RESIDUS QUADRATIQUES ET NOMBRE DE CLASSES

par

Dominique DUMONT

RÉSUMÉ. — Soit p un nombre premier $\equiv 3 \pmod 4$. Une formule classique de Dirichlet relie l'excédent des résidus sur les non résidus dans l'intervalle $[1, \frac{p-1}{2}]$ au nombre de classes $h(-p)$. C'est encore un problème ouvert que de donner de ce résultat une preuve directe et non analytique. Nous proposons ici un exposé détaillé et élémentaire du sujet, ainsi qu'une preuve analytique où la théorie des séries divergentes s'introduit naturellement.

1.— Un problème posé par Jacobi

Soit p un nombre premier. Les entiers n compris entre 1 et $p-1$ se répartissent en $(p-1)/2$ résidus quadratiques et $(p-1)/2$ non résidus. On obtient chaque résidu une fois et une seule en réduisant modulo p les carrés $1^2, 2^2, 3^2, \ldots, ((p-1)/2)^2$.

En effet si x^2 et y^2 sont deux éléments de cette liste, ils sont distincts car $x^2 - y^2 = (x-y)(x+y)$ ne peut être multiple de p, en outre les autres éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont $-1, -2, \ldots, -(p-1)/2$ qui redonnent les mêmes carrés. Il est clair que les résidus forment un sous-groupe multiplicatif de $(\mathbb{Z}/p\mathbb{Z})^*$ (le produit de deux résidus est un résidu, l'inverse d'un résidu également).

Dans tout notre exposé on suppose $p \equiv 3 \pmod 4$. De ce fait, l'entier $p - 1 = -1$ n'est jamais résidu. Car si cela était, l'involution $n \mapsto -n$ décomposerait l'ensemble des résidus en paires, ce qui est absurde puisque leur nombre $(p-1)/2$ est impair. On a au contraire

$$n \quad \text{résidu} \quad \Longleftrightarrow \quad -n = p - n \quad \text{non résidu.}$$

Si n est résidu, on écrit $\chi(n) = +1$ et sinon $\chi(n) = -1$. La lettre χ désigne donc le *caractère de Legendre* modulo p, nous préférons cette notation au symbole de Legendre $\left(\frac{n}{p}\right)$. Voici ce que donne la répartition entre résidus et non résidus pour les premières valeurs de p :

résidus : 1 2 4
non résidus : 3 5 6

$p = 7$

résidus : 1 3 4 5 9
non résidus : 2 6 7 8 10

$p = 11$

résidus :	1			4	5	6	7		9		11					16	17	
non résidus :		2	3					8		10		12	13	14	15			18

$$p = 19$$

rés. :	1	2	3	4		6		8	9			12	13			16		18			
non rés. :					5		7			10	11			14	15		17		19	20	21	22

$$p = 23$$

Considérons à présent les sommes partielles h_n de la série de terme général $\chi(n)$:

$$h_n = \chi(1) + \chi(2) + \cdots + \chi(n) \qquad (n \geq 1),$$

où l'on convient que $h_0 = 0$. Le graphe de la fonction $n \mapsto h_n$ est un chemin fait de pas montants de $+1$ ou descendants de -1. L'entier h_n est la hauteur du chemin au point d'abscisse n et représente l'excédent des résidus sur les non résidus dans l'intervalle $[1, n]$. Le chemin part de la hauteur $h_0 = 0$ pour revenir à la hauteur $h_{p-1} = 0$ et il est symétrique par rapport à la verticale en $(p-1)/2$ puisque $\chi(p-n) = -\chi(n)$. Posons

$$H = h_{(p-1)/2}$$

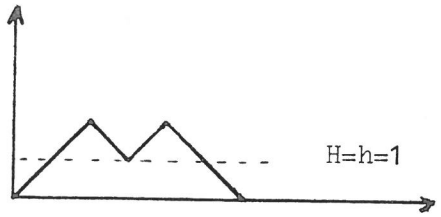
et appelons H la *hauteur centrale* du chemin. Il est clair que c'est un entier impair puisqu'on parvient à cette hauteur au bout d'un nombre impair de pas $((p-1)/2)$. Jacobi a observé et conjecturé que cette hauteur centrale est toujours *positive*. Rappelons qu'une preuve simple et directe (non analytique) de ce résultat reste un problème ouvert.

Il est assez naturel d'introduire également la *hauteur moyenne* h du chemin, définie par

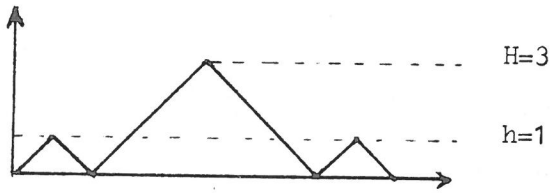
$$h = \frac{1}{p}(h_0 + h_1 + \cdots + h_{p-1})$$

et de se demander si elle est également positive. Nous allons voir que cela revient au même car les deux hauteurs sont liées par les relations :

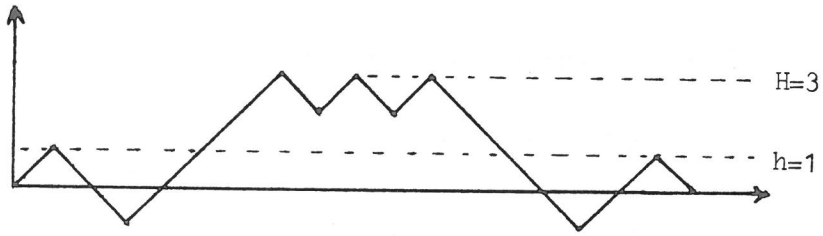
$$\begin{aligned} &\text{Si} \quad p \equiv 3 \pmod 8, \qquad H = 3h \\ &\text{Si} \quad p \equiv 7 \pmod 8, \qquad H = h. \end{aligned}$$



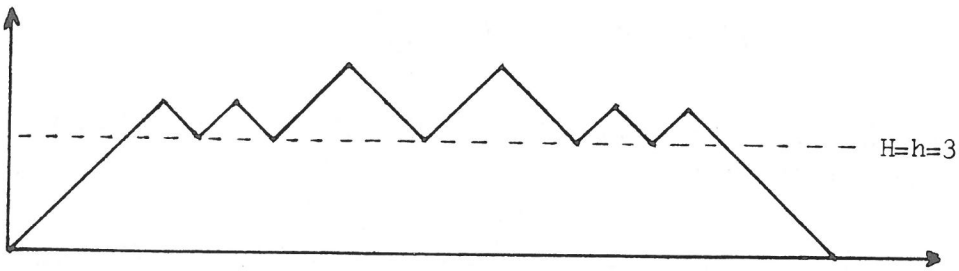
p=7



p=11



p=19



p=23

Chemin des résidus pour quelques valeurs de p, de hauteur centrale H et de hauteur moyenne h.

