Academie	Admis 2005	Admis 2015
AIX-MARSEILLE	7	11
AMIENS	3	3
BESANCON	7	7
BORDEAUX	20	11
CAEN	6	3
CLERMONT-FERRAND	6	1
CORSE	0	0
CRETEIL-PARIS-VERSAIL.	136	103
DIJON	3	3
GRENOBLE	19	17
GUADELOUPE	1	0
GUYANE	0	0
LA REUNION	0	1
LILLE	13	6
LIMOGES	0	0
LYON	51	28
MARTINIQUE	0	0
MAYOTTE	0	0
MONTPELLIER	5	4
NANCY-METZ	8	4
NANTES	13	2
NICE	2	5
NOUVELLE CALEDONIE	0	0
ORLEANS-TOURS	9	3
POITIERS	5	3
POLYNESIE FRANCAISE	0	0
REIMS	7	1
RENNES	35	34
ROUEN	3	2
STRASBOURG	15	7
TOULOUSE	14	15

Admis par académie, comparaison 2005-2015

Chapitre 3

Épreuve écrite de mathématiques générales

3.1 Énoncé

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 $\mathbb{Z}$ l'anneau des entiers et $\mathbb{N}$ 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 $\overline{a}_n$ de $\mathbb{Z}/n\mathbb{Z}$ sera la classe de a modulo n, que l'on écrira aussi $\overline{a}$ si le contexte s'y prête. On écrira $a \mid b$ pour « a divise b ».

On notera $\mathbb{P}$ 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 $\mathrm{val}_p(m)$. Le nombre m sera dit *sans facteur carré*, si $\mathrm{val}_p(m) = 0$ ou 1 pour tout p de $\mathbb{P}$.

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

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

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

On rappelle qu'une fonction q de $\mathbb{R}^2$ dans $\mathbb{R}$ 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 $\mathbb{R}^2$

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

1.1

Soit A la matrice de $M_2(\mathbb{R})$ associée à φ, et définie par $A = (\varphi(e_i;e_j))_{1 \leqslant i;j \leqslant 2}$.

1. Démontrer la formule $q(e+f) = q(e) + 2\varphi(e;f) + q(f)$.
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 φ_q) la matrice A (respectivement la forme bilinéaire φ).

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

3. Soit $'$ dans $GL(E)$. On définit la forme quadratique q' par $q'(e) = q('(e))$, $e \in E$. Soit P la matrice de $'$ 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 $'$ dans $GL(E)$ tel que $q''(e) = q'('(e))$ 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 $GL_2(\mathbb{R})$ telle que $A_{q'} = {}^tPA_qP$,
   (iii) il existe une base $(f_1;f_2)$ de E telle que $q(f_1) = a'$, $\varphi_q(f_1;f_2) = \frac{b'}{2}$, $q(f_2) = c'$.

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

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

5. Soit φ une isométrie pour la forme q et $M = Mat_{(e_1;e_2)}(\varphi)$. Quelles sont les valeurs possibles de $\det(M)$?

On notera $O(q;\mathbb{R})$ le sous-groupe de $GL_2(\mathbb{R})$ formé des matrices $M = Mat_{(e_1;e_2)}(u)$, où u est une isométrie pour q (on admettra qu'il s'agit bien d'un sous-groupe).
On note $SO(q;\mathbb{R}) = O(q;\mathbb{R}) \cap SL_2(\mathbb{R})$.

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

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

On suppose maintenant q définie positive.

7. Prouver que $SO(q;\mathbb{R})$ est isomorphe au groupe $SO_2(\mathbb{R})$ des rotations de l'espace vectoriel euclidien $\mathbb{R}^2$.
8. Montrer qu'il existe un réel $k > 0$ tel que, pour tout e dans E, on ait $q(e) > k\|e\|^2$, où $\|:\|$ désigne la norme euclidienne canonique de $\mathbb{R}^2$.

1.2

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

$$Mat_{(e_1;e_2)}(') \in SL_2(\mathbb{Z}) \text{ et } \forall (x;y) \in E,\ q'(x;y) = q('(x;y)).$$

1. Montrer que si Q_d est non vide, alors $d > 0$.
2. Montrer que si q' est proprement équivalente à q dans Q_d, alors $q' \in Q_d$.
3. Montrer que "*être proprement équivalente à*" définit une relation d'équivalence sur Q_d.

On notera S_d l'ensemble des classes d'équivalence dans Q_d pour cette relation. Pour tout q dans 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 $q^{-1}(m) \cap \mathbb{Z}^2$ de m par q, restreinte à $\mathbb{Z}^2$, est non vide.

On fixe deux formes q, q' dans Q_d.

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

Le but du problème est l'étude de l'équivalence propre des formes sur 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 Q_d est *réduite* si les conditions suivantes sont vérifiées :

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

1. Soit $k; k'$ des entiers. Montrer que $4k' - k^2$ est congru à 0 ou à -1 modulo 4.
2. Montrer que 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 Q_{20}.
4. Soit $q = [a;b;c]$ dans Q_d.
   (a) Montrer, en utilisant une matrice de $SL_2(Z)$ 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* 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 Q_d, on a $b^2 > 4b^2 - d$, 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 $SO(q;Z) = SO(q;R) \cap SL_2(Z)$.

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 $|y| > 2$.
   (b) Montrer que si $|y| = 1$, alors $(2ax + yb)^2 > b^2$ pour tout entier x. En déduire que l'équation ci-dessus n'a aucune solution entière pour $|y| > 1$.
   (c) En déduire que le groupe $SO(q;Z)$ est isomorphe à $Z/2Z$.

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 Q_d et tout entier $m > 0$, on notera

$$C_q(m) = q^{-1}(m) \cap Z^2 = \{(x;y) \in Z^2;\ q(x;y) = m\}\ ;\ C_q^1(m) = \{(x;y) \in C_q(m);\ \mathrm{pgcd}(x;y) = 1\}\ ;$$

de sorte que $C_q(m)$ est non vide dès que m est représentable par q. Si $C_q^1(m)$ est non vide, on dira que m est *primitivement représentable* par q.

1. Soit q dans 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 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 $k^2 \equiv -d\ [4m]$ et $k \equiv k'\ [2m]$. Montrer que l'on a $k'^2 \equiv -d\ [4m]$. On notera alors, sans ambiguïté :

$$T(d;m) := \{\overline{k} \in Z/2mZ;\ k^2 \equiv -d\,[4m]\}\ :$$

3. On fixe q dans Q_d, $(x;y)$ dans $C_q^1(m)$, supposé non vide. Soit $(u;v)$ un couple d'entiers tel que $vx - uy = 1$. On pose $n = 2B_q\big((x;y);(u;v)\big)$. En écrivant la matrice de q dans la base $\big((x;y);(u;v)\big)$ de R^2, montrer l'égalité

$$n^2 - 4mq(u;v) = -d:$$

4. Montrer que l'application θ_q de $C_q^1(m)$ vers $T(d;m)$ qui, à un couple $(x;y)$, associe la classe $\overline{2B_q\big((x;y);(u;v)\big)}$ 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 $\sigma \in SO(q;Z)$. Montrer que $\theta_q(\sigma(x;y)) = \theta_q(x;y)$, pour tout couple $(x;y)$ de $C_q^1(m)$.
   (b) Réciproquement, on suppose $(x;y)$ et $(x';y')$ dans $C_q^1(m)$ tels que $\theta_q(x';y') = \theta_q(x;y)$. Montrer qu'il existe alors un unique σ dans $SO(q;Z)$ tel que $(x';y') = \sigma(x;y)$.

