Exercice 1. [IMT MP/MPI 2024]
Soit $S : t \mapsto \sum_{n=0}^{+\infty} \frac{n^2+n+1}{n!} t^n$.

1. Déterminer le rayon de convergence R de cette série entière.
2. Calculer $S(t)$ sur $]-R, R[$.

Soit X une variable aléatoire à valeurs dans $\mathbb{N}$ telle que pour tout $t \in [-1,1]$, $G_X(t) = \lambda S(t)$, où $\lambda \in \mathbb{R}$.

3. Que vaut λ.
4. Calculer $\mathrm{P}(X = n)$ pour $n \in \mathbb{N}$.
5. Calculer $\mathrm{E}(X)$.

Solution :

1. *D'Alembert :* $R = +\infty$.
2. *Calcul avec réindiçage et séries exponentielles :* $S(t) = (t+1)^2 e^t$.
3. $1 = G_x(1) = \lambda S(1) = \lambda 4e$ *donc* $\lambda = \frac{1}{4e}$.
4. $G_X(t) = \sum_{n=0}^{+\infty} \mathrm{P}(X = n) t^n$, *par unicité des coefficients d'une série entière :* $\forall\, n \in \mathbb{N}$, $\mathrm{P}(X = n) = \frac{n^2+n+1}{4en!}$.
5. *Par dérivation de série entière et propriété de la fonction génératrice :*

$$\mathrm{E}(X) = G_X'(1) = \frac{1}{4e} S'(1) = \frac{1}{4e}\left(2(1+1) + (1+1)^2\right) e^1 = 2$$

Exercice 2. [IMT MP/MPI 2024]
Soient $f \in \mathscr{L}(\mathbb{R}^2, \mathbb{R}^3)$ et $g \in \mathscr{L}(\mathbb{R}^3, \mathbb{R}^2)$ telles que $\mathrm{rg}(f \circ g) = 2$. Calculer $\mathrm{rg}\, f$ et $\mathrm{rg}\, g$.

Solution :
$\mathrm{Im}(f \circ g) \subset \mathrm{Im}(f)$ *donc* $\mathrm{rg}(f) \geqslant \mathrm{rg}(f \circ g) = 2$ *et comme d'après le théorème du rang,* $\mathrm{rg}(f) = \dim(\mathbb{R}^2) - \dim(\mathrm{Ker}(f)) \leqslant 2$. *Ainsi* $\mathrm{rg}(f) = 2$.
Par théorème du rang on a aussi $\dim(\mathrm{Ker}(f \circ g)) = \dim(\mathbb{R}^3) - \mathrm{rg}(f \circ g) = 1$, *donc comme* $\mathrm{Ker}(g) \subset \mathrm{Ker}(f \circ g)$, $\dim(\mathrm{Ker}(g)) \leqslant 1$, *et g n'étant pas injective (son image étant de dimension strictement plus petite que la dimension de son espace de départ),* $\dim(\mathrm{Ker}(g)) = 1$, *donc* $\mathrm{rg}(g) = 2$.

Exercice 3. [Centrale Maths 2]
Soit p un nombre premier. On note

$$E_p = \left\{ n \in \mathbb{N} \,\middle|\, \forall (u,v) \in \mathbb{Z}^2, p \mid u^n + v^n \Longrightarrow (p \mid u \text{ ET } p \mid v) \right\}$$

1. Expliquer pourquoi l'on peut se restreindre à $(u,v) \in [\![0, p-1]\!]^2$ dans la définition de E_p.
2. En déduire une fonction Python de paramètres un nombre premier p et un entier naturel n renvoyant `True` si $n \in E_p$ et `False` sinon.
3. On note v_p la valuation 2-adique de $p-1$. Écrire une fonction Python de paramètre un nombre premier p calculant 2^{v_p}.
4. Déterminer à l'aide des fonctions précédentes 2^{v_p} et $E_p \cap [\![0,100]\!]$ pour tous les nombres premiers p inférieurs à 50. Que peut-on conjecturer ?
5. Déterminer E_2.

À partir de maintenant, on suppose $p \neq 2$. On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$.
On considère, pour $n \in \mathbb{N}$, l'application $\varphi_n : x \in \mathbb{F}_p \mapsto x^n$.

