

16. Sur les nombres premiers complexes qui sont à considérer dans la théorie des résidus des 5^e, 8^e et 12^e puissances.

C. G. J. Jacobi, professeur ordinaire à l'Université de Königsberg en Prusse
(Lu à l'Académie des Sciences le 16 mai 1839.)

Gauss, dans ses recherches sur les résidus biquadratiques, a introduit les nombres complexes de la forme $a + b\sqrt{-1}$ comme modules ou diviseurs. En faisant cela, il put établir, sur le caractère biquadratique de deux nombres premiers complexes de la forme $a + b\sqrt{-1}$ l'un par rapport à l'autre, une loi de réciprocité d'une simplicité et d'une perfection telles que le fameux théorème fondamental sur les résidus quadratiques, ce qu'il a appelé lui-même le joyau de l'arithmétique supérieure, la possède. Mais si simple que puisse paraître maintenant une telle introduction des nombres complexes comme modules, elle n'en appartient pas moins aux pensées les plus profondes de la science ; je ne crois même pas que l'arithmétique seule ait conduit à une pensée aussi cachée, mais qu'elle a été puisée dans l'étude des transcendentes elliptiques, et précisément dans cette espèce particulière de celles-ci que fournit la rectification de l'arc de la lemniscate. En effet, 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 exactement le rôle des nombres ordinaires. De même que l'on représente par des expressions rationnelles les fonctions trigonométriques de l'arc multiple n du cercle, de même on peut, au moyen de formules rationnelles, multiplier l'arc de la lemniscate par un nombre complexe $a + b\sqrt{-1}$; de même que l'on divise l'arc de cercle en n parties par la résolution d'une équation du $n^{\text{ième}}$ degré, de même on divise l'arc de la lemniscate en $a + b\sqrt{-1}$ parties par la résolution d'une équation du degré $aa + bb$. De même que l'on divise un arc de cercle, lorsqu'on doit le diviser en 15 parties, en 3 et en 5 parties, et que l'on trouve par ces deux divisions celle que l'on cherche, de même, pour diviser un arc de la lemniscate en 17 parties, on le divise en $1 + 4\sqrt{-1}$ et en $1 - 4\sqrt{-1}$ parties, et l'on compose la division en 17 parties à partir des deux. C'est ainsi que, dans l'étude de cette espèce particulière d'intégrales elliptiques, pour peu que l'on pénètre tant soit peu dans leur nature, on est nécessairement conduit à introduire les nombres $a + b\sqrt{-1}$ comme diviseurs. Or, bien que ces recherches du calcul intégral puissent paraître beaucoup plus compliquées et plus difficiles que cette simple pensée de la théorie des nombres, ce n'est cependant pas toujours le simple qui se présente en premier. Gauss assure dans les *Disquisitiones arithmeticae* pouvoir appliquer sa méthode de division du cercle à la division de la lemniscate entière, et promet à ce sujet un *amplum opus* à une époque où, selon ses propres indications ultérieures, il ne s'occupait certes pas encore des résidus biquadratiques. Il n'est pas non plus invraisemblable qu'il ait puisé à cette source les théorèmes fondamentaux sur les résidus biquadratiques. Abel fut le premier à accomplir cette promesse de Gauss, en donnant du moins les premières bases de cette extension des méthodes gaussiennes de division du cercle à la division de la lemniscate dans ses premiers travaux sur les transcendentes elliptiques, publiés dans le présent Journal. Une tâche aussi intéressante que difficile serait de dégager un sens géométrique de cette division de l'arc de la lemniscate en $a + b\sqrt{-1}$ parties, et de la

composition de parties $p^{\text{ièmes}}$ de l'arc à partir de sa division en $a + b\sqrt{-1}$ et en $a - b\sqrt{-1}$ parties. La géométrie a, dans les temps modernes, assigné avec succès une place à l'imaginaire aussi dans son domaine ; il est à espérer que, dans l'essor admirable qu'elle a pris entre les mains de Steiner, elle s'emparera aussi de ces idées plus abstraites. Il n'a fallu aucune pensée nouvelle pour trouver les lois de réciprocité cubiques ; il suffisait pour cela d'introduire de manière tout à fait analogue des nombres complexes de la forme $\frac{a+b\sqrt{-3}}{2}$, ou ceux qui sont composés des racines cubiques de l'unité, comme modules ou diviseurs. Ces recherches aussi peuvent être mises en relation avec la théorie d'intégrales elliptiques particulières. La loi de réciprocité pour les résidus cubiques, que j'ai communiquée dans une note antérieure, est encore plus simple que celle établie par Gauss pour les résidus biquadratiques, et se déduit tout à fait immédiatement de formules connues de la division du cercle.

