BOOK REVIEWS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 51, Number 1, January 2014, Pages 141–149
S 0273-0979(2013)01412-5
Article electronically published on June 10, 2013

Convolution and equidistribution: Sato-Tate theorems for finite fields Mellin transforms, by N. Katz, Annals of Mathematical Studies, 180, Princeton University Press, Princeton, NJ, 2012, viii+203 pages pp., ISBN 13: 978-0-691-15331-5, cloth, US $75.00

1. Equidistribution

The story of equidistribution in number theory began about a hundred years ago with H. Weyl's paper [18] concerning the distribution of sequences of real numbers modulo 1, and more generally that of points in euclidean space modulo a lattice. The theme of equidistribution has since become one of the most important unifying viewpoints in number theory. Equidistribution statements exist in many areas of number theory, which would otherwise seem to be very distant, and lead to sometimes surprising connections and applications (as can be seen, for instance, with the quantum unique ergodicity conjecture [15], expander graphs, especially Cayley graphs [13], ergodic theory of large groups [2], or the Sato-Tate conjecture [14], to give only examples taken from recent articles or reviews in the *Bulletin of the AMS*). Because equidistribution is a twin of the probabilistic idea of convergence in law, it also introduces strong links between arithmetic and fields, such as probability theory or ergodic theory. In addition to applications, one might add that equidistribution theorems are often by themselves extremely beautiful.

In this review, we will work with the following definition, which is sufficient: given a compact topological space X and a Borel probability measure μ on X (i.e., a Borel measure such that $\mu(X) = 1$), and given a sequence (Y_n) of (nonempty) finite sets[1] together with maps

$$\theta_n : Y_n \longrightarrow X,$$

one says that (Y_n, θ_n) becomes *equidistributed in X with respect to μ* if, for any continuous function $f : X \longrightarrow \mathbf{C}$, we have

$$\int_X f(x)d\mu(x) = \lim_{n\to+\infty} \frac{1}{|Y_n|} \sum_{y\in Y_n} f(\theta_n(y)). \tag{1.1}$$

It is not very difficult to derive an equivalent form of this definition which clarifies the terminology: we have equidistribution if and only if, for any Borel subset $A \subset X$

2010 *Mathematics Subject Classification.* Primary 11Txx, 20Gxx, 14Fxx.

[1] We use n as parameter, but this does not always range over positive integers; in Theorem 2.1, for instance, the parameter will be a finite field of size growing to infinity.

such that the boundary $\partial(A) = \bar{A} - \mathring{A}$ satisfies $\mu(\partial(A)) = 0$, we have

$$\mu(A) = \lim_{n\to+\infty} \frac{|\{y \in Y_n \mid \theta_n(y) \in A\}|}{|Y_n|}, \tag{1.2}$$

or in other words, if the "right" proportion (according to μ) of the $\theta_n(y)$ lies in the set A.

The original case considered by H. Weyl is that of $X = \mathbf{R}/\mathbf{Z}$, where the measure μ is given by the Lebesgue measure, and one considers a sequence $(x_j)_{j\geqslant 1}$ and takes $Y_n = \{1, \dots, n\}$ and

$$\theta_n(j) = x_j \,(\mathrm{mod}\, \mathbf{Z}), \text{ for } 1 \leqslant j \leqslant n.$$

If there is equidistribution for such a choice, one says that (x_n) is *equidistributed modulo* 1. Weyl's first important insight is that one can find another equivalent formulation by selecting a convenient family of "test functions" f for which one should check (1.1). He immediately proves the first case of what is now known as the *Weyl criterion* for equidistribution: a sequence (Y_n, θ_n) becomes equidistributed in $X = \mathbf{R}/\mathbf{Z}$ with respect to Lebesgue measure if and only if, for any nonzero integer $h \in \mathbf{Z}$, we have

$$\lim_{n\to+\infty} \frac{1}{|Y_n|} \sum_{y\in Y_n} e(h\theta_n(y)) = 0, \tag{1.3}$$

where $e(z) = e^{2i\pi z}$. The point is that the functions

$$f_h : x \mapsto e(hx) \tag{1.4}$$

for $h \in \mathbf{Z}$ are continuous functions whose linear combinations span a dense subset of the space of continuous functions on $\mathbf{R}/\mathbf{Z}$, and furthermore that for $h = 0$, the relation (1.1) is automatically satisfied, while for $h \neq 0$, the integral of f_h that appears on the right-hand side of (1.1) is zero. In the examples to be discussed in this review, it is by means of a suitable form of this criterion that equidistribution will be obtained.

