Quelques aspects des courses de nombres premiers

Alexandre Bailleul

ENS Paris-Saclay

Jeudi 20 janvier 2022

Organisation de l'exposé

1. Courses de nombres premiers

2. Courses dans les corps de nombres

3. Courses dans les corps de fonctions

Organisation de l'exposé

1. **Courses de nombres premiers**
2. Courses dans les corps de nombres
3. Courses dans les corps de fonctions

Le TNPPA

- Soit a, q entiers premiers entre eux. On peut montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv a \mod q$.

Le TNPPA

- Soit a, q entiers premiers entre eux. On peut montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv a \bmod q$. En fait, on peut montrer 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 entiers premiers entre eux. On peut montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv a \bmod q$. En fait, on peut montrer 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.

Le TNPPA

- Soit a, q entiers premiers entre eux. On peut montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv a \bmod q$. En fait, on peut montrer 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. Ce sont les morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ que l'on prolonge par 0 à $\mathbb{Z}/q\mathbb{Z}$ puis à $\mathbb{Z}$ par q-périodicité.

Le TNPPA

- Soit a, q entiers premiers entre eux. On peut montrer qu'il existe une infinité de nombres premiers p tels que $p \equiv a \bmod q$. En fait, on peut montrer 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. Ce sont les morphismes $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$ que l'on prolonge par 0 à $\mathbb{Z}/q\mathbb{Z}$ puis à $\mathbb{Z}$ par q-périodicité.

- Exemple : Le caractère χ_4 modulo 4 vérifiant $\chi(4n+1) = 1$ et $\chi(4n+3) = -1$.

Le TNPPA

- La fonction L associée au caractère χ est

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

Le TNPPA

- La fonction L associée au caractère χ est

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

- On montre qu'une telle fonction se prolonge à tout $\mathbb{C}$ avec éventuellement un pôle en 1. En étudiant la localisation des zéros de telles fonctions, on montre que

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

Le TNPPA

- La fonction L associée au caractère χ est

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

- On montre qu'une telle fonction se prolonge à tout $\mathbb{C}$ avec éventuellement un pôle en 1. En étudiant la localisation des zéros de telles fonctions, on montre 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 $\Re(s)>0$, alors $\Re(s)=\frac{1}{2}$. 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 $\frac{1}{\varphi(q)}\,\mathrm{Li}(x)$ ne dépend pas de a : il y a **équirépartition** des $p \bmod q$ 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 $4n + 1$ [...] »

- Il prétend aussi que $\sum_p (-1)^{\frac{p+1}{2}} e^{-pc} \underset{c \to 0}{\longrightarrow} +\infty$

Le biais de Tchebychev

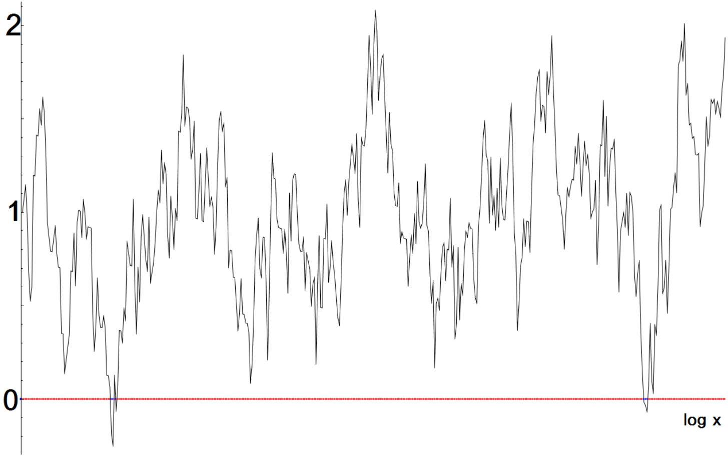
- En 1853, Tchebychev prétend dans une lettre que $\pi(x;4,3) > \pi(x;4,1)$ pour x suffisamment grand.

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 $4n+1$ [...] »

- Il prétend aussi que $\sum_p (-1)^{\frac{p+1}{2}} e^{-pc} \underset{c\to 0}{\longrightarrow} +\infty$ ($\Leftrightarrow$ Hypothèse de Riemann pour $L(s,\chi_4)$ d'après Hardy, Littlewood, Landau).

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)

Inégalités entre fonctions arithmétiques

- On a longtemps pensé que $\pi(x) < \mathrm{Li}(x)$ pour tout $x \geq 2$. Littlewood a montré en 1914 que $\pi(x) - \mathrm{Li}(x) = \Omega_{\pm}\left(x^{1/2}\frac{\log\log\log x}{\log x}\right)$.

Inégalités entre fonctions arithmétiques

- On a longtemps pensé que $\pi(x) < \mathrm{Li}(x)$ pour tout $x \geq 2$. Littlewood a montré en 1914 que $\pi(x) - \mathrm{Li}(x) = \Omega_{\pm}\left(x^{1/2}\frac{\log\log\log x}{\log x}\right)$.
- Le premier contre-exemple à $\pi(x) < \mathrm{Li}(x)$ vérifie $10^{19} \leq x \leq 10^{317}$ (nombre de Skewes). Les premières majorations « théoriques » étaient de l'ordre de $10^{10^{10^{34}}}$.