6. Montrer que : $\forall\, n \in \mathbb{N},\ n \in E_p \iff -1 \notin \mathrm{Im}(\varphi_n)$.
7. Montrer que $2^{v_p} \in E_p$.
8. On admet que le groupe multiplicatif $\mathbb{F}_p^*$ est cyclique. Montrer que $2^{v_p - 1} \notin E_p$.
9. Justifier la conjecture faite à la question 4 .

Solution :

1. *On effectue les divisions euclidienne de u et v : il existe $q_u, q_v, r_u, r_v \in \mathbb{Z}$ tels que $r_u, r_v \in [\![0, p-1]\!]$ et $u = q_u p + r_u$ et $v = q_v p + r_v$, si bien que*

$$\forall\, n \in \mathbb{N},\ u^n + v^n \equiv r_u^n + r_v^n \,[p] \quad \text{et} \quad u \equiv r_u \,[p] \text{ et } v \equiv r_v \,[p]$$

   Ainsi : $p \mid u^n + v^n$ si et seulement si $p \mid r_u^n + r_v^n$, et : $p \mid u$ et $p \mid v$ si et seulement si $p \mid r_u$ et $p \mid r_v$.
   On peut se ramener $(u,v) \in [\![0, p-1]\!]$.
2. *Un programme possible :*

```
def est_dans_Ep(p,n) :
    for u in range(p) :
        for v in range(p) :
            if (u**n+v**n)%p==0 and not (u%p==0 and v%p==0) :
                return False # un test au moins échoue
    return True # aucun test n'a échoué
```

3. *Un programme possible :*

```
def v(p) :
    a,puiss=p-1,1
    while a%2==0 :
    # on <<extrait>> toutes les puissances de 2
        puiss*=2
        a//=2
    return puiss
```

4. *Un programme possible :*

```
# génaration des premiers <50 :
liste_prem=[2]
for k in range(3,50) :
    test=True
    for p in liste_prem :
        if k%p==0 :
            test=False
    if test :
        liste_prem.append(k)

# fonction pour obtenir E_p inter [[0,100]]
def E(p) :
    res=[]
    for n in range(101) :
        if est_dans_Ep(p,n) :
            res.append(n)
    return(res)

# affichage demandé :
for p in liste_prem :
    print(v(p),E(p))
```

Il renvoie :

1 []

2 [0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100]

4 [0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100]

2 [0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100]

2 [0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100]

4 [0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100]

16 [0, 16, 32, 48, 64, 80, 96]

2 [0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100]

2 [0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100]

4 [0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100]

2 [0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100]

4 [0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100]

8 [0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96]

2 [0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100]

2 [0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100]

On conjecture : $E_2 = \varnothing$ et pour tout p premier impair, $E_p = 2^{v_p}\mathbb{N}$.

5. *Pour tout $n \in \mathbb{N}$, $1^n + 1^n \equiv 0\,[2]$ mais $2 \not| 1$, donc $E_2 = \varnothing$.*

6. *Il faut comprendre qu'il est équivalent de travailler dans $\mathbb{F}_p$ et de travailler avec des entiers $u, v \in [\![0, p-1]\!]$. De plus, si $x \in \mathbb{Z}$, alors $p \mid x \iff x = 0$ dans $\mathbb{F}_p$ (en confondant x et sa classe modulo p).*

   Soit $n \in \mathbb{N}$.

   - *On suppose que $n \in E_p$. Supposons par l'absurde que $-1 \in \mathrm{Im}(\varphi_n)$, alors il existe $v \in \mathbb{F}_p$ tel que $v^n = -1$.*

     En particulier $1^n + v^n = 0$ mais $1 \neq 0$ (tout ça dans $\mathbb{F}_p$), donc $n \notin E_p$: c'est absurde.

     Ainsi $-1 \notin \mathrm{Im}(\varphi_n)$.
   - *On suppose que $n \notin E_p$. Alors il existe $(u, v) \in \mathbb{F}_p$ non tous deux nuls tels que $u^n + v^n = 0$. Quitte à les échanger on suppose que $u \neq 0$, alors comme $\mathbb{F}_p$ est un corps, $u^{-1} \in \mathbb{F}_p$ et on a :*

     $$0 = (u^{-1})^n(u^n + v^n) = 1 + (u^{-1}v)^n$$

     donc $-1 = \varphi(u^{-1}v) \in \mathrm{Im}(\varphi_n)$.

