Séance du 13 janvier 2026

Exercice 10.

1) Donner trois définitions équivalentes de la relation de congruence $a \equiv b \pmod{n}$.

2) Démontrer ou réfuter les implications suivantes

   (a) $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n}$,

   (b) $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n} \implies a^c \equiv b^d \pmod{n}$,

   (c) $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}$,

   (d) $ab \equiv ac \pmod{n} \implies b \equiv c \pmod{n}$,

   (e) $ab \equiv ac \pmod{an} \implies b \equiv c \pmod{n}$.

3) Soient $a, b, c \in \mathbb{Z}$. On considère l'équation

$$ax + by = c \tag{E}$$

   d'inconnues $x, y \in \mathbb{Z}$ où $a, b, c \in \mathbb{Z}$ sont donnés.

   (a) Démontrer que si l'équation (E) admet une solution alors $a \wedge b \mid c$.

   (b) On suppose à partie de maintenant que $a \wedge b \mid c$. En déduire que l'équation (E) est équivalente à l'équation

$$a'x + b'y = c' \tag{E'}$$

   où

$$a' = \frac{a}{a \wedge b}, \qquad b' = \frac{b}{a \wedge b}n \qquad c' = \frac{c}{a \wedge b}.$$

   (c) Démontrer à l'aide de l'identité de Bézout que l'équation (E') admet une solution (x_0, y_0).

   (d) Soit (x, y) une autre solution de (E'), montrer que $a' \mid y - y_0$ et $b' \mid x - x_0$.

   (e) En déduire que l'ensemble des solutions de (E') est

$$\{(x_0 + b'k, y_0 - a'k) \mid k \in \mathbb{Z}\}.$$

   (f) Résoudre les équations diophantiennes

$$4x + 6y = 11, \tag{E_1}$$

$$5x + 2y = 1. \tag{E_2}$$

Solution.

1) Si $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}_{>0}$, on a

$$\begin{aligned} a \equiv b \pmod{n} &\iff n \mid b - a, \\ &\iff a \text{ et } b \text{ ont le même reste dans la division euclidienne par } n, \\ &\exists k \in \mathbb{Z},\ a = b + kn. \end{aligned}$$

2) (a) L'implication est vraie puisque si $n \mid b-a$ et $n \in d-c$ alors $n \mid b+d-(a+c)$.

(b) L'implication est fausse puisque

$$2 \equiv 2 \pmod 8, \quad 1 \equiv 9 \pmod 8$$

mais

$$2^1 \equiv 2 \not\equiv 0 \equiv 2^9 \pmod 8.$$

(c) L'implication est vraie. En effet, si $n \mid b-a$ et $n \mid d-c$ alors

$$n \mid (b-a)d + a(d-c) = bd - ac.$$

(d) L'implication est fausse puisque

$$2 \times 2 \equiv 2 \times 0 \pmod 4$$

alors que $2 \not\equiv 0 \pmod 4$.

(e) L'implication est vraie puisque s'il existe $k \in \mathbb{Z}$ vérifiant $ab = ac + kan$ alors on a $b = c + kn$ et donc $b \equiv c \pmod n$.

3) (a) Supposons que de tels entiers existent. Puisque $a \wedge b \mid a$ et $a \wedge b \mid b$, on a

$$a \wedge b \mid ax + by = c.$$

(b) Il suffit de diviser l'équation (E) par $a \wedge b$.

(c) Par définition de $a \wedge b$, on a $a' \wedge b' = 1$. Il existe donc $u, v \in \mathbb{Z}$ tels que

$$a'u + b'v = 1$$

et on a alors

$$a'(uc') + b'(vc') = c'.$$

(d) On a

$$a'x + b'y = a'x_0 + b'y_0 = c'$$

d'où

$$a'(x - x_0) = b'(y_0 - y).$$

En particulier, $a' \mid b'(y_0 - y)$ mais comme $a' \wedge b' = 1$, le lemme de Gauss nous garantit que $a' \mid y_0 - y$. De même, on a $b' \mid x - x_0$.

(e) D'après la question 3) (e), il existe $k_1, k_2 \in \mathbb{Z}$ tels que

$$x = x_0 + k_1 b', \quad y = y_0 + k_2 a'.$$

En substituant ces formules pour x et y dans (E'), on obtient

$$a'b'k_1 + a'b'k_2 = 0$$

et donc $k_1 = -k_2$. Ainsi, l'ensemble des solutions de (E') est inclus dans

$$\{(x_0 + b'k, y_0 - a'k) \mid k \in \mathbb{Z}\}.$$

L'inclusion réciproque étant claire, on a bien l'égalité entre les deux ensembles.

(f) Puisque $4 \wedge 6 = 2 \nmid 11$, l'équation (E_1) n'a pas de solutions.
On a $5 \wedge 2 = 1 \mid 1$ donc l'équation (E_2) admet des solutions et il n'y a pas de simplification à effectuer. Une solution particulière est donnée par $(1, -2)$ donc l'ensemble des solutions est donné par

$$\{(1 + 2k, -2 - 5k) \mid k \in \mathbb{Z}\}.$$

Questions.

- Énoncer et démontrer les tests de divisibilités par $3, 9, 11$.
- Le nombre 987654321 est-il premier ?
- Rappeler la définition du pgcd et du ppcm de deux entiers.
- Rappeler et démontrer le lien entre $a \wedge b$, $a \vee b$, a et b.
- Justifier que

$$\frac{a}{a \wedge b} \wedge \frac{b}{a \wedge b} = 1.$$

- Montrer que l'ensemble des solutions de l'équation

$$ax + by = 0$$

est un sous-groupe de $\mathbb{Z}^2$ isomorphe à $\mathbb{Z}$.

- Les sous-groupes de $\mathbb{Z}^2$ sont-ils tous de la forme $n\mathbb{Z} \times m\mathbb{Z}$?
- Rappeler le petit théorème de Fermat et en déduire que si $p \in \mathbb{P}$ alors la fonction polynomiale

$$x \mapsto x^p - x$$

définie sur $\mathbb{Z}/p\mathbb{Z}$ est est la fonction nulle.

- L'application $\mathbb{Z}/p\mathbb{Z}[X] \to \mathcal{F}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ est-elle injective ?

Séance du 20 janvier 2026

Exercice 13.

1) Donner la définition des suites adjacentes puis le théorème fondamental les concernant.
2) Le but de cette question est de démontrer le théorème des valeurs intermédiaires avec la méthode dite de la dichotomie.

   On considère une fonction $f : [a, b] \to \mathbb{R}$ continue et vérifiant $f(a) < 0$, $f(b) \geqslant 0$. On considère les suites $(a_n)_n$ et $(b_n)_n$ construites de la manière suivante :

   - $a_0 = a$ et $b_0 = b$,

– si a_n et b_n sont construits, on pose

$$\begin{cases} a_{n+1} = \frac{a_n+b_n}{2}, b_{n+1} = b_n \text{ si } f\left(\frac{a_n+b_n}{2}\right) < 0, \\ a_{n+1} = a_n, b_{n+1} = \frac{a_n+b_n}{2} \text{ si } f\left(\frac{a_n+b_n}{2}\right) \geqslant 0. \end{cases}$$

(a) Démontrer que les suites $(a_n)_n$ et $(b_n)_n$ sont adjacentes et convergent vers un réel $c \in [a, b]$.

(b) Montrer que $f(c) = 0$.

(c) Écrire un algorithme de dichotomie en se basant sur la preuve précédente. Il permettra d'obtenir une valeur approchée à ϵ près d'un zéro de f.

3) Le but de cette question est de démontrer que e est un nombre irrationnel. On considère pour cela les suites $(u_n)_n$ et $(v_n)_n$ définies par

$$u_n = \sum_{k=0}^{n} \frac{1}{k!}, \qquad v_n = u_n + \frac{1}{nn!}.$$

(a) Montrer que les suites $(u_n)_n$ et $(v_n)_n$ sont adjacentes et convergent vers e.

(b) En déduire que pour tout $n \in \mathbb{N}_{>0}$, on a

$$n!\, u_n < n!\, e \leqslant n!\, u_n + \frac{1}{n}.$$

(c) En déduire via un raisonnement par l'absurde que e est irrationnel.

Questions.

– Donner la définition de continuité.

– Montrer que si f est continue alors l'image par f d'un intervalle est un intervalle. Si l'intervalle est un segment, l'image est-elle un segment ?

– Montrer que si f et g sont continues alors $f + g$ l'est.

– Connaissez vous d'autres nombres irrationnels ?

– Justifier que si $(u_n)_n$ est $(v_n)_n$ sont adjacentes alors $u_n \leqslant v_n$.

– Avez vous une idée de la preuve du théorème fondamental des suites adjacentes ?

– Donner deux définitions de la fonction exponentielle.

– Démontrer le critère des séries alternées à l'aide de suites adjacentes.

Solution.

1) Deux suites $(a_n)_n$, $(b_n)_n$ sont adjacentes dites adjacentes lorsque

$$\begin{cases} (a_n)_n \text{ et } (b_n)_n \text{ sont monotones, de sens de variations opposés,} \\ a_n - b_n \xrightarrow[n\to+\infty]{} 0. \end{cases}$$

Le théorème fondamental sur les suites adjacentes affirme que deux suites adjacentes convergent vers le même réel.

2) (a) Par définition, $(a_n)_n$ est croissante tandis que $(b_n)_n$ est décroissante. De plus, on a

$$b_n - a_n = \frac{(b-a)}{2^n}$$

pour tout $n \in \mathbb{N}_{\geqslant 0}$. Elles sont donc adjacentes et d'après le théorème fondamental sur les suites adjacentes, elles convergent vers un réel $c \in \mathbb{R}$. Puisque $(a_n)_n$ et $(b_n)_n$ sont à valeurs dans $[a,b]$ qui est fermé, on a également $c \in [a,b]$.