En effet,

$$\begin{aligned} ph &= \sum_{n=1}^{p-1} \sum_{k=1}^{n} \chi(k) \\ &= \sum_{n=1}^{p-1} n\chi(p-n) \\ &= -\sum_{n=1}^{p-1} n\chi(n) \\ &= -\sum_{n=1}^{(p-1)/2} (n\chi(n) + (p-n)\chi(p-n)) \end{aligned}$$

$$ph = pH - 2\sum_{n=1}^{(p-1)/2} n\chi(n) \qquad (1)$$

D'autre part,

$$\begin{aligned} ph &= -\sum_{n\text{pair}} (n\chi(n) + (p-n)\chi(p-n)) \\ &= p\sum_{n\text{pair}} \chi(n) - 2\sum_{n\text{pair}} n\chi(n) \\ &= p\sum_{n=1}^{(p-1)/2} \chi(2m) - 2\sum_{n=1}^{(p-1)/2} 2m\chi(2m) \end{aligned}$$

$$ph = p\chi(2)H - 4\chi(2)\sum_{n=1}^{(p-1)/2} n\chi(n) \qquad (2)$$

En multipliant l'identité (1) par 2, l'identité (2) par $-\chi(2)$, et en ajoutant les deux on trouve :

$$H = (2 - \chi(2))h.$$

Pour calculer $\chi(2)$ on peut utiliser un résultat de Zolotareff [C] selon lequel $\chi(n)$ est la signature de la permutation de $(\mathbb{Z}/p\mathbb{Z})^*$ définie par $x \mapsto nx$. Or le mot $246\cdots(p-1)135\cdots(p-2)$ possède $1+2+3+\cdots+(p-1)/2 = (p^2-1)/8$ inversions, nombre qui est impair si $p \equiv 3 \pmod 8$ et pair si $p \equiv 7 \pmod 8$. D'où $\chi(2) = -1$ et $H = 3h$ dans le premier cas, $\chi(2) = 1$ et $H = h$ dans le second cas.

La hauteur moyenne nous conduit à donner une formulation simple d'une deuxième conjecture posée par Jacobi (sous une forme un peu différente) et démontrée par Dirichlet [D]:

la hauteur moyenne h est égale au nombre de classes $h(-p)$.

Il nous faut donc à présent définir ce que l'on entend par le *nombre de classes* $h(-p)$.

2.— Le nombre de classes h(-p)

Nous considérons l'ensemble $\mathcal{Q}(-p)$ des formes quadratiques

$$q(x,y) = ax^2 + bxy + cy^2$$

où les coefficients a, b, c sont des entiers tels que

$$b^2 - 4ac = -p, \qquad a > 0, \quad c > 0.$$

Pour en faire la collection, il suffit de choisir un entier impair arbitraire comme valeur de b, puis pour chaque choix de b de trouver tous les couples (a,c) tels que $b^2 + p = 4ac$. On obtient ainsi un ensemble infini de formes quadratiques.

Une autre manière d'engendrer un nombre infini de ces formes consiste à partir de l'une d'elle et à opérer des changements de variables tels que $t : (x,y) \mapsto (x, x+y)$, qui envoie $ax^2 + bxy + cy^2$ sur $ax^2 + (2a+b)xy + (a+b+c)y^2$, ou $s : (x,y) \mapsto (y,-x)$, qui envoie $ax^2 + bxy + cy^2$ sur $cx^2 - bxy + ay^2$. Or ces transformations préservent le discriminant, elles sont donc internes à $\mathcal{Q}(-p)$, et il en va de même de toute composée de s et de t. La transformation t, de matrice $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et la transformation s, de matrice $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, engendrent le groupe $SL_2(\mathbb{Z})$ formé de toutes les matrices à coefficients entiers $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ vérifiant $\alpha\delta - \beta\gamma = 1$ (matrices *unimodulaires.*) Nous dirons que deux formes quadratiques sont *équivalentes* si elles se correspondent par un changement de variables unimodulaire $(x,y) \mapsto (\alpha x + \beta y, \gamma x + \delta y)$.

L'ensemble quotient de $\mathcal{Q}(-p)$ par cette relation d'équivalence s'appelle l'ensemble des *classes de formes quadratiques.* Nous allons voir que cet ensemble est de cardinal fini, et son cardinal est précisément ce qu'on note $h(-p)$.

En sélectionnant un représentant dans chaque classe, nous parviendrons à une vision plus concrète de cet ensemble et à une méthode de calcul très simple de $h(-p)$.

A cet effet nous notons que le polynôme $q(x,1) = ax^2 + bx + c$ possède deux racines imaginaires conjuguées dont l'une, à savoir $z = (-b + i\sqrt{p})/2a$, appartient au demi-plan de Poincaré $\mathfrak{H}$ formé des nombres complexes de partie imaginaire > 0. Cette racine caractérise d'ailleurs la forme quadratique, car a, b, c sont premiers entre eux ($\Delta = -p$). Or le changement de variable t correspond sur le polynôme à $x \mapsto x + 1$, donc

sur cette racine à la translation $T : z \mapsto z - 1$. De même la transformation s correspond à l'inversion-symétrie $S : z \mapsto (-1/z)$. Le *groupe modulaire* est le groupe engendré par les homographies T et S. L'ensemble quotient de $\mathfrak{H}$ par l'action de ce groupe est représenté par le *domaine fondamental*

$$D = \{z \in \mathfrak{H}; \quad |z| \geq 1 \quad \text{et} \quad -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}\}.$$

Nous admettrons les propriétés suivantes du domaine fondamental (pour une démonstration, voir par exemple [S1] p.127-131) :

(i) tout élément de $\mathfrak{H}$ est équivalent à un élément de D

(ii) si deux éléments de D sont équivalents, ou bien ils sont sur les deux demi-droites verticales $\mathrm{Re}(z) = \pm\frac{1}{2}$ et se correspondent par T, ou bien ils sont sur le cercle trigonométrique $|z| = 1$ et se correspondent par S (dans les deux cas ils sont symétriques par rapport à l'axe des y)

(iii) l'homographie $z \mapsto z' = (\alpha z + \beta)/(\gamma z + \delta)$ qui envoie un élément z de $\mathfrak{H}$ sur son équivalent z' dans D est unique pourvu que $z' \neq i$ et que $z' \neq j$; la matrice $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ qui lui correspond dans $SL_2(\mathbb{Z})$ est donc unique au signe près.

