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

V.-A. LEBESGUE

Sur le symbole $\left(\frac{a}{b}\right)$ et quelques-unes de ses applications

Journal de mathématiques pures et appliquées 1re série, tome 12 (1847), p. 497-517.
<http://www.numdam.org/item?id=JMPA_1847_1_12__497_0>

Sur le symbole $\left(\frac{a}{b}\right)$ *et quelques-unes de ses applications;*

Par M. V.-A. LEBESGUE,

Correspondant de l'Institut, Professeur à la Faculté des Sciences de Bordeaux.

I.

Définition du symbole $\left(\frac{a}{b}\right)$, *d'après Legendre et M. Jacobi.*

Soient a, b deux nombres entiers premiers entre eux, qui ne sont pas tous deux négatifs et dont le second est impair; $\left(\frac{a}{b}\right)$ sera $+1$ ou -1, selon les cas dont voici l'énumération :

1°. Si b est un nombre premier positif, $\left(\frac{a}{b}\right)$ sera $+1$ ou -1, selon que b sera résidu ou non-résidu quadratique de p; autrement, $\left(\frac{a}{b}\right)$ sera le reste ± 1 de $a^{\frac{b-1}{2}}$ divisé par b (Legendre).

2°. Si b est un nombre composé positif, $b = pqr\ldots$, les facteurs p, q, r,... étant des nombres premiers égaux ou non, on aura

$$\left(\frac{a}{b}\right) = \left(\frac{a}{pqr\ldots}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\left(\frac{a}{r}\right)\cdots \text{ (Jacobi)}.$$

3°. Si b est un nombre négatif, on fera

$$\left(\frac{a}{-b}\right) = \left(\frac{a}{b}\right).$$

ou bien encore, en posant

$$\left(\frac{a}{-b}\right) = \left(\frac{a}{-1}\right)\left(\frac{a}{b}\right),$$

on fera

$$\left(\frac{a}{-1}\right) = 1 \text{ (Jacobi)}.$$

Voici des conséquences immédiates de ces définitions :

4°. $$\left(\frac{p}{q}\right)^2 = 1, \quad \left(\frac{p}{q}\right)^{2k} = 1, \quad \left(\frac{p}{q}\right)^{2k+1} = \left(\frac{p}{q}\right).$$

5°. $$\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\cdots = \left(\frac{a}{pq\ldots}\right).$$

6°. $$\left(\frac{abc\ldots}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\cdots.$$

7°. $$\left(\frac{k}{p}\right) = \left(\frac{l}{p}\right),$$

si l'on a $$k \equiv l \pmod{p}.$$

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

A ces propositions on joindra les suivantes, dont la démonstration exige quelques développements :

9°. $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \quad \left(\frac{-2}{p}\right) = (-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}} = (-1)^{\frac{(p-1)(p-3)}{8}}.$$

10°. $$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

ou

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

Dans cette dernière équation, p et q sont deux nombres impairs.

II.

Sur la démonstration des équations fondamentales.

Si l'on voulait énoncer les propositions exprimées par les équations précédentes, il suffirait de dire que les nombres premiers à un nombre impair p se partagent en deux classes : la première renfermant les nombres k, qui donnent

$$\left(\frac{k}{p}\right) = 1 ;$$

la seconde renfermant les nombres k, qui donnent

$$\left(\frac{k}{p}\right) = -1.$$

Pour p premier, la première classe est celle des résidus quadratiques, et la seconde, celle des non-résidus.

Pour p composé, $p = qrs\ldots$ (q, r, s,... étant premiers), la première classe est celle des nombres qui sont non-résidus quadratiques d'un nombre pair (0, 2, 4,...) des facteurs q, r, s,...; la seconde classe est celle des nombres qui sont non-résidus d'un nombre impair des mêmes facteurs q, r, s,....

Voici maintenant les principaux énoncés :

« Des nombres congrus suivant le module p sont de même classe.

» Un produit $abc\ldots$ sera de première ou de seconde classe relati-
» vement à p, selon que les facteurs $(a, b, c, \ldots)$ de seconde classe
» seront en nombre pair ou impair.

» Le nombre -1 est de première classe relativement aux nombres
» de forme $4q + 1$, et de seconde classe relativement aux nombres de
» forme $4q - 1$.

» Le nombre 2 est de première classe relativement aux nombres de
» forme $8k \pm 1$, et de seconde classe relativement aux nombres de
» forme $8k \pm 3$.

» Le nombre -2 est de première classe relativement aux nombres
» de forme $8k + 1$, $8k + 3$, et de seconde classe relativement aux
» nombres $8k + 5$, $8k + 7$.

» Les nombres premiers positifs p et q sont de même classe, l'un
» par rapport à l'autre quand p et q ne sont pas tous deux de forme
» $4q - 1$. C'est le contraire si p et q sont tous deux de forme $4q - 1$.
(Cette dernière proposition est la loi de réciprocité de Legendre.)

