Biais de Tchebychev exceptionnels sur les corps finis

Alexandre Bailleul

ENS Paris-Saclay

Lundi 16 janvier 2023

Avec L. Devin, D. Keliher, W. Li

Organisation de l'exposé

1. Le biais de Tchebychev
2. Le cas des corps finis
3. Biais exceptionnels

Organisation de l'exposé

Le TNPPA

- Soit $a, q \in \mathbb{Z}$ premiers entre eux. On sait que

$$\pi(x; q, a) \underset{x \to +\infty}{\sim} \frac{1}{\varphi(q)} \operatorname{Li}(x) = \frac{1}{\varphi(q)} \int_2^x \frac{\mathrm{d}t}{\log t},$$

où

$$\pi(x; q, a) := \#\{p \leq x \mid p \equiv a \bmod q\}.$$

Le TNPPA

- Soit $a, q \in \mathbb{Z}$ premiers entre eux. On sait que

$$\pi(x; q, a) \underset{x \to +\infty}{\sim} \frac{1}{\varphi(q)} \operatorname{Li}(x) = \frac{1}{\varphi(q)} \int_2^x \frac{\mathrm{d}t}{\log t},$$

où

$$\pi(x; q, a) := \#\{p \leq x \mid p \equiv a \bmod q\}.$$

- Pour démontrer cela, on utilise les **fonctions L de Dirichlet** associées aux **caractères de Dirichlet** modulo q :

$$L(s, \chi) = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}$$

avec

$$\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times.$$

Le TNPPA

- On montre que $L(s,\chi)$ se prolonge à tout $\mathbb{C}$ avec éventuellement un pôle en 1. En reliant $\sum_{n\leq x}\Lambda(n)\chi(n)$ à la localisation des zéros de $L(s,\chi)$, on montre plus précisément que

$$\pi(x;q,a)=\frac{1}{\varphi(q)}\operatorname{Li}(x)+O_q(x\exp(-c_q\sqrt{\log x})).$$

Le TNPPA

- On montre que $L(s,\chi)$ se prolonge à tout $\mathbb{C}$ avec éventuellement un pôle en 1. En reliant $\sum_{n\leq x}\Lambda(n)\chi(n)$ à la localisation des zéros de $L(s,\chi)$, on montre plus précisément que

$$\pi(x;q,a)=\frac{1}{\varphi(q)}\operatorname{Li}(x)+O_q(x\exp(-c_q\sqrt{\log x})).$$

- L'**hypothèse de Riemann généralisée** pour ces fonctions est que si $L(s,\chi)=0$ et $\mathfrak{Re}(s)>0$, alors $\mathfrak{Re}(s)=\frac{1}{2}$. Elle équivaut à l'estimation

$$\pi(x;q,a)=\frac{1}{\varphi(q)}\operatorname{Li}(x)+O(\sqrt{x}\log(qx)).$$

Équirépartition

- Dans le TNPPA, le terme principal $\frac{1}{\varphi(q)}\operatorname{Li}(x)$ ne dépend pas de a : il y a **équirépartition** des p mod q dans $(\mathbb{Z}/q\mathbb{Z})^\times$.

Équirépartition

- Dans le TNPPA, le terme principal $\frac{1}{\varphi(q)} \operatorname{Li}(x)$ ne dépend pas de a : il y a **équirépartition** des p mod q dans $(\mathbb{Z}/q\mathbb{Z})^\times$.
- La taille du reste $\left|\pi(x;q,a) - \frac{1}{\varphi(q)} \operatorname{Li}(x)\right|$ (conjecturée ou démontrée) ne dépend pas non plus de a.

Équirépartition

- Dans le TNPPA, le terme principal $\frac{1}{\varphi(q)} \operatorname{Li}(x)$ ne dépend pas de a : il y a **équirépartition** des p mod q dans $(\mathbb{Z}/q\mathbb{Z})^\times$.
- La taille du reste $\left|\pi(x;q,a) - \frac{1}{\varphi(q)} \operatorname{Li}(x)\right|$ (conjecturée ou démontrée) ne dépend pas non plus de a.
- **Question :** Pour $a \neq b$, peut-on comparer malgré tout $\pi(x;q,a)$ et $\pi(x;q,b)$?

Le biais de Tchebychev

- En 1853, Tchebychev prétend dans une lettre que $\pi(x;4,3) > \pi(x;4,1)$ pour x suffisamment grand.

Le biais de Tchebychev

- En 1853, Tchebychev prétend dans une lettre que $\pi(x;4,3) > \pi(x;4,1)$ pour x suffisamment grand.

Tchebychev (lettre à Fuss, 1853).

« En cherchant l'expression limitative des fonctions qui déterminent la totalité des nombres premiers de la forme $4n+1$ et de ceux de la forme $4n+3$, pris au-dessous d'une limite très grande, je suis parvenu à reconnaître que ces deux fonctions diffèrent notablement entre elles par leurs seconds termes, dont la valeur, pour les nombres $4n+3$, est plus grande que celle pour les nombres $4n+1$ [...] »

Le biais de Tchebychev

- En 1853, Tchebychev prétend dans une lettre que $\pi(x;4,3) > \pi(x;4,1)$ pour x suffisamment grand.

Tchebychev (lettre à Fuss, 1853).

« En cherchant l'expression limitative des fonctions qui déterminent la totalité des nombres premiers de la forme $4n+1$ et de ceux de la forme $4n+3$, pris au-dessous d'une limite très grande, je suis parvenu à reconnaître que ces deux fonctions diffèrent notablement entre elles par leurs seconds termes, dont la valeur, pour les nombres $4n+3$, est plus grande que celle pour les nombres $4n+1$ [...] »

- L'affirmation de Tchebychev n'est en réalité pas correcte : Littlewood a montré en 1914 que

$$\pi(x;4,3) - \pi(x;4,1) = \Omega_{\pm}\left(x^{1/2}\frac{\log\log\log x}{\log x}\right).$$

Le biais de Tchebychev

- En 1853, Tchebychev prétend dans une lettre que $\pi(x;4,3) > \pi(x;4,1)$ pour x suffisamment grand.

Tchebychev (lettre à Fuss, 1853).

