JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

C.-G.-J. JACOBI

Sur les nombres premiers complexes que l'on dit considérer dans la théorie des résidus de cinquième, huitième et douzième puissance

Journal de mathématiques pures et appliquées 1re série, tome 8 (1843), p. 268-272.
<http://www.numdam.org/item?id=JMPA_1843_1_8__268_0>

SUR LES NOMBRES PREMIERS COMPLEXES QUE L'ON DOIT CONSIDÉRER DANS LA THÉORIE DES RÉSIDUS DE CINQUIÈME, HUITIÈME ET DOUZIÈME PUISSANCE;

PAR M. C.-G.-J. JACOBI [*],

(Extrait du *Journal de M. Crelle*, tome XIX. — Traduction de M. FAYE.)

Dans ses recherches sur les résidus biquadratiques, M. Gauss a introduit les nombres complexes de la forme $a + b\sqrt{-1}$ comme modules ou comme diviseurs. Par là il a pu établir, sur le caractère biquadratique de deux nombres premiers complexes de la forme $a + b\sqrt{-1}$, une loi de réciprocité aussi simple et aussi complète que l'est ce fleuron de l'arithmétique la plus relevée, ce célèbre théorème fondamental sur les résidus quadratiques.

Mais, quelque simplicité que puisse apporter dans ces matières l'introduction des nombres complexes comme modules, elle n'en appartient pas moins aux plus profondes spéculations de la science; je dirai plus, il m'est impossible de croire que la seule arithmétique ait dirigé M. Gauss dans ces mystérieuses recherches; je penserais plutôt qu'il doit ces découvertes à l'étude des transcendantes elliptiques et probablement à l'espèce de celle qui donne la rectification des arcs de la lemniscate.

Par exemple, dans la théorie de la multiplication et de la division des arcs de la lemniscate, les nombres complexes de la forme $a+b\sqrt{-1}$ jouent précisément le rôle de nombres ordinaires. De même qu'on exprime rationnellement les fonctions trigonométriques des arcs de cercle multipliés par n, de même on peut multiplier les arcs de la lemniscate par un nombre complexe $a + b\sqrt{-1}$; de même qu'on divise le cercle en n parties par la résolution d'une équation du $n^{ième}$ degré, de même on peut diviser les arcs de la lemniscate en $a + b\sqrt{-1}$ parties par la résolution d'une équation du degré $a^2 + b^2$. Lorsqu'il s'agit de diviser un arc en 15 parties, on le partage en 3 et en 5, et on déduit de ces deux divisions la division cherchée; de même, lorsqu'il s'agit de diviser un arc de lemniscate en 17 parties, on le divise d'abord en $1 + 4\sqrt{-1}$ et en $1 - 4\sqrt{-1}$ parties, et on déduit de ces deux divisions celle en 17 parties.

[*] Lu à l'Académie royale de Berlin, le 16 mai 1839.

C'est ainsi que dans la recherche de chaque espèce particulière d'intégrale elliptique, pour peu qu'on veuille pénétrer leur nature, on se trouve inévitablement forcé d'introduire les nombres $a + b\sqrt{-1}$ comme diviseurs. Ces recherches de calcul intégral paraissent sans doute beaucoup plus compliquées et plus difficiles que les propositions ordinaires de la théorie des nombres, mais ce n'est pas toujours l'idée la plus simple qui se présente la première à l'esprit. M. Gauss assure, dans les *Disquisitiones arithmeticæ*, que sa méthode pour la division du cercle peut être appliquée à la lemniscate, et il promet un ample traité sur ce sujet, à une époque où il ne s'était certainement pas encore occupé des résidus biquadratiques.

C'est Abel qui, le premier, a su délier M. Gauss de sa promesse; il a du moins donné les premiers traits fondamentaux de l'extension à la lemniscate de la méthode de M. Gauss pour la division du cercle, dans son premier travail sur les transcendantes elliptiques publié par le Journal de M. Crelle. On résoudrait un problème aussi intéressant que difficile en interprétant géométriquement cette division de la lemniscate en $a + b\sqrt{-1}$ parties, et la détermination de la $p^{ième}$ partie d'un arc par sa division en $a + b\sqrt{-1}$ et en $a - b\sqrt{-1}$ parties. La géométrie, dans ces derniers temps, a assigné aux imaginaires une place dans son domaine, et les admirables travaux de M. Steiner sur ce sujet font espérer qu'elle finira par s'emparer complétement de ces idées abstruses.

