Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies.

J. P. G. Lejeune-Dirichlet

[Lu à l'Académie des Sciences de Berlin le 25 Juin 1835.]
(Extrait.)

Parmi les conséquences nombreuses et inattendues que M. Gauss a tirées de sa belle théorie des équations binômes, il y en a une qui présente une singularité très remarquable. La lettre p désignant un nombre premier $4m+1$ et q un nombre premier $4m+3$, il résulte de cette théorie que les deux expressions :

$$s = \sum_{i=0}^{i=p-1} \cos \frac{2i^2\pi}{p}, \qquad\qquad t = \sum_{i=0}^{i=q-1} \sin \frac{2i^2\pi}{q}$$

sont données par ces deux équations du second degré : $s^2 = p$, $t^2 = q$. On conclut de là $s = \pm\sqrt{p}$, $t = \pm\sqrt{q}$, où il ne s'agit plus que de fixer le signe qui doit être unique dans l'un et l'autre cas, les sommes précédentes étant complètement déterminées. En attribuant des valeurs particulières aux nombres p et q, on trouve toujours que c'est le signe supérieur qui doit avoir lieu, mais il est très difficile de prouver la généralité de ce résultat indiqué par l'induction. Dans ses *Disquisitiones arithmeticae* M. Gauss ne s'était pas attaché à lever cette difficulté singulière, mais il y est revenu dans un Mémoire particulier [1] que les géomètres regardent comme une des plus belles productions de ce profond analyste. La méthode dont il y fait usage, consiste à transformer les sommes précédentes, ou plutôt les expressions plus générales qui s'en déduisent, en y remplaçant les nombres premiers p et q par un entier quelconque 2, en produits de sinus d'arcs équidifférents, produits qui sont très faciles à évaluer et qui ne présentent plus aucune ambiguïté de signe. La difficulté de se rendre bien compte à quoi tient le succès des considérations délicates par lesquelles l'illustre auteur opère cette ingénieuse transformation, m'ayant fait rechercher, si on ne pourrait pas résoudre la même question sans y recourir, je suis parvenu au théorème suivant qui comprend les sommations précédentes :

"La somme de la série finie ou infinie :

$$F(\alpha) = c_0 + c_1 \cos\alpha + c_2 \cos 2\alpha + \ldots$$

étant connue, on peut toujours exprimer, au moyen de la fonction $F(\alpha)$, les nouvelles séries :

$$c_0 + c_1 \cos 1^2 \cdot \frac{2\pi}{n} + c_2 \cos 2^2 \cdot \frac{2\pi}{n} + \ldots,$$

$$c_1 \sin 1^2 \cdot \frac{2\pi}{n} + c_2 \sin 2^2 \cdot \frac{2\pi}{n} + \ldots,$$

qui ont les mêmes coefficients que la précédente."

Je me flatte que cette nouvelle manière de parvenir aux résultats si remarquables de M. Gauss pourra avoir quelque intérêt, l'histoire de la théorie des nombres nous montrant par de nombreux exemples, que c'est surtout dans cette partie de la science qu'il y a de l'avantage à envisager la

Transcription en LaTeX :Denise Vella-Chemla, septembre 2025.

[1] Summatio quarumdam serierum singularitum. Comment. recent, societ. Gottingen, Tom. 1., Gauss Werke, Band 11, 8.9. K.

même question sous des points de vue très différents. La méthode de M. Gauss était jusqu'à présent le seul moyen de vaincre la difficulté indiquée et qui consiste dans l'ambiguïté du signe. Celle que M. Libri a donnée, quoique très ingénieuse, ne paraît pas propre à résoudre cette difficulté puisqu'elle fait dépendre les sommes cherchées d'une équation du second degré. Pour faire disparaître l'ambiguïté que cette circonstance fait naître[2], le savant auteur a recours à l'expression transformée en produit, sans indiquer aucun moyen de parvenir à cette transformée. Mais ce passage de la somme au produit est à lui seul la question tout entière, puisqu'une fois effectué, il dispense de toute autre analyse, l'expression en produit étant du nombre de ceux qu'Euler a déterminés depuis longtemps par les considérations les plus simples.

§ 1.

L'analyse dont nous ferons usage, repose sur ces deux théorèmes :

"*La constante c remplissant la double condition* $0 < c \leq \frac{1}{2}\pi$ *et la fonction* $f(\beta)$ *étant continue depuis* $\beta = 0$ *jusqu'à* $\beta = c$, *l'intégrale* $\int_0^c \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta)d\beta$ *convergera vers la limite* $\frac{1}{2}\pi f(0)$ *pour des valeurs indéfiniment croissantes de l'entier positif* k."

"*Les constantes b et c étant telles qu'on ait* $0 < b < c \leq \frac{1}{2}\pi$, *et la fonction* $f(\beta)$ *étant supposée continue depuis* $\beta = b$ *jusqu'à* $\beta = c$, *l'intégrale* $\int_b^c \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta)d\beta$ *convergera dans la même circonstance vers la limite zéro*."

Ces théorèmes se démontrent facilement, comme je l'ai fait voir dans un précédent Mémoire[3], lorsqu'on suppose d'abord la fonction $f(\beta)$ toujours croissante, ou toujours décroissante entre les limites de l'intégration. Pour passer ensuite au cas général où cette fonction présente plusieurs maxima et minima entre ces limites, il suffit de décomposer les intégrales en d'autres entre les limites desquelles la fonction $f(\beta)$ n'est plus alternativement croissante et décroissante.

Au moyen de ces théorèmes on détermine facilement la limite vers laquelle converge l'intégrale :

$$\int_0^\alpha \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta)d\beta.$$

α désignant une constante positive quelconque, et la fonction $f(\beta)$ étant continue depuis $\beta = 0$ jusqu'à $\beta = \alpha$. Soit $l\pi$ le plus grand multiple de π contenu dans α, l'intégrale précédente sera la somme de celles-ci :

$$\int_0^{l\pi} \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta)d\beta, \qquad \int_{l\pi}^\alpha \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta)d\beta.$$

[2]Voyez le tome IX du Journal de Crelle, p. 187.

[3]Voyez le Journal de Crelle Tome IV p. 157 ou le "Repertorium der Physik von Dove und Moser", où la même démonstration est simplifiée à quelques égards. § 117 et 133 dans cette édition des Œuvres de G. Lejeune Dirichlet Werken. K.

La première étant décomposée en $2l$ autres prises entre les limites :

$$0 \text{ et } \frac{1}{2}\pi, \quad \frac{1}{2}\pi \text{ et } 2.\frac{1}{2}\pi, \quad 2.\frac{1}{2}\pi \text{ et } 3.\frac{1}{2}\pi, \quad \ldots, \quad (2l-1).\frac{1}{2}\pi \text{ et } 2l.\frac{1}{2}\pi,$$

si dans ces nouvelles intégrales l'on écrit au lieu de β :

$$\beta, \quad \pi - \beta, \quad \pi + \beta, \quad 2\pi - \beta, \quad \ldots, \quad l\pi - \beta,$$

et si l'on transforme ensuite les intégrales dont le rang est un nombre pair, d'après la formule :

$$\int_g^h \psi(\beta) d\beta = -\int_h^g \psi(\beta) d\beta$$

toutes ces intégrales s'étendront depuis $\beta = 0$ jusqu'à $\beta = \frac{1}{2}\pi$. En les réunissant donc et ayant égard à ce que k est un entier, il viendra :

$$\int_0^{\frac{1}{2}\pi} [f(\beta) + f(\pi - \beta) + f(\pi + \beta) + \ldots + f((l-1)\pi + \beta) + f(l\pi - \beta)] \frac{\sin(2k+1)\beta}{\sin\beta} d\beta,$$

expression qui, d'après le premier des théorèmes précédents, convergera pour des valeurs croissantes de k vers cette limite :

$$\pi \left(\frac{1}{2} f(0) + f(\pi) + f(2\pi) + \ldots + \frac{1}{2} f(l\pi) \right).$$

La seconde intégrale :

$$\int_{l\pi}^{\alpha} \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta) d\beta$$

