

OMNIPRÉSENCE DE SOMMES DE

KLOOSTERMAN

Journées Louis

Antoine

16-17/1/25

COURS 1

Je parlerai plus tard de la première
appartenance historique des sommes de Kloosterman,
mais je voudrais commencer par la première fois
que je les ai rencontrées moi :

→ questions d'équité répartition de
Sommes de Gauss

p nombre premier

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments

$\chi: \mathbb{F}_p \rightarrow \mathbb{C}^\times$ caractère non trivial

e.g. $\chi(x) = \exp\left(\frac{2\pi i}{p} x\right) = e\left(\frac{x}{p}\right)$

ils sont tous de la forme $\chi(ax)$ pour $a \in \mathbb{F}_p^\times$

$\chi: \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times$ caractère multiplicatif

↖ groupe cyclique
d'ordre $p-1$

Définition: la somme de Gauss

$$g(\chi, \chi) = \sum_{x \in \mathbb{F}_p^\times} \chi(x) \chi(x)$$

e.g. $\chi(x) = \begin{cases} 1 & x \text{ est un carré mod } p \\ -1 & x \text{ n'est pas un carré mod } p \end{cases}$

Alors $g(\chi, \chi) = \sum_{x \in \mathbb{F}_p} e\left(\frac{x^2}{p}\right)$ ←

série de Gauss quadratique

c'est celle qui intervient dans "loi" premier de loi loi de réciprocité quadratique

[En effet, $\sum_{x \in \mathbb{F}_p^*} e\left(\frac{x^2}{p}\right) = \sum_{x \in \mathbb{F}_p^*} \left(1 + \left(\frac{x}{p}\right)\right) e\left(\frac{x}{p}\right)$

orthogonalité des caractères
 $\sum_{x \in \mathbb{F}_p} \chi(x) = 0$ si χ non trivial

$= \sum_{x \in \mathbb{F}_p^*} e\left(\frac{x}{p}\right) + g(\chi, \chi)$

$\underbrace{\sum_{x \in \mathbb{F}_p^*} e\left(\frac{x}{p}\right)}_{-1}$

- Si χ est trivial, $g(\chi, \chi) = -1$
- Si χ n'est pas trivial, $|g(\chi, \chi)| = \sqrt{p}$

[En effet,

$|g(\chi, \chi)|^2 = g(\chi, \chi) \overline{g(\chi, \chi)}$

$= \sum_{x, y \in \mathbb{F}_p^*} \chi(x-y) \chi\left(\frac{x}{y}\right)$

$= \sum_{u = \frac{x}{y}} \sum_{u \in \mathbb{F}_p^*} \chi(u) \sum_{y \in \mathbb{F}_p^*} \chi(y(u-1))$

$= -1$ si $u \neq 1$

$= p - \sum_{u \in \mathbb{F}_p^*} \chi(u)$

$= p-1$ si $u=1$

$= p$

]

* Qu'est-ce qu'on peut dire de « l'angle »

$$\theta_{p,X} = \frac{g(Y,X)}{\sqrt{p}} \in S^1$$

Pour le cas particulier X de Legendre, formule close

$$= \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4} \\ i & \text{si } p \equiv 3 \pmod{4} \end{cases}$$

mais pas en général ...

Idee: faire varier tous les courbes X
et voir comment les points $\theta_{p,X} \in S^1$ sont
répartis. $\theta: X_n \rightarrow X$

Définition: (X, μ) espace topologique
compact muni d'une mesure de probabilité
on dit qu'une suite $(x_n)_n$ de points de X
est équidistribuée selon μ si pour toute
fonction continue $f: X \rightarrow \mathbb{C}$ on a

$$(*) \quad \int_X f(x) d\mu = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n \leq N} f(x_n)$$

Il suffit de tester la propriété pour une
classe de fonctions $\neq$ dont les antécédents

livrées sont dens dans $\mathcal{C}(X, \mathbb{C})$ avec la topologie de la convergence uniforme. ↑ fonctions continues

Dans le cas $X = S^1$, le théorème de Stone-Weierstrass implique donc qu'il suffit de tester (*) pour $f(z) = z^n$, $n \in \mathbb{Z}$.

