LYCEE CHARLEMAGNE
Lundi 3 février
M.P.S.I.2

2024 2025

TD17

◃0▹ ♡ A est une matrice carrée de taille 2 de trace 7 et de déterminant 10. Montrez alors : $A^2 = 7.A - 10.I_2$.
On pose $B = A - 2.I_2$ et $C = A - 5.I_2$. Montrez : $B.C = C.B$ et exprimez B^2 comme multiple de B et C^2 comme multiple de C.
Exprimez A comme combinaison de B et C.

Une bonne fois pour toutes : $A^2 - Tr(A).A + \det(A).I_2 = 0_{2,2}$. C'est toujours vrai.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a^2+b.c & b.(a+d) \\ c.(a+d) & b.c+d^2 \end{pmatrix} = (a+d).\begin{pmatrix} a & b \\ c & d \end{pmatrix} - (a.d-b.c).\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

C'est la formule de Hamilton et Cayley. Et elle admet une généralisation en taille n sur n, mais évidemment avec n termes, et c'est le polynôme caractéristique qui revient.

On développe $B.C = (A - 2.I_2).(A - 5.I_2) = A^2 - 2.A - 5.A + 10.I_2 = 0_{2,2}$ et de même $C.B = 0_{2,2}$.
B et C sont permutables mais en plus, les produits seront nuls.

$B^2 = A^2 - 4.A + 4.I_2$ car A et I_2 commutent.
$B^2 = (7.A - 10.I_2) - 4.A + 4.I_2$
$B^2 = 3.A - 6.I_2$
$B^2 = 3.B$

De même $C^2 = A^2 - 10.A + 25.I_2$
$C^2 = (7.A - 10.I_2) - 10.A + 25.I_2$
$C^2 = -3.A + 15.I_2$
$C^2 = (-3).C$

On combine ensuite $B = A - 2.I_2$ avec $C = A - 5.I_2$ pour arriver à $A = \dfrac{5.B - 2.C}{3}$.

On peut appliquer la formule du binôme car B et C sont permutables (de même que $\frac{5}{3}.B$ et $\frac{-2}{3}.C$).

On obtient a priori $n+1$ termes : $A^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k}.\left(\frac{5}{3}.B\right)^{n-k}.\left(\frac{-2}{3}.C\right)^{n-k}$.

Mais il n'en reste que deux car $B.C$ et $C.B$ donnent la matrice nulle : $A^n = \left(\frac{5}{3}.B\right)^n + \left(\frac{-2}{3}.C\right)^n$ ($k = 0$ et $k = n$).

De plus, en mettant en boucle $B^2 = 3.B$, on obtient $B^n = 3^{n-1}.B$. Et de même $C^n = (-3)^{n-1}.C$.

Il reste cette fois $A^n = \dfrac{5^n}{3}.B + \dfrac{2^n}{3}.C$.

Et de fait, c'est encore la diagonalisation de A présentée d'une autre façon...

◃1▹ ♡ Montrez que les matrices de taille 2 sur 2 à déterminant non nul forment un groupe pour la multiplication, non commutatif.
Montrez que l'ensemble des matrices de taille 2 sur 2 à coefficients entiers et à déterminant 1 en forme un sous-groupe.
En est il de même pour les matrices de taille 2 sur 2 à coefficients entiers et à déterminant 1 ou -1.

◃2▹ Montrez que $(A,\ B) \longmapsto Tr({}^tA.B)$ est un produit scalaire sur $(M_n(\mathbb{R}), +, .)$.
Déduisez $Tr(M^2) \leqslant Tr({}^tM.M)$ pour toute matrice M. Cas d'égalité ?
Déduisez $Tr(M^2) \geqslant -Tr({}^tM.M)$ pour toute matrice M. Cas d'égalité ?

◃3▹ ♣ Existe-t-il un produit scalaire de $(\mathbb{R}^2, +, .)$ pour lequel $\overrightarrow{i}$ est orthogonal à $\overrightarrow{i} + \overrightarrow{j}$, et $\overrightarrow{i} - \overrightarrow{j}$ est orthogonal à 4. $\overrightarrow{i} + \overrightarrow{j}$? Si oui, choisissez en un, et construisez une base orthonormée de premier vecteur colinéaire à $\overrightarrow{i}$.

On raisonne par analyse et synthèse. On écrit tout ce qu'on peut, et ensuite, on regarde si ce à quoi on est arrivé est cohérent.

On veut $\phi(\vec{i}, \vec{i}+\vec{j}) = 0$ et $\phi(\vec{i}-\vec{j}, 4.\vec{i}+\vec{j}) = 0$.
Ceci conduit à $\phi(\vec{i}, \vec{j}) = -\phi(\vec{i}, \vec{i})$ puis $\phi(\vec{j}, \vec{j}) = 4.\phi(\vec{i}, \vec{i}) - 3.\phi(\vec{i}, \vec{j})$ (symétrie...).
On sent que tout ceci est défini « à $\phi(\vec{i}, \vec{i})$ près ».

On va s'imposer $\phi(\vec{i}, \vec{i}) = 1$, ce qui ne restreint pas la généralité (ce qui serait idiot, ce serait de poser $\phi(\vec{i}, \vec{i}) = -3$ pour un produit scalaire).
On complète la matrice de Gram : $\begin{pmatrix} 1 & -1 \\ -1 & 7 \end{pmatrix}$.
Mais est ce bien une matrice de Gram ? Je vérifie la positivité des termes diagonaux et du déterminant, en taille 2 cela suffit.

Pas convaincus ? : $\left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix}\right) \longmapsto \begin{pmatrix} x & y \end{pmatrix} . \begin{pmatrix} 1 & -1 \\ -1 & 7 \end{pmatrix} . \begin{pmatrix} x' \\ y' \end{pmatrix}$ est évidemment bilinéaire symétrique.
Pour défini-positive, on calcule $\begin{pmatrix} x & y \end{pmatrix} . \begin{pmatrix} 1 & -1 \\ -1 & 7 \end{pmatrix} . \begin{pmatrix} x \\ y \end{pmatrix} = (x-y)^2 + 6.y^2$, c'est positif, et ce n'est nul que pour $x = y = 0$.

On a un produit scalaire.
On vérifie quand même (même si on a tout fait pour) :
$\begin{pmatrix} 1 & 0 \end{pmatrix} . \begin{pmatrix} 1 & -1 \\ -1 & 7 \end{pmatrix} . \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix} . \begin{pmatrix} 0 \\ 6 \end{pmatrix} = 0$
$\begin{pmatrix} 1 & -1 \end{pmatrix} . \begin{pmatrix} 1 & -1 \\ -1 & 7 \end{pmatrix} . \begin{pmatrix} 4 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \end{pmatrix} . \begin{pmatrix} 3 \\ 3 \end{pmatrix} = 0$

J'ai choisi $\vec{i}$ normé, j'en profite.
Il me faut un second vecteur : $\vec{j}$. Pardon. Un second vecteur orthogonal à $\vec{i}$: $\vec{i}\,\vec{j}$.
On le norme : $\dfrac{\vec{i}+\vec{j}}{\sqrt{6}}$ puisque $\begin{pmatrix} 1 & 1 \end{pmatrix} . \begin{pmatrix} 1 & -1 \\ -1 & 7 \end{pmatrix} . \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \end{pmatrix} . \begin{pmatrix} 0 \\ 6 \end{pmatrix} = 6$.

Vérification : On a une matrice de passage $P = \begin{pmatrix} 1 & \frac{1}{\sqrt{6}} \\ 0 & \frac{1}{\sqrt{6}} \end{pmatrix}$.
On l'inverse : $T = \begin{pmatrix} 1 & -1 \\ 0 & \sqrt{6} \end{pmatrix}$.
On vérifie : ${}^tT.T = \begin{pmatrix} 1 & 0 \\ -1 & \sqrt{6} \end{pmatrix} . \begin{pmatrix} 1 & -1 \\ 0 & \sqrt{6} \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & 7 \end{pmatrix} = G$.

◁ 4 ▷

♡ Montrez que l'équation $\vec{a} \wedge (\vec{i}+\vec{j}) = (\vec{j}+\vec{k})$ n'a pas de solution.
Montrez que l'équation $\vec{a} \wedge (\vec{i}+\vec{k}) = (\vec{i}-\vec{k})$ a des solutions.
Parmi les solutions l'équation $\vec{a} \wedge (\vec{i}+\vec{j}) = (\vec{i}-\vec{j})$ y en a-t-il qui sont solutions de $\vec{a} \wedge (\vec{i}-2.\vec{k}) = (4.\vec{i}+\vec{j}+2.\vec{k})$.

Rappel : pour $\vec{a}$ et $\vec{b}$ donnés dans $\mathbb{R}^3$, qui est $\vec{a} \wedge \vec{b}$?

S.I.I.	Physique	Mathématiques
$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \wedge \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} y.z'-z.y' \\ z.x'-x.z' \\ x.y'-y.x' \end{pmatrix}$	le vecteur positiviement orthogonal à $\vec{a}$ et $\vec{b}$, dont la norme est l'aire du parallélogramme défini par $\vec{a}$ et $\vec{b}$	l'unique vecteur vérifiant : $\forall \vec{c} \in \mathbb{R}^3$, $\det(\vec{a}, \vec{b}, \vec{c}) = (\vec{a} \wedge \vec{b}).\vec{c}$

Pour que $\vec{a} \wedge (\vec{i}+\vec{j}) = (\vec{j}+\vec{k})$ ait une solution, il faut déjà que $(\vec{j}+\vec{k})$ soit orthogonal à $(\vec{i}+\vec{j})$ (et aussi à $\vec{a}$, et que la norme soit correcte, mais qu'importe).
Or, $(\vec{j}+\vec{k})$ et $(\vec{i}+\vec{j})$ ont pour produit scalaire 1 et pas 0.

$\vec{a} \wedge (\vec{i}+\vec{k}) = (\vec{i}-\vec{k})$ a au moins une solution : $\vec{j} \wedge (\vec{i}+\vec{k}) = (\vec{i}-\vec{k})$.
Je la qualifie de solution particulière.
On a aussi des solutions « homogènes » : $(\alpha.\vec{i}+\alpha.\vec{k}) \wedge (\vec{i}+\vec{k}) = \vec{0}$.
On trouve que les $\vec{j}+\alpha.(\vec{i}+\vec{k})$ sont une famille entière de solutions.
Ce sont même toutes les solutions.

Peut on choisir α pour avoir aussi

$$\left(\overrightarrow{j}+\alpha.(\overrightarrow{i}+\overrightarrow{k})\right)\wedge(\overrightarrow{i}-2.\overrightarrow{k})=(4.\overrightarrow{i}+\overrightarrow{j}+2.\overrightarrow{k})$$

On veut $\begin{pmatrix}1\\ \alpha\\ \alpha\end{pmatrix}\wedge\begin{pmatrix}1\\ 0\\ -2\end{pmatrix}=\begin{pmatrix}4\\ 1\\ 1\end{pmatrix}$: on résout $-2.\alpha=1$, $\alpha+2=1$ et $-\alpha=1$. C'est incohérent.

◃5▹ Montrez : $\overrightarrow{BC}\wedge\overrightarrow{BD}=\overrightarrow{AB}\wedge\overrightarrow{AC}+\overrightarrow{AC}\wedge\overrightarrow{AD}+\overrightarrow{AD}\wedge\overrightarrow{AB}$ (juste avec la relation de Chasles et la multilinéarité).

Partons de $\overrightarrow{BC}\wedge\overrightarrow{BD}$ avec l'aide de Chasles et de ses relations :

$$\overrightarrow{BC}\wedge\overrightarrow{BD}=(\overrightarrow{AC}-\overrightarrow{AB})\wedge(\overrightarrow{AD}-\overrightarrow{AB})$$
$$\overrightarrow{BC}\wedge\overrightarrow{BD}=(\overrightarrow{AC}\wedge\overrightarrow{AD})-(\overrightarrow{AC}\wedge\overrightarrow{AB})-(\overrightarrow{AB}\wedge\overrightarrow{AD})+(\overrightarrow{AB}\wedge\overrightarrow{AB})$$
$$\overrightarrow{BC}\wedge\overrightarrow{BD}=(\overrightarrow{AC}\wedge\overrightarrow{AD})+(\overrightarrow{AB}\wedge\overrightarrow{AC})+(\overrightarrow{AD}\wedge\overrightarrow{AB})+(\overrightarrow{AB}\wedge\overrightarrow{AB})$$

en jouant sur les signes moins

$$\overrightarrow{BC}\wedge\overrightarrow{BD}=(\overrightarrow{AC}\wedge\overrightarrow{AD})+(\overrightarrow{AB}\wedge\overrightarrow{AC})+(\overrightarrow{AD}\wedge\overrightarrow{AB})$$

puisque $(\overrightarrow{AB}\wedge\overrightarrow{AB})$ est nul.

◃6▹ ♡ Montrez que $(A,\ B)\longmapsto Tr({}^tA.S.B)$ est un produit scalaire sur $(M_2(\mathbb{R}),+,.)$ sachant $S=\begin{pmatrix}3&2\\2&5\end{pmatrix}$. Calculez l'angle entre $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ et $\begin{pmatrix}0&0\\0&1\end{pmatrix}$.

◃7▹ Construisez un produit scalaire dans $(\mathbb{R}^3,+,.)$ pour que $(\overrightarrow{i},\ \overrightarrow{i}+\overrightarrow{j}+2.\overrightarrow{k},\ \overrightarrow{i}+\overrightarrow{j}+\overrightarrow{k})$ soit orthonormée.

◃8▹ ♡ Montrez que $(\begin{pmatrix}x\\y\end{pmatrix},\begin{pmatrix}x'\\y'\end{pmatrix})\longmapsto 34.x.x'-12.x.y'-12.x'.y+41.y.y'$ est un produit scalaire sur $(\mathbb{R}^2,+,.)$ (noté ϕ).
♣ Donnez deux vecteurs non nuls, orthogonaux à la fois pour ce produit scalaire et pour le produit scalaire usuel (c'est à dire $\phi(\overrightarrow{a},\ \overrightarrow{b})=\overrightarrow{a}.\overrightarrow{b}=0$).

On prend deux vecteurs, on calcule un réel.
Par commutativité de la multiplication dans $\mathbb{R}$, on a bien $34.x.x'-12.x.y'-12.x'.y+41.y.y'=34.x'.x-12.x'.y-12.x.y'+41.y'.y$.

En écrivant $34.x.x'-12.x.y'-12.x'.y+41.y.y'=\begin{pmatrix}x&y\end{pmatrix}.\begin{pmatrix}34&-12\\-12&41\end{pmatrix}.\begin{pmatrix}x'\\y'\end{pmatrix}$ et en utilisant ${}^tU.G.(\lambda.V+\mu.W)=\lambda.({}^tU.G.V)+\mu.({}^tU.G.W)$, on a la bilinéarité.
Pour la positivité, on prend x et y et on calcule :
$34.x^2-24.x.y+41.y^2=34.\left(x-\frac{12}{34}\right)^2+\left(41-\frac{12^2}{34}\right).y^2=34.\left(x-\frac{12}{34}\right)^2+\frac{625}{17}.y^2$
on reconnaît une somme de carrés de réels, c'est gagné.
Si de plus on suppose $34.\left(x-\frac{12}{34}\right)^2+\frac{625}{17}.y^2=0$, on aboutit à $x=y=0$.

On a bien une forme bilinéaire symétrique positive, défini-positive.

On cherche un couple $(\begin{pmatrix}x'\\y'\end{pmatrix},\begin{pmatrix}x'\\y'\end{pmatrix})$ vérifiant à la fois $\begin{array}{llll}x.x' & & +y.y' & =0\\ 34.x.x' & -12.(x'.y+y'.x) & +41.y.y' & =0\end{array}$.

On raisonne par équivalences $\begin{array}{llll}x.x' & & +y.y' & =0\\ & -12.(x'.y+y'.x) & +7.y.y' & =0\end{array}$ car on est en sciences et pas en bidouillages d'équations sans cervelle.
Comme l'orthogonalité des vecteurs se définit à proportionnalité près, on peut imposer par exemple $x=x'=1$ (diviser chaque vecteur par sa première composante).

Le système devient $\begin{array}{llll}1 & & +y.y' & =0\\ & -12.(y+y') & +7.y.y' & =0\end{array}$

On connaît le produit : $y.y'=-1$ et la somme : $y+y'=\frac{-7}{12}$.

On récupère y et y' (rôles symétriques) : $y = -\frac{4}{3}$ et $y' = \frac{3}{4}$.

On a un couple de vecteurs possible : $(\begin{pmatrix} 1 \\ -4/3 \end{pmatrix}, \begin{pmatrix} 1 \\ 3/4 \end{pmatrix})$.

On pourra préférer $\boxed{(\begin{pmatrix} 3 \\ -4 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \end{pmatrix})}$ et vérifier :

$\begin{pmatrix} 3 & -4 \end{pmatrix} . \begin{pmatrix} 4 \\ 3 \end{pmatrix} = 0$ et $\begin{pmatrix} 3 & -4 \end{pmatrix} . \begin{pmatrix} 34 & -12 \\ -12 & 41 \end{pmatrix} \begin{pmatrix} 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 & -4 \end{pmatrix} . \begin{pmatrix} 100 \\ 75 \end{pmatrix} = 0.$

Pour le professeur de mathématiques : il suffisait d'aller chercher deux vecteurs propres de la matrice réelle symétrique...

Parés côté **t**ennis, des taupins trichent sur les **m**aths. Des fe**ss**ées, ça fait mal à la nu**q**ue. Ce vieux cr**û** gâte le **g**out du **b**lanc. Des p**arr**ains se b**ut**ent, et ces br**ut**es sont privées de P**âq**ues. Que fait ce verr**at** das ce ch**am**p ? Con**f**inés, il faut remonter la **p**ente !
*Les conf**i**nés sont ils à l'abri des p**a**nnes ? Face au**x** ados dans les ly**c**ées, aux **p**ions et aux conf**i**nés, Blanquer prétend **rec**tifier les **no**tions. Grosse p**ei**ne à Suc**y**. Le **f**eu à la **N**ièvre. Combien de k**in**és conf**us** ? Des confi**n**és ont du mal à pi**g**er. Faut il conf**in**er les p**ort**eurs ?*
*On l'a trop **g**âté à la **t**aule. Ce **j**us sent le **c**oing. Faut il évac**u**er l'é**l**u ? Tr**ain** de Put**eaux**. Les cheminots **d**outent des **g**ares. Ce viticulteur a vu é**c**later bien des fûts. On observe des **b**ruits en **t**as. Ce cli**mat** trop chaud c'est à **Tho**non ? La dessinatrice **quê**te des **ma**quettes. Cette **B**u**z**in n'arrête pas de p**é**ter.*
L'employée qui fait des **c**olis s'attend à être **f**ouillée. Je laisse **p**asser ma belle-**m**ère. J'ai explosé quelques b**u**lles sur le quAI. Qu'est ce qui é**to**nne du cli**mat** ? La b**r**aise échauffe le tout. Coup de fou**d**re dans l'é**th**er, hier. Tu es bienve**n**u, tu peux déco**ll**er. Ma**n**ille aime les **f**eux. A cause des car**en**ces, on ne veut plus des B**é**Dés.

Gérard Durand Gérant du Rare (spécialiste des palindromes) :

Luc note : « Taré, tu palis si la .... rate ton ... ! ».

Ami, Sheila pompa Papon, là chez Mia. (syllabes).

Alec a soif : Ed (rapporte Luc, né ici, ... trop, par défi ?) osa cela. (Retrouvez le mot qui manque dans ce palindrome).

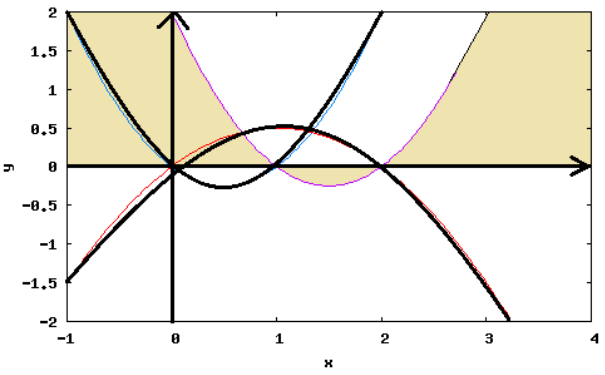
Oui, Dora ! Il .... au gourbi, ce bi, gourd obèse. Il adore, oui. (celui là, il est syllabique).

Mon Edmond, rare génie, venu à Noël à Segré, va ....., ... râpé par Luc, reçu, sa ..... sale ! On a une veine, Gérard, nom de nom !

J'ai enlevé quelques mots, mais comme ce sont des palindromes, vous pouvez retrouver les lettres qui manquent.

◃ 9 ▹

Montrez que $(P,\ Q) \longmapsto \sum_{k=0}^{2} P(k).Q(k)$ est un produit scalaire sur $(\mathbb{R}_2[X], +, .)$. Montrez que la famille $(X.(X-1),\ X.(2-X),\ (X-1).(X-2))$ est orthogonale pour ce produit scalaire.
Qui sont les polynômes orthogonaux au sous-espace vectoriel des polynômes constants ? Donnez une base de ce plan. Donnez même une base orthonormée.
Montrez que $P(X) \longmapsto P(X+1)$ (notée T) est un automorphisme de $(\mathbb{R}_2[X], +, .)$.



Forme, bilinéaire, symétrique. Tout ça c'est cadeau.

Positive car $\sum_{k=0}^{2} (P(k))^2$ est positif... ou nul.

Mais comment voulez vous que ceci soit nul ? En imposant $P(0) = P(1) = P(2) = 0$.
Alors que P est de degré inférieur ou égal à 2. Pauvre P, le voilà nul.
C'est bon, on a une forme bilinéaire symétrique positive défini-positive.

En nommant A, B et C les tris polynômes, quand on calcule quelquechose comme $A.B$, on a un polynôme factorisable par $X.(X-1).(X-2)$.

Il est nul en 0, 1 et 2. la somme $A(0).B(0) + A(1).B(1) + A(2).B(2)$ est nulle.
C'est bien pareil avec $A.C$ et $B.C$.

Pour être orthogonal à tous les polynômes constants, il suffit d'être orthogonal à 1.
La condition devient $P(0) + P(1) + P(2) = 0$.
pas grand chose à dire de plus.
On a le noyau d'une forme linéaire non nulle. C'est un sous-espace vectoriel e l'espace de départ, de dimension $3 - 1$. Ce qui fait 2.

Une base ? Il suffit de deux polynômes non colinéaires.
$X - 1$ est parfait comme premier polynôme ($P(1)$ est nul, $P(0)$ et $P(2)$ sont opposés).
$X^2 + a$ avec a bien ajusté : $X^2 - \dfrac{5}{3}$ par exemple.

On la veut orthonormée ?
On renorme le premier : $\dfrac{X-1}{\sqrt{2}}$ car $\phi(X-1,\ X-1) = 2$.
On construit le second par méthode de Schmidt : $X^2 - \dfrac{5}{3} - \phi\Big(X^2 - \dfrac{5}{3},\ \dfrac{X-1}{\sqrt{2}}\Big).\dfrac{X-1}{\sqrt{2}}$ (oui, $\overrightarrow{\varepsilon_2} - \phi(\overrightarrow{\varepsilon_2}, \overrightarrow{e_1}).\overrightarrow{e_1}$.

