Werk

Titel: Bullettino di bibliografia e di storia delle scienze matematiche e fisiche

Verlag: Tip. delle Scienze Matematiche e Fisiche

Jahr: 1885

Kollektion: mathematica

Signatur: 4 HLU IV, 5:18

Werk Id: PPN599471603_0018

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN599471603_0018|LOG_0022

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

SUR QUELQUES THÉORÈMES

QUI PEUVENT CONDUIRE

À LA LOI DE RÉCIPROCITÉ DE LEGENDRE;

PAR M. A. GENOCCHI

Soit n un nombre entier, et ρ une racine primitive de l'équation $x^n - 1 = 0$; on aura :

$$\frac{x^n - 1}{x - 1} = \prod_{k=1}^{k=n-1} (x - \rho^k),$$

le signe $\prod_{k=1}^{k=n-1}$ indiquant une multiplication étendue à toutes les valeurs $k = 1, 2, 3, \ldots n-1$. Si n est impair, en faisant $q = \frac{n-1}{2}$, on pourra écrire

$$\frac{x^n - 1}{x - 1} = \prod_{k=1}^{k=q} (x - \rho^k)(x - \rho^{n-k}) = \prod_{k=1}^{k=q} (x - \rho^k)(x - \rho^{-k}).$$

Soit β une autre racine primitive de l'équation $x^n - 1 = 0$, n étant impair; β^2 sera aussi une racine primitive de cette équation, et on pourra prendre $\rho = \beta^2$, ce qui donnera

$$(x - \rho^k)(x - \rho^{-k}) = (\beta^{-k}x - \beta^k)(\beta^k x - \beta^{-k}),$$

et par suite

$$(A) \qquad \frac{x^n - 1}{x - 1} = \prod_{k=1}^{k=q} (\beta^k x - \beta^{-k})(\beta^{-k} x - \beta^k).$$

Maintenant désignons par m un nombre impair premier à n, par α une racine primitive de l'équation $x^m - 1 = 0$, et par h l'un des nombres $1, 2, 3, \ldots \frac{m-1}{2}$: faisant $x = \alpha^h$, l'équation précédente deviendra

$$(B) \qquad \frac{\alpha^{nh} - \alpha^{-nh}}{\alpha^h - \alpha^{-h}} = \prod_{k=1}^{k=q} (\alpha^h\beta^k - \alpha^{-k}\beta^{-k})(\alpha^h\beta^{-k} - \alpha^{-h}\beta^k).$$

On obtient d'une manière semblable, en posant $p = \frac{m-1}{2}$,

$$(C) \qquad \frac{\beta^{mk} - \beta^{-mk}}{\beta^k - \beta^{-k}} = \prod_{h=1}^{h=p} (\alpha^h\beta^k - \alpha^{-h}\beta^{-k})(\alpha^{-h}\beta^k - \alpha^h\beta^{-k}).$$

Or, en étendant les multiplications aux pq combinaisons des valeurs de h et k, on a

$$\Pi(\alpha^h\beta^{-k} - \alpha^{-h}\beta^k) = (-1)^{pq} \Pi(\alpha^{-h}\beta^k - \alpha^h\beta^{-k}) :$$

donc les équations (B) et (C) donneront

$$\prod_{h=1}^{h=p}\left(\frac{\alpha^{nh}-\alpha^{-nh}}{\alpha^{h}-\alpha^{-h}}\right)=(-1)^{pq}\prod_{k=1}^{k=q}\left(\frac{\beta^{mk}-\beta^{-m}}{\beta^{k}-\beta^{-k}}\right).$$

Cette équation renferme un lemme de Gauss employé dans sa cinquième démonstration de la loi de réciprocité présentée à la Société de Gottingue le 10 février 1817 (*Comment. Gotting. recent.* Vol. IV, 1818). En effet, concevons qu'on divise par n tous les multiples mk en prenant les restes positifs ou négatifs, mais numériquement inférieurs à $\frac{1}{2}n$, et nommons m_1 le nombre des restes négatifs; concevons de même qu'en divisant par m tous les multiples nh, on prenne les restes numériquement inférieurs à $\frac{1}{2}m$, et qu'on désigne par n_1 le nombre des restes négatifs : il est visible que l'équation précédente revient à

$$(-1)^{n_1}=(-1)^{pq}\,.\,(-1)^{m_1},$$

et il en résulte que m_1+n_1, sera pair ou impair comme pq, ce qui est le lemme de Gauss.

