Agrégation interne 2000 de Mathématiques
1ère composition

solution proposée par Dany-Jack Mercier

IUFM de Guadeloupe, Morne Ferret,
BP399, Pointe-à-Pitre cedex 97159,
dany-jack.mercier@univ-ag.fr

NB : Le sujet de l'épreuve n'est pas joint à ce document. Il pourra être téléchargé au format pdf sur le site http://perso.wanadoo.fr/megamaths.

[0] [ag47] v1.23

Solution de la première composition de l'Agrégation interne 2000

Partie I

On notera indifféremment $\dot{a}$ ou $[a]_p$ la classe de a modulo p.

I.1. On a

$$\begin{aligned} \dot{x} \in (\mathbb{Z}/m\mathbb{Z})^\times &\Leftrightarrow \exists \dot{y} \in \mathbb{Z}/m\mathbb{Z} \text{ tel que } \dot{x}.\dot{y} = \dot{1} \\ &\Leftrightarrow \exists y \in \mathbb{Z} \quad \exists u \in \mathbb{Z} \quad xy + um = 1 \Leftrightarrow \operatorname{pgcd}(x, m) = 1. \end{aligned}$$

I.2.a. L'application σ est un homomorphisme du groupe $(\mathbb{Z}/m\mathbb{Z})^\times$ dans lui-même puisque $\sigma(\alpha\beta) = (\alpha\beta)^2 = \alpha^2\beta^2 = \sigma(\alpha)\sigma(\beta)$ pour tous $\alpha, \beta \in (\mathbb{Z}/m\mathbb{Z})^\times$. L'image S de ce morphisme sera donc un sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^\times$.

I.2.b. Compte tenu de I.1, $(\mathbb{Z}/5\mathbb{Z})^\times = \left\{\dot{1}, \dot{2}, \dot{3}, \dot{4}\right\}$ et $(\mathbb{Z}/15\mathbb{Z})^\times = \left\{\dot{1}, \dot{2}, \dot{4}, \dot{7}, \dot{8}, \dot{11}, \dot{13}, \dot{14}\right\}$.
Dans les deux cas et en élevant tous ces nombres au carré on trouve $S = \left\{\dot{1}, \dot{4}\right\}$.

I.3.a. Si p est premier, alors p est premier avec tout nombre entier x qu'il ne divise pas, et la question **I.1** montre que tout élément $\dot{x}$ non nul de $\mathbb{Z}/p\mathbb{Z}$ sera inversible.
On a montré que $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \left\{\dot{0}\right\}$ et que $\mathbb{Z}/p\mathbb{Z}$ est un corps.

I.3.b. L'égalité $\dot{1} = -\dot{1}$ entraîne $\dot{2} = \dot{0}$ et signifie que p divise 2. C'est impossible car p est premier et distinct de 2.

I.3.c. Les équivalences

$$\sigma(\alpha) = \dot{1} \Leftrightarrow \alpha^2 - \dot{1} = \dot{0} \Leftrightarrow (\alpha - \dot{1})(\alpha + \dot{1}) = \dot{0} \Leftrightarrow \alpha = \pm\dot{1}$$

montrent que $K = \left\{\dot{1}, -\dot{1}\right\}$.

I.3.d. Par décomposition canonique du morphisme σ on trouve $S = \operatorname{Im}\sigma \simeq (\mathbb{Z}/p\mathbb{Z})^\times / K$, d'où $\#S = \frac{p-1}{2} = p'$ en passant aux cardinaux.

I.3.e. On a $\#T = (p-1) - \#S = p'$. Si $s \in S$ alors $\theta s \in T$ (autrement $\theta s = s' \in S$ entraîne $\theta = s's^{-1} \in S$, ce qui est absurde d'après le choix de θ). On a montré l'inclusion $\{\theta s \,/\, s \in S\} \subset T$. Comme $\#T = p' = \#S = \#\{\theta s \,/\, s \in S\}$ (cette dernière égalité provenant du fait que l'application $s \mapsto \theta s$ est clairement une bijection de S sur $\{\theta s \,/\, s \in S\}$), cette inclusion est en fait une égalité.

