\infty} \chi(n) \frac{b(n)}{n} = 3h(-N)$$

On a donc deux séries, l'une infinie et convergente, l'autre finie, dont les premiers (et plus grands) termes sont asymptotiquement les mêmes et ayant la même somme. Pour terminer, on donne un exemple numérique.

$N = 203 = 7.29$

n	$\chi(n)\ a(n)$	$2\sqrt{N}\ \frac{\chi(n)\ b(n)}{n}$
1	28	28,495609 ...
2	-13	-14,247805 ...
7	-4	-4,070801 ...
11	-2	-5,181020 ...
14	1	2,035401 ...
17	2	3,352425 ...
22	0	2,590510 ...
29	0	0,982607 ...
34	.	-1,676212 ...
41	:	1,390030 ...
43	(a(n) = 0 pour n>17)	-1,325377 ...
53		1,075306 ...
58		-0,491304 ...
59		-0,965953 ...
61		0,934282 ...
73		0,780702 ...
77		0,740146 ...
79		-0,721408 ...
⋮		⋮

(Les valeurs omises de n ont $\chi(n)\ a(n) = \chi(n)\ b(n) = 0$). La somme des valeurs dans chacune des deux colonnes est égale à $12 = 3h(-203)$.

BIBLIOGRAPHIE

[1] HECKE E. - Mathematische Werke, p. 200

[2] HIRZEBRUCH F. and ZAGIER D. - Class numbers, continued fractions and the Hilbert modular group (to appear)

[3] MEYER C. - Über die Berechnung der Klassenzahl abelscher Körper über quadratischen Zahlkörpern. Akademie-Verlag, Berlin, 1957.

-:-:-:-

Don ZAGIER
Mathematisches Institut
Universität Bonn
D-5300 BONN
Wegelerstrasse 10