Si m et n sont deux nombres premiers, on a un autre lemme de Gauss qui est le troisième des théorèmes énoncés dans sa lettre du 30 avril 1807 à Sophie Germain, et qu'il a démontré dans les préliminaires de sa troisième démonstration de la loi de réciprocité présentée le 15 janvier 1808, et imprimée dans le Vol. XVI des *Comment. Societ. Gottingensis* (1808); cet autre lemme de Gauss donne par la notation de Legendre

$$\left(\frac{m}{n}\right)=(-1)^{m_1},\qquad\left(\frac{n}{m}\right)=(-1)^{n_1},$$

et il s'ensuit

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

loi de réciprocité.

Faisant $x=1$ dans l'équation (A) on obtient

$$n=(-1)^{q}.\prod_{k=1}^{k=q}(\beta^{k}-\beta^{-k})^{2}:$$

c'est la formule dont a fait usage Liouville en 1847 pour démontrer la même loi. J'ai exposé cette démonstration sous plusieurs formes différentes dans mon Mémoire de 1852.

Nous ferons aussi une application de l'équation (B) en prenant

$$\alpha=e^{\frac{2a\pi i}{m}},\quad\beta=e^{\frac{2b\pi i}{n}},$$

et désignant par a un nombre premier à m, par b un nombre premier à n,

et par i l'imaginaire $\sqrt{-1}$. Il viendra

$$\frac{\sin\frac{2anh\pi}{m}}{\sin\frac{2ah\pi}{m}} = 2^{2q}.(-1)^q.\prod_{k=1}^{k=q}\sin\frac{2\pi(anh+bmk)}{mn}\sin\frac{2\pi(anh-bmk)}{mn}.$$

Or en général, $\sin 2\pi x$ est positif si x surpasse un nombre entier d'une quantité inférieure ou égale à $\frac{1}{2}$, négatif si au contraire il y a un nombre entier qui surpasse x d'une quantité inférieure à $\frac{1}{2}$. Au moyen de cette remarque, on déduira de la formule qu'on vient d'écrire le théorème d'arithmétique suivant :

Soient m, n, a, b des nombres entiers positifs; m et n impairs et premiers entre eux, a premier à m, b premier à n; soit h un nombre entier déterminé quelconque, et k un nombre indéterminé qui prenne successivement les valeurs $1, 2, 3, \ldots \frac{n-1}{2}$. Divisez par mn toutes les valeurs que prendront les quantités $anh + bmk$, $anh - bmk$, en déterminant les quotients de manière que chaque reste soit *numériquement* inférieur à $\frac{1}{2}mn$, et soit λ le nombre total des restes *négatifs*. Divisez aussi ah et anh par m en prenant les restes numériquement inférieurs à $\frac{1}{2}m$; enfin soit $q = \frac{n-1}{2}$. Cela posé, le nombre $q + \lambda$ sera pair, si les restes de ah et anh sont de même signe, impair s'ils sont de signes contraires.

En supposant pour plus de simplicité $a = 1$, $b = 1$, et h l'un des termes de la suite $1, 2, 3, \ldots p$, p étant $= \frac{m-1}{2}$, on a un théorème particulier sur lequel je me suis appuyé dans la démonstration reproduite par les *Comptes rendus* (Séance du 16 février 1880), et qui a une certaine liaison avec celle de Liouville. On peut démontrer ce théorème particulier d'une manière directe ainsi qu'il suit.

Posons

$$r = \frac{mn-1}{2},\quad u = nh - mk,\quad v = nh + mk - r;$$

u et v, abstraction faite du signe, seront $< \frac{1}{2}mn$. Ayant divisé nh par m, soit l le quotient, h' le reste *positif*; nous aurons $nh = ml + h'$, $h < \frac{m}{2}$, et par suite $ml < nh < n\frac{m}{2}$, d'où $l < \frac{n}{2}$; donc mk sera plus petit que nh pour toutes les valeurs $k = 1, 2, 3, \ldots l$, mais pour ces seules valeurs, de sorte que

u aura l valeurs positives. J'observe que les nombres h' et u ne peuvent être nuls, car nh, étant inférieur à $\frac{1}{2}mn$, ne peut être multiple en même temps de m et de n. Mais nous aurons aussi $nh + mk = m(l + k) + h'$, $r = mq + p$, et par consequent, $nh + mk > r$ pour toutes les valeurs $k = q - l + 1$, $q - l + 2$, $q - l + 3, \ldots q - 1, q$; et aussi, pour l'autre valeur $k = q - l$ dans le cas de $h' > p$; en effet $q - l$ ne pourra pas être nul dans ce cas, puisque, si $q = l$, il s'ensuivrait