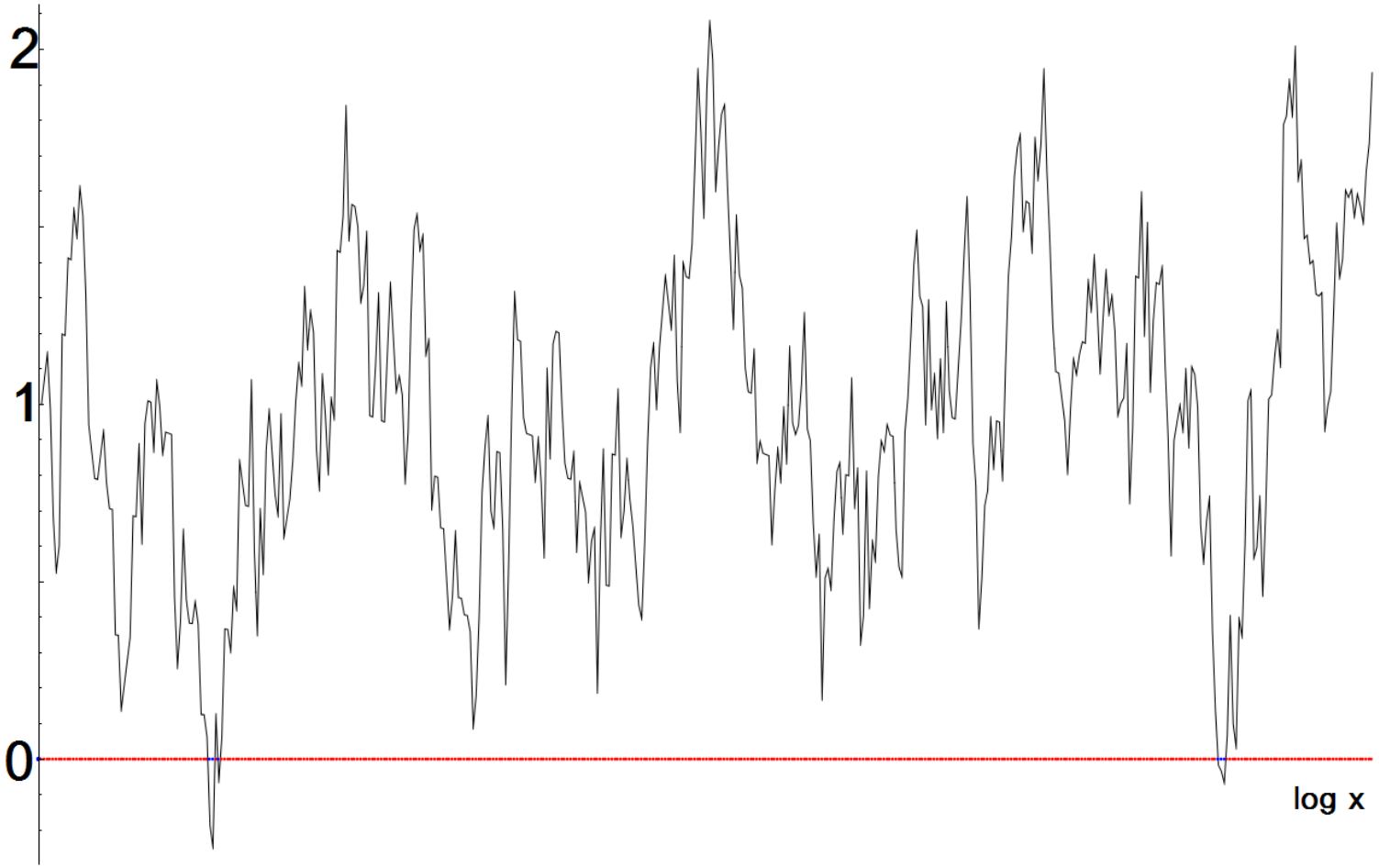
« En cherchant l'expression limitative des fonctions qui déterminent la totalité des nombres premiers de la forme $4n+1$ et de ceux de la forme $4n+3$, pris au-dessous d'une limite très grande, je suis parvenu à reconnaître que ces deux fonctions diffèrent notablement entre elles par leurs seconds termes, dont la valeur, pour les nombres $4n+3$, est plus grande que celle pour les nombres $4n+1$ [...] »

- L'affirmation de Tchebychev n'est en réalité pas correcte : Littlewood a montré en 1914 que

$$\pi(x;4,3) - \pi(x;4,1) = \Omega_{\pm}\left(x^{1/2}\frac{\log\log\log x}{\log x}\right).$$

Mais elle se vérifie numériquement, il semble y avoir « la plupart du temps » l'inégalité $\pi(x;4,3) > \pi(x;4,1)$.

Le biais de Tchebychev



$$\frac{\pi(x;4,3)-\pi(x;4,1)}{\sqrt{x}/\log x}, 10^4 \leq x \leq 10^8$$

(Daniel Fiorilli)

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Dans la « course » entre les premiers $p \equiv 3$ mod 4 et les premiers $p \equiv 1$ mod 4, qui est en tête le plus souvent ?

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Dans la « course » entre les premiers $p \equiv 3$ mod 4 et les premiers $p \equiv 1$ mod 4, qui est en tête le plus souvent ?

- **Conjecture (Knapowski-Turán, 1962) :**

$$d(\mathcal{P}_{4;3,1}) := \lim_{X \to +\infty} \frac{\#\mathcal{P}_{4;3,1} \cap [2, X]}{X} = 1.$$

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Dans la « course » entre les premiers $p \equiv 3$ mod 4 et les premiers $p \equiv 1$ mod 4, qui est en tête le plus souvent ?

- **Conjecture (Knapowski-Turán, 1962) :**

$$d(\mathcal{P}_{4;3,1}) := \lim_{X \to +\infty} \frac{\#\mathcal{P}_{4;3,1} \cap [2, X]}{X} = 1.$$

- **Kaczorowski, 1995 :** Si $L(s, \chi_4)$ vérifie GRH (hypothèse de Riemann généralisée), alors

$$\underline{d}(\mathcal{P}_{4;3,1}) < 0,9594595\ldots$$

et

$$\overline{d}(\mathcal{P}_{4;3,1}) > 0,999989360\ldots$$

Le biais de Tchebychev

On souhaite estimer la « taille » de

$$\mathcal{P}_{4;3,1} := \{x \geq 2 \mid \pi(x;4,3) > \pi(x;4,1)\}.$$

Dans la « course » entre les premiers $p \equiv 3$ mod 4 et les premiers $p \equiv 1$ mod 4, qui est en tête le plus souvent ?

