

Agrégation interne

Corrigé de la première épreuve de l'agreg' interne 2000

Merci d'avance de me signaler toutes les erreurs (petites ou grosses) qui auraient pu échapper à ma vigilance...

PARTIE I

Question 1

Pour $a \in \mathbb{Z}$, on a l'équivalence des assertions suivantes :

- (i) $[a]_m$ est inversible dans $\mathbb{Z}/m\mathbb{Z}$.
- (ii) Il existe $b \in \mathbb{Z}$ tel que $[a]_m \cdot [b]_m = [1]_m$.
- (iii) Il existe $b \in \mathbb{Z}$ tel que $[ab-1]_m = [0]_m$.
- (iv) Il existe $b \in \mathbb{Z}$ et $k \in \mathbb{Z}$ tels que $ab-1=km$.
- (v) a est premier avec m . (Bezout)

Ce qui établit donc bien le résultat.

Question 2-a

Sachant que $(\mathbb{Z}/m\mathbb{Z})^\times$ est un groupe commutatif pour le produit, on a, pour $\alpha, \beta \in (\mathbb{Z}/m\mathbb{Z})^\times$:

- (i) $\alpha^2 \in (\mathbb{Z}/m\mathbb{Z})^\times$ (car le produit est une loi de composition interne dans $(\mathbb{Z}/m\mathbb{Z})^\times$, et donc σ est bien à valeurs dans $(\mathbb{Z}/m\mathbb{Z})^\times$).
- (ii) $\sigma(\alpha\beta) = (\alpha\beta)^2 = \alpha^2\beta^2 = \sigma(\alpha)\sigma(\beta)$

Donc σ est bien un morphisme de groupes de $(\mathbb{Z}/m\mathbb{Z})^\times$ dans lui même, et donc son image S est un sous groupe de $(\mathbb{Z}/m\mathbb{Z})^\times$.

Question 2-b

Pour $m=5$:

On sait que $\mathbb{Z}/5\mathbb{Z} = \{[k]_5, k \in \{0,1,2,3,4\}\}$. La première question nous indique alors :

$$(\mathbb{Z}/5\mathbb{Z})^\times = \{[k]_{15}, k \in \{1,2,3,4\}\}.$$

Par ailleurs, en regardant les carrés de ces quatre éléments, on a :

$$([1]_5)^2 = [1^2]_5 = [1]_5 ; [2^2]_5 = [4]_5 ; [3^2]_5 = [9]_5 = [4]_5 ; [4^2]_5 = [16]_5 = [1]_5.$$

$$\text{Donc : } S = \{[1]_5, [4]_5\}.$$

Pour $m=15$:

En reprenant les mêmes raisonnements, on trouve :

$$(\mathbb{Z}/15\mathbb{Z})^\times = \{[k]_{15}, k \in \{1,2,4,7,8,11,13,14\}\}.$$

$$[1^2]_{15} = [1]_{15} ; [2^2]_{15} = [4]_{15} ; [4^2]_{15} = [16]_{15} = [1]_{15} ; [7^2]_{15} = [49]_{15} = [4]_{15} ; [8^2]_{15} = [64]_{15} = [4]_{15} ;$$

$$[11^2]_{15} = [121]_{15} = [1]_{15} ; [13^2]_{15} = [169]_{15} = [4]_{15} ; [14^2]_{15} = [196]_{15} = [1]_{15}.$$

$$\text{Donc : } S = \{[1]_{15}, [4]_{15}\}.$$

Question 3-a

On rappelle que $(\mathbb{Z}/p\mathbb{Z}) = \{[k]_p, k \in \{0,1,\dots, p-1\}\}$.

Donc $(\mathbb{Z}/p\mathbb{Z})^\times = \{[k]_p, k \in \{0,1,\dots, p-1\} \text{ et } k \text{ premier avec } p\}$.

Or, 0 n'est pas premier avec p , et pour $1 \leq k \leq p$, k est premier avec p , car p n'a pas de diviseur entre 1 et $p-1$. Donc $(\mathbb{Z}/p\mathbb{Z})^\times = \{[k]_p, k \in \{1,\dots, p-1\}\}$, et $\text{card}((\mathbb{Z}/p\mathbb{Z})^\times) = p-1$.

Question 3-b

$[1]_p - [-1]_p = [2]_p$ et 2 n'est pas un multiple de p , car $p \geq 3$. Donc $[1]_p \neq [-1]_p$.

Question 3-c

On a : $K = \{\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times, \text{ tel que } \alpha^2 = [1]_p\}$. Donc pour $\alpha \in K$, avec $\alpha = [a]_p$, on a :

a^2-1 est un multiple de p . Donc p divise $(a-1)(a+1)$. Sachant que p est premier, on a :
 soit p divise $a-1$, soit p divise $a+1$, ce que signifie donc :
 soit $[a]_p = [1]_p$, soit $[a]_p = [-1]_p$. Réciproquement, il est clair que ces deux éléments sont dans K .
 Donc $K = \{[1]_p, [-1]_p\}$.