Example 1.1. The standard example (indeed, the first in [18]) is that of the sequence $x_j = j\alpha$, where $\alpha \in \mathbf{R} - \mathbf{Q}$ is a fixed irrational number. Checking (1.3) is a simple matter of summing a finite geometric sequence whereas proving (1.2) directly is by no means easy, even more so when dealing with the analogue question for the equidistribution of the sequence $x_i = (i\alpha_1, \dots, i\alpha_k)$ in a higher-dimensional torus $(\mathbf{R}/\mathbf{Z})^k$, whereas the Weyl criterion extends very simply.

Remark 1.2. The reader may enjoy viewing the recent Minerva lecture of J.-P. Serre [16], which discuss equidistribution and topics related to it, in a context close to what we consider here.

2. Deligne's equidistribution theorem

The specific equidistribution result which leads to the heart of the matter for this review is Deligne's equidistribution theorem [1, Th. 2.1.12] (see also the versions of Katz [6, Ch. 3] and Katz and Sarnak [10, §9.2]). A full statement of this very general result involves necessarily many deep notions in algebraic geometry, but it has direct connections with the classical Chebotarev density theorem of algebraic number theory and is motivated by extremely concrete examples. We present one

here before giving an overview of the strategy of the proof, which depends crucially on Deligne's most general version of the Riemann Hypothesis over finite fields.

Let p be a prime number, and let k be a finite field of characteristic p. We denote by $\mathrm{tr}_{k/\mathbf{F}_p}$ the trace map from k to the subfield $\mathbf{F}_p$. For $a \in k^\times$, let

$$S(a;k) = \sum_{x \in k^\times} e\Big(\frac{\mathrm{tr}_{k/\mathbf{F}_p}(ax + x^{-1})}{p}\Big), \tag{2.1}$$

a sum which is a real number known as a *Kloosterman sum*. It was proved by A. Weil, as a consequence of the Riemann Hypothesis for curves over finite fields, that

$$|S(a;k)| \leqslant 2\sqrt{|k|},$$

for all $a \in k^\times$, and it was already known to Kloosterman that the exponent $1/2$ of $|k|$ in this bound cannot be replaced by any smaller constant. However, in view of the many applications of Kloosterman sums to analytic number theory, it is natural to ask for more precise information concerning the distribution of $S(a;k)$, or of the normalized sum $\frac{S(a;k)}{\sqrt{|k|}}$. This question (and more!) was answered by Katz [6], using Deligne's equidistribution theorem:

Theorem 2.1 (Katz)**.** *Let $X = [-2,2]$, and let μ be the Sato-Tate measure on X, defined by*

$$d\mu(x) = \frac{1}{\pi}\sqrt{1 - \frac{x^2}{4}}dx.$$

For a finite field k, let $Y_k = k^\times$, $\theta_k(a) = S(a;k)/\sqrt{|k|}$. Then, as the size of k goes to infinity, along any sequence of finite fields, the (Y_k, θ_k) become equidistributed in X with respect to μ.

We emphasize that this applies equally when taking a sequence of finite fields of order p^n for some fixed prime p, with $n \to +\infty$, or for the sequence of fields $\mathbf{F}_p$ as p tends to infinity.

A high-level description of the proof is the following:

Step 1 (Geometric interpretation of Kloosterman sums). Another rather deep result of Deligne gives an algebraic/geometric interpretation of the function $a \mapsto S(a;k)$ as the trace of Frobenius automorphisms acting on stalks of a *lisse étale* sheaf on the multiplicative group over $\mathbf{F}_p$. Concretely, this means that there exists a certain group, which we denote $\Pi_{\mathbf{F}_p}$ (it is the étale fundamental group of the multiplicative group over $\mathbf{F}_p$, and can be seen as the subgroup of the Galois group of the function field $\mathbf{F}_p(T)$ parameterizing finite separable extensions unramified outside 0 and ∞), and there exists a group homomorphism

