

# Aspects arithmétiques des matrices aléatoires et du chaos quantique

En 20 minutes

E. Kowalski

Université Bordeaux I

14 janvier 2006

# Matrices aléatoires

- On veut étudier des propriétés des matrices de grande taille.

# Matrices aléatoires

- On veut étudier des propriétés des matrices de grande taille.
- On considère les familles naturelles de groupes compacts :  $U(N)$ ,  $Sp(2N)$ ,  $O(N)$ ,  $SO(N)$ ,... Chacun admet une mesure de probabilité naturelle.

# Matrices aléatoires

- On veut étudier des propriétés des matrices de grande taille.
- On considère les familles naturelles de groupes compacts :  $U(N)$ ,  $Sp(2N)$ ,  $O(N)$ ,  $SO(N)$ ,... Chacun admet une mesure de probabilité naturelle.
- On s'intéresse à des limites quand  $N \rightarrow +\infty$ . Leur existence n'est pas du tout évidente.

# Matrices aléatoires

- On veut étudier des propriétés des matrices de grande taille.
- On considère les familles naturelles de groupes compacts :  $U(N)$ ,  $Sp(2N)$ ,  $O(N)$ ,  $SO(N)$ ,... Chacun admet une mesure de probabilité naturelle.
- On s'intéresse à des limites quand  $N \rightarrow +\infty$ . Leur existence n'est pas du tout évidente.
- Par exemple : espacement moyen des angles propres normalisés de matrices unitaires :  $\vartheta_j = \frac{N}{2\pi}\theta_j$ ,  $1 \leq j \leq N$ ,  $\theta_j \in [0, 2\pi]$ . On a

$$\frac{1}{N} \sum_{1 \leq j \leq N} \delta(\vartheta_{j+1} - \vartheta_j) \longrightarrow P(x) dx$$

où  $P(x)$  pour  $x \geq 0$  est  $E''(x)$ ,  $E(x)$  étant un déterminant de Fredholm  $\det(\text{Id} - Q_x)$  sur  $L^2([-1, 1])$ .

# Liens avec l'arithmétique

- Les valeurs  $\zeta(\frac{1}{2} + it)$  avec  $t$  grand sont « modélisées » par des valeurs sur le cercle unité du polynôme caractéristique de matrices unitaires de taille  $N \simeq \log \frac{|t|}{2\pi}$ . Par exemple, Keating et Snaith conjecturent

$$\int_0^T |\zeta(\frac{1}{2} + it)|^{2k} dt \sim a_k g_k T (\log T)^{k^2} \text{ quand } T \rightarrow +\infty,$$

où  $a_k$  est un facteur arithmétique « naturel » et

$$g_k = \lim_{N \rightarrow +\infty} \frac{1}{N^{k^2}} \int_{U(N)} \det(\text{Id} - U) dU = \prod_{j=0}^{k-1} \frac{j!}{(j+k)!}.$$

# Liens avec l'arithmétique

- Les valeurs  $\zeta(\frac{1}{2} + it)$  avec  $t$  grand sont « modélisées » par des valeurs sur le cercle unité du polynôme caractéristique de matrices unitaires de taille  $N \simeq \log \frac{|t|}{2\pi}$ . Par exemple, Keating et Snaith conjecturent

$$\int_0^T |\zeta(\frac{1}{2} + it)|^{2k} dt \sim a_k g_k T (\log T)^{k^2} \text{ quand } T \rightarrow +\infty,$$

où  $a_k$  est un facteur arithmétique « naturel » et

$$g_k = \lim_{N \rightarrow +\infty} \frac{1}{N^{k^2}} \int_{U(N)} \det(\text{Id} - U) dU = \prod_{j=0}^{k-1} \frac{j!}{(j+k)!}.$$

- Similairement, la valeur centrale  $L(f, \frac{1}{2})$  d'une fonction  $L$  de forme modulaire de grand conducteur  $q$  est « modélisée » par la valeur d'un polynôme caractéristique de matrices *orthogonales* de taille  $\simeq \log \frac{q}{2\pi}$ .