(Deligne)

Théorème: les $p-2$ angles $(\theta_p, x)_{x \text{ racine } p\text{-ième}}$ sont

équidistribués uniformément (= selon la mesure de Haar) dans S^1 lorsque $p \rightarrow \infty$.

Si l'on essaye de contourner la preuve, il faut démontrer

$$\frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) d\theta = \lim_{p \rightarrow \infty} \frac{1}{p-2} \sum_{x \neq 1} f(\theta_p, x)$$

- Pour $f=1$, les deux côtés sont 0
- Pour $f=z^n$ avec $n \neq 0$, l'intégrale est nulle et il faut donc démontrer

$$\lim_{p \rightarrow \infty} \frac{1}{p-2} \sum_{x \neq 1} \left(\frac{g(\psi, x)}{\sqrt{p}} \right)^n = 0$$

(c'est le critère d'équidistribution de Weyl)

(3)

Comme $g(\Psi, X) g(\bar{\Psi}, \bar{X}) = p$,

$$\left(\frac{g(\Psi, X)}{\sqrt{p}} \right)^{-n} = \left(\frac{g(\bar{\Psi}, \bar{X})}{\sqrt{p}} \right)^n$$

et on peut se réduire à $n \geq 1$ quitte à changer le caractère. On calcule:

$$g(\Psi, X)^n = \sum_{x_1, \dots, x_n \in \mathbb{F}_p^x} \Psi(x_1 + \dots + x_n) X(x_1 \dots x_n)$$

$$= \sum_{a \in \mathbb{F}_p^x} X(a) \sum_{\substack{x_1, \dots, x_n \in \mathbb{F}_p^x \\ x_1 \dots x_n = a}} \Psi(x_1 + \dots + x_n)$$

Summe de
Klosterman
 $Kl_n(a, p)$!

Si l'on somme sur tous les caractères non triviaux,

$$\begin{aligned} \sum_{X \neq 1} g(\Psi, X)^n &= -g(\Psi, 1)^n + \sum_{a \in \mathbb{F}_p^x} Kl_n(a, p) \cdot \sum_X X(a) \\ &= (-1)^{n+1} + (p-1) Kl_n(1, p) \end{aligned}$$

par orthogonalité de caractères. On a donc

Moni de savoir que

$$\frac{1}{p^{n/2}(p-2)} \cdot [(-1)^{n+1} + (p-1) \text{Kl}_n(1, p)] \xrightarrow{p \rightarrow \infty} 0$$

c'est-à-dire de donner la valeur absolue

$$\text{de } \text{Kl}_n(1, p) = \sum_{\substack{x_1, \dots, x_{n-1} \\ \in \mathbb{F}_p^\times}} \Psi\left(x_1 + \dots + x_{n-1} + \frac{1}{x_1 \dots x_{n-1}}\right).$$

- Borne triviale: $|\text{Kl}_n(a, p)| \leq (p-1)^{n-1}$

puisque l'on somme autant de termes de l'unité...

- Pour faire mieux, on peut remarquer que

$$X \mapsto g(\Psi, X)^n$$

est la transformée de Fourier au sens du
 groupe abélien fini $\mathbb{F}_p^\times$ de la fonction

$$a \mapsto \text{Kl}_n(a, p)$$

d'où par inversion de Fourier

$$\text{Kl}_n(a, p) = \frac{1}{p-1} \sum_X \overline{X(a)} g(\Psi, X)^n$$

la borne un peu meilleure $|\text{Kl}_n(a, p)| \leq p^{n/2}$

mais toujours insuffisant pour l'équité

Délogre: $|\text{Kl}_n(a, p)| \leq n p^{\frac{n-1}{2}}$

les sommes de Kloosterman chez Poincaré (1912)

« Fonctions modulaires et fonctions
fuchsienues » Ann. Fac. Sci. Toulouse

Cadre: construction de formes modulaires

Soit Γ un groupe agissant sur un
ensemble X . on cherche des fonctions $f: X \rightarrow \mathbb{C}$
satisfaisant à $f(\gamma \cdot x) = f(x)$ pour $\gamma \in \Gamma$
 $x \in X$

