LA CYCLOTOMIE JADIS ET NAGUÈRE

Autor(en): **Weil, André**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-46909

LA CYCLOTOMIE JADIS ET NAGUÈRE [1]

par André WEIL

Littéralement, « cyclotomie » signifie « division du cercle ». Les géomètres grecs ont enseigné à diviser le cercle en N parties égales, par la règle et le compas, pour N de la forme 2^n, $2^n.3$, $2^n.5$, $2^n.15$.

La découverte par Euler des relations entre fonctions trigonométriques et exponentielles ramenait le problème de la division du cercle à la résolution des équations binômes de la forme $X^n = 1$. Gauss, à 19 ans, reçut la médaille Fields (plus exactement il l'aurait reçue si elle avait existé) pour avoir résolu l'équation $X^{17} = 1$ par une succession de racines carrées, ce qui implique la division du cercle en 17 parties égales par la règle et le compas. Bien entendu, ce résultat, pour sensationnel qu'il fût, n'était pour Gauss qu'un premier pas dans la théorie des équations binômes.

1. C'est donc à juste titre qu'on qualifie de « cyclotomiques » les corps engendrés sur $\mathbf{Q}$ par les racines de l'unité, et leurs sous-corps, et le mot de « cyclotomie » pourrait s'appliquer à tout ce qui les concerne; on sait d'ailleurs, depuis Kronecker, que ces corps ne sont autres que les extensions abéliennes de $\mathbf{Q}$. Mais, depuis Jacobi, et pendant tout le XIX^e siècle, l'usage s'est établi de réserver ce mot (en allemand, *Kreist(h)eilung*) à l'étude de certaines sommes remarquables de racines de l'unité, qu'on a pris de nos jours (depuis Hasse, semble-t-il) l'habitude d'appeler « sommes de Gauss »; nous adopterons ce terme, qui est commode, mais historiquement peu justifié. Plus précisément, nous conviendrons d'appeler *somme de Gauss* relative au corps fini $\mathbf{F}_q$ à $q = p^n$ éléments toute somme

$$G = G(\chi, \psi) = \sum_{x \in \mathbf{F}_q^\times} \chi(x)\psi(x) \tag{1}$$

où χ est un caractère du groupe multiplicatif $\mathbf{F}_q^\times$, et ψ un caractère non trivial du groupe additif $\mathbf{F}_q$. Si ε est une racine primitive de $X^p = 1$, l'ensemble des valeurs de ψ est $\{1, \varepsilon, ..., \varepsilon^{p-1}\}$. Si χ est d'ordre m, m divise $q - 1$, et on peut écrire $q - 1 = mv$; on dira alors que G est *d'ordre* m; pour $m = 1$,

[1] Exposé au séminaire Bourbaki, Paris, juin 1974.

on a $G = -1$. Si r est un générateur du groupe cyclique $\mathbf{F}_q^\times$, χ est bien défini par la donnée de $\zeta = \chi(r)$, et ζ est une racine primitive de $Z^m = 1$; on peut écrire alors

$$(2) \qquad G = \sum_{i=0}^{q-2} \zeta^i \psi(r^i) = \sum_{i=0}^{m-1} \zeta^i \sum_{j=0}^{v-1} \psi(r^{i+mj}).$$

La première propriété de $G(\chi, \psi)$ qui nous saute aux yeux est que c'est un entier algébrique du corps $\mathbf{Q}(\zeta, \varepsilon)$, et que tous ses conjugués sur $\mathbf{Q}$ sont aussi des sommes de Gauss; si un automorphisme de $\mathbf{Q}(\zeta, \varepsilon)$ change ζ en ζ^t et ε en ε^u, il change $G(\chi, \psi)$ en $G(\chi^t, \psi^u)$. De plus, avec des « abus de notations » évidents, on a $\psi^u(x) = \psi(ux)$, et par suite:

$$(3) \qquad G(\chi, \psi^u) = \chi(u)^{-1} G(\chi, \psi),$$

ce qui implique aussitôt que $G(\chi. \psi)^m$ est dans $\mathbf{Q}(\zeta)$.

Notons aussi dès maintenant qu'on a, pour G défini par (1):

$$(4) \qquad G\bar{G} = \sum_{x,y} \chi(xy^{-1}) \psi(x-y) = \sum_{z \neq 0} \chi(z) \sum_{y \neq 0} \psi(y(z-1))$$

$$= q - 1 - \sum_{z \neq 0,1} \chi(z) = \begin{cases} q \text{ si } \chi \neq 1 \\ 1 \text{ si } \chi = 1. \end{cases}$$

Si $\mathbf{F}_q$ est le corps premier $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, on pourra prendre $\psi(x) = \varepsilon^x$, et on aura

$$(5) \qquad G = \sum_{x=1}^{p-1} \chi(x) \varepsilon^x = \sum_{i=0}^{p-2} \zeta^i \varepsilon^{r^i} = \sum_{i=0}^{m-1} \zeta^i \sum_{j=0}^{v-1} \varepsilon^{r^{i+mj}}.$$

2. Nous avons anticipé sur l'ordre historique, auquel nous revenons à présent. Les sommes (5) sont des cas particuliers des sommes introduites par Lagrange dans son grand mémoire ([1 a]) sur la théorie algébrique des équations (la théorie de Galois « avant la lettre »). C'est là que Lagrange montre, entre autre, comment engendrer une extension cyclique de degré m au moyen d'une racine m-ième, après adjonction, s'il y a lieu, des racines m-ièmes de l'unité (engendrement dit, bien à tort, « kummérien »). Il introduit les sommes

$$(6) \qquad y = x_1 + \alpha x_2 + \ldots + \alpha^{m-1} x_m,$$

où $\alpha^m = 1$, et où $x_1, \ldots, x_m$ sont les racines d'une équation de degré m, et il observe que y^m est invariant par toute permutation circulaire des x_i. Il fait voir par exemple qu'on « explique » ainsi les formules classiques de résolution par radicaux des équations du 3e et du 4e degré. Exposant à

nouveau sa méthode dans son *Traité* de 1808 ([1 b], Note XIII), il donne aux sommes (6) le nom de « *résolvantes* », qui leur est resté pendant tout le XIX^e siècle.

3. En 1801, dans la VII^e section des *Disquisitiones* ([2 a]), Gauss donne un exposé complet de la « théorie de Galois » de $\mathbf{Q}(\varepsilon)$ considéré comme extension cyclique de $\mathbf{Q}$ de degré $p-1$. Il montre en particulier que, pour $p-1 = mv$, $\mathbf{Q}(\varepsilon)$ possède un sous-corps k_m (et un seul) de degré m sur $\mathbf{Q}$, engendré sur $\mathbf{Q}$ par l'une quelconque des « périodes d'ordre m »:

$$\eta_i = \sum_{j=0}^{v-1} \varepsilon^{r^{i+mj}} \qquad (0 \leqslant i < m), \tag{7}$$

celles-ci étant permutées circulairement par les automorphismes de $\mathbf{Q}(\varepsilon)$ sur $\mathbf{Q}$.