Il n'était pas besoin d'idées nouvelles pour trouver les lois de la réciprocité cubique; il suffisait pour cela d'introduire d'une manière tout à fait analogue, comme modules ou comme diviseurs, les nombres complexes de la forme $\frac{a+b\sqrt{-3}}{2}$ ou d'autres semblables qui sont composés des racines cubiques de l'unité. On peut aussi rattacher ces recherches à la théorie de quelques intégrales elliptiques particulières. La loi de réciprocité pour les résidus cubiques, dont j'ai donné communication dans une Note précédente, est encore plus simple que celle que M. Gauss a posée pour les résidus biquadratiques, et elle se déduit immédiatement des formules connues pour la division du cercle.

Maintenant que M. Gauss a exposé, dans son second Mémoire sur les résidus biquadratiques, les éléments des nombres complexes de la forme $a + b\sqrt{-1}$, il reste encore à démêler parmi les méthodes et les solutions de l'arithmétique celles qui peuvent s'appliquer aussi à ces nombres complexes. Par exemple, on voit facilement que la méthode de Lagrange pour réduire les formes quadratiques peut s'étendre aussi aux expressions telles que $py^2 + qyz + rz^2$, dans lesquelles p, q, r, y, z représentent des nombres complexes de cette forme. Pour prendre la forme complexe la plus simple, $y^2 - \sqrt{-1}.z^2$, on peut prouver que tout nombre $a + b\sqrt{-1}$ qui divise une telle forme doit avoir aussi cette forme, et la démonstration est complétement analogue à celle de cette proposition connue que tout nombre qui divise $y^2 + z^2$ doit aussi être la somme de deux carrés. Soit $p = a^2 + b^2$ un nombre premier de la forme $8n + 1$; on

prouve aussitôt par les éléments de la théorie de ces nombres complexes que $\sqrt{-1}$ est le reste quadratique de $a + b\sqrt{-1}$, ou, ce qui revient au même, que $a + b\sqrt{-1}$ est diviseur d'une forme $y^2 - \sqrt{-1}.z^2$, et qu'ainsi il doit être de même forme en vertu du théorème cité plus haut. Si l'on partage cette expression en deux facteurs

$$y + \sqrt[4]{-1}.z \quad \text{et} \quad y - \sqrt[4]{-1}.z,$$

et qu'on pose

$$y = y' + y''\sqrt{-1}, \quad z = z' + z''\sqrt{-1},$$

où y', y'', z', z'' représentent des nombres réels entiers, alors on obtient $a + b\sqrt{-1}$ décomposé en deux facteurs,

$$y' + y''\sqrt{-1} + \sqrt[4]{-1}\,(z' + z''\sqrt{-1}),$$
$$y' + y''\sqrt{-1} - \sqrt[4]{-1}\,(z' + z''\sqrt{-1}),$$

c'est-à-dire en deux nombres complexes qui sont composés des racines huitièmes de l'unité.

Représentons par α la racine huitième de l'unité ou bien $\sqrt[4]{-1}$, et posons

$$\varphi\alpha = y' + y''\alpha^2 + z'\alpha + z''\alpha^3,$$

il viendra

$$a + b\sqrt{-1} = a + b\alpha^2 = \varphi\alpha.\varphi\alpha^5;$$

et si l'on remplace α par α^3,

$$a - b\sqrt{-1} = a - b\alpha^2 = \varphi\alpha^3.\varphi\alpha^7.$$

Le nombre premier $p = a^2 + b^2$, de la forme $8n + 1$, est ainsi toujours le produit des quatre nombres complexes

$$\varphi\alpha, \quad \varphi\alpha^3, \quad \varphi\alpha^5, \quad \varphi\alpha^7.$$

On voit facilement que le produit $\varphi\alpha.\varphi\alpha^3$ garde la forme $c + d\sqrt{-2}$, et que le produit $\varphi\alpha.\varphi\alpha^7$ garde la forme $e + f\sqrt{2}$. Les trois manières dont on peut ranger ces quatre facteurs deux à deux donnent l'expression du même nombre premier sous trois formes

$$a^2 + b^2, \quad c^2 + 2d^2, \quad e^2 + 2f^2,$$

qui sont déduites ici d'une source commune, en sorte que les six nombres a, b, c, d, e, f sont exprimés rationnellement par quatre autres nombres y', y'', z', z''. Cette décomposition des nombres premiers de la forme $8n+1$ en quatre facteurs complexes composés des huit racines de l'unité peut aussi être obtenue par les méthodes ordinaires de l'arithmétique. Ces mêmes méthodes peuvent encore servir à démontrer que les nombres premiers de la forme $12n + 1$ peuvent être décomposés en quatre facteurs complexes formés des racines douzièmes de l'unité; les trois combinaisons deux à deux que l'on

