

SESSION 2015

AGRÉGATION CONCOURS EXTERNE

Section : MATHÉMATIQUES

COMPOSITION DE MATHÉMATIQUES GÉNÉRALES

Durée : 6 heures

L'usage de tout ouvrage de référence, de tout dictionnaire et de tout matériel électronique (y compris la calculatrice) est rigoureusement interdit.

Dans le cas où un(e) candidat(e) repère ce qui lui semble être une erreur d'énoncé, il (elle) le signale très lisiblement sur sa copie, propose la correction et poursuit l'épreuve en conséquence.

De même, si cela vous conduit à formuler une ou plusieurs hypothèses, il vous est demandé de la (ou les) mentionner explicitement.

NB : La copie que vous rendrez ne devra, conformément au principe d'anonymat, comporter aucun signe distinctif, tel que nom, signature, origine, etc. Si le travail qui vous est demandé comporte notamment la rédaction d'un projet ou d'une note, vous devrez impérativement vous abstenir de signer ou de l'identifier.

Tournez la page S.V.P.

Les calculatrices, téléphones, tablettes, ordinateurs et autres appareils électroniques similaires, ainsi que les documents sont interdits. La qualité de la rédaction sera un facteur important d'appréciation des copies. On invite donc le candidat à produire des raisonnements clairs, complets et concis. Le candidat peut utiliser les résultats énoncés dans les questions ou parties précédentes ; il veillera toutefois à préciser la référence du résultat utilisé.

Introduction, notations et conventions

Pour tout ensemble fini X , $\#X$ désignera le cardinal de X .

On note \mathbf{Z} l'anneau des entiers et \mathbf{N} l'ensemble des entiers positifs. On notera $a \equiv b[n]$ pour signifier que les entiers a et b sont congrus modulo n . L'élément \bar{a}_n de $\mathbf{Z}/n\mathbf{Z}$ sera la classe de a modulo n , que l'on écrira aussi \bar{a} si le contexte s'y prête. On écrira $a \mid b$ pour « a divise b ».

On notera \mathcal{P} l'ensemble des nombres premiers positifs. Pour tout nombre premier p , la p -valuation d'un nombre m est la puissance de p dans la décomposition en facteurs premiers de m . On la notera $\text{val}_p(m)$. Le nombre m sera dit *sans facteur carré*, si $\text{val}_p(m) = 0$ ou 1 pour tout p de \mathcal{P} .

Pour tout p premier, on notera \mathbf{F}_p le corps $\mathbf{Z}/p\mathbf{Z}$.

Soit E un espace vectoriel réel de dimension finie, on notera $\text{GL}(E)$ le groupe des endomorphismes inversibles de E . Si \underline{e} est une base de E , et ϕ un endomorphisme de E , alors $\text{Mat}_{\underline{e}}(\phi)$ sera la matrice de ϕ dans la base \underline{e} . Le déterminant d'un endomorphisme ou d'une matrice sera noté \det .

Si \mathbf{A} est un sous-anneau du corps des réels, $M_n(\mathbf{A})$ sera l'anneau des matrices carrées de taille n à coefficients dans \mathbf{A} . Si M est une matrice de $M_n(\mathbf{A})$, tM désignera sa transposée. On notera $\text{GL}_n(\mathbf{A})$ le groupe des matrices inversibles dans l'anneau $M_n(\mathbf{A})$ et $\text{SL}_n(\mathbf{A})$ le sous-groupe constitué des matrices de déterminant 1.

On rappelle qu'une fonction q de \mathbf{R}^2 dans \mathbf{R} telle que $q(x, y) = ax^2 + bxy + cy^2$, avec a, b, c des réels, est une forme quadratique. La forme quadratique q sera dite *définie positive* si ses valeurs sont strictement positives, sauf pour $(x, y) = (0, 0)$.

Le sujet est composé de cinq parties. Les parties 2 et 3 utilisent la partie 1, mais sont, dans une large mesure, indépendantes entre elles. La partie 4 est indépendante des parties qui précèdent.