évidemment nulle lorsque $\alpha = l\pi$, devient généralement :

$$\int_0^{\alpha - l\pi} \frac{\sin(2k+1)\beta}{\sin\beta} f(l\pi + \beta) d\beta,$$

en y remplaçant β par $l\pi + \beta$. Lorsque $\alpha - l\pi$ ne surpasse pas $\frac{1}{2}\pi$, il résulte du premier théorème qu'elle converge vers la limite $\frac{1}{2}\pi f(l\pi)$; dans le cas où $-l\pi$ est compris entre $\frac{1}{2}\pi$ et π, on décomposera l'intégrale précédente en deux autres prises l'une depuis $\beta = 0$ jusqu'à $\beta = \frac{1}{2}\pi$, l'autre depuis $\beta = \frac{1}{2}\pi$ jusqu'à $\beta = \alpha - l\pi$. La première deviendra toujours $\frac{1}{2}\pi f(l\pi)$ pour $k = \infty$, tandis que la seconde qui, par le changement de β en $\pi - \beta$, prend la forme :

$$\int_{(l+1)\pi - \alpha}^{\frac{1}{2}\pi} \frac{\sin(2k+1)\beta}{\sin\beta} f((l+1)\pi - \beta) d\beta,$$

converge vers la limite zéro en vertu du second théorème.

En réunissant ce qui précède, on voit que l'intégrale :

$$\int_0^{\alpha} \frac{\sin(2k+1)\beta}{\sin\beta} f(\beta) d\beta$$

lorsque l'entier positif k qu'elle renferme devient infini, prend toujours cette valeur :

$$\pi\left(\frac{1}{2}f(0)+f(\pi)+f(2\pi)+\ldots+f(l\pi)\right)=\frac{1}{2}\pi f(0)+\pi\sum_{s=1}^{s=l}f(s\pi),$$

$l\pi$ désignant le plus grand multiple de π contenu dans α. Il n'y a d'exception que lorsque α est un multiple exact de π, le dernier terme $\pi f(l\pi)$ devant, dans ce cas, être réduit à la moitié de sa valeur.

§ 2.

Considérons les deux intégrales [4]:

$$\int_{-\infty}^{\infty}\cos(\alpha^2)d\alpha=a,\qquad\int_{-\infty}^{\infty}\sin(\alpha^2)d\alpha=b,$$

Quoiqu'on sache qu'on a $a=\sqrt{\frac{1}{2}\pi}, b=\sqrt{\frac{1}{2}\pi}$, nous n'avons pas besoin de supposer connues les valeurs de ces deux constantes qui se présentent d'elles-mêmes dans l'analyse que nous allons développer. Si l'on pose dans la première intégrale $\alpha=\beta+g$, β désignant une nouvelle variable et g étant une constante réelle quelconque, il viendra :

$$\int_{-\infty}^{\infty}\cos(\beta+g)^2d\beta=\int_{-\infty}^{\infty}\cos(\beta^2+g^2)\cos 2g\beta.d\beta-\int_{-\infty}^{\infty}\sin(\beta^2+g^2)\sin 2g\beta.d\beta=a.$$

La seconde intégrale étant évidemment nulle, cette équation prendra la forme :

$$\cos(g^2)\int_{-\infty}^{\infty}\cos(\beta^2)\cos 2g\beta.d\beta-\sin(g^2)\int_{-\infty}^{\infty}\sin(\beta^2)\cos 2g\beta.d\beta=a.$$

On trouve d'une manière toute semblable :

$$\sin(g^2)\int_{-\infty}^{\infty}\cos(\beta^2)\cos 2g\beta.d\beta+\cos(g^2)\int_{-\infty}^{\infty}\sin(\beta^2)\cos 2g\beta.d\beta=b.$$

En éliminant successivement chacune de ces deux intégrales, on aura ces équations connues :

$$\int_{-\infty}^{\infty}\cos(\beta^2)\cos 2g\beta.d\beta=a\cos(g^2)+b\sin(g^2),$$

$$\int_{-\infty}^{\infty}\sin(\beta^2)\cos 2g\beta.d\beta=b\cos(g^2)-a\sin(g^2).$$

[4]Il n'est peut-être pas inutile de prévenir une difficulté que l'emploi de ces deux intégrales pourrait faire naître. Quelques auteurs ont énoncé qu'une intégrale prise entre des limites infinies devient nécessairement indéterminée, lorsque la fonction sous le signe ne s'évanouit pas à ces deux limites. Les intégrales que nous considérons ne satisfont pas à cette condition et sont néanmoins complètement déterminées, comme on le voit sur le champ en les mettant sous cette autre forme :

$$\int_0^{\infty}\frac{\cos\beta}{\sqrt{\beta}}d\beta,\quad\int_0^{\infty}\frac{\sin\beta}{\sqrt{\beta}}d\beta.$$

Il résulte de là que les intégrales $\int\cos(\alpha^2)d\alpha$, $\int\sin(\alpha^2)d\alpha$ prises depuis $\alpha=-p$ jusqu'à $\alpha=p$, convergent l'une et l'autre vers une limite fixe, lorsque la quantité positive p croît indéfiniment, soit que cette augmentation se fasse d'une manière continue, soit qu'elle ait lieu, comme dans ce qui va suivre, par sauts et suivant une loi quelconque. Il n'en serait pas de même pour l'intégrale $\int\cos\alpha\,d\alpha$, qu'on suppose quelquefois égale à zéro, et qui est essentiellement indéterminée, du moins tant qu'on la considère en elle-même.

Si l'on pose :

$$\beta = \frac{1}{2}\alpha\sqrt{\frac{n}{2\pi}}, \qquad g = i\sqrt{\frac{2\pi}{n}},$$

α étant une nouvelle variable, et n et i désignant des constantes positives que l'on considérera comme des entiers dans ce qui va suivre, il viendra :

$$\int_{-\infty}^{\infty} \cos\left(\frac{n\alpha^2}{8\pi}\right)\cos i\alpha\ d\alpha = 2\sqrt{\frac{2\pi}{n}}.\left(a\cos\frac{2i^2\pi}{n} + b\sin\frac{2i^2\pi}{n}\right),$$

$$\int_{-\infty}^{\infty} \sin\left(\frac{n\alpha^2}{8\pi}\right)\cos i\alpha\ d\alpha = 2\sqrt{\frac{2\pi}{n}}.\left(b\cos\frac{2i^2\pi}{n} - a\sin\frac{2i^2\pi}{n}\right)$$

Cela posé, soit :

$$F(\alpha) = c_0 + c_1\cos\alpha + c_2\cos 2\alpha + \ldots = \sum c_j\cos j\alpha \tag{1}$$

une série de cosinus finie ou infinie. On suppose seulement que lorsque la série se prolonge à l'infini, elle est convergente et exprime une fonction continue de α. Les équations précédentes étant multipliées par c_i si l'on somme ensuite entre les mêmes limites que dans l'équation (1), on aura :

$$\begin{cases} \displaystyle\int_{-\infty}^{\infty} \cos\frac{n\alpha^2}{8\pi}F(\alpha)d\alpha = 2\sqrt{\frac{2\pi}{n}}(aG + bH), \\ \displaystyle\int_{-\infty}^{\infty} \sin\frac{n\alpha^2}{8\pi}F(\alpha)d\alpha = 2\sqrt{\frac{2\pi}{n}}(bG - aH). \end{cases} \tag{2}$$

où j'ai fait pour abréger :

$$\sum c_i\cos\frac{2i^2\pi}{n} = G, \qquad \sum c_i\sin\frac{2i^2\pi}{n} = H. \tag{3}$$