I.3.f. L'application $\chi_p : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ est trivialement surjective, et c'est un homomorphisme de groupes multiplicatifs puisque :

$$\forall \alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^\times \quad \chi_p(\alpha\beta) = \chi_p(\alpha)\chi_p(\beta). \quad (*)$$

Pour vérifier cela, on envisage les quatre cas possibles. Si α et β sont des carrés, alors $\alpha\beta$ aussi et les deux membres de $(*)$ valent 1. Si α et β ne sont pas des carrés, on peut écrire $\alpha = \theta s$ et $\beta = \theta s'$ comme indiqué en **I.3.e**, où $s, s' \in S$ et $\theta \in T$. Dans ce cas $\alpha\beta = \theta^2 ss'$ appartient à S puisque S est un groupe et que θ^2, s et s' appartiennent à S. On a donc $\chi_p(\alpha\beta) = 1$, $\chi_p(\alpha) = \chi_p(\beta) = -1$ et l'égalité $(*)$ est assurée. Le dernier cas à envisager est celui où l'un des éléments α, β est dans S et l'autre dans T. Par exemple $\alpha \in S$ et $\beta \in T$. Dans ce cas $\alpha\beta = \gamma \in T$ (sinon $\gamma \in S$ entraîne $\beta = \alpha^{-1}\gamma \in S$, absurde) et $(*)$ est encore bien vérifiée.

I.3.g. Soit $f : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ un épimorphisme quelconque de $(\mathbb{Z}/p\mathbb{Z})^\times$ sur $\{\pm 1\}$. Si $\alpha \in S$, il existe $\beta \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $\alpha = \beta^2$ et donc $f(\alpha) = f(\beta)^2 = 1$. Comme f est surjective, il existe $\theta \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $f(\theta) = -1$. On a alors $\theta \in T$ (puisque l'on vient de voir que l'image de tout carré est 1). Si maintenant $\alpha \in T$, il existe $s \in S$ tel que $\alpha = \theta s$ (**I.3.e**), et l'on obtient

$$f(\alpha) = f(\theta s) = f(\theta) f(s) = (-1) \times 1 = -1.$$

En conclusion

$$f(\alpha) = \begin{cases} 1 \text{ si } \alpha \in S, \\ -1 \text{ si } \alpha \in T, \end{cases}$$

et $f = \chi_p$.

I.4.

$\dot{a}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$	$\dot{5}$	$\dot{6} = -\dot{5}$	$\dot{7} = -\dot{4}$	$\dot{8} = -\dot{3}$	$\dot{9} = -\dot{2}$	$\dot{10} = -\dot{1}$
$\dot{a}^2$	$\dot{1}$	$\dot{4}$	$\dot{9}$	$\dot{5}$	$\dot{3}$	$\dot{3}$	$\dot{5}$	$\dot{9}$	$\dot{4}$	$\dot{1}$
$\left(\frac{a}{11}\right)$	1	-1	1	1	1	-1	-1	-1	1	-1

Partie II

II.1. Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $p-1$, et le Théorème de Lagrange montre que $\alpha^{p-1} = \dot{1}$ pour tout élément α de ce groupe. On en déduit $\left(\alpha^{p'} - \dot{1}\right)\left(\alpha^{p'} + \dot{1}\right) = \dot{0}$ d'où $\alpha^{p'} = \pm\dot{1}$.

II.2.a. L'application

$$\begin{array}{rccc} \Phi : & (\mathbb{Z}/p\mathbb{Z})^\times & \to & \left\{\pm\dot{1}\right\} \\ & \alpha & \mapsto & \alpha^{p'} \end{array}$$

est clairement un morphisme de groupes, et le groupe $\left\{\pm\dot{1}\right\}$ est trivialement isomorphe à $\{\pm 1\}$, de sorte que l'application φ de l'énoncé apparaisse comme la composée de ces deux homomorphismes.

II.2.b. On a $\varphi\left(\dot{1}\right) = 1$ puisque $\dot{1}^{p'} = \dot{1}$. Si l'on avait $\alpha^{p'} = \dot{1}$ pour tout α dans $(\mathbb{Z}/p\mathbb{Z})^\times$, le polynôme $X^{p'} - \dot{1}$ possèderait $p-1 = 2p'$ racine dans le corps $\mathbb{Z}/p\mathbb{Z}$, ce qui est absurde puisque son degré est $p' < 2p'$. Il existera donc au moins un élément α tel que $\alpha^{p'} = -\dot{1}$ et $\varphi(\alpha) = -1$. L'application φ sera surjective.