1 Généralités sur les formes quadratiques sur \mathbf{R}^2

Dans cette section, E désigne le \mathbf{R} -espace vectoriel \mathbf{R}^2 muni de sa base canonique (e_1, e_2) . On note π une forme bilinéaire symétrique de $E \times E$ vers \mathbf{R} , et $q = q_\pi$, de E dans \mathbf{R} , sa forme quadratique associée définie par $q(u) = \pi(u, u)$, $u \in E$.

1.1

Soit A la matrice de $M_2(\mathbf{R})$ associée à π , et définie par $A = (\pi(e_i, e_j))_{1 \leq i, j \leq 2}$.

1. Démontrer la formule $q(e + f) = q(e) + 2\pi(e, f) + q(f)$.

2. On écrit la matrice A sous la forme

$$A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix},$$

avec a, b, c des réels. Montrer que (a, b, c) est l'unique triplet tel que $q(x, y) = ax^2 + bxy + cy^2$ pour tout (x, y) dans E .

On notera dans la suite A_q (respectivement π_q) la matrice A (respectivement la forme bilinéaire π).

On dira que la forme q est non dégénérée si $\det A_q \neq 0$. On notera également $q = [a, b, c]$.

3. Soit φ dans $GL(E)$. On définit la forme quadratique q' par $q'(e) = q(\varphi(e))$, $e \in E$. Soit P la matrice de φ dans la base (e_1, e_2) , calculer $A_{q'}$ en fonction de P et A_q .

Dans la suite, on dira que deux formes quadratiques q' et q'' de E sont *congruentes* s'il existe φ dans $GL(E)$ tel que $q''(e) = q'(\varphi(e))$ pour tout e dans E .

4. Soit donc $q = [a, b, c]$ fixée et $q' = [a', b', c']$ une forme quadratique sur E de matrice associée $A_{q'}$. Montrer que les conditions suivantes sont équivalentes :

- (i) q et q' sont congruentes,
- (ii) il existe une matrice P de $GL_2(\mathbf{R})$ telle que $A_{q'} = {}^t P A_q P$,
- (iii) il existe une base (f_1, f_2) de E telle que $q(f_1) = a'$, $\pi_q(f_1, f_2) = \frac{b'}{2}$, $q(f_2) = c'$.

On suppose dans la suite de cette section que la forme q est non dégénérée.

Un endomorphisme θ de E est une isométrie pour la forme q si $q(\theta(e)) = q(e)$ pour tout e de E .

5. Soit θ une isométrie pour la forme q et $M = \text{Mat}_{(e_1, e_2)}(\theta)$. Quelles sont les valeurs possibles de $\det(M)$?

On notera $O(q, \mathbf{R})$ le sous-groupe de $GL_2(\mathbf{R})$ formé des matrices $M = \text{Mat}_{(e_1, e_2)}(\theta)$, où θ est une isométrie pour q (on admettra qu'il s'agit bien d'un sous-groupe).

On note $SO(q, \mathbf{R}) = O(q, \mathbf{R}) \cap SL_2(\mathbf{R})$.

Soient q et q' congruentes avec q non dégénérée. On fixe un automorphisme φ tel que $q' = q \circ \varphi$.

6. Donner des conditions nécessaires et suffisantes pour qu'une matrice M de $M_2(\mathbf{R})$ appartienne à $SO(q, \mathbf{R})$ (on donnera ces conditions sous forme matricielle). Expliciter ensuite un isomorphisme entre les groupes $SO(q, \mathbf{R})$ et $SO(q', \mathbf{R})$.

On suppose maintenant q définie positive.

7. Prouver que $SO(q, \mathbf{R})$ est isomorphe au groupe $SO_2(\mathbf{R})$ des rotations de l'espace vectoriel euclidien \mathbf{R}^2 .

8. Montrer qu'il existe un réel $k > 0$ tel que, pour tout e dans E , on ait $q(e) \geq k\|e\|^2$, où $\|\cdot\|$ désigne la norme euclidienne canonique de \mathbf{R}^2 .

