Courses de polynômes irréductibles dans les corps de fonctions

Youssef Sedrati (Université de Lorraine, IECL)

Laboratoire de Mathématiques Pures et Appliqués, Calais
17 mars 2022

Plan

Biais de Chebyshev

- $\pi(x; q, a) = \left| \{p \leqslant x \,|p \equiv a \mod q\} \right|.$

Biais de Chebyshev

- $\pi(x; q, a) = |\{p \leqslant x \mid p \equiv a \mod q\}|$.

En 1853, Chebyshev a remarqué que, pour la plupart des $x \geqslant 2$, $\pi(x; 4, 3) > \pi(x; 4, 1)$.

Biais de Chebyshev

- $\pi(x; q, a) = |\{p \leqslant x \,|p \equiv a \mod q\}|$.

En 1853, Chebyshev a remarqué que, pour la plupart des $x \geqslant 2$, $\pi(x; 4, 3) > \pi(x; 4, 1)$.

Remarque

- Pour $x < 26861$ on a toujours $\pi(x; 4, 1) < \pi(x; 4, 3)$.
- Pour $x = 26861$, on a $\pi(x; 4, 1) > \pi(x; 4, 3)$.

Théorème (Littlewood 1914)

$\pi(x; 4, 3) - \pi(x; 4, 1)$ change de signe pour une infinité d'entiers x.

Biais de Chebyshev

Soit $(a, q) = 1$ et $(b, q) = 1$ tel que $a \not\equiv b \mod q$. On considère :

$$S_{q;a,b} = \{x \geqslant 2 \mid \pi(x; q, a) > \pi(x; q, b)\}$$

Kaczorowski a montré sous l'hypothèse de Riemann généralisée que la densité naturelle de $S_{q;a,b}$ n'existe pas.

Biais de Chebyshev

Afin de remédier à ce problème Rubinstein et Sarnak (1994) ont utilisé la densité logarithmique définie ainsi :

Définition

La densité logarithmique d'un borélien S de $\mathbb{R}^+$ est quand elle existe :

$$\delta(S) = \lim_{X \longrightarrow +\infty} \frac{1}{\log X} \int_2^X \mathbb{1}_S(t) \frac{dt}{t} = \lim_{Y \longrightarrow +\infty} \frac{1}{Y} \int_{\log 2}^Y \mathbb{1}_S(e^t) dt$$

Théorème (Rubinstein et Sarnak, 1994)

Sous 'certaines hypothèses', l'ensemble $S_{q;a,b}$ a une densité logarithmique strictement positive et elle satisfait :

$$\delta(S_{q;a,b}) > \frac{1}{2} \iff b \text{ est un carré modulo } q \textit{ et } a \text{ ne l'est pas}$$

$$\delta(S_{q;a,b}) = \frac{1}{2} \iff a \textit{ et } b \text{ sont simultanément des carrés modulo } q$$

$$\textit{ou } a \textit{ et } b \text{ ne le sont pas}$$

En particulier, ils ont prouvé conditionnellement que

$$\delta(S_{4;3,1}) = 0.9959...$$

Biais de Chebyshev

- Soit $2 \leqslant r \leqslant \phi(q)$ et $\mathcal{A}_r(q)$ l'ensemble des r-uplet de classes de résidus distinctes $(a'_1, a'_2, \ldots, a'_r)$ modulo q qui sont premiers avec q.
- Pour $(a_1, a_2, \ldots, a_r) \in \mathcal{A}_r(q)$, $S_{q;a_1,a_2,\ldots,a_r}$ désignera l'ensemble des $x \geqslant 2$ tel que

$$\pi(x; q, a_1) > \pi(x; q, a_2) > \cdots > \pi(x; q, a_r).$$

Biais de Chebyshev

Théorème (Rubinstein et Sarnak, 1994)

Sous 'certaines hypothèses', on a $\delta(S_{q;a_1,a_2,\dots,a_r}) > 0$.