La question de la résolution par radicaux était trop implantée dans les esprits pour que Gauss pût la laisser complètement de côté. Soit qu'il ait eu connaissance directement ou indirectement de la méthode de Lagrange (comme il est vraisemblable), soit qu'il l'ait retrouvée par lui-même (comme il est possible), il l'applique aux corps intermédiaires entre $\mathbf{Q}$ et $\mathbf{Q}(\varepsilon)$; si k_m est comme plus haut, et si k est un sous-corps de k_m, cela conduit à former des résolvantes de Lagrange au moyen des η_i et de racines de l'unité auxiliaires, d'ordre $< p$. Pour $k = \mathbf{Q}$, ces résolvantes ne sont autres que les sommes (5). Mais Gauss ne semble pas leur attacher d'importance; il note en passant la relation $G\,\overline{G} = p$, et cela seulement pour dire que l'extraction de racines $(G^m)^{1/m}$ se ramène à une racine carrée et à la division par m d'un arc de cercle. Quand un peu plus tard Lagrange, dans son *Traité* ([1 b], Note XIV) donne un exposé des résultats de Gauss basé principalement sur les sommes (5), il se fait vertement critiquer par Gauss, pour n'avoir pas suffisamment tenu compte de l'ambiguïté qui résulte de l'emploi des racines de l'unité d'ordre $< p$.

4. Comme Gauss le fait voir, les périodes η_i ont une table de multiplication

$$\eta_i \eta_j = \sum_k N_{ijk} \eta_k \tag{8}$$

où les N_{ijk} sont des entiers naturels, apparentés aux nombres de solutions des congruences $AX^m + BY^m \equiv C \pmod{p}$. Ce fait a des conséquences arithmétiques importantes, dont Gauss a aperçu quelques-unes (pour le

cas $m = 3$) dès les *Disq.* Plus tard, il en a développé d'autres pour $m = 4$ ([2 d]). Mais il s'est surtout intéressé au cas $m = 2$, le seul où il ait cru pouvoir utiliser les « sommes de Gauss » de préférence aux « périodes » (sans doute parce qu'alors il n'y a pas à introduire d'irrationalité accessoire). On a alors:

$$G = \eta_0 - \eta_1 = 1 + 2\eta_0 = \sum_{x=0}^{p-1} \varepsilon^{x^2}. \tag{9}$$

Ici (3) donne $\bar{G} = \pm G$, donc $G^2 = \pm p$ d'après (4), le signe étant donné par $p \equiv \pm 1 \pmod 4$. Il s'ensuit que le corps quadratique k_2 contenu dans $\mathbf{Q}(\varepsilon)$ est $\mathbf{Q}(\sqrt{\pm p})$.

5. Comme Gauss le signale dès les *Disq.*, ce résultat se généralise à la somme

$$G = \sum_{x=0}^{N-1} \alpha^{x^2},$$

où α est une racine primitive N-ième de l'unité, avec N impair quelconque; on a $G^2 = \pm N$, ce qui pose le problème de la détermination du signe de G, par exemple pour $\alpha = e^{2\pi i/N}$; énoncé sous cette forme, le problème n'est pas algébrique. « Nous observons », dit Gauss dans les *Disq.* (avec une ambiguïté sans doute voulue) qu'on a toujours $G = +\sqrt{N}$ resp. $+ i\sqrt{N}$. En fait, il n'en obtint la démonstration qu'en 1805; celle-ci, publiée en 1811 ([2 b]) s'apparente, d'une manière très visible pour nous, à ses recherches (qu'il n'a pas publiées) sur les fonctions thêta. Pour $N = pq$, avec p, q premiers, Gauss en tire sa quatrième démonstration de la loi de réciprocité quadratique. Ce travail a donné lieu, et jusqu'à une époque toute récente, à d'importantes généralisations, que nous laisserons complètement de côté.

6. En 1818, Gauss publia sa sixième démonstration de la loi de réciprocité quadratique ([2 c]); elle est basée, elle aussi, sur les sommes de Gauss d'ordre 2, mais envisagées d'un point de vue strictement algébrico-arithmétique. Soit G défini par (9). Soit q un nombre premier impair $\neq p$; posons $p = 2p' + 1$, $q = 2q' + 1$. Au moyen du symbole de Legendre, la loi de réciprocité s'écrit:

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

On a vu qu'on a $G^2 = (-1)^{p'} p$, d'où

$$G^{q-1} = (-1)^{p'q'} \cdot p^{q'} \equiv (-1)^{p'q'} \left(\frac{p}{q}\right) \bmod q .$$

Mais on a aussi, d'après la formule du binôme:

$$G^q \equiv \sum_x \varepsilon^{qx^2} = \left(\frac{q}{p}\right) G \bmod q ,$$

d'où la loi de réciprocité, puisque G est premier à q. Bien entendu Gauss ne se permet pas (ostensiblement) d'écrire des congruences dans l'anneau $\mathbf{Z}[\varepsilon]$; il les remplace par des congruences modulo $(q, 1+X+\ldots+X^{p-1})$ dans l'anneau $\mathbf{Z}[X]$. Néanmoins il est incompréhensible que Jacobi, Cauchy et Eisenstein, tour à tour, aient publié des démonstrations virtuellement identiques à celle-là (et qu'ils aient même soulevé entre eux des questions de priorité à ce sujet) avant qu'Eisenstein ne fît observer qu'à la présentation près c'était toujours la sixième démonstration de Gauss.