Pour obtenir les intégrales précédentes, on les supposera d'abord prises depuis $\alpha = -(4k+1)\pi$ jusqu'à $\alpha = (4k+1)\pi$, k désignant un nombre entier positif quelconque que l'on considérera ensuite comme infini. Chacune de ces deux intégrales étant décomposée en $4k+1$ nouvelles intégrales dont les limites résultent des expressions $(2h-1)\pi$ et $(2h+1)\pi$ en attribuant à h toutes les valeurs entières depuis $h = -2k$ jusqu'à $h = 2k$, si l'on pose ensuite $\beta = 2h\pi + \gamma$ dans chacune de ces nouvelles intégrales, en observant qu'on a, d'après l'équation (1), $F(2h\pi + \gamma) = F(\gamma)$, il viendra :

$$\int_{-\pi}^{\pi} d\gamma F(\gamma)\sum\cos\frac{n}{8\pi}(\gamma + 2h\pi)^2, \qquad \int_{-\pi}^{\pi} d\gamma F(\gamma)\sum\sin\frac{n}{8\pi}(\gamma + 2h\pi)^2,$$

les sommations s'étendant depuis $h = -2k$ jusqu'à $h = 2k$. En réunissant les termes de la première somme qui correspondent à des valeurs opposées de h, cette somme prendra cette autre forme :

$$\cos\frac{n\gamma^2}{8\pi} + \sum_{h=1}^{h=2k}\left(\cos\frac{n}{8\pi}(\gamma + 2h\pi)^2 + \cos\frac{n}{8\pi}(\gamma - 2h\pi)^2\right)$$
$$= \cos\frac{n\gamma^2}{8\pi} + 2\sum_{h=1}^{h=2k}\cos\frac{n}{8\pi}(\gamma^2 + 4h^2\pi^2)\cos\frac{hn\gamma}{2}.$$

Le facteur $\cos\frac{n}{8\pi}(\gamma^2+4h^2\pi^2)$ n'a évidemment que deux valeurs différentes, à savoir :

$$\cos\left(\frac{n\gamma^2}{8\pi}\right) \qquad \text{ou} \qquad \cos\left(\frac{n\gamma^2}{8\pi}+\frac{n\pi}{2}\right),$$

selon que h est pair ou impair, puisque h^2, dans le premier cas, a la forme 4μ et, dans le second, celle-ci : $4\mu+1$. Il viendra donc en réunissant séparément les termes pour lesquels h est pair et ceux où h est impair :

$$\cos\frac{n\gamma^2}{8\pi}(1+2\cos n\gamma+2cos2n\gamma+\ldots+2\cos kn\gamma)$$
$$+\cos\left(\frac{1}{2}n\pi+\frac{n\gamma^2}{8\pi}\left[2\cos\frac{1}{2}n\gamma+2\cos 3\left(\frac{1}{2}n\gamma\right)+\ldots+2\cos(2k-1)\left(\frac{1}{2}n\gamma\right)\right]\right.$$

En substituant pour ces deux séries les expressions connues :

$$\frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin\frac{1}{2}n\gamma}, \qquad \frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin\frac{1}{4}n\gamma}-\frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin\frac{1}{2}n\gamma},$$

il viendra :

$$\frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin\frac{1}{4}n\gamma}\cos\left(\frac{1}{2}n\pi+\frac{n\gamma^2}{8\pi}\right)+\frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin\frac{1}{2}n\gamma}\left[\cos\frac{n\gamma^2}{8\pi}-\cos\left(\frac{1}{2}n\pi+\frac{n\gamma^2}{8\pi}\right)\right]$$

La somme que la seconde intégrale renferme, est pareillement :

$$\frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin\frac{1}{4}n\gamma}\sin\left(\frac{1}{2}n\pi+\frac{n\gamma^2}{8\pi}\right)+\frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin\frac{1}{2}n\gamma}\left[\sin\frac{n\gamma^2}{8\pi}-\sin\left(\frac{1}{2}n\pi+\frac{n\gamma^2}{8\pi}\right)\right]$$

Ces expressions ayant la même valeur pour γ et pour $-\gamma$, et la même circonstance ayant lieu pour $F(\gamma)$ en vertu de l'équation (1), il est permis de n'étendre les intégrations que depuis $\gamma=0$ jusqu'à $\gamma=\pi$ et de doubler les résultats. On trouve ainsi ces deux expressions :

$$2\int_0^\pi \frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin\frac{1}{4}n\gamma}\cos\left(\frac{1}{2}n\pi+\frac{n\gamma^2}{8\pi}\right)F(\gamma)d\gamma$$
$$+2\int_0^\pi \frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin\frac{1}{2}n\gamma}\left[\cos\frac{n\gamma^2}{8\pi}-\cos\left(\frac{1}{2}n\pi+\frac{n\gamma^2}{8\pi}\right)\right]F(\gamma)d\gamma,$$

$$2\int_0^\pi \frac{\sin(4k+1)\frac{1}{4}n\gamma}{\sin\frac{1}{4}n\gamma}\sin\left(\frac{1}{2}n\pi+\frac{n\gamma^2}{8\pi}\right)F(\gamma)d\gamma$$
$$+2\int_0^\pi \frac{\sin(2k+1)\frac{1}{2}n\gamma}{\sin\frac{1}{2}n\gamma}\left[\sin\frac{n\gamma^2}{8\pi}-\sin\left(\frac{1}{2}n\pi+\frac{n\gamma^2}{8\pi}\right)\right]F(\gamma)d\gamma.$$

Si l'on pose $\frac{1}{4}n\gamma=\beta$ dans la première et dans la troisième intégrale, et $\frac{1}{2}n\gamma=\beta$ dans la seconde

et la quatrième, ces expressions prennent la forme :

$$\frac{8}{n}\int_0^{\frac{n\pi}{4}} \frac{\sin(4k+1\grave{a}\beta}{\sin\beta}\cos\left(\frac{1}{2}n\pi+\frac{2\beta^2}{n\pi}\right)F\left(\frac{4\beta}{n}\right)d\beta$$
$$+\frac{4}{n}\int_0^{\frac{n\pi}{2}} \frac{\sin(2k+1)\beta}{\sin\beta}\left[\cos\frac{\beta^2}{2n\pi}-\cos\left(\frac{1}{2}n\pi+\frac{\beta^2}{2n\pi}\right)\right]F\left(\frac{2\beta}{n}\right)d\beta,$$

$$\frac{8}{n}\int_0^{\frac{n\pi}{4}} \frac{\sin(4k+1\grave{a}\beta}{\sin\beta}\sin\left(\frac{1}{2}n\pi+\frac{2\beta^2}{n\pi}\right)F\left(\frac{4\beta}{n}\right)d\beta$$
$$+\frac{4}{n}\int_0^{\frac{n\pi}{2}} \frac{\sin(2k+1)\beta}{\sin\beta}\left[\sin\frac{\beta^2}{2n\pi}-\sin\left(\frac{1}{2}n\pi+\frac{\beta^2}{2n\pi}\right)\right]F\left(\frac{2\beta}{n}\right)d\beta.$$

Les limites de ces expressions correspondant à $k=\infty$ résultent immédiatement du théorème énoncé à la fin du premier paragraphe : en substituant ces valeurs dans les équations (2) et multipliant par $\frac{1}{2}\sqrt{\frac{n}{2\pi}}$, il viendra :

$$aG+bH=\sqrt{\frac{\pi}{2n}}\cdot\left(1+\cos\frac{n\pi}{2}\right)F(0)+4\sqrt{\frac{\pi}{2n}}\cdot\sum\cos\left(\frac{n\pi}{2}+\frac{2s^2\pi}{n}\right)F\left(\frac{4s\pi}{n}\right)$$
$$+2\sqrt{\frac{\pi}{2n}}\cdot\sum\left[\cos\frac{s^2\pi}{2n}-\cos\left(\frac{n\pi}{2}+\frac{s^2\pi}{2n}\right)\right]F\left(\frac{2s\pi}{n}\right),$$

$$bG-aH=\sqrt{\frac{\pi}{2n}}\cdot\sin\frac{n\pi}{2}F(0)+4\sqrt{\frac{\pi}{2n}}\cdot\sum\sin\left(\frac{n\pi}{2}+\frac{2s^2\pi}{n}\right)F\left(\frac{4s\pi}{n}\right)$$
$$+2\sqrt{\frac{\pi}{2n}}\cdot\sum\left[\sin\frac{s^2\pi}{2n}-\sin\left(\frac{n\pi}{2}+\frac{s^2\pi}{2n}\right)\right]F\left(\frac{2s\pi}{n}\right).$$

Dans chacune de ces deux équations la première somme s'étend depuis $s=1$ jusqu'au plus grand entier contenu dans $\frac{1}{4}n$, la seconde depuis $s=1$ jusqu'au plus grand entier contenu dans $\frac{1}{2}n$, le dernier terme de la seconde somme devant être réduit à moitié lorsque $\frac{1}{2}n$ est un nombre entier, et la même chose ayant lieu pour la première lorsque $\frac{1}{4}n$ est aussi un entier.