Question 3-d

σ étant un morphisme de groupes de noyau K et d'image S , on a donc

Le quotient $(\mathbb{Z}/p\mathbb{Z})^\times$ par K est un groupe isomorphe à S . Donc $\text{card}(S)$ est égal au cardinal du groupe quotient $(\mathbb{Z}/p\mathbb{Z})^\times / K$, à savoir : $\text{card}((\mathbb{Z}/p\mathbb{Z})^\times) / \text{card}(K) = (p-1)/2 = p'$. On a donc bien :

$$\text{card}(S) = p'$$

Proposons maintenant une preuve directe :

Soit $\alpha \in S$. Ainsi α peut s'écrire $\alpha = \sigma(\beta)$. Déterminons alors les autres antécédents de α :

$\alpha = \sigma(\gamma)$ équivaut alors à $\sigma(\gamma) = \sigma(\beta)$, ce qui signifie donc, sachant que σ est un morphisme de groupes : $\sigma(\gamma\beta^{-1}) = 1$, ou, en d'autres termes, $\gamma\beta^{-1} \in K$. Compte tenu de $K = \{[1]_p, [-1]_p\}$, ceci équivaut donc à : $\gamma = \beta$ ou $\gamma = -\beta$, et ces deux valeurs sont distinctes vu que $[1]_p \neq [-1]_p$.

Donc chaque élément de S a exactement 2 antécédents, et donc d'après le lemme des bergers, $2\text{card}(S) = \text{card}((\mathbb{Z}/p\mathbb{Z})^\times) = p-1 = 2p'$. On retrouve donc le résultat.

Question 2-e

On a donc : $\text{card}(S) + \text{card}(T) = \text{card}((\mathbb{Z}/p\mathbb{Z})^\times)$. Donc $\text{card}(T) = p'$.

Regardons, pour $\theta \in T$, l'ensemble $\theta S = \{\theta s, s \in S\}$.

L'application f définie sur $(\mathbb{Z}/p\mathbb{Z})^\times$ par $f(\alpha) = \theta\alpha$ est une translation, et est bijective. Donc, en remarquant que $\theta S = f(S)$, on en déduit que $\text{card}(\theta S) = \text{card}(S) = p' = \text{card}(T)$.

Or, soit $\alpha = \theta s$ un élément quelconque de θS . Alors $\alpha \notin S$, car sinon, sachant que S est un sous groupe, $\alpha s^{-1} = \theta$ appartiendrait à S , ce qui est en contradiction avec $\alpha \in T$. Donc θS est inclus dans T et a même cardinal. D'où $\theta S = T$.

Question 2-f

On remarque d'abord que χ_p est bien surjectif, à valeurs dans $\{-1, 1\}$, vu que ni S , ni T ne sont vides (ils ont pour cardinal $p' \geq 1$).

Soit alors $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^\times$. Compte tenu de la commutativité du produit et quitte à échanger α et β , trois cas peuvent se produire : soit ils appartiennent tous deux à S , soit ils appartiennent tous deux à T , soit $\alpha \in S$ et $\beta \in T$. Etudions les un à un :

Si $\alpha, \beta \in S$:

Alors $\alpha\beta \in S$ (S est un sous groupe), et $\chi_p(\alpha\beta) = 1 = \chi_p(\alpha)\chi_p(\beta)$.

Si $\alpha \in S$ et $\beta \in T$:

Alors $\alpha\beta \notin S$ (même raisonnement qu'en 2-e), et $\chi_p(\alpha\beta) = -1 = \chi_p(\alpha)\chi_p(\beta)$.

Si $\alpha \in T$ et $\beta \in T$:

Sachant qu'alors $T = \alpha S$ (cf 2-e), β peut donc s'écrire :

$\beta = \alpha s$ avec $s \in S$. Donc $\alpha\beta = \alpha^2 s$; or par définition de S , $\alpha^2 \in S$, et donc $\alpha^2 s \in S$, c-à-d $\alpha\beta \in S$.

Donc $\chi_p(\alpha\beta) = 1 = \chi_p(\alpha)\chi_p(\beta)$.

On a donc bien établi que pour tout $\alpha, \beta \in S$, on a : $\chi_p(\alpha\beta) = \chi_p(\alpha)\chi_p(\beta)$, et donc :

χ_p est bien un morphisme surjectif de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\{-1, 1\}$.