Si l'on dispose déjà d'une fonction $F: X \rightarrow \mathbb{C}$
invariante sous l'action d'un sous-groupe $B \subset \Gamma$,
on peut considérer la moyenne

$$f(x) = \sum_{g \in B \backslash \Gamma} F(g \cdot x) \leftarrow \begin{array}{l} \text{bien défini} \\ \text{par invariance} \\ \text{de } F! \end{array}$$

$\cup_{x \in Bx}$

$$\text{Alors } f(\gamma x) = \sum_{g \in B \backslash \Gamma} F(g \gamma x) = \sum_{g' \in B \backslash \Gamma} F(g' x)$$

car la multiplication par γ permute les
classes Bx . Bien sûr, il faut que la somme
converge...

Poincaré applique cette technique à

$$\mathbb{H} = \{z = x + iy \in \mathbb{C} \mid y > 0\}$$

muni de l'action de $SL_2(\mathbb{R})$ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}$$

Cette action étant transitive, on considère
en général le sous-groupe arithmétique $SL_2(\mathbb{Z})$
et même des sous-groupes de congruence

$$\Gamma_0(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{array}{l} ad - bc = 1 \\ \underline{c \equiv 0 \pmod{q}} \end{array} \right\}$$

Une fonction modulaire est alors une
fonction $f: \mathbb{H} \rightarrow \mathbb{C}$ (holomorphe + croissance
modérée au bord de $\mathbb{H}$)

$$f\left(\frac{az+b}{cz+d}\right) = f(z)$$

En général, il est plus simple de construire
des fonctions modulaires de poids k

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

et l'on peut obtenir alors des fonctions modulaires
en prenant des quotients f_1/f_2 de fonctions du
même poids. le sous-groupe est

$\Gamma_\infty \rightarrow B = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\} \subset \Gamma_0(q)$
stabilisateur
du cusp ∞

Un élément de B agit par $z \mapsto z+n$
sur H , donc il suffit de prendre pour F
une fonction 1-périodique, par exemple

$$e(mz) \text{ pour } m \in \mathbb{Z}$$

la première tentative de série de Poincaré

$$P_m(z) = \sum_{g \in B \backslash \Gamma_0(q)} e(mgz)$$

diverge toujours, mais la modification

$$P_m^{(k)}(z) = \sum_{g \in B \backslash \Gamma_0(q)} \frac{e(mgz)}{(cz+d)^k}$$

converge pour tout $k > 2$ et tout $m \geq 0$ par comparaison

(*) avec la série d'Eisenstein $\sum_{\substack{c,d \in \mathbb{Z} \\ (c,d)=1}} \frac{1}{(cz+d)^k}$
qui est "essentielle" de $m=0$. Elle définit
alors une forme modulaire de poids k .

Proposition: la série de Poincaré a
un développement de Fourier (pour $m \geq 1$)

$$P_m^{(k)}(z) = \sum_{n \geq 1} \underline{P_m^k(n)} \cdot e(nz)$$

$$\text{où } p_m^{(k)}(n) = \left(\frac{n}{m}\right)^{\frac{k-1}{2}} \left[\delta_{m,n} - \frac{1}{(2\pi i)^k} \sum_{\substack{c \geq 1 \\ q|c}} \frac{1}{c} S(m, n, c) J_{k-1} \left(\frac{4\pi \sqrt{mn}}{c} \right) \right]$$

$$\text{où } S(m, n, c) = \sum_{x \in (\mathbb{Z}/c\mathbb{Z})^\times} e\left(\frac{mx + nx^{-1}}{c}\right)$$

est la série de Kloosterman et

$$J_{k-1}(z) = \left(\frac{z}{2}\right)^{k-1} \sum_{n \geq 0} \frac{(-1)^n}{n! (n+k-1)!} \left(\frac{z}{2}\right)^{2n}$$

est la fonction de Bessel.

$$= \frac{1}{2\pi i} \int_{|x|=1} e^{\frac{z}{2} \left(x + \frac{1}{x}\right)} \frac{dx}{x^k}$$