Pour déduire de ces équations les sommations dont il a été question dans le préambule de ce Mémoire, supposons la série (1) composée de n termes et tous ses coefficients égaux à l'unité. On aura alors:

$$F(\alpha)=1+\cos\alpha+\cos 2\alpha+\ldots+\cos(n-1)\alpha=\frac{1}{2}+\frac{\sin\left(n-\frac{1}{2}\right)\alpha}{2\sin\frac{1}{2}\alpha},$$

et la fonction $F\left(\frac{2t\pi}{n}\right)$ sera évidemment nulle, lorsque t est un nombre entier non-divisible par n. Il résulte de là, en ayant égard aux limites des sommations précédentes, que tous leurs termes disparaissent, et comme on a aussi $F(0)=n$, il viendra simplement :

$$aG+bH=\left(1+\cos\frac{1}{2}n\pi\right)\cdot\sqrt{\frac{1}{2}n\pi},\qquad bG-aH=\sin\frac{1}{2}n\pi\cdot\sqrt{\frac{1}{2}n\pi}.$$

Pour déterminer les deux quantités a et b, indépendantes de n, il suffira de donner à n une valeur particulière. Posant par exemple $n=1$, on aura $G=1, H=0$, et les équations précédentes

deviendront $a = \sqrt{\frac{1}{2}\pi}$, $b = \sqrt{\frac{1}{2}\pi}$. On a donc généralement, quel que soit n :

$$G + H = \left(1 + \frac{1}{2}n\pi\right) \cdot \sqrt{n}, \qquad G - H = \sin\frac{1}{2}n\pi \cdot \sqrt{n},$$

et par conséquent :

$$G = \frac{1}{2}\left(1 + \cos\frac{1}{2}n\pi + \sin\frac{1}{2}n\pi\right)\sqrt{n}, \qquad H = \frac{1}{2}\left(1 + \cos\frac{1}{2}n\pi - \sin\frac{1}{2}n\pi\right)\sqrt{n}.$$

En attribuant successivement à n ces 4 formes : $4\mu, 4\mu+1, 4\mu+2, 4\mu+3$ et remettant pour G et H les séries que ces lettres représentent d'après les équations (3), on aura :

$$\sum \cos\frac{2i^2\pi}{n} = \sqrt{n}, \quad \sum \sin\frac{2i^2\pi}{n} = \sqrt{n}, \quad n = 4\mu,$$

$$\sum \cos\frac{2i^2\pi}{n} = \sqrt{n}, \quad \sum \sin\frac{2i^2\pi}{n} = 0, \qquad n = 4\mu+1,$$

$$\sum \cos\frac{2i^2\pi}{n} = 0, \qquad \sum \sin\frac{2i^2\pi}{n} = 0, \qquad n = 4\mu+2,$$

$$\sum \cos\frac{2i^2\pi}{n} = 0, \qquad \sum \sin\frac{2i^2\pi}{n} = \sqrt{n}, \quad n = 4\mu+3,$$

les sommations s'étendant depuis $i = 0$ jusqu'à $i = n - 1$.

§ 3.

Je ne terminerai pas cet extrait, sans avoir rappelé les considérations extrêmement simples par lesquelles M. Gauss, dans le Mémoire déjà cité, a déduit des expressions précédentes, la loi de réciprocité qui existe entre deux nombres premiers impairs quelconques.

Le nombre premier impair p étant considéré comme diviseur, le reste provenant d'un carré quelconque non-divisible par p, sera évidemment compris parmi ceux que donne la série :

$$1^2, 2^2, 3^2, \ldots \left(\frac{p-1}{2}\right)^2 ;$$

et l'on prouve facilement que ces restes que je désignerai par :

(I) $$a_1, a_2, a_3, \ldots, a_{\frac{p-1}{2}},$$

pris dans un ordre quelconque, sont tous différents entre eux. Soient encore :

(II) $$b_1, b_2, b_3, \ldots, b_{\frac{p-1}{2}},$$

ceux des nombres $1, 2, 3, \ldots, p-1$ que la série (I) ne renferme pas. Cela posé, le nombre quelconque q non-divisible par p, est dit résidu ou non-résidu quadratique par rapport au diviseur p, selon que le reste de q appartient à la série (I) ou à la série (II), et l'on s'assure facilement que les restes de :

$$1^2.q,\ \ 2^2.q,\ \ 3^2.q, \ldots\ \ \left(\frac{p-1}{2}\right)^2.q,$$

abstraction faite de l'ordre, coïncident avec (I) ou (II), selon que le premier ou le second de ces deux cas a lieu[5].

Considérons la somme $\sum_{s=0}^{s=p-1} e^{s^2.\frac{2\pi}{p}\sqrt{-1}}$ dans laquelle e désigne à l'ordinaire la base des logarithmes népériens. Comme p est impair, il résulte des expressions du paragraphe précédent que cette somme est $\sqrt{p}$ ou $\sqrt{p}.\sqrt{-1}$ selon que p a la forme $4\mu+1$ ou celle-ci : $4\mu+3$ Cette double valeur étant donnée par la formule unique $\sqrt{p}(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2}$, on aura :

$$\sum_{s=0}^{s=p-1} e^{s^2.\frac{2\pi}{p}\sqrt{-1}} = \sqrt{p}(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2}.$$

Si l'on met à part le premier terme et que l'on réunisse deux à deux les termes correspondant à s et à $p-s$, en ayant égard à l'équation évidente :

$$e^{s^2.\frac{2\pi}{p}\sqrt{-1}} = e^{(p-s)^2\frac{2\pi}{p}\sqrt{-1}},$$

il viendra :

$$1 + 2\sum_{s=1}^{s=\frac{p-1}{2}} e^{s^2.\frac{2\pi}{p}\sqrt{-1}} = \sqrt{p}(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2},$$

ou ce qui revient au même, en rejetant les multiples de $2\pi\sqrt{-1}$ dans l'exposant :

$$1 + 2\sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s.\frac{2\pi}{p}\sqrt{-1}} = \sqrt{p}(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2},$$

On a pareillement :

$$P = \sum_{s=0}^{s=p-1} e^{s^2.\frac{2q\pi}{p}\sqrt{-1}} = 1 + 2\sum_{s=1}^{s=\frac{p-1}{2}} e^{s^2.\frac{2q\pi}{p}\sqrt{-1}},$$

et comme les restes de la série $1^2.q, 2^2.q, 3^2.q, \ldots, \left(\frac{p-1}{2}\right)^2.q$, coïncident avec (I) ou (II), selon que q est ou n'est pas résidu quadratique par rapport à p, on a respectivement dans ces deux cas, en négligeant toujours les multiples de $2\pi\sqrt{-1}$ dans l'exposant :

$$P = 1 + 2\sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s.\frac{2\pi}{p}\sqrt{-1}} \quad \text{ou} \quad P = 1 + 2\sum_{s=1}^{s=\frac{p-1}{2}} e^{b_s.\frac{2\pi}{p}\sqrt{-1}}$$

[5]Disquisitiones arithmeticae. Sect. IV.

expressions dont la seconde, en vertu de l'équation évidente :

$$\sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s.\frac{2\pi}{p}\sqrt{-1}} + \sum_{s=1}^{s=\frac{p-1}{2}} e^{b_s.\frac{2\pi}{p}\sqrt{-1}} = \sum_{s=1}^{s=p-1} e^{s.\frac{2\pi}{p}\sqrt{-1}} = -1,$$

se change en :

$$P = -1 - 2\sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s.\frac{2\pi}{p}\sqrt{-1}}.$$

Si donc l'on désigne par δ l'unité prise positivement ou négativement selon que q est ou n'est pas résidu quadratique par rapport à p, on aura l'équation qui comprend les deux cas :

$$\sum_{s=0}^{s=p-1} e^{s^2.\frac{2q\pi}{p}\sqrt{-1}} = \delta\left(1 + 2\sum_{s=1}^{s=\frac{p-1}{2}} e^{a_s.\frac{2\pi}{p}\sqrt{-1}}\right) = \delta\sqrt{p}(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2}.$$

Si l'on suppose que q est aussi un nombre premier impair, on aura par une simple permutation :

$$\sum_{t=0}^{t=q-1} e^{t^2.\frac{2p\pi}{q}\sqrt{-1}} = \varepsilon\sqrt{q}(\sqrt{-1})^{\left(\frac{q-1}{2}\right)^2}$$

où $\varepsilon = +1$ ou $= -1$, selon que p est ou n'est pas résidu quadratique de q.