Inégalités entre fonctions arithmétiques

- On a longtemps pensé que $\pi(x) < \mathrm{Li}(x)$ pour tout $x \geq 2$. Littlewood a montré en 1914 que $\pi(x) - \mathrm{Li}(x) = \Omega_{\pm}\left(x^{1/2}\frac{\log\log\log x}{\log x}\right)$.
- Le premier contre-exemple à $\pi(x) < \mathrm{Li}(x)$ vérifie $10^{19} \leq x \leq 10^{317}$ (nombre de Skewes). Les premières majorations « théoriques » étaient de l'ordre de $10^{10^{10^{34}}}$.
- Littlewood a aussi montré que $\pi(x;4,3) - \pi(x;4,1) = \Omega_{\pm}\left(x^{1/2}\frac{\log\log\log x}{\log x}\right)$, donc l'inégalité de Tchebychev n'est pas toujours vraie.

Inégalités entre fonctions arithmétiques

- On a longtemps pensé que $\pi(x) < \mathrm{Li}(x)$ pour tout $x \geq 2$. Littlewood a montré en 1914 que $\pi(x) - \mathrm{Li}(x) = \Omega_{\pm}\left(x^{1/2}\frac{\log\log\log x}{\log x}\right)$.

- Le premier contre-exemple à $\pi(x) < \mathrm{Li}(x)$ vérifie $10^{19} \leq x \leq 10^{317}$ (nombre de Skewes). Les premières majorations « théoriques » étaient de l'ordre de $10^{10^{10^{34}}}$.

- Littlewood a aussi montré que $\pi(x;4,3) - \pi(x;4,1) = \Omega_{\pm}\left(x^{1/2}\frac{\log\log\log x}{\log x}\right)$, donc l'inégalité de Tchebychev n'est pas toujours vraie. On ne dispose pas de résultat analogue pour $\pi(x;q,a) - \pi(x;q,b)$ inconditionnellement.

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 $p \equiv 3 \bmod 4$ et les premiers $p \equiv 1 \bmod 4$, 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 $p \equiv 3 \bmod 4$ et les premiers $p \equiv 1 \bmod 4$, 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 $p \equiv 3 \bmod 4$ et les premiers $p \equiv 1 \bmod 4$, 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 LI est vraie modulo q et les $L(s,\chi)$ avec $\chi \in X_q$ satisfont GRH alors :

- Si $a \equiv \square[q]$ et $b \equiv \square[q]$, ou si $a \not\equiv \square[q]$ et $b \not\equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.

Les résultats de Rubinstein et Sarnak

Si LI est vraie modulo q et les $L(s,\chi)$ avec $\chi \in X_q$ satisfont GRH alors :

- Si $a \equiv \square[q]$ et $b \equiv \square[q]$, ou si $a \not\equiv \square[q]$ et $b \not\equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.
- Si $a \not\equiv \square[q]$ et $b \equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) > \frac{1}{2}$.

Les résultats de Rubinstein et Sarnak

Si LI est vraie modulo q et les $L(s,\chi)$ avec $\chi \in X_q$ satisfont GRH alors :

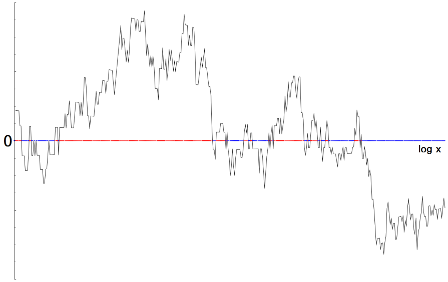
- Si $a \equiv \square[q]$ et $b \equiv \square[q]$, ou si $a \not\equiv \square[q]$ et $b \not\equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.
- Si $a \not\equiv \square[q]$ et $b \equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) > \frac{1}{2}$.
- **Théorème central limite** :
$$\max_{a,b \text{ premiers avec } q} \left| \delta(\mathcal{P}_{q;a,b}) - \frac{1}{2} \right| \underset{q \to +\infty}{\longrightarrow} 0.$$

Les résultats de Rubinstein et Sarnak

Si LI est vraie modulo q et les $L(s,\chi)$ avec $\chi \in X_q$ satisfont GRH alors :

- Si $a \equiv \square[q]$ et $b \equiv \square[q]$, ou si $a \not\equiv \square[q]$ et $b \not\equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) = \frac{1}{2}$.
- Si $a \not\equiv \square[q]$ et $b \equiv \square[q]$ alors $\delta(\mathcal{P}_{q;a,b}) > \frac{1}{2}$.
- **Théorème central limite** :

$$\max_{a,b \text{ premiers avec } q} \left| \delta(\mathcal{P}_{q;a,b}) - \frac{1}{2} \right| \underset{q \to +\infty}{\longrightarrow} 0.$$



$$\frac{\pi(x;101,3) - \pi(x;101,1)}{\sqrt{x}/\log x},$$

$$10^4 \le x \le 10^8$$

(Daniel Fiorilli)

La méthode de Rubinstein-Sarnak

Trois étapes :

1) Utilisation d'une **formule explicite** (sous GRH) :

La méthode de Rubinstein-Sarnak

Trois étapes :

1) Utilisation d'une **formule explicite** (sous GRH) :

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

les γ_χ étant les parties imaginaires des zéros des $L(s,\chi)$.