Autre solution : Un générateur g de $(\mathbb{Z}/p\mathbb{Z})^\times$ est d'ordre $p-1 = 2p'$, donc $g^{p'} \neq [1]_p$. La question **II.1** montre alors que $g^{p'} = [-1]_p$. Comme $\varphi\left(\dot{1}\right) = 1$, on conclut à la surjectivité de φ.

II.2.c. L'application $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$ est un morphisme surjectif et l'unicité de la question **I.3.g** montre que $\varphi = \chi_p$. Par suite

$$\forall \alpha = [a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times \quad \varphi(\alpha) = \chi_p(\alpha) = \left(\frac{a}{p}\right).$$

Cela se traduit ainsi :

$\star$ Si $\alpha^{p'} = [1]_p$, i.e. si $a^{p'} \equiv 1\ (p)$, alors $1 = \chi_p(\alpha) = \left(\frac{a}{p}\right)$,

$\star$ Si $\alpha^{p'} = [-1]_p$, i.e. si $a^{p'} \equiv -1\ (p)$, alors $-1 = \chi_p(\alpha) = \left(\frac{a}{p}\right)$.

Dans tous les cas $a^{p'} \equiv \left(\frac{a}{p}\right)\ (p)$.

II.3. On applique la formule **II.2.c.** pour obtenir :

$$\left(\frac{-1}{p}\right) = 1 \Leftrightarrow (-1)^{p'} \equiv 1\ (p) \Leftrightarrow p' \equiv 0\ (2) \Leftrightarrow p \equiv 1\ (4)$$

et

$$\left(\frac{-1}{p}\right) = -1 \Leftrightarrow (-1)^{p'} \equiv -1\ (p) \Leftrightarrow p' \equiv 1\ (2) \Leftrightarrow p \equiv 3\ (4).$$

Partie III

III.1. On a

$$f_0(0) = \sum_{k=0}^{m-1} e^{\frac{i2\pi k^2}{m}} \text{ et } f_0(2\pi) = \sum_{k=0}^{m-1} e^{\frac{i2\pi(k+1)^2}{m}} = \sum_{k=1}^{m} e^{\frac{i2\pi k^2}{m}} = \sum_{k=0}^{m-1} e^{\frac{i2\pi k^2}{m}}$$

puisque $e^{\frac{i2\pi m^2}{m}} = 1$. Par conséquent $f_0(0) = f_0(2\pi)$ et f coïncide avec f_0 sur tout l'intervalle $[0, 2\pi]$. La fonction f_0 est somme de fonctions de classe C^∞ sur $[0, 2\pi]$, donc sera de classe C^∞ sur $[0, 2\pi]$. Par suite f sera de classe C^∞ sur $[0, 2\pi]$, et, étant périodique, sera de classe C^∞ sur chacun des intervalles $[n2\pi, n2\pi + 2\pi]$. Pour montrer que f est continue sur tout $\mathbb{R}$, il suffit de vérifier que f est continue en chacun des points $n2\pi$ (où $n \in \mathbb{Z}$). Comme f est continue sur chacun des intervalles $[n2\pi - 2\pi, n2\pi]$ et $[n2\pi, n2\pi + 2\pi]$, on déduit effectivement

$$\lim_{t \to n2\pi_-} f(t) = f(n2\pi) = \lim_{t \to n2\pi_+} f(t).$$

III.2.a. On a

$$c_n = \frac{1}{2\pi}\int_0^{2\pi} e^{-int} f(t)\, dt = \frac{1}{2\pi}\int_0^{2\pi} e^{-int} \sum_{k=0}^{m-1} e^{i\frac{(t+2\pi k)^2}{2\pi m}}\, dt = \frac{1}{2\pi}\sum_{k=0}^{m-1}\int_0^{2\pi} e^{i\left(-nt + \frac{(t+2\pi k)^2}{2\pi m}\right)}\, dt.$$