Esquisse de preuve

$$* \quad \Gamma_0(q) = B \cup \left(\bigcup_{\substack{c > 0 \\ c \equiv 0 \pmod{q}}} \bigcup_{\substack{d \text{ m.d. } c \\ (c,d)=1}} B \begin{pmatrix} a & b \\ c & d \end{pmatrix} B \right)$$

$\uparrow$ n'importe
 quels a, b avec
 $ad - bc = 1$

* On décompose la somme avec

$$p_m^{(k)}(z) = e(mz) + \sum_{\substack{c > 0 \\ c \equiv 0 \pmod{q}}} \sum_{\substack{d \text{ m.d. } c \\ (c,d)=1}} I(c, d; z)$$

$$\text{où } I(c, d; z) = \sum_{n \in \mathbb{Z}} \frac{e\left(m\left|\frac{a}{c} - \frac{1}{c(c(z+n)+d)}\right|\right)}{(c(z+n)+d)^k} \quad (6)$$

et maintenant on utilise la formule de Poisson

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n)$$

pour une fonction $f(x)$ et sa transformée de

Fourier $\hat{f}(y) = \int_{\mathbb{R}} f(x) e(-xy) dx$, supposant

qu'elles sont toutes les deux dans $L^1(\mathbb{R})$.

on obtient alors l'expression

$$\begin{aligned} I(c, d; z) &= \sum_{n \in \mathbb{Z}} \int_{\mathbb{R}} \frac{e\left(m\left|\frac{a}{c} - \frac{1}{c(c(z+r)+d)}\right|\right)}{(c(z+r)+d)^k} e(-nr) dr \\ &= \sum_{n \in \mathbb{Z}} e\left(\frac{ma + nd}{c}\right) \left(\int_{-\infty + iy}^{+\infty + iy} \frac{e\left(\frac{-m}{c^2 r} - nr\right)}{(cr)^k} dr \right) \end{aligned}$$

$u = z + r + \frac{d}{c}$

$y = \text{Im}(z)$

$e(nz)$

une de Kloosterman

intégrale de Bessel

et on vérifie que l'intégrale s'annule pour $n \leq 0$

□

La seule chose que Lurancé dit dans son
papier sur les séries de Christensen est

« je ne parviens à établir que [...] n'est pas nulle en général »

et que « il n'y a aucune raison pour qu'il
y ait des relations linéaires entre les valeurs
des fonctions de Bessel [...] correspondant aux
différentes valeurs de c », il n'y a donc
aucune raison pour que ce coefficient s'annule

(En fait, les séries de Lurancé $P_m^{(k)}(z)$
représentent les formes modulaires marginales de
poids k pour le groupe $\Gamma_0(q)$).

$$\langle f, P_m^{(k)} \rangle = \int_{\Gamma \backslash \mathbb{H}} f(z) \overline{P_m^{(k)}(z)} \operatorname{Im}(z)^k dz$$
$$= a_m(f)$$

↑
coefficient
de la $n^{\text{ème}}$ série.

les sommes de Kloosterman chez Kloosterman
 « on the representation of numbers in
 the form $ax^2 + by^2 + cz^2 + dt^2 \gg$ (1926)

Théorème (Lagrange)

Tout entier n s'écrit comme somme de 4 carrés, c'est-à-dire est représenté par la forme quadratique

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \quad (*)$$

Plus généralement, on peut se donner des entiers $a, b, c, d \in \mathbb{Z}_{\geq 1}$ et se demander quels sont les entiers représentés par

$$ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$$

(*) et même une formule explicite

$$r_{2,4}(n) = 8 \sum_{\substack{d|n \\ 4 \nmid d}} d$$

Conj: Tout $N \equiv 4 \pmod{24}$
 assez grand,

$$N = p_1^2 + p_2^2 + p_3^2 + p_4^2$$

les formes sont classifiées selon:

- si elles représentent tous les entiers positifs
- sinon

mais d'après Rammingen, il n'y a que 55 valeurs de (a, b, c, d) pour lesquelles c'est le cas,

par exemple $(1, 2, 4, 13)$.