Question 3-g

Soit f un morphisme de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\{-1, 1\}$:

Soit alors $\alpha \in S$. Il existe donc $\beta \in S$ tel que $\alpha = \beta^2$. De ce fait :

$f(\alpha) = f(\beta^2) = (f(\beta))^2 = (\pm 1)^2 = 1$. Donc $f(\alpha) = \chi_p(\alpha)$ pour $\alpha \in S$.

Par ailleurs, sachant que f est surjective, il existe $\theta \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $f(\theta) = -1$. Remarquons de suite que θ ne saurait donc appartenir à S . Ainsi $T = \theta S$, et donc, si α est un élément de T , α s'écrit alors $\alpha = \theta s$ avec $s \in S$. Ainsi $f(\alpha) = f(\theta)f(s) = (-1) \cdot 1 = -1 = \chi_p(\alpha)$.

Donc, dans tous les cas, on a $f(\alpha) = \chi_p(\alpha)$ et donc $f = \chi_p$.
 χ_p est donc bien le seul morphisme surjectif de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\{-1, 1\}$.

Question 4

On a donc ainsi : $\left(\frac{a}{11}\right) = 1$ si, et seulement si a est un carré modulo 11.

Il reste donc à regarder les restes modulo 11 des carrés des entiers entre 1 et 10 :

$$[1^2]_{11} = [1]_{11}; [2^2]_{11} = [4]_{11}; [3^2]_{11} = [9]_{11}; [4^2]_{11} = [5]_{11}; [5^2]_{11} = [3]_{11}.$$

Il est en fait inutile de continuer car on a trouvé 5 valeurs distinctes et donc 5 éléments de S , avec $\text{card}(S) = 5$. Donc $S = \{[k]_{11}, k \in \{1, 4, 9, 5, 3\}\}$. Ainsi :

Pour $a \in \{1, 3, 4, 5, 9\}$, on a $\left(\frac{a}{11}\right) = 1$, et pour $a \in \{2, 6, 7, 8, 10\}$, on a : $\left(\frac{a}{11}\right) = -1$.

PARTIE II

Question 1

Soit $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$. Alors $\alpha^{2p'} = \alpha^{p-1}$. Or $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe d'ordre $p-1$ d'après le I-3-a, et donc l'ordre de α dans $(\mathbb{Z}/p\mathbb{Z})^\times$ divise $p-1$ (théorème de Lagrange), ce qui entraîne $\alpha^{p-1} = [1]_p$.

Ainsi $\alpha^{2p'} = [1]_p$, et donc $\alpha^{p'}$ vérifie l'équation $x^2 = [1]_p$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

Cette équation équivaut à $(x - [1]_p)(x + [1]_p) = [0]_p$, et, sachant que $(\mathbb{Z}/p\mathbb{Z})$ est un anneau intègre (c'est même un corps), elle équivaut à $x = \pm[1]_p$. Donc $\alpha^{p'} = \pm[1]_p$.

Question 2-a

Remarquons d'abord que, pour $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a : $\alpha^{p'} = [\varphi(\alpha)]_p$. Ainsi :

Soit $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^\times$. On a alors :

$$[\varphi(\alpha\beta)]_p = [(\alpha\beta)^{p'}]_p = [\alpha^{p'}]_p \cdot [\beta^{p'}]_p = [\varphi(\alpha)]_p \cdot [\varphi(\beta)]_p = [\varphi(\alpha)\varphi(\beta)]_p$$

Donc $[\varphi(\alpha\beta) - \varphi(\alpha)\varphi(\beta)]_p = [0]_p$, et donc $\varphi(\alpha\beta) - \varphi(\alpha)\varphi(\beta)$ est un multiple de p . Or, comme φ est à valeurs dans $\{-1, 1\}$, $\varphi(\alpha\beta) - \varphi(\alpha)\varphi(\beta) \in \{-2, 0, 2\}$. Comme $p \geq 3$, on a donc $\varphi(\alpha\beta) - \varphi(\alpha)\varphi(\beta)$ ne peut qu'être nul, ce qui nous donne $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$:

φ est bien un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\{-1, 1\}$.

Question 2-b

D'une part, on a $\varphi([1]_p) = 1$, et donc 1 a un antécédent par φ .

D'autre part, le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ étant cyclique, d'ordre $p-1 = 2p'$, il est donc isomorphe au groupe additif $\mathbb{Z}/(2p'\mathbb{Z})$. Ainsi l'existence d'un $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$ vérifiant $\alpha^{p'} = [-1]_p$ équivaut à l'existence d'un $\beta \in \mathbb{Z}/(2p'\mathbb{Z})$ vérifiant $p'\beta \neq [0]$ (on rappelle qu'il n'y a que 2 valeurs possibles pour $\alpha^{p'} = [-1]_p$), ce qui est le cas pour $\beta = [1]_{2p'}$.