La méthode de Rubinstein-Sarnak

Trois étapes :

1) Utilisation d'une **formule explicite** (sous GRH) :

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

les γ_χ étant les parties imaginaires des zéros des $L(s,\chi)$.

La méthode de Rubinstein-Sarnak

Trois étapes :

1) Utilisation d'une **formule explicite** (sous GRH) :

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

les γ_χ étant les parties imaginaires des zéros des $L(s,\chi)$.

2) Utilisation du **théorème de Kronecker-Weyl** $\Rightarrow$ existence d'une distribution limite $\mu_{q;a,b}$ (mesure de probabilité borélienne sur $\mathbb{R}$) pour $x \mapsto \frac{\pi(e^x;q,a)-\pi(e^x;q,b)}{e^{x/2}/x}$.

La méthode de Rubinstein-Sarnak

Trois étapes :

1) Utilisation d'une **formule explicite** (sous GRH) :

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

les γ_χ étant les parties imaginaires des zéros des $L(s,\chi)$.

2) Utilisation du **théorème de Kronecker-Weyl** $\Rightarrow$ existence d'une distribution limite $\mu_{q;a,b}$ (mesure de probabilité borélienne sur $\mathbb{R}$) pour $x \mapsto \frac{\pi(e^x;q,a)-\pi(e^x;q,b)}{e^{x/2}/x}$.

3) Utilisation de l'hypothèse LI pour établir la régularité de $\mu_{q;a,b}$, étudier sa fonction caractéristique et montrer l'existence de $\delta(\mathcal{P}_{q;a,b}) = \mu_{q;a,b}(]0,+\infty[)$.

L'hypothèse LI

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

L'hypothèse LI

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 $\gamma_1, \ldots, \gamma_n$ sont linéairement indépendants sur $\mathbb{Q}$, $x \mapsto \left(e^{i\gamma_1 x}, \ldots, e^{i\gamma_n x} \right)$ se comporte en moyenne comme un n-uplet de variables aléatoires **indépendantes** uniformes sur $\mathbb{S}^1$.

L'hypothèse LI

Théorème de Kronecker-Weyl : Si $\gamma_1, \dots, \gamma_n$ sont des réels alors le groupe à un paramètre $\left\{ \left(e^{i\gamma_1 x}, \dots, e^{i\gamma_n x} \right) \mid x \in \mathbb{R} \right\}$ est équiréparti dans un tore de dimension $\dim_{\mathbb{Q}} \mathrm{Vect}(\gamma_1, \dots, \gamma_n)$. En particulier, si $\gamma_1, \dots, \gamma_n$ sont linéairement indépendants sur $\mathbb{Q}$, $x \mapsto \left(e^{i\gamma_1 x}, \dots, e^{i\gamma_n x} \right)$ se comporte en moyenne comme un n-uplet de variables aléatoires **indépendantes** uniformes sur $\mathbb{S}^1$.

Conjecture (LI).

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

L'hypothèse LI

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 $\dim_{\mathbb{Q}} \mathrm{Vect}(\gamma_1, \ldots, \gamma_n)$. En particulier, si $\gamma_1, \ldots, \gamma_n$ sont linéairement indépendants sur $\mathbb{Q}$, $x \mapsto \left(e^{i\gamma_1 x}, \ldots, e^{i\gamma_n x}\right)$ se comporte en moyenne comme un n-uplet de variables aléatoires **indépendantes** uniformes sur $\mathbb{S}^1$.

Conjecture (LI).

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

L'hypothèse LI permet de traiter la somme sur les zéros dans la formule explicite comme une somme de variables aléatoires **indépendantes**, uniformes sur $\mathbb{S}^1$.

Organisation de l'exposé

1. Courses de nombres premiers
2. **Courses dans les corps de nombres**
3. Courses dans les corps de fonctions

Frobenius et Chebotarev

- Soit K un corps de nombres (extension finie de $\mathbb{Q}$). Dans K, le rôle que joue $\mathbb{Z}$ dans $\mathbb{Q}$ est joué par l'anneau $\mathcal{O}_K = \{x \in K \mid x \text{ entier algébrique}\}$.

Frobenius et Chebotarev

- Soit K un corps de nombres (extension finie de $\mathbb{Q}$). Dans K, le rôle que joue $\mathbb{Z}$ dans $\mathbb{Q}$ est joué par l'anneau $\mathcal{O}_K = \{x \in K \mid x \text{ entier algébrique}\}$. Comme $\mathbb{O}_K$ n'est en général pas factoriel, on s'intéresse aux idéaux premiers plutôt qu'aux éléments premiers.

Frobenius et Chebotarev

- Soit K un corps de nombres (extension finie de $\mathbb{Q}$). Dans K, le rôle que joue $\mathbb{Z}$ dans $\mathbb{Q}$ est joué par l'anneau $\mathcal{O}_K = \{x \in K \mid x \text{ entier algébrique}\}$. Comme $\mathbb{O}_K$ n'est en général pas factoriel, on s'intéresse aux idéaux premiers plutôt qu'aux éléments premiers.

- Soit L/K une extension galoisienne de corps de nombres de groupe de Galois G.

