

Obstruction au problème de la parité pour la conjecture binaire de Goldbach avec limitation de l'erreur

Posté sur le blog Wordpress de Terence Tao : 9 juillet 2014

Tags : conjecture de Goldbach, problème de la parité, théorie du crible

Deux des problèmes ouverts les plus célèbres de la théorie additive des nombres premiers sont la conjecture des nombres premiers jumeaux et la conjecture de Goldbach binaire. Leurs formulations sont assez similaires :

- **Conjecture des nombres premiers jumeaux** : L'équation $p_1 - p_2 = 2$ admet une infinité de solutions avec p_1, p_2 premiers.
- **Conjecture de Goldbach binaire** : L'équation $p_1 + p_2 = N$ admet au moins une solution avec p_1, p_2 premiers pour tout $N \geq 4$ pair donné.

Compte tenu de cette similarité, il n'est pas surprenant que les progrès partiels réalisés sur ces deux conjectures aient suivi une évolution assez similaire. La conjecture des nombres premiers jumeaux est généralement considérée comme légèrement plus simple que la conjecture de Goldbach binaire, mais, de manière générale, tout progrès réalisé sur l'une des conjectures a également conduit à des progrès comparables sur l'autre. (Par exemple, le théorème de Chen admet une version pour la conjecture des nombres premiers jumeaux et une autre pour la conjecture de Goldbach binaire.) De plus, la fameuse obstruction de parité est présente dans les deux problèmes, empêchant la résolution de l'une ou l'autre conjecture par la quasi-totalité des méthodes connues (voir cet article de blog précédent <https://terrytao.wordpress.com/2007/06/05/open-question-the-parity-problem-in-sieve-theory/> pour plus de détails).

Dans cet article, je souhaite souligner une divergence par rapport à ce principe général, concernant les versions à erreur bornée de ces deux conjectures :

- **Conjecture de Goldbach binaire à erreur bornée** : L'inégalité $0 < p_1 - p_2 < H$ admet une infinité de solutions avec p_1, p_2 premiers pour une certaine constante absolue H .
- **Conjecture de Goldbach binaire à erreur bornée** : L'inégalité $N \leq p_1 + p_2 \leq N + H$ admet au moins une solution avec p_1, p_2 premiers pour tout N suffisamment grand et une certaine constante absolue H .

La première de ces affirmations est désormais un théorème bien connu de Zhang, et le projet Polymath8b, hébergé sur ce blog, a réussi à abaisser H à $H = 246$ inconditionnellement, et à $H = 6$ en supposant la conjecture d'Elliott-Halberstam généralisée (GEH). Cependant, la seconde affirmation reste ouverte ; le meilleur résultat que le projet Polymath8b ait pu obtenir dans ce sens est que (en supposant GEH) au moins l'une des conjectures de Goldbach binaires avec erreur bornée, ou la conjecture des nombres premiers jumeaux sans erreur, devait être vraie.

Toutes les démonstrations connues du théorème de Zhang procèdent par des moyens de théorie du crible. Fondamentalement, elles prennent comme entrée des résultats d'équirépartition qui

Transcription / traduction de ce post de blog post Terence tao 2014 en L^AT_EX : Denise Vella-Chemla (assistance outils automatiques), mars 2026.

contrôlent la taille des écarts tels que

$$\Delta(f; a(q)) := \sum_{\substack{x \leq n \leq 2x \\ n \equiv a \pmod{q}}} f(n) - \frac{1}{\phi(q)} \sum_{x \leq n \leq 2x} f(n) \quad (1)$$

pour diverses classes de congruence $a \pmod{q}$ et diverses fonctions arithmétiques f , par exemple $f(n) = \Lambda(n + h_1)$ (ou plus généralement $f(n) = \alpha \beta(n + h_i)$ pour diverses valeurs de α, β). Après avoir soigneusement sélectionné des combinaisons linéaires de ces écarts, et en utilisant la borne inférieure de positivité triviale :

$$a_n \geq 0 \text{ pour tout } n \implies \sum_n a_n \geq 0, \quad (2)$$

on obtient finalement (pour H convenable) une borne inférieure non triviale de la forme :

$$\sum_{x \leq n \leq 2x} \nu(n) 1_A(n) > 0,$$

où ν est une fonction de pondération, et A est l'ensemble des n tels qu'il existe au moins deux nombres premiers dans l'intervalle $[n, n + H]$. Cela implique au moins une solution aux inégalités $0 < p_1 - p_2 < H$ avec $p_1, p_2 \sim x$, et le théorème de Zhang s'ensuit.

