

Épreuve écrite de mathématiques générales

Préambule

Le but de ce problème est d'étudier le nombre de solutions modulo un entier naturel q d'une congruence quadratique matricielle

$${}^tX SX \equiv T \pmod{q}$$

où S et T sont des matrices symétriques données à coefficients entiers, de tailles respectives $m \times m$ et $n \times n$, q est un entier strictement positif et l'inconnue X est une matrice d'entiers de taille $m \times n$, tX désignant sa transposée.

Soit R un anneau commutatif; dans ce préambule, on note 1_R son élément unité, mais on permet d'écrire 1 dans la rédaction. On note R^\times le groupe des éléments inversibles de R .

Étant donnés deux entiers m et n strictement positifs, on note $M_{m,n}(R)$ l'ensemble des matrices à m lignes et n colonnes à coefficients dans R .

Pour tout entier n strictement positif, on note $[1, n] = \{i \in \mathbb{Z} \mid 1 \leq i \leq n\}$; pour simplifier, on note $M_n(R)$, au lieu de $M_{n,n}(R)$, l'anneau des matrices carrées de taille $n \times n$ à coefficients dans R . Le déterminant d'une matrice carrée X à coefficients dans R est défini par la formule habituelle et noté $\det X$. On rappelle qu'une matrice de $M_n(R)$ est inversible si et seulement si son déterminant est dans l'ensemble R^\times des éléments inversibles de R . On note $GL_n(R)$ le groupe des éléments de $M_n(R)$ de déterminant dans le groupe R^\times .

On note 1_n la matrice unité de $M_n(R)$. On note $S_n(R)$ l'ensemble des matrices X de $M_n(R)$ symétriques, c'est-à-dire telles que ${}^tX = X$.

A. Solutions modulo un nombre premier impair

Dans cette partie **A.**, on fixe un nombre premier **impair** p et on considère deux matrices symétriques S et T , avec $S \in M_m(\mathbb{Z}/p\mathbb{Z})$ et $T \in M_n(\mathbb{Z}/p\mathbb{Z})$, de déterminants respectifs s et t non nuls. L'élément de la i -ème ligne et j -ème colonne de S (resp. T) est noté $s_{i,j}$ (resp. $t_{i,j}$).

On introduit l'ensemble $\mathcal{A}_p(S, T) = \{X \in M_{m,n}(\mathbb{Z}/p\mathbb{Z}) \mid {}^tX SX = T\}$ et on note $A_p(S, T)$ son cardinal.

A.I Un cas particulier

Dans cette section **A.I.**, on prend $m = 2$ et $n = 1$. Soit s et t deux éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$, $T = \begin{pmatrix} t \end{pmatrix}$ et $S = \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}$. La matrice T , de taille 1×1 , est identifiée à t ; ainsi $A_p(S, t)$ est le nombre de couples (x, y) dans $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ tels que $x^2 + sy^2 = t$.

1) Supposons que $-s$ soit un carré dans $\mathbb{Z}/p\mathbb{Z}$. Calculer $A_p(S, t)$.

2) On suppose dans toute la suite de cette section **A.I** que $-s$ n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

2.a. Montrer que le polynôme $X^2 + s$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$. Soit K un corps de rupture. Quel est le cardinal de K ?

2.b. Soit $F : K \rightarrow K$, $z \mapsto z^p$. Montrer que F est un automorphisme involutif de corps ($F \circ F = Id_K$) et déterminer ses points fixes.

2.c. Soit α une racine de $X^2 + s$ dans K . Montrer que $F(\alpha) = -\alpha$.

3) Soit $N : K^\times \rightarrow K^\times$, $z \mapsto z^{p+1}$.

3.a. Montrer que N est un morphisme de groupes d'image contenue dans $(\mathbb{Z}/p\mathbb{Z})^\times$.

3.b. Déterminer le cardinal du noyau et de l'image de N .

3.c. Calculer $N(x + y\alpha)$ pour $x, y \in \mathbb{Z}/p\mathbb{Z}$ non tous deux nuls.

4) Calculer $A_p(S, t)$.

A.II Préliminaires

Dans cette section **A.II**, m est un entier strictement positif et V un espace vectoriel de dimension finie m sur le corps $\mathbb{Z}/p\mathbb{Z}$.

1) Soit $b : V \times V \rightarrow \mathbb{Z}/p\mathbb{Z}$ une forme bilinéaire symétrique sur V .

1.a. Démontrer que si $b(x, x)$ est nul pour tout x dans V , alors la forme bilinéaire b est nulle.

1.b. Démontrer que V possède une base (e_1, \dots, e_m) orthogonale pour b , c'est-à-dire telle que pour tous i et j distincts dans $[1, m]$, $b(e_i, e_j) = 0$.

1.c. En déduire qu'il existe une matrice diagonale $D \in M_m(\mathbb{Z}/p\mathbb{Z})$ et une matrice inversible $P \in GL_m(\mathbb{Z}/p\mathbb{Z})$ telles que $S = {}^tPDP$.

2) Dans cette question **2**, on prend $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$ et on considère la forme bilinéaire b définie pour X et Y dans V par $b(X, Y) = {}^tXSY$.

Montrer que pour tout n entier strictement positif et tout T élément de $S_n(\mathbb{Z}/p\mathbb{Z})$, $A_p(S, T)$ est le nombre de n -uplets (v_1, \dots, v_n) d'éléments de V vérifiant $b(v_i, v_j) = t_{i,j}$ pour tous i et j dans $[1, n]$.

3) Vérifier que pour toutes matrices P de $GL_m(\mathbb{Z}/p\mathbb{Z})$ et Q de $GL_n(\mathbb{Z}/p\mathbb{Z})$, on a

$$A_p(S, T) = A_p({}^tPSP, {}^tQTQ).$$

4) Soit ϕ la fonction indicatrice d'Euler qui à un entier r strictement positif associe le nombre d'entiers de $[1, r]$ premiers à r .