On trouve $\dfrac{3.X^2 - 6.X + 1}{6}$. Autant prendre $3.X^2 - 6.X + 1$ qui est bien dans le sous-espace, et orthogonal au premier.

On le norme et on colle les deux $\left(\dfrac{X-1}{\sqrt{2}},\ \dfrac{3.X^2 - 6.X + 1}{\sqrt{6}}\right)$

Montrez que $P(X) \longmapsto P(X+1)$ (notée T) est un automorphisme de $(\mathbb{R}_2[X], +, .)$.

Existence : pas de problème.
Image : $P(X+1)$ est un polynôme de même degré.
Linéarité : $P(X+1) + Q(X+1) = (P+Q)(X+1)$ et pour $\lambda.P$.
Bijectivité : on donne l'application réciproque : $Q(X) \longmapsto Q(X-1)$.

◁ 10 ▷

Vrai ou faux : $\cos(a) = \cos(b) \Rightarrow a = b + 2.k.\pi$ *ou* $a + b = 2.k.\pi$
$(a = b + 2.k.\pi\ (\forall k \in \mathbb{Z})) \Rightarrow \sin(a) = -\sin(b)$

Vrai ou faux : si A commute avec B et C alors B commute avec C (matrices de taille 2 sur 2).

Vrai ou faux : $x \longmapsto \int_0^x f(t).dt$ a pour dérivée $t \longmapsto f(t)$.

Vrai ou con : $x \longmapsto x.\int_0^x f(t).dt$ a pour dérivée $x \longmapsto \int_0^x f(t).dt + x.f(t)$.

Lesquelles sont bonnes :

$[2.x] = 2.[x]$	$\exists x,\ [2.x] = 2.[x]$	$\forall x,\ [2.x] = 2.[x]$
$[2.x] \neq 2.[x]$	$\exists x,\ [2.x] \neq 2.[x]$	$\forall x,\ [2.x] \neq 2.[x]$

$\cos(a) = \cos(b) \Rightarrow a = b + 2.k.\pi$ *ou* $a + b = 2.k.\pi$

Mais k n'est pas quantifié ! Il est peut être complexe !

$(a = b + 2.k.\pi\ (\forall k \in \mathbb{Z})) \Rightarrow \sin(a) = -\sin(b)$
On ne peut pas avoir $(a = b + 2.k.\pi$ pour tous les k à la fois !
On ne quantifie pas n'importe comment.
C'est donc de la forme $(Faux \Rightarrow Truc)$. C'est donc vrai.

Mais il ne faut pas confondre avec $\forall k \in \mathbb{Z},\ (a = b + 2.k.\pi) \Rightarrow \sin(a) = -\sin(b)$ qui est faux...
sauf si a et b sont bien choisis.

Vrai ou faux : si A commute avec B et C alors B commute avec C (matrices de taille 2 sur 2).
Faux. I_2 commute avec $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ et I_2 commute avec $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.
Mais $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ ne commute pas avec $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Vrai ou faux : $x \longmapsto \int_0^x f(t).dt$ a pour dérivée $t \longmapsto f(t)$.
Vrai. Même si on a plus envie de dire $x \longmapsto \int_0^x f(t).dt$ a pour dérivée $x \longmapsto f(x)$.

Mais une fois que l'énoncé n'a pas figé x et t, on a $(t \longmapsto f(t)) = (x \longmapsto f(x))$ (qu'on appelle aussi f).

Vrai ou con : $x \longmapsto x.\int_0^x f(t).dt$ a pour dérivée $x \longmapsto \int_0^x f(t).dt + x.f(t)$.
Con ! Dans $x \longmapsto \int_0^x f(t).dt + x.f(t)$, qui est ce t ?
Ce qui est vrai c'est $x \longmapsto x.\int_0^x f(t).dt$ a pour dérivée $x \longmapsto \int_0^x f(t).dt + x.f(x)$ (et encore, pour $f$continue).

$[2.x] = 2.[x]$		$\exists x,\ [2.x] = 2.[x]$		$\forall x,\ [2.x] \neq 2.[x]$
qui est x ?		oui : $x = 0$		faux : il existe $x = 0$
$[2.x] \neq 2.[x]$		$\exists x,\ [2.x] \neq 2.[x]$		$\forall x,\ [2.x] \neq 2.[x]$
qui est x je le redis		vrai : $x = \frac{2}{3}$		encore ?

◃ 11 ▹

Retrouvez sans effort que (dans $(\mathbb{R}^3, +, .)$ pour le produit scalaire usuel) l'orthogonal du plan d'équation $x + y - 3.z = 0$ est $Vect(\overrightarrow{i} + \overrightarrow{j} - 3.\overrightarrow{k})$.

$x + y - 3.z = 0$ est l'équation d'un plan.
Mais elle s'écrit aussi $\begin{pmatrix} x \\ y \\ z \end{pmatrix} . \begin{pmatrix} 1 \\ 1 \\ -3 \end{pmatrix} = 0$. Et c'est alors l'équation de l'orthogonal de $Vect(\overrightarrow{i} + \overrightarrow{j} - 3.\overrightarrow{k})$.
C'est tout. Ces ensembles ont la même équation, ils sont égaux.

Existe-t-il un produit scalaire sur $(\mathbb{R}^3, +, .)$ pour lequel l'orthogonal du plan d'équation $x + y - z = 0$ soit $Vect(\overrightarrow{i} + \overrightarrow{j})$?

On prend une base du plan : $(\overrightarrow{i} - \overrightarrow{j},\ \overrightarrow{i} + \overrightarrow{k})$. On veut que ces deux vecteurs soient orthogonaux à $\overrightarrow{i} + \overrightarrow{j}$.
Il suffit de demander que $(\overrightarrow{i} - \overrightarrow{j},\ \overrightarrow{i} + \overrightarrow{k},\ \overrightarrow{i} + \overrightarrow{j})$ soit *orthφnomee*.
On écrit la matrice de passage $P = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. On l'inverse : $T = \frac{1}{2}.\begin{pmatrix} 1 & -1 & -1 \\ 0 & 0 & 2 \\ 1 & 1 & -1 \end{pmatrix}$ (calcul, ou expression de $\overrightarrow{i}$, $\overrightarrow{j}$ et $\overrightarrow{k}$ à l'aide des tris vecteurs.
On calcule ${}^tT.T = \frac{1}{2}.\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 3 \end{pmatrix}$.
La construction assure que c'est la matrice de Gram d'un produit scalaire. Et on vérifie que « être orthogonal à $\overrightarrow{i} + \overrightarrow{j}$, c'est vérifier
$\begin{pmatrix} x & y & z \end{pmatrix} . \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 3 \end{pmatrix} . \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = 0$ soit $x + y - z = 0$!

Existe-t-il un produit scalaire sur $(\mathbb{R}^3, +, .)$ pour lequel l'orthogonal du plan d'équation $x + y - z = 0$ soit $Vect(\overrightarrow{i} + \overrightarrow{k})$?

Le vecteur $\overrightarrow{i} + \overrightarrow{k}$ est dans le plan ; il vérifie l'équation.
Ceci reviendrait alors à imposer que ce vecteur soit orthogonal à lui même...
C'est impossible.

◃ 12 ▹

♡ Montrez que $(\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix})$ forme une base de $(M_2(\mathbb{R}), +, .)$. Est elle orthogonale pour le produit scalaire $(A, B) \longmapsto Tr({}^tA.B)$?
Donnez une matrice orthogonale aux trois premières pour ce produit scalaire.
Construisez un produit scalaire sur $(M_2(\mathbb{R}), +, .)$ pour lequel cette base est orthonormée *(en définissant par exemple le produit scalaire de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$)*. Calculez la norme de la matrice unité.
Existe-t-il S telle que ce produit scalaire soit $(A, B) \longmapsto Tr({}^tA.S.B)$? Donnez une base orthonormée de l'espace vectoriel des matrices de trace nulle. De toutes les matrices T de trace nulle, laquelle est la plus proche de I_2 *(c'est à dire, laquelle minimise $|T - I_2|^2$?)*.

A faire.

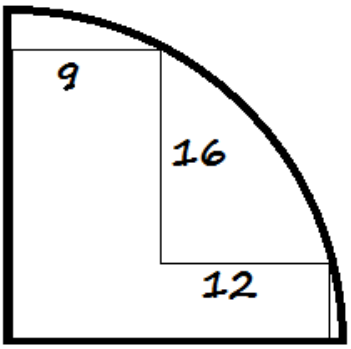
$\diamondsuit_1$ Calculez pour tout N $\sum_{0\leqslant k\leqslant n\leqslant N}\binom{n}{k}.2^k$.

$\diamondsuit_2$ Calculez $\sum_{k=0}^{n}\binom{n}{k}.\binom{n+1}{k}^{-1}$ et $\prod_{k=0}^{n}\binom{n}{k}.\binom{n+1}{k}^{-1}$.

$\diamondsuit_3$ On rappelle la table de la loi de la multiplication dans $(\mathbb{Z}_{/7.\mathbb{Z}},+,\times)$:

	1	2	3	4	5	6
1	1	2		4		
2	2		6			5
3	3	6				
4	4		5			
5		3			4	
6				3		

Complétez. On note M la matrice obtenue (de colonnes C_1 à C_6). Calculez sa trace. Calculez $C_1 - C_3 - C_4 + C_6$. Calculez $\det(M)$.



Retrouvez le rayon du cercle.

La somme $\sum_{0\leqslant k\leqslant n\leqslant N}\binom{n}{k}.2^k$ est une somme multiple qu'on découpe en tranches conditionnelles

$$\sum_{0\leqslant k\leqslant n\leqslant N}\binom{n}{k}.2^k=\sum_{n=0}^{N}\Big(\sum_{k=0}^{n}\binom{n}{k}.2^k\Big)=\sum_{n=0}^{N}(1+2)^n$$

On a ensuite une série géométrique, de somme $\dfrac{3^{N+1}-1}{3-1}$.

On commence par compléter la matrice/le tableau, sachant $14=0$, $12=5$ et autres formules agréables

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	8	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

La trace vaut 14 et si on réduit modulo 7, on trouve 0.
La combinaison $C_1 + C_6 - C_3 - C_4$ donne une colonne nulle (même sans notre modulo 7).
Je l'ai sans calcul (quoique). En ligne i, le coefficient de $C_k$est $i.k$. On calcule donc dans la combinaison $i.(1-3-4+6)$.

A quoi ceci sert il ? A dire

1	2	3	4	5	6
2	4	6	8	3	5
3	6	2	5	1	4
4	1	5	2	6	3
5	3	1	6	4	2
6	5	4	3	2	1

$\times$

1
0
-1
-1
0
1

=

0
0
0
0
0
0

de la forme $M.U = 0_5$.

Si la matrice M était inversible, on multiplierait à gauche par M^{-1} et on aurait $U = M^{-1}.0_5 = 0_5$. C'est donc que M n'est pas inversible. Et son déterminant est nul.

On commence par simplifier

$$\binom{n}{k}.\binom{n+1}{k}^{-1}=\frac{n!}{k!.(n-k)!}.\frac{k!.(n+1-k)!}{(n+1)!}=\frac{(n+1-k)}{n+1}$$

Quand on somme, on peut sortir $\dfrac{1}{n+1}$ et il reste $\sum_{k=0}^{n}(n+1-k)$. On la renverse en $\sum_{i=1}^{n+1} i$. la somme vaut finalement $\dfrac{(n+1).(n+2)}{2}.\dfrac{1}{n+1}$ et on la simplifie en $\dfrac{n+2}{2}$.

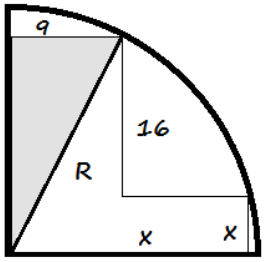
Pour le produit, on a $\dfrac{1}{n+1}$ dans chaque terme du produit. Agissant comme un compteur, il nous reste

$$\prod_{k=0}^{n}\binom{n}{k}.\binom{n+1}{k}^{-1}=\frac{\prod_{k=0}^{n}(n+1-k)}{(n+1)^{n+1}}=\frac{(n+1)!}{(n+1)^{n+1}}$$

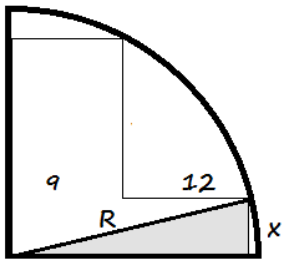
On préfèrera $\dfrac{n!}{(n+1)^n}$. Et on trouvera ça assez satisfaisant.

On va juste appliquer le théorème de Pythagore avec nos données et avec deux notations : R pour le ayon et x pour le côté non mesuré.
On a alors $R^2 = 9^2 + (16+x)^2$ et $R^2 = (9+12)^2 + x^2$.
On compare et on élimine R^2 puis x^2 :
$81 + 256 + 32.x + x^2 = 441 + x^2$ et donc $32.x = 104$.

On est déçu : x n'est même pas entier mais au moins il est rationnel : $x = \frac{14}{4}$ puis R vaut $\frac{85}{4}$.



Pythagore



21

◃13▹ Soit ϕ un produit scalaire sur $(M_2(\mathbb{R}),+,.)$ tel que la famille suivante soit une base orthonormée : $(\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}1&1\\1&0\end{pmatrix})$. Calculez la norme de la matrice unité. Calculez l'angle entre $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ et $\begin{pmatrix}0&1\\0&0\end{pmatrix}$. Existe-t-il S telle que ce produit scalaire soit $(A,B) \longmapsto Tr({}^tA.S.B)$?

Que cette famille soit une base de $(M_2(\mathbb{R}),+,.)$ me semble normal ; elle a le bon cardinal, et elle permet de reconstruire la base canonique [1].
On ne va pas expliciter ϕ plus que ça. On va dire que ϕexiste.
Et on écrit alors $\begin{pmatrix}1&0\\0&1\end{pmatrix} = -\frac{1}{3}.\begin{pmatrix}0&1\\1&1\end{pmatrix} + \frac{2}{3}.\begin{pmatrix}1&0\\1&1\end{pmatrix} + \frac{2}{3}.\begin{pmatrix}1&1\\0&1\end{pmatrix} - \frac{1}{3}.\begin{pmatrix}1&1\\1&0\end{pmatrix}$ (système ou tâtonnements).
Le « vecteur » I_2 a pour composantes $\left(\frac{-1}{3},\frac{2}{3},\frac{2}{3},\frac{-1}{3}\right)$ sur une base orthonormée, sa norme vaut $\sqrt{\frac{1}{9}+\frac{4}{9}+\frac{4}{9}+\frac{1}{9}}$. Ce qui fait $\frac{\sqrt{10}}{3}$.
Pourquoi pas...

On décompose aussi $\begin{pmatrix}1&0\\0&0\end{pmatrix} = -\frac{2}{3}.\begin{pmatrix}0&1\\1&1\end{pmatrix} + \frac{1}{3}.\begin{pmatrix}1&0\\1&1\end{pmatrix} + \frac{1}{3}.\begin{pmatrix}1&1\\0&1\end{pmatrix} + \frac{1}{3}.\begin{pmatrix}1&1\\1&0\end{pmatrix}$
$\begin{pmatrix}0&1\\0&0\end{pmatrix} = \frac{1}{3}.\begin{pmatrix}0&1\\1&1\end{pmatrix} - \frac{2}{3}.\begin{pmatrix}1&0\\1&1\end{pmatrix} + \frac{1}{3}.\begin{pmatrix}1&1\\0&1\end{pmatrix} + \frac{1}{3}.\begin{pmatrix}1&1\\1&0\end{pmatrix}$
Si on calcule le *prϕduit* scalaire des deux vecteurs, les termes en $\phi(\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}1&0\\1&1\end{pmatrix})$ s'en vont, d'autres (une matrice contre elle même) valent 1.
On a donc $\phi(\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix}) = \frac{-2}{3}.\frac{1}{3} + \frac{-2}{3}.\frac{1}{3} + \frac{1}{3}.\frac{1}{3} + \frac{1}{3}.\frac{1}{3} = \frac{-2}{9}$.
On a aussi $\phi(\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix}) = \frac{4}{9}+\frac{1}{9}+\frac{1}{9}+\frac{1}{9} = \frac{7}{9}$ pareil pour l'autre.
On effectue $\frac{\frac{-2}{8}}{\frac{\sqrt{7}}{3}.\frac{\sqrt{7}}{3}}$. Et si vous aimez $Arccos\left(\frac{-2}{7}\right)$ dites le moi.

◃14▹ ♡ Montrez que $(A,B) \longmapsto Tr({}^tA.B)$ est un produit scalaire sur $(M_3(\mathbb{R}),+,.)$. Calculez la norme de $\frac{1}{3}.\begin{pmatrix}2&-1&-2\\2&2&1\\1&-2&2\end{pmatrix}$ *(notée R)*. Donnez une matrice non nulle orthogonale à R.

La première question est une question de cours.
Forme : formats compatibles.
Symétrique : $Tr({}^tA.B) = Tr({}^t({}^tA.B)) = Tr({}^tB.A)$.
Bilinéaire : $Tr({}^tA.(\beta.B+\gamma.C)) = \beta.Tr({}^tA.B) + \gamma.Tr({}^tA.C)$.
Positive : $Tr({}^tA.A) = \sum_{i,j}(a_i^j)^2$.
Défini positive : $(\sum_{i,j}(a_i^j)^2 = 0) \Rightarrow (\forall i,\forall j,\ a_i^j = 0$.

Pour la norme, on calcule le produit $\begin{pmatrix}2&2&1\\-1&2&-2\\-2&1&2\end{pmatrix}.\begin{pmatrix}2&-1&-2\\2&2&1\\1&-2&2\end{pmatrix} = \begin{pmatrix}9&0&0\\0&9&0\\0&0&9\end{pmatrix}$ (seuls les termes diagonaux nous intéressent).

1. additionnez les toutes, divisez par 3, vous avez $\begin{pmatrix}1&1\\1&1\end{pmatrix}$, et ensuite, soustrayez une à une les matrices de la famille

Il y a un $\frac{1}{3}$ dans R et un dans ${}^tR$: ${}^tR.R = I_3$.
On a donc $||R|| = \sqrt{3}$

On veut une matrice vérifiant $Tr({}^tA.R) = 0$.
Inutile de poser des coefficients partout. On met plein de 0. Quand même pas 9, mais pas loin :
$\begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} . \begin{pmatrix} 2 & -1 & -2 \\ 2 & 2 & 1 \\ 1 & -2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & ? & ? \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ .La trace est nulle. la transposée de la matrice écrite est « orthogonale à R ».

Montrez que $M \longmapsto R.M$ et $M \longmapsto M.R$ sont deux isomorphismes de $(M_3(\mathbb{R}), +, .)$ qui préservent les normes.

Existence de l'application (et endo) : formats compatibles.
Linéarité : distributivité de la multiplication matricielle.
Bijectivité : on connait l'application réciproque : $N \longmapsto R^{-1}.N$ pour la première et $N \longmapsto N.R^{-1}$ pour la seconde.

On doit ensuite comparer la norme de M ($\sqrt{Tr({}^tM.M)}$) et celle de son image.
On calcule donc $\sqrt{Tr({}^t(R.M).(R.M)} = \sqrt{Tr({}^tM..{}^tR.R.M} = \sqrt{Tr({}^tM.M)}$ car ${}^tR.R = I_3$.

De même $\sqrt{Tr({}^t(M.R).(M.R)} = \sqrt{Tr({}^tR..{}^tM.M.R} = \sqrt{Tr(R.{}^tR..{}^tM.M} = \sqrt{Tr({}^tM.M)}$ en utilisant aussi cette fois $Tr(P.Q) = Tr(Q.P)$.

◁ 15 ▷ ♡ Construisez un produit scalaire sur $(\mathbb{R}^2, +, .)$ tel que la base $(\overrightarrow{i} + \overrightarrow{j},\ \overrightarrow{i} - 2.\overrightarrow{j})$ soit orthonormée (calculez par exemple $|\overrightarrow{i}|$, $|\overrightarrow{j}|$ et le produit scalaire de $\overrightarrow{i}$ et $\overrightarrow{j}$).

La chose semble cohérente, $(\overrightarrow{i} + \overrightarrow{j},\ \overrightarrow{i} - 2.\overrightarrow{j})$ est une base.
On a d'ailleurs les formules de changement de base : $x.\overrightarrow{i} + y.\overrightarrow{j} = \frac{2.x+1}{3}.(\overrightarrow{i} + \overrightarrow{j}) + \frac{x-y}{3}.(\overrightarrow{i} - 2.\overrightarrow{j})$ (petit système ou inversion sans se prendre la tête de $\begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix}$).
On va nommer $\overrightarrow{e_1}$ et $\overrightarrow{e_2}$ nos deux nouveaux vecteurs de base.

On calcule alors pour deux vecteurs
$\phi(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix}) = \phi\Big(\frac{2.x+1}{3}.\overrightarrow{e_1} + \frac{x-y}{3}.\overrightarrow{e_2},\ \frac{2.x+1}{3}.\overrightarrow{e_1} + \frac{x-y}{3}.\overrightarrow{e_2}\Big)$.On développe par multilinéarité.
Les deux termes $\phi(\overrightarrow{e_1}, \overrightarrow{e_1})$ et $\phi(\overrightarrow{e_2}, \overrightarrow{e_2})$ valent 1.
Les deux termes $\phi(\overrightarrow{e_1}, \overrightarrow{e_2})$ et $\phi(\overrightarrow{e_2}, \overrightarrow{e_1})$ sont nuls.
Il reste $\phi(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix}) = \frac{(2.x+y).(2.x'+y')}{9} + \frac{(x-y).(x'-y')}{9}$
On simplifie au maximum : $\phi(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix}) = \frac{5.x^2 + 2.y^2 + (x'.y + x.y')}{9} = \frac{1}{9}.\begin{pmatrix} x & y \end{pmatrix} . \begin{pmatrix} 5 & 1 \\ 1 & 2 \end{pmatrix} . \begin{pmatrix} x' \\ y' \end{pmatrix}$

On a construit une matrice symétrique, c'est bien parti. Et ses valeurs propres sont positives.

On vérifie $\frac{1}{9}.\begin{pmatrix} 1 & 1 \end{pmatrix} . \begin{pmatrix} 5 & 1 \\ 1 & 2 \end{pmatrix} . \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1$ | $\frac{1}{9}.\begin{pmatrix} 1 & 1 \end{pmatrix} . \begin{pmatrix} 5 & 1 \\ 1 & 2 \end{pmatrix} . \begin{pmatrix} 1 \\ -2 \end{pmatrix} = 0$ | $\frac{1}{9}.\begin{pmatrix} 1 & -2 \end{pmatrix} . \begin{pmatrix} 5 & 1 \\ 1 & 2 \end{pmatrix} . \begin{pmatrix} 1 \\ -2 \end{pmatrix} = 1$

On pouvait aussi partir de $\phi(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix}) = \begin{pmatrix} x & y \end{pmatrix} . \begin{pmatrix} a & b \\ b & c \end{pmatrix} . \begin{pmatrix} x' \\ y' \end{pmatrix}$
et imposer $\frac{1}{9}.\begin{pmatrix} 1 & 1 \end{pmatrix} . \begin{pmatrix} a & b \\ b & c \end{pmatrix} . \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1$ | $\frac{1}{9}.\begin{pmatrix} 1 & 1 \end{pmatrix} . \begin{pmatrix} a & b \\ b & c \end{pmatrix} . \begin{pmatrix} 1 \\ -2 \end{pmatrix} = 0$ | $\frac{1}{9}.\begin{pmatrix} 1 & -2 \end{pmatrix} . \begin{pmatrix} a & b \\ b & c \end{pmatrix} . \begin{pmatrix} 1 \\ -2 \end{pmatrix} = 1$
Trois équations, trois inconnues, c'est bon, surtout que le déterminant 3 sur 3 est non nul...