Frobenius et Chebotarev

- Soit K un corps de nombres (extension finie de $\mathbb{Q}$). Dans K, le rôle que joue $\mathbb{Z}$ dans $\mathbb{Q}$ est joué par l'anneau $\mathcal{O}_K = \{x \in K \mid x \text{ entier algébrique}\}$. Comme $\mathbb{O}_K$ n'est en général pas factoriel, on s'intéresse aux idéaux premiers plutôt qu'aux éléments premiers.

- Soit L/K une extension galoisienne de corps de nombres de groupe de Galois G. À tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ (sauf un nombre fini), on peut associer une classe de conjugaison « de Frobenius » $\mathrm{Frob}_{\mathfrak{p}}$ de G.

Frobenius et Chebotarev

- Soit K un corps de nombres (extension finie de $\mathbb{Q}$). Dans K, le rôle que joue $\mathbb{Z}$ dans $\mathbb{Q}$ est joué par l'anneau $\mathcal{O}_K = \{x \in K \mid x \text{ entier algébrique}\}$. Comme $\mathbb{O}_K$ n'est en général pas factoriel, on s'intéresse aux idéaux premiers plutôt qu'aux éléments premiers.

- Soit L/K une extension galoisienne de corps de nombres de groupe de Galois G. À tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ (sauf un nombre fini), on peut associer une classe de conjugaison « de Frobenius » $\mathrm{Frob}_{\mathfrak{p}}$ de G.

- Pour $L = \mathbb{Q}(\zeta_q)$, $K = \mathbb{Q}$, $G \simeq (\mathbb{Z}/q\mathbb{Z})^{\times}$ et pour $p \nmid q$, $\mathrm{Frob}_p = a \Leftrightarrow p \equiv a \bmod q$.

Frobenius et Chebotarev

- Soit K un corps de nombres (extension finie de $\mathbb{Q}$). Dans K, le rôle que joue $\mathbb{Z}$ dans $\mathbb{Q}$ est joué par l'anneau $\mathcal{O}_K = \{x \in K \mid x \text{ entier algébrique}\}$. Comme $\mathbb{O}_K$ n'est en général pas factoriel, on s'intéresse aux idéaux premiers plutôt qu'aux éléments premiers.

- Soit L/K une extension galoisienne de corps de nombres de groupe de Galois G. À tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ (sauf un nombre fini), on peut associer une classe de conjugaison « de Frobenius » $\mathrm{Frob}_{\mathfrak{p}}$ de G.

- Pour $L = \mathbb{Q}(\zeta_q)$, $K = \mathbb{Q}$, $G \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ et pour $p \nmid q$, $\mathrm{Frob}_p = a \Leftrightarrow p \equiv a \bmod q$.

- On a

$$\pi(x; C, L/K) := \#\{\mathfrak{p} \mid N(\mathfrak{p}) \leq x, \mathrm{Frob}_{\mathfrak{p}} = C\} \underset{x \to +\infty}{\sim} \frac{\#C}{\#G} \,\mathrm{Li}(x) \quad \text{(Chebotarev).}$$

Frobenius et Chebotarev

- Soit K un corps de nombres (extension finie de $\mathbb{Q}$). Dans K, le rôle que joue $\mathbb{Z}$ dans $\mathbb{Q}$ est joué par l'anneau $\mathcal{O}_K = \{x \in K \mid x \text{ entier algébrique}\}$. Comme $\mathbb{O}_K$ n'est en général pas factoriel, on s'intéresse aux idéaux premiers plutôt qu'aux éléments premiers.

- Soit L/K une extension galoisienne de corps de nombres de groupe de Galois G. À tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ (sauf un nombre fini), on peut associer une classe de conjugaison « de Frobenius » $\mathrm{Frob}_{\mathfrak{p}}$ de G.

- Pour $L = \mathbb{Q}(\zeta_q)$, $K = \mathbb{Q}$, $G \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ et pour $p \nmid q$, $\mathrm{Frob}_p = a \Leftrightarrow p \equiv a \bmod q$.

- On a
$$\pi(x; C, L/K) := \#\{\mathfrak{p} \mid N(\mathfrak{p}) \leq x, \mathrm{Frob}_{\mathfrak{p}} = C\} \underset{x \to +\infty}{\sim} \frac{\#C}{\#G} \mathrm{Li}(x) \quad \text{(Chebotarev)}.$$

- Si C_1, C_2 sont des classes de conjugaison de G, on veut étudier la densité logarithmique de
$$\mathcal{P}_{L/K;C_1,C_2} := \left\{ x \geq 2 \mid \frac{\pi(x; C_1, L/K)}{\#C_1} > \frac{\pi(x; C_2, L/K)}{\#C_2} \right\}.$$

Généralisation aux corps de nombres

Cas des nombres premiers	**Cas des corps de nombres**
Module q	Extension galoisienne L/K
p premier	$\mathcal{P}$ idéal premier de $\mathcal{O}_K$
Congruence $p \equiv a \bmod q$	Égalité $\mathrm{Frob}_{\mathfrak{p}} = C$
Caractère de Dirichlet modulo q	Caractère de représentations linéaires de G
Fonction L de Dirichlet	Fonction L d'Artin
TNPPA	Théorème de Chebotarev

Généralisation aux corps de nombres

Cas des nombres premiers	**Cas des corps de nombres**
Module q	Extension galoisienne L/K
p premier	$\mathcal{P}$ idéal premier de $\mathcal{O}_K$
Congruence $p \equiv a \bmod q$	Égalité $\mathrm{Frob}_{\mathfrak{p}} = C$
Caractère de Dirichlet modulo q	Caractère de représentations linéaires de G
Fonction L de Dirichlet	Fonction L d'Artin
TNPPA	Théorème de Chebotarev

Théorème (Ng, 2000).