- **Conjecture (Knapowski-Turán, 1962) :**

$$d(\mathcal{P}_{4;3,1}) := \lim_{X \to +\infty} \frac{\#\mathcal{P}_{4;3,1} \cap [2, X]}{X} = 1.$$

- **Kaczorowski, 1995 :** Si $L(s, \chi_4)$ vérifie GRH (hypothèse de Riemann généralisée), alors

$$\underline{d}(\mathcal{P}_{4;3,1}) < 0,9594595\ldots$$

et

$$\overline{d}(\mathcal{P}_{4;3,1}) > 0,999989360\ldots$$

- **Rubinstein-Sarnak, 1994 :** Si $L(s, \chi_4)$ vérifie GRH et LI (indépendance linéaire),

$$\delta(\mathcal{P}_{4;3,1}) := \lim_{X \to +\infty} \frac{1}{\log X} \int_2^X \mathbf{1}_{\mathcal{P}_{4;3,1}}(t) \frac{\mathrm{d}t}{t}$$

existe et $\delta(\mathcal{P}_{4;3,1}) \approx 0,9959\ldots$

Les résultats de Rubinstein et Sarnak

Si les caractères de Dirichlet modulo q vérifient LI et GRH alors :

- Si $a \equiv \square \bmod q$ et $b \equiv \square \bmod q$, ou si $a \equiv \boxtimes \bmod q$ et $b \equiv \boxtimes \bmod q$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.

Les résultats de Rubinstein et Sarnak

Si les caractères de Dirichlet modulo q vérifient LI et GRH alors :

- Si $a \equiv \square \bmod q$ et $b \equiv \square \bmod q$, ou si $a \equiv \boxtimes \bmod q$ et $b \equiv \boxtimes \bmod q$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.

- Si $a \equiv \boxtimes \bmod q$ et $b \equiv \square \bmod q$ alors $\frac{1}{2} < \delta(\mathcal{P}_{q;a,b}) < 1$.

Les résultats de Rubinstein et Sarnak

Si les caractères de Dirichlet modulo q vérifient LI et GRH alors :

- Si $a \equiv \square \bmod q$ et $b \equiv \square \bmod q$, ou si $a \equiv \boxtimes \bmod q$ et $b \equiv \boxtimes \bmod q$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.
- Si $a \equiv \boxtimes \bmod q$ et $b \equiv \square \bmod q$ alors $\frac{1}{2} < \delta(\mathcal{P}_{q;a,b}) < 1$.
- Si q est de la forme p^α ou $2p^\alpha$, alors $\frac{1}{2} < \delta(\mathcal{P}_{q;NR,R}) < 1$, où

$$\mathcal{P}_{q;NR,R} := \{x \geq 2 \mid \pi(x;q,NR) > \pi(x;q,R)\},$$

$$\pi(x;q,R) = \#\{p \leq x \mid p \equiv \square \bmod q\}$$

et

$$\pi(x;q,NR) = \#\{p \leq x \mid p \equiv \boxtimes \bmod q\}.$$

L'hypothèse LI

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma \geq 0 \mid \exists \chi \text{ caractère de Dirichlet mod } q, L\left(\frac{1}{2}+i\gamma, \chi\right)=0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

L'hypothèse LI

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma \geq 0 \mid \exists \chi \text{ caractère de Dirichlet mod } q, L\left(\frac{1}{2}+i\gamma, \chi\right)=0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

Elle est utilisée avec le **Théorème de Kronecker-Weyl :** Si $\gamma_1, \ldots, \gamma_n$ sont des réels alors le groupe à un paramètre $\left\{\left(e^{i\gamma_1 x}, \ldots, e^{i\gamma_n x}\right) \mid x \in \mathbb{R}\right\}$ est équiréparti dans un tore de dimension $\dim_{\mathbb{Q}} \operatorname{Vect}(\gamma_1, \ldots, \gamma_n)$.

L'hypothèse LI

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma \geq 0 \mid \exists \chi \text{ caractère de Dirichlet mod } q, L\left(\frac{1}{2}+i\gamma, \chi\right)=0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

Elle est utilisée avec le **Théorème de Kronecker-Weyl :** Si $\gamma_1, \ldots, \gamma_n$ sont des réels alors le groupe à un paramètre $\left\{\left(e^{i\gamma_1 x}, \ldots, e^{i\gamma_n x}\right) \mid x \in \mathbb{R}\right\}$ est équiréparti dans un tore de dimension $\dim_{\mathbb{Q}} \operatorname{Vect}(\gamma_1, \ldots, \gamma_n)$. En particulier si les γ_j sont linéairement indépendants sur $\mathbb{Q}$, alors les $e^{i\gamma_j x}$ se comportent comme des variables aléatoires **indépendantes** uniformes sur le cercle.

L'hypothèse LI

Conjecture (LI).

Le (multi)-ensemble $\left\{\gamma \geq 0 \mid \exists \chi \text{ caractère de Dirichlet mod } q, L\left(\frac{1}{2}+i\gamma, \chi\right)=0\right\}$ est linéairement indépendant sur $\mathbb{Q}$.

Elle est utilisée avec le **Théorème de Kronecker-Weyl :** Si $\gamma_1, \ldots, \gamma_n$ sont des réels alors le groupe à un paramètre $\left\{\left(e^{i\gamma_1 x}, \ldots, e^{i\gamma_n x}\right) \mid x \in \mathbb{R}\right\}$ est équiréparti dans un tore de dimension $\dim_{\mathbb{Q}} \operatorname{Vect}(\gamma_1, \ldots, \gamma_n)$. En particulier si les γ_j sont linéairement indépendants sur $\mathbb{Q}$, alors les $e^{i\gamma_j x}$ se comportent comme des variables aléatoires **indépendantes** uniformes sur le cercle.

