Traduction d'un extrait de A classical introduction to modern number theory de K. Ireland et M. Rosen, Springer, 1990, p. 69 et suivantes (Denise Vella-Chemla, juin 2023)[1]

2. Caractère quadratique de 2

Soit $\zeta = e^{2\pi i/8}$. Alors ζ est une racine primitive huitième de l'unité. Donc $0 = \zeta^8 - 1 = (\zeta^4 - 1)(\zeta^4 + 1)$. Puisque $\zeta^4 \neq 1$, on a $\zeta^4 = -1$. En multipliant par ζ^{-2} et en ajoutant alors ζ^{-2} au deux côtés de l'égalité, cela amène $\zeta^2 + \zeta^{-2} = 0$. Cette équation est également facilement dérivable de l'observation que $\zeta^2 = e^{i(\pi/2)} = i$.

Le caractère quadratique de 2 va maintenant être déduit de la relation

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2.$$

Appelons $\tau = \zeta + \zeta^{-1}$ et notons que et ζ et τ sont des nombres algébriques. On peut par conséquent travailler avec les congruences dans l'anneau des entiers algébriques.

Soit p un nombre premier impair dans $\mathbb{Z}$ et remarquons que

$$\tau^{p-1} = (\tau^2)^{(p-1)/2} = 2^{(p-1)/2} \equiv (2/p) \pmod{p}.$$

Il en découle que $\tau^p = (2/p)\tau \pmod{p}$. Par la proposition 6.1.6, $\tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \pmod{p}$.

En se rappelant que $\zeta^8 = 1$, on a $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ pour $p = \pm 1 \pmod 8$ et $\zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3}$ pour $p = \pm 3 \pmod 8$. Le résultat dans le dernier cas peut être simplifié en observant que $\zeta^4 = -1$ implique que $\zeta^3 = -\zeta^{-1}$. Ainsi $\zeta^p + \zeta^{-p} = -(\zeta + \zeta^{-1})$ si $p = \pm 3 \pmod 8$. Résumons

$$\zeta^p + \zeta^{-p} = \begin{cases} \tau, & \text{si } p \equiv \pm 1 \pmod 8, \\ -\tau, & \text{si } p \equiv \pm 3 \pmod 8, \end{cases}$$

Substituer ce résultat dans la relation $\tau^p \equiv (2/p)\tau \pmod{p}$ amène

$$(-1)^\varepsilon \tau \equiv \left(\frac{2}{p}\right) \tau \pmod{p}, \qquad \text{où } \varepsilon \equiv \frac{p^2 - 1}{8} \pmod 2.$$

Multiplions les deux côtés de la congruence par τ. Alors

$$(-1)^\varepsilon 2 \equiv \left(\frac{2}{p}\right) 2 \pmod{p},$$

ce qui implique que

$$-1^\varepsilon \equiv \left(\frac{2}{p}\right) \pmod{p}$$

Cette dernière congruence implique que $\left(\frac{2}{p}\right) = (-1)^\varepsilon$, qui est le résultat souhaité.

[1] On a utilisé la convention d'écrire le petit mot (mod ...) devant le module.

Euler (1707-1783), dans un article précédent a démontré que 2 est un résidu quadratique modulo les nombres premiers p avec $p \equiv 1 \pmod 8$. Sa méthode contient l'idée-clé de la preuve ci-dessous.

Euler suppose que $U(\mathbb{Z}/p\mathbb{Z})$ est un groupe cyclique. Gauss a été le premier à fournir une preuve rigoureuse de ce fait (voir le théorème 1 du chapitre 4). Soit λ un générateur de $U(\mathbb{Z}/p\mathbb{Z})$ et appelons $\gamma = \lambda^{(p-1)/8}$. Alors γ est d'ordre 8, de telle façon que $\gamma^4 = -1$ et $\gamma^2 + \gamma^{-2} = \overline{0}$. Donc, $(\gamma + \gamma^{-1})^2 = \gamma^2 + \overline{2} + \gamma^{-2} = \overline{2}$. Cela montre que $\overline{2}$ est un carré dans $U(\mathbb{Z}/p\mathbb{Z})$, ce qui est équivalent à dire que 2 est un résidu quadratique modulo p.