1.2

Soit d un entier. On note \mathcal{Q}_d l'ensemble des formes quadratiques définies positives sur E de la forme $q = [a, b, c]$, avec a, b, c dans \mathbf{Z} , tels que $4ac - b^2 = d$. On dira que deux formes quadratiques q et q' sont *proprement équivalentes* s'il existe un endomorphisme φ de E tel que

$$\text{Mat}_{(e_1, e_2)}(\varphi) \in \text{SL}_2(\mathbf{Z}) \text{ et } \forall (x, y) \in E, q'(x, y) = q(\varphi(x, y)).$$

- 1. Montrer que si \mathcal{Q}_d est non vide, alors $d > 0$.
- 2. Montrer que si q' est proprement équivalente à q dans \mathcal{Q}_d , alors $q' \in \mathcal{Q}_d$.
- 3. Montrer que "être proprement équivalente à" définit une relation d'équivalence sur \mathcal{Q}_d .

On notera S_d l'ensemble des classes d'équivalence dans \mathcal{Q}_d pour cette relation. Pour tout q dans \mathcal{Q}_d , on notera $[q]$ sa classe dans S_d . On dira dans la suite que la forme q *représente* l'entier m si l'image réciproque $q^{-1}(m) \cap \mathbf{Z}^2$ de m par q , restreinte à \mathbf{Z}^2 , est non vide.

On fixe deux formes q, q' dans \mathcal{Q}_d .

- 4. On suppose que q et q' sont proprement équivalentes. Établir alors une bijection entre $q^{-1}(m) \cap \mathbf{Z}^2$ et $q'^{-1}(m) \cap \mathbf{Z}^2$.
- 5. Montrer que, pour tout $m \in \mathbf{N}$, $q^{-1}(m) \cap \mathbf{Z}^2$ est fini.

Le but du problème est l'étude de l'équivalence propre des formes sur \mathcal{Q}_d , $d > 0$, ainsi que celle de la représentation des entiers par ces formes.

2 Z-congruence et nombre de classes

Soit d un entier strictement positif. Dans ce problème, on dira que la forme quadratique $[a, b, c]$ de \mathcal{Q}_d est *réduite* si les conditions suivantes sont vérifiées :

$$\begin{aligned} R1 : & b^2 \leq a^2 \leq c^2 \\ R2 : & \text{Si } a^2 = b^2, \text{ alors } b \geq 0. \end{aligned}$$

- 1. Soit k, k' des entiers. Montrer que $4k' - k^2$ est congru à 0 ou à -1 modulo 4.
- 2. Montrer que \mathcal{Q}_d est non vide si et seulement si d est congru à 0 ou à -1 modulo 4.

Dans la suite, d désignera un entier strictement positif congru à 0 ou à -1 modulo 4.

- 3. Après avoir montré que l'équation $x^2 + 5y^2 = 2$ n'a pas de solution entière, déduire que $[1, 0, 5]$ et $[2, 2, 3]$ ne sont pas proprement équivalentes dans \mathcal{Q}_{20} .
- 4. Soit $q = [a, b, c]$ dans \mathcal{Q}_d .
 - (a) Montrer, en utilisant une matrice de $\text{SL}_2(\mathbf{Z})$ bien choisie, que pour tout entier k , il existe un entier c' tel que q soit proprement équivalente à $[a, b + 2ka, c']$.
 - (b) Montrer que $[a, b, c]$ est proprement équivalente à $[c, -b, a]$.

5. Montrer que toute classe de S_d contient une forme réduite.

On pourra montrer que $q = [a, b, c]$ dans \mathcal{Q}_d implique $a, c > 0$, puis commencer par trouver un élément $[a_0, b_0, c_0]$ de $[q]$ vérifiant $-a_0 \leq b_0 \leq a_0$.

6. (a) Montrer que, pour toute forme réduite $q = [a, b, c]$ de \mathcal{Q}_d , on a $b^2 \geq 4b^2 - d$, puis, déduire l'inégalité $0 < a \leq \sqrt{\frac{d}{3}}$.

(b) Montrer que S_d est fini.

7. Calculer $\#S_{20}$, le cardinal de S_{20} .

On définit $SO(q, \mathbf{Z}) = SO(q, \mathbf{R}) \cap SL_2(\mathbf{Z})$.