Si les fonctions L d'Artin associées aux caractères irréductibles de G satisfont AC (conjecture d'Artin), GRH et LI, alors $\delta(\mathcal{P}_{L/K;C_1,C_2})$ existe, et en l'absence de zéros en $1/2$, $\delta(\mathcal{P}_{L/K;C_1,C_2}) - 1/2$ est du signe de $\frac{\#\sqrt{C_2}}{\#C_2} - \frac{\#\sqrt{C_1}}{\#C_1}$.

Formule explicite

- On a la formule explicite

$$\frac{x}{e^{x/2}}\left(\frac{\#G}{\#C_1}\pi(e^x;C_1,L/K)-\frac{\#G}{\#C_2}\pi(e^x;C_2,L/K)\right)$$
$$=\frac{\#\sqrt{C_2}}{\#C_2}-\frac{\#\sqrt{C_1}}{\#C_1}+\sum_{\chi\in\mathrm{Irr}(G)}\overline{\chi(C_2)-\chi(C_1)}\sum_{\gamma_\chi}\frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{x}\right).$$

- Avec LI, on voit les $e^{i\gamma_\chi x}$ comme des variables indépendantes uniformes sur le cercle.

Formule explicite

- On a la formule explicite

$$\frac{x}{e^{x/2}}\left(\frac{\#G}{\#C_1}\pi(e^x;C_1,L/K)-\frac{\#G}{\#C_2}\pi(e^x;C_2,L/K)\right)$$
$$=\frac{\#\sqrt{C_2}}{\#C_2}-\frac{\#\sqrt{C_1}}{\#C_1}+\sum_{\chi\in\mathrm{Irr}(G)}\overline{\chi(C_2)-\chi(C_1)}\sum_{\gamma_\chi}\frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{x}\right).$$

- Avec LI, on voit les $e^{i\gamma_\chi x}$ comme des variables indépendantes uniformes sur le cercle.

- Dans la somme sur les zéros, un $\gamma_\chi=0$ contribue à l'espérance : **l'espérance provient des quantités de racines carrées et des zéros en $1/2$.**

Formule explicite

- On a la formule explicite

$$\frac{x}{e^{x/2}}\left(\frac{\#G}{\#C_1}\pi(e^x;C_1,L/K)-\frac{\#G}{\#C_2}\pi(e^x;C_2,L/K)\right)$$
$$=\frac{\#\sqrt{C_2}}{\#C_2}-\frac{\#\sqrt{C_1}}{\#C_1}+\sum_{\chi\in\mathrm{Irr}(G)}\overline{\chi(C_2)-\chi(C_1)}\sum_{\gamma_\chi}\frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{x}\right).$$

- Avec LI, on voit les $e^{i\gamma_\chi x}$ comme des variables indépendantes uniformes sur le cercle.

- Dans la somme sur les zéros, un $\gamma_\chi = 0$ contribue à l'espérance : **l'espérance provient des quantités de racines carrées et des zéros en $1/2$.** Est-ce qu'on peut renverser le sens attendu du biais avec des zéros en $1/2$?

Formule explicite

- On a la formule explicite

$$\frac{x}{e^{x/2}}\left(\frac{\#G}{\#C_1}\pi(e^x;C_1,L/K)-\frac{\#G}{\#C_2}\pi(e^x;C_2,L/K)\right)$$
$$=\frac{\#\sqrt{C_2}}{\#C_2}-\frac{\#\sqrt{C_1}}{\#C_1}+\sum_{\chi\in\mathrm{Irr}(G)}\overline{\chi(C_2)-\chi(C_1)}\sum_{\gamma_\chi}\frac{e^{i\gamma_\chi x}}{\frac{1}{2}+i\gamma_\chi}+O\left(\frac{1}{x}\right).$$

- Avec LI, on voit les $e^{i\gamma_\chi x}$ comme des variables indépendantes uniformes sur le cercle.

- Dans la somme sur les zéros, un $\gamma_\chi=0$ contribue à l'espérance : **l'espérance provient des quantités de racines carrées et des zéros en** $1/2$**.** Est-ce qu'on peut renverser le sens attendu du biais avec des zéros en $1/2$?

- On trouve également

$$\mathrm{Var}(X(L/K;C_1,C_2)=2\sum_{\chi\in\mathrm{Irr}(G)}|\chi(C_1)-\chi(C_2)|^2\sum_{\gamma_\chi>0}\frac{1}{\frac{1}{4}+\gamma_\chi^2},$$

et la somme sur γ_χ est contrôlée par le **conducteur** d'Artin de χ : **la variance est contrôlée par la ramification dans** L/K.

