

# Arithmetic Aspects of Random Matrices and Quantum Chaos

In 20 minutes

E. Kowalski

Université Bordeaux I

January 14, 2006

# Random matrices

- The goal is to study properties of matrices of large size.

# Random matrices

- The goal is to study properties of matrices of large size.
- Consider the natural families of compact groups:  $U(N)$ ,  $USp(2N)$ ,  $O(N)$ ,  $SO(N)$ ,... Each carries a natural probability measure.

# Random matrices

- The goal is to study properties of matrices of large size.
- Consider the natural families of compact groups:  $U(N)$ ,  $USp(2N)$ ,  $O(N)$ ,  $SO(N)$ ,... Each carries a natural probability measure.
- We are interested in limits when  $N \rightarrow +\infty$ . The existence of such limits is by no means obvious.

# Random matrices

- The goal is to study properties of matrices of large size.
- Consider the natural families of compact groups:  $U(N)$ ,  $USp(2N)$ ,  $O(N)$ ,  $SO(N)$ ,... Each carries a natural probability measure.
- We are interested in limits when  $N \rightarrow +\infty$ . The existence of such limits is by no means obvious.
- Example: the mean spacing of normalized eigen-angles of unitary matrices; let  $\vartheta_j = \frac{N}{2\pi}\theta_j$ ,  $1 \leq j \leq N$ ,  $\theta_j \in [0, 2\pi]$ . Then we have

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

where  $P(x)$  for  $x \geq 0$  is  $E''(x)$ ,  $E(x)$  being a Fredholm determinant  $\det(\text{Id} - Q_x)$  on  $L^2([-1, 1])$ .

## Links with arithmetics

- The values  $\zeta(\frac{1}{2} + it)$  with  $t$  large are “modeled” by values on the unit circle of characteristic polynomials of unitary matrices of size  $N \simeq \log \frac{|t|}{2\pi}$ . For instance, Keating and Snaith conjecture

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

where  $a_k$  is a natural arithmetic factor and

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

## Links with arithmetics

- The values  $\zeta(\frac{1}{2} + it)$  with  $t$  large are “modeled” by values on the unit circle of characteristic polynomials of unitary matrices of size  $N \simeq \log \frac{|t|}{2\pi}$ . For instance, Keating and Snaith conjecture

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

where  $a_k$  is a natural arithmetic factor and

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

- Similarly, the central value  $L(f, \frac{1}{2})$  of the  $L$ -function of a modular form with large conductor  $q$  is “modeled” by values of the characteristic polynomial of *orthogonal* matrices of size  $\simeq \log \frac{q}{2\pi}$ .

# An example of prediction and confirmation

Theorem (G. Ricotta, to appear in *Duke Math. J.*)

Let  $k$  be fixed, let  $g$  be a fixed holomorphic modular form. As  $q \rightarrow +\infty$ , there exists a positive proportion of newforms  $f$  of weight  $k$  and level  $q$  such that  $L(f \times g, s)$  has at most 8 *real* zeros in  $]0, 1[$ .

# An example of prediction and confirmation

Theorem (G. Ricotta, to appear in *Duke Math. J.*)

Let  $k$  be fixed, let  $g$  be a fixed holomorphic modular form. As  $q \rightarrow +\infty$ , there exists a positive proportion of newforms  $f$  of weight  $k$  and level  $q$  such that  $L(f \times g, s)$  has at most 8 *real* zeros in  $]0, 1[$ .

- Essential tool: a long and difficult computation of the asymptotics of the mollified second moment of those  $L$ -functions.

# An example of prediction and confirmation

Theorem (G. Ricotta, to appear in *Duke Math. J.*)

Let  $k$  be fixed, let  $g$  be a fixed holomorphic modular form. As  $q \rightarrow +\infty$ , there exists a positive proportion of newforms  $f$  of weight  $k$  and level  $q$  such that  $L(f \times g, s)$  has at most 8 *real* zeros in  $]0, 1[$ .

- Essential tool: a long and difficult computation of the asymptotics of the mollified second moment of those  $L$ -functions.
- Conjectures of Conrey, Farmer and Zirnbauer predict very precisely the result of this computation, which provides a good way to check for discrepancies. Other heuristics justify that the result provide the desired result.

# Where to find random matrices?

- Nobody knows (yet) how to link directly global  $L$ -functions and random matrices.

# Where to find random matrices?

- Nobody knows (yet) how to link directly global  $L$ -functions and random matrices.
- Katz and Sarnak have studied the geometric analogue over finite fields, where “matrices ” appear naturally as representing the Frobenius automorphism acting on certain finite-dimensional vector spaces.