Utilisation d'une **formule explicite** :

$$\frac{\pi(e^x; q, a) - \pi(e^x; q, b)}{e^{x/2}/x} = \#\sqrt{\{b\}} - \#\sqrt{\{a\}} + \sum_{\chi \in X_q} \overline{\chi(b) - \chi(a)} \sum_{\gamma_\chi} \frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi} + O\left(\frac{1}{x}\right).$$

Organisation de l'exposé

Courses de polynômes irréductibles

- Soit $M \in \mathbb{F}_q[T]$ non constant et $A \in \mathbb{F}_q[T]$ premier avec M. Alors

$$\pi(n; M, A) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid \deg P \leq n, P \equiv A \bmod M\}$$
$$\underset{n \to +\infty}{\sim} \frac{q^n}{\varphi(M)n}.$$

Courses de polynômes irréductibles

- Soit $M \in \mathbb{F}_q[T]$ non constant et $A \in \mathbb{F}_q[T]$ premier avec M. Alors

$$\Pi(X; M, A) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid |P| = q^{\deg P} \leq X = q^n, P \equiv A \bmod M\}$$
$$\underset{X \to +\infty}{\sim} \frac{1}{\varphi(M)} \frac{X}{\log_q X}.$$

Courses de polynômes irréductibles

- Soit $M \in \mathbb{F}_q[T]$ non constant et $A \in \mathbb{F}_q[T]$ premier avec M. Alors

$$\pi(n; M, A) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid \deg P \leq n, P \equiv A \bmod M\}$$
$$\underset{n \to +\infty}{\sim} \frac{q^n}{\varphi(M)n}.$$

- On définit

$$\pi(n; M, \square) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid \deg P = n, P \equiv \square \bmod M\},$$

Courses de polynômes irréductibles

- Soit $M \in \mathbb{F}_q[T]$ non constant et $A \in \mathbb{F}_q[T]$ premier avec M. Alors

$$\pi(n; M, A) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid \deg P \leq n, P \equiv A \bmod M\}$$
$$\underset{n \to +\infty}{\sim} \frac{q^n}{\varphi(M)n}.$$

- On définit

$$\pi(n; M, \square) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid \deg P = n, P \equiv \square \bmod M\},$$

$$\mathcal{P}_{M;\boxtimes,\square} = \{X \geq 1 \mid \pi(X; M, \boxtimes) > \pi(X; M, \square)\}$$

Courses de polynômes irréductibles

- Soit $M \in \mathbb{F}_q[T]$ non constant et $A \in \mathbb{F}_q[T]$ premier avec M. Alors

$$\pi(n; M, A) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid \deg P \leq n, P \equiv A \bmod M\}$$
$$\underset{n \to +\infty}{\sim} \frac{q^n}{\varphi(M)n}.$$

- On définit

$$\pi(n; M, \square) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid \deg P = n, P \equiv \square \bmod M\},$$

$$\mathcal{P}_{M;\boxtimes,\square} = \{X \geq 1 \mid \pi(X; M, \boxtimes) > \pi(X; M, \square)\}$$

et, quand elle existe, $d(\mathcal{P}_{M;\boxtimes,\square}) := \lim_{X \to +\infty} \frac{1}{X} \#(\mathcal{P}_{M;\boxtimes,\square} \cap [\![1, X]\!])$ sa densité naturelle.

Courses de polynômes irréductibles

- Soit $M \in \mathbb{F}_q[T]$ non constant et $A \in \mathbb{F}_q[T]$ premier avec M. Alors

$$\pi(n; M, A) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid \deg P \leq n, P \equiv A \bmod M\}$$
$$\underset{n \to +\infty}{\sim} \frac{q^n}{\varphi(M) n}.$$

- On définit

$$\pi(n; M, \square) := \#\{P \in \mathbb{F}_q[T] \text{ irréductible} \mid \deg P = n, P \equiv \square \bmod M\},$$

$$\mathcal{P}_{M;\boxtimes,\square} = \{X \geq 1 \mid \pi(X; M, \boxtimes) > \pi(X; M, \square)\}$$

et, quand elle existe, $d(\mathcal{P}_{M;\boxtimes,\square}) := \lim_{X \to +\infty} \frac{1}{X} \#(\mathcal{P}_{M;\boxtimes,\square} \cap [\![1, X]\!])$ sa densité naturelle.

Théorème (Cha, 2008).

Soit $M \in \mathbb{F}_q[T]$ irréductible. Supposons LI_π pour les zéros des fonctions L de Dirichlet modulo M. Alors $d(\mathcal{P}_{M;\boxtimes,\square})$ existe et on a

$$1/2 < d(\mathcal{P}_{M;\boxtimes,\square}) < 1.$$

L'hypothèse LI_π

Théorème (Weil, 1940).

Pour tout caractère de Dirichlet primitif χ modulo $M \in \mathbb{F}_q[T]$, la fonction

$$L(s,\chi) = \sum_{A \in \mathbb{F}_q[T]} \frac{\chi(A)}{|A|^s} = \sum_{A \in \mathbb{F}_q[T]} \frac{\chi(A)}{q^{s \deg A}}$$

est un polynôme à coefficients entiers en $u = q^{-s}$:

$$\mathcal{L}(u,\chi) := L(s,\chi) = \prod_{j=1}^{M(\chi)} (1 - \alpha_j(\chi) u) \quad \text{avec } |\alpha_j(\chi)| = q^{1/2}.$$

L'hypothèse LI_π

Théorème (Weil, 1940).

Pour tout caractère de Dirichlet primitif χ modulo $M \in \mathbb{F}_q[T]$, la fonction

$$L(s,\chi) = \sum_{A \in \mathbb{F}_q[T]} \frac{\chi(A)}{|A|^s} = \sum_{A \in \mathbb{F}_q[T]} \frac{\chi(A)}{q^{s \deg A}}$$

est un polynôme à coefficients entiers en $u = q^{-s}$:

$$\mathcal{L}(u,\chi) := L(s,\chi) = \prod_{j=1}^{M(\chi)} (1 - \alpha_j(\chi) u) \quad \text{avec } |\alpha_j(\chi)| = q^{1/2}.$$

Conjecture (LI_π).

Pour tout caractère de Dirichlet primitif χ modulo M et $1 \leq j \leq M(\chi)$, on note $\alpha_j(\chi) = \sqrt{q} e^{i\theta_j(\chi)}$. Le (multi)-ensemble $(\{\theta_j(\chi) \mid \chi \in X_M^*, 1 \leq j \leq M(\chi)\} \cap]0,\pi[) \cup \{\pi\}$ est linéairement indépendant sur $\mathbb{Q}$.