7. *Supposons par l'absurde que $2^{v_p} \notin E_p$. Alors d'après la question précédente, $-1 \in \mathrm{Im}(\varphi_n)$ et on dispose de $x \in \mathbb{F}_p$ tel que $x^{2^{v_p}} = -1$.*

   Par définition de v_p, il existe m impair tel que $p - 1 = 2^{v_p}m$, si bien qu'en élevant l'égalité précédente à la puissance m il vient : $x^{2^{v_p}m} = (-1)^m = -1$. Mais $2^{v_p}m = p - 1$ et $2^{p-1} = 1$ (petit théorème de Fermat avec p premier et $2 \wedge p = 1$), donc $1 = -1$ dans $\mathbb{F}_p$, ce qui est impossible puisque $p \neq 2$.

   Ainsi $2^{v_p} \in E_p$.

8. *Soit g un générateur de $\mathbb{F}_p^*$ qui est de cardinal $p - 1$. En particulier, $(g^{\frac{p-1}{2}})^2 = 1$, donc dans le corps $\mathbb{F}_p$, $g^{\frac{p-1}{2}} = \pm 1$, mais ça ne peut être 1 sinon g n'engendre pas $\mathbb{F}_p^*$. On observe que $\dfrac{p-1}{2} = 2^{v_p - 1}m$ avec les notations des questions précédente, si bien que :*

   $$-1 = g^{\frac{p-1}{2}} = g^{2^{v_p-1}m} = (g^m)^{2^{v_p-1}} \in \mathrm{Im}(\varphi_{2^{v_p-1}}$$

   puis $2^{v_p-1} \geqslant 1$ lorsque $p \neq 2$. D'après 6. $2^{v_p-1} \notin E_p$.

9. *On peut montrer que si $n \in E_p$, alors pour tout $k \in \mathbb{N}$, $kn \in E_p$. En effet, pour tous $u, v \in \mathbb{F}_p$ tels que $u^{kn} + v^{kn} = 0$, on a $(u^k)^n + (v^k)^n = 0$, donc $u^k = 0$ et $v^k = 0$, donc puisque $\mathbb{F}_p$ est un corps, $u = v = 0$.*

   Ainsi comme $2^{v_p} \in E_p$, $2^{v_p}\mathbb{N} \in E_p$ (0 est toujours dans E_p pour $p \neq 2$).

   Supposons par l'absurde qu'il existe dans E_p un entier non multiple de 2^{v_p}, alors il s'écrit $n = 2^\alpha \beta$ où $\alpha < v_p$ et β est impair.

   Comme $2^{v_p-1} \notin E_p$, il existe $u, v \in \mathbb{F}_p$ non tous deux nuls tels que $u^{2^{v_p-1}} + v^{2^{v_p-1}} = 0$, donc $u^{2^{v_p-1}} = -v^{2^{v_p-1}}$. On pose $u' = u^{2^{v_p-1-\alpha}}$ et $v' = v^{2^{v_p-1-\alpha}}$ et on a : $(u')^{2^\alpha} = -(v')^{2^\alpha}$, et u' et v' non tous deux nuls. On élève à la puissance β impaire et il vient : $(u')^{2^\alpha\beta} = -(v')^{2^\alpha\beta}$, ou encore $(u')^n + (v')^n = 0$. Comme u' ou v' n'est pas nul, cela contredit $n \in E_p$, ce qui achève la preuve de la conjecture.

Exercice 4. [Centrale 1 MP/MPI 2024]
Soient $n \in \mathbb{N}^*$ et $p \in \{0,\dots,n\}$. On note R_p l'ensemble des matrices de $\mathcal{M}_n(\mathbb{C})$ de rang p.

1. Soient $M,N \in \mathcal{M}_n(\mathbb{C})$. Montrer que M et N sont de même rang si et seulement s'il existe P,Q dans $GL_n(\mathbb{C})$ telles que $M = PNQ$.
2. Soit F une partie finie de $\mathbb{C}$. Montrer que $C \setminus F$ est connexe par arcs.
   En déduire que R_p est connexe par arcs.
3. Déterminer l'adhérence et l'intérieur de R_p.

