Calculs rigoreux, Goldbach, et l'espoir des preuves formelles

(rappel et suite)

Harald Andrés Helfgott

NuScap, mai 2024

Le problème ternaire de Goldbach : qu'est-ce que c'est ? Que savions-nous ?

De la correspondance entre Leonhard Euler et Christian Goldbach :

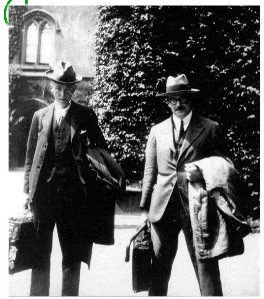
Conjecture ternaire, ou faible, de Goldbach (1742) ("problème des trois nombres premiers")
Tout nombre impair $n \geq 7$ est la somme de trois nombres premiers.

Conjecture binaire, ou forte, de Goldbach (1742) :
tout nombre pair $n \geq 4$ est la somme de deux nombres premiers.

La conjecture forte implique la conjecture faible.

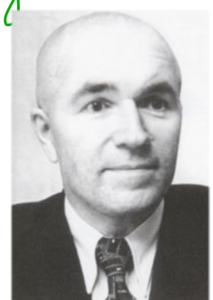
Le XXème siècle et maintenant

Hardy–Littlewood (1922)



Il y a un C tel que tout nombre impair $\geq C$ est la somme de trois nombres premiers si nous admettons l'hypothèse de Riemann généralisée (HRG)

Vinogradov (1937)

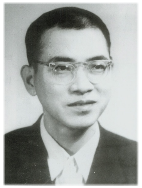


Le même résultat, inconditionnellement.

H.H. (2013) Tout nombre impair $n \geq 5$ est la somme de trois nombres premiers

Bornes pour Goldbach ternaire

Tout nombre impair $n \geq C$ est la somme de trois nombres premiers (Vinogradov)



Bornes pour C ? $C = 3^{3^{15}}$ (Borozdkin), $C = 3.33 \cdot 10^{43000}$ (Wang-Chen, 1989), $C = 2 \cdot 10^{1346}$ (Liu-Wang, 2002).

Vérification pour n petit : tout nombre pair $n \leq 4 \cdot 10^{18}$ est la somme de deux nombres premiers (Oliveira e Silva, Herzog et Pardi, 2012).
Ceci (+ calculs : escalier* des nombres premiers) montre que tout nombre impair $5 < n \leq 1.23 \cdot 10^{27}$ (2012) et maintenant aussi que tout nombre impair $5 < n \leq 8.875 \cdot 10^{30}$ (Helfgott et Platt, 2013) est la somme de trois nombres premiers.

*voir p. exemple Ramaré-Saouter

Escalier :

$p_1 < p_2 < p_3 \cdots$

t.q.

$p_{i+1} - p_i \leq K$ (disons)

Zut : $8.875 \cdot 10^{30}$ est beaucoup plus petit que $2 \cdot 10^{1346}$.

À vrai dire, le nombre de protons et neutrons dans l'univers observable est $\sim 10^{80}$.

Nous devons diminuer C : il doit passer de $2 \cdot 10^{1346}$ à $\sim 10^{30}$. Je l'ai fait passer à 10^{27}. ← et à moins encore

Esquisse de la preuve

voilà la partie (très facile)

vérifier Goldbach faible pour $n \le 10^{27}$

(Helfgott–Platt)

Méthode :

1. Goldbach fort pour $n \le 4 \cdot 10^{18}$ (Oliveira et Silva, Herzog, Pardi)

2. Construire l'escalier :
succession $p_1 < p_2 < p_3 < \dots < p_k < 10^{27} < p_{k+1}$
avec $p_{i+1} - p_i \le 4 \cdot 10^{18} - 5$

Alors : n impair, $n \le 10^{27}$ $\Longrightarrow \exists p$ s.t. $7 \le p \le 4 \cdot 10^{18}$ pair, donc (par 1.) $\exists p_1, p_2$ s.t. $n - p = p_1 + p_2$

VERIFIÉ FORMELLEMENT EN COQ
(Théry–Grégoire, annoncé en 2014)

PARTIE PRINCIPALE (analytique)

Estimation de sommes $\sum \Lambda(n) e^{2\pi i \alpha n}$ (séries de Fourier)

Fonction Λ de von Mangoldt :

$$\Lambda(n) = \begin{cases} \log p & \text{si } \exists p, r \text{ s.t. } n = p^r \\ 0 & \text{sinon} \end{cases}$$

ARCS MAJEURS
(α près d'un a/q avec q petit)
(assez technique et ennuyeux)
(partie IV du livre en ligne)
(utilise la vérification numérique de **HGR** (D. Platt) jusqu'à un certain T_0 et q)

Aha?

arcs mineurs
(long, compliqué, très délicat)
↳ m'a conduit à expliciter pas mal des matériaux de base de la théorie analytique des nombres

Difficultés dans la vérification de la preuve

Goldbach fort jusqu'à $4\cdot 10^{18}$ (Oliveira e Silva et al.) :
algorithme simple (crible d'Eratosthène segmentée),
grand calcul

· garde aux neutrinos !
· preuve formelle ?
(réduisons $4\cdot10^{18} \to 10^{12}$ (disons),
dé-optimisons pour simplifier le programme...)