Question 2-c

φ étant un morphisme surjectif de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans $\{-1, 1\}$, il est alors égal à χ_p (cf question I-3-g). Donc, si a est premier à p , on a :

$$[a^{p'}]_p = [1]_p \Leftrightarrow \chi_p([a]_p) = 1 \Leftrightarrow \left(\frac{a}{p}\right) = 1$$

Et de même :

$$[a^{p'}]_p = [-1]_p \Leftrightarrow \left(\frac{a}{p}\right) = -1$$

Ainsi, on a :

$$[a^{p'}]_p = \left[\left(\frac{a}{p} \right) \right]_p$$

Et finalement : $a^{p'} \equiv \left(\frac{a}{p} \right) \pmod{p}$

Question 3

On a donc : $\left(\frac{-1}{p} \right) \equiv (-1)^{p'} \pmod{p}$, et donc sachant que $\left(\frac{-1}{p} \right)$ vaut 1 ou -1 , il reste juste :

$\left(\frac{-1}{p} \right) = (-1)^{p'}$. Ainsi, si p est congru à 1 modulo 4, alors p' est un multiple de 2 et donc

$\left(\frac{-1}{p} \right) = 1$. Par contre, si p est congru à 3 modulo 4, alors $2p'$ est congru à 2 modulo 4, et donc

p' est lui congru à 1 modulo 2 : p' est impair et $\left(\frac{-1}{p} \right) = -1$. Comme p est impair, ce sont les deux seuls cas possibles, et le résultat s'en suit.

PARTIE III

Question 1

On regarde : $f_0(2\pi) = \sum_{k=0}^{m-1} \exp\left(i \frac{(2\pi + 2\pi k)^2}{2\pi m}\right) = \sum_{k=0}^{m-1} \exp\left(i \frac{2\pi(1+k)^2}{m}\right) = \sum_{k=1}^m \exp\left(i \frac{2\pi k^2}{m}\right)$

Or, en remarquant que pour $k=m$, on a : $\exp\left(i \frac{2\pi k^2}{m}\right) = \exp(2im\pi) = 1 = \exp(0)$.

Donc $\sum_{k=1}^m \exp\left(i \frac{2\pi k^2}{m}\right) = \sum_{k=0}^{m-1} \exp\left(i \frac{2\pi k^2}{m}\right) = f_0(0)$: on a bien prouvé : $f_0(2\pi) = f_0(0)$.

Par ailleurs, f_0 est clairement de classe C^∞ sur $[0, 2\pi]$, comme somme (finie) de fonctions de classe C^∞ sur $[0, 2\pi]$. Or, $f(2\pi) = f_0(0)$ par définition de f (périodicité), et $f_0(0) = f_0(2\pi)$. Donc en fait, f et f_0 coïncident sur $[0, 2\pi]$, et donc, f est de ce fait C^∞ sur $[0, 2\pi]$. Or, f étant 2π périodique, on en déduit que f est C^∞ sur $[2n\pi, 2(n+1)\pi]$ (pour tout n entier).

En particulier, f est donc continue sur au moins $\mathbb{R} \setminus (2\pi\mathbb{Z})$. Or f est par ailleurs continue à droite en 0, et à gauche en 2π , donc à gauche en 0. f est donc continue en 0, et donc, par périodicité, f est continue en chaque point de $2\pi\mathbb{Z}$. Finalement, f est continue sur $\mathbb{R}$.

Question 2-a

On calcule, à l'aide du changement de variable proposé :

$$\begin{aligned}
c_n &= \frac{1}{2\pi} \int_0^{2\pi} e^{-nit} f(t) dt = \sum_{k=0}^{m-1} \frac{1}{2\pi} \int_0^{2\pi} \exp\left(-nit + i \frac{(t + 2k\pi)^2}{2\pi m}\right) dt \\
&= \sum_{k=0}^{m-1} \frac{1}{2\pi} \int_{k-\frac{mn}{2}}^{k+1-\frac{mn}{2}} \exp\left(-ni2\pi\left(u - k + \frac{mn}{2}\right) + i \frac{\left(2\pi\left(u + \frac{mn}{2}\right)\right)^2}{2\pi m}\right) du \\
&= \sum_{k=0}^{m-1} \frac{1}{2\pi} \int_{k-\frac{mn}{2}}^{k+1-\frac{mn}{2}} \exp\left(-ni2\pi\left(u + \frac{mn}{2}\right) + i \frac{\left(2\pi\left(u + \frac{mn}{2}\right)\right)^2}{2\pi m}\right) du \\
&= \int_{-\frac{mn}{2}}^{\frac{mn}{2}} \exp\left(-i\pi mn^2 - 2ni\pi u + i \frac{2\pi}{m}\left(u^2 + mn u + \frac{m^2 n^2}{4}\right)\right) du \\
&= e^{-i\pi \frac{mn^2}{2}} \int_{-\frac{mn}{2}}^{\frac{mn}{2}} \exp\left(2i\pi\left(-nu + \frac{u^2}{m} + nu\right)\right) du
\end{aligned}$$