À propos de LI_π

- LI_π n'est **pas toujours vraie**

À propos de LI_π

- LI_π n'est **pas toujours vraie** :
  - Exemple (Cha) : $p = 5$, $M = T^5 + 3T^4 + 4T^3 + 2T + 2$ et χ_M le symbole de Legendre modulo M. Alors $\mathcal{L}(u, \chi_M) = 25u^4 - 25u^3 + 15u^2 - 5u + 1$ avec $\alpha_1 = \sqrt{5}e^{\frac{2i\pi}{5}}, \alpha_2 = \sqrt{5}e^{\frac{4i\pi}{5}}$ et on a $d(\mathcal{P}_{M;\boxtimes,\square}) \approx 40\% < \frac{1}{2}$.

À propos de LI_π

- LI_π n'est **pas toujours vraie** :
  - Exemple (Cha) : $p = 5$, $M = T^5 + 3T^4 + 4T^3 + 2T + 2$ et χ_M le symbole de Legendre modulo M. Alors $\mathcal{L}(u, \chi_M) = 25u^4 - 25u^3 + 15u^2 - 5u + 1$ avec $\alpha_1 = \sqrt{5}e^{\frac{2i\pi}{5}}, \alpha_2 = \sqrt{5}e^{\frac{4i\pi}{5}}$ et on a $d(\mathcal{P}_{M;\boxtimes,\square}) \approx 40\% < \frac{1}{2}$.
  - Exemple (Devin-Meng) : $q = 9$, $M = T^4 + 2T^3 + 2T + a^7$ où $\mathbb{F}_9 = \mathbb{F}_3(a)$. Alors $\mathcal{L}(u, \chi_M) = (1 - 3u)^2$, où χ_M est le caractère quadratique primitif modulo M, et on a $d(\mathcal{P}_{M;\boxtimes,\square}) = 1$.

À propos de LI_π

- LI_π n'est **pas toujours vraie** :
  - Exemple (Cha) : $p = 5$, $M = T^5 + 3T^4 + 4T^3 + 2T + 2$ et χ_M le symbole de Legendre modulo M. Alors $\mathcal{L}(u, \chi_M) = 25u^4 - 25u^3 + 15u^2 - 5u + 1$ avec $\alpha_1 = \sqrt{5}e^{\frac{2i\pi}{5}}, \alpha_2 = \sqrt{5}e^{\frac{4i\pi}{5}}$ et on a $d(\mathcal{P}_{M;\boxtimes,\square}) \approx 40\% < \frac{1}{2}$.
  - Exemple (Devin-Meng) : $q = 9$, $M = T^4 + 2T^3 + 2T + a^7$ où $\mathbb{F}_9 = \mathbb{F}_3(a)$. Alors $\mathcal{L}(u, \chi_M) = (1 - 3u)^2$, où χ_M est le caractère quadratique primitif modulo M, et on a $d(\mathcal{P}_{M;\boxtimes,\square}) = 1$.
  - Exemple (Cha) : $p = 3$, $M = T^3 + 2T + 1$ et χ_M le symbole de Legendre modulo M. Alors $\mathcal{L}(u, \chi_M) = 3u^2 - 3u + 1 = \left(1 - \sqrt{3}e^{\frac{i\pi}{6}}\right)\left(1 - \sqrt{3}e^{\frac{-i\pi}{6}}\right)$ et on a $d(\mathcal{P}_{M;\boxtimes,\square}) \approx 58,3\% > \frac{1}{2}$.

La borne de Kowalski

Théorème (Kowalski, 2008).

Soit $f \in \mathbb{Z}[T]$ unitaire sans facteur carré de degré $2g, g \geq 1$. Alors pour tout p premier impair ne divisant pas $\mathrm{disc}(f)$ et q puissance de p,

$$\frac{1}{q}\#\{t \in \mathbb{F}_q \setminus Z(f) \mid \mathcal{L}(u, \chi_{f(X)(X-t)}) \text{ ne satisfait pas } \mathsf{LI}_\pi\} \ll_g \frac{(\log q)^{1-\frac{1}{4g}}}{q^{\frac{1}{2A}}}$$

où $\chi_{f(X)(X-t)}$ est le caractère quadratique primitif modulo $f(X)(X-t)$, et $A = 2g^2 + g + 2$.

Idées de preuve

- Etape 1 : Si $\mathcal{L}(u, \chi_{f(T)(T-t)})$ ne satisfait pas LI_π, alors le groupe de Galois G de $\mathcal{L}(u, \chi_{f(T)(T-t)})$ n'est pas maximal ($\subsetneq W_{2g} = \mathfrak{S}_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g$, méthode de Girstmair).

Idées de preuve

- Etape 1 : Si $\mathcal{L}(u, \chi_{f(T)(T-t)})$ ne satisfait pas LI_π, alors le groupe de Galois G de $\mathcal{L}(u, \chi_{f(T)(T-t)})$ n'est pas maximal ($\subsetneq W_{2g} = \mathfrak{S}_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g$, méthode de Girstmair).

- Etape 2 : On en déduit que ou bien G n'agit pas transitivement sur les racines, ou bien G ne contient pas de transposition, ou bien la projection $p(G)$ de G sur $\mathfrak{S}_g$ ne contient pas de transposition, ou bien $p(G)$ ne contient pas de m-cycle avec $m > g/2$ premier.

Idées de preuve

- Etape 1 : Si $\mathcal{L}(u, \chi_{f(T)(T-t)})$ ne satisfait pas LI_π, alors le groupe de Galois G de $\mathcal{L}(u, \chi_{f(T)(T-t)})$ n'est pas maximal ($\subsetneq W_{2g} = \mathfrak{S}_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g$, méthode de Girstmair).

- Etape 2 : On en déduit que ou bien G n'agit pas transitivement sur les racines, ou bien G ne contient pas de transposition, ou bien la projection $p(G)$ de G sur $\mathfrak{S}_g$ ne contient pas de transposition, ou bien $p(G)$ ne contient pas de m-cycle avec $m > g/2$ premier.

- Etape 3 : Le grand crible de Kowalski et une technique de Chavdarov donnent une majoration en
$$\ll_g H_1^{-1} + H_2^{-1} + H_3^{-1} + H_4^{-1},$$
où les H_i s'estiment en comptant les polynômes $P \in \mathbb{F}_\ell[T], \ell \neq 2, p$ premier, vérifiant des conditions correspondant aux quatre conditions du point 2).