Dans le même ordre d'idées, on pourrait espérer utiliser des bornes sur les écarts telles que (1) (pour x comparable à N), ainsi que la borne inférieure triviale (2), pour obtenir (pour N suffisamment grand et H approprié) une borne inférieure non triviale de la forme :

$$\sum_{n \leq N} \nu(n) 1_B(n) > 0 \quad (3)$$

pour une certaine fonction de pondération ν , où B est l'ensemble des n tels qu'il existe au moins un nombre premier dans chacun des intervalles $[n, n + H]$ et $[N - n - H, n]$. Ceci impliquerait la conjecture de Goldbach binaire avec erreur bornée.

Cependant, l'obstruction de parité empêche une telle stratégie de fonctionner (pour une raison similaire à celle qui empêche toute borne de la forme $H \leq 4$ dans le théorème de Zhang, comme expliqué dans l'article de [Polymath8b](#)). La raison est la suivante : les arguments de la théorie du crible sont linéaires par rapport à la sommation et, de ce fait, tout argument de ce type fonctionnerait automatiquement dans un cadre pondéré où la sommation est pondérée par un poids non négatif $\omega(n) \geq 0$. Plus précisément, si l'on pouvait contrôler les écarts pondérés

$$\Delta(f\omega; a(q)) = \sum_{\substack{x \leq n \leq 2x \\ n \equiv a \pmod{q}}} f(n)\omega(n) - \frac{1}{\phi(q)} \sum_{x \leq n \leq 2x} f(n)\omega(n)$$

avec une précision sensiblement identique à celle des écarts non pondérés (1), alors, grâce à la version pondérée triviale :

$$a_n \geq 0 \text{ pour tout } n \implies \sum_n a_n \omega(n) > 0$$

de (2), tout argument de théorie du crible capable de prouver (3) serait également capable de prouver l'estimation pondérée :

$$\sum_{n \leq N} \nu(n) 1_B(n) \omega(n) > 0. \tag{4}$$

Cependant, (4) peut être réfuté par un choix approprié de poids, à savoir

$$\omega(n) := \prod_{i=1}^H (1 + \lambda(n) \lambda(n+i)) \times \prod_{j=0}^H (1 - \lambda(n) \lambda(N-n-j))$$

où $\lambda(n)$ est la fonction de Liouville, qui compte la parité du nombre de facteurs premiers d'un nombre donné n . Puisque $\lambda(n)^2 = 1$, on peut développer $\omega(n)$ comme la somme de 1 et d'un nombre fini d'autres termes, chacun étant le produit de deux translations (ou réflexions) ou plus de λ . Or, d'après le principe de Möbius (ou son analogue pour la fonction de Liouville), on s'attend généralement à ce que de tels produits de λ soient essentiellement orthogonaux à toute fonction arithmétique $f(n)$ issue d'une fonction multiplicative unique telle que Λ , même sur des progressions arithmétiques très courtes. Par conséquent, remplacer 1 par $\omega(n)$ dans (1) devrait avoir un effet négligeable sur l'écart. D'autre part, pour que $\omega(n)$ soit non nul, $\lambda(n+i)$ doit avoir le même signe que $\lambda(n)$. Par conséquent, le signe opposé à $\lambda(N-n-j)$ ne peut être premier simultanément pour tout $0 \leq i, j \leq H$, et donc $1_B(n) \omega(n)$ s'annule identiquement, ce qui contredit (4). Ceci exclut indirectement toute modification de la méthode de Goldston-Pintz-Yildirim/Zhang pour établir la conjecture de Goldbach binaire avec une erreur bornée.

L'argument précédent n'est pas irréfutable, et l'on peut envisager des solutions à ce problème. L'une d'elles consiste à supposer que le principe d'aléa de Möbius est tout simplement faux, auquel cas l'obstruction liée à la parité disparaît. Un bon exemple en est le résultat de Heath-Brown qui montre que s'il existe une infinité de zéros de Siegel (ce qui constitue une violation importante du principe d'aléa de Möbius), alors la conjecture des nombres premiers jumeaux est vérifiée. Une autre solution consiste à contrôler la divergence (1) pour les fonctions f qui sont des combinaisons de plusieurs fonctions multiplicatives, par exemple $f(n) = \Lambda(n) \Lambda(n+2)$. Cependant, contrôler de telles fonctions semble au moins aussi difficile que la conjecture des nombres premiers jumeaux (ce qui équivaut moralement à obtenir des bornes inférieures non triviales pour $\sum_{x \leq n \leq 2x} \Lambda(n) \Lambda(n+2)$). Une

troisième option consiste à ne pas utiliser d'argument issu de la théorie du crible, mais à tenter une méthode différente (par exemple, la méthode du cercle). Toutefois, la plupart des autres méthodes connues présentent également une linéarité en la variable " n " et je soupçonne qu'elles seraient vulnérables à une obstruction similaire. (Dans tous les cas, la méthode du cercle présente d'autres difficultés spécifiques pour aborder les problèmes binaires, comme expliqué dans cet article précédent <https://terrytao.wordpress.com/2012/05/20/heuristic-limitations-of-the-circle-method/>.)

