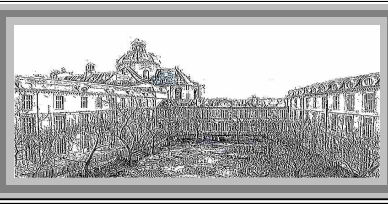
LYCEE CHARLEMAGNE
Lundi 4 mars
M.P.S.I.2



2023 2024

TD20

◦0◦ Si a, b, c, d, e, f et g sont sept nombres, écrivez avec une formule la plus courte (avec 21 symboles $\neq$) 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.

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

$-\sharp-$ Un nombre est dit **parfait** si il est égal à la somme de ses diviseurs propres *(dans ses diviseurs propres, il n'y a pas l'entier lui même)*.

◦1◦ Le programme ci-contre doit être corrigé, juste faites le :

```
def Parfait(n) :
....for k in range(n) :
........if n%k == 0 :
............S =+ k
....return S == n
```

Exemples : $6 = 1 + 2 + 3$ et $28 = 1 + 2 + 4 + 7 + 14$
Sachant que est $2^{17} - 1$ est premier, montrez que $(2^{17} - 1).2^{17-1}$ (égal à `8 589 869 056`) est parfait.

Un nombre **presque parfait** est la somme de certains de ses diviseurs. Justifiez que 204 est presque parfait. Justifiez que 158 ne l'est pas.
Sujet d'info avancé : écrivez un programme qui teste si `n` donné est presque parfait.

6 est le plus classique des nombres parfaits, c'est bien la somme $1 + 2 + 3$. Ensuite il y a l'égalité $28 = 1 + 2 + 4 + 7 + 14$.

Prenons comme proposé $(2^{17} - 1).2^{17-1}$ et dressons la liste de ses diviseurs, sachant qu'il est déjà décomposé sous forme de produit de facteurs premiers (des 2 et un certain $2^{17} - 1$ que l'on va appeler p).
Ses diviseurs sont 1, 2, p, $2.p$, 4, $4.p$, 8, $8.p$ et ainsi de suite, jusqu'à 2^{17-2}, $2^{17-2}.p$ et 2^{17-1}.
On somme tous ces diviseurs, en deux catégories :

* ceux avec juste des 2 : $1 + 2 + 4 + 8 + \ldots + 2^{17-1}$
* ceux avec p : $p + 2.p + 4.p + \ldots + 2^{17-2}.p$.

.

On rappelle la somme d'une série géométrique de raison a : $1 + a + a^2 + \ldots + a^n = \dfrac{1 - a^{n+1}}{1 - a}$ et de raison 2 : $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$.
Le total vaut $(2^{17} - 1) + p.(2^{17-1} - 1)$.
On arrange et remplace p par sa valeur : $(2^{17} - 1) + p.(2^{16} - 1) = (2^{17} - 1) + (2^{17} - 1).(2^{16} - 1) = (2^{17} - 1).(1 + 2^{16} - 1) = (2^{17} - 1).2^{17-1}$. Notre nombre est de retour ! Parfait ![1]

Le mauvais programme :

```
def Parfait(n) :
....for k in range(n) :
........if n%k == 0 :
............S =+ k
....return S == n
```

Le vrai programme :

```
def Parfait(n) :
....S = 0
....for k in range(1, n) :
........if n%k == 0 :
............S += k
....return S == n
```

Il faut initialiser l'accumulateur `S` à la valeur `0`.
`k` ne doit pas prendre la valeur `0`, on veut des diviseurs, attention à `n%0` qui pose problème. Mais on s'arrête bien à `n-1`.
Piège vicieux : `S += k` et non pas `S =+k` *(qui affecte à `S` la valeur `+k` et n'est pas vu comme une faute de syntaxe, une fois en salle d'info, on a passé dix minutes à détecter une erreur de cette forme, croyez moi, je l'ai retenue)*.

Vous aurez envie de terminer par

```
if S == n :
....return True
else :
....return False
```

C'est une perte de temps. Vous calculez un booléen `(S == n)`. Si il vaut `True` vous répondez `True`, et si il vaut `False` vous répondez `False`. Autant répondre le booléen !
Avec le test, c'est « gentillet » (une façon pour moi de ne pas dire « niais »).

1. Résultat général : si $2^p - 1$ est premier, alors $2^{p-1}.(2^p - 1)$ est parfait. Ce sont même tous les nombres parfaits pairs qui s'écrivent ainsi. Et pour l'instant, on n'a trouvé aucun nombre parfait impair.

Bon, d'accord, ce n'est pas une erreur. Mais ça montre que vous ne raisonnez pas encore comme une informaticienne, mais comme une matheuse ou une physicienne faisant de l'informatique.

Pour poursuivre, pour les nombres presque parfaits, voici les exemples :
On prend `204` et on dresse à la main la liste de ses diviseurs propres, sachant $204 = 2.2.3.17$:
`[1, 2, 3, 4, 6, 8, 12, 17, 24, 34, 51, 68, 102]` *(chaque fois qu'on a un diviseur d, on a son complément $204/d$).*

On cherche à atteindre un total de 204 avec ces nombres :
`204 = 102 + 51 + 34 + 12 + 2 + 3`
(comme l'énoncé dit que c'est possible, on en fait la somme, on regarde de combien on dépasse pour savoir qui on ne garde pas).

On recommence avec 158 : `[1, 2, 79]` et c'est tout car `79` est premier.
(pour s'en rendre compte, c'est vite fait, il n'est divisible ni par 2 ni par 3 ni par 5 ni par 7 et il n'y a pas besoin d'aller chercher plus loin, s'il avait un diviseur d plus grand, on aurait déjà rencontre $79/d$).
Ici, on ne voit pas comment atteindre 158 quand leur somme ne dépasse même pas 82.

J'aurais pu être plus gentil avec `174=29+58+87` ou plus méchant avec `288=1+ 2+4+6+8+9+12+16+18+24+32+36+48+72`.

Voici un script possible

```
def TestPresque(n) :
....L = [ ]
....for d in range(1, n) :
........if n%d == 0 :
............L.append(d)
....T = False
....for k in range(2**len(L)) :
....kk=k S, i, LL = 0, 0, [ ]
....while kk > 0 :
........if kk%2 == 1 :
............S += L[i]
............LL.append(L[i])
........kk = kk//2
........i+=1
....if S == n :
........return (True, LL)
....return False,[ ]
```

◦2◦

z est un complexe plus petit que 1 en module.
Montrez : $\dfrac{1}{1-z} = \sum_{k=0}^{+\infty} z^k$. Montrez $\sum_{n=0}^{+\infty} \dfrac{z^{2^n}}{1-z^{2^{n+1}}} = \dfrac{z}{1-z}$.

La première égalité, c'est du cours (série géométrique, pour les complexes de module strictement plus petit que 1 : $\sum_{n=0}^{N} z^n = \dfrac{1-z^{N+1}}{1-z}$ et z^{N+1} tend vers 0 quand N tend vers l'infini).
On part ensuite de cette formule, qu'on applique à $z^{2^{n+1}}$ (lui aussi pluspetit que 1).

$$\frac{1}{1-z^{2^{n+1}}} = \sum_{k=0}^{+\infty} \left(z^{2^{n+1}}\right)^k = \sum_{k=0}^{+\infty} z^{k.2^{n+1}}$$

On multiplie :

$$\frac{z^{2^n}}{1-z^{2^{n+1}}} = z^{2^n}.\sum_{k=0}^{+\infty} \left(z^{2^{n+1}}\right)^k = \sum_{k=0}^{+\infty} z^{k.2^{n+1}.2^n}$$

On somme :

$$\sum_{n=0}^{+\infty} \frac{z^{2^n}}{1-z^{2^{n+1}}} = \sum_{n,k} z^{(2.k+1).2^n}$$

Et tout entier naturel N (non nul) s'écrit $2^n.(2.k+1)$ pour n et k bien choisi.
Ceci consiste à prendre la décomposition en produit de facteurs premiers de N et à isoler $2^n.(3^a.5^b.7^d\ldots)$ avec le contenu de la parenthèse impair.

On a donc $\sum_{N>0} z^N$ et ceci vaut justement $\dfrac{z}{1-z}$ puisqu'il manque z^0.

◦3◦

♡ 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 :

$$\begin{array}{rcrrr} 2015 & = & 3 & \times 531 & +42 \\ 531 & = & 1 & \times 422 & +10 \\ 422 & = & 3 & \times 109 & +9 \\ 109 & = & 1 & \times 95 & +1 \\ 95 & = & 6 & \times 14 & +1 \\ 14 & = & 1 & \times 11 & +3 \\ 11 & = & 3 & \times 3 & +2 \\ 3 & = & 1 & \times 2 & +1 \\ 2 & = & 2 & \times 1 & \end{array}$$

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.

∘4∘

$(G,*)$ et $(H,\sharp)$ sont deux groupes. f est une application de $(G,*)$ dans $(H,\sharp)$ vérifiant $\forall(a,b)\in G,\ f(a*b) = f(a)\sharp f(b)$.
Montrez $f(e_G) = e_H$ (image du neutre = le neutre).
On pose $K = \{a\in G \mid f(a) = e_H\}$. Montrez que K est un sous groupe de $(G,*)$.
On pose $I = \{f(a) \mid a\in G\}$ (c'est à dire $y\in I \Leftrightarrow \exists a\in G,\ y = f(a)$. Montrez que I est un sous groupe de $(H,\sharp)$.
Montrez que si G est de cardinal fini, alors on a $Card(G) = Card(K)\times Card(I)$.

A faire.

∘5∘

♣ 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.

∘6∘ ♡ 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 [2])
Et on a $3617 \times 12345 - 822 \times 54321 = 3$.

∘7∘ ♡ 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

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

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 $15 = (2 + 7.k) \times 270 - (5 + 18.k) \times 105$

∘8∘ 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.

∘9∘ Le théorème de *BeZout* 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.

2. pardon, il y a aussi 1

Il suffit, pour a et b donnés, d'écrire $a.\dfrac{1}{a} + b.0 = 1$ si a est non nul

$$a.0 + b.\frac{1}{b} = 1 \text{ si } b \text{ est non nul}$$

Et si a et b sont nuls, impossible d'avoir $a.u + b.v = 1$.

∘10∘ **Résolvez $X^2 + 23.X + 24 = 0$ dans l'ensemble range(39) pour l'addition et la multiplication modulo 39**

Pour résoudre $X^2 + 23.X + 24 = 0$ d'inconnue X, on calcule le discriminant : $\Delta = 23^2 - 4.24 = 433$. On réduit modulo 39 : 4 car $39 \times 11 = 429$.
On extrait une racine carrée, c'est ici facile : $\delta = 2$.
On a deux racines : $(-23 + 2).2^{-1}$ et $(-23 - 2).2^{-1}$.

Qui est l'inverse de 2 ? C'est 20 car $2.20 = 40 = 1$.

Mais en fait, plus rapidement : $-23 = 16$. On effectue : $(16 + 2).2^{-1}$ et $(16 - 2).2^{-1}$: $\boxed{S = \{7,\ 9\}}$

Remarque : | *On peut aussi dire « on propose 7 et 9, elles conviennent, et l'équation n'a que deux racines.*

Mais en fait, c'est plus subtil.
Car 39 n'est pas premier.
La factorisation initiale est $X^2 + 23.X + 24 = X^2 - 16.X + 24$

$$\begin{aligned}
X^2 + 23.X + 24 &= (X-8)^2 - 64 + 24 \\
X^2 + 23.X + 24 &= (X-8)^2 - 40 \\
X^2 + 23.X + 24 &= (X-8)^2 - 1 \\
X^2 + 23.X + 24 &= (X-8)^2 - 1^2 \\
X^2 + 23.X + 24 &= (X-8-1).(X-8+1) \\
X^2 + 23.X + 24 &= (X-9).(X-7)
\end{aligned}$$

On a donc deux solutions : 9 et 7.
Et c'est tout...

Non, ce n'est pas tout.
L'anneau n'est pas intègre.
Un produit de facteurs est nul si l'un des facteurs est nul.
Mais aussi si l'un vaut 3 et l'autre 13
si l'un vaut 6 et l'autre 13
si l'un vaut 9 et l'autre 13
si l'un vaut 3 et l'autre 26
Il y a peut être d'autres racines, qu'on obtient en résolvant de multiples systèmes comme « $(x - 9) = 13$ et $(x - 7) = 6$ ».
Et on détecte d'autres solutions : 7,9, 22 et 33.

C'est aussi dû au fait que Δ (égal rappelons le à 4) avait plusieurs racines carrées : 2, 11, 28 et 37 !

∘11∘ **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.

∘12∘

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	

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

∘13∘

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

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

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

∘14∘

♡ On définit sur $\mathbb{N}^*$ la relation $\preccurlyeq$ par $(a \preccurlyeq b) \Leftrightarrow (a \textit{ divise } a + b)$.
Est elle réflexive ? Est elle symétrique ? Est elle antisymétrique ? Est elle transitive ?

On se donne a, b et c pour être tranquille et que tout soit quantifié.
On vérifie que a divise $a + a$ (dans un rapport 2).

On suppose que a divise $a + b$ et que b divise $a + b$.
On traduit $a + b = p.a$ et $a + b = q.b$ pour deux entiers naturel p et q.
On extrait : $b = (p - 1).a$ et on reporte : $p.a = q.(p - 1).a$.
On simplifie par a non nul : $p = q.(p - 1)$.
p est un multiple de $p - 1$ (alors qu'ils sont premiers entre eux !) : seule solution $p = 2$
On reporte : $a = b$.

On suppose que a divise $a + b$ et que b divise $b + c$.
On écrit $a + b = p.a$ et $b + c = q.b$ pour deux entiers p et q.
On a encore $b = (p - 1).a$ et $c = (q - 1).b$ puis $c = (p - 1).(q - 1).a$ et enfin $a + c = (quelquechose).a$.
a est en relation avec c.

Réflexive, antisymétrique et transitive ! C'est un ordre !

En fait, il faut l'avouer : a divise $a + b$ si et seulement si a divise b. C'est l'ordre habituel !

∘15∘

Soit $(G, *)$ un groupe et A un sous-groupe de G. On définit :
$N(A) = \{x \in G \mid \forall a \in A,\ x * a * x^{-1} \in A\}$ et $C(A) = \{x \in G \mid \forall a \in A,\ x * a * x^{-1} = a\}$.
Montrez que ce sont des sous-groupes de $(G, *)$.
Déterminez $N(A)$ et $C(A)$ pour $A = \{e\}$ *(sous groupe réduit au neutre)*.

$C(A) = \{x \in G \mid \forall a \in A,\ x*a*x^{-1} = a\}$ est formé des éléments x qui commutent avec tous les éléments de A.
On doit montrer inclusion, présence du neutre, stabilité et passage à l'inverse.
Les inclusions se lisent dans la définition : $N(A) = \{x \in G \mid \ldots\}$.
Pour le neutre, on vérifie $\boxed{\forall a \in A,\ e*a*e^{-1} = a \mid \forall a \in A,\ e*a*e^{-1} = a \in A}$
On peut le mettre dans le rôle du x des définitions.

On se donne x et y dans $N(A)$: $\forall a \in A,\ x*a*x^{-1} \in A$ et $\forall a \in A,\ y*a*y^{-1} \in A$.
On pose $z = x*y$ et on regarde si il est dans $N(A)$. On se donne donc un a quelconque dans A et on doit regarder si $z*a*z^{-1}$ est dans A. Cet élément s'écrit

$$(x*y)*a*(x*y)^{-1} = x*y*a*y^{-1}*x^{-1} = x*(y*a*y^{-1})*x^{-1}$$

Comme y est dans $N(A)$, l'élément $(y*a*y^{-1})$ est dans A. On le note α et $x*\alpha*x^{-1}$ est à son tour dans A puisque x est dans $C(A)$. On a prouvé $\forall a \in A,\ (x*y)*a*(x*y)^{-1} \in A$. On reconnait $x*y \in N(A)$.

On se donne x et y dans $C(A)$: $\forall a \in A,\ x*a*x^{-1} = a$ et $\forall a \in A,\ y*a*y^{-1} = a$
On pose $z = x*y$ et on calcule pour tout a de A :

$$(x*y)*a*(x*y)^{-1} = x*y*a*y^{-1}*x^{-1} = x*(y*a*y^{-1})*x^{-1} = x*a*x^{-1} = a$$

On a établi $\forall a \in A,\ (x*y)*a*(x*y)^{-1} = a$. On reconnait $x*y \in C(A)$. L'ensemble $C(A)$ est stable par la loi $*$.

On se donne x dans $N(A)$. On pose $z = x^{-1}$. On doit vérifier que pour tout a de A, $z*a*z^{-1}$ est dans A.
Or, on constate

$$z*a*z^{-1} = (x^{-1}*a*x) = (x*a^{-1}*x^{-1})^{-1}$$

Comme a est dans A, a^{-1} est aussi dans A. Comme x est dans $N(A)$, $x*a^{-1}*x^{-1}$ est dans A. Comme A est un groupe, son inverse $(x*a^{-1}*x^{-1})^{-1}$ y est aussi. C'est ce que l'on voulait.

On se donne x dans $C(A)$. On pose $z = x^{-1}$. On doit vérifier que pour tout a de A, $z*a*z^{-1} = a$, c'est à dire $x^{-1}*a*x = a$.
On doit prouver $(x*a^{-1}*x^{-1})^{-1} = a$ soit encore $x*a^{-1}*x^{-1} = a^{-1}$. Mais quand a est dans A, a^{-1} y est aussi. Et comme x est dans $C(A)$, on a $x*a^{-1}*x^{-1} = a^{-1}$. Gagné !

∘16∘

♡ 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.

∘17∘

♣ Résolvez $i.z = z.i$ d'inconnue z dans $\mathbb{H}$.
Résolvez $i.z = z.j$ d'inconnue z dans $\mathbb{H}$.
Montrez que dans $\mathbb{H}$ les six quaternions i, $-i$, j, $-j$, k et $-k$ sont racines du polynôme X^2+1.
Montrez que ce sont les seules *(indication : on rappelle que le module d'un quaternion $a+b.i+c.j+d.k$ est $\sqrt{a^2+b^2+c^2+d^2}$ et qu'on a $|z^2| = |z|^2$)*.
Quelles factorisations sont correctes :

$X^2+1 = (X+i).(X-i)$	$X^2+1 = (X-i).(X-j)$
$X^2+1 = (X-i).(X+i)$	$X^2+1 = (X+i).(X-i).(X+j).(X-j).(X+k).(X-k)$

On pose $z = a+i.b+j.c+k.d$ avec a, b, c et d réels.

On multiplie :

$i.z = i.(a+i.b+j.c+k.d)$	$z.i = (a+i.b+j.c+k.d).i$
$i.z = i.a-b+k.c-j.d)$	$z.i = a.i-b-k.c+j.d$

On identifie, et on trouve les complexes $a+i.b$ (partie en j et en k nulles).
Si la multiplication avait été commutative, on aurait trouvé $S = \mathbb{H}$. Ce n'est pas le cas.

On multiplie :

$i.z = i.(a+i.b+j.c+k.d)$	$z.j = (a+i.b+j.c+k.d).j$
$i.z = i.a-b+k.c-j.d)$	$z.j = j.a+b.k-c-i.d$

On identifie, on résout... $a = -d$ et $b = c$.
On a les quaternions de la forme $a.(1-k)+b.(i+j)$.

Rappel : On écrit $a.i$ ou $i.a$ c'est pareil. Car les réels commutent avec tout.
Mais on ne confond pas $a.i.j$ et $j.i.a$.

On a bien $i^2 = -1$, $j^2 = -1$ et $k^2 = -1$ puis aussi $(ia)^2 = (-j)^2 = (-k)^2 = -1$.
Mais le polynôme X^2+1 pourrait il avoir d'autres racines $a+b.i+c.j+d.k$.
On peut certes élever au carré et identifier : $a^2-b^2-c^2-d^2 = -1$, $a.b+\ldots = 0$ et ainsi de suite.

$X^2+1 = (X+i).(X-i)$	Vrai	$X^2+1 = (X-i).(X-j)$	Faux
$X^2+1 = (X-i).(X+i)$	Vrai	$X^2+1 = (X+i).(X-i).(X+j).(X-j).(X+k).(X-k)$	Faux

Il suffit de développer : $(X+i).(X-i) = X^2+i.X-i.X+(-i).i$ en prenant garde au fait que la multiplication n'est pas commutative.

Ensuite, X est un objet formel, donc $i.X$ et $X.i$, ce sera pareil.
Mais quand on va donner à X une valeur telle que j, ce ne sera plus le cas.
Donc, prudence.

Sinon, le terme constant de $(X-i).(X-j)$ n'est pas bon.
Et le degré du dernier est une absurdité.

Dans un anneau non commutatif, les polynômes ne se factorisent plus en fonction de leurs racines, d'ailleurs, ils peuvent en avoir plus que leur degré...

∘18∘

♡ Déterminez $Sup\{x-[x] \mid x \in [0,\ 5/2]\}$.
La borne supérieure est le plus petit majorant, par forcément dans l'ensemble.

La différence $x-[x]$ est toujours plus petite que 1. 1 est un majorant.
Elle n'est jamais atteinte.

Mais ce majorant est peut être la borne supérieure.
En effet, il existe des suites qui tendent vers 1. La suite des $\left(1-\frac{1}{n}-\left[1-\frac{1}{n}\right]\right)$ vaut $\left(1-\frac{1}{n}\right)$ et tend vers 1.

La borne supérieure vaut 1.

∘19∘

$(G,*)$ est un groupe. On enlève un élément, ça reste un groupe. Qui est G ?
$(G,*)$ est un groupe. On enlève deux élément, ça reste un groupe. Qui est G ? (deux solutions)
On pourra utiliser le théorème de Lagrange : le cardinal d'un sous-groupe divise le cardinal du groupe.

On note n le cardinal de G.
On enlève un élément (pas le neutre), et on a encore un groupe, donc un sous-groupe.
Et le cardinal d'un sous-groupe divise le cardinal du groupe. $n-1$ divise n.
n vaut 2.

Par exemple $(\{Id,\ \overrightarrow{(1\ 2)}\},\circ)$. *Et c'est* $\overrightarrow{(1\ 2)}$ *qu'on enlève, et il reste le groupe le plus simple.*
Ou alors $\{0,1\}$ *pour l'addition modulo* 2.

Pour le second, $n-2$ divise n.
n vaut 3 ou 4.
$\{0,\ 1,\ 2\}$ pour l'addition modulo 3 et on enlève 1 et 2.
Ou alors $\{1,\ j,\ j^2\}$ pour la multiplication, et on enlève j et j^2.

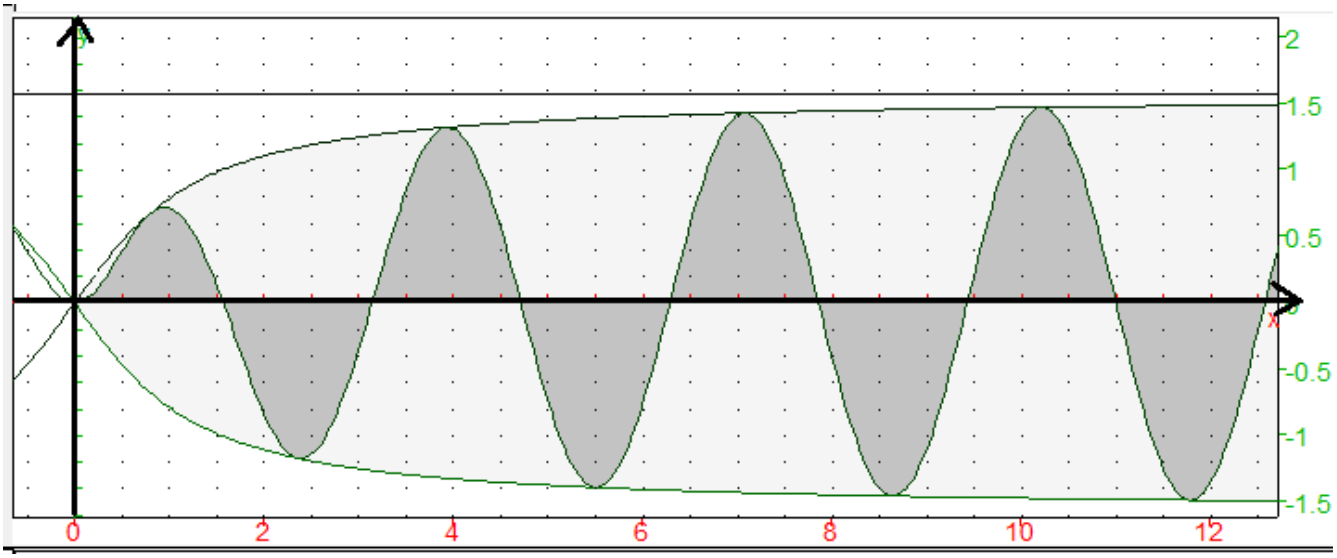
$\{0,\ 1,\ 2,\ 3\}$ pour l'addition modulo 4 et on enlève 1 et 3.
Ou alors $\{1,\ -1,\ i,\ -i\}$ pour la multiplication, et on enlève $-i$ et i.

Rappel : le cardinal d'un sous-groupe de $(G,*)$ *divise toujours le cardinal de* G.
C'est le théorème de Lagrange, il est officiellement au programme de seconde année.
Je vous le donnerai peut être en exercice.

∘20∘

Déterminez $Inf\{Arctan(t).\sin(t) \mid t \in \mathbb{R}^+\}$ et $Sup\{Arctan(t).\sin(t) \mid t \in \mathbb{R}^+\}$.

$Arctan(t)$ reste entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$.
$\sin(t)$ reste entre -1 et 1.
Le produit reste entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$.
mais il ne les atteint pas.
$\frac{\pi}{2}$ est un majorant.
Mais en prenant pour t les $\frac{\pi}{2}+2.k.\pi$ on a la suite des $Arctan\left(\frac{\pi}{2}+2.k.\pi\right)$ qui convergent vers $\frac{\pi}{2}$.
Un majorant vers lequel tend une suite de points de l'ensemble.
C'est la borne supérieure.



Et avec $-\frac{\pi}{2}+2.k.\pi$, on prouve que la borne inférieure vaut $-\frac{\pi}{2}$.

◦21◦

♡ 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 ?

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

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

On remonte de ligne en ligne

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

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

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

On confirme.

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

◦22◦

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)

∘23∘

Un sous-groupe de $(\mathbb{R}, +)$ dense dans $\mathbb{R}$. On admet que π est irrationnel.
1- Montrez que $\{a + 2.b.\pi \mid (a, b) \in \mathbb{Z}^2\}$ *(noté G)* est un sous-groupe de $(\mathbb{R}, +)$.

Purement technique.
0 s'obtient en prenant $0 + 2.0.\pi$.

Remarque : *Notons que si π avait été le rationnel $\frac{22}{7}$ on aurait pû obtenir aussi 0 sous la forme $(-44) + 2.7.\pi$.*

La somme de deux éléments tels que $a + 2.b.\pi$ et $a' + 2.b'.\pi$ est $(a + a') + 2.(b + b').\pi$ avec $a + a'$ et $b + b'$ entiers.

L'opposé de $a = 2.b.\pi$ est $(-a) + 2.(-b).\pi$ avec $(-a)$ et $(-b)$ entiers.

En revanche, on se dit que G ne doit pas être stable par multiplication *(à cause des π^2 non remplaçables en $a + 2.b.\pi$)*. Ce ne sera pas un anneau.

2- On pose $H = G \cap]-\infty, 0[$. Montrez que c'est une partie de $\mathbb{R}$ non vide majorée. On suppose que H a un plus grand élément, qu'on va noter α. Montrez par récurrence que pour tout n, $-n.\alpha$ est dans G.

H est formé des éléments strictement négatifs de G.

H est non vide, on y trouve $-1 + 2.0.\pi$.
Et H est majoré par 0.

Remarque : *Dans H on trouve aussi $411557987 - 131002976.\pi$ qui vaut quelquechose comme $-0.00000002535671\ldots$*
dont le physicien dira que ça vaut 0.
Mais pas le mathématicien, sinon π serait rationnel !

Il y a plusieurs possibilités :
H se termine sur un élément non nul, comme $\mathbb{Z} \cap]-\infty, 0[$ qui se termine sur -1.
H se termine en intervalle ouvert, comme $]-\infty, -2[$ par exemple.
H se termine ouvert aussi, mais sur 0 comme $\mathbb{Q} \cap]-\infty, 0[$ qui monte aussi près qu'on veut de 0.

On va voir qu'on est dans le dernier cas.

On va commencer par éliminer *(par l'absurde)* le premier cas.

Remarque : *Pourtant, si on avait eu $\pi = \frac{22}{7}$, les éléments de G se seraient écrits $\frac{7.a + 44.b}{7}$ avec a et b entiers. Le plus grand élément de H aurait été $-\frac{1}{7}$ atteint par $\frac{(-25).7 + 2.4.22}{7}$.*

H aurait un plus grand élément *(le dernier élément de G strictement négatif)*.
En tant que plus grand élément, il est dans H donc dans G.
Son opposé est dans G *(sous-groupe)*.
Et 0 est dans G.
Par stabilité additive, $0 - \alpha - \alpha \ldots - \alpha$ est dans G.
Proprement, on fait une récurrence.

A ce stade, G contient tous les multiples négatifs de α (rappelons que α lui même est négatif). Par passage au symétrique, il contient tous les multiples de α.
On a donc $\alpha.\mathbb{Z} \subset G$.
On va montrer l'inclusion dans l'autre sens, et aboutir à une contradiction.

3- Montrez alors que $G \cap]0, -\alpha[$ est vide. Montrez par récurrence sur n que chaque $]-n.\alpha, -(n+1).\alpha[\cap G$ est vide. Déduisez que 1 et $2.\pi$ sont tous deux de la forme $p.\alpha$ et $q.\alpha$ pour p et q entiers convenables. Concluez que π est rationnel. (? !)

Par l'absurde, si il y avait un élément x de G dans $]0, -\alpha[$, alors par passage à l'opposé, $-x$ serait dans G.
Mais $-x$ serait strictement négatif. Il serait donc dans $G \cap]-\infty, 0[$ qu'on a noté H.

Mais $-x$ serait plus grand que le plus grand élément de H.
Ceci s'appelle une contradiction.

Entre 0 et $-\alpha$, aucun élément de G.

On peut recommencer entre $-\alpha$ et $-2.\alpha$.

