Agrégation interne de Mathématiques
session 2000
première composition

Enoncé

http://perso.wanadoo.fr/megamaths

[0] [ag47e]

L'objet de ce problème est l'étude des sommes de Gauss $G(m) = \sum_{k=0}^{m-1} e^{2i\pi k^2/m}$ et la démonstration de la loi de réciprocité quadratique.

Bien que les quatre parties s'enchaînent logiquement, la rédaction de l'énoncé permet d'aborder la partie III de façon indépendante. Dans la partie IV, les références aux parties qui précèdent sont clairement indiquées. Toute question pourra être traitée en admettant les résultats des questions précédentes.

Si a, b et m sont trois éléments de l'anneau $\mathbf{Z}$ des entiers relatifs, la relation $a \equiv b \pmod{m}$ signifie que m divise $b - a$ dans $\mathbf{Z}$.

I . Carrés modulo m

Soit m un entier ≥ 2. On note $\mathbf{Z}/m\mathbf{Z}$ l'anneau des classes d'entiers *modulo* m, et $(\mathbf{Z}/m\mathbf{Z})^\times$ le groupe multiplicatif des éléments inversibles de $\mathbf{Z}/m\mathbf{Z}$.

On rappelle que, si p est un nombre premier, l'anneau $\mathbf{Z}/p\mathbf{Z}$ est un corps commutatif, et le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique.

Si $a \in \mathbf{Z}$ est un entier quelconque, on note $[a]_m$ la classe de a dans l'anneau $\mathbf{Z}/m\mathbf{Z}$.

1) Soit $a \in \mathbf{Z}$ un entier. Démontrer que, pour que $[a]_m$ soit inversible dans $\mathbf{Z}/m\mathbf{Z}$, il faut et il suffit que les entiers a et m soient premiers entre eux. (On pourra utiliser le théorème de Bézout).

2) Pour tout élément α de $(\mathbf{Z}/m\mathbf{Z})^\times$, on pose $\sigma(\alpha) = \alpha^2$.

a) Démontrer que l'application σ de $(\mathbf{Z}/m\mathbf{Z})^\times$ dans lui-même ainsi définie respecte la multiplication. En déduire que son image S est un sous-groupe de $(\mathbf{Z}/m\mathbf{Z})^\times$.

b) Pour $m = 5$, puis pour $m = 15$, expliciter la liste des entiers a, où $0 \leq a \leq m - 1$, pour lesquels $[a]_m$ est inversible dans $\mathbf{Z}/m\mathbf{Z}$, et, parmi ceux-ci, la liste de ceux pour lesquels $[a]_m$ appartient à S.

3) Soit p un nombre premier <u>impair</u> positif, c'est-à-dire ≥ 3. On pose $p = 2p' + 1$.

a) Démontrer que $(\mathbf{Z}/p\mathbf{Z})^\times$ possède $p - 1$ éléments.

b) Démontrer que les éléments $[-1]_p$ et $[1]_p$ sont distincts.

c) Soit K le noyau du morphisme σ défini en (I.2). Démontrer que K est constitué des deux éléments $[-1]_p$ et $[1]_p$.

d) En déduire que le nombre d'éléments de l'image S du morphisme σ est égal à p'.

e) On note T le complémentaire de S dans $(\mathbf{Z}/p\mathbf{Z})^\times$. Déterminer le cardinal de T. Démontrer que, si l'on fixe un élément θ de T, on a $T = \{\theta s,\ s \in S\}$.

f) Pour tout élément α de $(\mathbf{Z}/p\mathbf{Z})^\times$, on pose

$$\chi_p(\alpha) = \begin{cases} 1 & \text{si} \quad \alpha \in S, \\ -1 & \text{si} \quad \alpha \in T. \end{cases}$$

Démontrer que l'application χ_p de $(\mathbf{Z}/p\mathbf{Z})^\times$ dans le groupe multiplicatif $\{1,-1\}$ ainsi définie est un morphisme surjectif de groupes.

g) Démontrer que l'application χ_p est le seul morphisme surjectif du groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ dans le groupe multiplicatif $\{1,-1\}$.