7. Dans un projet de suite à la section VII des *Disq.* ([2 e]), Gauss, non seulement donne la démonstration de $G\bar{G} = p$, mais donne la formule de multiplication des sommes de Gauss. D'après (1), on peut écrire:

$$G(\chi,\psi)\, G(\chi',\psi) = \sum_{x.y\neq 0} \chi(x)\,\chi'(y)\,\psi(x+y)$$

$$= \sum_{z\neq 0} \psi(z) \Big[\sum_{\substack{x+y=z \\ x,y\neq 0}} \chi(x)\,\chi'(y) \Big] + \sum_{x\neq 0} \chi(x)\,\chi'(-x) .$$

Posons $\chi'' = \chi\chi'$. La dernière somme est 0 si $\chi'' \neq 1$ et $(q-1)\,\chi(-1)$ si $\chi'' = 1$; l'autre s'écrit $J.G(\chi'', \psi)$ à condition de poser:

$$J = J(\chi,\chi') = \sum_{x\neq 0,1} \chi(x)\,\chi'(1-x) . \tag{10}$$

Pour $\chi'' = 1$, on observe que $x \mapsto x(1-x)^{-1}$ est une bijection de $\mathbf{F}_q - \{0, 1\}$ sur $\mathbf{F}_q - \{0, -1\}$, ce qui donne pour J la valeur $-\chi(-1)$ si $\chi \neq 1$ et $q-2$ si $\chi = \chi' = 1$, donc, si $\chi \neq 1$:

$$G(\chi,\psi)\, G(\chi^{-1},\psi) = q\chi(-1) . \tag{11}$$

On est dans un cas trivial si $\chi = 1$ ou $\chi' = 1$. Si χ, χ', χ'' sont $\neq 1$, on a

$$G(\chi,\psi)\, G(\chi',\psi) = J(\chi,\chi') \cdot G(\chi'',\psi) . \tag{12}$$

Si ζ est comme plus haut une racine primitive de $Z^m = 1$, et si les ordres de χ, χ' sont m ou des diviseurs de m, (10) montre que $J = J(\chi, \chi')$ est dans $\mathbf{Z}[\zeta]$; d'après (12) et (4), on a $J\bar{J} = q$.

Par récurrence, on tire de (12) la formule

$$\prod_{i=1}^{n} G(\chi_i, \psi) = J \cdot G(\prod_{i=1}^{n} \chi_i, \psi), \tag{13}$$

où J est de nouveau un entier de $\mathbf{Q}(\zeta)$ si les ordres des χ_i divisent m. Si on pose $\chi_o = \prod_i \chi_i^{-1}$, on a, d'après (W2) et (11):

$$\prod_{i=0}^{n} G(\chi_i, \psi) = q\, \chi_o(-1) \cdot J\ , \tag{14}$$

ce qui montre que $\chi_o(-1) \cdot J$ dépend symétriquement de $\chi_o, \chi_1, \ldots, \chi_n$, ceux-ci étant soumis à la condition $\chi_o \chi_1 \ldots \chi_n = 1$. Par exemple, considérons un automorphisme τ de $\mathbf{Q}(\zeta)$; s'il change ζ en ζ^t, il change χ_i en χ_i^t; si donc $(\chi_o^t, \ldots, \chi_n^t)$ est une permutation de $(\chi_o, \ldots, \chi_n)$, J sera invariant par τ. On peut ainsi faire en sorte que J appartienne à un sous-corps donné de $\mathbf{Q}(\zeta)$.

8. Naturellement, chez Gauss et ses successeurs immédiats jusqu'à Kummer, il ne s'agit que des sommes de Gauss relatives à un corps premier $\mathbf{F}_p$ et des sommes J correspondantes. Il ne semble pas que Gauss lui-même ait aperçu l'importance arithmétique des entiers J. Pourtant, il aurait pu être frappé par le fait que, dès les cas $m = 3$ et $m = 4$, ces entiers donnent la décomposition des nombres premiers rationnels dans les corps $\mathbf{Q}(j)$, $\mathbf{Q}(i)$, où $j^3 = 1$, $i^4 = 1$; ce fait lui était connu sous une autre forme (il l'exprimait au moyen des « périodes »). Soit en effet $p \equiv 1 \bmod 3$ (resp. mod 4); soit χ l'un des deux caractères d'ordre 3 (resp. d'ordre 4) de $\mathbf{F}_p^\times$; alors $J(\chi, \chi)$ est un facteur premier de p dans $\mathbf{Q}(j)$ (resp. $\mathbf{Q}(i)$), et satisfait de plus à d'importantes congruences. C'est ce que découvrit Jacobi; il eut même l'audace, en 1827, d'en faire part à Gauss ([3 a]), qui se montra encourageant (avec une pointe de condescendance), mais pensa peut-être, tout comme un peu plus tard dans l'affaire des fonctions elliptiques, qu'un jeune éléphant marchait sur ses plates-bandes.

9. A la différence de Gauss, Jacobi reconnut aussitôt la portée de cette méthode « cyclotomique »; cela justifie le nom de « sommes de Jacobi » qu'on donne de nos jours aux entiers J, bien qu'elles figurent déjà, comme on a vu, dans les papiers secrets de Gauss, et que Cauchy les ait introduites et largement utilisées, à partir de 1829 (indépendamment de Jacobi), dans quelques notes préliminaires et surtout dans son grand mémoire de 1830 sur la théorie des nombres ([4]), paru avec des notes additionnelles en 1840.

Cauchy fut surtout frappé de la possibilité (qui résulte de la remarque de la fin du n° 7) de construire des sommes J contenues dans une extension quadratique donnée de $\mathbf{Q}$. Soit par exemple $l = 4n + 3$ premier; soient $r_0, \ldots, r_n$ les résidus quadratiques mod l. Soit $p \equiv 1 \bmod l$; soit χ un caractère d'ordre l de $\mathbf{F}_p$; pour $0 \leqslant i \leqslant n$, soit $\chi_i = \chi^{r_i}$; alors (14) définit un entier J du corps $k = \mathbf{Q}(\sqrt{-l})$, et on a $J\bar{J} = p^{n-1}$. D'autre part, Cauchy détermine la plus grande puissance p^v de p qui divise J; il peut donc affirmer que $4p^{n-1-2v}$ peut s'écrire sous la forme $x^2 + ly^2$. En langage moderne, cela signifie qu'on a, dans k, $(J) = p^v \mathfrak{p}^{n-1-2v}$, où $\mathfrak{p}$ est l'un des deux facteurs premiers de p. C'est là un résultat non trivial sur le groupe des classes d'idéaux de k, ou, dans le langage de l'époque, sur le groupe des classes de formes quadratiques de discriminant $-l$; Jacobi, en raisonnant de même (indépendamment de Cauchy), en tira même la conjecture correcte sur le nombre de ces classes, quelque temps avant que Dirichlet ne vérifiât cette conjecture en un travail célèbre (largement anticipé par Gauss, toujours dans ses « papiers secrets »).

10. Jacobi s'intéressa surtout aux applications de la « méthode cyclotomique » au problème le plus brûlant de la théorie des nombres à cette époque, la recherche des lois de réciprocité des n-ièmes puissances pour $n > 2$. Au sujet de la loi de réciprocité biquadratique, Gauss venait d'annoncer des résultats importants, en termes un peu grandiloquents (« mysterium maxime reconditum »). Fut-il vexé de voir Jacobi proclamer que ceux-ci se déduisaient « très simplement et très facilement » de sa méthode ? Toujours est-il qu'il ne publia jamais sa démonstration, qui était basée sur des principes tout différents. Jacobi non plus, d'ailleurs; la sienne resta enterrée dans ses notes de cours de Königsberg (1836-37); au dire de Jacobi, c'est celle même qui fut obtenue indépendamment, un peu plus tard, par Eisenstein encore étudiant. Pour les restes cubiques ([5 a]), on peut en présenter la partie essentielle comme suit.