- Ils ont également prouvé sous les mêmes conditions que

$$\Delta_r(q) := \max_{(a_1,a_2,\dots,a_r)\in\mathcal{A}_r(q)} \left|\delta(S_{q;a_1,a_2,\dots,a_r}) - \frac{1}{r!}\right| \longrightarrow 0 \text{ quand } q \longrightarrow \infty.$$

- P : polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.

Théorème des nombres premiers pour les polynômes

- P : polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.
- $\mathcal{M}$: l'ensemble des polynômes unitaires dans $\mathbb{F}_q[T]$.

Théorème des nombres premiers pour les polynômes

- P : polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.
- $\mathcal{M}$: l'ensemble des polynômes unitaires dans $\mathbb{F}_q[T]$.
- m polynôme unitaire de degré $M \geqslant 2$.

Théorème des nombres premiers pour les polynômes

- P : polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.
- $\mathcal{M}$: l'ensemble des polynômes unitaires dans $\mathbb{F}_q[T]$.
- m polynôme unitaire de degré $M \geqslant 2$.
- $\pi(N) := \#\{P | \deg(P) = N\}$.

Théorème des nombres premiers pour les polynômes

- P : polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.
- $\mathcal{M}$: l'ensemble des polynômes unitaires dans $\mathbb{F}_q[T]$.
- m polynôme unitaire de degré $M \geqslant 2$.
- $\pi(N) := \#\{P | \deg(P) = N\}$.
- $\pi(a, m, N) := \#\{P | P \equiv a \bmod m \text{ et } \deg(P) = N\}$.

Théorème des nombres premiers pour les polynômes

- P : polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.
- $\mathcal{M}$: l'ensemble des polynômes unitaires dans $\mathbb{F}_q[T]$.
- m polynôme unitaire de degré $M \geqslant 2$.
- $\pi(N) := \#\{P \mid \deg(P) = N\}$.
- $\pi(a, m, N) := \#\{P \mid P \equiv a \bmod m \text{ et } \deg(P) = N\}$.
- $S_N := \#\{m \in \mathcal{M} \mid \deg(m) = N\} = q^N$.

Théorème des nombres premiers pour les polynômes

- P : polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.
- $\mathcal{M}$: l'ensemble des polynômes unitaires dans $\mathbb{F}_q[T]$.
- m polynôme unitaire de degré $M \geqslant 2$.
- $\pi(N) := \#\{P \,|\, \deg(P) = N\}$.
- $\pi(a, m, N) := \#\{P \,|\, P \equiv a \bmod m \text{ et } \deg(P) = N\}$.
- $S_N := \#\{m \in \mathcal{M} \,|\, \deg(m) = N\} = q^N$.
- Pour tout réel x strictement positif, on définit : $\log_q x := \frac{\log x}{\log q}$.

Théorème des nombres premiers pour les polynômes

- P : polynôme irréductible unitaire dans $\mathbb{F}_q[T]$.
- $\mathcal{M}$: l'ensemble des polynômes unitaires dans $\mathbb{F}_q[T]$.
- m polynôme unitaire de degré $M \geqslant 2$.
- $\pi(N) := \#\{P | \deg(P) = N\}$.
- $\pi(a, m, N) := \#\{P | P \equiv a \bmod m \text{ et } \deg(P) = N\}$.
- $S_N := \#\{m \in \mathcal{M} | \deg(m) = N\} = q^N$.
- Pour tout réel x strictement positif, on définit : $\log_q x := \frac{\log x}{\log q}$.

