Convolution and Equidistribution

Sato-Tate Theorems for Finite-Field Mellin Transforms

Nicholas M. Katz

ANNALS OF MATHEMATICS STUDIES

Annals of Mathematics Studies

Number 180

CONVOLUTION AND EQUIDISTRIBUTION

Sato-Tate Theorems for Finite-Field Mellin Transforms

Nicholas M. Katz

PRINCETON UNIVERSITY PRESS
PRINCETON AND OXFORD
2012

Published by Princeton University Press, 41 William Street,
Princeton, New Jersey 08540

In the United Kingdom: Princeton University Press, 6 Oxford Street,
Woodstock, Oxfordshire OX20 1TW

Library of Congress Cataloging-in-Publication Data

Katz, Nicholas M., 1943-
Convolution and equidistribution : Sato-Tate theorems for finite-field Mellin transforms / Nicholas M. Katz.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-691-15330-8 (hardcover : alk. paper) – ISBN 978-0-691-15331-5 (pbk. : alk. paper) 1. Mellin transform. 2. Convolutions (Mathematics) 3. Sequences (Mathematics) I. Title.
QA432.K38 2012
515′.723–dc23 2011030224

British Library Cataloging-in-Publication Data is available

This book has been composed in LaTeX.
The publisher would like to acknowledge the author of this volume for providing the camera-ready copy from which this book was printed.

Printed on acid-free paper ∞
press.princeton.edu
Printed in the United States of America

1 3 5 7 9 10 8 6 4 2

Contents

Convolution and Equidistribution

Introduction

The systematic study of character sums over finite fields may be said to have begun over 200 years ago, with Gauss. The Gauss sums over $\mathbb{F}_p$ are the sums

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

for ψ a nontrivial additive character of $\mathbb{F}_p$, e.g., $x \mapsto e^{2\pi i x/p}$, and χ a nontrivial multiplicative character of $\mathbb{F}_p^\times$. Each has absolute value $\sqrt{p}$. In 1926, Kloosterman [**Kloos**] introduced the sums (one for each $a \in \mathbb{F}_p^\times$)

$$\sum_{xy=a \text{ in } \mathbb{F}_p} \psi(x+y)$$

which bear his name, in applying the circle method to the problem of four squares. In 1931 Davenport [**Dav**] became interested in (variants of) the following questions: for how many x in the interval $[1, p-2]$ are both x and $x+1$ squares in $\mathbb{F}_p$? Is the answer approximately $p/4$ as p grows? For how many x in $[1, p-3]$ are each of $x, x+1, x+2$ squares in $\mathbb{F}_p$? Is the answer approximately $p/8$ as p grows? For a fixed integer $r \geq 2$, and a (large) prime p, for how many x in $[1, p-r]$ are each of $x, x+1, x+2, ..., x+r-1$ squares in $\mathbb{F}_p$. Is the answer approximately $p/2^r$ as p grows? These questions led him to the problem of giving good estimates for character sums over the prime field $\mathbb{F}_p$ of the form

$$\sum_{x \in \mathbb{F}_p} \chi_2(f(x)),$$

where χ_2 is the quadratic character $\chi_2(x) := (\frac{x}{p})$, and where $f(x) \in \mathbb{F}_p[x]$ is a polynomial with all distinct roots. Such a sum is the "error term" in the approximation of the number of mod p solutions of the equation

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

by p, indeed the number of mod p solutions is exactly equal to

$$p + \sum_{x \in \mathbb{F}_p} \chi_2(f(x)).$$

And, if one replaces the quadratic character by a character χ of $\mathbb{F}_p^\times$ of higher order, say order n, then one is asking about the number of mod p solutions of the equation

$$y^n = f(x).$$

This number is exactly equal to

$$p + \sum_{\chi|\chi^n=\mathbb{1},\chi\neq\mathbb{1}} \sum_{x\in\mathbb{F}_p} \chi(f(x)).$$

The "right" bounds for Kloosterman's sums are

$$|\sum_{xy=a \text{ in } \mathbb{F}_\mathrm{p}} \psi(x+y)| \leq 2\sqrt{p}$$

for $a \in \mathbb{F}_p^\times$. For $f(x) = \sum_{i=0}^d a_i x^i$ squarefree of degree d, the "right" bounds are

$$|\sum_{x\in\mathbb{F}_p} \chi(f(x))| \leq (d-1)\sqrt{p}$$

for χ nontrivial and $\chi^d \neq \mathbb{1}$, and

$$|\chi(a_d) + \sum_{x\in\mathbb{F}_p} \chi(f(x))| \leq (d-2)\sqrt{p}$$

for χ nontrivial and $\chi^d = \mathbb{1}$. These bounds were foreseen by Hasse [**Ha-Rel**] to follow from the Riemann Hypothesis for curves over finite fields, and were thus established by Weil [**Weil**] in 1948.