A quelle condition sur a, b, c le polynôme $ax^2 + bx + c$ possède-t-il une racine dans le domaine fondamental ? Puisque $\mathrm{Re}(z) = (-b)/2a$ et $|z|^2 = z\bar{z} = c/a$, il est clair que la condition cherchée est

$$|b| \leq a \leq c.$$

Les deux premières propriétés du domaine fondamental se retraduisent en

(i) toute forme quadratique est équivalente à une forme telle que $|b| \leq a \leq c$ (on trouvera un algorithme explicite dans [O]) ;

(ii) si deux formes vérifiant $|b| \leq a \leq c$ sont équivalentes, alors ou bien $|b| = a$ et elles se correspondent par t, ou bien $a = c$ et elles se correspondent par s, dans les deux cas ces deux formes sont $ax^2 + bxy + cy^2$ et $ax^2 - bxy + cy^2$.

Nous sommes ainsi conduits à adopter la définition suivante : une forme quadratique $ax^2 + bxy + cy^2$ est dite *réduite* si $|b| \leq a \leq c$, avec la condition que si l'une de ces inégalités est une égalité, alors b doit être *positif* (b peut être négatif si les deux inégalités sont strictes).

En fait, comme nous n'étudions dans le cadre de cet article que les formes de discriminant $\Delta = -p$ avec p premier ≥ 7, le seul cas d'égalité qui se présente entre $|b|, a, c$, est celui où l'on prend $a = b = 1$ et où l'on obtient la forme $x^2 + xy + (p+1)/4$, appelée la forme réduite *principale*.

Il résulte des propriétés (i) et (ii) énoncées ci-dessus que chaque classe de formes quadratiques de discriminant $-p$ contient une unique forme

réduite. Le nombre des formes réduites est fini, car

$$p = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2, \quad \text{donc} \quad |b| \leq a \leq \sqrt{(p/3)}.$$

L'entier $h(-p)$ n'est autre que le nombre de ces formes réduites, et pour le calculer il suffit de dresser leur liste : on choisit d'abord b (impair et inférieur à $\sqrt{(p/3)}$), puis on cherche les couples (a, c) tels que $ac = (b^2 + p)/4$ et $|b| < a < c$ (sauf le cas d'égalité de la forme principale). Voir à ce sujet le tableau des formes réduites ci-dessous.

$p = 7$	$\|b\| = 1$	$ac = 2$	$x^2 + xy + 2y^2$	$h(-7) = 1$
$p = 11$	$\|b\| = 1$	$ac = 3$	$x^2 + xy + 3y^2$	$h(-11) = 1$
$p = 19$	$\|b\| = 1$	$ac = 5$	$x^2 + xy + 5y^2$	$h(-19) = 1$
$p = 23$	$\|b\| = 1$	$ac = 6$	$x^2 + xy + 6y^2$	
	$\|b\| = 1$	$ac = 6$	$2x^2 + xy + 3y^2$	
	$\|b\| = 1$	$ac = 6$	$2x^2 - xy + 3y^2$	$h(-23) = 3$
$p = 59$	$\|b\| = 1$	$ac = 15$	$x^2 + xy + 15y^2$	
	$\|b\| = 1$	$ac = 15$	$3x^2 + xy + 5y^2$	
	$\|b\| = 1$	$ac = 15$	$3x^2 - xy + 5y^2$	
	$\|b\| = 3$	$ac = 17$	pas de solution	$h(-59) = 3$
$p = 347$	$\|b\| = 1$	$ac = 87$	$x^2 + xy + 87y^2$	
	$\|b\| = 1$	$ac = 87$	$3x^2 + xy + 29y^2$	
	$\|b\| = 1$	$ac = 87$	$3x^2 - xy + 29y^2$	
	$\|b\| = 3$	$ac = 89$	pas de solution	
	$\|b\| = 5$	$ac = 93$	pas de solution	
	$\|b\| = 7$	$ac = 99$	$9x^2 + 7xy + 11y^2$	
	$\|b\| = 7$	$ac = 99$	$9x^2 - 7xy + 11y^2$	
	$\|b\| = 9$	$ac = 107$	pas de solution	$h(-347) = 5$

Formes réduites pour diverses valeurs de p

La troisième propriété du domaine fondamental se traduit comme suit : (iii) Toute forme quadratique $q(x, y)$ de discriminant $-p$ est équivalente à une unique forme réduite $q_i(x, y)$, et la matrice $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ appartenant à $SL_2(\mathbb{Z})$ qui fait passer de q à q_i est unique au signe près.

Avant d'aborder la démonstration de l'égalité de $h(-p)$ avec la hauteur moyenne h, nous ferons une courte digression sur le nombre de représentations d'un entier en sommes de trois carrés.

3.— Sommes de trois carrés

Rappelons que comme tout carré est $\equiv 0, 1,$ ou $4 \pmod 8$, un nombre congru à $7 \pmod 8$ ne peut être somme de trois carrés, et si un nombre

congru à 3 (mod 8) est somme de trois carrés ceux-ci sont impairs. Gauss a démontré que tout nombre congru à 3 (mod 8) est effectivement somme de trois carrés impairs (l'énoncé équivalent *tout nombre est somme de trois nombres triangulaires* était déjà conjecturé par Fermat). On trouvera une preuve algébrique de ce théorème dans [S1], et une preuve par les q-séries dans [A]. Gauss a également dénombré les représentations :

Théorème. *Soit n un entier naturel tel que $n \equiv 3 \pmod 8$ $(n \neq 3)$. Le nombre $r_3(n)$ de triplets ordonnés d'entiers impairs naturels (x, y, z) tels que $x^2 + y^2 + z^2 = n$ est égal à $3h(-n)$*

Exemples :	$11 = 9 + 1 + 1$	(3 représentations)	$r_3(11) = 3$
	$19 = 9 + 9 + 1$	(3 représentations)	$r_3(19) = 3$
	$59 = 49 + 9 + 1$	(6 représentations)	
	$59 = 25 + 25 + 9$	(3 représentations)	$r_3(59) = 9$
	$347 = 289 + 49 + 1$	(6 représentations)	
	$347 = 225 + 121 + 1$	(6 représentations)	
	$347 = 169 + 169 + 9$	(3 représentations)	$r_3(347) = 15$

Des variantes de ce théorème existent où, suivant Kronecker, on introduit le nombre $H(-n)$ des formes $ax^2 + bxy + cy^2$ telles que $|b| \leq 2a \leq 2c$, ou encore telles que $b > 0$, $b < 2a$, $b < 2c$. Dans le premier cas, on élargit le domaine fondamental à tout l'extérieur du cercle trigonométrique dans la bande $|\mathrm{Re}(z)| \leq 1$, dans le second cas à l'extérieur du cercle de diamètre $[-1, 0]$ dans la bande $-1 < \mathrm{Re}(z) < 0$. Il est facile de voir que chacun de ces deux domaines est la réunion de trois domaines congrus à D, par conséquent on a dans les deux cas $H(-n) = 3h(-n)$, et le théorème s'écrit simplement $r_3(n) = H(-n)$. Une preuve de ce théorème, rédigée dans un langage élémentaire, se trouve dans [W]. D'autre part une conséquence de ce théorème et de l'égalité $h = h(-p)$ est *l'égalité entre la hauteur centrale H et le nombre $r_3(p)$* dès que $p \equiv 3 \pmod 8$. On ne connaît pas de preuve directe de ce résultat.