(b) La fonction f étant continue et les suites $(a_n)_n$, $(b_n)_n$ étant convergentes de limite c , on a

$$f(c) = \lim_n f(a_n) = \lim_n f(b_n).$$

De plus, par définition des suites $(a_n)_n$, $(b_n)_n$, on a

$$f(a_n) \leqslant 0, \quad f(b_n) \geqslant 0$$

pour tout $n \in \mathbb{N}_{\geqslant 0}$. Ainsi, $f(c) \leqslant 0$ et $f(c) \geqslant 0$ d'où $f(c) = 0$.

3) (a) Si $n \geqslant 1$, on a

$$u_{n+1} - u_n = \frac{1}{(n+1)!} \geqslant 0,$$

$$\begin{aligned} v_{n+1} - v_n &= \frac{1}{(n+1)!} + \frac{1}{(n+1)(n+1)!} - \frac{1}{nn!} \\ &= \frac{n(n+1) + n - (n+1)^2}{n(n+1)(n+1)!} \\ &= \frac{-1}{n(n+1)(n+1)!} \\ &\leqslant 0. \end{aligned}$$

De plus, $v_n - u_n = \frac{1}{nn!} \xrightarrow[n\to+\infty]{} 0$ d'où $(u_n)_n$ et $(v_n)_n$ sont adjacentes et convergent donc vers la même limite. Finalement, on a

$$\lim_n u_n = \lim_n \sum_{k=1}^{n} \frac{1}{k!} = \sum_{k=1}^{+\infty} \frac{1}{k!} = e.$$

(b) Les suites $(u_n)_n$ et $(v_n)_n$ étant adjacentes, on a

$$u_n \leqslant e \leqslant v_n$$

pour tout $n \in \mathbb{N}_{>0}$. La suite $(u_n)_n$ étant strictement croissante, la première inégalité est même stricte. En multipliant par $n!$, on trouve alors

$$n!\, u_n < n!\, e \leqslant n!\, u_n + \frac{1}{n}.$$

(c) Raisonnons par l'absurde et supposons que $e = \frac{p}{q}$ avec $p, q \in \mathbb{N}_{>0}$. Alors, si $n \geqslant \max(q, 2)$, on a $n!\, u_n, n!\, e \in \mathbb{Z}$ et on a

$$n!\, u_n < n!\, e \leqslant n!\, u_n + \frac{1}{n} < n!\, u_n + 1.$$

Ainsi, $n!\, e$ est un entier compris strictement entre deux entiers consécutifs, ce qui est impossible. On en conclut que e est irrationnel.

Exercice 14.

1) Montrer que l'ensemble des solutions d'une équation différentielle linéaire homogène d'ordre 1 sur $\mathbb{R}$ est un espace vectoriel.

2) Énoncer le théorème de Cauchy-Lipschitz.

3) Rappeler et démontrer sa conséquence sur la structure de l'espace des solutions d'une équation différentielle linéaire homogène d'ordre 1 sur $\mathbb{R}$ lorsque le coefficient devant y' n'est jamais nul.

4) Démontrer via la méthode dite de la variation de la constante que si $p, f : \mathbb{R} \to \mathbb{R}$ sont continues alors les solutions de l'équation différentielle

$$y' + py = f$$

sont exactement les fonctions de la forme

$$t \mapsto \alpha e^{-\int_0^t p(x)\mathrm{d}x} + \int_0^t f(u) e^{\int_t^u p(x)\mathrm{d}x} \mathrm{d}u$$

avec $\alpha \in \mathbb{R}$.

5) Déterminer les fonctions développables en série entière autour de 0 qui sont solutions du problème de Cauchy

$$\begin{cases} y''(t) + ty'(t) + y(t) = 1, \\ y(0) = 0, \\ y'(0) = 0. \end{cases}$$

On pensera à préciser le rayon de convergence du développement en série entière de la solution.

6) (a) Résoudre l'équation différentielle

$$ty'(t) = 2y(t) \qquad (E)$$

sur $\mathbb{R}_+^*$ puis sur $\mathbb{R}_-^*$.

(b) Montrer que si y_+ est une solution de (E) sur $\mathbb{R}_+^*$ et y_- est une solution de (E) sur $\mathbb{R}_-^*$ alors

$$y : t \mapsto \begin{cases} y_+(t) \text{ si } t > 0 \\ 0 \text{ si } t = 0 \\ y_-(t) \text{ si } t < 0 \end{cases}$$

est une solution de (E) sur $\mathbb{R}$.

(c) En déduire que l'espace des solutions de (E) sur $\mathbb{R}$ est de dimension 2.

(d) Pourquoi le résultat de la question 6) (c) est-il étonnant ? Comment l'expliquez vous ?

Questions.

- Quelle structure possède l'espace des solutions d'une équation différentielle linéaire non-homogène d'ordre 1 ? Et l'espace des solutions de l'équation $y' = y^2$?
- Donner la définition de localement lipschitzien. Comment montrer qu'une fonction est localement lipschitzienne ?
- Résoudre le problème de Cauchy

$$\begin{cases} (1+t^2)y'(t) + y(t) = 1, \\ y(0) = 1. \end{cases}$$

- Généraliser la question 3) à une équation d'ordre n.
- Montrer que la fonction

$$F(\xi) = \int_{-\infty}^{+\infty} e^{-\pi^2 x^2} e^{2i\pi\xi x} \mathrm{d}x$$

est bien définie. En admettant qu'on peut commuter intégration et dérivation, déterminer une équation différentielle satisfaite par F puis déterminer une formule explicite pour F.

Solution.

1) Considérons une équation différentielle linéaire homogène d'ordre 1

$$ay' + by = 0$$

où $a, b : \mathbb{R} \to \mathbb{R}$ sont continues. La fonction nulle est clairement solution de cette équation et de plus, si y_1, y_2 sont des solutions et $\lambda \in \mathbb{R}$ alors on a

$$a(\lambda y_1 + y_2)' + b(\lambda y_1 + y_2) = \lambda(ay_1' + by_1) + ay_2' + by_2 = 0.$$

Ainsi, l'ensemble des solutions est une partie non vide et stable par combinaisons linéaires des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, c'en est donc un sous-espace vectoriel et a fortiori, un espace vectoriel.

2) Le théorème de Cauchy-Lipschitz affirme que si $f : U \to \mathbb{R}$ est définie sur un ouvert de $\mathbb{R}^2$, continue et localement lipschitzienne par rapport à sa seconde variable et si $(t_0, y_0) \in U$ alors le problème de Cauchy

$$\begin{cases} y'(t) = f(t, y(t)) \\ y(t_0) = y_0 \end{cases}$$

admet une unique solution maximale, définie sur un ouvert de $\mathbb{R}$ contenant t_0.

3) Le théorème de Cauchy-Lipschitz implique en particulier que l'espace des solutions $\mathcal{S}$ est de dimension 1. Un isomorphisme explicite avec $\mathbb{R}$ est donné, d'après le théorème de Cauchy-Lipschitz, par l'application

$$\begin{array}{ccc} \mathcal{S} & \to & \mathbb{R} \\ y & \mapsto & y(0) \end{array}.$$

4) Les solutions de l'équation homogène associée étant les fonctions de la forme

$$t \mapsto Ce^{-\int_0^t p(x)\mathrm{d}x}$$

avec $C \in \mathbb{R}$, on cherche une solution sous la forme

$$t \mapsto C(t)e^{-\int_0^t p(x)\mathrm{d}x}$$

avec $C : \mathbb{R} \to \mathbb{R}$. On a alors

$$\begin{aligned} y' + py = f &\iff C'e^{-\int_0^t p(x)\mathrm{d}x} - pCe^{-\int_0^t p(x)\mathrm{d}x} + pCe^{-\int_0^t p(x)\mathrm{d}x} = f \\ &\iff C'e^{-\int_0^t p(x)\mathrm{d}x} = f \\ &\iff C' = e^{\int_0^t p(x)\mathrm{d}x} f. \end{aligned}$$

Une solution est donc donnée par

$$t \mapsto e^{-\int_0^t p(x)\mathrm{d}x} \int_0^t e^{\int_0^u p(x)\mathrm{d}x} f(u)\mathrm{d}u = \int_0^t e^{\int_t^u p(x)\mathrm{d}x} f(u)\mathrm{d}u$$

et les solutions sont exactement les fonctions de la forme

$$t \mapsto \alpha e^{-\int_0^t p(x)} + \int_0^t f(u)e^{\int_t^u p(x)\mathrm{d}x}\mathrm{d}u$$

avec $\alpha \in \mathbb{R}$.

5) Considérons une série entière $y = \sum_{n\geqslant 0} a_n t^n$. On a

$$y'' + ty + y = 1 \iff \sum_{n\geqslant 0}(n+2)(n+1)a_{n+2}t^n + \sum_{n\geqslant 1} na_n t^n + \sum_{n\geqslant 0} a_n t^n = 1$$

donc (en supposant que le rayon de convergence est strictement positif) y est solution de l'équation différentielle si et seulement si

$$2a_2 + a_0 = 1, \qquad \forall n \geqslant 1,\ (n+2)(n+1)a_{n+2} + (n+1)a_n = 0.$$

Puisqu'on s'intéresse aux solutions vérifiant $y(0) = y'(0) = 0$, on peut supposer $a_0 = a_1 = 0$ et on trouve finalement que si y est solution de ce problème de Cauchy alors

$$a_0 = 0, \quad \forall n \geqslant 0,\ a_{2n+1} = 0, \qquad \forall n \geqslant 1,\ a_{2n} = \frac{(-1)^{n+1}}{2 \times 4 \times \cdots \times 2n} = \frac{(-1)^{n+1}}{2^n n!}.$$

Finalement, on voit que si y est solution de ce problème de Cauchy alors

$$y = \sum_{n\geqslant 1} \frac{(-1)^{n+1}}{2^n n!} t^{2n} = 1 - \sum_{n\geqslant 0} \frac{1}{n!}\Big(-\frac{t^2}{2}\Big)^n = 1 - e^{-\frac{t^2}{2}}.$$

Puisque le rayon de convergence de cette série entière vaut $+\infty$, on en déduit qu'il s'agit bien d'une solution au problème de Cauchy.

