Étude de l'irréductibilité des polynômes aléatoires de $\mathbb{Z}[X]$

Pierre-Alexandre Bazin

25 septembre 2023

Résumé

Une conjecture de Odlyzko et Poonen [10] affirme que si A est un polynôme unitaire aléatoire de degré n à coefficients tirés indépendamment et uniformément dans $\{0,1\}$ (à l'exception des coefficients dominant et constant, qui sont pris toujours égaux à 1), alors A est asymptotiquement presque sûrement irréductible lorsque le degré n tend vers l'infini. Nous explorons ici les divers travaux sur cette conjecture et notamment un récent article de Bary-Soroker, Koukoulopoulos et Kozma [1] prouvant la conjecture lorsque les coefficients ne sont pas pris dans $\{0,1\}$ mais plutôt sur un segment de longueur N assez grande.

1 Introduction

1.1 Le problème étudié

On s'intéresse ici à l'irréductibilité de polynômes unitaires aléatoires de $\mathbb{Z}[X]$ à coefficients indépendants. Dans toute la suite, on considérera donc un degré n et des mesures de probabilité $(\mu_j)_{j=0\dots n-1}$ sur $\mathbb{Z}$ (en général $\mu_j = \mu$ identique pour tout j et uniforme sur un intervalle de $\mathbb{Z}$), et A désignera alors (sauf mention contraire) un polynôme unitaire aléatoire

$$A(X) = \sum_{j=0}^{n} a_j X^j \in \mathbb{Z}[X], \text{ où } a_n = 1, a_j \sim \mu_j \forall j < n, \text{ et les } a_j \text{ sont indépendants.}$$

En 1936, Van der Waerden [11] a prouvé que A était souvent irréductible lorsque le degré n est fixé et on étend le support de la mesure μ :

Théorème 1 (Van der Waerden, 1936 [11])**.** *Si les a_j sont indépendants et pris uniformément sur un segment $[\![1, H]\!]$ et le degré n de A est fixé, alors*

$$\mathbb{P}(A = \sum_{j=0}^{n} a_j X^j \text{ irréductible et son groupe de Galois est } \mathfrak{S}_n) \to 1$$

lorsque $H \to \infty$.

Des estimations de la vitesse de convergence ont plus tard été données par Gallagher [7], puis Dietmann [5] et enfin très récemment Bhargava [3].

Lorsque le degré tend vers l'infini avec $\mu_j = \mu$ fixé (par exemple uniforme sur $\{0,1\}$, le problème reste cependant encore ouvert et on a la conjecture suivante, posée par Odlyzko et Poonen [10] :

Conjecture 1. *On suppose ici que $a_0 = a_n = 1$ et les autres a_j sont tirés indépendamment uniformément sur $\{0,1\}$. Alors*

$$\mathbb{P}(A = \sum_{j=0}^{n} a_j X^j \text{ irréductible}) \to 1$$

lorsque $n \to \infty$.

Remarque. *On a toujours $\mathbb{P}(X|A) = \mathbb{P}(a_0 = 0)$, d'où la nécessité de forcer le coefficient constant $a_0 \neq 0$ pour que la conjecture ci-dessus ait une chance d'être vraie.*
Remarquons aussi que $\mathbb{P}(X+1|A) = \mathbb{P}\left(A(-1) = \sum_{j=0}^{n}(-1)^j a_j\right) \asymp 1/\sqrt{n}$, donc on ne peut pas espérer mieux que $1 - O(1/\sqrt{n})$ comme minoration de $\mathbb{P}(A$ irréductible$)$.

C'est sur ce cas du degré tendant vers l'infini que l'on va désormais se concentrer.

1.2 Les résultats actuels

La conjecture ci-dessus a d'abord été étudiée par Konyagin [8], qui a obtenu les résultats suivants :

Théorème 2 (Konyagin, 1999 [8])**.** *Soit A choisi aléatoirement comme dans la conjecture 1. Alors il existe des constantes c, c' tels que quand $n \to \infty$, on a*

$$\mathbb{P}(A \text{ a un facteur de degré } \leq cn/\log n) \to 1$$

et

$$\mathbb{P}(A \text{ irréductible}) > c'/\log n.$$

Breuillard et Varjù [4] ont ensuite récemment démontré la conjecture 1, et même la vitesse de convergence en $O(1/\sqrt{n})$, sous l'hypothèse de Riemann généralisée. Ils obtiennent même une vitesse de convergence plus rapide si l'on s'autorise des facteurs cyclotomiques de petit degré (qui, comme $X+1$, vont avoir une probabilité de diviser A de l'ordre de n^c) :

Théorème 3 (Breuilard-Varjù, 2019 [4])**.** *On suppose l'hypothèse de Riemann pour les fonctions ζ_K des corps $K = \mathbb{Q}(a)$ pour tout entier algébrique a. Alors pour A le polynôme aléatoire de la conjecture 1, on a pour des constantes $c, C > 0$,*

$$\mathbb{P}(A \text{ s'écrit sous la forme } \Phi P) = 1 - O(e^{-c\sqrt{n}/\log n}$$

où P irréductible et Φ est un produit de facteurs cyclotomiques avec $\deg \Phi < C\sqrt{n}$.

Bary-Soroker, Koukoulopoulos et Kozma ont quant à eux amélioré la borne de Konyagin dans l'article [1] que j'ai étudié dans mon mémoire, sans supposer l'hypothèse de Riemann :

Théorème 4 (Bary-Soroker, Koukoulopoulos et Kozma, 2023 [1])**.** *Soit A choisi aléatoirement comme dans la conjecture 1. Alors il existe des constantes $\varepsilon, c, c' > 0$ tels que quand $n \to \infty$, on a*

$$\mathbb{P}(A \text{ a un facteur de degré } \leq \varepsilon n) = 1 - O(n^{-c})$$

et

$$\mathbb{P}(A \text{ irréductible}) > c'.$$

Leur méthode permet aussi d'obtenir une irréductibilité presque sûre lorsque les coefficients ne sont pas choisis dans $\{0,1\}$ mais dans un intervalle d'entiers de longueur N assez grande :

Théorème 5 (Bary-Soroker, Koukoulopoulos et Kozma, 2023 [1])**.** *On suppose ici que les coefficients de A (autres que le coefficient dominant) sont tirés indépendamment selon μ uniforme sur un segment $[\![a, a+N-1]\!] \subset [1, e^{n^\alpha}]$ de longueur $N \geq 35$, avec $\alpha < 1/2$. Il existe alors une constante $c > 0$ telle que*

$$\mathbb{P}(A \text{ irréductible}) > 1 - O_\alpha(n^{-c}).$$

(Un précédent article de Bary-Soroker et Kozma [2] obtient ce résultat lorsque N a au moins quatre facteurs premiers distincts.)

