UNIVERSITÉ DE RENNES 1

Préparation à l'agrégation

Exercices

Géométrie élémentaire

Exercice 1 : Trigonométrie du triangle

On considère un triangle ABC, et l'on note :

- α, β, γ les angles en A, B, C respectivement ;
- a, b, c les longueurs des côtés opposés à A, B, C respectivement ;
- p le demi-périmètre ;
- R le rayon du cercle circonscrit, r le rayon du cercle inscrit ;
- $\mathscr{A}$ l'aire du triangle.

Retrouver les formules bien connues suivantes.

1. $\alpha + \beta + \gamma = \pi$
2. $\cos\alpha = \frac{b^2+c^2-a^2}{2bc}$ (théorème d'Al-Kashi)
3. $\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R$
4. $\mathscr{A} = \frac{bc}{2}\sin\alpha = pr$
5. $\sin\alpha = \frac{2}{bc}\sqrt{p(p-a)(p-b)(p-c)}$
6. $\mathscr{A} = \sqrt{p(p-a)(p-b)(p-c)}$ (formule de Héron)
7. $\sin\frac{\alpha}{2} = \sqrt{\frac{(p-b)(p-c)}{bc}}$.

Quel est le rayon du cercle exinscrit en A, en fonction de a, b et c ?

Quelle est la distance de A au milieu de BC ?

Exercice 2

Soient A, B, C, A', B', C' six points d'un plan affine euclidien $\mathscr{E}$. On suppose les égalités de distances suivantes : $AB = A'B'$, $BC = B'C'$, $CA = C'A'$. Montrer qu'il existe une isométrie σ de $\mathscr{E}$ telle que $\sigma(A) = A'$, $\sigma(B) = B'$ et $\sigma(C) = C'$.

Exercice 3

Soient A, B, C trois points d'un plan euclidien $\mathscr{E}$. On note $a = BC$, $b = CA$, $c = AB$. Soit I l'image de A par projection orthogonale sur la droite (BC). La droite (AI) est appelée la

hauteur du triangle ABC issue de A. On suppose que le triangle ABC n'est pas rectangle, i.e. qu'il n'y a pas deux droites orthogonales parmis (AB), (BC) et (CA).

1. Montrer que $(\overrightarrow{BC} \mid \overrightarrow{BA}) = (\overrightarrow{BC} \mid \overrightarrow{BI})$ et $(\overrightarrow{CB} \mid \overrightarrow{CA}) = (\overrightarrow{CB} \mid \overrightarrow{CI})$.
2. Montrer que I est le barycentre de $(B, (\overrightarrow{CB} \mid \overrightarrow{CA}))$ et $(C, (\overrightarrow{BC} \mid \overrightarrow{BA}))$.
3. Montrer que $(\overrightarrow{BC} \mid \overrightarrow{BA}) = \frac{1}{2}\left(a^2 + c^2 - b^2\right)$.
4. Montrer que I est le barycentre de $(B, a^2 + b^2 - c^2)$ et $(C, c^2 + a^2 - b^2)$.
5. Montrer que I est le barycentre de $(B, (c^2 + a^2 - b^2)^{-1})$ et $(C, (a^2 + b^2 - c^2)^{-1})$.
6. Montrer que les trois hauteurs du triangle ABC ont un point commun, qui est barycentre de $(A, (b^2 + c^2 - a^2)^{-1})$, $(B, (c^2 + a^2 - b^2)^{-1})$ et $(C, (a^2 + b^2 - c^2)^{-1})$. (Ce point est appelé l'orthocentre du triangle).

Exercice 4

Montrer que l'aire d'un quadrilatère non croisé, inscrit dans un cercle, de côtés a, b, c, d, et de demi-périmètre $s = \frac{a+b+c+d}{2}$, est égale à $\sqrt{(s-a)(s-b)(s-c)(s-d)}$ (formule de Brahmagupta).