6) (a) Les solutions de l'équation différentielle (E) sur $\mathbb{R}_+^*$ et sur $\mathbb{R}_-^+$ sont exactement les fonctions de la forme

$$t \mapsto Ct^2$$

avec $C \in \mathbb{R}$.

(b) Considérons deux telles fonctions $y_+ : t \mapsto At^2$ et $y_- : t \mapsto Bt^2$. La fonction y ainsi définie est alors clairement continue sur $\mathbb{R}$. De plus, si $t > 0$, on a

$$\frac{y(t) - y(0)}{t} = At \xrightarrow[t\to 0]{} 0, \quad \frac{y(-t) - y(0)}{t} = Bt \xrightarrow[t\to 0]{} 0$$

donc y est dérivable en 0 et y' y est continue. Par construction, on a $ty'(t) = 2y(t)$ pour tout $t \in \mathbb{R}\backslash\{0\}$ et de plus, on a

$$0 = 2y(0) = 0 \cdots y'(0)$$

donc y est bien une solution de (E) sur $\mathbb{R}$.

(c) Posons $\mathrm{Sol}(\mathbb{R}_-^*)$, $\mathrm{Sol}(\mathbb{R}_+^*)$ et $\mathrm{Sol}(\mathbb{R})$ les ensembles des solutions de (E) sur $\mathbb{R}_-^*$, $\mathbb{R}_+^*$ et $\mathbb{R}$ respectivement et considérons l'application linéaire

$$\Phi : \begin{array}{ccc} \mathrm{Sol}(\mathbb{R}) & \to & \mathrm{Sol}(\mathbb{R}_-^*) \times \mathrm{Sol}(\mathbb{R}_+^*) \\ y & \mapsto & (y_{|\mathbb{R}_-^*}, y_{|\mathbb{R}_+^*}). \end{array}$$

D'après la question 6) (b), on peut également définir l'application

$$\Psi : \begin{array}{ccc} \mathrm{Sol}(\mathbb{R}_-^*) \times \mathrm{Sol}(\mathbb{R}_+^*) & \to & \mathrm{Sol}(\mathbb{R}) \\ (y_-, y_+) & \mapsto & y. \end{array}$$

Il est alors clair que Φ et Ψ sont des applications réciproques et donc que Φ est un isomorphisme d'espaces vectoriels. On en déduit que

$$\dim \mathrm{Sol}(\mathbb{R}) = \dim\Big(\mathrm{Sol}(\mathbb{R}_-^*) \times \mathrm{Sol}(\mathbb{R}_+^*)\Big) = \dim \mathrm{Sol}(\mathbb{R}_-^*) + \dim \mathrm{Sol}(\mathbb{R}_+^*) = 2.$$

(d) Le résultat de la question 6) (c) peut sembler étonnant puisque l'espace des solutions d'une équation différentielle linéaire homogène d'ordre 1 est généralement de dimension 1 d'après le théorème de Cauchy-Lipschitz.

La justification théorique de ce résultat est la suivante : le coefficient t devant y' dans l'équation (E) s'annule en $t = 0$. On ne peut donc pas mettre l'équation (E) sous la forme

$$y'(t) = f(t, y(t))$$

sur un intervalle contenant 0 et le théorème de Cauchy-Lipschitz ne s'applique donc pas.

Séance du 27 janvier 2026

Exercice 6.
On considère $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

1) Donner la définition d'une racine de multiplicité $k \in \mathbb{N}_{\geqslant 0}$ pour un polynôme $P \in \mathbb{F}[X]$.

2) Soient $P \in \mathbb{F}[X]$, $x \in \mathbb{F}$ et $k \in \mathbb{N}_{>0}$. Rappeler le critère faisant intervenir les dérivées de P pour que x soit une racine de multiplicité au moins k de P puis le démontrer.

3) (a) Déterminer les triplets $(a, b, c) \in \mathbb{R}^3$ tels que $X^5 + aX^2 + bX + c$ soit divisible par $(X-1)^3$ puis le factoriser en irréductibles sur $\mathbb{R}$ pour chacun des triplets trouvés.

   (b) Si $a, b, c \in \mathbb{R}$, on considère le polynôme

$$P(X) = X^6 - 5X^4 + aX^2 + bX + c \in \mathbb{R}[X].$$

   Déterminer les triplets (a, b, c) tels que P admette une racine d'ordre au moins 4 dans $\mathbb{R}$.

4) Démontrer que pour tout $n \in \mathbb{N}_{\geqslant 0}$, le polynôme

$$P = \sum_{k=0}^{n} \frac{1}{k!} X^k \in \mathbb{C}[X]$$

   est à racines simples.

5) (a) Montrer à l'aide du lemme de Rolle que si $P \in \mathbb{R}[X]$ est de degré $n \geqslant 2$ et scindé à racines simples alors P' est aussi scindé à racines simples.

   (b) En déduire que si $P = \sum_k a_k X^k \in \mathbb{R}[X]$ est de degré au moins 2 et scindé à racines simples, il n'existe pas d'entier $k \in \{0, \ldots, \deg P - 2\}$ tel que

$$a_k = a_{k+1} = 0.$$

Questions.

- Donner l'idée de la preuve du lemme de Rolle.
- Énoncer le théorème des accroissements finis ainsi que sa conséquence sur le lien entre la dérivée et la monotonie d'une fonction.
- Si la fonction polynomiale associée à un polynôme $P \in \mathbb{R}[X]$ est nulle, que peut-on dire de P ?
- La suite de fonctions $(\sum_{k=0}^{n} \frac{1}{k!} x^k)_{n \geqslant 0}$ converge-t-elle ? Dans quel sens ? Vers quelle fonction ?
- Montrer que la fonction cosinus n'est pas polynomiale sur $\mathbb{R}$ puis sur tout intervalle.
- Quels sont les polynômes irréductibles de $\mathbb{R}[X]$? de $\mathbb{C}[X]$?

– Combien de racines complexes distinctes possède le polynôme $\sum_{k=0}^{n} \frac{1}{k!} X^k$?

– Démontrer que si α est racine de multiplicité k pour P alors α est racine de multiplicité $k-1$ pour P'.

Solution.

1) Soient $P \in \mathbb{F}[X]$, $k \in \mathbb{N}_{\geqslant 0}$ et $x \in \mathbb{F}$. On dit que x est racine de multiplicité k pour P si et seulement si

$$k = \max\{s \in \mathbb{N}_{\geqslant 0} \mid (X-x)^s \mid P\}.$$

2) Le nombre x est une racine de multiplicité au moins k de P si et seulement si

$$P(x) = P'(x) = \cdots = P^{k-1}(x) = 0.$$

Supposons que $P(x) = P'(x) = \cdots = P^{k-1}(x) = 0$. D'après la formule de Taylor polynomiale, on a

$$P = \sum_{j \geqslant 0} \frac{P^{(j)}(x)}{j!}(X-x)^j = \sum_{j \geqslant k} \frac{P^{(j)}(x)}{j!}(X-x)^j = (X-x)^k \sum_{j \geqslant k} \frac{P^{(j)}(x)}{j!}(X-x)^{j-k}$$

d'où $(X-x)^k \mid P$.

Supposons réciproquement que x est une racine de multiplicité au moins k de P. Il existe donc $Q \in \mathbb{F}[X]$ tel que $P = (X-x)^k Q$. Considérons $s \in \{0, \ldots, k-1\}$. D'après la formule de Leibniz, on a

$$P^{(s)}(x) = \sum_{j=0}^{s} \binom{s}{j} k(k-1)\cdots(k-s+1)(x-x)^{k-s} Q^{(s_k)}(x) = 0$$

et donc

$$P(x) = P'(x) = \cdots = P^{k-1}(x) = 0.$$

3) (a) D'après la question 2), polynôme $X^5 + aX^2 + bX + c$ est divisible par $(X-1)^3$ si et seulement si

$$\begin{cases} a + b + c = -1, \\ 2a + b = -5, \\ 2a = -20. \end{cases}$$

Le seul triplet satisfaisant ce système d'équations est $(-10, 15, -6)$ et la factorisation en irréductibles du polynôme est alors

$$X^5 - 10X^2 + 15X - 6 = (X-1)^3(X^2 + 3X + 6).$$

(b) D'après la question 2), le polynôme $X^6 - 5X^4 + aX^2 + bX + c$ admet une racine d'ordre au moins 4 dans $\mathbb{R}$ si et seulement si il existe $x \in \mathbb{R}$ vérifiant

$$\begin{cases} x^6 - 5x^4 + ax^2 + bx + c = 0, \\ 6x^5 - 20x^3 + 2ax + b = 0, \\ 30x^4 - 60x^2 + 2a = 0, \\ 120x^3 - 120x = 0. \end{cases}$$

On doit donc avoir $x \in \{-1, 0, 1\}$. On trouve alors

$$(a, b, c) = \begin{cases} (15, 16, 5) \text{ si } x = -1, \\ (0, 0, 0) \text{ si } x = 0, \\ (15, -16, 5) \text{ si } x = 1. \end{cases}$$

4) Soit $x \in \mathbb{C}$ une racine multiple de P. On a alors

$$0 = P(x) - P'(x) = \frac{1}{n!} x^n$$

et donc $x = 0$. Puisque $P(0) \neq 0$, on en déduit que P n'a pas de racine multiple.

5) (a) Soit $P \in \mathbb{R}[X]$ de degré $n \geqslant 2$ et scindé à racines simples. Posons $x_1 < \cdots < x_n$ les racines de P. En appliquant le lemme de Rolle à chaque intervalle $[x_i, x_{i+1}]$ (et en utilisant le fait que P est à racines simples, on voit que pour tout $k \in \{1, \ldots, n-1\}$, il existe $y_k \in]x_k, x_{k+1}[$ vérifiant $P'(y_k) = 0$. Puisque $\deg P' = n - 1$, on en déduit que P' est aussi scindé à racines simples.