En fait, j'ai pu obtenir dans mon mémoire à partir de leur méthode une meilleure vitesse de convergence lorsque N est très grand :

Théorème 6. *On suppose ici que les coefficients de A (autres que le coefficient dominant) sont tirés indépendamment selon μ uniforme sur un segment $[\![a, a+N-1]\!] \subset [1, e^{n^\alpha}]$ de longueur N avec $\alpha < 1/2$. Pour tout $C > 0$, il existe une constante N_C (dépendant uniquement de C) telle que si $N > N_C$,*

$$\mathbb{P}(A \text{ s'écrit sous la forme } \Phi P) > 1 - O_\alpha(n^{-C})$$

où P irréductible et Φ est un produit de facteurs cyclotomiques de degré $< \sqrt{n}$.

Notamment si $N > N_{1/2}$, on obtient la borne (optimale)

$$\mathbb{P}(A \text{ irréductible}) > 1 - O_\alpha(1/\sqrt{n})$$

(les facteurs cyclotomiques arrivant avec une probabilité $O(1/\sqrt{n})$).

Dans le cas des coefficients dans $\{0,1\}$, on obtient une amélioration de la vitesse de convergence dans le théorème 4 au prix d'un ε plus faible :

Théorème 7. *Soit A choisi aléatoirement à coefficients dans $\{0,1\}$ comme dans la conjecture 1, et $C > 0$. Alors il existe $\varepsilon > 0$ (dépendant uniquement de C) tel que quand $n \to \infty$, on a*

$$\mathbb{P}(A \text{ a un facteur non cyclotomique de degré } \leq \varepsilon n) = 1 - O(n^{-C})$$

(ici, l'ajout de "non cyclotomique" est nécessaire lorsque $C > 1/2$.)

1.3 Résumé de la preuve de [1]

L'argument de [2, 1] commence par la remarque suivante : si B est un facteur de A de degré k, ce sera aussi le cas modulo tout facteur premier p. Ainsi, si les lois μ_j des coefficients de A sont uniformes modulo un produit $P = p_1 \dots p_r$ de facteurs premiers distincts (par exemple uniformes sur un segment de longueur multiple de P), on a

$$\begin{aligned}\mathbb{P}(A \text{ a un facteur de degré } k) &\leq \mathbb{P}(\forall i, A \mod p_i \text{ a un facteur de degré } k)\\ &= \prod_{i=1}^{r} \frac{\#\{A_{p_i} \in \mathbb{F}_{p_i}[X]_n^u \text{ ayant un facteur de degré } k\}}{p_i^n}.\end{aligned}$$

où $\mathbb{F}_p[X]_n^u$ est l'ensemble des polynômes unitaires de degré n de $\mathbb{F}_p[X]$.

En effet, dans ce cas, les $A \mod p_i$ sont uniformes sur $\mathbb{F}_{p_i}[X]_n^u$, et indépendants par le théorème des restes chinois. Ainsi, si l'on arrive à une majoration en $O(k^{-c_0})$ sur $\mathbb{P}(A$ a un facteur de degré k modulo $p_i)$, on aura une majoration en $O(k^{-rc_0})$ sur $\mathbb{P}(A$ a un facteur de degré $k)$ et donc, en sommant sur k, pour peu que $r > 1/c_0$, une majoration en $O(n_1^{1-rc_0})$ pour $\mathbb{P}(A$ a un facteur de degré $\geq n_1)$.

Pour obtenir une majoration utile de $\mathbb{P}(A$ irréductible) à partir de cette idée, il faut majorer séparément $\mathbb{P}(A$ a un facteur de degré $\leq n_1)$ pour un $n_1 = n^{\varepsilon}$, ce qui peut être fait en adaptant les arguments de Konyagin [8] lorsque les coefficients de A sont bornés par un $e^{n^{\alpha}}$ pour un $\alpha < 1/2$ (d'où l'intérêt de cette hypothèse dans le théorème 5). Plus de détails par rapport à cet aspect sont donnés en partie 2.1.

Pour obtenir la majoration de $\mathbb{P}(A \mod p_i$ a un facteur de degré $k)$, on peut citer un récent résultat de Meisner [9] estimant exactement cette probabilité :

Théorème 8 (Meisner [9])**.** *Si A_p suit une loi uniforme sur $\mathbb{F}_p[X]_n^u$, alors*

$$\mathbb{P}(A_p \text{ a un facteur de degré } k) \asymp k^{-Q(1/\log 2)} (\log k)^{-3/2},$$

où $Q(t) = t \log t - t + 1 = \int_1^t \log u \, du$.

Ainsi, on obtient le résultat du théorème 5 lorsque N a au moins $r = 12 = \lceil 1/Q(1/\log 2) \rceil$ facteurs premiers distincts.

L'article [2] arrivait cependant à obtenir le résultat dès que N a au moins 4 facteurs premiers distincts : en effet, bien que la majoration de Meisner soit optimale à k fixé, les événements "A a un facteur de degré k" sont fortement corrélés pour des k proches. Cette corrélation est due aux polynômes A ayant de nombreux facteurs irréductibles de petit degré (qui peuvent être multipliés pour donner des facteurs de degré k pour de nombreux k).

On définit donc les événements $\mathcal{E}_m$ "A a peu de facteurs irréductibles de petit degré modulo les p_i" :

Définition 1. *Pour $(A_1, \dots, A_r)$ aléatoire avec chaque A_i à valeurs dans $\mathbb{F}_{p_i}[X]_n^u$, on définit*

$$\mathcal{E}_m := \left\{ \prod_{i=1}^{r} \tau(A_i^{\leq m}) \leq (2em)^{tr \log 2} \right\},$$

où τ est la fonction nombre de diviseurs, $A^{\leq m}$ désigne le produit des facteurs irréductibles (pris avec multiplicité) de A de degré $\leq m$ et t est un paramètre qui sera fixé entre 1 et $1/\log 2$ en fonction de r.

Remarque. *On aurait pu définir plus simplement $\mathcal{E}_{m,p} := \{\tau(A_p^{\leq m}) \leq (2em)^{t \log 2}\}$ puis $\mathcal{E}_m = \bigcap_i \mathcal{E}_{m,p_i}$ (c'est l'approche utilisée dans l'article [1]). Cependant, coupler l'information sur les différents p_i dans la définition de $\mathcal{E}_m$ permettra d'obtenir une majoration en $O(n^{-rc})$ de $\mathbb{P}(\bigcup \bar{\mathcal{E}}_m)$ (plutôt que $O(n^{-c})$) ce qui permettra d'obtenir le théorème 6 en prenant r grand (dépendant de C).*

On pourra alors obtenir une bien meilleure majoration de

$$\mathbb{P}(\mathcal{E}_{k/(\log k)^2} \cap "A \text{ a un facteur de degré } k \text{ modulo tous les } p_i")$$

(qui sera suffisante dès que $r = 4$), puis majorer séparément $\mathbb{P}(\bigcup \bar{\mathcal{E}}_m)$ (notons que les $\bar{\mathcal{E}}_m$ sont maintenant clairement très similaires pour des m proches). Cet aspect est détaillé dans la partie 2.2.

