MATH. SCAND. 1 (1953)

SUR LE LEMME DE ZOLOTAREFF ET SUR LA LOI DE RÉCIPROCITÉ DES RESTES QUADRATIQUES

MARCEL RIESZ

Sommaire. Le but principal du présent travail est de donner une démonstration du lemme de Zolotareff qui ne sort pas du domaine des congruences quadratiques. On y arrive en écrivant la permutation considérée par Zolotareff comme produit de deux involutions (nos 2—3). Aux nos 4—5 on démontre que les symboles de Zolotareff et de Gauss sont identiques. Au no 6 on donne une variante de la troisième démonstration de Gauss. Aux nos 7—9 on montre de deux manières que, dans le cas d'un module composé impair, les symboles de Zolotareff et de Gauss sont identiques au symbole de Jacobi.

Introduction. Gauss, qui a été le premier à démontrer la loi de réciprocité des restes quadratiques, a donné en tout huit démonstrations de cette loi. La première de ces démonstrations, qui procède par induction, porte l'empreinte du génie de Gauss, mais est assez pénible à cause de la multitude des cas qu'il faut distinguer. Elle fut notablement simplifiée par Dirichlet [2] dans un mémoire paru en 1854, où Dirichlet insiste sur le caractère exceptionnel de cette démonstration dans les termes suivants (traduits de l'allemand).

« Parmi les nombreuses démonstrations de la loi de réciprocité, la première démonstration de Gauss, trouvée déjà en 1796 et insérée aux *Disquisitiones arithmeticae* (1801), m'a toujours paru particulièrement remarquable, non seulement à cause de l'idée tellement simple qui lui sert de base, mais encore parce que cette démonstration est la seule, que je sache, qui ne sort nulle part du domaine des congruences du second degré, auquel le théorème appartient lui-même, tandis que toutes les autres démonstrations connues reposent sur des principes qui paraissent plus ou moins étrangers au domaine en question. »

Kronecker [5] a appuyé sur le même point en 1876.

Un certain nombre des démonstrations auxquelles Dirichlet fait allusion, sont basées sur des méthodes transcendantes, ainsi deux démonstra-

Reçu le 25 mars 1953.

tions dues à Gauss et une démonstration très connue, due à Eisenstein. Cependant, la grande majorité des démonstrations en question reposent sur un théorème, appelé *lemme de Gauss*, primitivement point de départ de la démonstration la plus connue de Gauss, la troisième (1808). Gauss déduit ce lemme du *critère d'Euler*, qui, aussi simple qu'il soit, fait appel à une congruence d'ordre supérieur. Il en est de même de la démonstration, fondée sur la théorie des indices, du *lemme* extrêmement élégant *de Zolotareff* (1872) [8]. D'autre part, les deux lemmes résultent sur le champ l'un de l'autre, le passage ne faisant intervenir aucun élément étranger au problème.

Notre but primaire est de donner une démonstration du lemme de Zolotareff qui reste dans le cadre des congruences quadratiques. Aux nos 2—3 on montre que le symbole de Zolotareff est identique au symbole de Legendre quand le module est un nombre premier (impair), aux nos 4—5 on établit l'identité des symboles de Zolotareff et de Gauss, au no 6 on donne une variante de la troisième démonstration de Gauss, conduisant à la loi de réciprocité par l'intermédiaire d'une très belle formule due à Kronecker [5] et répondant aux desiderata de Dirichlet.

Dans la plupart de ces considérations on envisage aussi le cas des modules composés (impairs). Aux nos 7—9 on trouve deux démonstations du fait que, dans le cas généralisé, les symboles de Zolotareff et de Gauss sont identiques au symbole de Jacobi.

Ce qu'il y a de nouveau dans ce travail se restreint à la matière exposée aux nos 2, 3, 8. Le reste n'est que compilation, qui pourtant, je l'espère, pourra rendre quelques services au lecteur.

1. *Le lemme de Zolotareff* consiste en ceci.

Soit p un nombre premier impair et D un nombre entier non divisible par p. Les plus petits restes positifs des nombres

$$D, 2D, \ldots, (p-1)D \tag{1}$$

par rapport à p forment évidemment une permutation des nombres

$$1, 2, \ldots, p-1\,. \tag{2}$$

Suivant que cette permutation est paire ou impaire, D est reste quadratique ou non-reste quadratique par rapport à p.