Comme $t = 2\pi\left(u - k + \frac{mn}{2}\right)$, on trouve

$$\begin{aligned} -nt + \frac{(t+2\pi k)^2}{2\pi m} &= -n2\pi\left(u - k + \frac{mn}{2}\right) + \frac{2\pi\left(u + \frac{mn}{2}\right)^2}{m} \\ &= -nu2\pi + kn2\pi - \pi mn^2 + \frac{2\pi}{m}\left(u^2 + \frac{m^2n^2}{4} + umn\right) \\ &= \frac{2\pi u^2}{m} + kn2\pi - \frac{\pi mn^2}{2}. \end{aligned}$$

Ainsi

$$\begin{aligned} c_n &= \frac{1}{2\pi}\sum_{k=0}^{m-1}\int_{k-\frac{mn}{2}}^{k+1-\frac{mn}{2}} e^{i\left(\frac{2\pi u^2}{m}+kn2\pi-\frac{\pi mn^2}{2}\right)}\,2\pi du = e^{-i\frac{\pi mn^2}{2}}\sum_{k=0}^{m-1}\int_{k-\frac{mn}{2}}^{k+1-\frac{mn}{2}} e^{i\frac{2\pi u^2}{m}}\,du \\ &= e^{-i\frac{\pi mn^2}{2}}\int_{-\frac{mn}{2}}^{m-\frac{mn}{2}} e^{i\frac{2\pi u^2}{m}}\,du. \end{aligned}$$

III.2.b. Si $n = 2n'$ est pair,

$$e^{-i\frac{\pi mn^2}{2}} = e^{-i2\pi mn'^2} = 1.$$

Si $n = 2n' + 1$ est impair,

$$e^{-i\frac{\pi mn^2}{2}} = e^{-i\frac{\pi}{2}m\left(4n'^2+4n'+1\right)} = e^{-i\frac{\pi}{2}m} = (-i)^m.$$

III.2.c. On a

$$c_{2q} = \int_{-mq}^{m(1-q)} e^{i\frac{2\pi u^2}{m}}\,du = u_{-q}$$

et

$$c_{2q+1} = (-i)^m\int_{m\left(-q-\frac{1}{2}\right)}^{m\left(-q+\frac{1}{2}\right)} e^{i\frac{2\pi u^2}{m}}\,du = (-i)^m\,v_{-q}.$$

III.2.d. Rappelons le **Théorème de Dirichlet** valable pour toute application 2π-périodique f de $\mathbb{R}$ dans $\mathbb{C}$:

1) **Théorème de convergence simple** : Si f est de classe C^1 par morceaux, alors la série de Fourier de f converge en tout point t de $\mathbb{R}$ vers $\frac{f(t+)+f(t-)}{2}$.

2) **Théorème de convergence uniforme :** Si f est continue et C^1 par morceaux, alors la série de Fourier de f converge normalement, et donc uniformément, sur $\mathbb{R}$, vers la fonction f.

On trouvera une preuve de ce Théorème dans le Gostiaux ([1] 15.3 p. 285 et 15.4 p. 289) ou le Ramis ([2], Corollaire I de IV.3.5.4.2 & Théorème du IV.3.5.4.3).

Dans notre problème, la fonction f est continue sur tout $\mathbb{R}$ et de classe C^1 par morceaux. On peut donc affirmer que la série de fonctions $\sum_{n\in\mathbb{Z}} c_n e^{int}$ converge normalement vers f sur $\mathbb{R}$, et cela entraîne la convergence absolue de $\sum_{n\in\mathbb{Z}} c_n e^{int}$ vers $f(t)$ pour tout t fixé. En particulier $f(0) = \sum_{n\in\mathbb{Z}} c_n$. Dans la pratique, cela signifie que la série $\sum_{k\in\mathbb{N}}(c_k + c_{-k})$ est absolument convergente, et donc que toute série dont les termes sont extraits de la série $\sum_{k\in\mathbb{N}}(c_k + c_{-k})$, est absolument convergente. En particulier, les séries $\sum_{q=1}^{+\infty}(c_{2q} + c_{-2q})$ et $\sum_{q=1}^{+\infty}(c_{-2q+1} + c_{2q-1})$ sont absolument convergentes et

$$f(0) = c_0 + \sum_{k=1}^{+\infty}(c_k + c_{-k}) = c_0 + \sum_{q=1}^{+\infty}(c_{2q} + c_{-2q}) + \sum_{q=1}^{+\infty}(c_{-2q+1} + c_{2q-1}).$$

Compte tenu de **III.2.c**, on obtient

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

et les séries qui interviennent sont absolument convergentes.