Problème 1 : vérification formelle d'un programme avec une boucle

HGR jusqu'à T_0 et q :
calcul moyen-grand
(10^5 heures en 2013)
(valeurs de $\zeta(s)$ et $L(s,\chi)$)

utilise : arithmétique d'intervalle
(crlibm + int_double (Platt))

rapide, petite bibliothèque des fonctions,
non vérifiée formellement

Problème 2 : carte à Père Noël

mais vérifiée formellement

partie principale de la preuve

tâche principale :
preuves formelles pour la théorie analytique des nombres
(Prob 3 / grand programme)

calculs :
moyens-petits
utilise :
arithmétique d'intervalles
ball arithmetic

ARB/FLINT, MPFI
grande bibliothèque,
intégration dans C

Problème 4 : Père Noël :
... mais vérifiée formellement

transparence optative !

ce que nous croyons :

Où sont les zéros de $L(s, \chi)$?

Soit $\rho = \sigma + it$ un zéro non trivial quelconque de $L(s, \chi)$.

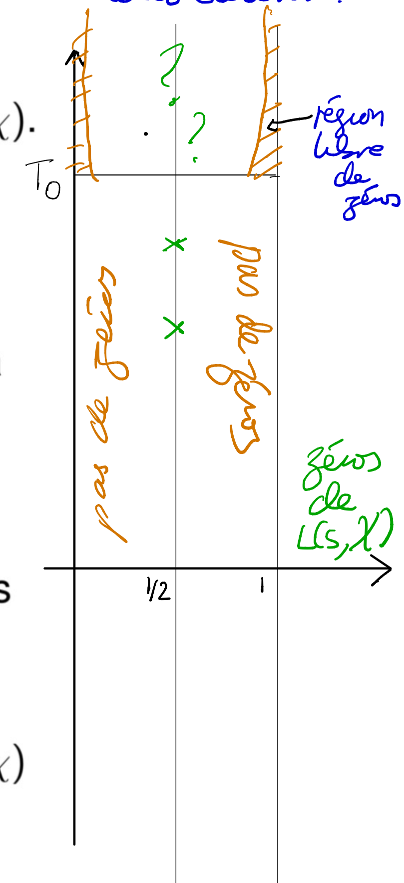
Ce que nous croyons :
$\sigma = 1/2$ (Hypothèse de Riemann généralisée (HRG))

Ce que nous savons :
$\sigma \leq 1 - \frac{1}{C \log q|t|}$ (région libre de zéros classique (**de la Vallée Poussin**, 1899), C explicite (McCurley 1984, Kadiri 2005)

Il y a des régions libres de zéros plus larges asymptotiquement (**Vinogradov-Korobov**, 1958) mais plus étroites, c'est-à-dire, pires, dans la pratique.

Ce que nous pouvons aussi savoir :
pour chaque χ, nous pouvons vérifier HRG pour $L(s, \chi)$ "jusqu'à un hauteur T_0". Ceci veut dire : vérifier que chaque zéro ρ avec $|\Im(\rho)| \leq T_0$ satisfait $\sigma = 1/2$.

ce que nous savons :



Hypothèse de Riemann : $\zeta(s)$ $(= L(s,\chi)$ pour χ trivial) transparence optatives 2

Comment vérifier HRG jusqu'à un hauteur T_0 et un module q ?

Ou même tout simplement l'hypothèse de Riemann (HR) jusqu'à T_0 ?

$$\xi(s) := \frac{1}{2} s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$$

Vrai aussi : $\xi(s) = \overline{\xi(\bar{s})}$

Or $\xi(s) = \xi(1-s)$ (équation fonctionnelle)

Alors, pour $s = 1/2 + it$: $t \in \mathbb{R}$

$\xi(s) \in \mathbb{R}$

Donc : pour trouver les zéros de $\xi(1/2+it)$,

(i.e., les zéros de $\zeta(1/2+it)$)

détectons les changements de signe de $\xi(s)$

Comment calculer $\zeta(1/2+it)$?

(et donc $\xi(1/2+it)$)

- Euler-Maclaurin (temps $\simeq |t|$)
- Équation fonctionnelle approchée / Riemann-Siegel (temps $\simeq \sqrt{|t|}$)

Qu'est-ce que "calculer" veut dire ?