4.a. Montrer que pour tout entier r strictement positif, $\sum_{d|r} \phi(d) = r$, la somme étant étendue à tous les entiers strictement positifs d diviseurs de r .

4.b. Soit K un corps fini commutatif à q éléments. Démontrer que pour tout entier strictement positif d diviseur de $q - 1$, l'ensemble des éléments de K^\times d'ordre divisant d est de cardinal au plus d .

4.c. En déduire que pour tout entier strictement positif d diviseur de $q - 1$, K^\times possède 0 ou $\phi(d)$ éléments d'ordre exactement d .

4.d. En déduire que K^\times est cyclique.

A.III Le cas $n = 1$

Soit $n = 1$; on a alors $T = t \in \mathbb{Z}/p\mathbb{Z}$ et $2st \neq 0$ où l'on rappelle que $s = \det S$.

Soit $\omega = \exp\left(\frac{2i\pi}{p}\right)$ une racine primitive p -ième de l'unité (on a $\omega \in \mathbb{C}^\times$).

Pour $\alpha \in \mathbb{Z}$, le nombre complexe ω^α ne dépend que de la classe a de α modulo p ; on le note ω^a : on admettra que l'on définit ainsi un morphisme $a \mapsto \omega^a$ du groupe additif $\mathbb{Z}/p\mathbb{Z}$ dans le groupe multiplicatif \mathbb{C}^\times .

Pour $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, on pose $\left(\frac{a}{p}\right) = 1$ s'il existe $b \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $a = b^2$, et $\left(\frac{a}{p}\right) = -1$ sinon. Ces notations seront utilisées dans toute la suite de la partie **A**.

1.a. Montrer qu'il y a dans $(\mathbb{Z}/p\mathbb{Z})^\times$ autant de carrés que de non carrés et que $a \mapsto \left(\frac{a}{p}\right)$ est un morphisme de groupes multiplicatifs $(\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$.

1.b. Pour $b \in \mathbb{Z}/p\mathbb{Z}$ calculer $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ab}$.

1.c. Pour $c \in (\mathbb{Z}/p\mathbb{Z})^\times$, on pose $G_c = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ca^2}$ et $H_c = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) \omega^{ca}$.

Démontrer qu'on a $G_c = H_c = \left(\frac{c}{p}\right) \cdot G_1$.

Dans ce qui suit, G_1 sera noté G .

2.a. Montrer que $pA_p(S, t) = \sum_{a, X} \omega^{a(tXSX-t)}$ où a parcourt $\mathbb{Z}/p\mathbb{Z}$ et X parcourt $M_{m,1}(\mathbb{Z}/p\mathbb{Z})$.

2.b. Soit D une matrice diagonale inversible élément de $M_m(\mathbb{Z}/p\mathbb{Z})$, de termes diagonaux s_1, \dots, s_m . Montrer que

$$pA_p(D, t) = p^m + \left(\frac{\det D}{p}\right) \cdot G^m \cdot \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right)^m \omega^{-at}$$

2.c. Montrer que $G^2 = \left(\frac{-1}{p}\right) \cdot p$.

Indication : On pourra appliquer à un cas particulier le résultat démontré dans la question précédente.

3) Pour $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ et k entier naturel on pose $\varepsilon_k^{(p)}(a) = \left(\frac{(-1)^{k/2}a}{p}\right)$ si k est pair et $\varepsilon_k^{(p)}(a) = 0$ sinon.

Cette notation sera utilisée dans la suite du problème.

3.a. Montrer qu'on a l'égalité :

$$A_p(S, t) = \begin{cases} p^{m-1} (1 - \varepsilon_m^{(p)}(s) p^{-m/2}) & \text{si } m \text{ est pair} \\ p^{m-1} (1 + \varepsilon_{m-1}^{(p)}(st) p^{(1-m)/2}) & \text{si } m \text{ est impair} \end{cases}$$

3.b. Préciser pour quelles valeurs de m , s et t la quantité $A_p(S, t)$ s'annule.

A.IV Le cas n quelconque

Dans cette section, on suppose $m \geq n$.

1) Soit $n \geq 2$; soit $T \in S_n(\mathbb{Z}/p\mathbb{Z})$ de déterminant $t \in (\mathbb{Z}/p\mathbb{Z})^\times$. Supposons $T = \begin{pmatrix} \delta & 0 \\ 0 & T_1 \end{pmatrix}$ avec $\delta \in (\mathbb{Z}/p\mathbb{Z})^\times$ et $T_1 \in S_{n-1}(\mathbb{Z}/p\mathbb{Z})$ inversible de déterminant t_1 .

1.a. Montrer que l'application qui à $X \in \mathcal{A}_p(S, T)$ fait correspondre sa première colonne induit une application γ de $\mathcal{A}_p(S, T)$ dans $\mathcal{A}_p(S, \delta)$.

1.b. Soit $C_1 \in \mathcal{A}_p(S, \delta)$. Montrer qu'il existe une matrice symétrique inversible S_1 dans $M_{m-1}(\mathbb{Z}/p\mathbb{Z})$ dont le déterminant s_1 vérifie $\left(\frac{\delta s_1}{p}\right) = \left(\frac{s}{p}\right)$, et telle que $\gamma^{-1}(C_1)$ soit de cardinal $A_p(S_1, T_1)$.

Indication : On pourra utiliser l'interprétation de la question 2 du Préliminaire en introduisant l'orthogonal W du vecteur C_1 pour la forme b de matrice S dans la base canonique de $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$.

2.a. En procédant par récurrence sur n , montrer que

$$A_p(S, T) = p^{mn-n(n+1)/2} \psi_{p,m,n}(s, t) \prod_{m-n < 2k < m} \left(1 - \frac{1}{p^{2k}}\right)$$

où

$$\psi_{p,m,n}(s, t) = \left(1 - \varepsilon_m^{(p)}(s)p^{-m/2}\right) \left(1 + \varepsilon_{m-n}^{(p)}(st)p^{(n-m)/2}\right)$$

2.b. À quelles conditions $A_p(S, T)$ est-il nul ?

