# SUR LA DENSITÉ MOYENNE DE FAUX TÉMOINS POUR UN ENTIER COMPOSÉ.

Johnathan DJELLA LEGNONGO

Laboratoire de Mathématiques et Applications (LMA) (UASZ / Sénégal)
Laboratoire de Recherche en Mathématiques et Applications (LAREMA) (ENS / Gabon)

Journées Algébriques du Gabon, 21 Mars 2025


# Parcours Académique

- Nationalité : Gabonaise
- Baccalauréat série $C$, Lycée d'État de l'Estuaire, 2014 Gabon.
- Licence en Mathématiques Fondamentales, Université des Sciences et Techniques de Masuku (USTM), 2017, Gabon.
- Master en Mathématiques et Application, Option Mathématiques Pures, Spécialité : Géométrie algébrique en 2019, Soutenu publiquement en 2020 (Covid19), Université Assane Seck de Ziguinchor (UASZ), Sénégal.
  **Sujet de Mémoire :** Conjectures de Weil.
- Inscription en thèse à UASZ, 2022.
- **Sujet de thèse :** Sur la densité moyenne des faux témoins pour un nombre composé et L'indépendance linéaire des sections globales d'un faisceau inversible.
- **Directeurs de thèse :**
  - Marie Salomon SAMBOU, Laboratoire de Mathématiques et Applications(LMA) de UASZ au Sénégal.
  - Tony Mack Robert EZOME MINTSA, Laboratoire de Recherche en Mathématiques et Applications (LAREMA) de Ecole Normale Supérieur au Gabon.
- Lieu : UASZ à Ziguinchor (Sénégal) & ENS à Libreville (Gabon).

# Contenu de la Thèse

On étudie la fiabilité de certains tests de pseudo-primalité.

- Critère de composition : Réciproque d'un théorème lié aux nombres premiers. Exemple : Petit théorème de Fermat.
- D'un critère de composition à un ensemble de témoins $W_n$ et une application : $P_n : W_n \longrightarrow \{\text{premier}, \text{composé}\}$, pour tout impair $n \in \mathbb{N}$.
- Un test de composition ou test de pseudo-primalité est la donnée pour tout entier $n$ d'un couple $(W_n, P_n)$.
- Si $n$ est composé, alors on appelle faux témoin tout élément $x$ de $W_n$ vérifiant $P_n(x) = \text{premier}$.
- Deux indicateurs pour mesurer l'efficacité et la fiabilité d'un test :
  - Densité de faux témoins $\mu = B_n(n)/W_n$, où $B_n$ est le cardinal des faux témoins.
  - Le temps de calcul (ou la complexité) de l'algorithme permettant de réaliser le test.
- Depuis Erdős et Pomerance en 1986 On regarde aussi $W_n$ comme une fonction arithmétique [1] : Une fonction arithmétique $f$ est une fonction définie sur $\mathbb{N}^* = \{1, 2, 3, ...\}$ à valeurs complexes.

  On étudie donc les moyennes $\frac{1}{x}\sum_{n\leq x} B_n$ et $\left(\prod_{\leq x} B_n\right)^{1/x}$, et l'existence d'un ordre normal.

1. *On the number of false witnesses for a composite number*, Math. Comput., 46 :259–279, 1986.

# Contenu de la thèse 2

- **Critère de composition pour le test de Miller-Rabin** :[2] Soit $n \geq 3$ un entier impair. On pose $n-1 = 2^k m$, où $m \in \mathbb{N}$ est impair. Si $n$ est premier alors $\forall x \in (\mathbb{Z}/n\mathbb{Z})^*$ : $x^m = 1$, ou $\exists i \in \{0, 1, 2, \ldots, k-1\},\ x^{2^i m} = -1$.
- **Critère de composition pour le test de Galois**[3] :
  Soit $S$ une $\mathbb{Z}/n\mathbb{Z}$-algèbre commutative fidèle libre de rang $d$. Soit $\sigma \in \mathrm{End}_{\mathbb{Z}/n\mathbb{Z}}(S)$. Soit $\Omega \subset S$ tel que la plus petite sous algèbre de $S$ contenant $\omega$ et stable par $\sigma$ est encore $S$. Supposons que $\sigma(\omega) = \omega^n, \forall \omega \in \Omega$. Si $n$ est premier, alors $\forall x \in S$ on a : $\sigma(x) = x^n$.
- On a $\mu_{\mathrm{MR}(n)} \leq \dfrac{1}{2^{t-1}}$ et $\mu_{\mathrm{Gal}(n)} \leq p^{-\frac{vd}{2}}(1 - 2/R - 4/T)$. Donc le test de Miller-Rabin est fort lorsque $n$ a un nombre de diviseurs $t$ très grand, et celui de Galois est fort lorsqu'il existe $p^\nu \mid n$, avec $\nu$ très grand.
- Couveignes, Ezome et Lercier proposent donc dans (3) un test qui combine les avantages d'un test de Galois et de $r$ tests de Miller-Rabin : c'est le test produit $\mathrm{MR}^r(n) \times \mathrm{Gal}(n)$.
- On note $MR(n)$ le cardinal de faux témoins du test de Miller-Rabin, $Gal(n, d)$ celui du test de Galois et $Str(r, n, d)$ celui du test produit étudié dans (3).

2. René Schoof, *Four primality testing algorithms*, In Algorithmic number theory. Lattices, number fields, curves and cryptography, pages 101–126. Cambridge : Cambridge University Press, 2008.