4.— La série divergente $\sum_1^\infty \chi(n)$

Nous allons voir que la hauteur moyenne h du chemin des résidus peut, en plusieurs sens que nous allons préciser, être considérée comme *la somme de la série divergente* $\sum_1^\infty \chi(n)$.

Rappelons que la fonction χ se prolonge à l'ensemble des entiers naturels par périodicité de période p, en convenant que $\chi(p) = 0$. De ce fait la suite des sommes partielles $h_n = \chi(1) + \chi(2) + \cdots + \chi(n)$ est également périodique de période p (car $h_p = 0$). Or il est clair que toute suite périodique converge au sens de Cesàro vers la moyenne de ses valeurs

sur une période, en l'occurrence h_n converge en moyennes de Cesàro vers h :

$$\lim_{n\to\infty} \frac{h_1 + h_2 + \cdots + h_n}{n} = h \qquad (C)$$

Des résultats classiques sur la sommabilité des séries divergentes permettent d'en déduire les limites suivantes :

$$\lim_{x\to 1^-} \sum_{n=1}^{\infty} \chi(n) x^n = h \qquad (A)$$

$$\lim_{s\to 0+} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = h \qquad (D)$$

$$\lim_{q\to 1^-} \sum_{n=1}^{\infty} \chi(n) \frac{n(1-q)q^n}{1-q^n} = h \qquad (L)$$

$$\lim_{q\to 1^-} \sum_{n=1}^{\infty} \chi(n) \frac{2q^n}{1+q^n} = h \qquad (L')$$

La sommabilité d'Abel (A) est plus puissante que (C) d'après un théorème classique dû à Frobenius, ou d'après un théorème moins connu [H2] mais un peu plus général de Hardy qui montre aussi que (L') résulte de (C) (La preuve de Hardy est élémentaire, et utilise essentiellement le fait que les différences premières et secondes des fonctions $f_n(x) = x^n$, ou des fonctions $f_n(x) = 2x^n/(1+x^n)$, sont positives au voisinage de 1). La sommabilité de Lambert (L) est également plus puissante que (C) [H1] (mais moins que (A), tandis que (L') n'est pas comparable à (A)), enfin la sommabilité (D) est plus puissante que (C) sur les séries dont les sommes partielles sont bornées, ce qui est le cas ici.

Pour démontrer l'égalité $h = h(-p)$, il suffit donc de démontrer que l'une de ces limites est aussi égale à $h(-p)$. C'est cette méthode que nous utiliserons, en choisissant la sommabilité (L'), où la variable est notée q car c'est la notation habituelle pour les séries de Lambert. Nous verrons que cette série est liée au problème combinatoire du dénombrement des représentations de l'entier n par les formes de discriminant $-p$.

5.— Représentations de n par les formes de discriminant $-p$

Soit n un entier naturel et $q(x,y) = ax^2 + bxy + cy^2$ une forme quadratique de discriminant $-p$. Une solution de l'équation

$$n = ax^2 + bxy + cy^2 \quad \text{avec} \quad (x,y) \in \mathbb{Z} \times \mathbb{Z}$$

s'appelle une *représentation de l'entier n par la forme q*. Si n est représenté par q il l'est aussi par toute forme équivalente à q et réciproquement,

puisque la matrice $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ et son inverse sont toutes deux à coefficients entiers. Les formes appartenant à une même classe d'équivalence représentent donc les mêmes entiers, et on ne restreint pas la généralité du problème en ne considérant que les représentations par les formes réduites. Etant donnés un entier n et une forme réduite q_i, deux questions naturelles se posent : le problème d'existence d'une représentation de n par q_i, et en cas de réponse affirmative le problème de déterminer le nombre $R(n, q_i)$ de couples (x, y) qui définissent des représentations de n par q_i. Schématiquement on peut dire qu'on sait résoudre le premier problème mais pas le second. En revanche on sait calculer le nombre *total* de représentations de n par l'ensemble des formes réduites, c'est-à-dire le nombre

$$R(n) = \sum_{i=1}^{i=h(-p)} R(n, q_i).$$

Le résultat est d'une remarquable simplicité. Nous démontrerons le théorème suivant (on peut l'attribuer sans doute à Gauss, mais il ne sera énoncé sous cette forme que par Dirichlet) :

Théorème. *Soit p un nombre premier $\equiv 3 \pmod 4$, $p \neq 3$, et χ le caractère de Legendre $\pmod p$. Le nombre total de représentations d'un entier n par le système des formes réduites de discriminant $-p$ est donné par :*

$$R(n) = 2 \sum_{d|n} \chi(d).$$

Exemples : $p = 7$, $n = 4$, il n'y a qu'une forme réduite, et on trouve facilement que l'équation $4 = x^2 + xy + 2y^2$ possède 6 solutions, qui sont $(2,0)$, $(-2,0)$, $(1,1)$, $(-1,-1)$, $(-2,1)$, $(2,-1)$, or on a bien $2(\chi(1) + \chi(2) + \chi(4)) = 6$.

$p = 23$, $n = 6$, l'équation $6 = x^2 + xy + 6y^2$ possède 4 solutions : $(0,1)$, $(0,-1)$, $(-1,1)$, $(1,-1)$, l'équation $6 = 2x^2 + xy + 3y^2$ possède 2 solutions $(1,1)$, $(-1,-1)$, et la troisième équation également 2 solutions, d'où en tout 8 solutions, or $2(\chi(1) + \chi(2) + \chi(3) + \chi(6)) = 8$.

Les paragraphes 6 et 7 sont consacrés à la démonstration de ce théorème selon une méthode classique directement inspirée des travaux de Gauss ([G][L]). Les paragraphes 8 et 9 font ensuite une traduction analytique du théorème via les séries de Lambert et les fonctions thêta.