2. Considérons dans un ordre d'idées plus général m éléments $u_1, u_2, \ldots, u_m$ et une permutation $v_1, v_2, \ldots, v_m$ de ces éléments. Posons $v_k = Tu_k$ ou, plus brièvement, $v = Tu$ et sgn $T = +1$ ou sgn $T = -1$ suivant que T est une permutation paire ou impaire ou, en d'autres ter-

mes, suivant que la transformation $u \to Tu$ conserve ou ne conserve pas la classe des permutations auxquelles on l'applique. Il est très facile de alcculer sgn T, dans le cas où T est une involution, ce qui veut dire que $T^{-1} = T$. Chaque cycle d'une telle permutation est constitué par un élément fixe $w \to w$ ou par une transposition $u \longleftrightarrow v$ $(u \neq v)$. Soient α le nombre des éléments fixes et β le nombre des transpositions. On a évidemment $\alpha + 2\beta = m$ et

$$\operatorname{sgn} T = (-1)^{\beta} = (-1)^{\frac{m-\alpha}{2}}.$$

Soient maintenant T' et T'' deux involutions et $T'T''$ leur produit, ce qui veut dire que $(T'T'')u = T'(T''u)$. On a manifestement $\operatorname{sgn}(T'T'') = \operatorname{sgn} T' \cdot \operatorname{sgn} T''$ et alors, dans des notations évidentes,

$$\operatorname{sgn}(T'T'') = (-1)^{m-\frac{\alpha'+\alpha''}{2}}.$$

En admettant encore que m est un nombre *pair*, hypothèse toujours remplie dans les cas particuliers qui suivent, on aura

$$\operatorname{sgn}(T'T'') = (-1)^{\frac{\alpha'+\alpha''}{2}}. \tag{3}$$

3. La transformation Z_D, qui consiste en ce que $u \to$ le plus petit reste positif de Du modulo p, n'est pas en général une involution (elle ne l'est que pour $D \equiv \pm 1$), mais elle peut toujours s'écrire comme le *produit de deux involutions* très simples.

u étant un élément quelconque de la suite (2), la congruence $uu' \equiv D \pmod{p}$ a une solution et une seule u' qui appartient à (2) elle aussi. Nous désignons cette solution par D/u et nous posons $D/u = T_D u$. Dans le cas particulier où $D = 1$ cela devient $1/u = T_1 u$. Il est clair que $Z_D = T_D T_1$ (d'une manière symbolique $Du = D/(1/u)$). Le nombre des éléments fixes de T_D étant désigné par α_D, on a d'après (3)

$$\operatorname{sgn} Z_D = (-1)^{\frac{\alpha_D+\alpha_1}{2}}. \tag{4}$$

Reste à calculer le dernier exposant, c'est-à-dire les nombres des éléments fixes de T_D et de T_1. Si D est reste quadratique mod. p, la congruence $x^2 \equiv D \pmod{p}$ aura deux solutions (mod. p) soit x et $p-x \not\equiv x$, et on a $\alpha_D = 2$, tandis que $\alpha_D = 0$ dans le cas où D est non-reste. Le nombre $D = 1$ est toujours reste (les deux solutions de $x^2 \equiv 1$ étant 1 et $p-1$). On a donc $\alpha_1 = 2$. L'exposant sera par suite $= 2$ quand D est reste et $= 1$ quand D est non-reste. Moyennant le *symbole de Legendre* (D/p) qui, *par définition*, est $= 1$ quand D est reste et $= -1$ quand D est non-reste quadratique suivant p, notre résultat peut s'écrire

$$\operatorname{sgn} Z_D = \left(\frac{D}{p}\right). \qquad \text{C.Q.F.D.}$$

En introduisant encore le symbole de Zolotareff $(D/p)_Z = \operatorname{sgn} Z_D$ et en désignant, pour plus de netteté, le symbole de Legendre par $(D/p)_L$, le résultat ci-dessus peut s'exprimer par la formule

$$\left(\frac{D}{p}\right)_L = \left(\frac{D}{p}\right)_Z, \tag{5}$$

valable dans les conditions posées, savoir que p est un nombre premier impair et que le nombre entier D n'est pas divisible par p. (D'ailleurs le résultat subsiste pour $p = 2$, mais il devient trivial.)