3. Jean-Marc Couveignes, Tony Ezome, and Reynald Lercier, *A faster pseudo-primality test*, Rend. Circ. Mat. Palermo (2), 61(2) :261–278, 2012.

# État de l'art

- **Le problème** : On ne sait rien de la fiabilité du test de Galois, et du test produit.
- **Notre travail** : Étudier $\frac{1}{x}\sum_{n\leq x} Gal(n,d)$ et $\left(\prod_{\leq x} Gal(n,d)\right)^{1/x}$, puis étudier $\frac{1}{x}\sum_{n\leq x} Str(r,n,d)$ et $\left(\prod_{\leq x} Str(r,n,d)\right)^{1/x}$.
- **Contributions antérieures** : On note $F(n) = \prod_{p|n}(n-1, p-1)$ le nombre de faux témoins du test de Fermat et posons : $\mathcal{L}(x) = \exp\left(\frac{\log x \log\log\log x}{\log\log x}\right)$ pour $x \geq 3$. Erdős et Pomerance[4], ont montré que :

## Théorème ( Moyennes de $F(n)$)

1. *Pour $x$ un réel très grand, on a :* $x^{15/23} < \frac{1}{x}\sum_{n\leq x} F(n) \leq x\mathcal{L}(x)^{-1}$.
2. *Il existe des constantes positives $c_1$, $c_2$ telles que :* $\left(\prod_{n\leq x} F(n)\right)^{1/x} = c_2(\log x)^{c_1} + O\left((\log x)^{c_1-1}\right)$.

- Comme $MR(n) \leq F(n)$, il vient naturellement que $\frac{1}{x}\sum_{n\leq x} MR(n)$ et $\left(\prod_{n\leq x} MR(n)\right)^{1/x}$ ont les mêmes bornes.

4. Paul Erdős & Carl Pomerance :*On the number of false witnesses for a composite number*, Math. Comput., 46 :259–279, 1986.

# Quelques résultats

## Théorème (Djella-Ezome-Luca)

*lorsque* $x \to \infty$,

$$x^{0.7039} < \frac{1}{x} \sum_{\substack{n \leq x \\ n \text{ impair et composé}}} Gal(n,d) \leq x^d \mathcal{L}(x)^{-1+o(1)}. \quad (1)$$

## Théorème (Djella-Ezome-Luca)

*Lorsque* $x \to \infty$,

$$x^{r+0.7039} < \frac{1}{x} \sum_{\substack{n \leq x \\ n \text{ impair et composé}}} Str(r,n,d) \leq x^{r+d} \mathcal{L}(x)^{-2+o(1)},. \quad (2)$$

Pour les moyennes géométriques, on peut consulter
**article :** Johnathan Djella, Tony Ezome and Florian Luca : Bad witnesses for a composite number. Acta Arithmetica 215 (2024), 11-32, https ://doi.org/10.4064/aa230512-17-2

# Il reste du travail

- Étudier l'existence d'un ordre normal pour le test de Galois, affiner les bornes...
- Implémenter et simuler comme Baillie, Fiori et Wagstaff [5] le test produit de Fermat et de Lucas décrit dans l'article de Baillie et Wagstaff [6].
- construire des extensions de Galoisiennes d'anneaux qui optimisent les performances du test de Galois.
- Grantham [7] a montré que tout pseudo-premier de Frobenius est aussi un pseudo-premier de Lucas et de Miller-Rabin. On ne sait rien sur le lien avec le test de Galois.
- La deuxième partie de ma thèse : L'INDÉPENDANCE LINÉAIRE DE CERTAINES SECTIONS GLOBALES D'UN FAISCEAU INVERSIBLES.

5. Robert Baillie, Andrew Fiori, and Samuel Standfield jun. Wagstaff, *Strengthening the Baillie-PSW primality test*, Math. Comput., 90(330) :1931–1955, 2021.

6. Robert Baillie and Samuel Standfield jun. Wagstaff : *Lucas pseudoprimes*, Math. Comput., 35 :1391–1417, 1980.

7. Jon Grantham, *Frobenius pseudoprimes*, Math. Comput., 70(234) :873–891, 2001.

# Écoles de recherche et rencontres

- 2019 : École d'été Franco-allemande (Dresden), Allemagne ; Biennale de Mathématiques à l'université Cheikh Anta Diop (UCAD) ; Workshop Épidémiologie (UASZ), Sénégal.
- 2021 : École de Théorie des Nombres à l'Institut des Mathématiques et de Sciences Physiques (IMSP), Bénin ; *African Mathematics School (online)* at Dschang University, Cameroon.
- 2022 :$3^{\text{ème}}$ édition des Journées Algébriques du Gabon.
- 2024 :$4^{\text{ème}}$ édition des Journées Algébriques du Gabon ; Workshop in Arithmetic and beyond at ENS, Gabon.
- 2025 : Journée LMA (UASZ), $5^{\text{ème}}$ édition des Journées Algébriques du Gabon.
- Rencontre déterminante : Florian Luca (Journées Algébriques 2022).

# Financement et Difficultés

- Financement initial :
  - 2022 : AFRIMATH (CNRS) finance les billets d'avion, PREMA 760€.
  - 2023 : Eropean Mathematical Society (EMS) 2000$.
  - 2024 : Fond propre.
- Difficultés : Financement, déplacement, temps, ressources...

EUROPEAN MATHEMATICAL SOCIETY

# Conclusion et Remerciements


- Remerciements à Salomon Sambou, Tony Ezome, Christian Maire, Florian Luca, CNRS, EMS, PREMA, USTM, UASZ, ENS, IMSP, et UCAD.


**Merci de votre attention !**