Si $p \not\equiv 1 \pmod 8$, cette preuve ne peut pas démarrer. Pourtant, la théorie des corps finis nous permet de mener à bien une preuve complète de la loi de réciprocité quadratique en utilisant l'idée d'Euler. Nous développerons la théorie des corps finis au chapitre 7.

3. Sommes quadratiques de Gauss

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

Tout au long de cette section, 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, cette somme est nulle.

Preuve. Si $a = 0 \pmod p$, alors $\zeta^a = 1$, et donc $\sum_{t=0}^{p-1} \zeta^{at} = p$. Si $a \neq 0 \pmod p$, alors $\zeta^a \neq 1$ et $\sum_{t=0}^{p-1} \zeta^{at} = (\zeta^{ap} - 1)/(\zeta^a - 1) = 0$. □

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

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

Toutes les sommes du reste de cette section seront sur le domaine de zéro à $p - 1$. On simplifiera la notation en évitant de réécrire ce fait à chaque fois.

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

Preuve. Par définition $(0/p) = 0$. Concernant les $p - 1$ termes restant dans la somme, la moitié sont des +1 et l'autre moitié sont des -1, puisque par le corollaire 1 de la proposition 5.1.2, il y a autant de résidus quadratiques que de non résidus quadratique mod p. □

Nous sommes maintenant en mesure d'introduire la notion de somme de Gauss.

Définition. $g_a = \sum_t (t/p)\zeta^{at}$ est appelée 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. Cela donne le résultat dans le cas où $a \equiv 0 \pmod{p}$.

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

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

On a utilisé le fait que at couvre un système complet de résidus mod p quand t le fait et que (x/p) et ζ^x dépendent seulement de la classe résiduelle de x modulo p.

Puisque $(a/p)^2 = 1$ quand $a \not\equiv 0 \pmod{p}$, notre résultat s'en déduit en multipliant l'équation $(a/p)g_a = g_1$ des deux côtés par (a/p). □

À partir de maintenant, on va changer g_1 en g. Il découle de la proposition 6.3.1 que $g_a^2 = g^2$ si $a \not\equiv 0 \pmod{p}$. On va maintenant déduire cette valeur commune.

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

PREUVE. L'idée de la preuve consiste à 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 découle que

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

Maintenant, notons 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 1, on obtient

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

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

Soit $p^* = (-1)^{(p-1)/2}p$. L'équation $g^2 = p^*$ est l'analogue souhaité de l'équation $\tau^2 = 2$. Soit $q \neq p$ un autre nombre premier impair. On procède de la façon suivante, pour démontrer la loi de réciprocité quadratique 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

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

En utilisant la proposition 6.1.6, on voit que

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

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

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

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

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

ce qui implique que

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

et finalement

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

Pour voir que ce résultat est ce que nous souhaitions, notons simplement 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 quadratique de Gauss que nous avons utilisée peut être considérablement généralisée. On présentera quelques-unes de ces généralisations après avoir développé la théorie des corps finis. Les sommes cubiques de Gauss seront utilisées pour démontrer la loi de réciprocité cubique, et les sommes de Gauss quartiques seront utilisées pour démontrer la loi de réciprocité biquadratique.

4. Le signe de la somme quadratique de Gauss[2]

Selon la proposition 6.3.2, la somme quadratique de Gauss a pour valeur $\pm\sqrt{p}$ si $p \equiv 1 \pmod{4}$ et $\pm i\sqrt{p}$ 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 que le signe plus est vérifiée dans chaque cas a été faite par Gauss et enregistrée dans son journal en mai 1801. Ce n'est que quatre ans plus tard qu'il a trouvé la démonstration. Le 30 août 1805, Gauss a noté dans son journal qu'il avait finalement terminé une preuve du "très élégant théorème mentionné en 1801". Il écrivit à son ami W. Olbers le 3 septembre 1805 qu'il s'était rarement passé une semaine depuis quatre ans sans qu'il ait essayé en vain de prouver sa conjecture. Finalement, selon Gauss, "Wie der Blitz einschlägt, hat sich das Räthsel gelöst..." (alors que la foudre tombait, le puzzle a été résolu).