REMARQUE I. Il résulte de la définition même du symbole de Zolotareff que ce symbole est un caractère du groupe multiplicatif mod. p c'est-à-dire que

$$\left(\frac{D_1 D_2}{p}\right)_Z = \left(\frac{D_1}{p}\right)_Z \left(\frac{D_2}{p}\right)_Z. \tag{6}$$

Frobenius [4] a fortement insisté sur ce point au début d'une analyse pénétrante des diverses démonstrations de la loi de réciprocité.

REMARQUE II. Il est clair que la valeur du symbole de Zolotareff est conservée, si l'on remplace la suite (2) par une suite arbitraire $\{\alpha_k\}$ de $p-1$ nombres incongrus et $\not\equiv 0 \pmod{p}$, les plus petits restes positifs de la suite (1) suivant p étant remplacés en même temps par ceux des restes des nombres $\{D\alpha_k\}$ qui appartiennent à la suite $\{\alpha_k\}$.

On peut aussi opérer avec les classes de restes (classes d'équivalence) suivant p, former leurs produits, leurs permutations etc. Si l'on traduit les définitions et le résultat qui précèdent dans le langage de ces classes, on arrive à un énoncé très clair et très concis. Néanmoins la transcription en question sera laissée de côté dans ce qui suit.

4. La définition du symbole de Zolotareff s'étend facilement au cas où *le module p n'est plus nécessairement un nombre premier, mais D est premier avec p.* Pour arriver à des résultats intéressants, nous supposons en outre que *p est un nombre impair* (positif).

On a en effet dans ces conditions (*cf.* le premier alinéa de la *Remarque* II) que, les nombres $\{\alpha_k\}$, $k = 1, 2, \ldots, p-1$, étant incongrus entre eux suivant p et non divisibles par p, il en est de même des nombres $\{D\alpha_k\}$. Ceux des restes de ces nombres qui appartiennent à la suite $\{\alpha_k\}$ fournissent donc une permutation Z_D de ces derniers nombres. Le signe (signature) de cette permutation ne dépend que de p et de D. *On pose aussi dans les nouvelles conditions* $(D/p)_Z = \operatorname{sgn} Z_D$.

Ce qu'on perd dans ce cas généralisé, c'est le renseignement précis sur le caractère quadratique de D par rapport à p que le symbole fournissait dans le cas d'un module premier (*cf.* les nos 7—9, où on montre que le symbole généralisé est identique au symbole de Jacobi; *voir*, en particulier, la fin du no 7).

On va maintenant démontrer que les symboles de Zolotareff et de Gauss — tous les deux définis soit dans les conditions primitives soit dans les conditions généralisées — sont identiques.

5. Tandis que le symbole de Zolotareff se rattache à des systèmes complets de restes incongrus ($\not\equiv 0$), le symbole de Gauss se rattache à des demi-systèmes de restes, c'est-à-dire à des suites de $(p-1)/2$ nombres $\{x_j\}$ tels que les $p-1$ nombres $\{\pm x_j\}$ constituent un système complet. Un tel demi-système est fourni par l'ensemble

$$\{x\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}. \tag{7}$$

Par le *reste minimum* (en valeur absolue) d'un nombre w modulo p, on entend le nombre $\overline{w}$, unique puisque p est impair, tel que $\overline{w} \equiv w \pmod{p}$ et $|\overline{w}| \leqq (p-1)/2$. Le reste minimum d'un nombre quelconque non divisible par p appartient évidemment à l'ensemble $\{\pm x\}$. Nous notons encore la relation évidente $\overline{-w} = -\overline{w}$.

Le *symbole de Gauss* $(D/p)_G$ se définit de la manière suivante.