Solution :

1. *Cours de sup : choisir une base du noyau, la compléter une une base de $\mathbb{C}^n$, considérer l'image des vecteurs ajoutés par f et justifier qu'ils forment une base de l'image de f, la compléter en une base de $\mathbb{C}^n$: toute matrice de rang r est alors équivalente à la matrice $J_{n,r} = \begin{pmatrix} I_r & O_{r,n-r} \\ O_{n-r,r} & O_{n-r,n-r} \end{pmatrix}$. Par transitivité de la relation d'équivalence on a le résultat.*
2. (a) *Notons $F = \{a_1,\dots,a_r\}$ où $r \in \mathbb{N}$. Soient $x,y \in \mathbb{C}$ distincts. Il n'y a qu'un nombre fini de $z \in \mathbb{C}$ tels que $[x,z]$ ou $[y,z]$ contient l'un des a_i, donc on peut trouver $z \in \mathbb{C}$ tel que le chemin $x \to z \to y$ obtenu en se déplaçant le long des segments précédents ne rencontre aucun des éléments de F : c'est un chemin continu, donc $C \setminus F$ est connexe par arcs.*

   (b) *On en déduit déjà que $GL_n(\mathbb{C})$ est connexe par arcs : si $A,B \in GL_n(\mathbb{C})$, alors $t \in \mathbb{C} \mapsto \det((1-t)A+tB)$ est polynomiale, elle n'admet qu'un nombre fini de racines, et on peut appliquer la question précédente : on dispose d'un chemin continue γ tel que $(1-\gamma(t))A+\gamma(t)B$ est dans $GL_n(\mathbb{C})$.*

   On peut alors passer de toute matrice de R_p à $J_{n,r}$ par des chemin continue entre I_n et P et I_n et Q.
3. • *Adhérence.*

   L'ensemble des matrices de rang $\leqslant p$ est un fermé : c'est l'image réciproque de 0 par l'application continue qui à une matrice associe la liste de ses mineurs d'ordre $r+1$. En jouant avec des coefficients qui tendent vers 0 sur la diagonale, on peut obtenir toute matrice de rang $r \in \int 0p$ comme limite d'une famille de matrices de R_p. Donc L'adhérence de R_p est l'ensemble des matrices de rang $\leqslant p$.

   • *Intérieur.*

   Si $p = n$, $R_n = GL_n(\mathbb{C})$ qui est ouvert, il est son propre intérieur.

   Si $p < n$, alors l'intérieur est vide (sinon il contient une matrice A et les matrices de la forme $A+\varepsilon I_n$ pour ε suffisamment petit, et parmi elles des matrices inversibles).

Exercice 5. [Centrale maths 2 MP 2024]

Soit p un nombre premier impair. Un entier a est un carré modulo p s'il existe $m \in \mathbb{N}$ tel que $a \equiv m^2\,[p]$.

1. (a) Écrire une fonction Python qui teste si l'entier p est premier.

   (b) On s'intéresse aux nombres premiers de la forme $p = 12a + b$ avec $a < 1000$ et $b \in \{1,3,5,7,9,11\}$. À l'aide de Python, afficher les couples (p,b) pour lesquels 3 est carré modulo p. Que remarque-t-on ? On suppose ce résultat toujours vrai.

   (c) À l'aide de Python, afficher les entiers $n \in [\![1,9999]\!]$ tels que $2^n - 1$ divise $3^n - 1$.

Soit $n \geqslant 2$ tel que $2^n - 1$ divise $3^n - 1$.

2. Montrer que n est impair.

3. (a) Pour $x, y \in (\mathbb{Z}/p\mathbb{Z})^*$, on définit $x \sim y$ si et seulement si $x^2 = y^2$. Montrer que $\sim$ est une relation d'équivalence sur $(\mathbb{Z}/p\mathbb{Z})^*$. Déterminer le cardinal d'une classe d'équivalence et en déduire celui de l'ensemble $\left\{x^2 \,\middle|\, x \in (\mathbb{Z}/p\mathbb{Z})^*\right\}$.

   (b) Montrer que, si $a \in \mathbb{Z}$ est carré modulo p tel que $a \wedge p = 1$, alors $a^{\frac{p-1}{2}} \equiv 1\,[p]$.

   (c) En admettant que l'équation $x^{\frac{p-1}{2}} = 1$ admet au plus $\dfrac{p-1}{2}$ solutions dans $(\mathbb{Z}/p\mathbb{Z})^*$, déterminer le nombre exact de solutions de cette équation dans $(\mathbb{Z}/p\mathbb{Z})^*$.

   (d) Montrer que, pour $a \in \mathbb{Z}$ non multiple de p, $a^{\frac{p-1}{2}} \equiv 1\,[p]$ si a est carré modulo p et $a^{\frac{p-1}{2}} \equiv -1\,[p]$ sinon.