Cependant, dans le cadre plus large de l'article [1] (théorème 5), la mesure μ (uniforme sur un segment de longueur N quelconque) ne sont en général pas exactement uniformes modulo P. On introduit donc un terme d'erreur $\Delta_A(m)$ défini ci-dessous :

Définition 2. *Étant donné $A_1 \in \mathbb{F}_{p_1}[X], \dots, A_r \in \mathbb{F}_{p_r}[X]$ unitaires aléatoires (non nécessairement indépendants), on définit l'écart total à l'uniformité de $(A_1, \dots, A_r)$ modulo les polynômes de degré $\leq m$,*

$$\Delta_{(A_1,\dots,A_r)}(m) := \sum_B \left| \mathbb{P}(\forall i, B_i | A_i) - \prod_{i=1}^{r} p_i^{-\deg B_i} \right|$$

où la somme porte sur les r-uplets de polynômes unitaires $B_i \in \mathbb{F}_{p_i}[X]$ tous de degré $\leq m$ et non multiples de X.

Remarque. *Ici, on a exclu les polynômes multiples de X dans la somme définissant $\Delta_{(A_1,\dots,A_r)}(m)$, car l'écart à l'uniformité pour ceux-ci serait trop important. Ceux-ci devront donc être traités à part dans les majorations de $\mathbb{P}(A \mod p$ a un facteur de degré $k)$, mais nous ne détaillerons pas cet aspect dans cette introduction.*

Lorsque μ est assez proche de l'uniformité modulo P (ce qui arrivera notamment pour μ uniforme sur un segment de longueur N assez grande comme dans le théorème 5) et A aléatoire de $\mathbb{Z}[X]$ à coefficients indépendants tirés selon μ, on pourra obtenir une majoration de $\Delta_{(A \mod p_i)_i}(n/2)$, qui permettra de prouver l'irréductibilité presque sûre de A (notons que A est irréductible dès qu'il n'a pas de facteur de degré $\leq n/2$). Lorsque μ est quelconque (par exemple uniforme sur $\{0,1\}$), on ne pourra cependant que contrôler $\Delta_{(A \mod p_i)_i}(\varepsilon n)$ pour un $\varepsilon > 0$, ce qui permettra d'obtenir uniquement un contrôle sur les facteurs de A de degré $\leq \varepsilon n$ (cf théorème 4).

Les techniques permettant de majorer $\Delta_{(A \mod p_i)_i}(m)$, reposant sur l'analyse de Fourier, seront présentées en partie 2.3. Nous ne détaillerons pas comment la présence de ces termes Δ_A influent sur les majorations de la partie 2.2 (mentionnons quand même que cela nécessite d'ajouter une condition sur le degré des $A_i^{\leq m}$ dans la définition de $\mathcal{E}_m$, car on ne contrôle pas l'écart à l'uniformité modulo les polynômes de grand degré).

2 Idées de la preuve

2.1 Polynômes ayant des facteurs de petit degré

On cherche ici à majorer la probabilité d'avoir un facteur de degré $\leq n^\varepsilon$ dans A. Pour cela, on commence par borner les coefficients des polynômes de $\mathbb{Z}[X]$ pouvant diviser A (en utilisant le fait que les coefficients de A sont bornés par $H = e^{n^\alpha}$), ce qu'on fait grâce au lemme ci-dessous. On majorera ensuite la probabilité pour chacun de ces facteurs de diviser A - notons ici qu'on peut se contenter des facteurs irréductibles, puisque tout polynôme ayant un facteur de degré $\leq n^\varepsilon$ a un facteur irréductible de degré $\leq n^\varepsilon$. (Ce ne sera pas le cas lorsqu'on s'intéressera aux facteurs modulo p de degré k.)

Lemme 9. *Soit A un polynôme unitaire de $\mathbb{Z}[X]$ dont tous les coefficients sont de valeur absolue $\leq H$. Alors toutes ses racines complexes sont de module $< H+1$.*

Démonstration. Avec $A = X^n + \sum_{i=0}^{n-1} a_i X^i$, et r une racine complexe de A, on a $A(r) = 0$ d'où

$$r^n = -\sum_{i=0}^{n-1} a_i r^i,$$

puis

$$|r|^n \leq \sum_{i=0}^{n-1} H|r|^i = H\frac{|r|^n - 1}{|r| - 1},$$

d'où si $r \geq 1, |r| - 1 \leq H\frac{|r|^n - 1}{|r|^n} < H$, d'où $|r| < H + 1$. □

Corollaire 10. *Avec les mêmes hypothèses sur A, si $D \in \mathbb{Z}[X]$ de degré m (unitaire) divise A, alors les coefficients de D sont de valeur absolue $< \max\{m; H+1\}^m$.*

Démonstration. Écrivons $D = (X - r_1)\dots(X - r_m)$ dans $\mathbb{C}[X]$. Tous les r_i sont alors des racines de A, donc de module $< H + 1$. On peut alors majorer par les relatons de Viète pour tout $j < m$, le j-ième coefficient

$$d_j = \sum r_{i_1} \dots r_{i_{m-j}} < \binom{m}{j}(H+1)^{m-j} \leq m^j(H+1)^{m-j} \leq \max\{m; H+1\}^m,$$

comme voulu. □

Ainsi, si $H \geq n$ (ce qui sera en pratique le cas, vu qu'on aura $H = e^{n^\alpha}$), pour D de degré m, chacun des m coefficients non-dominants de D peut prendre au plus $2(H+1)^m$ valeurs, soit $2^m(H+1)^{m^2}$ polynômes D possibles, et ce pour tout $m \leq n^\varepsilon$. Il y a ainsi au plus

$$\sum_{m=1}^{n^\varepsilon} 2^m(H+1)^{m^2} \leq \sum_{m=1}^{n^\varepsilon} 2^m(H+1)^{n^{2\varepsilon}} \leq 2^{n^\varepsilon}(H+1)^{n^{2\varepsilon}}$$

diviseurs de degré $\leq n^\varepsilon$ à considérer, dont on doit maintenant majorer la probabilité de diviser A.

Considérons donc maintenant un polynôme irréductible unitaire $D \in \mathbb{Z}[X]$ candidat à être diviseur de A. On a alors $D|A$ si et seulement si $A(r) = 0$, où r est une racine complexe de A. Remarquons ici que si $|r| > 1$, $A(r)$ prend des valeurs de l'ordre de r^n, et on pourra alors espérer une majoration exponentielle (en n) de $\mathbb{P}(A(r) = 0)$, qui pourra contrebalancer le terme en $(H+1)^{n^{2\varepsilon}}$ venant du nombre de diviseurs vu en partie précédente. À l'inverse, si $|r| = 1$ (ce qui arrive lorsque D est cyclotomique), $A(r)$ sera beaucoup plus faible et on aura une beaucoup moins bonne majoration. Pour illustrer cela, considérons les cas où $D = X - r$ est de degré 1.

— Si $r = \pm 1$, $A(r)$ est une somme (ou somme alternée) des a_i. On aura alors par le théorème central limite $\mathbb{P}(A(r) = 0) = O(1/\sqrt{n})$.