Following Weil's work, it is natural to "normalize" such a sum by dividing it by $\sqrt{p}$, and then ask how it varies in an algebro-geometric family. For example, one might ask how the normalized[1] Kloosterman sums

$$-(1/\sqrt{p}) \sum_{xy=a \text{ in } \mathbb{F}_\mathrm{p}} \psi(x+y)$$

vary with $a \in \mathbb{F}_p^\times$, or how the sums

$$-(1/\sqrt{p}) \sum_{x\in\mathbb{F}_p} \chi_2(f(x))$$

vary as f runs over all squarefree cubic polynomials in $\mathbb{F}_p[x]$. [In this second case, we are looking at the $\mathbb{F}_p$-point count for the elliptic curve $y^2 = f(x)$.] Both these sorts of normalized sums are real, and lie in the closed interval $[-2, 2]$, so each can be written as twice the cosine of a

[1]The reason for introducing the minus sign will become clear later.

unique angle in $[0,\pi]$. Thus we define angles $\theta_{a,p}$, $a \in \mathbb{F}_p^\times$, and angles $\theta_{f,p}$, f a squarefree cubic in $\mathbb{F}_p[x]$:

$$-(1/\sqrt{p}) \sum_{xy=ain\mathbb{F}_p} \psi(x+y) = 2\cos\theta_{a,p},$$

$$-(1/\sqrt{p}) \sum_{x\in\mathbb{F}_p} \chi_2(f(x)) = 2\cos\theta_{f,p}.$$

In both these cases, the Sato-Tate conjecture asserted that, as p grows, the sets of angles $\{\theta_{a,p}\}_{a\ \in\ \mathbb{F}_p^\times}$ (respectively $\{\theta_{f,p}\}_{f\ \in\ \mathbb{F}_p[x]\ \text{squarefree cubic}}$) become equidistributed in $[0,\pi]$ for the measure $(2/\pi)\sin^2(\theta)d\theta$. Equivalently, the normalized sums themselves become equidistributed in $[-2,2]$ for the "semicircle measure" $(1/2\pi)\sqrt{4-x^2}dx$. These Sato-Tate conjectures were shown by Deligne to fall under the umbrella of his general equidistribution theorem, cf. [**De-Weil II**, 3.5.3 and 3.5.7] and [**Ka-GKM**, 3.6 and 13.6]. Thus for example one has, for a fixed nontrivial χ, and a fixed integer $d \geq 3$ such that $\chi^d \neq \mathbb{1}$, a good understanding of the equidistribution properties of the sums

$$-(1/\sqrt{p}) \sum_{x\in\mathbb{F}_p} \chi(f(x))$$

as f ranges over various algebro-geometric families of polynomials of degree d, cf. [**Ka-ACT**, 5.13].

In this work, we will be interested in questions of the following type: fix a polynomial $f(x) \in \mathbb{F}_p[x]$, say squarefree of degree $d \geq 2$. For each multiplicative character χ with $\chi^d \neq \mathbb{1}$, we have the normalized sum

$$-(1/\sqrt{p}) \sum_{x\in\mathbb{F}_p} \chi(f(x)).$$

How are these normalized sums distributed as we **keep** f **fixed but vary** χ over all multiplicative characters χ with $\chi^d \neq \mathbb{1}$? More generally, suppose we are given some suitably algebro-geometric function $g(x)$, what can we say about suitable normalizations of the sums

$$\sum_{x\in\mathbb{F}_p} \chi(x)g(x)$$

as χ varies? This case includes the sums $\sum_{x\in\mathbb{F}_p} \chi(f(x))$, by taking for g the function $x \mapsto -1 + \#\{t \in \mathbb{F}_p | f(t) = x\}$, cf. Remark 17.7.