» La loi de Legendre s'étend à deux nombres quelconques positifs
» impairs. »

La démonstration de l'équation

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

pour p composé, revient à montrer qu'en posant $p = qrs\ldots$, ce qui donne

$$\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right)\left(\frac{-1}{r}\right)\left(\frac{-1}{s}\right)\cdots = (-1)^{\frac{q-1}{2}+\frac{r-1}{2}+\frac{s-1}{2}+\cdots},$$

on peut remplacer l'exposant $\frac{q-1}{2}+\frac{r-1}{2}+\frac{s-1}{2}+\cdots$ par l'exposant $\frac{qrs\ldots-1}{2}=\frac{p-1}{2}$. Il suffit donc de démontrer que les deux nombres $\frac{q-1}{2}+\frac{r-1}{2}+\cdots$ et $\frac{qr\ldots-1}{2}$ diffèrent d'un multiple de 2, puisque dans $(-1)^{\alpha+2\beta}=(-1)^{\alpha}(-1)^{2\beta}$ on peut supprimer le facteur $(-1)^{2\beta}=1$, quel que soit le signe de β. Or

$$\frac{q-1}{2}+\frac{r-1}{2}=\frac{q+r-2}{2};$$

donc

$$\frac{qr-1}{2}-\left(\frac{q-1}{2}+\frac{r-1}{2}\right)=\frac{qr-q-r+1}{2}=\frac{(q-1)(r-1)}{2},$$

nombre pair. Ainsi l'exposant $\frac{qr-1}{2}$ peut remplacer $\frac{q-1}{2}+\frac{r-1}{2}$. La démonstration est la même pour tant de facteurs qu'on voudra.

Quand l'équation

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

a été démontrée pour p premier, on passe, comme pour $\left(\frac{-1}{p}\right)$, au cas de p composé; cela fait, $\left(\frac{2}{p}\right)$ et $\left(\frac{-1}{p}\right)$ donnent $\left(\frac{-2}{p}\right)$. Il suffit donc de démontrer l'équation

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

pour p premier. C'est ce que M. Gauss fait ainsi :

Divisez les produits

$$k,\quad 2k,\quad 3k,\ldots,\quad \frac{p-1}{2}k,$$

par p, de manière à obtenir des restes positifs et $<p$,

$$r_1,\quad r_2,\quad r_3,\ldots,\quad r_{\frac{p-1}{2}};$$

si les restes $>\frac{p}{2}$ sont en nombre ν, vous aurez

$$\left(\frac{k}{p}\right)=(-1)^{\nu}.$$

Posez, en effet,

$$ak = p \cdot e\left(\frac{ak}{p}\right) + r_a;$$

a étant successivement $1, 2, 3, \ldots, \frac{p-1}{2}$, vous aurez $\frac{p-1}{2}$ équations qui, par la multiplication, donneront

$$1.2.3\ldots\left(\frac{p-1}{2}\right) k^{\frac{p-1}{2}} \equiv (-1)^{\nu}\ 1.2.3\ldots\frac{p-1}{2} \pmod{p},$$

d'où

$$\left(\frac{k}{p}\right) = (-1)^{\nu}.$$

Pour $k = 2$, ou $k = -2$, on trouve de suite les valeurs de ν, et l'on en conclut celles de $\left(\frac{2}{p}\right)$ et $\left(\frac{-2}{p}\right)$.

Quant à la démonstration de l'équation

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

pour le cas de p, q nombres premiers, positifs et impairs, voici comment M. Gauss l'a trouvée. Puisque l'on a

$$\left(\frac{k}{p}\right) = (-)^{\nu},$$

il suffit de savoir si ν est pair ou impair; or par l'addition des $\frac{p-1}{2}$ équations

$$a.k = p.e\left(\frac{ak}{p}\right) + r_a,$$

on trouve sans peine

$$\nu \equiv e\left(\frac{k}{p}\right) + e\left(\frac{2k}{p}\right) + \cdots + e\left(\frac{\frac{p-1}{2}k}{p}\right) \pmod{2},$$

k étant impair; ou bien encore, en posant

$$\varphi(k, p) = e\left(\frac{k}{p}\right) + e\left(\frac{2k}{p}\right) + \cdots + e\left(\frac{\frac{p-1}{2}k}{p}\right),$$

$$\nu \equiv \varphi(k, p) \pmod{2}.$$

Puisque l'on a

$$\left(\frac{q}{p}\right) = (-1)^{\varphi(q,p)},$$

et de même

$$\left(\frac{p}{q}\right) = (-1)^{\varphi(p,q)},$$

il en résultera

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\varphi(q,p)+\varphi(p,q)}.$$

Or M. Gauss a montré, par une transformation très-simple, que l'on a toujours

$$\varphi(q,p) + \varphi(p,q) = \frac{p-1}{2}\cdot\frac{q-1}{2};$$

de là la loi de réciprocité.

Au reste, comme l'a remarqué M. Eisenstein (Journal de M. Crelle, tome XXVIII), l'équation

$$\varphi(q,p) + \varphi(p,q) = \frac{p-1}{2}\cdot\frac{q-1}{2}$$

résulte presque immédiatement d'une construction géométrique fort simple.

Prenez deux axes de coordonnées rectilignes Ox, Oy, divisez-les, à partir de l'origine O, en parties égales à l'unité; par les points de division de chaque axe menez des parallèles à l'autre : ces deux systèmes de droites parallèles détermineront par leur intersection tous les points dont les coordonnées sont des nombres entiers. Menez par l'origine la droite ayant pour équation

$$y = \frac{q}{p}x,$$

puis formez le parallélogramme ayant pour côtés

$$Ox = \frac{1}{2}(p+1), \quad Oy = \frac{1}{2}(q+1).$$

Il renfermera $\frac{p-1}{2}\cdot\frac{q-1}{2}$ points d'intersection. La droite $y = \frac{q}{p}x$ partagera le parallélogramme en deux parties, dont l'une contiendra $\varphi(p,q)$ points d'intersection, et l'autre $\varphi(q,p)$; on aura donc

l'équation

$$\varphi(p, q) + \varphi(q, p) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

L'assertion précédente résulte de ce que pour toute courbe $y = \varphi(x$, si l'on fait $x = m$, m étant un entier, l'expression $e\varphi(m)$ indiquera combien, sur l'ordonnée répondant à l'abscisse entière m, il y a entre l'axe des x et la courbe, de points ayant une ordonnée aussi entière. Dans certains cas, mais non dans celui de la ligne $y = \frac{q}{p} x$, un point pourrait se trouver sur la courbe.