— Si $|r| \geq 2$, considérons $d > \log(2H+1)/\log 2$. Si l'on fixe les a_i pour i non multiple de d, alors il y a au plus un choix des a_{di} tel que $A(r) = 0$. En effet, la condition $A(r) = 0$ se réécrit

$$\sum_i a_{di} r^{di} = \sum_{d \nmid i} a_i r^i,$$

où le terme de droite est fixé et le terme de gauche est distinct pour chaque choix des a_{di} avec $|a_{di}| \leq 2H$ (car $|r|^d \geq 2^d > 2H+1$).
On obtient alors si μ uniforme sur un intervalle de longueur N,

$$\mathbb{P}(A(r) = 0) \leq (1/N)^{n/d} \leq e^{O(n/\log H)}.$$

Pour conduire le raisonnement du cas $|r| > 1$ aux polynômes non cyclotomiques de plus grand degré (pour lesquels on n'a plus nécessairement $|r| \geq 2$), on utilise un résultat de Dobrowolski [6] permettant quand même de minorer $|r|$ pour la plus grande racine r de D lorsque D est non cyclotomique, et on obtient quand même

$$\mathbb{P}(D|A) \leq e^{n^{1-o(1)}/\log H}.$$

Ainsi, en sommant sur les $(H+1)^{n^{2\varepsilon}}$ facteurs D possibles de degré $\leq n^\varepsilon$, on obtient si $H = e^{n^\alpha}$ et $\alpha + \varepsilon < 1/2$,

$$\begin{aligned}\mathbb{P}(A \text{ a un facteur irréductible de degré } \leq n^\varepsilon \text{ non cyclotomique}) &\leq 2^{n^\varepsilon}(H+1)^{n^{2\varepsilon}} e^{-n^{1-o(1)}/\log H} \\ &\leq e^{n^{\alpha+2\varepsilon+o(1)} - n^{1-\alpha-o(1)}} \\ &= e^{-n^{1-\alpha-o_{\alpha,\varepsilon}(1)}} = o_{\alpha,\varepsilon}(e^{-\sqrt{n}}).\end{aligned}$$

Quant aux facteurs cyclotomiques, on peut prouver que $\mathbb{P}(D|A) = O(n^{-d/2})$ si A cyclotomique de degré d et il y a au plus $\#\{d, \phi(d) \leq n^\varepsilon\} = O(n^\varepsilon \log\log n)$ polynômes cyclotomiques de degré $\leq n^\varepsilon$, d'où on peut déduire $\mathbb{P}(A \text{ a un facteur cyclotomique de degré } \leq n^\varepsilon) = O(1/\sqrt{n})$.

2.2 Polynômes ayant des facteurs de grand degré

On se place ici dans $\mathbb{F}_p[X]^u$ pour simplifier (les résultats s'adaptent dans $\prod_{i=1}^r \mathbb{F}_{p_i}[X]^u$). Dans cette partie, on fixe donc A un polynôme unitaire de degré n aléatoire suivant une loi uniforme sur $\mathbb{F}_p[X]_n^u$ et on définit

$$\mathcal{E}_m := \{\tau(A) \leq (2em)^{t \log 2}\},$$

où t est un paramètre pris entre 1 et $1/\log 2$.
On définit de plus $\mathcal{I}_m$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré total $\leq m$, et

$$\Sigma_m := \sum_{I \in I_m} \frac{1}{p^{\deg I}} \; ; \; \Pi_m := \prod_{I \in \mathcal{I}_m} \left(1 - \frac{1}{p^{\deg I}}\right).$$

Le théorème des nombres premiers dans $\mathbb{F}_p[X]$ affirme que le nombre de polynômes irréductibles de $\mathbb{F}_p[X]$ de degré k est $p^k/k + O(p^{k/2})$ (on a en fait la valeur explicite $\frac{1}{k}\sum_{d|k} \mu(d) p^{k/d}$), de sorte que

$$\Sigma_m = \sum_{k=1}^m \frac{1}{k} + O(1) = \log m + O(1) \text{ et } \Pi_m = e^{-\Sigma_m + O(1)} \asymp 1/m.$$

Ici, la valeur moyenne de $\tau(A^{\leq m})$ sera alors de l'ordre de $\sum_{B=B^{\leq m}} 1/p^{\deg B} = \Pi_m^{-1} \asymp m$, mais les valeurs de $\tau(A^{\leq m})$ vont se concentrer autour de $2^{\Sigma_m} \asymp m^{\log 2}$ (Σ_m correspondant au nombre moyen de facteurs irréductibles de $A^{\leq m}$). Ce phénomène, dû à la nature multiplicative de τ, est au cœur des résultats de cette partie (notons qu'on a pris $1 < t < 1/\log 2$, ce qui correspond à une borne sur $\tau(A^{\leq m})$ entre 2^{Σ_m} et Π_m^{-1} dans la définition de $\mathcal{E}_m$). On obtiendra alors les résultats suivants :

Lemme 11. *On a lorsque* $n/2 \geq k \geq 6m \log m$,

$$\mathbb{P}(\exists D|A \text{ de degré } k \cap \mathcal{E}_m) = O(m^{t \log 2 - 1}).$$

Lemme 12. *On a lorsque* $n \geq 6m \log m$ *et* $t > 1$,

$$\mathbb{P}(\bigcup_{m_1 \leq j \leq m} \bar{\mathcal{E}}_j) = O(\log m \cdot m_1^{-Q(t)}),$$

où on rappelle que $Q(t) = t \log t - t + 1 = \int_1^t \log u \, du$.

Avant de prouver ces lemmes, on donne un lemme permettant d'approximer la distribution de $A^{\leq m}$.

Lemme 13. *On a pour* $D \in \mathbb{F}_p[X]_n^u$ *fixé, si* $n = \deg A \geq \deg D + 6m \log m$,

$$\mathbb{P}(D|A; (A/D)^{\leq m} = 1) \leq 2 \cdot p^{-\deg D} \Pi_m.$$

(Notamment lorsque $D = D^{\leq m}$, *on obtient* $\mathbb{P}(A^{\leq m} = D) \leq 2 \cdot p^{-\deg D} \Pi_m$.*)*

Nous ne prouverons pas ce lemme ici ; notons simplement que le terme $p^{-\deg D}$ correspond à la condition $D|A$ et Π_m correspond à la condition $(A/D)^{\leq m} = 1$ (qui est équivalente à une non-divisibilité de A/D par tous les polynômes irréductibles de degré $\leq m$). On s'attendrait alors à avoir $\mathbb{P}(D|A; (A/D)^{\leq m} = 1) = 2 \cdot p^{-\deg D} \Pi_m$; cependant, la distribution de $A^{\leq m}$ est biaisée par le fait qu'on a toujours $\deg A^{\leq m} \leq \deg A = n$. Le lemme ci-dessus, dont la preuve repose sur le crible de Brun, affirme alors que ce biais n'est pas trop fort.