Dans $\mathbf{Z}[j]$, 3 admet le diviseur premier $\rho = j - 1$. Pour tout nombre premier π, premier à 3, soit $q = N(\pi) = 3n + 1$. Pour x premier à π, on notera (x/π) celle des racines de l'unité $1, j, j^2$ qui est $\equiv x^n \bmod \pi$, et on étend ce « symbole de Legendre » à un « symbole de Jacobi » par la règle $(x/\alpha\beta) = (x/\alpha) \cdot (x/\beta)$. Soit $p = 3v + 1$ premier rationnel, et soit π l'un de ses facteurs premiers dans $\mathbf{Z}[j]$; on peut, d'une manière et d'une seule, multiplier π par une racine (sixième) de 1 de manière que π devienne « primaire », c'est-à-dire $\equiv 1 \bmod 3$. Posons $\chi(x) = (x/\pi)$ pour $x \in \mathbf{F}_p^\times$; c'est un caractère d'ordre 3 de $\mathbf{F}_p^\times$. Sur $\mathbf{F}_p$, on prend $\psi(x) = e^{2\pi i x/p}$. Posons

$G = G(\chi, \psi)$, $J = J(\chi, \chi)$. On a alors $G(\chi^{-1}, \psi) = \bar{G}$, $G^2 = J\bar{G}$, $G^3 = pJ$, $G\bar{G} = J\bar{J} = p$, puis

$$(15) \qquad J = \sum_{x=2}^{p-1} \chi(x)\chi(1-x) \equiv \sum_{x=1}^{p-1} x^{\nu}(1-x)^{\nu} \bmod \pi .$$

Mais, pour $n \not\equiv 0 \bmod (p-1)$, on a $\sum_{1}^{p-1} x^n \equiv 0 \bmod p$; donc $J \equiv 0 \bmod \pi$. Comme $J\bar{J} = p$, J/π est donc une racine sixième de 1, qu'on détermine comme suit. On a posé $\rho = j - 1$, d'où $\rho^2 = -3j$ et $j^a = (1+\rho)^a \equiv 1 + \rho a \bmod 3$. Posons $\chi(x) = j^{i(x)}$; on a $i(xy) \equiv i(x) + i(y) \bmod 3$, d'où

$$J \equiv p - 2 + \rho\Big[\sum_{1}^{p-1} i(x) + \sum_{2}^{p-1} i(1-x)\Big] \equiv -1 + 2\rho \sum_{1}^{p-1} i(x)$$
$$\equiv -1 \bmod 3 ,$$

et par suite $J = -\pi$.

Soit maintenant σ premier dans $\mathbf{Z}[j]$, premier à $3p$; soit $s = N(\sigma) = \sigma\bar{\sigma}$; on a $s \equiv 1 \bmod 3$, $\chi^s = \chi$, donc

$$G^s \equiv \Sigma \chi(x)\psi(sx) \equiv \chi(s)^{-1} G \equiv (s/\pi)^{-1} G \bmod \sigma .$$

Mais d'autre part, si $s = 3t + 1$:

$$G^{s-1} = (G^3)^t = (-p\pi)^t \equiv (-\pi^2\bar{\pi}/\sigma) \bmod \sigma .$$

On a $(-1/\sigma) = (-1/\sigma)^3 = 1$, et aussi, par transport de structure, $(\bar{\pi}/\sigma) = (\pi/\bar{\sigma})^{-1}$. Comme G est premier à σ, la combinaison des relations ci-dessus donne alors $(s/\pi) = (\pi/s)$, ce qui est la « loi d'Eisenstein ». Si maintenant on prend p' premier rationnel $\neq p$, $\equiv 1 \bmod 3$, et que π' soit un facteur premier primaire de p', on peut, dans ce qui précède, remplacer π, s successivement par π, p' et par π', p et combiner les résultats. Cela donne d'abord $(\pi/\pi')^2 = (\pi'/\pi)^2$, d'où évidemment $(\pi/\pi') = (\pi'/\pi)$.

On a ainsi tout l'essentiel de la loi de réciprocité cubique dans $\mathbf{Z}[j]$; les résultats complémentaires sont faciles à obtenir. Notons aussi dès maintenant, sur l'exemple ci-dessus, une propriété de J à laquelle Jacobi et ses contemporains attachaient beaucoup d'importance. Pour $x \in \mathbf{F}_p^{\times}$, on a $\chi(x) = (x/\bar{\pi})^{-1} = (x^{-1}/\bar{\pi}) \equiv x^{p-1-\nu} \bmod \bar{\pi}$, donc, d'après (15):

$$J \equiv \sum_{x=1}^{p-1} x^{2\nu}(1-x)^{2\nu} \equiv -\binom{2\nu}{\nu} \bmod \bar{\pi} .$$

Cette congruence, jointe à $J \equiv 0 \bmod \pi$, détermine complètement J

modulo p au moyen du coefficient binomial $\binom{2v}{v}$; compte tenu d'inégalités triviales, on peut même dire qu'elle détermine J, donc π, d'une manière unique.

11. L'exemple du n° 10 contient déjà tous les traits caractéristiques de « la cyclotomie », c'est-à-dire de la théorie des sommes de Gauss et de Jacobi, telle qu'elle s'est développée au XIX^e siècle.

En premier lieu, pour utiliser ces sommes, il faut en déterminer la décomposition en facteurs premiers dans les corps cyclotomiques auxquels elles appartiennent. On a vu plus haut la solution pour les sommes d'ordre 3; pour l'ordre 4, elle est analogue; Jacobi examina aussi les sommes d'ordre 5, 8, 12, en utilisant le fait (dont il s'aperçut à cette occasion) que les corps correspondants n'ont que des idéaux principaux. Pour aller plus loin, évidemment, il fallait la création (par Kummer, à partir de 1845) de la théorie des idéaux. Ce qui en limita quelque temps la portée, c'est que Kummer (qui procédait par construction explicite des valuations dans les corps en question) ne traita d'abord que les corps $\mathbf{Q}(\zeta)$ avec $\zeta^l = 1$, l premier impair. L'un de ses premiers triomphes fut justement d'obtenir la décomposition en idéaux premiers de G^l dans $\mathbf{Z}[l]$, pour $\zeta^l = 1$, chaque fois que p est premier, $\equiv 1 \bmod l$, et que G est une somme de Gauss d'ordre l relative à $\mathbf{F}_p$. Un peu plus tard il s'aperçut (non pas pour les sommes de Gauss, mais, ce qui revient au même, pour les sommes de Jacobi) qu'on pouvait traiter de même les corps finis $\mathbf{F}_q$, ceux-ci se présentant comme corps de restes dans $\mathbf{Z}[\zeta]$ modulo un idéal premier $\mathfrak{p}$ (premier à l) de degré > 1 (v. [6]).