En multipliant les équations précédentes entre elles, il viendra :

$$\sum_{t=0}^{t=q-1}\sum_{s=0}^{s=p-1} e^{(q^2s^2+p^2t^2)\frac{2\pi}{pq}\sqrt{-1}} = \delta\varepsilon\sqrt{pq}(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2+\left(\frac{q-1}{2}\right)^2}.$$

ou ce qui est la même chose, en ajoutant $4st\pi\sqrt{-1}$ à l'exposant :

$$\sum_{t=0}^{t=q-1}\sum_{s=0}^{s=p-1} e^{(qs+pt)^2\frac{2\pi}{pq}\sqrt{-1}} = \delta\varepsilon\sqrt{pq}(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2+\left(\frac{q-1}{2}\right)^2}.$$

il est facile de voir qu'entre les limites de la double sommation $qs+pt$ ne saurait donner deux fois le même reste par rapport au diviseur pq ; car si les restes provenant de $qs+pt$ et de $qs'+pt'$ étaient égaux, $q(s-s')+p(t-t')$ serait divisible par pq, ce qui exige, s, s' étant compris entre 0 et $p-1$, et t, t' entre 0 et $q-1$, qu'on ait à la fois $s = s', t = t'$. Ces restes seront donc $0, 1, 2, \ldots, pq-1$, et l'on pourra les mettre à la place de la série de valeurs fournies par l'expression $qs+pt$, ce changement consistant évidemment à négliger des multiples de $2\pi\sqrt{-1}$ dans l'exposant. On aura ainsi

$$\sum_{s=0}^{s=pq-1} e^{s^2.\frac{2\pi}{pq}\sqrt{-1}} = \delta\varepsilon\sqrt{pq}(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2+\left(\frac{q-1}{2}\right)^2}$$

ou en remplaçant le premier membre par sa valeur qui résulte des expressions du paragraphe précédent :

$$\sqrt{pq}(\sqrt{-1})^{\left(\frac{pq-1}{2}\right)^2} = \delta\varepsilon\sqrt{pq}(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2+\left(\frac{q-1}{2}\right)^2}$$

et par conséquent :

$$\delta\varepsilon = (\sqrt{-1})^{\left(\frac{pq-1}{2}\right)^2-\left(\frac{p-1}{2}\right)^2-\left(\frac{q-1}{2}\right)^2}$$

et comme l'exposant est équivalent à l'expression :

$$\frac{1}{2}(p-1)(q-1)+(p-1)(q-1)\left(\frac{(p+1)(q+1)}{4}-1\right),$$

dont le second terme peut être négligé comme étant divisible par 4, il viendra :

$$\delta\varepsilon = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Cette équation renferme la loi de réciprocité, car il en résulte qu'on a $\delta = \varepsilon$, lorsque p et q sont l'un et l'autre de la forme $4\mu+1$ ou l'un de la forme $4\mu+1$, l'autre de la forme $4\mu+3$ et qu'au contraire on a $\delta = -\varepsilon$, lorsque p et q ont l'un et l'autre la forme $4\mu+3$.

Traduction d'un extrait de *Introduction to number theory* de Trygve Nagell, Université d'Uppsala, éds. John Wiley and Sons, New York, p. 177 et suiv.

53. Les sommes de Gauss. Dans ses recherches sur la construction des polygones réguliers, Gauss a été amené au problème de la détermination de sommes du type suivant :

$$\varphi(m,n)=\sum_{s=0}^{n-1}\left(\cos\frac{2\pi ms^2}{n}+i\sin\frac{2\pi ms^2}{n}\right), \tag{1}$$

où m et n sont des entiers, $n>0$. Après de nombreux efforts, il établit finalement le résultat suivant :

Théorème 99. *Si n est un entier naturel, on a*

$$\varphi(1,n)=\begin{cases}(1+i)\sqrt{n} & \text{pour } n\equiv 0 \pmod 4\\ \sqrt{n} & \text{pour } n\equiv 1 \pmod 4\\ 0 & \text{pour } n\equiv 2 \pmod 4\\ i\sqrt{n} & \text{pour } n\equiv 3 \pmod 4\end{cases}$$

Preuve. Posons

$$\varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}.$$

Pour $n\equiv 2 \pmod 4$, le théorème est trivial, puisque

$$\varepsilon^{\left(s+\frac{1}{2}n\right)^2}=\varepsilon^{s^2+sn+\frac{n^2}{4}}=-\varepsilon^{s^2}.$$

Par conséquent, la moitié des termes dans la somme (1) sont éliminés par l'autre moitié.

Supposons ensuite que n est impair, et posons $\frac{1}{2}(n-1)=\nu$. Soit m un entier premier à n, et posons $\varepsilon^m=\eta$. Dans l'identité polynomiale (6) du paragraphe 52 [6], on pose alors $h=n-1$ et $x=\eta^{-2}$. Puisque

$$\frac{1-\varepsilon^{2k-tn}}{1-\varepsilon^{-2k}}=-\varepsilon^{2k}$$

pour tout entier t, on obtient la relation suivante

$$1+\eta^2+\eta^6+\eta^{12}+\ldots+\eta^{n(n-1)}=(1-\eta^{-2})(1-\eta^{-6})\ldots(1-\eta^{-2n+4}),$$

ou

$$\sum_{k=0}^{n-1}\eta^{k(k+1)}=\eta^{-1-3-5-\ldots-(n-2)}\prod_{k=0}^{s-1}(\eta^{2k+1}-\eta^{-2k-1}). \tag{2}$$

Puisque

$$\eta^{(\nu-k)^2}=\eta^{\nu^2+k(k+1)}$$

[6] Gauss définit $F(x,h,k)=\dfrac{(1-x^h)(1-x^{h-1})\ldots(1-x^{h-k+1})}{(1-x)(1-x^2)\ldots(1-x^k)}$ et $f(x,h)=\sum_{k=0}^{h}(-1)^kF(x,h,k)$. Une démonstration permet d'aboutir à la formule (6) $f(x,h)=(1-x)(1-x^3)\ldots(1-x^{h-1})$.

on a

$$\eta^{\nu^2}\sum_{k=0}^{\nu}\eta^{k(k+1)} = 1+\eta+\eta^4+\eta^9+\ldots+\eta^{\nu^2}.$$

Par conséquent

$$\eta^{(n-k)(n-k+1)+\nu^2} = \eta^{k^2-k+\nu^2} = \eta^{k^2+\nu^2+(n-1)k} = \eta^{(\nu+k)^2},$$

et donc

$$\eta^{\nu^2}\sum_{k=1}^{\nu}\eta^{(n-k)(n-k+1)} = \eta^{\nu^2}\sum_{k=1}^{\nu}\eta^{k(k-1)} = \eta^{(\nu+1)^2}+\eta^{(\nu+2)^2}+\ldots+\eta^{(n-1)^2}.$$

Puisque

$$1+3+5+\ldots+(n-2) = \nu^2,$$

il découle de (2) que

$$1+\eta+\eta^4+\eta^9+\ldots+\eta^{(n-1)^2} = (\eta-\eta^{-1})(\eta^3-\eta^{-3})\ldots(\eta^{n-2}-\eta^{-n+2}).$$

Ici, le côté gauche est par définition égal à $\varphi(m,n)$ et donc, on a

$$\varphi(m,n) = \prod_{k=1}^{\frac{1}{2}(n-1)} 2i\sin\frac{(4k-2)m\pi}{n}. \tag{3}$$

Pour $m=1$, ce produit prend, par la formule (5) du paragraphe 51, la valeur

$$i^{\frac{1}{2}(n-1)}(-1)^{\left[\frac{n}{4}\right]}\cdot\sqrt{n}.$$

Par conséquent, on voit que $\varphi(1,n)$ prend la valeur $\sqrt{n}$ pour $n\equiv 1 \pmod 4$ et la valeur $i\sqrt{n}$ pour n tel que $n\equiv 3 \pmod 4$. Il ne reste que le cas $n\equiv 0 \pmod 4$.