Plus généralement, il n'y a aucun élément de G entre $-n.\alpha$ et $-(n+1).\alpha$.
Si il y avait un tel x dans $]-n.\alpha, -(n+1).\alpha[\cap G$, alors $x+(n+1).\alpha$ serait aussi dans G *(stabilité : x est dans G et tout multiple de α aussi)*.
Mais il serait dans $]-\alpha,\ 0[$ (parti de $-n.\alpha < x < -(n+1).\alpha$ et ajouter $(n+1).\alpha$).
Ce réel serait dans $G \cap]-\infty,\ 0[$ et serait plus grand que son plus grand élément. Contradiction.

Finalement, dans G il y a les multiples de α et rien qu'eux (double inclusion).

C'est cette égalité qui va nous conduire à une belle contradiction.
En effet, 1 est dans G *(écrire* $1 = 1 + 2.0.\pi$*)*.
Il est donc multiple de α *(de la forme* $-p.\alpha$ *avec* p *bien choisi dans* $\mathbb{N}^*$*)*.

$2.\pi$ est aussi dans G *(*$0 + 2.1.\pi$*)*. On l'écrit donc $-q.\alpha$ pour un q bien choisi aussi (et non nul).

Entre $1 = -p.\alpha$ et $2.\pi = -q.\alpha$, on élimine α : $2.\pi = \dfrac{q}{p}$.
π serait rationnel. Impossible.

Bilan : | *H n'a pas de plus grand élément.*
H ne se termine pas comme $]-\infty,\ -1]$ *inclus dans* $\mathbb{R}^-$.

4- Déduisez que la borne supérieure de H n'est pas atteinte. Déduisez qu'il existe une suite strictement croissante (a_n) d'éléments de G qui converge vers α. Que fait la suite $(a_n - a_{n+1})$? Est-elle dans G ?

En tant que partie de $\mathbb{R}$ non vide majorée H a une borne supérieure, c'est à dire « le plus petit de ses majorants ».

Cette borne supérieure ne peut pas être dans H sinon, ce serait son plus grand élément, ce qui a été réfuté à la question précédente.

H se termine donc par une borne supérieure non atteinte, comme $]-\infty,\ -1[$ ou l'ensemble des 2^{-n} qui a pour borne supérieur 0.

Si la borne supérieure n'est pas atteinte il existe une suite d'éléments de l'ensemble qui tend vers celle ci.
C'est du cours.

Cours : | *Si l'ensemble H a une borne supérieure α non atteinte alors il existe une suite d'éléments de H qui converge en croissant vers α.*
Le réel $\alpha - 1$ *est strictement plus petit que α. Ce n'est donc plus un majorant de H (α était le plus petit majorant).*
Il existe donc un élément a_0 *de H strictement plus grand que* $\alpha - 1$.
Mais comme α est un majorant de H, on fusionne $\alpha - 1 < a_0 < \alpha$.

On recommence en coupant en deux en $\dfrac{a_0+\alpha}{2}$ *(strictement entre* a_0 *et α.*
C'est un réel plus petit que α, donc ce n'est plus un majorant de α.
Il existe donc un élément de H entre $\dfrac{a_0+\alpha}{2}$ *et α.*
On le note a_1*. On a donc* $a_0 < \dfrac{a_0+\alpha}{2} < a_1 < \alpha$.

Supposons qu'on en est au rang n avec $a_n < \alpha$.
On considère le milieu $\dfrac{a_n+\alpha}{2}$.
Ce n'est plus un majorant de H, il existe donc un élément de H plus grand que lui (et plus petit que α).
On décide d'en appeler un a_{n+1}*. Et il ne peut être égal à α puisque α n'est pas dans H.*

Par construction, (a_n) *est une suite d'éléments deH .*
Elle est croissante : $a_n < \dfrac{a_n+\alpha}{2} < a_{n+1}$.
Elle converge vers α car à chaque étape on divise par 2 *et garde un intervalle encore plus petit.*
Pratiquement : $\alpha - \dfrac{1}{2^n} < a_{n+1} < \alpha$ *et le théorème d'encadrement permet de conclure.*

Mais alors, une astuce nous invite à regarder $(a_n - a_{n+1})$.
Chacune de ces différences d'éléments de H est dans G.
Mais par croissance, ces différences sont strictement négatives.

On a donc une suite d'éléments de H.
Mais elle converge vers $0 - 0$, c'est à dire 0.

On notera qu'il y a un risque étrange.
Pour n assez grand $a_n - a_{n+1}$ sera entre α et 0. Ce qui est refusé car il n'y a personne de H entre α et 0.

Mais ce n'est pas si étrange, α est en fait nul.
Et G se termine « contre 0 », comme $\mathbb{Q} \cap]-\infty, 0[$.
0 est sa borne supérieure non atteinte.

5- Déduisez que pour tout ε strictement positif il existe au moins un élément dans $]0, \varepsilon[\cap G$. Combien y en a-t-il en fait ?

Pour ε non nul *(strictement positif)*, il existera un $a_{n+1} - a_n$ pour n assez grand qui sera plus petit que ε *(puisque $a_{n+1} - a_n$tend vers 0)*.
Il y a donc au moins un élément de G entre 0 et ε.

Il y en a même une infinité.
En effet, ce qui a été fait pour ε peut être fait aussi pour $\varepsilon/2$, $\varepsilon/4$ et ainsi de suite.

Bilan : *A ce stade, on a tout un nuage d'élément de G autour de 0.*
Comme les rationnels.
Ou même les $\dfrac{1}{n+1}$.
Il va de soi que les $a_n + 2.b_n.\pi$proches de 0 doivent avoir a_n et b_n de signes opposés, très bien choisis, et très grands.

On va généraliser à tout $\mathbb{R}$.C'est partout que les éléments de G sont « en nuages ».

6- On se donne un intervalle $[a, b]$ non réduit à un point. Montrez qu'il existe un élément γ de G dans $]0, b - a[$. Montrez alors que $\left[\dfrac{b}{\gamma}\right].\gamma$ est dans G et aussi dans $[a, b]$.

En donnant à $b - a$ strictement positif le rôle du εde la question précédente, on a un γ de G entre 0 et $b - a$.

Le réel $\dfrac{b}{\gamma}$ existe, et a une partie entière qui vérifie $\dfrac{b}{\gamma} - 1 < \left[\dfrac{b}{\gamma}\right] \leqslant \dfrac{b}{\gamma}$.
On multiplie par γ strictement positif : $b - (b - a) < b - \gamma = \dfrac{b}{\gamma}.\gamma - \gamma < \left[\dfrac{b}{\gamma}\right].\gamma \leqslant \dfrac{b}{\gamma}.\gamma = b$ *(on exploite $\gamma < b - a$ et on renverse avec un signe moins)*.

Comme γ est dans G *(stable par additions successives et par passage à l'opposé)*, tous ses multiples sont dans G.

On a inséré l'élément $\left[\dfrac{b}{\gamma}\right].\gamma$ de G entre a et b. Victoire.

7- Combien y a-t-il de points de G dans $[a, b]$?

En fait, une infinité.

Ce qui a été fait en insérant un x de G dans $]a, b[$ peut être refait avec $]a, x[$ et $]x, b[$.
On a alors trois éléments de G dans $]a, b[$.
On recommence avec chaque sous intervalle obtenu.

On a autant d'éléments de G qu'on veut entre a et b.
Et autant qu'on veut, c'est ce qu'on appelle l'infini.

Bilan : *G est dense dans $\mathbb{R}$, comme $\mathbb{Q}$ et $R - \mathbb{Q}$.*

On notera qu'en revanche, $\mathbb{Z}$ ne l'est pas,
ni $\{a + 2.b.\dfrac{22}{7} \mid (a, b) \in \mathbb{Z}^2\}$ qui se limite aux $\dfrac{p}{7}$ avec p décrivant $\mathbb{Z}$.

8- On se donne λ dans $]-1,\ 1[$. On se donne ε strictement positif. On pose $I = [Arcsin(\lambda-\varepsilon),\ Arcsin(\lambda+\varepsilon)]$. Montrez qu'il existe au moins un élément g de G dans I. Déduisez $|\sin(g)-\lambda| \leqslant \varepsilon$. Déduisez qu'il existe n dans $\mathbb{N}$ vérifiant $|\sin(n)-\lambda| \leqslant \varepsilon$. Montrez qu'il existe aussi n' dans $\mathbb{N}$ vérifiant $|\sin(n')-\lambda| \leqslant \varepsilon/2$.

$\lambda-\varepsilon$ est plus petit que $\lambda+\varepsilon$, et $Arcsin$ est une fonction strictement croissante.
Les deux réels $Arcsin(\lambda-\varepsilon)$ et $Arcsin(\lambda-\varepsilon)$ sont bien distincts et classés dans cet ordre.

Attention : *L'énoncé devrait préciser une chose.*
Pour que ces deux arcsinus existent, il faut quand même que $\lambda-\varepsilon$ et $\lambda+\varepsilon$ soient entre -1 et 1.
Certes, λ est dans $]-1,\ 1[$, mais si ε est trop gros, la somme ou la différence peut sortir.
Il importe donc que ε soit assez petit pour garantir $\lambda-\varepsilon \geqslant -1$ et $\lambda+\varepsilon \leqslant 1$.
On imposera donc ε « petit » comme il dit le physicien ?
Mais petit comment ?
$\varepsilon \leqslant 1-\lambda$ et $\varepsilon \leqslant \lambda+1$ (quantités strictement positives, car λ ne vaut ni -1 ni 1.

D'après le lot de questions précédent, il y a une infinité d'éléments de G entre $Arcsin(\lambda-\varepsilon)$ et $Arcsin(\lambda+\varepsilon)$ *(aussi petit que soit cet intervalle)*.
On en note un $a+2.b.\pi$.
On écrit l'encadrement $Arcsin(\lambda-\varepsilon) \leqslant a+2.b.\pi \leqslant Arcsin(\lambda+\varepsilon)$.
On passe au sinus.
Mais est ce qu'on conserve les encadrements ?
Pas si le sinus n'est pas une application croissante.

Et justement, le sinus est une application dont le sens de variations change sans arrêt.
C'est dommage.

Mais coup de chance : $-\dfrac{\pi}{2} \leqslant Arcsin(\lambda-\varepsilon) \leqslant a+2.b.\pi \leqslant Arcsin(\lambda+\varepsilon) \leqslant \dfrac{\pi}{2}$, par construction de la fonction Arcsinus.
Et là, entre $-\pi/2$ et $\pi/2$ le sinus est croissant.
On peut donc déduire : $-1 \leqslant \sin(Arcsin(\lambda-\varepsilon)) \leqslant \sin(a+2.b.\pi) \leqslant \sin(Arcsin(\lambda+\varepsilon)) \leqslant 1$.
C'est le sens qui se simplifie bien : $\sin(Arcsin(t)) = t$ si t est une longueur entre -1 et 1.
On a donc : $-1 \leqslant \lambda-\varepsilon \leqslant \sin(a+2.b.\pi) \leqslant \lambda+\varepsilon \leqslant 1$.

On soustrait : $-\varepsilon \leqslant \sin(a+2.b.\pi)-\lambda \leqslant \varepsilon$.

Un réel entre $-\varepsilon$ et ε, c'est un réel « plus petit que ε en valeur absolue ».
On a bien $|\sin(a+2.b.\pi)-\lambda| \leqslant \varepsilon$.

Mais il est temps de dire que le sinus est $2.\pi$-périodique, et que justement b est entier.
On a fini par arriver à $|\sin(a)-\lambda| \leqslant \varepsilon$.

Il existe un entier dont le sinus est proche de λ (à ε près).

Exemple : *Par exemple, je vise $\lambda = \dfrac{1}{2}$.*
Il n'existe aucun entier n vérifiant $\sin(n) = \dfrac{1}{2}$ (il faudrait des irrationnels du type $\dfrac{\pi}{6}+2.k.\pi$).
Mais on peut avoir $\sin(n) \simeq \dfrac{1}{2}$ à 10^{-3} près : $\sin(3783) \simeq 0.4990005359424875\ldots$
On peut avoir aussi $\sin(n) \simeq \dfrac{1}{2}$ à 10^{-6} près : $\sin(191068) \simeq 0.49999991516126\ldots$.
On peut avoir aussi $\sin(n) \simeq \dfrac{1}{2}$ à 10^{-8} près : $\sin(69496223) \simeq 0.4999999941200154\ldots$.
Et ainsi de suite.
Mais seule la théorie sur le sous-groupe G a garanti cette existence.

Bon, ce qu'on a fait pour ε, on aurait pu le faire pour $\varepsilon/2$, pourquoi pas.

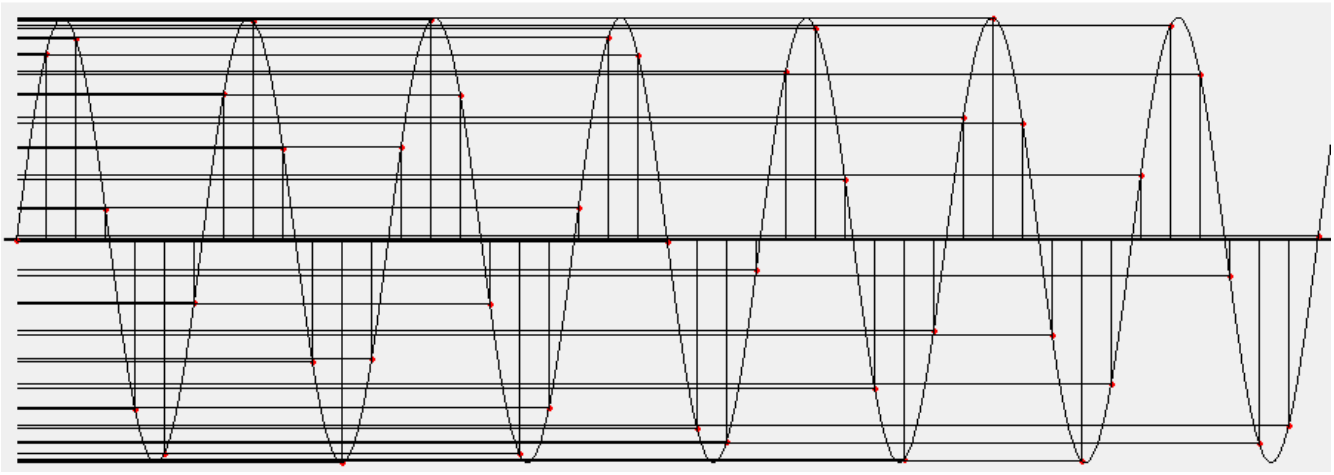
9- Déduisez qu'il existe une sous-suite de la suite $(\sin(k))_{k\in\mathbb{N}}$ qui converge vers λ.

On le fait pour des ε de plus en plus petit (des 2^{-p}). On a à chaque fois un nouvel entier n *(dépendant de εdonc de p)* satisfaisant $\sin(n) \simeq \lambda$ à 2^{-p} près.

Ces n nous donnent une suite d'entiers.
On l'ordonne par ordre croissant.

On a une suite d'entiers (n_p) vérifiant $|\sin(n_p) - \lambda| \leqslant 2^{-p}$ pour tout p.
La suite $(\sin(n_p))$ converge vers λ par encadrement.
Et elle est extraite de la suite initiale $(\sin(k))$.

10- Quel est l'ensemble des valeurs d'adhérences de la suite $(\sin(k))$?



Tout réel λ de $[-1, 1]$ est limite d'une suite extraite de $(\sin(k))$.

Remarque :
La suite $(\sin(k))$ est une vraie horreur.
Elle ne converge pas.
C'est déjà quand même un exemple intéressant pour que vous arrêtiez de dire « soit (u_n) une suite, je note μ sa limite ».
Mais pourquoi une suite serait elle obligée d'avoir une limite.
Tout ça parce qu'en TERMINABLE toutes les suites étudiées ont une limite.
Il existe en fait une grosse majorité de suites qui ne convergent pas.
Et « ne pas converger », ce n'est pas « partir vers l'infini », c'est « ne pas avoir de limite du tout, finie ou infinie ».
Il y a bien sûr l'exemple de $((1)^n)$ qui ne converge pas.
Mais elle a deux sous-suites qui convergent (limite 1 et limite -1).
Mais ici, la notre fait largement pire.
Elle se promène partout entre -1 et 1.
Et tout réel de $[-1, 1]$ peut être limite d'une sous-suite...

∘24∘ **2019 et 752 sont évidemment premiers entre eux. Pouvez vous donner une identité de Bézout qui les lie avec au moins un des entiers plus grands que 5000.**

On applique l'algorithme d'Euclide :

$$\begin{array}{rcrrr} 2019 &=& 2 &\times 752& +515\\ 752 &=& 1 &\times 515& +237\\ 515 &=& 2 &\times 237& +41\\ 237 &=& 5 &\times 41& +32\\ 41 &=& 1 &\times 32& +9\\ 32 &=& 3 &\times 9& +5\\ 9 &=& 1 &\times 5& +4\\ 5 &=& 1 &\times 4& +1 \end{array}$$

et

$$\begin{array}{rcrrr} 515 &=& 2019 &-\ 2& \times 752\\ 237 &=& 752 &-\ 1& \times 515\\ 41 &=& 515 &-\ 2& \times 237\\ 32 &=& 237 &-\ 5& \times 41\\ 9 &=& 41 &-\ 1& \times 32\\ 5 &=& 32 &-\ 3& \times 9\\ 4 &=& 9 &-\ 1& \times 5\\ 1 &=& 5 &-\ 1& \times 4 \end{array}$$

qui ne servira pas

Le p.g.c.d. vaut 1, et on remonte l'algorithme sous forme de déterminant en combinant les colonnes :

$$1 = \begin{vmatrix} 5 & 4 \\ 1 & 1 \end{vmatrix} = \begin{vmatrix} 5 & 9 \\ 1 & 2 \end{vmatrix} = \begin{vmatrix} 32 & 9 \\ 7 & 2 \end{vmatrix} = \begin{vmatrix} 32 & 41 \\ 7 & 9 \end{vmatrix}$$

$C2 = C2 + C1$; $C1 = C1 + 3.C2$; $C2 = C2 + 1.C1$

et ensuite

$$\begin{vmatrix} 32 & 41 \\ 7 & 9 \end{vmatrix} = \begin{vmatrix} 237 & 41 \\ 52 & 9 \end{vmatrix} = \begin{vmatrix} 237 & 515 \\ 52 & 113 \end{vmatrix} = \begin{vmatrix} 752 & 515 \\ 165 & 113 \end{vmatrix} = \begin{vmatrix} 752 \\ 165 \end{vmatrix}$$

$C1 = C1 + 5.C2$; $C2 = C2 + 2.C1$; $C1 = C1 + 1.C2$; $C2 = C2 + 2.C1$

On peut vérifier à quelques étapes : $5 \times 2 - 9 \times 1 = 1$ ou $237 \times 9 - 52 \times 41 = 1$ et enfin $\boxed{752 \times 443 - 2019 \times 165 = 1}$
On a une identité de Bézout.
Mais ses coefficients sont trop petits.

Mais cette fois, avec $\begin{vmatrix} 752 & 2019 \\ 165 & 443 \end{vmatrix} = 1$, on peut ajouter des lignes sur d'autres : $\begin{vmatrix} 752 & 2019 \\ 917 & 2462 \end{vmatrix} = 1$ $(L2 = L2 + L1)$

Insuffisant ? On double ($L2 = L2 + 2.L1$) : $\left|\begin{array}{cc} 752 & 2019 \\ 2421 & 6500 \end{array}\right| = 1$

◦25◦ On veut calculer le p.g.c.d. de 151 et 42. Euclide dit :

$$\begin{array}{rcrr} 151 &=& 3\times & 42 & +25 \\ 42 &=& 1\times & 25 & +17 \\ 25 &=& 1\times & 17 & +8 \\ 17 &=& 2\times & 8 & +1 \\ 8 &=& 8\times & 1 & \end{array}$$

Regardez et commentez ce qui suit :

$$\frac{151}{42} = 3 + \frac{25}{42} = 3 + \frac{1}{\frac{42}{25}} = 3 + \frac{1}{1 + \frac{17}{25}} = 3 + \frac{1}{1 + \frac{1}{\frac{25}{17}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{17}{8}}} = 3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{8}}}$$

On oublie le dernier : $\frac{151}{42} \simeq 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}} = 3 + \frac{1}{1 + \frac{1}{\frac{3}{2}}} = 3 + \frac{1}{\frac{5}{3}} = \frac{18}{5}$.

Et maintenant, que vaut le résultat du produit en croix : $151 \times 5 - 42 \times 18$?
Testez sur d'autres exemples. Justifiez le résultat obtenu.

C'est l'algorithme d'Euclide, sous une autre forme.
Et ça cache bien des choses qu'on n'aura pas le temps de voir car le programme doit avancer.

◦26◦ ♡ Trouvez tous les entiers qui sont à la fois congrus à 2 modulo 7, à 7 modulo 13 et à 13 modulo 2.

On veut les entiers qui soient à la fois congrus à 2 modulo 7, à 7 modulo 13 et à 13 modulo 2.

La dernière condition se réduit à $n \equiv 1\ [2]$. On traduit en introduisant des variables :

$$\exists(a,\ b,\ c),\ n = 2 + 7.a,\ n = 7 + 13.b,\ n = 1 + 2.c$$

c'est le théorème des « restes chinois » ou « congruences simultanées ».

Contentons nous des deux premières : $\left\{\begin{array}{rcrr} n &=& 2 & +7.a \\ n &=& 7 & +13.b \end{array}\right\} \Leftrightarrow \left\{\begin{array}{rcrr} n &=& 2 & +7.a \\ 5 &=& 7.a & -13.b \end{array}\right\}$

On cherche une identité de Bézout entre 7 et 13 : $2.7 - 1.13 = 1$ (désolé Euclide et Bézout, je n'ai pas eu besoin de vous).
On multiplie par 5 et on remplace

$$\left\{\begin{array}{rcrr} n &=& 2 & +7.a \\ n &=& 7 & +13.b \end{array}\right\} \Leftrightarrow \left\{\begin{array}{rcrr} n &=& 2 & +7.a \\ n &=& 7 & +13.b \\ 10.7 - 5.13 &=& 7.a & -13.b \end{array}\right\} \Leftrightarrow \left\{\begin{array}{rcrr} n &=& 2 & +7.a \\ n &=& 7 & +13.b \\ 7.(a-10) &=& 13.(b-5) & \end{array}\right\}$$

$a - 10$ est multiple de 13 et $b - 5$ est multiple de 7 (dans e même rapport).
On n'a plus qu'une variable : k vérifiant $a = 13.k + 7$ et $b = 7.k + 5$.
On reporte : $n = 2 + 7.(13.k + 10) = 7 + 13.(7.k + 5)$.
On trouve $n = 72 + 7.13.k$ avec k décrivant $\mathbb{Z}$ (qui veut vérifier : $72 = 2\ [7]$ et $72 = 7\ [13]$).
Il reste à tenir compte de l'autre congruence : n doit être impair. Il faut et il suffit que k soit impair.
$S_n = \{72 + 91.(2.p + 1) \mid p \in \mathbb{Z}\}$ (première solution positive : 163)

◦27◦ ♣ Quelle est la liste d'entiers naturels de somme 2018 dont le produit est le plus grand possible ?
♡ Quelle est la liste d'entiers naturels de somme 2018 dont le produit est le plus petit possible ?

Il faut prendre des facteurs différents de 1, mais il est rentable de les prendre égaux à 2 ou 3.

Par exemple, si il traîne dans le produit un facteur 7, remplacez le par 5 et 2 car 5×2 est meilleur que 7.
remplacez le par 4 et 3 car 4×3 est meilleur que 7.

Si vous avez un facteur a plus grand que 5, remplacez le par $a - 3$ et 3. En effet : $(a - 3).3 \geqslant a$ (c'est $2.a \geqslant 9$).
Si vous avez un facteur 4, gardez le, car 2.2 c'est pareil, et 3.1 c'est moins bien.
Si vous avez un facteur 3, gardez le.

On va donc prendre $3 + 3 + \ldots + 3 + 2$ avec 672 termes égaux à 3.
Le produit est $3^{272}.2$.

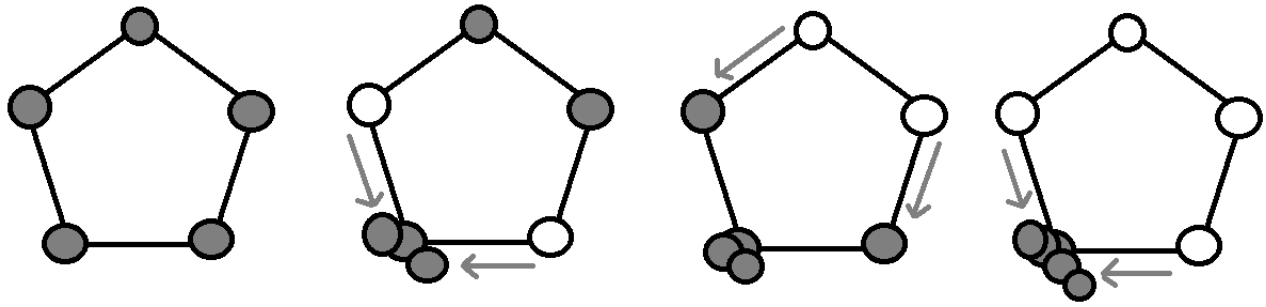
Et c'est 84433184062894209744271655170926464657035988285666030164227102363020008598918526269471079435077448604555846941792732496095475173743808816863726916688644627485778185232108739941091572887626946109107119387320874455984449590202008449832729870422150696190554349463300971400130551488165235893050690725308022386824659393676928 2

Pour minimiser le produit, on prend des 1, et le produit vaut 1.

Ou même : $2018 = 2018 + 0$ et le produit vaut 0.

◦28◦

Il y a cinq arbres en rond dans la cour. Sur chaque arbre, un corbeau. Toutes les dix secondes, deux corbeaux passent de leur arbre à un arbre voisin (droite ou gauche). En combien de temps est il possible que tous les corbeaux soient rassemblés sur un même arbre ?
Cette fois, il y a dix arbres, un corbeau par arbre, et deux corbeaux qui bougent à chaque fois. Combien de temps pour (peut-être) les rassembler tous sur un même arbre.



La second cas avec dix arbres est impossible.
Décidons qu'un arbre sur deux est un chêne et les autres des platanes *(en soi, le type d'arbre n'a pas d'importance)*.
Il y a donc initialement 5 oiseaux sur des chênes
5 oiseaux sur des platanes

Que se passe-t-il à chaque mouvement ?
Deux oiseaux quittent un arbres d'un type, et passent sur deux arbres voisins, donc d'un autre type.
Par exemple, deux corbeaux quittent un platane *(chacun ?)* et partent sur les deux chênes voisins.

On peut donc passer de situations des types suivants

5 chênes	puis	3 chênes	puis	1 chêne	puis	3 chênes
5 platanes		7 platanes		9 platanes		7 platanes

Quand j'écris « 9 platanes », je veux dire « 9 oiseaux sur des platanes ».

Une chose ne changera pas : les deux nombres seront toujours impairs.

Et de fait, il devient impossible d'arriver à

10 chênes	ou	0 chêne
0 platane		10 platanes

Or, « tous les oiseaux sur le même arbre » se formule nécessairement sous une de ces formes.

On note qu'on a cherché ici un « invariant ».

◦29◦

♡ `-a-` Déterminez $Sup\{\cos(x) + \sin(y) \mid (x, y) \in \mathbb{R}^2\}$.
`-b-` Déterminez $Sup\{\cos(x) + \sin(x) \mid x \in \mathbb{R}\}$.
`-c-` Déterminez $Sup\{\cos^2(x) + \sin^2(y) \mid (x, y) \in \mathbb{R}^2\}$.
`-d-` Déterminez $Sup\{\cos^2(x) + \sin^2(x) \mid (x, y) \in \mathbb{R}^2\}$.
`-e-` Déterminez $Sup\{\cos^2(x) + 2.\sin^2(x) \mid x \in \mathbb{R}\}$.

a	2	atteinte pour $x = 0$ et $y = \frac{\pi}{2}$
b	$\sqrt{2}$	atteinte en $\frac{\pi}{4}$ (écrire $\sqrt{2}.\cos\left(x - \frac{\pi}{4}\right)$)
c	2	atteinte pour $x = 0$ et $y = \frac{\pi}{2}$
d	1	atteinte quoi qu'on fasse !
e	2	$1 + \sin^2(x)$, donc en $\frac{\pi}{2}$: 2

∘30∘

On vous a dit "effectue le produit de i, j et k, dans $\mathbb{H}$ (Hamilton). Mais on ne vous a pas dit dans quel ordre. Combien de valeurs différentes pouvez vous obtenir ?
On vous a dit "effectue le produit de $1+i$, $1+j$ et $1+k$, dans $\mathbb{H}$". Mais on ne vous a pas dit dans quel ordre. Combien de valeurs différentes pouvez vous obtenir ?
On vous a dit "effectue le produit de $2.i$, $i+j$ et $i+k$, dans $\mathbb{H}$". Mais on ne vous a pas dit dans quel ordre. Combien de valeurs différentes pouvez vous obtenir ?

Première question.
Il y a six façons d'ordonner i, j et k. Et à chaque fois deux façons de mettre les parenthèses.

$(i.j).k = k^2 = -1$	$(j.i).k = -k^2 = 1$	$(i.k).j = -j^2 = 1$	$(k.i).j = j^2 = -1$	$(j.k).i = i^2 = -1$	$(k.j).i = -i^2 = 1$
$i.(j.k) = i^2 = -1$	$j.(i.k) = -j^2 = 1$	$i.(k.j) = -i^2 = 1$	$k.(i.j) = k^2 = -1$	$j.(k.i) = j^2 = -1$	$k.(j.i) = -k^2 = 1$

Bon, seulement deux valeurs.
Et la coïncidence des deux lignes vient de l'associativité qui est préservée...

∘31∘

Peut on dire que $\sum_{k=0}^{n} \pm k$ est égal à $\pm \sum_{k=0}^{n} k$ par linéarité ? Et si on considérait que cette somme est $\sum_{k=1}^{n} \varepsilon_k.k$ (quand $(\varepsilon_1, \dots \varepsilon_n)$ est choisi comme on veut dans $\{-1,1\}^n$) ? Elle peut aller de $-\frac{n.(n+1)}{2}$ à $\frac{n.(n+1)}{2}$ en ne prenant que des valeurs entières. Mais prend elle toutes les valeurs entières ?
Pour quelles valeurs de n existe-t-il un choix de signes $(\varepsilon_1, \dots \varepsilon_n)$ tel que la somme donne 0 ?