6. Soit n dans Z tel que $\overline{n} \in T(d;m)$. Montrer qu'il existe un unique entier l tel que $[m;n;l] \in Q_d$. En posant $q = [m;n;l]$, montrer que $\theta_q(1;0)$ (a un sens et) est égal à $\overline{n}$.

7. On fixe q et q' dans Q_d.
   (a) On suppose ici q et q' proprement équivalentes, avec $\tau \in SL_2(Z)$ tel que $q' = q \circ \tau$. Montrer l'égalité $\theta_q(\tau(x';y')) = \theta_{q'}(x';y')$, pour tout $(x';y')$ de $C_{q'}^1(m)$.
   (b) Réciproquement, on suppose $(x;y) \in C_q^1(m)$, $(x';y') \in C_{q'}^1(m)$, tels que $\theta_q(x;y) = \theta_{q'}(x';y')$. Montrer que q et q' sont proprement équivalentes.

8. Pour toute classe $[q] \in S_d$, on fixe un représentant q dans Q_d, et on note R_d l'ensemble des représentants ainsi fixés. Montrer l'égalité

$$\sum_{q \in R_d} \frac{\#C_q^1(m)}{\#SO(q;Z)} = \#T(d;m):$$

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 $\varepsilon_v(m)$ de x de $\mathbb{Z}/m\mathbb{Z}$ tels que $x^2 = \overline{v}_m$.

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.

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

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

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

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

3. Montrer que, pour tout v non multiple de p, $\varepsilon_v(p) = 1 + \left(\frac{v}{p}\right)$.
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 $\overline{v}_{p^\alpha}$ est un carré de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ si et seulement si $\overline{v}_p$ est un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$, puis, que $\varepsilon_v(p^\alpha) = 1 + \left(\frac{v}{p}\right)$.
5. Soit m un entier impair, $m > 3$ et v un entier premier à m. Montrer l'égalité

$$\varepsilon_v(m) = \prod_{p;\, \mathrm{val}_p(m)>0} \left(1 + \left(\frac{v}{p}\right)\right);$$

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

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

$$\left(\frac{a}{l}\right) = \prod_{p\in P\,;\mathrm{val}_p(l)>0} \left(\frac{a}{p}\right)^{\mathrm{val}_p(l)} ; \quad \left(\frac{a}{1}\right) = 1:$$

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

$$\#T(d;m) = \square_{-d}(m) = \sum \left(\frac{-d}{l}\right);$$

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 D_m l'ensemble des diviseurs positifs de m.

7. Expliciter une bijection entre 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

$$\sum_{e>0, e^2|m} \#T(d; \frac{m}{e^2}) = \sum_{0<l|m} \left(\frac{-d}{l}\right):$$

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

$$\#C_q(m) + \#C_{q'}(m) = 2 \sum_{e>0; e^2|m} \#T(20; \frac{m}{e^2}) = 2 \sum_{0<l|m} \left(\frac{-20}{l}\right):$$

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

$$X = \left\{(x_1;:::;x_p) \in F_5^p; \sum_{i=1}^{p} x_i^2 = 1\right\}:$$

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

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

   (b) Quel est le cardinal d'un hyperplan de l'espace affine 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 $\#X$ est congru à $1 + 5^a$ modulo p.

   (d) En déduire l'égalité $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$.

3. Montrer l'équivalence

$$p \in \{\bar{1};\bar{3};\bar{7};\bar{9}\} \subset \mathbb{Z}/20\mathbb{Z} \Longleftrightarrow \exists q \in Q_{20}; \exists (x;y) \in \mathbb{Z}^2; p = q(x;y):$$

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

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

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

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

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

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

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

$$\#\left\{(x; y) \in \mathbb{Z}^2,\ x^2 + 5y^2 = p^{2\alpha}\right\} = 2(1+2\alpha);\ \#\left\{(x; y),\ 2x^2 + 2xy + 3y^2 = p^{2\alpha+1}\right\} = 4(1+\alpha).$$

3.2 Rapport sur l'épreuve écrite de mathématiques générales

Généralités sur les formes quadratiques sur $\mathbb{R}^2$

1.1.1 Cette question demandait juste de mettre en exergue la bilinéarité et la symétrie de la forme. Elle n'a posé de soucis à personne excepté à des candidats, soit hors profil, soit sous l'emprise de leurs émotions.

1.1.2 Un bon pourcentage de candidats n'a vu dans cette question que le problème de l'unicité. Il faut bien sûr également que l'égalité ait lieu.

1.1.3 La formule bien connue $A_{q'} = {}^t P A_q P$ était attendue avec sa preuve. Les candidats n'ont pas toujours su sur quel pied danser avec cette question, qui était une question de cours. Il était attendu que la formule soit montrée dans le contexte du problème. La plupart a su prouver la formule ${}^tX A_{q'} X = {}^t X {}^t P A_q P X$, pour toute colonne X, mais n'a pas su conclure en utilisant l'unicité de 1.1.2.

1.1.5 A la question « quelles sont les valeurs possibles du déterminant d'une isométrie ? », les candidats ont répondu ± 1. Il y avait tout de même des pièges. D'une part, ici, la forme quadratique était non dégénérée, et les correcteurs ont attendu que cet argument intervienne explicitement. D'autre part, demander les valeurs possibles exige qu'elles soient réalisables. Sinon, la réponse « le déterminant est un nombre réel, voire complexe » aurait été tout aussi satisfaisante. Le pourcentage des candidats ayant abordé ce dernier point, ou tout au moins, ayant remarqué son existence, a été infime. Nous invitons à une réflexion collective sur le sens du mot « possible ».

1.1.6 Il fallait, pour cette question, avoir bien compris le rôle de la conjugaison dans l'algèbre linéaire. Ceux qui pensaient que l'application attendue était $M \mapsto PM$, voire $M \mapsto {}^t PMP$, ou autre chose de ce genre, doivent prendre un peu de recul pour refléchir à ce lien important et très général (il dépasse le cadre de l'algèbre linéaire), qui relie les groupes et les objets sur lesquels ils agissent, et qui se résumerait en une maxime : lorsque les objets sont en bijection, les groupes sont en conjugaison.

Une fois la bonne application trouvée, il fallait encore montrer que l'on avait un isomorphisme. Bien entendu, il fallait déjà voir que l'application était bien définie et exhiber un inverse. Les correcteurs ont été surpris de voir que certains candidats montraient que les groupes multiplicatifs étaient isomorphes à l'aide d'arguments d'espaces vectoriels (commutation avec l'addition, noyau nul...)

1.1.7 Il était attendu que l'on parle d'existence d'une base orthonormée, afin de pouvoir utiliser la question précédente.

1.1.8 Les candidats qui ont su montrer l'existence de k n'ont pas toujours su (ou pensé à) montrer que celui-ci était non nul.

1.2.1 Les candidats ont souvent abordé la question avec l'argument du signe du discriminant du trinôme. Attention toutefois, le trinôme $ax^2 + bx + c$ n'en est un que si a est non nul, ce qui n'a souvent pas été vérifié.

1.2.2 Demander de montrer que q' est dans Q_d demandait deux choses : d'une part qu'elle soit de discriminant d, mais aussi qu'elle soit définie positive. Ce dernier point a souvent été oublié.