(b) Supposons au contraire qu'il existe $k \in \{0, \ldots, \deg P - 2\}$ tel que

$$a_k = a_{k+1} = 0.$$

On a donc

$$\begin{cases} P^{(k)}(0) = k!\, a_k = 0 \\ P^{(k+1)}(0) = (k+1)!\, a_{k+1} = 0 \end{cases}$$

et en particulier, $P^{(k)}$ n'est pas à racines simples. Puisque $\deg P^{(k)} \geqslant 1$, on peut appliquer k fois la contraposée du résultat de la question 5) (a) et on voit que P n'est pas à scindé à racines simples.

Nous avons donc démontré la contraposée de la propriété voulue.

Exercice 12.

1) Rappeler la définition d'un nombre premier.

2) Écrire un algorithme (sous la forme d'une suite d'instructions) permettant de déterminer tous les nombres premiers inférieurs à une borne choisie par l'utilisateur. Justifier qu'il accomplit bien cette tâche.

3) On se propose de démontrer de plusieurs manières différentes l'existence d'une infinité de nombres premiers.

(a) Montrer que si $p_1, \ldots, p_n$ sont des nombres premiers distincts alors $p_1 \cdots p_n + 1$ admet un diviseur premier différent de $p_1, \ldots, p_n$. En déduire que $\mathbb{P}$ est infini.

(b) On admet que la série

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

est divergente. En déduire que $\mathbb{P}$ est infini.

(c) Si $n \in \mathbb{N}_{\geqslant 0}$, on pose $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat. Montrer que pour tout $n \in \mathbb{N}_{>0}$, on a

$$F_0 \cdots F_{n-1} = F_n - 2.$$

En déduire que $F_n \wedge F_0 \cdots F_{n-1} = 1$ et puis que $\mathbb{P}$ est infini.

(d) Montrer que si $p_1, \ldots, p_n$ sont des nombres premiers distincts tous congrus à 3 modulo 4 alors

$$4p_1 \cdots p_n - 1$$

admet un diviseur premier congru à 3 modulo 4 différent de $p_1, \ldots, p_n$. En déduire que $\mathbb{P} \cap (3 + 4\mathbb{Z})$ est infini.

(e) On admet que si -1 est un carré modulo $p \in \mathbb{P}$ alors $p \equiv 1 \pmod 4$. Montrer que si $p_1, \ldots, p_n$ sont des nombres premiers distincts tous congrus à 1 modulo 4 alors

$$4(p_1 \cdots p_n)^2 + 1$$

admet un diviseur premier congru à 1 modulo 4 différent de $p_1, \ldots, p_n$. En déduire que $\mathbb{P} \cap (1 + 4\mathbb{Z})$ est infini.

Questions.

- Comment tester si un nombre est divisible par $2, 3, 4, 5, 6, 8, 9, 10, 11$?
- Démontrer le test de divisibilité par 3.
- Les ensembles $\mathbb{P} \cap 4\mathbb{Z}$ et $\mathbb{P} \cap (2 + 4\mathbb{Z})$ sont-ils infinis ?
- Montrer que si n n'a pas de diviseur premier inférieur à $\sqrt{n}$ alors n est premier.
- Connaissez vous une estimation du nombre de nombres premiers inférieurs à x ?
- Énoncer le théorème fondamental de l'arithmétique.
- Rappeler les formules du PGCD et du PPCM en fonctions des décompositions en facteurs premiers et démontrer que $(a \wedge b)(a \vee b) = |ab|$.

Solution.

1) Un entier positif $n \in \mathbb{N}_{\geqslant 0}$ est premier si $n \neq 1$ et si n n'est divisible que par 1 et lui-même.

2) On considère l'algorithme (dit du crible d'Eratosthène) suivant :

- Écrire tous les nombres de 2 à n.
- Entourer le premier nombre non barré.
- Barrer tous ses multiples (sauf lui-même).
- Recommencer avec le prochain nombre non barré.
- S'arrêter lorsqu'on dépasse $\sqrt{n}$.

Par construction, les nombres entourés sont exactement ceux qui ne sont multiples d'aucun nombre inférieur, ce sont donc les nombres premiers. L'arrêt à $\sqrt{n}$ provient du fait que si n n'est pas premier alors il admet un diviseur non trivial inférieur ou égal à $\sqrt{n}$.

3) (a) Considérons de tels entiers $p_1, \dots, p_n$. Clairement, $p_1 \cdots p_n + 1 \wedge p_i = 1$ pour tout $i = 1, \dots, n$. Ainsi, tous les diviseurs premiers de $p_1 \cdots p_n + 1$ sont distincts de $p_1, \dots, p_n$ et un tel diviseur premier existe. En appliquant ce même raisonnement sous l'hypothèse que $\mathbb{P} = \{p_1, \dots, p_n\}$, on voit par l'absurde que $\mathbb{P}$ est infini.

(b) Si $\mathbb{P}$ était fini alors cette série serait une somme finie et serait donc convergente.

(c) On procède par récurrence sur $n \in \mathbb{N}_{>0}$.

Initialisation : On a $F_1 = 5 = 3 - 2 = F_0 - 2$ donc la propriété est vraie au rang 1.

Hérédité : Soit $n \in \mathbb{N}_{>0}$ vérifiant

$$F_0 \cdots F_{n-1} = F_n - 2.$$

On a

$$\begin{aligned} F_0 \cdots F_n &= F_n^2 - 2F_n \\ &= 2^{2^{n+1}} + 2^{2^n+1} + 1 - 2^{2^n+1} - 2 \\ &= F_{n+1} - 2. \end{aligned}$$

donc la propriété est également vraie au rang $n+1$.

Par le principe de récurrence, la propriété est vraie pour tout $n \in \mathbb{N}_{>0}$.

Puisqu'aucun nombre de Fermat n'est pair, on en déduit clairement qu'ils sont premiers entre eux. En particulier, tous les nombres de Fermat ont des diviseurs premiers distincts, ce qui fournit une infinité de nombres premiers distincts.

(d) Une fois de plus, l'entier $4p_1 \cdots p_n - 1$ est premier avec $p_1, \dots, p_n$ et de plus, on a

$$4p_1 \cdots p_n - 1 \equiv 3 \pmod 4.$$

Puisqu'un produit de nombres congrus à 1 modulo 4 est aussi congru à 1 modulo 4, on en déduit que $4p_1 \cdots p_n - 1$ admet un diviseur premier congru à 3 modulo 4, qui est donc différent de $p_1, \dots, p_n$. L'ensemble $\mathbb{P} \cap (3 + 4\mathbb{Z})$ est donc infini.

(e) De même, l'entier

$$N \coloneqq 4(p_1 \cdots p_n)^2 + 1$$

est premier avec $p_1, \dots, p_n$. Considérons un diviseur premier p de N, qui est donc différent de $p_1, \cdots, p_n$. On a

$$(2p_1 \cdots p_n)^2 \equiv -1 \pmod p$$

donc -1 est un carré modulo p et donc $p \equiv 1 \pmod 4$. On en déduit que l'ensemble $\mathbb{P} \cap (1+4\mathbb{Z})$ est infini puisqu'on peut construire autant de tels nombres premiers qu'on le souhaite.

Séance du 29 janvier 2026

Exercice. m, n, k, ν désignent des entiers naturels non nuls et $p < q$ des nombres premiers distincts.
Soit ψ l'application qui a un entier naturel non nul associe le nombre de ses diviseurs positifs :

$$\begin{array}{rcccl} & & \mathbb{N}^* & \to & \mathbb{N}^* \\ \psi & : & n & \mapsto & \mathrm{Card}\left(\{d \in \mathbb{N}^* \mid d|n\}\right). \end{array}$$

1) Calculer $\psi(n)$ pour $n \in [\![1, 20]\!]$.

2) Calculer $\psi(p)$, $\psi(pq)$ et vérifier les résultats correspondants de la question 1.

3) Calculer $\psi\left(2^k\right)$, $\psi\left(3^k\right)$ puis $\psi\left(p^k\right)$ et vérifier les résultats correspondants de la question 1.

4) Si $n = \prod_{i=1}^{\nu} p_i^{\alpha_i}$ est la décomposition en produit de facteurs premiers de n, donner l'expression de $\psi(n)$.

Questions.

– Montrer que si $n \wedge m = 1$ alors $\psi(nm) = \psi(n)\psi(m)$.

Exercice. m, n, k, d, ν désignent des entiers naturels non nuls et $p < q$ des nombres premiers distincts.
On rappelle que la notation $m \wedge n$ désigne le PGCD des entiers m et n et qu'en particulier, ces entiers sont dits premiers entre eux ssi $m \wedge n = 1$.
L'indicatrice d'Euler est l'application φ définie par :

$$\begin{array}{rcccl} & & \mathbb{N}^* & \to & \mathbb{N}^* \\ \varphi & : & n & \mapsto & \mathrm{Card}\left(\{d \in \mathbb{N}^* \mid d \leqslant n, d \wedge n = 1\}\right). \end{array}$$

1) Calculer $\varphi(n)$ pour $n \in [\![1, 20]\!]$.

2) Calculer $\varphi(p)$, $\varphi(pq)$ et vérifier les résultats correspondants de la question 1.
Indication : dresser la liste des multiples de p et la liste des multiples de q.

3) Calculer $\varphi\left(2^k\right)$, $\varphi\left(3^k\right)$ puis $\varphi\left(p^k\right)$ et vérifier les résultats correspondants de la question 1.

4) À quoi correspond $\varphi(n)$ pour l'anneau $\mathbb{Z}/n\mathbb{Z}$?

5) Si $m \wedge n = 1$, montrer que $\varphi(mn) = \varphi(m)\varphi(n)$.
Indication : que dire des anneaux $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$ quand $m \wedge n = 1$?

6) Si $n = \prod_{i=1}^{\nu} p_i^{\alpha_i}$ est la décomposition en produit de facteurs premiers de n, donner l'expression de $\varphi(n)$.
Indication : utiliser les résultats des questions 3. et 5.