Idées de preuve

- Etape 1 : Si $\mathcal{L}(u, \chi_{f(T)(T-t)})$ ne satisfait pas LI_π, alors le groupe de Galois G de $\mathcal{L}(u, \chi_{f(T)(T-t)})$ n'est pas maximal ($\subsetneq W_{2g} = \mathfrak{S}_g \ltimes (\mathbb{Z}/2\mathbb{Z})^g$, méthode de Girstmair).

- Etape 2 : On en déduit que ou bien G n'agit pas transitivement sur les racines, ou bien G ne contient pas de transposition, ou bien la projection $p(G)$ de G sur $\mathfrak{S}_g$ ne contient pas de transposition, ou bien $p(G)$ ne contient pas de m-cycle avec $m > g/2$ premier.

- Etape 3 : Le grand crible de Kowalski et une technique de Chavdarov donnent une majoration en
$$\ll_g H_1^{-1} + H_2^{-1} + H_3^{-1} + H_4^{-1},$$
où les H_i s'estiment en comptant les polynômes $P \in \mathbb{F}_\ell[T], \ell \neq 2, p$ premier, vérifiant des conditions correspondant aux quatre conditions du point 2).

- Etape 4 : On termine en utilisant des estimations de théorie analytique des nombres (minoration de sommes de fonctions multiplicatives sur les entiers sans facteurs carrés par Lau-Wu).

Organisation de l'exposé

1. Le biais de Tchebychev
2. Le cas des corps finis
3. **Biais exceptionnels**

Quelques notations

- À partir de maintenant,
  $\mathcal{H}_n(\mathbb{F}_q) := \{f \in \mathbb{F}_q[T] \mid f$ unitaire sans facteur carré de degré $n\}$ et pour $f \in \mathcal{H}_n(\mathbb{F}_q)$, χ_f désigne le caractère quadratique primitif modulo f. On note $g = \left\lfloor \frac{n-1}{2} \right\rfloor$ le genre de la courbe $y^2 = f$.

Quelques notations

- À partir de maintenant,
  $\mathcal{H}_n(\mathbb{F}_q) := \{f \in \mathbb{F}_q[T] \mid f \text{ unitaire sans facteur carré de degré } n\}$ et pour $f \in \mathcal{H}_n(\mathbb{F}_q)$, χ_f désigne le caractère quadratique primitif modulo f. On note $g = \left\lfloor \frac{n-1}{2} \right\rfloor$ le genre de la courbe $y^2 = f$.

- On s'intéresse au signe de

$$\begin{aligned}\Pi(n;\chi_f) := \frac{n}{q^{n/2}} \Big(&\#\{h \in \mathbb{F}_q[t] \mid \chi_f(h) = 1, h \text{ irréductible et } \deg h = n\} \\ &- \#\{h \in \mathbb{F}_q[t] \mid \chi_f(h) = -1, h \text{ irréductible et } \deg h = n\} \Big) \\ = \frac{n}{q^{n/2}} &\sum_{\substack{\deg h = n \\ h \text{ irréductible}}} \chi_f(h).\end{aligned}$$

Quelques notations

- À partir de maintenant,
  $\mathcal{H}_n(\mathbb{F}_q) := \{f \in \mathbb{F}_q[T] \mid f \text{ unitaire sans facteur carré de degré } n\}$ et pour $f \in \mathcal{H}_n(\mathbb{F}_q)$, χ_f désigne le caractère quadratique primitif modulo f. On note $g = \left\lfloor \frac{n-1}{2} \right\rfloor$ le genre de la courbe $y^2 = f$.

- On s'intéresse au signe de

$$\begin{aligned}\Pi(n;\chi_f) := \frac{n}{q^{n/2}}\Big(&\#\{h \in \mathbb{F}_q[t] \mid \chi_f(h) = 1, h \text{ irréductible et } \deg h = n\} \\ &- \#\{h \in \mathbb{F}_q[t] \mid \chi_f(h) = -1, h \text{ irréductible et } \deg h = n\}\Big) \\ = \frac{n}{q^{n/2}} &\sum_{\substack{\deg h = n \\ h \text{ irréductible}}} \chi_f(h).\end{aligned}$$

- Quand f est irréductible, c'est le signe de $\pi(n; f, \square) - \pi(n; f, \boxtimes)$!

Formules explicites

- On dispose de **formules explicites** pour les quantités telles que $\Pi(n; \chi_f)$:

Formules explicites

- On dispose de **formules explicites** pour les quantités telles que $\Pi(n;\chi_f)$:

$$\Pi(n;\chi_f) = -\left(m_0(\chi_f)+\tfrac{1}{2}\right) - \left(m_\pi(\chi_f)+\tfrac{1}{2}\right)(-1)^n - \sum_{\theta_j\neq 0,\pi} m_{\theta_j}(\chi_f)e^{in\theta_j(\chi_f)} + O_f\left(q^{-\frac{n}{6}}\right),$$

où $m_\theta(\chi_f)$ désigne la multiplicité de $\sqrt{q}e^{i\theta}$ comme zéro de $\mathcal{L}(u,\chi_f)$.

Formules explicites

- On dispose de **formules explicites** pour les quantités telles que $\Pi(n;\chi_f)$:

$$\Pi(n;\chi_f) = -\left(m_0(\chi_f)+\tfrac{1}{2}\right) - \left(m_\pi(\chi_f)+\tfrac{1}{2}\right)(-1)^n - \sum_{\theta_j\neq 0,\pi} m_{\theta_j}(\chi_f)e^{in\theta_j(\chi_f)} + O_f\left(q^{-\frac{n}{6}}\right),$$

  où $m_\theta(\chi_f)$ désigne la multiplicité de $\sqrt{q}e^{i\theta}$ comme zéro de $\mathcal{L}(u,\chi_f)$.
- On pose

$$\Delta_f(n) := \left(m_0(\chi_f)+\tfrac{1}{2}\right) + \left(m_\pi(\chi_f)+\tfrac{1}{2}\right)(-1)^n + \sum_{\theta_j\neq 0,\pi} m_{\theta_j}(\chi_f)e^{in\theta_j(\chi_f)}.$$

Formules explicites

- On dispose de **formules explicites** pour les quantités telles que $\Pi(n;\chi_f)$:

$$\Pi(n;\chi_f) = -\left(m_0(\chi_f)+\tfrac{1}{2}\right) - \left(m_\pi(\chi_f)+\tfrac{1}{2}\right)(-1)^n - \sum_{\theta_j\neq 0,\pi} m_{\theta_j}(\chi_f)e^{in\theta_j(\chi_f)} + O_f\left(q^{-\frac{n}{6}}\right),$$

où $m_\theta(\chi_f)$ désigne la multiplicité de $\sqrt{q}e^{i\theta}$ comme zéro de $\mathcal{L}(u,\chi_f)$.