1.2.4 Il fallait ici proposer une bijection, puis prouver que c'en était une. Généralement, la bijection proposée était la bonne. En revanche, la preuve demandait d'être un peu minutieux : la bijection devait être bien définie dans les deux sens, et selon deux critères, un critère d'intégrité, et un critère de représentation de m.

Z-congruence et nombre de classes

2.1 Question souvent abordée, avec beaucoup de succès. On peut toutefois regretter que les candidats préfèrent, par sécurité, travailler par congruence dans $\mathbb{Z}$, plutôt que par égalité, dans un quotient.

2.2 La partie « seulement si » n'a posé de problème à personne puisqu'elle découlait directement de la question précédente. La réciproque, en revanche, était plus délicate. Il fallait d'une part donner explicitement une forme quadratique de discriminant d fixé, et ensuite montrer que celle-ci était définie positive (le signe du discriminant n'étant pas suffisant).

2.3 On sait tous au fond de soi pourquoi $x^2 + 5y^2 = 2$ n'a pas de solution entière. Mais manifestement, tout le monde ne sait pas le montrer de façon simple et convaincante, avec de petites inégalités bien senties. Les correcteurs ont dû assister, les yeux plissés, à des combats contre $\sqrt{\frac{2}{5}}$. Parfois, des inégalités qui omettaient les valeurs absolues montraient correctement que l'équation n'a pas de solution dans $\mathbb{N}$, en oubliant les entiers négatifs. En revanche, l'autre question, plus subtile, a été abordée avec plus de succès.

2.4 Il fallait ici exhiber deux matrices. Ceux qui ont abordé la question l'ont généralement bien fait. Evidemment, ceux qui avaient un peu de culture et connaissaient les générateurs classiques de $\mathrm{PSL}_2(\mathbb{Z})$ avaient un coup d'avance et ont dû être avantagés.

2.5 Cette question était délicate. Dans un premier temps, il fallait faire de la réduction en utilisant les matrices de 2.4 a), puis 2.4 b). Mais ensuite, il fallait remarquer que ce que faisait 2.4 b) détricotait légèrement l'intervention de 2.4 a). Très peu de candidats l'ont remarqué, et seules de très bonnes copies ont su déjouer le piège.

2.6 (b) Les candidats qui ont abordé la question ont parfois su montrer correctement qu'il y avait un nombre fini de formes réduites. Mais ils ont souvent oublié de montrer que cela répondait effectivement à la question, c'est-à-dire que cela prouvait qu'il y avait un nombre fini de classes d'équivalence. Or, il n'était pas clair qu'il y avait une bijection entre classes d'équivalence et forme réduites.

Représentabilité d'un entier par une forme

3.3 On a retrouvé ici une erreur tragique bien connue des enseignants : la confusion entre matrice et endomorphisme. Une matrice M avait parfois deux valeurs différentes selon la base choisie. Il convient donc d'agiter quelques crécelles : lorsque l'on change de base, l'endomorphisme ne change pas, la matrice, si.

3.4 Le lemme de Gauss était attendu. Il faut, à ce stade, savoir résoudre l'équation entière $au + bv = 1$ quand a et $b$sont premiers entre eux. Bien entendu, il fallait aussi voir que la question posée se ramenait à celle-ci.

Nombre de solutions d'une équation modulaire

4.1 Comme pour la partie 1.1, il faut savoir reconnaître une question de cours : on ne pouvait pas imaginer avoir répondu à la question en dégainant la formule de l'indicatrice d'Euler. Le mot « justifier » était assez clair.

4.2 (a) Les candidats ont été d'une rapidité fulgurante pour énoncer que $x^2 = 1$ possédait 2 solutions : 1 et -1. Il fallait quand même rappeler que l'on travaillait sur un corps (donc intègre). Mais cela ne suffisait pas : il fallait aussi voir que ce corps était de caractéristique différente de 2 (pour que 1 et -1 soient distincts).

4.2 (b) Il s'agissait d'une question classique et un candidat bien préparé connaissait en général la solution. L'improviser *ex nihilo* un jour d'écrit était une tâche difficile.

4.4 (a) Cette question a été souvent traitée. Les candidats ont bien pensé à prouver que l'application naturelle de $\mathbb{Z}/p^2\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}$ est bien définie, mais ils ont souvent utilisé des moyens archaïques pour le prouver. A l'ère de l'algèbre dite moderne, il faudrait savoir utiliser le passage au quotient.

Ensuite la surjectivité de l'application naturelle n'impliquait pas directement la surjectivité de l'application de $(\mathbb{Z}/p^2\mathbb{Z})^*$ sur $(\mathbb{Z}/p\mathbb{Z})^*$, ni même que celle-ci soit bien définie.

Nombre de solutions d'équations quadratiques.

5.2 (b) Les adeptes du grappillage ont apprécié cette question à sa juste valeur, en remarquant que le cardinal d'un sous-espace, sur un corps fini, est déterminé par la dimension. Il faut toutefois rappeler que l'existence d'une base est primordial dans ce résultat.

3.3 Corrigé de l'épreuve de mathématiques générales

3.3.1 Commentaires mathématiques généraux

Le théorème des deux carrés de Fermat est un exemple type de ce qu'un énoncé simple peut dissimuler de richesses. Après s'être demandé quels entiers m se décomposent en somme de deux carrés d'entiers, on cherche à comprendre de combien de façons on peut effectuer une telle décomposition pour m fixé. On peut ensuite généraliser cette question au cas des formes entières binaires : soit q une forme quadratique sur $\mathbb{R}^2$ de la forme $q(x;y) = ax^2 + bxy + cy^2$, avec a, b, c entiers, quel est le cardinal de l'ensemble $C_q(m)$ des solutions entières de l'équation $q(x;y) = m$? Ou, pour un point de vue inverse, m fixé dans $\mathbb{Z}$ quels sont les formes entières binaires qui *représentent* m, *i.e.* telles que $q(x;y) = m$ possède une solution entière ? Ce problème, devenu un classique, a permis d'ouvrir des voies insoupçonnées tracées par Lagrange, Gauss, Dirichlet, Dedekind et autres mathématiciens d'envergure. Nous nous contenterons d'en visiter la porte d'entrée.

Tout d'abord, ce cardinal est-il fini ? Le meilleur moyen de s'en assurer est d'imposer à q d'être une forme quadratique définie ; l'ensemble des solutions est alors un compact discret pour la topologie naturelle de $\mathbb{R}^2$, donc fini. On supposera donc que q est définie positive et m strictement positif. On notera $C_q(m)$ l'ensemble des solutions entières de l'équation.

Comme q est homogène de degré 2, on sait qu'une solution $(x;y)$ de $C_q(l)$ fournit une solution $(ex;ey)$ de $C_q(e^2l)$, ce qui permet de réduire l'étude à celle de l'ensemble $C_q^1(m)$ des couples $(x;y)$ de solutions d'entiers premiers entre eux.

Maintenant, l'idée habituelle est de partitionner $C_q^1(m)$, et rien de mieux pour cela que de penser à une action de groupe. Le premier groupe (ou presque) qui vient à l'esprit est le groupe $SO(q;\mathbb{Z})$ des isométries entières, de déterminant 1, qui respectent la forme q. On voit qu'il agit naturellement sur $C_q(m)$ et même sur $C_q^1(m)$. Cette action est d'ailleurs « simplifiée » par le fait que les stabilisateurs sont triviaux, puisque $(0;0)$ n'est jamais solution ; chaque orbite a donc même cardinal que le groupe. Compter les éléments de $C_q^1(m)$ se ramène donc à compter le nombre orbites.

