

Progrès récents dans la formalisation de la théorie des nombres

Riccardo Brasca

*Université Paris Cité
Institut de Mathématiques de Jussieu-Paris Rive Gauche*

2 juin 2025

Introduction

Dans les dernières années il y a eu des progrès spectaculaires dans la formalisation de la théorie des nombres

On va esquisser ce qui a été fait récemment et ce qui peut être fait dans le futur proche

On va se concentrer sur Lean, mathlib et d'autres projets liés

Plus généralement, on parlera du développement d'une bibliothèque de mathématiques formelles

Exemples de formalisation en théorie *algébrique* des nombres plutôt que analytique.

Dans `mathlib` elle plus développée

Raisons sociologiques plutôt que techniques

La situation est en train de s'améliorer

Theorem

Let K be a number field. Then $\zeta_K(s)$ converges absolutely for $\Re(s) > 1$ and has a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$ with residue

$$\lim_{s \rightarrow 1^+} (s - 1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} \text{Reg}_K h_K}{w_K \sqrt{|D_K|}}$$

```
/--**Dirichlet class number formula** -/  
theorem tendsto_sub_one_mul_dedekindZeta_nhdsGT :  
  Tendsto (fun s : ℝ ↦ (s - 1) * dedekindZeta K s)  
    (ℕ[>] 1) (ℕ (dedekindZeta_residue K)) := by  
  ...
```

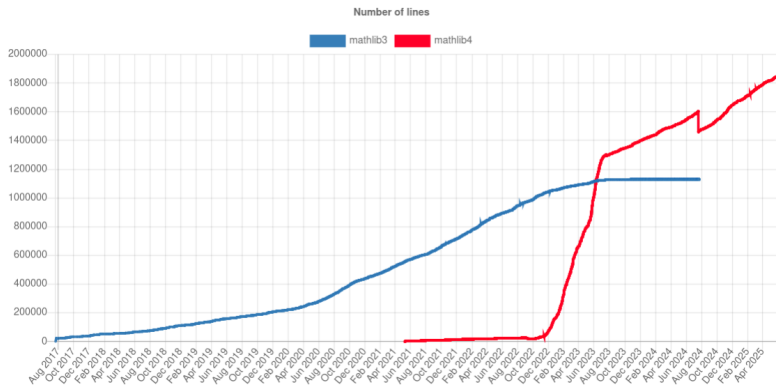
Ce qui existe déjà

- Corps des nombres
- Corps cyclotomiques
- Décomposition des idéaux pour les extensions
- Groupes de classes, unités
- Fonctions zêta
- Courbes elliptiques
- Forme modulaires
- ...

Comment mathlib évolue

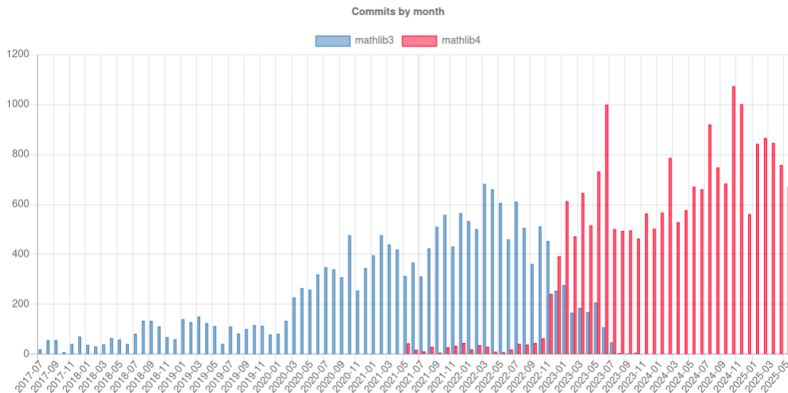
Plus de 200K résultats et 100K définitions

576 contributeurs



Comme mathlib évolue

Beaucoup de (petites) contributions tous les jours



Un projet en cours: formes modulaires

`mathlib` connaît déjà les bases de la théorie, pour $GL_2/\mathbb{Q}$:

- définitions
- q -développement
- série de Eisenstein

Beaucoup reste à faire:

- non-cuspidalité des séries de Eisenstein
- propriétés du q -développement
- considérer niveaux plus généraux que $\Gamma(n)$
- algèbres de Hecke (beaucoup est dans FLT)
- ...

Projets plus ambitieux:

- Courbes modulaires
- Représentations galoisiennes associées aux formes modulaires
- Formes automorphes
- ...

Tout le monde peut contribuer, en ouvrant un *pull request*

Actuellement il y a plus de 1500 pull requests ouvertes

Environ 330 pull requests prêtes pour être examinées dont une quinzaine en théorie des nombres

Où va-t-on?

L'organisation générale de `mathlib` est gérée par 26 *maintainers*

L'objectif principal est d'avoir une bibliothèque complète et cohérente qui peut être utilisée par des projets externes

Les projets externes ont souvent un objectif précis: ce sont les prérequis qui permettent d'améliorer la bibliothèque

Tout le monde peut examiner une pull request
En plus de *maintainers* il y a des *reviewers* qui sont aussi responsables de la qualité du code

Lean assure que les maths dans une pull request sont correctes

Les *définitions* et les *énoncés* doivent par contre être vérifiées par des humains

Cela est parfois très compliqué, par exemple récemment pour la définition de corps local ou de variété algébrique

On est parfois amenés à faire des *refactors*

Le processus de révision peut être long, mais il garantit que

- `mathlib` se construit de manière cohérente
- les résultats sont énoncés dans une généralité correcte
- le code est de bonne qualité

Parfois ça amène à des questions mathématiquement non triviales, comme sur les universes

En conclusion

- `mathlib` a un niveau comparable à un premier cours d'arithmétique en M2
- résultats comme le théorème de Chebotarev sont formalisables en quelques mois
- résultats comme la théorie du corps de classes sont des projets à long terme
- la plus part de résultats de recherche contemporaine restent hors de portée