This way, they obtain theoretical evidence of the type:

$$\lim_{N \rightarrow +\infty} \lim_{q \rightarrow +\infty} (\text{quantity over } \mathbf{F}_q \text{ with matrices of size } N)$$
$$= \lim_{N \rightarrow +\infty} (\text{analogue quantity for random matrices of size } N).$$

# Where to find random matrices?

- Nobody knows (yet) how to link directly global  $L$ -functions and random matrices.
- Katz and Sarnak have studied the geometric analogue over finite fields, where “matrices ” appear naturally as representing the Frobenius automorphism acting on certain finite-dimensional vector spaces.

This way, they obtain theoretical evidence of the type:

$$\begin{aligned} & \lim_{N \rightarrow +\infty} \lim_{q \rightarrow +\infty} (\text{quantity over } \mathbf{F}_q \text{ with matrices of size } N) \\ &= \lim_{N \rightarrow +\infty} (\text{analogue quantity for random matrices of size } N). \end{aligned}$$

- It would be very desirable to *remove the inner limit over  $q$*  to obtain even more convincing evidence.

## An example of a Katz-Sarnak type family

Here is an example of what turns out to be doable. Let  $f \in \mathbf{Z}[X]$  be monic of degree  $2g$  with simple roots,  $p \nmid \text{disc}(f)$ ,  $\mathbf{F}_q$  field with  $q = p^k$  elements. For  $t \in \mathbf{F}_q$  such that  $f(t) \neq 0$ , let  $C_t$  be the smooth projective model (of genus  $g$ ) of the plane curve over  $\mathbf{F}_q$  with equation

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

Let

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

be the zeta function of  $C_t/\mathbf{F}_q$ .

## ... with matrices of large size...

- It can be expressed as (F.K. Schmidt, A. Weil)

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

where  $F_t$  (Frobenius) acts here as a symplectic similitude on a fixed space of dimension  $2g$ . The limit  $g \rightarrow +\infty$  is therefore the random matrix limit; the symmetry type is symplectic.

## ... with matrices of large size...

- It can be expressed as (F.K. Schmidt, A. Weil)

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

where  $F_t$  (Frobenius) acts here as a symplectic similitude on a fixed space of dimension  $2g$ . The limit  $g \rightarrow +\infty$  is therefore the random matrix limit; the symmetry type is symplectic.

- A result of J-K. Yu shows that  $F_t$ , as  $t$  varies, is equidistributed in the group of symplectic similitudes (with the correct multiplier).

.. where analytic number theory comes into play

Theorem (E. K.; to appear in *Crelle*)

There exists an absolute constant  $C \geq 0$  such that

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

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

.. where analytic number theory comes into play

Theorem (E. K.; to appear in *Crelle*)

There exists an absolute constant  $C \geq 0$  such that

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

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

- This is still not good for fixed  $q$ ,  $g \rightarrow +\infty$ , but it allows “diagonal” limits where  $g \rightarrow +\infty$  as long as  $q$  is slightly larger than  $e^{g^2}$ .

## .. where analytic number theory comes into play

### Theorem (E. K.; to appear in *Crelle*)

There exists an absolute constant  $C \geq 0$  such that

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

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

- This is still not good for fixed  $q$ ,  $g \rightarrow +\infty$ , but it allows “diagonal” limits where  $g \rightarrow +\infty$  as long as  $q$  is slightly larger than  $e^{g^2}$ .
- The method is based on the injection of classical ideas of analytic number theory, the large-sieve inequalities. It uses crucially the results of Deligne on the Riemann Hypothesis over finite fields.

## Other “random” matrices...

- The previous result concerning irreducibility of some polynomials suggests the following question: let  $n \geq 1$  (fixed, to begin with),  $X \geq 1$ . How many matrices  $M \in SL(n, \mathbf{Z})$  such that  $\|M\| \leq X$  have reducible characteristic polynomial  $\det(\text{Id} - MX) \in \mathbf{Z}[X]$ ?

## Other “random” matrices...

- The previous result concerning irreducibility of some polynomials suggests the following question: let  $n \geq 1$  (fixed, to begin with),  $X \geq 1$ . How many matrices  $M \in SL(n, \mathbf{Z})$  such that  $\|M\| \leq X$  have reducible characteristic polynomial  $\det(\text{Id} - MX) \in \mathbf{Z}[X]$ ?
- One may also wish to replace the group  $SL(n, \mathbf{Z})$  by more general “arithmetic” groups, such as  $Sp(2n, \mathbf{Z})$ , or finite (even infinite) index subgroups.