4) Comme dans la question (I.3), on désigne par p un nombre premier impair positif. Pour tout nombre entier $a \in \mathbf{Z}$, non divisible par p, on pose

$$\left(\frac{a}{p}\right) = \chi_p([a]_p).$$

On a vu dans la question (I.3) que le nombre $\left(\frac{a}{p}\right)$ est égal à 1 ou -1, et qu'il ne dépend que de la classe de a *modulo* p. Il est appelé *symbole de Legendre*.

Calculer le nombre $\left(\frac{a}{11}\right)$ pour tout entier a tel que $1 \leq a \leq 10$.

II . Symbole de Legendre

Comme dans la partie I, soit p un nombre premier impair positif. On pose $p = 2p' + 1$. On se propose de calculer, en fonction des valeurs de p, le symbole de Legendre $\left(\frac{-1}{p}\right)$.

1) Soit α un élément de $(\mathbf{Z}/p\mathbf{Z})^\times$. Démontrer que l'on a $\alpha^{2p'} = [1]_p$, et en déduire que $\alpha^{p'}$ est égal à $[1]_p$ ou $[-1]_p$ (on utilisera les résultats de la question (I.3)).

2) Pour tout élément α de $(\mathbf{Z}/p\mathbf{Z})^\times$, on pose

$$\varphi(\alpha) = \begin{cases} 1 & \text{si} \quad \alpha^{p'} = [1]_p \\ -1 & \text{si} \quad \alpha^{p'} = [-1]_p \end{cases}$$

a) Démontrer que l'on définit ainsi un morphisme φ du groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ dans le groupe multiplicatif $\{1,-1\}$.

b) Démontrer que le morphisme φ est surjectif (on pourra utiliser le fait que le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique).

c) En déduire que, pour tout nombre entier a premier à p, on a

$$a^{p'} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

3) Démontrer les équivalences suivantes :

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4,$$
$$\left(\frac{-1}{p}\right) = -1 \iff p \equiv 3 \pmod 4.$$

III . Sommes de Gauss par la méthode de Dirichlet

Soit m un entier ≥ 1. Pour tout nombre réel $t \in [0, 2\pi]$, on pose

$$f_0(t) = \sum_{k=0}^{m-1} \exp\Big(i \, \frac{(t+2\pi k)^2}{2\pi m} \Big).$$

On note f la fonction périodique sur $\mathbf{R}$, de période 2π, qui coïncide avec f_0 sur $[0, 2\pi[$.

1) Démontrer l'égalité $f_0(0) = f_0(2\pi)$. Démontrer que, pour tout entier $n \in \mathbf{Z}$, la fonction f est de classe C^∞ sur l'intervalle $[2\pi n, 2\pi(n+1)]$, et qu'elle est continue sur $\mathbf{R}$.

2) Pour tout entier $n \in \mathbf{Z}$, on note c_n le coefficient de Fourier

$$c_n = \frac{1}{2\pi} \int_0^{2\pi} e^{-int} \, f(t) \, dt.$$

a) En utilisant le changement de variable $u = \dfrac{t}{2\pi} + k - \dfrac{mn}{2}$, démontrer l'égalité

$$c_n = e^{-i\pi m n^2/2} \int_{-mn/2}^{m-mn/2} e^{2i\pi u^2/m} \, du.$$

b) Calculer la valeur de $\exp\big(-i\pi \frac{mn^2}{2}\big)$ suivant la parité de l'entier n.

c) Pour tout entier $q \in \mathbf{Z}$, on pose

$$u_q = \int_{mq}^{m(q+1)} e^{2i\pi u^2/m} \, du, \qquad v_q = \int_{m(q-\frac{1}{2})}^{m(q+\frac{1}{2})} e^{2i\pi u^2/m} \, du.$$

Démontrer les égalités

$$c_{2q} = u_{-q} \qquad \text{et} \qquad c_{2q+1} = e^{-i\pi m/2} \, v_{-q}.$$

d) Démontrer que les séries $\sum_{q=1}^{\infty} (u_q + u_{-q})$ et $\sum_{q=1}^{\infty} (v_q + v_{1-q})$ sont absolument convergentes et que l'on a

$$f(0) = u_0 + \sum_{q=1}^{\infty} (u_q + u_{-q}) + e^{-i\pi m/2} \sum_{q=1}^{\infty} (v_q + v_{1-q}).$$