B. Matrices à coefficients dans l'anneau $\mathbb{Z}/q\mathbb{Z}$

Soit q un entier naturel strictement positif; on note π_q le morphisme canonique d'anneaux $\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$ et, si q' est un entier naturel strictement positif multiple de q , $\pi_{q,q'}$ le morphisme canonique d'anneaux $\mathbb{Z}/q'\mathbb{Z} \rightarrow \mathbb{Z}/q\mathbb{Z}$. On pourra remarquer l'égalité $\pi_{q,q'} \circ \pi_{q'} = \pi_q$. Si n et m sont des entiers strictement positifs et M un élément de $M_{m,n}(\mathbb{Z})$, on note aussi $\pi_q(M)$ la matrice élément de $M_{m,n}(\mathbb{Z}/q\mathbb{Z})$ dont les coefficients sont les images par π_q des coefficients de M ; on définit de manière analogue $\pi_{q,q'}(M)$ si q' est un multiple de q et si M est élément de $M_{m,n}(\mathbb{Z}/q'\mathbb{Z})$. On considérera comme évidentes les propriétés des applications π_q et $\pi_{q,q'}$ relativement à la somme des matrices, au produit d'une matrice par un scalaire, au produit des matrices, à la transposition des matrices et au déterminant.

On dira que les matrices M_1 et M_2 de même taille et à coefficients dans \mathbb{Z} , resp. $\mathbb{Z}/q'\mathbb{Z}$, sont congrues modulo q si $\pi_q(M_1) = \pi_q(M_2)$, resp. si q divise q' et $\pi_{q,q'}(M_1) = \pi_{q,q'}(M_2)$; cette relation sera notée $M_1 \equiv M_2 \pmod{q}$.

Dans ce qui suit, m et n représentent deux entiers strictement positifs tels que $m \geq n$ et S et T deux matrices symétriques, $S \in S_m(\mathbb{Z})$ et $T \in S_n(\mathbb{Z})$, de déterminants respectifs s et t non nuls. Pour tout entier naturel impair q premier avec st , on pose

$$\mathcal{A}_q(S, T) = \{X \in M_{m,n}(\mathbb{Z}/q\mathbb{Z}) \mid {}^t X \pi_q(S) X = \pi_q(T)\}$$

et on note $A_q(S, T)$ le cardinal de cet ensemble. Pour $a \in \mathbb{Z}$ et p premier impair, on pose $\chi_a(p) = 0$ si p divise a , $\chi_a(p) = 1$ si a est un carré non nul modulo p , et sinon $\chi_a(p) = -1$.

1) Soit q un entier strictement positif quelconque.

1.a. On suppose $q = q_1 q_2$, où q_1 et q_2 sont premiers entre eux.

Montrer que l'application $X \mapsto (\pi_{q_1, q}(X), \pi_{q_2, q}(X))$ établit une bijection entre

$$M_{m,n}(\mathbb{Z}/q\mathbb{Z}) \text{ et } M_{m,n}(\mathbb{Z}/q_1\mathbb{Z}) \times M_{m,n}(\mathbb{Z}/q_2\mathbb{Z}).$$

1.b. Montrer que la bijection trouvée au 1.b induit une bijection entre

$$\mathcal{A}_q(S, T) \text{ et } \mathcal{A}_{q_1}(S, T) \times \mathcal{A}_{q_2}(S, T).$$

1.c. On suppose $q = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ où p_1, \dots, p_r sont des nombres premiers impairs deux à deux distincts et $\alpha_1, \dots, \alpha_r$ sont des entiers strictement positifs. Pour tout i dans $[1, r]$, on pose $q_i = p_i^{\alpha_i}$. Démontrer que

$$A_q(S, T) = \prod_{i=1}^r A_{q_i}(S, T)$$

2) Dans cette question p désigne un nombre premier impair premier avec st et α est un entier naturel ≥ 1 . On considère une matrice $X \in M_{m,n}(\mathbb{Z})$ telle que $\pi_{p^\alpha}(X) \in \mathcal{A}_{p^\alpha}(S, T)$ et on pose $\tilde{X} = \pi_p(X)$ et $\tilde{S} = \pi_p(S)$.

2.a. Montrer que l'application $u : H \mapsto {}^t \tilde{X} \tilde{S} H$, est une application $\mathbb{Z}/p\mathbb{Z}$ -linéaire surjective $M_{m,n}(\mathbb{Z}/p\mathbb{Z})$ dans $M_n(\mathbb{Z}/p\mathbb{Z})$.

2.b. Montrer que l'application $v : H \mapsto {}^t \tilde{X} \tilde{S} H + {}^t H \tilde{S} \tilde{X}$ est une application $\mathbb{Z}/p\mathbb{Z}$ -linéaire surjective de $M_{m,n}(\mathbb{Z}/p\mathbb{Z})$ dans $S_n(\mathbb{Z}/p\mathbb{Z})$.

2.c. Montrer que le cardinal du noyau de l'application linéaire de la question précédente est $p^{mn - \frac{n(n+1)}{2}}$.

3) Montrer qu'il existe une matrice U dans $M_{m,n}(\mathbb{Z})$ telle que la matrice $Y = X + p^\alpha U$ de $M_{m,n}(\mathbb{Z})$ satisfasse $\pi_{p^{\alpha+1}}(Y) \in \mathcal{A}_{p^{\alpha+1}}(S, T)$.

4) Dédurre de ce qui précède que l'application

$$\pi_{p^\alpha, p^{\alpha+1}} : M_{m,n}(\mathbb{Z}/p^{\alpha+1}\mathbb{Z}) \rightarrow M_{m,n}(\mathbb{Z}/p^\alpha\mathbb{Z})$$

induit une application $r_\alpha : \mathcal{A}_{p^{\alpha+1}}(S, T) \rightarrow \mathcal{A}_{p^\alpha}(S, T)$ surjective, et que les cardinaux des images réciproques par r_α des singletons valent tous $p^{mn - \frac{n(n+1)}{2}}$.