# Un exemple de prédiction et de vérification

Théorème (G. Ricotta, à paraître dans Duke Math. J.)

Soit  $k$  fixé,  $g$  forme automorphe holomorphe fixée. Lorsque  $q \rightarrow +\infty$ , il existe une proportion positive de formes automorphes  $f$  de poids  $k$  et niveau  $q$  telles que  $L(f \times g, s)$  a au plus 8 zéros *réels* dans  $]0, 1[$ .

# Un exemple de prédiction et de vérification

Théorème (G. Ricotta, à paraître dans Duke Math. J.)

Soit  $k$  fixé,  $g$  forme automorphe holomorphe fixée. Lorsque  $q \rightarrow +\infty$ , il existe une proportion positive de formes automorphes  $f$  de poids  $k$  et niveau  $q$  telles que  $L(f \times g, s)$  a au plus 8 zéros réels dans  $]0, 1[$ .

- Ingrédient essentiel : un calcul long et difficile de l'asymptotique du moment d'ordre 2 mollifié des fonctions  $L$  en question.

# Un exemple de prédiction et de vérification

## Théorème (G. Ricotta, à paraître dans Duke Math. J.)

Soit  $k$  fixé,  $g$  forme automorphe holomorphe fixée. Lorsque  $q \rightarrow +\infty$ , il existe une proportion positive de formes automorphes  $f$  de poids  $k$  et niveau  $q$  telles que  $L(f \times g, s)$  a au plus 8 zéros réels dans  $]0, 1[$ .

- Ingrédient essentiel : un calcul long et difficile de l'asymptotique du moment d'ordre 2 mollifié des fonctions  $L$  en question.
- Des conjectures dues à Conrey, Farmer et Zirnbauer permettent de prédire rapidement le résultat de ce calcul, ce qui permet de vérifier le calcul. D'autres heuristiques justifient que le calcul aboutisse en définitive au résultat voulu.

# Où trouver des matrices aléatoires ?

- Personne ne sait encore lier directement les fonctions  $L$  globales aux matrices aléatoires.

# Où trouver des matrices aléatoires ?

- Personne ne sait encore lier directement les fonctions  $L$  globales aux matrices aléatoires.
- Katz et Sarnak ont étudié l'analogie géométrique sur des corps finis où des « matrices » apparaissent naturellement, comme représentant l'automorphisme de Frobenius agissant sur certains espaces vectoriels de dimension fini.

Ils obtiennent des confirmations théoriques du type suivant :

$$\lim_{N \rightarrow +\infty} \lim_{q \rightarrow +\infty} (\text{quantité sur } \mathbf{F}_q \text{ avec des matrices de taille } N)$$
$$= \lim_{N \rightarrow +\infty} (\text{quantité analogue pour matrices aléatoires de taille } N).$$

# Où trouver des matrices aléatoires ?

- Personne ne sait encore lier directement les fonctions  $L$  globales aux matrices aléatoires.
- Katz et Sarnak ont étudié l'analogie géométrique sur des corps finis où des « matrices » apparaissent naturellement, comme représentant l'automorphisme de Frobenius agissant sur certains espaces vectoriels de dimension fini.

Ils obtiennent des confirmations théoriques du type suivant :

$$\lim_{N \rightarrow +\infty} \lim_{q \rightarrow +\infty} (\text{quantité sur } \mathbf{F}_q \text{ avec des matrices de taille } N)$$
$$= \lim_{N \rightarrow +\infty} (\text{quantité analogue pour matrices aléatoires de taille } N).$$

- On souhaite *enlever la limite intérieure sur  $q$*  pour obtenir des résultats plus convaincants.

