Croissance stricte du nombre de points fixes de l'automorphisme intérieur f_n aux doubles de nombres premiers, fatalement
Denise Vella-Chemla pilotant l'ia claude, juillet 2026

Remarque : cette note démontre une observation formulée dans *"Qui utilise des automorphismes intérieurs sans en avoir conscience"* (début novembre 2024)

https://denisevellachemla.eu/automorphismes-interieurs.pdf :

le nombre de points fixes de l'automorphisme f_n (calculé par le programme en annexe, C'est malheureusement dans la ligne marquée de $*****$ que j'ai introduit la circularité fatale.) croît strictement, au sein de la sous-suite des $n \equiv 2 \pmod 4$, exactement aux valeurs n qui sont le double d'un nombre premier. Toutes les formules ci-dessous ont été vérifiées numériquement contre la sortie du programme pour $n = 6, \ldots, 102$ avant rédaction de la preuve.

1. Rappel des définitions

Pour n pair, $n \geq 6$, on note $N = \{6, 8, \ldots, n\}$ l'ensemble des pairs déjà traités par la boucle principale du programme au moment où l'on atteint n. Le programme construit, de façon *cumulative* (la liste `decompositions` n'est jamais réinitialisée), un ensemble

$$D_n = \Big\{ (a,\, n' - a) \ : \ n' \in N,\ a \text{ premier impair},\ 3 \leq a \leq n'/2 \Big\}.$$

L'automorphisme intérieur appliqué au pas n est $\text{autom}(n, d) = (d_1, n - d_2)$ pour $d = (d_1, d_2)$. Un élément $d \in D_n$ est un *point fixe* de $\text{autom}(n, \cdot)$ si et seulement si $d_1 = d_1$ (toujours vrai) et $d_2 = n - d_2$, c'est-à-dire

$$d_2 = \frac{n}{2}.$$

On note $F(n) = \Big|\{ d \in D_n : d_2 = n/2 \}\Big|$ le nombre de points fixes calculé par le programme (variable `nbptsfixesautom`).

Remarque [Correction mineure de la note de 2024] : la note de 2024 annonce $F(n) = \pi(n/2)$ pour n de la forme $4k + 2$, où π est la fonction de comptage usuelle des nombres premiers (comptant 2). Le théorème 2 ci-dessous montre que la formule exacte est $\pi(n/2) - 1$ (on ne compte que les nombres premiers *impairs* $\leq n/2$, 2 étant structurellement exclu). Par exemple pour $n = 22$: $\pi(11) = 5$ (les premiers $2, 3, 5, 7, 11$), mais l'annexe du document de 2024 donne bien 4 points fixes pour f_{22}, pas 5. La formule correcte, vérifiée sur les 49 valeurs $n = 6, \ldots, 102$, est $\pi(n/2) - 1$.

2. Formule fermée pour $F(n)$

Lemme 1. *Soit n pair, $n \geq 6$, et $m = n/2$. Alors*

$$F(n) = \Big|\{ a \text{ premier impair} \ : \ 3 \leq a \leq m,\ \ m + a \text{ pair}\}\Big|.$$

Démonstration. Par définition, $F(n)$ compte les couples (a, n') avec $n' \in N$, a premier impair, $3 \leq a \leq n'/2$, et $n' - a = m$. La dernière condition donne $n' = m + a$, ce qui détermine n' de façon unique à partir de a. Il reste à traduire les contraintes portant sur n' en contraintes portant sur a :

- $a \leq n'/2 = (m+a)/2 \iff 2a \leq m+a \iff a \leq m$.
- $n' \geq 6$: comme $m \geq 3$ (car $n \geq 6$) et $a \geq 3$, on a $n' = m + a \geq 6$ automatiquement.
- $n' \leq n = 2m$: équivaut à $a \leq m$, déjà obtenu.
- $n' \in N$ signifie de plus que n' est pair (c'est la seule condition non encore traduite), soit $m+a$ pair.

Chaque a premier impair vérifiant $3 \leq a \leq m$ et $m + a$ pair fournit donc exactement un couple (a, n') valide, et réciproquement. D'où la formule. □

Théorème 2. *Soit n pair, $n \geq 6$, et $m = n/2$.*

1. *Si $n \equiv 0 \pmod 4$ (c'est-à-dire m pair), alors $F(n) = 0$.*
2. *Si $n \equiv 2 \pmod 4$ (c'est-à-dire m impair), alors*

$$F(n) = \Big|\{\, p \text{ premier } : \ p \text{ impair}, \ p \leq m \,\}\Big| = \pi(m) - 1.$$

Démonstration. Dans la formule du Lemme 1, a est toujours impair (c'est une contrainte de construction : seuls des a impairs entrent dans D_n). La condition "$m + a$ pair" équivaut donc à "m impair", puisque la somme de deux entiers est paire si et seulement si ils ont même parité, et a est ici toujours impair.

Cas 1 : m pair. Alors $m + a$ est impair pour tout a impair, donc aucun a ne satisfait la condition du Lemme 1, et $F(n) = 0$.

Cas 2 : m impair. Alors $m + a$ est pair pour tout a impair, donc la condition de parité est automatiquement satisfaite, et $F(n)$ compte simplement les premiers impairs a avec $3 \leq a \leq m$. Comme 2 est le seul nombre premier pair, ce compte vaut exactement $\pi(m) - 1$ (on retire 2 du compte usuel $\pi(m)$), pour $m \geq 2$. □

3. Croissance stricte aux doubles de nombres premiers

On restreint maintenant l'attention à la sous-suite $(n_k)_{k \geq 1}$ des entiers $n_k = 4k + 2$ ($n_1 = 6, n_2 = 10, n_3 = 14, \dots$), seule sous-suite sur laquelle F n'est pas identiquement nulle.