Premiers commentaires

10 juillet 2014 4 :57

Stijn Hanson

Article très intéressant. Quelles sont les preuves actuelles du caractère aléatoire de la fonction de Möbius ? Autrement dit, existe-t-il des éléments qui pourraient nous amener à penser que le principe d'aléa de la fonction de Möbius est erroné ?

Réponse

10 juillet 2014, 22 :45

Terence Tao

Nous disposons de plusieurs résultats qui affirment que $\sum_n \mu(n)f(n)$ présente une simplification non triviale pour de nombreuses fonctions f raisonnables ; voir par exemple cet article récent de Liu et Sarnak (<https://arxiv.org/pdf/1406.7243>) pour quelques exemples. Nous avons également démontré la petitesse de la fonction de Möbius dans les normes d'uniformité de Gowers, grâce aux travaux de Ben Green, Tamar Ziegler et moi-même (voir <https://arxiv.org/pdf/1009.3998>).

Bien que nous n'ayons aucune raison de remettre en cause l'heuristique de pseudo-aléa de la fonction de Möbius sur les entiers, la situation est plus subtile sur les corps de fonctions, en particulier en caractéristique faible. Par exemple, une observation de Swan (voir : lien dysfonctionnel du site remplacé ici ¹) montre que si f est un polynôme quelconque de $\mathbb{F}_2[t]$, alors $(1+tf)^8+t^3$ est toujours sans facteur carré et possède un nombre pair de facteurs irréductibles ; par conséquent, $\mu((1+tf)^8+t^3)$ vaut identiquement 1, ce qui contrevient à l'heuristique de pseudo-aléa de Möbius sur les corps de fonctions. Conrad et Conrad présentent d'autres exemples de ce type. Cependant, ce phénomène semble être localisé à une faible caractéristique (et à un degré élevé) et ne semble pas avoir d'impact sur la situation au-delà des entiers.

10 juillet 2014 11 :46

Eytan Paldi

Le problème de parité implique (comme déjà remarqué) que pour $k = 2$, pour toute région admissible R (c'est-à-dire satisfaisant les conditions sur $R + R$), sa M -valeur ne peut pas dépasser 2. Cette application au problème variationnel de Selberg est assez remarquable dans le sens où il semble assez difficile de prouver que $M(R) \leq 2$ pour toute région admissible R par une méthode analytique directe, et la seule preuve connue passe par le problème de parité.

1. Note de la traductrice : Lien dysfonctionnel aujourd'hui, on pense que c'est peut-être cette référence qui était fournie alors.

11 juillet 2014 00 :57

gowers

Après un article aussi intéressant, j'hésite à faire une remarque aussi triviale, mais je me permets de la faire : il y a quelque chose d'étrange dans votre dernière phrase (celle entre parenthèses), qui donne l'impression qu'il manque quelques mots par inadvertance.

[Corrigé, merci – T.]

12 juillet 2014 9 :49

Gil Kalai

Le problème de parité s'applique-t-il également à l'affirmation selon laquelle il existe une infinité de solutions pour $p - q = T$ où p et q sont premiers et T est un nombre fixe autre que 2 ?

13 juillet 2014 21 :31

Terence Tao

Oui. En règle générale, lorsqu'on essaie de trouver une paire première (p, q) dans un graphe G sur les nombres naturels (ou sur les "presque premiers"), le problème de parité se pose comme une obstruction chaque fois que le graphe G est 2-colorable (ou même "presque 2-colorable", dans le sens où la proportion d'arêtes monochromes est minuscule), en supposant que la 2-coloration est "non arithmétique" dans un certain sens (de sorte qu'elle ne présente pas de corrélation avec des choses comme la fonction de Möbius). C'est le cas, par exemple, du graphe à arêtes (n, m) avec $n - m = T$, qui peut être 2-coloré par une simple coloration des classes de congruence, ainsi que du graphe de Goldbach à erreur bornée $n + m = N + O(1)$, qui peut être 2-coloré après suppression des nombres proches de $N/2$ (en supposant, pour les besoins de la démonstration, qu'il n'existe pas de nombres premiers de la forme $N/2 + O(1)$). En revanche, le graphe à arêtes (n, m) avec $|n - m| \leq 6$ n'est pas sujet à cette obstruction, même en se restreignant aux entiers premiers avec 2 et 3, en raison de la présence de triangles. Le cas $|n - m| \leq 4$ est plus intéressant. Au départ, il semble y avoir des triangles, ce qui laisse espérer que le problème de parité n'est pas présent ici, mais après avoir supprimé les multiples de 2 et 3, tous les triangles disparaissent et le problème de parité devient évident.