MATHS & EXPERT

Collection « Concours Préparatoires » — R. Abed

CLASSES PRÉPARATOIRES MPSI

Concours d'Entrée en Première Année MPSI

Lydex & Prépa Zahraoui

Compilation intégrale des sujets de Mathématiques

2019 – 2021 – 2022 – 2023 – 2024

Au programme :

- ✔ Analyse : suites, fonctions, intégrales, équations fonctionnelles, séries
- ✔ Algèbre : matrices, réduction, arithmétique, groupes, anneaux
- ✔ Problèmes classiques : Newton, fonction Γ, formule de Legendre, $SL_2(\mathbb{Z})$
- ✔ Corrigés synthétiques, fiches astuces et méthodes en fin d'ouvrage

Centres AZ-CPGE (Al Zahrawi) | CPGE Abulcasis

2024/2025

Avant-propos

Ce document rassemble l'intégralité des épreuves de mathématiques du **Concours d'Entrée en Première Année MPSI** (Centres AZ-CPGE Al Zahrawi et CPGE Abulcasis) sur la période **2019–2024**. L'ensemble des exercices et problèmes a été réorganisé thématiquement et réparti en deux grandes parties :

- **Partie I — Analyse** : fonctions, intégrales à paramètre, suites récurrentes, équations fonctionnelles, méthode de Newton, fonction Gamma, intégrale de Gauss ;
- **Partie II — Algèbre** : matrices et réduction, arithmétique dans $\mathbb{Z}$, anneaux et corps, groupe $SL_2(\mathbb{Z})$, dénombrement.

Chaque énoncé est accompagné d'une étiquette indiquant son **millésime d'origine**, permettant de repérer l'évolution du niveau d'exigence du concours au fil des sessions. En fin d'ouvrage, une **section de corrigés synthétiques** reprend les exercices les plus emblématiques — méthode de Newton, formule de Legendre, fonction Γ d'Euler et intégrale de Gauss, sommes de deux carrés, générateurs de $SL_2(\mathbb{Z})$ — avec, pour chacun, les étapes clés de la démonstration et une **fiche méthode** dégageant les techniques transférables à d'autres exercices.

Mode d'emploi

- Chaque énoncé porte une étiquette Année rappelant le concours d'origine.
- Les encadrés **teal** signalent un rappel de cours ou une définition utile.
- Les encadrés **or** signalent une astuce de rédaction ou de calcul.
- Les encadrés **corail** en fin de document contiennent les corrigés.

Math & Expert — R. Abed
Professeur Agrégé de Mathématiques

Table des matières

CHAPITRE 1

Analyse

Cette partie regroupe l'ensemble des exercices et problèmes d'analyse des sessions 2019 à 2024, organisés par grand thème : fonctions définies par une intégrale, équations fonctionnelles, méthode de Newton, fonction Γ et intégrale de Gauss, dérivation sous le signe intégral.

1. Fonctions définies par une intégrale — continuité et dérivabilité

Exercice 1.1 — Étude d'une fonction définie par une intégrale à bornes variables

2019

Soit $f : \mathbb{R}_+^* \to \mathbb{R}$ définie par $f(x) = \displaystyle\int_x^{2x} \frac{1}{\ln(1+t^2)}\,\mathrm{d}t$ et $g : \mathbb{R}_+^* \to \mathbb{R}$ définie par $g(x) = \displaystyle\int_1^x \frac{1}{\ln(1+t^2)}\,\mathrm{d}t$.

1. Exprimer f en fonction de g.

2. Montrer que f est dérivable sur $]0,+\infty[$ et que

$$\forall x > 0, \quad f'(x) = \frac{1}{\ln(1+4x^2)} - \frac{1}{\ln(1+x^2)}.$$

3. Montrer que

$$\forall x > 0, \quad \frac{x}{\ln(1+4x^2)} \leqslant f(x) \leqslant \frac{x}{\ln(1+x^2)}.$$

(a) En déduire les limites de f en $+\infty$ et en 0.

(b) En déduire que la courbe représentative de f présente au voisinage de $+\infty$ une branche parabolique.

4. Donner le tableau de variation de f.

5. Donner l'allure de la courbe représentative de f.

Rappel

Pour une fonction définie par $f(x) = \int_{u(x)}^{v(x)} h(t)\,\mathrm{d}t$ avec u, v dérivables et h continue, on dérive

via une primitive H de h : $f(x) = H(v(x)) - H(u(x))$, d'où $f'(x) = v'(x)\,h(v(x)) - u'(x)\,h(u(x))$.

Exercice 1.2 — Continuité d'une fonction définie par une intégrale paramétrée

2023

On considère $f : [0,1] \to \mathbb{R}$ continue et $\varphi, \psi : \mathbb{R} \to \mathbb{R}$ définies par

$$\forall x \in \mathbb{R}, \quad \varphi(x) = \int_0^1 f(t)\sin(xt)\ \mathrm{d}t \quad \text{et} \quad \psi(x) = \int_0^1 t\,f(t)\cos(xt)\ \mathrm{d}t.$$

1. Montrer que $\forall u, v \in \mathbb{R},\ |\sin(u) - \sin(v)| \leqslant |u - v|$.

2. En déduire que φ est continue sur $\mathbb{R}$.

3. Montrer que $\forall u, v \in \mathbb{R},\ |\sin(u) - \sin(v) - (u-v)\cos(v)| \leqslant \dfrac{(u-v)^2}{2}$.

4. En déduire que φ est dérivable sur $\mathbb{R}$ et que $\varphi' = \psi$.

(*Cet exercice s'inscrit dans un problème plus large, voir Exercice 2 du concours 2023, comportant également une question préliminaire sur* $\displaystyle\int_a^x (x-t)g''(t)\ \mathrm{d}t = g(x) - g(a) - (x-a)g'(a)$.)

★ **Astuce**

Pour montrer la continuité ou la dérivabilité d'une fonction $\varphi(x) = \int_0^1 f(t)\,\Phi(x,t)\ \mathrm{d}t$, on majore $|\Phi(x,t) - \Phi(y,t)|$ **uniformément en** t par une quantité ne dépendant que de $|x-y|$ (souvent via une inégalité de type accroissements finis sur sin ou cos), puis on intègre cette majoration sur $[0,1]$.

Exercice 1.3 — Fonction de classe C^∞ définie par une intégrale — récurrence

Soit f une fonction de classe C^2 sur $[a,b]$ et $x \in]a,b]$. On définit $g : [a,b] \to \mathbb{R}$ par

$$\forall t \in [a,b], \quad g(t) = f(x) - f(t) - f'(t)(x-t) - A(x-t)^2$$

où A est une constante réelle telle que $g(a) = 0$.

1. Justifier que g est de classe C^1.

2. Montrer qu'il existe $c \in]a,x[$ tel que $g'(c) = 0$.

3. En déduire la formule de Taylor-Lagrange : $\exists\, c \in [a,x]$ tel que

$$f(x) = f(a) + f'(x)(x-a) + \frac{f''(c)}{2}(x-a)^2.$$

Partie I — Étude de $\displaystyle F(x) = \int_0^1 f(xu)g(u)\ \mathrm{d}u$**.** On suppose $f, g : \mathbb{R} \to \mathbb{R}$ continues et non nulles.

4. Justifier que F est une application de $\mathbb{R}$ vers $\mathbb{R}$.

5. Soit $x_0 \in \mathbb{R}$ fixé, $I = [-|x_0| - 1, |x_0| + 1]$ et, pour $h \in [-1,1]$,

$$\Delta_h = \int_0^1 |f(x_0u + hu) - f(x_0u)|\ \mathrm{d}u.$$

(a) Vérifier que $\forall h \in [-1,1], \forall u \in [0,1]$, on a $x_0u \in I$ et $x_0u + hu \in I$.

(b) Soit $\varepsilon > 0$ fixé. En utilisant le théorème de Heine, montrer que $\exists\, \alpha > 0,\ \forall h \in [-\alpha, \alpha],\ \Delta_h \leqslant \varepsilon$.

6. En déduire que F est continue sur $\mathbb{R}$.

7. On suppose f de classe C^2 sur $\mathbb{R}$.

(a) Justifier l'existence de $M_1, M_2 > 0$ tels que $\forall t \in I,\ |f''(t)| \leqslant M_1$ et $|g(t)| \leqslant M_2$.

