Maths en herbe

Da Silva Mathieu (LMO, équipe AGA)

21 janvier 2026

université PARIS-SACLAY | ÉCOLE DOCTORALE de mathématiques Hadamard (EDMH)

Mon parcours

- 2017-2019 : CPGE MPSI (Lycée Lakanal, Sceaux) - MP* (Lycée Saint-Louis, Paris)
- 2019-2020 : L3 - Magistère à Orsay + admission à l'ENS Paris-Saclay sur second concours
- 2020-2021 : M1 Hadamard (ENS Paris-Saclay)
- 2021-2022 : M2 Formation à l'enseignement supérieur + agrégation externe
- 2022-2023 : M2 Recherche (M2 de mathématiques fondamentales à Jussieu)
- Depuis 2023 : thèse en théorie des nombres sur le sujet "Statistiques arithmétiques et points rationnels sur les variétés algébriques", dirigée par David Harari, Régis de la Bretèche et Kevin Destagnol. Financement : CDSN.

Motivations

Soit $F \in \mathbb{Z}[x_0, \ldots, x_n]$ un polynôme. L'étude des solutions rationnelles ou entières de l'équation

$$F(x_0, \ldots, x_n) = 0$$

est un problème ancien et difficile.

Exemples :

- Triplets pythagoriciens : $x^2 + y^2 = z^2$,
- Dernier théorème de Fermat : $x^n + y^n = z^n$ $(n \geqslant 3)$,
- Écriture d'un entier comme une valeur prise par un polynôme : $m = F(x_0, \ldots, x_n)$.

À l'heure actuelle, on ne sait pas caractériser les entiers n qui peuvent s'écrire comme la somme de trois cubes d'entiers relatifs. Voir par exemple la vidéo de Numberphile `https://www.youtube.com/watch?v=wymmCdLdPyM`.

Motivations

Plusieurs questions naturelles peuvent alors se poser.

- Q1 Étant donnée une telle équation, en existe-t-il au moins une solution $(x_0, \ldots, x_n)$ dans $\mathbb{Q}^{n+1}$ ou dans $\mathbb{Z}^{n+1}$? En cas d'existence de solution(s), en existe-t-il un nombre fini ou bien une infinité ?
- Q2 Dans le cas où une équation n'a pas de solutions rationnelles, quelles sont les obstructions à l'existence de telle solutions ?
- Q3 Dans le cas où il en existe une infinité, que peut-on dire de quantitatif ? (*cf* conjecture de Manin-Peyre)

Motivations

Q1 En 1900, Hilbert propose 23 problèmes qu'il juge alors important de résoudre durant le siècle à venir. Le 10ème problème de Hilbert pose la question de l'existence d'un algorithme prenant en entrée un polynôme $F \in \mathbb{Z}[x_0, \ldots, x_n]$ et renvoyant "oui" si F admet une solution dans $\mathbb{Z}^{n+1}$, "non" sinon.

En 1970, Matiyasevitch prouve qu'il n'existe pas de tel algorithme et résout alors ce problème. La question est toujours ouverte si on remplace $\mathbb{Z}$ par $\mathbb{Q}$.

Il s'agit d'un domaine de recherche toujours actif.

Motivations

Q2 Les seuls complétés de $\mathbb{Q}$ sont $\mathbb{R}$ (pour la valeur absolue usuelle) et les corps p-adiques $\mathbb{Q}_p$ (pour $|x|_p := p^{-v_p(x)}$, p premier). Comme $\mathbb{Q}$ est naturellement inclus dans chacun de ces corps, il est clair que si une équation diophantienne admet une solution dans $\mathbb{Q}^{n+1}$, alors elle admet au moins une solution dans $\mathbb{R}$ et dans chaque $\mathbb{Q}_p$.

La réciproque est fausse en général (voir le contre-exemple de Selmer $3x^3 + 4y^3 + 5z^3 = 0$ pour les solutions non nulles), mais si une équation la satisfait on dit qu'elle vérifie le principe de Hasse. C'est par exemple le cas des coniques (polynômes homogènes de degré 2) à coefficients rationnels (théorème de Hasse–Minkowski).