- On pose

$$\Delta_f(n) := \left(m_0(\chi_f)+\tfrac{1}{2}\right) + \left(m_\pi(\chi_f)+\tfrac{1}{2}\right)(-1)^n + \sum_{\theta_j\neq 0,\pi} m_{\theta_j}(\chi_f)e^{in\theta_j(\chi_f)}.$$

Si LI_π est vraie, Δ_f oscille harmonieusement autour de sa moyenne $m_0(\chi_f)+\frac{1}{2} > 0$!

Formules explicites

- On dispose de **formules explicites** pour les quantités telles que $\Pi(n;\chi_f)$:

$$\Pi(n;\chi_f) = -\left(m_0(\chi_f)+\tfrac{1}{2}\right) - \left(m_\pi(\chi_f)+\tfrac{1}{2}\right)(-1)^n - \sum_{\theta_j\neq 0,\pi} m_{\theta_j}(\chi_f)e^{in\theta_j(\chi_f)} + O_f\left(q^{-\frac{n}{6}}\right),$$

où $m_\theta(\chi_f)$ désigne la multiplicité de $\sqrt{q}e^{i\theta}$ comme zéro de $\mathcal{L}(u,\chi_f)$.

- On pose

$$\Delta_f(n) := \left(m_0(\chi_f)+\tfrac{1}{2}\right) + \left(m_\pi(\chi_f)+\tfrac{1}{2}\right)(-1)^n + \sum_{\theta_j\neq 0,\pi} m_{\theta_j}(\chi_f)e^{in\theta_j(\chi_f)}.$$

Si LI_π est vraie, Δ_f oscille harmonieusement autour de sa moyenne $m_0(\chi_f)+\frac{1}{2} > 0$! On s'attend donc à ce que $\Pi(n;\chi_f)$ soit strictement négatif plus de la moitié du temps.

Biais complet

Théorème (B.-Devin-Keliher-Li, 2022, "Biais complet").

On a

$$\frac{1}{\#\mathcal{H}_n(\mathbb{F}_q)}\#\{f \in \mathcal{H}_n(\mathbb{F}_q) \mid d(\Delta_f > 0) = 1\} \ll_{g,p} \frac{\log q}{q^{1/A}}$$

où $A = 2g^2 + g + 2$.

Biais complet

- Etape 1 : Si $d(\Delta_f > 0) = 1$, alors $d(\Delta_f(2n) > 0) = d(\Delta_f(2n+1) > 0) = 1$, et à l'aide d'une inégalité de variance, on montre que $m_0(\chi_f) > m_\pi(\chi_f)$ (et en particulier q est un carré).

Biais complet

- Etape 1 : Si $d(\Delta_f > 0) = 1$, alors $d(\Delta_f(2n) > 0) = d(\Delta_f(2n+1) > 0) = 1$, et à l'aide d'une inégalité de variance, on montre que $m_0(\chi_f) > m_\pi(\chi_f)$ (et en particulier q est un carré).

- Etape 2 : Majoration
$\#\{f \in \mathcal{H}_n(\mathbb{F}_q) \mid d(\Delta_f > 0) = 1\} \leq \#\{f \in \mathcal{H}_n(\mathbb{F}_q) \mid m_0(\chi_f) > 0\}$.

Biais complet

- Etape 1 : Si $d(\Delta_f > 0) = 1$, alors $d(\Delta_f(2n) > 0) = d(\Delta_f(2n+1) > 0) = 1$, et à l'aide d'une inégalité de variance, on montre que $m_0(\chi_f) > m_\pi(\chi_f)$ (et en particulier q est un carré).

- Etape 2 : Majoration
$\#\{f \in \mathcal{H}_n(\mathbb{F}_q) \mid d(\Delta_f > 0) = 1\} \leq \#\{f \in \mathcal{H}_n(\mathbb{F}_q) \mid m_0(\chi_f) > 0\}$.

- Etape 3 : On utilise une version améliorée du grand crible de Kowalski, avec espace de paramètres $\mathcal{H}_n(\mathbb{F}_q)$, pour se ramener au comptage de

$$\left\{ P \in \mathbb{F}_\ell[T] \text{ unitaire} \mid \deg P = 2g, P(X) = q^{-g} X^{2g} P\left(\frac{q}{X}\right), P(\sqrt{q}) = 0 \right\},$$

pour tout nombre premier $\ell \neq 2, p$.

Biais d'ordre inférieur

Théorème (B.-Devin-Keliher-Li, 2022, "Biais d'ordre inférieur").

On a

$$\frac{1}{\#\mathcal{H}_n(\mathbb{F}_q)}\#\{f \in \mathcal{H}_n(\mathbb{F}_q) \mid d(\Delta_f = 0) > 0\} \ll_{g,p} \frac{\log q}{q^{1/A}}$$

où $A = 2g^2 + g + 2$.

Biais d'ordre inférieur

- Etape 1 : Si $d(\Delta_f = 0) > 0$ alors en particulier $\{n \in \mathbb{N} \mid \Delta_f(n) = 0\}$ est infini.

Biais d'ordre inférieur

- Etape 1 : Si $d(\Delta_f = 0) > 0$ alors en particulier $\{n \in \mathbb{N} \mid \Delta_f(n) = 0\}$ est infini. Or Δ_f est une **suite récurrente linéaire** !

Biais d'ordre inférieur

- Etape 1 : Si $d(\Delta_f = 0) > 0$ alors en particulier $\{n \in \mathbb{N} \mid \Delta_f(n) = 0\}$ est infini. Or Δ_f est une **suite récurrente linéaire** !