$$ml + h' > mq + p, \text{ ou } nh > r,$$

tandis que r est égal à $np + q$, et que h ne surpasse pas p. Ainsi le nombre v aura l valeurs positives si $h' < \frac{m}{2}$, et en aura $l + 1$ si $h' > \frac{m}{2}$. Donc le nombre des valeurs positives de v est égal à celui des valeurs positives de u lorsque le reste h' est inférieur à $\frac{1}{2}m$, et le surpasse d'une unité dans le cas contraire : de là résulte le théorème particulier que nous avons indiqué et qui se trouve énoncé aux *Comptes rendus*.

On peut généraliser le lemme de Gauss proposé dans la lettre à Sophie Germain.

Soient m et n deux entiers premiers entre eux; λ le nombre des entiers inférieurs à $\frac{1}{2}n$ et premiers à n; représentons ces entiers par $b_1, b_2, \ldots b_\lambda$, et divisons par n les multiples

$$b_1 m, b_2 m, \ldots b_\lambda m,$$

de manière à avoir des restes positifs ou négatifs, mais numériquement inférieurs à $\frac{1}{2}n$. Si m_1 désigne le nombre des restes négatifs, $m^\lambda - (-1)^{m_1}$ sera divisible par n.

Nommons, en effet, $h_1, h_2, \ldots h_\lambda$, les quotients, et $k_1, k_2, \ldots k_\lambda$ les restes de ces divisions : on aura

$$b_1 m = h_1 n + k_1, b_2 m = h_2 n + k_2, \ldots b_\lambda m = h_\lambda n + k_\lambda,$$

ce qui montre que les restes $k_1, k_2, \ldots k_\lambda$ seront tous premiers à n, car k_r par exemple ne pourrait avoir de commun avec n un facteur premier qui ne divisât aussi b_r ou m, en vertu de l'équation $b_r m = h_r n + k_r$. Mais, de plus, ces restes seront tous numériquement inégaux, car si l'on eût $k_r = \pm k_{r'}$ les équations $b_r m = h_r n + k_r$, $b_{r'} m = h_{r'} n + k_{r'}$ donneraient $(b_r \mp b_{r'}) m = (h_r \mp h_{r'}) n$, et n étant premier à m devrait être diviseur du nombre $b_r \mp b_{r'}$, tandis que b_r et $b_{r'}$ sont $< \frac{1}{2}n$, et par suite $b_r \mp b_{r'}$, est numériquement inférieur à n. Donc la suite $k_1, k_2, \ldots k_\lambda$ sera composée des mêmes termes, abstraction faite de leurs signes et de leur ordre, que l'autre suite $b_1, b_2, \ldots b_\lambda$, et l'on en déduira

$$k_1 k_2 \ldots k_\lambda = (-1)^{m_1} \cdot b_1 b_2 \ldots b_\lambda.$$

Or, en multipliant membres à membres les λ équations précédentes, et supprimant les multiples de n, on obtiendra

$$b_1 b_2 \ldots b_\lambda \cdot m^\lambda \equiv k_1 k_2 \ldots k_\lambda \pmod{n} :$$

donc

$$b_1 b_2 \ldots b_\lambda \left[m^\lambda - (-1) m_1\right] \equiv 0 \pmod{n},$$

c'est-à-dire que n sera diviseur de $m^\lambda - (-1)^{m_1}$, puisque le facteur $b_1 b_2 \ldots b_\lambda$ est premier à n.

Lorsque n est premier, la suite $b_1, b_2, \ldots b_\lambda$ est celle des nombres naturels $1, 2, 3 \ldots \frac{n-1}{2}$, et on a $\lambda = \frac{n-1}{2}$; donc alors $m^{\frac{n-1}{2}} - (-1)^{m_1}$ est divisible par n, d'où le lemme de Gauss $\left(\frac{m}{n}\right) = (-1)^{m_1}$.

Dans tous les cas $m^{2\lambda} - 1$ sera divisible par n, car il est le produit des deux nombres $m^\lambda + 1$ et $m^\lambda - 1$, et on aura ainsi un théorème d'Euler.