(b) En utilisant Taylor-Lagrange, montrer que

$$\forall h \in [-1,1], \quad \left| F(x_0+h) - F(x_0) - h \int_0^1 u f'(x_0 u) g(u)\ \mathrm{d}u \right| \leqslant \frac{h^2 M_1 M_2}{6}.$$

(c) En déduire que F est dérivable en x_0, en donnant une expression de $F'(x_0)$.

8. Montrer que F est de classe C^1 sur $\mathbb{R}$.

9. On suppose f de classe C^∞ sur $\mathbb{R}$. Établir par récurrence que F est de classe C^∞ sur $\mathbb{R}$ et que

$$\forall p \in \mathbb{N},\ \forall x \in \mathbb{R}, \quad F^{(p)}(x) = \int_0^1 u^p f^{(p)}(xu) g(u)\ \mathrm{d}u.$$

2. Équations fonctionnelles

Rappel

La densité de $\mathbb{Q}$ dans $\mathbb{R}$ est l'outil clé pour passer d'une équation fonctionnelle vérifiée sur $\mathbb{Q}$ à une équation vérifiée sur $\mathbb{R}$ tout entier, **à condition de disposer d'un argument de continuité**.

Exercice 2.1 — Équations de Cauchy — additive, multiplicative et sur la norme euclidienne

Partie 1 — Densité de $\mathbb{Q}$ dans $\mathbb{R}$.

1. Soient $u, v \in \mathbb{R}$ tels que $u < v$.

(a) Montrer que $\exists\, q \in \mathbb{N}^*$ tel que $\dfrac{1}{q} < v - u$.

(b) En déduire que $\exists\, r \in \mathbb{Q}$ tel que $u < r < v$. On dit que $\mathbb{Q}$ est dense dans $\mathbb{R}$.

2. Soit $x \in \mathbb{R}$. Montrer que $\exists\, (r_n)_n$ une suite de rationnels telle que $r_n \to x$.

3. Soit $f : \mathbb{R} \to \mathbb{R}$ continue en 0 et vérifiant $\forall x, y \in \mathbb{R},\ f(x+y) = f(x) + f(y)$.

(a) Montrer que f est continue sur $\mathbb{R}$.

(b) Montrer que $\forall r \in \mathbb{Q},\ f(r) = r f(1)$.

(c) Conclure que $f(x) = x \cdot f(1)$ pour tout $x \in \mathbb{R}$.

4. Soit $f : \mathbb{R} \to \mathbb{R}$ continue, non nulle, telle que $\forall x, y \in \mathbb{R},\ f(x+y) = f(x)f(y)$.

(a) Montrer que $\forall x \in \mathbb{R},\ f(x) > 0$.

(b) En posant $g(x) = \ln(f(x))$, montrer que $\exists\, \lambda \in \mathbb{R}$ tel que $f(x) = \mathrm{e}^{\lambda x}$.

5. Soit $f : \mathbb{R} \to \mathbb{R}$ continue non nulle telle que $\forall x, y \in \mathbb{R},\ f\left(\sqrt{x^2+y^2}\right) = f(x)f(y)$.

(a) Montrer que si f est non nulle, alors $f > 0$.

(b) En considérant $g : \mathbb{R}^+ \to \mathbb{R}$, $g(x) = f(\sqrt{x})$, déterminer l'expression de f.

6. Déterminer les fonctions $f : \mathbb{R}^+ \to \mathbb{R}$ continues telles que $\forall x, y \in \mathbb{R}^+,\ f(xy) = xf(y) + yf(x)$.
(*On pourra commencer par considérer* $g :]0, +\infty[\to \mathbb{R}$, $g(x) = \dfrac{f(x)}{x}$.)

Partie 2 — Une équation de type Tchebychev.
On cherche les fonctions f définies sur $\mathbb{R}$, à valeurs dans $[-1, 1]$, vérifiant $f(2x) = 2(f(x))^2 - 1$ pour tout $x \in \mathbb{R}$, avec $f(0) = 1$ et telles que $\dfrac{1 - f(x)}{x^2}$ admette une limite a quand $x \to 0$.

1. Justifier que tout $x \in [-1, 1]$ s'écrit de façon unique $x = \cos(\theta)$ avec $\theta \in [0, \pi]$.

2. Vérifier $\lim\limits_{\theta \to 0} \dfrac{1 - \cos(\theta)}{\theta^2} = \dfrac{1}{2}$ et montrer, pour $\theta \in [0, \frac{\pi}{2}]$:

$$\frac{2\theta}{\pi} \leqslant \sin(\theta) \quad \text{et} \quad \cos(\theta) \leqslant 1 - \frac{\theta^2}{\pi}.$$

3. Soit f une solution. On pose, pour x fixé et $n \in \mathbb{N}$, $f\left(\dfrac{x}{2^n}\right) = \cos(\theta_n)$ avec $\theta_n \in [0, \pi]$.

(a) Montrer que f est continue en 0 et que $\theta_n \to 0$.

(b) Montrer qu'il existe N tel que pour $n \geqslant N$, $\theta_{n+1} = \dfrac{\theta_n}{2}$. Établir que $a \geqslant 0$ et que $f(x) = \cos\left(x\sqrt{2a}\right)$.

3. Méthode de Newton et suites récurrentes

Exercice 3.1 — Méthode de Newton — convergence quadratique

Soient $a < b$ et $f : [a, b] \to \mathbb{R}$ deux fois dérivable, f'' continue, telle que :

$$f(a) > 0, \quad f(b) < 0, \quad \forall x \in [a, b],\ f'(x) < 0, \quad \forall x \in [a, b],\ f''(x) > 0.$$

I. Étude d'une fonction.

1. Montrer que $f(x) = 0$ admet une unique solution $c \in]a, b[$.

2. Soit $x_0 \in [a, b]$. Déterminer le point d'intersection de la tangente en x_0 avec l'axe des abscisses. On note $g(x) = x - \dfrac{f(x)}{f'(x)}$.

3. Montrer que g est dérivable, g' continue sur $[a, b]$, et calculer g'.

4. Étudier les variations de g.

5. On admet l'existence de $m, M > 0$ tels que $\forall x \in [a, b],\ |f'(x)| \geqslant m$ et $|f''(x)| \leqslant M$. En appliquant le TAF à f puis à f', montrer l'existence de $L > 0$ tel que

$$\forall x \in [a, b], \quad |g(x) - c| \leqslant L \cdot |x - c|^2.$$

II. Étude d'une suite. Soit (u_n) définie par $u_0 = a$, $u_{n+1} = g(u_n)$.

6. Montrer que (u_n) est croissante et majorée par c.

7. Montrer que (u_n) converge vers c.

8. À l'aide de la question 5, montrer qu'il existe $k > 0$ tel que

$$\forall n \in \mathbb{N}, \quad |u_n - c| \leqslant k \left(\frac{c-a}{k}\right)^{2^n}.$$

★ Astuce

La méthode de Newton converge **quadratiquement** : l'erreur est majorée par $L \cdot |x_n - c|^2$, ce qui se traduit par une décroissance en k^{1-2^n} – le nombre de décimales exactes double presque à chaque itération. Le couple d'hypothèses signe de f' / signe de f'' garantit la monotonie et la convexité nécessaires à l'encadrement.

4. Fonction Gamma et intégrale de Gauss

Rappel

L'**intégrale de Gauss** $\displaystyle\int_0^{+\infty} \mathrm{e}^{-t^2}\,\mathrm{d}t = \frac{\sqrt{\pi}}{2}$ est un résultat fondamental qui apparaît dans de nombreux problèmes de concours, le plus souvent obtenu **sans** recourir aux intégrales doubles, via une fonction auxiliaire dont on calcule la dérivée.

Exercice 4.1 — Dérivation sous le signe intégral et calcul de l'intégrale de Gauss

Soit f définie sur $\mathbb{R}$ par $f(x) = \displaystyle\int_0^{\pi/4} \exp\left(\frac{-x}{\cos^2(t)}\right)\,\mathrm{d}t$, et F définie par $F(x) = \displaystyle\int_0^{x} \mathrm{e}^{-u^2}\,\mathrm{d}u$. On admet que F admet une limite réelle en $+\infty$, qu'on se propose de calculer.