5) Déterminer $A_{p^\alpha}(S, T)$ pour tout $\alpha \geq 1$.

6) Soit q un entier naturel impair ≥ 1 premier avec st .

6.a. Exprimer $A_q(S, T)$ en fonction de m, n, s, t, q et des facteurs premiers de q .

6.b. À quelle condition $A_q(S, T)$ est-il nul ?

7) On note \mathcal{P} l'ensemble des nombres premiers ne divisant pas $2st$; pour tout entier h strictement positif, on pose $\mathcal{P}_h = \mathcal{P} \cap [1, h]$ et on note q_h le produit des éléments de \mathcal{P}_h . On fixe $m \geq 1$ et $n \geq 1$ de sorte que $m > n + 2$.

7.a. Montrer que la suite $\left(A_{q_h}(S, T) / q_h^{mn - \frac{n(n+1)}{2}} \right)_{h \geq 1}$ a une limite finie strictement positive.

7.b. Soit $Q_h = \prod_{p \in \mathcal{P}_h} p^h = q_h^h$.

Montrer que la suite $\left(A_{Q_h}(S, T) / Q_h^{mn - \frac{n(n+1)}{2}} \right)_{h \geq 1}$ a une limite finie strictement positive.

A.I

1) Si $s = -\alpha^2$ avec $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$, on a $x^2 + sy^2 = (x - \alpha y)(x + \alpha y)$. Comme p est impair, la matrice $\begin{pmatrix} 1 & -\alpha \\ 1 & \alpha \end{pmatrix}$ est inversible. Donc pour tout $t \in (\mathbb{Z}/p\mathbb{Z})^\times$, l'ensemble $\mathcal{A}_p(S, t)$ est en bijection avec $\{(u, v) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times; uv = t\}$ par $(x, y) \mapsto (x - \alpha y, x + \alpha y)$. Ce dernier ensemble est de cardinal $p - 1$; on a donc $A_p(S, t) = p - 1$.

2.a. Un polynôme de degré deux à coefficients dans un corps commutatif est irréductible si et seulement si il n'a pas de racine dans ce corps. Ici, $X^2 + s$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$. Le choix d'une racine de $X^2 + s$ dans K fournit un homomorphisme surjectif et injectif d'anneaux $\mathbb{Z}/p\mathbb{Z}[X]/(X^2 + s) \rightarrow K$. Le terme de gauche est un espace vectoriel de dimension 2 sur $\mathbb{Z}/p\mathbb{Z}$ (de base $\{1, \overline{X}\}$ où \overline{X} désigne la classe de X modulo $(X^2 + s)$). Le corps K est donc d'ordre p^2 .

2.b. On a $F(0) = 0$, $F(1) = 1$ et $F : K^\times \rightarrow K^\times$ est un homomorphisme de groupes multiplicatifs. Pour voir que F est additif, il suffit de noter par la formule du binôme de Newton que les coefficients binomiaux $\binom{p}{i}$ ($i = 1, \dots, p-1$) sont divisibles par p . C'est clair car $i! \cdot (p-i)! \binom{p}{i} = p!$ est divisible par p . Comme les deux premiers facteurs sont premiers à p , c'est que p divise le troisième. Ainsi F est un homomorphisme de corps. Tout homomorphisme de corps est injectif. Comme K est fini, F est donc bijectif. On a $F \circ F(z) = z^{p^2}$. Comme K^\times est un groupe d'ordre $p^2 - 1$, on a pour tout $z \in K^\times$, $z^{p^2-1} = 1$, donc $z^{p^2} = z$. Cette relation est aussi satisfaite par 0, donc on a $F \circ F = Id_K$.

Si $z^p = z$, z est racine du polynôme $X^p - X$ de degré p . Par le petit théorème de Fermat, ce polynôme a exactement p racines. Le noyau de $F - Id_K$ est donc $\mathbb{Z}/p\mathbb{Z}$.

2.c. Soit $\alpha \in K$ une racine de $X^2 + s$. $F(\alpha)$ est encore racine de $X^2 + s$ car $s \in \mathbb{Z}/p\mathbb{Z}$ est fixé par F . Comme $\alpha \notin \mathbb{Z}/p\mathbb{Z}$, on a $F(\alpha) \neq \alpha$. Comme l'autre racine est $-\alpha$, on a $F(\alpha) = -\alpha$.

3.a. On a $N(z) = zF(z)$. C'est donc un homomorphisme multiplicatif de K^\times dans lui-même. De plus $(N(z))^p = z^{p^2+p} = z^{1+p} = N(z)$ car $F \circ F = Id_K$. Ainsi, $N(z) \in (\mathbb{Z}/p\mathbb{Z})^\times$.

3.b. Si $N(z) = 1$, z est racine de $X^{p+1} - 1$; ainsi l'ordre de $\text{Ker } N$ est au plus $p + 1$ et celui de $\text{Im } N$ au plus $p - 1$. Comme celui de K^\times est $(p - 1)(p + 1)$, on tire de l'isomorphisme $K^\times / \text{Ker } N \cong \text{Im } N$ que $\text{Card Ker } N = p + 1$ et $\text{Card Im } N = p - 1$.

3.c. On a $N(x + y\alpha) = (x + y\alpha)F(x + y\alpha) = (x + y\alpha)(x - y\alpha) = x^2 - y^2\alpha^2 = x^2 + sy^2$.