12. La décomposition en facteurs premiers ne détermine les sommes en question qu'à une unité près; c'était déjà insuffisant pour les sommes d'ordre 3 et 4; il en est ainsi à plus forte raison pour les sommes d'ordre l, puisqu'il y a alors une infinité d'unités dans $\mathbf{Z}[\zeta]$, d'après le théorème de Dirichlet (publié en 1846). Aussi recherche-t-on des précisions supplémentaires sous forme de congruences. Comme au n° 11, celles-ci sont de deux sortes:

(a) les unes, pour les sommes relatives à $\mathbf{F}_p$ (resp. $\mathbf{F}_q$ avec $q = p^n$) donnent, non seulement leur ordre, mais leur partie principale aux places déterminées par les facteurs premiers de p;

(b) les autres, encore plus importantes, concernent le comportement local de ces sommes dans $\mathbf{Q}_l(\zeta)$, ou plus généralement aux places correspondant

aux facteurs premiers de m dans $\mathbf{Q}(\zeta)$ s'il s'agit de sommes d'ordre m non premier, et si $\zeta^m = 1$.

Ces questions ont conduit Kummer et Eisenstein à développer des techniques très raffinées d'analyse p-adique, malheureusement tombées par la suite dans un profond oubli.

13. Enfin, soulignons à nouveau que, pour Eisenstein et Kummer, la cyclotomie apparaissait surtout comme un moyen pour aborder le problème des lois de réciprocité, dans le cadre où celui-ci s'est posé jusqu'à Hilbert. Pour la loi des m-ièmes puissances, l'exemple de Gauss suggérait de se placer dans le corps $\mathbf{Q}(\zeta)$ et non au-delà, avec ζ, comme toujours, racine primitive de $Z^m = 1$. Pour $\mathfrak{p}$ premier à m dans $\mathbf{Z}[\zeta]$, de norme q, et x premier à $\mathfrak{p}$, on note $(x/\mathfrak{p})$ celle des racines ζ^i qui est $\equiv x^{(q-1)/m} \bmod \mathfrak{p}$; on étend ce « symbole de Legendre » à un « symbole de Jacobi » par la règle $(x/\mathfrak{ab}) = (x/\mathfrak{a}).(x/\mathfrak{b})$. On se propose alors d'obtenir une expression, la plus explicite possible, pour $(x/y).(x/y)^{-1}$, et aussi les « lois complémentaires » donnant $(x/\mathfrak{p})$ quand x est une unité ou bien divise m.

Finalement les espoirs placés par Jacobi, Eisenstein et Kummer dans la cyclotomie ne se réalisèrent que partiellement. Elle donne la « loi d'Eisenstein », c'est-à-dire la valeur de $(x/y).(y/x)^{-1}$ quand x (ou y) est dans $\mathbf{Z}$; ce n'est déjà pas un mince résultat. Pour $m = 4$, par un hasard heureux, on peut en tirer l'énoncé complet de la loi de réciprocité biquadratique au moyen des propriétés axiomatiques « évidentes » du symbole (x/y), c'est-à-dire, comme on dirait de nos jours, en faisant de la K-théorie; c'est ce que faisait sans doute Jacobi dans son cours de Königsberg, et c'est ce que fit Eisenstein, qui par la suite appliqua ses idées sur la K-théorie à des problèmes beaucoup plus généraux. Mais de plus en plus, jusqu'à la fin de sa courte vie, Eisenstein se consacra plutôt à la mise en œuvre de la théorie des fonctions elliptiques en vue de ses applications arithmétiques; c'est de là en particulier qu'il tire les lois de réciprocité pour $m = 8$. Pendant le même temps, Kummer, se limitant une fois pour toutes aux lois des l-ièmes puissances pour l premier impair (et même en fait pour l « régulier »), faisait servir la cyclotomie, avec plein succès, à la recherche des « lois complémentaires », mais, à son grand chagrin, dut constater vers 1853 qu'avec ces résultats et la loi d'Eisenstein elle avait fourni tout ce dont elle était capable.

14. En 1890, Stickelberger reprit et compléta les résultats de Jacobi, Kummer et Eisenstein qui donnent la partie principale des sommes de Gauss

et d'Eisenstein. Nous allons résumer son travail ([7]) en langage p-adique, ce qui ne change rien au fond des choses mais permet d'être bref.

Soient p premier, $q = p^n$, et ω une racine primitive de $W^{q-1} = 1$; $k = \mathbf{Q}_p(\omega)$ est l'extension non ramifiée de $\mathbf{Q}_p$ de degré n; on peut identifier $\mathbf{F}_q$ avec $\mathbf{Z}_p[\omega]/(p)$, et $\mathbf{F}_p$ avec $\mathbf{Z}_p/(p)$. Les automorphismes de k sur $\mathbf{Q}_p$ transforment ω en ω^{p^ν} pour $0 \leqslant \nu < n$, de sorte que, si t désigne la trace prise dans $k/\mathbf{Q}_p$, on a:

$$t(\omega^i) = \omega^i + \omega^{ip} + \ldots + \omega^{ip^{n-1}}, \tag{16}$$

et $t(\omega^i)$ est dans $\mathbf{Z}_p$.

Soit ε une racine primitive de $X^p = 1$ dans une extension de k; pour $a \in \mathbf{Z}_p$, on définit ε^a de la manière évidente (par continuité p-adique, si l'on veut). Alors $x \mapsto \varepsilon^{t(x)}$, pour $x \in \mathbf{Z}_p[\omega]$, définit, par passage au quotient, un caractère ψ du groupe additif $\mathbf{F}_q$. D'autre part, l'ensemble des racines de $X^q = X$ dans k est $M = \{0, 1, \omega, \ldots, \omega^{q-2}\}$; ce sont les représentants multiplicatifs de $\mathbf{F}_q$ dans k. Si donc, pour $x \in \mathbf{Z}_p[\omega]$, on note μ_x l'élément de M qui est $\equiv x \bmod p$, $x \mapsto \mu_x$ définit par passage au quotient un caractère de $\mathbf{F}_q^\times$ à valeurs dans k, et tout caractère de $\mathbf{F}_q^\times$, à valeurs dans k, est de la forme $x \mapsto \mu_x^{-a}$. Toutes les sommes de Gauss relatives à $\mathbf{F}_q$, sauf la somme triviale égale à -1, s'écrivent donc dans $k(\varepsilon)$ sous la forme:

$$g_a = \sum_\mu \mu^{-a} \varepsilon^{t(\mu)} \qquad (0 < a < q-1), \tag{17}$$

la somme étant étendue aux $\mu \in M^\times = M - \{0\}$.