Root number et zéros en $1/2$

- **Observation :** Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}),$$

où la constante $W(\chi)$ (*root number*) est $+1$ ou -1.

Root number et zéros en $1/2$

- **Observation :** Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}),$$

où la constante $W(\chi)$ (*root number*) est $+1$ ou -1. **Si** $W(\chi) = -1$ **alors** $L(1/2,\chi,L/K) = 0$ **!**

Root number et zéros en $1/2$

- **Observation :** Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}),$$

  où la constante $W(\chi)$ (*root number*) est $+1$ ou -1. **Si** $W(\chi) = -1$ **alors** $L(1/2,\chi,L/K) = 0$ **!**

- Il y a deux familles de caractères irréductibles réels : les caractères **orthogonaux** et les caractères **symplectiques**.

Root number et zéros en $1/2$

- **Observation :** Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}),$$

  où la constante $W(\chi)$ (*root number*) est $+1$ ou -1. **Si** $W(\chi) = -1$ **alors** $L(1/2,\chi,L/K) = 0$ **!**

- Il y a deux familles de caractères irréductibles réels : les caractères **orthogonaux** et les caractères **symplectiques**.

- **Fröhlich-Queyrut, 1973 :** Si χ est orthogonal, $W(\chi) = +1$.

Root number et zéros en $1/2$

- **Observation :** Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}),$$

  où la constante $W(\chi)$ (*root number*) est $+1$ ou -1. **Si** $W(\chi) = -1$ **alors** $L(1/2,\chi,L/K) = 0$ **!**

- Il y a deux familles de caractères irréductibles réels : les caractères **orthogonaux** et les caractères **symplectiques**.

- **Fröhlich-Queyrut, 1973 :** Si χ est orthogonal, $W(\chi) = +1$.

- Tous les exemples connus de root numbers -1, et *a fortiori* de zéros en $1/2$ correspondent à des caractères symplectiques

Root number et zéros en $1/2$

- **Observation :** Si χ est réel, on a l'équation fonctionnelle

$$\Lambda(1-s,\chi) = W(\chi)\Lambda(s,\chi) \quad (\Lambda(s,\chi) = L(s,\chi,L/K) \times \text{facteurs Gamma}),$$

où la constante $W(\chi)$ (*root number*) est $+1$ ou -1. **Si** $W(\chi) = -1$ **alors** $L(1/2,\chi,L/K) = 0$ **!**

- Il y a deux familles de caractères irréductibles réels : les caractères **orthogonaux** et les caractères **symplectiques**.

- **Fröhlich-Queyrut, 1973 :** Si χ est orthogonal, $W(\chi) = +1$.

- Tous les exemples connus de root numbers -1, et *a fortiori* de zéros en $1/2$ correspondent à des caractères symplectiques $\Rightarrow$ renforcement d'hypothèse LI^+.

Hypothèse LI^+ et groupes de quaternions

Conjecture (LI^+).

$L/\mathbb{Q}$ vérifie LI et pour tout $\lambda \in \mathrm{Irr}(G^+)$, $L(1/2, \lambda, L/\mathbb{Q}) = 0$ si et seulement si λ est symplectique et $W(\lambda) = -1$.

Hypothèse LI^+ et groupes de quaternions

Conjecture (LI^+).

$L/\mathbb{Q}$ vérifie LI et pour tout $\lambda \in \mathrm{Irr}(G^+)$, $L(1/2, \lambda, L/\mathbb{Q}) = 0$ si et seulement si λ est symplectique et $W(\lambda) = -1$.

- Les groupes

$$\mathbb{H}_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$$

possèdent 2^n éléments, $2^{n-2} + 3$ caractères irréductibles et 2^{n-3} caractères symplectiques.

Hypothèse LI^+ et groupes de quaternions

Conjecture (LI^+).

$L/\mathbb{Q}$ vérifie LI et pour tout $\lambda \in \mathrm{Irr}(G^+)$, $L(1/2, \lambda, L/\mathbb{Q}) = 0$ si et seulement si λ est symplectique et $W(\lambda) = -1$.

- Les groupes

$$\mathbb{H}_{2^n} := \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2, yxy^{-1} = x^{-1} \rangle$$

possèdent 2^n éléments, $2^{n-2} + 3$ caractères irréductibles et 2^{n-3} caractères symplectiques. De plus, $-1 := x^{2^{n-2}}$ a $2^{n-1} + 1$ racines carrées et 1 n'en a que 2.

Biais modérés opposés

Théorème (B. , 2020).

Supposons GRH et LI^+ pour les fonctions L d'Artin qui interviennent. Soit f une fonction telle que $f(n) \underset{n\to+\infty}{\longrightarrow} +\infty$. Il existe deux familles $(K_d)_d$ et $(L_d)_d$ d'extensions galoisiennes de $\mathbb{Q}$ telles que $\mathrm{Gal}(K_d/\mathbb{Q}) \simeq \mathrm{Gal}(L_d/\mathbb{Q}) \simeq \mathbb{H}_8$, $\mathbb{Q}(\sqrt{d}) \subset K_d \cap L_d$,

$$0 < 1/2 - \delta(\mathcal{P}_{K_d/\mathbb{Q};1,-1}) \ll \frac{1}{f(d)}$$

et

$$0 < \delta(\mathcal{P}_{L_d/\mathbb{Q};1,-1}) - 1/2 \ll \frac{1}{f(d)}.$$

Biais extrêmes opposés

Théorème (B. , 2020).