4) Notons qu'étant donnés deux éléments x, y de $\mathbb{Z}/p\mathbb{Z}$, on a $x + y\alpha \in K^\times$ si et seulement si x et y sont non-nuls. On peut donc écrire $\mathcal{A}_p(S, t) = \{z \in K^\times; N(z) = t\}$. Choisissons $z_0 \in K^\times$ tel que $N(z_0) = t$. On a alors $N(z) = t$ si et seulement si $N(zz_0^{-1}) = 1$, c'est-à-dire $zz_0^{-1} \in \text{Ker } N$. Ainsi $z \mapsto zz_0^{-1}$ est une bijection de $\mathcal{A}_p(S, t)$ vers $\text{Ker } N$. L'ordre de $\mathcal{A}_p(S, t)$ est donc $p + 1$ par 3.b.

A.II

1.a. On a $b(x, y) = \frac{1}{2}[b(x + y, x + y) - b(x, x) - b(y, y)]$. Si donc $b(t, t) = 0$ pour tout vecteur t , on a $b = 0$.

1.b. On raisonne par récurrence sur la dimension de V . Si $b = 0$ il n'y a rien à démontrer. Sinon, on prend $e_1 \in V$ tel que $b(e_1, e_1) \neq 0$. La relation $x = x - \frac{b(e_1, x)}{b(e_1, e_1)} \cdot e_1 + \frac{b(e_1, x)}{b(e_1, e_1)} \cdot e_1$ montre que V est somme directe de la droite engendrée par e_1 et de son orthogonal V_1 . On applique alors l'hypothèse de récurrence à V_1 pour conclure.

1.c. On prend $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$ et $b(X, Y) = {}^tXSY$. Soit P l'inverse de la matrice d'une base orthogonale de b . On a $S = {}^tPDP$ où D est diagonale.

2) La relation ${}^tXSX = T$ signifie pour tout i, j $b(v_i, v_j) = t_{i,j}$.

3) L'application

$$\mathcal{A}_p(S, T) \rightarrow \mathcal{A}_p({}^tPSP, {}^tQTQ), \quad X \mapsto P^{-1}XQ$$

est bijective.

4.a. On partitionne l'intervalle $[1, r]$ de \mathbb{Z} en les sous-ensembles $\Phi(d)$ constitués des entiers dont le plus grand commun diviseur avec r est r/d , d parcourant l'ensemble des diviseurs positifs de r . La multiplication par r/d établit une bijection de $\Phi(d)$ avec l'ensemble des entiers premiers à d dans $[1, d]$. Son ordre est $\phi(d)$. On a donc $r = \sum_{d|r} \phi(d)$.

4.b. Un élément $x \in K^\times$ est d'ordre divisant d si et seulement si il est racine du polynôme de degré d $X^d - 1$. Il y a donc au plus d tels éléments dans K^\times .

4.c. Si K^\times possède un élément x d'ordre d (diviseur $q - 1$), il possède au moins d éléments d'ordre divisant d . Il en possède au plus d par la question précédente, donc exactement d , qui forment un groupe cyclique engendré par x . L'ensemble $(K^\times)_d$ des éléments d'ordre exactement d est donc d'ordre $\phi(d)$.

4.d. Si pour un diviseur d de $q - 1$ il n'y a pas d'élément d'ordre d (i.e. $(K^\times)_d = \emptyset$), on a $q - 1 = \text{Card } K^\times = \sum_{\delta|q-1} \text{Card } (K^\times)_\delta < \sum_{\delta|q-1} \phi(\delta) = q - 1$, ce qui est une contradiction.

A.III

1.a. L'homomorphisme $(\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^2$ a pour noyau $\{\pm 1\}$. Son image est donc d'indice 2 dans $(\mathbb{Z}/p\mathbb{Z})^\times$. C'est dire qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Soit a un non carré, tout non carré peut s'écrire ax^2 . Ainsi le produit de deux non carrés est un carré (et le produit d'un carré par un non carré est un non-carré, et le produit de deux carrés est un carré). Ceci montre que $x \mapsto \left(\frac{a}{p}\right)$ est un homomorphisme.

1.b. Si $b \in (\mathbb{Z}/p\mathbb{Z})^\times, a \mapsto ab$ est bijective, donc $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ab} = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^a = \frac{\omega^p - 1}{\omega - 1} = 0$. Si $b = 0$, on a $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ab} = p$.

1.c. On a $G_c = 1 + 2 \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ca}$. D'autre part, $H_c = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ca} - \sum_{a \notin (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ca}$. Comme $c \in (\mathbb{Z}/p\mathbb{Z})^{\times}$, on a $\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{ac} = 0 = 1 + \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} + \sum_{a \notin (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac}$, donc $1 + \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} = - \sum_{a \notin (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac}$. Ainsi, $H_c = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} + 1 + \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}} \omega^{ac} = G_c$.

2.a. Par 1.b, la somme $\frac{1}{p} \sum_{a \in (\mathbb{Z}/p\mathbb{Z})} \omega^{ab}$ vaut 1 ou 0 suivant que b est nul ou pas. Donc $pA_p(S, t) = \sum_{X \in M_{m,1}(\mathbb{Z}/p\mathbb{Z})} \frac{1}{p} \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{a(tXSX-t)}$. D'où la formule annoncée.

2.b. On a ${}^tXDX = \sum_{i=1}^m s_i x_i^2$ donc $\omega^{a({}^tXDX-t)} = \omega^{as_1 x_1^2} \dots \omega^{as_m x_m^2} \omega^{-at}$ et $pA_p(S, t) = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \omega^{-at} \left(\sum_{x_1 \in \mathbb{Z}/p\mathbb{Z}} \omega^{as_1 x_1^2} \right) \dots \left(\sum_{x_m \in \mathbb{Z}/p\mathbb{Z}} \omega^{as_m x_m^2} \right)$

La contribution du terme $a = 0$ vaut p^m . De plus, on a pour chaque $i = 1, \dots, m$. $\sum_{x_i \in \mathbb{Z}/p\mathbb{Z}} \omega^{as_i x_i^2} = G_{as_i} = \left(\frac{as_i}{p}\right)G$. Donc $pA_p(S, t) = p^m + \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} \left(\frac{as_1}{p}\right) \dots \left(\frac{as_m}{p}\right)G$ et comme $\left(\frac{s_1}{p}\right) \dots \left(\frac{s_m}{p}\right) = \left(\frac{D}{p}\right)$, on a : $pA_p(S, t) = p^m + G^m \left(\frac{D}{p}\right) \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} \left(\frac{a}{p}\right)^m$.