On peut remplacer le lemme de Gauss par d'autres propositions analogues. Au lieu de multiplier m par les entiers inférieurs à $\frac{1}{2}n$, on peut le multiplier par les entiers *pairs* inférieurs à n, ou par les entiers *impairs* inférieurs également à n, et diviser les produits par n en prenant les restes positifs: dans le premier cas le nombre des restes *impairs*, et celui des restes *pairs* dans le second, déterminera la valeur de $\left(\frac{m}{n}\right)$.

On peut aussi choisir pour multiplicateurs les puissances

$$g, g^2, g^3, \ldots g^{\frac{n-1}{2}}$$

d'une racine *primitive* g de n: la valeur de $\left(\frac{m}{n}\right)$ sera déterminée par le nombre des produits congrus aux autres puissances

$$g^{\frac{n-1}{2}+1}, \quad g^{\frac{n-1}{2}+2}, \quad g^{\frac{n-1}{2}+3}, \ldots g^{n-1}.$$

Ces observations étaient comprises dans mon Mémoire *Sur la théorie des résidus quadratiques* reçu dans la séance du 6 Novembre 1852 par l'Académie Royale de Belgique. Une autre généralisation du même lemme de Gauss a été donnée par M. Schering en 1876 (*Monatsberichte der k. pr. Akademie der Wissenschaften zu Berlin, aus dem Jahre* 1876, pag. 330–331), et j'en ai fait usage dans les *Comptes rendus*.

Dans son deuxième Mémoire sur les résidus biquadratiques du 15 avril 1831 Gauss a étendu l'analyse indéterminée aux expressions $t + u\sqrt{-1}$, t et u désignant des nombres entiers positifs ou négatifs. Il a reconnu que par cette

extension qui conduit à des questions d'un ordre plus élevé, on parvient à une proposition comparable en simplicité et en élégance à la loi de réciprocité de Legendre. Dirichlet a démontré ce théorème dans le Journal de Crelle, tom. IX, pag. 379–389, travail daté de septembre 1832, et a observé de plus que l'expression plus générale $t + u\sqrt{a}$, où a désigne un nombre entier sans diviseur carré, donne lieu à des théorèmes analogues susceptibles d'une démonstration toute semblable. On appelle nombre entier complexe toute expression de la forme indiquée $t + u\sqrt{-1}$, et ce nombre est premier lorsqu'il ne peut être décomposé en deux facteurs différens l'un et l'autre de ± 1 et $\pm\sqrt{-1}$. Un nombre complexe $\alpha + \beta\sqrt{-1}$ est ou n'est pas résidu quadratique de $A + B\sqrt{-1}$ selon qu'il existe ou qu'il n'existe pas d'expression $x + y\sqrt{-1}$, telle que $(x + y\sqrt{-1})^2 - (\alpha + \beta\sqrt{-1})$ soit divisible par $A + B\sqrt{-1}$. Or Dirichlet démontre que le nombre $1 + \sqrt{-1}$ (dont le module a 2 pour carré) est résidu ou non résidu quadratique du nombre premier $A + B\sqrt{-1}$ selon que l'on a $A + B \equiv \pm 1$, ou $\equiv \pm 3 \pmod 8$; et ensuite que si $\alpha + \beta\sqrt{-1}$ et $A + B\sqrt{-1}$ désignent deux nombres premiers complexes (β et B étant pairs et pouvant se réduire à zéro), le premier sera ou ne sera pas résidu quadratique du second, selon que le second est ou n'est pas résidu quadratique du premier.

C'est la loi de réciprocité pour les nombres complexes.

Je rappelle enfin une *Note sur les nombres complexes* que j'avais adressée à Liouville et qu'il a insérée en septembre 1854 dans le Tome XIX de son Journal, pag. 281–288, en l'accompagnant de ces paroles bienveillantes:

« Il y a très–longtemps que cette Note m'a été adressée et qu'elle aurait » dû être imprimée. L'auteur a depuis publié des recherches plus étendues » sur la théorie des nombres. Je crois pourtant que le présent article peut » encore aujourd'hui être mis utilement sous les yeux du lecteur. »

Dans cette Note la dénomination de nombres complexes était appliquée généralement aux polynomes

$$a + a_1 r + a_2 r^2 + \ldots + a_{n-1} r^{n-1},$$

où n est un nombre premier réel différent de 2, r une racine imaginaire de l'équation $r^n = 1$ et les coefficients $a, a_1, a_2, \ldots a_{n-1}$ sont réels et entiers. Après quelques théorèmes sur les nombres, j'y donnais la démonstration de Liouville à peu près comme dans le Mémoire *Sur la théorie des résidus quadratiques*.