Dans le cas où le principe de Hasse est vérifié, les seules obstructions à l'existence de solutions rationnelles ou entières proviennent des solutions réelles ou des solutions modulo p premier.

Point de vue géométrique

Rappelons que $\mathbb{P}^n(\mathbb{Q})$ désigne le quotient de $\mathbb{Q}^{n+1} \setminus \{0\}$ par la relation d'équivalence

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists \lambda \in \mathbb{Q}^*,\ (x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n).$$

La classe de $(x_0, \ldots, x_n)$ est notée $[x_0 : \ldots : x_n]$ et est appelée **point rationnel**.

Si $F \in \mathbb{Z}[x_0, \ldots, x_n]$ est un polynôme **homogène**, l'équation $F(x_0, \ldots, x_n) = 0$ définit alors une variété algébrique projective V_F et ses solutions $x \in \mathbb{P}^n(\mathbb{Q})$ sont appelées points rationnels de V_F. Dans ce cas, le problème peut donc se reformuler comme l'étude de l'existence de points rationnels sur certaines variétés algébriques projectives.

Statistiques arithmétiques

On se propose d'étudier le problème de l'existence de solution de façon **quantitative** en répondant à $Q1$ en moyenne. Afin de mesurer la taille/compléxité d'un point $\mathrm{y} \in \mathbb{P}^n(\mathbb{Q})$, on définit sa hauteur par

$$H(\mathrm{y}) = \max(|y_0|, \ldots, |y_n|),$$

où $(y_0, \ldots, y_n)$ est un représentant de y dans $\mathbb{Z}^{n+1}$ vérifiant $\mathrm{pgcd}(y_0, \ldots, y_n) = 1$.

Étant donnée une famille d'équations / de variétés

$$\mathcal{F} := \{F_{\mathrm{y}}(\mathrm{x}) = 0\}_{\mathrm{y} \in \mathbb{P}^n(\mathbb{Q})}$$

avec $F_{\mathrm{y}} \in \mathbb{Z}[x_0, \ldots, x_k]$ homogènes, on peut alors considérer pour $B \geqslant 2$ la quantité

$$N(B; \mathcal{F}) := \# \left\{ \mathrm{y} \in \mathbb{P}^n(\mathbb{Q}) : \begin{array}{c} H(\mathrm{y}) \leqslant B \\ \exists \mathrm{x} \in \mathbb{P}^k(\mathbb{Q}), F_{\mathrm{y}}(\mathrm{x}) = 0 \end{array} \right\}.$$

Question : comment se comporte $N(B; \mathcal{F})$ quand B tend vers $+\infty$?

Exemples

Considérons la famille de coniques

$$\mathcal{C}_0 := \{y_0x_0^2 + y_1x_1^2 + y_2x_2^2 = 0\}_{[y_0:y_1:y_2]\in\mathbb{P}^2(\mathbb{Q})}.$$

- En 1990, Serre a obtenu via le grand crible la majoration

$$N(B;\mathcal{C}_0) \leqslant C\frac{B^3}{(\log B)^{3/2}}$$

où $C > 0$ est une constante indépendante de B, prouvant alors qu'asymptotiquement, 0% des coniques de cette famille possèdent une solution rationnelle.

- Dans les années qui ont suivies, Guo et Hooley ont obtenu indépendamment une minoration

$$N(B;\mathcal{C}_0) \geqslant C'\frac{B^3}{(\log B)^{3/2}}$$

avec $C' > 0$ une constante indépendante de B.

Ainsi, l'ordre de grandeur de $N(B;\mathcal{C}_0)$ est $\frac{B^3}{(\log B)^{3/2}}$.