◁ 16 ▷ Montrez que $(P,\ Q) \longmapsto \sum_{k=0}^{n} P^{(k)}(0).Q^{(k)}(0)$ est un produit scalaire sur $(\mathbb{R}_n[X], +, .)$. Donnez une base orthonormée.

Forme	La somme est un réel.
Symétrique	La multiplication est commutative dans $\mathbb{R}$.
(Bi)linéaire	La dérivation est linéaire $\sum_{k=0}^{n} P^{(k)}(0).(\alpha.Q+\beta.R)^{(k)}(0) = \alpha.\sum_{k=0}^{n} P^{(k)}(0).Q^{(k)}(0) + \beta.\sum_{k=0}^{n} P^{(k)}(0).R^{(k)}(0)$
Positive	Quand on calcule $\sum_{k=0}^{n} P^{(k)}(0).P^{(k)}(0)$ on a une somme de carrés de réels.
Défini p.	On prend P, on suppose que cette somme est nulle. C'est forcément que chaque terme est nul. Chaque $P^{(k)}(0)$ pour k de 0 à n est nul. Et alors ? Mais si on écrit $P(X)=\sum_{i=0}^{n} a_i.X^i$, on trouve $P^{(k)}(0)=k!.a_k$. C'est donc que chaque a_k est nul. Et P est le polynôme nul. Question : qui s'est arrêté fièrement à « tous les $P^{(k)}(0)$ sont nuls, alors que le but est bel et bien « P est nul ». D'autre part, vous voyez le rapport entre $P^{(k)}(0)=k!.a_k$ et la formule de Taylor ?

Si on regarde les polynômes 1, X, X^2 jusqu'à X^n, ils sont deux à deux orthogonaux pour ce produit scalaire.
En effet, quand on met X^i face à X^j, leurs dérivées en 0 sont toutes nulles, sauf la i^{emme} pour l'un et la j^{ieme} pour l'autre. mais ces deux termes ne seront pas e »en vis à vis » dans la somme de 0 à n.

Mais ces vecteurs ne sont pas normés. C'est $\frac{X^i}{\sqrt{i!}}$qu'il faut prendre. [2].

$(P,\ Q) \longmapsto \sum_{k=0}^{3} P^{(k)}(k).Q^{(k)}(k)$ est il un produit scalaire sur $(\mathbb{R}_3[X],+,.)$?

Le lot de propriétés élémentaires passe bien.
Tout ce qui pose problème est « défini positif ».

On prend P et on suppose $\sum_{k=0}^{3}(P^{(k)}(k))^2=0$. Il faut aboutir à $P=0$.

Déjà, la somme de carrés de réelles nulle donne que chacun des quatre $P^{(k)}(k)$ est nul.
On écrit $P(X)=a+b.X+c.X^2+d.X^3$.
La condition $P^{(3)}(3)=0$ donne $6.d=0$. P s'écrit $P(X)=a+b.X+c.X^2$
On reporte dans $P^{(2)}(2)=0$ donne $c=0$.On continue, et finalement, P est nul (système triangulaire).

◁ 17 ▷

Vérifiez que ces formes bilinéaires symétriques sont des produits scalaires
et dites moi si la dérivation est un produit scalaire pour celles sur $Vect(\sin,\cos)$:

$(a.\cos+b.\sin,\ \alpha.\cos+\beta.\sin)$	$a.\alpha+b.\beta$
$(a.\cos+b.\sin,\ \alpha.\cos+\beta.\sin)$	$a.\alpha+2.b.\beta$
$(a.\cos+b.\sin,\ \alpha.\cos+\beta.\sin)$	$a.\alpha++a.\beta+b.\alpha+3.b.\beta$
$(f,\ g)$	$f(0).g(0)+f'(0).g'(0)$
$(f,\ g)$	$\int_0^{2.\pi} f(t).g(t).dt$

$Vect(\sin,\cos)$ est l'espace des applications de la forme $t \longmapsto a.\cos(t)+b.\sin(t)$.

Toutes ces formes existent (pour l'une, il faut évoquer la continuité).
Elles sont symétriques (commutativités...).
Elles sont linéaires par rapport à la première fonction, puis bilinéaires.

On teste ensuite une fonction $a.\cos+b.\sin$contre elle même :

a^2+b^2	positif
$a^2+2.b^2$	positif
$a^2+2.a.b+3.b^2$	$(a+b)^2+2.b^2$ positif
$(f(0))^2+(f'(0))^2$	positif
$\int_0^{2.\pi}(f(t))^2.dt$	positif

mot clef : carrés de réels »

2. je me dis qu'appeler i la variable de sommation va peut être vous induire en erreur ; quand certains croisent i! ils voient la factorielle de la racine de -1

On suppose cette quantité nulle.
Les trois premières donnent $a = b = 0$, la fonction est nulle.
La quatrième donne $f(0) = f'(0) = 0$. Et en écrivant $a.\cos + b.\sin$ on a encore $a = b = 0$.
La dernière est un classique, f par continuité est nulle sur $[0,\ 2.\pi]$ puis nulle partout car périodique (combinaison de sinus et cosinus).

Nos formes sont toutes les produits scalaires.

La dérivation est un endomorphisme de $Vect(\sin,\ \cos)$, puisqu'elle est linéaire et transforme $a.\sin + b.\cos$ en $-b.\sin + a.\cos$.

Reste à voir si les produits scalaires sont préservés.
A-t-on $\phi(f,\ g) = \phi(f',\ g')$.
Par bilinéarité, on n'a as besoin de le vérifier pour toutes les applications, il suffit de le vérifier pour une base : $\phi(\cos,\cos) = \phi(-\sin,-\sin)$, $\phi(\sin,\sin) = \phi(\cos,\cos)$, $\phi(\cos,\sin) = \phi(-\sin,\cos)$.

Les deux premières donnent deux fois la même chose, et la dernière impose $\phi(\cos,\sin) = 0$.On regarde alors :

	$\phi(\cos,\cos) = \phi(\sin,\sin)$	$\phi(\cos,\sin) = 0$	
$a.\alpha + b.\beta$	oui	oui	☺
$a.\alpha + 2.b.\beta$	non	oui	
$a.\alpha + +a.\beta + b.\alpha + 3.b.\beta$	non	non	
$f(0).g(0) + f'(0).g'(0)$	oui	oui	☺
$\int_0^{2.\pi} f(t).g(t).dt$	oui	oui	☺

Attention : Trois lignes☺ donnent la même réponse : la dérivation est une isométrie.
Mais en fait, c'est le même produit scalaire trois fois (à un facteur π près), sur l'espace $Vect(\sin,\ \cos)$.
Faites le calcul...

◁ 18 ▷

On va faire de l'arithmétique *(diviseurs, p.g.c.d., Euclide)* sur un ensemble plus gros que $\mathbb{Z}$, contenant $\sqrt{2}$.

I∼0) On commence par redémontrer que $\sqrt{2}$ est irrationnel, mais en évitant le raisonnement que tout le monde fait[a].
On pose $A = \{n \in \mathbb{N}^* \mid n.\sqrt{2} \in \mathbb{N}\}$. Montrez : $\forall n \in A,\ n.\sqrt{2} - n \in A$. Concluez que A est vide. Concluez pour $\sqrt{2}$.

a. le site CutTheJKnot a référencé trente preuves, pourquoi tout le monde donne la même et fait semblant de croire qu'il faut retenir la même pour tous et pas une autre...

On suppose *(peut être à tort)* que n est dans A.
On regarde alors $\sqrt{2}.n - n$. Comme n est dans A, c'est la différence de deux entiers. C'est un entier.
Il est non nul, puisque $\sqrt{2}$ ne vaut pas 1 et n est non nul.
On le multiplie par $\sqrt{2}$: $\sqrt{2}.(\sqrt{2}.n - n) = 2.n - \sqrt{2}.n$. C'est encore la différence de deux entiers, c'est un entier.
On a bien tout pour dire : $\sqrt{2}.n - n$ est dans A.

Mais ce nouvel entier est strictement plus petit que n *(c'est* $(\sqrt{2}-1).n$ *avec* $\sqrt{2}-1$ *plus petit que* 1*)*.

On est parti pour avoir dans A une suite strictement décroissante d'entiers naturels. C'est étrange.

Plus simplement, on arrive à : « A est vide ».
S'il ne l'était pas, on noterait a son plus petit élément *(toute partie de* $\mathbb{N}$ *non vide admet un plus petit élément)*. Et $\sqrt{2}.a - a$ serait encore dans A, ce qui contredirait la « minimalité » de a.

Il n'existe pas d'entier non nul n vérifiant $n.\sqrt{2} \in \mathbb{N}$.
Il n'existe pas de couple d'entiers non nuls $(n,\ m)$ vérifiant $n.\sqrt{2} = m$.
Il n'existe pas de couple d'entiers non nuls $(n,\ m)$ vérifiant $\frac{m}{n} = \sqrt{2}$. C'est bon, $\sqrt{2} \notin \mathbb{Q}$.

Déduisez que si un réel x s'écrit $a + b.\sqrt{2}$ avec a et b entiers, alors a et b sont uniques.

C'est l'irrationalité de $\sqrt{2}$ qui sert ensuite à garantir l'unicité d'écriture des éléments de E qui sert mine de rien

dans la suite.

Vous n'avez peut être pas conscience qu'on en a besoin pour dire « on prend $x = a + b.\sqrt{2}$ on pose $(\!|x|\!) = |a^2 - 2.b^2|$ ».
Il faut en effet qu'on sache pour x donné qui sont a et b. Si un élément pouvait avoir plusieurs écritures $x = a + b.\sqrt{2} = a' + b'.\sqrt{2}$, que poserait on ? $(\!|x|\!) = |a^2 - 2.b^2|$ ou $(\!|x|\!) = |a'^2 - 2.b'^2|$?
Je ne vous en veux pas de n'avoir pas vu cette subtilité.

On prend donc deux écritures d'un élément de E : $x = a + b.\sqrt{2} = a' + b'.\sqrt{2}$. On fait passer de l'autre côté : $(a - a') = \sqrt{2}.(b' - b)$.
Si $b' - b$ est non nul, par quotient, $\sqrt{2}$ est rationnel.
Forcément $b' - b$ est nul, et en reportant $a' - a$ aussi.
On a bien obtenu $a = a'$ et $b = b'$.

On pose $E = \mathbb{Z} + \sqrt{2}.\mathbb{Z} = \{a + b.\sqrt{2} \mid (a,\ b) \in \mathbb{Z}^2\}$, $\alpha_n = (\sqrt{2}+1)^n$ et $\beta_n = (\sqrt{2}-1)^n$ pour tout n de $\mathbb{N}$.
Montrez la suite d'inégalités pour les éléments suivants de E :
$0 < 17 - 12.\sqrt{2} < 53 - 37.\sqrt{2} < -19 + 14.\sqrt{2} < 97 - 68.\sqrt{2} < 8 - 5.\sqrt{2} < 42 - 29.\sqrt{2} < 1$ [a]

a. Au fait, on est en maths. Il est donc hors de question que votre preuve passe par $\sqrt{2} \simeq 1,4142135623...$ (mnémotechnique : J'AIME L'ŒIL DE L'AMI NICOLAS, GARÇON DE SUP). S'il vous plait : aucun symbole $\simeq$, de l'intelligence...

Pour le tri, on va montrer par exemple $97 - 68.\sqrt{2} < 8 - 5.\sqrt{2}$ en étudiant la différence $-89 + 63.\sqrt{3}$ et en prouvant $63.\sqrt{2} > 89$ en élevant au carré : $63^2.2 = 7938 > 7921 = 89^2$. Oui, tout se ramène à des calculs dans $\mathbb{N}$.

$0 < 17 - 12.\sqrt{2}$	$< 53 - 37.\sqrt{2}$	$< -19 + 14.\sqrt{2}$	$< 97 - 68.\sqrt{2}$	$< 8 - 5.\sqrt{2}$	$< 42 - 29.\sqrt{2}$	< 1
$12.\sqrt{2} < 17$	$25.\sqrt{2} < 36$	$72 < 51.\sqrt{2}$	$82.\sqrt{2} < 116$	$89 < 63.\sqrt{2}$	$24.\sqrt{2} < 34$	$41 < 29.\sqrt{2}$
$17^2 = 289$	$36^2 = 1296$	$51^2.2 = 5202$	$116^2 = 13456$	$63^2.2 = 7938$	$34^2 = 1156$	$29^2.2 = 1682$
$12^2.2 = 288$	$25^2.2 = 1250$	$72^2 = 5184$	$82^2.2 = 13448$	$89^2 = 1921$	$24^2.2 = 1152$	$41^2 = 1681$

Ah qu'il est agréable de savoir faire des calculs sans se ridiculiser à appuyer sur des touches.

D'accord, il y a des calculatrices.
De même qu'il y a des taxis pour traverser le bois de Vincennes, alors pourquoi tant de gens font le tour du Bois de Vincennes en courant ? Pour le plaisir de l'effort physique. Avec la récompense du muscle qui dit merci.

I∼0) Montrez l'existence de deux suites d'entiers naturels (r_n) et (i_n) vérifiant $\alpha_n = r_n + \sqrt{2}.i_n$ pour tout n.
Exprimez r_{n+1} et i_{n+1} à l'aide de r_n et i_n et exprimez β_n à l'aide de r_n et i_n.

On va aborder la question par l'astuce de l'algèbre. En montrant qu'on a une structure stable, ce qui permettra ensuite de mettre en boucle cette stabilité pour tout avoir directement.

Donc, le point de départ : $\boxed{(E, +) \text{ est un groupe commutatif.}}$

On a la stabilité en écrivant des $(a + b.\sqrt{2}) + (c + d.\sqrt{2}) = (a + c) + (b + d).\sqrt{2}$ avec a, b, c et d entiers et aussi $a + c$ et $b + d$.
Pour le neutre, la question est : 0 est il dans E ? Oui : $0 = 0 + 0.\sqrt{2}$.

Si vous affirmez juste « 0 est le neutre », vous n'avez pas répondu à la question.

Pour l'opposé, il faut dire non seulement « c'est $-a - b.\sqrt{2}$ », mais surtout « et il est dans E ».

Si vous écrivez juste des formules et ne vérifiez pas où l'élément est, vous faites de la chimie, pas des maths.

Et l'associativité est acquise sans emplir la page de formules, puisque c'est l'addition dans $\mathbb{R}$!

Mille et mille fois, je vous le redis : je me fiche de savoir si vous savez tartiner des formules sur des pages. Je dois surveiller si vous savez raisonner. Et ça, ça demande un cerveau !

Allons plus loin : $\boxed{(E, +, .) \text{ est un anneau.}}$
On montre la stabilité par multiplication : $(a + b.\sqrt{2}).(c + d.\sqrt{2}) = (a.c + 2.b.d) + (a.d + b.c).\sqrt{2}$.

Ensuite, la multiplication est associative, et distributive sur l'addition, on est dans $\mathbb{R}$!

> *Qui a perdu à la fois son temps et sa crédibilité auprès de moi en développant $(a+b.\sqrt{2}).(c+d.\sqrt{2}).(e+f.\sqrt{2})$ sur trois ou quatre lignes ? Bref, qui a le nez collé dans le guidon au lieu de regarder la route ?*

On a un anneau. Commutatif évidemment. Avec un neutre : $1 = 1 + 0.\sqrt{2}$.

Reprenons : $(E, +, .)$ est un anneau.
Les deux éléments $1+\sqrt{2}$ et $\sqrt{2}-1$ sont dans E. Par produits successifs, chaque $(1+\sqrt{2})^n$ et $(\sqrt{2}-1)^n$ est dans E *(récurrence évidente)*.
C'est tout.

Mais on peut aussi développer $(1+\sqrt{2})^n$ par la formule du binôme et séparer les termes en fonction de leur parité :

$$(1+\sqrt{2})^n = \sum_{k=0}^{n} \binom{n}{k}.1^{n-k}.\sqrt{2}^k = \quad {\scriptstyle k=2.p} \quad \sum_{p=0}^{[n/2]} \binom{n}{2.p}.2^p \quad \text{c'est } r_n$$

$$ {\scriptstyle k=2.p+1} \quad +\Big(\sum_{p=0}^{[(n-1)/2]} \binom{n}{2.p+1}.2^p\Big).\sqrt{2} \quad \text{et } i_n$$

On a séparé sous la forme $r_n + \sqrt{2}.i_n$.

Si on développe cette fois $(\sqrt{2}-1)^n$ on a

$$(\sqrt{2}-1)^n = \sum_{k=0}^{n} \binom{n}{k}.(-1)^{n-k}.\sqrt{2}^k \quad {\scriptstyle k=2.p} \quad = \sum_{p=0}^{[n/2]} (-1)^{n-2.p} \binom{n}{2.p}.2^p \quad \text{c'est } (-1)^n.r_n$$

$$ {\scriptstyle k=2.p+1} \quad +\Big(\sum_{p=0}^{[(n-1)/2]} \binom{n}{2.p+1}.(-1)^{n-2.p-1}2^p\Big).\sqrt{2} \quad \text{et } (-1)^{n+1}.i_n$$

C'est gagné aussi pour β_n et on a $\boxed{\beta_n = (-1)^n.(r_n - \sqrt{2}.i_n)}$ pour tout n.

Mais on peut aussi se lancer dans une récurrence.

> *Oui, c'est en variant les points de vue qu'on avance en maths. Il n'y a pas un chemin et une méthode à appliquer à chaque fois. Pas de recette systématique à appliquer comme un automate. Au contraire, il faut apprendre à « penser de travers », « pas comme les autres », « pas comme la fois précédente ». Pour certains c'est la grande difficulté des maths. Pour d'autres, c'est leur grande richesse. Si vous mangez toujours les mêmes saveurs, c'est fade. Alors que c'est si génial de manger un plat épicé le lundi, une soupe le mardi, du sucré-salé le mercredi, de l'aigre doux le jeudi, un poisson le vendredi, un falafel à shabbat et de jeûner un peu le dimanche.*

On initialise

α_n	1	$1+\sqrt{2}$	$3+2.\sqrt{2}$	$7+5.\sqrt{2}$
r_n	1	1	3	7
i_n	0	1	2	5

Prenons un entier naturel n et supposons qu'il existe r_n et i_n vérifiant $\alpha_n = r_n. + i_n.\sqrt{2}$. L'objectif est de prouver l'existence de r_n et i_n.
On multiplie : $\alpha_{n+1} = \alpha_n.(1+\sqrt{2}) = (r_n + i_n.\sqrt{2}).(1+\sqrt{2}) = (r_n + 2.i_n) + (r_n + i_n)$.
On pose alors : $\boxed{r_{n+1} = r_n + 2.i_n \text{ et } i_{n+1} = r_n + i_n}$
On constate qu'ils existent et que ce sont deux entiers. La récurrence s'achève.

> *Attention. la récurrence prouve l'existence des deux suites. Et la formule $r_{n+1} = r_n + 2.i_n$ et $i_{n+1} = r_n + i_n$ est donnée dans la récurrence. Mais ce n'est pas elle que l'on prouve par récurrence. Elle est morceau de la récurrence et sert à d'autres récurrences après. Ne mélangez pas tout, et cessez de ne vouloir que prouver des formules.*

∼0) Complétez d'ailleurs $\begin{pmatrix} r_n \\ i_n \end{pmatrix} = \begin{pmatrix} ◐ & ◑ \\ ◖ & ◗ \end{pmatrix} . \begin{pmatrix} r_{n+1} \\ i_{n+1} \end{pmatrix}$ *(oui, je l'ai posé dans le mauvais sens)*.

On écrit $\begin{pmatrix} r_{n+1} \\ i_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} . \begin{pmatrix} r_n \\ i_n \end{pmatrix}$ et $\boxed{\begin{pmatrix} r_{n+1} \\ i_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} . \begin{pmatrix} r_n \\ i_n \end{pmatrix}}$ en inversant la matrice ou en

résolvant un système *(c'est la même chose !)*.
On note qu'on a alors $\begin{pmatrix} r_n \\ i_n \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^n . \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ avec le mot « suite géométrique de raison matricielle ».

∼0) Montrez que r_n et i_n sont toujours premiers entre eux.

Pour prouver que r_n et $i_n$sont premiers entre eux, le bon réflexe en sortant de Terminale est de faire une récurrence.
On montre que c'est vrai pour les premiers *(par exemple* 1 *et* 0 *ou même* 1 *et* 1*)*.
Ensuite, on se donne un entier n et on suppose que $r_n$et $i_n$sont premiers entre eux.
On cherche qui sont alors les entiers qui divisent r_{n+1} et i_{n+1} *(objectif : il n'y a que* 1*)*.
Soit d qui divise à la fois r_{n+1} et i_{n+1}. Il divise alors leur différence : d divise $r_{n+1} - i_{n+1} = i_n$. Mais si d divise i_{n+1} et i_n, il divise leur différence r_n. A présent, d divise $r_n$et i_n. Par hypothèse de récurrence, le seul d possible est 1.
r_{n+1} et i_{n+1} ont peur seul diviseur commun 1, ils sont premiers entre eux.
Le résultat est initialisé et héréditaire, il est vrai pour tout n.

Mais en fait, il y a plus simple : $\alpha_n.\beta_n = (1+\sqrt{2})^n.(\sqrt{2}-1)^n = \left((1+\sqrt{2}).(\sqrt{2}-1)\right)^n = 1^n = 1$.
Or, $\alpha_n = r_n + \sqrt{2}.i_n$ et $\beta_n = (-1)^n.(r_n - \sqrt{2}.i_n)$. On a donc $\alpha_n.\beta_n = (r_n)^2 - 2.(i_n)^2$.
On écrit tout ceci $\boxed{r_n.r_n - 2.i_n.i_n = \pm 1}$ et on a une identité de Bézout entre r_n et i_n. Ils sont premiers entre eux.

C'est là que les maths sont plus esthétiques que calculatoires.
Pour certains, c'est flippant.
Pour d'autres, c'est enthousiasmant.

On peut aussi prouver : $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^n = \begin{pmatrix} r_n & 2.i_n \\ i_n & r_n \end{pmatrix}$ par récurrence sur n, passer au déterminant : $(-1)^n = (r_n)^2 - 2.(i_n)^2$. On a encore une identité de Bézout *(la même)*.