Théorème des nombres premiers pour les polynômes (TNPP)

Soit $N \in \mathbb{N}^*$. Alors :

$$\pi(N) = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

Quelques analogies entre corps de nombres et corps de fonctions

Corps des nombres	Corps des fonctions
$\mathbb{Z}$	$A = \mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Les nombres premiers	les polynômes irréductibles unitaires
Valeur absolue $\lvert n \rvert$	norme d'un polynôme $\lvert f \rvert = q^{\deg(f)}$
$n = p_1^{e_1} ... p_t^{e_t}$	$f = \alpha P_1^{e_1} ... P_t^{e_t}$
$\phi(n) = \# (Z/nZ)^*$	$\phi(m) = \# (F_q[T]/mF_q[T])^*$
$\pi(x) \sim \frac{x}{\log(x)}$	$\pi(N) = \frac{S_N}{\log_q(S_N)} + O\left(\frac{\sqrt{S_N}}{\log_q(S_N)}\right)$
$\pi(x, q, a) \sim \frac{x}{\phi(q)\log(x)}$	$\pi(a, m, N) = \frac{S_N}{\phi(m)\log_q(S_N)} + O\left(\frac{\sqrt{S_N}}{\log_q(S_N)}\right)$

Problématique

- $\mathcal{B}_r(m)$ l'ensemble des r-uplet de classes de résidus distinctes $(b'_1, b'_2, \ldots, b'_r)$ modulo m qui sont premiers avec m.

Problématique

- $\mathcal{B}_r(m)$ l'ensemble des r-uplet de classes de résidus distinctes $(b'_1, b'_2, \ldots, b'_r)$ modulo m qui sont premiers avec m.

On considère :

$$P_{m;a_1,a_2,a_3,..,a_r} = \left\{ X \in \mathbb{N}^* \mid \sum_{N=1}^{X} \pi(a_1; m, N) > \sum_{N=1}^{X} \pi(a_2; m, N) > \ldots > \sum_{N=1}^{X} \pi(a_r, m, N) \right\}$$

Problématique

- $\mathcal{B}_r(m)$ l'ensemble des r-uplet de classes de résidus distinctes $(b'_1, b'_2, \dots, b'_r)$ modulo m qui sont premiers avec m.

On considère :

$$P_{m;a_1,a_2,a_3,..,a_r} = \left\{ X \in \mathbb{N}^* \mid \sum_{N=1}^{X} \pi(a_1; m, N) > \sum_{N=1}^{X} \pi(a_2; m, N) > \dots > \sum_{N=1}^{X} \pi(a_r, m, N) \right\}$$

On s'intéresse particulièrement à l'étude de la densité naturelle de $P_{m;a_1,a_2,a_3,..,a_r}$:

$$\delta_m := \delta(P_{m;a_1,a_2,a_3,..,a_r}) := \lim_{X \longrightarrow +\infty} \frac{\#\left(P_{m;a_1,a_2,a_3,..,a_r} \cap \{1, .., X\}\right)}{X}$$

si elle existe.

Caractères et fonctions L de Dirichlet

Définition

Soit $m \in \mathcal{M}$ de degré $M \geqslant 1$. Un caractère de Dirichlet modulo m est une fonction $\chi : F_q[T] \longrightarrow \mathbb{C}$ qui vérifie les conditions suivantes :

1. $\forall a, b \in F_q[T]$, on a : $\chi(a + bm) = \chi(a)$.
2. $\forall a, b \in F_q[T]$, on a : $\chi(ab) = \chi(a)\chi(b)$.
3. $\chi(a) \neq 0$ si et seulement si $(a, m) = 1$.

Caractères et fonctions L de Dirichlet

Définition

Soit $m \in \mathcal{M}$ de degré $M \geqslant 1$. Un caractère de Dirichlet modulo m est une fonction $\chi : F_q[T] \longrightarrow \mathbb{C}$ qui vérifie les conditions suivantes :

1. $\forall a, b \in F_q[T]$, on a : $\chi(a + bm) = \chi(a)$.
2. $\forall a, b \in F_q[T]$, on a : $\chi(ab) = \chi(a)\chi(b)$.
3. $\chi(a) \neq 0$ si et seulement si $(a, m) = 1$.