Sous GRH et LI^+ pour les fonctions L d'Artin qui interviennent, il existe deux familles $(\mathcal{Q}_n^+)_{n\geq 3}$ et $(\mathcal{Q}_n^-)_{n\geq 3}$ d'extensions galoisiennes de $\mathbb{Q}$ telles que $\mathrm{Gal}(\mathcal{Q}_n^+/\mathbb{Q}) \simeq \mathrm{Gal}(\mathcal{Q}_n^-/\mathbb{Q}) \simeq \mathbb{H}_{2^n}$ et

$$c_1 \exp\left(-c_2 2^n\right) < 1 - \delta(\mathcal{P}_{\mathcal{Q}_n^+/\mathbb{Q};1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right)$$

et

$$c_1 \exp\left(-c_2 2^n\right) < \delta(\mathcal{P}_{\mathcal{Q}_n^-;1,-1}) < \exp\left(-c_3 \frac{2^n}{n}\right).$$

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

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

- On définit $\mathcal{P}_{M;A,B} = \{X \geq 1 \mid \pi(X; M, A) > \pi(X; M, B)\}$ et, quand elle existe,

$$d(\mathcal{P}_{M;A,B}) := \lim_{X \to +\infty} \frac{1}{X} \#(\mathcal{P}_{M;A,B} \cap [\![1, X]\!]).$$

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 $\mathcal{P}_{M;A,B} = \{X \geq 1 \mid \pi(X; M, A) > \pi(X; M, B)\}$ et, quand elle existe,

$$d(\mathcal{P}_{M;A,B}) := \lim_{X\to+\infty} \frac{1}{X}\#(\mathcal{P}_{M;A,B} \cap [\![1, X]\!]).$$

Théorème (Cha, 2008).

Supposons LI_π pour les zéros des fonctions L de Dirichlet modulo M. Alors $d(\mathcal{P}_{M;A,B})$ existe et en l'absence de zéros en $1/2$, $d(\mathcal{P}_{M;A,B}) - 1/2$ est du signe de $\#\sqrt{\{B\}} - \#\sqrt{\{A\}}$.

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 $\mathcal{P}_{M;A,B} = \{X \geq 1 \mid \pi(X; M, A) > \pi(X; M, B)\}$ et, quand elle existe,

$$d(\mathcal{P}_{M;A,B}) := \lim_{X \to +\infty} \frac{1}{X} \#(\mathcal{P}_{M;A,B} \cap [\![1, X]\!]).$$

Théorème (Cha, 2008).

Supposons LI_π pour les zéros des fonctions L de Dirichlet modulo M. Alors $d(\mathcal{P}_{M;A,B})$ existe et en l'absence de zéros en $1/2$, $d(\mathcal{P}_{M;A,B}) - 1/2$ est du signe de $\#\sqrt{\{B\}} - \#\sqrt{\{A\}}$.

Démonstration. Similaire : formule explicite, utilisation du théorème de Kronecker-Weyl **discret**, utilisation de LI_π.

L'hypothèse LI_π

Théorème (Weil).

Pour tout caractère de Dirichlet non principal χ modulo $M \in \mathbb{F}_q[T]$, la fonction $L(s,\chi)$ est un polynôme à coefficients entiers en $u = q^{-s}$:

$$\mathcal{L}(u,\chi) := L(s,\chi) = \prod_{j=1}^{M(\chi)} (1 - \gamma_j(\chi)u)$$

et on a $|\gamma_j(\chi)| = q^{1/2}$.

L'hypothèse LI_π

Théorème (Weil).

Pour tout caractère de Dirichlet non principal χ modulo $M \in \mathbb{F}_q[T]$, la fonction $L(s,\chi)$ est un polynôme à coefficients entiers en $u = q^{-s}$:

$$\mathcal{L}(u,\chi) := L(s,\chi) = \prod_{j=1}^{M(\chi)} (1 - \gamma_j(\chi)u)$$

et on a $|\gamma_j(\chi)| = q^{1/2}$.

Conjecture (LI_π).

Le (multi)-ensemble $(\{\gamma_j(\chi) \mid \chi \in X_M\} \cap]0,\pi[) \cup \{\pi\}$ est linéairement indépendant sur $\mathbb{Q}$.

L'hypothèse LI_π

Théorème (Weil).

Pour tout caractère de Dirichlet non principal χ modulo $M \in \mathbb{F}_q[T]$, la fonction $L(s,\chi)$ est un polynôme à coefficients entiers en $u = q^{-s}$:

$$\mathcal{L}(u,\chi) := L(s,\chi) = \prod_{j=1}^{M(\chi)} (1 - \gamma_j(\chi)u)$$

et on a $|\gamma_j(\chi)| = q^{1/2}$.

Conjecture (LI_π).

Le (multi)-ensemble $(\{\gamma_j(\chi) \mid \chi \in X_M\} \cap]0,\pi[) \cup \{\pi\}$ est linéairement indépendant sur $\mathbb{Q}$.

- LI_π n'est **pas toujours vraie**...