Finalement, on obtient bien :

$$c_n = e^{-i\pi \frac{mn^2}{2}} \int_{-\frac{mn}{2}}^{\frac{mn}{2}} e^{\frac{2i\pi u^2}{m}} du$$

Question 2-b

Si n est pair : alors n^2 est un multiple de 4 et $n^2/2$ est un entier pair et $\exp(-i\pi mn^2/2)=1$.

Si n est impair, avec $n=2k+1$: alors $n^2=4(k^2+k)+1$, et donc :

$$\exp(-i\pi mn^2/2)=\exp(-i\pi m/2)=(-i)^m.$$

Question 2-c

On a :

$$c_{2q} = \int_{-mq}^{m-mq} \exp\left(\frac{2i\pi u^2}{m}\right) du = u_{-q}$$

et :

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

Question 2-d

On remarque d'abord que f est continue, 2π -périodique et C^1 par morceaux sur $\mathbb{R}$. Donc la série de Fourier de f converge normalement vers f sur $\mathbb{R}$; en d'autres termes, la série de fonctions (de la variable t) $\sum_{n \in \mathbb{Z}} c_n(f) e^{nit}$ converge normalement vers f . Or, la norme infinie sur

$\mathbb{R}$ de $c_n(f) e^{int}$ est $|c_n(f)|$. Donc la série $\sum_{n \geq 1} |c_n(f)| + |c_{-n}(f)|$ converge.

Comme il s'agit d'une série à termes positifs, il s'en suit que les deux séries :

$\sum_{n \geq 1} |c_{2n}(f)| + |c_{-2n}(f)|$ et $\sum_{n \geq 1} |c_{2n+1}(f)| + |c_{-2n-1}(f)|$ convergent. Donc, compte tenu du 2-c, les

deux séries proposées convergent absolument.

De plus, on a (la convergence normale entraînant la convergence simple absolue, donc la convergence absolue en 0) :

$$f(0) = \sum_{n=-\infty}^{+\infty} c_n$$

et cette série est absolument convergente. On peut donc regrouper les termes :

$$f(0) = c_0 + \sum_{n=1}^{\infty} (c_{2n} + c_{-2n}) + \sum_{n=0}^{\infty} (c_{2n+1} + c_{-2n-1})$$

Soit encore :

$$f(0) = c_0 + \sum_{n=1}^{\infty} (u_n + u_{-n}) + e^{-i\pi m/2} \sum_{n=0}^{\infty} (v_{-n} + v_{n+1})$$

On fait le changement d'indice $q=n+1$ dans la deuxième série et on obtient :

$$f(0) = c_0 + \sum_{n=1}^{\infty} (u_n + u_{-n}) + e^{-i\pi m/2} \sum_{q=1}^{\infty} (v_{1-q} + v_q)$$

Question 3-a

Pour $X > 0$, on fait une intégration par parties :

$$\int_1^X \frac{e^{2i\pi y}}{\sqrt{y}} dy = \left[\frac{1}{2i\pi} \frac{e^{2i\pi y}}{\sqrt{y}} \right]_1^X - \frac{1}{2i\pi} \int_1^X \left(\frac{-1}{2} \right) \frac{e^{2i\pi y}}{y^{\frac{3}{2}}} dy$$

Or, l'intégrale impropre $\int_1^{+\infty} \frac{e^{2i\pi y}}{y^{\frac{3}{2}}} dy$ est clairement absolument convergente, et la partie entre

crochets a une limite finie quand X tend vers l'infini. D'où la convergence de $\int_1^{+\infty} \frac{e^{2i\pi y}}{\sqrt{y}} dy$.

Par ailleurs, on a, au voisinage de 0, l'équivalent : $\left| \frac{e^{2i\pi y}}{\sqrt{y}} \right|_{y \rightarrow 0^+} \sim \frac{1}{\sqrt{y}}$, et $\int_0^1 \frac{dy}{\sqrt{y}}$ est convergente.

On vient donc d'établir l'absolue convergence de $\int_0^1 \frac{e^{2i\pi y}}{\sqrt{y}} dy$, et par suite $\int_0^{+\infty} \frac{e^{2i\pi y}}{\sqrt{y}} dy$ est bien convergente.