6.— Dénombrement des représentations primitives

Examinons comment collectionner des entiers représentés par une forme réduite donnée $q_i(x, y) = a_i x^2 + b_i xy + c_i y^2$. Il est clair que a_i fait partie de ces entiers (on fait $x = 1$ et $y = 0$), de même que

les premiers coefficients de toutes les formes équivalentes à q_i. Plus précisément si $q(x,y) = ax^2 + bxy + cy^2$ est équivalente à q_i, il existe une matrice unimodulaire $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ telle que $q(x,y) = q_i(\alpha x + \beta y, \gamma x + \delta y)$, d'où $a = q(1,0) = q_i(\alpha,\gamma)$. Notons que α et γ sont premiers entre eux, car $\alpha\delta - \beta\gamma = 1$. On dit alors que $q_i(\alpha,\gamma)$ est une représentation *primitive* de a par q_i. Nous allons voir qu'on obtient ainsi tous les entiers qui possèdent une représentation primitive par q_i. En globalisant à l'ensemble des formes réduites, on a le théorème de dénombrement suivant :

Théorème [Gauss]. *Soit un nombre premier $p \equiv 3 \pmod 4$, $p \neq 3$, et soit n un entier ≥ 1. Alors les définitions suivantes du nombre $r(n)$ sont équivalentes :*

(a) *$r(n)$ est le nombre total de représentations primitives de n, c'est-à-dire de triplets (q_i,α,γ) tels que $n = q_i(\alpha,\gamma)$, où q_i est une forme réduite, et α,γ sont deux entiers relatifs premiers entre eux*

(b) *$r(n)$ est le nombre de formes quadratiques $q(x,y) = ax^2 + bxy + cy^2$ telles que $a = n$, $-2n < b < 2n$, et $b^2 - 4ac = -p$*

(c) *$r(n)$ est le nombre de solutions x dans $(\mathbb{Z}/4n\mathbb{Z})$ de l'équation $x^2 \equiv -p$.*

Précisons d'abord que deux entiers relatifs α et γ sont dits premiers entre eux s'il existe β et δ tels que $\alpha\delta - \beta\gamma = 1$. Donc, 1 et 0 par exemple sont premiers entre eux. D'autre part, on considère dans le dénombrement les représentations $n = q_i(\alpha,\gamma)$ et $n = q_i(-\alpha,-\gamma)$ comme distinctes, on dit qu'elles sont associées.

Partons de deux représentations primitives associées : $n = q_i(\alpha,\gamma) = q_i(-\alpha,-\gamma)$. D'après le théorème de Bezout, il existe β et δ tels que $\alpha\delta - \beta\gamma = 1$. Posons $q(x,y) = q_i(\alpha x + \beta y, \gamma x + \delta y)$. Il est clair que le premier coefficient de la forme q n'est autre que n, puisque $q(1,0) = q_i(\alpha,\gamma)$. Comme il existe une infinité de choix de (β,δ), il existe une infinité de formes q répondant à la question. Montrons cependant qu'il en existe une et une seule dont le deuxième coefficient b vérifie $0 \leq b \leq 2n-1$. Pour cela nous devons comparer b à b', deuxième coefficient d'une forme q' obtenue à l'aide d'un autre choix (β',δ'). Or nous savons que ces choix distincts de coefficients de Bezout sont liés par les relations suivantes :

$$\beta - \beta' = k\alpha, \quad \delta - \delta' = k\gamma,$$

où k est un entier relatif arbitraire. On a donc successivement :

$$\begin{aligned}
q(x,y) &= a_i(\alpha x + \beta y)^2 + b_i(\alpha x + \beta y)(\gamma x + \delta y) + c_i(\gamma x + \delta y)^2\\
b &= 2a_i\alpha\beta + b_i(\alpha\delta + \beta\gamma) + 2c_i\gamma\delta\\
b' &= 2a_i\alpha\beta' + b_i(\alpha\delta' + \beta'\gamma) + 2c_i\gamma\delta'\\
b - b' &= 2a_ik\alpha^2 + 2b_ik\alpha\gamma + 2c_ik\gamma^2\\
b - b' &= 2kn.
\end{aligned}$$

Il existe donc une valeur et une seule de k pour laquelle $1 \leq b \leq 2n-1$ (car $b \neq 0$). La valeur de b étant déterminée, celle de c est tirée de l'équation $b^2 - 4nc = -p$. Nous avons donc défini une application qui à une paire de représentations primitives associées de n fait correspondre une forme q de discriminant $-p$ telle que $a = n$ et $1 \leq b \leq 2n-1$. Cette application est surjective puisque toute forme q est équivalente à une forme réduite q_i, et elle est injective d'après la propriété (iii) des formes réduites (unicité de q_i et unicité de la matrice unimodulaire au signe près). Les deux ensembles sont donc en bijection, et on double le cardinal de chacun d'eux en considérant d'un coté le nombre de représentations primitives de n, de l'autre en adjoignant les formes où b est changé en $-b$, c'est-à-dire en transformant l'inégalité en $-2n < b < 2n$. En résumé, b satisfait

$$b^2 = -p + 4nc \qquad \text{et} \qquad -2n < b < 2n.$$

Il est clair que l'application $b \mapsto x$ qui à b associe sa classe x dans l'anneau $\mathbb{Z}/4n\mathbb{Z}$ est une bijection sur l'ensemble des solutions de $x^2 \equiv -p \pmod{4n}$, car la connaissance de x détermine celle de b, et par suite celle de la forme q. Ceci achève la démonstration du théorème.

A présent nous allons calculer ce nombre $r(n)$ en fonction du caractère de Legendre χ modulo p.

Théorème. *Sous les mêmes hypothèses que le théorème précédent, on a :*
— *si p^2 divise n, $r(n) = 0$*
— *si p^2 ne divise pas n, $r(n)$ est donné par la formule :*

$$\frac{1}{2}r(n) = \prod_{q \text{ premier } | n} (1 + \chi(q)).$$

Nous allons d'abord montrer que $r_1(n) = \frac{1}{2}r(n)$ est une fonction multiplicative de n, puis l'évaluer sur les composantes primaires de n.

Or on sait classiquement que le nombre $\rho(n)$ de solutions d'une équation $x^2 = a$ dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ est une fonction multiplicative de n, c'est-à-dire que si m et n sont premiers entre eux on a $\rho(mn) = \rho(m)\rho(n)$. Cela résulte du théorème dit des restes chinois qui construit une bijection entre les solutions z de l'équation dans $\mathbb{Z}/mn\mathbb{Z}$ et les couples (x, y), où x et y sont respectivement des solutions dans $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$.

Nous désignons donc par $\rho(n)$ le nombre de solutions de

$$x^2 \equiv -p \pmod{n} \quad (x \in \mathbb{Z}/n\mathbb{Z}),$$

et commençons par évaluer $\rho(4)$, $\rho(8)$, $\rho(16)$ etc.