Extensions de corps de fonctions

- Soit L/K une extension galoisienne géométrique (même corps des constantes) de corps de fonctions de courbes sur $\mathbb{F}_q$, de groupe de Galois G. Comme pour les corps de nombres, à chaque diviseur premier de K non ramifié dans L on associe une classe de conjugaison de Frobenius dans G.

Extensions de corps de fonctions

- Soit L/K une extension galoisienne géométrique (même corps des constantes) de corps de fonctions de courbes sur $\mathbb{F}_q$, de groupe de Galois G. Comme pour les corps de nombres, à chaque diviseur premier de K non ramifié dans L on associe une classe de conjugaison de Frobenius dans G.

- On définit $\pi(X; C, L/K), \mathcal{P}_{L/K;C_1,C_2}, d(\mathcal{P}_{L/K;C_1,C_2})$ de manière analogue à précédemment.

Extensions de corps de fonctions

- Soit L/K une extension galoisienne géométrique (même corps des constantes) de corps de fonctions de courbes sur $\mathbb{F}_q$, de groupe de Galois G. Comme pour les corps de nombres, à chaque diviseur premier de K non ramifié dans L on associe une classe de conjugaison de Frobenius dans G.
- On définit $\pi(X; C, L/K), \mathcal{P}_{L/K;C_1,C_2}, d(\mathcal{P}_{L/K;C_1,C_2})$ de manière analogue à précédemment.

Théorème (Cha-Im, 2011).

Supposons LI_π pour les zéros des fonctions L d'Artin associées aux caractères irréductibles de G. Alors $d(\mathcal{P}_{L/K;C_1,C_2})$ existe et en l'absence de zéros en $1/2$, $d(\mathcal{P}_{L/K;C_1,C_2}) - \frac{1}{2}$ est du signe de $\frac{\#\sqrt{C_2}}{\#C_2} - \frac{\#\sqrt{C_1}}{\#C_1}$.

Extensions de corps de fonctions

- Soit L/K une extension galoisienne géométrique (même corps des constantes) de corps de fonctions de courbes sur $\mathbb{F}_q$, de groupe de Galois G. Comme pour les corps de nombres, à chaque diviseur premier de K non ramifié dans L on associe une classe de conjugaison de Frobenius dans G.

- On définit $\pi(X; C, L/K), \mathcal{P}_{L/K;C_1,C_2}, d(\mathcal{P}_{L/K;C_1,C_2})$ de manière analogue à précédemment.

Théorème (Cha-Im, 2011).

Supposons LI_π pour les zéros des fonctions L d'Artin associées aux caractères irréductibles de G. Alors $d(\mathcal{P}_{L/K;C_1,C_2})$ existe et en l'absence de zéros en $1/2$, $d(\mathcal{P}_{L/K;C_1,C_2}) - \frac{1}{2}$ est du signe de $\frac{\#\sqrt{C_2}}{\#C_2} - \frac{\#\sqrt{C_1}}{\#C_1}$.

- On retrouve les courses de polynômes irréductibles avec des extensions de Carlitz de $\mathbb{F}_q(x)$.

À propos de LI_π

Théorème (Kowalski, 2008).

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

$$\#\{t \in \mathbb{F}_q \mid \mathbb{F}_q(x,y)/\mathbb{F}_q(x), \text{ où } y^2 = f(x)(x-t), \text{ ne satisfait pas } \mathrm{Li}_\pi\} = O_g(q^{1-\gamma_g})$$

quand $q \to +\infty$, avec $0 < \gamma_g \underset{g \to +\infty}{\to} 0$.

Un théorème central limite

Théorème (B., 2020).

Fixons $K := \mathbb{F}_q(x)$. Soit $n \geq 3$ tel que $q \equiv 1 \bmod n$. Pour tout $d > n$, on suppose que l'on dispose d'un polynôme $f_d \in \mathbb{F}_q[x]$ sans facteur carré de degré d tel que l'extension L_d/K satisfasse LI_π, où $L_d = K(y)$ avec $y^n = f_d$. Alors

$$\max_{C_1, C_2 \in \mathrm{Gal}(L_d/K)^\sharp} \left| \delta(\mathcal{P}_{L_d/K; C_1, C_2}) - \frac{1}{2} \right| \asymp_n \frac{1}{\sqrt{d}}.$$

Un théorème central limite

Théorème (B., 2020).

Fixons $K := \mathbb{F}_q(x)$. Soit $n \geq 3$ tel que $q \equiv 1 \bmod n$. Pour tout $d > n$, on suppose que l'on dispose d'un polynôme $f_d \in \mathbb{F}_q[x]$ sans facteur carré de degré d tel que l'extension L_d/K satisfasse LI_π, où $L_d = K(y)$ avec $y^n = f_d$. Alors

$$\max_{C_1, C_2 \in \mathrm{Gal}(L_d/K)^\sharp} \left| \delta(\mathcal{P}_{L_d/K;C_1,C_2}) - \frac{1}{2} \right| \asymp_n \frac{1}{\sqrt{d}}.$$

Démonstration. Traduction probabiliste, estimation de la fonction caractéristique, inégalité de Berry-Esseen, contrôle de la variance à l'aide du genre de la courbe superelliptique $y^n = f_d$.

Merci de votre attention.