$$\varrho : \Pi_{\mathbf{F}_p} \longrightarrow \mathrm{GL}_2(\mathbf{C}) \tag{2.2}$$

and special conjugacy classes $\mathrm{Fr}_{a,k} \subset \Pi_k$ defined for any finite extension $k/\mathbf{F}_p$ and $a \in k^\times$, such that

$$\mathrm{tr}(\varrho(\mathrm{Fr}_{a,k})) = -\frac{S(a;k)}{\sqrt{|k|}}$$

for all $a \in k^\times$. These classes are called the *geometric Frobenius conjugacy classes at a*. Furthermore, for each a, the element $\varrho(\mathrm{Fr}_{a,k})$ is conjugate to a unique *unitary* matrix $\theta_{a,k}$ in $\mathrm{SU}_2(\mathbf{C})$ (note in passing that the existence of ϱ with such properties

already immediately implies the Weil bound for Kloosterman sums). Theorem 2.1 is then obtained from a more abstract statement:

Theorem 2.2 (Sato-Tate law for families of Kloosterman sums)**.** *For any sequence of finite fields with $|k| \to +\infty$, the conjugacy classes $\theta_{a,k}$ for $a \in k^\times$ become equidistributed in the space X of conjugacy classes in $\mathrm{SU}_2(\mathbf{C})$ with respect to the image of the probability Haar measure ν on $\mathrm{SU}_2(\mathbf{C})$.*

Indeed, it is an elementary exercise to check that X can be identified with the interval $[-2,2]$ via the trace of matrices in $\mathrm{SU}_2(\mathbf{C})$, in such a way that the image of ν to $[-2,2]$ becomes the Sato-Tate measure of Theorem 2.1; since $\mathrm{tr}(\theta_{a,k}) = -S(a;k)/\sqrt{|k|}$ (and ν is symmetric), Theorem 2.1 follows.

Step 2 (Finding the space). Deligne's equidistribution theorem generalizes Theorem 2.2 and applies to the distribution of the image of Frobenius conjugacy classes of very general algebraic varieties U/k_0 defined over a finite field k_0, under certain homomorphisms of their fundamental groups

$$\tau : \pi_1(U,\bar{\eta}) \longrightarrow \mathrm{GL}_r(\mathbf{C}), \qquad r \geqslant 1$$

(see [10, Ch. 9]). Under suitable conditions, Deligne shows that, as k/k_0 runs over finite extensions with increasing degree, *there is always some equidistribution statement* for the images $\theta_{x,k}$ of the Frobenius conjugacy classes for $x \in U(k)$ (or, more precisely, for the semisimple parts of $\tau(\mathrm{Fr}_{x,k})$ in the sense of Jordan decomposition). The corresponding space X (and the measure μ) are determined as being, in some sense, *the simplest possible compatible with the data*. Namely, the set of all images under τ of the Frobenius conjugacy classes $\mathrm{Fr}_{x,k}$, relative to all finite extensions k of k_0 and to all points $x \in U(k)$, is dense with respect to the Zariski topology in some linear algebraic group G, which is called the *monodromy group* of τ, and which turns out to be semisimple.[2] Then, part of the unstated assumptions shows that all the conjugacy classes $\theta_{x,k}$ intersect a fixed maximal compact subgroup $K \subset G$, and that the corresponding conjugacy class $\tilde{\theta}_{x,k}$ of K is well defined. The space $K^\sharp$ of conjugacy classes of K is the space in which equidistribution will happen, and the corresponding measure is the image μ_K of the probability Haar measure of K under the quotient map $K \longrightarrow K^\sharp$.

Step 3 (Proving equidistribution). So, Deligne proves that, as k runs over extensions of k_0, the classes $\tilde{\theta}_{x,k}$ for $x \in U(k)$ become equidistributed in $K^\sharp$ with respect to μ_K. The argument is in principle straightforward: there is a natural Weyl criterion for equidistribution in this setting, where the functions (1.4) are replaced by the characters

$$\chi(g) = \mathrm{tr}(\pi(g)), \qquad g \in K^\sharp$$

of the nontrivial irreducible unitary finite-dimensional continuous representations

$$\pi : K \longrightarrow \mathrm{U}_m(\mathbf{C})$$

of K (although these characters do not suffice to describe all functions on the group K, they suffice for conjugacy-invariant functions, i.e., for functions on the space X). One must therefore prove that

$$\frac{1}{|U(k)|} \sum_{x \in U(k)} \mathrm{tr}(\pi \circ \tau)(\mathrm{Fr}_{x,k}) \longrightarrow 0$$