Les solutions de l'équation ne peuvent provenir que de congruences x impaires, or il est facile de vérifier que les carrés impairs sont congrus à 1

(mod 4), à 1 (mod 8), à 1 et 9 (mod 16), à 1, 9, 17 et 25 (mod 32) etc. Par suite on a toujours :

$$\rho(4) = 2.$$

En revanche :

$$p \equiv 7 \pmod 8 \Rightarrow -p \equiv 1 \pmod 8 \Rightarrow \rho(8) = \rho(16) = \rho(32) = \cdots = 4,$$

$$p \equiv 3 \pmod 8 \Rightarrow -p \equiv 5 \pmod 8 \Rightarrow \rho(8) = \rho(16) = \rho(32) = \cdots = 0.$$

D'après la définition (c) du théorème précédent, on a $r_1(n) = \frac{1}{2}\rho(4n)$. Montrons à présent que r_1 est multiplicative. Soient m et n premiers entre eux. L'un des deux au moins est impair, par exemple m, de ce fait 4 est premier avec m, et m est premier avec $4n$. D'où successivement,

$$\begin{aligned} r_1(mn) &= \frac{1}{2}\rho(4mn) \\ &= \frac{1}{2}\rho(m)\rho(4n) \\ &= \rho(m)r_1(n) \\ &= \frac{1}{2}\rho(4)\rho(m)r_1(n) \\ &= \frac{1}{2}\rho(4m)r_1(n) \\ &= r_1(m)r_1(n). \end{aligned}$$

A présent nous allons établir que si q est un nombre premier distinct de p, alors $r_1(q^k) = 1 + \chi(q)$, où $k \geq 1$.

Examinons séparément le cas $q = 2$. D'après le calcul ci-dessus,

$$p \equiv 7 \pmod 8 \implies r_1(2^k) = \frac{1}{2}\rho(2^{k+2}) = 2,$$

$$p \equiv 3 \pmod 8 \implies r_1(2^k) = \frac{1}{2}\rho(2^{k+2}) = 0,$$

d'où, d'après ce que nous avons vu au paragraphe 1, $r_1(2^k) = 1 + \chi(2)$.

Soit à présent q un nombre premier impair ($q \neq p$). On a donc $r_1(q^k) = \rho(q^k)$. Montrons d'abord que $\rho(q) = 1 + \chi(q)$. Or l'équation $x^2 \equiv -p \pmod q$ a des solutions si et seulement si $-p$ est résidu quadratique (mod q), et il y a alors deux solutions opposées x_0 et $-x_0$. Or d'après la loi de réciprocité quadratique,

$$q \equiv 1 \pmod 4 \implies \left(\frac{-p}{q}\right) = \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \chi(q),$$

$$q \equiv 3 \pmod 4 \implies \left(\frac{-p}{q}\right) = -\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \chi(q),$$

donc le nombre de solution est bien égal à $1 + \chi(q)$.

Considérons maintenant les solutions de l'équation $x^2 \equiv -p \pmod{q^k}$. Elles fournissent des solutions de l'équation avec $k = 1$ par réduction (mod q). Donc si $\chi(q) = -1$, il n'y a pas de solution. Supposons au contraire que $\chi(q) = 1$, c'est-à-dire que $-p$ soit résidu modulo q. Nous allons montrer que l'équation possède alors deux solutions. Les solutions x, si elles existent, sont à rechercher dans l'ensemble Φ des éléments de l'anneau $\mathbb{Z}/q^k\mathbb{Z}$ qui sont premiers avec q, ensemble qui a pour cardinal $q^k - q^{k-1}$. Désignons par Φ^+ le sous-ensemble de Φ constitué des éléments qui, lorsqu'on les réduit (mod q), donnent des résidus quadratiques (mod q). Le cardinal de Φ^+ est $\frac{1}{2}(q^k - q^{k-1})$. D'autre part l'application $x \mapsto x^2$ envoie Φ dans Φ^+. Si nous démontrons que tout élément de Φ^+ possède au plus deux antécédents par cette application, il est clair que nous aurons prouvé à la fois la surjectivité de cette application, et le fait que tout élément de Φ^+, en particulier $-p$, possède exactement deux antécédents, ce que nous voulions démontrer. Soient donc x et y deux éléments de Φ tels que $x^2 \equiv y^2 \pmod{q^k}$. L'entier q^k divise $x^2 - y^2 = (x - y)(x + y)$, et en fait q^k divise l'un ou l'autre des facteurs, car sinon q diviserait les deux facteurs, donc leur somme $2x$, donc x, ce qui est absurde. Donc x et y sont égaux ou opposés dans l'anneau, ce qu'il fallait démontrer.

Il ne reste plus qu'à envisager le cas où $q = p$. Il est clair que $r_1(p) = \rho(p) = 1 + \chi(p) = 1$, car l'équation $x^2 \equiv -p \equiv 0 \pmod{p}$ a une solution unique. En revanche, si $k \geq 2$, $r_1(p^k) = \rho(p^k) = 0$, car l'équation $x^2 \equiv -p \pmod{p^k}$ n'a pas de solution (une solution x serait multiple de p, donc x^2 serait multiple de p^2 ce qui est absurde). Ceci achève la démonstration du théorème.

7.— Dénombrement des représentations quelconques

Nous sommes à présent en mesure d'achever la démonstration de l'identité

$$R(n) = 2\sum_{d|n} \chi(d) \qquad (n \geq 1) \tag{1}$$

Notons d'abord que la formule démontrée pour $r(n)$ s'écrit de façon très similaire, puisqu'en développant le produit on obtient, pourvu que p^2 ne divise pas n,

$$r(n) = 2\sum_{f|n} \chi(f)$$

où la somme s'étend aux diviseurs f qui sont *sans facteurs carrés* (produits de nombres premiers distincts).

Soit n un entier ≥ 1 et $n = q_i(x, y)$ une représentation de cet entier, non nécessairement primitive, par une forme réduite q_i. Si d est le pgcd de x et de y, il est clair que d^2 divise n, et que $n/d^2 = q_i(x/d, y/d)$ est une représentation primitive de n/d^2. Réciproquement à toute représentation primitive de n/dr correspond une unique représentation de n. D'où la formule suivante, où la somme est effectuée sur les diviseurs carrés de n :

$$R(n) = \sum_{d^2|n} r(n/d^2) \qquad (n \geq 1) \tag{2}$$

Nous supposerons d'abord que p^2 ne divise pas n, donc aucun de ses diviseurs. Cela se réécrit

$$\begin{aligned} R(n) &= \sum_{d^2|n} 2 \sum_{f|(n/d^2)} \chi(f) \\ &= 2 \sum_{d^2|n} \sum_{fd^2|n} \chi(f) \\ &= 2 \sum_{e|n} \chi(e) \end{aligned}$$

car tout entier (en l'occurrence tout diviseur e de n) s'écrit d'une manière et d'une seule comme le produit d'un carré et d'un nombre sans facteur carré.