Remarque. *Une version plus générale du lemme, adaptée au cas de* r *nombres premiers, est donnée dans ([1], Lemme 8.2). Celle-ci permet aussi de majorer l'écart à la distribution attendue par un terme en* Δ_A *(introduit en définition 2) lorsque* A *n'est pas uniforme modulo* p.

Nous pouvons maintenant prouver les lemmes 11 et 12.

Démonstration. (du lemme 11)
On va ici exploiter le fait que sous la condition de l'événement $\mathcal{E}_m$, il y a peu de choix de $D^{\leq m}$ pour D divisant A, puisque $D^{\leq m}$ doit diviser $A^{\leq m}$. On a alors

$$\begin{aligned}
&\mathbb{P}(\exists D|A \text{ de degré } k \cap \mathcal{E}_m) \\
&\leq \sum_{\deg D = k} \mathbb{P}(D|A \cap \mathcal{E}_m) \\
&= \sum_{H \in \mathcal{E}_m, H = H^{\leq m}} \sum_{\deg D = k} \mathbb{P}(D|A \cap A^{\leq m} = H) \\
&= \sum_{H \in \mathcal{E}_m, H = H^{\leq m}} \sum_{B|H} \sum_{\deg E = k - \deg B, E^{\leq m} = 1} \mathbb{P}(BE|A \cap A^{\leq m} = H) \\
&= \sum_{H \in \mathcal{E}_m, H = H^{\leq m}} \sum_{B|H} \sum_{\deg E = k - \deg B, E^{\leq m} = 1} \mathbb{P}(HE|A \cap (A/HE)^{\leq m} = 1) \\
&\leq \sum_{H \in \mathcal{E}_m, H = H^{\leq m}} \sum_{B|H} \sum_{\deg E = k - \deg B, E^{\leq m} = 1} \frac{2\Pi_m}{p^{\deg HE}} && \text{(lemme 13)} \\
&= \sum_{H \in \mathcal{E}_m, H = H^{\leq m}} \frac{2\Pi_m}{p^{\deg H}} \sum_{B|H} \mathbb{P}(E^{\leq m} = 1) && \text{où } E \text{ uniforme sur } \mathbb{F}_p[X]_{k - \deg B}^u \\
&\leq \sum_{H \in \mathcal{E}_m, H = H^{\leq m}} \frac{2\Pi_m}{p^{\deg H}} \tau(H) \cdot 2\Pi_m && \text{(lemme 13)} \\
&\leq \sum_{H = H^{\leq m}} \frac{2\Pi_m}{p^{\deg H}} (2em)^{t \log 2} \cdot 2\Pi_m && \text{par définition de } \mathcal{E}_m \\
&= 4 \cdot (2em)^{t \log 2} \Pi_m = O(m^{t \log 2 - 1}).
\end{aligned}$$

□

Ici, on a gagné un facteur $m^{t \log 2 - 1}$ par rapport au nombre moyen de facteurs de degré k d'un A quelconque (qui est de 1) en forçant $A^{\leq m}$ à avoir moins de facteurs que la moyenne (par un facteur $m^{t \log 2 - 1}$.

Démonstration. (du lemme 12)

On exploite ici le fait que les $\bar{\mathcal{E}}_j$ sont similaires pour des j proches. En effet, si l'on écrit

$$\mathcal{E}'_m := \{\tau(A^{\leq m}) \geq 2^{t\Sigma_m}\},$$

on aura toujours $\bar{\mathcal{E}}_j \subset \mathcal{E}'_{2m}$ pour tout $j \in [m, 2m]$ (car $A^{\leq j} | A^{\leq 2m}$ et $(2ej)^{tr\log 2} \geq (2em)^{t\log 2} \geq 2^{t\Sigma_{2m}}$).

Ainsi, on aura alors

$$\mathbb{P}(\bigcup_{m_1 \leq j \leq m} \bar{\mathcal{E}}_m) \leq \mathbb{P}(\bigcup_{m_1 \leq 2^j \leq 2m} \bar{\mathcal{E}}'_{2^j} \leq \sum_{m_1 \leq 2^j \leq m} \mathbb{P}(\mathcal{E}'_{2^j}),$$

où la somme ne contient maintenant plus que $O(\log m)$ termes. Pour conclure, il suffit alors de prouver $\mathbb{P}(\mathcal{E}'_m) = O(m^{-Q(t)})$ (sous la condition $n \geq 6m\log m$ qui servira à appliquer le lemme 13).

Pour cela, on utilise l'astuce de Rankin. On introduit donc $s > 0$ et on écrit $\mathbb{1}_{\mathcal{E}'_m} \leq (\tau(A^{\leq m})2^{-t\Sigma_m})^s$. Ainsi,

$$\begin{aligned}
\mathbb{P}(\mathcal{E}'_m) &\leq \mathbb{E}((\tau(A^{\leq m})2^{-t\Sigma_m})^s) \\
&\leq \sum_{B=B^{\leq m}} 2\frac{\Pi_m}{p^{\deg B}} \cdot (\tau(B)2^{-t\Sigma_m})^s && \text{(lemme 13)} \\
&= 2\Pi_m \cdot 2^{-ts\Sigma_m} \prod_{I \text{ irr. } \deg I \leq m} \sum_{\nu=0}^{\infty} \frac{(\nu+1)^s}{p^{\nu \deg I}} && \text{(produit eulérien)} \\
&\leq 2\Pi_m \cdot 2^{-ts\Sigma_m} \cdot e^{\sum_{I \text{ irr. } \deg I \leq m} \sum_{\nu=1}^{\infty} \frac{(\nu+1)^s}{p^{\nu \deg I}}} \\
&= 2\Pi_m \cdot 2^{-ts\Sigma_m} \cdot e^{\sum_{I \text{ irr. } \deg I \leq m} \frac{2^s}{p^{\deg I}} + O(1)} && \text{(ici } \sum_{I \text{ irr. } \deg I \leq m} \sum_{\nu=2}^{\infty} \frac{(\nu+1)^s}{p^{\nu \deg I}} \text{ converge quand } m \to \infty) \\
&= 2\Pi_m \cdot e^{(2^s - ts\log 2)\Sigma_m + O(1)} \\
&= 2\Pi_m \cdot e^{(t - t\log t)\Sigma_m + O(1)} && \text{en prenant la valeur optimale } s = \log_2(t) > 0 \text{ (ici } t > 1) \\
&= O(m^{-Q(t)}).
\end{aligned}$$