Selon une procédure désormais bien convenue, on cherche un invariant « palpable », permettant de caractériser les orbites de cette action. Compter les orbites revient à compter le nombre d'invariants possibles. L'invariant proposé se construit ainsi : le fait que $(x;y)$ est dans $C_q^1(m)$ implique en particulier que $(x;y)$ peut se compléter en une $\mathbb{Z}$-base directe de $\mathbb{Z}^2$, par Bezout. Notons, $((x;y);(u;v))$ une telle base. On remarque alors que, si Φ_q désigne la forme polaire de q, $2\Phi_q((x;y);(u;v))$ réduit modulo $2m$ ne dépend que de $(x;y)$ et non pas du choix de $(u;v)$. On voit aussi qu'il s'agit là d'un invariant pour l'action de $SO(q;\mathbb{Z})$. Mieux, il sépare les orbites du groupe.

Reste à savoir dans quel ensemble raisonnable on va aller chercher cet invariant. Comme le déterminant est un invariant de changement de $\mathbb{Z}$-bases pour une forme quadratique entière, on obtient que $n :=$

$(2\Phi_q((x;y);(u;v)))$ vérifie $n^2 \equiv b^2 - 4ac$ modulo $4m$. Ceci engage à poser $d = 4ac - b^2$ et

$$T(d;m) := \{\overline{k} \in \mathbb{Z}/2m\mathbb{Z};\ k^2 \equiv -d\,[4m]\}\,;$$

en vérifiant qu'il n'y a pas ambiguïté dans cette définition.

On peut énoncer maintenant le résultat clef du problème : 1) tout d'abord, ce que nous venons de voir, c'est-à-dire que l'application $\overline{\Phi}_q$ qui à une $SO(q;\mathbb{Z})$-orbite dans $C_q^1(m)$ envoie l'élément de $T(d;m)$ défini plus haut, est injective. 2) Réciproquement, tout élément de $T(d;m)$ caractérise une classe de forme entière binaire modulo $SL_2(\mathbb{Z})$-congruence. On obtient alors, en fixant un ensemble R_d de représentants de formes de « déterminant » d pour l'action par congruence de $SL_2(\mathbb{Z})$ la formule

$$\sum_{q \in R_d} \frac{\#C_q^1(m)}{\#SO(q;\mathbb{Z})} = \#T(d;m):$$

Pour tirer des résultats effectifs de cette formule, il est nécessaire de travailler encore un peu de part et d'autre de l'égalité. Le membre de droite demande de passer par le symbole de Legendre, la réciprocité quadratique, et le lemme chinois. Le membre de gauche demande une compréhension pratique des orbites de congruence pour les formes entières binaires. Pour cela, Lagrange a défini une notion de forme réduite, qui fournit une forme normale pour chaque orbite de congruence. Il ne reste plus qu'à faire de petits calculs.

3.3.2 L'organisation du sujet

La partie **1** du problème est là pour rappeler au candidat les outils fondamentaux des formes quadratiques, dans le cadre de la dimension 2. Tout d'abord sur $\mathbb{R}$, où l'on revoit la mise sous forme matricielle d'une forme quadratique. La principale piqûre de rappel de la section **1.1** est la triple façon de concevoir la congruence : (i) l'existence d'un passage par composition à droite, pour deux formes quadratiques fixées, (ii) la formule matricielle de congruence, (iii) l'existence d'une base faisant passer d'une matrice à l'autre, pour une forme quadratique fixée. On introduit le groupe d'isométrie d'une forme quadratique, et on regarde comment la congruence se traduit sur les groupes d'isométrie. La section **1.2** explore le problème des formes entières binaires. On voit que le déterminant est un invariant de congruence. On commence ensuite à s'intéresser à l'ensemble des solutions entières de l'équation $q(x;y) = m$. On montre qu'il est fini, et que son cardinal ne dépend que de la classe de congruence des formes définies positives.

La partie **2** concerne l'équivalence propre des formes entières binaires, c'est-à-dire, la $SL_2(\mathbb{Z})$-congruence. On définit les formes dites réduites et on montre que toute classe de congruence contient une telle forme. On en déduit que l'ensemble des classes est fini. On introduit ce qui va devenir l'exemple courant du problème : le cas où le déterminant vaut 20. On montre ensuite que pour les formes réduites « générales », *ie* telles que $a \neq c$, le groupe d'isotropie est le groupe à 2 éléments.

La partie **3** est essentiellement consacrée à la correspondance de Gauss-Dirichlet. On fixe deux entiers $m; d > 0$. On établit donc une correspondance biunivoque entre la donnée d'un couple constitué d'une part d'une classe d'équivalence propre de forme q de déterminant d, d'autre part d'une classe pour l'action de $SO(q)$ de solution primitive de l'équation $q(x;y) = m$, et la donnée d'un élément d'un ensemble $T(d;m)$ défini par des résidus quadratiques. Le nœud du problème est démêlé.

La partie **4** s'intéresse au membre de droite de la formule obtenue en **3**, c'est-à-dire au cardinal de $T(d;m)$. On s'y pose une question classique chez les groupes cycliques : comment caractériser les carrés de $\mathbb{Z}/m\mathbb{Z}$? Les outils pour y répondre sont encore plus classiques : utilisation de la surjection canonique, du passage au quotient, du théorème de Lagrange. En particulier, on définit le symbole de Legendre que l'on généralise en un symbole de Jacobi, et le résultat vient d'un relèvement classique des carrés par la surjection naturelle de $\mathbb{Z}/p^{\alpha}\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}$, puis par le lemme chinois.

La partie 5 aboutit à des résultats explicites sur le nombre de solutions d'équations quadratiques, et ce, sur l'exemple courant $d = 20$ sur lequel on a collecté des informations tout au long du problème. L'exemple est facilité par le fait qu'il n'y a que deux classes de formes proprement équivalentes, ainsi, pour être sûr que l'on est dans une classe, il suffit de voir que l'on est pas dans l'autre...Il faut aussi calculer concrètement des symboles de Legendre, et pour cela, on doit utiliser la loi de réciprocité quadratique de Gauss. On obtient cette loi par une méthode de géométrie sur un corps fini, en calculant de deux façons le cardinal d'une nappe quadratique.

Les bonus

Concours oblige, on n'a malheureusement pas pu mettre tous les jolis éléments de la théorie, qui pourtant valent le détour. Voici quelques scènes qui ont été coupées au montage.

A toute classe d'équivalence propre de forme entière binaire, on a unicité de la forme réduite– on n'a montré que l'existence.

Pour une forme q entière binaire, le groupe $SO(q;Z)$ ne dépend bien sûr à isomorphisme près que de la classe de congruence à laquelle il appartient. Or, on n'a calculé le groupe d'isotropie d'une forme réduite $q = [a;b;c]$ que dans le cas $a < c$. Il n'est pas beaucoup plus difficile d'obtenir le résultat complet :

$$SO(q;Z) \text{ est isomorphe à } \begin{cases} Z/6Z & \text{si b=a=c} \\ Z/4Z & \text{si 0= b<a=c} \\ Z/2Z & \text{sinon} \end{cases}$$

Pour finir sur la plus belle partie de la théorie, qui était le but inaccessible du problème : la « partie VI », signalons que l'on peut construire une structure de groupe sur l'ensemble des classes d'équivalence propre des formes entières binaires de déterminant d donné. La façon la plus simple de comprendre cette structure est d'exhiber une bijection entre cet ensemble et l'ensemble des classe d'idéaux de $Z[\frac{1}{2}\sqrt{-d}]$. Comme ce dernier possède une structure naturelle de groupe, on utilise juste un transport de structure. Le résultat est le suivant : si un entier m, resp. m', est représenté par q, resp. q', dans Q_d, alors cette structure de groupe permet de trouver q'' qui représente l'entier mm'.