[2] Examples of groups of this type are SL_n, SO_n, Sp_{2g}, and finite products of them.

as $[k : k_0] \to +\infty$. The "Weyl sums" in this limit can be considered as (far-reaching) analogues of exponential sums over finite fields. Applying his very general version of the Riemann Hypothesis to estimate these sums, Deligne proves that, for any nontrivial irreducible representation π of K and any extension k of k_0, we have

$$\frac{1}{|U(k)|}\Big|\sum_{x\in U(k)} \mathrm{tr}(\pi\circ\tau)(\mathrm{Fr}_{x,k})\Big| \leqslant C(\pi,k_0)|k|^{-1/2},$$

for some constant $C(\pi, k_0)$, concluding the proof of the Weyl criterion.

Thus, in the situation of Deligne's theorem, once the technical assumptions we have hidden have been checked (and this is often easy), the problem of determining the distribution properties of the corresponding Frobenius conjugacy classes (and their often diophantinally concrete invariants, such as their traces) is immediately reduced to that of determining the corresponding monodromy group G, which then determines the compact subgroup K and its Haar measure.

This is not an easy problem, as the reader may suspect. It is similar in spirit with the problem of finding the Galois group of a field extension defined by some polynomial equation. Over the years, many tools have been developed to compute the monodromy group (most notably by N. Katz, see for instance [6, 8–10]), and thus many concrete cases can now be settled. For Kloosterman sums, the answer is that for all finite base fields k_0, the monodromy group is $G = \mathrm{SL}_2$, with maximal compact subgroup $\mathrm{SU}_2(\mathbf{C})$, and so one obtains Theorem 2.2.

Remark 2.3. (1) The argument we have sketched does not deal with sequences of finite fields where the characteristic changes, e.g., to the fields $\mathbf{F}_p$ as $p \to +\infty$. This type of question is indeed very delicate (see [7] for a discussion by Katz) but the constant $C(\pi, k_0)$ can sometimes be estimated explicitly enough (for instance, it may be bounded independently of p, see in particular [10, §9.6]).

(2) Concretely, once we know—or guess—that the relevant group here is $G = \mathrm{SL}_2$, it is not very difficult to check that the Weyl sums above are of the form

$$W_m(k) = \frac{1}{|k|-1}\sum_{a\in k^\times} U_m\Big(\frac{S(a;k)}{\sqrt{|k|}}\Big),$$

where $m \geqslant 1$ and $U_m \in \mathbf{Z}[X]$ is the mth Chebychev polynomial determined by

$$U_m(2\cos\theta) = \frac{\sin((m+1)\theta)}{\sin(\theta)}$$

for $\theta \in [0, \pi]$. It is a pleasant exercise to prove directly that $W_m(k) \to 0$ as $|k| \to +\infty$ for $1 \leqslant i \leqslant 4$, and to ponder some further cases (see, e.g., [4, §4.4]).

3. Mellin transforms over finite fields

The theory described briefly in the previous section deserves maybe to be called "classical" by now. It has been used to great effect for many purposes, in particular by Katz and Sarnak [10] in their study of function-field analogues of the conjectured relationships between random matrices and zeros of the zeta function and other L-functions. But curiosity (or the demand of applications) did not stop at the situation encoded in Deligne's theorem, where one considers equidistribution of families parameterized by an algebraic variety.