III.3.a. Montrons que cette intégrale converge. Il y a seulement un problème en 0 et un problème en $+\infty$ puisque la fonction $y \mapsto \frac{e^{i2\pi y}}{\sqrt{y}}$ est définie et de classe C^∞ sur tout $\mathbb{R}_+^*$. Fixons $c \in \mathbb{R}_+^*$. L'intégrale $\int_0^c \frac{e^{i2\pi y}}{\sqrt{y}}\,dy$ est absolument convergente en 0 puisque $\left|\frac{e^{i2\pi y}}{\sqrt{y}}\right| = \frac{1}{\sqrt{y}}$ et puisque

$$\lim_{A\to 0}\int_A^c \frac{1}{\sqrt{y}}\,dy = \lim_{A\to 0}\left[2\sqrt{y}\right]_A^c = 2\sqrt{c}$$

existe. Si $A > 0$, une intégration par partie donne

$$\begin{aligned}\int_c^A e^{i2\pi y}y^{-\frac{1}{2}}\,dy &= \left[\frac{e^{i2\pi y}}{i2\pi}y^{-\frac{1}{2}}\right]_c^A - \int_c^A \frac{e^{i2\pi y}}{i2\pi}\left(-\frac{1}{2}\right)y^{-\frac{3}{2}}\,dy \\ &= \frac{e^{i2\pi A}}{i2\pi}A^{-\frac{1}{2}} - \frac{e^{i2\pi c}}{i2\pi}c^{-\frac{1}{2}} + \frac{1}{i4\pi}\int_c^A \frac{e^{i2\pi y}}{y^{\frac{3}{2}}}\,dy. \qquad (*)\end{aligned}$$

Comme $A \mapsto e^{i2\pi A}$ est bornée et $\lim_{A\to+\infty} A^{-\frac{1}{2}} = 0$ on trouve $\lim_{A\to+\infty}\frac{e^{i2\pi A}}{i2\pi}A^{-\frac{1}{2}} = 0$. L'intégrale $\int_c^{+\infty}\frac{e^{i2\pi y}}{y^{\frac{3}{2}}}\,dy$ est absolument convergente puisque $\int_c^{+\infty}\frac{1}{y^{\frac{3}{2}}}\,dy$ converge. La formule $(*)$ montre maintenant que la limite

$$\lim_{A\to+\infty}\int_c^A e^{i2\pi y}y^{-\frac{1}{2}}\,dy$$

existe, autrement dit que l'intégrale généralisée $\int_c^{+\infty} e^{i2\pi y}y^{-\frac{1}{2}}\,dy$ converge. En conclusion, les convergences des intégrales $\int_0^c \frac{e^{i2\pi y}}{\sqrt{y}}\,dy$ et $\int_c^{+\infty}\frac{e^{i2\pi y}}{\sqrt{y}}\,dy$ prouvent celle de $\int_0^{+\infty}\frac{e^{i2\pi y}}{\sqrt{y}}\,dy$.

III.3.b. La fonction $x \mapsto e^{i2\pi x^2}$ est paire, donc il suffit de montrer que $\int_0^{+\infty} e^{i2\pi x^2}\,dx$ converge. Soit $c \in \mathbb{R}_+^*$ fixé et $A > c$. Par le changement de variable $t = x^2$, on trouve

$$\int_c^A e^{i2\pi x^2}\,dx = \int_{c^2}^{A^2} e^{i2\pi t}\frac{1}{2\sqrt{t}}\,dt = \frac{1}{2}\int_{c^2}^{A^2}\frac{e^{i2\pi t}}{\sqrt{t}}\,dt$$

et la question précédente montre que $\int_{c^2}^{A^2}\frac{e^{i2\pi t}}{\sqrt{t}}\,dt$ tend vers une limite quand A tend vers $+\infty$. Il en sera donc de même de $\int_c^A e^{i2\pi x^2}\,dx$.