Une question plus intéressante est donc:

- formes qui représentent presque tous les entiers

vs

- formes qui ont un nombre fini d'entiers non représentés

Par exemple, $x_1^2 + x_2^2 + 5x_3^2 + 5x_4^2$ ne représente ps 3 mais d'après Lagrange tous les autres entiers!

Théorème (Klostermann) Supposons qu'il n'y a ps d'structure de congruence. Alors tout entier n assez grand est représenté par $a_1 x_1^2 + \dots + d x_k^2$.

Dans sa thèse, Klostermann avait traité le

cas de 5 variables pour lequel la méthode du cercle s'applique directement "without any new idea", mais en 4 variables le travail d'analyse est plus grand que le travail pur

« The proof is difficult and a very deep analysis is needed »

(2)

Cette analyse fait intervenir les sommes doubles

$$\sum_{\substack{a \leq n \leq b \\ (n, q) = 1}} e\left(\frac{c\bar{n}}{q}\right)$$

↑
l'importante est
celle qui est
entre $n\bar{n} \equiv 1$
mod q

et la méthode de completion qui est expliquée hier dans la notation (si $b-a < q$)

$$\left| \sum_{\substack{a \leq n \leq b \\ (n, q) = 1}} e\left(\frac{c\bar{n}}{q}\right) \right| \leq (1 + \log q) \max_{1 \leq m \leq q} |S(m, c; q)|$$

$$\text{où } S(m, c; q) = \sum_{\substack{n=1, \dots, q \\ (n, q) = 1}} e\left(\frac{mn + c\bar{n}}{q}\right)$$

est la fonction
Klosterman.

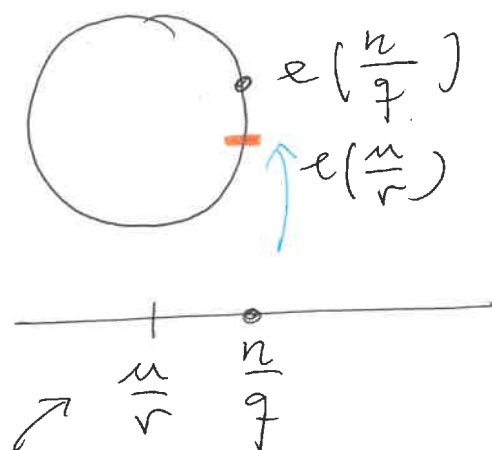
Idee de comment le $\bar{n}$ arrive dans la
fonction

longueur du
segment

$$\frac{nv - nq}{qr} = \frac{1}{qr}$$

et alors $nv \equiv 1$
mod q !

la plus
petite
fonction
réduite avec
denominateur $\leq Q$



Conclusion: Il faut avoir des bons
lens pour les sons $S(m, c; q)$!
La gestion se réduit à traiter le
cas où q est premier.

(3)

Théorème (Kloosterman, 1926) Soit p un nombre premier. Pour tous m, c premiers à p ,

$$|S(m, c; p)| \leq 2 p^{3/4}$$

on change un peu la notation: pour ψ, φ des caractères additifs de $\mathbb{F}_p$ posons

$$S(\psi, \varphi) = \sum_{x \in \mathbb{F}_p^\times} \psi(x) \varphi(x^{-1})$$

de sorte qu'on retrouve $S(m, n; p)$ pour les caractères $\psi(x) = e(m \frac{x}{p})$ et $\varphi(x) = e(n^{-1} \frac{x}{p})$.

Ce sont des nombres réels:

$$\overline{S(\psi, \varphi)} = \sum_{x \in \mathbb{F}_p^\times} \psi(-x) \varphi(-x^{-1}) = S(\psi, \varphi)$$

car le conjugué de ψ coïncide avec son inverse. De plus,

$$S(\psi_b, \varphi_{b^{-1}}) = S(\psi, \varphi) \quad \text{pour tout } b \in \mathbb{F}_p^\times$$

(avec la notation $\psi_b(x) = \psi(bx)$.)