Around mid-2003, both Z. Rudnick (motivated by applications to his work with Kurlberg [11] and Rosenzweig on the so-called *quantum cat map* [12]) and R. Evans

asked N. Katz about sums which do not fit this framework. In a nutshell, whereas the Kloosterman sums (2.1) for a fixed $k/\mathbf{F}_p$ can be seen as the discrete *Fourier transform* of the function φ on k defined by

$$\varphi(x) = \begin{cases} e\Big(\frac{\mathrm{tr}_{k/\mathbf{F}_p}(x^{-1})}{p}\Big) & \text{if } x \neq 0, \\ 0 & \text{if } x = 0, \end{cases}$$

one might also wish (or need) to consider discrete *Mellin transforms*, parameterized by multiplicative characters χ of $k^\times$. In other words, for some given function φ defined on $k^\times$, one wishes to understand the function

$$\chi \mapsto \mathcal{M}_\varphi(\chi) = \frac{1}{\sqrt{|k|}} \sum_{x \in k^\times} \varphi(x)\chi(x),$$

where χ runs over the set $X(k)$ of complex-valued multiplicative characters $\chi : k^\times \longrightarrow \mathbf{C}^\times$. Rudnick's question to Katz concerned $R(\chi; k) = \mathcal{M}_{\alpha_k}(\chi)$, where k is a finite extension of $\mathbf{F}_p$ and

$$\alpha_k(x) = e\Big(\frac{\mathrm{tr}_{k/\mathbf{F}_p}((x+1)/(x-1))}{p}\Big), \text{ for } x \neq 1, \quad \alpha_k(1) = 0. \tag{3.1}$$

The $R(\chi; k)$ are real numbers and satisfy $|R(\chi; k)| \leqslant 2$ if χ is not the trivial character. Rudnick asked about the distribution of $\theta_k(\chi) = R(\chi; k)$ as the size of k gets large and χ runs over $X(k) - \{1\}$. One can perform numerical experiments, which suggest strongly once more that these sums become equidistributed with respect to the Sato-Tate measure. The question raised by Rudnick was:

> Can one prove this equidistribution statement, despite the fact that we are not in the context of Deligne's equidistribution theorem?

We have here a very new setting for equidistribution questions. It is extremely remarkable that N. Katz succeeded in finding an algebraic framework in which this result can be established, as a special case of a very general equidistribution theorem for the Mellin transforms of functions φ "of algebraic origin". The book of N. Katz under review explains this surprising achievement.

To be more precise, given a finite field k_0, one begins with an "input object" on the multiplicative group $\mathbf{G}_m/k_0$, given typically by a representation

$$\tau : \Pi_{k_0} \longrightarrow \mathrm{GL}_m(\mathbf{C}), \tag{3.2}$$

where Π_{k_0} is the étale fundamental group of the multiplicative group over k_0.

For any finite extension k/k_0, Katz considers the Mellin transforms of the functions given by the trace of Frobenius conjugacy classes; i.e., he considers

$$\chi \mapsto \mathcal{M}_{\varphi_k}(\chi), \quad \text{where} \quad \varphi_k(x) = \mathrm{tr}\,\tau(\mathrm{Fr}_{x,k}). \tag{3.3}$$

For $k_0 = \mathbf{F}_p$, some basic formalism shows that the functions α_k in (3.1) are of this type for a suitable τ taking values in $\mathrm{GL}_2(\mathbf{C})$, which is independent of k. Thus an equidistribution statement for this type of Mellin transforms will answer the question of Rudnick.

4. Katz's equidistribution theorem

As in Deligne's theorem, there are two relatively distinct parts of the work of Katz. The first general theorem shows that (for suitable input objects) there is always *some* equidistribution theorem, and that this happens again in some space

of conjugacy classes in a maximal compact subgroup of a certain linear algebraic group $\tilde{G}$, with respect to Haar measure. Then, in any given concrete case (such as Rudnick's), what remains to be done is to compute the group $\tilde{G}$ to know what shape the equidistribution theorem takes. An important difference with Deligne's theorem is that the group $\tilde{G}$ is not necessarily semisimple, but merely reductive (so, for instance, it may be that $\tilde{G} = \mathrm{GL}_n$, which is not semisimple).

The first step contains the essential difference with Deligne's theorem. Indeed, in Section 2, the monodromy group G is almost immediately visible from the data of the representation (2.2), as the Zariski-closure of the image of the Frobenius conjugacy classes. But for the Mellin transform, there is no such data that suggests a definition of $\tilde{G}$.

Instead, Katz constructs the group in a striking way using the theory of *Tannakian categories*. Roughly speaking, this theory shows that one can recognize a linear algebraic group G over an algebraically closed field (say $\mathbf{C}$, for simplicity) from the category Rep_G of its finite-dimensional $\mathbf{C}$-linear representations, provided one sees the latter as equipped with the additional structure of direct sums, contragredient, tensor product, and various compatibility relations between these, where the most fundamental structures are that of the *tensor product* and the operation of forgetting the group action, associating to a representation the underlying vector space (this is a so-called *fiber functor*).