III.3.c. On a

$$\begin{aligned}u_0 + \sum_{q=1}^{+\infty}(u_q + u_{-q}) &= u_0 + \sum_{q=1}^{+\infty}\int_{mq}^{m(q+1)} e^{i\frac{2\pi u^2}{m}}\,du + \sum_{q=1}^{+\infty}\int_{-mq}^{m(-q+1)} e^{i\frac{2\pi u^2}{m}}\,du \\ &= \int_0^m e^{i\frac{2\pi u^2}{m}}\,du + \int_m^{+\infty} e^{i\frac{2\pi u^2}{m}}\,du + \int_{-\infty}^0 e^{i\frac{2\pi u^2}{m}}\,du = \int_{-\infty}^{+\infty} e^{i\frac{2\pi u^2}{m}}\,du \\ &= \sqrt{m}\int_{-\infty}^{+\infty} e^{i2\pi v^2}\,dv = J\sqrt{m} \text{ par le changement de variable } v = \frac{u}{\sqrt{m}}.\end{aligned}$$

On montrerait de même que $\sum_{q=1}^{+\infty}(v_q + v_{1-q}) = J\sqrt{m}$. En remplaçant dans la formule du **III.2.d**, on obtient bien $f(0) = J\left(1 + e^{-i\frac{\pi m}{2}}\right)\sqrt{m}$.

III.3.d. Pour $m=1$, $f(0)=J\left(1+e^{-i\frac{\pi}{2}}\right)=J(1-i)$. Ici $f(0)=1$ donc $J=\frac{1}{1-i}$.

III.3.e. En remplaçant dans (1),

$$f(0)=\frac{(1+e^{-i\frac{\pi m}{2}})\sqrt{m}}{1-i}=\sum_{k=0}^{m-1}e^{\frac{i2\pi k^2}{m}}=G(m),$$

d'où

$$G(m)=\frac{(1+(-i)^n)\sqrt{m}}{1-i}.$$

Partie IV

IV.1.a. Il faut vérifier que l'image $e^{i\frac{2\pi k}{m}}$ de la classe $[k]_m$ est indépendante du choix du représentant k de la classe. Si $[k]_m=[k']_m$, alors m divise $k-k'$ et l'on a bien

$$e^{i\frac{2\pi k}{m}}=e^{i\frac{2\pi(k-k')}{m}}e^{i\frac{2\pi k'}{m}}=e^{i\frac{2\pi k'}{m}}.$$

IV.1.b. On applique $(P1)$ et l'on reconnaît la somme d'une progression géométrique de raison $e^{i\frac{2k}{m}}$:

$$\sum_{x\in\mathbb{Z}/m\mathbb{Z}}\varepsilon_m(x)=\sum_{k=0}^{m-1}e^{i\frac{2\pi k}{m}}=\frac{1-\left(e^{i\frac{2\pi}{m}}\right)^m}{1-e^{i\frac{2k}{m}}}=0.$$

IV.2.a. Si $k-h=2mu$, alors $k^2=h^2+4m^2u^2+4muh$ et

$$e^{i2\pi\frac{k^2}{4m}}=e^{i2\pi\frac{h^2}{4m}}e^{i2\pi\left(mu^2+uh\right)}=e^{i2\pi\frac{h^2}{4m}}.$$

IV.2.b. La question précédente permet d'écrire

$$\sum_{k=0}^{2m-1}e^{i2\pi\frac{k^2}{4m}}=\sum_{k=0}^{2m-1}e^{i2\pi\frac{(k+2m)^2}{4m}}=\sum_{k'=2m}^{4m-1}e^{i2\pi\frac{k'^2}{4m}}$$

d'où

$$2H(2m)=2\sum_{k=0}^{2m-1}e^{i2\pi\frac{k^2}{4m}}=\sum_{k=0}^{2m-1}e^{i2\pi\frac{k^2}{4m}}+\sum_{k=2m}^{4m-1}e^{i2\pi\frac{k^2}{4m}}=\sum_{k=0}^{4m-1}e^{i2\pi\frac{k^2}{4m}}=G(4m).$$

IV.2.c. Appliquons **IV.2.b.** avec $2m$ à la place de m, et utilisons l'expression de $G(m)$ obtenue en **III.3.e**. On obtient

$$2H(4m)=G(8m)=\frac{\left(1+e^{-i4\pi m}\right)\sqrt{8m}}{1-i}=\frac{4\sqrt{2}}{1-i}\sqrt{m}=2(1+i)\sqrt{2}\sqrt{m}$$

soit $H(4m)=(1+i)\sqrt{2}\sqrt{m}=2\left(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right)\sqrt{m}=2\omega\sqrt{m}$.