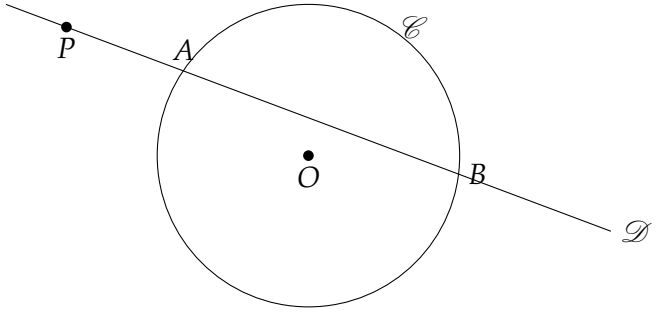
Exercice 5

Soient $e_1, \ldots, e_n$ des vecteurs de $\mathbb{R}^n$. Notons A la matrice de la famille $e_1, \ldots, e_n$ dans la base canonique de $\mathbb{R}^n$. Notons $(\cdot \mid \cdot)$ le produit scalaire usuel de $\mathbb{R}^n$, et soit $G = \left((e_i \mid e_j)\right)_{1 \leqslant i,j \leqslant n}$.
Montrer que $\det(G) = \det(A)^2$.

Exercice 6

On se place dans le plan euclidien. Soit $\mathscr{C}$ un cercle, de centre O et de rayon r, et soit P un point.

On considère une droite $\mathscr{D}$ passant par P et coupant $\mathscr{C}$ en deux points A et B. On appelle puissance de P par rapport à $\mathscr{C}$ le produit $\overline{PA}\,\overline{PB}$ (en tenant compte des orientations). Montrer que ce produit ne dépend pas du choix de $\mathscr{D}$. Discuter le cas où $\mathscr{D}$ est tangente à $\mathscr{C}$.



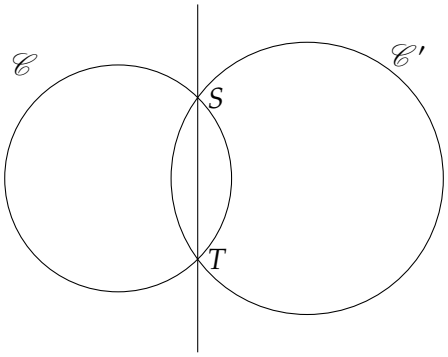
Montrer que :

(i) P est à l'intérieur du disque de bord $\mathscr{C}$ si et seulement si sa puissance est strictement négative ;

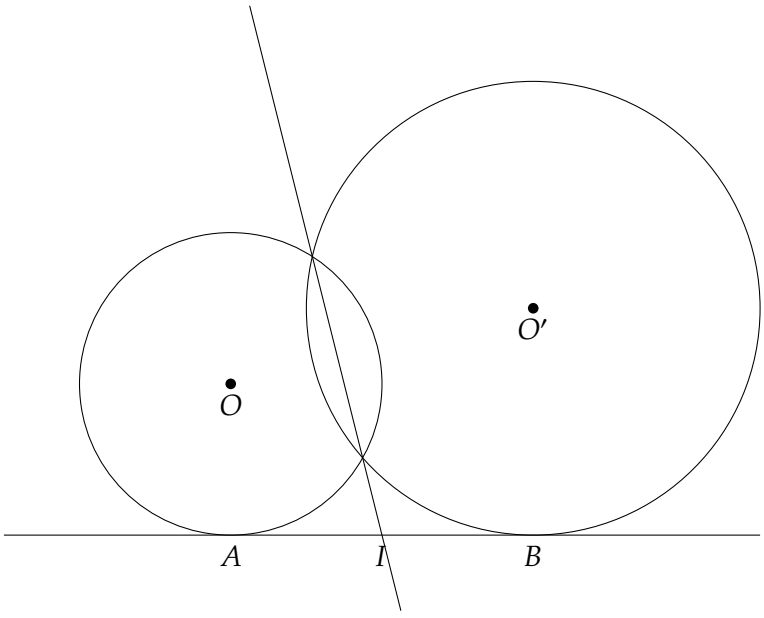
(ii) P est sur $\mathscr{C}$ si et seulement si sa puissance est nulle ;

(iii) P est à l'extérieur du disque de bord $\mathscr{C}$ si et seulement si sa puissance est strictement positive.

On considère deux cercles $\mathscr{C}$ et $\mathscr{C}'$ non concentriques. Montrer que l'ensemble des points ayant la même puissance par rapport à $\mathscr{C}$ et à $\mathscr{C}'$ est une droite, orthogonale à la droite passant par les centres de $\mathscr{C}$ et $\mathscr{C}'$. Si $\mathscr{C}$ et $\mathscr{C}'$ se coupent en deux points S et T, montrer que c'est la droite (ST).



Dans la figure suivante, qu'est le point I ?