1. Justifier que F est dérivable sur $\mathbb{R}$ et donner sa dérivée.

2. Montrer par récurrence que $\forall n \in \mathbb{N}, \forall u \in \mathbb{R}$, $\mathrm{e}^u = \displaystyle\sum_{k=0}^{n} \frac{u^k}{k!} + \frac{1}{n!}\int_0^u (u-t)^n \mathrm{e}^t\,\mathrm{d}t$, puis en déduire que

$$\forall n \in \mathbb{N}, \forall u \in \mathbb{R}, \quad \left|\mathrm{e}^u - \sum_{k=0}^{n} \frac{u^k}{k!}\right| \leqslant \frac{|u|^{n+1}}{(n+1)!}\mathrm{e}^{|u|}.$$

3. Soit $x \in \mathbb{R}$, $h \in \mathbb{R}^*$. On pose $\Delta(h) = \dfrac{f(x+h)-f(x)}{h} + \displaystyle\int_0^{\pi/4} \frac{1}{\cos^2(t)} \exp\left(\frac{-x}{\cos^2(t)}\right)\,\mathrm{d}t$. Transformer $\Delta(h)$ et majorer $|\Delta(h)|$; en déduire que f est dérivable et que

$$f'(x) = -\int_0^{\pi/4} \frac{1}{\cos^2(t)} \exp\left(\frac{-x}{\cos^2(t)}\right)\,\mathrm{d}t.$$

4. Montrer, à l'aide d'un encadrement de f, que f tend vers 0 en $+\infty$.

5. Pour $x \in \mathbb{R}$, déterminer une expression de $F(x)$ par le changement de variable $u = x\tan(t)$.

6. On pose $g(x) = f(x^2)$.

(a) Exprimer $g'(x)$ en fonction de $F(x)$.

(b) En déduire une expression de g à l'aide de F^2.

(c) Conclure que $\lim_{x\to+\infty} \int_0^x \mathrm{e}^{-t^2}\,\mathrm{d}t = \dfrac{\sqrt{\pi}}{2}$.

★ Astuce

Stratégie type pour ce genre de problème : on relie F à une fonction auxiliaire f (ou g) par une relation différentielle simple (ici $g'(x) = -2xF(x)$), on intègre cette relation pour obtenir une identité algébrique entre F^2 et g, puis on fait tendre $x \to +\infty$ en utilisant les comportements asymptotiques déjà établis.

Exercice 4.2 — Construction de la fonction Γ d'Euler et lien avec Gauss

Pour $n \in \mathbb{N}^*$ et $x \geqslant 1$, on pose $\Gamma_n(x) = \displaystyle\int_0^n t^{x-1}\left(1-\frac{t}{n}\right)^n \mathrm{d}t$.

Partie 1 — Définition de Γ.

1. Montrer que $\forall n \in \mathbb{N}^*, \forall x \geqslant 1,\ \Gamma_n(x) \leqslant \displaystyle\int_0^n t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t$.

2. Montrer que $\forall n \in \mathbb{N}^*, \forall t \in [0,n[,\ n\ln\left(1-\frac{t}{n}\right) \leqslant (n+1)\ln\left(1-\frac{t}{n+1}\right)$.

3. Soit $g(t) = t^{x-1}\mathrm{e}^{-t/2}$ sur $[0,+\infty[$. Montrer que g est majorée.

4. En déduire que $(\Gamma_n(x))_{n\geqslant 1}$ converge vers un réel noté $\Gamma(x)$.

5. Sachant qu'il existe $a_0, \dots, a_n \in \mathbb{R}$ tels que $\dfrac{n!}{x(x+1)\cdots(x+n)} = \displaystyle\sum_{k=0}^{n} \frac{a_k}{x+k}$,

(a) montrer que $\forall k,\ a_k = (-1)^k\binom{n}{k}$;

(b) en déduire que $\forall x \geqslant 1,\ \Gamma_n(x) = \dfrac{n!\,n^x}{x(x+1)\cdots(x+n)}$;

(c) en déduire que $\Gamma(x+1) = x\,\Gamma(x)$;

(d) déterminer $\Gamma(k)$ pour $k \in \mathbb{N}^*$.

Partie 2 — Étude locale de Γ en 1 (constante d'Euler γ).

6. Soit $u_n = \displaystyle\sum_{k=1}^{n}\frac{1}{k} - \ln(n)$. Montrer que (u_n) est décroissante, donc convergente, de limite γ.

7. Montrer que $\forall u \geqslant 0,\ \ln(1+u) = u - \displaystyle\int_0^u \frac{u-t}{(1+t)^2}\,\mathrm{d}t$, puis que $|\ln(1+u)-u| \leqslant \dfrac{u^2}{2}$.

8. Montrer que $\forall n \in \mathbb{N}^*,\ \displaystyle\sum_{k=1}^{n}\frac{1}{k^2} \leqslant 2$.

9. Soit $\varepsilon > 0$. Montrer que

$$\ln(\Gamma_n(1+\varepsilon)) - \ln(\Gamma_n(1)) = \varepsilon\left(\ln(n) - \sum_{k=1}^{n+1}\frac{1}{k}\right) + \sum_{k=1}^{n+1}\left(\frac{\varepsilon}{k} - \ln\left(1+\frac{\varepsilon}{k}\right)\right),$$

puis que $\displaystyle\sum_{k=1}^{n+1}\left(\frac{\varepsilon}{k}-\ln\left(1+\frac{\varepsilon}{k}\right)\right)\leqslant\varepsilon^2$.

10. En déduire que $\displaystyle\lim_{\varepsilon\to0}\frac{\ln(\Gamma(1+\varepsilon))}{\varepsilon}=-\gamma$, puis que Γ est dérivable en 1 et donner $\Gamma'(1)$.

Partie 3 — Retour à l'expression intégrale de Γ.

10. Montrer que $\forall n\in\mathbb{N}^*,\ \forall t\geqslant0,\ 0\leqslant\mathrm{e}^{-t/n}-\left(1-\dfrac{t}{n}\right)\leqslant\dfrac{t^2}{2n^2}$.

11. Montrer que pour $a>0$, $\forall n\geqslant a,\ \forall x\geqslant1$,

$$\left|\int_0^a t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t-\int_0^a t^{x-1}\left(1-\frac{t}{n}\right)^n\,\mathrm{d}t\right|\leqslant\frac{a^{x+2}}{2n(x+2)}.$$

12. Montrer qu'il existe $M>0$ tel que $\forall n,\forall a\in]0,n]$, $\displaystyle\int_a^n t^{x-1}\left(1-\frac{t}{n}\right)^n\,\mathrm{d}t\leqslant M\mathrm{e}^{-a/2}$.

13. En déduire que $\forall a>0$, $\left|\displaystyle\int_0^a t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t-\Gamma(x)\right|\leqslant M\mathrm{e}^{-a/2}$.

14. Conclure que $\Gamma(x)=\displaystyle\lim_{a\to+\infty}\int_0^a t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t=\int_0^{+\infty}t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t$.

15. Sachant que $\displaystyle\int_0^{+\infty}\mathrm{e}^{-t^2}\,\mathrm{d}t=\frac{\sqrt{\pi}}{2}$ (intégrale de Gauss), calculer $\Gamma\left(\dfrac{3}{2}\right)$.

★ Astuce

Le lien entre $\Gamma(\frac{3}{2})$ et l'intégrale de Gauss se fait via le changement de variable $t=u^2$ dans $\Gamma(\frac{1}{2})=\int_0^{+\infty}t^{-1/2}\mathrm{e}^{-t}\,\mathrm{d}t$, qui donne $\Gamma(\frac{1}{2})=2\int_0^{+\infty}\mathrm{e}^{-u^2}\,\mathrm{d}u=\sqrt{\pi}$; on conclut ensuite avec la relation $\Gamma(x+1)=x\Gamma(x)$.