On fait parcourir à x la suite $\{x\}$, on désigne par μ *le nombre des restes minima des produits* Dx *qui sont négatifs* et on pose

$$\left(\frac{D}{p}\right)_G = (-1)^{\mu}. \tag{8}$$

Pour voir que ce symbole coïncide avec celui de Zolotareff, appliquons la transformation Z_D au système complet $\{x^*\} = \{\pm x\}$ écrit dans l'ordre naturel, c'est-à-dire que $x_1^* < x_2^*$ implique que x_1^* précède x_2^*. La transformation s'exprime par la formule $x^* \to \overline{Dx^*}$. On entend par une *inversion* une constellation telle que

$$u < v \text{ et } \overline{Du} > \overline{Dv}.$$

Si l'on pose $-u = u'$ et $-v = v'$, on aura en même temps l'inversion

$$v' < u' \text{ et } \overline{Dv'}(= -\overline{Dv}) > \overline{Du'}(= -\overline{Du}).$$

Si les couples (u, v) et (u', v') sont différents, les deux inversions se compensent en tant qu'il ne s'agit que de la classe de la permutation $x^* \to \overline{Dx^*}$. Dans le cas où les deux couples coïncident, les deux inversions simultanées se réduisent à une seule. On a évidemment dans ce cas $u = -v$ et

$v = -u$, $-v = u < v$ et $-\overline{Dv} = \overline{Du} > \overline{Dv}$, ce qui veut dire que v est positif et $\overline{Dv}$ négatif. Il y aura donc autant d'inversions non compensées qu'il y a des nombres $v > 0$ tels que $\overline{Dv} < 0$. Le nombre de ces inversions est donc égal au nombre μ introduit par Gauss et

$$\left(\frac{D}{p}\right)_Z = \operatorname{sgn} Z_D = (-1)^\mu = \left(\frac{D}{p}\right)_G . \tag{9}$$

REMARQUE III. Le fait que la valeur du symbole de Zolotareff est indépendante du système complet auquel on applique la transformation Z_D entraîne que la valeur du symbole de Gauss est indépendante du demi-système moyennant laquel on calcule cette valeur. D'une manière plus précise: Les nombres z_j étant les éléments d'un demi-système arbitraire $\{z_j\}$ et μ le nombre des produits Dz_j qui admettent des restes appartenant au demi-système complémentaire $\{-z_j\}$, la parité du nombre μ est indépendante du demi-système $\{z_j\}$. (Pour une autre démonstration de ce fait *voir* Scholz [7], p. 75.)

Retournons un instant au cas particulier d'un *module premier*. L'identité (9) combinée avec l'identité (5) nous fournit $(D/p)_L = (D/p)_G$. Cette dernière identité constitue le *lemme de Gauss*.

6. En nous plaçant de nouveau dans les conditions généralisées, nous allons déduire la loi de réciprocité relative au symbole de Gauss. Les nombres positifs p et q étant impairs et premiers entre eux, écrivons les suites

$$\{x\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\} \quad \text{et} \quad \{y\} = \left\{1, 2, \ldots, \frac{q-1}{2}\right\} . \tag{10}$$

Posons pour tout $x \in \{x\}$

$$qx = g_x p + r_x, \quad 0 < r_x < p , \tag{11}$$

c'est-à-dire que r_x est le plus petit reste positif de qx suivant p. On introduit aussi les restes minima (en valeur absolue) ϱ_x, en posant $\varrho_x = r_x$ ou $\varrho_x = r_x - p$ suivant que $r_x < p/2$ ou $r_x > p/2$. Les ϱ_x sont positifs dans le premier cas et négatifs dans le second. On a toujours $|\varrho_x| < p/2$ ou, ce qui revient au même, $|\varrho_x| \in \{x\}$.

Puisque p et q sont impairs, on obtient de (11), $x \equiv g_x + r_x \pmod 2$, ce qui peut aussi s'écrire

$$x \equiv g_x + \varrho_x \equiv g_x + |\varrho_x| \pmod 2 \quad \text{quand } \varrho_x > 0 \tag{12}$$

et

$$x \equiv g_x + p + \varrho_x \equiv g_x + |\varrho_x| + 1 \pmod 2 \quad \text{quand } \varrho_x < 0 . \tag{13}$$

Les $|\varrho_x|$ sont différents entre eux. On a en effet $\varrho_k \pm \varrho_l \equiv q(k \pm l) \pmod p$. Puisque q est premier avec p et que $k \pm l$ n'est pas divisible par p

si $k \neq l$ (vu que $k \in \{x\}, l \in \{x\}$), on a aussi $\varrho_k \pm \varrho_l \not\equiv 0 \pmod{p}$ et, à plus forte raison, $\varrho_k \pm \varrho_l \neq 0$. Il en résulte que l'ensemble des valeurs $|\varrho_x|$ est identique à l'ensemble $\{x\}$.