8. On suppose que la forme quadratique $q = [a, b, c]$ est réduite et que $a < c$.

(a) Montrer que $d > a^2$ et déduire que l'équation $(2ax + by)^2 + dy^2 = 4a^2$ n'a pas de solution entière pour $|y| \geq 2$.

(b) Montrer que si $|y| = 1$, alors $(2ax + by)^2 \geq b^2$ pour tout entier x . En déduire que l'équation ci-dessus n'a aucune solution entière pour $|y| \geq 1$.

(c) En déduire que le groupe $SO(q, \mathbf{Z})$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.

3 Représentabilité d'un entier par une forme

On rappelle que d est un entier strictement positif congru à 0 ou -1 modulo 4.

Pour toute forme quadratique q de \mathcal{Q}_d et tout entier $m > 0$, on notera

$$\mathcal{C}_q(m) = q^{-1}(m) \cap \mathbf{Z}^2 = \{(x, y) \in \mathbf{Z}^2, q(x, y) = m\}, \mathcal{C}_q^1(m) = \{(x, y) \in \mathcal{C}_q(m), \text{pgcd}(x, y) = 1\},$$

de sorte que $\mathcal{C}_q(m)$ est non vide dès que m est représentable par q . Si $\mathcal{C}_q^1(m)$ est non vide, on dira que m est *primitivement représentable* par q .

1. Soit q dans \mathcal{Q}_d . Montrer qu'un entier $m > 0$ est représentable par q si et seulement s'il s'écrit $m'k^2$, où k est un élément de \mathbf{N} et $m' > 0$ un entier primitivement représentable par q .

2. On fixe dans la suite un entier $m > 0$. Soit k, k' deux entiers tels que $k^2 \equiv -d \pmod{4m}$ et $k \equiv k' \pmod{2m}$. Montrer que l'on a $k'^2 \equiv -d \pmod{4m}$. On notera alors, sans ambiguïté :

$$T(d, m) := \{\bar{k} \in \mathbf{Z}/2m\mathbf{Z}, k^2 \equiv -d \pmod{4m}\}.$$

3. On fixe q dans \mathcal{Q}_d , (x, y) dans $\mathcal{C}_q^1(m)$, supposé non vide. Soit (u, v) un couple d'entiers tel que $vx - uy = 1$. On pose $n = 2\pi_q((x, y), (u, v))$. En écrivant la matrice de q dans la base $((x, y), (u, v))$ de \mathbf{R}^2 , montrer l'égalité

$$n^2 - 4mq(u, v) = -d.$$

4. Montrer que l'application ν_q de $\mathcal{C}_q^1(m)$ vers $T(d, m)$ qui, à un couple (x, y) , associe la classe $2\pi_q((x, y), (u, v))$ modulo $2m$, est bien définie. On montrera en particulier qu'elle ne dépend pas du choix du couple (u, v) défini ci-dessus.

5. (a) Soit $\theta \in SO(q, \mathbf{Z})$. Montrer que $\nu_q(\theta(x, y)) = \nu_q(x, y)$, pour tout couple (x, y) de $\mathcal{C}_q^1(m)$.

- (b) Réciproquement, on suppose (x, y) et (x', y') dans $\mathcal{C}_q^1(m)$ tels que $\nu_q(x', y') = \nu_q(x, y)$. Montrer qu'il existe alors un unique θ dans $\text{SO}(q, \mathbf{Z})$ tel que $(x', y') = \theta(x, y)$.
6. Soit n dans \mathbf{Z} tel que $\bar{n} \in T(d, m)$. Montrer qu'il existe un unique entier l tel que $[m, n, l] \in \mathcal{Q}_d$. En posant $q = [m, n, l]$, montrer que $\nu_q(1, 0)$ (à un sens et) est égal à \bar{n} .
7. On fixe q et q' dans \mathcal{Q}_d .
- (a) On suppose ici q et q' proprement équivalentes, avec $\varphi \in \text{SL}_2(\mathbf{Z})$ tel que $q' = q \circ \varphi$. Montrer l'égalité $\nu_q(\varphi(x', y')) = \nu_{q'}(x', y')$, pour tout (x', y') de $\mathcal{C}_{q'}^1(m)$.
- (b) Réciproquement, on suppose $(x, y) \in \mathcal{C}_q^1(m)$, $(x', y') \in \mathcal{C}_{q'}^1(m)$, tels que $\nu_q(x, y) = \nu_{q'}(x', y')$. Montrer que q et q' sont proprement équivalentes.
8. Pour toute classe $[q] \in S_d$, on fixe un représentant q dans \mathcal{Q}_d , et on note R_d l'ensemble des représentants ainsi fixés. Montrer l'égalité