Quand l'équation

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

a été prouvée pour des nombres positifs premiers, on passe sans difficulté au cas de p premier et q composé, puis de ce cas à celui de p et q composés; enfin, de ce cas, on passe à celui où l'un des nombres p, q est négatif. Pour la démonstration de ce dernier cas, il suffit de remarquer que l'on a toujours $(-1)^{\alpha} = (-1)^{-\alpha}$, c'est-à-dire que l'on peut changer le signe de l'exposant de -1.

III.

Calcul du symbole $\left(\frac{a}{b}\right)$.

C'est une conséquence directe des formules qui précèdent.

Soit, pour exemple, proposé de calculer $\left(\frac{-3778}{773}\right)$; comme on a $-3778 = -1.2.1889$, il en résultera

$$\left(\frac{-3778}{773}\right) = \left(\frac{-1}{773}\right)\left(\frac{2}{773}\right)\left(\frac{1889}{773}\right);$$

et comme $773 = 4.193 + 1 = 8.96 + 5$, on aura

$$\left(\frac{-1}{773}\right) = 1, \quad \left(\frac{2}{773}\right) = -1, \quad \left(\frac{-3778}{773}\right) = -\left(\frac{1889}{773}\right).$$

D'ailleurs la division donne $1889 = 2.773 + 343$; de là

$$\left(\frac{1889}{773}\right) = \left(\frac{343}{773}\right).$$

Par la loi de réciprocité, on a

$$\left(\frac{343}{773}\right) = \left(\frac{773}{343}\right);$$

or $773 = 343 . 2 + 87$, donc

$$\left(\frac{773}{343}\right) = \left(\frac{87}{343}\right).$$

Mais, par la loi de réciprocité, on a

$$\left(\frac{87}{343}\right) = -\left(\frac{343}{87}\right);$$

et comme $343 = 87 . 3 + 82$, il en résulte

$$\left(\frac{343}{87}\right) = \left(\frac{82}{87}\right) = \left(\frac{2}{87}\right)\left(\frac{41}{87}\right) = \left(\frac{41}{87}\right) = \left(\frac{87}{41}\right).$$

De plus, $87 = 2 . 41 + 5$ donne

$$\left(\frac{87}{41}\right) = \left(\frac{5}{41}\right) = \left(\frac{41}{5}\right),$$

et $41 = 5 . 8 + 1$ donne enfin

$$\left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

On aura donc

$$\left(\frac{-3778}{773}\right) = -1 \times -\left(\frac{343}{87}\right) = \left(\frac{343}{87}\right) = 1.$$

Ainsi tout dépend de la recherche du plus grand commun diviseur de deux nombres. Or cette recherche peut être effectuée de plusieurs manières.

On peut prendre tous les quotients par défaut, ou de manière à avoir des restes positifs plus petits que les diviseurs; c'est la méthode ordinaire. On peut prendre les quotients de manière à obtenir des restes impairs; on obtient ainsi l'algorithme de M. Eisenstein (Journal de M. Crelle, tome XXVII), dont l'énoncé est très-simple. On peut prendre les quotients de manière à obtenir des restes pairs $\pm 2^m r$, en supposant r impair; dans ce cas, r sert de nouveau diviseur. Le nombre des divisions devient d'autant moindre que les facteurs 2^m sont

plus grands. L'algorithme est d'un énoncé moins simple; mais, en général, il est préférable pour la brièveté du calcul.

Algorithme de M. Eisenstein. — Soit à calculer $\left(\frac{p}{p_1}\right)$, où l'on suppose p, p_1 positifs impairs premiers entre eux et tels que $p > p_1$, tous les cas pouvant se ramener à celui-là. On divisera p par p_1, on prendra le quotient pair afin d'avoir un reste impair, et comme il pourra être positif ou négatif, on le représentera par $\varepsilon_1 p_2$, ε_1 étant ± 1, et p_2 un entier positif $< p_1$. On opérera sur p_1 et p_2 comme sur p et p_1, et comme ces deux nombres sont premiers entre eux, on finira par tomber sur un reste $\varepsilon_{n+1} = \pm 1$. Soient donc les équations

$$p = p_1 Q_1 + \varepsilon_1 p_2, \quad p_1 = p_2 Q_2 + \varepsilon_2 p_3, \ldots, \quad p_{i-1} = p_i Q_i + \varepsilon_i p_{i+1}, \ldots,$$
$$p_n = p_{n+1} Q_{n+1} + \varepsilon_{n+1}.$$

Si l'on représente par ν le nombre des équations

$$p_{i-1} = p_i Q_i + \varepsilon_i p_{i+1},$$

où p_i et $\varepsilon_i p_{i+1}$ sont tous deux de forme $4k - 1$, on aura

$$\left(\frac{p}{p_1}\right) = (-1)^{\nu}.$$

Cela se prouve sans difficulté comme plus haut.