Il nous reste à démontrer que la formule (1) est encore valide quand p^2 divise n. Alors n s'écrit $n = p^{2k}n'$, où p^2 ne divise pas n' et $k \geq 1$. Montrons sur la formule (2) que $R(n) = R(n')$. Tout diviseur carré d^2 de n s'écrit $d^2 = p^{2l}d'^2$, où p ne divise pas d'. Par suite, $n/d^2 = p^{2k-2l}(n'/d'^2)$. Pour tout diviseur carré d^2 tel que $l < k$, on aura $r(n/d^2) = 0$. Dans l'identité (2) on peut donc restreindre la somme aux d^2 pour lesquels $l = k$, d'où $R(n) = R(n')$. Or la formule (1) est valide pour n', et il est clair sur cette formule qu'on peut restreindre la sommation aux diviseurs d de n' non multiple de p (pour les autres, $\chi(d) = 0$). Dans ces conditions cette même formule appliquée à n donne le même résultat, elle est donc valide pour n.

8.— Série thêta associée

Pour traduire la relation obtenue entre fonctions arithmétiques multiplicatives en termes de séries génératrices, on a le choix entre les séries de Dirichlet et les q-séries. C'est ce second point de vue que nous adopterons. Dans la suite, q désigne selon le contexte soit une variable formelle, soit un nombre réel tel que $|q| < 1$ (et non une forme quadratique, non plus qu'un nombre premier comme dans le paragraphe 6...). A toute forme réduite

$a_i x^2 + b_i xy + c_i y^2$ on associe la série-double

$$\theta_i(q) = \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}} q^{a_i m^2 + b_i mn + c_i n^2}.$$

En sommant sur toutes les formes réduites on introduit donc la série génératrice du nombre $R(n)$:

$$\Theta(q) = \sum_{i=1}^{i=h(-p)} \theta_i(q)$$

$$\Theta(q) = h(-p) + \sum_{n\geq 1} R(n) q^n$$

$$\Theta(q) = h(-p) + 2\sum_{n\geq 1} \chi(n) \frac{q^n}{1-q^n},$$

la dernière identité n'étant que la traduction à l'aide d'une série de Lambert de la relation entre les fonctions arithmétiques R et χ.

Exemples avec $p = 7$ et $p = 23$:

$$\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}} q^{m^2+mn+2n^2} = 1 + 2\Big(\frac{q}{1-q} + \frac{q^2}{1-q^2} - \frac{q^3}{1-q^3} + \frac{q^4}{1-q^4} - \cdots\Big)$$

$$\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}} (q^{m^2+mn+6n^2} + 2q^{2m^2+mn+3n^2})$$

$$= 3 + 2\Big(\frac{q}{1-q} + \frac{q^2}{1-q^2} + \frac{q^3}{1-q^3} + \frac{q^4}{1-q^4} - \frac{q^5}{1-q^5} + \frac{q^6}{1-q^6} - \cdots\Big)$$

On notera que dans le cas $p = 23$ on a $\theta_2(q) = \theta_3(q)$ puisqu'on passe de la deuxième forme $2m^2 + mn + 3m^2$ à la troisième $2m^2 - mn + 3m^2$ en changeant (m, n) en $(-m, n)$. Au sujet de cet exemple, signalons une identité dans le genre de celles qu'alignait Ramanujan dans ses papiers ([R], p. 353-357), mais dont la démonstration ([S2]) sort des limites de notre article :

$$\theta_1(q) - \theta_2(q) = 2q \prod_{n\geq 1} (1-q^n)(1-q^{23n}).$$

Pour faire apparaître la série de Lambert tordue du procédé de sommabilité (L'), nous observons que

$$\frac{2q^n}{1+q^n} = \frac{2q^n}{1-q^n} - \frac{4q^{2n}}{1-q^{2n}}$$

d'où l'on tire immédiatement :

$$\sum_{n\geq 1}\chi(n)\frac{2q^n}{1+q^n} = h(-p) + \Theta(q) - 2\Theta(q^2).$$

Pour démontrer l'égalité $h = h(-p)$, nous sommes donc ramenés à démontrer que $\lim_{q\to 1^-}(\Theta(q) - 2\Theta(q^2)) = 0$, et pour cela il nous faut étudier le développement asymptotique de $\Theta(q)$ au voisinage de 1.

9.— Preuve de l'égalité $h = h(-p)$

Nous allons d'abord obtenir sans difficulté l'équivalent :

$$\Theta(q) \sim \frac{2\pi h(-p)}{\sqrt{p}}\frac{1}{1-q} \qquad (q \to 1^-).$$

Ce résultat s'obtient par un raisonnement géométrique, en notant que pour chaque forme réduite, l'ellipse $a_i x^2 + b_i xy + c_i y^2 \leq 1$ a pour aire $2\pi/\sqrt{p}$, par suite l'ellipse homothétique $a_i x^2 + b_i xy + c_i y^2 \leq n$ a pour aire $2n\pi/\sqrt{p}$, d'où, en comptant les points à coordonnées entières dans les $h(-p)$ ellipses, l'équivalent

$$R(1) + R(2) + \cdots + R(n) \sim \frac{2n\pi h(-p)}{\sqrt{p}}.$$

Mais cela signifie que la suite $R(n)$ tend en moyennes de Cesàro vers $2\pi h(-p)/\sqrt{p}$, d'où le résultat d'après l'implication $(C) \Rightarrow (A)$ signalée au paragraphe 4.

Pour obtenir le résultat escompté cela s'avère insuffisant, nous avons besoin du terme suivant du développement asymptotique, que nous obtiendrons en ayant recours à *l'équation fonctionnelle* de la fonction Θ, laquelle s'obtient classiquement en utilisant la formule sommatoire de Poisson à deux dimensions. Posons

$$q = e^{-\frac{2\pi t}{\sqrt{p}}}, \qquad q' = e^{-\frac{2\pi}{\sqrt{p}t}},$$

où t est donc réel > 0. Si l'on définit la fonction ϑ par $\vartheta(t) = \Theta(q)$, l'équation fonctionnelle s'écrit simplement $\vartheta(t) = (1/t)\vartheta(1/t)$, d'où pour la fonction Θ :

$$\Theta(q) = \frac{2\pi}{\sqrt{p}}\frac{1}{\log(1/q)}\Theta(q').$$

Or quand $q \to 1^-$, alors $t \to 0^+$, par suite $q' \to 0^+$, et le développement asymptotique de $\Theta(q')$ commence simplement par :

$$\Theta(q') = h(-p) + 2q' + o(q').$$

Or on a :

$$q' = e^{-\frac{4\pi^2}{p}\frac{1}{\log(1/q)}}$$

d'où $q' = o((1-q)^n)$ pour tout $n \geq 1$, et donc aussi :

$$\Theta(q) = \frac{2\pi h(-p)}{\sqrt{p}}\frac{1}{\log(1/q)} + o(1-q)^n,$$

et il est maintenant clair que $\Theta(q) - 2\Theta(q^2) = o(1)$, ce qui achève la démonstration de l'égalité $h = h(-p)$.