Des preuves ultérieures ont été trouvées par Dirichlet, Cauchy, Kronecker, Mertens, Schur, et d'autres. Dans cette section, on présente l'une des démonstrations de Kronecker.

[2]Dans cette section, la somme de Gauss g sera dénotée par $g(\chi)$ avec $\chi(t) = (t/p)$ par définition.

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 du chapitre "lemme de Gauss"), il suffit de montrer que $1 + x + \ldots + x^{p-1}$ n'a pas de factorisation 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 où chacun a un degré plus grand que un. En posant $x = 1$, on obtient $p = f(1)g(1)$. On peut donc supposer que $g(1) = 1$. En utilisant un trait au-dessus des nombres pour désigner les classes de congruences modulo p, on conclut que $\overline{g}(\overline{1}) \neq \overline{0}$. D'un autre côté, puisque $p| \binom{p}{j}, j = 1, \ldots, p-1$, on a $x^p - 1 = (x-1)^p \pmod p$ et la division des deux côtés à la fois par $x - 1$ nous montre que $1 + x + +x^{p-1} \equiv (x-1)^{p-1} \pmod p$. Par le théorème 2, le chapitre 1 et la proposition 3.3.2 il s'ensuit que $g(x) \equiv (x-1)^s \pmod p$ pour quelques entiers positifs s. Pourtant, 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 plus tard.

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

PREUVE. On a $x^p - 1 = (x-1)\prod_{j=1}^{p-1}(x - \zeta^j)$. Divisons par $x - 1$ et posons $x = 1$ pour obtenir $p = \prod_r (1 - \zeta^r)$, où le produit est calculé sur tout ensemble complet de représentants des classes suivant un sous-groupe non nulles modulo p. On voit facilement que les entiers $\pm(4k-2)$, $k = 1, 2, \ldots, (p-1)/2$ forment un tel système de restes. Donc

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

tous les produits étant sur $k = 1, 2, \ldots, (p-1)/2$. □

Proposition 6.4.3.

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

PREUVE. Par la Proposition 6.4.2, on a seulement à calculer le signe du produit. Le produit est

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

Mais $\sin((4k-2)/p)\pi < 0$ if $(p+2)/4 < k \leq (p-1)/2$. Il en découle que le produit a $(p-1)/2 - [(p+2)/4]$ termes négatifs et on voit 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 recherché 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 complété 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 également 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 $1 + x + \ldots + x^{p-1}$ and $x - 1$ 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 $z^{(p-1)/2}$ du côté gauche de (3) est

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

De l'autre côté par l'exercice 21, le coefficient de $z^{(p-1)/2}$ du côté droit de (3) est pA/B où $p \not| B$, A et B étant des nombres entiers. En égalant les coefficients, en multipliant par $B((p-1)/2)!$ et en réduisant modulo p, on obtient que

$$\begin{aligned}
\sum_{j=1}^{p-1} \chi(j) j^{(p-1)/2} &\equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{(p-1)/2} (4k-2) \pmod{p} \\
&\equiv \varepsilon(2.4.6 \ldots p-1) \prod_{k=1}^{(p-1)/2} (2k-1) \\
&\equiv \varepsilon(p-1)! \\
&\equiv -\varepsilon(p)
\end{aligned}$$

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

Par la proposition 5.1.2, $j^{(p-1)/2} \equiv \chi(j) \pmod{p}$, ainsi on a

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

et donc

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

Puisque $\varepsilon = \pm 1$, on conclut finalement que $\varepsilon = 1$. Ceci conclut la démonstration.

Les résultats peuvent être énoncés de la façon suivante

Théorème 1. *La valeur de la somme quadratique de Gauss $g(\chi)$ est donnée par*

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