On aura tendance à estimer que $\pm 1 \pm 1 \pm 1$ peut valoir -3, -1, 1 ou 3.
tandis que $\pm(1+1+1)$ vaut juste -3 ou 3.

• Pour n égal à 0, on a une somme (vide) qui atteint tout de -0 à 0.
• Pour n égal à 1, on a -1 et 1 (mais pas 0).sous-g
• Pour n égal à 2, on a

$1+2$	$-1+2$
$1-2$	$-1-2$

On rate au moins 0.
• Pour n égal à 3, il y a huit sommes

$1+2+3$	$1+2-3$	$1-2+3$	$-1+2+3$
$-1-2-3$	$-1-2+3$	$-1+2-3$	$1-2-3$

Certes 0 est atteint, mais il y a treize entiers de -6 à 6. On ne les aura pas tous.

Pour n égal à 4, voici en tout cas comment avoir 0 :

n	somme
3	$1+2-3$
4	$1-2-3+4$
5	impossible
6	impossible

Si on peut atteindre 0 pour n, alors on l'atteint aussi pour $n=4$ avec
(la somme avec n termes)+$(n+1)-(n+2)-(n+3)+(n+4)$.

Comme on sait l'atteindre pour 3 et 4, on l'atteint pour

3	7	11	15	...	les $4.p+3$
4	8	12	16	...	les $4.p+4$

Peut on atteindre 0 pour n de la forme $4.p+1$? Non. Par un argument de parité.
La somme « avec que des signes + » est $\sum_{k=1}^{4.p+1} k = (4.p+1).(2.p+1)$, elle est impaire.
Changeons le signe devant un certains k. La somme évolue de $2.k$. Elle garde la même parité. Et même si on change le signe de plein de termes, elle reste impaire...
Impossible donc.

De même pour n de la forme $4.p+2$, on a la même impossibilité. Par exemple $\pm 1 \pm 2 \pm 3 \pm 4 \pm 5 \pm 6$ est impair.
Modulo 2, il vaut $1+0+1+0+1+0$. C'est donc raté, il ne pourra pas valoir 0.
Le même raisonnement tient pour tout autre entier congru à 2 modulo 4.

Bilan : on peut atteindre 0 avec des sommes bien choisies pour les entiers congrus à 0 ou 3 modulo 4.

∘32∘

Entre 1 et 1 105, il y a 221 multiples de 5 ; il y a 65 multiples de 17, et enfin 85 multiples de 13.
Dois je en déduire que entre 1 et 1 105, il y a $1105-(221+65+85)$ nombres premiers avec 1105 ?

Un nombre n est premier avec 1005 si et seulement si il n'a aucun diviseur commun avec 1105. C'est la définition.
Or, qui sont les diviseurs de 1105 ? Justement :5, 17 et 13.

On doit donc éliminer les multiples de 5
les multiples de 17
et les multiples de 13.

Mais évidemment, il y a ceux qu'on a décompté deux fois : les multiples de 5×13
les multiples de 5×17
les multiples de 17×13

Il faut donc les ajouter.
Et se poser la question : 1105, on l'a compté et décompté combien de fois.

On voit venir la formule $Card(A \cup B \cup C) = Card(A) + Card(B) + Card(C) - Card(A \cap B) - Card(A \cap C) - Card(B \cap C) + Card(A \cap B \cap C)$.

Finalement, en se disant que les nombres cités dans l'énoncé sont « il y a $\frac{1105}{5}$ multiples de 5 »
« il y a $\frac{1105}{13}$ multiples de 13 »
« il y a $\frac{1105}{17}$ multiples de 17 »

la formule va être $1105 - \frac{1105}{5} - \frac{1105}{13} - \frac{1105}{17} + \frac{1105}{13.17} + \frac{1105}{5.17} + \frac{1105}{5.13} - \frac{1105}{1105}$

On effectue le calcul : $\boxed{768}$

On peut même le compacter, pour qui connaît la belle idée : $1105.\left(1-\frac{1}{5}\right).\left(1-\frac{1}{13}\right).\left(1-\frac{1}{17}\right)$

On peut aussi dresser la liste :

```
def pgcd(a, b) : #un classique, cherchez pas, c'est Euclide
....if b == 0 :
........return a
....return (pgcd(b, a%b))
```
(dernier reste non nul des divisons euclidiennes successives)

Le script proprement dit :

```
L = [ ]
for k in range(1, 1106) : #on les fait défiler
....if pgcd(k, 1105) == 1 :
........L.append(k)
print(len(L))
```

```
[1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 14, 16, 18, 19, 21, 22, 23, 24, 27, 28, 29, 31, 32, 33, 36, 37, 38, 41, 42, 43, 44, 46, 47, 48, 49, 53, 54,
56, 57, 58, 59, 61, 62, 63, 64, 66, 67, 69, 71, 72, 73, 74, 76, 77, 79, 81, 82, 83, 84, 86, 87, 88, 89, 92, 93, 94, 96, 97, 98, 99, 101, 103,
106, 107, 108, 109, 111, 112, 113, 114, 116, 118, 121, 122, 123, 124, 126, 127, 128, 129, 131, 132, 133, 134, 137, 138, 139, 141, 142, 144,
146, 147, 148, 149, 151, 152, 154, 157, 158, 159, 161, 162, 163, 164, 166, 167, 168, 171, 172, 173, 174, 176, 177, 178, 179, 181, 183, 184,
186, 188, 189, 191, 192, 193, 194, 196, 197, 198, 199, 201, 202, 203, 206, 207, 209, 211, 212, 213, 214, 216, 217, 218, 219, 222, 223, 224,
226, 227, 228, 229, 231, 232, 233, 236, 237, 239, 241, 242, 243, 244, 246, 248, 249, 251, 252, 253, 254, 256, 257, 258, 259, 261, 262, 263,
264, 266, 267, 268, 269, 271, 274, 276, 277, 278, 279, 281, 282, 283, 284, 287, 288, 291, 292, 293, 294, 296, 297, 298, 301, 302, 303, 304,
307, 308, 309, 311, 313, 314, 316, 317, 318, 319, 321, 322, 324, 326, 327, 328, 329, 331, 332, 333, 334, 336, 337, 339, 341, 342, 343, 344,
346, 347, 348, 349, 352, 353, 354, 356, 358, 359, 361, 362, 363, 366, 367, 368, 369, 371, 372, 373, 376, 378, 379, 381, 382, 383, 384, 386,
387, 388, 389, 392, 393, 394, 396, 397, 398, 399, 401, 402, 404, 406, 407, 409, 411, 412, 413, 414, 417, 418, 419, 421, 422, 423, 424, 426,
427, 428, 431, 432, 433, 434, 436, 437, 438, 439, 441, 443, 444, 446, 447, 448, 449, 451, 452, 453, 454, 456, 457, 458, 461, 462, 463, 464,
466, 467, 469, 471, 472, 473, 474, 477, 478, 479, 482, 483, 484, 486, 487, 488, 489, 491, 492, 496, 497, 498, 499, 501, 502, 503, 504, 506,
508, 509, 511, 512, 513, 514, 516, 517, 518, 519, 521, 522, 523, 524, 526, 528, 529, 531, 532, 534, 536, 537, 538, 539, 541, 542, 543, 547,
548, 549, 551, 552, 553, 554, 556, 557, 558, 562, 563, 564, 566, 567, 568, 569, 571, 573, 574, 576, 577, 579, 581, 582, 583, 584, 586, 587,
588, 589, 591, 592, 593, 594, 596, 597, 599, 601, 602, 603, 604, 606, 607, 608, 609, 613, 614, 616, 617, 618, 619, 621, 622, 623, 626, 627,
628, 631, 632, 633, 634, 636, 638, 639, 641, 642, 643, 644, 647, 648, 649, 651, 652, 653, 654, 656, 657, 658, 659, 661, 662, 664, 666, 667,
668, 669, 671, 672, 673, 674, 677, 678, 679, 681, 682, 683, 684, 686, 687, 688, 691, 692, 693, 694, 696, 698, 699, 701, 703, 704, 706, 707,
708, 709, 711, 712, 713, 716, 717, 718, 719, 721, 722, 723, 724, 726, 727, 729, 732, 733, 734, 736, 737, 738, 739, 742, 743, 744, 746, 747,
749, 751, 752, 753, 756, 757, 758, 759, 761, 762, 763, 764, 766, 768, 769, 771, 772, 773, 774, 776, 777, 778, 779, 781, 783, 784, 786, 787,
788, 789, 791, 792, 794, 796, 797, 798, 801, 802, 803, 804, 807, 808, 809, 811, 812, 813, 814, 817, 818, 821, 822, 823, 824, 826, 827, 828,
829, 831, 834, 836, 837, 838, 839, 841, 842, 843, 844, 846, 847, 848, 849, 851, 852, 853, 854, 856, 857, 859, 861, 862, 863, 864, 866, 868,
869, 872, 873, 874, 876, 877, 878, 879, 881, 882, 883, 886, 887, 888, 889, 891, 892, 893, 894, 896, 898, 899, 902, 903, 904, 906, 907, 908,
909, 911, 912, 913, 914, 916, 917, 919, 921, 922, 924, 926, 927, 928, 929, 931, 932, 933, 934, 937, 938, 939, 941, 942, 943, 944, 946, 947,
948, 951, 953, 954, 956, 957, 958, 959, 961, 963, 964, 966, 967, 968, 971, 972, 973, 974, 976, 977, 978, 979, 981, 982, 983, 984, 987, 989,
991, 992, 993, 994, 996, 997, 998, 999, 1002, 1004, 1006, 1007, 1008, 1009, 1011, 1012, 1013, 1016, 1017, 1018, 1019, 1021, 1022, 1023, 1024,
1026, 1028, 1029, 1031, 1032, 1033, 1034, 1036, 1038, 1039, 1041, 1042, 1043, 1044, 1046, 1047, 1048, 1049, 1051, 1052, 1056, 1057, 1058,
1059, 1061, 1062, 1063, 1064, 1067, 1068, 1069, 1072, 1073, 1074, 1076, 1077, 1078, 1081, 1082, 1083, 1084, 1086, 1087, 1089, 1091, 1093,
1094, 1096, 1097, 1098, 1099, 1101, 1102, 1103, 1104]
```

On préférera nettement la liste de ceux qu'on a enlevés :

```
[5, 10, 13, 15, 17, 20, 25, 26, 30, 34, 35, 39, 40, 45, 50, 51, 52, 55, 60, 65, 68, 70, 75, 78, 80, 85, 90,
91, 95, 100, 102, 104, 105, 110, 115, 117, 119, 120, 125, 130, 135, 136, 140, 143, 145, 150, 153, 155, 156,
160, 165, 169, 170, 175, 180, 182, 185, 187, 190, 195, 200, 204, 205, 208, 210, 215, 220, 221, 225, 230, 234,
235, 238, 240, 245, 247, 250, 255, 260, 265, 270, 272, 273, 275, 280, 285, 286, 289, 290, 295, 299, 300, 305,
306, 310, 312, 315, 320, 323, 325, 330, 335, 338, 340, 345, 350, 351, 355, 357, 360, 364, 365, 370, 374, 375,
377, 380, 385, 390, 391, 395, 400, 403, 405, 408, 410, 415, 416, 420, 425, 429, 430, 435, 440, 442, 445, 450,
455, 459, 460, 465, 468, 470, 475, 476, 480, 481, 485, 490, 493, 494, 495, 500, 505, 507, 510, 515, 520, 525,
527, 530, 533, 535, 540, 544, 545, 546, 550, 555, 559, 560, 561, 565, 570, 572, 575, 578, 580, 585, 590, 595,
598, 600, 605, 610, 611, 612, 615, 620, 624, 625, 629, 630, 635, 637, 640, 645, 646, 650, 655, 660, 663, 665,
670, 675, 676, 680, 685, 689, 690, 695, 697, 700, 702, 705, 710, 714, 715, 720, 725, 728, 730, 731, 735, 740,
741, 745, 748, 750, 754, 755, 760, 765, 767, 770, 775, 780, 782, 785, 790, 793, 795, 799, 800, 805, 806, 810,
815, 816, 819, 820, 825, 830, 832, 833, 835, 840, 845, 850, 855, 858, 860, 865, 867, 870, 871, 875, 880, 884,
885, 890, 895, 897, 900, 901, 905, 910, 915, 918, 920, 923, 925, 930, 935, 936, 940, 945, 949, 950, 952, 955,
960, 962, 965, 969, 970, 975, 980, 985, 986, 988, 990, 995, 1000, 1001, 1003, 1005, 1010, 1014, 1015, 1020,
1025, 1027, 1030, 1035, 1037, 1040, 1045, 1050, 1053, 1054, 1055, 1060, 1065, 1066, 1070, 1071, 1075, 1079,
1080, 1085, 1088, 1090, 1092, 1095, 1100, 1105]
```

◦33◦ ♡ Résolvez le système $\left\{\begin{array}{rcll} n & = & 3 & [5] \\ n & = & 7 & [9] \\ n & = & 1 & [4] \end{array}\right\|$ d'inconnue entière n.

Un système de congruences simultanées.

On commence par $\left\{\begin{array}{rcll} n & = & 0 & [5] \\ n & = & 0 & [9] \end{array}\right\|$: les multiples de 45.

puis $\left\{\begin{array}{rcll} n & = & 3 & [5] \\ n & = & 7 & [9] \end{array}\right\|$: $S = \{43 + 45.k \mid k \in \mathbb{Z}\}$ (particulière plus homogènes).

On passe à $\left\{\begin{array}{rcll} n & = & 43 & [45] \\ n & = & 1 & [4] \end{array}\right\|$.

On teste $43 = 3\ [4]$, $43 + 45 = 0\ [4]$ et $43 + 45 + 45 = 1\ [4]$.

L'entier 133 est solution particulière.

Les solutions : $\boxed{\{133 + 180.p \mid p \in \mathbb{Z}\}}$

◦34◦ ♡ 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.

Appelons a et b les deux entiers. Puis c, d, e et ainsi de suite les restes.

$$\begin{array}{rcrl} a & = & 1 & \times b \quad +c \\ b & = & 34 & \times c \quad +d \\ c & = & 2 & \times d \quad +e \\ d & = & 2 & \times e \quad +f \\ e & = & 2 & \times f \quad +g \\ f & = & 1 & \times g \quad +h \\ g & = & 2 & \times h \end{array}$$

et le dernier reste est nul.

Comme on nous dit que le dernier reste non nul est 3 : $h = 3$ (et tous les nombres de l'étude sont multiples de 3).

On remonte pas à pas
$\begin{array}{rcrl} a & = & 1 & \times b \quad +c \\ b & = & 34 & \times c \quad +d \\ c & = & 2 & \times d \quad +e \\ d & = & 2 & \times e \quad +f \\ e & = & 2 & \times f \quad +g \\ f & = & 1 & \times g \quad +3 \\ g & = & 2 & \times 3 \end{array}$ puis
$\begin{array}{rcrl} a & = & 1 & \times b \quad +c \\ b & = & 34 & \times c \quad +d \\ c & = & 2 & \times d \quad +e \\ d & = & 2 & \times e \quad +f \\ e & = & 2 & \times f \quad +6 \\ f & = & 1 & \times 6 \quad +3 \\ 6 & = & 2 & \times 3 \end{array}$ et
$\begin{array}{rcrl} a & = & 1 & \times b \quad +c \\ b & = & 34 & \times c \quad +d \\ c & = & 2 & \times d \quad +e \\ d & = & 2 & \times e \quad +9 \\ e & = & 2 & \times 9 \quad +6 \\ 9 & = & 1 & \times 6 \quad +3 \\ 6 & = & 2 & \times 3 \end{array}$

et
$\begin{array}{rcrl} a & = & 1 & \times b \quad +c \\ b & = & 34 & \times c \quad +d \\ c & = & 2 & \times d \quad +24 \\ d & = & 2 & \times 24 \quad +9 \\ 24 & = & 2 & \times 9 \quad +6 \\ 9 & = & 1 & \times 6 \quad +3 \\ 6 & = & 2 & \times 3 \end{array}$ jusqu'à
$\begin{array}{rcrl} 4887 & = & 1 & \times 4749 \quad +138 \\ 4749 & = & 34 & \times 138 \quad +57 \\ 138 & = & 2 & \times 57 \quad +24 \\ 57 & = & 2 & \times 24 \quad +9 \\ 24 & = & 2 & \times 9 \quad +6 \\ 9 & = & 1 & \times 6 \quad +3 \\ 6 & = & 2 & \times 3 \end{array}$

On confirme être partis de 4887 et 4749.

```
def pgcd(a,b) :
....while b>0 :
........k = a//b
........r = a%b
........print(a,k,b,r)
........a=b
........b=r
....return a
```

L'instruction `gcd=pgcd(4887,4749)` affiche

4887	1	4749	138
4749	34	138	57
138	2	57	24
57	2	24	9
24	2	9	6
9	1	6	3
6	2	3	0

et la valeur 3 est donne à gcd, mais pas affichée.

Pour $\begin{array}{rcrcl} a &=& 0 &\times b& +c \\ b &=& 4 &\times c& +d \\ c &=& 1 &\times d& +e \\ d &=& 1 &\times e& +f \\ e &=& 30 &\times f& +g \\ f &=& 11 &\times g& \end{array}$ et un reste gal à 3 : $\begin{array}{rcrcl} a &=& 0 &\times b& +c \\ b &=& 4 &\times c& +d \\ c &=& 1 &\times d& +e \\ d &=& 1 &\times e& +f \\ e &=& 30 &\times f& +3 \\ f &=& 11 &\times 3& \end{array}$

On trouve
$$\begin{array}{rcrcl} a &=& 0 &\times 9102& +2019 \\ 9102 &=& 4 &\times 2019& +1026 \\ 2019 &=& 1 &\times 1026& +993 \\ 1026 &=& 1 &\times 993& +33 \\ 993 &=& 30 &\times 33& +3 \\ 33 &=& 11 &\times 3& \end{array}$$

Les deux nombres initiaux sont 9102 et 2019, mais donnés dans le « mauvais ordre », ce qui explique le premier quotient nul.

Petite question : pourquoi un exercice aussi simple et clair que celui ci ne figure dans aucun manuel d'arithmétique ?

◦35◦

Exprimez le $p.g.c.d.$ de a^2 et b^2 à l'aide du $p.g.c.d.$ de a et b.
Exprimez le $p.g.c.d.$ de $2.a$ et $2.b$ à l'aide du $p.g.c.d.$ de a et b.
Exprimez le $p.g.c.d.$ de $a!$ et $b!$ à l'aide du $p.g.c.d.$ de a et b si nécessaire.

$p.g.c.d.(a^2,\ b^2) = \Big(p.g.c.d(a,b)\Big)^2$

$p.g.c.d.(2.a,\ 2.b) = 2.\Big(p.g.c.d(a,b)\Big)$

Supposons par symétrie des rôles $a \leqslant b$ alors $p.g.c.d.(a!,\ b!) = a!$ puisque $a!$ divise $b!$.

◦36◦

Peut on avoir $p.g.c.d.(a,\ b) = 2016$, $p.g.c.d.(b,\ c) = 2017$ et $p.g.c.d.(c,\ a) = 2018$?
Si oui, combien de solutions ?
Information : $2^5.3^2.7$, tandis que 2017 et 673 sont premiers.

◦37◦

On pose $A = \{a,\ b,\ c\}$ et $B = \{b,\ c,\ d\}$. Donnez un élément qui est dans $P(A \cup B)$ mais pas dans $P(A) \cup P(B)$. Combien y a-t-il d'éléments dans $P(A) \cup P(B)$? Combien y a-t-il d'éléments dans $P(A \times B)$?Combien y a-t-il d'éléments dans $P(A) \times P(B)$?

$P(A) = \Big\{\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{a,b\},\ \{a,c\},\ \{b,c\},\ \{a,b,c\}\Big\}$

$P(B) = \Big\{\emptyset,\ \{b\},\ \{c\},\ \{d\},\ \{b,c\},\ \{b,d\},\ \{c,d\},\ \{b,c,d\}\Big\}$

$P(A) \cup P(B) = \Big\{\emptyset,\ \{a\},\ \{b\},\ \{c\},\ \{d\},\ \{a,b\},\ \{a,c\},\ \{b,c\},\ \{b,d\},\ \{c,d\},\ \{a,b,c\},\ \{b,c,d\}\Big\}$

En revanche $A \cup B = \{a,\ b,\ c,\ d\}$ et $P(\{a,\ b,\ c,\ d\})$ contient $\{a,d\}$ et $\{a,b,c,d\}$.

Le cardinal de $P(A) \cup P(B)$ est $8 + 8 - 4$ (les parties $\emptyset$, $\{b\}$, $\{c\}$ et $\{b,c\}$ sont là deux fois).
La liste des douze parties est au dessus.
En revanche, $P(A \cup B)$ est de cardinal 2^4.

$A \times B$ est de cardinal 9 :

	a	b	c
b	(a,b)	(b,b)	(c,b)
c	(a,c)	(b,c)	(c,c)
d	(a,d)	(b,d)	(c,d)

(ce sont bien neuf couples distincts).

On a donc 2^9 éléments dans $P(A \times B)$. Ce qui fait 512.

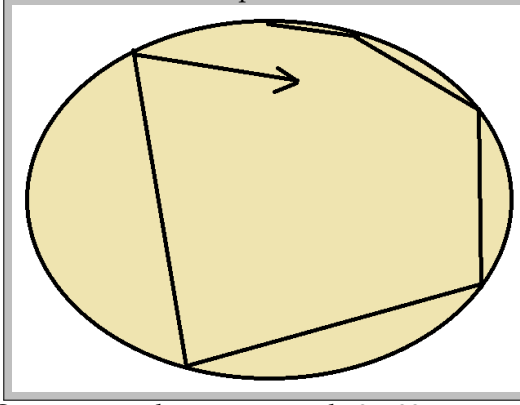
$P(A)$ était de cardinal 8 et $P(B)$ aussi.$P(A) \times P(B)$ est de cardinal 64, je pourrais même en dresser une liste/tableau

	$\emptyset$	$\{a\}$	$\{b\}$	$\{c\}$	$\{a,b\}$	$\{a,c\}$	$\{b,c\}$	$\{a,b,c$
$\emptyset$	$(\emptyset,\emptyset)$	$(\{a\},\emptyset)$	$(\{b\},\emptyset)$	$(\{c\},\emptyset)$	$(\{a,b\},\emptyset)$	$(\{a,c\},\emptyset)$	$(\{b,c\},\emptyset)$	$(\{a,b,c\}$
$\{b\}$	$(\emptyset,\{b\})$	$(\{a\},\{b\})$	$(\{b\},\{b\})$	$(\{c\},\{b\})$	$(\{a,b\},\{b\})$	$(\{a,c\},\{b\})$	$(\{b,c\},\{b\})$	$(\{a,b,c\},$
$\vdots$								
$\{c,d\}$	$(\emptyset,\{c,d\})$	$(\{a\},\{c,d\})$	$(\{b\},\{c,d\})$					
$\{b,c,d\}$							$(\{b,c\},\{b,c,d\})$	$(\{a,b,c\},\{$

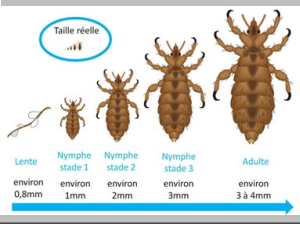
je vous laisse compléter.
Et je vous laisse prendre conscience que ce ne sont pas des objets simplistes comme ceux que vous avez manipulé en Terminale, au collège ou en calcul.
Mais ce sont quand même des couples formés de parties...

∘38∘

Nous sommes cent personnes assises en rond *(pardon en cercle)* dans la cour. Un pou qui est sur mon crâne et qui en a assez de patiner décide de sauter sur la tête de mon voisin. Mais de là, il saute à nouveau, mais cette fois, en avançant de deux têtes. Puis de trois. Puis de quatre. Puis de cinq *(ce pou est croisé avec une puce)*. A chaque fois, il saute une tête de plus.



C'est ainsi qu'en dix sauts, il est sur un individu presque diamétralement opposé. Finira-t-il par revenir sur ma tête ? Existe-t-il un emplacement du cercle d'individus où vous serez assuré(e) d'échapper au pou ?



On numérote les personnes de 0 à 99.
On a alors une suite des positions du pou : $p_0 = 0$, $p_1 = 1$, $p_2 = 3$ et plus généralement $p_{n+1} = p_n + (n+1)$, à condition de réduire modulo 100.
La formule générale est $p_n = \dfrac{n.(n+1)}{2}$.

La question est « évite-t-on des valeurs ? ».
Une remarque : la suite est périodique de période 200.
$p_{n+200} = \dfrac{(n+200).(n+201)}{2} = \dfrac{n.(n+1)}{2} + 200.n + 20100 = \dfrac{n.(n+1)}{2}$ modulo 100
(on peut dire aussi que quand le pou saut de 205, c'est comme quand il saute de 5, et sachant que p_{200} est égal à 0 modulo 100...).

Si dans les 200 premiers sauts il a évité des têtes, il continuera à les éviter.

```
def Pou(n) :
....L = [ ]
....p = 0
....for k in range(n) : #saute petit pou
........p = (p+k)%100 #nouvelle position
........if not(p in L) :
............L.append(p)
....L.sort() #on la trie pour la lisibilité
....return L #une liste à afficher
```

Voici les premiers emplacements (avant le tour complet) :
`[0, 1, 3, 5, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91]`
et ensuite :
`[0, 1, 3, 5, 6, 10, 15, 20, 21, 25, 28, 31, 35, 36, 45, 51, 53, 55, 65, 66, 71, 76,`

`78, 90, 91]` (pas dans l'ordre de parcours...)
et une fois qu'on a tourné tourné...
`[0, 1, 3, 5, 6, 10, 11, 15, 16, 20, 21, 25, 26, 28, 30, 31, 35, 36, 40, 41, 45, 46, 50, 51, 53, 55, 56, 60, 61, 65, 66, 70, 71, 75, 76, 78, 80, 81, 85, 86, 90, 91, 95, 96]`
Et vous savez où vous placer pour l'éviter.

Reste à prouver maintenant si on veut éviter Python :
$\forall n \in \mathbb{N}$, $\frac{n.(n+1)}{2} \neq 2$ [100]. Ca doit pouvoir se faire.

```
#prg ni optimisé, ni clean
```
#le but du prg : "'le programme prend en entrée le nombre de personnes assises en cercle et affiche avec le module turtle le trajet du pou mutant puce. Le seul problème est le nombre de saut de la puce pour lequel je n'ai pas mis de borne (pour l'instant, le pou saute autant de fois qu'il y a de personnes) on pourrait faire une boucle `while` afin de voir si toutes les personnes sont touchées par le pou... "'

```
#importation de module graphique cool
import turtle

#variables, listes
n = int(input("Nombre de personnes en cercle : "))
Liste = [ i+1 for i in range(n)]
effe = [Liste[0]]
listepos, effet = [], []
alpha = effe[0]

for c in range(1, n+1) : #la partie qui serait à modifier est ici, je le ferais si je m'ennuie
....alpha +=c
....if alpha<n :
........effe.append(alpha)
....else :
........alpha = alpha%n
........effe.append(alpha)

for vara in range(1, n+1) :
....if effe[vara] ==1 :
........print("Le pou mutant puce est revenu sur le crâne de Mr.Choquet au bout de "+str(vara)+"
sauts")

#tracé du cercle :
turtle.penup( )
turtle.goto(0,-100)
turtle.pendown( )
for i in range(n) :
....turtle.dot( )
....listepos.append(turtle.position( ))#liste de l'ensemble des pos
....turtle.circle(100, 360/n)

turtle.penup( )

for k in range(len(effe)) :
....effet.append(effe[k]-1) #création d'une nouvelle liste
....#qui respecte l'indentation python

turtle.pendown( )
for var in range(len(effet)-1) :
....turtle.goto(listepos[effet[var]])
turtle.penup( )
```

◦39◦ ♡ Pouvez vous trouver une partie A de $\mathbb{R}$ vérifiant

a	$Sup\{x \mid x \in A\} = 1$ et $Sup\{x^2 \mid x \in A\} = 2$
b	$Sup\{x \mid x \in A\} = 2$ et $Sup\{x^2 \mid x \in A\} = 1$
c	$Sup\{x \mid x \in A\} = 1$ et $Sup\{\sin(x) \mid x \in A\} = 1$
d	$Sup\{x \mid x \in A\} = 1$ et $Sup\{x - y \mid x \in A,\ y \in A\} = 5$

Pour a, une possibilité est $[-\sqrt{2},\ 1]$

Si il existe une suite d'éléments de A qui converge vers 2, la suite des carrés va converger vers 4. Et $Sup\{x^2 \mid x \in A\}$ ne sera plus majoré par 1 (mais « au mieux par 4).
b est impossible.

Pour le c, prenons $\left[-\frac{3.\pi}{2},\ 1\right]$.

Pour le d je propose $[-4,\ 1]$.
La borne supérieure est 1 (atteinte pour $x = 1$).
On encadre $-4 \leqslant x \leqslant 1$
$-4 \leqslant y \leqslant 1$
$-1 \leqslant -y \leqslant 4$
$-5 \leqslant x - y \leqslant 5$
L'ensemble $\{x - y \mid x \in A,\ y \in A\}$ est majoré par 5 (et le majorant 5 est atteint).

En fait, avec $Sup\{b - a \mid b \in A$ et $a \in A\}$, on mesure la longueur d'un ensemble A. On dit aussi « son diamètre » (plus grande distance entre deux points de A).

◦40◦ ♣ Devant vous n pièces, toutes orientées côté pile. A chaque fois, vous avez le droit de retourner toutes les pièces sauf une. Le but est qu'en un certain nombre d'opérations, toutes les pièces affichent leur côté face. Avec n égal à 2, c'est évidemment facile $(P - P) \to (P - F) \to (F - F)$. Donnez une solution en quatre coups pour n égal à 4. Donnez une solution en six coups pour n égal à 6. Montrez qu'il n'y a pas de solution pour n égal à 5. Finalement, quelles sont les valeurs de n pour lesquelles il y a une solution *(et pour vous, $n = 0$ est solution ?)*.
♯ Et si vous écriviez le programme Python qui pour n donné dans la liste des possibles affiche les étapes successives *(programme récursif ?)*.

retourner toutes sauf...	P	P	P	P
1	P	F	F	F
2	F	F	P	P
3	P	P	P	F
4	F	F	F	F

En 4 coups.

