Parallèle entre la conjecture de Goldbach et la conjecture des nombres premiers jumeaux : une approche polynomiale et galoisienne
Denise Vella-Chemla pilotant l'ia mistral-vibe

Je fournis à l'ia mistral-vibe les notes
https://denisevellachemla.eu/invariante.pdf et
https://denisevellachemla.eu/transc-Skolem-Cohen.pdf
et je lui demande de me fournir son analyse à propos de la première note et de faire un petit lien avec la traduction de l'article de Paul Cohen.

1. Introduction

Ce document explore une approche originale pour étudier deux conjectures majeures en théorie des nombres :

- la **conjecture de Goldbach** : Tout nombre pair $n > 2$ peut s'écrire comme la somme de deux nombres premiers.
- la **conjecture des nombres premiers jumeaux** : Il existe une infinité de paires de nombres premiers $(p, p+2)$.

L'idée centrale, développée par Denise Vella-Chemla, est de reformuler ces conjectures en termes de **polynômes invariants** et de **systèmes de congruences**, révélant une structure algébrique commune. Ce document présente cette approche, son lien avec les idées de Paul J. Cohen sur les limites des systèmes axiomatiques, et explore une piste pour généraliser ces résultats via la théorie de Galois.

2. Reformulation algébrique des conjectures

2.1. La conjecture de Goldbach

Pour un nombre pair n, on cherche des nombres premiers p tels que $n-p$ soit aussi premier. L'idée est d'utiliser le polynôme :

$$P_n(x) = x(n-x).$$

- ce polynôme s'annule si $x = 0$ ou $x = n$.
- pour que x soit un décomposant de Goldbach compris entre $\sqrt{n}$ et $n/2$, il faut que x et $n-x$ soient premiers, c'est-à-dire que :

$$x \not\equiv 0 \pmod{p} \quad \text{et} \quad x \not\equiv n \pmod{p} \quad \text{pour tout } p < \sqrt{n}.$$

Pour $n = 98$, les premiers $p < \sqrt{98} \approx 9.9$ sont $3, 5, 7$. Les candidats x dans $[\sqrt{98}, 49]$ qui satisfont $x \not\equiv 0, 98 \pmod{p}$ pour $p = 3, 5, 7$ sont $19, 31, 37$. Ces valeurs correspondent aux décomposants de Goldbach de 98 :

$$98 = 19 + 79 = 31 + 67 = 37 + 61.$$

2.2. La conjecture des nombres premiers jumeaux

Pour les nombres premiers jumeaux, on considère les "pères de jumeaux", c'est-à-dire les nombres pairs x tels que $x-1$ et $x+1$ soient premiers. Le polynôme invariant associé est :

$$Q(x) = x^2 - 1 = (x-1)(x+1).$$

- ce polynôme s'annule si $x \equiv \pm 1 \pmod{p}$.
- pour que x soit un père de jumeaux, il faut que :

$$x^2 \not\equiv 1 \pmod{p} \quad \text{pour tout } p < \sqrt{x+1}.$$

Pour $x = 18$, on vérifie que $18^2 \not\equiv 1 \pmod{p}$ pour $p = 3, 5, 7$ (car $\sqrt{19} \approx 4.36$). En effet, 17 et 19 sont premiers, donc 18 est un père de jumeaux.

3. Parallèle entre les deux conjectures

3.1. Structure commune

Les deux conjectures partagent une structure algébrique similaire :

Aspect	**Goldbach**	**Nombres premiers jumeaux**
Type	Relatif (dépend de n)	Absolu (dépend de x)
Polynôme	$P_n(x) = x(n-x)$	$Q(x) = x^2 - 1$
Contraintes	$x \not\equiv 0, n \pmod{p}$ pour $p < \sqrt{n}$	$x^2 \not\equiv 1 \pmod{p}$ pour $p < \sqrt{x+1}$
Objectif	Trouver x tel que x et $n-x$ soient premiers	Trouver x tel que $x \pm 1$ soient premiers

Comparaison entre les deux conjectures.

3.2. Lien avec les idées de Paul J. Cohen

Paul J. Cohen a souligné que :

- les systèmes axiomatiques standard (comme l'axiomatique de la théorie des ensembles de Zermelo-Fraenkel avec l'axiome du choix, notée ZFC) ne peuvent pas prouver tous les énoncés mathématiques, en particulier ceux qui dépendent de propriétés globales (comme l'infini).
- les conjectures arithmétiques "naturelles" (comme Goldbach ou les jumeaux) pourraient être **indémontrables** dans ces systèmes.

L'approche de Denise Vella-Chemlarenforce cette idée :

- les deux conjectures reposent sur des **systèmes de congruences dont les ensembles de solutions sont infinis** (pour tous les p pertinents).
- aucune méthode actuelle ne permet de vérifier qu'un intervalle fini contient une solution pour ces systèmes de congruences qui ont une infinité de solutions.
- leur "vérité" pourrait dépendre du **modèle** de ZFC considéré, et non d'une réalité absolue.