CHAPITRE 2

Algèbre

Cette partie regroupe les exercices et problèmes d'algèbre des sessions 2019 à 2024 : matrices et diagonalisation, arithmétique dans $\mathbb{Z}$ (nombres premiers, formule de Legendre), anneaux et entiers d'Eisenstein, groupe $SL_2(\mathbb{Z})$, dénombrement et fonctions arithmétiques.

1. Matrices, diagonalisation et puissances

Rappel

Diagonaliser $A = PDP^{-1}$ permet de calculer $A^n = PD^nP^{-1}$ sans récurrence directe sur A^n. La méthode-type : (1) calculer le polynôme caractéristique $\det(xI - A)$, (2) trouver ses racines, (3) déterminer les vecteurs propres associés, (4) exploiter Cayley-Hamilton ($P^2 - (\operatorname{tr} P)P = \det(P)\, I_2$ pour une matrice 2×2) pour obtenir P^{-1} sans calcul direct.

Exercice 1.1 — Diagonalisation d'une matrice 2×2 et calcul de A^n

On considère $A = \begin{pmatrix} 5 & -3 \\ 4 & -2 \end{pmatrix}$. L'objectif est de trouver $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $D = \begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}$ telles que $A = PDP^{-1}$.

1. Soit $x \in \mathbb{R}$. Déterminer $Q(x) = \det(xI_2 - A)$.

2. Donner x_1, x_2 les racines de Q, avec $x_1 < x_2$.

3. Calculer $X_1 = A - x_1 I_2$ et $X_2 = A - x_2 I_2$, puis trouver deux colonnes non nulles $C_1 = \begin{pmatrix} \alpha \\ \gamma \end{pmatrix}$, $C_2 = \begin{pmatrix} \beta \\ \delta \end{pmatrix}$ à coefficients entiers naturels telles que $X_1 C_1 = 0$ et $X_2 C_2 = 0$.

4. On forme P à l'aide de C_1, C_2 et D à l'aide de x_1, x_2.

(a) Calculer $P^2 - (\alpha + \delta)P$.

(b) En déduire P^{-1}.

(c) Vérifier que $PDP^{-1} = A$.

5. Montrer par récurrence que $D^n = \begin{pmatrix} 1 & 0 \\ 0 & 2^n \end{pmatrix}$ pour tout $n \geqslant 1$.

6. En déduire une expression de A^n pour $n \geqslant 1$.

2. Matrices conjuguées et groupe $SL_2(\mathbb{K})$

Exercice 2.1 — Matrices conjuguées dans $SL_2(\mathbb{K})$ et conditions sur un corps

2024

On se donne un anneau $\mathbb{K}$ commutatif. On pose $SL_2(\mathbb{K}) = \{M \in M_2(\mathbb{K}) \mid \det(M) = 1\}$. Deux matrices $A, B \in M_2(\mathbb{K})$ sont dites *conjuguées* dans $SL_2(\mathbb{K})$ s'il existe $P \in SL_2(\mathbb{K})$ tel que $A = P^{-1}BP$.

Partie 1.

1. Déterminer l'ensemble des $(b, d) \in \mathbb{Z} \times \mathbb{Z}$ tels que $\begin{pmatrix} 3 & b \\ 2 & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

2. Déterminer l'ensemble des $(x, y) \in \mathbb{N} \times \mathbb{N}$ tels que $\begin{pmatrix} x & -1 \\ 1-2y & y-3 \end{pmatrix} \in SL_2(\mathbb{Z})$.

3. Soit $(a, d) \in \mathbb{Z} \times \mathbb{Z}$.

(a) Si $(a, d) \notin \{(1, 1), (-1, -1)\}$: l'ensemble des (b, c) tels que $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ est-il non vide ? infini ?

(b) Même question lorsque $(a, d) \in \{(1, 1), (-1, -1)\}$.

Partie 2. On considère $\lambda \in \mathbb{K}^*$ et $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$.

4. Montrer que A et B sont conjuguées dans $SL_2(\mathbb{K})$ si et seulement si λ est un carré dans $\mathbb{K}$.

5. Donner une CNS pour que A et B soient conjuguées dans $SL_2(\mathbb{K})$ pour $\mathbb{K} = \mathbb{C}$, puis pour $\mathbb{K} = \mathbb{R}$.

6. Montrer que $\forall \lambda \in \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$, A et B sont conjuguées dans $SL_2(\mathbb{Z}/3\mathbb{Z})$.

7. Déterminer les valeurs de $\lambda \in \mathbb{Z}/7\mathbb{Z}$ pour lesquelles A et B sont conjuguées dans $SL_2(\mathbb{Z}/7\mathbb{Z})$.

8. Montrer que si λ, μ sont des carrés dans $\mathbb{K}$, alors $\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ sont conjuguées dans $SL_2(\mathbb{K})$.

Exercice 2.2 — Générateurs du groupe $SL_2(\mathbb{Z})$

On note $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \,\middle|\, ad - bc = 1 \right\}$, et $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On note $\langle S, T \rangle$ l'ensemble des produits de matrices de $\{S, T, T^{-1}\}$. On veut montrer $SL_2(\mathbb{Z}) = \langle S, T \rangle$.

1. Calculer S^2 et montrer que $\forall n \in \mathbb{Z}$, $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

2. Montrer que si $M \in \langle S, T \rangle$, alors $-M \in \langle S, T \rangle$.

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$; quitte à remplacer M par $-M$, on suppose $c \in \mathbb{N}$. On raisonne par récurrence sur c.

3. On suppose $c = 0$.

(a) Montrer que M est de la forme $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ ou $\begin{pmatrix} -1 & m \\ 0 & -1 \end{pmatrix}$, $m \in \mathbb{Z}$.

(b) En déduire que, dans les deux cas, $M \in \langle S, T \rangle$.

4. On suppose l'hypothèse de récurrence : toute matrice $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ de $SL_2(\mathbb{Z})$ avec $0 < z \leqslant c-1$ est dans $\langle S, T \rangle$. On effectue la division euclidienne $a = qc + r$, $0 \leqslant r < c$.

(a) Vérifier que $ST^{-q}M = \begin{pmatrix} u & v \\ r & w \end{pmatrix}$ et déterminer u, v, w.

(b) Appliquer l'hypothèse de récurrence pour conclure que $M \in \langle S, T \rangle$.

★ Astuce

Les preuves par **descente infinie / récurrence sur un paramètre entier décroissant** (c ici) sont une technique classique en algèbre des matrices entières : on construit, à partir d'une matrice donnée, une nouvelle matrice de paramètre strictement plus petit appartenant au même ensemble, ce qui permet de remonter jusqu'au cas de base ($c = 0$).

3. Arithmétique dans $\mathbb{Z}$ — nombres premiers et formule de Legendre

Rappel

La **fonction p-adique** $v_p(a) = \max\{k \in \mathbb{N} \mid p^k \text{ divise } a\}$ permet de quantifier précisément la puissance de p qui divise un entier ; elle est centrale pour établir la **formule de Legendre** donnant $v_p(n!)$.

Exercice 3.1 — Majoration de $\pi(2^n)$ par les coefficients binomiaux

Pour $n \in \mathbb{N}^*$, on note $\pi(n)$ le nombre d'entiers premiers inférieurs ou égaux à n. On veut majorer $\pi(2^n)$.

On pourra utiliser sans démonstration : si des nombres premiers deux à deux distincts divisent un entier n, leur produit divise n ; et si n est premier avec chacun des $a_1, \dots, a_q$, alors n est premier avec leur produit.

1. Montrer que $\forall n \in \mathbb{N}^*,\ C_n^n \leqslant 2^{2n}$ (remarquer que $2^{2n} = (1+1)^{2n}$).

2. Soit p premier, $n+1 \leqslant p \leqslant 2n$. Montrer que p divise C_{2n}^n (utiliser $C_{2n}^n = \dfrac{(n+1)(n+2)\cdots 2n}{n!}$).