... leading to...

- In this case, we can expect an analogue of the large sieve inequality. It boils down to estimating sums of the type

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

where

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

is obtained using a linear representation of  $SL(n, \mathbf{Z}/d\mathbf{Z})$ .

... leading to...

- In this case, we can expect an analogue of the large sieve inequality. It boils down to estimating sums of the type

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

where

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

is obtained using a linear representation of  $SL(n, \mathbf{Z}/d\mathbf{Z})$ .

- These sums may be treated by reducing to a problem of counting integral points with bounded norm in congruence subgroups

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

## ... the spectrum of the Laplacian...

- Typically, there is an expansion

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

where the exponents with  $\operatorname{Re}(s_j) < n^2 - n$  depend on  $d$  (and  $n$ ) and correspond to the spectrum of the Laplacian on the quotient  $\Gamma_n(d) \backslash SL(n, \mathbf{R})$  (non compact, with finite volume).

## ... the spectrum of the Laplacian...

- Typically, there is an expansion

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

where the exponents with  $\operatorname{Re}(s_j) < n^2 - n$  depend on  $d$  (and  $n$ ) and correspond to the spectrum of the Laplacian on the quotient  $\Gamma_n(d) \backslash SL(n, \mathbf{R})$  (non compact, with finite volume).

- The essential point is to have a uniform “spectral gap”*

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

*independently of the level  $d$ .* This is a deep result, which for  $n = 2$  is due to Selberg. In the case  $n \geq 3$ , a result of this type is due to Luo, Rudnick et Sarnak. It uses methods based on the study of zeros of automorphic  $L$ -functions.

## ...to Arithmetic Quantum Chaos...

- The study of the spectrum of the Laplacian on quotients like  $\Gamma_n(d)\backslash SL(n, \mathbf{R})$  for large eigenvalues is the subject matter of “arithmetic quantum chaos”. Rudnick and Sarnak conjecture that the normalized  $L^2$  eigenfunctions converge weakly to Haar measure as  $\lambda \rightarrow +\infty$ .

## ...to Arithmetic Quantum Chaos...

- The study of the spectrum of the Laplacian on quotients like  $\Gamma_n(d)\backslash SL(n, \mathbf{R})$  for large eigenvalues is the subject matter of “arithmetic quantum chaos”. Rudnick and Sarnak conjecture that the normalized  $L^2$  eigenfunctions converge weakly to Haar measure as  $\lambda \rightarrow +\infty$ .
- The study of small eigenvalues as the level  $d$  tends to infinity seems analogue, but is badly understood. G. Ricotta is investigating the  $L^\infty$  norm of eigenfunctions on  $\Gamma_2(d)\backslash SL(2, \mathbf{R})$  with respect to the level, where new arithmetic phenomena occur, compared with the case of fixed  $d$  and  $\lambda \rightarrow +\infty$  investigated by Iwaniec and Sarnak.

## ...and to the Langlands program!

- One may hope to show this way that “almost all” unimodular  $n \times n$  matrices have irreducible characteristic polynomial.

## ...and to the Langlands program!

- One may hope to show this way that “almost all” unimodular  $n \times n$  matrices have irreducible characteristic polynomial.
- For *symplectic* matrices: everything should work... except that the “spectral gap” is not obvious. The most direct method seems to say that eigenfunctions of the Laplacian may be chosen to be eigenfunctions of the Hecke operators, and then Langlands predicts the existence of an automorphic function on  $SL(2n, \mathbf{Z})$  with the same spectral parameters... for which the result of L-R-S apply.

## Some dreams and hopes

- The basic conjecture of Arithmetic Quantum Chaos for  $SL(2, \mathbf{R})$  has been proved (in the co-compact case) by E. Lindenstrauss using methods of ergodic theory (Ratner theory, entropy computations). Ratner theory in particular has many other unexpected arithmetic applications (e.g. in diophantine approximation). A major problem is to quantify all those results.

# Some dreams and hopes

- The basic conjecture of Arithmetic Quantum Chaos for  $SL(2, \mathbf{R})$  has been proved (in the co-compact case) by E. Lindenstrauss using methods of ergodic theory (Ratner theory, entropy computations). Ratner theory in particular has many other unexpected arithmetic applications (e.g. in diophantine approximation). A major problem is to quantify all those results.
- Recently, Katz has found a new method, highly arithmetic, for determining the symmetry type of an algebraic family (“the Larsen alternative”). It would be interesting to find the analogue of this for global  $L$ -functions.