Autre algorithme. — Si l'on prend, au contraire, les quotients impairs afin d'avoir des restes pairs, on aura la suite d'équations

$$p = p_1 Q_1 + 2^{m_1}\varepsilon_1 p_2, \quad p_1 = p_2 Q_2 + 2^{m_2}\varepsilon_2 p_3, \ldots, \quad p_{i-1} = p_i Q_i + 2^{m_i}\varepsilon_i p_{i+1}, \ldots$$
$$p_n = p_{n+1} Q_{n+1} + 2^{m_{n+1}}\varepsilon_{n+1}.$$

Si l'on représente par ν le nombre des équations

$$p_{i-1} = p_i Q_i + 2^{m_i}\varepsilon_i p_{i+1},$$

où p_i et $\varepsilon_i p_{i+1}$ sont tous deux de forme $4k - 1$, et par μ le nombre des équations, où à un diviseur p_i de forme $8k \pm 3$ réponde un facteur 2^{m_i} à exposant impair, on aura

$$\left(\frac{p}{p_1}\right) = (-1)^{\mu+\nu}.$$

Autre algorithme. — Si l'on fait la recherche du plus grand commun diviseur à la manière ordinaire, et que l'on représente les restes successifs par $2^{m_1}p_2$, $2^{m_2}p_3$,..., 1 ; et que l'on désigne par

λ le nombre des exposants impairs m_i répondant à $p_i = 8k \pm 3$;

μ le nombre des exposants impairs m_i répondant à $p_{i+2} = 8k \pm 3$;

ν le nombre des diviseurs p_i de forme $4k - 1$ répondant à des restes où p_{i+1} a la même forme ;

on aura

$$\left(\frac{p}{p_1}\right) = (-1)^{\lambda+\mu+\nu}.$$

En appliquant ces trois règles à $\left(\frac{3785}{2933}\right)$, on trouve :

1°. $3785 = 2933.2 - 2081$, $2933 = 2081.2 - 1229$, $2081 = 1229.2 - 377$;
$1229 = 377.4 - 279$, $377 = 279.2 - 181$, $279 = 181.2 - 85$;
$181 = 85.2 + 11$, $85 = 11.8 - 3$, $11 = 3.4 - 1$.

Ici $\nu = 2$ et $\left(\frac{3785}{2933}\right) = 1$.

2°. La deuxième règle donne

$3785 = 2933.1 + 4.213$, $2933 = 213.13 + 4.41$, $213 = 41.5 + 8$.

Ici $\mu = 0$, $\nu = 0$ et $\left(\frac{3785}{2933}\right) = 1$.

3°. La troisième règle donne

$3785 = 2933.1 + 852$, $2933 = 852.3 + 377$, $852 = 377.2 + 98$;
$377 = 98.3 + 83$, $98 = 83.1 + 15$, $83 = 15.5 + 8$;
$15 = 8.1 + 7$, $8 = 7.1 + 1$.

Ici, à cause de $852 = 2^2.213$, $98 = 2.49$, $8 = 2^3$, on trouve

$$\lambda = 0,\ \mu = 1,\ \nu = 1 \text{ et } \left(\frac{3785}{2933}\right) = 1.$$

Il est bon de faire remarquer que, dans tous les cas, si l'on est

conduit à une division donnant le reste $\pm 2^m r^2$, toutes les divisions suivantes sont inutiles pour le calcul du symbole $\left(\frac{p}{p_1}\right)$. (Troisième exemple : $98 = 2 \cdot 49 = 2 \cdot 7^2$.)

Règle tirée du calcul de

$$\varphi(k, p) = e\left(\frac{k}{p}\right) + e\left(\frac{2k}{p}\right) + \ldots + e\left(\frac{\frac{p-1}{2}k}{p}\right).$$

M. Gauss a prouvé que l'on a, pour k impair,

$$\left(\frac{k}{p}\right) = (-1)^{\varphi(k, p)};$$

et, pour k pair,

$$\left(\frac{k}{p}\right) = (-1)^{\varphi(k, p) + \frac{p^2-1}{8}}.$$

Il a d'ailleurs donné un algorithme qui fournit la valeur exacte de $\varphi(k, p)$, d'où l'on déduit une règle fort simple pour déterminer si $\varphi(k, p)$ est pair ou impair. Cette même règle donnera donc la valeur de $\left(\frac{k}{p}\right)$ pour le cas de p nombre premier. Nous verrons plus loin qu'elle s'étend au cas de p nombre impair quelconque. L'algorithme de M. Gauss résout donc complétement la question; il est également fondé sur la recherche d'un plus grand commun diviseur. Mais, comme il emploie non-seulement les restes, mais encore les quotients, les algorithmes précédents seront préférables pour la brièveté du calcul. Pour cet algorithme, *voyez* le Mémoire intitulé : *Démonstration nouvelle et développements nouveaux du théorème fondamental de la théorie des résidus quadratiques*, présentés à la Société royale des Sciences de Gœttingue, le 11 février 1817, par M. C.-F. Gauss. — *Voyez* aussi le tome III de ce Journal, page 142.

IV.

Première application. — Détermination du signe des sommes

$$S = \sum \sin i^2 \frac{2h\pi}{p}, \quad C = \sum \cos i^2 \frac{2h\pi}{p},$$

prises de $i = 0$ *à* $i = p - 1$, h *est premier à* p.

Dans son Mémoire sur la sommation de certaines séries singulières, M. Gauss a donné une règle pour la détermination du signe des sommes S, C, dont la valeur absolue est $\sqrt{p}$, quand elles ne sont pas nulles.