7) Si $d|n$, on définit l'ensemble $N(n,d)$ par

$$N(n,d) = \{k \in \mathbb{N}^* \mid k \leqslant n, k \wedge n = d\}.$$

Donner le cardinal de $N(n,d)$ puis déduire que

$$n = \sum_{d|n} \varphi(d).$$

Indication : remarquer que tout entier compris entre 1 et n est dans un et un seul des ensembles $N(n,d)$ pour $d|n$.

Questions.

- Rappeler la définition de PGCD et PPCM et la formule permettant de les calculer via une décomposition en facteurs premiers.
- Démontrer que $(a \wedge b)(a \vee b) = |ab|$.
- Démontre que dans $\mathbb{Z}/n\mathbb{Z}$, $\text{ord}(\overline{k}) = \frac{n}{n \wedge k}$. En déduire que si $d \mid n$, il y a $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.
- En déduire que pour tout diviseur d de n, il y a un unique sous-groupe d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.
- Á l'aide de la question 7), démontrer que $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

Exercice. Soit un ensemble S, un groupe G noté multiplicativement et d'élément neutre $e_{_G}$ et une application

$$\begin{array}{rccc} \varphi & : & G \times S & \to & S \\ & & (g,s) & \mapsto & \varphi(g,s) = g \star s \end{array}$$

vérifiant

1) $\forall g_1, g_2 \in G, \forall s \in S : \varphi\left(g_1, \varphi(g_2,s)\right) = \varphi(g_1 g_2, s)$, c'est à dire $g_1 \star (g_2 \star s) = (g_1 g_2) \star s$
2) $\forall s \in S : \varphi(e_{_G}, s) = s$, c'est à dire $e_{_G} \star s = s$

On dit alors que le groupe G agit (ou opère) sur l'ensemble S.
L'application φ définit une "multiplication" externe $\star$ des éléments s de S par les éléments g de G, de la même manière qu'on a une multiplication externe des vecteurs d'un $\mathbb{K}$-espace vectoriel par les éléments du corps $\mathbb{K}$.

1) Montrer que le groupe G agit sur lui-même via l'action dite de *translation*

$$\begin{array}{rccc} t & : & G \times G & \to & G \\ & & (g,h) & \mapsto & t(g,h) = gh \end{array}.$$

Ici $S = G$ et $\star$ est la loi de composition interne du groupe G.

2) Montrer que le groupe G agit sur lui-même via l'action dite de *conjugaison*

$$\begin{array}{rccl} c & : & G \times G & \to & G \\ & & (g,h) & \mapsto & c(g,h) = ghg^{-1} = \tau_g(h) \end{array}$$

Ici $S = G$ et $\star$ est l'opération de conjugaison.

Soit un groupe G opérant sur un ensemble S et $s \in S$.

3) Soit $s \in S$. Montrer que $G_s := \{g \in G \,|\, g \star s = s\}$ est un sous-groupe de G.
On l'appelle le *stabilisateur* de s.

4) Montrer que $G_{g\star s} = gG_sg^{-1}$.
Le stabilisateur de $g \star s$ est le conjugué du stabilisateur de s.

5) Montrer que la relation binaire $\mathfrak{R}$ définie sur $S \times S$ par

$$s_1 \mathfrak{R} s_2 \Leftrightarrow \exists g \in G : g \star s_1 = s_2$$

est une relation d'équivalence.

Questions.

- Avez-vous des applications des actions de groupes.
- Montrer que les orbites partionnent X.
- Rappeler la structure de groupe sur $S(X)$.
- Justifier qu'une action de groupe équivaut à un morphisme dans $S(X)$.
- Montrer le théorème de Cayley via l'action par translation.
- Quel est le stabilisateur d'un élément pour l'action par conjugaison ?
- Connaissez-vous des groupes non-abéliens ?
- Étant donné $s \in S$, établir une bijection entre G/G_s et $G \cdot s$.

Exercice. Le but de cet exercice est de voir plusieurs démonstrations du résultat suivant :

$$\forall p \in \mathbb{P}, \forall n \in \mathbb{N}^*, n^p \equiv n[p]$$

Dans la suite, p désignera un nombre premier et n un entier naturel.

1) Quelle structure possède $(\mathbb{Z}/p\mathbb{Z}, +, \times)$?

2) Quel est l'ordre du groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$? En déduire, en utilisant le théorème de Lagrange, que

$$\forall n \in \mathbb{N}, n \wedge p = 1 \Rightarrow n^{p-1} \equiv 1[p]$$

puis le résultat attendu.

3) **Autre démonstration.**

(a) Vérifier que le résultat est vrai pour $n = 0$, $n = 1$.

(b) Donner l'énoncé du lemme de Gauss pour des entiers.

(c) Rappeler rapidement pourquoi $\binom{p}{k}$ est toujours un entier naturel non nul (on attend deux réponses différentes).

(d) Que peut-on dire de $\binom{p}{k}$ $[p]$ pour $k \in [\![0, p]\!]$?

Indication : distinguer plusieurs cas selon les valeurs de k.

(e) Le résultat de la première question permet de supposer que le résultat est vrai pour un entier $n \in \mathbb{N}$.

Montrer que sous cette hypothèse, on a alors $(n+1)^p \equiv n+1[p]$.

Indication : utiliser la formule du binôme de Newton.

(f) Conclure.

4) **Nombres de Carmichael.**

Ce sont les entiers q non premiers qui vérifient la propriété $\forall n \in \mathbb{N}^*, n^q \equiv n[q]$. Le plus petit tel q est $q = 561$.

Écrire un programme en Python qui permet de vérifier que $q = 561$ est un nombre de Carmichael.

Questions.

– Comment calculer un inverse dans $\mathbb{Z}/n\mathbb{Z}$?

– Généraliser le petit théorème de Fermat à $\mathbb{Z}/n\mathbb{Z}$.

– Montrer que $X^{p-1} - 1 = \prod_{k=1}^{p-1}(X - \overline{k})$. En déduire le théorème de Wilson

$$(p-1)! \equiv -1 \pmod{p}.$$

– Sur $\mathbb{Z}/p\mathbb{Z}$, un polynôme non nul peut-il avoir une fonction polynomiale associée nulle ? Est-ce possible sur $\mathbb{R}$?

– Rappeler deux définitions du coefficient binomial $\binom{n}{k}$ et démontrer de deux manières différentes que

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Séance du 3 février 2026

Exercice 1.
Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}_{>0}$.

1) Rappeler la définition du plus grand diviseur commun de a et b et énoncer l'identité de Bézout.

2) Décrire l'algorithme d'Euclide (sans remontée) et démontrer qu'il permet de calculer le PGCD voulu.

3) Rappeler la définition de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

4) Démontrer que la classe de a modulo n est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.

5) Résoudre les équations

$$(a)\ \ 8x \equiv 16 \pmod{57}, \qquad (b)\ \ 8x \equiv 16 \pmod{58},$$

$$(c)\ \ 8x \equiv 15 \pmod{58}.$$

Questions.

- A quelle condition l'anneau $\mathbb{Z}/n\mathbb{Z}$ est-il un corps ?
- Est-ce que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z}$ en tant que groupes ?
- Démontrer que tout groupe monogène fini G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec $n = |G|$.
- Donner une condition nécessaire et suffisante pour que l'équation $ax \equiv b \pmod{n}$ admette une solution. Et pour que la solution soit unique ?
- On dit qu'un élément non-nul x de $\mathbb{Z}/n\mathbb{Z}$ est un diviseur de zéro s'il existe $y \in \mathbb{Z}/n\mathbb{Z}\backslash\{\overline{0}\}$ tel que $xy = \overline{0}$. Montrer que tout élément de $\mathbb{Z}/n\mathbb{Z}$ est soit nul, soit inversible, soit un diviseur de zéro.
- Quels sont les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$?

Solution.

1) Le plus grand diviseur commun de a et b est l'unique entier $d \in \mathbb{N}_{>0}$ (parfois noté $a \wedge b$) vérifiant les deux propriétés suivantes :

$$d \mid a \text{ et } d \mid b,$$

$$\forall c \in \mathbb{Z},\ \Big[(c \mid a \text{ et } c \mid b) \implies c \mid d\Big].$$

L'identité de Bézout assure alors l'existence d'entiers $u, v \in \mathbb{Z}$ vérifiant

$$au + bv = d.$$

2) Commençons par remarquer que si $a = bq + r$ est la division euclidienne de a par b alors les couples (a, b) et (b, r) ont les mêmes diviseurs communs et en particulier, $a \wedge b = b \wedge r$. En effet, si $c \mid a$ et $c \mid b$ alors $c \mid a - bq = r$ et réciproquement, si $c \mid b$ et $c \mid r$ alors $c \mid bq + r = a$.

On considère alors l'algorithme suivant (écrit ici en langage Python) :

```
while r != 0 :
    r = a%b
    a = b
    b = r
return b
```

Puisque la suite des restes est une suite strictement décroissante d'entiers positifs, la boucle s'arrête après un nombre fini d'itérations. Notons $\tilde{r}$ la dernière valeur non-nulle prise par la variable r. D'après le résultat de conservation du PGCD obtenu précédemment, on a $a \wedge b = \tilde{r} \wedge 0 = \tilde{r}$ donc l'algorithme proposé permet effectivement de calculer $a \wedge b$.

3) Ensemblistement, $\mathbb{Z}/n\mathbb{Z}$ est donné par l'ensemble des classes d'équivalences de $\mathbb{Z}$ pour la relation de congruence modulo n, c'est-à-dire

$$\mathbb{Z}/n\mathbb{Z} = \Big\{\{m + kn \mid k \in \mathbb{Z}\} \mid m \in \mathbb{Z}\Big\}.$$

On le munit d'une structure d'anneau avec les opérations

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ (\overline{k}_1, \overline{k}_2) & \mapsto & \overline{k_1 + k_2} \end{array}, \qquad \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ (\overline{k}_1, \overline{k}_2) & \mapsto & \overline{k_1 k_2} \end{array}.$$

4) Soit $a \in \mathbb{Z}$ vérifiant $a \wedge n = 1$. D'après l'identité de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $au + nv = 1$. En particulier, on a

$$\overline{an} = \overline{au + nv} = \overline{1}$$

d'où $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Supposons réciproquement que $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Il existe donc $b \in \mathbb{Z}$ vérifiant $\overline{a}\overline{b} = \overline{1}$. On en déduit qu'il existe $k \in \mathbb{Z}$ tel que

$$ab + nk = 1.$$

Puisque $a \wedge n$ divise à la fois a et n, on en déduit que $a \wedge n$ divise 1 et donc $a \wedge n = 1$.