- borne sur le terme d'erreur rigoureuse
- arithmétique d'intervalle : $f([a,b]) \subset [c,d]$

$\xi(1/2+it_0) \in [r_0, r_1]$, $r_1 < 0$

$\xi(1/2+it_1) \in [r_0', r_1']$, $r_0' > 0$

$\Rightarrow \exists$ au moins un zéro de ξ

Ah bon. Mais comment savoir si nous avons trouvé tous les zéros de $\zeta(\sigma+it)$ avec $0\le t\le T$ ($0<\sigma<1$ disons)?

Transparence optionnelle 3

Nous avons une formule avec borne pour

$N(T)$ = nombre de zéros de $\xi(s)$ avec $0\le \mathrm{Re}\, s\le 1$, $0\le \mathrm{Im}\, s\le T$
(c-à-d. de $\zeta(s)$)

$$N(T)=\frac{T}{2\pi}\log\frac{T}{2\pi}+S(T)+\frac{7}{8}+\text{terme d'erreur}$$
$\left(<\frac{1}{20T}\right)$

Nous savons que
$S(T)=O(\log T)$ — et nous avons des bornes plus précises sur $\int_{T_0}^{T_1} S(t)\,dt$

Nous montrons que s'il y avait même un zéro non trouvé (parce que: $\mathrm{Re}\, s=1/2$), nous aurions une contradiction à cette borne.

TB. Quoi de l'HGR?

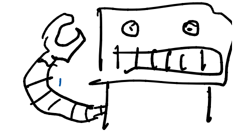
Même procédure.

\+ il est possible de calculer pas mal de valeurs $L(s,\chi)$ d'un coup: beaucoup de χ différents,
ou beaucoup de t différents (Booker)

Transformée rapide de Fourier

Résultat (Platt)
HGR est vraie pour $q\le 400000$ et $|t|\le 10^8/q$.

D'accord. Qu'est-ce que tu disais sur l'arithmétique d'intervalle?



ARB, MPFI, int_double.h de D. Platt
(basé sur Crlibm)

Pour $a, a' > 0$, $[a,b]\cdot[a',b'] \subset [aa', bb']$ etc. a, b de la forme $\frac{n}{2^k}$

Qu'en est-il d'exp, sin, Γ, ...?

Approche (a) : bibliothèque de fonctions correctement arrondies (Crlibm, MPFR, etc.)
$\longrightarrow$ bibliothèque avec arithmétique d'intervalle

JE VOUS MENS
sur sin, exp, ...

Crlibm, MPFR, etc. implémentent sin, exp, etc. correctement arrondies
(en logiciel)

(le standard IEEE garantit seulement $+, -, \cdot, /, \sqrt{\ }$)

INTEL

Approche (b) : bibliothèque d'arithmétique d'intervalle pas forcément avec précision maximale (ARB)

bibliothèque très riche

(pas toujours super-rapide, mais, ...)

PROBLÈME: Il n'y a aucune preuve formelle qu'aucune de ces bibliothèques soit correcte!
(ou souci)

Note: Intel dans les années 90, des GPUs dans nos jours, etc, ont aussi menti sur $+, -, \cdot, /, \sqrt{\ }$!

(C'est ce que COQ, Lean, etc. peuvent offrir est trop lent pour être pratique pour des grands calculs)

Déjà avoir une bibliothèque d'arithmétique d'intervalle avec une preuve formelle qu'elle soit correcte serait très bien.

(riche en fonctions, haute précision, raisonnablement rapide ...)

(pas forcement maximale pour double, disons, mais capable de quadruple (en plus lent))

Est-il possible de désirer plus?

Disons que nous voulons

$$\sum_{\substack{p \leq 10^{14} \\ p \text{ premier}}} 1/p$$

avec 3 chiffres decimales de précision après la virgule

($\sim 3 \cdot 10^{12}$ summands)

approche 1: arithmétique d'intervalle

→ surcoût payé $3 \cdot 10^{12}$ fois

approche 2: l'erreur à chaque pas est $\leq 2^{-52}$

Donc, l'erreur total est $\leq 3.11 \cdot 10^{12} \cdot 2^{-52} \leq 0.0007$

mais:

· fairez-vous confiance à un être humain avec un calcul plus compliqué de ce terme?

· alors, une preuve formelle?

J'AI DIT EN JANVIER 2023:

AUCUN SYSTÈME EXISTANT (Coq, Lean, etc.) NE PEUT "COMPRENDRE" LES BOUCLES

(sauf: en utilisant de l'arithmétique d'intervalle $3 \cdot 10^{12}$ fois!)

Cela était vrai en 2018 - ca. 2022

Retournons sur le problème 1 : crible d'Eratosthène

Nous voulons une implementation du crible
+ une preuve formelle du fait que l'implementation est correcte (pour tout N)

("preuve extrinsèque" — non pas une preuve de longueur ≃ N pour un N donné !)