Quand m et n sont des nombres premiers entre eux, et si h est un entier, on va démontrer le lemme :

$$\varphi(hm,n)\cdot\varphi(hn,m) = \varphi(h,mn). \tag{4}$$

En fait, en posant

$$E(x) = \cos 2\pi x + i\sin 2\pi x,$$

on a

$$\begin{aligned}\varphi(hm,n)\cdot\varphi(hn,m) &= \sum_{s,t}E\left(\frac{hms^2}{n}+\frac{hnt^2}{m}\right)\\ &= \sum_{s,t}E\left(\frac{h(ms+nt)^2}{mn}\right) = \sum_{k=0}^{mn-1}E\left(\frac{hk^2}{mn}\right) = \varphi(h,mn)\ ;\end{aligned}$$

car par le théorème 33 [7], les nombres $ms+nt$ couvrent un système complet de résidus modulo mn quand s et t couvrent un système complet de résidus modulo m et modulo n respectivement.

[7] *Rappel* : **Théorème 33** : si les nombres naturels m et n sont premiers entre eux, si x couvre un système complet de résidus modulo n et si y couvre un système complet de résidus modulo m, alors les mn nombres de la forme $mx+ny$ forment un système complet de résidus modulo mn.

De (4), on obtient pour $h = 1$ et $m = 2^\beta$, si n est impair :

$$\varphi(1, 2^\beta n) = \varphi(n, 2^\beta) \cdot \varphi(2^\beta, n). \tag{5}$$

Si β est pair, on obtient clairement

$$\varphi(2^\beta, n) = \sum_{k=0}^{n-1} E\left(\frac{2^\beta k^2}{n}\right) = \sum_{k=0}^{n-1} E\left(\frac{k^2}{n}\right) = \varphi(1, n). \tag{6}$$

Si β est impair, on a

$$\varphi(2^\beta, n) = \sum_{k=0}^{n-1} E\left(\frac{2^\beta k^2}{n}\right) = \sum_{k=0}^{n-1} E\left(\frac{2k^2}{n}\right) = \varphi(2, n). \tag{7}$$

Par la formule (6) du paragraphe 51 [8], on obtient

$$\varphi(2, n) = (-i)^{\frac{1}{2}(n-1)} \cdot \sqrt{n}. \tag{8}$$

Par conséquent

$$\varphi(n, 4) = 2(1 - i^n) \tag{9}$$

et

$$\varphi(n, 8) = 4\left(\cos\frac{\pi n}{4} + i \sin\frac{\pi n}{4}\right) = \sqrt{8}(1 + i)i^{\frac{1}{2}(n-1)}. \tag{10}$$

Finalement, pour $m = 2^\beta$ et $\beta \geq 4$, on a

$$\sum_{k=0}^{m-1} E\left(\frac{nk^2}{m}\right) = \sum_{k=0}^{\frac{m}{2}-1} E\left(\frac{n(2k+1)^2}{m}\right) + 2\sum_{k=0}^{\frac{m}{4}-1} E\left(\frac{4nk^2}{m}\right).$$

Dans le côté droit de la première somme, les nombres $(2k+1)^2$ sont $\equiv 1 \pmod 8$, et, si $\mu = \frac{m}{8}$, la valeur de cette somme est clairement

$$4\sum_{t=0}^{n-1} E\left(\frac{n(8t+1)}{n}\right) = 4E\left(\frac{n}{m}\right)\sum_{t=0}^{n-1} E\left(\frac{nt}{\mu}\right) = 0$$

puisque $\mu > 1$. De cela, on conclut que

$$\varphi(m, n) = 2\varphi\left(n, \frac{m}{4}\right), \tag{11}$$

quand n est impair, et que de plus, m est une puissance de 2 qui est > 8.

---

[8] *Rappel :* **Paragraphe 51, formule (6) :** $\prod_{k=1}^{\frac{1}{2}(n-1)} 2\sin\frac{(8k-4)\pi}{n} = (-1)^{\frac{1}{2}(n-1)} \cdot \sqrt{n}.$

Finalement, par des utilisations répétées des formules (5), (6), (11) et (9), on obtient, si β est pair et ≥ 2 :

$$\varphi(1, 2^\beta n) = \varphi(1, n)\varphi(n, 4)\sqrt{\frac{2^\beta}{4}} = (1+i)\sqrt{2^\beta n},$$

et par des utilisations répétées des formules (5), (7), (8), (11) et (10), si β est impair et ≥ 3 :

$$\varphi(1, 2^\beta n) = \varphi(2, n)\varphi(n, 8)\sqrt{\frac{2^\beta}{8}} = (1+i)\sqrt{2^\beta n}.$$

Ainsi, le théorème 99 est complètement démontré.

Traduction d'un extrait de *A classical introduction to modern number theory*, de Kenneth Ireland et Michael Rosen, éds. Springer-Verlag New York Inc, 1972, p. 70 et suiv.

§ 3. Sommes quadratiques de Gauss

Étant donnée la relation $(\zeta + \zeta^{-1})^2 = 2$ du paragraphe 2, on peut se demander s'il existe une relation similaire lorsqu'on remplace 2 par un nombre premier impair p. La réponse est oui, et, de plus, la loi complète de réciprocité quadratique découle de cette nouvelle relation en utilisant la méthode du paragraphe 2.

Tout au long de ce paragraphe, ζ dénotera $e^{2\pi i/p}$, une racine primitive $p^{\text{ième}}$ de l'unité.

Lemme 1. $\sum_{t=0}^{p-1} \zeta^{at}$ *est égal à* p *si* $a \equiv 0 \pmod{p}$. *Sinon, il est nul.*

Preuve : Si $a \equiv 0 \pmod{p}$ alors $\zeta^a = 1$ et donc $\sum_{t=0}^{p-1} \zeta^{at} = p$. Si $a \not\equiv 0 \pmod{p}$, alors $\zeta^a \neq 1$ et $\sum_{t=0}^{p-1} = (\zeta^{ap} - 1)/(\zeta^a - 1) = 0$.

Corollaire. $p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x,y)$, *où* $\delta(x,y) = 1$ *si* $x \equiv y \pmod{p}$ *et* $\delta(x,y) = 0$ *si* $x \not\equiv y \pmod{p}$.

Preuve : La preuve est immédiate à partir du lemme 1.

Toutes les sommes du reste de ce paragraphe seront calculées sur le domaine de 0 à $p-1$. Cela simplifiera la notation en évitant d'écrire ce fait à chaque fois.

Lemme 2. $\sum_t (t/p) = 0$ *où* (t/p) *est le symbole de Legendre.*

Preuve : Par définition $(0/p) = 0$. Parmi les $p-1$ termes restant dans la somme, la moitié sont égaux à $+1$ et la moitié valent -1, puisque par le corollaire 1 de la proposition 5.1.2, il y a autant de résidus quadratiques que de résidus non quadratiques mod p.

Nous pouvons maintenant introduire la notion de somme de Gauss.

Définition. $g_a = \sum_t (t/p)\zeta^{at}$ est appelé une somme quadratique de Gauss.

Proposition 6.3.1. $g_a = (a/p)g_1$.

Preuve : Si $a \equiv 0 \pmod{p}$ alors $\zeta^{at} = 1$ pour tout t, et $g_a = \sum (t/p) = 0$ par le lemme 2. Ceci donne le résultat dans le cas où $a \equiv 0 \pmod{p}$.