Il n'y a pas de solution pour n impair.
On note 0 et 1 les états des pièces.
Au départ une liste de 0 et normalement à la fin, une liste de 1.
Considérons la somme des valeurs des états. On doit passer de 0 à n.
A chaque fois, on retourne $n - 1$ pièces.
Il y a donc $n - 1$ pièces qui passent de 0 à 1 ou de 1 à 0.
Chacune augmente ou diminue de 1.
La parité de chacune change.
Mais il y a $n - 1$ changements de parité.
Globalement, la parité de la somme ne change pas.
Elle ne pourra donc pas passer de 0 à n si n est impair.

On peut aussi regarder la parité de « nombre de piles moins nombre de face ».

Remarque : *Mais notre argument ne prouve pas qu'il y a une solution pour chaque n pair. Il montre jusque que c'est impossible pour n impair.*
Et que l'argument « somme des états » ne donne pas d'incohérence pour n pair.
Mais « pas d'incohérence de ce côté » ne dit pas « existence d'une solution » !

Mais on a une méthode pour passer de n à $n + 2$. On agit en deux coups sur les deux premières, et ensuite, on connaît la méthode pour les n dernières. Et cette méthode se fait en n coups, donc un nombre pair. les deux premières clignotent mais reviennent à leur état F F.

retourner toutes sauf...	P	P	P	P	...	P
1	P	F	F	F	...	F
2	F	F	P	P	...	P
nombre pair d'étapes						
n	F	F	F			F

En fait, l'algorithme est

pour i de début à fin :
retourner tout L[i]
et en fait : retourner tout, puis retourner L[i] une nouvelle fois.

```
def piece(n) :
....if n%2 !=0 :
........return('impossible à calculer')
....L=n*[False]
....p=0
....print(L)
....for i in range(n) :
........for k in range(n) :
............if L[k]==False :
................L[k]=True
............else :
................L[k]=False
........if L[p]==False :
............L[p]=True
........else :
............L[p]=False
........p+=1
....print(L)
```

```
def piece (n) :
    if (n%2) != 0 :
        return (False)
    L=['P' for k in range (n)]
    print(L)
    for i in range (n) :
        S=L[i]
        L=L[:i]+L[i+1:]
        for k in range (n-1) :
            if L[k]=='P':
                L[k]='F'
            else :
                L[k]='P'
        L=L[:i]+[S]+L[i:]
        print (L)
```

◦41◦ Calculez module et argument de $\sqrt{2+\sqrt{2}}+i.\sqrt{2-\sqrt{2}}$.

Son module vaut $\sqrt{2+\sqrt{2}+2-\sqrt{2}}$ c'est à dire 2.
Et son argument est un angle de $]0,\ \pi/2[$ dont la tangente se calcule

$$\frac{\sqrt{2-\sqrt{2}}}{\sqrt{2+\sqrt{2}}}=\frac{2-\sqrt{2}}{\sqrt{2+\sqrt{2}}.\sqrt{2-\sqrt{2}}}=\frac{2-\sqrt{2}}{\sqrt{4-2}}=\sqrt{2}-1$$

On connait : $\pi/8$ et donc : $\boxed{\sqrt{2+\sqrt{2}}+i.\sqrt{2-\sqrt{2}}=2.e^{i.\pi/8}}$

◦42◦ **Ce chacal urine. Le baron guéri. Bon, rions ! Me voilà, trolls affriolants ! Un raton. Essai de défi transcendant. Élu gratiné. Y grec ! Magyare stalinienne. Sylvie a dessiné. L'apaisé s'y amusa, ils virent César hélas ! Fard de gala en déshérence.** Là, on est sur des lignes de R.E.R. à moins de dix minutes de **prias** ou aux terminus.

Ce chacal urine. Arcueil-Cachan.
Le baron guéri. Bourg la Reine.
Bon, rions ! Robinson.
Me voilà, trolls affriolants ! Maisons-Alfort Alfortville.
Un raton. Tournan.
Essai de défi transcendant. Stade de France Saint-Denis.
Élu gratiné. Argenteuil.
Y grec ! Cergy.
Magyare stalinienne. Saint-Germain en Laye.
Fard de gala en déshérence. La Défense. Grande Arche.
Sylvie a dessiné. Issy-Val de Seine.
L'apaisé s'y amusa, Massy-Palaiseau.
ils virent César hélas ! Versailles-Chantiers.

◦43◦ On pose `M = [[-8, 6, 3], [-9, 7, 3], [0, 0, 1]]`. Donnez son polynôme caractéristique et son spectre. On pose $A = \frac{M+2.I_3}{3}$ et $B = \frac{I_3 - M}{3}$. Calculez $A.B$, $B.A$, A^2, B^2 et A^n pour tout n. Exprimez M à l'aide de A et B. Déduisez la forme de M^n.

On part de $\begin{pmatrix} -8 & 6 & 3 \\ -9 & 7 & 3 \\ 0 & 0 & 1 \end{pmatrix}$. On trouve sa trace : 0, son déterminant (dernière ligne) : -2, et la somme de ses mineurs de taille 2 : $\begin{vmatrix} 7 & 3 \\ 0 & 1 \end{vmatrix} + \begin{vmatrix} -8 & 3 \\ 0 & 1 \end{vmatrix} + \begin{vmatrix} -8 & 6 \\ -9 & 7 \end{vmatrix}$.

Le polynôme caractéristique se calcule aussi vite $\begin{vmatrix} -8-X & 6 & 3 \\ -9 & 7-X & 3 \\ 0 & 0 & 1-X \end{vmatrix} = (1-X).\begin{vmatrix} -8-X & 6 \\ -9 & 7-X \end{vmatrix}$

Sous forme développée : $\boxed{X^3 - 3.X + 2}$ et sous forme factorisée $\boxed{(X-1)^2.(X-2)}$

Le spectre est $[1,\ 1,\ -2]$, en mentionnant que 1 est valeur propre double.

On sait que ça pose problème pour la diagonalisation. Mais ce n'est pas forcément un obstacle complet. Il se peut qu'on trouve un plan entiers de vecteurs propres pour la valeur propre 1. Ici, ce serait d'ailleurs le cas. Mais on va suivre une autre méthode.

On calcule donc $A = \frac{M+2.I_3}{3} = \begin{pmatrix} -2 & 2 & 1 \\ -3 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ et $B = \frac{I_3 - M}{3} = \begin{pmatrix} 3 & -2 & -1 \\ 3 & -2 & -1 \\ 0 & 0 & 0 \end{pmatrix}$.

On effectue

	A	B
A	A	$0_{3,3}$
B	$0_{3,3}$	B

Par récurrence immédiate : $\boxed{\forall n \in \mathbb{N}^*,\ A^n = A}$

On initialise à 1, c'est évident, et pour l'hérédité : $A^{n+1} = A^n.A = A.A = A$. C'est tout.

Comment perdre des points sur cette question : écrire $\forall n \in \mathbb{N},\ A^n = A$ au lieu de $\forall n \in \mathbb{N}^*,\ A^n = A$. La formule n'est pas valable pour n égal à 0.
Comment perdre du temps sur cette formule (comme la grosse majorité des élèves hélas, mais ce n'est pas grave, il y a de la place en non étoile pour une majorité d'élèves...) : on calcule tout au niveau des coefficients avec des colonnes qui tombent sur des lignes... alors qu'on a fait une fois le seul calcul utile : $A^2 = A$; il ne reste plus qu'à travailler à l'étage des matrices tout de suite...

On fait de même : $B^n = B$ pour tout n de $\mathbb{N}^*$

En fait, A et B sont des matrices de projecteurs.

On reconstruit : $\boxed{M = A - 2.B}$ On élève à la puissance n par la formule du binôme de Newton et tous ceux qui l'ont précédé *(on se doit de justifier : $A.B = B.A$)* $\boxed{M^n = \sum_{k=0}^{n} \binom{n}{k}.A^{n-k}.(-2.B)^k}$

Mais dans cette formule, dès que A rencontre B, il ne reste rien puisque $A.B = 0_{3,3}$.
Il n'y a que deux termes : $k = 0$ et $k = n$: $M^n = A^n + (-2)^n.B^n = A + (-2)^n.B$

$$M^n = \begin{pmatrix} -2 & 2 & 1 \\ -3 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix} + (-2)^n.\begin{pmatrix} 3 & -2 & -1 \\ 3 & -2 & -1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -2+3.(-2)^n & 2-2.(-2)^n & 1-(-2)^n \\ -3+3.(-2)^n & 3-2.(-2)^n & 1-(-2)^n \\ 0 & 0 & 1 \end{pmatrix}$$

On aurait pu conjecturer vite cette formule, puis la prouver par récurrence sur n.
Le bloc $\begin{pmatrix} -2+3.(-2)^n & 2-2.(-2)^n \\ -3+3.(-2)^n & 3-2.(-2)^n \end{pmatrix}$ correspond à la diagonalisation élémentaire de $\begin{pmatrix} -8 & 6 \\ -9 & 7 \end{pmatrix}$, comme on pouvait s'y attendre.

◦44◦ En quel point du graphe de $x \longmapsto x^2$ la tangente au graphe passe-t-elle par $(1, -2)$? En quel point du graphe de $x \longmapsto x^2$ la tangente au graphe est elle à égale distance de $(1, -2)$ et de $(0, 0)$?

L'équation de la tangente au graphe en a est $y = 2.a.(x-a) + a^2$ (forme $y = f'(a).(x-a) + f(a)$).
On veut qu'elle passe par $(1,\ -2)$: $-2 = 2.a.(1-a) + a^2$. On résout : $a = 1 + \sqrt{3}$ et $a = 1 - \sqrt{3}$.

On mesure pour la seconde partie de l'exercice, la distance d'un point à une droite.
La formule est dans le cours : mettre les coordonnées du point dans l'équation normalisée de la droite.

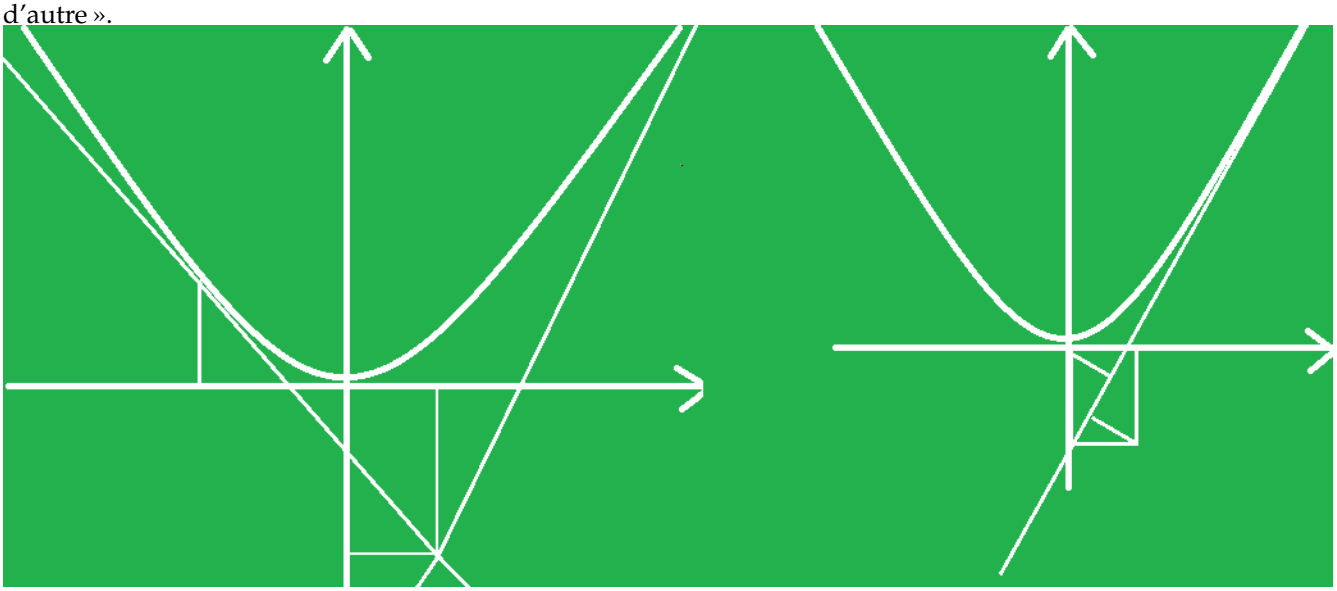
Équation de la droite T_a	Équation normalisée	Distance	Distance à $(0,\ 0)$
$2.a.x - y - a^2 = 0$	$\frac{2.a.x - y - a^2}{\sqrt{4.a^2+1}} = 0$	$\frac{2.a + 2 - a^2}{\sqrt{4.a^2+1}}$	$\frac{a^2}{\sqrt{4.a^2+1}}$

On nous force et contraint à résoudre $|2.a + 2 - a^2| = a^2$.

On distingue deux équations possibles :

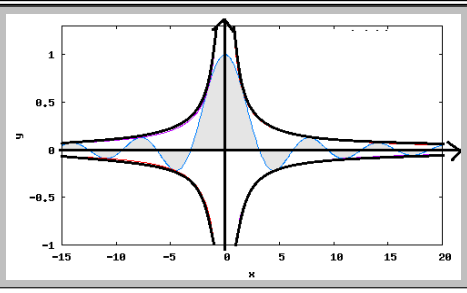
$2.a+2-a^2=a^2$	$-2.a-2+a^2=a^2$
$\frac{1+\sqrt{5}}{2}$ et $\frac{1-\sqrt{5}}{2}$	$a=-1$

On a deux familles de solutions, car les deux points peuvent être du même côté de la tangente, ou « de part et d'autre ».



◦45◦

On définit : $f = x \longmapsto \frac{\sin(x)}{x}$. Montrez qu'on prolonge f par continuité en 0. Montrez que f est dérivable en 0 *(limite de taux d'accroissements)*. Calculez aussi $f''(0)$ après en avoir prouvé l'existence par limité de taux d'accroissements.
On admet que f est de classe C^∞. En utilisant la formule de Leibniz pour $f.Id$, calculez $f^{(n)}(0)$ pour tout n.



La limite de f en 1 vient de l'équivalent classique $\sin(x) \sim_{x\to 0} x$.
Ou de la limite de taux d'accroissement $\frac{\sin(x)-\sin(0)}{x-0}$.

Mais maintenant les taux de f :

$$\frac{f(x)-f(0)}{x-0} = \frac{\frac{\sin(x)}{x}-1}{x} = \frac{\sin(x)-x}{x^2} = \frac{x-\frac{x^3}{6}+o(x^3)-x}{x^2} = -\frac{x}{6}+o(x)$$

f est dérivable en 0 et $f'(0)$ est nul.

On a $f.Id = \sin$ (à l'étage des fonctions).

On dérive n fois le premier membre par la formule de Leibniz :

$$(f.Id)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} . f^{(n-k)}.Id^{(k)} = \sum_{k=0}^{1} \binom{n}{k} . f^{(n-k)}.Id^{(k)} = 1.f^{(n)}.Id + n.f^{(n-1)}$$

On calcule en 0 et il ne reste que $n.f^{(n-1)}(0) = \sin^{(n)}(0)$.
Mais les dérivées successives du sinus sont connues. On décalle d'un cran pour la lisibilité :

$$f^{(p)}(0) = \frac{\sin^{(p+1)}(0)}{p+1} = \begin{array}{llll} \frac{1}{p+1} & si & p= & 0\ [4] \\ 0 & si & p= & 1\ [4] \\ \frac{-1}{p+1} & si & p= & 2\ [4] \\ 0 & si & p= & 3\ [4] \end{array}$$

◦46◦ Donnez (si vous la trouvez) la limite de $\frac{1}{n}+\frac{1}{n}+\ldots+\frac{1}{n}$ quand n tend vers l'infini.

Bon, c'est clair, ça n'a pas de sens.
Si les points de suspension disent qu'il y a k termes avec k donné, la somme tend vers 0.
Si les points de suspension disent qu'il y a n termes (la variable), la somme tend vers 1.
Et si les points de suspensions disent qu'il y en a $2.n$, la somme converge vers 2.
Et je vous laisse compter les termes pour qu'elle tend vers $+\infty$.

◦47◦ ♡ Montrez que $\sqrt{n^2+3}-\sqrt{n^2+1}$ est équivalent à $\frac{1}{n}$ quand n tend vers l'infini.
Est-il équivalent à $\frac{1}{n}+\frac{1}{n^2}$ quand n tend vers l'infini ?

La quantité conjuguée ! Vous y pensez ?

$$\sqrt{n^2+3}-\sqrt{n^2+1}=\frac{(n^2+3)-(n^2+1)}{\sqrt{n^2+3}+\sqrt{n^2+1}}=\frac{2}{\sqrt{n^2+3}+\sqrt{n^2+1}}$$

A présent, le numérateur vaut 2 et le dénominateur est équivalent à $2.n$.
Si on doit le justifier par un quotient :

$$\frac{\frac{2}{\sqrt{n^2+1}+\sqrt{n^2+3}}}{\frac{1}{n}}=\frac{2}{\sqrt{1+\frac{3}{n^2}}+\sqrt{1+\frac{1}{n^2}}}$$

Il tend bien vers 1.

Et le terme $\frac{1}{n^2}$ne dit rien de plus.

$$\frac{\frac{2}{\sqrt{n^2+1}+\sqrt{n^2+3}}}{\frac{1}{n}+\frac{1}{n^2}}=\frac{1}{1+\frac{1}{n}}\times\frac{2}{\sqrt{1+\frac{3}{n^2}}+\sqrt{1+\frac{1}{n^2}}}$$

En fait,

$$\sqrt{n^2+3}-\sqrt{n^2+1}\sim\frac{1}{n}\sim\frac{1}{n}+\frac{1}{n^2}\sim\frac{1}{n}+\frac{123}{n^2}\sim\frac{1}{n}-\frac{\pi^4}{n^2}\sim\frac{1}{n}+\frac{10^{13}.e^6}{n.\sqrt{n}}$$

et ainsi de suite

CCP 2009 MP 3 heures

I∼0) p et q sont deux entiers naturels. Montrez que $((1,0),\ (X,0),\ldots,(X^{p-1},0),\ (0,1),\ (0,X),\ldots(0,X^{q-1}))$ est une base de $\mathbb{C}_{p-1}[X]\times\mathbb{C}_{q-1}[X]$ (base notée $\mathbb{B}$, espace vectoriel noté E).

Comme on ne connaît pas a priori la dimension de l'espace vectoriel (sauf à dire que la famille proposée est déjà une base), on va montrer que touté élément se décompose suivant cette famille, d'une façon unique.

Un élément $\mathbb{C}_{p-1}[X]\times\mathbb{C}_{q-1}[X]$ est de la forme $(P,\ Q)$ avec $P=\sum_{i=0}^{p-1}\lambda_i.X^i$ et $Q=\sum_{j=0}^{q-1}\mu_j.X^j$.

On écrit alors $(P,\ Q)=(P,\ 0)+(0,\ Q)$

$$(P,\ Q)=\Big(\sum_{i=0}^{p-1}\lambda_i.X^i,\ 0\Big)+\Big(0,\ \sum_{j=0}^{q-1}\mu_j.X^j\Big)$$

$$(P,\ Q)=\sum_{i=0}^{q-1}\lambda_i.\Big(X^p,\ 0\Big)+\sum_{j=0}^{q-1}\mu_j.\Big(0,\ .X^j\Big)$$

Le caractère générateur est obtenu.
On se donne ensuite $p+q$ complexes (de λ_0 à λ_{p-1} et de μ_0 à μ_{q-1}).

On suppose $\sum_{i=0}^{p-1}\lambda_i.\Big(X^i,\ 0\Big)+\sum_{j=0}^{q-1}\mu_j.\Big(0,\ .X^j\Big)=(0,\ 0)$.

On refait le calcul précédent en sens inverse, jusqu'à aboutir à $\Big(\sum_{i=0}^{p-1}\lambda_i.X^i,\ \sum_{j=0}^{q-1}\mu_j..X^j\Big) = (0,\ 0)$.

On identifie (couple) : $\sum_{i=0}^{p-1}\lambda_i.X^i = 0$ et $\sum_{j=0}^{q-1}\mu_j..X^j = 0$.

On identifie (bases de $(\mathbb{C}_{truc}[X],+,.)$) : tous les λ_i et tous les μ_j sont nuls.

Il s'ensuit que E est de dimension $p+q$.
C'est bon signe pour le mettre en bijection avec $(\mathbb{C}_{p+q-1}[X],+,.)$.

I∼1) A et B sont deux polynômes, de degrés respectifs q et p, qu'on écrira sous forme factorisée $A(X) = \lambda_A.\prod_{j=1}^{q}(X-\alpha_j)$ et $B(X) = \lambda_B.\prod_{j=1}^{p}(X-\beta_j)$ mais aussi développée sur la base canonique $A(X) = \sum_{k=0}^{q}a_k.X^k$ et $B(X) = \sum_{k=0}^{p}b_k.X^k$. On définit f sur E par $f((P,Q)) = A.P + B.Q$. Montrez que f est linaire.
Montrez que $Im(f)$ est inclus dans $\mathbb{C}_{p+q-1}[X]$.

f prend un couple de polynômes et associe un nouveau polynôme *(il faut parler de polynôme avant de parler de degré, non ?)*..

Regardons le degré :

A	P	B	Q
degré $= q$	degré $\leqslant p-1$	degré $= p$	degré $\leqslant q-1$
$A.P$		$B.Q$	
degré $\leqslant q+p-1$		degré $\leqslant q+p-1$	
$A.P + B.Q$			
degré $\leqslant p+q-1$			

Rappel : $\deg(P.Q) = \deg(P) + \deg(Q)$ et $\deg(P.Q) \leqslant Max(\deg(P),\ \deg(Q))$.

Pour la linéarité de f, il faut se souvenir qu'au départ on a des couples.
On prend donc deux couples : $(P_1,\ Q_1)$ et $(P_2,\ Q_2)$.
On calcule la somme : $(P_1,\ Q_1) + (P_2,\ Q_2) = (P_1+P_2,\ Q_1+Q_2)$
puis l'image de la somme : $f((P_1+P_2,\ Q_1+Q_2)) = A.(P_1+P_2) + B.(Q_1+Q_2)$.
On distribue et regroupe, et c'est un jeu d'enfant de retrouver $f((P_1,\ Q_1)) + f((P_2,\ Q_2))$.

On se donne ensuite un réel (un seul !) : α. On multiplie le couple par α : $\alpha.(P_1,\ Q_1) = (\alpha.P_1,\ \alpha.Q_1)$.
On calcule son image : $A.(\alpha.P_1) + B.(\alpha.Q_1)$ et on peut mettre α en facteur : $\alpha.(A.P_1 + B.Q_1)$.

I∼2) On rappelle qu'on pose $Ker(f) = \{(P,Q) \in E \mid f((P,Q)) = 0\}$. Montrez que $Ker(f)$ est un sous-espace vectoriel de $(E,+,.)$.

On définit le noyau de f linéaire. Il faut montrer que c'est un espace vectoriel. De fait, un sous-espace vectoriel de l'espace de départ.
On va dire que c'est un résultat général, et même du cours bientôt...
On prend f linéaire de $(E,+,.)$ dans $(F,+,.)$.
Le vecteur nul de E est dans le noyau : $f(\overrightarrow{0}) = f(0.\overrightarrow{0}) = 0.f(\overrightarrow{0}) = \overrightarrow{0}$.
On prend deux vecteurs $\overrightarrow{u}$ et $\overrightarrow{v}$ dans le noyau ($f(\overrightarrow{u}) = \overrightarrow{0}$ et $f(\overrightarrow{v}) = \overrightarrow{0}$). On se donne deux complexes α et β.
Par linéarité $f(\alpha.\overrightarrow{u} + \beta.\overrightarrow{v}) = \alpha.f(\overrightarrow{u}) + \beta.f(\overrightarrow{v}) = \alpha.\overrightarrow{0} + \beta.\overrightarrow{0} = \overrightarrow{0}$. On reconnaît : $\alpha.\overrightarrow{u} + \beta.\overrightarrow{v}$ est dans le noyau.

I∼3) Montrez que f est injective, si et seulement si $Ker(f)$ est égal à $\{(0,\ 0)\}$.

C'est du cours aussi que de dire que f est injective si et seulement si son noyau est réduit au seul vecteur nul.
$\boxed{\Rightarrow}$ On suppose f injective.
Le vecteur nul est dans le noyau ($f(\backslash vo) = \overrightarrow{0}$ déjà vu) : $\{\overrightarrow{0}\} \subset Ker(f)$.
Prenons un (autre ?) vecteur du noyau : $\overrightarrow{u}$. On traduit : $f(\overrightarrow{u}) = \overrightarrow{0} = f(\overrightarrow{0})$.
Par injectivité de f : $\overrightarrow{u} = \overrightarrow{0}$. Le vecteur nul est donc tout seul dans le noyau.

$\boxed{\Leftarrow}$ On suppose que le noyau est réduit au vecteur nul.
On veut montrer que f est injective. On prend $\overrightarrow{u}$ et $\overrightarrow{v}$ ayant la même image.
On traduit : $f(\overrightarrow{u}) = f(\overrightarrow{v})$. On transforme en $f(\overrightarrow{u}) - f(\overrightarrow{v}) = \overrightarrow{0}$ puis $f(\overrightarrow{u} - \overrightarrow{v}) = \overrightarrow{0}$ (par linéarité).
Le vecteur $\overrightarrow{u} - \overrightarrow{v}$ est dans le noyau. Il est donc nul (seul vecteur du noyau). Ayant $\overrightarrow{u} - \overrightarrow{v} = \overrightarrow{0}$, on a bien $\overrightarrow{u} = \overrightarrow{v}$.

I∼4) Montrez que si A et B ont une racine commune r si et seulement $Ker(f)$ n'est pas réduit à $(0,\ 0)$.

Passons à la partie qui n'est pas du cours.
On suppose que A et B ont une racine commune r. Sans perdre la généralité (quitte à ré-indexer l'ordre des racines), on peut dire : $r = \alpha_1 = \beta_1$.
On veut trouver P et Q vérifiant $A.P + B.Q = 0$.
Facile, il suffit de prendre $P = B$ et $Q = -A$: $A.B + B.(-A) = A.B - B.A = 0$ (ce sont des polynômes, pas des matrices).
Mais voilà, B est de degré p et dans la forme $A.P + B.Q$, P doit être de degré $p - 1$.
Pareil pour Q.
Mais si on se passait du terme commun ? Pour ne pas l'avoir en double.
On a $A(X) = \lambda_A.(X - r).\prod_{j=2}^{q}(X - \alpha_j)$ et $B(X) = \lambda_B.(X - r).\prod_{j=2}^{p}(X - \beta_j)$.

Posons $P(X) = \lambda_B.\prod_{j=2}^{p}(X - \beta_j)$ et $Q(X) = -\lambda_A.\prod_{j=2}^{q}(X - \alpha_j)$ (toutes les racines, sauf r).
Cette fois, P est de degré$p - 1$ et Q est de degré $q - 1$.
On calcule : $A(X).P(X) = \lambda_A.(X - r).\prod_{j=2}^{q}(X - \alpha_j).\lambda_B.\prod_{j=2}^{p}(X - \beta_j)$

$$\text{et } B(X).Q(X) = -\lambda_B.(X - r).\prod_{j=2}^{p}(X - \beta_j).\lambda_A.\prod_{j=2}^{q}(X - \alpha_j).$$

ce sont les mêmes polynômes, au signe près. La somme est bien nulle.
Le couple $\left(\lambda_B.\prod_{j=2}^{p}(X - \beta_j),\ -\lambda_A.\prod_{j=2}^{q}(X - \alpha_j)\right)$ est bien dans le noyau.
En toute généralité, si la racine commune était $\alpha_{i_0} = \beta_{j_0}$on aurait pris $\left(\lambda_B.\prod_{i\neq i_0}(X - \beta_j),\ -\lambda_A.\prod_{j\neq j_0}(X - \alpha_j)\right)$

On va prouver la réciproque. On suppose que A et B n'ont aucune racine commune.
Il faut alors prouver que le noyau est réduit à 0.
Il faut alors prouver que le noyau est réduit à $\overrightarrow{0}$. Parlons vecteurs !
Il faut alors prouver que le noyau est réduit à $(0,\ 0)$. Mais les vecteurs sont des couples de polynômes.
Prenons un couple $(P,\ Q)$ dans le noyau. On a alors $A.P + B.Q = 0$.
On fait passer de l'autre côté : $-A.P = B.Q$.
A divise le premier membre.
Il divise donc le second.
Mais que dit le lemme de Gauss : si A divise $B.Q$ mais est premier avec B alors A divise Q.

> *Le lemme de Gauss est connu pour les entiers : si a divise b.q et que a est premier avec b alors il divise q.*
> *Mais ici, c'est quoi des polynômes premiers entre eux dans $\mathbb{C}$?*
> *C'est des polynômes sans racines commune ?*
> *Oui. Et c'est donc le cas pour A et B.*
> *Mais sinon, prenons une à une les racine α_i de A.*
> *On a $A(\alpha_i) = 0$. On reporte : $0 = -A(\alpha_i).P(\alpha_i) = B(\alpha_i).Q(\alpha_i)$.*
> *Comme $B(\alpha_i)$ est non nul (pas de racine commune), on a forcément $Q(\alpha_i)$.*
> *Le polynôme Q a les mêmes racines que A, il est divisible par A.*
> *Même si il y a des racines multiples...*

Que fait on maintenant que A divise Q ? on regarde les degrés.
A est de degré q et Q est de degré inférieur ou égal à $q - 1$.
Il y a une contradiction dont on ne se tire qu'en ayant $Q = 0$ (polynôme nul).

On reporte ce $Q = 0$ dans $A.P + B.Q = 0$.
On trouve $A.P = 0$. Et par intégrité dans l'espace des polynômes : P est nul à son tour.

On a bien « A et B n'ont pas de racine commune implique $Ker(f) = \{[0,\ 0)\}$ ».

		f injective avec $f=(P,Q)\longmapsto A.P+B.Q$
A ce stade	$\Leftrightarrow$	$Ker(f)=0$
	$\Leftrightarrow$	A et B n'ont pas de racine commune

On va compléter avec la bijectivité (car les deux espaces ont la même dimension) et le théorème de Bézout : $\exists(P,Q)\in E,\ A.P+B.Q=1$.

I∼5) **Montrez que l'ensemble des $f(C)$ quand C décrit $\mathbb{B}$ est une famille génératrice de $Im(f)$.**

C'est un résultat du cours que l'image d'une famille génératrice du départ est une famille génératrice de d'image. Ou que l'image d'une base du départ est une famille génératrice de l'image.