Dans le cas où $d = 4$, le groupe est trivial puisque l'anneau $Z[i]$ est principal, et le résultat est lié à la formule bien connue de multiplicativité de la norme de C

$$(x^2 + y^2)(u^2 + v^2) = (xu - yv)^2 + (xv + yu)^2 :$$

Illustrons ceci avec l'exemple courant où $d = 20$. On a vu qu'il n'y avait que deux classes de formes entières binaires ; le groupe est forcément $Z/2Z$. L'élément neutre est la classe de la norme $[1;0;5]$, l'autre est donc $[2;2;3]$. Une formule qui met en lumière la multiplicativité dans la représentation des entiers est donnée par

$$(2x^2 + 2xy + 3y^2)(2u^2 + 2uv + 3v^2) = (2xu + xv + yu + 2yv)^2 + 5(xv + yu + yv)^2 :$$

qui correspond à $\bar{1} + \bar{1} = \bar{0}$ dans $Z/2Z$.

3.3.3 Correction détaillée

1- Généralités sur les formes quadratiques sur R^2

1.1

1. On développe $q(e+f) = \varphi(e+f;e+f)$. La bilinéarité de φ donne $q(e) + \varphi(e;f) + \varphi(f;e) + q(f)$. La symétrie de φ donne le résultat.

2. Par la question 1.1.1, on a bien

$$q(x;y) = q(x;0) + 2\varphi\big((x;0);(0;y)\big) + q(0;y) = ax^2 + bxy + cy^2$$

Pour l'unicité, on utilise, par exemple, l'évaluation en $(1;0)$, $(0;1)$, $(1;1)$, qui nous donne l'unicité de a, c, et $a+b+c$, donc celle du triplet $(a;b;c)$.

3. Si on pose $U = \begin{pmatrix} x \\ y \end{pmatrix}$, alors $q(x;y)$ est la valeur de la matrice 1×1 donnée par ${}^tUA_qU$. Il vient d'une part $q'(x;y) = {}^tUA_{q'}U$ et d'autre part $q'(x;y) = {}^t(PU)A_q(PU) = {}^tU({}^tPA_qP)U$.
Par l'unicité montrée dans la question précédente, il vient $A_{q'} = {}^tPA_qP$.

4. La question précédente montre que (i) implique (ii) et la réciproque est immédiate.
(i)⇒(iii). Soit $q' = q\circ\varphi$, avec $\varphi \in GL(E)$. Posons $f_i = \varphi(e_i)$, $i = 1;2$. Alors, $(f_1;f_2)$ est une base et $a' = q'(e_1) = q\big(\varphi(e_1)\big) = q(f_1)$. Les autres égalités sont similaires.
(iii)⇒(i). Soit φ l'élément de $GL(E)$ qui envoie la base $(e_1;e_2)$ sur la base $(f_1;f_2)$. D'après l'hypothèse, en notant φ' la forme polaire de q', on voit que l'égalité $\varphi'(x;y) = \varphi\big(\varphi(x);\varphi(y)\big)$ est valable sur la base $(e_1;e_2)$ et donc sur tout E puisque, d'après 1.1.2, une forme quadratique sur E est entièrement déterminée par les valeurs de sa forme polaire sur une base.

5. D'après 1.1.3, on a $A_q = {}^tMA_qM$. Donc,

$$\det(A_q) = \det({}^tM)\det(A_q)\det(M) = \det(M)^2\det(A_q);$$

Comme $\det(A_q) \neq 0$, il vient $\det(M) = \pm 1$.
Maintenant, est-ce que ces valeurs sont atteintes ? C'est bien évident pour 1 puisque la matrice identité est toujours une isométrie. Pour -1, on peut faire deux cas :
Si $a \neq 0$, dans ce cas, la matrice $\begin{pmatrix} 1 & b/a \\ 0 & -1 \end{pmatrix}$ fait l'affaire.
Si $c \neq 0$, le cas est similaire. Et si $a = c = 0$, on peut prendre $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

6. On a vu que ${}^tMA_qM = A_q$ est équivalent à $M \in O(q)$. Pour que M soit dans $SO(q)$, il faut ajouter la condition $\det(M) = 1$.
L'isomorphisme est donné par $M \mapsto P^{-1}MP$, où P est la matrice de φ .
Pour prouver qu'il est bien (co)défini, on voit d'une part, que $\det(P^{-1}MP) = \det(M)$, et d'autre part, que ${}^tMA_qM = A_q$ implique ${}^t(P^{-1}MP)({}^tPA_qP)(P^{-1}MP) = {}^tPA_qP$.
C'est clairement un morphisme de groupes puisque $P^{-1}MNP = (P^{-1}M)(PP^{-1}NP)$, et il est bijectif d'inverse $M \mapsto PMP^{-1}$.

7. Par le procédé de Gram-Schmidt, il existe une base orthonormée $(f_1;f_2)$ pour q (car q est définie positive). Soit φ l'automorphisme qui envoie $(e_1;e_2)$ sur $(f_1;f_2)$, alors $q\circ\varphi$ a pour matrice I_2. L'assertion découle donc de 1.1.6.

8. L'homogénéité, de part et d'autre de l'inégalité, fait que l'on peut se restreindre au cas où e est sur le cercle unité, qui est compact. Soit donc k le minimum de q, atteint sur le cercle qui est compact.
On a donc bien $k > 0$ car q est définie positive et que le minimum est atteint sur un point clairement non nul.

1.2

1. Soit $q = [a;b;c]$ dans Q_d. On a q définie positive, et donc $a = q(1;0) > 0$. On a donc a non nul, et la méthode de Gauss (voire la décomposition canonique !) prouve que

$$\frac{1}{a}q(x;y) = (x + \frac{b}{2a}y)^2 + \frac{d}{4a^2}y^2.$$

Si, par l'absurde, $d \leq 0$, la forme q se factorise sur $\mathbb{R}$ en produit de deux formes linéaires et donc elle n'est plus définie positive, puisqu'elle peut alors s'annuler sur le noyau d'une forme linéaire (une droite).

On aurait pu aussi avancer que, comme q est définie positive, les valeurs propres de A_q sont toutes deux strictements positives et donc le déterminant de A_q, égal à $d/4$ est strictement positif.

2. Tout d'abord, si $q' = q \circ \varphi$, alors la positivité de q implique celle de q'. La formule de congruence 1.1.4 (ii) montre que les déterminants des matrices A_q et $A_{q'}$ sont les mêmes, puisque φ est dans $SL_2(\mathbb{Z})$.
3. Cela vient du fait que $SL_2(\mathbb{Z})$ est un groupe. Plus précisément : la relation est réflexive car $I_2 \in SL_2(\mathbb{Z})$, symétrique car $SL_2(\mathbb{Z})$ est stable par inversion et transitive car $SL_2(\mathbb{Z})$ est stable par multiplication.
4. Si on note $q' = q \circ \varphi$, avec $\varphi \in SL_2(\mathbb{Z})$, alors $(x;y) \mapsto \varphi^{-1}(x;y)$ fournit la bijection. On note que si $q(x;y) = m$, alors $q'(\varphi^{-1}(x;y)) = q(x;y) = m$. Cette application est donc bien définie car, de plus, $\varphi^{-1} \in GL_2(\mathbb{Z})$, et donc envoie un couple d'entier sur un couple d'entier. La bijection réciproque est $(x;y) \mapsto \varphi(x;y)$ est également bien définie car $\varphi \in GL_2(\mathbb{Z})$.
5. Soit $e = xe_1 + ye_2$, $x;y \in \mathbb{Z}$, tel que $q(e) = m$. Par 1.1.8,

$$x^2;y^2 \leq x^2 + y^2 = ||e||^2 \leq \frac{m}{k}.$$

Ce qui prouve que $|x|;|y| \leq \sqrt{\frac{m}{k}}$. Comme x et y sont entiers, il ne peut y avoir qu'un nombre fini de vecteurs e dans $q^{-1}(m) \cap \mathbb{Z}^2$.