5) (a) On a $8 \wedge 57 = 1$ donc $\overline{8}$ est inversible dans $\mathbb{Z}/57\mathbb{Z}$. Son inverse étant donné par $\overline{-7}$, on a

$$\begin{aligned} 8x \equiv 16 \pmod{57} &\iff x \equiv (-7) \times 16 \pmod{57} \\ &\iff x \equiv 2 \pmod{57}. \end{aligned}$$

(b) On a $8 \wedge 58 \neq 1$ donc la méthode précédente ne peut pas s'appliquer directement. Cependant, on peut remarquer que

$$\begin{aligned} 8x \equiv 16 \pmod{58} &\iff \exists k \in \mathbb{Z},\ 8x + 58k = 16 \\ &\iff \exists k \in \mathbb{Z},\ 4x + 29k = 8 \\ &\iff 4x \equiv 8 \pmod{29}. \end{aligned}$$

Puisque $4 \wedge 29 = 1$, on peut appliquer la méthode précédente :

$$\begin{aligned} 4x \equiv 8 \pmod{29} &\iff x \equiv (-7) \times 8 \pmod{29} \\ &\iff x \equiv 2 \pmod{29}. \end{aligned}$$

(c) Comme précédemment, on a $8 \wedge 58 \neq 1$ mais puisque $8 \wedge 58 \nmid 15$, ne peut pas affirmer que

$$8x \equiv 15 \pmod{58} \iff 4x \equiv \frac{15}{2} \pmod{29}$$

étant donné que la proposition de droite n'a pas de sens. On peut cependant écrire

$$8x \equiv 15 \pmod{58} \iff \exists k \in \mathbb{Z},\ 8x + 58k = 15$$

et remarquer qu'aucun $x \in \mathbb{Z}$ ne vérifie la proposition de droite puisque $2 \mid 8x + 58k$ pour tous $x, k \in \mathbb{Z}$ mais $2 \nmid 15$. Ainsi, l'ensemble des solutions de cette solution est l'ensemble vide.

Exercice 4.
Soit $n \in \mathbb{N}_{>0}$ et soit $A \in M_n(\mathbb{R})$. On considère le système d'équations différentielles

$$X' = AX \tag{1}$$

où $X : \mathbb{R} \to \mathbb{R}^n$.
On suppose A diagonalisable.

1) Montrer que le système différentiel (1) est équivalent au système

$$Y' = DY \tag{2}$$

où $A = PDP^{-1}$ avec $P \in GL(n, \mathbb{R})$, $D \in M_n(\mathbb{R})$ diagonale et $Y = P^{-1}X$.

2) En déduire les solutions de (1).

3) Résoudre le système différentiel

$$\begin{cases} x' = 10x + 2y - 8z, \\ y' = -5x + 2y + 7z, \\ z' = 4x + 2y - 2z. \end{cases}$$

On considère maintenant l'équation différentielle linéaire homogène du second ordre à coefficients constants

$$y'' + by' + cy = 0. \tag{3}$$

4) En introduisant une deuxième équation $y' = z$, réécrire l'équation (3) sous la forme d'un système différentiel

$$X' = AX$$

avec $A \in M_2(\mathbb{R})$.

5) Calculer le polynôme caractéristique χ_A de A. Que reconnait-on ?

6) En déduire les solutions de l'équation différentielle (3) lorsque χ_A est scindé à racines simples sur $\mathbb{R}$.

7) Proposer une généralisation de ce résultat pour une équation différentielle linéaire homogène d'ordre $n \in \mathbb{N}_{>0}$ à coefficients constants.

Questions.

- Quel est l'impact des valeurs propres de la matrice A sur le comportement asymptotique des solutions ?
- Le résultat de la question 6) est-il toujours vrai lorsque χ_A n'est pas scindé à racines simples sur $\mathbb{R}$?
- Donner la définition ainsi que plusieurs caractérisation des matrices diagonalisables.
- Donner un exemple de matrice non-diagonalisable.
- Énoncer le théorème de Cayley-Hamilton.
- Rappeler les formules pour les termes de degré $n-1$ et 0 dans le polynôme caractéristique d'une matrice $A \in M_n(\mathbb{R})$.

Solution.

1) Fixons P, D de telles matrices. La dérivée étant linéaire, on a

$$\begin{aligned} X' = AX &\iff X' = PDP^{-1}X \\ &\iff P^{-1}X' = DP^{-1}X \\ &\iff (P^{-1}X)' = D({}^{-1}X) \\ &\iff Y' = DY. \end{aligned}$$

2) Notons $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ les coefficients diagonaux de D et $y_1, \dots, y_n : \mathbb{R} \to \mathbb{R}$ les coordonnées de Y. Le système (2) étant

$$\begin{aligned} y_1' &= \lambda_1 y_1 \\ &\vdots \\ y_n' &= \lambda_n y_n, \end{aligned}$$

les solutions de (1) sont données par

$$X(t) = P\,{}^t(C_1 e^{\lambda_1 t} \cdots C_n e^{\lambda_n t})$$

où $C_1, \dots, C_n \in \mathbb{R}$.

3) En diagonalisant la matrice du système, on trouve par exemple

$$\begin{pmatrix} 10 & 2 & -8 \\ -5 & 2 & 7 \\ 4 & 2 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 3 \\ -1 & 1 & -2 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{pmatrix} \begin{pmatrix} 1 & 1 & 3 \\ -1 & 1 & -2 \\ 1 & 1 & 1 \end{pmatrix}^{-1}.$$

D'après la question 1), les solutions du système sont exactement les fonctions de la forme

$$t \mapsto \begin{pmatrix} 1 & 1 & 3 \\ -1 & 1 & -2 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} A \\ Be^{4t} \\ Ce^{6t} \end{pmatrix} = \begin{pmatrix} A + Be^{4t} + 3e^{6t} \\ -A + Be^{4t} - 2e^{6t} \\ A + Be^{4t} + Ce^{6t} \end{pmatrix}.$$

4) Posons $z = y'$. On a alors

$$y'' + by' + cy = 0 \iff \begin{cases} y' = z \\ z' = -cy - bz \end{cases} \iff X' = MX$$

avec

$$X = \begin{pmatrix} y \\ z \end{pmatrix}, \qquad M = \begin{pmatrix} 0 & 1 \\ -c & -b \end{pmatrix}.$$

5) On a

$$\begin{aligned} \chi_M(\lambda) &= \begin{vmatrix} \lambda & -1 \\ c & \lambda + b \end{vmatrix} \\ &= \lambda(\lambda + b) + c \\ &= \lambda^2 + b\lambda + c. \end{aligned}$$

L'équation $\chi_M(\lambda) = 0$ est exactement l'équation caractéristique de (3).

6) Supposons χ_M scindé à racines simples sur $\mathbb{R}$ et notons $\lambda_1, \lambda_2 \in \mathbb{R}$ ses racines. La matrice M est alors diagonalisable sur $\mathbb{R}$ avec les valeurs propres λ_1, λ_2. D'après les relations coefficients-racines, on a

$$M = \begin{pmatrix} 0 & 1 \\ -\lambda_1\lambda_2 & \lambda_1 + \lambda_2 \end{pmatrix}.$$

En diagonalisant M, on obtient

$$A = \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix}^{-1}$$

donc les solutions du système introduit sont exactement les fonctions

$$t \mapsto \begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \begin{pmatrix} Ae^{\lambda_1 t} \\ Be^{\lambda_2 t} \end{pmatrix} = \begin{pmatrix} Ae^{\lambda_1 t} + Be^{\lambda_2 t} \\ \lambda_1 e^{\lambda_1 t} + \lambda_2 e^{\lambda_2 t} \end{pmatrix}$$

et les solutions de (3) sont les fonctions de type

$$t \mapsto Ae^{\lambda_1 t} + Be^{\lambda_2 t}$$

avec $A, B \in \mathbb{R}$.

7) Si

$$y^{(n)} + a_1 y^{(n-1)} + \cdots a_{n-1} y' + a_n y = 0$$

est une équation différentielle linéaire homogène à coefficients constants pour laquelle le polynôme

$$\lambda^n + a_1 \lambda^{n-1} + \cdots + a_{n-1}\lambda + a_n$$

est scindé à racines simples alors ses solutions sont les fonctions de la forme

$$t \mapsto A_1 e^{\lambda_1 t} + \cdots A_n e^{\lambda_n t}$$

où $\lambda_1, \ldots, \lambda_n$ sont les racines du polynôme précédent et $A_1, \ldots, A_n \in \mathbb{R}$.

Séance du 5 février 2026

Exercice. Soit G un groupe et H, K deux sous-groupes de G. On définit $HK = \{hk \mid h \in H, k \in K\}$. Montrer que HK est un sous-groupe de G si et seulement $HK = KH$.

Exercice. 1) Montrer que si $(G, \times)$ est tel que :

- G est un ensemble non vide,
- $\times$ est une loi de composition interne associative sur G,
- $\exists e \in G, \forall g \in G, e \times g = g$ (existence d'un élément neutre à gauche),
- $\forall g \in G, \exists h \in G, h \times g = e$ (existence d'un inverse à gauche),

alors $(G, \times)$ est un groupe. Autrement dit, montrer que l'élément neutre à gauche est aussi un élément neutre à droite et que les inverses à gauche sont aussi des inverses à droite.

Dans la suite, G est un groupe et $n \in \mathbb{N}_{>0}$.

2) Soit $x \in G$ d'ordre n. Quel est l'ordre de x^2 ?

3) Supposons que tous les éléments de G sont d'ordre au plus 2.