Cette règle peut être réduite à une expression plus simple, et si l'on pose $p = 2^m p'$, p' étant impair, le symbole $\left(\frac{h}{p'}\right)$ fera connaître les sommes S et C au moyen des règles suivantes. Soient

$$S = \sum \sin i^2 \frac{2h\pi}{p} = A \left(\frac{h}{p'}\right) \sqrt{p}, \quad C = \sum \cos i^2 \frac{2h\pi}{p} = B \left(\frac{h}{p'}\right) \sqrt{p},$$

les nombres A et B auront les valeurs suivantes :

$m = 0$, $p' = 4q + 1$, $A = 0$, $B = 1$;

$m = 0$, $p' = 4q - 1$, $A = 1$, $B = 0$;

$m = 1$, $p' = 4q \pm 1$, $A = 0$, $B = 0$;

$m = 2n$, $p' = 4q + 1$, $A = (-1)^{\frac{h-1}{2}}$, $B = 1$;

$m = 2n$, $p' = 4q - 1$, $A = 1$, $B = (-1)^{\frac{h-1}{2}}$;

$m = 2n + 1$, $p' = 4q + 1$, $A = (-1)^{\frac{(h-1)(h-3)}{8}}$, $B = (-1)^{\frac{h^2-1}{8}}$;

$m = 2n + 1$, $p' = 4q - 1$, $A = (-1)^{\frac{h^2-1}{8}}$, $B = (-1)^{\frac{(h-1)(h-3)}{8}}$.

Ce tableau montre que le changement de $p' = 4q + 1$ en $p' = 4q - 1$ ne fait que changer A en B, et réciproquement. Je vais présenter brièvement la démonstration, renvoyant pour plus de détails au Mémoire de M. Gauss.

Si l'on pose

$$\sum x^{i^2 h} = 1 + x^h + x^{4h} + x^{9h} + \ldots + x^{(p-1)^2 h} = \mathrm{F}(h, p),$$

sous la condition de h premier à p et de $x^p = 1$, qui donne

$$x = \cos \frac{2\pi}{p} + \sin \frac{2\pi}{p} \sqrt{-1},$$

on aura, pour cette valeur de x,

$$\mathrm{F}(h, p) = \sum \left(\cos i^2 \frac{2h\pi}{p} + \sin i^2 \frac{2h\pi}{p} \sqrt{-1} \right) = \mathrm{C} + \mathrm{S} \sqrt{-1}.$$

C'est donc du calcul de $\mathrm{F}(h, p)$ que dépend celui des sommes désignées par S et C.

Soit $p = a.b.c...$, les nombres a, b, c,... étant premiers entre eux: on sait que, pour trouver un nombre k tel que l'on ait

$$k \equiv \alpha \pmod{a}, \qquad k \equiv \beta \pmod{b}, \qquad k \equiv \gamma \pmod{c}, \quad \text{etc.},$$

il suffit de poser

$$\mathrm{A} \frac{p}{a} \equiv 1 \pmod{a}, \quad \mathrm{B} \frac{p}{b} \equiv 1 \pmod{b}, \quad \mathrm{C} \frac{p}{c} \equiv 1 \pmod{c}, \quad \text{etc.},$$

et de prendre

$$k \equiv \mathrm{A} \frac{p}{a} \alpha + \mathrm{B} \frac{p}{b} \beta + \mathrm{C} \frac{p}{c} \gamma + \ldots \pmod{p = abc\ldots}.$$

Or, si l'on prend successivement :

Pour α, les nombres $1, 4, 9, \ldots, (a-1)^2$;
Pour β, les nombres $1, 4, 9, \ldots, (b-1)^2$;
Pour γ, les nombres $1, 4, 9, \ldots, (c-1)^2$;

et ainsi de suite, on trouvera,

Pour k ou i^2, les nombres $1, 4, 9, \ldots, (p-1)^2$.

Il suit de là que l'équation

$$x^{i^2 h} = \left(x^{\frac{p}{a}}\right)^{\alpha^2 \mathrm{A} h} \cdot \left(x^{\frac{p}{b}}\right)^{\beta^2 \mathrm{B} h} \cdot \left(x^{\frac{p}{c}}\right)^{\gamma^2 \mathrm{C} h} \ldots$$

donnera, en supposant

$$x^{\frac{p}{a}} = x_1, \quad x^{\frac{p}{b}} = x_2, \quad x^{\frac{p}{c}} = x_3, \quad \text{etc.},$$

et, par suite,

$$x_1^a = 1, \quad x_2^b = 1, \quad x_3^c = 1, \quad \text{etc.},$$

l'équation fondamentale

$$F(h, p) = F(h, abc\ldots) = F(Ah, a).F(Bh, b).F(Ch, c)\ldots,$$

en supposant

$$F(Ah, a) = 1 + x_1^{Ah} + x_1^{4Ah} + x_1^{9Ah} + \ldots + x_1^{(a-1)^2 Ah} = \sum x_1^{a^2 Ah};$$

et ainsi des autres.

Il suffit donc de calculer $F(Ah, a)$ dans l'hypothèse de a premier ou puissance d'un nombre premier.

Soit donc $a = q^m$; comme dans la somme $\sum x_1^{a^2 Ah}$ on peut négliger, comme étant égale à zéro, la somme des termes où a n'est pas divisible par q, on trouvera sans difficulté, pour le cas de $q = 2$,

1°. $$F(Ah, 2) = 0;$$

2°. $$F(Ah, 4) = \left(1 + \sin\frac{Ah\pi}{2}\sqrt{-1}\right)\sqrt{4},$$

$$= \left[1 + (-1)^{\frac{Ah-1}{2}}\sqrt{-1}\right]\sqrt{4},$$

et généralement,

$$F(Ah, 2^{2m}) = \left[1 + (-1)^{\frac{Ah-1}{2}}\sqrt{-1}\right]\sqrt{2^{2m}};$$

3°. $$F(Ah, 8) = \left(\cos\frac{Ah\pi}{4} + \sin\frac{Ah\pi}{4}\sqrt{-1}\right)4,$$

$$= (-1)^{\frac{(Ah)^2-1}{8}}\left[1 + (-1)^{\frac{Ah-1}{2}}\sqrt{-1}\right]\sqrt{8}.$$

et généralement,

$$F(Ah, 2^{2m+1}) = (-1)^{\frac{(Ah)^2-1}{8}}\left[1 + (-1)^{\frac{Ah-1}{2}}\sqrt{-1}\right]\sqrt{2^{2m+1}}$$

