DS 1 : 4h

Élements de correction

Questions de cours :

1. $(\mathbb{R},+)$, $(\mathbb{R}+^*,\times)$, $(\mathcal{M}_n(\mathbb{R}),+)$, $(GL_n(\mathbb{R}),\times)$ sont des groupes.

2. **a.** $\det : (GL_n(\mathbb{K}),\times) \to (\mathbb{K}^*,\times)$.
$\mathrm{Tr} : (\mathcal{M}_n(\mathbb{K}),+) \to (\mathbb{K},+)$.
$\exp : (\mathbb{C},+) \to (\mathbb{C}^*,\times)$

b. On demandait d'en DEDUIRE le résultat ! Il fallait donc utiliser les morphismes et ne pas utiliser la caractérisation des sous groupes.
$SL_n(\mathbb{C}) = \{M \in \mathcal{M}_n(\mathbb{C}) | \det(M) = 1\}$ pour la loi de multiplication des matrices est le noyau du déterminant. C'est donc un sous groupe tout comme $(2i\pi\mathbb{Z},+)$ qui est le noyau de la fonction exponentielle.

3. Les idéaux de $\mathbb{K}[X]$ sont exactement les (P) pour $P \in \mathbb{K}[X]$. Démonstration dans le cours.

4. Soit f un morphisme de groupes de $(\mathbb{Z},+)$ dans $(\mathbb{Q},+)$. Soit $a = f(1) \in \mathbb{Q}$. Si $a = 0$, f est le morphisme nul qui n'est pas bijectif. Sinon, $f(\mathbb{Z}) = a\mathbb{Z}$. Or $a\mathbb{Z} \neq \mathbb{Q}$ car $\frac{a}{2} \in \mathbb{Q}$ mais $\frac{a}{2} \notin a\mathbb{Z}$.
Dans tous les cas, f n'est pas bijectif.

Problème 1 :

Préliminaires :

1. Soit $n \in \mathbb{N}$ qui n'est pas un carré parfait (le carré d'un entier naturel). On suppose par l'absurde que $\sqrt{n} = \frac{a}{b}$ avec $a \wedge b = 1$.

a. On peut supposer que b est un entier strictement positif (quitte à prendre l'opposé de a). On ne peut pas avoir $b = 1$ car sinon, $\sqrt{n} = a \in \mathbb{Z}$ or n n'est pas un carré parfait. Donc $b \geq 2$. Par le théorème de décomposition en produit de nombres premiers, b admet donc un diviseur p premier.
Au passage, on rappelle que 1 n'est pas premier.

b. Alors $n = \frac{a^2}{b^2}$. Réflexe de raisonnement arithmétique : on ne manipule pas des fractions ! On réécrit donc $nb^2 = a^2$. Ainsi, $np^2 = a^2$, donc p divise $a^2 = a \times a$. Comme p est un nombre premier, par le lemme de Gauss, p divise a (ou p divise a...).
Ainsi, a et b sont divisibles par p donc ne sont pas premiers entre eux. Contradiction et résultat : $\sqrt{n}$ n'est pas rationnel.

2. Soit p un nombre premier et $k \in [1, p-1]$.

a. On remarque que $k!(p-k)!\binom{p}{k} = p! = p \times (p-1)!$. Donc p divise $k!(p-k)!\binom{p}{k}$.

Or p est premier avec tout entier $j \in [1, p-1]$. Donc p est premier avec tout produit d'entiers $j \in [1, p-1]$. Ainsi, $p \wedge k!(p-k)!$ car $k \in [1, p-1]$.

Par le lemme de Gauss, p divise donc $\binom{p}{k}$ pour tout $k \in [1, p-1]$.

Attention : p ne divise pas $\binom{p}{0}$ ni $\binom{p}{p}$...

b. En travaillant dans $\mathbb{Z}/p\mathbb{Z}$, le dernier résultat se traduit en $\binom{p}{k} \equiv 0 \bmod p$ pour tout $k \in [1, p-1]$. Pour tout $(a, b) \in \mathbb{Z}^2$, comme $\mathbb{Z}/p\mathbb{Z}$ est un anneau commutatif, on peut appliquer la formule du binôme de Newton et on obtient :

$$(a+b)^p \equiv \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = 0 + a^p + b^p \bmod p.$$

3. **a.** On peut remarquer que si $x^2 \equiv d \bmod p$, alors $(-x)^2 = d \bmod p$. Il suffit donc de calculer $0^2, 1^2, 2^2, ..., \frac{(p-1)}{2}^2$ modulo p car alors $(p-1)^2 = 1^2$, $(p-2)^2 = 2^2$... etc...