Une autre conséquence du développement asymptotique de Θ est le résultat suivant :

$$\lim_{q\to 1^-} \sum_{n\geq 1} \frac{\chi(n)}{n}\frac{nq^n}{1-q^n} = \lim_{q\to 1^-} \frac{1}{2}(1-q)\Theta(q) = \frac{\pi h(-p)}{\sqrt{p}}.$$

Or cela signifie que la série $\sum \chi(n)/n$ est sommable au sens de Lambert (L), avec pour somme le second membre. Or cette série est convergente, car plus généralement la série de Dirichlet $L(s) = \sum \chi(n)/n^s$ converge dans le demi-plan $Re(s) > 0$ du seul fait que les sommes partielles h_n sont bornées. Le procédé de Lambert étant régulier, on a donc :

$$L(1) = \sum_{n\geq 1} \frac{\chi(n)}{n} = \frac{\pi h(-p)}{\sqrt{p}}.$$

Exemples ($p = 7$ et $p = 23$) :

$$1 + \frac{1}{2} - \frac{1}{3} + \frac{1}{4} - \frac{1}{5} - \frac{1}{6} + \frac{1}{8} + \frac{1}{9} - \frac{1}{10} + \frac{1}{11} - \frac{1}{12} - \frac{1}{13} + \cdots = \frac{\pi}{\sqrt{7}}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} - \frac{1}{7} + \frac{1}{8} + \frac{1}{9} - \frac{1}{10} + \frac{1}{11} + \frac{1}{12} + \cdots = \frac{3\pi}{\sqrt{23}}$$

Remarque : On peut répartir en gros les démonstrations habituelles de la positivité de la hauteur H en deux catégories, selon qu'elles font ou non appel explicitement au nombre de classes $h(-p)$ (cf.[B],[M] etc...). On peut néanmoins noter que dans les deux cas elles utilisent comme étape essentielle le calcul des sommes des séries ci-dessus (et le fait que ces sommes sont positives). Dans notre présentation le point essentiel est l'identité $L(0) = h = h(-p)$, et non pas $L(1) = \pi h(-p)/\sqrt{p}$. Il est vrai que ces deux identités sont le reflet l'une de l'autre par l'équation fonctionnelle de la fonction L.

10.— Autres discriminants

La théorie de la réduction des formes quadratiques ne se limite nullement à des discriminants $\Delta = -d$, où d est un nombre premier congru à 3 (mod 4) et au moins égal à 7 (cf. [L][O]). Nous nous bornerons ici à signaler les identités qu'on trouve dans les deux cas particuliers les plus importants : $\Delta = -4$ et $\Delta = -3$:

$$\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}} q^{m^2+n^2} = 1 + 4\Big(\frac{q}{1-q} - \frac{q^3}{1-q^3} + \frac{q^5}{1-q^5} - \frac{q^7}{1-q^7} - \cdots\Big)$$

$$\sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}} q^{m^2+mn+n^2} = 1 + 6\Big(\frac{q}{1-q} - \frac{q^2}{1-q^2} + \frac{q^4}{1-q^4} - \frac{q^5}{1-q^5} + \cdots\Big)$$

La première de ces deux identités est le célèbre théorème de Jacobi sur le nombre de représentations d'un entier comme somme de deux carrés. Dans la seconde identité, le caractère est le caractère de Legendre modulo 3. Les coefficients 4 et 6 qui apparaissent en facteurs expriment le fait que les formes quadratiques $x^2 + y^2$ et $x^2 + xy + y^2$ ont respectivement 4 et 6 automorphismes. Par suite toute forme quadratique de discriminant -4 (resp. -3) s'envoie sur la première (resp. la seconde) à l'aide de 4 (resp. 6) changements de variables unimodulaires, au lieu de 2 comme pour les formes de discriminant $-p$ que nous avons considéré dans cet article.

BIBLIOGRAPHIE

[A] Andrews (G.). — EUREKA! num $=\Delta+\Delta+\Delta$, *Jour. of Number Theory* , t. **23**, 1986, p. 215–293.

[B] Berndt (B.). — Periodic Bernoulli Numbers, Summation Formulas and Applications, in "Theory and Applications of special Functions"', *ed. Askey, Acad. Press*, t. , 1975, p. 143–189.

[C] Cartier (P.). — Sur une généralisation des symboles de Legendre-Jacobi, *Ens. Math.*, t. **16**, 1970, p. 31–48.

[D] Dirichlet (L.). — Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des nombres, *J. Reine Angew.*, t. **19**, 1839, p. 324–369.

[G] Gauss (C.F.). — Disquisitiones Arithmeticae.

[H1] Hardy (G.H.). — *Divergent series.* — Oxford, Clarendon Press—1949.

[H2] Hardy (G.H.). — Some theorems concerning infinite series, *Math. Annalen*, t. **64**, 1907, p. 77–94.

[J] Jacobi . — Observatio arithmetica de numero classium divisorum quadraticorum formae $yy+Azz$, designante A numerum primum formae $4n+3$, *J. Reine Angew.*, t. **9**, 1834, p. 189–192.

[L] Landau (E.). — *Vorlesungen uber Zahlentheorie.* — ed. Hirzel, Leipzig—1927.

[M] Moser (L.). — A theorem on quadratic residues, *Proc. Amer. Math. Soc.*, t. **2**, 1951, p. 503–504.

[O] OESTERLE (J.). — Le problème de Gauss sur le nombre de classes, *Ens. Math.*, t. **34**, 1988, p. 43-67.
[R] RAMANUJAN (S.). — *The lost notebook and other unpublished papers.* — Springer Verlag—1988.
[S1] SERRE (J.P.). — *Cours d'Arithmétique.* — P.U.F., Paris—1969.
[S2] SERRE (J.P.). — Modular forms and Galois representations, in Algebraic number fields, *Proc. Symp. LMS London, ed. Frhlich, Acad. Press*, t. , 1977, p. .
[W] WEIL (A.). — Sur les sommes de trois et quatre carrés, *Ens. Math.*, t. **20**, 1974, p. 215–222.

Dominique DUMONT
Département de Mathématiques
7, Rue René-Descartes
67084 Srasbourg Cedex