3. En déduire que le produit des nombres premiers compris entre $n+1$ et $2n$ divise C_{2n}^n.

4. En déduire que $C_{2n}^n \geqslant n^{\pi(2n)-\pi(n)}$.

5. En déduire que $\forall n \geqslant 2,\ \pi(2n) - \pi(n) \leqslant \dfrac{2n \ln 2}{\ln n}$.

6. Montrer par récurrence que $\forall n \geqslant 2,\ \pi(2^n) \leqslant \displaystyle\sum_{k=2}^{n} \frac{2^k}{k-1}$.

Exercice 3.2 — Valuation p-adique de $n!$ et formule de Legendre

2021

Soit $n \geqslant 2$ un entier et p un nombre premier. Pour $k \geqslant 0$, on pose $U_k = \{a \in [\![1, n]\!] \mid p^k \text{ divise } a\}$ et $\Omega_k = \{a \in [\![1, n]\!] \mid v_p(a) = k\}$.

1. Déterminer $m = \sup\{k \in \mathbb{N} \mid p^k \leqslant n\}$ en fonction de n et p.

2. **(a)** Montrer que $\forall k \in [\![0, m]\!]$, $U_{k+1} \subsetneq U_k$, et que $U_k = \emptyset$ pour $k > m$.

(b) Montrer que $\Omega_0, \dots, \Omega_m$ sont deux à deux disjoints et que leur réunion est $[\![1, n]\!]$.

3. **(a)** Établir que $\forall k \geqslant 0,\ \Omega_k = U_k \setminus U_{k+1}$.

(b) Calculer $\mathrm{Card}(U_k)$ puis $\mathrm{Card}(\Omega_k)$ en fonction de n, p.

4. Montrer que $v_p(n!) = \displaystyle\sum_{k=1}^{m} k \cdot \mathrm{Card}(\Omega_k)$ et en déduire la **formule de Legendre** :

$$v_p(n!) = \sum_{k=1}^{m} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

★ Astuce

La formule de Legendre $v_p(n!) = \sum_{k \geqslant 1} \lfloor n/p^k \rfloor$ est l'outil de référence pour déterminer le nombre de zéros terminaux de $n!$ en base 10 (via $v_5(n!)$, qui est toujours $\leqslant v_2(n!)$), ou pour étudier la divisibilité de coefficients binomiaux.

Exercice 3.3 — Tout premier $p \equiv 1 \pmod 4$ est somme de deux carrés (méthode de l'involution de Za

On montre que pour tout nombre premier p de la forme $4m+1$, il existe $(a, b) \in \mathbb{N}^2$ tel que $p = a^2 + b^2$. Soit $S = \{(x, y, z) \in (\mathbb{N}^*)^3 \mid x^2 + 4yz = p\}$, et

$$S_1 = S \cap \{x < y - z\}, \quad S_2 = S \cap \{y - z < x < 2y\}, \quad S_3 = S \cap \{2y < x\}.$$

1. Justifier que S est un ensemble fini.

2. Montrer que si $y, z \in \mathbb{N}^*$, alors $(y - z, y, z) \notin S$ et $(2y, y, z) \notin S$.

3. En déduire que $S = S_1 \cup S_2 \cup S_3$.

On définit f sur S par

$$f(x, y, z) = \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{si } (x, y, z) \in S_1 \\ (2y - x,\ y,\ x - y + z) & \text{si } (x, y, z) \in S_2 \\ (x - 2y,\ x - y + z,\ y) & \text{si } (x, y, z) \in S_3 \end{cases}$$

4. Montrer les inclusions $f(S_1) \subset S_3$, $f(S_2) \subset S_2$, $f(S_3) \subset S_1$.

5. En déduire que $f(S) \subset S$.

6. Vérifier que $\forall (x, y, z) \in S,\ f(f(x, y, z)) = (x, y, z)$.

7. Justifier les égalités $f(S) = S$, $f(S_1) = S_3$, $f(S_2) = S_2$, $f(S_3) = S_1$.

8. f peut-elle avoir un point fixe dans S_1 ? dans S_3 ? Justifier.
9. Montrer que f admet un unique point fixe sur S, qu'on déterminera.
10. En déduire que $\mathrm{Card}(S)$ est impair.
11. Soit $g : S \to S$, $(x, y, z) \mapsto (x, z, y)$.
    (a) Justifier que $g \circ g = \mathrm{id}$ et que g possède au moins un point fixe dans S.
    (b) En déduire que p s'écrit comme somme de deux carrés d'entiers naturels.
12. **Unicité (à l'échange de a et b près).** Supposons $p = a^2 + b^2 = c^2 + d^2$, $a, b, c, d \in \mathbb{N}^*$.
    (a) Montrer que $(ad - bc)(ad + bc) \equiv 0 \pmod{p}$, puis que $p \mid ad - bc$ ou $p \mid ad + bc$.
    (b) Si $p \mid ad - bc$: vérifier $p^2 = (ad - bc)^2 + (ac + bd)^2$, en déduire $a = c,\ b = d$.
    (c) Si $p \mid ad + bc$: vérifier $p^2 = (ad + bc)^2 + (ac - bd)^2$, en déduire $a = d,\ b = c$.

★ **Astuce**
L'involution de Zagier (1990) est une preuve « sans mots » du théorème des deux carrés de Fermat : on exhibe une involution f sur un ensemble fini S ayant un **unique** point fixe, ce qui force $\mathrm{Card}(S)$ à être impair ; une seconde involution naturelle g doit alors, elle aussi, avoir un point fixe – lequel fournit directement la décomposition $p = a^2 + b^2$.

4. Anneaux — les entiers d'Eisenstein $\mathbb{Z}[j]$

Exercice 4.1 — Division euclidienne et idéaux dans l'anneau des entiers d'Eisenstein

On note $\mathbb{Z}[j] = \{a + bj \mid a, b \in \mathbb{Z}\}$ où $j = \mathrm{e}^{i2\pi/3}$.

1. Montrer que $\mathbb{Z}[j]$ est un anneau commutatif, intègre et unitaire.
2. Représenter l'élément $z = a + jb$ avec $a, b \in \mathbb{N}$.
3. Pour $z \in \mathbb{C}$, on pose $N(z) = z\bar{z}$.
   (a) Calculer $N(u)$ pour $u = a + jb \in \mathbb{Z}[j]$, en fonction de a et b.
   (b) Montrer que pour $u \in \mathbb{Z}[j]$, u est inversible si et seulement si $N(u) = 1$.
4. Conclure que les inversibles de $\mathbb{Z}[j]$ sont exactement les racines sixièmes de l'unité $\mathbb{U}_6 = \{z \in \mathbb{C} \mid z^6 = 1\}$.
5. (a) Montrer que $\forall z \in \mathbb{C},\ \exists\,(x, y) \in \mathbb{R}^2$ unique tel que $z = x + jy$.
   (b) Montrer que $\forall z \in \mathbb{C},\ \exists\,\alpha \in \mathbb{Z}[j]$ tel que $N(z - \alpha) < 1$.
   (c) Y a-t-il unicité de α ?
6. Soient $z_1, z_2 \in \mathbb{Z}[j]$, $z_2 \neq 0$. Montrer l'existence de $(q, r) \in \mathbb{Z}[j] \times \mathbb{Z}[j]$ tels que $z_1 = z_2 q + r$ et $N(r) < N(z_2)$.
7. Le couple (q, r) précédent est-il unique ?
   On appelle *idéal* de $\mathbb{Z}[j]$ une partie I sous-groupe de $(\mathbb{Z}[j], +)$ telle que $\forall u \in \mathbb{Z}[j], \forall z \in I,\ uz \in$

I. Soit I un idéal non nul, $A = \{N(z) \mid z \in I \setminus \{0\}\}$, et $\beta \in I \setminus \{0\}$ tel que $N(\beta) = \min A$.

8. Montrer que $I = \beta\mathbb{Z}[j] = \{\beta q \mid q \in \mathbb{Z}[j]\}$.

Rappel

$\mathbb{Z}[j]$ est, comme $\mathbb{Z}$, un **anneau euclidien** : la fonction $N(z) = z\bar{z} = |z|^2$ joue le rôle du stathme euclidien (analogue de la valeur absolue sur $\mathbb{Z}$), ce qui permet d'y développer toute l'arithmétique usuelle (division euclidienne, Bézout, idéaux principaux).

5. Dénombrement et fonctions arithmétiques

Exercice 5.1 — Fonction somme des diviseurs σ et nombres parfaits

2024

Pour $n \in \mathbb{N}^*$, on note D_n l'ensemble des diviseurs positifs de n et $\sigma(n) = \sum_{d \in D_n} d$. *Exemple :* $\sigma(10) = 1 + 2 + 5 + 10 = 18$.