Les carrés de $\mathbb{Z}/11\mathbb{Z}$ sont donc$\{(0 \bmod 11)^2, (1 \bmod 11)^2, (2 \bmod 11)^2, (3 \bmod 11)^2, (4 \bmod 11)^2, (5 \bmod 11)^2\} = \{\overline{0}, \overline{1}, \overline{4}, \overline{9}, \overline{5}, \overline{3}\}$.

Ceux de $\mathbb{Z}/17\mathbb{Z}$ sont $\{\overline{0}, \overline{1}, \overline{4}, \overline{9}, \overline{-1}, \overline{-9}, \overline{2}, \overline{-2}, \overline{-4}$.

b. Effectivement !

4. Soit $n \geq 2$. $S_n = \sum_{k=0}^{n-1} \exp(\frac{2ik\pi}{n}) = \sum_{k=0}^{n-1} \left(\exp(\frac{2i\pi}{n})\right)^k$ est une somme de premiers termes d'une suite géométrique. On rappelle que sa raison $\exp(\frac{2i\pi}{n})$ est différente de 1 car $n \geq 2$. Donc $S_n = \frac{1 - \exp(\frac{2in\pi}{n})}{1 - \exp(\frac{2i\pi}{n})} = 0$ car $\exp(\frac{2in\pi}{n}) = 1$.

Partie 1 :

1. **a.** $\mathbb{Z}[\delta]$ est une intersection de sous-anneaux de $(\mathbb{C}, +, \times)$.

En particulier $(\mathbb{Z}[\delta], +)$ est une intersection de sous groupes additifs, donc un sous groupe additif de $(\mathbb{C}, +)$.

Si $(a, b) \in \mathbb{Z}[\delta]^2$, alors pour tout A sous anneau de $(\mathbb{C}, +, \times)$ contenant δ, $a \in A$ et $B \in A$. Comme A est un sous anneau (donc stable par produit interne), $a \times b \in A$. Finalement, $a \times b \in \bigcap_{A \in A_\delta} A = \mathbb{Z}[\delta]$.

De même, $1 \in \mathbb{Z}[\delta]$ (rédaction laissée au lecteur non passif).

Ainsi, $\mathbb{Z}[\delta]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

b. Si B est un sous-anneau de $(\mathbb{C}, +, \times)$ contenant δ, alors $B \in A_\delta$. En particulier, $\mathbb{Z}[\delta] = B \bigcap \left(\bigcap_{A \in A_\delta \setminus \{B\}}\right)$ est une partie de B. Donc $\mathbb{Z}[\delta] \subset B$.

On vient de montrer que $\mathbb{Z}[\delta]$ est le plus petit sous-anneau de $(\mathbb{C}, +, \times)$ contenant δ.

2. **a.** Supposons $\delta \in \mathbb{Z}$. Alors $\mathbb{Z}$ est un sous anneau de $\mathbb{C}$ contenant δ. Par statut minimal de $\mathbb{Z}[\delta]$, on a donc $\mathbb{Z}[\delta] \subset \mathbb{Z}$.

MAIS, n'oublions pas de remarquer que $1 \in \mathbb{Z}[\delta]$. Alors pour tout $n \in \mathbb{Z}$, $n \cdot 1 \in \mathbb{Z}[\delta]$ qui est un sous groupe additif de $\mathbb{C}$. Donc $\mathbb{Z} \subset \mathbb{Z}[\delta]$.

FInalement,

$$\mathbb{Z}[\delta] = \mathbb{Z}.$$

b. On procède par double inclusion.

L'une est classique : si $\delta \in \mathbb{Z}[\delta]$, alors par stabilité du produit et donc des puissances en particulier, $\forall k \in \mathbb{N}, \delta^k \in \mathbb{Z}[\delta]$. Comme $\mathbb{Z}[\delta]$ est un sous groupe additif de $\mathbb{C}$, $\forall a_k \in \mathbb{Z}, a_k\delta^k \in \mathbb{Z}[\delta]$. Finalement, pour tout $P \in \mathbb{Z}[X]$, $P(\delta) \in \mathbb{Z}[\delta]$. Donc :

$$\{P(\delta)|P \in \mathbb{Z}[X]\} \subset \mathbb{Z}[\delta].$$

Réciproquement, il serait plus délicat de montrer que tout élément de $\mathbb{Z}[\delta]$ est un polynôme en δ. Il faut donc une autre approche, utilisant les propriétés de $\mathbb{Z}[\delta]$.