On peut aussi le faire avec l'équivalence de la norme quadratique avec la norme sup, ou bien alors, avec la propriété qu'un espace topologique compact et discret est fini.

2- $\mathbb{Z}$-congruence et nombre de classes

1. C'est tout simplement que les carrés de l'anneau $\mathbb{Z}/4\mathbb{Z}$ sont $\bar{0}$ et $\bar{1}$.
2. Si $q = [a;b;c]$ est dans Q_d, alors $d = 4ac - b^2$ et d est congru à 0 ou -1 modulo 4, par ce qui précède. Inversement, si d est congru à 0 ou -1 modulo 4, alors il existe des entiers k et k' tels que $d = 4k' - k^2$ et $q = [1;k;k']$ est dans Q_d.
   Il reste à montrer que la forme q est définie positive. Ceci provient de la décomposition canonique

$$q(x;y) = x^2 + kxy + k'y^2 = (x + \frac{k}{2}y)^2 + \frac{d}{4}y^2.$$

3. L'égalité $x^2 + 5y^2 = 2$ avec x, y entiers, implique $|y| < 1$ et donc $y = 0$, ce qui donne $x^2 = 2$.
   L'équation n'a donc pas de solution entière alors que $2x^2 + 2xy + 3y^2 = 2$ possède $(1;0)$ comme solution entière. En utilisant 1.2.4, on obtient que $[1;0;5]$ et $[2;2;3]$ ne sont pas proprement équivalentes.
4. (a) On prend $P = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, qui appartient à $SL_2(\mathbb{Z})$, et on applique 1.1.4 (ii).
   (b) Idem avec $P = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

5. C'est une application des deux questions précédentes. Soit $q = [a; b; c]$ dans une classe fixée de S_d. On a : $a; c > 0$ car $a = q(1; 0)$ qui est strictement positif et de même $c = q(0; 1) > 0$. Quitte à changer b en $b + 2ka$, en utilisant 2.4 a), avec k un entier compris entre $-\frac{1}{2} - \frac{b}{2a}$ et $\frac{1}{2} - \frac{b}{2a}$, on se ramène au cas où $-a \leq b \leq a$ et donc $b^2 \leq a^2$. Maintenant, choisissons $q = [a; b; c]$ dans la classe fixée tel que $|b|$ soit minimal. D'après ce qui précède, on a donc $b^2 \leq a^2$ et, en utilisant 2.4 b), on a également $b^2 \leq c^2$. Toujours en utilisant 2.4 b), on peut supposer, quitte à échanger a et c, que $a \leq c$. On a donc bien les inégalités R_1.
   De plus, si $a^2 = b^2$, et $b < 0$, et donc $b = -a$, on peut choisir $k = 1$ et on se ramène à $b = a$ positif. On a donc R_2.
6. (a) On a $b^2 = 4ac - d > 4b^2 - d$ et donc $b^2 \leq \frac{d}{3}$. Puis,
$$0 < a^2 \leq ac = \frac{1}{4}(b^2 + d) \leq \frac{1}{4}(\frac{d}{3} + d) = \frac{d}{3};$$
   (b) Par 2.5, on a une application surjective qui, à une forme réduite, associe sa classe de S_d. il suffit donc de montrer que le nombre de formes réduites possibles est fini. Or, pour une forme réduite, le nombre de $(a; b)$ possibles est fini par 2.6 a), et c est déterminé par a, b et d; explicitement $c = \frac{1}{4a}(d + b^2)$, car $a \neq 0$.
7. On cherche les formes réduites possibles. Par 2.6 a) les seules possibilités pour $(a; b)$ sont $(2; b)$, avec $-1 \leq b \leq 2$, ou $(1; b)$ avec $0 \leq b \leq 1$. Après un cas par cas (on a six cas), seuls $(a; b) = (1; 0)$, avec $c = 5$, et $(2; 2)$, avec $c = 3$ survivent à la condition $4ac - b^2 = 20$. On trouve donc $S_{20} \leq 2$ par ce qui précède, et $S_{20} > 2$ par 1.2.3. Conclusion $S_{20} = 2$.
8. (a) $d = 4ac - b^2 > 4a^2 - a^2 > a^2$. L'autre assertion devient claire.
   (b) On fixe $y = \pm 1$, et on étudie la fonction $x \mapsto (2ax + yb)^2$ sur $\mathbb{R}$. Elle est décroissante pour $x \leq -\frac{yb}{2a}$ et croissante pour $x > -\frac{yb}{2a}$. Comme $|\frac{yb}{2a}| < 1$, forme réduite oblige, il suffit de vérifier l'inégalité pour $x = -1; 0; 1$. Ce qui est immédiat. L'autre assertion devient claire puisque $4a^2 > b^2 + d$ impliquerait $a > c$.
   (c) Soit $M = \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}$ dans $SO(q; \mathbb{Z})$. Par 1.1.4 (iii), on se ramène à chercher x, y, x', y' entiers, tels que
$$q(x; y) = a;\ \beta_q\big((x; y); (x'; y')\big) = b/2;\ q(x'; y') = c;\ xy' - x'y = 1:$$
   Par les deux questions qui précèdent, la première équation n'a que deux solutions $(1; 0)$ et $(-1; 0)$. Quitte à multiplier M par $-I_2$, qui appartient bien à $SO(q; \mathbb{Z})$, on peut se ramener au cas où $(x; y) = (1; 0)$. La dernière équation donne $y' = 1$, puis la seconde donne $x' = 0$.

3- Représentabilité d'un entier par une forme

1. Soit m représentable par q, soit $(x; y)$ un couple d'entiers tels que $q(x; y) = m$, et $k = \text{pgcd}(x; y)$. On pose $x' = \frac{x}{k}$, $y' = \frac{y}{k}$, de sorte que $\text{pgcd}(x'; y') = 1$ par homogénéité du pgcd, il vient $k^2 q(x'; y') = m$, et donc $m' := \frac{m}{k^2}$ est primitivement représentable par q.
   La réciproque est claire.
2. On élève au carré $k' = k + 2em$, avec e entier, et on développe k'^2. Il vient immédiatement que k^2 et k'^2 sont congrus modulo 4.
3. La matrice de q dans cette nouvelle base est égale à $\begin{pmatrix} m & \frac{n}{2} \\ \frac{n}{2} & q(u; v) \end{pmatrix}$. L'invariance de d par congruence, 1.2.2, montre alors l'égalité.