2.c. Prenons $m = 1$, $s_1 = 1$ et $t = 1$. On a $A_p(S, 1) = 2$ donc comme $G_{-1} = \left(\frac{-1}{p}\right)G$, on a $2p = p + G\left(\frac{-1}{p}\right)G$, soit $p = G^2\left(\frac{-1}{p}\right)$, ou encore $G^2 = \left(\frac{-1}{p}\right)p$.

3.a. Pour S symétrique non-dégénérée quelconque, on applique A.II 1.c et 3 pour se ramener à S diagonale, de déterminant $s_1 \dots s_m = s$. On obtient donc $pA(S, t) = p^m + \left(\frac{s}{p}\right)G^m \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} \left(\frac{a}{p}\right)^m$.

Si $m = 2r$, on a $G^m \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} \left(\frac{a}{p}\right)^m = -\left(\frac{-1}{p}\right)^r p^r$, donc $pA(S, t) = p^m \left(1 - \left(\frac{(-1)^{m/2} s}{p}\right) p^{-m/2}\right)$ d'où la formule annoncée.

Si $m = 2r + 1$, on a $G^m \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^{\times}} \omega^{-at} \left(\frac{a}{p}\right)^m = \left(\frac{-t}{p}\right)G^{m+1} = \left(\frac{-t}{p}\right)\left(\frac{-1}{p}\right)^{r+1} p^{r+1}$ donc $pA(S, t) = p^m \left(1 + \left(\frac{(-1)^{(m-1)/2} st}{p}\right) p^{(1-m)/2}\right)$. D'où la formule annoncée.

3.b. Le seul cas de nullité intervient lorsque $m = 1$ et lorsque st n'est pas un carré.

A.IV

1.a. On écrit $X = (C_1, X_1)$ où C_1 est un vecteur colonne et $X_1 \in M_{m, n-1}(\mathbb{Z}/p\mathbb{Z})$. Alors un calcul par blocs montre que ${}^tXSX = T$ équivaut à ${}^tC_1SC_1 = \delta$, ${}^tX_1SX_1 = T_1$ et ${}^tC_1SX_1 = 0$. L'application $X \mapsto C_1$ induit donc en particulier une application $\gamma : \mathcal{A}(S, T) \rightarrow \mathcal{A}(S, \delta)$.

1.b. Soit W l'orthogonal de C_1 dans l'espace quadratique $V = M_{m,1}(\mathbb{Z}/p\mathbb{Z})$ muni de $b(v, w) = {}^t v S w$. Soit $(v_i)_{i=2, \dots, m}$ une base de W . Soit $S_1 = (b(v_i, v_j))_{2 \leq i, j \leq m}$ la matrice de b dans cette base. Soit $T_1 = (t_{i,j})_{2 \leq i, j \leq n}$. Par la question précédente, on peut réécrire l'ensemble $\gamma^{-1}(C_1)$ comme

$$\{(w_2, \dots, w_n) \in W^{n-1}; b(w_i, w_j) = t_{i,j} \text{ pour tout } i, j \in [2, m]\}$$

Soit $X'_1 \in M_{m-1, n-1}(\mathbb{Z}/p\mathbb{Z})$ la matrice des coordonnées des vecteurs colonnes w_j dans la base des v_i . On peut réécrire l'ensemble $\gamma^{-1}(C_1)$ comme

$$\mathcal{A}(S_1, T_1) = \{X'_1 \in M_{m-1, n-1}(\mathbb{Z}/p\mathbb{Z}); {}^t X'_1 S_1 X'_1 = T_1\}$$

Soit P la matrice de la base (v_1, \dots, v_m) . On a

$$\begin{pmatrix} \delta & 0 \\ 0 & S_1 \end{pmatrix} = {}^t P S P$$

Donc si $s_1 = \det S_1$, on a $\delta s_1 = s(\det P)^2$ et $(\frac{\delta s_1}{p}) = (\frac{s}{p})$.

2.a. Pour $n = 1$, vue la convention sur les cas de nullité de $\varepsilon_k^{(p)}(a)$, les formules pour $A_p(S, t)$ distinguant m pair ou impair peuvent être synthétisées en la seule formule $A_p(S, t) = p^{m-1} \psi_{p,m,1}(s, t)$. Si le résultat est vrai pour $n - 1$, soit $T \in S_n(\mathbb{Z}/p\mathbb{Z})$; quitte à remplacer T par ${}^t Q T Q$, ce qui ne change pas $A_p(S, T)$ par A.II.3, on peut supposer T diagonale (et en particulier de la forme de la question 1.2 ci-dessus. Avec les notations de la question 1.b, on a $A_p(S, T) = A_p(S, \delta) A_p(S_1, T_1)$. Par hypothèse de récurrence, $A_p(S_1, T_1) = p^{(m-1)(n-1) - (n-1)n/2} \psi_{p,m-1,n-1}(s_1, t_1) \prod_{m-n+1 < 2k < m} (1 - \frac{1}{p^{2k}})$. et $A_p(S, \delta) = p^{m-1} \psi_{p,m,1}(s, \delta)$. Trai-

tons par exemple le cas où m et n sont pairs. On observe que

- $(m-1)(n-1) - n(n-1)/2 + (m-1) = mn - n(n+1)/2$
 - $\psi_{p,m,1}(s, \delta) = 1 - (\frac{(-1)^{m/2} s}{p}) p^{-m/2}$ et
 - $\psi_{p,m-1,n-1}(s_1, t_1) = 1 + (\frac{(-1)^{(m-n)/2} s_1 t_1}{p}) p^{(n-m)/2}$, et comme par la question 1.2 on a $s_1 t_1 \delta^2 = s t u^2$, on trouve $\psi_{p,m,1}(s, \delta) \psi_{p,m-1,n-1}(s_1, t_1) = \psi_{p,m,n}(s, t)$. Comme on a aussi
 - $\prod_{m-n < 2k < m} (1 - \frac{1}{p^{2k}}) = \prod_{m-n+1 < 2k < m} (1 - \frac{1}{p^{2k}})$
- on voit donc en multipliant $A_p(S, \delta)$ et $A_p(S_1, T_1)$ que

$$A_p(S, T) = p^{mn - n(n+1)/2} \psi_{p,m,n}(s, t) \prod_{m-n < 2k < m} (1 - \frac{1}{p^{2k}})$$

comme annoncé. Les autres cas se traitent de même.