1. Montrer que n est premier si et seulement si $\sigma(n) = n + 1$.

2. Pour p premier et $\alpha \in \mathbb{N}^*$, calculer $\sigma(p^\alpha)$.

3. Soient $a, b \in \mathbb{N}^*$ avec $a \wedge b = 1$, et $f : D_a \times D_b \to D_{ab}$, $(k, l) \mapsto kl$.

(a) Montrer que f est injective.

(b) Soit $d \in D_{ab}$, $k = d \wedge a$, $l = d \wedge b$. Montrer que $d = kl$ et conclure que f est bijective.

(c) En déduire que $\sigma(ab) = \sigma(a)\sigma(b)$.

4. En déduire que $\forall s \in \mathbb{N}^*$, $\forall a_1, \dots, a_s \in \mathbb{N}^*$ premiers entre eux deux à deux,

$$\sigma\left(\prod_{k=1}^{s} a_k\right) = \prod_{k=1}^{s} \sigma(a_k).$$

5. Pour $n \geqslant 2$, exprimer $\sigma(n)$ à partir de la décomposition en facteurs premiers de n. *Application : n est dit **parfait** si $\sigma(n) = 2n$ (par exemple 6 est parfait).*

6. Montrer que les nombres parfaits pairs sont exactement les **nombres d'Euclide** $E_k = 2^k(2^{k+1} - 1)$, $k \in \mathbb{N}^*$, où $2^{k+1} - 1$ est premier.

★ Astuce

σ est une fonction **multiplicative** ($\sigma(ab) = \sigma(a)\sigma(b)$ si $a \wedge b = 1$) : c'est la technique générale pour calculer $\sigma(n)$ – on décompose $n = \prod p_i^{\alpha_i}$ et on utilise $\sigma(p^\alpha) = \dfrac{p^{\alpha+1} - 1}{p - 1}$ sur chaque facteur premier.

CHAPITRE 3

Corrigés synthétiques et fiches méthodes

Cette section reprend, sous forme **synthétique**, les démonstrations des exercices les plus emblématiques de la compilation : méthode de Newton, intégrale de Gauss et fonction Γ, formule de Legendre, sommes de deux carrés, générateurs de $SL_2(\mathbb{Z})$. Chaque corrigé est suivi d'une **fiche méthode** qui dégage la technique transférable à d'autres exercices.

1. Méthode de Newton

Corrigé — Méthode de Newton — convergence quadratique

1. Unicité de la solution. f est continue, strictement décroissante ($f' < 0$) sur $[a, b]$, avec $f(a) > 0 > f(b)$: par le TVI strictement monotone, il existe un unique $c \in]a, b[$ tel que $f(c) = 0$.
2. Tangente. La tangente en x_0 a pour équation $y = f(x_0) + f'(x_0)(x - x_0)$; elle coupe l'axe des abscisses en $x = x_0 - \dfrac{f(x_0)}{f'(x_0)} = g(x_0)$.
3–4. Dérivée et variations de g. On calcule

$$g'(x) = 1 - \frac{f'(x)^2 - f(x)f''(x)}{f'(x)^2} = \frac{f(x)f''(x)}{f'(x)^2}.$$

Comme $f'' > 0$ sur $[a, b]$, le signe de g' est celui de $f(x)$: $g' > 0$ sur $[a, c[$ (car $f > 0$, f décroissante de $f(a) > 0$ à $f(c) = 0$) et $g' < 0$ sur $]c, b]$. Ainsi g croît puis décroît, avec un maximum en c où $g(c) = c$.
5. Majoration quadratique. Par le TAF appliqué à f entre x et c : $f(x) = f(x) - f(c) = f'(\xi)(x - c)$ pour un ξ entre x et c. Puis le TAF appliqué à f' entre ξ et x donne $|f'(\xi) - f'(x)| \leqslant M|\xi - x| \leqslant M|x - c|$. On combine :

$$g(x) - c = x - c - \frac{f(x)}{f'(x)} = \frac{f'(x)(x - c) - f(x)}{f'(x)} = \frac{(f'(x) - f'(\xi))(x - c)}{f'(x)},$$

d'où $|g(x) - c| \leqslant \dfrac{M}{m}|x - c|^2 = L|x - c|^2$ avec $L = M/m$.
6–7. Convergence de (u_n). Comme g croît sur $[a, c]$ avec $g(c) = c$ et $u_0 = a \in [a, c]$ (puisque $f(a) > 0$, donc $a < c$), une récurrence immédiate donne $u_n \in [a, c]$ et $u_{n+1} = g(u_n) \geqslant u_n$ (car $g(x) \geqslant x$ sur $[a, c]$, vu la position de la tangente sous une fonction convexe). La suite (u_n) est donc croissante et majorée par c : elle converge vers une limite $\ell \in [a, c]$ vérifiant $\ell = g(\ell)$, donc $f(\ell) = 0$, donc $\ell = c$ par unicité.

8. Vitesse de convergence. En itérant l'inégalité $|u_{n+1}-c| \leqslant L|u_n-c|^2$, on pose $k=L$ et on montre par récurrence

$$|u_n-c| \leqslant \frac{1}{k}\big(k|u_0-c|\big)^{2^n} = k\left(\frac{c-a}{k}\right)^{2^n} \quad \text{(à un ajustement de constante près).}$$

☞ Fiche méthode — Convergence quadratique d'une suite récurrente

- **Schéma général.** Une suite $u_{n+1}=g(u_n)$ converge vers un point fixe c de g avec une vitesse **quadratique** dès qu'on dispose d'une majoration du type $|g(x)-c| \leqslant L|x-c|^2$ au voisinage de c.
- **Obtenir cette majoration.** Combiner **deux applications successives du théorème des accroissements finis** (une sur f, une sur f') est la technique standard pour faire apparaître un carré $(x-c)^2$.
- **Monotonie et bornage.** Étudier le signe de g' via le signe de $f\cdot f''$ (et non directement g') simplifie souvent les calculs, car $g' = \dfrac{f\,f''}{(f')^2}$ a le signe de $f\cdot f''$.
- **Convergence accélérée.** Une fois la majoration quadratique établie, itérer donne $|u_n-c| \leqslant k^{1-2^n}\cdot|u_0-c|^{2^n}$: le nombre de décimales correctes **double** approximativement à chaque itération – c'est la signature de la méthode de Newton, à comparer à la convergence linéaire (géométrique) d'une suite récurrente ordinaire.

2. Intégrale de Gauss et fonction Γ

Corrigé — Calcul de $\displaystyle\int_0^{+\infty} \mathrm{e}^{-t^2}\,\mathrm{d}t$ par dérivation sous le signe intégral

Idée directrice. On relie $g(x)=f(x^2)$ à $F(x)^2$ via une relation différentielle, en s'appuyant sur la dérivée de $f(x)=\displaystyle\int_0^{\pi/4} \exp\!\left(\frac{-x}{\cos^2 t}\right)\mathrm{d}t$.

Étape 1 (dérivée de f). On justifie, à l'aide de l'inégalité de Taylor avec reste intégral sur l'exponentielle, que f est dérivable avec

$$f'(x) = -\int_0^{\pi/4} \frac{1}{\cos^2 t}\exp\!\left(\frac{-x}{\cos^2 t}\right)\mathrm{d}t.$$

La majoration $|h| \leqslant \dfrac{|h|}{\cos^2 t} \leqslant 2|h|$ sur $[0,\pi/4]$ permet de contrôler le taux d'accroissement de f de façon uniforme en t.

Étape 2 (comportement asymptotique). En encadrant l'intégrande, on montre $f(x) \xrightarrow[x\to+\infty]{} 0$.

Étape 3 (changement de variable). Pour $x\in\mathbb{R}$, le changement $u = x\tan t$ (donc $\mathrm{d}u = \dfrac{x}{\cos^2 t}\,\mathrm{d}t$) transforme $f(x)$ en une expression faisant apparaître $F(x)=\displaystyle\int_0^x \mathrm{e}^{-u^2}\,\mathrm{d}u$: précisément $f(x) =$

$\frac{1}{x}\int_0^x \mathrm{e}^{-x^2-u^2}\,x\,\mathrm{d}u$, ce qui se réécrit en termes de e^{-x^2} et F.