4. Par la question précedente, on voit que l'élément associé est bien dans $T(d;m)$.
   Par le lemme de Gauss, on voit qu'un autre choix $(u';v')$ de complément implique
   $$(u';v') = (u;v) + k(x;y):$$
   On obtient alors que
   $$\overline{2\mathcal{B}_q\big((x;y);(u';v')\big)} \text{ et } \overline{2\mathcal{B}_q\big((x;y);(u;v)\big)}$$
   sont congrus modulo $2q(x;y) = 2m$.
5. (a) Si $(x;y)$ est dans $C^1(m)$, alors, $q\big(\mathcal{B}(x;y)\big) = q(x;y) = m$. De plus, comme $\mathcal{B}$ est à coefficients dans $\mathbb{Z}$, on a $\mathcal{B}(x;y)$ dans $C(m)$. Enfin, comme $\mathcal{B}(k(x;y)) = k\mathcal{B}(x;y)$, on voit que $\mathcal{B}(x;y)$ est dans $C^1(m)$.
   Puisque $\mathcal{B}$ est de déterminant 1, on a que le déterminant du bivecteur $\big(\mathcal{B}(x;y);\mathcal{B}(u;v)\big)$ est égal au déterminant du bivecteur $\big((x;y);(u;v)\big)$, c'est-à-dire 1. Le résultat vient alors de l'invariance de $\mathcal{B}_q$ par $\mathcal{B}$.
   (b) Unicité : par 1.1.7, $\mathcal{B}$ est une rotation et le stabilisateur d'un élément non nul par une rotation est l'identité.
   Existence : on construit donc, par les hypothèses de l'énoncé, deux bases directes, respectivement $\big((x;y);(u;v)\big)$ et $\big((x';y');(u';v')\big)$, telle que les matrices de q dans ces bases sont de la forme, respectivement
   $$\begin{pmatrix} m & \frac{n}{2} \\ \frac{n}{2} & q(u;v) \end{pmatrix} \text{ et } \begin{pmatrix} m & \frac{n'}{2} \\ \frac{n'}{2} & q(u';v') \end{pmatrix};$$
   avec n et n' congrus modulo $2m$. On se ramène, par la matrice de passage de 2.4 a), au cas où $n = n'$ et donc $q(u;v) = q(u';v')$ par invariance du déterminant. Les deux matrices sont alors égales, et l'endomorphisme $\mathcal{B}$ qui envoie la première base sur la seconde vérifie bien les propriétés voulues.
6. Comme $n \in T(d;m)$, on a $n^2 = -d + 4ml$, pour un l. L'unicité de l est claire car m non nul. L'élément $\mathcal{B}_q(1;0)$ a un sens car $(1;0)$ est bien dans $C^1_q(m)$ et il vaut $\overline{2\mathcal{B}_q\big((1;0);(0;1)\big)} = n$.
7. (a) On a encore, comme dans 5 a), $\varphi(x';y') \in C^1_q(m)$, puisque $(x';y') \in C^1_{q'}$ et $q' = q \circ \varphi$. Il suffit ensuite de remarquer, toujours comme dans 5 a), que le déterminant du bivecteur $\big(\varphi(x;y);\varphi(u;v)\big)$ est égal au déterminant du bivecteur $\big((x;y);(u;v)\big)$, c'est-à-dire 1. Le reste découle de la définition de $\mathcal{B}_q$.
   (b) On construit deux bases directes $\underline{e}$ et $\underline{e}'$ telles que la matrice de q dans $\underline{e}$ est égale à celle de q' dans $\underline{e}'$. On procède pour cela exactement comme pour la preuve de 3.5 b). L'endomorphisme φ de $SL_2(\mathbb{Z})$ qui envoie $\underline{e}'$ sur $\underline{e}$ vérifie alors $q' = q \circ \varphi$.
8. Pour chaque q dans R_d, on considère un élément $(x;y)$ de $C^1_q(m)$ et on lui associe $\mathcal{B}_q(x;y)$ dans $T(d;m)$. Par 3.5 a), cette valeur est invariante pour l'action de $SO(q;\mathbb{Z})$ et ne dépend donc pas de l'élément choisi dans $SO(q;\mathbb{Z}):(x;y)$.
   On définit donc une application de l'ensemble des orbites $C^1_q(m)/SO(q;\mathbb{Z})$ dans $T(d;m)$. On obtient alors une application dont l'ensemble de départ est la réunion disjointe des $C^1_q(m)/SO(q;\mathbb{Z})$, pour q parcourant R_d, dont l'ensemble d'arrivée est $T(d;m)$.
   Par l'unicité montrée en 3.5 b), on a
   $$\#C^1_q(m)/SO(q;\mathbb{Z}) = \frac{\#C^1_q(m)}{\#SO(q;\mathbb{Z})};$$
   Si on montre que l'application construite est bijective, on aura donc l'égalité voulue.
   Pour des q choisis dans des classes distinctes, les $\mathcal{B}_q(x;y)$ sont distincts, par 3.7 b). De plus, pour q fixé dans R_d, $\mathcal{B}_q(x';y') = \mathcal{B}_q(x;y)$ implique $SO(q;\mathbb{Z}):(x;y) = SO(q;\mathbb{Z}):(x';y')$, par 3.5 b). On a donc l'injectivité.

Maintenant, si l'on part d'un élément $\overline{n}$ de $T(d;m)$, alors, par 3.6, on peut trouver une forme q, et un couple $(x;y)$ tels que $\overline{n} = \overline{\square}_q(x;y)$. L'élément $\overline{\square}_q(x;y)$, pour $(x;y)$ dans $C_q^1(m)$, ne dépend pas du représentant choisi dans la classe de q par 3.7 a), donc, on peut choisir q dans R_d, puis $(x;y)$ par 1.2.4. D'où la surjectivité.