Question 3-b

Pour $X > 0$, on fait le changement de variable $y=x^2$, qui constitue un C^1 -difféomorphisme de $\mathbb{R}^{*+}$ dans lui même. On a donc l'égalité suivante entre intégrales convergentes :

$$\int_0^{\infty} \frac{e^{2i\pi y}}{\sqrt{y}} dy = \int_0^{\infty} 2e^{2i\pi x^2} dx,$$

ce qui prouve au passage la convergence de l'intégrale de droite, et par parité, de $\int_{-\infty}^{\infty} e^{2i\pi x^2} dx$.

Question 3-c

On reprend la formule du 4-d :

$$f(0) = \int_0^m e^{2i\pi u^2/m} du + \sum_{q=1}^{\infty} \left(\int_{mq}^{m(q+1)} e^{2i\pi u^2/m} du + \int_{-mq}^{m(1-q)} e^{2i\pi u^2/m} du \right) \\ + e^{-i\pi m/2} \sum_{q=1}^{\infty} \left(\int_{m(q-1/2)}^{m(q+1/2)} e^{2i\pi u^2/m} du + \int_{m(-q+1/2)}^{m(-q-1/2)} e^{2i\pi u^2/m} du \right)$$

De là, en remarquant que la relation de Chasles donne dans les deux sommations des intégrales sur $\mathbb{R}$, convergentes d'après la question précédente (ce ne sont pas tout à fait les mêmes mais le

changement de variable affine $\frac{u}{\sqrt{m}} = x$ permet de passer de l'une à l'autre). Il reste donc :

$$f(0) = \int_{-\infty}^{+\infty} e^{2i\pi u^2/m} du + e^{-i\pi m/2} \int_{-\infty}^{+\infty} e^{2i\pi u^2/m} du = (1 + e^{-i\pi m/2}) \int_{-\infty}^{+\infty} e^{2i\pi u^2/m} du$$

Et le changement de variable $\frac{u}{\sqrt{m}} = x$ donne alors :

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

Question 3-d

En particulier, pour $m=1$, on obtient :

$$f(0) = (1-i)J$$

Or, on a :

$$f(0) = \sum_{k=0}^0 \exp\left(i \frac{(2k\pi)^2}{2\pi}\right) = 1$$

Finalement, on obtient :

$$J = \frac{1}{1-i} = \frac{1+i}{2}.$$

Question 3-e

En reprenant la formule de $f(0)$ pour m quelconque, on obtient :

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

Donc :

$$G(m) = \frac{1+i}{2} (1 + e^{-i\pi m/2}) \sqrt{m}.$$

PARTIE IV

Question 1-a

Existence :

Soit τ l'application définie par : $\tau : \begin{cases} \mathbb{Z} \rightarrow \mathbb{C} \\ t \rightarrow e^{2ik\pi/m} \end{cases}$. τ est clairement un morphisme de groupes

entre $(\mathbb{R}, +)$ et $(\mathbb{C}, \cdot)$, dont le noyau est $m\mathbb{Z}$. Le théorème de factorisation des morphismes nous indique alors que τ induit un morphisme ε_m de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{C}$ vérifiant :

$$\forall k \in \mathbb{Z}, \varepsilon_m([k]_m) = \tau(k) = e^{2ik\pi/m}.$$

Unicité :

La relation définissant ε_m donne explicitement la valeur de $\varepsilon_m(\omega)$ pour $\omega \in \mathbb{Z}/m\mathbb{Z}$, ce qui prouve l'unicité.

Question 1-b

On pose $\alpha = e^{2i\pi/m}$, et ainsi :

$$\sum_{x \in \mathbb{Z}/m\mathbb{Z}} \varepsilon_m(x) = \sum_{k=0}^{m-1} \alpha^k = \frac{1 - \alpha^m}{1 - \alpha} = 0$$

Question 2-a

On suppose donc que $k \equiv h \pmod{2m}$. Donc il existe un entier u tel que $k-h=2mu$.

Donc, en élevant au carré la relation $k=h+2mu$, on obtient : $k^2-h^2=4hmu+4m^2u^2$, et donc : $k^2 \equiv h^2 \pmod{4m}$, et donc $k^2/4m-h^2/4m$ est un entier, d'où :

$$\frac{e^{2i\pi k^2/4m}}{e^{2i\pi h^2/4m}} = e^{2i\pi(k^2/4m-h^2/4m)} = 1,$$

ce qui entraîne bien le résultat voulu.