Étape 4 (la relation clé). En posant $g(x) = f(x^2)$, on calcule $g'(x) = 2x\,f'(x^2) = -2x\displaystyle\int_0^{\pi/4} \frac{\mathrm{e}^{-x^2/\cos^2 t}}{\cos^2 t}\,\mathrm{d}t = -2x\int_0^{+\infty} \mathrm{e}^{-x^2(1+u^2)}\,\mathrm{d}u$ (changement $u = \tan t$), et le changement $u = v/x$ donne

$$g'(x) = -2\int_0^x \mathrm{e}^{-x^2-v^2}\,\mathrm{d}v\cdot \mathrm{e}^0 = -2\mathrm{e}^{-x^2}\int_0^x \mathrm{e}^{-v^2}\,\mathrm{d}v = -2F(x)F'(x) = -\left(F^2\right)'(x).$$

Donc $g(x)+F(x)^2$ est constante, égale à sa valeur en 0 : $g(0) = f(0) = \dfrac{\pi}{4}$ et $F(0) = 0$, d'où

$$\boxed{T(x) := g(x) + F(x)^2 = \frac{\pi}{4} \quad \text{pour tout } x \in \mathbb{R}.}$$

Étape 5 (conclusion). Quand $x \to +\infty$, $g(x) = f(x^2) \to 0$ (étape 2), donc $F(x)^2 \to \dfrac{\pi}{4}$, et comme $F(x) \geqslant 0$,

$$\lim_{x\to+\infty} \int_0^x \mathrm{e}^{-t^2}\,\mathrm{d}t = \frac{\sqrt{\pi}}{2}.$$

☞ Fiche méthode — Dérivation sous le signe intégral et intégrales « non calculables » explicitement

- **Pourquoi cette méthode ?** e^{-t^2} n'a pas de primitive exprimable avec les fonctions usuelles : on ne calcule **jamais** F directement, mais on construit une fonction auxiliaire (f ou T) dont la dérivée s'annule, ce qui donne une relation algébrique exacte.
- **Schéma reproductible.**
  1. Construire $f(x) = \int_{\text{borne fixe}} \varphi(x,t)\,\mathrm{d}t$ liée au problème (souvent une intégrale sur un segment borné, donc sans souci de convergence).
  2. Dériver sous le signe intégral (justifier rigoureusement : uniformité de la majoration en t, théorème de Heine si nécessaire).
  3. Faire apparaître, via un changement de variable bien choisi (souvent $u = x\tan t$ ou $u = xt$), un lien entre f' et $F\cdot F' = \frac{1}{2}(F^2)'$.
  4. En déduire que $f(x^2)+F(x)^2$ (ou une combinaire analogue) est **constante**.
  5. Évaluer la constante en $x = 0$ (valeurs simples), puis passer à la limite $x \to +\infty$ en utilisant un encadrement indépendant de F pour montrer que $f \to 0$.
- **Lien avec Γ.** L'intégrale de Gauss correspond à $\Gamma(1/2) = \sqrt{\pi}$ via $t = u^2$: c'est la passerelle naturelle entre les deux problèmes classiques de concours.

Corrigé — Construction de Γ par convergence de Γ_n – points clés

Idée directrice. $\Gamma_n(x) = \int_0^n t^{x-1}(1-t/n)^n\,\mathrm{d}t$ est une approximation de $\int_0^{+\infty} t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t$, fondée sur $(1-t/n)^n \to \mathrm{e}^{-t}$.

Monotonie en n. L'inégalité $n\ln(1-t/n) \leqslant (n+1)\ln(1-t/(n+1))$ traduit la **croissance en**

n de la suite $(1-t/n)^n$ pour t fixé (à n assez grand) : cela permet d'appliquer un théorème de convergence monotone « fait main » (sans recourir au théorème de convergence dominée, hors programme).

Bornage et limite. $g(t)=t^{x-1}\mathrm{e}^{-t/2}$ étant majorée sur $\mathbb{R}^+$ (croissance polynomiale dominée par l'exponentielle), on en déduit que $\Gamma_n(x)$ est une suite croissante majorée, donc convergente : c'est la définition de $\Gamma(x)$.

Formule explicite. La décomposition en éléments simples $\dfrac{n!}{x(x+1)\cdots(x+n)}=\sum_{k=0}^{n}\dfrac{(-1)^k\binom{n}{k}}{x+k}$, combinée à n intégrations par parties successives de Γ_n, donne la formule fermée $\Gamma_n(x)=\dfrac{n!\,n^x}{x(x+1)\cdots(x+n)}$, d'où $\Gamma(x+1)=x\Gamma(x)$ par passage à la limite, et $\Gamma(k)=(k-1)!$ pour $k\in\mathbb{N}^*$.

Lien avec Gauss. $\Gamma(1/2)=\int_0^{+\infty}t^{-1/2}\mathrm{e}^{-t}\,\mathrm{d}t\xrightarrow{t=u^2}2\int_0^{+\infty}\mathrm{e}^{-u^2}\,\mathrm{d}u=\sqrt{\pi}$, donc $\Gamma(3/2)=\dfrac{1}{2}\Gamma(1/2)=\dfrac{\sqrt{\pi}}{2}$.

3. Formule de Legendre

Corrigé — Valuation p-adique de $n!$

2021

Partition de $[\![1,n]\!]$. Pour $k\geqslant 0$, $U_k=\{a\leqslant n\mid p^k\mid a\}$ vérifie $U_{k+1}\subset U_k$ (strictement, dès que $U_{k+1}\neq U_k$), et $\Omega_k=U_k\setminus U_{k+1}$ regroupe exactement les entiers de valuation p-adique **égale** à k. Les Ω_k partitionnent $[\![1,n]\!]$ car tout entier a une valuation p-adique bien définie et finie (bornée par $m=\lfloor\log_p n\rfloor$).

Cardinaux. $\mathrm{Card}(U_k)=\left\lfloor\dfrac{n}{p^k}\right\rfloor$ (nombre de multiples de p^k dans $[\![1,n]\!]$), donc

$$\mathrm{Card}(\Omega_k)=\mathrm{Card}(U_k)-\mathrm{Card}(U_{k+1})=\left\lfloor\frac{n}{p^k}\right\rfloor-\left\lfloor\frac{n}{p^{k+1}}\right\rfloor.$$

Sommation par paquets. Chaque entier $a\in\Omega_k$ contribue k fois le facteur p dans $n!=\prod_{a=1}^{n}a$, donc

$$v_p(n!)=\sum_{k=1}^{m}k\cdot\mathrm{Card}(\Omega_k)=\sum_{k=1}^{m}k\left(\left\lfloor\frac{n}{p^k}\right\rfloor-\left\lfloor\frac{n}{p^{k+1}}\right\rfloor\right).$$

Un **réindexage en sommation par paquets** (technique d'Abel discrète : on regroupe les termes en $\lfloor n/p^k\rfloor$ plutôt qu'en $k\cdot(\dots)$) donne directement

$$\boxed{v_p(n!)=\sum_{k=1}^{m}\left\lfloor\frac{n}{p^k}\right\rfloor.}$$

☞ Fiche méthode — Comptage par partition selon la valuation p-adique

- **Principe.** Pour calculer une somme indexée par une propriété arithmétique (ici, la valuation v_p), on partitionne l'ensemble selon les valeurs de cette propriété, puis on relie chaque « strate » Ω_k à un ensemble plus simple à compter (U_k = multiples de p^k), via $\Omega_k=U_k\setminus U_{k+1}$.

- **Le réflexe utile.** $\mathrm{Card}(U_k) = \lfloor n/p^k \rfloor$ est immédiat (compter les multiples de p^k jusqu'à n) ; c'est nettement plus simple que de compter directement $\mathrm{Card}(\Omega_k)$.
- **Réindexation télescopique.** La somme $\sum_k k(\lfloor n/p^k \rfloor - \lfloor n/p^{k+1} \rfloor)$ se télescope en $\sum_k \lfloor n/p^k \rfloor$: c'est un argument d'**Abel discret / sommation par parties** à reconnaître systématiquement dès qu'apparaît une somme du type $\sum k\,(a_k - a_{k+1})$.
- **Applications classiques.** Nombre de zéros terminaux de $n!$ ($v_5(n!)$), divisibilité des coefficients binomiaux (théorème de Kummer), preuves d'irrationalité de certaines constantes.