∼0) Écrivez un script `Python` qui prend en entrée `n` et retourne les deux entiers r_n et i_n [a].

```
def Fonction(n) :
.....
....return(rn, in)
```

a. quand on dit prend un entrée `n` et retourne `rn` et `in`, on attend et pas des trucs avec des `n = int(input('Donnez l'entier n : '))` jusqu'à `print(rn, in)` qui est juste du dialogue gentillet avec l'ordinateur et pas de la programmation

Pour la procédure `Python`, on a faire une boucle, avec des valeurs qu'on modifie au fur et à mesure, et qu'on appelle justement r et i.
C'est facile la programmation. Il suffit d'écrire ce que l'on ferait à la main. Sans aller imaginer des trucs dans tous les sens.

```
def DS2(n) :
....r, i = 1, 0
....for k in range(n) :
........r, i = r+2*i, r+i
....return(r, i)
```

∼0) Que pensez vous de l'idée de l'élève Regercées-Iféfroi : on identifie $a + b.\sqrt{2}$ à la matrice $\begin{pmatrix} a & 2.b \\ b & a \end{pmatrix}$, et on regarde addition, multiplication, division.

Profitons tout de suite de la belle idée :

$(a+b.\sqrt{2}) + (c+d.\sqrt{2}) = (a+c) + (b+c).\sqrt{2}$	$\begin{pmatrix} a & 2.b \\ b & a \end{pmatrix} + \begin{pmatrix} c & 2.d \\ d & c \end{pmatrix} = \begin{pmatrix} (a+c) & 2.(b+d) \\ (b+d) & (a+c) \end{pmatrix}$
$(a+b.\sqrt{2}).(c+d.\sqrt{2}) = (a.c+2.b.d) + (a.d+b.c).\sqrt{2}$	$\begin{pmatrix} a & 2.b \\ b & a \end{pmatrix} . \begin{pmatrix} c & 2.d \\ d & c \end{pmatrix} = \begin{pmatrix} (a.c+2.b.d) & 2.(b+d) \\ (b.c+a.d) & (a+c) \end{pmatrix}$
$0 = 0 + 0.\sqrt{2}$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ est neutre additif
$1 = 1 + 0.\sqrt{2}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est neutre multiplicatif
$a + b.\sqrt{2}$ a pour module $a^2 - 2.b^2$	$\begin{pmatrix} a & 2.b \\ b & a \end{pmatrix}$ a pour déterminant $a^2 - 2.b^2$

La dernière avec la deuxième permet de passer de « le déterminant du produit des matrices est le produit des déterminants » (oui : $\det(A.B) = \det(A).\det(B)$)
à « le module du produit est le produit des modules ».

I∼0) Pour tout élément $a + b.\sqrt{2}$ de E, on définit son module $\Vert x \Vert = |a^2 - 2.b^2|$. Montrez que le module d'un élément de E est toujours un entier. Combien d'éléments de E ont un module nul ?
I∼1) Montrez que $(E, +, .)$ est un anneau dans lequel le module du produit est le produit des modules.

S'il s'agit de démontrer que $(E, +.)$ est un anneau, c'est fait plus haut. Mais il reste à prouver que le module d'un élément de E est toujours un entier naturel. C'est évident.

Et il reste à prouver que le module du produit est le produit des modules. Une question gentille et juste calculatoire.
On se donne a, b, c et d.
On doit comparer $|a^2 - 2.b^2|.|c^2 - 2.d^2|$ et $|(a.c + 2.b.d)^2 - 2.(a.d + b.c)^2|$.
Les deux valent $|a^2.c^2 - 2.a^2.d^2 - 2.b^2.c^2 + 4.b^2.d^2|$, et les $4.a.b.c.d$ se sont simplifiés.
. *On l'obtient facilement avec les déterminants...*

Est il possible que le module soit nul ? Il faut avoir, avec les notations déjà prises : $a^2 - 2.b^2 = 0$.
Mais si b est non nul, ceci revient à avoir $\sqrt{2}$ rationnel égal à $\frac{b}{a}$ (au signe près).
La seule solution est donc $a = b = 0$.

Le seul élément de module nul est 0.

∼0) Montrez que chaque α_n et chaque β_n est dans E et a pour module 1 *(pensez à calculer $\alpha_n.\beta_n$)*.

Le module de α_n est $(r_n)^2 - 2.(i_n)^2$ ce qui ne semble pas très pratique.
Calculons néanmoins : $\alpha_n.\beta_n = (1 + \sqrt{2})^n.(\sqrt{2} - 1)^n = \Big((\sqrt{2} + 1).(\sqrt{2} - 1)\Big)^n = 1^n = 1$.
On passe aux modules : $\Vert \alpha_n.\beta_n \Vert = 1$. Et par propriété $\Vert \alpha_n \Vert . \Vert \beta_n \Vert = 1$.
Comme les deux nombres sont des entiers naturels, on a forcément $\Vert \alpha_n \Vert = 1$ et $\Vert \beta_n \Vert = 1$.

I∼0) Soient u et v deux réels distincts *($u < v$)* ; montrez que $p.\beta_n$ est dans E et est entre u et v pour $n = \left[\frac{\ln(v-u)}{\ln(\sqrt{2}-1)}\right] + 1$ et $p = \left[\frac{u}{\beta_n}\right] + 1$ *(on commencera par montrer : $0 \leqslant \beta_n \leqslant v - u$)*.

On va montrer que tout intervalle non réduit à un point contient une infinité d'éléments de E.

On se donne donc u et v avec $u < v$.
On définit $n = \left[\frac{\ln(v-u)}{\ln(\sqrt{2}-1)}\right] + 1$. Par construction de « partie entière plus 1 », on a $n \geqslant \frac{\ln(v-u)}{\ln(\sqrt{2}-1)}$ et donc par produit en croix : $n.\ln(\sqrt{2} - 1) \leqslant \ln(v - u)$.

> *Non, je ne me suis pas trompé sur le sens ! En effet, $\ln(\sqrt{2} - 1)$ est négatif, en tant que logarithme d'un réel de $]0,\ 1[$. On croisera souvent cette histoire.*

On passe à l'exponentielle, croissante : $(\sqrt{2} - 1)^n \leqslant (v - u)$. C'est bien $\beta_n \leqslant v - u$.

> *On va avancer à petits pas, plus petits que la longueur de l'intervalle $v - u$.*

Ensuite, on choisit p avec encore une partie entière : $p = \left[\frac{u}{\beta_n}\right] + 1$.
On a donc deux inégalités : $\frac{u}{\beta_n} \leqslant p \leqslant \frac{u}{\beta_n} + 1$.
On multiplie par le réel positif β_n : $u \leqslant p.\beta_n \leqslant u + \beta_n$.
On exploite ce que l'on a fait avant : $u \leqslant p.\beta_n \leqslant u + \beta_n < u + (v - u) = v$.
Le réel $p.\beta_n$ est bien entre u et v.

> *Par petit pas, quand on a atteint u on ne peut pas avoir dépassé v.*

Le réel $p.\beta_n$ est dans E car c'est $\beta_n + \beta_n + \ldots + \beta_n$, somme d'éléments de E.

Et même si p est négatif, on commence par dire que $-\beta_n$ est dans le groupe $(E, ++)$.

L'ensemble E est à l'image de $\mathbb{Q}$: très morcelé, mais quand même présent partout.

I∼0) Montrez qu'un élément x de E est inversible d'inverse dans E si et seulement si son module vaut 1 *(attention, il y a deux sens, pour l'un, pensez à $\Vert x.x^{-1}\Vert$)*.
On notera U l'ensemble des élément de E de module 1.
I∼1) Soit x un élément de U, d'écriture $a + b.\sqrt{2}$. On suppose $1 \leqslant x < 1 + \sqrt{2}$. Montrez alors $-1 \leqslant a - b.\sqrt{2} \leqslant 1$ et $0 \leqslant 2.a \leqslant 2 + \sqrt{2}$. Déduisez la valeur de a puis de b.
I∼2) Soit x un élément de U plus grand que 1. Montrez qu'il existe un entier k vérifiant $\alpha_k \leqslant x < \alpha_{k+1}$. Déduisez alors $1 \leqslant x.\beta_k < \alpha_1$ puis $x = \alpha_k$.
I∼3) Montrez que les seuls éléments de U sont les α_n, les β_n, les $-\alpha_n$ et les $-\beta_n$.

I∼0) Un élément x de E est dit premier si $\forall(u,\ v) \in E^2,\ x = u.v \Rightarrow (u \in U \text{ ou } v \in U)$ *(les nombres premiers dans $\mathbb{Z}$ sont caractérisés par $\forall(u,\ v) \in E^2,\ p = u.v \Rightarrow (|u| = 1 \text{ ou } |v| = 1)$)*. Montrez que les α_n sont dans P *(ensemble des nombres premiers)*. Montrez que $3 + \sqrt{2}$, $9 + 5.\sqrt{2}$, $5 - 13.\sqrt{2}$ sont dans P *(calculez leur module)*.

On donne quelques nombres, on calcule la norme de chacun

nombre	$3 + \sqrt{2}$	$9 + 5.\sqrt{2}$	$5 - 13.\sqrt{2}$
norme	7	31	313

On part de $9 + 5.\sqrt{2} = u.v$ avec u et v dans E. On doit montrer que u ou v est dans U.
On passe au module : $31 = \Vert u\Vert.\Vert v\Vert$ *(propriété du module)*.
Comme 31 est premier, on déduit $\Vert u\Vert = 1$ et $\Vert v\Vert = 31$ *(ou le contraire)*.
Mais on a montré $\Vert u\Vert = 1 \Rightarrow u \in U$. C'est donc que u *(ou v)* est dans U.

Ce raisonnement s'étend à tout élément de E dont le module est un entier premier. C'est le cas des trois ici étudiés.

Montrez que $8 + 3.\sqrt{2}$ n'est pas dans P.

Passons à $8 + 3.\sqrt{2}$, de module 46.
Et alors ? On n'invente pas une réciproque idiote. Ce n'est pas parce que le module se factorise que l'élément de E se factorise.
Mais ça nous donne une piste. Si on veut avoir $8 + 3.\sqrt{2} = u.v$ il faut avoir $\Vert u\Vert.\Vert v\Vert = 46$ sans qu'aucun ne vaille 1.
On peut tenter d'avoir $\Vert u\Vert = 23$ et $\Vert v\Vert = 2$ par exemple.
On tente $v = \sqrt{2}$. Et on devine ce à quoi on pouvait penser tout de suite : $\boxed{8 + 3.\sqrt{2} = (0 + 1.\sqrt{2}).(3 + 4.\sqrt{2})}$

∼0) Donnez des éléments de module 7. Déduisez que 7 n'est pas dans P.

L'entier 7 a pour module 49.
On tente donc de factoriser $7 = u.v$ avec $\Vert u\Vert = 7$ et $\Vert v\Vert = 7$, puisque ce sera la seule façon de faire.
Par exemple $3 + \sqrt{2}$. On met en face $3 - \sqrt{2}$ et on vérifie : $(3 + \sqrt{2}).(3 - \sqrt{2}) = 9 - 2 = 7$.
C'est un peu étonnant, mais 7 n'est donc plus premier quand on passe à E.
Et aussi $7 = (1 + 2.\sqrt{2}).(2.\sqrt{2} - 1)$.

∼0) Montrez : $\forall(u,\ v) \in \mathbb{Z}^2,\ u^2 - 2.v^2 = 5 \Rightarrow (5|u \text{ et } 5|v)$. Déduisez que 5 est dans P.

On doit établir un lemme : $\forall(u,\ v) \in \mathbb{Z}^2,\ u^2 - 2.v^2 = 5 \Rightarrow (5|u \text{ et } 5|v)$.
Il faut montrer que si $u^2 - 5.v^2$ vaut 5, alors u et v sont multiples de 5.
On dresse la liste des carrés modulo 5 :

u modulo 5	0	1	2	3	4
u^2 modulo 5	0	1	4	4	1

On dresse la liste des $u^2 - 2.v^2$ modulo 5

$u^2 - 2.v^2$	0	1	2	3	4	u modulo 5
0	0	1	4	4	1	
1	$-2 = 3$	$-1 = 4$	2	2	4	
2	$-3 = 2$	$-2 = 3$	1	1	3	
3	$-3 = 2$	$-2 = 3$	1	1	3	
4	$-2 = 3$	$-1 = 4$	2	2	4	
v modulo 2						

On voit qu'effectivement, la somme $u^2 - 2.v^2$ n'est congrue à 0 modulo 5 que pour u et v multiples de 5.

Passons à la primalité de 5. On suppose que 5 est produit de deux éléments de E : $5 = u.v$.
On passe au module : $25 = (\!|u|\!).(\!|v|\!)$.
Si on refuse que l'un des modules vaille 1 (puisque ceci permet alors de conclure $u \in U$ ou $v \in U$), on est obligé d'avoir $(\!|u|\!) = 5$ et $(\!|v|\!) = 5$.
Mais alors, en écrivant u sous la forme $r + \sqrt{2}.s$, le résultat préliminaire donne r et i sont multiples de 5. On les écrit $5.r'$ et $5.i'$. On reporte $u = 5.(r' + i'.\sqrt{2})$. On vérifie son module : $(\!|u|\!) = (5.r')^2 - 2.(5.i')^2 = 25.(r'^2 - 2.i'^2)$. Il vaut au moins 25, c'est une contradiction.

En fait, avec notre résultat préliminaire et ses modulo 5, on a montré que la norme d'un élément de E ne pouvait pas valoir 5.

I∼0) Passons à l'existence d'une division euclidienne dans E. On se donne x et y dans E avec y non nul ($x = a + i.b$ et $y = c + i.d$). Il faut prouver l'existence de q et r dans E vérifiant $x = q.y + r$ et r plus petit que b. Quel sens donner à « r plus petit que b » : $(\!|r|\!) < (\!|y|\!)$.
Voici des exemples de l'algorithme :

x	y	$\frac{x}{y}$	q	r
$5+\sqrt{2}$	$3+\sqrt{2}$	$\frac{5+\sqrt{2}}{3+\sqrt{2}} = \frac{13-2.\sqrt{2}}{(3+\sqrt{2}).(3-\sqrt{2})} = (2) + \left(-\frac{1}{7} - \frac{2.\sqrt{2}}{7}\right)$	2	$-1-\sqrt{2}$
$7+\sqrt{2}$	$3-\sqrt{2}$	$\frac{7+\sqrt{2}}{3-\sqrt{2}} = \frac{23+10.\sqrt{2}}{7} = (3+\sqrt{2}) + \left(\frac{2}{7} + \frac{3.\sqrt{2}}{7}\right)$	$3+\sqrt{2}$	$\sqrt{2}$
23	$6+5.\sqrt{2}$	$\frac{23}{6+5.\sqrt{2}} = \frac{-138+115.\sqrt{2}}{14} = -10+8.\sqrt{2} + \left(\frac{2+3.\sqrt{2}}{14}\right)$	$-10+8.\sqrt{2}$	$3+2.\sqrt{2}$

Divisez $11+7.\sqrt{2}$ par $5+2.\sqrt{2}$. Divisez $2020+2019.\sqrt{2}$ par $7+5.\sqrt{2}$. Divisez $2019+\sqrt{2}$ par $17+8.\sqrt{2}$. Expliquez l'algorithme général, et justifiez.

On décrypte l'algorithme général :

- On part de $x = a + \sqrt{2}.b$ et $y = c + \sqrt{2}.d$ non nul.
- On calcule le quotient en utilisant la quantité conjuguée : $\frac{a+b.\sqrt{2}}{c+d.\sqrt{2}} = \frac{(a+b.\sqrt{2}).(c-d.\sqrt{2})}{(c+d.\sqrt{2}).(c-d.\sqrt{2})}$.
- On sépare : $\frac{x}{y} = \frac{a.c-2.b.d}{c^2-2.d^2} + \sqrt{2}.\frac{b.c-a.d}{c^2-2.d^2}$ avec $c^2 - 2.d^2$ non nul.
- Les deux rationnels $\frac{a.c-2.b.d}{c^2-2.d^2}$ et $\frac{b.c-a.d}{c^2-2.d^2}$ ne sont pas forcément entiers, mais on peut les approximer par un entier.

En pratique, on arrondit un réel r à l'entier le plus proche :
∘ si r est entre $[r]$ et $[r]+0,5$, on prend $[r]$
∘ si r est entre $[r]+0,5$ et $[r]+1$, on prend $[r]+1$.
L'entier choisi n vérifie $|r-n| \leqslant \frac{1}{2}$.

- On a donc n et m vérifiant $\left|\frac{a.c-2.b.d}{c^2-2.d^2} - n\right| \leqslant \frac{1}{2}$ et $\left|\frac{b.c-a.d}{c^2-2.d^2} - m\right| \leqslant \frac{1}{2}$.
- On sépare : $\frac{x}{y} = n + m.\sqrt{2} + \left(\frac{a.c-2.b.d}{c^2-2.d^2} - n\right) + \sqrt{2}.\left(\frac{b.c-a.d}{c^2-2.d^2} - m\right)$.

Le terme du bout est plutôt « petit »...

- On pose donc $q = n + m.\sqrt{2}$ et on remultiplie par y : $x = y.q + \left(\left(\frac{a.c-2.b.d}{c^2-2.d^2} - n\right) + \sqrt{2}.\left(\frac{b.c-a.d}{c^2-2.d^2} - m\right)\right).(c+d.\sqrt{2})$.
- Le terme $\left(\left(\frac{a.c-2.b.d}{c^2-2.d^2} - n\right) + \sqrt{2}.\left(\frac{b.c-a.d}{c^2-2.d^2} - m\right)\right).(c+d.\sqrt{2})$ est il bien le reste ?
  - Déjà, est il dans E ? Sous cette forme, ce n'est pas gagné, mais sous la forme $x - y.q$, c'est normal, car on a un anneau.
  - On calcule sa norme : $(\!|\left(\left(\frac{a.c-2.b.d}{c^2-2.d^2} - n\right) + \sqrt{2}.\left(\frac{b.c-a.d}{c^2-2.d^2} - m\right)\right).(c+d.\sqrt{2})|\!)$ en rappelant que la norme du produit est le produit des normes :

$\left(\!\left|\left(\frac{a.c-2.b.d}{c^2-2.d^2}-n\right)+\sqrt{2}.\left(\frac{b.c-a.d}{c^2-2.d^2}-m\right)\right|\!\right).(c+d.\sqrt{2})\!\right| = \left(\!|u+v.\sqrt{2}|\!\right).\left(\!|c+d.\sqrt{2}|\!\right) = \left(\!|u+v.\sqrt{2}|\!\right).\left(\!|y|\!\right)$
avec $|u| = \left|\frac{a.c-2.b.d}{c^2-2.d^2}-n\right| \leqslant \frac{1}{2}$ et $|v| = \left|\frac{a.d-b.c}{c^2-2.d^2}-m\right| \leqslant \frac{1}{2}$.
• On élève au carré $-\frac{1}{4} \leqslant u^2 \leqslant \frac{1}{4}$ et $-\frac{1}{2} \leqslant 2.v^2 \leqslant \frac{1}{2}$ puis $-\frac{1}{2} \leqslant -2.v^2 \leqslant \frac{1}{2}$.
• On somme : $-\frac{3}{4} \leqslant u^2 - 2.v^2 \leqslant \frac{3}{4}$.
• On revient au module : $\left(\!\left|\left(\frac{a.c-2.b.d}{c^2-2.d^2}-n\right)+\sqrt{2}.\left(\frac{b.c-a.d}{c^2-2.d^2}-m\right)\right|\!\right).(c+d.\sqrt{2})\!\right| \leqslant \frac{3}{4}.\left(\!|y|\!\right) < \left(\!|y|\!\right)$.

C'est ce que l'on voulait.

On applique l'algorithme :

x	y	$\frac{x}{y}$	$n+...$	$m+...$	q	r
11 $+7.\sqrt{2}$	$5+2.\sqrt{2}$	$\frac{11+7.\sqrt{2}}{5+2.\sqrt{2}} = \frac{27+13.\sqrt{2}}{17}$	$2-\frac{7}{17}$	$1-\frac{4}{17}$	$2+\sqrt{2}$	$-3-2.\sqrt{2}$
2020 $+2019.\sqrt{2}$	$7+5.\sqrt{2}$	$\frac{2020+2019.\sqrt{2}}{7+5.\sqrt{2}} = 6050-4033.\sqrt{2}$	6050	-4033	6050 $-4033.\sqrt{2}$	0
2019 $+\sqrt{2}$	$17+8.\sqrt{2}$	$\frac{2019+\sqrt{2}}{17+8.\sqrt{2}} = \frac{4901-2305.\sqrt{2}}{23}$	$213+\frac{2}{23}$	$-100-\frac{5}{23}$	213 $213-100.\sqrt{2}$ $-100.\sqrt{2}$	$-2-3.\sqrt{2}$

Il manque un détail : l'unicité de la division euclidienne.
On part de $x = y.q + r$ et $x = y.q' + r'$ avec r et r' de module plus petit que celui de y.
On va prouver : $q = q'$ et $r = r'$.
On fait passer d'un côté : $y.(q'-q) = r - r'$.
On passe au module : $\left(\!|y|\!\right).\left(\!|q'-q|\!\right) = \left(\!|r-r'|\!\right)$.
Or, le membre de droite a un module strictement plus petit que celui de y. C'est donc que $q'-q$ a un module plus petit que 1.
C'est donc que son module est nul. On déduit $q = q'$. On reporte : $r = r'$.

Donnez le p.g.c.d. de $91+49.\sqrt{2}$ et $37-4.\sqrt{2}$.

On part de deux nombres et on applique l'algorithme d'Euclide *(divisions euclidiennes successives)* jusqu'au dernier reste non nul

$$\begin{array}{ccccc}
(91+49.\sqrt{2}) & = & (3+2.\sqrt{2})\times & (37-4.\sqrt{2}) & +(-4-13.\sqrt{2}) \\
(37-4.\sqrt{2}) & = & (1-2.\sqrt{2})\times & (-4-13.\sqrt{2}) & +(15+5.\sqrt{2}) \\
(-4-13.\sqrt{2}) & = & (0-1.\sqrt{2})\times & (15+5.\sqrt{2}) & +(6+2.\sqrt{2}) \\
(15+5.\sqrt{2}) & = & (2+0.\sqrt{2})\times & (6+2.\sqrt{2}) & +(3+\sqrt{2}) \\
6+2.\sqrt{3} & = & (2+0.\sqrt{2}) & (3+\sqrt{2}) & +0
\end{array}$$

Le dernier reste non nul est $3+\sqrt{2}$. C'est lui le *p.g.c.d.*
On vérifie : $\frac{91+49.\sqrt{2}}{3+\sqrt{2}} = 25+8.\sqrt{2}$ et $\frac{37+4.\sqrt{2}}{3+\sqrt{2}} = 17-7.\sqrt{2}$.
On peut vérifier que $25+8.\sqrt{2}$ et $17-7.\sqrt{2}$ *(de modules 497 et 191)* sont premiers entre eux.

On peut ensuite écrire une identité de Bézout. Mais on n'a pas que ça à faire.

◃ 19 ▹

Pouvez vous trouver deux matrices A et B de taille 2 sur 2 telles que les spectres soient

A	B	$A+B$
$\{1,3\}$	$\{1,5\}$	$\{4,6\}$

,

A	B	$A+B$
$\{1,3\}$	$\{2,5\}$	$\{1,4\}$

,

A	B	$A+B$
$\{0,3\}$	$\{2,5\}$	$\{4,6\}$

(trois exercices dont une réponse NON).