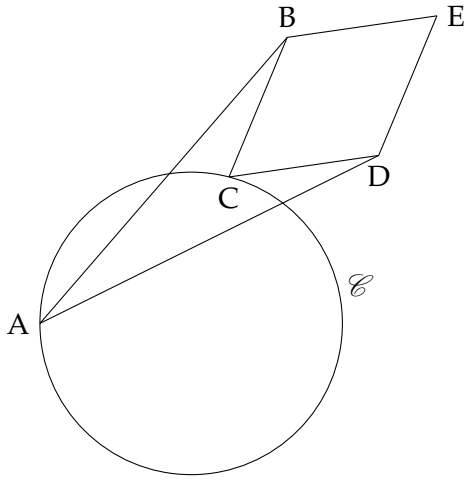
Exercice 7 : Trisection de l'angle

Rappeler pourquoi la trisection de l'angle ne peut pas être réalisée en général à la règle et au compas. Donner un exemple où la trisection à la règle et au compas est possible.

Montrer que la trisection de l'angle peut être réalisée avec une règle graduée (i.e. une règle portant deux points à distance fixée) et un compas.

Exercice 8 : Inverseur

On considère la figure suivante, avec $AB = AD$ et $BC = CD = DE = EB$ des longueurs fixées.



Montrer que, lorsque le point C parcourt le cercle $\mathscr{C}$ (le point A est fixé, et les points B, C, D, E bougent en conséquence), le point E reste sur une même droite.

Exercice 9

Soit E un espace vectoriel euclidien, de dimension n. Notons $(\cdot \mid \cdot)$ le produit scalaire. Soit $(e_i)_{1 \leqslant i \leqslant m}$ une famille d'éléments de E, telle que

$$(e_i \mid e_j) < 0 \qquad (\forall i, j \in \{1, \dots, m\}, i \neq j).$$

Montrer que $m \leqslant n + 1$.

Exercice 10

Soient E et F deux espaces vectoriels euclidiens. Soit $f : E \to F$ une application (ensembliste) telle que $f(0) = 0$ et f préserve les distances (i.e. $\left\|f(x) - f(y)\right\| = \left\|x - y\right\|$, quels que soient $x, y \in E$). Montrer que f est une isométrie (en particulier, f est linéaire).

Montrer que ce n'est plus vrai si l'on omet l'hypothèse $f(0) = 0$.

Soit $\theta : \mathbb{R}_+ \to \mathbb{R}$ une application, et soit $f : \mathbb{C} \to \mathbb{C}$ définie par $f(z) = ze^{i\theta(|z|)}$. On munit $\mathbb{C}$ du produit scalaire $u, v \mapsto \mathscr{R}e(\overline{u}v)$. Montrer que l'application f vérifie $f(0) = 0$ et $\left\|f(z)\right\| = \|z\|$ $(\forall z \in \mathbb{C})$. Montrer que f est une isométrie si et seulement si θ est constante.

Exercice 11

On considère la boule unité de $M_n(\mathbb{R})$ muni de la norme d'application linéaire associée à la norme euclidienne (i.e. $\|M\| = \sup_{x\in\mathbb{R}^n\setminus\{0\}} \frac{\|M(x)\|_2}{\|x\|_2}$. On dit qu'un point de cette boule est extrémal s'il n'est pas le milieu d'un segment non réduit à un point dont les extrémités sont dans la boule. L'objectif de cet exercice est de montrer que l'ensemble des points extrémaux de la boule unité est exactement l'ensemble $O_n(\mathbb{R})$ des matrices orthogonales.

1. Notons $\mathscr{B}$ la boule unité. Si $A = \frac{U+V}{2}$ est orthogonale et si U et V sont dans $\mathscr{B}$, montrer que U et V sont orthogonales et que pour tout $x \in \mathbb{R}^n$ les vecteurs $U(x)$ et $V(x)$ sont colinéaires. En déduire que A est extrémale.
2. Si $A \in \mathscr{B} \setminus O_n(\mathbb{R})$, montrer que A n'est pas extrémale. On pourra utiliser la décomposition polaire de la matrice A, noter qu'une matrice symétrique peut être diagonalisée dans une base orthonormée, et noter que les valeurs propres ainsi obtenues sont dans l'intervalle $[-1, 1]$.

Exercice 12 : Topologie du plan projectif réel

Montrer que $\mathbf{P}^2(\mathbb{R})$ est homéomorphe à

$$S^2 \;/\; r \sim -r$$

(où S^2 désigne la sphère d'équation $x^2 + y^2 + z^2 = 1$ dans $\mathbb{R}^3$).

Montrer que la calotte polaire $x \geqslant \frac{1}{2}$ est homéomorphe à un disque.