This very abstract principle means not only that groups with the "same representation theory" are isomorphic, but more importantly that given any category Cat endowed with abstract versions of these extra data, there is a linear algebraic group G over $\mathbf{C}$ for which Cat "is" the category Rep_G of representations of G (see [17] for a very readable account that puts this type of result in a natural perspective starting from classical Galois theory).

What Katz does, for an input object τ, as described at the end of the previous section, is to define a priori a Tannakian category Cat_τ for which the associated group $\tilde{G}$ is the one he requires. Although the technical details are rather daunting (crucial use is made of ideas of Gabber and Loeser [3] and of a fiber functor defined by Deligne), one ingredient has a concrete incarnation: the objects of Cat_τ are themselves of the same flavor as the representation τ, and hence have associated trace functions φ_k defined for extension fields k/k_0, and the abstract tensor product on Cat_τ is provided by a convolution operation which, at the level of the trace functions corresponds to the operation

$$(\varphi_1 \star \varphi_2)(x) = -\frac{1}{\sqrt{|k|}} \sum_{y \in k^\times} \varphi_1(y)\varphi_2(xy^{-1})$$

of multiplicative convolution of functions on $k^\times$.

The outcome of the Tannakian formalism is the construction of a group $\tilde{G}$ associated to an input object (3.2), together with a natural injection

$$\tilde{G} \subset \mathrm{GL}_r(\mathbf{C})$$

for some $r \geqslant 1$. Morever, for every finite extension k/k_0 and multiplicative character $\chi \in X(k)$, this formalism provides a well-defined conjugacy class $\theta_{\chi;k}$ in a maximal compact subgroup $\tilde{K}$ of $\tilde{G}$ such that

$$\mathcal{M}_{\varphi_k}(\chi) = \mathrm{tr}(\theta_{\chi;k}).$$

Katz shows that an equidistribution theorem follows from these facts by another argument involving the Weyl criterion (using characters of representations of $\tilde{K}$) and Deligne's form of the Riemann Hypothesis over finite fields.

Remark 4.1. An enlightening example is to take the Mellin transform of a nontrivial additive character, i.e., for a prime p and a finite extension $k/\mathbf{F}_p$, to take

$$\varphi_k(x) = e\Big(\frac{\mathrm{tr}_{k/\mathbf{F}_p}(x)}{p}\Big).$$

The Mellin transforms of these functions are just the normalized Gauss sums of the multiplicative characters χ of k, and it a well-known fact that these are complex numbers of modulus 1 for $\chi \neq 1$. In that case, the group $\tilde{G}$ is simply the group $\mathrm{GL}_1 = \mathbf{C}^\times$ (note that this is not a semisimple group), and its maximal compact subgroup is the circle $\mathbf{S}^1$. The theorem of Katz thus recovers the fact (see [6]) that the Gauss sums of nontrivial characters of a finite extension $k/\mathbf{F}_p$ with $|k| \to +\infty$ become equidistributed on the unit circle with respect to the Haar measure. The reader is invited to write down what the original Weyl criterion entails in this situation and to see how the result reduces to estimates for certain character sums in many variables (see, e.g., [5, Th. 21.6]).

5. About the book

There are roughly three different parts in the book of Katz which explains this theory and its applications. The introduction and the first overview chapter recall the context and explain at a high level the Tannakian strategy and how it implies the equidistribution theorem using Deligne's version of the Riemann Hypothesis. The main abstract theorem is then proved, and further formalism is established in the second part, up to Chapter 13 (in particular with respect to some basic knowledge of properties of $\tilde{G}$ such as the existence of a $\tilde{G}$-invariant nondegenerate bilinear form). There follow numerous examples of computation of $\tilde{G}$, which involve often very ingenious arguments concerning linear algebraic groups, and a few chapters concerning the problem of extending the equidistribution to sequences of finite fields with increasing characteristic as in Remark 2.3 (instead of extensions of a fixed k_0).