Prenons un vecteur $\overrightarrow{v}$ de l'image de f. Il s'écrit $f(\overrightarrow{a})$ pour au moins un $\overrightarrow{a}$ de E.

On décompose ce $\overrightarrow{a}$ sous la forme $\Big(\sum_{i=0}^{p-1}\lambda_i.X^i,\ \sum_{j=0}^{q-1}\mu_j..X^j\Big)$.

Par définition : $\overrightarrow{u}=f\Big(\Big(\sum_{i=0}^{p-1}\lambda_i.X^i,\ \sum_{j=0}^{q-1}\mu_j..X^j\Big)\Big)$

par linéarité $\overrightarrow{u}=\sum_{i=0}^{p-1}\lambda_i.f((X^i,\ 0))+\sum_{j=0}^{q-1}\mu_j.f((0,\ .X^j))$.

Le vecteur $\overrightarrow{u}$ est combinaison linéaire des $f(C)$ lorsque C décrit la liste double des $f((X^i,\ 0))$ et des$f((0,\ X^j))$.
Il est combinaison des vecteurs de la famille image de la base.

La lourdeur vient ici de ce que la base est lourde d'écriture avec des couples.
Reprenons le cas général.
On prend $\overrightarrow{u}$ dans l'ensemble image. Il s'écrit $\overrightarrow{u}=f(\overrightarrow{a})$ pour au moins un vecteur $\overrightarrow{a}$ de E.
Ce $\overrightarrow{a}$ se décompose en $\sum_{i=1}^{d}x_i.\overrightarrow{e_i}$.
Par linéarité : $\overrightarrow{u}=f(\overrightarrow{a})=f\Big(\sum_{i=1}^{d}x_i.\overrightarrow{e_i}\Big)=\sum_{i=1}^{d}x_i.f(\overrightarrow{e_i})$.
On reconnaît $\overrightarrow{u}\in Vect(f(\overrightarrow{e_1}),\dots f(\overrightarrow{e_d}))$.

I∼6) **Montrez que c'est une base de $Im(f)$ si et seulement si $Ker(f)$ est réduit à $\{(0,0)\}$.**

Ayant une famille génératrice de $Im(f)$, elle sera une base de $Im(f))$ si et seulement si elle est libre.
Sa liberté va être liée à l'injectivité de f et au noyau. C'est du cours là encore.
Je garde l'idée d'appeler $\overrightarrow{e_1}$ à $\overrightarrow{e_{p+q}}$ les vecteurs de la base de E, de $(1,\ 0)$ jusqu'à $(0,\ X^{q-1})$ en passant par $(X^{p-1},\ 0)$ et $(0,\ 1)$ à la « mi-parcours ».

$\boxed{\Rightarrow}$ On suppose que le noyau de f est réduit à $\overrightarrow{0}$, on va montrer que la famille des images $(f(\overrightarrow{e_1}),\dots f(\overrightarrow{e_{p+q}}))$ est libre.

On suppose donc qu'on a une combinaison $\sum_{i=1}^{p+q}\lambda_i.f(\overrightarrow{e_i})$ qui est nulle.

On écrit alors par linéarité : $f\Big(\sum_{i=1}^{p+q}\lambda_i.\overrightarrow{e_i}\Big)=\overrightarrow{0}$.

On reconnaît : $\sum_{i=1}^{p+q}\lambda_i.\overrightarrow{e_i}\in Ker(f)$.

Mais comme le noyau est réduit à $\overrightarrow{0}$ (en fait ici le couple de polynôme $(0,\ 0)$), on a $\sum_{i=1}^{p+q}\lambda_i.\overrightarrow{e_i}=\overrightarrow{0}$.

Il est temps d'utiliser que les $\overrightarrow{e_i}$ forment une base de E (donc une famille libre) : les λ_i sont tous nuls.

$\boxed{\Leftarrow}$ On suppose que que la famille des images $f(\overrightarrow{e_1},\dots\overrightarrow{e_{p+q}})$ est libre et génératrice de $Im(f)$, on va que le noyau de f est réduit à $\overrightarrow{0}$.
Déjà, le vecteur $\overrightarrow{0}$ est dans le noyau.
Prenons un (autre ?) vecteur du noyau. Est il forcément nul ?
C'est un $\overrightarrow{a}$ de $(E,+,.)$ vérifiant $f(\overrightarrow{a})=\overrightarrow{0}$ *(vecteur nul à l'arrivée)*.
On décompose $\overrightarrow{a}$ sur la base de départ : $\overrightarrow{a}=\sum_i\lambda_i.\overrightarrow{e_i}$ *(on n'en est pas encore à « il est nul », je le concède...)*.

Par définition et par linéarité $\overrightarrow{0} = f(\overrightarrow{a}) = f\Big(\sum_i \lambda_i.\overrightarrow{e_i}\Big) = \sum_i \lambda_i.f(\overrightarrow{e_i})$.

Mais la famille des $f(\overrightarrow{e_i})$ est supposée libre.
On en déduit que les λ_i sont nuls *(on approche)*.
On reporte : $\overrightarrow{a} = \sum_i 0.\overrightarrow{e_i} = \overrightarrow{0}$.

I∼7) Montrez que f est bijective de E dans $(\mathbb{C}_{p+q-1}[X], +, .)$ si et seulement si $Ker(f)$ est réduit à $\{(0,0)\}$.

La famille des images a pour cardinal $p+q$.
On a donc prouvé que $Im(f)$ est de dimension $p+q$ si et seulement si $Ker(f)$ est réduit à $\overrightarrow{0}$.

Mais $Im(f)$ est inclus dans $\mathbb{C}_{p+q-1}[X]$ qui est lui même de dimension $p+q$.
Un de nos théorèmes pour flemmards dit « un espace vectoriel F inclus dans G est égal à G si et seulement F et G ont la même dimension ».

Ici, on a donc finalement

	A et B n'ont pas de racine commune		f est bijective de E dans $\mathbb{C}_{p+q-1}[X]$
$\Leftrightarrow$	$Ker(f) = 0$		
$\Leftrightarrow$	f est injective		
$\Leftrightarrow$	$(f(\overrightarrow{e_1}), \dots f(\overrightarrow{e_{p+q}}))$ est libre		
$\Leftrightarrow$	$(f(\overrightarrow{e_1}), \dots f(\overrightarrow{e_{p+q}}))$ est une base de $Im(f)$		
$\Leftrightarrow$	$Im(f) = \mathbb{C}_{p+q-1}[X]$		
$\Leftrightarrow$	f est bijective de E dans $\mathbb{C}_{p+q-1}[X]$		

On va compléter ensuite avec $\det(M_{A,B}) \neq 0$.

$II \sim 0$ On construit la matrice $M_{A,B}$:

$$\begin{pmatrix} a_0 & & & & b_0 & & \\ a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & & a_0 & & \vdots & & b_0 \\ a_q & & a_1 & a_0 & \vdots & & b_1 \\ & \ddots & \vdots & a_1 & b_p & & \vdots \\ & & a_q & & & \ddots & \vdots \\ & & & a_q & & & b_q \end{pmatrix}$$

Elle est de format $p+q$ sur $p+q$ et les positions non remplies sont des 0.
Par exemple $A = 1 + 2.X + 3.X^2$
et $B = 4 + 5.X + 6.X^2 + 7.X^3$:

$$\begin{pmatrix} 1 & 0 & 0 & 4 & 0 \\ 2 & 1 & 0 & 5 & 4 \\ 3 & 2 & 1 & 6 & 5 \\ 0 & 3 & 2 & 7 & 6 \\ 0 & 0 & 3 & 0 & 7 \end{pmatrix}.$$

Calculez le déterminant de cette matrice $M_{A,B}$ donnée en exemple à droite.

$$\begin{vmatrix} 1 & 0 & 0 & 4 & 0 \\ 2 & 1 & 0 & 5 & 4 \\ 3 & 2 & 1 & 6 & 5 \\ 0 & 3 & 2 & 7 & 6 \\ 0 & 0 & 3 & 0 & 7 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 4 & 0 \\ 0 & 1 & 0 & -3 & 4 \\ 0 & 2 & 1 & -6 & 5 \\ 0 & 3 & 2 & 7 & 6 \\ 0 & 0 & 3 & 0 & 7 \end{vmatrix}$$ par combinaison $L_2 = L_2 - 2.L_1$ et $L_3 = l_3 - 3.L_1$.

On développe par rapport à la première colonne et on recommence :

$$\begin{vmatrix} 1 & 0 & 0 & 4 & 0 \\ 2 & 1 & 0 & 5 & 4 \\ 3 & 2 & 1 & 6 & 5 \\ 0 & 3 & 2 & 7 & 6 \\ 0 & 0 & 3 & 0 & 7 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -3 & 4 \\ 2 & 1 & -6 & 5 \\ 3 & 2 & 7 & 6 \\ 0 & 3 & 0 & 7 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -3 & 4 \\ 0 & 1 & 0 & -3 \\ 0 & 2 & 16 & -6 \\ 0 & 3 & 0 & 7 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -3 \\ 2 & 16 & -6 \\ 3 & 0 & 7 \end{vmatrix}$$

On ajoute cette fois le triple de la première colonne sur la dernière $\begin{vmatrix} 1 & 0 & -3 \\ 2 & 16 & -6 \\ 3 & 0 & 7 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 2 & 16 & 0 \\ 3 & 0 & 16 \end{vmatrix}$.

Le résultat cherché vaut $\boxed{256}$ (ou même 2^8 si vous préférez).

II∼0) Calculez le déterminant de la matrice dans le cas $A = X^2 - 3.X + 2$ et $B = X^3 - 2.X^2 - 5.X + 6$.
La question est ensuite « êtes vous capables de comprendre une consigne de remplissage » et de l'appliquer : $A = X^2 - 3.X + 2$ et $B = X^3 - 2.X^2 - 5.X + 6$ sont donnés dans le mauvais sens pour la base « canonique ».

Avec $A = 2 - 3.X + X^2$ et $B = 6 - 5.X - 2.X^2 + X^3$: $\begin{pmatrix} 2 & 0 & 0 & 6 & 0 \\ -3 & 2 & 0 & -5 & 6 \\ 1 & -3 & 2 & -2 & -5 \\ 0 & 1 & -3 & 1 & -2 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$

La matrice est de taille 5. On agit en colonnes pour développer par rapport à la première ligne :

$$\begin{vmatrix} 2 & 0 & 0 & 6 & 0 \\ -3 & 2 & 0 & -5 & 6 \\ 1 & -3 & 2 & -2 & -5 \\ 0 & 1 & -3 & 1 & -2 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix} = \begin{vmatrix} 2 & 0 & 0 & 0 & 0 \\ -3 & 2 & 0 & 4 & 6 \\ 1 & -3 & 2 & -5 & -5 \\ 0 & 1 & -3 & 1 & -2 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix} = 2. \begin{vmatrix} 2 & 0 & 4 & 6 \\ -3 & 2 & -5 & -5 \\ 1 & -3 & 1 & -2 \\ 0 & 1 & 0 & 1 \end{vmatrix}$$

On continue en colonnes : $\begin{vmatrix} 2 & 0 & 0 & 6 & 0 \\ -3 & 2 & 0 & -5 & 6 \\ 1 & -3 & 2 & -2 & -5 \\ 0 & 1 & -3 & 1 & -2 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix} = 2. \begin{vmatrix} 2 & 0 & 4 & 6 \\ -3 & 2 & -5 & -7 \\ 1 & -3 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{vmatrix} = 2. \begin{vmatrix} 2 & 4 & 6 \\ -3 & -5 & -7 \\ 1 & 1 & 1 \end{vmatrix}$.

On termine avec Sarrus ou en nettoyant encore : $\begin{vmatrix} 2 & 0 & 0 & 6 & 0 \\ -3 & 2 & 0 & -5 & 6 \\ 1 & -3 & 2 & -2 & -5 \\ 0 & 1 & -3 & 1 & -2 \\ 0 & 0 & 1 & 0 & 1 \end{vmatrix} = 2. \begin{vmatrix} 2 & 2 & 4 \\ -3 & -2 & -4 \\ 1 & 0 & 0 \end{vmatrix} = 0.$

Tout ça pour arriver à « déterminant nul ».

II∼1) Écrivez une procédure `Python` qui prend en entrées deux listes de coefficients `A` et `B` (sur l'exemple ci dessus `[1, 2, 3]` et `[3, 4, 5]`) et retourne la matrice $M_{A,B}$ sous forme de liste de listes.

On doit d'abord mesurer la longueur de chaque liste A et B, et en déduire la taille de la matrice.
Attention, si A est de degré q, sa liste a $q+1$ coefficients.
Ensuite, on remplit a priori une matrice avec des 0 partout, puisque ce sont eux qui sont majoritaires.
Exemple : $A = 1 + 2.X + 3.X^2$ et $B = 4 + 5.X + 6.X^2 + 7.X^3$:
A=[1, 2, 3] et B=[4, 5, 6, 7]

```
q = len(A)-1 et p= len(B)-1
M = [[0 for k in range(p+q)] for i in range(p+q)]
```

On vient de créer $\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

On prend un par un les coefficients de A :

```
for i in range(len(A)) : c = A[i]
```

On les place dans les q premières colonnes en décalant peu à peu :

```
for k in range(q) : M[i+k][k] = c
```

	c	$k=0$	$k=1$	$k=2$
$i=0$	1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
$i=1$	2	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$
$i=2$	3	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 3 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 3 & 2 & 1 & 0 & 0 \\ 0 & 3 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 \\ 3 & 2 & 1 & 0 & 0 \\ 0 & 3 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 \end{pmatrix}$

On recommence avec les coefficients de B.

```
for i in range(len(B)) :
...c = B[i]
...for k in range(p) :
......M[i+k][q+k] = c
```

De $\begin{pmatrix} 1&0&0&0&0\\ 2&1&0&0&0\\ 3&2&1&0&0\\ 0&3&2&0&0\\ 0&0&3&0&0 \end{pmatrix}$ pour $i=0$ et $k=0$ à $\begin{pmatrix} 1&0&0&4&0\\ 2&1&0&5&4\\ 3&2&1&6&5\\ 0&3&2&7&6\\ 0&0&3&0&7 \end{pmatrix}$ pour $i=3$ et $k=1$.

```
def Mat(A,B) :
....q, p = len(A)-1, len(B)-1
....M = [[0 for k in range(p+q)] for i in range(p+q)]
....for i in range(len(A)) :
........c = A[i]
........for k in range(p) :
............M[i+k][k] = c
....for i in range(len(B)) :
........c = B[i]
........for k in range(q) :
............M[i+k][p+k] = c
....return M
```

II∼2) On appelle résultant de A et B le déterminant de la matrice $M_{A,B}$. Qui est le résultat de A et A ? Le résultant est il un opérateur commutatif ?

Quand B est égale à A, les colonnes sont égales deux à deux.
Le résultant de A et A est nul.
Et c'est vrai que A et A ont au moins une racine commune !

Si on permute A et B, on passe de

$$\begin{pmatrix} a_0 & & & & b_0 & & \\ a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & & a_0 & & \vdots & & b_0 \\ a_q & & a_1 & a_0 & \vdots & & b_1 \\ & \ddots & \vdots & a_1 & b_p & & \vdots \\ & & a_q & & & \ddots & \vdots \\ & & & a_q & & & b_q \end{pmatrix} \text{ à } \begin{pmatrix} b_0 & & & a_0 & & & b_0 & & \\ b_1 & \ddots & & a_1 & \ddots & & b_1 & \ddots & \\ \vdots & & b_0 & \vdots & & a_0 & \vdots & & b_0 \\ \vdots & & b_1 & a_q & & a_1 & a_0 & \vdots & b_1 \\ b_p & & \vdots & & \ddots & \vdots & a_1 & b_p & \vdots \\ & \ddots & \vdots & & & a_q & & \ddots & \vdots \\ & & b_q & & & & a_q & & b_q \end{pmatrix}$$

On a appliqué une permutation sur les colonnes. Un cycle.
Au mieux, les deux déterminants sont égaux. Au pire, il y a un changement de signes.

Sur un exemple : $\begin{vmatrix} 1&0&0&4&0\\ 2&1&0&5&4\\ 3&2&1&6&5\\ 0&3&2&7&6\\ 0&0&3&0&7 \end{vmatrix} = \begin{vmatrix} 0&0&4&0&1\\ 1&0&5&4&2\\ 2&1&6&5&3\\ 3&2&7&6&0\\ 3&0&7&0&0 \end{vmatrix} = \begin{vmatrix} 0&4&0&1&0\\ 0&5&4&2&1\\ 1&6&5&3&2\\ 2&7&6&0&3\\ 3&0&7&0&0 \end{vmatrix} = \begin{vmatrix} 4&0&1&0&0\\ 5&4&2&1&0\\ 6&5&3&2&1\\ 7&6&0&3&2\\ 0&7&0&0&3 \end{vmatrix}$

On a appliqué trois fois un cycle $\overrightarrow{(1\,2\,3\,4\,5)}$ de signature 1.

Sur un autre exemple : X^2-3 et $X^2-2.X-7$

$$\begin{vmatrix} -3&0&-7&0\\ 0&-3&-2&-7\\ 1&0&1&-2\\ 0&1&0&1 \end{vmatrix} = - \begin{vmatrix} 0&-7&0&-3\\ -3&-2&-7&0\\ 0&1&-2&1\\ 1&0&1&0 \end{vmatrix} = \begin{vmatrix} -7&0&-3&0\\ -2&-7&0&-3\\ 1&-2&1&0\\ 0&1&0&1 \end{vmatrix}$$

avec cette fois deux quadricycles ayant chacun pour signature -1.

Globalement, le grand cycle de taille $(p+q)$ a pour signature $(-1)^{p+q-1}$.
On l'applique p fois. Le signe est $(-1)^{p.(p+q-1)}$.

II∼3) Calculez le résultant de A et A' quand A est le polynôme $a.X^2+b.X+c$.

Pour $A = c + b.X + a.X^2$ (et $A' = b + 2.a.X$) , la matrice est de taille 3 :
$\begin{pmatrix} c & b & 0 \\ b & 2.a & b \\ a & 0 & 2.a \end{pmatrix}$ a pour déterminant $\boxed{a.(4.a.c - b^2)}$

II∼4) Calculez le résultant de A et A' quand A est le polynôme $X^3 + a.X + b$.

Pour $A = b + a.X + X^3$ (et $A' = a + 3.X^2$) , la matrice est de taille 5 :
$\begin{pmatrix} b & 0 & a & 0 & 0 \\ a & b & 0 & a & 0 \\ 0 & a & 3 & 0 & a \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{pmatrix}$ a pour déterminant $\boxed{4.a^3 + 27.b^2}$ *(jouer sur les colonnes pour que les* 1 *en bas effacent les* 3*).*

III∼0) Montrez que si le couple de polynômes $(P,\ Q)$ a pour composantes sur la base E le vecteur U, alors le polynôme $f((P,\ Q))$ a pour composantes $M_{A,B,}.U$ sur la base canonique de $(\mathbb{C}_{p+q-1}[X], +, .)$.

On se donne deux polynômes P et Q qu'on écrit respectivement $\sum_{i=0}^{p-1} \lambda_i.X^i$ et $\sum_{j=0}^{q-1} \mu_j.X^j$.

Le couple $(P,\ Q)$ a pour composantes sur la base canonique le grand vecteurs fait des λ_i et des μ_j, de taille $p + q$.
On va calculer son image $A.P + B.Q$ et la décomposer sur la base canonique de $(\mathbb{C}_{p+q-1}[X], +, .)$:
$\Big(\sum_{k=0}^{q} a_k.X^k\Big).\Big(\sum_{i=0}^{p-1} \lambda_i.X^i\Big) + \Big(\sum_{m=0}^{p} b_m.X^m\Big).\Big(\sum_{j=0}^{q-1} \mu_j.X^j\Big)$.
On développe et o,n cherche le terme en X^n pour chaque n de 0 à $p + q - 1$ (degré maximal de $A.P + B.Q$).

Formellement mais sans détailler les variables : $A.P + B.Q = \sum a_k.\lambda_i.X^{k+i} + \sum b_m.\mu_j.X^{m+j}$.
Chaque X^nsera présent avec coefficient $\sum_{k+i=n} a_k.\lambda_i + \sum_{m+j=n} b_m.\mu_j$.
Et c'est ce qu'on croise quand on effectue le produit

et qu'on cherche le coefficient de ligne i.

$$\begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & \ddots & & b_1 & \ddots & \\ \vdots & & a_0 & \vdots & & b_0 \\ a_q & & a_1 & a_0 \; \vdots & & b_1 \\ & \ddots & \vdots & a_1 \; b_p & & \vdots \\ & & a_q & & \ddots & \vdots \\ & & & a_q & & b_q \end{pmatrix} \cdot \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_{p-1} \\ \mu_0 \\ \mu_1 \\ \vdots \\ \mu_{q-1} \end{pmatrix}$$

Allez, prenons p et q pas trop grands pour saisir :
$A = a_0 + a_1.X + a_2.X^2$ et $B = b_0 + b_1.X + b_2.X^2 + b_3.X^3$.

On se donne un couple $(\lambda_0 + \lambda_1.X + \lambda_2.X^2,\ \mu_0 + \mu_1.X)$ de composantes $\begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \lambda_2 \\ \mu_0 \\ \mu_1 \end{pmatrix}$.

Le produit matriciel est alors

$$\begin{pmatrix} a_0 & 0 & 0 & b_0 & 0 \\ a_1 & a_0 & 0 & b_1 & b_0 \\ a_2 & a_1 & a_0 & b_2 & b_1 \\ 0 & a_2 & a_1 & b_3 & b_2 \\ 0 & 0 & a_2 & 0 & b_3 \end{pmatrix} \cdot \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \lambda_2 \\ \mu_0 \\ \mu_1 \end{pmatrix} = \begin{pmatrix} a_0.\lambda_0 & & & +b_0.\mu_0 & \\ a_1.\lambda_0 & a_0 & 0 & +b_1.\mu_0 & +b_0.\mu_1 \\ a_2.\lambda_0 & a_1.\lambda_1 & +a_0.\lambda_2 & b_2.\mu_0 & +b_1.\mu_1 \\ & a_2.\lambda_1 & +a_1.\lambda_2 & b_3.\mu_0 & +b_2.\mu_1 \\ & & a_2.\lambda_2 & & +b_3.\mu_1 \end{pmatrix}$$

Et ceci représente le polynôme
$$\begin{array}{c} (a_0.\lambda_0 + b_0.\mu_0).1 \\ +(a_1.\lambda_0 + a_0.\lambda_1 + b_1.\mu_0 + b_0.\mu_1).X \\ +(a_2.\lambda_0 + a_1.\lambda_1 + a_0.\lambda_2 + b_2.\mu_0 + b_1.\mu_1).X^2 \\ +(a_2.\lambda_1 + a_1.\lambda_2 + b_3.\mu_0 + b_1.\mu_2).X^3 \\ +(a_2.\lambda_2 + b_3.\mu_1).X^5 \end{array}$$

Et c'est bien le résultat réordonné du produit
$(a_0 + a_1.X + a_2.X^2).(\lambda_0 + \lambda_1.X + \lambda_2.X^2) + (b_0 + b_1.X + b_2.X^2 + b_3.X^3).(\mu_0 + \mu_1.X)$
que je vous recommande de développer par un tableau :

	a_0	$+a_1.X$	$+a_2.X^2$
λ_0			
$+\lambda_1.X$			
$+\lambda_2.X^2$			

et

	b_0	$+b_1.X$	$+b_2.X^2$	$+b_3.X^3$
μ_0				
$+\mu_1.X$				

Pouvait on mener une narration sans trop de points de suspension ?
La solution pour ne pas trainer des sommes partout consistait à ne pas montrer la propriété

« l'image du tout vecteur de composantes $\begin{pmatrix} \lambda_0 \\ \vdots \\ \mu_{q-1} \end{pmatrix}$ sur la base C est le vecteur $M_{A,B}.U$ sur la base canonique »

mais à montrer

« l'image du tout vecteur de la base C (composantes $U = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$) est le vecteur $M_{A,B}.U$ sur la base canonique ».

Si la propriété est prouvée pour chaque vecteur de la base C, par linéarité, il s'étend à tout vecteur de E.
On a donc juste à regarder l'image de chaque couple $(X^i,\ 0)$ et de chaque couple $(0,\ X^j)$.
Chacune de ces images devra coïncider avec une colonne de la matrice $M_{A,B}$.
Et c'est le cas. $(X^i,\ 0)$ a pour image $X^i.A + 0.B$.
Et c'est donc le vecteur $\sum_{k=0}^{q-1} a_k.X^{i+k}$.

Maintenant que f est bien associée à la matrice $M_{A,B}$, la suite d'équivalences s'agrandit :

	A et B n'ont pas de racine commune
$\Leftrightarrow$	$Ker(f) = 0$
$\Leftrightarrow$	f est injective
$\Leftrightarrow$	$(f(\overrightarrow{e_1}), \dots f(\overrightarrow{e_{p+q}}))$ est libre
$\Leftrightarrow$	$(f(\overrightarrow{e_1}), \dots f(\overrightarrow{e_{p+q}}))$ est une base de $Im(f)$
$\Leftrightarrow$	$Im(f) = \mathbb{C}_{p+q-1}[X]$
$\Leftrightarrow$	f est bijective de E dans $\mathbb{C}_{p+q-1}[X]$
$\Leftrightarrow$	$M_{A,B}$ est inversible
$\Leftrightarrow$	$\det(M_{A,B})$ est non nul

Le calcul (automatisé) de $\det(M_{A,B})$ permet de détecter si les deux polynômes ont une racine commune. Sans même calculer les racines, sans dire laquelle est la racine commune quand le déterminant est nul.

Un programme sur ordinateur permet de trouver tout de suite si deux polynômes ont une racine commune. Sans aucun calcul approché.

IV∼0) Montrez que $X^2 - s.X + p$ et $X^2 - s'.X + p'$ ont une racine commune au moins si et seulement si $p^2 + p.s'^2 + p'.s^2 + p'^2$ est égal à $2.p.p' + (p + p').s.s'$.

Profitions de ce qu'on a montré pour dire que $X^2 - s.X + p$ et $X^2 - s'.X + p'$ ont une racine commune si et seulement si l'application appelée f n'est pas injective.
On annule le déterminant de la matrice associée, de taille 4 sur 4 :

$$\begin{vmatrix} p & 0 & p' & 0 \\ -s & p & -s' & p' \\ 1 & -s & 1 & -s' \\ 0 & 1 & 0 & 1 \end{vmatrix} = \begin{vmatrix} p & 0 & p' & 0 \\ -s & p-p' & -s' & p' \\ 1 & -s+s' & 1 & -s' \\ 0 & 0 & 0 & 1 \end{vmatrix} = \begin{vmatrix} p & 0 & p' \\ -s & p-p' & -s' \\ 1 & -s+s' & 1 \end{vmatrix}$$

On développe par rapport à la première ligne $p.\begin{vmatrix} p-p' & -s' \\ -s+s' & 1 \end{vmatrix} + p'.\begin{vmatrix} -s & p-p' \\ 1 & -s+s' \end{vmatrix}$.
Après simplifications, on trouve exactement $p^2 + p.s'^2 + p'.s^2 + p'^2 - 2.p.p' - (p + p').s.s'$.

Pouvait on trouver ce résultat autrement ?
Oui, on pouvait calculer les deux racines du premier polynôme : α_1 et α_2, calculer les racines du second : β_1 et β_2, puis calculer un produit de différences astucieuses :

$(\alpha_1 - \beta_1)$	$\times(\alpha_2 - \beta_1)$
$\times(\alpha_1 - \beta_2)$	$\times(\alpha_2 - \beta_2)$

Ce produit est nul si et seulement si un des α_i est égal à un des β_j.
On développe des formules en $\frac{s \pm \sqrt{s^2 - 4.p}}{2} - \frac{s' \pm \sqrt{s'^2 - 4.p'}}{2}$
et on espère tomber sur le terme $p^2 + p.s'^2 + p'.s^2 + p'^2 - 2.p.p' - (p + p').s.s'$.

Plus astucieux : on note α_1 et α_2 les deux racines du premier polynôme. On sait $\alpha_1 + \alpha_2 = s$ et $\alpha_1.\alpha_2$.
On dit que α_1 est une racine du second polynôme si et seulement si $P_2(\alpha_1)$ est nul.
α_2 est une racine du second polynôme si et seulement si $P_2(\alpha_2)$ est nul
α_1 ou α_2 est une racine du second polynôme si et seulement si $P_2(\alpha_1).P_2(\alpha_1)$ est nul.
On va donc calculer $((\alpha_1)^2 - s'.\alpha_1 + p').((\alpha_2)^2 - s'.\alpha_2 + p')$.

On développe : $(\alpha_1.\alpha_2)^2 - s'.\alpha_1.\alpha_2.(\alpha_1+\alpha_2) - s'.p'.(\alpha_1+\alpha_2) + (s')^2.(\alpha_1+\alpha_2) + +p'.((\alpha_1)^2+(\alpha_2)^2) + (p')^2$.
On remplace $\alpha_1+\alpha_2$ par s, $\alpha_1.\alpha_2$ par p et $(\alpha_1)^2+(\alpha_2)^2$ par $s^2-2.p$.
On retrouve le critère indiqué.

V∼0) Dans cette partie : $A = X^4+X^3+1$ et $B = X^3-X+1$. Écrivez la matrice $M_{A,B}$ (format ?), calculez son déterminant. Montrez que A et B n'ont pas de racine commune.

Pour $A = X^4+X^3+1$ et $B = X^3-X+1$, on trouve une matrice de taille 7 !

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

C'est du calcul par combinaisons *(sauf si vous aimez la règle de Sarrus avec 7! termes)*, le déterminant vaut 1.

Concours : *Notice du concours CCINP :*
Les calculatrices sont autorisées.
Il n'est pas demandé le détail des calculs sur la copie lorsque le candidat aura besoin de calculer un déterminant, un produit de matrices, l'inverse d'une matrice ou tout autre calcul.
Par exemple, pour un déterminant, il pourra se contenter d'écrire le déterminant à calculer et de donner sa réponse.
Trop de chance ! Mais pas pour vous...

Pour $A = X^4+X^3+1$ et $B = X^3-X+1$, on trouve une matrice de taille 7 !

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & -1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

C'est du calcul par combinaisons *(sauf si vous aimez la règle de Sarrus avec 7! termes)*, le déterminant vaut 1.