Idee de Kloosterman: toute ligne

$$\sum_{\substack{\psi, \varphi \\ \text{non triviaux}}} |S(\psi, \varphi)|^{2k} \leq M \quad \text{pour } k \geq 1$$

donne lieu à une somme

$$(p-1) |S(\varphi, \psi)|^{2k} = \sum_{b \in \mathbb{F}_p^\times} |S(\varphi_b, \psi_b)|^{2k} \leq M$$

d'où $|S(\varphi, \psi)| \leq \sqrt[2k]{\frac{M}{p-1}}$. on peut en

faire calculer les premières valeurs :

$$\sum_{\psi, \varphi \neq 1} |S(\varphi, \psi)|^{2k} = \begin{cases} (p-1)^2 & k=0 \\ (p-1)(p^2-p-1) & k=1 \\ (p-1)(2p^3-3p^2-3p-1) & k=2 \end{cases}$$

et la dernière égalité donne la borne

$$|S(\varphi, \psi)| < 2p^{3/4}$$

on note en passant que

$$\sum_{\psi, \varphi} |S(\varphi, \psi)|^4 \leq \max_{\psi, \varphi} |S(\varphi, \psi)|^2 \cdot \sum_{\psi, \varphi} |S(\varphi, \psi)|^2$$

et donc il existe φ, ψ tels que

$$|S(\varphi, \psi)|^2 \geq \frac{2p^3-3p^2-3p-1}{p^2-p-1} > 2p-2$$

Preuve: on compare la somme pour toutes les courbes de genre

$$\sum_{\psi, \varphi} |S(\varphi, \psi)|^{2k} - 2(p-1) - (p-1)^{2k}$$

(9)

la somme sur tous les caractères

$$\sum_{\psi, \varphi} |S(\psi, \varphi)|^{2k} = \sum_{\psi, \varphi} \sum_{\substack{x_1, \dots, x_k \in \mathbb{F}_p^\times \\ y_1, \dots, y_k \in \mathbb{F}_p^\times}} (\psi(x_1 + \dots + x_k - y_1 - \dots - y_k) \\ \times \varphi(\frac{1}{x_1} + \dots + \frac{1}{x_k} - \frac{1}{y_1} - \dots - \frac{1}{y_k})) \\ = p^2 \cdot |X_k(\mathbb{F}_p)|$$

$$\text{où } X_k(\mathbb{F}_p) = \left\{ (x, y) \in (\mathbb{F}_p^\times)^{k+k} \mid \begin{array}{l} \sum x_i = \sum y_i \\ \sum \frac{1}{x_i} = \sum \frac{1}{y_i} \end{array} \right\}$$

• Pour $k=1$, $|X_k(\mathbb{F}_p)| = p-1$

• Pour $k=2$, $\begin{cases} x_1 + x_2 = y_1 + y_2 \\ \frac{1}{x_1} + \frac{1}{x_2} = \frac{1}{y_1} + \frac{1}{y_2} \end{cases}$

* Solutions évidentes : on fixe (x_1, x_2)

et on prend $(y_1, y_2) = (x_1, x_2)$ ou $(y_1, y_2) = (x_2, x_1)$

Il y en a $2(p-1)^2 - (p-1)$.

* d'autres ? $(y_1 + y_2, \frac{1}{y_1} + \frac{1}{y_2})$ étant donnés, quels sont les valeurs possibles de (y_1, y_2) :

$$\frac{1}{y_1} + \frac{1}{y_2} = \frac{y_1 + y_2}{y_1 y_2}$$

Si $\frac{1}{y_1} + \frac{1}{y_2} \neq 0$, on peut donc déterminer y_1, y_2 à partir de $(y_1 + y_2, \frac{1}{y_1} + \frac{1}{y_2})$, puisque c'est le cas pour les paires symétriques $(y_1 + y_2, y_1 y_2)$. Donc les nouvelles solutions possibles sont de la forme $(x_1, -x_1, y_1, -y_1)$. Il y en a $(p-1)^2$ mais celles où $y_1 \in \{\pm 1\}$ ont déjà été comptées, d'où $(p-1)^2 - 2(p-1)$. Au total:

$$|X_2(\mathbb{F}_p)| = 3(p-1)^2 - 3(p-1)$$

ce qui donne la formule! □

Remarque: supposons qu'on s'écarte déjà que $|Kl_2(a; p)| \leq 2\sqrt{p}$, de sorte que

$$-2 \leq \frac{Kl_2(a; p)}{\sqrt{p}} \leq 2$$

~~partir d'un certain rang $2\sqrt{p}$ pour p assez grand, on a $|Kl_2(a; p)| < 2\sqrt{p}$ pour $p \rightarrow \infty$~~