Les gens travaillent :

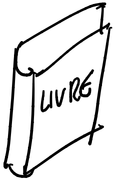
Coq :

- compilateurs formellement verifiés pour langages analogues à C/Rust/etc
- Eratosthène : projet 2024 (demander à Assia Mahboubi)

Lean :

Quelle est la structure de ma preuve de Goldbach faible?

toute formalisation est la bienvenue !



Partie I

Théorie analytique des nombres explicite

version de Dec 2019 en ligne

la partie I est ici basée en part sur des travaux antérieurs (Ramaré, etc.); cette dépendance est maintenant moindre

Formalisation possible?

Jusqu'à présent, seulement un livre (Apostol, niveau licence)

Cela vaudrait bien la peine, mais il y a beaucoup de travail à faire, même sans explicitation

Quelques calculs moyen-grands (vérification de HRG jusqu'à T_0 et q donnés, vérification de $\left|\sum_{n\leq x}\mu(n)\right| \leq \sqrt{x}$ pour $x \leq 10^{14}$, etc.)

Partie II

crible quadratique
grand crible

importance technique générale

petits calculs

Partie III

sommes $\sum \Lambda(n) e^{2\pi i \alpha n}$ sur les arcs mineurs

spécifique au problème de Goldbach faible; applications à des problèmes similaires

Partie IV

arcs majeurs, fonctions spéciales

Partie V

comptabilité

· Beaucoup de travail mathématique "normal", avec des calculs en arithmétique d'intervalle ici et là

petits calculs: en Sagemath, dans l'archive LaTeX

calculs moyens: en C ou Sagemath (code aussi disponible)

exemples:

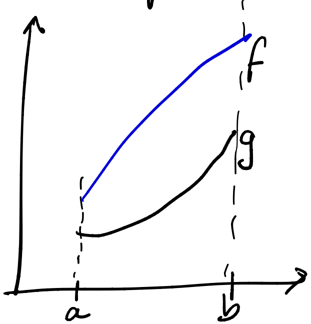
· vérifier quelque chose pour les nombres premiers $p \le 10^5$

· vérifier quelque chose pour $p < 10^9$ ou $p < 10^{12}$.

· vérifier $\left|\sum_{n \le x} \mu(n)\right| \le \sqrt{x}$ pour $x \le 10^{12}$

· calculer des intégrales complexes de longueur $\simeq 10^5$ ou $\simeq 10^6$.

·



Nous pouvons voir (littéralement) que

$$f(x) > g(x) \quad \forall x \in [a,b]$$

Pour le prouver: bisection + arithmétique d'intervalle

$$\mu(n) = \begin{cases} (-1)^k & \text{si } n = p_1 p_2 \cdots p_k, \; p_1, p_2, \dots, p_k \text{ distincts} \\ 0 & \text{sinon} \end{cases}$$

Résultats explicites de base

devrait être très facile à formaliser: $\left|\sum_{n \le x} \mu(n)/n\right| \le 1 \quad \forall x > 0$ (parce que: court et élémentaire)

devrait être plus difficile à formaliser: $\left|\sum_{n \le x} \frac{\mu(n)}{n}\right| \le \frac{0.0144}{\log x} \quad \forall x > 96955$ (Ramaré)

$$\left|\sum_{n \le x} \frac{\mu(n)}{n}\right| \le 7.47 \cdot 10^{-6} + \frac{4.93}{\sqrt{x}} \quad \forall x \ge 1$$

(Chirre–Helfgott)

(utilisent des vérifications de RH et/ou régions libres de zéros)

Suggestions générales:

1 (court/moyen terme)

- sur la vérification (partielle) de longues preuves (p.e. la mienne):

se concentrer sur

- ce qui est réutilisable (résultats de base dans la théorie analytique des nombres explicite, vérifications de RH/GRH)

→ même une grande partie de la théorie non-explicite reste à vérifier!
(à formaliser: un livre type Montgomery-Vaughan, Davenport/Koukoulopoulos, etc.)

- preuves formelles pour des routines d'arithmétique d'intervalle
  - raisonnablement rapides (≤ 10 fois plus lentes que l'arithmétique "naïve")
  - avec une bibliothèque assez riche de fonctions, capacités d'intégration complexe, etc.
  - de bonne précision, même précision réglable (>double), mais pas forcément toujours maximale pour le format

⇑ fonctions correctement arrondies

dépend de

cui: ×10 est important; ×100 serait coûteux)

JG MENS

INTEL

2 (plus ambitieux et "open-ended")

preuves formelles du fait que certains algorithmes numériques sont corrects à une certaine précision, sans utiliser forcément de l'arithmétique d'intervalle (dans les parties "intensives": grandes boucles)

2 → 1