3) a) Etudier la convergence de l'intégrale impropre $\displaystyle\int_0^{\infty} \frac{e^{2i\pi y}}{\sqrt{y}} \, dy$.

b) Démontrer que l'intégrale impropre $\mathrm{J} = \displaystyle\int_{-\infty}^{+\infty} e^{2i\pi x^2} dx$ est convergente.

c) Démontrer que l'on a

$$f(0) = \mathrm{J} \, (1 + e^{-i\pi m/2}) \sqrt{m}. \tag{1}$$

d) En écrivant la relation (1) de c) dans le cas particulier $m = 1$, calculer la valeur de J.

e) En déduire, pour tout entier $m \geq 1$, la valeur de la somme $\mathrm{G}(m) = \displaystyle\sum_{k=0}^{m-1} e^{2i\pi k^2/m}$.

IV . Loi de réciprocité quadratique

Dans cette partie du problème, on pose $\omega = e^{2i\pi/8}$. Pour tout entier $m \geq 1$, on pose

$$\mathrm{G}(m) = \sum_{k=0}^{m-1} e^{2i\pi k^2/m}, \qquad \mathrm{H}(m) = \sum_{k=0}^{m-1} e^{2i\pi k^2/2m}.$$

Si p et q sont deux entiers > 0 , on pose

$$\mathrm{L}(p,q) = \sum_{r=0}^{p-1} e^{4i\pi qr^2/p}.$$

Si X *est un ensemble fini, non vide, et si* f *est une application de* X *dans* C , *on note* $\sum_{x\in \mathrm{X}} f(x)$ *la somme de tous les nombres complexes* $f(x)$ *lorsque* x *parcourt l'ensemble* X . *On pourra utiliser, sans chercher à les démontrer, les propriétés suivantes :*

(P1) *Si* Y *est un ensemble fini non vide et si* ϕ *est une bijection de* Y *sur* X , *on a*

$$\sum_{y\in \mathrm{Y}} (f\circ\phi)(y) = \sum_{x\in \mathrm{X}} f(x).$$

(P2) *Plus généralement, si* Y *est un ensemble fini non vide et si* ϕ *est une application surjective de* Y *sur* X , *pour tout élément* x *de* X , *on note* $\phi^{-1}(x)$ *l'ensemble des éléments* y *de* Y *tels que* $\phi(y) = x$. *Si tous les ensembles* $\phi^{-1}(x)$, *pour* $x \in \mathrm{X}$, *ont le même nombre* K *d'éléments, alors on a*

$$\sum_{y\in \mathrm{Y}} (f\circ\phi)(y) = \mathrm{K} \sum_{x\in \mathrm{X}} f(x).$$

(P3) *Si l'ensemble* X *est la réunion d'une suite finie* $(\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{N})$ *d'ensembles finis non vides et deux à deux disjoints (partition de* X), *on a*

$$\sum_{x\in \mathrm{X}} f(x) = \sum_{j=1}^{\mathrm{N}} \Big(\sum_{x\in \mathrm{X}_j} f(x) \Big).$$

1) a) Soit m un entier ≥ 2 . Démontrer qu'il existe une unique application ϵ_m de $\mathbf{Z}/m\mathbf{Z}$ dans C telle que, pour tout entier $k \in \mathbf{Z}$, on ait $\epsilon_m([k]_m) = e^{2i\pi k/m}$.

b) Démontrer l'égalité $\sum_{x\in \mathbf{Z}/m\mathbf{Z}} \epsilon_m(x) = 0$.

2) Soit toujours m un entier ≥ 2 .

a) Vérifier que, si k et h sont des entiers tels que $k \equiv h \pmod{2m}$, on a $e^{2i\pi k^2/4m} = e^{2i\pi h^2/4m}$.

b) Démontrer l'égalité $\sum_{k=0}^{2m-1} e^{2i\pi k^2/4m} = \sum_{k=2m}^{4m-1} e^{2i\pi k^2/4m}$. En déduire l'égalité $2\,\mathrm{H}(2m) = \mathrm{G}(4m)$.

c) En utilisant le calcul de la question (III,3), démontrer que l'on a $\mathrm{H}(4m) = 2\omega\sqrt{m}$.