4- Nombre de solutions d'une équation modulaire

1. Les éléments de $\mathbb{Z}/p^{\square}\mathbb{Z}$ sont les classes modulo $p^{\square}$ des éléments de $[0;p^{\square}-1]$. Un élément $\overline{x}$ est inversible si et seulement si x est premier avec $p^{\square}$. On se ramène donc à compter les entiers de $[0;p^{\square}-1]$ non multiples de p.
2. (a) Comme p est impair, son noyau est ± 1, de cardinal 2. Le nombre de carrés est donc
$$\#\mathrm{Im}(\ ) = \frac{\#(\mathbb{Z}/p\mathbb{Z})^*}{\#\ker} = \frac{p-1}{2}.$$
   (b) « Seulement si » découle du théorème de Lagrange qui dit que l'ordre d'un élément divise l'ordre du groupe, qui est ici égal à $p-1$.
   « Si » : par cardinalité, car le nombre de solutions d'une équation d'un polynôme de degré $\frac{p-1}{2}$ sur un corps (commutatif!) est inférieur à $\frac{p-1}{2}$.
3. On fait deux cas selon si v est un carré ou non modulo p. Comme p est impair et v non nul, il y a soit 0 soit 2 solutions.
4. (a) La surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/p\mathbb{Z}$ passe au quotient de $p^{\square}\mathbb{Z}$. L'image d'un élément $\overline{x}$ de $\mathbb{Z}/p^{\square}\mathbb{Z}$ est nulle si et seulement si x est multiple de p, et donc si et seulement si $\overline{x}$ est non inversible.
   Le morphisme $\square$ est la restriction à $(\mathbb{Z}/p^{\square}\mathbb{Z})^*$ de ce passage au quotient. Son image est donc $(\mathbb{Z}/p\mathbb{Z})^*$.
   Son noyau est donc d'ordre $\frac{p^{\square-1}(p-1)}{p-1} = p^{\square-1}$, qui est premier avec 2. Par l'identité de Bezout, il existe des entiers u et v tels que $2u + p^{\square-1}v = 1$. Tout élément x du noyau vaut, par le théorème de Lagrange : $x = x^1 = x^{2u+p^{\square-1}v} = (x^u)^2$.
   (b) « Seulement si » est clair car le passage au quotient est un morphisme.
   Montrons le « si » : par surjectivité du morphisme multiplicatif , l'image réciproque d'un carré contient un carré, et par la question précédente, tous les antécédents d'un carré fixé sont des carrés puisqu'ils sont tous égaux modulo le noyau de .
   Au bilan, on peut compter le nombre de carrés de $(\mathbb{Z}/p^{\square}\mathbb{Z})^*$ car ce sont les antécédents des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$; il y en a $\frac{p-1}{2} \cdot \#\ker = \frac{p^{\square-1}(p-1)}{2}$. En considérant le morphisme de groupe $\square : x \mapsto x^2$ de $(\mathbb{Z}/p^{\square}\mathbb{Z})^*$, on obtient que $\#\ker\square = 2$. On montre la dernière assertion comme en 3).
   On peut montrer que $\#\ker\square = 2$ *de façon plus élémentaire en prouvant tout simplement que si* a^2-1 *est multiple de* $p^{\square}$, p *impair, alors* $a-1$ *ou* $a+1$ *est multiple de* $p^{\square}$.
5. On décompose d'abord $\mathbb{Z}/m\mathbb{Z}$ par le lemme chinois (l'image d'un carré est un k-uplet de carrés), et on applique ensuite la question 4.4 b).
6. Montrons la première égalité. On montre tout d'abord l'égalité
$$\#T(d;m) = \frac{1}{2}\#\{x \in \mathbb{Z}/4m\mathbb{Z};\ x^2 = -\overline{d}_{4m}\};$$
   Cela provient de 3.2 et du fait que le noyau du morphisme naturel $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ est d'ordre 2.
   On montre ensuite l'égalité

$$\frac{1}{2}\#\{x \in \mathbb{Z}/4m\mathbb{Z};\ x^2 = -\bar{d}_{4m}\} = \#\{x \in \mathbb{Z}/m\mathbb{Z};\ x^2 = -\bar{d}_m\}$$

.

Effectivement, par le lemme chinois, qui identifie $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ à $\mathbb{Z}/4m\mathbb{Z}$ (m est impair), on se ramène à trouver les couples de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ dont le carré est $(-\bar{d}_4; -\bar{d}_m)$. On se sert donc du fait qu'un carré de $\mathbb{Z}/4\mathbb{Z}$ possède 2 racines carrées.

Enfin, la seconde égalité provient directement du développement du produit dans la question 4.5.

7. Pour tout v qui divise m, on note $\mathrm{val}_p(v) = 2s_p(v) + r_p(v)$, la division euclidienne de $\mathrm{val}_p(v)$ par 2. La bijection est donnée par $v \mapsto (l; e)$, où $l = \prod_p p^{r_p(v)}$ et $e = \prod_p p^{s_p(v)}$. La bijection inverse est donnée par $(l; e) \mapsto le^2$.
8. C'est juste une synthèse des questions 4.6 et 4.7. Il suffit de réindexer la somme en utilisant la bijection.

5- Nombre de solutions d'équations quadratiques.

1. Par 2.7, q et q' constituent un choix de représentants de S_{-20}. On a, par 3.7,

$$\#C_q(m) + \#C_{q'}(m) = \sum_{e>0; e^2|m} \#C_q^1(\frac{m}{e^2}) + \#C_{q'}^1(\frac{m}{e^2}):$$

Par 3.8 et 2.8, il vient donc

$$\#C_q(m) + \#C_{q'}(m) = 2 \sum_{e>0; e^2|m} \#T(20; \frac{m}{e^2}):$$

La dernière égalité est claire par 4.8.

2. (a) On fait opérer de façon cyclique $\mathbb{Z}/p\mathbb{Z}$ sur X. Les orbites singletonnes correspondent aux solutions de $px^2 = 1$; il y en a donc $1 + \left(\frac{p}{5}\right)$ par 4.3. Les autres orbites sont de cardinal p.

   (b) Le même qu'un espace vectoriel de dimension $n-1$ (existence d'une base !), donc 5^{n-1}.

   (c) On voit que l'on a bien un changement de variables (inversibilité).
   L'équation devient (puisque modulo 5, on a $-4 = 1$), $\sum_{j=1}^{a} u_j u'_j + u_p^2 = 1$. Si tous les u_j, $1 \leqslant j \leqslant a$ sont nuls, on a $2:5^a$ solutions. Sinon, chaque donnée de u_j, $1 \leqslant j \leqslant a$, non tous nuls et u_p quelconque fournit un hyperplan de solutions, soit, par la question qui précède, en $5^{a-1}:(5^a - 1):5 = 5^{p-1} - 5^a$ solutions. Soit en tout $5^{p-1} + 5^a$. Par Fermat, on a, modulo p, $1 + 5^a$ solutions.

   (d) Par 4.2 (b), on a donc $1 + \left(\frac{5}{p}\right)$ solutions à l'équations. Comme p est impair, et que le symbole de Legendre ne peut prendre que les valeurs 1 et -1, en comparant 5.2 a) et 5.2 c), on obtient l'égalité.

3. D'après la question 5.1, cela revient à trouver p tel que $1 + \left(\frac{-20}{p}\right)$ est non nul. Or, par multiplicativité du symbole de Legendre, ceci vaut $1 + \left(\frac{-5}{p}\right) = 1 + (-1)^{\frac{p-1}{2}} \left(\frac{5}{p}\right) = 1 + (-1)^{\frac{p-1}{2}} \left(\frac{p}{5}\right)$.
   Donc, ce nombre est non nul si et seulement si on est dans les deux cas suivants : soit p congru à 1 modulo 4 et p congru à 1, 4 modulo 5, soit p congru à 3 modulo 4 et p congru à 2,3 modulo 5. En utilisant l'isomorphisme du lemme chinois, on obtient bien l'assertion demandée.

4. Montrons la première équivalence, la seconde en découlera par la question qui précède.
   Si $p = x^2+5y^2$ alors p est congru à x^2+y^2 modulo 4 et donc ne peut être congru à 3 modulo 4. Par élimination p ne peut être congru qu'à 1 ou 9 modulo 20. Réciproquement, si p est congru à 1 ou 9 modulo 4, alors par la question précédente, p est représenté par x^2+5y^2 ou par $2x^2+2xy+3y^2$. Il suffit de montrer qu'il n'est pas représenté par $2x^2+2xy+3y^2$. Supposons $p = 2x^2+2xy+3y^2$, cela implique y impair et donc $x(x+y)$ pair. Donc modulo 4, p vaut $3y^2$ donc 3. Ce qui est impossible.

5. (a) Comme $[q]$ est ici la seule classe de forme quadratique possible, par congruence modulo 4 (voir question précédente), on obtient par la question 5.1

$$\#C_q(p^\alpha) = 2\sum_{0\le k\le \alpha}\left(\frac{-20}{p^k}\right) = 2\sum_{0\le k\le \alpha}\left(\frac{-20}{p}\right)^k = 2(1+\alpha)$$

   car $\left(\frac{-20}{p}\right) = 1$.

   (b) Il suffit de remarquer que dans ce cas $p^{2\alpha}$ est congru à 1 modulo 4 et $p^{2\alpha+1}$ à 3 modulo 4. La méthode est analogue.