Ce point acquis, on voit que si x parcourt le système $\{x\}$, $|\varrho_x|$ en fera de même, ce qui donne $\Sigma_x |\varrho_x| = \Sigma_x x$. En désignant avec Gauss le nombre des ϱ_x négatifs par μ, on tire de (12) et de (13)

$$\sum_x g_x + \mu \equiv 0 \pmod{2} \text{ ou } \mu \equiv \sum_x g_x \pmod{2},$$

et, par conséquent,

$$\left(\frac{q}{p}\right)_G = (-1)^{\mu} = (-1)^{\Sigma_x g_x}.$$

Il résulte de la formule (11) que $g_x = [qx/p]$. Cela étant, on va donner une seconde interprétation de $\Sigma_x g_x$. En effet, si l'on fixe le nombre $x \in \{x\}$, l'expression $qx - py$ est évidemment positive pour $y = 1, 2, \ldots,$ $[qx/p]$, nombres qui appartiennent à $\{y\}$ $(qx/p < q \cdot \frac{1}{2}p/p = q/2)$, tandis que l'expression est négative pour tout autre $y \in \{y\}$. La somme $\Sigma_x g_x$ est donc égale au nombre des couples $x \in \{x\}, y \in \{y\}$ pour lesquels $qx - py > 0$ ou, ce qui revient au même, $y/q - x/p < 0$. On a ainsi établi la formule de Kronecker

$$\left(\frac{q}{p}\right)_G = \operatorname{sgn} \prod_{x,y} \left(\frac{y}{q} - \frac{x}{p}\right), \qquad x \in \{x\}, y \in \{y\}. \tag{14a}$$

Il vient par symétrie

$$\left(\frac{p}{q}\right)_G = \operatorname{sgn} \prod_{x,y} \left(\frac{x}{p} - \frac{y}{q}\right), \qquad x \in \{x\}, y \in \{y\}. \tag{14b}$$

Chacun des produits contient $((p-1)/2)((q-1)/2)$ facteurs. Ces facteurs ayant des signes opposés dans les deux produits, on obtient la loi de réciprocité

$$\left(\frac{q}{p}\right)_G \left(\frac{p}{q}\right)_G = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \tag{15}$$

Dans les formules ci-dessus on peut évidement substituer le symbole de Zolotareff à celui de Gauss. Dans le cas particulier, où *p et q sont des nombres premiers* (impairs), nos formules subsistent aussi pour le *symbole de Legendre*. La formule (15) exprime, dans ce cas particulier, *la loi de réciprocité proprement dite, relative à deux nombres premiers impairs*. Cette loi se présente ici avec une démonstration qui répond aux desiderata de Dirichlet.

7. Nous allons montrer que, dans le cas généralisé, les symboles de

Zolotareff et de Gauss, identiques entre eux, sont aussi identiques au symbole de Jacobi.

Soit n un nombre impair positif et D un nombre entier premier avec n. Il est clair que la *Remarque* I peut encore s'appliquer dans les conditions généralisées, c'est-à-dire que le symbole (soit de Zolotareff, soit de Gauss) (D/n) possède un caractère multiplicatif par rapport à D, savoir $(D_1D_2/n)=(D_1/n)(D_2/n)$. Or le symbole possède un caractère multiplicatif aussi par rapport à n, savoir

$$\left(\frac{D}{n_1n_2}\right)=\left(\frac{D}{n_1}\right)\left(\frac{D}{n_2}\right). \tag{16}$$

Pour le voir, posons $n_1n_2 = n$ et admettons d'abord que D aussi est un nombre impair positif. On a alors, en vertu de la loi de réciprocité et de la *Remarque* I,

$$\left(\frac{D}{n}\right)=(-1)^{\frac{D-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{D}\right)=(-1)^{\frac{D-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n_1}{D}\right)\left(\frac{n_2}{D}\right)=(-1)^N\left(\frac{D}{n_1}\right)\left(\frac{D}{n_2}\right),$$

avec

$$N=\frac{D-1}{2}\left(\frac{n_1n_2-1}{2}-\frac{n_1-1}{2}-\frac{n_2-1}{2}\right) \tag{17}$$

$$=\frac{D-1}{2}\,\frac{(n_1-1)(n_2-1)}{2}\equiv 0\ (\mathrm{mod.}\ 2),$$

ce qui entraîne (16) pour tout nombre impair positif D.