Pour le cas de q premier impair, les formules de M. Gauss

donneront

$$F(Ah, q) = \left(\frac{Ah}{q}\right)(\sqrt{-1})^{\left(\frac{q-1}{2}\right)^2}\sqrt{q},$$

$$F(Ah, q^\alpha) = \left(\frac{Ah}{q^\alpha}\right)(\sqrt{-1})^{\left(\frac{q^\alpha-1}{2}\right)^2}\sqrt{q^\alpha}.$$

D'après ces formules particulières, si l'on pose $p = q^\alpha r^\beta s^\gamma \ldots$, q, r, s étant des nombres premiers impairs, on aura

$$F(h, p) = F(Ah, q^\alpha) \cdot F(Bh, r^\beta) \cdot F(Ch, s^\gamma) \ldots,$$

ou, ce qui revient au même par la substitution,

$$F(h, p) = \left(\frac{Ah}{q^\alpha}\right)\left(\frac{Bh}{r^\beta}\right)\left(\frac{Ch}{s^\gamma}\right)\cdots(\sqrt{-1})^{\left(\frac{q^\alpha-1}{2}\right)^2+\left(\frac{r^\beta-1}{2}\right)^2+\left(\frac{s^\gamma-1}{2}\right)^2+\cdots}\sqrt{p}.$$

Or, d'après les règles pour le calcul des symboles $\left(\frac{Ah}{q^\alpha}\right)$, etc., on trouve

$$\left(\frac{Ah}{q^\alpha}\right)\left(\frac{Bh}{r^\beta}\right)\left(\frac{Ch}{s^\gamma}\right)\cdots = \left(\frac{h}{p}\right)\cdot\left(\frac{A}{q^\alpha}\right)\left(\frac{B}{r^\beta}\right)\left(\frac{C}{s^\gamma}\right)\cdots.$$

D'ailleurs la congruence

$$A\frac{p}{q^\alpha} \equiv 1 \pmod{q^\alpha},$$

ou, ce qui revient au même, la congruence

$$Ar^\beta s^\gamma \ldots \equiv 1 \pmod{q^\alpha},$$

donne

$$\left(\frac{A}{q^\alpha}\right) = \left(\frac{r^\beta}{q^\alpha}\right)\left(\frac{s^\gamma}{q^\alpha}\right)\cdots.$$

De même,

$$\left(\frac{B}{r^\beta}\right) = \left(\frac{q^\alpha}{r^\beta}\right)\left(\frac{s^\gamma}{r^\beta}\right)\cdots,$$

$$\left(\frac{C}{s^\gamma}\right) = \left(\frac{q^\alpha}{s^\gamma}\right)\left(\frac{r^\beta}{s^\gamma}\right)\cdots;$$

et ainsi de suite.

On aura donc

$$\left(\frac{A}{q^\alpha}\right)\left(\frac{B}{r^\beta}\right)\left(\frac{C}{s^\gamma}\right)\cdots = \left(\frac{q^\alpha}{r^\beta}\right)\left(\frac{r^\beta}{q^\alpha}\right)\times\left(\frac{q^\alpha}{s^\gamma}\right)\left(\frac{s^\gamma}{q^\alpha}\right)\times\left(\frac{r^\beta}{s^\gamma}\right)\left(\frac{s^\gamma}{r^\beta}\right)\cdots$$

$$= (-1)^{\frac{q^\alpha-1}{2}\cdot\frac{r^\beta-1}{2}+\frac{q^\alpha-1}{2}\cdot\frac{s^\gamma-1}{2}+\frac{r^\beta-1}{2}\cdot\frac{s^\gamma-1}{2}+\cdots}$$

$$= (\sqrt{-1})^{2\cdot\frac{q^\alpha-1}{2}\cdot\frac{r^\beta-1}{2}+2\cdot\frac{q^\alpha-1}{2}\cdot\frac{s^\gamma-1}{2}+2\cdot\frac{r^\beta-1}{2}\cdot\frac{s^\gamma-1}{2}+\cdots};$$

d'où résulte

$$F(h, p) = \left(\frac{h}{p}\right)(\sqrt{-1})^{\left(\frac{q^\alpha-1}{2}+\frac{r^\beta-1}{2}+\frac{s^\gamma-1}{2}+\cdots\right)^2}\sqrt{p},$$

ou bien

$$(A)\qquad F(h, p) = \left(\frac{h}{p}\right)(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2}\sqrt{p},$$

comme pour le cas de p nombre premier.

Soit maintenant $p = 2^m.p'$ et p' impair, on fera

$$\iota^2 \equiv A p'.\alpha^2 + 2^m.B\beta^2 \pmod{2^m.p'},$$

et il viendra

$$F(h, p) = F(Ah, 2^m).F(Bh, p').$$

Pour $m = 1$, le facteur

$$F(Ah, 2) = 0;$$

donc

$$F(h, p) = 0.$$

Pour $m = 2n$, la congruence

$$Ap' \equiv 1 \pmod{2^{2n}}$$

donne

$$A \equiv p' \pmod 4; \quad \text{d'où} \quad Ah \equiv hp' \pmod 4.$$

De même, la congruence

$$2^{2n}B \equiv 1 \pmod{p'}$$

donne

$$\left(\frac{B}{p'}\right) = 1, \quad \text{d'où} \quad \left(\frac{Bh}{p'}\right) = \left(\frac{h}{p'}\right);$$

d'où la formule

$$(B)\quad F(h, 2^{2n}p') = \left(\frac{h}{p'}\right)\left[1 + (-1)^{\frac{hp'-1}{2}}\sqrt{-1}\right](\sqrt{-1})^{\left(\frac{p'-1}{2}\right)^2}\sqrt{p}.$$