Par statut minimal de $\mathbb{Z}[\delta]$, il suffit de montrer que $\{P(\delta)|P \in \mathbb{Z}[X]\}$ est un sous anneau de $\mathbb{C}$ contenant δ. D'après la question **1.b**, nous aurons alors l'inclusion $\mathbb{Z}[\delta] \subset \{P(\delta)|P \in \mathbb{Z}[X]\}$.

On montre facilement que $\{P(\delta)|P \in \mathbb{Z}[X]\}$ est un sous groupe additif de $\mathbb{C}$, que $\{P(\delta)|P \in \mathbb{Z}[X]\}$ est stable par produit et que $1 = \delta^0 \in \{P(\delta)|P \in \mathbb{Z}[X]\}$...

c. NON : par exemple, $i = i^5$ dans $\mathbb{Z}[i]$.

3. a. La relation est réflexive, symétrique et transitive. Aucune difficulté.

b. Définissons les lois $+_p$ et $\times_p$ suivante sur $\mathbb{Z}[\delta]/(p)$:

Pour $(\dot{a}, \dot{b}) \in (\mathbb{Z}[\delta]/(p))^2$, on pose $\dot{a} +_p \dot{b} := a \dot{+} b$ et $\dot{a} \times_p \dot{b} := a \dot{\times} b$.

Il suffit de montrer que le résultat ne dépend pas du choix des représentants des classes $\dot{a}$ et $\dot{b}$.

Par construction, ϕ est bien un morphisme (immédiat) et surjectif car tout élément $\dot{a} \in \mathbb{Z}[\delta]/(p)$ admet $a \in \mathbb{Z}[\delta]$ comme antécédent.

Partie 2 :

On suppose dans cette partie que le nombre complexe δ vérifie les conditions $\delta \notin \mathbb{Z}$ et $\delta^2 \in \mathbb{Z}$. On note $d = \delta^2$.

L'entier p est toujours premier et impair.

1. D'après la question **2.b**, $\mathbb{Z}[\delta] = \{P(\delta)|P \in \mathbb{Z}[X]\}$.

Soit $P \in \mathbb{Z}[X]$. Alors $P(\delta) = \sum_{n=0}^{N} a_n\delta^n = \sum_{k=0}^{N/2} a_{2k}\delta^{2k} + \sum_{k=0}^{N/2} a_{2k+1}\delta^{2k+1}$.

Or $\delta^{2k} = d^k \in \mathbb{Z}$. Donc par somme et produits d'entiers, $P(\delta) = n_0 + m_0\delta$ en posant $n_0 = \sum_{k=0}^{N/2} a_{2k}d^k \in \mathbb{Z}$ et $m_0 = \sum_{k=0}^{N/2} a_{2k+1}d^k \in \mathbb{Z}$.

Finalement,

$$\mathbb{Z}[\delta] = \{n_0 + \delta m_0|(n_0, m_0) \in \mathbb{Z}^2\}.$$

2. 1er cas : si $d < 0$, alors $\delta \in i\mathbb{R}$. Soient (n, m) et (n', m') couples d'entiers tels que $a = n + \delta m = n' + \delta m'$. Par unicité des parties réelles et imaginaires des nombres complexes, $n = n'$ et $m = m'$.

2eme cas : si $d > 0$, alors $\delta \in \mathbb{R} \setminus \mathbb{Q}$ d'après les préliminaires. Soient (n, m) et (n', m') couples d'entiers tels que $a = n + \delta m = n' + \delta m'$. Si $m \neq m'$, alors $\delta = \dfrac{n - n'}{m - m'} \in \mathbb{Q}$ ce qui est absurde. Donc $m = m'$ et par suite, $n = n'$.

On suppose toujours p premier impair et on suppose que $d \wedge p = 1$.