$$\sum_{q \in R_d} \frac{\#\mathcal{C}_q^1(m)}{\#\text{SO}(q, \mathbf{Z})} = \#T(d, m).$$

4 Nombre de solutions d'une équation modulaire

Cette partie est, dans une large mesure, indépendante des précédentes. Elle a pour but de calculer le cardinal de $T(d, m)$.

Soit m un entier impair et v un entier premier à m . On se propose de déterminer le nombre $\mu_v(m)$ de x de $\mathbf{Z}/m\mathbf{Z}$ tels que $x^2 = \bar{v}_m$.

Dans les questions qui suivent (question 1. à question 4.), p est un nombre premier impair positif, α un entier strictement positif et v est un entier premier à p .

- Justifier que l'ordre du groupe $(\mathbf{Z}/p^\alpha\mathbf{Z})^*$ des inversibles de $\mathbf{Z}/p^\alpha\mathbf{Z}$ est égal à $p^{\alpha-1}(p-1)$.
- Dans cette question, $\alpha = 1$.
 - L'application ψ de $(\mathbf{Z}/p\mathbf{Z})^*$ dans lui-même définie par $\psi(x) = x^2$ est clairement un morphisme de groupes. Quel est son noyau ? Quel est le nombre de carrés de $(\mathbf{Z}/p\mathbf{Z})^*$?
 - Montrer que \bar{v}_p est un carré de $(\mathbf{Z}/p\mathbf{Z})^*$ si et seulement si $\bar{v}_p^{\frac{p-1}{2}} = \bar{1}_p$.

Dans la suite, pour tout nombre premier p impair positif, et tout entier a non multiple de p , on notera

$\left(\frac{a}{p}\right)$ le symbole de Legendre (à ne pas confondre avec les coefficients binomiaux) défini par

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } \bar{a}_p \text{ est un carré dans } (\mathbf{Z}/p\mathbf{Z})^* \\ -1 & \text{sinon} \end{cases}.$$

On a donc $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p]$.

- Montrer que, pour tout v non multiple de p , $\mu_v(p) = 1 + \left(\frac{v}{p}\right)$.

4. (a) Soit l'application ϕ de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ qui envoie la classe d'un entier x modulo p^α sur la classe de x modulo p . Vérifier que ϕ est bien définie et est un morphisme surjectif de groupes. En déduire que son noyau est inclus dans le sous-groupes des carrés de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.
On pourra s'intéresser au cardinal du noyau.
- (b) Montrer que \bar{v}_{p^α} est un carré de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ si et seulement si \bar{v}_p est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$, puis, que $\mu_v(p^\alpha) = 1 + \binom{v}{p}$.
5. Soit m un entier impair, $m \geq 3$ et v un entier premier à m . Montrer l'égalité

$$\mu_v(m) = \prod_{p, \text{val}_p(m) > 0} \left(1 + \binom{v}{p}\right),$$

où $\text{val}_p(m)$ désigne la p -valuation de m pour tout nombre premier p de \mathcal{P} .

Pour a entier, on note désormais, pour tout l impair premier avec a ,

$$\binom{a}{l} = \prod_{p \in \mathcal{P}, \text{val}_p(l) > 0} \binom{a}{p}^{\text{val}_p(l)}, \quad \binom{a}{1} = 1.$$

6. Montrer, pour tout m impair premier à d , les égalités successives

$$\#T(d, m) = \mu_{-d}(m) = \sum \binom{-d}{l},$$

où la somme porte sur les entiers positifs l divisant m et sans facteur carré.