Définition

Soit $m \in \mathcal{M}$ de degré $M \geqslant 1$ et χ un caractère de Dirichlet modulo m. La fonction L associée à χ est définie par :

$$L(s, \chi) := \sum_{\substack{f \in F_q[T] \\ f \text{ unitaire}}} \frac{\chi(f)}{|f|^s} = \prod_P \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1} \text{ pour } \Re(s) > 1$$

Avec $|f| = q^{\deg(f)}$

En effectuant le changement de variable $u = q^{-s}$, on définit pour chaque caractère χ modulo m : $\mathcal{L}(u, \chi) := L(s, \chi)$.

Fonctions L de Dirichlet

En effectuant le changement de variable $u = q^{-s}$, on définit pour chaque caractère χ modulo m : $\mathcal{L}(u, \chi) := L(s, \chi)$.

Théorème (Weil)

Soit χ^* le caractère primitif modulo un polynôme $m(\chi^*)$ qui induit un caractère non principal de Dirichlet modulo m. Soit $M(\chi^*)$ le degré de $m(\chi^*)$. Alors :

- Si χ^* est pair on a $\mathcal{L}(u, \chi^*) = (1 - u) \prod_{i=1}^{M(\chi^*)-2} (1 - \gamma_{\chi_i} u)$.
- Si χ^* est impair on a $\mathcal{L}(u, \chi^*) = \prod_{i=1}^{M(\chi^*)-1} (1 - \gamma_{\chi_i} u)$.

Avec γ_{χ_i} un nombre complexe de module $\sqrt{q}$.

LI pour les corps de fonctions

On fixe un ensemble V de caractères non principaux de Dirichlet modulo m qui est fermé par action de conjugaison.

LI (hypothèse d'indépendance linéaire pour les corps de fonctions)

On dit que (LI $\bigstar$) est vérifiée sur V si le multi-ensemble :

$$\bigcup_{\chi \in V} \left\{ \theta \in [0, \pi] \mid \mathcal{L}((\sqrt{q}e^{i\theta})^{-1}, \chi) = 0 \right\} \cup \{\pi\}$$

est linéairement indépendant sur Q.

- Dans toute la suite, quand l'ensemble V n'est pas précisé, on considérera que V est l'ensemble de tous les caractères non principaux de Dirichlet modulo m.

Théorème (Cha, 2008)

Supposons que (LI ★) est vraie. Alors :

$$\delta_m = \int_{x_1 > .. > x_r} d\mu \left(x_1, .., x_r \right)$$

Où μ est la mesure de probabilité qui correspond à un certain vecteur aléatoire $X_{m;a_1,..,a_r} = (X(m, a_1), .., X(m, a_r))$.

Biais de Chebyshev dans les corps de fonctions

On définit $a(N)$ et $b(N)$ comme étant respectivement le nombre de premiers de degré N congrus à un résidu quadratique modulo m et le nombre de premiers de degré N congrus à un non-résidu quadratique modulo m. On considère

$$P_{m;R,N} = \left\{ X \in \mathbb{N}^* \text{tel que} \sum_{N=1}^{X} a(N) > \sum_{N=1}^{X} b(N) \right\}$$

Biais de Chebyshev dans les corps de fonctions

On définit $a(N)$ et $b(N)$ comme étant respectivement le nombre de premiers de degré N congrus à un résidu quadratique modulo m et le nombre de premiers de degré N congrus à un non-résidu quadratique modulo m. On considère

$$P_{m;R,N} = \left\{ X \in \mathbb{N}^* \text{tel que} \sum_{N=1}^{X} a(N) > \sum_{N=1}^{X} b(N) \right\}$$

Théorème (Cha, 2008)

Supposons que m est irréductible. Sous (LI $\bigstar$) sur le singleton $\{\chi_{quad}\}$, on a $\delta(P_{m;R,N}) < 1/2$.