3. Soit $\dot{a} \in \mathbb{Z}[\delta]/(p)$ tel que $\dot{a}^2 = \dot{0}$, c'est à dire $(n + \dot{\delta} m)^2 = \dot{0}$ donc il existe (n', m') entiers tels que $(n + \delta m)^2 = n^2 + 2\delta nm + dm^2 = p(n' + \delta m')$.

L'unicité de l'écriture démontrée dans la question précédente permet d'écrire alors :

$2nm = pm'$ et $n^2 + dm^2 = pn'$. En particulier, p divise $2nm$ et $n2 + dm^2$. Comme p est impair, donc premier avec 2, par le lemme de Gauss, p divise n ou m.

Si $p|m$, comme $p|n^2 + dm^2$, alors $p|n^2$ et finalement $p|n$.

De même, si $p|n$, alors $p|m^2d$ et comme p est premier avec d, $p|b$.

Ainsi, $p|n\delta + m$ c'est à dire $(n + \dot{\delta} m)^2 = \dot{0}$.

Pour tout $a \in \mathbb{Z}[\delta]$, si $a = n + \delta m$, on note $a^c = n - \delta m$ et $N(a) = a \times a^c$.

4. Soit $a \in \mathbb{Z}[\delta]$, $N(a) = n^2 - dm^2 \in \mathbb{Z}$ par somme et produit d'entiers.

5. Pour $a' = n' + \delta m'$, on remarque que $N(aa') = ... = N(a)N(a')$.
De plus, on remarque que si $\dot{a} = \dot{b}$, alors $N(a) \bmod p = N(b) \bmod p$
Si $\dot{a}$ est inversible dans $\mathbb{Z}[\delta]/(p)$ on a donc $1 = N(1) \bmod p = N(aa^{-1}) \bmod p = (N(a) \bmod p)(N(a^{-1} \bmod p)$.
Donc $N(a)$ est inversible modulo p, c'est à dire $N(a) \wedge p = 1$.
Réciproquement, si $N(a) \wedge p = 1$, alors $N(a)$ est inversible modulo p et alors $aa^c N(x)^{-1} \equiv N(x)N(x)^{-1} \equiv 1 \bmod p$.
Donc a est inversible d'inverse $a^c N(a)^{-1}$.

6. Supposons que d n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$. Soit $\dot{a}$ non inversible dans $/Z[\delta]/(p)$. Alors d'après ce qui précède, $p \wedge N(a) \neq 1$ donc $p|N(a)$ car p est premier. Ainsi, si $a = n + \delta m$, $p|n^2 - \delta m^2$, c'est à dire $dm^2 \equiv n^2 \bmod p$.
Si p ne divise pas m, alors $m \bmod p$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$ (qui est un corps) et $d \equiv a^2 b^{-2} \equiv (ab^{-1})^2 \bmod p$, ce qui contredit l'hypothèse faite sur d.
Ainsi, p divise m puis p divise n^2 et donc n. Donc $\dot{a} = n \dot{+} \delta m = \dot{0}$.
Le seul élément non inversible de $\mathbb{Z}[\delta]/(p)$ est donc l'élément nul donc $\mathbb{Z}[\delta]/(p)$ est un corps.

Partie 3 :

Soit :

$$q : \begin{cases} ((\mathbb{Z}/p\mathbb{Z})^*, \times) & \to & ((\mathbb{Z}/p\mathbb{Z})^*, \times) \\ (x \bmod p) & \mapsto & (x \bmod p)^2 \end{cases}$$

1. L'application q est un morphisme de groupes MULTIPLICATIFS et $\ker q = \{x \in \mathbb{Z}/p\mathbb{Z} | x^2 = (1 \bmod p)\}$.
Or $x^2 = (1 \bmod p) \Leftrightarrow x^2 - (1 \bmod p) = (x - (1 \bmod p))(x + (1 \bmod p)) = 0$.
Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps (donc intègre), on en déduit que $x = \pm(1 \bmod p)$. Ainsi, $\ker q = \{(1 \bmod p), (-1 \bmod p)\}$.

2. Dans un exercice, on a montré le théorème du rang pour les morphismes de groupes :

$$\text{Card}\,((\mathbb{Z}/p\mathbb{Z})^*) = \text{Card}(\text{Ker } q) \cdot \text{Card}(\text{Im } q).$$

3. Ici, $Card(\ker q) = 2$. De plus les carrés non nuls sont exactement les éléments dans l'image de la fonction q. Donc le nombre de carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$ est égal à $Card(Im(q)) = \dfrac{Card((\mathbb{Z}/p\mathbb{Z})^*)}{2} = \dfrac{p-1}{2}$.