Après que Gauss, dans son second mémoire sur les résidus biquadratiques, a traité les éléments des nombres complexes de la forme $a + b\sqrt{-1}$, il reste à distinguer, parmi les méthodes et les résultats de l'arithmétique, ceux qui conservent leur validité pour ces nombres complexes. Ainsi, par exemple, on voit facilement que la méthode de Lagrange pour réduire les formes quadratiques peut aussi s'étendre à des expressions telles que $pyy + qyz + rzz$, dans lesquelles p, q, r, y, z désignent des nombres complexes du type indiqué. Pour prendre la forme complexe la plus simple, $yy - \sqrt{-1} \cdot zz$, on peut démontrer que tout nombre $a + b\sqrt{-1}$ qui divise une telle forme doit lui-même avoir la même forme, et la démonstration est parfaitement analogue à celle du théorème connu selon lequel tout nombre qui divise la forme $yy + zz$ est de nouveau la somme de deux carrés. Si $p = aa + bb$ est un nombre premier de la forme $8n + 1$, on démontre à partir des éléments de la théorie de ces nombres complexes que $\sqrt{-1}$ est résidu quadratique de $a + b\sqrt{-1}$, ou, ce qui revient au même, que $a + b\sqrt{-1}$ est diviseur d'une forme $yy - \sqrt{-1} \cdot zz$, donc, d'après le théorème que l'on vient de remarquer, a lui-même cette forme. Si l'on décompose cette forme en les deux facteurs $y + \sqrt{-1} \cdot z$ et $y - \sqrt{-1} \cdot z$, et que l'on pose

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

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

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

c'est-à-dire en deux nombres complexes composés des racines $8^{\text{ièmes}}$ de l'unité. Si l'on écrit α pour la racine $8^{\text{ième}}$ de l'unité, ou pour $\sqrt{-1}$, et que l'on pose

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

alors

$$a + b\sqrt{-1} = a + b\alpha^2 = \Phi\alpha \cdot \Phi\alpha^5,$$

et, si l'on pose α^3 pour α ,

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

Le nombre premier $p = aa + bb$, de la forme $8n + 1$, est donc toujours le produit des quatre nombres complexes

$$\Phi\alpha \cdot \Phi\alpha^3 \cdot \Phi\alpha^5 \cdot \Phi\alpha^7.$$

On voit facilement que le produit $\Phi\alpha \cdot \Phi\alpha^3$ prend la forme $c + d\sqrt{-2}$ et le produit $\Phi\alpha \cdot \Phi\alpha^7$ la forme $e + f\sqrt{2}$. Les trois manières

d'ordonner les quatre facteurs en deux paires donnent donc les représentations du même nombre premier sous les trois formes $a^2 + b^2$, $c^2 + 2d^2$, $e^2 + 2f^2$, qui sont ici déduites d'une source commune, de sorte que les six nombres a, b, c, d, e, f s'expriment de manière rationnelle au moyen de quatre autres nombres y', y'', z', z'' . On peut aussi déduire cette décomposition des nombres premiers de la forme $8n + 1$ en quatre facteurs complexes, composés de huit racines de l'unité, par les méthodes ordinaires de l'arithmétique. Par les mêmes méthodes, on démontre aussi que les nombres premiers de la forme $12n + 1$ se décomposent en quatre facteurs complexes composés des racines 12^{èmes} de l'unité; les trois manières différentes d'ordonner ces quatre facteurs en deux paires donnent les représentations du nombre premier par les trois formes $a^2 + b^2$, $c^2 + 3d^2$, $e^2 - 3f^2$. On peut donner pour la découverte de ces décompositions des règles faciles, selon lesquelles M. le maître d'études supérieures Zornow, à Königsberg, a eu l'amabilité de calculer pour moi ces décompositions pour les nombres premiers de la forme $8n + 1$ et $12n + 1$ jusqu'à 1000.