Les matrices de spectre $\{1,3\}$ sont diagonalisables (deux valeurs propres distinctes, chaque valeur propre apporte un vecteur propre, on a deux vecteurs propres indépendants, donc une matrice de passage). Elles sont donc de la forme $P.\begin{pmatrix}1&0\\0&3\end{pmatrix}.P^{-1}$, avec en particulier $\begin{pmatrix}1&0\\0&3\end{pmatrix}$ et $\begin{pmatrix}3&0\\0&1\end{pmatrix}$.

On raisonnement de même pour « spectre $\{1,5\}$ », avec cette fois les $Q.\begin{pmatrix}1&0\\0&3\end{pmatrix}.Q^{-1}$ et en particulier $\begin{pmatrix}1&0\\0&5\end{pmatrix}$ et $\begin{pmatrix}5&0\\0&1\end{pmatrix}$.

On tient une solution facile :

$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$	$+\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$	$=$	$\begin{pmatrix} 6 & 0 \\ 0 & 4 \end{pmatrix}$
spectre $\{1,3\}$	$\{5,\ 1\}$		$\{6,\ 4\}$

On peut ensuite cacher les choses avec $P.\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}.P^{-1} + P.\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}.P^{-1} = P.\begin{pmatrix} 6 & 0 \\ 0 & 4 \end{pmatrix}.P^{-1}$ Ça, c'est l'art du « poseur d'exercices ».

Pour le triplet

A	B	$A+B$
$\{1,\ 3\}$	$\{2,\ 5\}$	$\{1,\ 4\}$

, la même idée ne convient plus.

D'ailleurs, aucune idée ne convient. Et c'est rapide. Regardez la trace

matrice	A	B	$A+B$
spectre	$\{1,\ 3\}$	$\{2,\ 5\}$	$\{1,\ 4\}$
trace	4	7	5

On n'a pas $Tr(A+B) = Tr(A) + Tr(B)$. Le problème n'a pas de solution.

La même idée avec

A	B	$A+B$
$\{0,\ 3\}$	$\{2,\ 5\}$	$\{4,\ 6\}$

?

matrice	A	B	$A+B$
spectre	$\{0,\ 3\}$	$\{2,\ 5\}$	$\{6,\ 4\}$
trace	3	7	10

c'est cohérent. Mais ça ne prouve pas qu'il y a une solution[3].

Il faut vraiment construire une solution.

Cette fois, ce n'est pas avec des jeux sur

	$\begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}$	$\begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}$
$\begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix}$	$\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$
$\begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$	$\begin{pmatrix} 8 & 0 \\ 0 & 2 \end{pmatrix}$

qu'on trouve une solution.

Il faut jouer sur $P.\begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}.P^{-1}$ et $Q.\begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix}.Q^{-1}$.

Ou sur $Q^{-1}.P.\begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}.P^{-1}.Q$ et $\begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix}$.

On va donc prendre une matrice R inversible, et poser $A = R.\begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}.R^{-1}$ avec R inversible et $B = \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix}$.

Par construction,

matrice	trace	déterminant	polynôme caractéristique	spectre
$A = R.\begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}.R^{-1}$	3	0	$X^2 - 3.X$	$\{0,\ 3\}$
$B = \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix}$	7	10	$X^2 - 7.X + 10$	$\{2,\ 5\}$
$A+B$	10	?	$X^2 - 10.X +$?	$\{4,\ 6\}$

La condition nécessaire et suffisante est $\det(A+B) = 24$.

Si on n'arrive pas à avoir ça ! Prenons même R assez simple pour commencer : $\begin{pmatrix} 1 & 1 \\ a & b \end{pmatrix}$.

Le calcul « à la main » donne $A + B = \dfrac{1}{b-a}.\begin{pmatrix} 8.a - 5.b & -3.a \\ 3.b & 2.a - 5.b \end{pmatrix}$.

On effectue : $\det(A+B) = \dfrac{16.a - 25.b}{a-b}$.

C'est faisable, avec $a = 1$ et $b = 8$ par exemple.

On résume :

matrice	trace	déterminant	polynôme caractéristique	spectre
$A = \frac{1}{3}.\begin{pmatrix} 1 & -1 \\ -8 & 8 \end{pmatrix}$	3	0	$X^2 - 3.X$	$\{0,\ 3\}$
$B = \begin{pmatrix} 5 & 0 \\ 0 & 2 \end{pmatrix}$	7	10	$X^2 - 7.X + 10$	$\{2,\ 5\}$
$A+B = \frac{1}{3}.\begin{pmatrix} 16 & -1 \\ -8 & 14 \end{pmatrix}$	10	24	$X^2 - 10.X + 24$	$\{4,\ 6\}$

D'autres réponses sont possibles.

---

3. Point important à nouveau : montrer qu'il n'y a pas d'incohérence ne montre pas qu'il y a une solution, on est d'accord ! L'incohérence peut être ailleurs. On raisonne !

◁ 20 ▷ On a posé : $n = 88\,825$ et $p = 7\,267$. Votre voisin a écrit : $192\,171.p - 15\,722.n = 7$. Vous en déduisez : $p.g.c.d.(n,\ p) = 7$.
Vous avez tort. Pourquoi ?

C'est une identité de Bézout ?
Elle dit que 7 est dans $\{a.n + b.p \mid (a, b) \in \mathbb{Z}^2\}$.
Ce qui signifie que 7 est dans « le plus petit sous-groupe de $(\mathbb{Z}, +)$ contenant n et p ».
Mais ce n'est pas forcément un générateur de cet ensemble (plus petit élément non nul).

7 est un multiple du p.g.c.d.
Et ici, le p.g.c.d. vaut 1 : $27\,453.p - 2\,246.n = 1$.
Et on a tout multiplié par 7.

Le cours dit :	si d est le p.g.c.d. alors il existe a et b vérifiant $a.n + b.p = d$.
Et il ajoute	tout nombre de la forme $a.n + b.p$ est un multiple du p.g.c.d. (mais pas forcément « le p.g.c.d. »).

◁ 21 ▷ ♡ Montrez que $\phi = (a,\ b) \longmapsto 2^a.(2.b + 1)$ est bijective de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}^*$.
Ecrivez un script Python qui prend en entrée n et retouve son antécédent par ϕ.

$\phi = (a,\ b) \longmapsto 2^a.(2.b + 1)$ prend eeux entiers et définit un entier.
Elle va de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$.

On n'atteindra jamais 0. $Im(\phi) \subset \mathbb{N}^*$.

Si vous me dite tout de suite $Im(\phi)) = \mathbb{N}^*$, vous n'avez rien compris. Il y a tout le boulot de la surjectivité.

Prenons deux couples $(a,\ b)$ et $(c,\ d)$ et supposons qu'ils ont la même image.
On a donc $2^a.(2.b + 1) = 2^c.(2.d + 1)$.
On étudie cette égalalité modulo 2.
Proprement, on suppose $a \neq c$. Par symétrie des rôles, on peut aupposer $a > c$. On divise alors de chaque côté par 2^c : $2^{a-c}.(2.b + 1) = (2.d + 1)$.
Le membre de droite est impair. Celui de gauche est pair. Il y a une contradiction.
On a donc foércément $a = c$.
On reporte : $2^a.(2; b + 1) = 2^a.(2.d + 1)$. On aboutit sans effort à $b = d$.

Du travail « évident ». Mais trop d'élèves se perdent dans les variables, faute de s'être demandé « je démontre quoi ? ».

Pour la surjectivité, il faut trouver un antécédent $(a,\ b)$ à tout entier naturel N donné.
On se donne N et on le décompose en produit de facteurs premiers : $N = 2^\alpha.3^\beta.5^\gamma.\ldots$ (produit fini, mais moche à indexer hormis en $\prod_i (p_i)^{\alpha_i}$).
Le produit $3^\beta.5^\gamma.\ldots$ est impair. On peut l'écrire $2.b + 1$.
Et ona alors $N = 2^\alpha.(2.b + 1)$. On pose $a = \alpha$ et c'est fini.

L'application est donc bien bijective de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}^*$.

Qui sont les crétins qui avec des réflexes de « j'ai des théorèmes, mais pas de vision géométrique » ont essayé à tout prix de sortir un truc du type « application strictement croissante donc injective ». On n'a pas de relation d'ordre sur $\mathbb{N} \times \mathbb{N}$!

Un exemple : 2022 est pair et non multiple de 4, il a pour antécédent $(1,\ 505)$
2023 est impair, il a pour antécédent $(0,\ 1012)$
2024 est multiple de 8, il a pour antécedent $(3,\ 126)$

Démarche : pour N donné, trouver l'exposant de 2 en divisant par 2 tant que c'est possible (e en incrémentant un compteur).
Une fois qu'on a un nombre impair, on l'écrit $2.b + 1$.

```
def Reciproque(N) : #int -> int x int
....n = N #pour ne pas abimer N
....a = 0 #compteur
....while N%2 == 0 : #tant que n est pair
........n = n//2 #on divise par 2
........a += 1
....b = (n-1)//2 #pour n = 2.b+1
....return (a,b)
```

◁ 22 ▷ Résolvez $\begin{vmatrix} 1 & 1 & 1 \\ x & 4 & 7 \\ x^3 & 4^3 & 7^3 \end{vmatrix} = 0$ (devrez vous développer ?).

Si on développe par rapport à la première colonne, c'est une équation de degré 3 : $1.\begin{vmatrix} 4 & 7 \\ 4^3 & 7^3 \end{vmatrix} - x.\begin{vmatrix} 1 & 1 \\ 4^3 & 7^3 \end{vmatrix} + x^3.\begin{vmatrix} 1 & 1 \\ 4 & 7 \end{vmatrix}$.

Une racine évidente est $x = 4$ (deux colonnes égales, déterminant nul $\begin{vmatrix} 1 & 1 & 1 \\ 4 & 4 & 7 \\ 4^3 & 4^3 & 7^3 \end{vmatrix} = 0$).

Une autre racine est $x = 7$ pour la même raison.
Et comme la somme des racines est nulle (pas de coefficient en x^2), on a les trois racines : 4, 7 et -11.
Inutile d'en chercher d'autres : $S = \{-11,\ 4,\ 7\}$.

La nullité de $\begin{vmatrix} 1 & 1 & 1 \\ -11 & 4 & 7 \\ -11^3 & 4^3 & 7^3 \end{vmatrix}$ saute moins aux yeux, mais je compte sur certains d'entre vous pour saisir quand même la combinaison à faire...

◁ 23 ▷ J'ai tracé un quadrilatère $(A,\ B,\ C,\ D)$ dans le plan. J'ai mesuré ses quatre côtés et une de ses diagonales. J'ai trouvé les mesures suivantes, triées par ordre croissant :

4	8	11	20	30

Dites moi laquelle est la longueur d'une des diagonales *(et prouvez le)*.

Indiquez comment retrouver alors la longueur de l'autre diagonale. Combien de valeurs peut prendre cette longueur de l'autre diagonale ?

Point de départ de cet exercice : si on a un triangle, on mesure les longueurs des côtés ; mais si on a les longueurs des côtés, on n'a pas forcément un triangle.

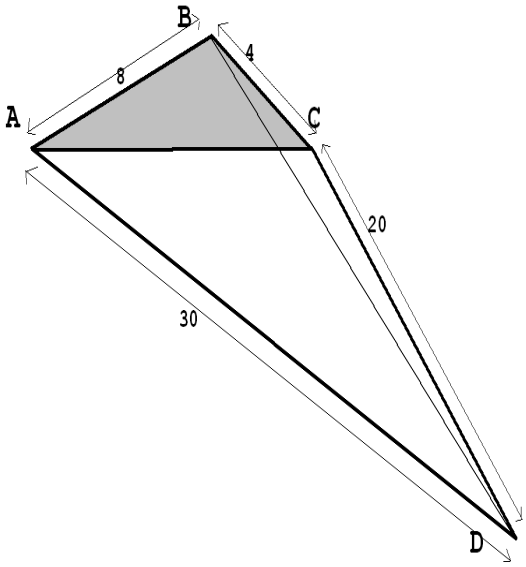
Par exemple, il est impossible d'avoir un triangle $(A,\ B,\ C)$ vérifiant $AB = 1$, $BC = 2$ et $AC = 15$, on est d'accord.
Or, un quadrilatère dont on a tracé une des diagonales est fait de deux triangles accolés. Il y a donc des relations entre les cinq longueurs données.
Alors, quelles sont les conditions sur les trois longueurs d'un triangle ?
On considéré un triangle de sommets A, B et C et de côtés a, b et c *(notation canonique : $AB = c$ et ainsi de suite)*. Quitte à ordonner, on suppose $a \leqslant b \leqslant c$. On a trois inégalités triangulaires à écrire et manipuler *(sachant $a \leqslant b \leqslant c$)* :

$AB \leqslant AC + BC$	$c \leqslant a + b$	$c - b \leqslant a$	formule 1
$AC \leqslant AB + BC$	$a \leqslant b + c$	peu utile	
$BC \leqslant AB + AC$	$b \leqslant a + c$	$b - a \leqslant c$	formule 2

Quitte maintenant à choisir le nom des quatre sommets du quadrilatère, on les nomme dans l'ordre A, B, C et D, et on considère que la diagonale mesurée est AC.
La question est : de 4 8 11 20 30, qui est AC ? On raisonne en étudiant chaque cas, un par un. On élimine ceux qui sont incohérents, et s'il n'en reste qu'un, c'est le bon.

On suppose $AC = 4$. On a alors deux triangles (ABC) et (ACD) dont le plus petit côté vaut 4. La formule (1) nous dit que la différence des deux autres cotés ne peut pas dépasser 4. C'est possible avec un triangle de mesures $(4, 8, 11)$, mais on n'a plus de possibilités pour l'autre : $(4,\ 20,\ 35)$ n'est pas cohérent.
On élimine $AC = 4$.

• On suppose $AC = 8$. Là encore, il faut deux couples de côtés dont la différence ne dépasse pas 8. C'est encore possible avec $(4, 8, 11)$ mais pas avec $(8, 20, 30)$ *(et je ne parle pas des* $(4, 8, 20)$ *et autres)*.
On élimine $AC = 4$.



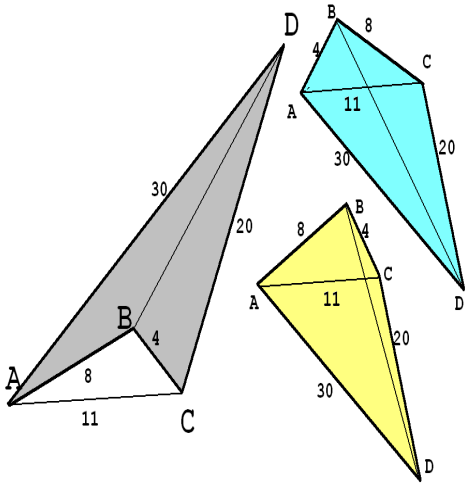
• On suppose $AC = 11$. On peut assembler un triangle $(4, 8, 11)$ et un triangle $(11, 20, 30)$. Il n'y a aucune incohérence.
On peut garder $AC = 11$.

• On suppose $AC = 20$ *(une grande diagonale !)*. Les côtés du quadrilatère valent 4, 8, 11 et 30. On a donc deux triangles dont un côté vaut 20. L'un d'entre eux est de la forme $(x, 20, 30)$, et l'autre prend les deux longueurs qui restent. Mais, qu'il s'agisse de $(11, 8, 20)$, $(4, 8, 20)$, $(4, 11, 20)$ c'est incohérent.
On élimine $AC = 20$.

• On suppose $AC = 30$. C'est encore pire. Comment pouvez vous alors avoir deux triangles de grand côté 30, avec les longueurs 4, 8, 11 et 20 ? Déjà, $4 + 8 + 11 + 20$ n'atteint pas 60.

Bref, par élimination, il ne reste que $AC = 11$
L'un des côtés du quadrilatère vaut 30. Il faut donc avec un côté de longueur au moins $30 - 11$. La seule solution est donc 20.
Les deux derniers côtés sont 4 et 8.
On a deux solutions *(à symétrie et rotation près)* :

$AB = 8$	$BC = 4$	$CD = 20$	$DA = 30$
$AB = 4$	$BC = 8$	$CD = 20$	$DA = 30$



On va chercher à mesurer l'autre diagonale dans le premier cas. Mais il y a l'autre cas.
On choisit un repère associé à notre problème, comme toujours en géométrie cartésienne.
On place l'origine en A qui a alors pour coordonnées $(0, 0)$.
On oriente l'axe Ox pour que C soit dessus : $C(11, 0)$.
On doit alors placer B à distance 8 de A ($x^2 + y^2 = 64$) et à distance 4 de C ($(x - 11)^2 + y^2 = 16$). On résout et on choisit l'orientation de Oy pour que y_B soit positif : $B\left(\frac{169}{22}, \frac{22.\sqrt{2415}}{484}\right)$.
On fait de même pour placer D : $x^2 + y^2 = 900$, $(x - 11)^2 + y^2 = 400$: $D\left(\frac{621}{22}, \frac{66.\sqrt{5551}}{484}\right)$.
Il ne reste plus qu'à calculer la distance BC *(application numérique totalement inutile :* $\sqrt{\frac{128\,339 + 21.\sqrt{273\,585}}{484}}$ *soit environ* 24*)*.
Mais il y a d'autres solutions quatre quadrilatères dont deux convexes en changeant des signes...

◃ 24 ▹ Si a, b, c, d, e, f et g sont sept nombres, écrivez avec une formule la plus courte (avec 21 symboles $=$) qu'ils sont tous distincts.

On visualise si nécessaireavec un graphe complet à sept sommets a à g et on doit passer une fois (et une seule) par chaque arête.
On peut partir du sommet qu'onveut, on finira sur le même.
Chaque fois qu'on arrive sur un sommet, il reste une arête pour repartir.

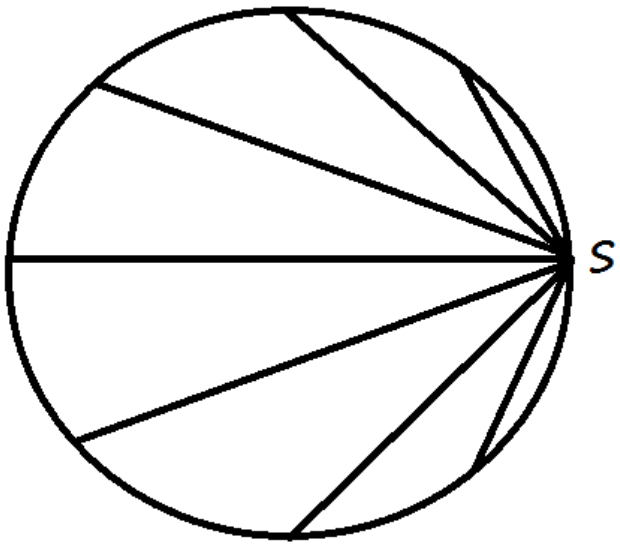
$$a \neq b \neq c \neq d \neq e \neq f \neq g \neq a \neq c \neq e \neq g \neq b \neq d \neq f \neq a \neq d \neq g \neq c \neq f \neq b \neq e \neq a$$

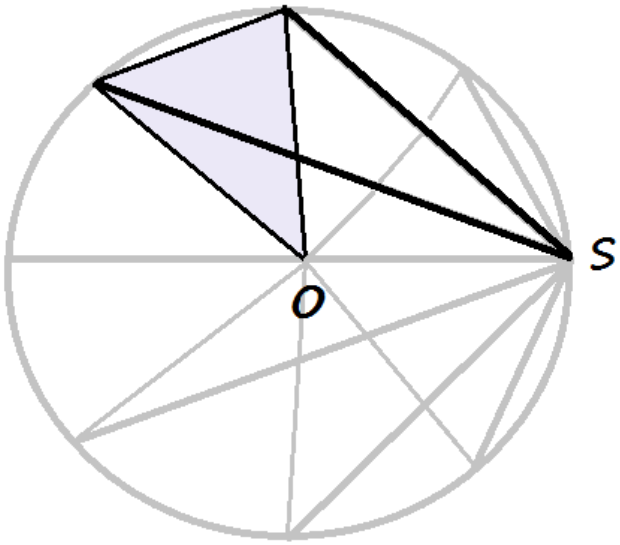
◁ 25 ▷ Un polygone convexe régulier a 527 diagonales. Calculez le plus petit angle non nul entre deux diagonales *(étape intermédiaire : calculez le nombre de sommets)*.

Prenons un polygone à n sommets (et n côtés).
De chaque sommet partent $n-3$ diagonales le sommet voit $n-1$ autres sommets
mais quand on le relie à l'un de ses deux voisins, on n'a pas une diagonale
mais un côté
Mais avec $n.(n-3)$, chaque diagonale A_iA_k est comptée deux fois (une fois par A_i et une fois par A_k).

On a donc ici : $\dfrac{n.(n-3)}{2} = 527$.
On a une équation du second degré $n^2 - 3.n - 1054 = 0$.
Les deux racines sont -31 et 34. On gardera 34.

Et maintenant, que est l'angle entre deux diagonales (issues d'un même sommet, c'est ambigu).
Par théorème de l'angle au centre.





L'angle en S est à chaque fois la moitié de l'angle en O.
Et tous les angles en O sont égaux à $\dfrac{2.\pi}{n}$ puisque le disque est découpé en n parts.
Les angles entre les diverses diagonales valent donc tous ici $\dfrac{\pi}{34}$.

◁ 26 ▷ Placez aux huit sommets d'un cube les entiers de 1 à 8.
Il faut ensuite que pour chaque face, le produit des quatre entiers aux quatre coins de la face soit la valeur imposée sur le patron du développement du cube ci contre :

	280		
96	1344	420	30
	144		

C'est déjà un problème de factorisation.

	2.2.2.5.7		
2.2.2.2.2.3	2.2.2.2.2.2.3.7	2.2.3.5.7	2.3.5
	2.2.2.2.3.3		

Après c'est du repérage dans l'espace pour comprendre qui sont les sommets communs à trois faces dans le patron du dé.
Par exemple, le 5 est facile à placer.

	2.2.2.5.7		
2.2.2.2.2.3	2.2.2.2.2.2.3.7	2.2.3.5.7	2.3.5
	2.2.2.2.3.3		

7 5

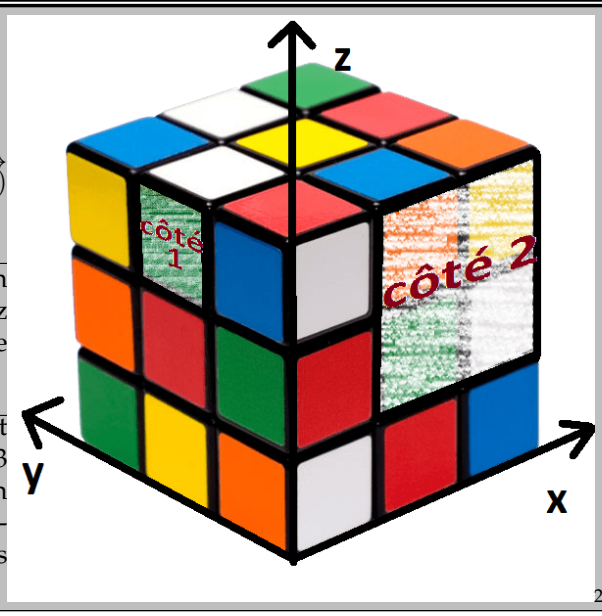
Il en est de même du 7.
Autour de la face 2.3.5, il ne peut y avoir que le 2, le 3, le 5 et... le 1. Et par exemple, le 3 ne peut pas être à côté de

la face supérieure qui n'en contient pas...
Autour de la face 2.2.3.5.7 on a déjà le 5 et le 7, il reste au choix : 4 et 3 ou alors 2 et 6.
Je vous laisse finir.