Maintenant supposons que $a \not\equiv 0 \pmod{p}$. Alors

$$\left(\frac{a}{p}\right) g_a = \sum_t \left(\frac{at}{p}\right) \zeta^{at} = \sum_x \left(\frac{x}{p}\right) \zeta^x = g_1.$$

Nous avons utilisé le fait que at couvre un système résiduel complet mod p lorsque c'est le cas pour t et le fait que (x/p) et ζ^x dépendent seulement de la classe résiduelle de x modulo p.

Puisque $(a/p)^2 = 1$ lorsque $a \not\equiv 0 \pmod{p}$, notre résultat découle de la multiplication de l'équation $(a/p)g_a = g_1$ des deux côtés par (a/p). □

Nous noterons désormais g_1 par g. Il résulte de la proposition 6.3.1 que $g_a^2 = g^2$ si $a \not\equiv 0 \pmod{p}$. Nous allons maintenant en déduire cette valeur commune.

Proposition 6.3.2. $g^2 = (-1)^{(p-1)/2} p$.

Preuve : L'idée de la preuve est d'évaluer la somme $\sum_a g_a g_{-a}$ de deux manières.

Si $a \not\equiv 0 \pmod{p}$, alors $g_a g_{-a} = (a/p)(-a/p)g^2 = (-1/p)g^2$. Il en résulte que

$$\sum_a g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1)g^2.$$

Maintenant, remarquons que

$$g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta^{a(x-y)}.$$

En sommant les deux côtés sur a et en utilisant le corollaire du lemme I, on est amené à

$$\sum_a g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \delta(x,y)p = (p-1)p.$$

En utilisant ces résultats ensemble, on obtient $(-1/p)(p-1)g^2 = (p-1)p$. Donc, $g^2 = (-1/p)p$. □

Posons $p^* = (-1)^{(p-1)/2} p$. L'équation $g^2 = p^*$ est l'analogue souhaité de l'équation $\tau^2 = 2$. Soit $q \neq p$ un autre nombre premier impair. Pour démontrer la loi de réciprocité quadratique, on procède en travaillant avec des congruences mod q dans l'anneau des entiers algébriques :

$$g^{q-1} = (g^2)^{(q-1)/2} = p^{*(q-1)/2} \equiv \left(\frac{p^*}{q}\right) \pmod{q}.$$

Par conséquent

$$g^q \equiv \left(\frac{p^*}{q}\right) g \pmod{q}.$$

En utilisant la proposition 6.1.6, on voit que

$$g^q = \left(\sum \left(\frac{t}{p}\right)\zeta^t\right)^q \equiv \left(\frac{t}{p}\right)^q \zeta^{qt} \equiv g_q \pmod{q}.$$

Il découle de cela que $g^q \equiv g_q \equiv (q/p)g \pmod{q}$. et donc

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{p}\right) g \pmod{q}.$$

En multipliant les deux côtés par g, et en utilisant le fait que $g^2 = p^*$

$$\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^* \pmod{q},$$

qui implique que

$$\left(\frac{t}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q}.$$

et finalement

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

Pour voir que ce résultat est celui que nous recherchons, il suffit de remarquer que

$$\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) = (-1)^{((q-1)/2)((p-1)/2)} \left(\frac{p}{q}\right)$$

La notion de somme de Gauss quadratique que nous avons utilisée peut être considérablement généralisée. Nous présenterons certaines de ces généralisations après avoir développé la théorie des corps finis. Les sommes de Gauss cubiques seront utilisées pour prouver la loi de réciprocité cubique, et les sommes de Gauss quartiques seront utilisées pour prouver la réciprocité biquadratique.

§ 4 **Le signe de la somme de Gauss quadratique**[9]

Selon la proposition 6.3.2, la somme de Gauss quadratique a pour valeur $\pm\sqrt{p}$ si $p \equiv 1 \pmod{4}$ et pour valeur $\pm i\sqrt{p}$ si $p \equiv 3 \pmod{4}$. Ainsi, la valeur de $g(\chi)$ est déterminée au signe près. La détermination du signe est un problème beaucoup plus difficile. La conjecture selon laquelle le signe plus est le signe correct dans chaque cas a été formulée par Gauss et consignée dans son journal en mai 1801. Ce n'est que quatre ans plus tard qu'il en a trouvé une preuve. Le 30 août 1805, Gauss a noté dans son journal qu'une preuve du "théorème très élégant mentionné en 1801" avait finalement été obtenue. Il a écrit à son ami W. Olbers le 3 septembre 1805 que rarement une semaine s'était écoulée depuis quatre ans sans qu'il n'essaie en vain de prouver sa conjecture. Finalement, selon Gauss, "Wie der Blitz einschlägt, hat sich das Räthsel gelöst..." [10].

Par la suite, des preuves ont été trouvées par Dirichlet, Cauchy, Kronecker, Mertens, Schur et d'autres. Dans cette section, nous présentons l'une des preuves de Kronecker.

[9] Dans ce paragraphe, la somme de Gauss g sera notée $g(\chi)$ avec $\chi(t) = (t/p)$ par définition.

[10] "comme la foudre frappe l'énigme a été résolue."

Comme dans la section précédente $\zeta = e^{2\pi i/p}$, alors $1, \zeta, \ldots, \zeta^{p-1}$, sont les racines de $x^p - 1$.

Proposition 6.4.1. *Le polynôme* $1 + x + \ldots + x^{p-1}$ *est irréductible dans* $\mathbb{Q}[x]$.

Preuve : Par l'exercice 4 à la fin de ce chapitre ("lemme de Gauss"), il suffit de montrer que $1 + x + \ldots + x^{p-1}$ n'a pas de factorisation non triviale dans $\mathbb{Z}[x]$. Supposons, au contraire, que $1 + x + x^2 + \ldots + x^{p-1} = f(x)g(x)$ où $f(x), g(x) \in \mathbb{Z}[x]$ et chacun a un degré supérieur à un. En posant $x = 1$, on obtient $p = f(1)g(1)$. Par conséquent, on peut supposer $g(1) = 1$. En utilisant une barre pour désigner la réduction modulo p, nous concluons que $\overline{g}(\overline{1}) \neq \overline{0}$. D'autre part, puisque $p \left| \binom{p}{j} \right., j = 1, \ldots, p-1$, on a $x^p - 1 = (x-1)^p \pmod p$ et la division des deux côtés par $x-1$ montre que $1 + x + \ldots + x^{p-1} = (x-1)^{p-1} \pmod p$. D'après le théorème 2, chapitre 1 et la proposition 3.3.2, il s'ensuit que $g(x) = (x-1)^s \pmod p$ pour un entier positif s. Cependant, cela contredit le fait que $g(\overline{1}) \neq (\overline{0})$, et la preuve est complète. □

En combinant la proposition ci-dessus avec la proposition 6.1.7, on voit que si $g(\zeta) = 0$ pour $g(x) \in \mathbb{Q}[x]$ alors $1 + x + \ldots + x^{p-1} | g(x)$. Cette observation sera utile ultérieurement.

Proposition 6.4.2. $\displaystyle\prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2 = (-1)^{(p-1)/2} p.$

Preuve : On a $x^p - 1 = (x-1)\displaystyle\prod_{j=1}^{p-1}(x - \zeta^j)$. Divisons par $x - 1$ et posons $x = 1$ pour obtenir $p = \displaystyle\prod_r (1 - \zeta^r)$, sur tout ensemble complet de classes résiduelles modulo p. Les entiers $\pm(4k-2), k = 1, 2, \ldots, (p-1)/2$ sont facilement considérés comme un tel système de résidus

$$\begin{aligned} p &= \prod (1 - \zeta^{4k-2}) \prod (1 - \zeta^{-(4k-2)}) \\ &= \prod (\zeta^{-(2k-1)} - \zeta^{2k-1}) \prod (\zeta^{2k-1} - \zeta^{-(2k-1)}) \\ &= (-1)^{(p-1)/2} \prod (\zeta^{2k-1} - \zeta^{-(2k-1)})^2, \end{aligned}$$

tous les produits se calculant pour $k = 1, 2, \ldots, (p-1)/2$.