4. On suppose que p divise $2^n - 1$.

   (a) Montrer que 3 est un carré modulo p.

   (b) En admettant le résultat de 1.(b), démontrer la conjecture de 1.(c).

Solution :

1. (a) Un programme possible :

```
def est_premier(n) :
    if n==0 or n==1 :
        return False
    for d in range(2,n) :
    # on cherche les diviseurs autres que 1 et n
        if n%d==0 :
            return False
    return True
```

(b) Un programme possible :

```
res=[]
for a in range(1000) :
    for b in range(1,12,2) :
        p=12*a+b
        if est_premier(p) :
            test=False
            for m in range(p) :
                if (m**2-3)%p==0 :
                    test=True
            if test :
                res+=[[p,b]]
print(res)
```

Les couples (p,b) *pour lesquels* 3 *est un carré modulo* p *sont ceux pour lesquels* $b \in \{1,11\}$ *(*3 *étant à part puisque modulo* 3, 3 *est nul, c'est un carré modulo* 3*). Plus précisément on observe :* 3 *est carré modulo* p *si et seulement si* $p \equiv \pm 1\,[12]$.

(c) *Un programme possible :*

```
res=[]
for n in range(1,10000) :
    if (3**n-1)%(2**n-1)==0 :
        res+=[n]
print(res)
```

Seul 1 *convient.*

2. *Si* n *est pair, il s'écrit* $n=2m$ *où* $m \in \mathbb{N}^*$ *puis* $2^n-1=4^m-1=(4-1)\sum_{k=0}^{n-1} 4^k \equiv 0\,[3]$, *mais comme* $3 \not| 3^n-1$, 2^n-1 *ne peut pas diviser* 3^n-1.
Ainsi n *est impair.*

3. (a) *Vérification immédiate, la classe de* x *a exactement deux éléments* x *et* $-x$ *(distincts car* $p \neq 2$ *et pas d'autres car* $\mathbb{Z}/p\mathbb{Z}$ *est intègre). On obtient alors une partition de* $(\mathbb{Z}/p\mathbb{Z})^*$ *en ensembles de cardinal* 2 *: il y a donc* $\dfrac{p-1}{2}$ *carrés dans* $(\mathbb{Z}/p\mathbb{Z})^*$.

   (b) *Il existe* $m \in \mathbb{Z}/p\mathbb{Z}$ *tel que* $a=b^2$, *si bien que* $a^{\frac{p-1}{2}}=b^{p-1} \equiv 1\,[p]$ *d'après le théorème de Fermat puisque* $a \wedge p = 1$ *donc* $b^2 \wedge p = 1$ *donc* $b \wedge p = 1$.

   (c) *La question 3.(a) fournit* $\frac{p-1}{2}$ *solutions à cette équation, et comme il ne peut y en avoir d'autre, ce sont exactement les solutions.*

   (d) *Dans tous les cas, dans le corps* $\mathbb{Z}/p\mathbb{Z}$, *si* $a \neq 0$, *alors* $a^{p-1}=1$ *donc* $\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)=0$. *Les deux questions précédentes montrent que* a *est carré modulo* p *si et seulement si* $a^{\frac{p-1}{2}} \equiv 1\,[p]$, *et donc dans les autres cas,* $a^{\frac{p-1}{2}} \equiv -1\,[p]$.

4. (a) *Par transitivité* $p \mid 3^n-1$ *donc* $3^n \equiv 1\,[p]$. *Par ailleurs* n *est impair, donc* $3^{n+1}=(3^{\frac{n+1}{2}})^2 \equiv 3\,[p]$. 3 *est bien un carré modulo* p.

   (b) *Sachant que* n *est impair, si* $n \geqslant 3$, *alors* 2^n-8 *est divisible par* 8 *mais aussi par* 3 *(calcul modulo 3 en exploitant l'imparité de* n*), donc* $2^n \equiv 8\,[24]$ *donc aussi modulo 12 : on a montré que* $2^n-1 \equiv 7\,[12]$.

Mais d'après ce qui précède, tous les facteurs premiers de 2^n-1 *sont* ± 1 *modulo* 12*, donc* 2^n-1 *est* ± 1 *modulo* 12 *: c'est absurde.*

Ainsi seul $n=1$ *convient (il convient bien).*