3) Soient p et q deux nombres impairs > 0 premiers entre eux. Etant donnés deux entiers a et $b \in \mathbf{Z}$, on note $[\![a,b]\!]$ l'ensemble des entiers $n \in \mathbf{Z}$ tels que $a \leq n \leq b$.

a) Soit E l'ensemble produit $[\![0,3]\!] \times [\![0,p-1]\!] \times [\![0,q-1]\!]$. Pour $(\ell,r,s) \in \mathrm{E}$, on pose

$$k(\ell,r,s) = \ell pq + 4rq + 4sp,$$

et on note $\overline{k}(\ell,r,s)$ la classe de $k(\ell,r,s)$ dans le groupe $\mathbf{Z}/4pq\mathbf{Z}$. Démontrer que l'application $\overline{k}$ ainsi définie est une bijection de l'ensemble E sur $\mathbf{Z}/4pq\mathbf{Z}$.

b) En déduire l'égalité

$$\mathrm{H}(4pq) = \Big(\sum_{\ell=0}^{3} e^{2i\pi pq\ell^2/8}\Big)\Big(\sum_{r=0}^{p-1} e^{4i\pi qr^2/p}\Big)\Big(\sum_{s=0}^{q-1} e^{4i\pi ps^2/q}\Big).$$

4) Soient toujours p et q deux nombres impairs > 0 premiers entre eux.

a) Calculer la somme $\displaystyle\sum_{\ell=0}^{3} e^{2i\pi pq\ell^2/8}$.

b) En déduire qu'avec les notations introduites au début de la partie IV, on a

$$\mathrm{H}(4pq) = 2\,\omega^{pq}\,\mathrm{L}(p,q)\,\mathrm{L}(q,p).$$

c) Calculer $\mathrm{L}(1,p)$ et $\mathrm{L}(p,1)$.

5) On suppose que p est un nombre premier impair positif, que q est un nombre impair positif et premier à p, et on rappelle que l'on a posé $\displaystyle\mathrm{L}(p,q) = \sum_{r=0}^{p-1} e^{4i\pi qr^2/p}$.

a) Déduire de (IV,1) l'égalité $\quad 1 + \displaystyle\sum_{x\in(\mathbf{Z}/p\mathbf{Z})^\times} \epsilon_p([2]_p\,x) = 0.$

b) Dans la première partie, on a défini le morphisme σ du groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ dans lui-même par $\sigma(x) = x^2$; on a noté S l'image de l'application σ, et T le complémentaire de S dans $(\mathbf{Z}/p\mathbf{Z})^\times$. Démontrer les relations

$$\mathrm{L}(p,q) = 1 + \sum_{x\in(\mathbf{Z}/p\mathbf{Z})^\times} \epsilon_p([2q]_p\,\sigma(x)) = 1 + 2\sum_{y\in\mathrm{S}} \epsilon_p([2q]_p\,y).$$

c) Supposons que la classe $[q]_p$ appartienne à S. Démontrer que l'on a

$$\mathrm{L}(p,q) = 1 + 2\sum_{x\in\mathrm{S}} \epsilon_p([2]_p\,x).$$

En déduire que l'on a $\mathrm{L}(p,q) = \mathrm{L}(p,1)$.

d) Supposons que la classe $[q]_p$ appartienne à T. Démontrer que l'on a

$$\mathrm{L}(p,q) = 1 + 2\sum_{x\in\mathrm{T}} \epsilon_p([2]_p\,x).$$

Démontrer que l'on a $\mathrm{L}(p,q) + \mathrm{L}(p,1) = 0$.

Avec les notations des parties I et II, on a donc dans les deux cas $\mathrm{L}(p,q) = \left(\frac{q}{p}\right)\mathrm{L}(p,1)$.

6) On suppose enfin que p et q sont des nombres premiers impairs, positifs et distincts. On pose $p = 2p' + 1$ et $q = 2q' + 1$. Démontrer la relation

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