2.b. Le seul cas de nullité de $A_p(S, T)$ se produit lorsque $m = n$ et que st n'est pas un carré.

B.

1.a. et **1.b.** se traitent simultanément en observant que, lorsque q_1 et q_2 sont premiers entre eux, le lemme chinois induit un isomorphisme d'anneaux $M_{m,n}(\mathbb{Z}/q_1 q_2 \mathbb{Z}) \cong M_{m,n}(\mathbb{Z}/q_1 \mathbb{Z}) \times M_{m,n}(\mathbb{Z}/q_2 \mathbb{Z})$.

1.c. est immédiat à partir des questions ci-dessus.

2.a. Soit $\tilde{T} = \pi_p(T)$. Soit $H_1 \in M_n(\mathbb{Z}/p\mathbb{Z})$. Soit $H_2 \in M_n(\mathbb{Z}/p\mathbb{Z})$ telle que $H_1 = \tilde{T}H_2$; posons $H = \tilde{X}H_2 \in M_{m,n}(\mathbb{Z}/p\mathbb{Z})$. On a ${}^t\tilde{X}\tilde{S}H = {}^tX\tilde{S}\tilde{X}H_2 = \tilde{T}H_2 = H_1$.

2.b. Comme p est impair, toute matrice symétrique $H_1 \in S_n(\mathbb{Z}/p\mathbb{Z})$ s'écrit $H_2 + {}^tH_2$ pour une matrice $H_2 \in M_n(\mathbb{Z}/p\mathbb{Z})$; par la question précédente, il existe $H \in M_{m,n}(\mathbb{Z}/p\mathbb{Z})$ tel que ${}^t\tilde{X}\tilde{S}H = H_2$. Ceci montre la surjectivité de $H \mapsto {}^t\tilde{X}\tilde{S}H + {}^tH\tilde{S}\tilde{X}$.

2.c. Le noyau de l'application ci-dessus est de dimension $mn - n(n+1)/2$. Donc son cardinal est $p^{mn-n(n+1)/2}$.

3) On abrège $\pi_{p^\alpha}(X) = X_\alpha$. Si ${}^tX_\alpha S_\alpha X_\alpha = T_\alpha$, posons $Y = X + p^\alpha U$. Cherchons $U \in M_{m,n}(\mathbb{Z})$ de sorte que ${}^tY S Y \equiv T \pmod{p^{\alpha+1}}$. On peut réécrire cette relation comme ${}^t(X + p^\alpha U)S(X + p^\alpha U) \equiv T \pmod{p^{\alpha+1}}$, ou encore, en posant ${}^tX S X = T + p^\alpha \Theta : {}^tU S X + {}^tX S U \equiv \Theta \pmod{p}$. Par la question 2.2, cette congruence a une solution $U \in M_{m,n}(\mathbb{Z})$.

4) Étant donnée $X \in M_{m,n}(\mathbb{Z})$ telle que ${}^tX S X \equiv T \pmod{p^\alpha}$, l'ensemble $\{\pi_p(U) \in M_{m,n}(\mathbb{Z}/p\mathbb{Z}); {}^tU S X + {}^tX S U \equiv \Theta \pmod{p}\}$ est une variété linéaire affine de direction de dimension $mn - n(n+1)/2$. C'est donc un ensemble d'ordre $p^{mn-n(n+1)/2}$. Ainsi, r_α est surjective et l'image inverse de chaque singleton est d'ordre $p^{mn-n(n+1)/2}$.

5) On en déduit que

$$A_{p^\alpha} = p^{(\alpha-1)(mn-n(n+1)/2)} p^{mn-n(n+1)/2} \psi_{p,m,n}(s, t) \prod_{m-n < 2k < m} \left(1 - \frac{1}{p^{2k}}\right) =$$

$$p^{\alpha(mn-n(n+1)/2)} \psi_{p,m,n}(s, t) \prod_{m-n < 2k < m} \left(1 - \frac{1}{p^{2k}}\right).$$

6.a. On a

$$A_q(S, T) = A_{p_1^{\alpha_1}}(S, T) \dots A_{p_r^{\alpha_r}}(S, T) = q^{\alpha(mn-n(n+1)/2)} \prod_i \psi_{p_i, m, n}(s, t) \prod_{m-n < 2k < m} \left(1 - \frac{1}{p_i^{2k}}\right)$$

6.b. La nullité de $A_q(S, T)$ ne se produit que lorsque $m = n$ et que st n'est pas un carré modulo l'un des facteurs premiers de q .

7.a. On a $A_{q_h}(S, T)/q_h^{mn-n(n+1)/2} = \prod_i \psi_{p_i, m, n}(s, t) \prod_{m-n < 2k < m} \left(1 - \frac{1}{p_i^{2k}}\right)$ On a $m > n + 2$ donc en particulier $m/2 > 3/2$ et $(m-n)/2 > 1$; donc les produits infinis $\prod_i \left(1 - \left(\frac{(-1)^{m/2} s}{p_i}\right) p_i^{-m/2}\right)$ et $\prod_i \left(1 - \left(\frac{(-1)^{(m-n)/2} st}{p_i}\right) p_i^{-(m-n)/2}\right)$ sont absolument convergents.