La conjecture de Loughran-Smeets

En 2016, Loughran et Smeets ont généralisé les travaux de Serre sur les coniques et ont majoré finement la quantité $N(B;\mathcal{F})$ pour une large classe de familles de variétés/d'équations $\mathcal{F}$. Ils obtiennent une majoration de la forme

$$N(B;\mathcal{F}) \leqslant C\frac{B^{n+1}}{(\log B)^{\Delta(\mathcal{F})}}$$

où $\Delta(\mathcal{F}) \geqslant 0$ est un invariant dépendant de la géométrie de la famille $\mathcal{F}$, et où $C > 0$ est une constante indépendante de B. Ils conjecturent alors qu'on a en fait, sous de bonnes hypothèses,

$$N(B;\mathcal{F}) \underset{B\to+\infty}{\sim} c_{\mathcal{F}}\frac{B^{n+1}}{(\log B)^{\Delta(\mathcal{F})}}$$

avec $c_{\mathcal{F}} > 0$ une constante.

La conjecture de Loughran-Smeets

En 2022, Loughran, Rome et Sofos conjecturent en plus une formule close pour la constante $c_{\mathcal{F}}$ au moyen d'invariants géométriques associés à la famille $\mathcal{F}$. Ils vérifient alors leur conjecture dans le cas de la famille $\mathcal{C}_0$ et répondent à la question de Serre (1990) en montrant que

$$N(B;\mathcal{C}_0) \underset{B\to+\infty}{\sim} c_0 \frac{B^3}{(\log B)^{3/2}}$$

avec $c_0 > 0$ explicite sous forme d'un produit eulérien.

Le but de ma thèse est d'accroître le nombre de familles $\mathcal{F}$ pour lesquelles on sait estimer $N(B;\mathcal{F})$ afin de tester cette conjecture et observer ce qu'il se passe quand on s'éloigne un peu du cadre de Loughran-Smeets.

Premier résultat

Théorème 1 (Da Silva, 2025)

Si $\boldsymbol{F} := (F_0, F_1, F_2) \in \mathbb{Z}[y_0, \ldots, y_n]^3$ avec les F_i homogènes, irréductibles de même degré d, et avec n "très grand" devant d, alors la conjecture de Loughran-Smeets est vérifiée par la famille de coniques à coefficients polynomiaux

$$\mathcal{C}_{\boldsymbol{F}} := \{F_0(\mathrm{y})x_0^2 + F_1(\mathrm{y})x_1^2 + F_2(\mathrm{y})x_2^2 = 0\}_{\mathrm{y}\in\mathbb{P}^n(\mathbb{Q})}.$$

Outil principal : Méthode du cercle, repose sur l'égalité

$$\int_0^1 e^{2i\pi\theta F(y_0,\ldots,y_n)}\mathrm{d}\theta = \begin{cases} 1 \text{ si } F(y_0,\ldots,y_n) = 0 \\ 0 \text{ sinon,} \end{cases}$$

que l'on peut alors sommer sur les $(y_0, \ldots, y_n) \in \mathbb{Z}^{n+1}$ vérifiant $\mathrm{pgcd}(y_0, \ldots, y_n) = 1$ et $\max |y_i| \leqslant B$.

Second résultat

Si L est un corps de nombre et si $F \in \mathbb{Z}[s,t]$ est une forme quadratique irréductible sur $\mathbb{Q}$, on considère la famille

$$\mathcal{F}_{L,F} := \{N_{L/\mathbb{Q}}(x) = F(s,t)\}_{(s,t)\in\mathbb{Z}^2}$$

où $N_{L/\mathbb{Q}}$ désigne la norme de L et x désigne un élément de L.

Théorème 2 (Da Silva, 2026 à venir)

Si le groupe de Galois de L est abélien d'ordre D, si L est suffisamment sympathique (son anneau des entiers est principal), et si $N(B;\mathcal{F}_{L,F}) > 0$, alors l'ordre de grandeur de $N(B;\mathcal{F}_{L,F})$ est

$$\begin{cases} \dfrac{B^2}{(\log B)^{1-\frac{1}{D}}} & \text{si } F \text{ est irréductible sur } L \\ \dfrac{B^2}{(\log B)^{1-\frac{2}{D}}} & \text{sinon.} \end{cases}$$

Outils : théorie algébrique des nombres, géométrie des nombres (comptage de points dans des réseaux), théorie analytique des nombres (crible et formule de Perron).

Merci pour votre attention !