En même temps que je faisais ces considérations, je portai mon attention sur certaines propriétés des nombres complexes auxquelles conduit la théorie de la division du cercle. J'ai remarqué dans la note mentionnée que, si λ est un diviseur de $p - 1$, le nombre premier p peut, et en général de plusieurs manières différentes, être représenté comme produit de deux nombres complexes composés des racines $\lambda^{\text{èmes}}$ de l'unité. Or il arrive, et l'on peut le démontrer par la théorie de la division du cercle elle-même, que l'on peut multiplier entre eux plusieurs de ces nombres complexes et diviser de nouveau le produit par d'autres nombres complexes de même espèce, de sorte que le quotient soit également un nombre complexe entier, sans que l'on voie comment les nombres complexes du dénominateur s'éliminent contre ceux du numérateur. Un examen attentif de ce fait remarquable me conduisit à la conviction que ces facteurs complexes du nombre premier p doivent eux-mêmes, en général, être de nouveau composés, de sorte que, si on les résout en les véritables nombres premiers complexes, les nombres premiers complexes qui forment les facteurs du dénominateur puissent s'éliminer un à un contre les facteurs premiers du numérateur. Comme j'étais déjà parvenu à ce résultat par une tout autre voie pour $\lambda = 8$ et $\lambda = 12$, j'osai tenter l'essai assez laborieux avec $\lambda = 5$, et en effet je réussis, pour les nombres premiers de la forme $5n + 1$, avec lesquels je fis l'essai, à décomposer chacun de leurs deux facteurs composés des racines 5^{èmes} de l'unité encore une fois en deux facteurs entiers de même espèce; après quoi il ne fut pas difficile de trouver une démonstration générale de cette décomposabilité. Ainsi donc les nombres premiers de la forme $5n + 1$, $8n + 1$, $12n + 1$ peuvent se représenter comme produits de quatre nombres complexes entiers, composés respectivement des racines 5^{èmes}, 8^{èmes}, 12^{èmes} de l'unité. Il ressort d'ailleurs que, pour les nombres premiers de la forme $5n + 1$, une autre combinaison deux à deux des quatre facteurs donne leur représentation sous la forme $a^2 - 5b^2$.

Les nouveaux facteurs sont nécessairement des nombres premiers. Si en effet $f\alpha$ est l'un d'eux, où α désigne respectivement, pour les trois espèces de nombres premiers, une racine primitive 5^{ième}, 8^{ième}, 12^{ième} de l'unité, alors $f\alpha$ ne peut pas être représenté comme produit de deux nombres complexes entiers de même espèce $\varphi\alpha$ et $\psi\alpha$, à moins que l'un de ceux-ci ne soit tel que le produit de ses quatre valeurs de l'unité soit égal à l'unité. Car on voit facilement que le produit des quatre valeurs de $f\alpha$, $\varphi\alpha$, $\psi\alpha$ est un nombre réel, et comme le produit des quatre valeurs de $f\alpha$ est un nombre premier, les deux autres produits ne peuvent pas donner des nombres réels qui soient tous deux simultanément différents de l'unité, puisque leur produit devient égal au nombre premier.

Entre ces nombres premiers $f\alpha$, on a à chercher, dans la théorie des résidus des puissances 5^{ièmes}, 8^{ièmes} et 12^{ièmes}, les lois de réciprocité, et il serait peut-être possible de les trouver par simple induction, après que l'on connaît leur vraie forme, si une telle induction n'était pas extrêmement pénible. Si l'on étend les lois de réciprocité aux nombres composés, tout à fait comme je l'ai fait dans la note communiquée précédemment à l'Académie relativement aux résidus quadratiques, cubiques et biquadratiques, on peut déduire immédiatement de la théorie de la division du cercle les théorèmes de réciprocité simples, relativement aux résidus des puissances 5^{ièmes}, 8^{ièmes} et 12^{ièmes}, pour le cas particulier où l'un des nombres est réel. Quant à savoir s'il sera possible, au moyen de nouveaux artifices, de déduire de la même source les théorèmes plus généraux pour deux nombres complexes quelconques, cela doit être réservé à des recherches ultérieures.