IV.3.a.

$$\begin{array}{rccc}\overline{k}: & E & \to & \mathbb{Z}/4pq\mathbb{Z}\\ & (l,r,s) & & [lpq+4rq+4sp]_{4pq}\end{array}$$

Comme E et $\mathbb{Z}/4pq\mathbb{Z}$ ont même cardinal, l'application $\overline{k}$ sera bijective si et seulement si elle est injective. Supposons donc que (l,r,s) et (l',r',s') soient deux éléments de E tels que

$$lpq+4rq+4sp=l'pq+4r'q+4s'p.$$

On aura $(lp+4r-l'p-4r')\,q=4\,(s'-s)\,p$. Comme p est premier avec q et divise le premier membre, le Théorème de Gauss montre que p divise $lp+4r-l'p-4r'$, et donc p divisera $4\,(r-r')$. Le Théorème de Gauss montre encore que p divise $r-r'$. Comme $1\leq|r-r'|\leq p-1$, on aura nécessairement $r=r'$, et donc

$$lpq+4sp=l'pq+4s'p.$$

On tire maintenant $(lp-l'p)\,q=4\,(s'-s)\,p$, d'où $(l-l')\,q=4\,(s'-s)$. Comme q est premier avec 4, le Théorème de Gauss montre que q divise $s'-s$ et les inégalités $1\leq|s-s'|\leq q-1$ entraînent $s=s'$. En remplaçant, il vient $lpq=l'pq$ d'où $l=l'$. L'application $\overline{k}$ est bien injective, donc bijective.

IV.3.b.

$$\begin{aligned}H\,(4pq) &= \sum_{k=0}^{4pq-1}e^{i2\pi\frac{k^2}{8pq}}=\sum_{[k]_{pq}\in\mathbb{Z}/4pq\mathbb{Z}}e^{i2\pi\frac{k^2}{8pq}}=\sum_{(l,r,s)\in E}e^{i2\pi\frac{[k(l,r,s)]^2}{8pq}}\\ &= \sum_{(l,r,s)\in E}e^{i2\pi\frac{(lpq+4rq+4sp)^2}{8pq}}=\sum_{(l,r,s)\in E}e^{i2\pi\frac{(lpq+4rq+4sp)^2}{8pq}}.\end{aligned}$$

On a

$$\frac{1}{8pq}\,(lpq+4rq+4sp)^2=\frac{1}{8pq}\left(l^2p^2q^2+16r^2q^2+16s^2p^2+8lpq^2r+8lp^2qs+16rspq\right)$$

donc

$$e^{i2\pi\frac{(lpq+4rq+4sp)^2}{8pq}}=e^{i2\pi\frac{1}{8pq}\left(l^2p^2q^2+16r^2q^2+16s^2p^2\right)}=e^{i2\pi\frac{pql^2}{8}}\times e^{i4\pi\frac{qr^2}{p}}\times e^{i4\pi\frac{ps^2}{q}}.$$

Par suite

$$H\,(4pq)=\sum_{(l,r,s)\in E}e^{i2\pi\frac{pql^2}{8}}\times e^{i4\pi\frac{qr^2}{p}}\times e^{i4\pi\frac{ps^2}{q}}=\left(\sum_{l=0}^{3}e^{i2\pi\frac{pql^2}{8}}\right)\left(\sum_{r=0}^{p-1}e^{i4\pi\frac{qr^2}{p}}\right)\left(\sum_{s=0}^{q-1}e^{i4\pi\frac{ps^2}{q}}\right).$$

IV.4.a. Comme $\omega=e^{i\frac{2\pi}{8}}$ est une racine primitive 8-ième de l'unité, on a $\omega^8=1$ et $\omega^4=-1$, donc

$$\begin{aligned}\sum_{l=0}^{3}e^{i2\pi\frac{pql^2}{8}} &= 1+e^{i2\pi\frac{pq}{8}}+e^{i2\pi\frac{4pq}{8}}+e^{i2\pi\frac{9pq}{8}}=1+\omega^{pq}+\omega^{4pq}+\omega^{9pq}\\ &= 1+\omega^{pq}+(-1)^{pq}+\omega^{pq}=2\omega^{pq}.\end{aligned}$$