♣$_0$ On pose $\tau = \overrightarrow{(1\,2)}$ et $\sigma = \overrightarrow{(1\,2\,3\,4\,5)}$. Décomposez $\overrightarrow{(1\,3)}$ et $\overrightarrow{(2\,3)}$ uniquement avec des σ et des τ.

♡$_1$ Le polynôme $X^3 + p.X + q$ a pour racines a, b et c. On définit $\alpha = a + b.c$, $\beta = b + a.c$ et $\gamma = c + a.b$. Exprimez $\alpha + \beta + \gamma$ et $\alpha.\beta.\gamma$ à l'aide de p et q. Donnez le polynôme de racines α, β et γ.

♣$_1$ Un Rubik'Cube est formé de vingt sept cubes articulés, et donc aussi soixante quatre « sommets » numérotés de 0 à 63 ou de $(0,0,0)$ à $(3,3,3)$, c'est comme vous voulez. Combien de carrés de côté unité pouvez vous tracer ayant pour sommets quatre de ces points ? Combien de carrés pouvez vous tracer ayant pour sommets quatre de ces points ?



◃ 27 ▹

2018

Le polynôme $X^3 + p.X + q$ a pour racines a, b et c. On a donc $a + b + c = 0$, $a.b + a.c + b.c = p$ et $a.b.c = -q$. Plus d'autres relations comme $a^2 + b^2 + c^2 = (a + b + c)^2 - 2.(a.b + a.c + b.c) = -2.p$.
On définit $\alpha = a + b.c$, $\beta = b + a.c$ et $\gamma = c + a.b$. Les rôles sont symétriques.
sans aucun effort : $\boxed{\alpha + \beta + \gamma = (a + b + c) + (a.b + a.c + b.c) = p}$
On y va courageusement : $\alpha.\beta.\gamma = (a.b + a^2.c + b^2.c + a.b.c^2).(c + a.b)$
puis $\alpha.\beta.\gamma = \begin{matrix} a.b.c & +a^2.c^2 & +b^2.c^2 & +a.b.c^3 \\ a^2.b^2 & +a^3.b.c & +a.b^3.c & +a^2.b^2.c^2 \end{matrix}$.
On regroupe par symétrie : $\alpha.\beta.\gamma = (a.b.c) + (a^2.b^2 + a^2.c^2 + b^2.c^2) + (a.b.c^3 + a.c.b^3 + b.c.a^3) + (a^2.b^2.c^2)$.
On traite ce qu'on peut directement : $(a.b.c) + (a^2.b^2.c^2) = q^2 - q$.
On a aussi rapidement $(a.b.c^3 + a.c.b^3 + b.c.a^3) = (a.b.c).(a^2 + b^2 + c^2) = 2.p.q$.
Pour $(a^2.b^2 + a^2.c^2 + b^2.c^2)$ on développe $(a.b + a.c + b.c)^2$ auquel on doit soustraire des termes en $2.(a.b).(a.c)$.
On a donc $(a^2.b^2 + a^2.c^2 + b^2.c^2) = (a.b + a.c + b.c)^2 - 2.(a.b.c).(a + b + c) = p^2$.
On regroupe : $\boxed{\alpha.\beta.\gamma = q^2 - q + 2.p.q + p^2}$ *(bon, ça n'a rien de spécial, hormis $(p+q)^2 - q$).*
Pour la suite, on va calculer la somme des doublets $\alpha.\beta + \alpha.\gamma + \beta.\gamma$: $\begin{matrix} a.b & +c.a^2 & +c.b^2 & +a.b.c^2 \\ a.c & +a.b^2 & +c.b^2 & +a.c.b^2 \\ b.c & +b.a^2 & +c.a^2 & +b.c.a^2 \end{matrix}$

Dois je encore vous dire qu'en mettant les calculs sous forme de tableau, on n'y perd rien et on est efficace ?

On a des termes simples : $a.b + a.c + b.c = p$,
puis $a.b.c^2 + a.c.b^2 + b.c.a^2 = (a.b.c).(a + b + c) = 0$
et enfin $a^2.c + a^2.b + b^2.a + b^2.c + c^2.a + c^2.b = (a + b + c).(a.b + a.c + b.c) - 3.a.b.c = 3.q$.
On termine $\boxed{\alpha.\beta + \alpha.\gamma + \beta.\gamma = p + 3.q}$
On peut conclure avec le polynôme
$\boxed{(X - \alpha).(X - \beta).(X - \gamma) = X^3 - p.X^2 + (p + 3.q).X + q - (p + q)^2}$

On a deux outils : τ qui échange deux éléments, et σ qui fait tourner tout le monde d'un cran.
On veut échanger 2 et 3. On les place en 1 et 2 par σ, on permute alors 1 et 2 avec τ, puis on les remet en 2 et 3.
On va donc essayer $\sigma \circ \tau \circ \sigma^{-1} = \overrightarrow{(1\,2\,3\,4\,5)} \circ \overrightarrow{(1\,2)} \circ \overleftarrow{(1\,2\,3\,4\,5)} =$

$$\begin{matrix} & 1 & 2 & 3 & 4 & 5 \\ \overleftarrow{(1\,2\,3\,4\,5)} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 5 & 1 & 2 & 3 & 4 \\ \overrightarrow{(1\,2)} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 5 & 2 & 1 & 3 & 4 \\ \overrightarrow{(1\,2\,3\,4\,5)} & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 & 4 & 5 \end{matrix} = \overrightarrow{(2\,3)}$$

Si les exposants négatifs sont interdits : $\boxed{\overrightarrow{(2\,3)} = \sigma \circ \tau \circ \sigma^{-1} = \sigma \circ \tau \circ \sigma^4}$

Et si on a mal joué : $\sigma^{-1} \circ \tau \circ \sigma = \overleftarrow{(1\,2\,3\,4\,5)} \circ \overrightarrow{(1\,2)} \circ \overrightarrow{(1\,2\,3\,4\,5)} = \begin{matrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 5 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 4 & 5 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 2 & 3 & 4 & 1 \end{matrix} = \overrightarrow{(1\,5)}$

Ça ne sert à rien.

Il faut échanger le 1 et le 3. On ne peut pas le faire avec juste τ ; ils sont trop loin l'un de l'autre.
Mais on sait échanger le 2 et le 3. Si on échange alors 1 et 2 et qu'on remet en place, on doit avoir gagné :

$$\overrightarrow{(1\,2)} \circ \overrightarrow{(2\,3)} \circ \overrightarrow{(1\,2)} = \begin{matrix} \overrightarrow{(1\,2)} \\ \overrightarrow{(2\,3)} \\ \overrightarrow{(1\,2)} \end{matrix} \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{matrix} = \overrightarrow{(1\,3)}$$

On peut donc écrire $\boxed{\overrightarrow{(1\,3)} = \tau \circ \sigma \circ \tau \circ \sigma^{-1} \circ \tau}$ Mais il y a d'autres solutions.

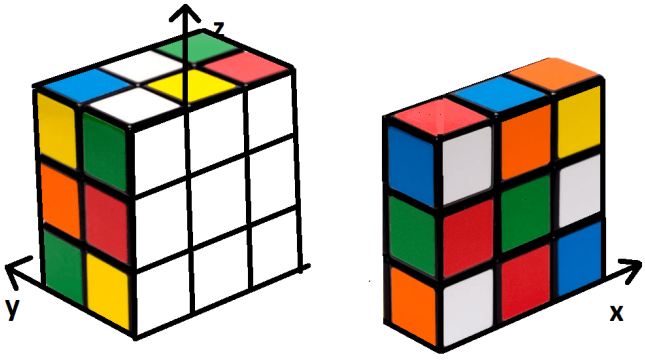
On a bien des points, et si on prend le repère, ils ont des coordonnées $(i,\ j,\ k)$ avec i, j et k pouvant valoir 0, 1, 2 ou 3. On a quatre choix pour chacun, d'où effectivement $4 \times 4 \times 4$ points possibles.
On regarde les carrés de côté 1. Ce sont les faces des petits cubes.
On peut s'y prendre mal, quoique.
Il y a 27 petits cubes *(neuf par tranche)*. Chacun a six faces carrées. On a donc 6×27 carrés.
Mais beaucoup sont comptés deux fois. Tous, sauf les faces à l'extérieur du grand cube. Il y en a neuf par face du grand cube, et donc 9×6 carrés qui ne sont pas comptés deux fois, mais une seule.

mini faces carrées	mini faces carrés compté
27×6	6×9

On arrive à la formule $\dfrac{6 \times 27 - 6 \times 9}{2} + 6 \times 9$. Tous calculs faits : $\boxed{108 \text{ carrés de côté 1}}$

Si vous n'avez compté que les carrés visibles : 54.

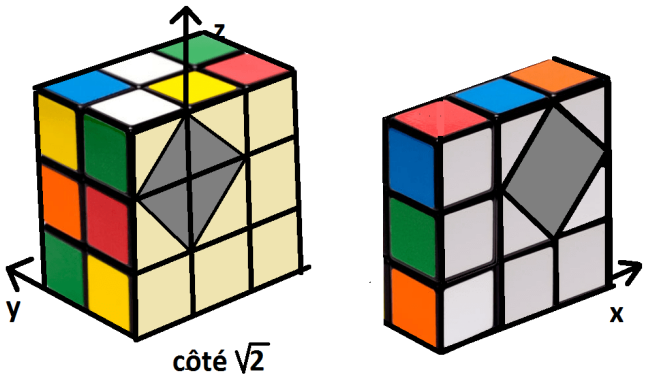
Autre approche : on regarde dans chaque plan de coupe du cube. De tels plans sont similaires à chaque face visible du cube, mais ils sont plus nombreux.
Sur un tel plan, on voit neuf carrés.



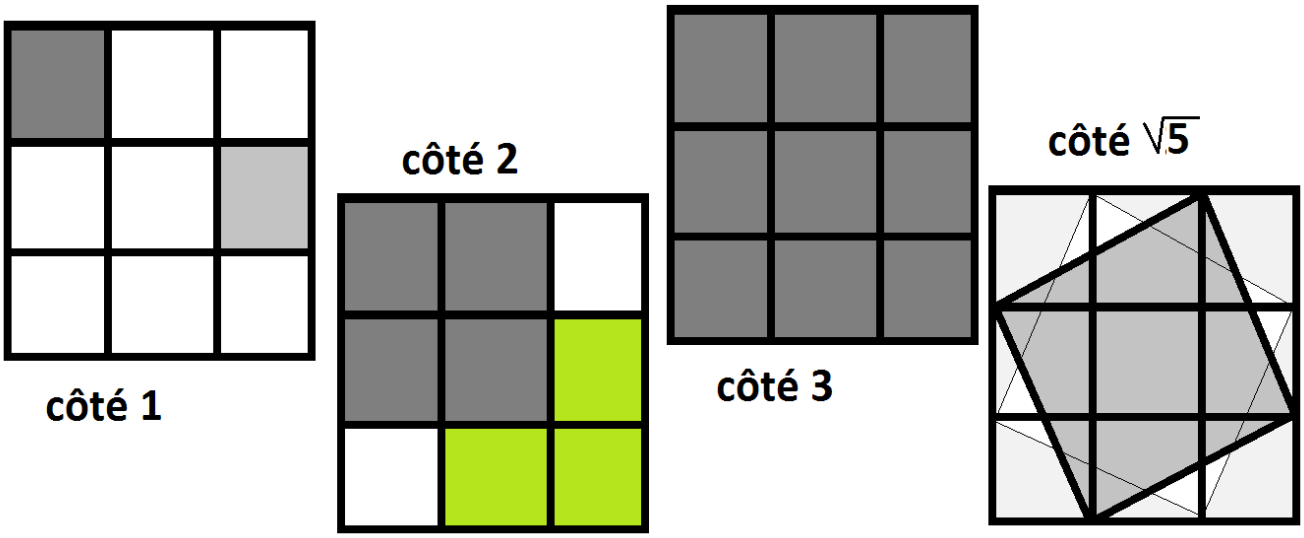
Il reste à compter ces plans. Il y en a de trois types : horizontaux, verticaux comme xOz ou verticaux comme yOz.
Pour chaque type, il y a quatre niveaux de coupe : par exemple pour les horizontaux : équation $z = 0$, équation $z = 1$, équation $z = 2$, équation $z = 3$.
On a donc douze plans de coupes, avec à chaque fois neuf carrés.
Le total est (là encore) de 108 carrés.

Mais il y a plusieurs formats de carrés possibles : taille 1, taille 2, taille 3.
On regarde dans chacun des douze plans de coupe

taille 1 sur 1	taille 2 sur 2	taille 3 sur 3
9	4	1



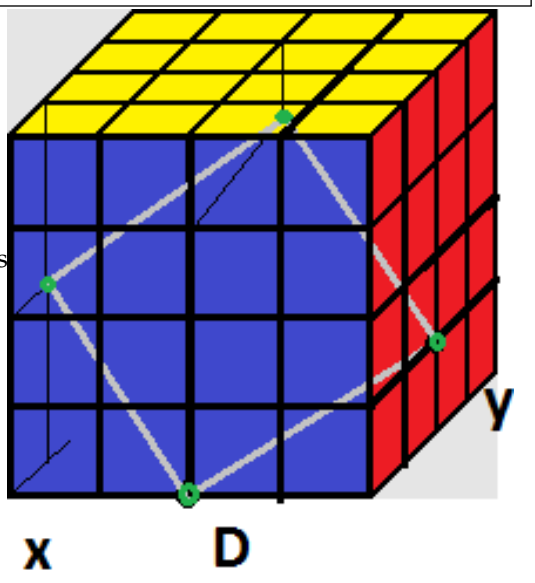
On multiplie donc par 12.
Mais on a oublié des carrés. Si si ! Ceux de côté $\sqrt{2}$. Il ne fallait pas les oublier ceux là.
Il y en a quatre par plan de coupe. On peut les nommer Nord-ouest, Nord-Est, Sud-Est et Sud-Ouest.
Sur le schéma ci-contre, on voit Nord-ouest et Nord-Est de deux plans de coupe parallèles.
Et on a aussi des modèles de côté $\sqrt{5}$.



	taille 1 sur 1	taille 2 sur 2	taille 3 sur 3	taille $\sqrt{2}$ sur $\sqrt{2}$	taille $\sqrt{5}$ sur $\sqrt{5}$
par plan de coupe	9	4	1	4	2
au total	108	48	12	48	24

On a un total de 240 carrés qu'on ne tracera pas.

D'autant qu'il faut se poser une autre question. Peut il exister des carrés qui ne soient pas dans des plans de coupe ?



Peut on avoir des carrés « inclinés » ?
Dans un Rubik's cube de taille 4 sur 4, on peut aller chercher les quatre points suivants :

$A(0, 2, 1)$	$B(2, 3, 3)$	$C(4, 1, 2)$	$D(2, 0, 0)$

Les quatre vecteurs sont alors

$\overrightarrow{AB}\begin{pmatrix}2\\1\\2\end{pmatrix}$	$\overrightarrow{BC}\begin{pmatrix}2\\-2\\-1\end{pmatrix}$	$\overrightarrow{CD}\begin{pmatrix}-2\\-1\\-2\end{pmatrix}$	$\overrightarrow{DA}\begin{pmatrix}-2\\2\\1\end{pmatrix}$

On a $\overrightarrow{AB} = -\overrightarrow{CD}$: on a un parallélogramme.
On a aussi $\overrightarrow{AB} \perp \overrightarrow{BC}$: on a un rectangle.
On a enfin $|\overrightarrow{AB}| = |\overrightarrow{BC}|$: on a un carré.
Mais il faudrait justement des vecteurs deux à deux orthogonaux, de même norme, pas trop longs pour qu'on ne sorte pas du cube. On pourrait par exemple prendre le modèle ci dessus, mais il nous fait déborder du cube 3 sur 3 à cause des 2 qui s'additionnent.

◃ 28 ▹

Montrez que ce sont des sous-groupes de $(\mathbb{R}, +)$:

$\mathbb{Z}$	$\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\ b) \in \mathbb{Z}^2\right\}$	$\left\{\frac{a}{7}+\frac{2.b}{5}+c \mid (a,\ b,\ c) \in \mathbb{Z}^3\right\}$	$\left\{a.\sqrt{4}+b.\sqrt{25} \mid (a,\ b) \in \mathbb{Z}^2\right\}$
$\mathbb{Q}$	$\left\{a+\sqrt{2}.b \mid (a,\ b) \in \mathbb{Z}^2\right\}$	$\left\{a+\sqrt{2}.b+c.\sqrt{3} \mid (a,\ b,\ c) \in \mathbb{Z}^2\right\}$	

Lesquels peuvent s'écrire sous la forme $\{a.p \mid p \in \mathbb{Z}\}$ pour au moins un réel a bien choisi ?

Les inclusions dans $\mathbb{R}$ sont acquises.

Le neutre est présent en prnant $a = b = 0$ ou $a = b = c = 0$.

La stabilité s'écrit par exemple $\frac{a}{7}+\frac{2.b}{5}+\frac{a'}{7}+\frac{2.b'}{5}=\frac{a+a'}{7}+\frac{2.(b+b')}{5}$.

Le passage au symétrique repose sur le fait qu'on peut passer d'un couple $(a,\ b)$ à un couple $(-a,\ -b)$ tout aussi dans $\mathbb{Z}^2$.

$\mathbb{Z} = 1.\mathbb{Z}$	$\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\ b) \in \mathbb{Z}^2\right\} = \frac{1}{35}.\mathbb{Z}$	$\left\{\frac{a}{7}+\frac{2.b}{5}+c \mid (a,\ b,\ c) \in \mathbb{Z}^3\right\} = \frac{1}{35}.\mathbb{Z}$	$\left\{a.\sqrt{4}+b.\sqrt{25} \mid (a,\ b) \in \mathbb{Z}^2\right\} = 1.\mathbb{Z}$

Comment prouver $\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\ b) \in \mathbb{Z}^2\right\} = \frac{1}{35}.\mathbb{Z}$?
Par double inclusion.
Tous les éléments de la forme $\frac{a}{7}+\frac{2.b}{5}$ sont en fait des $\frac{k}{35}$ avec k de la forme $5.a + 14.b$.
Tout élément de la forme $\frac{k}{35}$ avec k entier sont de la forme $\frac{5.a+14.b}{35}$ en écrivant $k = 5.a + 14.b$ avec a et b bien choisis. C'est Bézout qui le dit : $5.\mathbb{Z} + 14.\mathbb{Z} = \mathbb{Z}$.

L'ensemble $\left\{\frac{a}{7}+\frac{2.b}{5}+c \mid (a,\ b,\ c) \in \mathbb{Z}^3\right\}$ est inclus dans $\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\ b) \in \mathbb{Z}^2\right\}$
En effet, chaque $\frac{a}{7}+\frac{2.b}{5}+c$ s'écrit aussi $\frac{a+7.c}{7}+\frac{2.b}{5}$.

L'ensemble $\left\{\frac{a}{7}+\frac{2.b}{5} \mid (a,\ b) \in \mathbb{Z}^2\right\}$ est inclus dans $\left\{\frac{a}{7}+\frac{2.b}{5}+c \mid (a,\ b,\ c) \in \mathbb{Z}^3\right\}$
En effet, chaque $\frac{a}{7}+\frac{2.b}{5}$ s'écrit aussi $\frac{a+7.c}{7}+\frac{2.b}{5}+0$.

L'ensemble d'écriture étrange $\left\{a.\sqrt{4}+b.\sqrt{25} \mid (a,\ b) \in \mathbb{Z}^2\right\}$ est $2.\mathbb{Z} + 5.\mathbb{Z}$. Et c'est $\mathbb{Z}$ puisque 2 et 5 sont premiers entre eux.

$\mathbb{Q}$	$\left\{a+\sqrt{2}.b \mid (a,\ b) \in \mathbb{Z}^2\right\}$	$\left\{a+\sqrt{2}.b+c.\sqrt{3} \mid (a,\ b,\ c) \in \mathbb{Z}^2\right\}$	

Aucun de ces ensembles ne peut s'écrire $\{a.k \mid k \in \mathbb{Z}\}$.
Un ensemble de la forme $a.\mathbb{Z}$ cotient « le premier élément après 0 » (et c'est a).
Or, dans $\mathbb{Q}$ il n'y a pas de plus petit rationnel strictement positif.

Une jolie preuve par l'absurde pour $\left\{a+\sqrt{2}.b \mid (a,\ b) \in \mathbb{Z}^2\right\}$.
Supposons qu'il soit de la forme $\{k.\alpha \mid k \in \mathbb{Z}\}$ pour un α bien choisi (« générateur de l'ensemble).
Alors $1+\sqrt{2}.b$ est dans cet ensemble, et s'écrit donc $p.\alpha$ pour un entier p bien choisi.
De même $0 + 1.\sqrt{2}$ est dans cet ensemble, et s'écrit donc $q.\alpha$ pour un entier q bien choisi.

On calcule alors $\sqrt{2}=\frac{0+1.\sqrt{2}}{1+0.\sqrt{2}}=\frac{q.\alpha}{p.\alpha}=\frac{q}{p}$.
Le réel $\sqrt{2}$ serait rationnel ! Impossible !

◁ 29 ▷ On définit sur $\mathbb{Z} \times \mathbb{Z}^*$ une relation et deux lois :

$(a,\ b)\Re(\alpha,\ \beta)$	$(a,\ b) \oplus (c,\ d)$	$(a,\ b) \otimes (c,\ d)$
si et seulement si	est égal à	est égal à
$a.\beta = b.\alpha$	$(a.d + b.c,\ b.d)$	$(a.c,\ b.d)$

Montrez que ce sont des lois internes sur $\mathbb{Z} \times \mathbb{Z}^*$, commutatives, associatives.
Donnez le neutre de chacune.
Montrez que les deux lois sont compatibles avec $\Re$ $\left.\begin{array}{c}(a,\ b)\Re(\alpha,\ \beta)\\ et\\ (c,\ d)\Re(\gamma,\ \delta)\end{array}\right\} \Rightarrow \left\{\begin{array}{c}((a,\ b) \oplus (c,\ d))\Re((\alpha,\ \beta) \oplus (\gamma, \delta))\\ et\\ ((a,\ b) \otimes (c,\ d))\Re((\alpha,\ \beta) \otimes (\gamma, \delta))\end{array}\right\}$.
Montrez que tout élément de $\mathbb{Z} \times \mathbb{Z}^*$ admet *(modulo $\Re$)* un symétrique pour l'addition *(c'est à dire pour tout q il existe q' vérifiant $q \oplus q'\Re(0,1)$)*.
Montrez que tout élément de $\mathbb{Z}^* \times \mathbb{Z}^*$ admet (modulo $\Re$) un symétrique pour la multiplication *(c'est à dire pour tout q il existe q' vérifiant $q \otimes q'\Re(1,1)$)*.
Est il vrai que la multiplication est directement distributive sur l'addition ?
Montrez que tout élément est en relation par $\Re$ avec un élément irréductible (a, b) avec a et b premiers entre eux et b positif.
Que venez vous de construire ? Était ce passionnant ?