Quelques définitions

Soit $a \in \mathbb{F}_q[T]$ tel que $(a, m) = 1$, on définit :

$$C_m(a) := -1 + \sum_{\substack{b^2 \equiv a \bmod m \\ b \in (\mathbb{F}_q[T]/m)^*}} 1,$$

et :

$$N_m := 2 \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \sum_{\Im(\gamma_\chi) > 0} \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|^2 \sim \frac{q}{q-1} \phi(m) \log_q |m|.$$

Quelques définitions

On définit également les quantités suivantes :

$$B_m(a_j, a_k) := \sum_{\substack{\chi \bmod m \\ \chi \neq \chi_0}} \sum_{\Im(\gamma_\chi)>0} (\chi(a_j/a_k) + \chi(a_k/a_j)) \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|^2 \ll \phi(m).$$

et :

$$C_m := \max_{1 \leqslant i \leqslant r} |C_m(a_i)| \quad \text{et} \quad B_m := \max_{1 \leqslant j < k \leqslant r} |B_m(a_j, a_k)|$$

pour tout $(a_1, .., a_r) \in \mathcal{B}_r(m)$.

Formule asymptotique de la densité $\delta_{m;a_1,a_2}$

Théorème (Sedrati, 2021)

Soit $m \in \mathcal{M}$ de degré assez grand. Supposons que (LI $\bigstar$) est vérifiée. Soit $(a_1, a_2) \in \mathcal{B}_2(m)$, alors :

$$\delta_{m;a_1,a_2} = \frac{1}{2} - \frac{(\sqrt{q}+q)}{2(q-1)} \frac{(C_m(a_1) - C_m(a_2))}{\sqrt{2\pi V_m(a_1,a_2)}} + O\left(\frac{C_m(1)^2(\log_q|m|)^2}{V_m(a_1,a_2)}\right),$$

où $V_m(a_1, a_2) = 2\left(N_m - B_m(a_1, a_2)\right)$.

Formule asymptotique de la densité $\delta_{m;a_1,..,a_r}$

Théorème (Sedrati, 2021)

Soit $m \in \mathcal{M}$ de degré assez grand et $r \geqslant 3$ un entier. Supposons que (LI $\bigstar$) est vérifiée. Soit $(a_1, \ldots, a_r) \in \mathcal{B}_r(m)$ alors :

$$\delta_m = \frac{1}{r!} - \frac{(q+\sqrt{q})}{2\sqrt{N_m}(q-1)} \sum_{j=1}^{r} \alpha_j(r) C_m(a_j) + \frac{1}{N_m} \sum_{1 \leqslant j < k \leqslant r} \beta_{j,k}(r) B_m(a_j, a_k)$$

$$+ \frac{q+q^2}{4N_m(q-1)^2} \left(\sum_{j=1}^{r} \lambda_j(r) C_m(a_j)^2 + 2 \sum_{1 \leqslant j < k \leqslant r} \beta_{j,k}(r) C_m(a_j) C_m(a_k) \right)$$

$$+ O_r\left(\frac{1}{N_m} + \frac{C_m B_m}{N_m^{3/2}} + \frac{B_m^2}{N_m^2} \right).$$

Différence entre $r = 2$ et $r \geqslant 3$

Soit
$$\tilde{\Delta}_r(m) := \max_{(a_1,a_2,\ldots,a_r)\in\mathcal{A}_r(m)} \left|\delta_{m;a_1,\ldots,a_r} - \frac{1}{r!}\right|.$$

Corollaire (Sedrati, 2021)

Sous les mêmes hypothèses on a :
$$\tilde{\Delta}_2(m) = \frac{1}{|m|^{1/2+o(1)}}.$$

Corollaire (Sedrati, 2021)