# Un exemple de famille à la Katz-Sarnak

Voici un exemple de ce qu'il est possible de faire. Soit  $f \in \mathbf{Z}[X]$  unitaire de degré  $2g$  à racines simples,  $p \nmid \text{disc}(f)$ ,  $\mathbf{F}_q$  un corps à  $q = p^k$  éléments. Pour  $t \in \mathbf{F}_q$  tel que  $f(t) \neq 0$ , soit  $C_t$  le modèle projectif lisse (de genre  $g$ ) de la courbe plane définie sur  $\mathbf{F}_q$  d'équation

$$y^2 = f(x)(x - t).$$

Soit

$$Z(C_t) = \exp\left(\sum_{f \geq 1} \frac{|C_t(\mathbf{F}_{q^f})|}{f} T^f\right)$$

la fonction zéta de  $C_t/\mathbf{F}_q$ .

## ... avec des matrices de grande taille...

- On peut écrire (F.K. Schmidt, A. Weil)

$$Z(C_t) = \frac{P_t(T)}{(1-T)(1-qT)}, \text{ avec } P_t = \det(\text{Id} - TF_t) \in \mathbf{Z}[T]$$

où  $F_t$  (Frobenius) agit ici comme similitude symplectique sur un espace (fixe) de dimension  $2g$ . La limite  $g \rightarrow +\infty$  est donc la limite des matrices aléatoires, dans le groupe symplectique.

## ... avec des matrices de grande taille...

- On peut écrire (F.K. Schmidt, A. Weil)

$$Z(C_t) = \frac{P_t(T)}{(1-T)(1-qT)}, \text{ avec } P_t = \det(\text{Id} - TF_t) \in \mathbf{Z}[T]$$

où  $F_t$  (Frobenius) agit ici comme similitude symplectique sur un espace (fixe) de dimension  $2g$ . La limite  $g \rightarrow +\infty$  est donc la limite des matrices aléatoires, dans le groupe symplectique.

- Un résultat de J-K. Yu montre que  $F_t$ , lorsque  $t$  varie, est équiréparti dans les similitudes symplectiques (avec le bon multiplicateur).

.. où la théorie analytique des nombres intervient

Théorème (E. K. ; à paraître dans Crelle)

Il existe une constante  $C \geq 0$  absolue telle que

$$|\{t \in \mathbf{F}_q \mid P_t \text{ est réductible}\}| \leq Cq^{1-\gamma_g}(\log q),$$

où  $\gamma_g = \frac{1}{4g^2+3g+5}$ .

## .. où la théorie analytique des nombres intervient

Théorème (E. K. ; à paraître dans Crelle)

Il existe une constante  $C \geq 0$  absolue telle que

$$|\{t \in \mathbf{F}_q \mid P_t \text{ est réductible}\}| \leq Cq^{1-\gamma_g}(\log q),$$

où  $\gamma_g = \frac{1}{4g^2+3g+5}$ .

- Ceci est encore « insuffisant » pour  $q$  fixé,  $g \rightarrow +\infty$ , mais permet de faire une limite « diagonale » où  $g \rightarrow +\infty$  tant que  $q$  est un peu plus grand que  $e^{g^2}$ .

## .. où la théorie analytique des nombres intervient

Théorème (E. K. ; à paraître dans Crelle)

Il existe une constante  $C \geq 0$  absolue telle que

$$|\{t \in \mathbf{F}_q \mid P_t \text{ est réductible}\}| \leq Cq^{1-\gamma_g}(\log q),$$

où  $\gamma_g = \frac{1}{4g^2+3g+5}$ .

- Ceci est encore « insuffisant » pour  $q$  fixé,  $g \rightarrow +\infty$ , mais permet de faire une limite « diagonale » où  $g \rightarrow +\infty$  tant que  $q$  est un peu plus grand que  $e^{g^2}$ .
- La méthode est basée sur l'injection d'idées « classiques » de théorie analytique des nombres : les inégalités de « grand crible ». Elle utilise cruciallement les résultats de Deligne sur l'hypothèse de Riemann sur les corps finis.