Posons

$$M = S^1 \times \left]-\frac{1}{2}, \frac{1}{2}\right[\;/\; (x, y) \sim (-x, -y).$$

Montrer que $\mathbf{P}^2(\mathbb{R})$ s'obtient en collant un disque le long du bord de M.

Montrer en considérant la projection sur la première composante que l'on peut définir une surjection continue $p\colon M \to S^1$ telle que l'image inverse d'un point soit homéomorphe à $\left]-\frac{1}{2}, \frac{1}{2}\right[$.

Montrer que le complémentaire de $S^1 \times \{0\} \;/\; (x, 0) \sim (-x, 0)$ dans M est connexe.

Soit $x \in S^1$. Montrer que $M \setminus p^{-1}(x)$ est homéomorphe à un rectangle. En déduire que M est un ruban de Möbius, et que $\mathbf{P}^2(\mathbb{R})$ s'obtient un collant un disque le long du bord d'un ruban de Möbius.

Théorie des groupes

Exercice 13

La réunion de deux sous-groupes peut-elle être un sous-groupe ? Préciser en donnant une condition nécessaire et suffisante.

Exercice 14

Écrire $(\mathbb{Z}/651\mathbb{Z})^\times$ comme produit de groupes cycliques, et expliciter l'isomorphisme.

Exercice 15

Soit G un groupe abélien. On suppose que G contient un élément x d'ordre m et un élément y d'ordre n. Donner un élément de G qui soit d'ordre $\mathrm{ppcm}(m, n)$.

Exercice 16

Montrer que si $m > 2$ et $n > 2$ sont deux entiers premiers entre eux, le groupe $(\mathbb{Z}/mn\mathbb{Z})^\times$ n'est pas cyclique.

Montrer que si $p > 2$ est premier et $k \geqslant 1$, alors le groupe $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique.

Pour quels entiers $n \geqslant 1$ le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ?

Exercice 17

Soit G un groupe fini, et soit p le plus petit diviseur non trivial de l'ordre de G. Montrer que tout sous-groupe de G d'indice p est distingué.

Exercice 18 : Sous-groupes d'ordre 6 de $\mathfrak{A}_4$

Montrer simplement que $\mathfrak{A}_4$ n'a pas de sous-groupe d'ordre 6.

Exercice 19 : Lemme de Cauchy

Rappelons l'énoncé du lemme de Cauchy : si G est un groupe fini d'ordre multiple d'un nombre premier p, alors G contient un élément d'ordre p.

1. Montrer le lemme de Cauchy dans le cas où G est cyclique.
2. Montrer le lemme dans le cas où G est un produit de groupes cycliques. Montrer si G est abélien alors le lemme de Cauchy se déduit du théorème de structure des groupes abéliens ?
3. Montrer que le lemme de Cauchy se déduit aussi de l'existence des sous-groupes de Sylow (sans supposer que G est abélien).
4. Sans utiliser les résultats de classification des groupes abéliens, montrer le lemme dans ce cas. (On pourra procéder par récurrence sur l'ordre du groupe).
5. Déduire le lemme de Cauchy dans le cas général à partir du cas abélien. (On pourra considérer l'action de G sur lui-même par conjugaison).

6. Démontrer directement le lemme de Cauchy dans le cas général. (On pourra considérer l'action par permutation circulaire de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble des p-uples d'éléments de G dont le produit est l'élément neutre).

Exercice 20

Quel est le centre du groupe $\mathrm{GL}_n(K)$?

Exercice 21 : Groupes d'ordre 12

Quelles sont les classes d'isomorphisme de groupes non abéliens d'ordre 12 ? Qu'en est-il des groupes abéliens ?

Exercice 22 : Groupes de petit cardinal

Quelles sont les classes d'isomorphisme de groupes d'ordre inférieur ou égal à 8 ?

Anneaux et corps

Exercice 23

1. Soit A un anneau euclidien (qui n'est pas un corps). Montrer qu'il existe un $x \in A$, non nul et non inversible, tel que la projection canonique $A \twoheadrightarrow A/(x)$ induise une surjection $A^\times \cup \{0\} \twoheadrightarrow A/(x)$.
2. Montrer que $A/(x)$ est alors un corps.
3. On considère l'anneau $\mathbb{Z}[\sqrt{N}]$, pour un entier $N < 0$ sans facteur carré. Déterminer $\mathbb{Z}[\sqrt{N}]^\times$.
4. Si $x \in \mathbb{Z}[\sqrt{N}]$, calculer le cardinal de $\mathbb{Z}[\sqrt{N}]/(x)$.
5. en déduire que si $N < -3$ alors l'anneau $\mathbb{Z}[\sqrt{N}]$ n'est pas euclidien.
6. Qu'en est-il pour $N = -1$? pour $N = -2$?