A fortiori les produits $\prod_i \left(1 - \frac{1}{p_i^{2k}}\right)$ pour $2k \in]m-n, m[$. Leur limite sont des nombres strictement positifs. Il en va donc de même pour leur produit fini.

7.b. L'argument est identique car $A_{Q_h}(S, T)/Q_h^{mn-n(n+1)/2} = A_{q_h}(S, T)/q_h^{mn-n(n+1)/2}$

Rapport des correcteurs

Le problème portait sur l'étude, pour deux matrices symétriques S et T à coefficients dans \mathbb{Z} données de tailles respectives m et n , des nombres $A_q(S, T)$ de solutions $X \in M_{m,n}(\mathbb{Z}/q\mathbb{Z})$ de la congruence ${}^tX S X \equiv T \pmod{q}$. On faisait l'hypothèse simplificatrice que les matrices sont définies positives et que q est premier à $2\det S \cdot \det T$.

La partie A concernait le cas où q est premier ; la partie B consistait à déduire le cas général du cas A . La partie $A.I$ proposait de calculer le nombre $A_p(S, T)$ pour $m = 2$ et $n = 1$ en distinguant selon que $-\det S$ est un carré ou non modulo p .

La première question de cette partie a semble-t'il posé problème à de nombreux candidats. Elle reposait sur l'identité remarquable $a^2 - b^2 = (a - b)(a + b)$. Elle a occasionné les dénombrements les plus variés, conduisant parfois à des résultats absurdes. Pour les écrire, il a fallu que le candidat renonce au bon sens dont il aurait fait preuve en physique : une erreur de calcul peut conduire à trouver un cardinal égal à $\frac{p}{2}$ (pour p premier impair), ou à l'infini, pour un ensemble fini. Mais alors, le "bon sens physique", valable aussi en algèbre, aurait pu suggérer une relecture du calcul...

La confusion entre (auto)morphisme de corps, de groupes et d'espaces vectoriels a conduit certains candidats à ne pas vérifier la multiplicativité de F ainsi que la condition $F(1) = 1$, et inversement, elle en a conduit d'autres à vérifier l'additivité de N et à chercher son noyau comme l'ensemble des z tels que $N(z) = 0$.

Il faut essayer de dégager les structures algébriques concernées par les questions avant de se lancer dans les vérifications.

Attention dans 2.c, on ne peut écrire sans précaution $\alpha = i\sqrt{-s}$ (vu que $i \in \mathbb{C}$ et $s \in \mathbb{F}_p$).

Dans $A.I$ et dans $B.1$, on a beaucoup vu d'énoncés de questions copiés. C'est une remarque générale : recopier ou plagier l'énoncé ne rapporte rien !

La première question de $A.II$ a également surpris les correcteurs. On a vu des formes quadratiques définies et positives sur \mathbb{F}_p . La méthode de Gram-Schmidt ne s'applique que dans le contexte d'une forme quadratique réelle définie positive. C'est cependant souvent la méthode choisie pour montrer l'existence d'une base orthogonale dans le cadre du corps \mathbb{F}_p ! Une erreur du même ordre a souvent été le recours à une "diagonalisation" de la forme quadratique avec matrice de passage orthogonale. Cette confusion classique dans le cadre réel de la réduction d'une forme quadratique avec la diagonalisation d'une matrice symétrique devient vraiment absurde sur \mathbb{F}_p car une matrice symétrique n'est même plus nécessairement diagonalisable (comme le montre l'exemple de $\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}$ sur \mathbb{F}_5).

En fait, on traite la question 1.b de $A.I$ par récurrence sur la dimension. Il faut cependant rédiger les récurrences et non se contenter de les amorcer en finissant par un "et ainsi de suite".

Une erreur courante, moins grave certes, est de penser que dans l'écriture $S = {}^tPDP$, la matrice P est la matrice de passage de la base canonique de K^n à la base orthogonale construite, alors que c'est l'inverse.

La cyclicité de K^\times a souvent été mal traitée ; les questions 4.a-4.d occasionnent des réponses floues voire fausses alors que les candidats peuvent penser les avoir traitées correctement.

Certains ont tenté d'adapter une démonstration différente de celle demandée, en général sans succès. Encore une remarque générale : pour obtenir les points d'une question, il s'agit de répondre exactement à la question telle qu'elle est posée, y compris s'il s'agit d'une question de cours.

Le simple bon sens montre qu'on ne répond pas à *A.II.1.b* en citant le théorème du cours affirmant qu'il existe une base orthogonale, de même qu'on ne répond pas à *4.a-4.d* en citant celui qui affirme que K^\times est cyclique !

A.III Le symbole de Legendre et les sommes de Gauss semblaient connus des candidats, mais trop souvent les calculs proposés se sont bornés à une suite d'égalités non justifiées (et parfois erronées, conduisant malgré tout au résultat). Les formules écrites laissent souvent entendre que l'ensemble dans lequel vivent les sommes de Gauss n'est pas clair : on lit souvent que si p divise b , $\sum_a \omega^{ab} = p = 0$ et que $e^{2i\pi/p} \in \mathbb{F}_p$ (!) La réalité est que les sommes de Gauss sont des nombres complexes !

La partie *A.III.3* n'a été abordée que par très peu de candidats.

Dans *A.IV*, seule la première question a été souvent abordée.

Pour la partie *B1*, de nombreuses copies proposaient une démonstration très pénible de l'injectivité. Certains candidats ont montré qu'ils n'avaient pas compris le théorème chinois, qu'ils pouvaient néanmoins citer, puisqu'ils affirmaient que la surjectivité sur le produit résultait de la surjectivité sur chacun des facteurs. En général, seules les questions évidentes du *B.II* ont été abordées. Les autres questions n'ont concerné que quelques candidats.