Pour $m = 2n + 1$, la congruence

$$Ap' \equiv 1 \pmod{2^{2n+1}},$$

où $n > 1$, donne

$$A \equiv p' \pmod 8, \quad \text{d'où} \quad Ah \equiv hp' \pmod 8.$$

De même, la congruence

$$2^{2n+1}B \equiv 1 \pmod{p'}$$

donne

$$\left(\frac{B}{p'}\right) = \left(\frac{2}{p'}\right) \quad \text{et} \quad \left(\frac{Bh}{p'}\right) = \left(\frac{2h}{p'}\right);$$

on aura donc

$$(C)\quad F(h, 2^{2n+1}p') = (-1)^{\frac{h^2-1}{8}}\left(\frac{h}{p'}\right)\left[1 + (-1)^{\frac{hp'-1}{2}}\sqrt{-1}\right](\sqrt{-1})^{\left(\frac{p'-1}{2}\right)^2}\sqrt{p}.$$

Les trois formules (A), (B), (C) donnent immédiatement tous les cas particuliers énoncés au commencement de ce paragraphe.

Comme le calcul des symboles $\left(\frac{h}{p}\right)$, $\left(\frac{h}{p'}\right)$ est très-court, on a, pour déterminer le signe des sommes S et C, un moyen plus court encore que celui qui se tire de l'algorithme de M. Gauss (*Sur la sommation de quelques séries*, tome V de ce Journal). Je vais rappeler ici cette règle et la comparer à la précédente. Cette comparaison, qui conduit à une démonstration de la loi de réciprocité (la quatrième de M. Gauss), fait voir encore comment, connaissant $\varphi(h, p)$, on peut trouver $\left(\frac{h}{p}\right)$.

Autre règle pour le signe des sommes S *et* C.

Soient h et p deux nombres premiers entre eux; représentons par $e\left(\frac{kh}{p}\right)$ l'entier immédiatement au-dessous de la fraction $\frac{kh}{p}$: posons $p' = e\left(\frac{p}{2}\right)$, savoir, $p' = \frac{p-1}{2}$ pour p impair, et $p' = \frac{p}{2}$ pour p pair.

Faisons, de plus,

$$\varphi(h, p) = e\left(\frac{h}{p}\right) + e\left(\frac{2h}{p}\right) + e\left(\frac{3h}{p}\right) + \ldots + e\left(\frac{p'h}{p}\right),$$

et

$$(h, p) = (-1)^{\varphi(h, p)}.$$

Le signe de (h, p) donnera celui des sommes S et C au moyen des formules suivantes :

1°. p impair,

$$\text{(A')} \qquad F(h, p) = (-1)^{(h+1)\frac{p^2-1}{8}} (h, p) \left(\sqrt{-1}\right)^{\left(\frac{p-1}{2}\right)^2} \sqrt{p};$$

2°. p double d'un impair,

$$F(h, p) = 0;$$

3°. p divisible par 4, $p = 4p'$ et p' impair,

$$\text{(B')} \qquad F(h, p) = (h, 2p')\left[(-1)^{\frac{h-1}{2}} + \sqrt{-1}\right]\sqrt{p};$$

4°. p divisible par 4, $p = 4p'$ et p' pair,

$$\text{(C')} \qquad F(h, p) = (h, 2p')\left[1 + (-1)^{\frac{h-1}{2}}\sqrt{-1}\right]\sqrt{p}.$$

La comparaison des formules (A) et (A') donne

$$(a) \qquad (-1)^{h+1\frac{p^2-1}{8}} (h, p) = \left(\frac{h}{p}\right).$$

Pour h impair,

$$\left(\frac{h}{p}\right) = (h, p);$$

c'est la règle donnée plus haut.

La comparaison des formules (B) et (B') donne, à cause de $p = 4p'$ et $p' = 4q \pm 1$,

$$(b) \qquad \begin{cases} (h, 2p') = (-1)^{\frac{h-1}{2}}\left(\frac{h}{p'}\right), & \text{pour} \quad p' = 4q + 1, \\ (h, 2p') = \left(\frac{h}{p'}\right), & \text{pour} \quad p' = 4q - 1. \end{cases}$$

La comparaison des formules (C) et (C′), pour $\frac{p}{4} = 2^{2n} p_1$, ou bien $p = 2^{2n+2} p_1$, donne

$$(c) \qquad \begin{cases} (h, 2^{2n+1} p_1) = \left(\frac{h}{p_1}\right), & \text{pour } p_1 = 4q+1, \\ (h, 2^{2n+1} p_1) = (-1)^{\frac{h-1}{2}} \left(\frac{h}{p_1}\right), & \text{pour } p_1 = 4q-1. \end{cases}$$

Enfin, la comparaison des formules (C) et (C′), pour le cas de $\frac{p}{4} = 2^{2n-1} p_1$, donne

$$(d) \qquad \begin{cases} (h, 2^{2n} p_1) = (-1)^{\frac{h^2-1}{8}} \left(\frac{h}{p_1}\right), & \text{pour } p_1 = 4q+1, \\ (h, 2^{2n} p_1) = (-1)^{\frac{(h-1)(h-3)}{8}} \left(\frac{h}{p_1}\right), & \text{pour } p_1 = 4q-1. \end{cases}$$

On voit donc que si l'on suppose $p = 2^m p_1$ et p_1 impair, les formules (a), (b), (c), (d) feront, dans tous les cas, connaître (h, p) au moyen de $\left(\frac{h}{p_1}\right)$.