Dans $k(\varepsilon)$, $\pi = \varepsilon - 1$ est un élément premier, et on a, pour tout $z \in \mathbf{Z}_p$:

$$\varepsilon^z = (1+\pi)^z = \sum_0^\infty \pi^i \binom{z}{i}, \tag{18}$$

d'où, pour g_a, la série convergente

$$g_a = \sum_{i=0}^\infty A_{a,i}\, \pi^i, \qquad A_{a,i} = \sum_\mu \mu^{-a} \binom{t(\mu)}{i}. \tag{19}$$

Exprimons $t(\mu)$ au moyen de (16), et observons que l'identité formelle $(1+T)^{\Sigma x_\rho} = \prod (1+T)^{x_\rho}$ donne

$$\binom{\Sigma\, x_\rho}{i} = \sum_{\Sigma i_\rho = i} \left(\prod_\rho \binom{x_\rho}{i_\rho} \right).$$

On obtient:

$$(20) \qquad A_{a,i} = \sum_{(i_\rho)} \sum_{\mu} \mu^{-a} \prod_{\rho} \binom{\mu^{p^\rho}}{i_\rho}$$

où $0 \leqslant \rho < n$, où la deuxième somme est étendue à $\mu \in M^\times$, et la première à tous les systèmes d'indices $(i_o, ..., i_{n-1})$ tels que $\sum i_\rho = i$; pour a donné, on va déterminer la plus petite valeur de i pour laquelle $A_{a,i} \neq 0$. Les coefficients du binôme qui figurent au second membre sont des polynômes en μ à coefficients dans $\mathbf{Q}$; d'ailleurs $\sum \mu^b$ a la valeur $q-1$ ou 0 suivant que b est ou non multiple de $q-1$.

Puisque $0 < a < q-1$, on peut écrire $a = \sum a_\rho p^\rho$ avec $0 \leqslant a_\rho < p$ pour $0 \leqslant \rho < n$. On a

$$(21) \quad \sum a_\rho = \min \left(\sum j_\rho \mid \sum j_\rho p^\rho \equiv a \bmod q-1 ; j_\rho \geqslant 0 \ (0 \leqslant \rho < n) \right),$$

le minimum étant atteint seulement pour $j_o = a_o, ..., j_{n-1} = a_{n-1}$. En effet, si l'un des j_ρ, par exemple j_λ, est $> p$, on peut diminuer $\sum j_\rho$ en remplaçant j_λ par $j_\lambda - p$ et $j_{\lambda+1}$ (resp. j_o si $\lambda = n-1$) par $j_{\lambda+1} + 1$ (resp. $j_o + 1$); mais si tous les j_ρ sont $< p$, on a $\sum j_\rho p^\rho = a$, d'où $j_\rho = a_\rho$ pour tout ρ.

Cela posé, supposons $A_{a,i} \neq 0$. Le second membre de (20) doit donc contenir un terme de degré $\equiv 0 \bmod q-1$; cela implique qu'il y a des entiers i_ρ, j_ρ tels que $\sum i_\rho = i$, $0 \leqslant j_\rho \leqslant i_\rho$, $\sum j_\rho p^\rho \equiv a \bmod q-1$, donc $i \geqslant \sum a_\rho$ d'après (21). De plus, si $i = \sum a_\rho$, ces conditions impliquent $i_\rho = j_\rho = a_\rho$ pour tout ρ, ce qui donne:

$$(22) \qquad A_{a,i} = (q-1) \prod_{\rho} (a_\rho !)^{-1} .$$

La partie principale de g_a est donc $-\prod_{\rho} (\pi^{a_\rho}/a_\rho !)$. C'est le résultat définitif sur la question; on peut dire que pour l'essentiel il se trouvait déjà dans Kummer. On en déduit évidemment la partie principale des sommes de Jacobi, que Jacobi avait déjà calculée dans des cas assez généraux ([3 b]). Les méthodes de Stickelberger et de Kummer, et même sans doute celles de Jacobi, ne diffèrent pas, pour l'essentiel, de celle qu'on vient d'exposer. Comme ce résultat donne l'ordre de toute somme de Gauss (ou de Jacobi) relative à $\mathbf{F}_q$, en toute place p-adique, il contient évidemment aussi la décomposition de toutes ces sommes en facteurs premiers.

15. Tout cela ne touche pas à la question (b) du n° 12, qui, en revanche, est liée, d'une part à la démonstration de la loi d'Eisenstein, et d'autre part à la propriété des sommes de Jacobi de définir des caractères de Hecke.

Commençons par la première, en nous plaçant d'abord dans le cas le plus général; nous suivons Eisenstein ([5 b]) librement, mais d'assez près.

Soit ζ une racine primitive de $Z^m = 1$; soit $k = \mathbf{Q}(\zeta)$. Soit $\mathfrak{p}$ idéal premier (premier à m) dans k, de norme $q = p^n$; on identifie $\mathbf{F}_q$ avec $\mathbf{Z}[\zeta]/\mathfrak{p}$; alors $(x/\mathfrak{p})$ détermine un caractère χ d'ordre m sur $\mathbf{F}_q$. Soit ε une racine primitive de $X^p = 1$; soit t la trace prise dans $\mathbf{F}_q/\mathbf{F}_p$; $x \mapsto \varepsilon^{t(x)}$ est un caractère additif ψ de $\mathbf{F}_q$. Posons $\Phi(\mathfrak{p}) = (-1)^m G(\chi, \psi)^m$; Φ ne dépend pas du choix de ε; on l'étend à tous les idéaux premiers à m dans k par la règle $\Phi(\mathfrak{ab}) = \Phi(\mathfrak{a})\Phi(\mathfrak{b})$. Appliquant le résultat du n° 14 à $G(\chi, \psi)$ aux places de k déterminées par $\mathfrak{p}$ et ses conjugués, on trouve facilement la décomposition de l'idéal principal $(\Phi(\mathfrak{p}))$, puis de $(\Phi(\mathfrak{a}))$, en facteurs premiers; elle est donnée par une puissance symbolique

$$(\Phi(\mathfrak{a})) = \mathfrak{a}^{\Theta}, \tag{23}$$

où Θ est un élément de l'anneau de groupe du groupe de Galois de $k/\mathbf{Q}$, défini comme suit. Pour tout $t \in (\mathbf{Z}/m\mathbf{Z})^\times$, soit σ_t l'automorphisme de k qui change ζ en ζ^t. Alors on a

$$\Theta = \sum_{\substack{0<t<m \\ (t,m)=1}} t \cdot \sigma_{-t}^{-1} \tag{24}$$

(résultat obtenu par Kummer pour m premier).