On a construit $(\mathbb{Q}, +, .)$ à partir de $(\mathbb{Z}, +, .)$.

◁ 30 ▷ ♡ La relation « ne pas être inclus dans » est elle réflexive, symétrique, antisymétrique, transitive sur $P(\mathbb{R})$? Est elle compatible avec $\cap$? Est elle compatible avec $\cup$?

On donne des contre-exemple.

propriété	contre-exemple	justification	conclusion
Réflexive.	$A = \emptyset$	0n a $A \subset A$. On n'a donc pas $A \not\subset A$.	raté
Symétrique.	$A = \{1,\ 2\}$ et $B = \{1\}$	On a $A \not\subset B$ mais on n'a pas $B \not\subset A$.	raté
Antisymétrique.	$A = \{1\}$ et $B = \{2\}$	On a à la fois $A \not\subset B$ et $B \not\subset A$. Mais on n'a pas $A = B$.	raté
Transitive	$A = \{1]$, $B = \{2\}$, $C = \{1\}$	On a $A \not\subset B$ et $B \not\subset C$ mais on n'a pas $A \not\subset C$	raté

Elle n'a rien pour me plaire.

Peut on passer à coup sûr de $A \not\subset B$ à $A \cap C \not\subset B \cap C$?
Non : $A = \{1\}$, $B = \{2\}$ et $C = \{3\}$.

Peut on passer à coup sûr de $A \not\subset B$ à $A \cap C \not\subset B \cap C$?
Non : $A = \{1\}$, $B = \{2\}$ et $C = \{1,\ 2\}$.

Elle me plait de moins en moins.

◁ 31 ▷ Soit $(G, *)$ un groupe à onze éléments, et a un élément de G différent du neutre e. Montrez, en étudiant $p \longmapsto a^p$ de $\mathbb{N}$ dans G qu'il existe deux exposants p et q distincts vérifiant $a^p = a^q$ *(a^p désigne $a * a * \ldots a$ p fois)*. Déduisez qu'il existe r dans $\mathbb{N}^*$ vérifiant $a^r = e$.
Déduisez que a^{-1} *(inverse de a)* est une puissance de a. Montrez qu'il existe même r dans $\mathbb{N}^*$ vérifiant $a^r = e$ et $a^k \neq e$ pour tout k de 1 à $r - 1$.
Quel est alors le cardinal de $\{a^k \mid 0 \leqslant k < r\}$ *(noté A)* et montrez que cette partie est un sous-groupe de $(G, *)$.
On définit sur G le relation $\bowtie$ par $(x \bowtie y) \Leftrightarrow (\exists k \in \mathbb{N},\ y = x * a^k)$. Montrez que c'est une relation d'équivalence.
On suppose qu'il y a un élément b de G qui n'est pas dans A. Montrez qu'alors $\{b * a^k \mid 0 \leqslant k < r\}$ *(noté B)* a le même cardinal que A et aucun élément en commun avec A.
On suppose qu'il y a un élément c de G qui n'est ni dans A ni dans B. Montrez qu'alors $\{c * a^k \mid 0 \leqslant k < r\}$ *(noté C)* a le même cardinal que A et aucun élément en commun avec A ni avec B.
En notant que l'on "tranche" G en parties ayant toutes le même cardinal, concluez que le cardinal de A vaut 1 ou 11 *(mais on a déjà éliminé 1)*.
Concluez que G est égal à A et est commutatif.
Par quoi pouvez vous remplacer 11 ?

Tout groupe de cardinal premier est engendré par un élément. Et il est donc forcément commutatif.
C'est ce qu'on va prouver ici.

On s'est donné a.. Par stabilité du groupe (= « loi interne »), les éléments a, $a * a$, $a * a * a$ et ainsi de suite sont tous dans G.
Mais G est un ensemble fini.
On est donc obligé de retomber au bout d'un moment sur un élément déjà pris.

Proprement, si tous les a^n étaient différents, la liste $[a,\ a^2,\ a^3, \dots a^{12}]$ serait faite de douze éléments distincts de G, ce qui n'est pas possible.

Il existe donc deux indices distincts p et q vérifiant $a^p = a^q$.

Par symétrie des rôles, on va supposer $p < q$. On a donc $a * a * a \dots * a = a * a * \dots * a * \dots a$ avec p éléments d'un côté et q de l'autre.
On simplifie par a de chaque côté (en composant par a^{-1} qui existe puisqu'on est dans un groupe).
Quitte à avoir même posée $q = p + r$, on simplifie p fois de suite par a.
Il reste e du côté gauche (le neutre), et a^r de l'autre.

On a donc obtenu $a^r = e$ (avec r strictement positif, sachant que par convention naturelle on avait déjà $a^0 = e$).

On a $a * a * a \dots * a = e$ (avec r termes). On en met un de côté :
$a * a^{r-1} = a^{r-1} * a = e$.
On reconnaît la définition du symétrique de a. Et c'est donc a^{r-1} qui tient ce rôle.

> *Prenons un exemple avec les entiers de* 0 *à* 10 *pour l'addition modulo* 11 *(la loi* $*$ *est donc l'addition).*
> *On part de* 3 *et on calcule ses « puissances » successives :* $3, 3*3 = 6, 3*3*3 = 9, 3*3*3*3 = 1, 3*3*3*3*3 = 4,$ $3*3*3*3*3*3 = 7, 3*3*3*3*3*3*3 = 10,$
> $3*3*3*3*3*3*3*3 = 2, 3*3*3*3*3*3*3*3*3 = 5, 3*3*3*3*3*3*3*3*3*3 = 8$ *pour l'instant toutes les valeurs sont distinctes.*
> *Mais si on continue :* $3*3*3*3*3*3*3*3*3*3*3 = 0$ *et* $3*3*3*3*3*3*3*3*3*3*3*3 = 3$.
> *On vient de retrouver un élément déjà présent dans la liste.*
> *On a donc* $3 = 3*3*3*3*3*3*3*3*3*3*3*3*3 = 3$.
> *On simplifie :* $0 = 3*3*3*3*3*3*3*3*3*3*3*3*3*3$ *(on le savait, mais bon...).*
> *On déduit que le symétrique de* 3 *est* $3*3*3*3*3*3*3*3*3*3*3*3$ *(avec un terme de moins).*

A ce stade, il existe un entier r vérifiant $a^r = e$. Mais est ce le plus petit ?
Pas forécement. Mais si on regarde l'ensemble $\{q \in \mathbb{N}^* \mid a^q = e\}$, c'est une partie de $\mathbb{N}^*$ non vide (on y a trouvé un r).
Il suffit de prendre ensuite le plus petit élément de cet ensemble (vous auriez dit « prenons le premier r tel que $a^r = e$, mais auriez vous pensé à dire qu'il en existait au moins un ?).
En tant que premier, il vérifie $a^r = e$. Et comme il n'y en a pas avant, on a $a^k \neq e$ pour tout k entre 1 et $r - 1$.

Les élémentsa^k avec k entre 1 et r sont différents de e.
Mais sont ils tous différents entre eux ?

Si tel est le cas, la liste $[a^0,\ a^1,\ a^2, \dots a^{r-1}]$ sera faite de r éléments distincts.

Et justement, si pour deux d'entre eux, p et q (avec $0 \leqslant p < q < r$ par symétrie des rôles) on avait $a^p = a^q$, on aurait $a^{q-p} = e$ avec $q - p$ entre 1 et $r - 1$ ce qui est contradictoire.

L'ensemble $\{a^0,\ a^1,\ a^2, \dots a^{r-1}\}$ contient donc bien r éléments exactement.

> *r est appelé « ordre de a », et l'ensemble $\{a^0,\ a^1,\ a^2, \dots a^{r-1}\}$ est un sous-groupe de $(G, *)$. C'est même le plus petit sous-groupe de $(G, *)$ contenant a.*
> *On l'appelle sous-groupe engendré par a.*
> *Si le grupe $(G, *)$ est celui des entiers de* 0 *à* 11 *pour l'addition modulo* 12 *(donc à* 12 *éléments attention), le sous groupe engendré par* 0 *est* $\{0\}$, *le sous groupe engendré par* 1 *est* $\{0, 1, 2, 3, \dots 11\}$. *Le sous-groupe engendré par* 2 *est* $\{0, 2, 4, 6, 8, 10\}$. *le sous groupe engdneré par* 3 *est* $\{0, 3, 6, 9\}$. *Celui engendré par* 4 *est* $\{0, 4, 8\}$. *mais celui engendré par* 5 *reprand tous les entiers de* 0 *à* 11 *(dans l'ordre* $[0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7]$ *si vous y tenez. Et si vous avez deviné, tout va dépendre de « a et* 12 *sont ils premiers entre eux ? ».*

On va ensuite construire la relation d'équivalence « modulo ce sous-groupe ».
On se donne x, y et z (histoire de tout quantifier).

•$_R$ On vérifie $x \bowtie x$. E, effet $(\exists k \in \mathbb{N},\ x = x * a^k)$, il suffit de prendre $k = 0$ (ou r).

•$_S$ On suppose $(x \bowtie y)$. On traduit $(\exists k \in \mathbb{N},\ y = x * a^k)$. Quitte à réduire modulo r, on peut supposer $0 \leqslant k < r$.
On a alors $(y * a^{(r-k)} = x * a^k * a^{r-k} = x)$. On a l'entier $r - k$ qui vérifie $(x = y.a^{r-k})$. On reconnaît $y \bowtie x$.

$\bullet_T$ On suppose à la fois $x \bowtie y$ et $y \bowtie x$. On traduit : $(\exists k \in \mathbb{N},\ y = x * a^k)$ et $(\exists k' \in \mathbb{N},\ z = y * a^{k'})$.
On enchasse $(\exists q \in \mathbb{N},\ z = x * a^q)$ avec tout simplement $q = k + k'$.
On reconnaît $x \bowtie z$.

La relation est réflexive, symétrique et transitivie, c'est une relation d'équivalence et elle va permettre de découper G en tranches.

> *L'erreur sur ce type de question des élèves sans compréhension mathémtique.*
> *Vouloir passer de* $(\exists k \in \mathbb{N},\ y = x * a^k)$ *et* $(\exists k \in \mathbb{N},\ z = y * a^k)$ *à* $(\exists k \in \mathbb{N},\ z = x * a^k)$*, sans comprendre que* $\exists k$ *signifie qu'il existe au moins un k mais qu'il doit changer à chaque fois qu'on change de x et de y.*
> *Bref, un problème fondamental de variables.*
> *Donc de maths.*

Combien d'éléments dans chaque classe d'équivalence ?
Dans la classe d'équivalence de x, il y a tous les y s'écrivant $y = x * a^k$ pour k dans $\mathbb{N}$.
Mais en fait, k va juste de 0 (inclus) à r (exclu), puisqu'ensuite, ce snt les mêmes valeurs qui reviennent.
Et les r éléments de la forme $x * a^k$ sont tous distincts.

> *Si on avait* $x * a^k = x * a^p$ *on aurait* $a^k = a^p$ *en composant par le symétrique de x, puis* $a^{k-p} = e$ *et donc* $k - p = 0$*.*

On a découpé G en classes d'équivalance (disons qu'il y en a c), toutes de même cardinal r.
Comme elles forment une partition, on a $Card(G) = c \times r$ (nombre de classes fois cardinal de chacune).

Mais comme $Card(G)$ est un nombre premier [4], on déduit que c vaut 1 et r vaut 11.

> *La solution* $c = 11$ *et* $r = 1$ *donne* $x = e$ *qu'on a refusé de prendre.*

Il n'y a donc qu'une classe. Et comme le neutre est dans une d'entre elles, on peut dire que cette classe est celle de e.

> *Au fait, avez vous reconnu ici la démonstration du théorème de Lagrange : le cardinal d'un sous-groupe divise le cardinal du groupe.*
> *Et ici, comme le cardinal du groupe est premier, àa ne nous laisse que deux sous groupes possibles : le neutre tout seul (cardinal* 1*), le groupe tout entier (cardinal* 11*).*

On a donc finalement

$$G = classe\ de\ e = \{e * a^k \mid k \in \mathbb{N}\} = \{e * a^k \mid 0 \leqslant k < r\}$$

Notre groupe de cardinal premier est donc de la forme « les puissances d'un quelconque de ses éléments, autre que le neutre ».

On appelle ceci un groupe monogène (engendré par un élément).
Et en tant qu'ensemble des a^k, il est commutatif : $x * y = a^k * a^p = a^{k+p} = a^{p+k} = a\hat{}p * a\hat{}k = y * x$
Bilan : tout groupe de cardianl p premier est monogène et donc forcément commutatif.

> *Il n'y aura donc qu'un modèle de groupe de cardinal* 2*. De même, un seule modèle de groupe de cardinal* 3*. De même pour* 5 *et* 7*. Et à chaque fois, ils sont commutatifs.*
> *En revanche, on peut construire un groupe de cardinal* 4 *qui n'est pas monogène. Mais il est commutatif.*
> *Et pour un cardinal* 6*, le groupe* $(S_3, \circ)$ *est un groupe ni monogène, ni commutatif.*
> *Je vous laisse chercher les groupes de cardianl* 8 *puis* 9 *et* 10*.*
> *On notera qu'un groupe de cardinal* 10 *peut contenir des sous groupes (commutatifs) de cardinal* 2 *et de cardinal* 5*.*
> *Il y a plein de choses passionnantes là dessus, mas patience.*

◁ 32 ▷ Combien le groupe $(\mathbb{Z}_{48.\mathbb{Z}}, +)$ a-t-il de sous-groupes ?

♡ Pour tout groupe $(G, *)$, on note Z l'ensemble $\{a \in G \mid \forall b \in G,\ a * b = b * a\}$. Montrez que Z est égal à G si et seulement si $(G, *)$ est commutatif. Montrez que Z est un sous-groupe de $(G, *)$.

Z est ce que l'on appelle le centre » du groupe G.

4. oui, je vends la èche, on peut remplacer 11 par n'importe quel nombre premier

Z est égal à G si et seulement si tous les a de G sont dans Z, ce qui revient à dire $\forall a \in G,\ \forall b \in G,\ a * b = b * a$.

Les éléments de Z sont ceux qui « commutent avec tout le monde ».
Par définition, ce sont des éléments de G.

Le neutre est dans Z.

On prend a et α dans G (on traduit : $\begin{array}{l}\forall b \in G,\ a * b = b * a\\ \forall b \in G,\ \alpha * b = b * \alpha\end{array}$).
On veut savoir si $a * \alpha$ est dans G.
On se donne b quelconque, et on calcule $(a * \alpha) * b$ et $b * (a * \alpha)$: sont ils égaux :

$(a * \alpha) * b = a * (\alpha * b)$ par associativité
$(a * \alpha) * b = a * (b * \alpha)$ car α est dans Z
$(a * \alpha) * b = (a * b) * \alpha$ par associativité
$(a * \alpha) * b = (b * a) * \alpha$ car a est dans Z
$(a * \alpha) * b = b * (a * \alpha)$

On reconnaît que $a * \alpha$ est dans Z.

On se donne a dans G (on traduit : $\forall b \in G,\ a * b = b * a$).
On s'interroge : a^{-1} (dont l'existence est assurée car on est dans G) est il dans Z.
On se donne b quelconque et on veut comparer $a^{-1} * b$ et $b * a^{-1}$.
On prend l'initiative de partir de $a * b = b * a$
et de multiplier à droite et à gauche par a^{-1} :
$a^{-1} * (a * b) * a^{-1} = a^{-1} * (b * a) * a^{-1}$
on simplifie par associativité $(a^{-1} * a) * b * a^{-1} = a^{-1} * b * (a * a^{-1})$
et c'est pile poil ce que l'on voulait

Remarque :
Un type d'exercice qui peut être fatal.
Il est hyper simple, il demande juste à ce que vous posiez correctement vos variables et surtout vos questions.
Mais il montre si vous avez compris ou non.

Il n'y a aucune connaissance encyclopédique, aucune capacité à calculer vite bien, à sortir le bon théorème au bon moment, à avoir appris par couer trente huit méthodes et quatre cent trente sept exercices du livre.

Juste la question « savez vous raisonner ». Et c'est terrible de s'entendre dire « non ».

Ou pour le moins « pas encore, car tu n'as pas passé le cap de tes blocages ».

◃ 33 ▹ **Quel est le plus petit sous groupe de $(range(2019), +_{mod\ 2019})$ contenant 51 ?**

Raisonnons déjà par conditions nécessaires pour commencer.

Si un sous-groupe de $(range(2019), +_{mod\ 2019})$ contient 51, il contient $51 + 51$, $51 + 51 + 51$ et ainsi de suite.
Il contient tous les multiples de 51. Jusqu'à 2040. On réduit : 21 est dans le sous-groupe.

Le sous-groupe contient 51 et 21, il contient leur différence : 30.

Il contient 30 et 21, il contient leur différence : 9.

Il contient 9, 18 et 21, il contient 3.Et l'algorithme d'Euclide s'arrête ici (car c'est bien lui !).

Le sous groupe contient 3, il contient tous ses multiples.

Et si on s'arrêtait là ? Et si on passait à la condition suffisante ?

L'ensemble $\{3.k \mid k\ in\ range(673)\}$ est une partie de 2019, contenant 0.
Elle est stable par addition. La somme de deux multiples de 3 reste un multiple de 3, même quand on la réduit modulo 3×673.
Et l'opposé de $3.k$ est $(673 - k).3$, c'est encore un multiple de 3.

Remarque : puis-je sanctionner l'élève qui se contentera de répondre $\{(51.k) \bmod 2019 \mid k \text{ in } range(2019)\}$

◁ 34 ▷ On prend l'ensemble des entiers de 1 à 28 pour la multiplication modulo 29 *(on rappelle que c'est un groupe, donnez la liste des inverses si vous en avez le courage)*. ?
Montrez que $\{7^k \mid 0 \leqslant k \leqslant 6\}$ en est un sous-groupe. Est-ce encore le cas pour $\{2^k \mid 0 \leqslant k \leqslant 6\}$?
Montrez que $\{12^k \mid 0 \leqslant k \leqslant 3\}$ en est un sous-groupe. Est-ce encore le cas pour $\{2^k \mid 0 \leqslant k \leqslant 3\}$?
Montrez que $\{5^k \mid 0 \leqslant k \leqslant 13\}$ en est un sous-groupe. Est-ce encore le cas pour $\{2^k \mid 0 \leqslant k \leqslant 13\}$?
Bon, quelle valeur de q faut il prendre pour que $\{2^k \mid 0 \leqslant k \leqslant q\}$ soit un sous-groupe de l'ensemble initial ?
Quelle est la probabilité que vous ayez eu envie de traiter cet exercice si vous avez le profil à aller en P.S.I. avec ou sans étoile

A faire.

◁ 35 ▷ Trouvez le reste (et juste le reste) de la division euclidienne de $X^n + 1$ par $X^2 - 3.X + 2$, en donnant à X des valeurs particulières bien choisies.

On imagine la division :

$$X^n + 1 = (X^2 - 3.X + 2).Q(X) + a.X + b$$

avec a et b à déterminer. On calcule en 1 et en 2 :

$$1^n + 1 = (1^2 - 3.1 + 2).Q(1) + a + b,\ 2^n + 1 = (2^2 - 3.2 + 2).Q(2) + 2.a + b$$

On trouve un petit système rapide à résoudre : $\left\{ \begin{array}{rcrcl} a & + & b & = & 2 \\ 2.a & + & b & = & 2^n + 1 \end{array} \right|$.
Sans effort : $a = 2^n - 1$ et $b = 3 - 2^n$. On écrit la formule définitive

$$X^n + 1 = (X^2 - 3.X + 2).Q(X) + (2^n - 1).X + 3 - 2^n$$

On vérifie pour n égal à 0 *:* $1 + 1 = (X^2 - 3.X + 2).0 + (1 - 1).X + 3 - 1$ *et* $X + 1 = (X^2 - 3.X + 2).0 + (2 - 1).X + 3 - 2$

Autre approche :

$$\frac{X^n + 1}{(X-1).(X-2)} = Q(X) + \frac{\alpha}{X-1} + \frac{\beta}{X-2}$$

et on calcule α et β par la méthode des pôles

$$\frac{X^n + 1}{(X-1).(X-2)} = Q(X) + \frac{2}{X-1} + \frac{2^n + 1}{X-2}$$

$$\frac{X^n + 1}{(X-1).(X-2)} = Q(X) + \frac{2.(X-2) + (2^n + 1).(X-1)}{(X-1).(X-2)}$$

Il ne reste plus qu'à multiplier par $X^2 - 3.X + 2$.

◁ 36 ▷ ♠ On pose $A = \begin{pmatrix} 0 & 2 & -1 \\ -1 & 3 & -1 \\ -1 & 2 & 0 \end{pmatrix}$. Calculez son polynôme caractéristique.
Montrez que A n'admet qu'une valeur propre, que l'on déterminera.
A est elle diagonalisable ?
Trouvez un polynôme P de degré le plus petit possible *(mais quand même non nul)* vérifiant $P(A) = 0_{M_2(\mathbb{R})}$.
Déterminez pour tout n donné le reste de la division euclidienne de X^n par $(X-1)^2$.
Déduisez la forme de A^n.

◃ 37 ▹ ♠ On pose $A = \begin{pmatrix} 9 & -15 & -4 \\ 6 & -11 & -3 \\ -2 & 6 & 2 \end{pmatrix}$. Calculez la trace et le déterminant de A. Complétez : $A^3 = Tr(A).A^2 + \ldots A + \det(A).I_3$.
Donnez les racines du polynômes $X^3 - 3.X + 2$.
On note R_n le reste de la division euclidienne de X^n par $X^2 - 3.X + 3$ (caractérisé par $X^n = (X^3 - 3.X + 2).Q_n(X) + R_n(X)$). Calculez $R_n(1)$ et $R_n(-2)$.
Calculez aussi $R_n'(1)$. Déduisez la forme de $R_n(X)$. Indiquez comment terminer pour obtenir A^n.
♣ Un élève prétend que A est semblable à $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$. Montrez qu'effectivement ces deux matrices ont même trace, même déterminant. Montrez aussi $Tr(A^2) = Tr(D^2)$, et même $Tr(A^n) = Tr(D^n)$. Mais un autre élève explique que si A et D étaient semblables, alors les trois colonnes de $A - I_3$ devraient être proportionnelles. Concluez qu'effectivement A n'est pas diagonalisable.

A faire.

◃ 38 ▹ ♡ J'ai appliqué l'algorithme d'Euclide à deux polynômes $A(X)$ et $B(X)$. Les quotients sont dans l'ordre $X^2 + 1$, $X + 2$ et $X + 1$. Le dernier reste non nul est $X - 3$. Pouvez vous retrouver A et B ?