4. Par le théorème de Lagrange, on montre la formule d'Euler :

$$\forall x \in \mathbb{Z}, x \wedge p = 1 \Rightarrow x^{\varphi(p)} \equiv 1 \bmod p.$$

(ici, $\varphi(p) = p - 1$).

5. En posant $y = x^{(p-1)/2}$, on obtient $y^2 = x^{p-1} = (1 \bmod p)$. Donc $y \in \ker q$ et finalement, $y = x^{(p-1)/2}$ est congru à 1 ou (-1) modulo p.

6. Il y a exactement $\dfrac{p-1}{2}$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$.
Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc intègre, l'équation polynomiale $x^{(p-1)/2} - 1$ de degré $\dfrac{p-1}{2}$ admet au plus $\dfrac{p-1}{2}$ solutions. Or, si x est le carré de y, forcément $x^{(p-1)/2} = y^{p-1} = 1$, donc x est solution.
Ainsi, l'équation polynomiale $x^{(p-1)/2} - 1$ admet exactement $\dfrac{p-1}{2}$ solutions qui sont exactement les carrés modulo p.

7. **a.** Remarquons qu'étant donné que p est impair, $p > 2$ et $(-1)^k = 1$ si et seulement si $k \in 2\mathbb{Z}$. Alors :

(-1) est un carré dans $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow (-1)^{(p-1)/2} = 1 \bmod p \Leftrightarrow (p-1)/2 \in 2\mathbb{Z} \Leftrightarrow p - 1 \in 4/Z \Leftrightarrow p \equiv 1 \bmod 4$.

b. On retrouve que 2 est un carré modulo 17 mais pas modulo 11 en calculant $2^{(p-1)/2}$ modulo p pour $p = 11$ puis $p = 17$.

Soient des entiers n et n' non divisibles par p.

8. — si n et n' sont des carrés de $\mathbb{Z}/p\mathbb{Z}$, alors $n^{(p-1)/2} \equiv 1$ et $(n')^{(p-1)/2} \equiv 1$, donc $(nn')^{(p-1)/2} = 1 \times 1 = 1$. Ainsi, nn' est un carré modulo p.
— si n est un carré de $\mathbb{Z}/p\mathbb{Z}$ et n' n'est pas un carré de $\mathbb{Z}/p\mathbb{Z}$, $n^{(p-1)/2} \equiv 1$ et $(n')^{(p-1)/2} \equiv -1$, donc $(nn')^{(p-1)/2} = 1 \times (-1) = -1$. Ainsi, nn' n'est pas un carré modulo p.
— si n et n' ne sont pas des carrés de $\mathbb{Z}/p\mathbb{Z}$, alors $n^{(p-1)/2} \equiv -1$ et $(n')^{(p-1)/2} \equiv -1$, donc $(nn')^{(p-1)/2} = (-1) \times (-1) = 1$. Ainsi, nn' est un carré modulo p.

9. Soit $j = \exp(\frac{2i\pi}{3})$. On suppose en plus $p \neq 3$.

a. Dans $\mathbb{C}$, j est inversible et $j^{-1} = j^2$ car $j^3 = 1$. Or $j^2 \in \{P(j) | P \in \mathbb{Z}[X]\} = \mathbb{Z}[j]$. Donc j est inversible dans $\mathbb{Z}[j]/(p)$ d'inverse $\dot{j^2} = j^2$.

On pose $b = j - j^{-1}$, élément de $\mathbb{Z}[j]/(p)$.

b. Alors $b^2 = (j - j^{-1})^2 = j^2 - 2 + j^{-2} = j^2 - 2 + j^4 = j^2 - 2 + j = -3 + (1 + j + j^2) = -3$ car $1 + j + j^2 = 0$.

Ainsi, (-3) est le carré de $\dot{b}$ dans $\mathbb{Z}[j]/(p)$. Attention : b n'est pas un élément de $\mathbb{Z}$...

Comme $p > 3$, p ne divise pas (-3).

Alors (-3) est un carré modulo $p \Leftrightarrow (-3)^{(p-1)/2} = 1 \bmod p \Leftrightarrow$(dans $\mathbb{Z}[j]/(p)$), $(b^2)^{(p-1)/2} = \dot{1} \Leftrightarrow b^{p-1} = \dot{1} \Leftrightarrow b^p = b$ car b est inversible dans $\mathbb{Z}[j]/(p)$ car $b^2 = \dot{-3}$ est inversible modulo p pour $p > 3$.