Soit $r \geqslant 3$ un entier. Il existe des constantes strictement positives $c_1(r)$, $c_2(r)$ et un entier $m_0 \in \mathbb{N}^*$ tel que si $\deg(m) \geqslant m_0$ et (LI $\bigstar$) est vraie alors
$$\frac{c_1(r)}{\log_q|m|} \leqslant \tilde{\Delta}_r(m) \leqslant \frac{c_2(r)}{\log_q|m|}.$$

Définition

Une course $\{m; a_1, ..a_r\}$ est dite non biaisée si pour toute permutation $\sigma \in S_r$ on a :

$$\delta_{m;a_{\sigma(1)},..,a_{\sigma(r)}} = \frac{1}{r!}.$$

Différence entre $r = 2$ et $r \geqslant 3$

Définition

Une course $\{m; a_1, ..a_r\}$ est dite non biaisée si pour toute permutation $\sigma \in S_r$ on a :

$$\delta_{m;a_{\sigma(1)},..,a_{\sigma(r)}} = \frac{1}{r!}.$$

Théorème (Cha, 2008)

Soit $m \in \mathcal{M}$. Supposons que LI est vraie. Soit $(a_1, a_2) \in \mathcal{B}_2(m)$. Si a_1, a_2 sont tous les deux des résidus quadratiques modulo m (ou des non-résidus quadratiques modulo m) alors la course $\{m; a_1, a_2\}$ est non biaisée.

Différence entre $r = 2$ et $r \geqslant 3$

$\hookrightarrow$ Si a_1, a_2 et a_3 sont tous des résidus quadratiques modulo m (ou des non-résidus quadratiques modulo m) alors la course $\{m; a_1, a_2, a_3\}$ est-elle non biaisée ?

Différence entre $r = 2$ et $r \geqslant 3$

$\hookrightarrow$ Si a_1, a_2 et a_3 sont tous des résidus quadratiques modulo m (ou des non-résidus quadratiques modulo m) alors la course $\{m; a_1, a_2, a_3\}$ est-elle non biaisée ?

Dans le cas des corps de nombres, la réponse est non.

(Feuerverger et Martin, 2000)

Sous 'certaines hypothèses', on a :

$$\delta(S_{8;3,5,7}) = \delta(S_{8;7,3,5}) > \frac{1}{6}, \quad \delta(S_{8;5,3,7}) = \delta(S_{8;7,3,5}) < \frac{1}{6}$$

et

$$\delta(S_{12;5,7,11}) = \delta(S_{12;11,7,5}) > \frac{1}{6}, \quad \delta(S_{12;5,11,7}) = \delta(S_{12;7,11,5}) < \frac{1}{6}.$$

Différence entre $r = 2$ et $r \geqslant 3$

Théorème (Sedrati, 2021)

Soit $r \geqslant 3$ un entier, $m \in \mathcal{M}$ de degré assez grand. Supposons que (LI $\bigstar$) est vraie. Alors il existe

- $(a_1, \ldots, a_r) \in \mathcal{B}_r(m)$ tel que $a_1, \ldots, a_r$ sont tous des **résidus quadratiques** modulo m et la course $\{m; a_1, a_2, \ldots, a_r\}$ est biaisée.
- $(b_1, \ldots, b_r) \in \mathcal{B}_r(m)$ tel que $b_1, \ldots, b_r$ sont tous des **non-résidus quadratiques** modulo m et la course $\{m; b_1, b_2, \ldots, b_r\}$ est biaisée.