Question 2-b

On fait dans la deuxième sommation le changement d'indice $k=h+2m$ (ce qui revient à appliquer la propriété (P₁) avec $\phi : h \rightarrow h+2m$, qui est une bijection de $Y=\{1,2,\dots,2m-1\}$ dans $X=\{2m,\dots,4m-1\}$) :

$$\sum_{k=2m}^{4m-1} e^{2ik^2\pi/m} = \sum_{h=0}^{2m-1} e^{2i(h+2m)^2\pi/m}.$$

Et, d'après la question précédente, comme $h+2m \equiv h \pmod{2m}$, on a : $e^{2i(h+2m)^2\pi/m} = e^{2ih^2\pi/m}$.
D'où :

$$\sum_{k=2m}^{4m-1} e^{2ik^2\pi/m} = \sum_{h=0}^{2m-1} e^{2i(h+2m)^2\pi/m} = \sum_{h=0}^{2m-1} e^{2ih^2\pi/m}.$$

Par suite :

$$G(4m) = \sum_{k=2m}^{4m-1} e^{2ik^2\pi/m} + \sum_{h=0}^{2m-1} e^{2ih^2\pi/m} = 2 \sum_{h=0}^{2m-1} e^{2ih^2\pi/m} = 2H(2m).$$

Question 2-c

$$\text{Ainsi, } H(4m) = (1/2).G(8m) = \frac{1}{2} \frac{1+i}{2} (1 + e^{-i\pi 8m/2}) \sqrt{8m} = e^{i\pi/4} (1 + e^{-4\pi mi}) \sqrt{m} = 2\omega \sqrt{m}.$$

Question 3-a

Remarquons d'abord que $\text{Card}(E) = 4pq = \text{Card}(\mathbb{Z}/4pq\mathbb{Z})$. Il suffit donc d'établir l'injectivité de $\bar{k}$ pour établir sa bijectivité. Supposons donc que (avec des notations évidentes) :

$$[lpq+4rq+4sp]_{4pq} = [l'pq+4r'q+4s'p]_{4pq}$$

Ainsi, $4pq$ divise $pq(l-l') + 4q(r-r') + 4p(s-s')$.

Ainsi p divise $4q(r-r')$, et p est premier avec 4 et q , donc avec $4q$, et divise de ce fait $(r-r')$.

Or $1-p \leq r-r' \leq p-1$, et donc $r-r'=0$.

On prouve de même $l=l'$ et $s=s'$.

D'où l'injectivité, puis la bijectivité de $\bar{k}$.

Question 3-b

On a $H(4pq) = \sum_{k=0}^{4pq-1} e^{2i\pi k^2/8pq}$. Or, d'après la question 2-a, la valeur de $e^{2i\pi k^2/8pq}$ ne dépend que

de la classe de k modulo $4pq$. La bijectivité de $\bar{k}$ (cf question précédente) nous permet donc de transformer la sommation sous la forme :

$$H(4pq) = \sum_{(l,r,s) \in E} \exp\left(\frac{2i\pi(lpq+4rq+4sp)^2}{8pq}\right).$$

Puis on développe :

$$H(4pq) = \sum_{(l,r,s) \in E} \exp\left(\frac{2i\pi(l^2 p^2 q^2 + 16r^2 q^2 + 16s^2 p^2 + 8lprq^2 + 8sqp^2 + 32rqsp)}{8pq}\right).$$

On supprime tous les termes multiples de $2i\pi$:

$$H(4pq) = \sum_{(l,r,s) \in E} \exp\left(2i\pi(l^2 p^2 q^2 + 16r^2 q^2 + 16s^2 p^2) / 8pq\right).$$

On fait le ménage :

$$H(4pq) = \sum_{(l,r,s) \in E} \exp\left(2i\pi\left(l^2 pq / 8\right)\right) \cdot \exp\left(2i\pi\left(2r^2 q / p\right)\right) \cdot \exp\left(2i\pi\left(2s^2 p / q\right)\right).$$

Et enfin, on reconnaît le développement d'un produit :

$$H(4pq) = \left(\sum_{l=0}^3 \exp\left(2i\pi\left(l^2 pq / 8\right)\right)\right) \left(\sum_{r=0}^{p-1} \exp\left(2i\pi\left(2r^2 q / p\right)\right)\right) \left(\sum_{s=0}^{q-1} \exp\left(2i\pi\left(2s^2 p / q\right)\right)\right)$$

Et on a bien la formule voulue.

Question 4-a

On additionne le plus bêtement du monde :

$$\sum_{l=0}^3 e^{2i\pi l^2 pq / 8} = 1 + \omega^{pq} + \omega^{4pq} + \omega^{9pq}$$

Or, $\omega^4 = -1$ et $\omega^8 = 1$. Il reste donc :

$$\sum_{l=0}^3 e^{2i\pi l^2 pq / 8} = 1 + \omega^{pq} + (-1)^{pq} + \omega^{pq} = 2\omega^{pq}$$

(car pq est nécessairement impair). En d'autres termes :

$$\sum_{l=0}^3 e^{2i\pi l^2 pq / 8} = 2\omega^{pq} = 2e^{2i\pi pq / 8}.$$

Question 4-b

Il n'y a qu'à assembler ce dernier résultat avec la formule du 3-b et la définition de $L(p,q)$ (et de $L(q,p)$) donnée en début de partie.