□

Lorsqu'on utilise plusieurs nombres premiers $p_1, \ldots, p_r$, on peut gagner un facteur r dans l'exposant dans les lemmes 11 et 12. On obtient alors en posant par exemple $m(n) := n/(\log n)^2$, pour $n_1 \leq n_2$ avec $\log n_2 = n_1^{o(1)}$ (par exemple $n_1 = n^\varepsilon$ et $n_2 = n/2$),

$$\begin{aligned}
&\mathbb{P}(\exists D | A \text{ de degré } k \text{ pour un } k \in [n_1, n_2]) \\
&\leq \sum_{n_1 \leq k \leq n_2} \mathbb{P}(\exists D | A \text{ de degré } k \cap \mathcal{E}_{m(k)}) + \mathbb{P}\left(\bigcup_{m(n_1) \leq m \leq m(n_2)} \bar{\mathcal{E}}_m\right) \\
&\leq \sum_{n_1 \leq k \leq n_2} O_{r,t}\left(m(k)^{r(1-t\log 2)}\right) + O_{r,t}\left((\log n_2) \cdot m(n_1)^{-rQ(t)}\right) \\
&= O_{r,t}(n_1^{r(1-t\log 2)-1+o(1)}) + O_{r,t}(n_1^{-rQ(t)+o(1)}) \text{ car } \log n_2 = n_1^{o(1)} \\
&= O_r\left(n_1^{-c_r}\right) \text{ en choisissant bien } t,
\end{aligned}$$

où

$$c_r := \sup_{1 \leq t \leq 1/\log 2} \min\{r(1 - t\log 2) - 1; r(t\log t - t + 1)\}.$$

On donne ici quelques valeurs remarquables de c_r : $c_4 = 0,01\ldots > 0; c_{14} = 0,52\ldots > 1/2; c_{23} = 1,03\ldots > 1$. Notons aussi que $c_r \asymp r$ quand $r \to \infty$ et notamment $c_r \to \infty$.

Remarque. *Pour obtenir le théorème 6, il sera utile d'utiliser le résultat deux fois : en effet, si l'on note pour $C > 0$, r_C un nombre assez grand pour avoir $c_{r_C} > C$ et N_C un nombre assez grand pour pouvoir majorer $\Delta_{(A \mod p_i)_{i \leq r_C}}(n/2)$ (cf partie 2.3) où l'on a pris p_i le i-ième nombre premier, on aura alors*

$$\mathbb{P}(\exists D | A \text{ de degré } \in [n^\varepsilon, n/2]) = O_C(n^{-\varepsilon C})$$

en appliquant le résultat ci-dessus.

Mais en observant qu'on peut aussi majorer $\Delta_{(A \mod p_i)_{i \leq r_{C/\varepsilon}}}(\delta n)$ pour un δ qui dépend de C/ε, on obtient

$$\mathbb{P}(\exists D | A \text{ de degré } \in [n^\varepsilon, \delta n]) = O_{C,\varepsilon}(n^{-\varepsilon C/\varepsilon}) = O_{C,\varepsilon}(n^{-C}),$$

et séparément

$$\mathbb{P}(\exists D | A \text{ de degré } \in [\delta n, n/2]) = O_C((\delta n)^{-C}) = O_{C,\varepsilon}(n^{-C}),$$

ce qui permet d'obtenir une majoration globale en $O(n^{-C})$ plutôt que $O(n^{-\varepsilon C})$.

2.3 Majoration de $\Delta_{(A \mod p_i)_i}$

On va ici encore pour simplifier ne considérer qu'un seul facteur premier p. On a donc A un polynôme aléatoire de degré n à coefficients indépendants tirés selon les μ_j et on cherche à majorer

$$\Delta(m) := \sum_{B\in\mathbb{F}_p[X]^u, \deg B\leq m, X\nmid B} \left|\mathbb{P}(B|A \mod p) - p^{-\deg B}\right|.$$

Pour cela, remarquons que la condition $B|A \mod p$ correspond à l'annulation de certaines combinaisons linéaires des coefficients (indépendants) de $A \mod p$. On va alors pouvoir majorer $\left|\mathbb{P}(B|A \mod p) - p^{-\deg B}\right|$ via une analyse de Fourier.

Définissons alors $c_{-i}(F)$ le coefficient en X^{-i} d'une série de Laurent $F \in \mathbb{F}_p((X))/\mathbb{F}_p[X]$. On a alors pour tout B,

$$\mathbb{1}_{B|A} = \frac{1}{p^{\deg B}} \sum_{C\in\mathbb{F}_p[X]/(B)} e^{\frac{2i\pi}{p}c_{-1}(AC/B)}.$$

(En effet, $c_{-1}(AC/B)$ prendra chaque valeur de $\mathbb{F}_p$ le même nombre de fois lorsque C parcourt $\mathbb{F}_p[X]/(B)$, sauf lorsque $A \mod B = 0$.) Le choix ici de c_{-1} comme forme linéraire vers $\mathbb{F}_p$ sera utile plus tard.

En écrivant alors $\hat{\mu}_j(\theta) := \mathbb{E}(e^{2i\pi\theta a_j})$ la transformée de Fourier de μ_j (où $\theta \in \mathbb{R}/\mathbb{Z}$), et passant à l'espérance dans l'égalité ci-dessus, on obtient alors avec $A = \sum a_j X^j$,

$$\begin{aligned}
\mathbb{P}(B|A) - \frac{1}{p^{\deg B}} &= \frac{1}{p^{\deg B}} \sum_{C\in\mathbb{F}_p[X]/(B), C\neq 0} \mathbb{E}(e^{\frac{2i\pi}{p}c_{-1}(AC/B)}) && (C=0 \text{ donne le terme principal } \frac{1}{p^{\deg B}})\\
&= \frac{1}{p^{\deg B}} \sum_{C\in\mathbb{F}_p[X]/(B), C\neq 0} \mathbb{E}(e^{\frac{2i\pi}{p}\sum_{j=0}^n a_j c_{-1}(X^jC/B)})\\
&= \frac{1}{p^{\deg B}} \sum_{C\in\mathbb{F}_p[X]/(B), C\neq 0} \prod_{j=0}^n \mathbb{E}(e^{\frac{2i\pi}{p}a_j c_{-1}(X^jC/B)}) && \text{car les } a_j \text{ sont indépendants}\\
&= \frac{1}{p^{\deg B}} \sum_{C\in\mathbb{F}_p[X]/(B), C\neq 0} \prod_{j=0}^n \hat{\mu}_j\left(\frac{1}{p}c_{-1}(X^jC/B)\right)\\
&= \frac{1}{p^{\deg B}} \sum_{C\in\mathbb{F}_p[X]/(B), C\neq 0} \prod_{j=0}^n \hat{\mu}_j\left(\frac{1}{p}c_{-j-1}(C/B)\right).
\end{aligned}$$

Ici, le coefficient dominant de A est toujours égal à 1 ; on a donc $\hat{\mu}_n(t) = e^{2i\pi t}$ et $|\hat{\mu}_n(t)| = 1$ pour tout t. Ainsi, en sommant sur B et en appliquant l'inégalité triangulaire, on obtient pour tout m,

$$\begin{aligned}
\Delta_(m) &= \sum_{B\in\mathbb{F}_p[X]^u, \deg B\leq m, X\nmid B} \left|\mathbb{P}(B|A) - \frac{1}{p^{\deg B}}\right|\\
&\leq \sum_{B\in\mathbb{F}_p[X]^u, \deg B\leq m, X\nmid B} \frac{1}{p^{\deg B}} \sum_{C\in\mathbb{F}_p[X]/(B), C\neq 0} \prod_{j=0}^{n-1} \left|\hat{\mu}_j\left(\frac{c_{-j-1}(C/B)}{p}\right)\right|.
\end{aligned}$$

Il sera alors utile de regrouper les termes en fonction de la valeur de $C/B := (C_i/B_i)_i \in \mathbb{F}_p(X)/\mathbb{F}_p[X] := \mathcal{Q}$.