On a une suite de divisions :
$$\begin{array}{rcll} A(X) & = & B(X) & .(X^2+1) \quad +R_1(X) \\ B(X) & = & R_1(X) & .(X+2) \quad +R_2(X) \\ R_1(X) & = & R_2(X) & .(X+1) \end{array}.$$
Le dernier reste non nul est $X - 3$. C'est lui $R_2(X)$. On trouve donc R_1 par la dernière ligne : $R_1 = X^2 - X - 6$.
On retrouve $B(X)$ par la précédente : $X^3 + X^2 - 7.X - 15$.
Et la première donne $A(X) = X^5 + X^4 - 6.X^3 - 13.X^2 - 8.X - 21$.
On ne sait pas forcément si c'est $A(X) = X^5 + X^4 - 6.X^3 - 13.X^2 - 8.X - 21$ et $B(X) = X^3 + X^2 - 7.X - 15$ ou le contraire, mais on connaît « A et B ».

L'exercice peut être posé niveau bac, avec des entiers.

◃ 39 ▹ ♡ En appliquant l'algorithme d'Euclide, j'ai trouvé les quotients successifs
1, 34, 2, 2, 2, 1 et 2
et le dernier reste non nul valait 3. Qui étaient les deux nombres initiaux ?
Même question, avec le même dernier reste et pour quotients 0, 4, 1, 1, 30 et 11.

◃ 40 ▹ ♡ Déterminez le p.g.c.d. de 2^{2015} et 2^{531}.
Déterminez le p.g.c.d. de 2^{2015} et $2^{2015} - 1$.
Déterminez le p.g.c.d. de $2^{2015} - 1$ et $2^{531} - 1$ (divisions euclidiennes successives ?)

Les diviseurs de 2^{2015} et 2^{531} ne sont que des 2^k et le plus grand est 2^{531} lui même.
D'ailleurs, dès que l'un est multiple de l'autre, leur p.g.c.d. est le plus petit des deux !

Si un nombre divise 2^{2015} et $2^{2015} - 1$, il divise leur différence et ne peut valoir que 1.
Le plus grand diviseur commun et même unique diviseur de 2^{2015} et $2^{2015} - 1$ est 1.

On commence (parce qu'on connaît la réponse) par écrire un algorithme d'Euclide sur les exposants :
$$\begin{array}{rcrll} 2015 & = & 3 & \times 531 & +42 \\ 531 & = & 1 & \times 422 & +10 \\ 422 & = & 3 & \times 109 & +9 \\ 109 & = & 1 & \times 95 & +1 \\ 95 & = & 6 & \times 14 & +1 \\ 14 & = & 1 & \times 11 & +3 \\ 11 & = & 3 & \times 3 & +2 \\ 3 & = & 1 & \times 2 & +1 \\ 2 & = & 2 & \times 1 & \end{array}$$
On écrit alors $2^{2015} - 1 = 2^{3.531+422} - 1$
$2^{2015} - 1 = 2^{3.531+422} - 2^{422} + 2^{422} - 1$
$2^{2015} - 1 = (2^{3.531} - 1).2^{422} + 2^{422} - 1$
$2^{2015} - 1 = (2^{531} - 1).(2^{2.531} + 2^{531} + 1) + 2^{422} - 1$ (formule $a^3 - 1 = (a-1).(a^2 + a + 1)$)
On a une formule du type $2^{2015} - 1 = (2^{531} - 1).Q + 2^{422} - 1$.
Ceci prouve que tout nombre qui divise $2^{2015} - 1$ et $2^{531} - 1$ devra diviser $2^{531} - 1$ (évidemment) et $2^{422} - 1$.
Et que tout nombre qui diviser $2^{531} - 1$ et $2^{422} - 1$ devra diviser $2^{2015} - 1$ et $2^{531} - 1$.

En notant $DC(a,b)$ l'ensemble des diviseurs communs de a et b, on a $DC(2^{2015}-1,\ 2^{531}-1) = DC(2^{531}-1,\ 2^{422}-1)$.
Et parmi ces diviseurs communs, il y a le plus petit : $pgcd(2^{2015}-1,\ 2^{531}-1) = pgcd(2^{531}-1,\ 2^{422}-1)$.

On recommence avec $2^{531}-1 = 2^{1.422+109}-1$
$2^{531}-1 = 2^{1.422+109} - 2^{109} + 2^{109} - 1$
$2^{531}-1 = (2^{422}-1).2^{109} + 2^{109} - 1$
Cette fois, tout diviseur de $2^{531}-1$ et $2^{422}-1$ est un diviseur de $2^{422}-1$ et $2^{109}-1$ (et vice versa).
On a donc cette fois $DC(2^{2015}-1,\ 2^{531}-1) = DC(2^{531}-1,\ 2^{422}-1) = DC(2^{422}-1,\ 2^{109}-1)$.

On en refait une : $2^{95}-1 = 2^{6.14+11}-1$
$2^{95}-1 = 2^{6.14+11} - 2^{11} + 2^{11} - 1$
$2^{95}-1 = (2^{6.14}-1).2^{11} + 2^{11} - 1$
$2^{95}-1 = (2^{14}-1).(2^{14.5} + 2^{14.4} + 2^{14.3} + 2^{14.2} + 2^{14} + 1) + 2^{11} - 1$ (formule $a^6 - 1 = (a-1).(a^5 + \ldots + a + 1)$)
Ceci nous donne $DC(2^{95}-1,\ 2^{14}-1) = DC(2^{14}-1,\ 2^{11}-1)$.

En mettant tout bout à bout : $DC(2^{2015}-1,\ 2^{531}-1) = DC(2^{531}-1,\ 2^{422}-1) = DC(2^{422}-1,\ 2^{109}-1) = \ldots = DC(2^3-1,\ 2^2-1)$.
Et parmi tous ces diviseurs communs, il y a le p.g.c.d.
Et il vaut 1.

Généralisation : si a et b sont premiers entre eux, alors 2^a-1 et 2^b-1 sont premiers entre eux.

◁ 41 ▷

♣ J'ai calculé tous les restes des divisions euclidiennes de 2018 par les entiers de 1 à 2018 (`[2018%k for k in range(1, 2019)]`). Quel est le plus petit obtenu ? Quel est le plus grand obtenu.
Ça se traite sans Python.

0 est dans la liste, c'est 2018 % 2018.
Mais même 2018 % 1 ou 2018 % 2.

Le maximum est atteint pour 1010 et il vaut 1008.
On a en effet $2018 = 1 \times 1010 + 1008$. Donc la valeur est atteinte (milieu de liste).

Pour k plus petit que 1009, le reste est inférieur ou égal à k, et ne peut donc pas atteindre 1008.
Pour k plus grand que 1009, le quotient vaut 1 et le reste vaut $2018-k$, et il ne peut plus atteindre 1008.

◁ 42 ▷

♡ Donnez le *p.g.c.d.* de 1 234 et 4 321, et donnez une identité de Bézout.
Donnez le *p.g.c.d.* de 12 345 et 54 321, et donnez une identité de Bézout.

1234 et 4321 sont premiers entre eux, et on a $-1082 \times 1234 + 309 \times 4321 = 1$.

12345 et 54321 ont pour diviseur commun 3 (et c'est tout[5])
Et on a $3617 \times 12345 - 822 \times 54321 = 3$.

◁ 43 ▷

♡ Donnez une identité de Bézout entre 270 et 105 dont un coefficient soit plus grand que 1000.

On en trouve déjà une :

$$\begin{array}{rcrrr} 270 &=& 105 &\times 2& +60 \\ 105 &=& 60 &\times 1& +45 \\ 60 &=& 45 &\times 1& +15 \\ 45 &=& 15 &\times 3& \end{array}$$

on remonte

$$\begin{array}{rcll} 15 &=& 60 & -45 \\ 15 &=& 60 & -(105-60) \\ 15 &=& 2\times 60 & -105 \\ 15 &=& 2\times(270-105\times 2) & -105 \\ 15 &=& 2\times 270 & -5\times 105 \end{array}$$

Cette décomposition n'est pas valide, car les coefficients sont « petits ».
Mais on en trouve d'autres : $15 = (2+105.k)\times 270 - (5+270.k)\times 105$
Reste à prendre k égal à 4 par exemple.

Si vous les vouliez toutes $15 = (2+7.k)\times 270 - (5+18.k)\times 105$

5. pardon, il y a aussi 1

◃44▹ Combien y a-t-il d'entiers entre 1 et 2020 dont le p.g.c.d. avec 2020 est 2 ?
Combien y a-t-il d'entiers entre 1 et 2020 dont le p.g.c.d. avec 2020 est 10 ?

De tels entiers doivent être pairs.
Mais pas multiples de 4 sinon le p.g.c.d. vaudrait 4 (dans 2020 il y a un 4).
Pour l'instant, en gros, un quart des entiers.
Mais il faut éliminer aussi les multiples de 5, sinon le p.g.c.d. vaudrait 10.
Et les multiples de 101.

Mais il ne faut pas pousser. Il ne faux pas par exemple décompter deux fois 1010 qui est multiple de 2, de 5 et de 101.

Et pour les flemmards :

```
def pgcd(a, b) :
....while b != 0 :
........a, b = b a%b
....return a
#plus classique que ça, tu meurs...
```

```
C = 0
for k in range(1, 2021) :
....C += int(pgcd(k,2020)==2)
print(C)
```

Réponse : 400.

Et pour un p.g.c.d. de10 : il y en a cent.

◃45▹ Le théorème de *Be*$\mathbb{Z}$*out* c'est $\forall (a,b) \in \mathbb{Z}^2,\ \Big((\exists (u,\ v) \in \mathbb{Z}^2,\ a.u + b.v = 1) \Leftrightarrow (a \wedge b = 1)\Big)$.
Mais on a aussi *Be*$\mathbb{N}$*out* et *Be*$\mathbb{Q}$*out* $\forall (a,b) \in \mathbb{N}^2,\ \Big((\exists (u,\ v) \in \mathbb{N}^2,\ a.u + b.v = 1) \Leftrightarrow (Be\mathbb{N}out)\Big)$
$\forall (a,b) \in \mathbb{Z},\ \Big((\exists (u,\ v) \in \mathbb{Q}^2,\ a.u + b.v = 1) \Leftrightarrow (Be\mathbb{Q}out)\Big)$

Dans $\mathbb{N}$, si on a $\exists (u,\ v) \in \mathbb{N}^2,\ a.u + b.v = 1$, on n'a guère le choix.
Comme les entiers valent au moins 0 et ensuite 1,
la seule façon d'avoir 1 est d'avoir $a = u = 1$ et $b = 0$ ou $v = 0$.
ou $b = v = 1$ et $a = 0$ ou $u = 0$
Bref, l'un des deux vaut 1 et l'autre vaut ce qu'il veut.

Avec des coefficients dans $\mathbb{Q}$, il me semble que tout couple d'entiers vérifie le théorème de Be$\mathbb{Q}$out.
Il suffit, pour a et b donnés, d'écrire $a.\dfrac{1}{a} + b.0 = 1$ si a est non nul
$a.0 + b.\dfrac{1}{b} = 1$ si b est non nul
Et si a et b sont nuls, impossible d'avoir $a.u + b.v = 1$.

◃46▹ Peut on trouver trois entiers naturels a, b et c vérifiant le système $a \wedge b = 12$ (p.g.c.d.), $b \vee c = 120$ (p.p.c.m.) et $c \wedge a = 5$?

La formule $a \wedge b = 12$ (le plus grand diviseur commun de a et b est 12) nous dit que a et b sont des multiples de 12.
b est de la forme $12.\beta$ avec β entier.
Mais 120 est un multiple commun de b et c.
C'est donc que b est un diviseur de 120, en même temps que multiple de 12.
b peut valoir 12, 24, 60 ou 120.

Mais en plus, a et c sont multiples de 5 (à cause de $c \wedge a = 5$).
Et a est multiple de 12. Il est donc multiple de 60.
b ne peut valoir 60 ou 120. Sinon, le *p.g.c.d.* de a et b ne serait plus 12 mais 60 (ou 120).

Prenons $b = 12$. c doit contenir un facteur 10 pour avoir $b \vee c = 120$. Mais alors le p.g.c.d. de a et c ne vaut plus 5 mais 10.

Prenons $b = 24$. c doit contenir un facteur 5, comme a.
Le triplet $(60,\ 24,\ 5)$ convient.

◃47▹ On veut résoudre $(p.g.c.d.(a,\ b))^2 + a.b = 101$. Montrez que le *p.g.c.d.* vaut 1. Résolvez.
Et pour $(p.g.c.d.(a,\ b))^2 + a.b = 400$?

On note d le p.g.c.d. de a et b, et on écrit : $a = d.\alpha$ et$b = d.\beta$ avec α et β premiers entre eux.

L'équation devient $d^2 + d^2.\alpha.\beta = 101$.
d^2 divise 101. mais 101 est premier. La seule valeur possible de d est donc 1.

L'équation s'écrit alors $1 + \alpha.\beta = 101$ avec α et β premiers entre eux.
$\alpha.\beta$ vaut 100. On a des possibilités, dont on élimine celles qui donnent des entiers ayant un diviseur commun non trivial

1	2	4	5	10	symétrie des rôles
100	50	25	20	10	
oui	non	oui	non	non	

$S_{a,b} = \{(1,100),\ (100,1),\ (4,25),\ (25,4)\}$

◁ 48 ▷ Calculez le p.g.c.d. et le p.p.c.m. de $X^5 - X^4 + 2.X^3 + 1$ et de $X^5 + X^4 + 2.X^2 - 1$.
Appliquez un algorithme d'Euclide.

On ne devine pas de racines commune, on va appliquer l'algorithme d'Euclide tel qu'on le pratique sur les entiers.
Des divisions euclidiennes successives jusqu'à avoir un reste nul.
Rappel sur les entiers :

154	=	3.34	+	18	
34	=	1.18	+	16	
18	=	1.16	+	2	
16	=	8.2			
le pgcd vaut 2					

Donc ici

$(X^5 + X^4 + 2.X^2 - 1)$	=	$1 \times (X^5 - X^4 + 2.X^3 + 1)$	+	$(2.X^4 - 2.X^3 + 2.X^2 - 2)$
$(X^5 - X^4 + 2.X^2 - 1)$	=	$\left(\frac{X}{2}\right)(2.X^4 - 2.X^3 + 2.X^2 - 2)$	+	$(X^3 + X + 1)$
$(2.X^4 - 2.X^3 + 2.X^2 - 2)$	=	$(2.X - 2).(X^3 + X + 1)$	+	0
le PGCD vaut $(X^3 + X + 1)$				

Et les divisions sont

$X^5 + X^4 + 2.X^2 - 1$ | | $X^5 - X^4 + 2.X^3 + 1$ $-(X^5 - X^4 + 2.X^3 + 1)$ | | $-\ -\ -\ -\ -$ $-\ -\ -\ -\ -$ | | 1 $2.X^4 - 2.X^3 + 2.X^2 - 2$ | |	
$X^5 - X^4 + 2.X^3 + 1$ | | $2.X^4 - 2.X^3 + 2.X^2 - 2$ $-(X^5 - X^4 + X^3 - X)$ | | $-\ -\ -\ -\ -$ $-\ -\ -\ -\ -\ -$ | | $\frac{X}{2}$ $X^3 + X + 1$ | |	
$2.X^4 - 2.X^3 + 2.X^2 - 2$ | | $X^3 + X + 1$ $-(2.X^4 + 2.X^2 + 2.X)$ | | $-\ -\ -\ -$ $-\ -\ -\ -\ -$ | | $2.X - 2$ $-2.X^3 - 2.X - 2$ | | $-(2.X^3 - 2.X - 2)$ | | $-\ -\ -\ -$ | | 0 | |

Il ne reste qu'à factoriser en posant de nouvelles divisions :

$$(X^5 - X^4 + 2.X^3 + 1) = (X^3 + X + 1).(X^2 - X + 1)$$

X^5	$-X^4$	$+2.X^3$			$+1$	| |	X^3	$+X$	$+1$		
$-(X^5$		$+X^3$	$+X^2)$			| |	$-$	$-$	$-$	$-$	
$-$	$-$	$-$	$-$	$-$	$-$	| |	X^2	$-X$	$+1$		
	$-X^4$	$+X^3$	$-X^2$		$+1$	| |					
	$-(-X^4$		$-X^2$	$-X)$		| |					
	$-$	$-$	$-$	$-$	$-$	| |					
		X^3		$+X$	$+1$	| |					
		$-(X^3$		$+X$	$+1)$	| |					
		$-$	$-$	$-$	$-$	| |					
					0	| |					

$$(X^5 + X^4 + 2.X^2 - 1) = (X^3 + X + 1).(X^2 + X - 1)$$

X^5	$+X^4$		$+2.X^2$		-1	| |	X^3	$+X$	$+1$		
$-(X^5$		$+X^3$	$+X^2)$			| |	$-$	$-$	$-$	$-$	
$-$	$-$	$-$	$-$	$-$	$-$	| |	X^2	$+X$	-1		
	X^4	$-X^3$	$+X$		-1	| |					
	$-(X^4$		$+X^2$	$+X)$		| |					
	$-$	$-$	$-$	$-$	$-$	| |					
		$-X^3$		$-X$	-1	| |					
		$-(X^3$		$+X$	$+1)$	| |					
		$-$	$-$	$-$	$-$	| |					
					0	| |					

On note que sur $\mathbb{C}$ on peut factoriser d'avantage :

$$(X^5 - X^4 + 2.X^3 + 1) = (X^3 + X + 1).\left(X - \frac{1 - i.\sqrt{3}}{2}\right).\left(X - \frac{1 + i.\sqrt{3}}{2}\right)$$

$$(X^5 + X^4 + 2.X^2 - 1) = (X^3 + X + 1).\left(X - \frac{-1 - \sqrt{5}}{2}\right).\left(X - \frac{-1 + \sqrt{5}}{2}\right)$$

et il faut encore • factoriser $X^3 + X + 1$ par les formules de Cardan :

trouver la racine réelle : $\sqrt[3]{\frac{-1 + \sqrt{\frac{31}{27}}}{2}} + \sqrt[3]{\frac{-1 - \sqrt{\frac{31}{27}}}{2}}$

• factoriser par celle ci

• trouver les deux racines complexes conjuguées du trinôme du second degré

◁ 49 ▷

♡ Donnez une liste de onze entiers consécutifs dont aucun n'est premier.
Montrez que de $2019! + 2$ à $2019! + 2018$, il y a 2017 nombres, et qu'aucun d'entre eux n'est un nombre premier.
Écrivez un script **`Python`** qui pour N donné trouve la première liste de N entiers consécutifs dont aucun n'est premier *(on supposera qu'on dispose d'une fonction qui teste si un nombre donné est premier)*.

[114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124]
Vous pouvez vérifier, aucun n'est premier.

Un classique pour trouver de telles longues listes sans nombres premiers (même si ce n'est pas la plus simple.
• $2019! + 2$ est pair, il n'est pas premier
• $2019! + 3$ est multiple de 3, il n'est pas premier (dans $2019!$ il y a des facteurs 3)
• $2019! + 4$ est pair, il n'est pas premier
• $2019! + 4$ est multiple de 5, il n'est pas premier
• $2019! + k$ se factorise en $k.(1 + 1.2019.3 \ldots (k-1).(k+1) \ldots 2019019)$: il n'est pas premier.
Et cette liste est faite de 2017 nombres.

J'en veux 11.
Je crée une liste.
Tant qu'elle est trop courte, un entier n avance.
Si il est compose je le colle dans la liste qui s'agrandit (sera-t-elle un jour assez longue ?)
Si il est premier, je remets la liste à vide, et on continue.

```
n=3
L = [ ]
while len(L)<11 :
....if not(TestP(n)) :
........L.append(n)
....else :
........L=[]
....n+=1
```

L'exécution pas à pas donne
`n=3, L = [ ]`
`n=4, L = [4]`

```
n=5, L = [ ]
n=6, L = [6]
n=7, L = [ ]
n=8, L = [8]
n=9, L = [8, 9]
n=10, L = [8, 9, 10]
n=11, L = [ ]
n=12, L = [12]
n=13, L = [ ]
n=14, L = [14]
n=15, L = [14, 15]
n=16, L = [14, 15, 16]
n=17, L = [ ]
n=18, L = [18]
```

jusqu'à

```
n=109, L = [ ]
n=110, L = [110]
n=111, L = [110, 111]
n=112, L = [110, 111, 112]
n=113, L = [ ]
n=114, L = [114]
n=115, L = [114, 115]
n=116, L = [114, 115, 116]
n=117, L = [114, 115, 116, 117]
n=118, L = [114, 115, 116, 117, 118]
```

et ainsi de suite

```
n=123, L = [114, 115, 116, 117, 118, 119, 120, 121, 122, 123]
n=124, L = [114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124]
```

et là c'est fini.

◁ 50 ▷

♡ J'ai calculé le p.g.c.d. de 2017 (premier !) et a par algorithme d'Euclide. Évidemment, j'ai trouvé 1.
Les quotients successifs ont été 4, 2, 4, 1,3, 3 et 3.
Qui est a ?

$$\begin{array}{rcrcl} a & = & 2017\times 4 & + & b \\ 2017 & = & b\times 2 & + & c \\ b & = & c\times 4 & + & d \\ c & = & d\times 1 & + & e \\ d & = & e\times 3 & + & f \\ e & = & f\times 3 & + & g \\ f & = & g\times 3 & & \end{array}$$

, avec le dernier reste non nul égal à 1 : $g = 1$.

On remonte de ligne en ligne

$$\begin{array}{rcrcll} a & = & 2017\times 4 & + & b & \\ 2017 & = & b\times 2 & + & c & \textit{ah non} \\ b & = & c\times 4 & + & d & b = 205 \\ c & = & d\times 1 & + & e & c = 43 \\ d & = & e\times 3 & + & f & d = 33 \\ e & = & f\times 3 & + & g & e = 10 \\ f & = & g\times 3 & & \textit{donc} & g = 1 \textit{ et } f = 3 \end{array}$$

C'est donc que le pgcd a été calculé dans l'autre sens :

$$\begin{array}{rcrcll} 2017 & = & a\times 4 & + & b & \\ a & = & b\times 2 & + & c & a = 453 \\ b & = & c\times 4 & + & d & b = 205 \\ c & = & d\times 1 & + & e & c = 43 \\ d & = & e\times 3 & + & f & d = 33 \\ e & = & f\times 3 & + & g & e = 10 \\ f & = & g\times 3 & & \textit{donc} & g = 1 \textit{ et } f = 3 \end{array}$$

On confirme.

```
def gcd(a, b) :
....while b != 0 :
........print(a//b)
........a, b = b, a%b
....return b
```

◁ 51 ▷ Résolvez dans $\mathbb{N}^2$ le système « $p.g.c.d.(a,b) = 84$ et $a + b = 2016$ ».

Comme on nous donne le p.g.c.d., on factorise : $a = 84 \times \alpha$ et $b = 84 \times \beta$ avec α et β entiers premiers entre eux.

L'équation donne alors $\alpha \wedge \beta = 1$ et $\alpha + \beta = 24$.

Par symétrie des rôles, on va jusqu'à moitié et on élimine les cas « non premiers entre eux » (pas de méthode universelle, on y va « à l'arrache ») :

	1	2	3	4	5	6	7	8	9	10	11	12
	23	22	21	20	19	18	17	16	15	14	13	12
	oui				oui		oui				oui	

On a huit couples : (84, 1932), (420, 1596), (588, 1428), (924, 1092), (1092, 924), (1428, 588), (1596, 420), (1932, 84)