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

IV.4.c. On a $L\,(1,p)=\sum_{r=0}^{0}e^{i4\pi pr^2}=1$. La formule du **IV.4.b** s'écrit ici

$$H\,(4p)=2\omega^{p}L\,(1,p)\,L\,(p,1)\,,$$

et comme $H(4m) = 2\omega\sqrt{m}$ d'après **IV.2.c**, on obtient

$$2\omega\sqrt{p} = 2\omega^p L(p,1)$$

d'où $L(p,1) = \omega^{1-p}\sqrt{p}$.

IV.5.a. L'élément $[2]_p$ est inversible, donc l'application $x \mapsto [2]_p x$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$, et l'on peut écrire

$$1 + \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} \varepsilon_p\left([2]_p x\right) = 1 + \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} \varepsilon_p(x) = \sum_{x\in\mathbb{Z}/p\mathbb{Z}} \varepsilon_p(x) = 0$$

d'après **IV.1**.

IV.5.b.

$$\begin{aligned} L(p,q) &= \sum_{r=0}^{p-1} e^{i4\pi\frac{qr^2}{p}} = 1 + \sum_{[r]_p\in(\mathbb{Z}/p\mathbb{Z})^\times} e^{i4\pi\frac{qr^2}{p}} = 1 + \sum_{[r]_p\in(\mathbb{Z}/p\mathbb{Z})^\times} \varepsilon_p\left([2q]_p [r]_p^2\right) \\ &= 1 + \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} \varepsilon_p\left([2q]_p \sigma(x)\right). \end{aligned}$$

Si $y \in S$, alors $\sigma^{-1}(y)$ est toujours une paire d'après la partie I. On peut appliquer $(P2)$ pour obtenir

$$L(p,q) = 1 + 2\sum_{y\in S} \varepsilon_p\left([2q]_p y\right).$$

IV.5.c. Si $[q]_p \in S$, $[q]_p$ est un carré et l'application $y \mapsto [q]_p y$ est une bijection de S dans S. Par conséquent

$$L(p,q) = 1 + 2\sum_{y\in S} \varepsilon_p\left([2]_p [q]_p y\right) = 1 + 2\sum_{x\in S} \varepsilon_p\left([2]_p x\right).$$

La même formule peut être appliquée pour calculer $L(p,1)$ puisque $[1]_q \in S$. On en déduit $L(p,q) = L(p,1)$.

IV.5.d. Si $[q]_p \in T$, l'application $y \mapsto [q]_p y$ est une bijection de S dans T (**I.3.e**) donc

$$L(p,q) = 1 + 2\sum_{y\in S} \varepsilon_p\left([2]_p [q]_p y\right) = 1 + 2\sum_{x\in T} \varepsilon_p\left([2]_p x\right).$$

On a alors

$$\begin{aligned} L(p,q) + L(p,1) &= \left(1 + 2\sum_{x\in T} \varepsilon_p\left([2]_p x\right)\right) + \left(1 + 2\sum_{x\in S} \varepsilon_p\left([2]_p x\right)\right) \\ &= 2\left(1 + \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^\times} \varepsilon_p\left([2]_p x\right)\right) = 2\left(\sum_{x\in(\mathbb{Z}/p\mathbb{Z})} \varepsilon_p(x)\right) = 0. \end{aligned}$$

IV.6. D'après **IV.4.b** et **IV.2.c**

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

Comme l'on vient de voir que $L(p,q) = \left(\frac{q}{p}\right) L(p,1)$ et comme $L(p,1) = \omega^{1-p}\sqrt{p}$ d'après **IV.4.c**, on obtient

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

soit

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \omega^{p+q-pq-1} = \omega^{2p'+1+2q'+1-(2p'+1)(2q'+1)-1} = \omega^{-4p'q'} = (-1)^{p'q'}\,.$$

That's All Folks !

References

[1] B. Gostiaux, Cours de mathématiques Spéciales, tome 3 : Analyse fonctionnel et calcul différentiel, PUF, 1993.

[2] E. Ramis, C. Deschamps, J. Odoux, Cours de Mathématiques Spéciales, Volume **4**, Séries et Equations Différentielles, Masson, 1989.