Pour $F \in \mathcal{Q}$, F s'écrit de manière unique $F = R/Q$ avec $Q \in \mathbb{F}_p[X]^u$ et $\deg R_i < \deg Q_i, R_i \wedge Q_i = 1$ pour tout i. Notons alors $\mathrm{den}(F) := Q$ son dénominateur.

Les valeurs de B, C donnant alors $C/B = F$ sont alors les $C = DR, B = DQ$ où $D \in \mathbb{F}_p[X]^u, \deg D + \deg Q \leq m$ et $X \nmid D, X \nmid Q = \mathrm{den}(F)$. On a aussi $F \neq 0$ (et donc $\deg \mathrm{den}\, F \neq 0$, puisque F est défini modulo 1) quand $C \neq 0$, d'où

$$\begin{aligned}
\Delta(m) &\leq \sum_{F\in\mathcal{Q}, F\neq 0, \deg \mathrm{den}(F)\leq m, X\nmid \mathrm{den}(F)} \sum_{D\in\mathbb{F}_p[X]^u, \deg D\leq m} \frac{1}{p^{\deg D} p^{\mathrm{den}(F)}} \prod_{j=0}^{n-1} \left|\hat{\mu}_j\left(\frac{c_{-j-1}(F)}{p}\right)\right|\\
&= (m+1)\sum_{l=1}^m p^{-l} \cdot \sum_{F\in\mathcal{Q}, \deg \mathrm{den}(F)=l, X\nmid \mathrm{den}(F)} \prod_{j=0}^{n-1} \left|\hat{\mu}_j\left(\frac{c_{-j-1}(F)}{p}\right)\right|\\
&=: (m+1)\sum_{l=1}^m p^{-l}\delta(l)
\end{aligned}$$

après avoir regroupé selon le degré du dénominateur de F.

Ici, les $\hat{\mu}_j(c/p)$ sont faibles lorsque μ_j est proche de l'uniformité modulo p : en effet lorsque μ est uniforme modulo p, on a $\hat{\mu}(c/p) = 0$ pour tout c (sauf pour $c = 0 \mod p$, pour lequel on obtient $\mu(0) = 1$ quelque soit μ). Lorsque μ est uniforme sur un segment de longueur n, on aura pour $\theta \neq 0$, $|\hat{\mu}(\theta)| \leq (N \sin(\pi\theta))^{-1}$ (et donc $|\hat{\mu}(c/p)| \leq (N \sin(\pi/p))^{-1}$), qui est bien très faible quand N assez grand.

On présente maintenant la majoration de $\delta(l)$. Avant cela, on donne un petit lemme assurant que les c_{-j} ne sont pas trop souvent nuls pour F non nul.

Lemme 14. *Soit $F \in \mathcal{Q}$ avec $\deg \operatorname{den}(F) = l$. Si $c_{-j}(F) = 0$ pour tout $1 \leq j \leq l$, alors $F = 0$.*

Démonstration. Si l'on écrit $F = R/Q$ avec Q unitaire et $\deg R < \deg Q = l$, on a $1/Q = X^{-l} + \dots$ puis si $R = r_j X^j + \dots$ de degré $0 \leq j < l$, on a $c_{-l+j}(F) = r_j \neq 0$. Ainsi, si $c_{-j}(F) = 0$ pour tout $1 \leq j \leq l$, alors $r = 0$ et $F = 0$. □

Lemme 15. *Soit $l \in \mathbb{N}$ et $(f_j)_{j<2l}$ un ensemble de fonctions de $\mathbb{R}/\mathbb{Z} \to \mathbb{R}_+$. On a alors*

$$\sum_{F \in \mathcal{Q}, \deg \operatorname{den}(F) = l} \prod_{j=0}^{2l-1} f_j(c_{-j-1}(F)/p) \leq \prod_{j=0}^{2l-1} \sum_{c \in \mathbb{Z}/p\mathbb{Z}} f_j(c/p).$$

Démonstration. On a

$$\prod_{j=0}^{2l-1} \sum_{c \in \mathbb{Z}/p\mathbb{Z}} f_j(c/p) = \sum_{c_{-1}, \dots, c_{-2l} \in \mathbb{Z}/p\mathbb{Z}} \prod_{j=0}^{2l-1} f_j(c_{-j-1}/p),$$

donc il suffit de prouver que

$$F \mapsto (c_{-j}(F))_{1 \leq j \leq 2l}$$

est injective lorsque F parcourt les éléments de $\mathbb{F}_p(X)/\mathbb{F}_p[X]$ tels que $\deg \operatorname{den}(F) = l$.

Or si $F, F' \in \mathbb{F}_p(X)/\mathbb{F}_p[X]$ avec $\deg \operatorname{den}(F) = \deg \operatorname{den}(F') = l$, on a $\operatorname{den}(F - F') | \operatorname{den}(F) \operatorname{den}(F')$ d'où $\deg \operatorname{den}(F - F') \leq 2l$. Ainsi, si $c_{-j}(F) = c_{-j}(F')$ pour tout $j \leq 2l$, on a $c_{-j}(F - F') = 0$ pour ces j puis $F = F'$ par le lemme 14 comme voulu. □

En appliquant à $f_j = \hat{\mu}_j$ (supposons $\mu_j = \mu$ pour tout j pour simplifier) et en majorant brutalement $|\hat{\mu}_j| \leq 1$ pour $2l \leq j < n$, on obtient alors lorsque $2l \leq n$,

$$\delta(l) \leq \left(\sum_{c \in \mathbb{Z}/p\mathbb{Z}} |\hat{\mu}(c/p)| \right)^{2l}.$$

Ainsi, si l'on arrive par ailleurs à majorer les $\delta(l)$ pour les l faibles (ce qu'on fera à la fin de cette sous-partie), on aura une bonne majoration de $\Delta(n/2) \leq (m+1) \sum_{l \leq m} p^{-l} \delta(l)$ lorsque

$$\sum_{c \in \mathbb{Z}/p\mathbb{Z}} |\hat{\mu}(c/p)| < \sqrt{p}$$

(on obtient en effet dans ce cas $p^{-l}\delta(l) \leq c^l = e^{-\varepsilon l}$ pour un $c = (\sum_{c \in \mathbb{Z}/p\mathbb{Z}} |\hat{\mu}(c/p)|)^2/p < 1$ et $\varepsilon = -\log c > 0$, dont la somme sur l converge.)