4. Sommes de deux carrés

Corrigé — Tout premier $p \equiv 1 \pmod 4$ est somme de deux carrés (involution de Zagier) 2023

Schéma de la preuve. On travaille sur $S = \{(x,y,z) \in (\mathbb{N}^*)^3 \mid x^2 + 4yz = p\}$, fini car $x^2 \leqslant p$ et $4yz \leqslant p$ contraignent x, y, z à un nombre fini de valeurs.
L'involution f. Elle est définie par cas selon la position de x par rapport à $y - z$ et $2y$ (d'où la partition $S = S_1 \sqcup S_2 \sqcup S_3$, les cas-limites $x = y - z$ et $x = 2y$ étant exclus par un argument de parité/positivité). Un calcul direct vérifie $f \circ f = \mathrm{id}_S$, et f échange $S_1 \leftrightarrow S_3$ tout en stabilisant S_2.
Point fixe unique. Sur S_1 et S_3, f n'a pas de point fixe (car f les échange strictement) ; le seul point fixe possible est dans S_2, et un calcul montre qu'il est unique : $(x,y,z) = (1,1,(p-1)/4)$. Donc $\mathrm{Card}(S)$ est **impair**.
La seconde involution g. $g(x,y,z) = (x,z,y)$ vérifie aussi $g \circ g = \mathrm{id}$. Sur un ensemble **fini de cardinal impair**, toute involution possède au moins un point fixe (les orbites sous une involution sont de taille 1 ou 2 ; un cardinal impair force l'existence d'au moins une orbite de taille 1). Un point fixe de g vérifie $y = z$, donc $p = x^2 + 4y^2 = x^2 + (2y)^2$: c'est la décomposition cherchée.
Unicité. Si $p = a^2 + b^2 = c^2 + d^2$, l'identité de Brahmagupta-Fibonacci $p^2 = (ad - bc)^2 + (ac + bd)^2 = (ad + bc)^2 + (ac - bd)^2$ combinée à $p \mid ad - bc$ ou $p \mid ad + bc$ (car p divise leur produit $(ad)^2 - (bc)^2 \equiv 0$) force l'un des deux termes de la décomposition à être nul, d'où $\{a,b\} = \{c,d\}$.

☞ **Fiche méthode — Arguments de parité par involutions**

- **Le principe clé.** Sur un ensemble fini E, une involution ($f \circ f = \mathrm{id}$) partitionne E en orbites de taille 1 (points fixes) ou 2 (paires $\{x, f(x)\}$). Donc $\mathrm{Card}(E) \equiv$ (nombre de points fixes) $\pmod 2$.
- **Stratégie en deux temps.** (1) Construire une première involution dont on contrôle *exactement* le nombre de points fixes (souvent 0 ou 1), pour en déduire la parité de $\mathrm{Card}(E)$; (2) construire une **seconde** involution « naturelle », liée à la propriété qu'on veut démontrer, et utiliser la parité obtenue en (1) pour garantir qu'elle a un point fixe.
- **Pourquoi c'est puissant.** Cette méthode évite tout argument analytique ou de comptage explicite : elle est purement combinatoire et s'applique à de nombreux théorèmes d'existence en arithmétique (cf. aussi les preuves combinatoires du petit théorème de Fermat).
- **Identité à retenir.** Brahmagupta-Fibonacci : le produit de deux sommes de deux carrés est

une somme de deux carrés, de deux façons différentes – utile pour les questions d'unicité de décomposition.

5. Générateurs de $SL_2(\mathbb{Z})$

Corrigé — $SL_2(\mathbb{Z}) = \langle S, T\rangle$ par récurrence descendante

2023

Calculs préliminaires. $S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2$, et une récurrence immédiate donne $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ pour tout $n \in \mathbb{Z}$. Comme $S^2 = -I_2 \in \langle S, T\rangle$, on a $-M = S^2 M \in \langle S, T\rangle$ dès que $M \in \langle S, T\rangle$: on peut donc toujours se ramener au cas $c \geqslant 0$ en remplaçant M par $-M$ si besoin.

Cas de base $c = 0$**.** Si $c = 0$, $ad = 1$ donc $(a, d) = (1, 1)$ ou $(-1, -1)$, et $M = \begin{pmatrix} \pm 1 & m \\ 0 & \pm 1 \end{pmatrix} = \pm T^m \in \langle S, T\rangle$.

Pas de récurrence. Pour $c \geqslant 1$, on suppose le résultat acquis pour tout $c' < c$. On effectue $a = qc + r$ $(0 \leqslant r < c)$ et on calcule

$$ST^{-q}M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ a - qc & b - qd \end{pmatrix} = \begin{pmatrix} -c & -d \\ r & b - qd \end{pmatrix}.$$

Cette nouvelle matrice a un coefficient en position $(2, 1)$ égal à $r < c$: par hypothèse de récurrence, elle appartient à $\langle S, T\rangle$. Comme $S, T \in \langle S, T\rangle$ qui est stable par produit et passage à l'inverse, on en déduit

$$M = T^q S^{-1} (ST^{-q}M) \in \langle S, T\rangle.$$

Conclusion. Par récurrence forte sur $c \in \mathbb{N}$, toute matrice de $SL_2(\mathbb{Z})$ à coefficient $c \geqslant 0$ est dans $\langle S, T\rangle$; le cas $c < 0$ s'y ramène via $-M$. Donc $SL_2(\mathbb{Z}) = \langle S, T\rangle$.

☞ Fiche méthode — Algorithme d'Euclide matriciel

- **Analogie avec Bézout.** La construction $ST^{-q}M$ réalise, au niveau matriciel, exactement l'étape d'une **division euclidienne** : on « réduit » le coefficient c modulo lui-même, exactement comme l'algorithme d'Euclide réduit le second argument d'un pgcd.
- **Pourquoi** T^{-q} **et** S **?** Multiplier par $T^{-q} = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}$ effectue l'opération $a \mapsto a - qc = r$ sur la première ligne ; multiplier ensuite par S permute les lignes pour amener r en position $(2, 1)$, là où se trouvait c – ce qui crée la décroissance nécessaire à la récurrence.
- **Récurrence forte sur un entier positif strictement décroissant** : c'est le même schéma de preuve que pour l'algorithme d'Euclide (terminaison) ou pour la descente infinie de Fermat.
- **Généralisation.** Cette méthode (groupe engendré par des matrices « élémentaires » agissant comme des opérations de pivot) se retrouve pour $GL_n(\mathbb{Z})$, $SL_n(\mathbb{Z})$, ou pour montrer que les transvections engendrent $SL_n(\mathbb{K})$.

6. Synthèse générale

☞ Panorama des grandes techniques rencontrées

Technique	Idée clé et exemples typiques
Densité de $\mathbb{Q}$ dans $\mathbb{R}$	Étendre une propriété de $\mathbb{Q}$ à $\mathbb{R}$ via continuité (équations de Cauchy).
Dérivation sous le signe intégral	Construire une fonction auxiliaire, dériver, identifier une relation algébrique constante (intégrale de Gauss, fonction Γ).
Double accroissements finis	Faire apparaître un terme quadratique $(x-c)^2$ (méthode de Newton).
Sommation par paquets (Abel discret)	Réindexer une somme télescopique (formule de Legendre).
Involutions sur ensemble fini	Argument de parité pour prouver l'existence d'un point fixe (deux carrés de Fermat).
Récurrence forte décroissante	Construire un objet de paramètre strictement plus petit dans le même ensemble (générateurs de $SL_2(\mathbb{Z})$, algorithme d'Euclide).
Multiplicativité des fonctions arithmétiques	Réduire le calcul aux nombres premiers via CRT (fonction σ).

– Fin de la compilation Math & Expert, Concours MPSI 2019–2024 –

R. Abed, Professeur Agrégé de Mathématiques