Concours : *Notice du concours CCINP :*
Les calculatrices sont autorisées.
Il n'est pas demandé le détail des calculs sur la copie lorsque le candidat aura besoin de calculer un déterminant, un produit de matrices, l'inverse d'une matrice ou tout autre calcul.
Par exemple, pour un déterminant, il pourra se contenter d'écrire le déterminant à calculer et de donner sa réponse.
Trop de chance ! Mais pas pour vous...

Le déterminant est non nul, la matrice est inversible.
C'est donc que A et B n'ont pas de racine commune.
Le tout sans même connaître les six racines.

Raccourci : *Mais il y a plus court : $A(X) = (X+1).B(X) + X^2$ (vérifier : $(X+1).(X^3-X+1)+X^2$).*
On passe à une éventuelle racine commune a : $A(a) = (X+1).B(a) + a^2$, il reste $0 = 0 + a^2$.
La seule racine commune serait 0, et 0 n'est pas racine.

V∼1) Montrez qu'en utilisant la matrice $M_{A,B,}$ on peut trouver un couple de polynômes $(P_0,\ Q_0)$ vérifiant $A.P_0 + B.Q_0 = 1$. D'ailleurs, trouvez en un, par la méthode que vous voulez.

L'application $f = (P,\ Q) \longmapsto P.A + Q.B$ est donc bijective de $\mathbb{C}_2[X] \times \mathbb{C}_3[X]$ dans $\mathbb{C}_6[X]$ *(dimension 7 de part et d'autre)*.
Le polynôme 1 a donc un unique antécédent $(P_0,\ Q_0)$.
L'équation de Bézout $A.P + B.Q = 1$ a une solution *(et une seule)* dans $\mathbb{C}_2[X] \times \mathbb{C}_3[X]$.

Histoire : *Si Étienne Bézout a laissé son nom à une identité, ce n'est pas à celle en $a.p + b.q = 1$ pour a et b entiers premiers entre eux.*
rappelons qu'elle porte le nom de Bachet de Méziriac.
Bézout a donné son nom à cette identité sur les polynômes.

Pour trouver cette solution, on doit trouver l'antécédent de 1 par f.

Ceci revient à résoudre $M.U = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. On trouve $U = M^{-1}.\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$.

A-t-on vraiment besoin de calculer $M^{-1} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 1 & 0 & 1 & -1 \\ -1 & -1 & 0 & 0 & 1 & 0 & 1 \\ 0 & -1 & -1 & 0 & 0 & 1 & 0 \\ 1 & 0 & -1 & -1 & 0 & 0 & 1 \\ 2 & 1 & 0 & 0 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 & -1 & 0 & 0 \end{pmatrix}$
(oui, j'ai un ordinateur quand je tape le corrigé).
On a juste besoin de la première colonne puisqu'on multiplie par le vecteur fait d'un 1 et plein de 0.
D'ailleurs on pouvait aussi trouver la solution par les formules de Cramer.

Bref, on trouve $\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 1 & 0 & 1 & -1 \\ -1 & -1 & 0 & 0 & 1 & 0 & 1 \\ 0 & -1 & -1 & 0 & 0 & 1 & 0 \\ 1 & 0 & -1 & -1 & 0 & 0 & 1 \\ 2 & 1 & 0 & 0 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 & -1 & 0 & 0 \end{pmatrix} . \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 0 \\ 1 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 2 \\ 1 \end{pmatrix}$
Il s'agit des composantes sur la base canonique de notre solution
(et la base canonique, c'est $((1,0),\ (X,0),\ (X^2,0),\ (0,1),\ (0,X),\ (0,X^2),\ (0,X^3)$
On a donc $P = 1 - X - X^2$ et $Q = X + 2.X^2 + X^3$.

On vérifie : $\boxed{(X^4+X^3+1).(-X^2-X+1)+(X^3-X+1).(X^3+2.X^2+X)=1}$

Mais c'est peut être un peu lourd.
Après tout, on pouvait poser neuf inconnues et résoudre un système après avoir développé et identifié.
$(1+X^3+X^4).(a+b.X+c.X^2)+(1-X+X^3).(\alpha+\beta.X+\gamma.X^2+\delta.X^3)=1$

En soi, ce n'est pas très différent de l'inversion de la matrice, car en développant et identifiant, on a le système

$$\begin{array}{rrrrrrrl} a & & & +\alpha & & & = & 1 \\ & b & & -\alpha & +\beta & & = & 0 \\ & & c & & -\beta & +\gamma & = & 0 \\ a & & & +\alpha & & -\gamma & +\delta & = & 0 \\ a & +b & & & +\beta & & & = & 0 \\ & b & +c & & & +\gamma & & = & 0 \\ & & c & & & & +\delta & = & 0 \end{array}$$

En fait, c'est exactement la même chose !

Sinon, on peut aussi appliquer l'algorithme d'Euclide et remonter.
Non pas avec des divisions euclidiennes entre entiers. Mais avec des divisions euclidiennes entre polynômes.

Exemple avec des entiers 2022 et 143 :

a	$=$	q	$\times b$	$+r$
2022	$=$	$14\times$	143	$+20$
143	$=$	$7\times$	20	$+3$
20	$=$	$6\times$	3	$+2$
3	$=$	$1\times$	2	$+1$
2	$=$	$2\times$	1	

et

2	0	2	2	1	4	3
(1	4	3)		$-$	$-$	$-$
$-$	$-$	$-$		1	4	
	5	9	2			
	(5	7	2)			
	$-$	$-$	$-$			
		2	0			

Avec des polynômes :

A	$=$	q	$\times B$	$+R$
X^4+X^3+1	$=$	$(X+1)\times$	(X^3-X+1)	$+(X^2)$
X^3-X+1	$=$	$X\times$	X^2	$+(-X+1)$
X^2	$=$	$(-X-1)\times$	$(-X+1)$	$+1$
$(-X+1)$	$=$	$(-X+1)\times$	1	

On s'arrête au dernier reste non nul.
Les deux polynômes sont bien premiers entre eux.

Il n reste qu'à remonter :

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

Et la dernière ligne est bien celle obtenue plus haut.

V∼2) Déterminez tous les couples solutions dans $(\mathbb{C}[X])^2$ de $A.P+B.Q=1$ *(pensez que vous avez une solution particulière, et écrive* $(P-P_0).A=(Q_0-Q).B$*).*

Même sans avoir trouvé la solution $(P_0,\ Q_0)$, on peut se contenter de la nommer.
On cherche alors les autres solutions en résolvant $A.P+B.Q=1$.
Comme on a une solution particulière, l'équation devient $A.P+B.Q=1=A.P_0+B.Q_0$.
On réunit d'un côté et de l'autre : $A.(P_0-P)=B.(Q-Q_0)$.
Comme A divise le premier membre, il divise aussi le second.
Mais comme il est premier avec B, il divise $Q-Q_0$ (c'est Gauss !).
On écrit alors $Q-Q_0=A.K$ avec K polynôme quelconque.
On reporte et simplifie : $P-P_0=-B.K$.

On a nos solutions : $\boxed{A.(P_0-B.K)+B.(Q_0+A.K)=1 \text{ avec } K \text{ décrivant } (\mathbb{C}[X],+,.)}$ comme pour l'équation de Bézout dans $\mathbb{Z}$.

VI∼0) En utilisant les polynômes $A=X^2-3$ et $B=(y-X)^2-7$, trouvez un polynôme de degré 4 à coefficients entiers admettant pour racine $\sqrt{3}+\sqrt{7}$.

Une approche possible ? On se dit que si on a une racine, on doit avoir ses conjugués sur $\mathbb{Z}$, comme $x-i.y$ est le conjugué de $x+i.y$ sur $\mathbb{R}$.
On pense donc au polynôme dont les quatre racines sont $\sqrt{3}+\sqrt{7}$ mais aussi $\sqrt{3}+\sqrt{7}$, $\sqrt{3}+\sqrt{7}$ et $\sqrt{3}+\sqrt{7}$ car on se dit qu'il y a plusieurs formes de conjugaison.

On va développer étape par étape

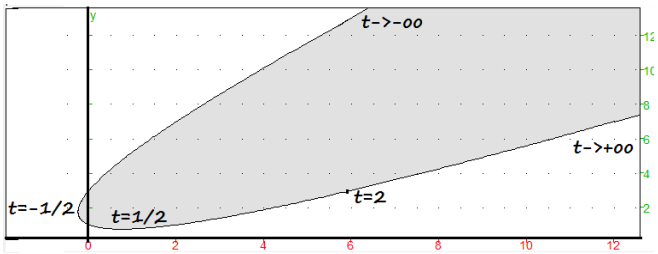
$(X-\sqrt{3}-\sqrt{7}).$ $(X-\sqrt{3}-\sqrt{7}).$	$(X-\sqrt{3}-\sqrt{7}).$ $(X-\sqrt{3}-\sqrt{7})$
$((X-\sqrt{3})^2-7).$	$((X+\sqrt{3})^2-7)$
$(X^2-4-2.\sqrt{3}.X).$	$(X^2-4+2.\sqrt{3}.X).$
$(X^2-4)^2-(2.\sqrt{3}.X)^2$	

Le polynôme $(X^2-4)^2-12.X^2$ convient. C'est $\boxed{X^4-20.X^2+16}$

On peut aussi poser $a=\sqrt{3}+\sqrt{7}$, élever au carré : $a^2=10+2.\sqrt{21}$, isoler$(a^2-10)=2.\sqrt{21}$ et élever à nouveau au carré : $(a^2-10)^2=21^2$.

Et dans l'esprit du sujet ?
On note $a=\sqrt{3}$. a est racine commune des deux polynômes X^2-3 et $(X-\sqrt{3}+\sqrt{7})^2-7$.
On note $b=\sqrt{3}+\sqrt{7}$. Les deux polynômes X^2-3 et $(X-y)^2-7$ ont une racine commune.
Leur résultant est nul.
On écrit la matrice pour $-3+X^2$ et $y^2-7-2.y.X+X^2$: $\begin{pmatrix} -3 & 0 & y^2-7 & 0 \\ 0 & -3 & -2.y & y^2-7 \\ 1 & 0 & 1 & -2.y \\ 0 & 1 & 0 & 1 \end{pmatrix}$.
Le déterminant de cette matrice vaut $\begin{vmatrix} -3 & 0 & y^2-7 & 0 \\ 0 & 4-y^2 & -2.y & y^2-7 \\ 1 & 2.y & 1 & -2.y \\ 0 & 0 & 0 & 1 \end{vmatrix}$ et on aboutit à $y^4-20.y^2+16$.

VII∼0) On a représenté graphiquement pour vous ci contre l'arc paramétré Γ « mouvement d'une particule en fonction du temps » : $\left\{\begin{array}{rcrcr} x(t) & = & t^2 & +t & \\ y(t) & = & t^2 & -t & +1 \end{array}\right.$ *(la construction d'arcs paramétrés était encore au programme en 2009)*. On se donne deux polynômes P et Q à coefficients réels et l'on pose pour tout triplet $(x,\ y,\ t)$ de $\mathbb{R}^3$: $A(t) = P(t) - x$ et $B(t) = Q(t) - y$. Établissez que si un point M de coordonnées $(x,\ y)$ appartient à la courbe de représentation paramétrique $\left\{\begin{array}{rcl} x(t) & = & P(t) \\ y(t) & = & Q(t) \end{array}\right.$ alors les fonctions polynômes ont une racine commune.



Un point $(x,\ y)$ est sur la courbe $x(t) = P(t)$, $y(t) = Q(t)$ si et seulement si il existe t_0 vérifiant $P(t_0) = x$ et $Q(t_0 = y$.
On remplace : $A(t_0) + x = x$ et $B(t_0) + y = y$.
Ceci revient à dire que A et B ont une racine commune.
On demande donc que $-x + t + t^2$ et $-y + 1 - t + t^2$ aient une racine commune.
On construit a matrice $\begin{pmatrix} -x & 0 & -y+1 & 0 \\ 1 & -x & -1 & -y+1 \\ 1 & 1 & 1 & -1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$.
On calcule son déterminant : $x^2 + y^2 - 2.x.y - 4.y + 3$.
La critère est donc là.

Ouf, j'ai compris le rapport avec nos résultants ! Et vous ?

VII∼1) Déduisez qu'un point M de coordonnées $(x,\ y)$ appartenant à la courbe Γ vérifie $x^2 + y^2 - 2.x.y - 4.y + 3 = 0$. Mettez l'équation $x^2 + y^2 - 2.x.y - 4.y + 3 = 0$ sous la forme $\begin{pmatrix} x & y & 1 \end{pmatrix}.S.\begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = 0$ où S est une matrice symétrique. Donnez le polynôme caractéristique de S et son nombre de valeurs propres réelles..

Sinon, pourquoi ne pas se contenter de reporter :
$x^2 + y^2 - 2.x.y - 4.y + 3 = (t^2 + t)^2 + (t^2 - t + 1) - 2.(t^2 + t).(t^2 - t + 1) - 4.(t^2 - t + 1) + 3$.
Vous savez quoi, on trouve 0.
Et on a gagné un point en allant lire la fin de l'énoncé, sans même avoir cherché à comprendre un truc avec des variables partout...

Gagnons des points même sans avoir fait ce qui précède.

Peut on mettre $x^2 + y^2 - 2.x.y - 4.y + 3$ sous la forme $\begin{pmatrix} x & y & 1 \end{pmatrix}.\begin{pmatrix} a & b & c \\ d & e & f \\ c & f & g \end{pmatrix}.\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$?

Oui : $\begin{pmatrix} x & y & 1 \end{pmatrix}.\begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & -2 \\ 0 & -2 & 3 \end{pmatrix}.\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$ et on peut interpréter les coefficients :

$\begin{pmatrix} 1 & o & o \\ o & o & o \\ o & o & o \end{pmatrix}$ pour x^2	$\begin{pmatrix} o & o & o \\ o & 1 & o \\ o & o & o \end{pmatrix}$ pour y^2	$\begin{pmatrix} o & o & o \\ o & o & o \\ o & o & 3 \end{pmatrix}$ pour 3
$\begin{pmatrix} o & -1 & o \\ -1 & o & o \\ o & o & o \end{pmatrix}$ pour $-2.x.y$	$\begin{pmatrix} o & o & 0 \\ o & o & o \\ 0 & o & o \end{pmatrix}$ pour $0.x$	$\begin{pmatrix} o & o & o \\ o & o & -2 \\ o & -2 & o \end{pmatrix}$ pour $-4.y$

Son polynôme caractéristique est $\boxed{X^3 - 5.X^2 + 2.X + 4}$

Il a trois racines réelles. On le sait en traçant un tableau de variations. Extrema en $\frac{5-\sqrt{19}}{2}$ et $\frac{5+\sqrt{19}}{2}$ avec des changements de signes.
En revanche, il n'y a pas de racine évidente...

∘48∘

Sujet du vingtième siècle. Première partie (sur quatre) d'un sujet (E.N.S. filière PC) consistant, destiné à démontrer un théorème établi par Roger Apery[a] *en 1978 :* $\sum_{k=1}^{+\infty} \frac{1}{k^3}$ *est irrationnel.*

a. *mathématicien français, fils d'immigré grec, 1916-1994, lycée Faidherbe à Lille, lycée Louis le Grand (il habitait alors à Paris le quartier de la Goutte d'Or), E.N.S., premier à l'agrégation de maths, un des membres fondateurs en 1941 du Front National (non, celui de 1941, dans le cours d'histoire : on vous en a parlé « Front National (de la Résistance) », confondez pas !), sur sa pierre tombale au colombarium du Père Lachaise, il est gravé* $1+\frac{1}{8}+\frac{1}{27}+\ldots \neq \frac{p}{q}$,

I∼0) La suite (a_n) est définie par $a_1 = 2$ et pour tout n : $\boxed{a_{n+1} = (a_n)^2 - a_n + 1}$ Calculez a_n pour n de 1 à 5. Montrez que c'est une suite d'entiers naturels strictement croissante, divergente.

On calcule les premiers termes :

$a_1 = 2$	$a_2 = 2^2 - 2 + 1$	$a_3 = 3^2 - 3 + 1$	$a_4 = 7^2 - 7 + 1$	$a_5 = 43.42 + 1$	
	$a_2 = 3$	$a_3 = 7$	$a_4 = 43$	$a_5 = 1807$	$a_6 = 3263443$

Non, a_6 n'était pas demandé.

Par récurrence immédiate, chaque terme est un entier.
Et même un entier naturel ? On montre que a est croissante : $a_{n+1} - a_n = (a_n - 1)^2 \geqslant 0$ pour tout n.
Comme elle croît et que son premier terme vaut 2, ils sont tous plus grands que 2 donc naturels.

Mais comme ils sont plus grands que 2 : $a_{n+1} - a_n = (2-1)^2 \geqslant 1$ pour tout n.
La suite est strictement croissante.

Mais alors : $a_n \geqslant n + 1$ puisque à chaque étape, $a_n$augmente au moins de 1.

Par minoration, a_n tend vers $+\infty$ avec n.

I∼1) Écrivez un script Python qui prend en entrée n et retourne a_n.

```
def a(n) :
....x = 2
....for k in range(n-1) :
........x = x*(x-1)+1
....return x
```

La seule difficulté : combien de boucles : `range(n-1)`, `range(n)` ou `range(n-2)` ?
Testez sur un exemple.

Et si vous tapez `x = x**2-x+1`, vous êtes bon en I.P.T., mais vous n'êtes pas un vrai informaticien. Vous n'avez aucune pitié pour la machine, et vous demandez à l'ordinateur de calculer des choses idiotes.

```
def A(n) :
....L=[2]
....for k in range(n-1) :
........last = L[-1]
........L.append(last*(last-1)+1)
....return L
```

Ça c'est si vous voulez tous les termes de la suite.

I∼2) Montrez pour n supérieur ou égal à 2 : $2^{2^{n-2}} + 1 \leqslant a_n \leqslant 2^{2^{n-1}}$.

La relation $2^{2^{n-2}} + 1 \leqslant a_n \leqslant 2^{2^{n-1}}$ va faire l'objet d'une récurrence, n'en déplaise à maître chocos pourfendeur des inductions.
Elle est vraie au rang 2 : $2^1 + 1 = a_2 \leqslant 2^2$.
Prenons un rang n quelconque, et supposons $2^{2^{n-2}} + 1 \leqslant a_n \leqslant 2^{2^{n-1}}$.
On applique $x \longmapsto x.(x-1)+1$, croissante sur $[1, +\infty[$ (et on y est justement).

$$(2^{2^{n-2}} + 1).2^{2^{n-2}} + 1 \leqslant a_n.(a_n - 1) + 1 \leqslant 2^{2^{n-1}}.(2^{2^{n-1}} - 1) + 1$$

On développe $2^{2.2^{n-2}} + 2^{2^{n-2}} + 1 \leqslant a_{n+1} \leqslant 2^{2.2^{n-1}} - 2^{2^{n-1}} + 1$ (car $(2^a)^2 = 2^{2.a}$).

On remplace : $2^{2^{n-1}}+1+2^{2^{n-2}} \leqslant a_{n+1} \leqslant 2^{2^n}-2^{2^{n-1}}+1$
On majore et minore encore : $2^{2^{n-1}}+1 \leqslant 2^{2^{n-1}}+1+2^{2^{n-2}} \leqslant a_{n+1} \leqslant 2^{2^n}-2^{2^{n-1}}+1 \leqslant 2^{2^n}$ car $2^{2^{n-1}}$ vaut au moins 2^0 c'est à dire 1.
L'hérédité est établie.

II∼0) Déduisez pour n plus grand que 7 : $\dfrac{\ln(a_n)}{a_n} \leqslant \dfrac{1}{2^{19+n}}$.

L'inégalité précédente passe au logarithme (application croissante) : $\ln(a_n) \leqslant \ln(2^{2^{k-1}}) = 2^{k-1}.\ln(2)$.

On divise par un réel positif : $\dfrac{\ln(a_n)}{a_n} \leqslant \dfrac{2^{k-1}.\ln(2)}{a_n}$.

On exploite la minoration (pour majorer, on minore le dénominateur) : $\dfrac{\ln(a_n)}{a_n} \leqslant \dfrac{2^{n-1}.\ln(2)}{2^{2^{n-2}}+1}$.

Ça ne ressemble pas trop à $\dfrac{\ln(a_n)}{a_n} \leqslant \dfrac{1}{2^{19+n}}$. A moins d'avoir $\dfrac{2^{n-1}.\ln(2)}{2^{2^{n-2}}+1} \leqslant \dfrac{1}{2^{19+n}}$.
Ceci revient à demander $2^{18+2.n}.\ln(2) \leqslant 2^{2^{n-2}}+1$.

II∼1) Déduisez que la série de terme général $\dfrac{\ln(a_n)}{a_n}$ converge, et écrivez un script qui calcule sa somme à 10^{-5} près (on trouvera 1.08239).

Pour tout n, le terme général $\dfrac{\ln(a_n)}{a_n}$ existe et est positif.
On a une série à termes positifs, il suffit de la majorer par une série de référence.
Ici, justement : $\dfrac{\ln(a_n)}{a_n} \leqslant \dfrac{1}{2^{19}}.\dfrac{1}{2^n}$.
La série géométrique de terme général $\frac{1}{2^{19}}.\frac{1}{2^n}$ converge (et sa somme se calcule même, mais qu'importe).
Par majoration de séries à termes positifs, la série de terme général $\dfrac{\ln(a_n)}{a_n}$ pour n plus grand que 7 converge.
En ajoutant la somme finie $\displaystyle\sum_{n=1}^{6} \frac{\ln(a_n)}{a_n}$, on a l'existence de $\displaystyle\sum_{n=1}^{+\infty} \frac{\ln(a_n)}{a_n}$.
Mais pas sa valeur. Mais on va y venir.

En tant que série à termes positifs, la suite $\Big(\displaystyle\sum_{n=1}^{N} \frac{\ln(a_n)}{a_n}\Big)$ est croissante.
Elle converge en croissant vers sa limite. Et donc, pour N assez grand (plus grand que certain $N_\varepsilon$avec ici ε égal à 10^{-5}), on aura $\displaystyle\sum_{n=1}^{N} \frac{\ln(a_n)}{a_n}$ entre $\Big(\displaystyle\sum_{n=1}^{+\infty} \frac{\ln(a_n)}{a_n}\Big) - \varepsilon$ et $\Big(\displaystyle\sum_{n=1}^{N} \frac{\ln(a_n)}{a_n}\Big)$.
Ceci a lieu en fait dès que le reste $\displaystyle\sum_{n=N+1}^{+\infty} \frac{\ln(a_n)}{a_n}$ est plus petit que ε.

Et si on se laissait guider par la proposition : pourquoi ne pas prendre $N = 6$?
On a alors un reste $\displaystyle\sum_{n=7}^{+\infty} \frac{\ln(a_n)}{a_n}$ qui se majore par $\displaystyle\sum_{n=7}^{+\infty} \frac{1}{2^{19+n}}$.
Explicitement $\displaystyle\sum_{n=7}^{N} \frac{1}{2^{19+n}} = \frac{\frac{1}{2^{19+7}} - \frac{1}{2^{20+N}}}{1-\frac{1}{2}}$ et donc en passant à la limite sur N : $\displaystyle\sum_{n=7}^{N} \frac{1}{2^{19+n}} = 2.\frac{1}{2^{19+7}} = \frac{1}{2^{25}}$.
On majore avec l'héritage de l'informatique : $2^{10} \geqslant 10^3$: $S - \displaystyle\sum_{n=1}^{6} \frac{\ln(a_n)}{a_n} \leqslant \frac{1}{32.10^6}$. C'est parfait pour cinq chiffres exactes et même pis.
Pour la lisibilité, j'ai décidé de noter S la somme de la série.

Ensuite, le programme :

```
from math import *
a = 2
S = log(a)/a
for n in range(5) :
....a = a*(a-1)+1
....S += log(a)/a
```

II∼2) Déduisez que la suite $\left(\prod_{n=1}^{N} \sqrt[a_n]{a_n}\right)$ est majorée, et donnez un majorant $\boxed{w}$ le plus petit possible avec trois chiffres exacts.

Mais qui est ensuite $\left(\prod_{n=1}^{N} \sqrt[a_n]{a_n}\right)$?

C'est $\left(\exp\left(\sum_{n=1}^{N} \frac{\ln(a_n)}{a_n}\right)\right.$ puisque $\sqrt[x]{x} = x^{\frac{1}{x}} = e^{\frac{\ln(x)}{x}}$.

Par croissance de la suite et de l'exponentielle, cette suite converge en croissant vers e^S (vous l'ai-je dit ? S est la somme de la série).

Comme la suite converge en croissant, il suffit de prendre $w = e^S$ comme majorant.
Et $e^{1.08239}$ doit faire l'affaire. Et vous croyez que je vais vous calculer ça sans machine ?

III∼0) Montrez pour tout N de $\mathbb{N}^*$: $\sum_{n=1}^{N} \frac{1}{a_n} = 1 - \frac{1}{a_{N+1} - 1}$.

La formule $\sum_{n=1}^{N} \frac{1}{a_n} = 1 - \frac{1}{a_{N+1} - 1}$ va se démontrer par récurrence sur n.
On initialise.
On suppose pour un n donné : $\sum_{n=1}^{N} \frac{1}{a_n} = 1 - \frac{1}{a_{N+1} - 1}$.

$$\sum_{n=1}^{N+1} \frac{1}{a_n} = \sum_{n=1}^{N} \frac{1}{a_n} + \frac{1}{a_{N+1}} \text{ en ajoutant un terme}$$
$$\sum_{n=1}^{N+1} \frac{1}{a_n} = 1 - \frac{1}{a_{N+1} - 1} + \frac{1}{a_{N+1}} \text{ en remplaçant}$$
$$\sum_{n=1}^{N+1} \frac{1}{a_n} = 1 - \frac{1}{(a_{N+1} - 1).(a_{N+1})} \text{ en réduisant}$$
$$\sum_{n=1}^{N+1} \frac{1}{a_n} = 1 - \frac{1}{(a_{N+1} - 1).(a_{N+1})} \text{ en remplaçant.}$$

Ou alors on cherche la somme télescopique. Trop classe !
On pose $\alpha_n = \frac{1}{a_n - 1}$ (dont l'existence est assurée).
On calcule comme par hasard

$$\alpha_{n+1} - \alpha_n = \frac{1}{a_{n+1} - 1} - \frac{1}{a_n - 1} = \frac{1}{a_n.(a_n - 1)} - \frac{1}{a_n - 1} = \frac{1 - a_n}{a_n.(a_n - 1)} = -\frac{1}{a_n}$$

3

La somme $\sum_{n=1}^{N} \frac{1}{a_n}$ est la somme télescopique $\sum_{n=1}^{N} (\alpha_n - \alpha_{n+1})$. Elle donne bien $1 - \frac{1}{a_{N+1} - 1}$.

3. plus j'avance et plus je me dis que vraiment, écrire $(a_n)^2 - a_n + 1$ n'était pas la bonne idée, tandis que $a_n.(a_n - 1) + 1$ était la bonne idée ; on dit merci les réflexes d'informaticien

III∼1) Pour tout n on pose $\boxed{C(n)=\dfrac{n!}{\prod_{i=1}^{k}\left(\left[\frac{n}{a_i}\right]!\right)}}$ où k est l'unique entier vérifiant $a_k \leqslant n < a_{k+1}$.

Calculez $C(10)$. La formule $C(n)=n!.\prod_{i=1}^{+\infty}\left(\left[\frac{n}{a_i}\right]!\right)^{-1}$ serait elle cohérente ?

On a posé $C(10)=\dfrac{10!}{\prod_{i=1}^{k}\left(\left[\frac{10}{a_i}\right]!\right)}$. Mais qui est k ? L'entier vérifiant $a_k \leqslant 10 < a_{k+1}$. Sachant $a=[2,\ 3,\ 7,\ 43,\ 1807,\ 3263443...]$,
on a $a_3 \leqslant 10 < a_4$.

On donc $\boxed{C(10)=\dfrac{10!}{\left(\left[\frac{10}{2}\right]!\right).\left(\left[\frac{10}{3}\right]!\right).\left(\left[\frac{10}{7}\right]!\right)}=\dfrac{10!}{5!.3!.1!}=\dfrac{10.9.8.7.6.5.4.3.2.1}{(1.2.3.4.5).(1.2.3)}=5040}$

Peut on remplacer $\dfrac{n!}{\prod_{i=1}^{k}\left(\left[\frac{n}{a_i}\right]!\right)}$ par $\dfrac{n!}{\prod_{i=1}^{+\infty}\left(\left[\frac{n}{a_i}\right]!\right)}$?

De l'une à l'autre, il manque $\prod_{i=k+1}^{+\infty}\left(\left[\frac{n}{a_i}\right]!\right)$ (si déjà ce produit infini a un sens).

Mais comme a_{k+1} est plus grand que n, ainsi que les suivants chaque quotient $\dfrac{n}{a_i}$ est entre 0 et 1.

Chaque $\left[\dfrac{n}{a_i}\right]$ vaut 0.

Chaque $\left[\dfrac{n}{a_i}\right]!$ vaut 1.

Le produit (d'une infinité de termes) vaut 1.

On a bien $\boxed{\dfrac{n!}{\prod_{i=1}^{k}\left(\left[\frac{n}{a_i}\right]!\right)}=\dfrac{n!}{\prod_{i=1}^{+\infty}\left(\left[\frac{n}{a_i}\right]!\right)}}$ Et pour gagner de la place, mon énoncé l'a écrit avec des exposants « -1 ».

III∼2) Écrivez un script `Python` qui pour n donné calcule $C(n)$.

Pour créer C, on va multiplier et diviser des factorielles. tant pis si ce qui suit n'est pas ce qu'il se fait de mieux.

```
def Facto(N) :
....P = 1
....for k in range(N) :
.........P *= k+1
....return P
```

Ensuite, il faut créer le numérateur et le dénominateur.
Mais pour le dénominateur, il faut combien de factorielles ? C'est une boucle conditionnelle : tant que a_i est plus petit que n.

```
def C(n) :
....Numer = Facto(n)
....Denom = 1
....a = 2
....while a*(a-1)+1 < n :
........Quo = n//a
........Denom *= Facto(Quo)
........a = a*(a-1)+1
....return Numer//Denom
```

III∼3) Montrez, en pensant aux coefficients du multinôme que chaque $C(n)$ est entier.

Les coefficients multinomiaux sont des choses comme $\dfrac{10!}{5!.3!.2!}$ ou $\dfrac{17!}{8!.6!.2!.1!}$.

Ils sont de la forme $\dfrac{N!}{(a_1)!.(a_2)!\ldots(a_p)!}$ avec $a_1+a_2+\ldots+a_p=m$.