Pour aller plus loin, il nous faut calculer les valeurs explicites des symboles $(-1/n)$ et $(2/n)$. Quant au premier, on tire immédiatement de la définition du symbole de Gauss que

$$\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}.$$

Le symbole $(2/n)$ s'obtient facilement, si l'on observe que la transformation Z_2 appliquée à la suite $1, 2, \ldots, n-1$ produit $1+2+\ldots+(n-1)/2 = (n^2-1)/8$ inversions. On a donc

$$\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}.$$

Le calcul exécuté dans la formule (17) met en évidence que la relation (16) est valide pour $D = -1$. Si l'on observe encore que le carré $(4k\pm1)^2$ de tout nombre impair est $\equiv 1$ (mod. 8), on voit par un calcul analogue que la relation (16) tient aussi pour $D = 2$. Enfin, en recourant de nouveau à la *Remarque* I, on voit que la formule (16) subsiste pour un nombre composé D arbitraire.

Ce point acquis, décomposons n en ses facteurs premiers $n = \Pi p$, les p étant différents ou non. La formule (16) nous donne immédiatement

$$\left(\frac{D}{n}\right) = \Pi \left(\frac{D}{p}\right), \tag{18}$$

où, d'après (5), on peut entendre par (D/p) le symbole de Legendre.

C'est par le dernier produit que Jacobi a défini la généralisation remarquable du symbole de Legendre qui porte son nom et que nous désignons par $(D/n)_J$. Nous avons donc, en fin de compte, démontré que

$$\left(\frac{D}{n}\right)_Z = \left(\frac{D}{n}\right)_G = \left(\frac{D}{n}\right)_J \tag{19}$$

REMARQUE IV. On sait depuis les travaux de Gauss que la condition nécessaire et suffisante pour que D soit reste quadratique par rapport à un nombre impair n est que D soit reste quadratique de tous les facteurs premiers de n. Il en résulte que, si D est reste quadratique de n, on a $(D/n) = 1$, mais la réciproque n'est pas vraie. Pour que (D/n) soit égal à 1 il faut et il suffit évidemment que les p suivant lesquels D est non-reste soient en nombre pair.

8. Pour montrer que la méthode utilisée aux n^{os} 2—3 dans le cas d'un module premier peut aussi s'appliquer dans le cas d'un module composé impair, nous indiquons ici une seconde démonstration du fait que dans ce dernier cas les symboles de Zolotareff et de Jacobi sont identiques.

Soit donc n un nombre composé impair. Nous répartissons les nombres $1, 2, \ldots, p-1$ en des systèmes partiels Σ_d, chaque tel système étant constitué par les nombres qui ont le même plus grand commun diviseur d avec n. En posant $n/d = n'$, le système Σ_d sera constitué par les nombres $d\xi$, ξ parcourant tous les nombres $< n'$ qui sont premiers avec n'. D étant un nombre premier avec n, la transformation Z_D transforme chaque système partiel Σ_d en lui-même. Cela étant, on pourra étudier l'effet de Z_D sur chaque Σ_d séparément et former ensuite le « produit » de ces effets.

La transformation $u \to Du \pmod{n}$ avec $u = d\xi \in \Sigma_d$ est identique à la transformation $\xi \to D\xi \pmod{n'}$. En appliquant le procédé donné au n^o 3, on écrit cette transformation comme le produit de deux involutions et on obtient pour chaque système partiel une relation de la forme

$$\operatorname{sgn} Z_D = (-1)^{\frac{\alpha_D + \alpha_1}{2}},$$

α_D étant le nombre des solutions de la congruence $x^2 \equiv D \pmod{n'}$. On voit facilement que $\alpha_D = \alpha_1$ quand D est reste quadratique, tandis que

$\alpha_D = 0$ quand D est non-reste quadratique suivant n'. L'exposant est donc égal à α_1 dans le premier cas et à $\frac{1}{2}\alpha_1$ dans le second. Vu que α_1 est un nombre pair, le symbole de Zolotareff relatif au système partiel est donc égal à 1 si D est reste quadratique suivant n' et égal à $(-1)^{\frac{1}{2}\alpha_1}$ quand D est non-reste.