## D'autres matrices « aléatoires »...

- Les résultats précédents portant sur l'irréductibilité de certains polynômes caractéristiques suggèrent la question suivante : soit  $n \geq 1$  fixé,  $X \geq 1$ . Combien de matrices  $M \in SL(n, \mathbf{Z})$  telles que  $\|M\| \leq X$  sont telles que  $\det(\text{Id} - MX) \in \mathbf{Z}[X]$  soit irréductible ?

## D'autres matrices « aléatoires »...

- Les résultats précédents portant sur l'irréductibilité de certains polynômes caractéristiques suggèrent la question suivante : soit  $n \geq 1$  fixé,  $X \geq 1$ . Combien de matrices  $M \in SL(n, \mathbf{Z})$  telles que  $\|M\| \leq X$  sont telles que  $\det(\text{Id} - MX) \in \mathbf{Z}[X]$  soit irréductible ?
- On peut aussi vouloir remplacer le groupe  $SL(n, \mathbf{Z})$  par un groupe « arithmétique » plus général, par exemple les matrices symplectiques  $Sp(2n, \mathbf{Z})$ , ou des sous-groupes d'indice fini (voire infini).

... amènent au...

- Dans ce cas, un analogue du grand crible peut être considéré. Il se ramène à des problèmes d'estimation de sommes du type

$$\sum_{\substack{M \in SL(n, \mathbf{Z}) \\ \|M\| \leq X}} \text{Tr}(\rho_d(M))$$

où

$$\rho_d : SL(n, \mathbf{Z}) \rightarrow SL(n, \mathbf{Z}/d\mathbf{Z}) \xrightarrow{\tilde{\rho}_d} GL(\deg(\tilde{\rho}_d), \mathbf{C})$$

est obtenue à l'aide d'une représentation linéaire de  $SL(n, \mathbf{Z}/d\mathbf{Z})$ .

## ... amènent au...

- Dans ce cas, un analogue du grand crible peut être considéré. Il se ramène à des problèmes d'estimation de sommes du type

$$\sum_{\substack{M \in SL(n, \mathbf{Z}) \\ \|M\| \leq X}} \text{Tr}(\rho_d(M))$$

où

$$\rho_d : SL(n, \mathbf{Z}) \rightarrow SL(n, \mathbf{Z}/d\mathbf{Z}) \xrightarrow{\tilde{\rho}_d} GL(\text{deg}(\tilde{\rho}_d), \mathbf{C})$$

est obtenue à l'aide d'une représentation linéaire de  $SL(n, \mathbf{Z}/d\mathbf{Z})$ .

- Ces sommes peuvent se traiter en se ramenant à des problèmes de points entiers et de norme bornée dans les sous-groupes de congruences

$$\Gamma_n(d) = \{M \in SL(n, \mathbf{Z}) \mid M \equiv \text{Id} \pmod{d}\}.$$

## ... spectre du laplacien...

- Typiquement on a un développement

$$\sum_{\substack{M \in \Gamma_n(d) \\ \|M\| \leq X}} 1 = \frac{c_n}{|SL(n, \mathbf{Z}/d\mathbf{Z})|} X^{n^2-n} + \sum_j c_{n,j} X^{s_j} + \dots$$

où les exposants avec  $\operatorname{Re}(s_j) < n^2 - n$  dépendent de  $d$  (et  $n$ ) et correspondent au spectre du laplacien sur le quotient  $\Gamma_n(d) \backslash SL(n, \mathbf{R})$  (non compact, de volume fini).

## ... spectre du laplacien...

- Typiquement on a un développement

$$\sum_{\substack{M \in \Gamma_n(d) \\ \|M\| \leq X}} 1 = \frac{c_n}{|SL(n, \mathbf{Z}/d\mathbf{Z})|} X^{n^2-n} + \sum_j c_{n,j} X^{s_j} + \dots$$

où les exposants avec  $\operatorname{Re}(s_j) < n^2 - n$  dépendent de  $d$  (et  $n$ ) et correspondent au spectre du laplacien sur le quotient  $\Gamma_n(d) \backslash SL(n, \mathbf{R})$  (non compact, de volume fini).