Ils sont entiers, car en fait par exemple $\dfrac{10!}{5!.3!.2!}=\dfrac{10!}{5!.5!}.\dfrac{5!}{3!.2!}$

$$\frac{17!}{8!.6!.2!.1!} = \frac{17!}{8!.9!}.\frac{9!}{6!.3!};\frac{3!}{2!.1!}$$

$$\frac{N!}{(a_1)!.(a_2)!\ldots(a_p)!} = \frac{N!}{(a_1)!.(N-a_1)!}.\frac{(N-a_1)!}{(a_2)!.(N-a_1-a_2)!}.\frac{(N-a_1-a_2)!}{(a_3)!.(N-a_1-a_2-a_3)!}\cdots\frac{(N-a_1-a_2-\ldots-a_{p-2})!}{(a_{p-1})!(a_p)!}$$

Et tous les termes sont des binomiaux. Leur produit est donc un entier.

$C(n)$ est le quotient $\dfrac{n!}{\prod_{i=1}^{k}\left(\left[\frac{n}{a_i}\right]!\right)}$. Serait il un multinomial ?

Ce serait le cas si on avait $\sum_{i=1}^{k}\left[\frac{n}{a_i}\right] = n$.

Mais en fait, on a $\sum_{i=1}^{k}\frac{n}{a_i} = n.\sum_{i=1}^{k}\frac{1}{a_i} = n - \frac{n}{a_{k+1}-1}$ avec $n < a_{k+1}$
d'où $a_{k1+} - 1 \geqslant n$
et $\dfrac{n}{a_{k+1}-1} \leqslant 1$

La somme est entre n et $n-1$.

Quand chaque terme est transformé en un entier, il diminue : $\sum_{i=1}^{k}\left[\frac{n}{a_i}\right] \leqslant n$

Un exemple : $n = 20$ donne $\frac{20}{2}+\frac{20}{3}+\frac{20}{7} = 20 - \frac{20}{42}$ et donc $\left[\frac{20}{2}\right]+\left[\frac{20}{3}\right]+\left[\frac{20}{7}\right] = 10+6+2 = 18 < 20$

$n = 21$ donne $\frac{21}{2}+\frac{21}{3}+\frac{21}{7} = 21 - \frac{21}{42}$ et donc $\left[\frac{21}{2}\right]+\left[\frac{21}{3}\right]+\left[\frac{21}{7}\right] = 10+7+3 = 20 < 21$

$n = 22$ donne $\frac{22}{2}+\frac{22}{3}+\frac{22}{7} = 22 - \frac{20}{42}$ et donc $\left[\frac{22}{2}\right]+\left[\frac{22}{3}\right]+\left[\frac{22}{7}\right] = 11+7+3 = 21 < 22$

Et donc par rapport à un multinomial, il manque des termes. Au dénominateur.
Si on les met, il faut les remettre au numérateur, et le multinomial est multiplié par u entier.

n	$(C(n))$	multinomial choisi	
20	$\frac{20!}{10!.6!.2!}$	$\frac{20!}{10!.6!.4!}$	$C(20) = \frac{20!}{10!.6!.4!}.3.4$
21	$\frac{21!}{10!.7!.2!}$	$\frac{21!}{10!.7!.4!}$	$C(21) = \frac{21!}{10!.7!.4!}.3.4$
22	$\frac{22!}{11!.7!.3!}$	$\frac{22!}{11!.7!.4!}$	$C(22) = \frac{22!}{11!.7!.4!}.4$
		ou $\frac{22!}{12!.7!.3!}$	$C(22) = \frac{22!}{12!.7!.3!}.12$

La formule propre sera $\dfrac{n!}{\prod_{i=1}^{k}\left(\left[\frac{n}{a_i}\right]!\right)} = \dfrac{n!}{(n-S)!.\prod_{i=1}^{k}\left(\left[\frac{n}{a_i}\right]!\right)}.(n-S)!$ en posant $S = \sum_{i=1}^{k}\left[\frac{n}{a_i}\right]$.

Par construction $n-S$ est un entier naturel. Le quotient $\dfrac{n!}{(n-S)!.\prod_{i=1}^{k}\left(\left[\frac{n}{a_i}\right]!\right)}$ est un coefficient multinomial puisque la somme des entiers du dénominateur vaut n.
Et le multiplicateur $(n-S)!$ est entier.
Le nombre $C(n)$ est un entier.

III∼4) Montrez : $C(n) \leqslant n^n.\prod_{i=1}^{k}\left[\frac{n}{a_i}\right]^{-[n/a_i]}$ et respirez un grand coup.

On doit prouver $C(n) \leqslant n^n.\prod_{i=1}^{k}\left[\frac{n}{a_i}\right]^{-[n/a_i]}$ c'est à dire $n!.\prod_{i=1}^{k}\left(\left[\frac{n}{a_i}\right]!\right)^{-1} \leqslant n^n.\prod_{i=1}^{k}\left[\frac{n}{a_i}\right]^{-[n/a_i]}$.

Il est tentant de faire appel à $n! \leqslant n^n$ (dans les deux produits il y a n termes, mais ceux du premier vont de 1 à n tandis que ceux du second valent tous n).
Mais ce qui serait bien pour le numérateur (majoration) ne l'est plus pour le dénominateur.

Sauf si vous passez de $n! \leqslant n^n$ *et* $\prod_{i=1}^{k}\left[\frac{n}{a_i}\right]! \leqslant \prod_{i=1}^{k}\left(\left[\frac{n}{a_i}\right]\right)^{[n/a_i]}$ *au quotient indiqué.*

On rappelle que $a \leqslant b$ *et* $c \leqslant d$ *ne donne pas du tout* $\frac{a}{c} \leqslant \frac{b}{d}$. *On a bien* $2 \leqslant 5$ *et* $4 \leqslant 5$ *mais pas* $\frac{4}{2} \leqslant \frac{5}{5}$.

Pour se simplifier la vie, on va noter $b_i = \left[\frac{n}{a_i}\right]$ pour chaque i et donc $b_1 + \ldots + b_k$ est inférieur ou égal à n.

Partons alors du premier membre : $C(n) = \dfrac{n!}{(b_1)!.(b_2)!\ldots(b_n)!}$.

On l'écrit $C(n) = \dfrac{n!}{m!}.\dfrac{m!}{(b_1)!.(b_2)!\ldots(b_n)!}$ pour avoir comme à la question précédente un coefficient multinomial.

Pour faire intervenir le membre de droite, on multiplie et divise par $(b_1)^{b_1}.(b_2)^{b_2}\ldots(b_k)^{b_k}$:

$$C(n) = \frac{n!}{m!(b_1)^{b_1}.(b_2)^{b_2}\ldots(b_k)^{b_k}}.\frac{m!}{(b_1)!.(b_2)!\ldots(b_n)!}.(b_1)^{b_1}.(b_2)^{b_2}\ldots(b_k)^{b_k}$$

Vous ne voyez rien d'intelligent à écrire ? Moi non plus...
sauf si je repense à la formule du multinôme.

L'entier $\dfrac{m!}{(b_1)!.(b_2)!\ldots(b_n)!}.(b_1)^{b_1}.(b_2)^{b_2}\ldots(b_k)^{b_k}$ est un des multiples termes du développement de $(b_1 + \ldots + b_k)^m$ (celui où chaque b_i a pour exposant b_i lui même).

> *C'est comme si on cherchait le terme en* $12^{12}.7^7.3^3$ *dans* $(12+7+3)^{22}$.
> *Il a pour coefficient* $\dfrac{22!}{12!.7!.3!}$ *et on est donc en face de* $\dfrac{22!}{12!.7!.3!}.12^{12}.7^7.3^3$.

Comme c'est l'un des termes de la somme (de termes positifs), il est plus petit que la somme :

$$\frac{m!}{(b_1)!.(b_2)!\ldots(b_n)!}.(b_1)^{b_1}.(b_2)^{b_2}\ldots(b_k)^{b_k} \leqslant m^m$$

A ce stade :

$$C(n) = \frac{n!}{m!(b_1)^{b_1}.(b_2)^{b_2}\ldots(b_k)^{b_k}}.\frac{m!}{(b_1)!.(b_2)!\ldots(b_n)!}.(b_1)^{b_1}.(b_2)^{b_2}\ldots(b_k)^{b_k} \leqslant \frac{n!}{m!(b_1)^{b_1}.(b_2)^{b_2}\ldots(b_k)^{b_k}}.m^m$$

> *On peut dire qu'on progresse, on n'est plus si loin de* n^n.
> *Enfin si, mais bon...*

On arrange : $C(n) \leqslant \dfrac{n^n}{(b_1)^{b_1}.(b_2)^{b_2}\ldots(b_k)^{b_k}}.\dfrac{n!.m^m}{n^n.m!}$. Ah, oui, ça ressemble à ce qu'on veut.

On a juste à prouver que $\dfrac{n!.m^m}{n^n.m!}$ est plus petit que 1.

> *Exemple : saurez vous prouver :* $\dfrac{23!.20^{20}}{23^{23}.20!} \leqslant 1$ *?*
> *Moi je trouve que rien que ça, c'est une question en soi.*

Je l'écris $\dfrac{\prod_{k=1}^{n} k.\prod_{i=1}^{m} m}{\prod_{i=1}^{n} n.\prod_{k=1}^{m} k}$ et même $\dfrac{\prod_{k=1}^{n} k.\prod_{i=1}^{m} m}{\prod_{k=1}^{m} k.\prod_{i=1}^{n} n}$

puis $\dfrac{\prod_{k=m+1}^{n} k.\prod_{i=1}^{m} m}{\prod_{i=1}^{n} n}$. Il y a au total n termes au numérateur $(n-m+m)$
n termes au numérateur (tous égaux à n)

Chaque terme du dénominateur est plus grand que chaque terme du numérateur.
Le quotient est plus petit que 1. C'est ce qu'on voulait !

> *Sur notre exemple :* $\dfrac{23!.20^{20}}{23^{23}.20!} = \dfrac{23!}{20!}.\dfrac{.20^{20}}{23^{23}} = \dfrac{20^{20}.21.22.23}{23^{23}} = \dfrac{20.20\ldots20.21.22.23}{23.23\ldots23.23.23.23}$.
> *Il y a* 23 *termes au numérateur et* 23 *termes au dénominateur.*
> *Ce quotient est plus petit que* 1.

III∼5) Montrez que si a et n sont des entiers vérifiant $0 < a \leqslant n$, alors on a $\dfrac{\left(\frac{n}{a}\right)^{n/a}}{\left[\frac{n}{a}\right]^{[n/a]}} \leqslant \left(\frac{e.n}{a}\right)^{(a-1)/a} a$.

a. indication : montrez déjà $\dfrac{n-a+1}{a} \leqslant \left[\frac{n}{a}\right]$

On veut montrer $\dfrac{\left(\frac{n}{a}\right)^{n/a}}{\left[\frac{n}{a}\right]^{[n/a]}} \leqslant \left(\frac{e.n}{a}\right)^{(a-1)/a}$.

Comme proposé, on montre déjà $\dfrac{n-a+1}{a} \leqslant \left[\frac{n}{a}\right]$.

On rappelle : $x - 1 < [x] \leqslant x$ (pour avoir la partie entière de x, on descend, mais on ne descend pas de plus que 1).

On a donc $\dfrac{n}{a} - 1 < \left[\frac{n}{a}\right] \leqslant \dfrac{n}{a}$

$$\frac{n-a}{a} < \left[\frac{n}{a}\right] \leqslant \frac{n}{a}$$

A poursuivre...

III∼6) Déduisez : $C(n) \leqslant n^{k+1}.e^k.w^n$ (oui, il y a des n et des k, c'est logique, et w a bien été défini plus haut).

IV∼0) p est un nombre premier inférieur ou égal à n. On pose $q = \left[\dfrac{\ln(n)}{\ln(p)}\right]$. Montrez : $p^q \leqslant n < p^{q+1}$.

IV∼1) Montrez pour tout m entre 1 et n que l'exposant de p dans $m!$ est $\displaystyle\sum_{j=1}^{q} \left[\frac{m}{p^j}\right]$.

IV∼2) Déduisez l'exposant de p dans $C(n)$.

IV∼3) Montrez pour tout réel x de $[1, +\infty[$ et tout k de $\mathbb{N}^*$: $\displaystyle\sum_{i=1}^{k} \left[\frac{x}{a_i}\right] \leqslant [x]$ (indication : montrez déjà $\left[\frac{x}{a}\right] = \left[\frac{[x]}{a}\right]$).

V∼0) Pour tout n, on note $\boxed{d_n}$ le p.p.c.m. des entiers de 2 à n (par exemple $d_6 = 60$), calculez d_{11}.

On vérifie : le p.p.c.m. de 2, 3, 4, 5 et 6 est un multiple de ces entiers.
L'entier 60 convient.
Mais est ce le plus petit ?
Notre entier doit être multiple de 2, 4 et 6 : c'est un multiple de 12.
multiple de 5 : c'est un multiple de 60.
C'est donc 60.

Et pour les entiers plus petits, ou plus grands :

2											2	
2	3										6	×3
2	3	4									12	×2
2	3	4	5								60	×5
2	3	4	5	6							60	
2	3	4	5	6	7						420	×7
2	3	4	5	6	7	8					840	×2
2	3	4	5	6	7	8	9				2520	×3
2	3	4	5	6	7	8	9	10			2520	
2	3	4	5	6	7	8	9	10	11		27720	×11

La colonne de droite indique le multiplicateur.

Pour passer d'un d_n au suivant, on exploite l'associativité du p.p.c.m.

$$p.p.c.m.(2,\ 3,\ 4,\ \ldots n,\ n+1) = p.p.c.m.\Big(p.p.c.m.(2,\ 3,\ 4,\ \ldots n),\ n+1\Big) = p.p.c.m.(d_n,\ n+1)$$

Et si $n+1$ est premier, il faut multiplier par $n+1$ qui n'était pas encore présent dans le produit.
Si en revanche $n+1$ est déjà dans le produit, ce n'est pas la peine d'en demander plus.

Mais comment calculer effectivement ce nouveau p.p.c.m. ?
On utilise la relation $p.p.c.m.(a,b) \times p.g.c.d.(a,\ b) = a \times b$, qu'on écrit aussi $p.p.c.m.(a,\ b) = \dfrac{a \times b}{p.g.c.d.(a,\ b)}$ ou même $p.p.c.m.(a,\ b) = a \times \dfrac{b}{p.g.c.d.(a,\ b)}$.

On va donc avancer suivant une boucle.
On commence à 1 et à chaque fois, on multiplie par $\dfrac{n}{p.g.c.d.(p_{n-1},\ n)}$.

V∼1) Écrivez un script Python qui prend en entrée n et calcule d_n.

```
def d(n) :
....p = 1
;...for k in range(1, n+1) :
........pgcd = gcd(p, k)
........p *= k//pgcd
....return p
```

On sait qu'à chaque fois $\dfrac{k}{p.g.c.d.(p,k)}$ sera bien un entier, par définition du « diviseur commun ».

Et pour trouver le p.g.c.d. de deux entiers ? Euclide :

```
def gcd(a ,) :
....while b > 0 :
........a, b = b, a%b
....return a
```

Pour information : $d(20) = 232\,792\,560 = 2^4.3^2.5.7.11.13.17$
$d(30) = 2\,329\,089\,562\,800 = 2^4.3^2.5.7.11.13.17.19.23.29$
$d(100) = 69720375229712477164533808935312303556800$

V∼2) Déduisez des parties précédentes que $C(n)$ est un multiple de d_n.

V∼3) Montrez qu'à partir d'un rang n_0 on a $d_n \leqslant 3^n$.

∘49∘ Existe-t-il M vérifiant $Com(M) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Même question avec $Com(M) = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

∘50∘ ♡ Sachant $a+b=3$ et $6^a+6^b=42$, calculez a^6+b^6.

∘51∘ $\dfrac{4}{3.5} + \dfrac{9}{8.10} + \dfrac{25}{24.26} + \dfrac{64}{63.65} + \ldots = \displaystyle\sum_{n=2}^{+\infty} \dfrac{(F_n)^2}{((F_n)^2-1).((F_n)^2+1)} = ?$.
Et si vous ne trouvez pas, écrivez au moins le programme qui calcule cette somme de 2 à N donné.

∘52∘ Pour tout n, on pose $F_n = 2^{(2^n)} + 1$. Calculez F_1 à F_4. Vérifiez qu'ils sont premiers.
Montrez que F_5 est divisible par 641.
Montrez : $\displaystyle\prod_{k=0}^{n} F_k = F_n - 2$.
Montrez que si un entier p divise F_n et F_N $(n < N)$ alors p divise 2.
Déduisez que $F_n$et F_N sont premiers entre eux.
Pour tout n, on note p_n le plus petit nombre premier qui divise F_n.
Montrez que la suite des (p_n) est une suite contenant une infinité de termes.
Écrivez tant qu'on y est un script Python qui détermine p_n pour n donné.

∘53∘

♡ Pour tout entier naturel n, on note $\varphi(n)$ le nombre d'entiers entre 0 et 1 qui sont ptemiers avec n ($p.g.c.d.(n,k=1)$.
Montrez : $\varphi(p)=p-1$ si p est premier.
Montrez : $\varphi(p^2)=p^2-p$ et plus généralement $\varphi(p^k)=p^k-p^{k-1}$ pour p premier et k entier.
p et q sont deux entiers premiers distincts. Justifiez : $\varphi(p.q)=p.q-p-q+1$.
Démontrez : $\varphi(2022)=2022.\left(1-\frac{1}{1}\right).\left(1-\frac{1}{3}\right).\left(1-\frac{1}{337}\right)$, $\varphi(2023)=2023.\left(1-\frac{1}{7}\right).\left(1-\frac{1}{17}\right)$ et $\varphi(2024)=2024.\left(1-\frac{1}{2}\right).\left(1-\frac{1}{11}\right).\left(1-\frac{1}{23}\right)$.

Pour p premier, tous les entiers de 1 à $p-1$ inclus sont premiers avec p (quel diviseur commun pourraient ils avoir ?).
On en a $p-1$ (pour l'informaticien, le décompte se fait : c'est $range(1,\ p)$, et donc on a $p-1$ éléments).

Qui sont les entiers de 1 à p^2 qui sont premiers avec p ?
Qui sont les entiers de 1 à p^2 qui ne sont pas premiers avec p ?
Qui sont les entiers de 1 à p^2 qui ont un diviseur commun avec p ?
Qui sont les entiers de 1 à p^2 qui sont multiples de p ? Ce sont les $k.p$ avec $k\in range(1,\ p)$.
Il faut donc éliminer p entiers parmi les p^2. Il en reste p^2-p.

Pour p^k, on doit juste prendre p^k entiers et éliminer les multiples de p. Ce sont les $j.p$ avec j pouvant aller de 1 à p^{k-1}.
Il y en a p^{k-1}.
On a donc bien p^k-p^{k-1} entiers premiers avec p.

Exemple : $p=3$ et $k=3$. Ecrivez les entiers de 1 à 27 et enlevez les 9 multiples de 3.

Cette fois, on a deux entiers premiers, comme 5 et 7.
On va de 1 à $p\times q$ (de 1 à 35).
Qui faut il élminer (on raosnne comme souvent en proababilités par événement complémentaire).
On doit élimner ceux qui ont un facteur commun avec $p\times q$.
C'est à dire ceux qui ont un facteur p et aussi ceux qui ont un facteur q.
On doit éliminer les multiples de p et les multiples de q.

Mais attention, $Card(M_p\cup M_q)=Card(M_p)+Card(M_q)-Card(M_p\cap M_q)$.

Il y a q nombres de la forme $k\times p$ (k de 1 à q) et p nombres de la forme $j.q$ (j de 1 à p).
Mais il y en a un (et un seul) qu'on a décompté deux fois : $p\times q$.

On a donc $p\times q-p-q+1$ nombres à compter.

Sur notre exemple :

il y a 35 nombre sde 1 à 35							
5	10	15	20	25	30	35	on en enlève 7
7	14	21	28	35			on en enlève 5
							il faut remettre 35

$2022=2\times 3\times 337$.
On a donc 2022 nombres.
Il faut enlever • les multiples de 2 : il y en 1011
• les multiples de 3 : il y en a 674
• les mutiples de 337 : il y en a 6
Mais attention aux multiples de 6. On les a enlevés deux fois. Il faut les recompter.
Allez, proprement, on note M_2 les multiples de k.
On doit trouver le cardinal de $M_2\cup M_3\cup M_{337}$.
C'est $Card(M_2)+Card(M_3)+Card(M_{337})-Card(M_2\cap M_3)-Card(M_2\cap M_{337})-Card(M_3\cap M_{337})+Card(M_2\cap M_3\cap M_{337})$.

Cette formule vient de $1_{A\cup B\cup C}=1_{A\cup B\cup C}-1_{A\cup B}-1_{A\cup C}-1_{B\cup C}+1_{A\cap B\cap C}$
qui elle même vient par formule de de Morgan de $(1-1_{A\cup B\cup C})=(1-1_A).(1-1_B).(1-1_C)$.

Or, chaque M_k a pour cardinal $\dfrac{2022}{k}$.

Bref, on doit soustraire à 2022 la somme alternée $\dfrac{2022}{2}+\dfrac{2022}{3}+\dfrac{2022}{337}-\left(\dfrac{2022}{2.3}+\dfrac{2022}{2.337}+\dfrac{2022}{3.337}\right)+\dfrac{2022}{2.3.337}$.

On a donc une formule du type $N-\dfrac{N}{a}-\dfrac{N}{b}-\dfrac{N}{c}+\dfrac{N}{a.b}+\dfrac{N}{a.c}+\dfrac{N}{b.c}-\dfrac{N}{a.b.c}$.

C'est bien $\varphi(2022)=2022.\left(1-\dfrac{1}{1}\right).\left(1-\dfrac{1}{3}\right).\left(1-\dfrac{1}{337}\right)$.

On fait visiblement de même avec $2023=7.17^2$.

On enlève les $\dfrac{2023}{7}$ multiple de 7 et les $\dfrac{223}{17}$ mutiples de 17, et on remet les $\dfrac{2023}{7\times 17}$ multiples de 7×17.

On peut même raconter la formule générale.

Elle tient compte des facteurs premiers de N, mais finalement pas de leur exposant.

∘54∘

Inversez $\begin{pmatrix}1&2&-1\\2&5&1\\2&5&2\end{pmatrix}$ puis $\begin{pmatrix}1&2&-1&0\\2&5&1&1\\2&5&2&3\\3&5&-6&0\end{pmatrix}$ par la méthode du pivot de Gauss.

$\left[\begin{array}{ccc\|ccc}1&2&-1&1&0&0\\2&5&1&0&1&0\\2&5&2&0&0&1\end{array}\right]$	$\left[\begin{array}{ccc\|ccc}1&2&-1&1&0&0\\0&1&3&-2&1&0\\0&1&4&-2&0&1\end{array}\right]$	$\left[\begin{array}{ccc\|ccc}1&2&-1&1&0&0\\0&1&3&-2&1&0\\0&0&1&0&-1&1\end{array}\right]$
	$L2=L2-2.L1$ $L3=L3-2.L1$	$L3=L3-L2$
$\left[\begin{array}{ccc\|ccc}1&2&0&1&-1&1\\0&1&0&-2&4&-3\\0&0&1&0&-1&1\end{array}\right]$	$\left[\begin{array}{ccc\|ccc}1&2&0&5&-9&7\\0&1&0&-2&4&-3\\0&0&1&0&-1&1\end{array}\right]$	$\begin{pmatrix}5&-9&7\\-2&4&-3\\0&-1&1\end{pmatrix}$
$L1=L1+L3$ $L2=L2-3.L3$	$L1=L1-2.L2$	c'est elle

∘55∘

Résolvez par pivot de Gauss, et discutez :

$\begin{cases}x+2.y=1\\2.x+y=2\\3.x+4.y=1\end{cases}$	$\begin{cases}x-y+3.z=1\\2.x-2.y+z=3\\2.x-y-z=0\end{cases}$	$\begin{cases}x+2.y=1\\2.x+y=2\\3.x+4.y=3\end{cases}$
a	b	c
$\begin{cases}x-2.y+z=1\\-x+3.z=5\\x-3.y+z=1\\x+4.y-z=a\end{cases}$	$\begin{cases}a.x+b.y+z=1\\x+a.b.y+z=b\\x+b.y+a.z=1\end{cases}$	$\begin{cases}x+2.y+z+2.t+3.u=1\\x+3.y+z+2.t=1\\y-3.u=-1\end{cases}$
d	e	f
$\begin{cases}x+y-z=a\\x-y=b\\x+4.y+z=c\end{cases}$	$\begin{cases}x-y+z=\lambda.x\\2.x-5.y+4.z=\lambda.y\\2.x-7.y+6.z=\lambda.z\end{cases}$	$\begin{cases}x+y+z+t=1\\x+2.y+2.z+2.t=3\\x+2.y+3.z+3.t=5\\x+2.y+3.z+4.t=9\end{cases}$
g	h	i

$\begin{cases}x+2.y=1\\2.x+y=2\\3.x+4.y=1\end{cases}$	$\begin{cases}x-y+3.z=1\\2.x-2.y+z=3\\2.x-y-z=0\end{cases}$	$\begin{cases}x+2.y=1\\2.x+y=2\\3.x+4.y=3\end{cases}$
$\begin{cases}x+2.y=1\\-3.y=0\\-2.y=-2\end{cases}$	$\begin{cases}x-y+3.z=1\\-5.z=1\\y-7.z=-2\end{cases}$	$\begin{cases}x+2.y=1\\-3.y=0\\-2.y=0\end{cases}$
$S_{(x,y)}=\emptyset$	$\begin{cases}x-y=8/5\\y=-17/5\\z=-1/5\end{cases}$	$\begin{cases}x=1\\y=0\\y=0\end{cases}$
	$\begin{cases}x=-9/5\\y=-17/5\\z=-1/5\end{cases}$	$S_{(x,y)}=\{(1,0)\}$
	$S_{(x,y,z)}=\left\{\left(\dfrac{-9}{5},\dfrac{-17}{5},\dfrac{-1}{5}\right]\right\}$	

∘56∘

On suppose qu'il n'y a qu'un nombre fini de nombres premiers congrus à 3 modulo 4 : notés de p_1 à p_N. On définit alors $4.p_1 \dots p_N - 1$ *(noté Q)*. Montrez que Q admet au moins un diviseur premier. Montrez que Q admet au moins un diviseur premier congru à 3 modulo 4. Montrez que ce diviseur ne peut pas être l'un des p_i.
Déduisez : il y a une infinité de nombres premiers congrus à 3 modulo 4.

Il se peut que Q soit premier, auquel cas, Q est lui même undiviseur premier de Q.
Mais de toutes façons, tout entier (à part 1) admet au moins un diviseur premier.

C'est une question idiote, sans aucune difficulté. Mais elle est là pour définir des objets pour la suite.

Pour montrer qu'ua moins un diviseur premier de Q est congru à 3 modulo 4, on raisonne par l'absurde.
On supposoe qu'aucun diviseur premier q de Q n"est congru à 3 modulo 4.
C'est donc qu'ils sont tous congrus à 1, 2 ou 4.
Mais un nombre premier congru à 4, je n'ai pas ça en magasin.
De même, il n'y a qu'un nombre premier qui soit congru à 2 modulo 4, c'est 2. Or, Q est impair. 2 n'est donc pas un de ses diviseurs.
On a donc éliminé, il ne reste que « les diviseurs premiers de Q sont tous congrus à 1 modulo 4 ».

Mais alors, leur produit est aussi congru à 1 modulo 4.

> *Par récurrence immédiate, le produit de deux entiers congrus à* 1 *modulo* 4 *est congru à* 1 *modulo* 4.
> *Et maintenant qu'on parle de congruences, il suffit de dire qu'il y a compatibilité avec la multiplication.*
> *S'il vous plait, contentez vous de dire* $q = 1[4]$ *et* $r = 1[4] \Rightarrow (q \times r) = 1[4]$ *», c'est directe.*
> *Et ne m'alourdissez pas votre copie avec des* $q = 4.k + 1$ *et* $r = 4.i + 1$ *et autres indigestions de ce type. On n'est plus au collège !*

Or, Q est congru à -1 modulo 4 et non à 1.

Ainsi, par élimination, au moins un des facteurs premiers de Q est congru à 3 modulo 4. Nommons le q.

Se pourrait il que q soit déjà l'un des p_i ?
On aurait alors q divise Q et q divise $4 \times p_1 \times p_2 \dots \times p_N$ (puisque c'est l'un d'eux).
q divise donc la différence des deux. Et cette différence vaut 1. Ce qui n'est pas possible pour un nombre premier q.

On a donc trouvé un nouveau nombre premier congru à 3 modulo 4.

Ceci contredit qu'il n'y en ait eu que N.

C'est donc que l'ensemble des nombres premiers congrus à 3 modulo 4 est infini.

Un exemple pour saisir.
On a trouvé les nombres premiers suivants, tous congrus à 3 *modulo* 4 *:* 3, 7, 23 *et* 67, *et on dit que c'est tout (faut il variment être con, et n'avoir pas vu* 11 *ou* 31, *mais tant pis).*
On construit alors $Q = 4.3.7.23.67 - 1 = 129443$.
On le décompose en produit de facteurs premiers : il est premier.
Et congru à 3 *modulo* 4 *(vous avez vu* 129443*).*

Celui qui serait parti de 3, 7, 11 *et* 23 *trouvait* $Q = 21251$. *Et cette fois, la factorisation donnait* $21251 = 79 \times 269$. *Et c'est* 79 *qui est congru à* 3 *modulo* 4.

On notera qu'on recommence alors avec $Q = 4.3.7.11.23.79 - 1$ *qui va nous donner* 193×8699. *Devinez lequel est congru à* 3 *modulo* 4.

∘57∘

On rappelle la définition de l'ordre d'un élément dans un groupe $(G, *)$ de neutre e : $Ord(a) = Inf\{n > 0 \mid a^n = 1\}$ (si un tel n existe).
On suppose que $(G, *)$ est commutatif
a est d'ordre 5 et b d'ordre 7.
Montrez que $a * b$ est d'ordre 35.
Montrez que ce n'est plus forcément vrai si $(G, *)$ n'est pas commutatif.

Pour un groupe non commutatif, on peut prendre $\overrightarrow{(1\,2\,3\,4\,5)}$ et $\overrightarrow{(6\,7\,8\,9\,10\,11\,12)}$ d'ordres 5 et 7.

Leur composée est le cycle $\overrightarrow{(1\ 2\ \dots\ 11\ 12)}$ qui est d'ordre 12.