Le nombre α_1 qui, par définition, est égal au nombre des solutions de la congruence $x^2 \equiv 1 \pmod{n'}$, ne dépend que de n'. En posant donc $\alpha_1 = \psi(n')$, on obtient pour le symbole de Zolotareff relatif à la suite entière $\{1, 2, \ldots, n-1\}$

$$\left(\frac{D}{n}\right)_Z = (-1)^{\frac{1}{2}\Sigma\psi(n')}, \tag{20}$$

la sommation étant étendue à tous les diviseurs n' de n suivant lesquels D est non-reste.

9. C'est la dernière expression à laquelle Schering a su réduire le symbole de Gauss dans le cas d'un module impair composé. Il a aussi montré que cette expression coïncide avec le symbole de Jacobi. Ce n'est que ce dernier point qui nous intéresse ici, et nous allons brièvement indiquer le raisonnement par lequel Schering [6] a établi ce point; *voir* aussi Bachmann [1], p. 193.

Nous citons d'abord deux propositions dues à Gauss; *cf.* Dirichlet [3] p. 81.

I. On a pour tout nombre impair n, $\psi(n) = 2^\varkappa$, $\varkappa$ étant le nombre des facteurs premiers *différents* de n.

II. Tout nombre D premier avec le nombre premier impair p est en même temps reste ou non-reste quadratique de toutes les puissances p^α $(\alpha \geqq 1)$.

On voit à l'aide de la proposition I que le second membre de (20) ne sera pas changé si l'on supprime tous les n' qui admettent au moins deux facteurs premiers différents. Il ne reste donc que les n' de la forme p^α où p^α divise n et D est non-reste par rapport à p^α. La dernière hypothèse revient, d'après la proposition II, à ce que D est non-reste par rapport à p. D'après la proposition I, chaque telle puissance p^α apporte à $\frac{1}{2}\Sigma\psi(n')$ une contribution égale à 1. Donc si $n = \Pi p_k^{\pi_k}$ les p_k étant différents entre eux, l'expression (20) se réduit à $(-1)^{\Sigma\pi_l}$, où les p_l sont ceux des facteurs premiers p_k de n suivant lesquels D est non-reste. Vu que $(D/p_l) = -1$, la dernière expression est égale à $\Pi(D/p_l)^{\pi_l}$. Pour les p_k autres que les p_l, on a $(D/p_k) = 1$. Le produit précédent pourra donc être étendu à tous les p_k, qui divisent n, sans que sa valeur soit changée. Dès lors, en posant $n = \Pi p$, les nombres premiers p étant différents ou

non, on voit que le second membre de (20) est égal au symbole de Jacobi (*cf.* (18))

$$\Pi\left(\frac{D}{p}\right) = \left(\frac{D}{n}\right)_J,$$

résultat qui met en évidence que les symboles de Zolotareff et de Jacobi ont des valeurs identiques.

BIBLIOGRAPHIE

1. P. Bachmann, *Niedere Zahlentheorie* I, Leipzig, 1902.
2. P. G. Lejeune Dirchlet, *Über den ersten von Gauss gegebenen Beweis des Reciprocitätsgesetzes in der Theorie der quadratischen Reste*, J. reine angew. Math. 47 (1854), 139–150. (Werke II, Berlin, 1897, 123–138.)
3. P. G. Lejeune Dirichlet, *Vorlesungen über Zahlentheorie*, Vierte Auflage, Braunschweig, 1894.
4. G. Frobenius, *Über das quadratische Reciprocitätsgesetz*, S.-Ber. Preuss. Akad. Wiss. Berlin, math.-naturw. Kl. 1914 (I), 335–349, 484–488.
5. L. Kronecker, *Über das Reciprocitätsgesetz*, S.-Ber. Preuss. Akad. Wiss. Berlin, math.-naturw. Kl. 1876, 331–341. (Werke II, Leipzig, 1897, 13–23.)
6. E. Schering, *Zur Theorie der quadratischen Reste*, Acta math. 1 (1882), 153–170.
7. A. Scholz, *Einführung in die Zahlentheorie*, Sammlung Göschen 1131, Berlin, 1939.
8. Zolotareff, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouvelles Annales de Math. (2^e série) 11 (1872), 354–362.

UNIVERSITÉ DE LUND, SUÈDE