- Etape 2 : Une suite récurrente linéaire s'annulant une infinité de fois est **dégénérée** (théorème de Skolem-Mahler-Lech) : elle admet deux racines caractéristiques $\beta_i \neq \beta_j$ telles que $\frac{\beta_i}{\beta_j}$ est une racine de l'unité.

Biais d'ordre inférieur

- Etape 1 : Si $d(\Delta_f = 0) > 0$ alors en particulier $\{n \in \mathbb{N} \mid \Delta_f(n) = 0\}$ est infini. Or Δ_f est une **suite récurrente linéaire** !

- Etape 2 : Une suite récurrente linéaire s'annulant une infinité de fois est **dégénérée** (théorème de Skolem-Mahler-Lech) : elle admet deux racines caractéristiques $\beta_i \neq \beta_j$ telles que $\frac{\beta_i}{\beta_j}$ est une racine de l'unité.

- Etape 3 : On utilise à nouveau le grand crible de Kowalski pour se ramener au comptage de

$$\left\{ P \in \mathbb{F}_\ell[T] \text{ unitaire} \mid \deg P = 2g, P(X) = q^{-g} X^{2g} P\left(\frac{q}{X}\right), \right.$$
$$\left. \exists \alpha \neq \beta \in \overline{\mathbb{F}_\ell}, P(\alpha) = P(\beta) = 0 \text{ avec } \left(\frac{\alpha}{\beta}\right)^d = 1 \right\},$$

pour tout nombre premier $\ell \neq 2, p$.

Biais dans la mauvaise direction

Théorème (B.-Devin-Keliher-Li, 2022, "Biais dans la mauvaise direction").

On a

$$\frac{1}{\#\mathcal{H}_n(\mathbb{F}_q)}\#\{f \in \mathcal{H}_n(\mathbb{F}_q) \mid d(\Delta_f \leq 0) > \frac{1}{2}\} \ll_{g,p} \frac{(\log q)^{1-\delta_g}}{q^{1/2A}}$$

où $A = 2g^2 + g + 2$ et $\delta_g \underset{g\to+\infty}{\sim} \frac{7}{24g} > \frac{1}{4g}$.

Biais dans la mauvaise direction

- Etape 1 : Si $d(\Delta_f \leq 0) > \frac{1}{2}$ alors la distribution des valeurs de Δ_f n'est pas symétrique par rapport à sa moyenne $m_0(\chi_f) + \frac{1}{2} > 0$, et donc le tore engendré par $\{(n\pi, n\theta_1(\chi_f), \ldots, n\theta_g(\chi_f)) \mid n \in \mathbb{N}\}$ dans $(\mathbb{R}/\mathbb{Z})^{g+1}$ ne contient pas $(\pi, \ldots, \pi)$.

Biais dans la mauvaise direction

- Etape 1 : Si $d(\Delta_f \leq 0) > \frac{1}{2}$ alors la distribution des valeurs de Δ_f n'est pas symétrique par rapport à sa moyenne $m_0(\chi_f) + \frac{1}{2} > 0$, et donc le tore engendré par $\{(n\pi, n\theta_1(\chi_f), \ldots, n\theta_g(\chi_f)) \mid n \in \mathbb{N}\}$ dans $(\mathbb{R}/\mathbb{Z})^{g+1}$ ne contient pas $(\pi, \ldots, \pi)$.

- Etape 2 : On montre que ça équivaut à l'existence d'une relation $k_0\pi + \sum_{j=1}^{g} k_j\theta_j(\chi_f) \equiv 0 \bmod 2\pi$ avec $k_0, \ldots, k_g \in \mathbb{Z}$ de somme paire.

Biais dans la mauvaise direction

- Etape 1 : Si $d(\Delta_f \leq 0) > \frac{1}{2}$ alors la distribution des valeurs de Δ_f n'est pas symétrique par rapport à sa moyenne $m_0(\chi_f) + \frac{1}{2} > 0$, et donc le tore engendré par $\{(n\pi, n\theta_1(\chi_f), \ldots, n\theta_g(\chi_f)) \mid n \in \mathbb{N}\}$ dans $(\mathbb{R}/\mathbb{Z})^{g+1}$ ne contient pas $(\pi, \ldots, \pi)$.

- Etape 2 : On montre que ça équivaut à l'existence d'une relation $k_0\pi + \sum_{j=1}^{g} k_j\theta_j(\chi_f) \equiv 0 \bmod 2\pi$ avec $k_0, \ldots, k_g \in \mathbb{Z}$ de somme paire.

- Etape 3 : On a donc $(-1)^{k_0} \prod_{j=1}^{g} \alpha_j(\chi_f)_j^k \in \mathbb{Z}$, et est donc fixé par G. Cela implique que la suite est dégénérée, ou que G ne contient pas certains types de permutations.

Biais dans la mauvaise direction

- Etape 1 : Si $d(\Delta_f \leq 0) > \frac{1}{2}$ alors la distribution des valeurs de Δ_f n'est pas symétrique par rapport à sa moyenne $m_0(\chi_f) + \frac{1}{2} > 0$, et donc le tore engendré par $\{(n\pi, n\theta_1(\chi_f), \ldots, n\theta_g(\chi_f)) \mid n \in \mathbb{N}\}$ dans $(\mathbb{R}/\mathbb{Z})^{g+1}$ ne contient pas $(\pi, \ldots, \pi)$.

- Etape 2 : On montre que ça équivaut à l'existence d'une relation $k_0\pi + \sum_{j=1}^{g} k_j\theta_j(\chi_f) \equiv 0 \bmod 2\pi$ avec $k_0, \ldots, k_g \in \mathbb{Z}$ de somme paire.

- Etape 3 : On a donc $(-1)^{k_0} \prod_{j=1}^{g} \alpha_j(\chi_f)_j^k \in \mathbb{Z}$, et est donc fixé par G. Cela implique que la suite est dégénérée, ou que G ne contient pas certains types de permutations.

- Etape 4 : On relie la présence d'un type de permutation à l'existence de nombres premiers ℓ tels que $\mathcal{L}(u, \chi_f)$ admette un certain type de factorisation (théorème de Dedekind), et on conclut avec le grand crible.

Merci de votre attention.

"On ne s'est jamais donné autant de mal pour majorer le cardinal de l'ensemble vide."