peut faire avec ces quatre facteurs donnent les expressions du nombre premier sous les trois formes

$$a^2 + b^2, \quad c^2 + 3d^2, \quad e^2 - 3f^2.$$

Pour trouver ces décompositions, on peut suivre des règles faciles d'après lesquelles M. le professeur Zornow, à Kœnigsberg, a eu la bonté de calculer pour moi ces décompositions pour les nombres premiers de la forme $8n + 1$ et $12n + 1$ jusqu'à 1000.

A l'époque où je m'occupais de ces considérations, je dirigeai mon attention sur certaines propriétés des nombres complexes auxquelles conduit la théorie de la division du cercle. J'ai remarqué dans la Note citée que, si λ est un diviseur de $p - 1$, le nombre premier p peut être représenté de plusieurs manières comme produit de deux nombres complexes formés des racines $\lambda^{ièmes}$ de l'unité. Il arrive alors, et on peut le démontrer par la théorie de la division du cercle, que l'on peut multiplier entre eux plusieurs de ces nombres complexes et diviser ensuite leur produit par d'autres nombres complexes du même genre, de telle sorte que le quotient soit aussi un nombre complexe entier, et cela sans qu'on voie comment les nombres complexes du dénominateur disparaissent devant ceux du numérateur. Je me suis convaincu, en considérant directement cette circonstance remarquable, que ces facteurs complexes du nombre premier p doivent être, en général, combinés de nouveau, de telle sorte que si on les décompose en vrais nombres premiers complexes, alors ceux qui forment les facteurs du dénominateur se laissent détruire isolément par les facteurs du numérateur. Comme j'étais déjà parvenu à ce résultat par une voie tout à fait différente pour $\lambda = 8$ et pour $\lambda = 12$, je risquai aussi cette recherche un peu pénible pour $\lambda = 5$, et, en effet, je réussis, pour les nombres premiers de la forme $5n + 1$, à décomposer leurs deux facteurs composés des racines de l'unité en deux nouveaux facteurs entiers de même genre; et ainsi il n'était pas difficile de trouver une démonstration générale de la possibilité de cette décomposition. Les nombres premiers de la forme $5n + 1$, $8n + 1$, $12n + 1$ peuvent donc être représentés par les produits de quatre nombres complexes entiers qui sont respectivement composés des racines cinquième, huitième et douzième de l'unité. En outre, il est clair que pour les nombres premiers de la forme $5n + 1$, on pourra les représenter sous la forme $a^2 - 5b^2$ au moyen d'une autre combinaison par couple de leurs quatre facteurs.

Les nouveaux facteurs sont nécessairement des nombres premiers. Soit, par exemple, $f\alpha$ un de ces nombres, dans lequel α est pour les trois genres de nombres premiers respectivement une racine cinquième, huitième, douzième de l'unité; alors $f\alpha$ ne pourra être représenté par le produit de deux nombres entiers complexes de la même forme $\varphi\alpha$ et $\psi\alpha$, à moins que l'un de ces derniers ne soit tel que le produit de ses quatre valeurs ne soit égal à l'unité. Car l'on voit facilement que le produit des quatre valeurs de $f\alpha$, $\varphi\alpha$ et $\psi\alpha$ est un nombre réel; et comme le produit des quatre valeurs de $f\alpha$ est un nombre premier, les deux autres produits ne peuvent donner de nombres réels qui soient tous les deux et en même temps différents de l'unité, puisque leur produit devient égal au nombre premier.

Il reste à chercher la loi de réciprocité entre les nombres premiers $f\alpha$, par la théorie des restes des puissances cinquième, huitième et douzième, et il serait peut-être facile de les trouver par une simple induction, puisque l'on connaît leur véritable forme, si une pareille induction ne devait être extrêmement pénible. Si l'on étend la loi de réciprocité aux nombres composés, comme je l'ai fait dans une Note précédemment communiquée à l'Académie sur les résidus quadratiques, cubiques et biquadratiques, on pourra déduire immédiatement de la théorie de la division du cercle les lois simples de réciprocité, par rapport aux restes des cinquième, huitième et douzième puissances, pour le cas particulier où l'un des nombres serait réel. Il reste à décider par des recherches ultérieures si de nouveaux artifices permettront de déduire de la même source les lois générales pour deux nombres complexes.