Finalement -3 est un carré dans $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow b^p = b$ dans $\mathbb{Z}[j]/(p)$.

c. Or, $b^p = (j - j^{-1})^p = j^p + (-j^{-1})^p = j^p - j^{-p}$ car p est impair.

Ainsi, (-3) est un carré modulo $p \Leftrightarrow j^p - j^{-p} = j - j^{-1}$.

On remarque que $j^p - j^{-p}$ est respectivement égal à

- 0 si $p \equiv 0[3]$,
- $j - j^{-1}$ si $p \equiv 1[3]$,
- $j^2 - j^{-2}$ si $p \equiv 3[3]$.

Finalement, (-3) est un carré $\Leftrightarrow p \equiv 1[3]$.

d. D'après la question **8.**, 3 est un carré de $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow (-3)$ et (-1) sont tous les deux carrés ou bien ni (-3) ni (-1) ne sont des carrés.

Donc $p \equiv 1[3]$ et $p \equiv 1[4]$ (c'est à dire $p \equiv 1[12]$) ou bien $p \equiv (-1 - [3]$ et $p \equiv (-1)[4]$ (c'est à dire $p \equiv (-1)[12]$)

10. Soit $\omega = \exp(i\frac{\pi}{4})$, vu comme élément de $\mathbb{Z}[\omega]/(p)$ d'inverse $\omega^{-1} = -\omega$ et $b = \omega - \omega^{-1}$

On calcule $b^2 = \omega^2 - 2\omega^{-2} = 2$.

Donc par un raisonnement similaire, 2 est un carré $\Leftrightarrow b^p = \omega^p + \omega^{-p} = b$.

On remarque que pour des valeurs de p impair :

- si $p \equiv 1[8], b^p = b$
- si $p \equiv 3[8], b^p = -b$
- si $p \equiv 5[8], b^p = -b$
- si $p \equiv 7[8], b^p = b$

Finalement, 2 est un carré modulo $p \Leftrightarrow p = \pm 1[8]$.

Partie 4 :

Le nombre p est toujours un nombre premier impair.

On définit la fonction de Legendre L_p Soit $\zeta = \exp(\frac{2i\pi}{p})$.

On définit la somme de Gauss relative à p par le nombre complexe $G = \sum_{a\in\mathbb{Z}/p\mathbb{Z}} L_p(a)\zeta^a$.

1. a. Soit $(a,t) \in \mathbb{Z}^2$. Alors $L_p(a^2t) = L_p(a^2) \times L_p(t) = L_p(t)$ car a^2 est un carré donc $L_p(a^2) = 1$.

b. Soit $S = \sum_{(a,b)\in((\mathbb{Z}/p\mathbb{Z})^*)^2} L_p(ab)\zeta^{a+b}$.

À tout couple $(a,b) \in (\mathbb{Z}/p\mathbb{Z}^*)^2$, on peut associer un unique couple (a,t) en posant $t = ba^{-1}$. L'élément t est inversible par produit d'inversibles. Ainsi,

$S = \sum_{(a,t)\in((\mathbb{Z}/p\mathbb{Z})^*)^2} L_p(a(at))\zeta^{a+(at)}$

$= \sum_{(a,t)\in((\mathbb{Z}/p\mathbb{Z})^*)^2} L_p(a^2t)\zeta^{a(1+t)}$

$= \sum_{(a,t)\in((\mathbb{Z}/p\mathbb{Z})^*)^2} L_p(t)\zeta^{a(1+t)}$

$= \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^*} L_p(t)\left(\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \zeta^{a(1+t)}\right)$

Pour $t = (-1)$, $\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \zeta^{a(1+t)} = (p-1)$ (nombre de termes tous égaux à 1)

Pour $t \neq (-1)$, $\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \zeta^{a(1+t)} = \sum_{b\in(\mathbb{Z}/p\mathbb{Z})^*} \zeta^b$ par un changement d'indices et donc

$\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \zeta^{a(1+t)} = \left(\sum_{b\in(\mathbb{Z}/p\mathbb{Z})} \zeta^b\right) - \zeta^0 = 0 - 1 = (-1)$ en complétant la somme.