○ supposons que les angles soient réels avec les trois de notation α aléatoires dans un sous-groupe compact $K \subset SU_2$. Alors

$$SU_2 \ni \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \begin{matrix} |\alpha|^2 + |\beta|^2 \\ = 1 \end{matrix} \begin{matrix} \text{avec } \alpha, \beta \in \mathbb{F}_p^* \\ \text{et } \alpha \neq \pm \beta \end{matrix} \left(\frac{Kl_2(a; p)}{\sqrt{p}} \right)_{a \in \mathbb{F}_p^*}$$

$$\alpha + \bar{\alpha} = 2\operatorname{Re}(\alpha)$$

$$\begin{aligned}
 \int_K |T_2(g)|^4 d\mu &= \lim_{p \rightarrow \infty} \frac{1}{p-1} \sum_{a \in \mathbb{F}_p} \left(\frac{\text{Kl}_2(a; p)}{\sqrt{p}} \right)^4 \\
 &= \lim_{p \rightarrow \infty} \frac{2p^3 - 3p^2 - 3p - 1}{p^2(p-1)} \\
 &= 2
 \end{aligned}$$

Une théorie ("alternative de Kersh")

implique alors que sont K et fini

sont $K = \mathbb{Q}(\sqrt{2})$

↓ w est fini,
ce sont un
entier
algébrique.

→ Comment le groupe apparaît ?

$$\rho: \pi_1(X) \longrightarrow GL_n(\mathbb{C}) \quad \text{représentation}$$

$$\rho: \pi_1^{\text{ét}}(X) \longrightarrow GL_n(\overline{\mathbb{Q}}_p) \quad \text{représentation}$$

Frob_x

$$x \in X(\mathbb{F}_p)$$

H plus petit
sous-groupe fermé qui
contient $\rho(\text{Frob}_x)$.

K compact
maximal dans H .

①

les sommes de Kloosterman chez Weil (1948)
« on me apportait des sommes »

Théorème (Weil) $|Kl_2(a; p)| \leq 2\sqrt{p}$

Je vais essayer de décrire comment
démontrer ce résultat d'une manière du
nombre de points sur une courbe algébrique
sur un corps fini.

$\mathbb{F}_q$ corps fini à q éléments

$f \in \mathbb{F}_q[X]$ polynôme de degré ≥ 3

qui n'est pas un carré dans $\mathbb{F}_q[X]$

$$C_f: y^2 = f(x)$$

$$|C_f(\mathbb{F}_q)| = \left| \left\{ (x, y) \in \mathbb{F}_q^2 \mid y^2 = f(x) \right\} \right|$$

Théorème (hypothèse de Riemann sur les
corps finis, Weil ¹⁹⁴¹⁻¹⁹⁴⁸ — prouvée
par Serre ¹⁹⁶⁹) Si $q > 4(\deg f)^2$,

$$| |C_f(\mathbb{F}_q)| - q | < 8 \deg f \sqrt{q}.$$

Idee de la preuve

$$\mathbb{F}_p \subset \mathbb{F}_{p^n} \subset \overline{\mathbb{F}_p}$$

avec application trace $\text{tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p} : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_p$

$$\text{tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x) = x + x^p + \dots + x^{p^{n-1}}$$

on définit la somme arithmétique

$$S_n(\psi, \varphi) = \sum_{x \in \mathbb{F}_{p^n}^\times} \psi(\text{tr}(x)) \varphi(\text{tr}(x^{-1}))$$

et on considère la série génératrice

$$Z(\psi, \varphi) = \exp \left(\sum_{n=1}^{\infty} S_n(\psi, \varphi) \frac{T^n}{n} \right)$$