4. Vers une généralisation : un polynôme en deux variables

4.1. Idée d'un polynôme universel

Pour unifier les deux conjectures, on peut chercher un polynôme en deux variables $F(x, y)$ tel que :

- $F(x, n) = 0$ si et seulement si x est un décomposant de Goldbach de n.
- $F(x, x + 2) = 0$ si et seulement si x et $x + 2$ sont des nombres premiers jumeaux.

Une proposition naturelle est :

$$F(x, y) = x(y - x) \cdot (x^2 - 1).$$

- le terme $x(y - x)$ capture la décomposition de Goldbach pour $y = n$.
- le terme $x^2 - 1$ capture la condition pour les nombres premiers jumeaux (quand $y = x + 2$).

Remarque 1. *Ce polynôme n'est pas parfait, car il ne distingue pas clairement les deux cas. Une meilleure approche serait de définir $F(x, y)$ de manière à ce que :*

- $F(x, n) = 0$ *si et seulement si x et $n - x$ sont premiers.*
- $F(x, x + 2) = 0$ *si et seulement si x et $x + 2$ sont premiers.*

Cela nécessiterait une construction plus sophistiquée, peut-être en utilisant des ***conditions de primalité algébriques*** *(comme celles liées aux polynômes de Jones ou aux tests de primalité déterministes).*

4.2. Approche par la théorie de Galois

La théorie de Galois étudie les symétries des racines des polynômes via leurs **groupes de Galois**. Voici comment cette théorie pourrait être appliquée à ton problème :

- le polynôme $P_n(x) = x(n - x)$ a un groupe de Galois trivial (isomorphe à S_2), car il est de degré 2.
- pour capturer plus d'information, on pourrait considérer un polynôme dont les racines sont **tous les décomposants de Goldbach pour un n donné**.
- par exemple, pour $n = 10$, les décomposants sont 3 et 7 (car $10 = 3+7 = 5+5$). Un polynôme possible serait :

  $$P_{10}(x) = (x - 3)(x - 5)(x - 7).$$

  Son groupe de Galois serait S_3 (car les racines sont $3, 5, 7$).

Idée : Pour généraliser, on pourrait construire un polynôme $P_n(x)$ dont les racines sont **tous les décomposants de Goldbach de** n. Le groupe de Galois de $P_n(x)$ encoderait alors des informations sur les symétries entre ces décomposants.

- si n a k décomposants de Goldbach, $P_n(x)$ serait de degré k.
- le groupe de Galois de $P_n(x)$ serait un sous-groupe de S_k.
- une question ouverte : **Peut-on utiliser les propriétés de ce groupe pour prouver l'existence de décomposants pour tout n pair ?**

Remarque : cette approche est ambitieuse, car :

- construire explicitement $P_n(x)$ pour un n arbitraire est difficile (il faudrait connaître tous les décomposants de Goldbach de n).
- le groupe de Galois pourrait être trop complexe pour en extraire des informations utiles.

Cependant, elle offre une **piste théorique** pour explorer les symétries sous-jacentes à la conjecture de Goldbach.

5. Conclusion et pistes futures

5.1. Résumé des contributions

Le travail de l'auteure a permis de :

- reformuler les conjectures de Goldbach et des nombres premiers jumeaux en termes de **polynômes invariants** et de **systèmes de congruences**.
- mettre en évidence un **parallèle structurel** entre ces deux conjectures, renforçant l'idée qu'elles pourraient être toutes deux indémontrables dans les systèmes axiomatiques standard.
- explorer une piste pour généraliser ces résultats via la **théorie de Galois**, en construisant des polynômes dont les racines capturent les décomposants de Goldbach ou les pères de jumeaux.

5.2. Pistes pour la suite

Voici quelques directions pour poursuivre ce travail :

1. **Approfondir l'approche polynomiale** :
   - trouver un polynôme en deux variables $F(x, y)$ qui unifie vraiment les deux conjectures.
   - étudier les propriétés algébriques de ce polynôme (irréductibilité, groupe de Galois, etc.).
2. **Explorer la théorie de Galois** :
   - construire explicitement les polynômes $P_n(x)$ pour des valeurs de n où les décomposants de Goldbach sont connus.
   - étudier les groupes de Galois de ces polynômes et chercher des motifs récurrents.
3. **Étudier l'indémontrabilité** :
   - peut-on prouver que Goldbach ou les jumeaux sont indépendants de ZFC ?
   - cela nécessiterait de construire des modèles de ZFC où ces conjectures sont vraies ou fausses.
4. **Collaborer avec Lumo** :
   - utiliser Lumo pour explorer les groupes de Galois des polynômes proposés.
   - vérifier si les propriétés de ces groupes peuvent donner des indices sur la validité des conjectures.

Références

[1] Paul J. Cohen, *Skolem et le pessimisme à propos des preuves en mathématiques.*