Question 4-c

On a :

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

Par ailleurs, on vient de voir : $H(4p) = 2\omega^p L(p,1) L(1,p)$. Or, on sait (question 2-c) que :

$H(4p) = 2\omega\sqrt{p}$. Il reste donc : $H(4p) = 2\omega\sqrt{p} = 2\omega^p L(p,1)$. Finalement :

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

Question 5-a

On sait, d'après la question 1-b, que : $\sum_{x \in (\mathbb{Z}/p\mathbb{Z})} \varepsilon_p(x) = 0$. Or $[0]_p$ est le seul élément non

inversible de $\mathbb{Z}/p\mathbb{Z}$, vu que p est premier.

Cette relation peut donc s'écrire : $\varepsilon_p([0]_p) + \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \varepsilon_p(x) = 0$, soit encore :

$$1 + \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \varepsilon_p(x) = 0.$$

Or, étant donné que $[2]_p$ n'est pas nul, $[2]_p$ est inversible, et l'application définie sur le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ par : $x \rightarrow [2]_p \cdot x$ est bijective de $(\mathbb{Z}/p\mathbb{Z})^\times$ dans lui-même. La relation ci-dessus peut alors s'écrire :

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

Question 5-b

On écrit d'abord, en partant de la définition de $L(p,q)$:

$$L(p,q) = \sum_{r=0}^{p-1} e^{4i\pi q r^2 / p} = 1 + \sum_{k=1}^{p-1} \varepsilon_p \left([2qk^2]_p \right) = 1 + \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \varepsilon_p \left([2q]_p \sigma(x) \right)$$

La première égalité demandée est donc bien établie. On continue en remarquant que pour $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\sigma(x) \in S$, et que pour $y \in S$, l'équation d'inconnue $x \in (\mathbb{Z}/p\mathbb{Z})^\times$: $\sigma(x) = y$ a exactement deux solutions : en effet, elle en a au moins une, notée y_0 par définition même de S , et l'équation équivaut alors à $\sigma(x) = \sigma(y_0)$, soit encore à $\sigma(xy_0^{-1}) = 1$, c'est à dire $xy_0^{-1} \in K$, avec $K = \ker \sigma$, et on a vu que K a exactement deux éléments.

Ainsi, en utilisant la propriété (P2), on peut écrire :

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

Et la deuxième égalité est bien prouvée.

Question 5-c

En supposant que $[q]_p$ appartienne à S , alors, en utilisant la structure de groupe de S , on a la bijectivité de l'application définie de S dans S par : $y \rightarrow [q]_p y$.

Donc (c'est la propriété (P1)) :

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

ou, en d'autres termes :

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

On voit alors que le deuxième membre ne dépend pas de q tel que $[q]_p \in S$. On peut donc en particulier écrire, comme $[1]_p \in S$: $L(p,q) = L(p,1)$.

Question 5-d

On utilise le même raisonnement si $[q]_p \in T$, sauf que cette fois l'application : $y \rightarrow [q]_p y$ est une bijection de S sur T : en effet, les deux ensembles ont le même nombre d'éléments, l'application est injective car $[q]_p$ est inversible (q est premier avec p), et elle est bien à valeurs dans T d'après le I-3-e. On obtient alors bien :

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

Par ailleurs comme $[1]_p \in S$, on a d'après la relation ci dessus :

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

Donc on peut écrire :

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

Et finalement :

$$L(p,q) + L(p,1) = 2 \left(1 + \sum_{y \in (\mathbb{Z}/p\mathbb{Z})^\times} \varepsilon_p \left([2]_p y \right) \right) = 0 \quad (\text{d'après le 5-a}).$$

Question 6

Il faut aller à la pêche aux résultats :

Ainsi $L(p,q).L(q,p) = \left(\frac{q}{p} \right) L(p,1) \left(\frac{p}{q} \right) L(q,1)$. Or, $L(p,1) = \omega^{1-p} \sqrt{p}$, et $L(q,1) = \omega^{1-q} \sqrt{q}$.

On obtient donc :

$$L(p,q).L(q,p) = \left(\frac{q}{p} \right) \left(\frac{p}{q} \right) \omega^{2-p-q} \sqrt{pq}$$

Or, selon le 4-b :

$$L(p,q)L(q,p)=\frac{1}{2}\omega^{-pq}H(4pq).$$

Et, d'après la question 2-c de la partie III, $H(4pq)=2\omega\sqrt{pq}$.

Ainsi :

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

On touche alors (enfin) au but :

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

Et la loi de réciprocité quadratique s'en trouve démontrée.