Proposition (Carlitz) Si ψ et φ sont

non triviaux, alors

$$Z(\psi, \varphi) = 1 + S(\psi, \varphi)T + pT^2$$

on en déduit qu'il existe $\alpha_\psi, \beta_\psi \in \mathbb{C}$

tel que

$$\alpha_\psi \beta_\psi = p$$

$$\alpha_\psi + \beta_\psi = -S(\psi, \varphi)$$

$$Z(\psi, \varphi)$$

$$= (1 - \alpha_\psi T)(1 - \beta_\psi T)$$

(2)

et il s'agit de voir que $|\alpha_\Psi| = |\beta_\Psi| = \sqrt{p}$.

Si $\Psi: \mathbb{F}_p \rightarrow \mathbb{C}^\times$ est un caractère fixe, alors tout caractère est de la forme $\Psi_a(x) = \Psi(ax)$, pour $a \in \mathbb{F}_p$ et

$$S(\Psi_a, \Psi_b) = \sum_{x \in \mathbb{F}_p^\times} \Psi(ax + bx^{-1})$$

posons $g(x) = ax + \frac{b}{x}$.

lemme: $|\{y \in \mathbb{F}_{p^n} \mid y^p - y = x\}| = \sum_{\Psi} \Psi(\text{tr}(x))$

$[y^p - y = x \text{ a une solution (et alors elle en a } p) \iff \text{tr}(x) = 0]$

$$\Rightarrow \sum_{\Psi} S_n(\Psi_a, \Psi_b) = \sum_{\Psi} \sum_{x \in \mathbb{F}_p^\times} \Psi(\text{tr}(g(x)))$$

$$= |\{(x, y) \in \mathbb{F}_{p^n}^\times \times \mathbb{F}_{p^n} \mid y^p - y = g(x)\}|$$

• Pour $\Psi = 1$, $S_n(\Psi_a, \Psi_b) = p^n - 1$ N_n

• Pour $\Psi \neq 1$, $\sum_{n=1}^{\infty} S_n(\Psi, \Psi) \frac{T^n}{n} \Rightarrow S_n(\Psi, \Psi) = (\alpha^n + \beta^n)$

$$= -\log(1 - \alpha T) - \log(1 - \beta T)$$

$$= + \sum (\alpha^n + \beta^n) \frac{T^n}{n}$$

$$\Rightarrow N_n = p^n - 1 - \sum_{\Psi \neq 1} (\alpha_{\Psi}^n + \beta_{\Psi}^n)$$

Regardons l'équation $y^p - y = ax + \frac{b}{x}$

En multipliant par x

$$ax^2 - (y^p - y)x + b = 0$$

$\forall n$ on a polynôme en x , le discriminant,
 vaut $(y^p - y)^2 - 4ab$ et on a donc

$$N_n = \left\{ (y, z) \in \mathbb{F}_{p^n}^2 \mid z^2 = \underbrace{(y^p - y)^2 - 4ab}_{\text{polynôme de degré } 2p} \right\}$$

Par le théorème,

$$|N_n - p^n| < 16 p \sqrt{p^n} \quad \text{pour } n \text{ assez grand } (p^n > 16p)$$

on en déduit:

$$\frac{1}{p} \left| \sum_{\Psi \neq 1} (\alpha_{\Psi}^n + \beta_{\Psi}^n) \right| \leq 16 p^{n/2}$$

et on conclut par le lemme suivant:

(3)

lemme: $w_1, \dots, w_2 \in \mathbb{C}$, $A, B \in \mathbb{R}_{>0}$

Si $\left| \sum_{j=1}^2 w_j^n \right| \leq AB^n$ pour n assez grand, alors $|w_j| \leq B$.

(prendre $A = 16p$, $B = \sqrt{p}$)

preuve:
$$f(z) = \sum_{n \geq 1} \left(\sum_{j=1}^2 w_j^n \right) z^n$$

$$= \sum_{j=1}^2 \frac{1}{1 - w_j z}$$

converge dans le disque $|z| < \frac{1}{B}$, et
donc les pôles $1/w_j$ ont $|1/w_j| \geq \frac{1}{B}$

□