Pour la première égalité, on pourra comparer $\#T(d, m)$ avec $\#\{x \in \mathbb{Z}/4m\mathbb{Z}, x^2 = -\bar{d}_{4m}\}$ et utiliser le lemme chinois.

Soit m un entier premier avec d . On note \mathcal{D}_m l'ensemble des diviseurs positifs de m .

7. Expliciter une bijection entre \mathcal{D}_m et l'ensemble des couples (l, e) d'entiers positifs tels que e^2 divise m et où l , sans facteur carré, divise $\frac{m}{e^2}$.
8. En déduire

$$\sum_{e > 0, e^2 | m} \#T(d, \frac{m}{e^2}) = \sum_{0 < l | m} \binom{-d}{l}.$$

5 Nombre de solutions d'équations quadratiques.

On étudie, dans cette partie, quelques équations quadratiques dans le cas où $d = 20$.

1. Soit m un entier strictement positif, premier avec 20. On pose $q = [1, 0, 5]$ et $q' = [2, 2, 3]$.
Montrer que

$$\#C_q(m) + \#C_{q'}(m) = 2 \sum_{e > 0, e^2 | m} \#T(20, \frac{m}{e^2}) = 2 \sum_{0 < l | m} \binom{-20}{l}.$$

On note dans la suite, $p = 2a + 1$ un nombre premier positif impair tel que $p \neq 5$. Soit

$$\mathcal{X} = \left\{ (x_1, \dots, x_p) \in \mathbb{F}_5^p, \sum_{i=1}^p x_i^2 = 1 \right\}.$$

2. (a) Montrer que $\#\mathcal{X}$ est congru à $1 + \binom{p}{5}$ modulo p .

On pourra faire opérer le groupe cyclique $\mathbf{Z}/p\mathbf{Z}$ sur \mathcal{X} et appliquer la formule des classes.

- (b) Quel est le cardinal d'un hyperplan de l'espace affine \mathbf{F}_5^n , pour tout entier n ?
 (c) En effectuant le changement de variables $u_j = x_j + 2x_{a+j}$, $u'_j = x_j - 2x_{a+j}$, $1 \leq j \leq a$, $u_p = x_p$, montrer que $\#\mathcal{X}$ est congru à $1 + 5^a$ modulo p .
 (d) En déduire l'égalité $\binom{5}{p} = \binom{p}{5}$.

3. Montrer l'équivalence

$$\bar{p} \in \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\} \subset \mathbf{Z}/20\mathbf{Z} \iff \exists q \in \mathcal{Q}_{20}, \exists (x, y) \in \mathbf{Z}^2, p = q(x, y).$$

On pourra chercher, modulo 20, les nombres premiers impairs tels que $1 + \binom{-20}{p}$ est non nul.

4. On veut maintenant affiner l'assertion précédente. Soit p premier distinct de 2 et 5. Montrer les équivalences suivantes

$$\bar{p} \in \{\bar{1}, \bar{9}\} \subset \mathbf{Z}/20\mathbf{Z} \iff \exists (x, y) \in \mathbf{Z}^2, p = x^2 + 5y^2,$$

$$\bar{p} \in \{\bar{3}, \bar{7}\} \subset \mathbf{Z}/20\mathbf{Z} \iff \exists (x, y) \in \mathbf{Z}^2, p = 2x^2 + 2xy + 3y^2.$$

On pourra éliminer des possibilités en regardant les égalités modulo 4 et en considérant la parité de x et de y .

5. (a) Montrer que pour tout nombre premier p congru à 1 ou 9 modulo 20, et tout α entier positif, on a

$$\#\{(x, y) \in \mathbf{Z}^2, x^2 + 5y^2 = p^\alpha\} = 2(1 + \alpha).$$

- (b) Montrer que pour tout nombre premier p congru à 3 ou 7 modulo 20, et tout β entier positif, on a

$$\#\{(x, y) \in \mathbf{Z}^2, x^2 + 5y^2 = p^{2\beta}\} = 2(1 + 2\beta), \quad \#\{(x, y), 2x^2 + 2xy + 3y^2 = p^{2\beta+1}\} = 4(1 + \beta).$$