Proposition 6.4.3.

$$\prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = \begin{cases} \sqrt{p}, & \text{si} \quad p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{si} \quad p \equiv 3 \pmod 4. \end{cases}$$

Preuve : Par la proposition 6.4.2, on doit seulement calculer le signe du produit. Le produit est égal à

$$i^{(p-1)/2} \prod_{k=1}^{(p-1)/2} 2 \sin \frac{(4k-2)\pi}{p}.$$

Mais $\sin((4k-2)/p)\pi < 0$ si $(p+2)/4 < k \leq (p-1)/2$. Il découle de cela que le produit a $(p-1)/2 - [(p+2)/4]$ termes négatifs et on voit facilement que ce nombre est égal à $(p-1)/4$ ou $(p-3)/4$, selon que $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$, respectivement. Le résultat en découle immédiatement. □

Par la proposition 6.3.2 et la proposition 6.4.2, on sait que

$$g(\chi) = \varepsilon \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}), \tag{1}$$

où $\varepsilon = \pm 1$. L'évaluation de la somme de Gauss est complétée par la proposition 6.4.3 si on peut montrer que $\varepsilon = +1$. L'argument suivant de Kronecker montre que c'est le cas. Voir aussi l'exercice 22.

Proposition 6.4.4. $\varepsilon = +1$.

Preuve : Considérons le polynôme

$$f(x) = \sum_{j=1}^{p-1} \chi(j) x^j - \varepsilon \prod_{k=1}^{(p-1)/2} (x^{2k-1} - x^{p-(2k-1)}). \tag{2}$$

Alors $f(\zeta) = 0$ par (1) et $f(1) = 0$ par le lemme 2. Par le commentaire précédant la proposition 6.4.2 et le fait que $1 + x + \ldots + x^{p-1}$ et $x - 1$ sont premiers entre eux, on conclut que $x^p - 1 | f(x)$. Écrivons que $f(x) = (x^p - 1)h(x)$ et remplaçons x par e^z pour obtenir

$$\sum_{j=1}^{p-1} \chi(j) e^{jz} - \varepsilon \prod_{k=1}^{(p-1)/2} (e^{(2k-1)z} - e^{z(p-(2k-1))}) = (e^{pz} - 1)h(e^z). \tag{3}$$

On voit facilement que le coefficient de $z^{(p-1)/2}$ sur le côté gauche de (3) est égal à

$$\frac{\displaystyle\sum_{j=1}^{p-1} \chi(j) j^{(p-1)/2}}{((p-1)/2)!} - \varepsilon \prod_{k=1}^{(p-1)/2} (4k - p - 2)$$

D'un autre côté par l'exercice 21, le coefficient de $z^{(p-1)/2}$ du côté droit de (3) est pA/B où $p \nmid B$, A et B étant des entiers. En rendant les coefficients égaux, en multipliant par $B((p-1)/2)!$ et en réduisant modulo p, on obtient que

$$\begin{aligned}
\sum_{j=1}^{p-1} \chi(j) j^{(p-1)/2} &\equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{(p-1)/2} (4k-2) \pmod p \\
&\equiv \varepsilon(2 \cdot 4 \cdot 6 \ldots (p-1)) \prod_{k=1}^{(p-1)/2} (2k-1) \\
&\equiv \varepsilon(p-1)! \\
&\equiv -\varepsilon \pmod p
\end{aligned}$$

en utilisant le théorème de Wilson (corollaire de la proposition 4.1.1).

Par la proposition 5.1.2 $j^{(p-1)/2} \equiv \chi(j) \pmod{p}$, de telle façon qu'on a

$$\sum_{j=1}^{p-1} \chi(j)^2 \equiv (p-1) \equiv -\varepsilon \pmod{p}$$

et par conséquent

$$\varepsilon \equiv 1 \pmod{p}.$$

Puisque $\varepsilon = \pm 1$, on conclut finalement que $\varepsilon = 1$. Cela conclut la preuve. □

On peut énoncer le résultat de la façon suivante :

Théorème 1. *La valeur de la somme quadratique de* Gauss $\sum g(\chi)$ *est égale à*

$$g(\chi) = \begin{cases} \sqrt{p}, & \text{si} \quad p \equiv 1 \pmod{4}, \\ \\ i\sqrt{p}, & \text{si} \quad p \equiv 3 \pmod{4}. \end{cases}$$

Notes

Dans le célèbre onzième supplément à *Vorlesungen über Zahlentheorie* de J. P. G. Lejeune-Dirichlet [127] (1893), R. Dedekind a introduit le concept de nombre algébrique (§ 164) ainsi que celui d'entier algébrique (§ 173). Pourtant l'utilisation de certains entiers algébriques tels que les sommes de Gauss pour démontrer la loi de réciprocité quadratique était apparue plus tôt chez Eisenstein, Jacobi, et d'autres. Parmi les différentes preuves de ce théorème données par Gauss, la quatrième (1811) et la sixième (1818) sont d'une importance centrale. La quatrième preuve est un corollaire du remarquable calcul que Gauss a effectué de la somme classique de Gauss. Alors que, comme on l'a mentionné dans le paragraphe 6, il a démontré ce résultat en 1805, ce n'est qu'en 1811 qu'il a publié la démonstration dans son célèbre article "Summierung gewisser Reihen von besonderer Art" [34]. Dans cet article, il montre plus généralement que si n est un entier positif quelconque alors $\sum_{t \equiv 0}^{n-1} \zeta^{t^2}$ prend la valeur $\sqrt{n}$ ou $i\sqrt{n}$ selon que $n \equiv 1 \pmod 4$ ou $n \equiv 3 \pmod 4$. Ici, $\zeta = e^{2ni/n}$ [11], l'argument est assez ingénieux. On peut trouver la preuve en anglais dans Nagell [60], p. 174-180. Il n'est pas difficile de dériver la loi de réciprocité quadratique de ce résultat (voir, par exemple, Dirichlet [125], p. 253-256).

La sixième et dernière preuve publiée de Gauss de la loi de réciprocité quadratique a été publiée en 1818 sous le titre "Neue Beweise und Erweiterungen des Fundamentalsatzes in der Lehre von den Quadratischen Resten" [34], p. 496-510. Gauss mentionne dans l'introduction de cet article que pendant des années, il avait cherché une méthode qui pourrait se généraliser aux cas

[11] coquille ? $e^{2\pi i/n}$

cubique et biquadratique et que finalement ses efforts inlassables furent couronnés de succès ("... die unermüdliche Arbeit wurde endlich von glücklichem Erfolge gekrönt.[12]"). Le but de la publication de la sixième preuve, dit-il, était de conclure la partie de l'arithmétique supérieure traitant des résidus quadratiques et de dire, en un sens, adieu ("... und so diesem Teile der höheren Arithmetik gewissermassen Lebewohl zu sagen."[13]) Dans cette démonstration, GAUSS considère le polynôme $f_k(x) = \sum_{t=0}^{p-1} \chi(t)x^{kt}$ et prouve, sans utiliser de racines d'unité, que $1 + x + \ldots + x^{p-1}$ divise $f_1(x)^2 - (-1)^{(p-1)/2}p$ aussi bien que $f_q(x) - (q/p)f_1(x)$. La réciprocité en découle en notant que $f_q(x) \equiv f_1(x)^q \pmod{q}$. La démonstration que nous avons donnée dans la section 3 revient à poser $x = \zeta_p$, dans ce qui précède et à travailler avec des congruences dans l'anneau des entiers algébriques. Cette observation a été faite (au moins) par Cauchy, Eisenstein et Jacobi (par ordre alphabétique) et constitue un tremplin vers l'étude des lois de réciprocité supérieures via les sommes de GAUSS.

L'étudiant débutant aura intérêt à étudier plusieurs introductions classiques à la théorie des nombres algébriques. Outre Dirichlet et Dedekind mentionnés précédemment, nous citons E. Landau [165] et E. Hecke [44]. De nombreux ouvrages de niveaux de difficulté variables ont récemment paru. Nous mentionnons ici W. Adams et L. Goldstein [84], LeVeque [180], ainsi que H. Pollard et H. Diamond [63]. L'ouvrage de Hecke vient de paraître en anglais (*Algebraic Number Theory*, Springer-Verlag, 1981).

[12] "...le travail acharné a finalement été couronné d'un heureux succès".

[13] "...et ainsi dire au revoir à cette partie de l'arithmétique supérieure."