Remarque. *Lorsqu'on travaille avec r nombres premiers $p_1, \dots, p_r$ plutôt qu'un seul, la condition sur $\hat{\mu}$ doit être remplacée par la condition suivante : pour tous Q, R, l avec $QR = P = p_1 \dots p_r$, $Q > 1$ et $l \in \mathbb{Z}/R\mathbb{Z}$, on a*

$$\sum_{k \in \mathbb{Z}/Q\mathbb{Z}} |\hat{\mu}(k/Q + l/R)| < \sqrt{Q}.$$

En prenant le minimum possible $r = 4$ et $P = 2 \cdot 3 \cdot 5 \cdot 7 = 210$, cette condition est vérifiée pour μ uniforme sur un segment de longueur N dès que $N \geq 35$, ce qui permet d'obtenir le théorème 5.

Remarque. *Lorsque $2ls \leq n$ pour un $s \geq 1$, on peut obtenir en appliquant l'inégalité de Hölder puis le lemme 15 sur s segments disjoints de longueur $2l$ de $[1, n]$, une inégalité plus forte $\delta(l) \leq \left(\sum_{c \in \mathbb{Z}/p\mathbb{Z}} |\hat{\mu}(c/p)|^s \right)^{2l}$. Ainsi, lorsqu'on n'a pas la majoration en $\sqrt{Q}$ ci-dessus pour $\hat{\mu}$, en choisissant s assez grand pour avoir la condition cette condition pour $\hat{\mu}^s$, on arrive à majorer (en $e^{-\varepsilon l}$) $\delta(l)$ pour $l \leq n/2s$, ce qui permet d'obtenir une majoration de $\Delta(n/2s)$ et le théorème 4.*

On termine cette partie en expliquant comment majorer $\delta(l)$ lorsque l est petit. Pour cela, on exploite le fait que les $c_{-j-1}(F)$ ne s'annulent pas trop souvent lorsque $X \nmid \mathrm{den}(F)$. En effet, l'écriture en série de Laurent de F_i s'étend alors à l'infini avec des coefficients non nuls au moins tous les l termes (par le lemme 14 appliqué aux $X^j F$). Notons de plus qu'on a au plus p^{2l} fractions $F \in Q$ avec un dénominateur de degré l, on obtient alors

$$\delta(l) \leq p^{2l} \cdot \left(\max_{c \in \mathbb{Z}/p\mathbb{Z}, c \neq 0} |\hat{\mu}(c/p)| \right)^{n/l-1}$$

(notons qu'ici on a $\hat{\mu}(0) = 1$ mais $\max_{c \in \mathbb{Z}/p\mathbb{Z}, c \neq 0} |\hat{\mu}(c/p)| < 1$), ce qui fournit une majoration en $O(e^{-\varepsilon\sqrt{n}})$ de $p^{-l}\delta(l)$ lorsque $l \leq c\sqrt{n}$ pour des constantes $c, \varepsilon > 0$ (dépendant de μ et p). En utilisant la majoration en $e^{-\varepsilon' l}$ obtenue plus tôt pour $p^{-l}\delta(l)$ pour les $c\sqrt{n} < l \leq m$ (où $m = n/2$ ou $m = n/2s$ selon le cas), on arrive à

$$\Delta(m) = O(e^{-\varepsilon\sqrt{n}})$$

pour un $\varepsilon > 0$.

3 Une autre piste

On a ici commencé par réduire A modulo p pour se ramener à l'anneau principal (mieux compris) $\mathbb{F}_p[X]$. Une alternative aurait pu être de se ramener à $\mathbb{Z}$ en évaluant A en un entier a. Ainsi, si $A = I_1 \dots I_r$ fixé a r facteurs irréductibles, $A(a) = I_1(a) \dots I_r(a)$ aura (en moyenne sur a) r fois plus de facteurs premiers qu'un entier typique de cette forme (c'est-à-dire, $r/\log y$ facteurs premiers entre y et ey au lieu des habituels $\sum_{y \leq p \leq ey} 1/p \sim 1/\log y$ sous de bonnes conditions sur y). Cet aspect est au cœur de l'article de Breuillard et Varjù [4], qui prouvent par ailleurs qu'un facteur premier p arrive bien avec probabilité $1/p$ dans $A(a)$ lorsque A aléatoire (sauf lorsque p divise un polynôme cyclotomique de petit degré en a) et en déduisent ainsi qu'un polynôme aléatoire A est irréductible.

Références

[1] L. Bary-Soroker, D. Koukoulopoulos et G. Kozma. « Irreducibility of random polynomials : General measures ». In : *Inventiones Mathematica* 233 (2023), p. 1041-1120. URL : https://dms.umontreal.ca/~koukoulo/documents/publications/irreducible.pdf.

[2] L. Bary-Soroker et G. Kozma. « Irreducible polynomials of bounded height ». In : *Duke Mathematical Journal* 169.4 (2020), p. 579-598. DOI : 10.1215/00127094-2019-0047. URL : https://doi.org/10.1215/00127094-2019-0047.

[3] M. Bhargava. *Galois groups of random integer polynomials and van der Waerden's Conjecture*. 2022. arXiv : 2111.06507 [math.NT].

[4] E. Breuillard et P. P. Varjú. « Irreducibility of random polynomials of large degree ». In : *Acta Mathematica* 223.2 (2019), p. 195-249. DOI : 10.4310/ACTA.2019.v223.n2.a1. URL : https://doi.org/10.4310/ACTA.2019.v223.n2.a1.

[5] R. Dietmann. « On the distribution of Galois groups ». In : *Mathematika* 58.1 (2012), p. 35-44.

[6] E. Dobrowolski. « On a question of Lehmer and the number of irreducible factors of a polynomial ». In : *Acta Arithmetica* 34.4 (1979), p. 391-401. URL : https://www.impan.pl/en/publishing-house/journals-and-series/acta-arithmetica/all/34/4/102213/on-a-question-of-lehmer-and-the-number-of-irreducible-factors-of-a-polynomial.

[7] P. X. Gallagher. « On the distribution of primes in short intervals ». In : *Mathematika* 23.1 (1976), p. 4-9.

[8] S. Konyagin. « On the number of irreducible polynomials with 0,1 coefficients ». In : *Acta Arithmetica* 88.4 (1999), p. 333-350. URL : https://www.impan.pl/en/publishing-house/journals-and-series/acta-arithmetica/all/88/4/110736/on-the-number-of-irreducible-polynomials-with-0-1-coefficients.

[9] P. Meisner. *Erdős' Multiplication Table Problem for Function Fields and Symmetric Groups*. 2018. arXiv : 1804.08483 [math.NT].

[10] A. M. Odlyzko et B. Poonen. « Zeros of polynomials with 0,1 coefficients ». In : *L'Enseignement Mathématique* 39 (1993), p. 317-348. URL : https://www-users.cse.umn.edu/~odlyzko/doc/arch/polynomial.zeros.pdf.

[11] B.L. van der Waerden. « Die Seltenheit der Gleichungen mit Affekt ». In : *Mathematische Annalen* 109 (1934), p. 13-16. URL : http://eudml.org/doc/159666.