Although the motivation is, as explained, extremely concrete, it is a fact that the arguments involved in the proof are among the deepest in algebraic geometry (for instance, as Katz explains, in order to establish the existence of the necessary Tannakian categories and the associated convolution operation, one must necessarily work in the context of a certain category of perverse sheaves). The reviewer can attest that a study of the underlying structures of algebraic geometry, even at a relatively modest level, can be repayed very richly. Once a certain basic understanding is reached, this book, like the others written by N. Katz, reveals itself to be very precisely and sharply written, and to be full of riches. And finally, this theory shows spectacularly how some of the most abstract ideas of algebra and algebraic geometry may be essential to solving extremely concrete problems.

Acknowledgments

Thanks to A. Chambert-Loir, É. Fouvry, F. Jouve, P. Kurlberg, Z. Rudnick, L. Rosenzweig, and P. Sarnak for their comments and corrections.

References

[1] Pierre Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252 (French). MR601520 (83c:14017)

[2] Manfred Einsiedler, *The ergodic theory of lattice subgroups [book review of MR 2573139]*, Bull. Amer. Math. Soc. (N.S.) **48** (2011), no. 3, 475–480, DOI 10.1090/S0273-0979-2011-01335-0. MR2816388

[3] Ofer Gabber and François Loeser, *Faisceaux pervers l-adiques sur un tore*, Duke Math. J. **83** (1996), no. 3, 501–606, DOI 10.1215/S0012-7094-96-08317-9 (French). MR1390656 (97i:14016)

[4] Henryk Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics, vol. 17, American Mathematical Society, Providence, RI, 1997. MR1474964 (98e:11051)

[5] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR2061214 (2005h:11005)

[6] Nicholas M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, vol. 116, Princeton University Press, Princeton, NJ, 1988. MR955052 (91a:11028)

[7] Nicholas M. Katz, *Exponential sums over finite fields and differential equations over the complex numbers: some interactions*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 269–309, DOI 10.1090/S0273-0979-1990-15922-1. MR1032857 (91d:11067)

[8] Nicholas M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies, vol. 124, Princeton University Press, Princeton, NJ, 1990. MR1081536 (93a:14009)

[9] Nicholas M. Katz, *Moments, monodromy, and perversity: a Diophantine perspective*, Annals of Mathematics Studies, vol. 159, Princeton University Press, Princeton, NJ, 2005. MR2183396 (2006j:14020)

[10] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. MR1659828 (2000b:11070)

[11] Pär Kurlberg and Zeév Rudnick, *On the distribution of matrix elements for the quantum cat map*, Ann. of Math. (2) **161** (2005), no. 1, 489–507, DOI 10.4007/annals.2005.161.489. MR2150390 (2006h:81091)

[12] Pär Kurlberg, Lior Rosenzweig, and Zeév Rudnick, *Matrix elements for the quantum cat map: fluctuations in short windows*, Nonlinearity **20** (2007), no. 10, 2289–2304, DOI 10.1088/0951-7715/20/10/001. MR2356110 (2008k:81117)

[13] Alexander Lubotzky, *Expander graphs in pure and applied mathematics*, Bull. Amer. Math. Soc. (N.S.) **49** (2012), no. 1, 113–162, DOI 10.1090/S0273-0979-2011-01359-3. MR2869010 (2012m:05003)

[14] Barry Mazur, *Finding meaning in error terms*, Bull. Amer. Math. Soc. (N.S.) **45** (2008), no. 2, 185–228, DOI 10.1090/S0273-0979-08-01207-X. MR2383303 (2009c:11083)

[15] Peter Sarnak, *Spectra of hyperbolic surfaces*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), no. 4, 441–478, DOI 10.1090/S0273-0979-03-00991-1. MR1997348 (2004f:11107)

[16] J-P. Serre: Inaugural Minerva Lecture, "Equidistribution", `https:www.math.princeton.edu/events/seminars/minerva-lectures/inaugural-minerva-lectures-i-equidistribution`

[17] Tamás Szamuely, *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, Cambridge, 2009. MR2548205 (2011b:14064)

[18] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. **77** (1914).

Emmanuel Kowalski

ETH Zürich – D-MATH Rämistrasse 101, CH-8092 Zürich, Switzerland

E-mail address: `kowalski@math.ethz.ch`