- *Le point essentiel est d'avoir un « trou spectral » uniforme*

$$n^2 - n - \operatorname{Re}(s_j) \geq \delta_n > 0$$

*indépendant du niveau  $d$ . C'est un résultat profond, qui dans le cas  $n = 2$  est dû à Selberg. Dans le cas  $n \geq 3$ , un résultat de ce type est dû à Luo, Rudnick et Sarnak. Il fait appel à des méthodes basées sur l'étude des zéros de fonctions  $L$  automorphes.*

## ...au chaos quantique arithmétique...

- L'étude du spectre du laplacien sur des quotients du type  $\Gamma_n(d) \backslash SL(n, \mathbf{R})$  pour les grandes valeurs propres est le sujet du « chaos quantique arithmétique ». Rudnick et Sarnak conjecturent que les fonctions propres  $L^2$  normalisées convergent faiblement vers la mesure de Haar lorsque  $\lambda \rightarrow +\infty$ .

## ...au chaos quantique arithmétique...

- L'étude du spectre du laplacien sur des quotients du type  $\Gamma_n(d) \backslash SL(n, \mathbf{R})$  pour les grandes valeurs propres est le sujet du « chaos quantique arithmétique ». Rudnick et Sarnak conjecturent que les fonctions propres  $L^2$  normalisées convergent faiblement vers la mesure de Haar lorsque  $\lambda \rightarrow +\infty$ .
- L'étude des petites valeurs propres lorsque le niveau  $d$  tend vers l'infini semble analogue, mais est encore mal compris. G. Ricotta étudie la norme  $L^\infty$  de fonctions propres sur  $\Gamma_2(d) \backslash SL(2, \mathbf{R})$  par rapport au niveau, où des phénomènes arithmétiques nouveaux apparaissent par rapport à l'étude pour  $d$  fixé et  $\lambda \rightarrow +\infty$  faite par Iwaniec et Sarnak.

## ...et au programme de Langlands !

- On peut espérer montrer ainsi que « presque toute » matrice unimodulaire  $n \times n$  a polynôme caractéristique irréductible.

## ...et au programme de Langlands !

- On peut espérer montrer ainsi que « presque toute » matrice unimodulaire  $n \times n$  a polynôme caractéristique irréductible.
- Pour les matrices *symplectiques* : tout marche... si ce n'est que le « trou spectral » n'est pas évident à obtenir. La méthode la plus directe semble de dire que les fonctions propres du laplacien peuvent être choisies fonctions propres des opérateurs de Hecke, et que Langlands prédit qu'il existe alors une fonction automorphe sur  $SL(2n, \mathbf{Z})$  avec les mêmes valeurs propres... à laquelle on peut appliquer le résultat de L-R-S...

# Un peu de prospective

- Pour le Chaos Quantique Arithmétique, dans le cas de  $SL(2, \mathbf{R})$ , la conjecture basique a été démontrée (dans le cas co-compact) par E. Lindenstrauss en faisant appel à des méthodes de théorie ergodique (théorie de Ratner, calculs d'entropie...) La théorie de Ratner en particulier s'est révélée pleine d'applications arithmétiques inattendues, par exemple en approximation diophantienne. Obtenir des résultats quantitatifs est un problème majeur.

# Un peu de prospective

- Pour le Chaos Quantique Arithmétique, dans le cas de  $SL(2, \mathbf{R})$ , la conjecture basique a été démontrée (dans le cas co-compact) par E. Lindenstrauss en faisant appel à des méthodes de théorie ergodique (théorie de Ratner, calculs d'entropie...) La théorie de Ratner en particulier s'est révélée pleine d'applications arithmétiques inattendues, par exemple en approximation diophantienne. Obtenir des résultats quantitatifs est un problème majeur.
- Récemment, Katz a développé une méthode très arithmétique pour trouver le type de symétrie (unitaire, orthogonal, symplectique) d'une famille algébrique (« l'alternative de Larsen »). Il serait intéressant de trouver l'analogue pour des fonctions  $L$  pour éclairer le cas global.