   (a) Montrer que pour tous $x, y \in G$, on a $x^2 y^2 = (xy)^2$.

   (b) En déduire que G est abélien.

4) Supposon que G soit d'ordre 4. Montrer que G est abélien.

Exercice. 1) Donner l'ensemble des isométries du plan qui laissent invariant un triangle équilatéral (faire une figure). Quelle structure possède cet ensemble ?

2) Donner les éléments du groupe symétrique $\mathfrak{S}_3$ (le groupe des permutations de l'ensemble $\{1, 2, 3\}$). Comparer avec l'ensemble obtenu dans la question précédente.

3) Donner l'ensemble des isométries du plan qui laissent invariant un carré (faire une figure). Quelle est sa structure ?

4) Donner les éléments du groupe symétrique $\mathfrak{S}_4$ (le groupe des permutations de l'ensemble $\{1,2,3,4\}$). Comparer avec l'ensemble obtenu dans la question précédente.

5) Donner l'ensemble des isométries du plan qui laissent invariant un hexagone régulier. Quelle structure possède-t-il ?

6) Sans donner les éléments du groupe symétrique $\mathfrak{S}_6$ (le groupe des permutations de l'ensemble $\{1,2,3,4,5,6\}$), que pouvez-vous dire de l'ensemble obtenu dans la question précédente par rapport à $\mathfrak{G}_6$?

7) De manière générale, on note $\mathbb{D}_n$ (ou parfois $\mathbb{D}_{2n}$) et on appelle groupe diédral le groupe des $2n$ isométries du plan qui laissent invariant un n-gone régulier (ou polygone régulier à n côtés).

   (a) Écrire la table de multiplication de $\mathbb{D}_3$ et donner deux générateurs σ (une symétrie) et τ (une rotation) de ce groupe. Comparer $\sigma \circ \tau$ et $\tau \circ \sigma^{-1}$. Donner $o(\sigma)$ et $o(\tau)$.

   (b) Écrire la table de multiplication de $\mathbb{D}_4$ et donner deux générateurs σ et τ de ce groupe. Comparer $\sigma \circ \tau$ et $\tau \circ \sigma^{-1}$. Donner $o(\sigma)$ et $o(\tau)$.

   (c) Donner deux générateurs de $\mathbb{D}_n$ et les relations qui les unissent.

   (d) Montrer que $\mathbb{D}_6 \simeq \mathfrak{S}_3 \times \mathfrak{S}_2$.

Questions.

- Rappeler la classification des isométries en dimension 2. Comment les distinguer ?
- Quel est le groupe des isométries d'un triangle isocèle non-équilatéral ? D'un triangle quelconque ?
- A l'aide d'une action de groupe, montrer que $\mathfrak{S}_3 \simeq \mathbb{D}_3$.
- A-t-on $\mathfrak{S}_4 \simeq \mathbb{D}_4$?
- Écrire la liste des éléments de $\mathbb{D}_n$.
- Le groupe $\mathbb{D}_n$ est-il abélien ? Cyclique ?
- Donner un sous-groupe de $\mathbb{D}_n$ isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- Déterminer le centre de $\mathbb{D}_n$.
- Étant donné deux sous-groupe H et K de G, donner une condition nécessaire et suffisante pour que $H \times K \simeq G$.

Exercice. Soit G un groupe. Pour tout $a \in G$, on définit l'application

$$\tau_a : \begin{array}{ccc} G & \to & G \\ g & \mapsto & gag^{-1} \end{array} .$$

1) Démontrer que pour tout $a \in G$, τ_a est un endomorphisme de G.

2) En déduire que si $a \in G$, $\{aga^{-1} \mid g \in G\}$ est un sous-groupe de G.

3) Calculer $\tau_a \circ \tau_b$ pour $a, b \in G$.

4) En déduire que pour tout $a \in G$, τ_a est bijective et déterminer son inverse.

5) Montrer que $\{\tau_a \mid a \in G\}$ est un sous-groupe du groupe $\mathrm{Aut}(G)$ des automorphismes de G.

On l'appelle groupe des automorphismes intérieurs de G.

Exercice. Pour chaque question, on note $p_1 < p_2 < \cdot < p_n$ des nombres premiers.

1) Considérer le nombre $N = 1 + \prod_{i=1}^{n} p_i$ et conclure.

2) Considérer le nombre $N = 1 + p_n!$ et conclure.

3) (a) Montrer que l'ensemble des entiers du type $4k+1$ (avec $k \in \mathbb{Z}$) est stable par produit.

(b) Si il n'existe qu'un nombre fini de nombres premiers alors il n'existe évidemment qu'un nombre fini de nombres premiers du type $4k-1$ (avec $k \in \mathbb{Z}$). On les notera $q_1, \ldots, q_m$. Soit $N = 4\prod_{i=1}^{m} q_i - 1$. Justifier que N admet un diviseur premier du type $4k-1$ et conclure.

4) on considère les nombres de Fermat $F_n = 2^{2^n} + 1$ (pour $n \in \mathbb{N}_{\geqslant 0}$).

(a) Calculer de tête F_n pour $n \leqslant 3$. Que constate-t-on ?

(b) En utilisant l'algorithme d'exponentiation rapide, calculer manuellement F_4. Combien de doit-on effectuer pour vérifier que F_4 est premier ? On ne demande pas de poser ces divisions.

(c) Constatant vers 1640 que F_0, F_1, F_2, F_3 et F_4 sont tous les cinq premiers, Fermat conjectura un peu vite que tous les nombres F_n étaient premiers.

Calculer manuellement F_5.

(d) Euler, vers 1732 montra que F_5 était divisible par 641. Vérifier manuellement que $F_5 = 641 \times 6700417$. Combien de divisions Euler dut-il effectuer pour aboutir à ce résultat ?

(e) Prouver que pour tout $n \in \mathbb{N}_{\geqslant 0}$, $\prod_{i=0}^{n} F_i = F_{n+1} - 2$.

(f) En déduireq ue si $i \neq j$ alors $F_i \wedge F_j = 1$ puis conclure.

5) On considère le nombre de Mersenne $M = 2^{p_n} - 1$ et un facteur premier q de M.

(a) On raisonne modulo q. Donner l'ordre de 2 dans le groupe multiplicatif $(\mathbb{Z}/q\mathbb{Z})^*$.

(b) En considérant l'ordre de ce groupe, déduire que $p_n < q$ et conclure.

Séance du 10 février 2026

Exercice 2.
On considère les deux propriétés suivantes pour $P \in \mathbb{R}[X]$:

$$(i)\ \ \forall x \in \mathbb{R},\ P(x) \geqslant 0, \qquad (ii)\ \ \exists A, B \in \mathbb{R}[X],\ P = A^2 + B^2.$$

1) En s'inspirant de l'égalité
$$|z|^2|w|^2 = |zw|^2,$$
montrer que si $P, Q \in \mathbb{R}[X]$ vérifient (ii) alors PQ aussi.

2) Montrer que les polynômes irréductibles, unitaires et de degré 2 de $\mathbb{R}[X]$ vérifient (ii).

3) Soit $P \in \mathbb{R}[X]$ de décomposition en facteurs irréductibles
$$P = \lambda \prod_{i=1}^{n} (X - a_i)^{\alpha_i} \prod_{j=1}^{m} (X^2 + p_j X + q_j)^{\beta_j}.$$
On suppose que P vérifie la condition (i). Démontrer successivement que :
   (a) les entiers α_i sont tous pairs,
   (b) $\lambda > 0$,
   (c) P vérifie la condition (ii).

4) Établir finalement l'équivalence des conditions (i) et (ii).

Questions.

- Quels sont les polynômes à coefficients réels strictement positifs sur $\mathbb{R}$?
- Comment démontrer la formule des racines d'un polynôme du second degré sur $\mathbb{R}$?
- Donner le lien entre les racines d'un polynôme et ses coefficients.
- Si un polynôme à coefficients réels est positif sur $\mathbb{Q}$, l'est-il sur $\mathbb{R}$?
- Si un polynôme à coefficients réels est positif sur $\mathbb{Z}$, l'est-il sur $\mathbb{R}$?
- Résoudre $x^2 + 6x + 5 = 0$ dans $\mathbb{Z}/97\mathbb{Z}$.
- Expliquer graphiquement où trouver l'abscisse de l'extremal global d'un polynôme du second degré.

Solution.

1) Si $z = a + ib, w = c + id \in \mathbb{C}$, l'égalité
$$|z|^2|w|^2 = |zw|^2,$$
donne
$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$
Cette dernière égalité étant également valable si $a, b, c, d \in \mathbb{R}[X]$, on en déduit que si P et Q vérifie (ii) alors PQ aussi.

2) Soit $P = X^2 + bX + c$ un polynôme irréductible unitaire de degré 2 de $\mathbb{R}[X]$. Son discriminant $b^2 - 4c$ est alors strictement négatif et on a

$$P = \left(X + \frac{b}{2}\right)^2 + \left(\frac{1}{2}\sqrt{4c - b^2}\right)^2$$

d'où P vérifie (ii).

3) (a) Si un α_i est impair, le facteur $(X - a_i)^{\alpha_i}$ change de signe autour de a_i tandis que le reste du produit est de signe constant au voisinage de a_i. On en déduit que P ne peut pas vérifie la condition (ii) si un α_i est impair et donc que tous les α_i sont pairs si P vérifie la condition (i).

(b) Puisque tous les α_i sont pairs que que les termes de degré 2 sont strictement positifs car unitaires et irréductibles, on en déduit que le signe de P est donné par celui de λ. En particulier, $\lambda > 0$.

(c) D'après les questions 3) (b), 3) (a), 2), $\lambda > 0$ donc λ vérifie (ii) :

$$\lambda = 0^2 + \sqrt{\lambda}^2,$$

$\alpha_i \in 2\mathbb{N}$ donc chaque terme $(X - a_i)^{\alpha_i}$ vérifie la condition (ii) :

$$(X - a_i)^{\alpha_i} = \left((X - a_i)^{\frac{\alpha_i}{2}}\right)^2 + 0^2$$

et chaque terme $X^2 + p_j X + q_j$ vérifie la condition (ii).