En particulier, on peut appliquer (23) à un idéal principal $\mathfrak{a} = (\alpha)$, de sorte qu'on peut écrire

$$\Phi(\alpha) = \varepsilon(\alpha) \cdot \alpha^{\Theta}, \tag{24}$$

où $\varepsilon(\alpha)$ est une unité de k. Mais d'autre part la valeur absolue des sommes de Gauss est donnée par (4); on en déduit aussitôt $|\Phi(\mathfrak{a})|^2 = N(\mathfrak{a})^m$; tenant compte de (23) et (24), il s'ensuit que l'unité $\varepsilon(\alpha)$, ainsi que tous ses conjugués dans k, sont de valeur absolue 1. Le théorème de Kronecker montre qu'alors $\varepsilon(\alpha)$ est une racine de l'unité, de la forme $\pm\zeta^i$.

Soit maintenant $\mathfrak{p}'$ un idéal premier, premier à m, de norme $q' = p'^{n'} = mv + 1$. Pour $\mathfrak{p}$, χ, ψ comme précédemment, et $\mathfrak{p}$ premier à p', posons $G = G(\chi, \psi)$; on a:

$$G^{q'} \equiv \Sigma \chi(x)\psi(q'x) \equiv \chi(q')^{-1} G \equiv \left(\frac{N(\mathfrak{p}')}{\mathfrak{p}}\right)^{-1} G \bmod p'.$$

Mais on a aussi (cf. le cas $m = 3$ au n° 10):

$$G^{q'-1} = (G^m)^v \equiv \left(\frac{(-1)^m \Phi(\mathfrak{p})}{\mathfrak{p}'}\right) \equiv \left(\frac{\Phi(\mathfrak{p})}{\mathfrak{p}'}\right) \bmod \mathfrak{p}'.$$

Il s'ensuit qu'on a, chaque fois que $N(\mathfrak{a})$, $N(\mathfrak{b})$ sont premiers entre eux et à m:

$$\left(\frac{N(\mathfrak{b})}{\mathfrak{a}}\right) = \left(\frac{\Phi(\mathfrak{a})}{\mathfrak{b}}\right)^{-1},$$

puisqu'il en est ainsi pour $\mathfrak{a} = \mathfrak{p}$, $\mathfrak{b} = \mathfrak{p}'$. Prenons $\mathfrak{a} = (\alpha)$, et appliquons (24), en observant qu'on a, par transport de structure, pour $tu \equiv 1 \bmod m$, c'est-à-dire $\sigma_u = \sigma_t^{-1}$:

$$\left(\frac{\alpha^{\sigma_u}}{\mathfrak{b}}\right) = \left(\frac{\alpha}{\mathfrak{b}^{\sigma_t}}\right)^{\sigma_u} = \left(\frac{\alpha}{\mathfrak{b}^{\sigma_t}}\right)^{u}.$$

On obtient ainsi:

$$\left(\frac{N(\mathfrak{b})}{\alpha}\right) = \left(\frac{\varepsilon(\alpha)}{\mathfrak{b}}\right)^{-1} \cdot \left(\frac{\alpha}{N(\mathfrak{b})}\right). \tag{25}$$

16. Pour tirer de là la loi d'Eisenstein, nous nous restreignons maintenant (comme le faisait Eisenstein dès le début) au cas où m est un nombre premier impair l. Dans ce cas, on a, avec $G = G(\chi, \psi)$ comme tout à l'heure:

$$(-G)^l \equiv -\sum_{x \neq 0} \chi(x)^l \psi(lx) \equiv -\sum_{x \neq 0} \psi(lx) = 1 \mod l,$$

donc $\Phi(\mathfrak{a}) \equiv 1 \bmod l$ quel que soit $\mathfrak{a}$ (ce qui répond à la question (b) du n° 12), et par suite $\varepsilon(\alpha) = \pm 1$ chaque fois que α est tel que $\alpha^{\Theta} \equiv 1 \bmod (\zeta - 1)^2$; il suffit pour cela qu'on ait $\alpha \equiv x \bmod (\zeta - 1)^2$ avec $x \in \mathbf{Z} - l\mathbf{Z}$; Eisenstein dit alors que α est « primaire ». En langage moderne, ces résultats font voir aussi que $\mathfrak{a} \mapsto \Phi(\mathfrak{a})$ est un « caractère de Hecke » (un « Grössencharakter ») de conducteur $(\zeta - 1)^2$. Si dans (25) on prend α « primaire », et qu'on prenne pour $\mathfrak{b}$ un idéal premier $\mathfrak{p}$ de norme $q = p^n$, on obtient $(p/\alpha)^n = (\alpha/p)^n$. Mais n divise $l - 1$, donc est premier à l. On a donc $(p/\alpha) = (\alpha/p)$, d'où finalement $(a/\alpha) = (\alpha/a)$ chaque fois que a est entier rationnel premier à l, et que α est premier à a et « primaire ». C'est la loi d'Eisenstein.

17. En ce qui concerne les développements plus récents, nous serons très brefs.

Pour mémoire, rappelons que les sommes de Gauss figurent parmi les facteurs constants locaux dans les équations fonctionnelles des fonctions L; ces facteurs sont dits aussi « nombres radiciels » (« root-numbers », « Wurzelzahlen »), sans doute parce que Hilbert, qui avait une sorte de

génie pour les mauvaises terminologies, s'était avisé de baptiser « Wurzelzahl » ce qu'avant lui on nommait « résolvante de Lagrange », et « Lagrange'sche Wurzelzahl » ce qu'on a nommé ici somme de Gauss. Les facteurs constants des équations fonctionnelles, pour les séries L de Dirichlet, apparaissent pour la première fois dans le calcul de $L(1)$ par Dirichlet; ce calcul n'est pas autre chose, en substance, que la vérification de l'équation fonctionnelle qui relie $L(1)$ à $L(0)$. Naturellement, ils reparaissent, sous une forme plus générale, dans les équations fonctionnelles des fonctions L de Hecke, puis d'Artin. Ils ont fait l'objet de travaux considérables de Dwork et de Langlands, complétés en dernier lieu par Deligne. Langlands a mis en évidence le rôle essentiel joué par ces facteurs dans la théorie des représentations. L'auteur de ces lignes offre une médaille (en chocolat) à celui qui proposera la meilleure dénomination pour les facteurs en question.