Course m-extrêmement biaisée

Définition

Soit $r \geqslant 3$ un entier, $m \in \mathcal{M}$ de degré assez grand. On dit qu'une course $\{m; a_1, .., a_r\}$ est m-extrêmement biaisée s'il existe une permutation $\sigma \in S_r$ et une constante $c(q,r) > 0$ tel que :

$$\left|\delta_{m;a_{\sigma(1)},..,a_{\sigma(r)}} - \frac{1}{r!}\right| \geqslant \frac{c(q,r)}{\log |m|}.$$

Course m-extrêmement biaisée

Définition

Soit $r \geqslant 3$ un entier, $m \in \mathcal{M}$ de degré assez grand. On dit qu'une course $\{m; a_1, .., a_r\}$ est m-extrêmement biaisée s'il existe une permutation $\sigma \in S_r$ et une constante $c(q, r) > 0$ tel que :

$$\left|\delta_{m;a_{\sigma(1)},..,a_{\sigma(r)}} - \frac{1}{r!}\right| \geqslant \frac{c(q, r)}{\log |m|}.$$

Théorème (Sedrati, 2021)

Soit $r \geqslant 3$ un entier, $(a_1, .., a_r) \in \mathcal{B}_r(m)$ fixé et $m \in \mathcal{M}$ de degré assez grand. Supposons que (LI $\bigstar$) est vraie alors :
La course $\{m; a_1, .., a_r\}$ est m-extrêmement biaisée ssi l'une des deux conditions suivantes est vérifiée :

- $\exists\, 1 \leqslant j \neq k \leqslant r$ tel que $a_j + a_k = 0$.
- $\exists\, 1 \leqslant j \neq k \leqslant r$ tel que a_j/a_k est une puissance de premier.

Que se passe-t-il quand (LI $\bigstar$) est fausse ?

Théorème (Cha, 2008)

Soit $m \in \mathcal{M}$ de degré $\geqslant 2$. Supposons que (LI $\bigstar$) est vérifiée. Soit $(a_1, a_2, a_3) \in \mathcal{B}_3(m)$ tel qu'il existe $\rho \not\equiv 1 \mod m$ qui satisfait les conditions suivantes :

$$\rho^3 \equiv 1 \mod m, \quad a_2 \equiv a_1\rho \mod m, \quad a_3 \equiv a_1\rho^2 \mod m.$$

Alors la course $\{m; a_1, a_2, a_3\}$ est non biaisée.

Que se passe-t-il quand (LI $\bigstar$) est fausse ?

Ce dernier théorème se révèle faux quand (LI $\bigstar$) n'est pas vérifiée. En effet, l'exemple suivant le montre :

Exemple (Sedrati, 2021)

Pour $m = T^2 + T + 1 \in \mathbb{F}_3[T]$, (LI $\bigstar$) est fausse. Si on considère $\rho = T \in \mathbb{F}_3[T]$, $a_1 = 2 \in \mathbb{F}_3[T]$, $a_2 = 2T \in \mathbb{F}_3[T]$ et $a_3 = T + 1 \in \mathbb{F}_3[T]$ alors :

$$\delta_{m;a_3,a_2,a_1} = \frac{1}{4} \neq \frac{1}{6}.$$

Que se passe-t-il quand (LI $\bigstar$) est fausse ?

La généralisation du théorème de Littlewood n'est pas vraie pour les corps de fonctions. En effet :

Exemple (Sedrati, 2021)

Pour $m = T^2 + T + 1 \in \mathbb{F}_3[T]$, on obtient, pour tous les entiers positifs suffisamment grands X, que $\sum_{N=1}^{X} \pi(T, m, N) < \sum_{N=1}^{X} \pi(T+1, m, N)$.
Dans ce cas, on obtient trivialement que

$$\delta_{m;T,T+1} = 0.$$

Que se passe-t-il quand (LI ★) est fausse ?

Rappel

Sous certaines hypothèses, Rubinstein et Sarnak ont prouvé que pour tout $(a_1, \ldots, a_r) \in \mathcal{A}_r(q)$ on a $\delta(S_{q;a_1,a_2,\ldots,a_r}) > 0$.

Ceci n'est pas valable en générale dans le cas des corps de fonctions.

Exemple (Sedrati, 2021)

Pour $m = T(T+1)(T+2) \in \mathbb{F}_3[T]$, on a :

$$\delta_{m;1,T^2+1} = 0.$$

Merci pour votre attention !