Finalement,

$$S = (p-1)\cdot L_p(-1) - \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^*\setminus\{-1\}} L_p(t).$$

c. Remarquons que $\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} L_p(a) = 0$ car il y a autant de carrés modulo p que de "non-carrés" modulo p. Cette somme est donc constituée d'autant de 1 que de (-1).

Alors $G^2 = \left(\sum_{a\in(\mathbb{Z}/p\mathbb{Z})} L_p(a)\zeta^a\right)\cdot\left(\sum_{b\in(\mathbb{Z}/p\mathbb{Z})} L_p(b)\zeta^b\right)$

$= \left(\sum_{a\in(\mathbb{Z}/p\mathbb{Z})^*} L_p(a)\zeta^a\right)\cdot\left(\sum_{b\in(\mathbb{Z}/p\mathbb{Z})^*} L_p(b)\zeta^b\right)$ car $L_p(0) = 0$

$= \left(\sum_{(a,b)\in((\mathbb{Z}/p\mathbb{Z})^*)^2} L_p(a)L_p(b)\zeta^a\zeta^b\right)$

$= \left(\sum_{(a,b)\in((\mathbb{Z}/p\mathbb{Z})^*)^2} L_p(ab)\zeta^{a+b}\right)$

$= S = (p-1)\cdot L_p(-1) - \sum_{t\in(\mathbb{Z}/p\mathbb{Z})^*\setminus\{-1\}} L_p(t)$ d'après ce qui précède

$= p \cdot L_p(-1) - \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^*} L_p(t) = pL_p(-1) - \sum_{t \in (\mathbb{Z}/p\mathbb{Z})} L_p(t) = pL_p(-1) - 0.$

Finalement,

$$G^2 = p \cdot (-1)^{(p-1)/2}.$$

2. Soient p et q deux nombres premiers impairs distincts.

a. On a déjà vu que $L_p(a) = L_p(q^2a) = L_p(q) \cdot L_p(qa)$.
Si $L_p(a) = 0$, alors $L_p(a) = (L_p(a))^q$.
Si $L_p(a) = 1$, alors $L_p(a) = (L_p(a)p)^q$
Enfin, si $L_p(a) = (-1)$, alors $L_p(a) = (L_p(a))^q$ car q est impair.

b. Posons $t = aq$ comme précédemment.

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} (L_p(a)\zeta^a)^q \mod q = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} ((L_p(a))^q \zeta^{aq}) \mod q$$
$$= \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} L_p(q)L_p(aq)\zeta^{aq} \mod q$$
$$= \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^*} L_p(q)L_p(t)\zeta^t \mod q$$
$$= L_p(q) \cdot \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^*} L_p(t)\zeta^t \mod q$$
$$= L_p(q) \cdot G \mod q.$$

c. En utilisant la question **2.b** des préliminaires,

$$G^q \equiv \left(\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} L_p(a)\zeta^a \right)^q \mod q = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} (L_p(a)\zeta^a)^q \mod q \equiv L_p(q) \cdot G \mod q.$$

d. D'après la question **1.c**, $(G^2)^{(q-1)/2} \cdot G \mod q = (p \cdot (-1)^{(p-1)/2})^{(q-1)/2} \cdot G \mod q$
$= p^{(q-1)/2} \cdot (-1)^{(p-1)(q-1)/4} \cdot G \mod q$
$= L_q(p) \cdot (-1)^{(p-1)(q-1)/4} \cdot G \mod q$

3. Finalement, on obtient par **2.c** et **2.c** :
$L_p(q)G \equiv G^q \equiv (G^2)^{(q-1)/2} \equiv (-1)^{(p-1)(q-1)/4} L_q(p)G \mod q.$
Ainsi, $L_p(q)G \equiv (-1)^{(p-1)(q-1)/4} L_q(p)G \mod q.$
En multipliant par G, on obtient :
$L_p(q)G^2 \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} L_q(p)G^2 \mod q$
donc par **1.c** :
$L_p(q)p(-1)^{(p-1)/2} \equiv (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} L_q(p)p(-1)^{(p-1)/2} \mod q$
Or $p \wedge q = 1$ donc $p(-1)^{(p-1)/2} = \pm p$ est inversible dans $\mathbb{Z}/q\mathbb{Z}$. Finalement,

$$L_p(q) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} L_q(p).$$