Exercice 24

Soit A un anneau commutatif intègre. Soit I l'idéal de $A[X, Y]$ engendré par $X + Y$.

1. Montrer que $A[X, Y]/I$ est isomorphe à l'anneau $A[X]$.
2. L'idéal I est-il premier ? Est-il maximal ?

Exercice 25

Soit A un anneau commutatif. On dit que $x \in A$ est nilpotent s'il existe $n > 0$ tel que $x^n = 0$.

1. Montrer que l'ensemble N des éléments nilpotents de A est un idéal de A.
2. Montrer que le quotient A/N n'a pas d'élément nilpotent.
3. Trouver un exemple d'anneau A avec deux éléments x et y nilpotents tels que $x + y$ n'est pas nilpotent.
4. Montrer que A n'a pas d'élément nilpotent si et seulement si tout élément inversible de $A[X]$ est constant.

Exercice 26

On considère un polynôme unitaire de degré 4,

$$P(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{C}[X].$$

1. Montrer que l'on peut voir les racines de P comme les abscisses des points d'intersection de deux coniques, dont l'une est une parabole.
2. On considère le faisceau de coniques engendré par ces deux coniques. Montrer que rechercher les coniques dégénérées dans ce faisceau revient à chercher les racines d'un polynôme de degré 3.
3. En considérant une de ces coniques dégénérées, montrer que l'on peut ramener la recherche des racines de P à celle des racines d'un polynôme de degré 3 puis de polynômes de degré 2. En déduire que les racines de P peuvent s'exprimer à l'aide de radicaux. (On suppose connue la formule de Cardan-Tartaglia).

Exercice 27

Soit A un anneau commutatif unitaire, qui contient exactement $n > 0$ diviseurs de 0. Montrer que A a au plus $(n + 1)^2$ éléments. Donner un exemple où il y a égalité.

Corps finis

Exercice 28

Montrer que tout anneau commutatif intègre fini est un corps.

Exercice 29

Un corps fini peut-il être algébriquement clos ?

Exercice 30

Montrer que tout morphisme de corps est injectif.

Exercice 31

Soit $P = X^3 + 2X + 1 \in \mathbb{F}_3[X]$. Posons $\mathbb{L} = \mathbb{F}_3[X]/(P)$ et α la classe de X dans $\mathbb{L}$.

1. Montrer que $\mathbb{L}$ est un corps. Quelle est sa caractéristique ? Son cardinal ? Donner une base du $\mathbb{F}_3$-espace vectoriel $\mathbb{L}$.
2. Quels sont les ordres possibles pour les éléments de $\mathbb{L}^\times \setminus \mathbb{F}_3^\times$ (dans le groupe $\mathbb{L}^\times$).
3. L'objet de la question est de montrer que α est un générateur de $\mathbb{L}^\times$.
   (a) Montrer que $\alpha^{13} = -1$ si et seulement si P divise $(X-1)^4X + 1$ dans $\mathbb{F}_3[X]$.
   (b) Conclure.
4. Le polynôme $Q = X^4 + X^3 + X^2 + X + 1$ a-t-il une racine dans $\mathbb{L}$?

Exercice 32

Soit $P = X^2 + X + 2 \in \mathbb{F}_5[X]$. On note $\mathbb{K} = \mathbb{F}_5[X]/(P)$ et α la classe de X dans $\mathbb{K}$.

1. Montrer que $\mathbb{K}$ est un corps. Quelle est sa caractéristique ? Son cardinal ? En donner une base comme $\mathbb{F}_5$-espace vectoriel.
2. Exprimer toutes les puissances distinctes de α dans cette base. Quel est l'ordre de α dans $\mathbb{K}^\times$?
3. Montrer que $\mathbb{F}_5 = \left\{x \in \mathbb{K} / x = x^5\right\}$.
4. Soit $a \in \mathbb{K} \setminus \mathbb{F}_5$. Montrer que le polynôme $P_a = (X-a)(X-a^5)$ est irréductible dans $\mathbb{F}_5[X]$.
5. Montrer que si $Q \in \mathbb{F}_5[X]$ alors a est racine de Q si et seulement si P_a divise Q.
6. Factoriser le polynôme $X^{25} - X$ dans $\mathbb{F}_5[X]$ et donner les racines dans $\mathbb{K}$ de chaque facteur.

