

## 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  $1 \times 1$ , 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  $\alpha$  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  $\phi$  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  $\omega^\alpha$  ne dépend que de la classe  $a$  de  $\alpha$  modulo  $p$  ; on le note  $\omega^a$  : 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  $\gamma$  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  $\pi_q$  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  $\pi_q$  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  $\pi_q$  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  $\alpha$  est un entier naturel  $\geq 1$ . 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  $r_\alpha$  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  $\geq 1$  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.

---