De plus, on obtient par récurrence, en utilisant la question 1), qu'un produit de polynômes vérifiant la condition (ii) vérifie également la propriété (ii). Ainsi, P vérifie la condition (ii).

(d) D'après la question 3) (c), on a $(ii) \implies (i)$. Réciproquement, si $P \in \mathbb{R}[X]$ vérifie (ii) alors on a

$$\forall x \in \mathbb{R},\ P(x) = A(x)^2 + B(x)^2 \geqslant 0$$

et donc P vérifie (i).

Exercice 3.
Le déplacement d'un pendule simple est régit par l'équation différentielle

$$\theta'' + \frac{g}{\ell}\sin\theta = 0$$

où $\theta : \mathbb{R} \to \mathbb{R}$ est l'angle du pendule au cours du temps, g est la constante de pesanteur et ℓ est la longueur du pendule.

1) Faire un dessin représentant la situation de l'énoncé.

2) Pourquoi l'approximation $\sin\theta \approx \theta$ est-elle envisageable lorsque la position initiale du pendule est proche de l'équilibre ?

3) En déduire une formule approchée pour l'angle du pendule au cours du temps en supposant que le pendule est lâché au temps $t = 0$ à l'angle θ_0.

4) En déduire une approximation de la période du mouvement du pendule.

Questions.

- Comment pourrait-on obtenir une estimation plus précise de la position du pendule ?
- Est-il satisfaisant que la solution approchée trouvée soit périodique ?
- Donner le DSE de sin.
- Comment démontrer l'existence et l'unicité d'une solution à l'équation du pendule simple ?

Solution.

2) Lorsque la position initiale du pendule est proche de l'équilibre, $\theta(t)$ sera proche de 0. Le développement limité $\sin x = x + o(x)$ valide au voisinage de 0 rend alors raisonnable d'approcher $\sin\theta$ par θ.

3) En utilisant l'approximation proposée à la question 1), on comprend qu'on peut approcher θ par une solution $\tilde{\theta}$ de l'équation différentielle

$$\tilde{\theta}'' + \frac{g}{\ell}\tilde{\theta} = 0.$$

Il s'agit d'une équation différentielle linéaire homogène d'ordre 2 dont l'équation caractéristique est

$$r^2 + \frac{g}{\ell} = 0.$$

Ses solutions sont donc les fonctions de la forme

$$t \mapsto A\cos(\omega t) + B\sin(\omega t)$$

avec $A, B \in \mathbb{R}$ et où $\omega \coloneqq \sqrt{\frac{g}{\ell}}$. La dérivée de θ au temps $t = 0$ correspondant à la vitesse initiale donnée au pendule, on en déduit que $\tilde{\theta}$ vérifie également les conditions initiales

$$\tilde{\theta}(0) = \theta_0, \quad \tilde{\theta}'(0) = 0.$$

Ces conditions se traduisent par

$$A = \theta_0, \quad \omega B = 0$$

et donc la formule approchée est donnée par

$$\tilde{\theta}(t) = \theta_0 \cos(\omega t).$$

4) La fonction $\cos(\omega t)$ étant $\frac{2\pi}{\omega}$-périodique, on en déduit que la période du pendule vaut approximativement $2\pi\sqrt{\frac{\ell}{g}}$.

Exercice 8.
Soit $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. On dit qu'une famille $(P_1, \ldots, P_s) \in \mathbb{F}[X]^s$ est échelonnée en degré si

$$n < m \implies \deg P_n < \deg P_m.$$

1) Démontrer qu'une famille échelonnée en degré de $\mathbb{F}[X]\backslash\{0\}$ est libre dans le $\mathbb{F}$-espace vectoriel $\mathbb{F}[X]$.

2) (a) En déduire que pour tout $a \in \mathbb{F}$, et tout polynôme $P \in \mathbb{F}[X]$, il existe d'uniques scalaires $\lambda_0, \dots, \lambda_{\deg P} \in \mathbb{F}$ vérifiant
$$P = \sum_{k=0}^{\deg P} \lambda_k (X-a)^k.$$

(b) Démontrer que pour tout $k \in \{0, \dots, \deg P\}$, on a
$$\lambda_k = \frac{1}{k!} P^{(k)}(a).$$

3) Soit $n \in \mathbb{N}_{>0}$. On considère la dérivation discrète
$$\Delta : \begin{array}{ccc} \mathbb{F}[X] & \to & \mathbb{F}[X] \\ P & \mapsto & P(X+1) - P(X) \end{array}.$$

(a) Justifier que Δ induit un endomorphisme de $\mathbb{F}_n[X]$.

(b) Montrer que la famille $(H_0, \dots, H_n)$ définie par
$$\begin{cases} H_0 = 1 \\ H_k = \frac{X(X-1)\cdots(X-k+1)}{k!} \text{ si } k \geqslant 1 \end{cases}$$
est une base de $\mathbb{F}_n[X]$ puis calculer la matrice de $\Delta_{|\mathbb{F}_n[X]}$ dans cette base.

(c) Sans faire plus de calculs, diriez-vous que $\Delta_{|\mathbb{F}_n[X]}$ est diagonalisable ?

(d) Montrer que pour tout $P \in \mathbb{F}[X]$, il existe $k \in \mathbb{N}_{\geqslant 0}$ vérifiant $\Delta^k(P) = 0$ mais que pourtant, Δ n'est pourtant pas nilpotent.

Questions.

- Donner la définition d'endomorphisme diagonalisable et en donner des caractérisations.
- Diagonaliser la matrice $\begin{pmatrix} 0 & -2 \\ 1 & -3 \end{pmatrix}$.
- Montrer que $\Delta : \mathbb{F}[X] \to \mathbb{F}[X]$ est surjective mais pas injective. Est-ce normal ?
- Donner la définition d'endomorphisme nilpotent.
- La formule de Taylor polynomiale est-elle vraie sur $\mathbb{Z}/p\mathbb{Z}$?
- Montrer que les sous-espaces des fonctions paires et impaires de $\mathbb{R}$ dans $\mathbb{R}$ sont supplémentaires.
- Énoncer le théorème de Cayley-Hamilton. En déduire qu'une matrice est nilpotente si et seulement si ses valeurs propres sont toutes nulles.

Solution.

1) Soit $(P_1, \dots, P_s) \in \mathbb{F}[X]^s$ une famille échelonnée en degré et soient $a_1, \dots, a_s \in \mathbb{F}^s$ vérifiant

$$\sum_{i=1}^{s} a_i P_i.$$

Puisque la famille $(P_1, \dots, P_s)$ est échelonnée en degré, le terme de degré $\deg P_s$ du membre de gauche est $a_s C_s X^{\deg P_s}$ où C_s est le coefficient dominant de P_s. Ce terme étant nul, on doit avoir a_s. En procédant par récurrence finie descendante, on trouve similairement que

$$a_s = a_{s-1} = \cdots = a_1 = 0$$

et donc que la famille $(P_1, \dots, P_s)$ est libre.

2) (a) Soient $a \in \mathbb{F}$ et $P \in \mathbb{F}[X]$ de degré n. La famille $(1, X-a, \dots, (X-a)^n)$ étant échelonnée en degré, la question 1) nous assure que c'est une famille libre de $\mathbb{F}_n[X]$. Puisque son cardinal est égal à la dimension de $\mathbb{F}_n[X]$ (c'est-à-dire $n+1$), on en déduit que c'est une base de $\mathbb{F}_n[X]$. En particulier, de tels scalaires existent et sont uniques.

(b) Il s'agit d'une simple vérification : si $k \in \{0, \dots, \deg P\}$, on a

$$\begin{aligned}
\frac{1}{k!} P^{(k)}(a) &= \frac{1}{k!} \sum_{i=k}^{\deg P} \lambda_i i(i-1)\cdots(i-k+1)(X-a)^{i-k} \\
&= \frac{k(k-1)\cdots(k-k+1)}{k!} \lambda_k \\
&= \lambda_k.
\end{aligned}$$

3) (a) Si $P \in \mathbb{F}[X]$, on a $\deg P(X+1) = \deg P$ donc $\deg(P(X+1) - P(X)) \leqslant \deg P$ et il suit que Δ induit un endomorphisme de $\mathbb{F}_n[X]$.

(b) Cette famille de $\mathbb{F}_n[X]$ est échelonnée en degré et est donc libre d'après la question 1). Puisque son cardinal est égal à la dimension de $\mathbb{F}_n[X]$, on en déduit que c'est une base de $\mathbb{F}_n[X]$.

On a

$$\Delta(H_0) = 1 - 1 = 0,$$

$$\Delta(h_1) = X + 1 - X = 1 = H_1$$

et si $k \in \{2, \dots, n\}$, on a

$$\begin{aligned}
\Delta(H_k) &= \frac{(X+1)X(X-1)\cdots(X-k+2)}{k!} - \frac{X(X-1)\cdots(X-k+1)}{k!} \\
&= \frac{X(X-1)\cdots(X-k+2)}{k!}(X+1-X+k-1) \\
&= \frac{X(X-1)\cdots(X-k+2)}{k!} k \\
&= H_{k-1}.
\end{aligned}$$

Ainsi, la matrice de $\Delta_{|\mathbb{F}_n[X]}$ dans cette base est

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

(c) L'endomorphisme $\Delta_{|\mathbb{F}_n[X]}$ n'admet que la valeur propre 0 mais n'est pas l'endomorphisme nul, il ne peut donc pas être diagonalisable.

(d) D'après la question 3) (b), l'endomorphisme $\Delta_{|\mathbb{F}_n[X]}$ est nilpotent d'indice $n+1$ pour tout $n \in \mathbb{N}_{>0}$. Ainsi, si $P \in \mathbb{F}[X]$, on a $\Delta^{\deg P+1}(P) = 0$.

Cependant, pour tout $n \in \mathbb{N}_{>0}$, on a

$$\Delta^n(H_n) = H_0 = 1 \neq 0$$

donc Δ n'est pas nilpotent.