Sur les sommes $\sum \sin \frac{i^2+i}{2} \cdot \frac{2h\pi}{p}$, $\sum \cos \frac{i^2+i}{2} \cdot \frac{2h\pi}{p}$.

Ces sommes se déduisent très-facilement des sommes S et C. Voici les résultats pour p impair, car elles sont nulles pour p pair. Le nombre h est premier à p :

$$p = 4q+1, \quad \sum \sin \frac{i^2+i}{2} \cdot \frac{2h\pi}{p} = (-1)^{h+1 \cdot \frac{p^2-1}{8}} \left(\frac{h}{p}\right) \sin q \frac{h\pi}{p} \cdot \sqrt{p},$$

$$\sum \cos \frac{i^2+i}{2} \cdot \frac{2h\pi}{p} = (-1)^{h+1 \cdot \frac{p^2-1}{8}} \left(\frac{h}{p}\right) \cos q \frac{h\pi}{p} \cdot \sqrt{p};$$

$$p = 4q-1, \quad \sum \sin \frac{i^2+i}{2} \cdot \frac{2h\pi}{p} = (-1)^{h+1 \cdot \frac{p^2-1}{8}} \left(\frac{h}{p}\right) \cos q \frac{h\pi}{p} \cdot \sqrt{p},$$

$$\sum \cos \frac{i^2+i}{2} \cdot \frac{2h\pi}{p} = (-1)^{h+1 \cdot \frac{p^2-1}{8}} \left(\frac{h}{p}\right) \sin q \frac{h\pi}{p} \cdot \sqrt{p}.$$

Pour démontrer ces formules, il suffit de calculer

$$S_1 = \sum \left(\cos i^2 \frac{2h\pi}{8p} + \sin i^2 \frac{2h\pi}{p} \sqrt{-1} \right).$$

Soient d'abord p pair et h impair, on reconnaît de suite que la partie de S_1, où $i = 2k$, a la même valeur que la somme entière S; et comme l'autre partie, où $i = 2k + 1$ et $i^2 = 4(k^2 + k) + 1$, revient à

$$4 \left(\cos \frac{2h\pi}{8p} + \sin \frac{2h\pi}{8p} \sqrt{-1} \right) \sum \left(\cos \frac{k^2 + k}{2} \cdot \frac{2h\pi}{p} + \sin \frac{k^2 + k}{2} \cdot \frac{2h\pi}{p} \sqrt{-1} \right),$$

les sommes en question seront nulles.

Pour p impair et h impair, la partie de la somme S_1, où $i = 2k$, se réduisant à

$$\sum \left(\cos k^2 \frac{2h\pi}{2p} + \sin k^2 \frac{2h\pi}{2p} \sqrt{-1} \right),$$

sera nulle, l'autre partie devra donc être égalée à S_1. Mais la décomposition en facteurs donne

$$S_1 = 4 \left(\cos \frac{2ph\pi}{8} + \sin \frac{2ph\pi}{8} \sqrt{-1} \right) \left(\frac{2h}{p} \right) (\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2} \sqrt{p};$$

d'où, par la division,

$$\sum \left(\cos \frac{k^2 + k}{2} + \sin \frac{k^2 + k}{2} \sqrt{-1} \right)$$

$$= \left(\frac{2h}{p} \right) \left(\cos \frac{p^2 - 1}{4} \frac{h\pi}{p} + \sin \frac{p^2 - 1}{4} \frac{h\pi}{p} \sqrt{-1} \right) (\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2} \sqrt{p};$$

savoir, pour $p = 4q + 1$,

$$(-1)^{qh} \left(\frac{2h}{p} \right) \left(\cos q \frac{h\pi}{p} + \sin q \frac{h\pi}{p} \sqrt{-1} \right) \sqrt{p};$$

et, pour $p = 4q - 1$,

$$(-1)^{qh} \left(\frac{2h}{2} \right) \left(\sin q \frac{h\pi}{p} + \cos q \frac{h\pi}{p} \sqrt{-1} \right) \sqrt{p}.$$

Mais comme h est impair,

$$(-1)^{qh} = (-1)^{q} = (-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right),$$

le facteur $(-1)^{qh}\left(\frac{2h}{p}\right)$ se réduira à $\left(\frac{h}{p}\right)$.

Pour h pair, on posera $h = p - h'$, d'où h' impair; alors

$$\frac{2h\pi}{p} = 2\pi - \frac{2h'\pi}{p}.$$

Il faudra donc changer, dans le résultat, h en $-h'$; mais

$$\left(\frac{-h'}{p}\right) = \left(\frac{h-p}{p}\right) = \left(\frac{h}{p}\right) \quad \text{et} \quad q\frac{-h'\pi}{p} = q\frac{(h-p)\pi}{p} = q\frac{h\pi}{p} - q\pi:$$

on aura donc

$$\sin q\frac{-h'\pi}{p} = (-1)^{q}\sin q\frac{h\pi}{p}, \quad \cos q\frac{-h'\pi}{p} = (-1)^{q}\cos q\frac{h\pi}{p};$$

comme h est pair,

$$(-1)^{q} = (-1)^{q(h+1)} = (-1)^{h+1\cdot\frac{p^2-1}{8}},$$

d'où la formule donnée plus haut.

Si l'on remplace $(-1)^{h+1\cdot\frac{p^2-1}{8}}\left(\frac{h}{p}\right)$ par (h, p), on aura les valeurs données dans le Mémoire cité plus haut (tome V de ce Journal, page 52).