18. Lorsqu'on rencontre des nombres algébriques qui, ainsi que tous leurs conjugués, ont une valeur absolue de la forme $p^{n/2}$ avec p premier, on est toujours tenté, de nos jours, de se demander si ce sont des racines de fonctions zêta en caractéristique p. Il en est effectivement ainsi des sommes de Gauss et de Jacobi, comme Hasse et Davenport s'en sont aperçus en 1934 ([8]; cf. [9 a]); c'est même à cette occasion qu'ils ont découvert l'importante relation entre sommes de Gauss à laquelle leur nom est resté attaché. En particulier, les sommes de Jacobi d'ordre m sont racines (ou pôles, suivant la dimension) des fonctions zêta des variétés $\sum a_i X_i^m = 0$; rétrospectivement, on constate que des cas particuliers, exprimés dans un autre langage, étaient déjà connus de Gauss, et que des cas assez généraux sont implicites chez Kummer. Notons en passant, à titre de curiosité historique, que le célèbre *Tagebuch* de Gauss s'ouvre et se referme sur la cyclotomie: il débute, en date du 30 mars 1796, par la division du cercle en 17 parties; il se termine, le 9 juillet 1814, par une note sur le nombre de solutions de $1 = x^2 + y^2 + x^2y^2$ dans $\mathbf{F}_p$, relié à « la théorie des résidus biquadratiques » (donc aux « périodes » d'ordre 4).

Quant à la relation de Hasse-Davenport, elle relie les sommes de Gauss d'ordre m dans $\mathbf{F}_q$ et dans une extension $\mathbf{F}_Q$ de $\mathbf{F}_q$. Soit $Q = q^N$; soient t et n la trace et la norme dans $\mathbf{F}_Q/\mathbf{F}_q$; soit $G = G(\chi, \psi)$ une somme de Gauss relative à $\mathbf{F}_q$; soit G' la somme de Gauss de $G(\chi \circ n, \psi \circ t)$ relative à F_Q. Alors on a $-G' = (-G)^N$. Soit dit en passant, ceci montre une fois de plus qu'on a pris « le mauvais signe » dans la notation usuelle des sommes de Gauss. Il n'est sans doute pas trop tard pour rectifier cette faute.

19. On peut appliquer les résultats cités au n° 18, sur les fonctions zêta des variétés $\sum a_i X_i^m = 0$ (et, notons-le en passant, de toutes les variétés qu'on peut définir comme quotients de ces dernières par des groupes finis d'automorphismes) au calcul des fonctions zêta de ces mêmes variétés sur des corps de nombres algébriques. On trouve que ces fonctions sont des produits de fonctions L de Hecke, ce qui revient à dire que les sommes de Jacobi définissent des caractères de Hecke dans les corps cyclotomiques. Comme on l'a vu au n° 16, un cas particulier important (relatif aux sommes $(-G)^l$, où G est une somme de Gauss d'ordre l premier impair) formait le fond de la démonstration d'Eisenstein pour sa loi de réciprocité. En fait, il s'agit là d'un résultat très général sur les caractères de Hecke « cyclotomiques » dans tous les corps abéliens sur $\mathbf{Q}$ (cf. [9 b, c]); naturellement, ce sont les corps totalement imaginaires qui sont intéressants de ce point de vue.

Une fois obtenus ces caractères, on peut se proposer d'étudier les fonctions L de Hecke qui leur correspondent, et notamment leurs valeurs $L(s)$ pour s entier. Il y a lieu de citer à ce sujet un résultat remarquable de Chowla et Selberg (v. [10]); convenablement interprété, celui-ci fait voir que la valeur, en $s = 1$, de la fonction L définie par un certain caractère « cyclotomique » sur $\mathbf{Q}(\sqrt{-n})$ (pour n premier $\equiv 3 \bmod 4$, c'est celui même qu'on a défini d'après Cauchy au n° 9) s'exprime élémentairement au moyen de π et des valeurs de la fonction $\Gamma(s)$ pour $s = a/n$, $0 < a < n$. On pourrait sans doute aller beaucoup plus loin dans cette voie.

BIBLIOGRAPHIE

[1] LAGRANGE. (a) Réflexions sur la résolution algébrique des équations, *Nouveaux Mém. de l'Acad. R. des Sc. et B.-L. de Berlin*, 1770-1771 = *Oeuvres*, vol. III, p. 332;
(b) Traité de la résolution numérique des équations. 2e éd., Paris 1808, Notes XIII-XIV = *Oeuvres*, vol. VIII, p. 295-367.

[2] GAUSS. (a) Disquisitiones arithmeticae. 1801 = *Werke*, vol. I;
(b) Summatio serierum quorundam singularium. 1811 = *Werke*, vol. II, p. 11;
(c) Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae, 1818 = *Werke*, vol. II, p. 51;
(d) Theoria residuorum biquadraticorum. *Commentatio prima*, 1828 = *Werke*, vol. II, p. 65;
(e) Disquisitionum circa aequationes puras ulterior evolutio. *Werke*, vol. II, p. 243.

[3] JACOBI. (a) Briefe an Gauss. *Werke*, vol. VII, p. 391-400;
(b) Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie. *Berl. Monatsber.* 1837, p. 127 = *Crelles J. Vol. 30* (1846), p. 166 = *Werke*, vol. VI, p. 254.

[4] CAUCHY. Mémoire sur la Théorie des Nombres. *Mém. Ac. Sc.* XVII (1840) = *Oeuvres* (I), vol. III.

[5] EISENSTEIN. (a) Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. *Crelles J. 27* (1844), p. 289;
(b) Beweis der allgemeinsten Reciprocitätsgesetze zwischen reellen und complexen Zahlen. *Monatsber. d. k. Akad. d. Wiss. zu Berlin*, 1850, p. 189.
[6] KUMMER. Ueber die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. *Crelles J. 44* (1851), p. 93.
[7] STICKELBERGER, L. Ueber eine Verallgemeinerung der Kreistheilung. *Math. Ann. 37* (1890), p. 321.
[8] DAVENPORT, H. und H. HASSE. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *Crelles J. 172* (1935), p. 151.
[9] WEIL, A. (a) Numbers of solutions of equations in finite fields. *Bull. Am. Math. Soc. 55* (1949), p. 197;
(b) Jacobi sums as „Grössencharaktere". *Trans. Am. Math. Soc. 73* (1952), p. 487;
(c) Sommes de Jacobi et caractères de Hecke. *Gött. Nachr.* (à paraître).
[10] SELBERG, A. and S. CHOWLA. On Epstein's Zeta-Function. *Crelles J. 227* (1967), p. 86.

(Reçu le 22 juin 1974)

André Weil

The Institute for Advanced Study
Princeton, N.J., 08540