∘58∘ ♡ Déterminez la limite quand n tend vers l'infini de $\dfrac{\sum\limits_{\substack{k\leqslant 2.n\\ k\ pair}} k}{\sum\limits_{\substack{k\leqslant 2.n\\ k\ impair}} k}$.

Formules connues :

$\sum\limits_{k=0}^{2.n} k = \dfrac{2.n.(2.n+1)}{2}$	$\sum\limits_{\substack{0\leqslant k\leqslant 2.n\\ k\ pair}} k = \sum\limits_{p=0}^{n} 2.p = 2.\sum\limits_{p=0}^{n} p = n.(n+1)$
	$\sum\limits_{\substack{0\leqslant k\leqslant 2.n\\ k\ impair}} k = \sum\limits_{k=0}^{n} k - \sum\limits_{\substack{0\leqslant k\leqslant 2.n\\ k\ pair}} k = n^2$ (connu)

Le quotient vaut $\dfrac{n^2+n}{n^2}$ et il tend vers 1 comme on s'en doute (proportion des pairs et des impairs).

∘59∘ ♡ N est un entier naturel fixé. Montrez que les suites $\left(\dfrac{2^n}{n+1}\right)_{n\in\mathbb{N}}$, $\left(\dfrac{2^n}{N+1}\right)_{n\in\mathbb{N}}$ et $\left(\dfrac{2^N}{n+1}\right)_{n\in\mathbb{N}}$ sont monotones.

Pour la première : $\dfrac{2^{n+1}}{n+2} \geqslant \dfrac{2^n}{n+1}$ pour tout n (soustraire, réduire au dénominateur commun).

Pour la seconde $\dfrac{2^{n+1}}{N+1} \geqslant \dfrac{2^n}{N+1}$ pour tout n.

Pour la troisième : $\dfrac{2^N}{n+2} \leqslant \dfrac{2^N}{n+1}$.

∘60∘ Calculez $S_n = \sum\limits_{0\leq p\leq q\leq n} 2^p.3^q$. Calculez $O_n = \sum\limits_{\substack{0\leq p\leq n\\ 0\leq q\leq n}} 2^q.3^p$. Calculez $H_n = \sum\limits_{0\leq q\leq n} 2^q.3^q$. Calculez $E_n = \sum\limits_{0\leq p\leq n} 2^{2.p}.3^{3.p}$. Calculez $L_n = \sum\limits_{0\leq p\leq q\leq n} 2^q.3^q$ (attention, q a son rôle, c'est un compteur).

∘61∘ Partant de `A`, je propose les variantes suivantes ; indiquez le résultat pour chacune

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

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

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

D
```
def gcd(a, b) :
....while b == 0 :
........(a, b) = (b, a%b)
....return a
```

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

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

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

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

I
```
def gcd(a, b) :
....while b == 0 :
........a, b = b, a%b
....return a
```

∘62∘ Montrez : $\sqrt{2.\sqrt{3.\sqrt{4}}} + \sqrt{4.\sqrt{3.\sqrt{2}}} \leqslant 5,5$.

Le physicien dira : je calcule avec la calculatrice.
Le matheux dira : je vais prouver

$$\sqrt{2.\sqrt{3.\sqrt{4}}} + \sqrt{4.\sqrt{3.\sqrt{2}}} \leqslant \frac{11}{2}$$

pour n'avoir que des entiers dans l'écriture.

On note

$$\sqrt{2.\sqrt{3.\sqrt{4}}} = \sqrt{2.\sqrt{6}} = 2^{1/2}.6^{1/4} = \sqrt[4]{2.2.2.6}$$

On note aussi

$$\sqrt{4.\sqrt{3.\sqrt{2}}} = 2.\sqrt[4]{3.\sqrt{2}} = 2.\sqrt[8]{3^2.2} = 2.\sqrt[8]{3.3.2.1.1.1.1.1}$$

Pourquoi faire tout ça ? Parce qu'on connaît la comparaison des moyennes :

$$\sqrt{a.b} \leqslant \frac{a+b}{2},\ \sqrt[4]{a.b.c.d} \leqslant \frac{a+b+c+d}{4},\ \sqrt[8]{a_1.a_2\dots a_8} \leqslant \frac{a_1+a_2+\dots+a_8}{8}$$

(on a la première de multiples façons dans le cours, et on emboite la première dans elle même pour avoir les autres).
On a donc

$$\sqrt{2.\sqrt{3.\sqrt{4}}} = \sqrt[4]{2.2.2.6} \leqslant \frac{2+2+2+6}{4} = 3$$

$$\sqrt{4.\sqrt{3.\sqrt{2}}} = 2.\sqrt[8]{3.3.2.1.1.1.1.1} \leqslant 2.\frac{3+3+2+1+1+1+1+1}{8} = \frac{13}{4}$$

Voilà, c'est fini, c'est super joli...
et ça ne serrt à rien ajoute le physicienqui repose sa calculatrice.
Et le même physicien ira à un concert, ou dans un musée ou face à un coucher de soleil et il dira c'est beau.
Mais il lui manquera une partie du sens de la beauté pour trouver jolie cette démonstration.

◦63◦ Calculez $3+\dfrac{1}{7+\dfrac{1}{15+\dfrac{1}{1}}}$ et $3+\dfrac{1}{7+\dfrac{1}{15}}$ à 10^{-7} près.

Qui sont $1+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{1+\dots}}}$, $2+\dfrac{1}{2+\dfrac{1}{2+\dfrac{1}{2+\dots}}}$ et $2+\dfrac{1}{1+\dfrac{1}{2+\dfrac{1}{1+\frac{1}{2+\frac{1}{1+\dots}}}}}$?

Donnez le dévelmoppement en fraction continuée de $\sqrt{5}$.

Le premier vaut $\dfrac{355}{113}$ et vaut 3.1415929 à 10^{-7} près.

Le second vaut $\dfrac{333}{106}$ et donne 3.1415094 à 10^{-7} près.

Ca doit vous arppeler π. D'ailleurs, si j'avais coupé plus tôt, vous aviez $3+\dfrac{1}{7}=\dfrac{22}{7}$ qu'on vous a peut être donné dans les petits classes comme approximation de π.

Pour les fractions suivantes, sans chercher à justifier leur existence,on leur donne un nom et on trouve une relation vérifiée par le nombre.

$a=1+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{1+\dots}}}$	$a=1+\dfrac{1}{a}$	et $a>0$
	$a^2-a-1=0$	$a=\dfrac{1+\sqrt{5}}{2}$
$b=2+\dfrac{1}{2+\dfrac{1}{2+\dfrac{1}{2+\dots}}}$	$b=2+\dfrac{1}{b}$	et $b>0$
	$b^2-2.b-1=0$	$b=1+\sqrt{2}$
$c=2+\dfrac{1}{1+\dfrac{1}{2+\dfrac{1}{1+\frac{1}{2+\frac{1}{1+\dots}}}}}$	$c=2+\dfrac{1}{1+\dfrac{1}{c}}$	
	$c^2-2.c-2=0$ et $c+1\neq 0$	$c=1+\sqrt{3}$

Pour $\sqrt{5}$, on pose $x=\sqrt{5}$ et on cherche une mise en boucle similaire :

$$\sqrt{5}=2+(\sqrt{5}-2)=2+\frac{5-4}{2+\sqrt{5}}=2+\frac{1}{2+\sqrt{5}}=2+\frac{1}{4+(\sqrt{5}-2)}=2+\frac{1}{4+\frac{(5-4)}{2+\sqrt{5}}}$$

Le nombre intéressant est donc $2+\sqrt{5}$ qui vérifie $x=4+\frac{1}{x}$ et se met en boucle ;

$$\sqrt{5}=2+\cfrac{1}{4+\cfrac{1}{4+\cfrac{1}{4+\frac{1}{4+\ldots}}}}$$

∘64∘ Montrez que pour résoudre $\left|\begin{array}{rcll} n & = & \alpha & [7] \\ n & = & \beta & [12] \end{array}\right|$ il suffit de savoir résoudre $\left|\begin{array}{rcll} n & = & 1 & [7] \\ n & = & 0 & [12] \end{array}\right|$ et $\left|\begin{array}{rcll} n & = & 0 & [7] \\ n & = & 1 & [12] \end{array}\right|$.

Trouvez l'inverse de 12 dans $\mathbb{Z}_{7.\mathbb{Z}}$ et déduisez les solutions de $\left|\begin{array}{rcll} n & = & 1 & [7] \\ n & = & 0 & [12] \end{array}\right|$.

Trouvez l'inverse de 7 dans $\mathbb{Z}_{12.\mathbb{Z}}$ et déduisez les solutions de $\left|\begin{array}{rcll} n & = & 0 & [7] \\ n & = & 1 & [12] \end{array}\right|$.

Montrez que pour résoudre $\left|\begin{array}{rcll} n & = & \alpha & [7] \\ n & = & \beta & [15] \\ n & = & \gamma & [16] \end{array}\right|$ il suffit de savoir résoudre $\left|\begin{array}{rcll} n & = & 1 & [7] \\ n & = & 0 & [15] \\ n & = & 0 & [16] \end{array}\right|$ et deux autres systèmes similaires.

Trouvez l'inverse de 15, de 16 et de 15.16 dans $\mathbb{Z}_{7.\mathbb{Z}}$ et déduisez les solutions de $\left|\begin{array}{rcll} n & = & 1 & [7] \\ n & = & 0 & [15] \\ n & = & 0 & [16] \end{array}\right|$.

Résolvez $\left|\begin{array}{rcll} n & = & 1 & [7] \\ n & = & 2 & [15] \\ n & = & 4 & [16] \end{array}\right|$.

Si l'on a trouvé n_1 et n_2 vérifiant $\left|\begin{array}{rcll} n_1 & = & 1 & [7] \\ n_1 & = & 0 & [12] \end{array}\right|$ et $\left|\begin{array}{rcll} n_2 & = & 0 & [7] \\ n_2 & = & 1 & [12] \end{array}\right|$ alors l'entier $p=\alpha.n_1+\beta.n_2$ vérifie

$$\left|\begin{array}{rcll} p & = & 1.\alpha+0.\beta & [7] \\ p & = & 0.\alpha+1.\beta & [12] \end{array}\right|$$

et c'est une solution particulière cherchée.

Dans $\mathbb{Z}_{7.\mathbb{Z}}$ l'inverse de 12 est 3 (car $3.12=36=35+1=1$)
on déduit $3.12=1$ *mod* 7 puis $\left|\begin{array}{rcll} 36 & = & 1 & [7] \\ 36 & = & 0 & [12] \end{array}\right|$.
Dans $\mathbb{Z}_{12.\mathbb{Z}}$, l'inverse de 7 est -5 (c'est à dire 7)
on déduit $7.7=1[12]$ on a une solution particulière $\left|\begin{array}{rcll} 49 & = & 0 & [7] \\ 49 & = & 1 & [12] \end{array}\right|$.

Résumé : on a une solution particulière de

$$\left|\begin{array}{rcll} n & = & \alpha & [7] \\ n & = & \beta & [12] \end{array}\right| : 36.\alpha+49.\beta$$

Résolvons $\left|\begin{array}{rcll} n & = & 1 & [7] \\ n & = & 0 & [15] \\ n & = & 0 & [16] \end{array}\right|$ en cherchant un nombre nul modulo 15 et 16 (multiple de 15.16) et égal à 1 modulo 7.

15 est son propre inverse modulo7.	L'inverse de 7 modulo 15 est 13.	L'inverse de 7 modulo 16 est 7.
L'inverse de 16 modulo 7 est 4.	L'inverse de 16 modulo 15 est 16.	L'inverse de 15 modulo 16 est 15.
L'inverse de 15.16 modulo 7 est 4.	L'inverse de 7.16 modulo 15 est 13.	L'inverse de 7.15 modulo 7 est 105.
$\left\|\begin{array}{rcll} 4.(15.16) & = & 1 & [7] \\ 4.(15.46) & = & 0 & [15] \\ 4.(15.16) & = & 0 & [16] \end{array}\right\|$	$\left\|\begin{array}{rcll} 13.(7.16) & = & 0 & [7] \\ 13.(7.16) & = & 1 & [15] \\ 13.(7.16) & = & 0 & [16] \end{array}\right\|$	$\left\|\begin{array}{rcll} 105.(7.15) & = & 1 & [7] \\ 105.(7.15) & = & 0 & [15] \\ 105.(7.15) & = & 0 & [16] \end{array}\right\|$

Par combinaison une solution de $\left|\begin{array}{lcll} n & = & \alpha & [7] \\ n & = & \beta & [15] \\ n & = & \gamma & [16] \end{array}\right|$ est

$$\alpha.(4.(15.16)) + \beta.(13.(7.16)) + \gamma.(105.(7.15))$$

Et on a toutes les solutions en ajoutant les solutions homogènes : $\left|\begin{array}{lcll} h & = & 0 & [7] \\ h & = & 0 & [15] \\ h & = & 0 & [16] \end{array}\right|$: $H = (7.15.16).\mathbb{Z}$.

◦65◦

Un nombre dernier est un nombre qui a beaucoup de diviseurs ; c'est à dire qui a plus de diviseurs que tous les entiers plus petits que lui. Écrivez un programme qui liste des quarante premiers entiers derniers *(et pas des quarante derniers nombres premiers)*.

On va avoir besoin d'une procédure qui compte le nombre de diviseurs d'un entier `n` :

```
def NbDiv(n) :
....Nb = 0
....for k in range(1, n+1) :
........if n%k == 0 :
............Nb += 1
....return Nb
```

Ensuite, on met en boucle avec un `NbMax` qui monte dès qu'on a un nouveau record, et une liste `L` qu'on agrandit peu à peu :

```
L = []
NbMax = 0
for n in range(1, beaucoup) :
....if NbDiv(n) > NbMax :
........L.append(n)
........NbMax = NbDiv(n)
print(L)
```

Reste la question du beaucoup. Combien pour avoir 40 nombres derniers ?
On va remplacer la boucle for par une boucle while :

```
L = []
NbMax = 0
n = 1
while len(L) < 40 :
....if NbDiv(n) > NbMax :
........L.append(n)
........NbMax = NbDiv(n)
....n += 1
print(L)
```

Et plus proprement, pour ne pas calculer deux fois la même quantité :

```
L = []
NbMax = 0
n = 1
while len(L) < 40 :
....NbDivn = NbDiv(n)
....if NbDivn > NbMax :
........L.append(n)
........NbMax = NbDivn
....n += 1
print(L)
```

Liste des vingt premiers avec leur nombre de diviseurs :
`[1, 1], [2, 2], [4, 3], [6, 4], [12, 6], [24, 8], [36, 9], [48, 10], [60, 12], [120, 16], [180, 18], [240, 20], [360, 24], [720, 30], [840, 32], [1260, 36], [1680, 40], [2520, 48], [5040, 60], [7560, 64]]`

Au fait, pourquoi est on sûr qu'on aura bien 40 nombres derniers ?
Simplement parce que tout record finit par être dépassé. Si il y avait un dernier nombre dernier, il s'appellerait G et aurait D diviseurs. mais alors le nombre 2^D aurait $D+1$ diviseurs. Fermez le ban, fin du raisonnement par l'absurde.

◦66◦

Sachant qu'il y a 168 nombres premiers entre 1 et 1000, lequel de ces quatre nombres est leur somme :

11 569	76 127	57 298	81 744

Déjà, la liste commence par 2, mais ensuite ils sont tous impairs.
Il y a donc modulo 2 un nombre pair et 167 impairs.
La somme vaut $0 \times 1 + 167 \times 1$ mdoulo 2. Nombre impair.

On en élimine deux :

11 569	76 127	57 298	81 744
		non	non

Le premier semble un peu petit, mais il doit y avoir un autre argument pour l'éliminer.

Ensuite, l'informaticien brutal vérifie.

```
def est-premier(n) : #int -> boolean
....for k in range(2, n) : #la liste des entiers de 1 à n-1
........if n%k == 0 : #il y a un diviseur propre
............return False #le nombre n'est pas premier
....return True #aucun diviseur propre, il est premier
```

Et maintenant, la procédure.

```
def les_premiers(N) :
....s, c = 0, 0 #somme et compteur
....for n in range(N+1) :#ne pas essayer 1, et aller jusqueà n inclus
........if est_premier(n) : #le test précédent
............c += 1 #compteur
............s+= n #somme
....return s, c #la somme et le compteur
```

L'informaticien plus rusé optimise son test en créant au fur et à mesure une liste desnombres premiers.
Et pour tester si un nouveau nombre n est premier, il suffit de voir si il est divisible par un des nombres déjà croisés.

```
def les_premiers(N) : #int -> int, int, list of int
....prem = [ ] #liste des nombres premiers
....s, c = 0, 0 #somme et compteur
....for n in range(N+1) :#ne pas essayer 1, et aller jusqueà n inclus
........test =
........for p in prem :
............test *= n%p #n est il divisible par au moins un des nombres premiers de la liste
........if test != 0 :
............prem.append(n) #oui, un nouveau nombre premier
............c += 1 #compteur
............s+= n #somme
....return s, c, prem #la somme, le compteur et la liste
```

On notera qu'avec `len(prem)` on peut se passer du compteur `c`.

◦67◦

Vous avez les entiers de 1 à 200 *(inclus)*. Vous en tirez cinq. Combien de tirages possibles ?
Combien de tirages contiennent exactement deux nombres pairs et exactement deux nombres premiers.
pour information, le 46^{ieme} nombre premier est 199.
Les raisonnements qui suivent sont faux,, pourquoi ?

- $\bullet_1$ Il y a cent nombres pairs, d'où $\binom{200}{100}$ et 46 nombres premiers : on additionne $\binom{200}{46}$: $\binom{200}{100}+\binom{200}{46}$.
- $\bullet_2$ Il y a cent nombres pairs, d'où $\binom{100}{2}$ et 46 nombres premiers : on additionne $\binom{46}{2}$: $\binom{100}{2}+\binom{46}{2}$.
- $\bullet_3$ Il y a cent nombres pairs, d'où $\binom{100}{2}$ et 46 nombres premiers : on multiplie $\binom{46}{2}$: $\binom{100}{2}\times\binom{46}{2}$.
- $\bullet_4$ Il y a cent nombres pairs, d'où $\binom{200}{100}$ et 46 nombres premiers dans ce qu'il reste : on additionne $\binom{200}{46}$: $\binom{200}{100}.\binom{100}{46}$.
- $\bullet_5$ Il y a cent nombres pairs, d'où $\binom{200}{100}$ et 46 nombres premiers dans ce qu'il reste, et il faut prendre un dernier élément dans ce qu'il reste encore : $\binom{100}{2}.\binom{46}{2}.\binom{54}{1}$ *(il y a bien* 54 *nombres impairs, non premiers)*.

Trouvez la vraie réponse.

◦68◦

Un nombre second est un nombre produit de deux nombres premiers distincts. Écrivez un script qui pour `N` donné calcule combien entre `0` et `N` il y a de nombres seconds *(en supposant que vous avez un programme* **`prem`** *qui teste si un nombre est premier)*.
L'ensemble des nombres seconds est il stable par addition ? Par multiplication ?

```
def EstPremier(n) :
....for k in range(2, n) :
........if n%k == 0 :
............return False
....return True
```

on suppose N déjà donné, on fait de l'info, pas du dialogue avec l'ordinateur

```
Prem = [] #liste des nombres premiers, vide pour l'instant
for k in range(2,N+1) : #on va chercher parmi les entiers avant N
....if EstPremier(k) :
........Prem.append(k) #on mémorise les entiers premiers
Second = [ ]
for k in range(len(Prem)) : #pour un produit de deux nombres premiers, il en faut déjà un
....for i in range(k) : #et un autre, qui sera plus petit que le premier
........Sec = Prem[k]*Prem[i] #on calcule leur produit
.........if Sec<N+1 : #mais on ne le garde que si il est plus petit que N
............Second.append(Sec)
```

D'autres scripts sont possibles.

```
def TestSecond(n) :
....for k in range(2,n) :
........if n%k == 0 : #déjà k est un diviseur de n
............if EstPremier(k) : #et il est premier
................if EstPremier(n//k) : #et l'autre facteur est premier
....................if n !=k*k : #et ce n'est pas deux fois le même facteur premier
........................return True #on a gagne, n est second
....return False #aucun k n'a convenu, n n'est pas second
```

On a crée un test, reste à l'utiliser.

```
Seconds = []
for n in range(N+1) :
....if TestSecond(n) :
........Seconds.append(n)
```

Aucune stabilité additive, ni multiplicative, par les deux contre-exemples que voici :
6 et 10 sont des nombres seconds.
Leur somme 16 ne l'est pas, de même que leur produit.

◦69◦

Le corps de base est l'ensemble des entiers de 0 à $p-1$ (p est un nombre premier au moins égal à 5, je sais). On pose $A = \begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}$. L'application linéaire est $\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto A.\begin{pmatrix} x \\ y \end{pmatrix}$. Déterminez la dimension du noyau de f et de l'image de f (elle peut dépendre de p).
Déterminez aussi la dimension du noyau et de l'image de $M \longmapsto A.M$ de $M_{2,2}(\{0,\dots p-1\})$ dans lui même.

Si la matrice est inversible, l'application est bijective (c'est même une équivalence).

Et si elle est bijective (d'inverse $X \longmapsto A^{-1}.X$), alors son noyau est réduit à $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ et son image est le plan entier [4].

On calcule le déterminant (utile d'ailleurs pour résoudre $\begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}.\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$).

Il vaut 13. Qu'il faut réduire évetuellement modulo p.
Mais si p dépasse 13, $\det(A)$ vaut 13, et 13 est non nul.
Et p vaut au moins 5 pour que 4 ait un sens. On traite donc les premiers cas à part :

	$p=5$	$p=7$	$p=11$	$p=13$	$p>13$
déterminant	$\det(A)\neq 0$	$\det(A)\neq 0$	$\det(A)\neq 0$	$\det(A)=0$	$\det(A)\neq 0$
noyau	$Ker(f)=\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\}$	$Ker(f)=\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\}$	$Ker(f)=\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\}$	à voir	$Ker(f)=\{\begin{pmatrix} 0 \\ 0 \end{pmatrix}\}$
image	$Im(f)=range(p)^2$	$Im(f)=range(p)^2$	$Im(f)=range(p)^2$	à voir	$Im(f)=range(p)^2$

Au fait On ne confondra pas $range(p)^2$ et $range(p^2)$.

Quand p vaut 13, on résout $\begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}.\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.
Les deux équations sont proportionnelles. On passe de la première à la seconde en multipliant par 10 puisque $4.10 = 40 = 1$ et $3.10 = 30 = 4$.
On résout donc juste $x + 4.y = 0$ soit $x = 9.y$.
On trouve les vecteurs de la forme $\begin{pmatrix} 9.y \\ y \end{pmatrix}$ c'est $Vect(\begin{pmatrix} 9 \\ 1 \end{pmatrix})$ ou $Vect(\begin{pmatrix} 5 \\ 2 \end{pmatrix})$. On peut vérifier $\begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}.\begin{pmatrix} 5 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

Pour l'ensemble image, on calcule $\begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}.\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$ et $\begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}.\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$.

Toutes les autres images sont combinaisons des deux : $\begin{pmatrix} 4 & 3 \\ 1 & 4 \end{pmatrix}.\begin{pmatrix} x \\ y \end{pmatrix} = x.\begin{pmatrix} 4 \\ 1 \end{pmatrix} + y.\begin{pmatrix} 3 \\ 4 \end{pmatrix}$.

Mais les deux vecteurs sont proportionnels : $\begin{pmatrix} 3 \\ 4 \end{pmatrix} = 4.\begin{pmatrix} 4 \\ 1 \end{pmatrix}$.

L'ensemble image est $Vect(\begin{pmatrix} 4 \\ 1 \end{pmatrix})$.

Application $M \longmapsto A.M - M.A$. A faire.

---

4. qui est tombé dans le piège et a dit « son image est $\R^2$ » ? non, son image est $range(p)^2$, c'est tout !

◦70◦ On se donne n réels a_1 à a_n. Pour tout k, on note $S_k = \sum_{i=0}^{n} (a_i)^k$ et σ_k la k^{ieme} fonction symétrique des racines $\sigma_k = \sum_{i_1<i_2<\ldots<i_k} a_{i_1}.a_{i_2}\ldots a_{i_k}$.

Exprimez à l'aide des S_k

$$\begin{vmatrix} \sigma_1 & 1 \\ 2.\sigma_2 & \sigma_1 \end{vmatrix} \quad \begin{vmatrix} \sigma_1 & 1 & 0 \\ 2.\sigma_2 & \sigma_1 & 1 \\ 3.\sigma_3 & \sigma_2 & \sigma_1 \end{vmatrix} \quad \begin{vmatrix} \sigma_1 & 1 & 0 & 0 \\ 2.\sigma_2 & \sigma_1 & 1 & 0 \\ 3.\sigma_3 & \sigma_2 & \sigma_1 & 1 \\ 4.\sigma_4 & \sigma_3 & \sigma_2 & \sigma_1 \end{vmatrix} \quad \begin{vmatrix} \sigma_1 & 1 & 0 & 0 & 0 \\ 2.\sigma_2 & \sigma_1 & 1 & 0 & 0 \\ 3.\sigma_3 & \sigma_2 & \sigma_1 & 1 & 0 \\ 4.\sigma_4 & \sigma_3 & \sigma_2 & \sigma_1 & 1 \\ 5.\sigma_5 & \sigma_4 & \sigma_3 & \sigma_2 & \sigma_1 \end{vmatrix}$$

Exprimez à l'aide des σ_k :

$$\begin{vmatrix} S_1 & 1 \\ S_2 & S_1 \end{vmatrix} \quad \begin{vmatrix} S_1 & 1 & 0 \\ S_2 & S_1 & 2 \\ S_3 & S_2 & S_1 \end{vmatrix} \quad \begin{vmatrix} S_1 & 1 & 0 & 0 \\ S_2 & S_1 & 2 & 0 \\ S_3 & S_2 & S_1 & 3 \\ S_4 & S_3 & S_2 & S_1 \end{vmatrix} \quad \begin{vmatrix} S_1 & 1 & 0 & 0 & 0 \\ S_2 & S_1 & 2 & 0 & 0 \\ S_3 & S_2 & S_1 & 3 & 0 \\ S_4 & S_3 & S_2 & S_1 & 4 \\ S_5 & S_4 & S_3 & S_2 & S_1 \end{vmatrix}$$

Donnez *(même sans preuve)* la formule générale, mais pas avec des points de suspension, mais une formule pour le terme général de la matrice dont on calcule le déterminant.

$$\begin{vmatrix} \sigma_1 & 1 \\ 2.\sigma_2 & \sigma_1 \end{vmatrix} = (\sigma_1)^2 - 2.\sigma_2 = \Big(\sum a_k\Big)^2 - 2.\sum_{i,j} a_i.a_j = \sum_k (a_k)^2 = S_2$$

puisque $(\sigma_1)^2$ est le carré de la somme (somme des carrés plus somme des doublets).

$$\begin{vmatrix} \sigma_1 & 1 & 0 \\ 2.\sigma_2 & \sigma_1 & 1 \\ 3.\sigma_3 & \sigma_2 & \sigma_1 \end{vmatrix} = (\sigma_1)^3 + 3.\sigma_3 - 3.\sigma_1.\sigma_2 = \Big(\sum_k a_k\Big)^3 - 3.\Big(\sum_{i,j} a_i.a_j\Big).\Big(\sum_k a_k\Big) + 3.\sum_{i,j,k} a_i.a_j.a_k$$

Or, la somme $\Big(\sum a_k\Big)^3$ contient • la somme des cubes
• la somme des termes an $(a_i)^2.a_j$ (avec facteur 3 venant de $\frac{3!}{2!.1!}$)
• la somme des termes an $a_i.a_j.a_k$ (avec facteur 6 venant de $\frac{6!}{1!.1!.1!}$)

Le terme $\Big(\sum_{i,j} a_i.a_j\Big).\Big(\sum_k a_k\Big)$ contient • la somme des $a_i.aj.a_k$
• mais aussi la somme des $(a_i)^2.a_k$ pour $i = k$ et celle des $a_i.(a_j)^2$

Bref, après simplifications, il ne reste que

$$\begin{vmatrix} \sigma_1 & 1 & 0 \\ 2.\sigma_2 & \sigma_1 & 1 \\ 3.\sigma_3 & \sigma_2 & \sigma_1 \end{vmatrix} = \sum_k (a_k)^3 = S_3$$

Pour ceux qui le souhaitent : $(a+b+c)^3 = a^3+b^3+c^3+3.(a^2.b+a^2.c+b^2.a+b^2.c+c^2.a+c^2.b)+6.(a.b.c)$
$3.(a+b+c).(a.b+a.c+b.c) = 3.(a^2.b+a^2.c+b^2.a+b^2.c+c^2.a+c^2.b)+9.(a.b.c)$

Un calcul courageux donne $\begin{vmatrix} \sigma_1 & 1 & 0 & 0 \\ 2.\sigma_2 & \sigma_1 & 1 & 0 \\ 3.\sigma_3 & \sigma_2 & \sigma_1 & 1 \\ 4.\sigma_4 & \sigma_3 & \sigma_2 & \sigma_1 \end{vmatrix} = \sum_k (a_k)^4 = S_4$.

Et si on ose, le dernier déterminant donne S_5(somme des puissnces cnquièmes).

De même

$$\begin{vmatrix} S_1 & 1 \\ S_2 & S_1 \end{vmatrix} = \Big(\sum_k a_k\Big)^2 - \sum_k (a_k)^2 = 2.\sigma_2$$

(toujours la somme des carrés et le carré de la somme)

puis

$$\begin{vmatrix} S_1 & 1 & 0 \\ S_2 & S_1 & 2 \\ S_3 & S_2 & S_1 \end{vmatrix} = \Big(\sum_k a_k\Big)^3 - 3.\Big(\sum_k a_k\Big).\Big(\sum_i (a_i)^2\Big) + 2.\Big(\sum_i (a_i)^3\Big) = 6.\sigma_3$$

Là encore, en version rapide dans $(a+b+c)^3 - 3.(a+b+c).(a^2+b^2+c^2) + 2.(a^3+b^3+c^3)$
les a^3 *sont au nombre de* $1-3+2$*, ils s'en vont*
les $a^2.b$ *sont au nombre de* $3-3$*, ils s'en vont*
les $a.b.c$ *sont au nombre de* 6 *et c'est tout*

Je vous laisse imaginer la suite.

Et vous me laissez trouver un joli devoir pour expliquer ces formules.