Exercice 33

Quels sont les sous-corps de $\mathbb{F}_{64}$?

Exercice 34

On considère la suite d'entiers définie par

(i) $u_0 = 3, u_1 = 0, u_2 = 2$;

(ii) $u_{n+3} = u_n + u_{n+1}$ pour $n \geqslant 0$.

Montrer que si p est un nombre premier, alors u_p est multiple de p. (On pourra déterminer l'image de u_n dans un corps bien choisi. Notez que, comme pour le petit théorème de Fermat, la réciproque est fausse).

Exercice 35 : Nombres de Carmichael

Un entier n est appelé nombre de Carmichael si, pour tout entier a entre 1 et $n-1$ premier avec n, on a $a^{n-1} = 1 \pmod{n}$.

1. Soit $N > 1$ un entier. On suppose qu'il existe un nombre premier p tel que $p^2 \mid N$. Posons $a = 1 + \frac{N}{p}$. Montrer que a est d'ordre p dans $(\mathbb{Z}/N\mathbb{Z})^\times$.
2. En déduire qu'un nombre de Carmichael est toujours sans facteur carré.
3. Montrer qu'un entier $n > 1$ sans facteur carré est un nombre de Carmichael si et seulement si pour tous les nombre premiers p divisant n on a $(p-1) \mid (n-1)$.

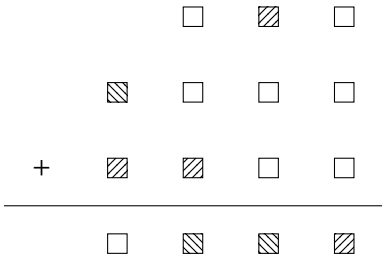
Exercice 36

Décomposer le polynôme $X^4 + 1$ en produit de facteurs irréductibles dans $\mathbb{F}_7[X]$.

Équations diophantiennes

Exercice 37

Retrouver les chiffres correspondant à l'addition.



Exercice 38

Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également, et de donner le reste au cuisinier. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et 6 d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Survient alors un naufrage, et seuls 6 pirates, le cuisinier et le trésor sont sauvés. Le partage laisserait 5 pièces d'or à ce dernier. Il décide alors d'empoisonner les autres survivants. Quelle est la fortune minimale que peut espérer le cuisinier ?

Exercice 39

Déterminer tous les entiers $n > 1$ tels que $n^2 \mid 2^n + 1$.

Exercice 40

Montrer qu'il n'y a pas d'entier impair $n > 1$ tel que $a^{n-1} \equiv -1 \pmod{n}$ pour un certain $a \in \mathbb{Z}$.

Exercice 41

On considère une conique $\mathscr{C}$ du plan affine, identifié à $\mathbb{R}^2$ après choix d'un système de coordonnées.

1. Montrer que les coordonnées des points d'intersection de $\mathscr{C}$ avec une droite sont données par des équations de degré au plus 2. En déduire qu'il y a au plus deux points d'intersection.
2. On considère une droite dont un point d'intersection avec $\mathscr{C}$ est connu. Montrer que les coordonnées de l'autre point d'intersection (s'il existe) sont données par des équations de degré 1.
3. Si $\mathscr{C}$ est donnée par une équation définie sur $\mathbb{Q}$ et si l'on connaît sur $\mathscr{C}$ un point à coordonnées rationnelles, montrer que l'on peut paramétrer les points de $\mathscr{C}$ à coordonnées rationnelles par une famille de droites de pentes rationnelles.

En déduire les solutions entières de l'équation $a^2 + b^2 = c^2$.

Exercice 42

1. Trouver tous les entiers a, b, c vérifiant $1 < a < b < c$ et tels que $(a-1)(b-1)(c-1)$ divise $abc - 1$.
2. Résoudre $3x^2 - y^4 = x^3 - 8y^3 + 50$ avec x et y entiers positifs.

Dénombrement

Exercice 43

Si n est un entier naturel non nul, on appellera *partition de n* une égalité

$$n = n_0 + \cdots + n_k$$

avec $n_0, \cdots, n_k$ des entiers naturels non nuls.

Montrer que le nombre de partitions de n en entiers impairs est égal au nombre de partitions de n en entiers distincts, en construisant une bijection explicite entre les deux. (On pourra considérer l'écriture en base deux des entiers n_i et de leur mutliplicité).