Remarque : sur la suite complète des pairs $n = 6, 8, 10, 12, \dots$ (pas de 2), F n'est **pas** monotone : elle alterne entre une valeur croissante (aux $n \equiv 2 \pmod 4$) et 0 (aux $n \equiv 0 \pmod 4$), comme le montre l'annexe du document de 2024 $(1, 0, 2, 0, 3, 0, 3, 0, \dots)$. L'énoncé de croissance stricte n'a donc de sens que restreint à la sous-suite (n_k) des $n \equiv 2 \pmod 4$, et c'est ce que l'on démontre ci-dessous.

Corollaire 3. *Pour tout $k \geq 2$,*

$$F(n_k) > F(n_{k-1}) \iff n_k \text{ est le double d'un nombre premier.}$$

De plus $F(n_k) \geq F(n_{k-1})$ toujours (la sous-suite est faiblement croissante), et lorsque l'inégalité est stricte, elle l'est exactement de 1.

Démonstration. Posons $m_k = n_k/2 = 2k+1$, de sorte que m_k est impair et $m_{k+1} = m_k + 2$ (l'écart entre deux termes consécutifs de la sous-suite, ramené à m, est toujours 2). D'après le théorème 2 (cas m impair) :

$$F(n_k) = \Big|\{\, p \text{ premier impair} : p \leq m_k \,\}\Big|.$$

En passant de m_{k-1} à $m_k = m_{k-1} + 2$, un seul entier impair nouveau entre dans l'intervalle de comptage, à savoir m_k lui-même (l'entier $m_{k-1} + 1$, pair, ne peut jamais être premier impair et n'est de toute façon pas compté). Donc :

$$F(n_k) - F(n_{k-1}) = \begin{cases} 1 & \text{si } m_k \text{ est premier} \\ 0 & \text{sinon.} \end{cases}$$

En particulier $F(n_k) \geq F(n_{k-1})$, avec égalité stricte de 1 exactement quand m_k est premier. Or $n_k = 2m_k$: dire que m_k est premier revient exactement à dire que n_k est le double d'un nombre premier. D'où le résultat. □

4. Portée et limites du résultat

Le résultat ci-dessus est maintenant complètement démontré, et confirme précisément l'observation de la note de 2024, à la correction près de la formule ($\pi(m) - 1$ et non $\pi(m)$). Il faut cependant en mesurer la portée exacte :

Remarque : la croissance stricte de F aux doubles de nombres premiers n'est, une fois la formule fermée du théorème 2 établie, qu'une reformulation directe du fait que la fonction de comptage des nombres premiers impairs augmente de 1 exactement aux nombres premiers - ce qui est vrai par construction même de cette fonction. Ce n'est pas un fait profond sur les nombres premiers ; c'est une conséquence mécanique de la définition de $F(n)$ comme comptage de premiers dans un intervalle croissant.

Remarque [Sur l'analogie avec la preuve en une page de Zagier que tout nombre premier de la forme $4k+1$ est somme de deux nombres premiers, preuve qui utilise l'existence d'un point fixe en définissant une involution sur un ensemble de cardinal impair] : la note de 2024 suggère que cette construction pourrait mener à une preuve qui ressemblerait à celle de Zagier" de l'existence d'une décomposition de Goldbach pour tout n pair. Il faut noter une différence structurelle importante avec l'involution de Zagier : dans la preuve de Zagier, l'involution agit sur l'ensemble des triplets (x, y, z) solutions de $x^2 + 4yz = p$ pour p premier *donné* - la primalité de p est l'hypothèse de départ, et l'existence d'un point fixe de l'involution (établie par un argument de parité) démontre une propriété *supplémentaire* de p (être somme de deux carrés). Ici, à l'inverse, l'ensemble D_n sur lequel agit f_n est construit en supposant déjà que a est premier (c'est la condition de construction de D_n, pas une conclusion de l'argument). L'automorphisme f_n et ses points fixes ne disent donc rien sur l'existence d'une décomposition de Goldbach de n : ils comptent, parmi les décompositions *déjà connues* comme ayant un premier en première coordonnée, celles qui sont symétriques par rapport à $n/2$. La primalité, qui est la difficulté centrale de la conjecture de Goldbach, est ici une hypothèse d'entrée de D_n, non une conclusion de l'argument sur les points fixes. En l'état, cette piste ne rapproche donc pas d'une preuve de la conjecture de Goldbach ; elle donne un résultat correct et maintenant démontré, mais sur un objet auxiliaire ($F(n)$) dont le comportement encode directement π, sans rien ajouter sur la question ouverte de l'existence des décompositions elles-mêmes.

Annexe : programme de calcul des points fixes

```
def premier(atester):
    if atester in [0, 1]: return False
    if atester in [2, 3, 5, 7]: return True
    k = 2
    while True:
        if k * k > atester: return True
        else:
            if atester % k == 0: return False
            else: k = k + 1

def autom(n,d):
    return([d[0],n-d[1]])

decompositions = []
for n in range(6,104,2):
    print('',n,'::::',end='')
    for x in range(3,n//2+1,2):
        if premier(x):      %*********************
            decompositions.append([x,n-x])
    for y in range(3,n-1,2):
        nbdecompo = 0
        for d in decompositions:
            if d[1] == y:
                nbdecompo = nbdecompo+1
        print(nbdecompo,'  ',end='')
    print('')
    print('application de l automorphisme f-' ,n)
    nbptsfixesautom = 0
    for d in decompositions:
        if d[0] == autom(n,d)[0] and d[1] == autom(n,d)[1]:
            nbptsfixesautom = nbptsfixesautom+1
    print('nb pts fixes de l automorphisme : ',nbptsfixesautom)
```