The earliest example we know in which this sort of question of variable χ is addressed is the case in which $g(x)$ is taken to be $\psi(x)$, so that we are asking about the distribution on the unit circle S^1 of the $p-2$ normalized Gauss sums

$$-(1/\sqrt{p})\sum_{x\in\mathbb{F}_p^\times}\psi(x)\chi(x),$$

as χ ranges over the nontrivial multiplicative characters. The answer is that as p grows, these $p-2$ normalized sums become more and more equidistributed for Haar measure of total mass one in S^1. This results [**Ka-SE**, 1.3.3.1] from Deligne's estimate [**De-ST**, 7.1.3, 7.4] for multi-variable Kloosterman sums. There were later results [**Ka-GKM**, 9.3, 9.5] about equidistribution of r-tuples of normalized Gauss sums in $(S^1)^r$ for any $r \geq 1$. The theory we will develop here "explains" these last results in a quite satisfactory way, cf. Corollary 20.2.

Most of our attention is focused on equidistribution results over larger and larger finite extensions of a given finite field. Emanuel Kowalski drew our attention to the interest of having equidistribution results over, say, prime fields $\mathbb{F}_p$, that become better and better as p grows. This question is addressed in Chapter 28, where the problem is to make effective the estimates, already given in the equicharacteristic setting of larger and larger extensions of a given finite field. In Chapter 29, we point out some open questions about "the situation over $\mathbb{Z}$" and give some illustrative examples.

We end this introduction by pointing out two potential ambiguities of notation.

(1) We will deal both with lisse sheaves, usually denoted by calligraphic letters, most commonly $\mathcal{F}$, on open sets of $\mathbb{G}_m$, and with perverse sheaves, typically denoted by roman letters, most commonly N and M, on $\mathbb{G}_m$. We will develop a theory of the Tannakian groups $G_{geom,N}$ and $G_{arith,N}$ attached to (suitable) perverse sheaves N. We will also on occasion, especially in Chapters 11 and 12, make use of the "usual" geometric and arithmetic monodromy groups $G_{geom,\mathcal{F}}$ and $G_{arith,\mathcal{F}}$ attached to lisse sheaves $\mathcal{F}$. The difference in typography, which in turns indicates whether one is dealing with a perverse sheaf or a lisse sheaf, should always make clear which sort of G_{geom} or G_{arith} group, the Tannakian one or the "usual" one, is intended.

(2) When we have a lisse sheaf $\mathcal{F}$ on an open set of $\mathbb{G}_m$, we often need to discuss the representation of the inertia group $I(0)$ at 0 (respectively the representation of the inertia group $I(\infty)$ at ∞) to which $\mathcal{F}$ gives rise. We will denote these representations $\mathcal{F}(0)$ and $\mathcal{F}(\infty)$ respectively. We will also wish to consider Tate twists $\mathcal{F}(n)$ or $\mathcal{F}(n/2)$ of $\mathcal{F}$ by **nonzero** integers n or half-integers $n/2$. We adopt the convention that $\mathcal{F}(0)$ (or $\mathcal{F}(\infty)$) always means the representation of the

corresponding inertia group, while $\mathcal{F}(n)$ or $\mathcal{F}(n/2)$ with n a nonzero integer always means a Tate twist.

CHAPTER 1

Overview

Let k be a finite field, q its cardinality, p its characteristic,

$$\psi : (k, +) \to \mathbb{Z}[\zeta_p]^\times \subset \mathbb{C}^\times$$

a nontrivial additive character of k, and

$$\chi : (k^\times, \times) \to \mathbb{Z}[\zeta_{q-1}]^\times \subset \mathbb{C}^\times$$

a (possibly trivial) multiplicative character of k.

The present work grew out of two questions, raised by Ron Evans and Zeev Rudnick respectively, in May and June of 2003. Evans had done numerical experiments on the sums

$$S(\chi) := -(1/\sqrt{q}) \sum_{t \in k^\times} \psi(t - 1/t)\chi(t)$$

as χ varies over all multiplicative characters of k. For each χ, $S(\chi)$ is real, and (by Weil) has absolute value at most 2. Evans found empirically that, for large $q = \#k$, these $q - 1$ sums were approximately equidistributed for the "Sato-Tate measure"[1] $(1/2\pi)\sqrt{4 - x^2}dx$ on the closed interval $[-2, 2]$, and asked if this equidistribution could be proven.

Rudnick had done numerical experiments on the sums

$$T(\chi) := -(1/\sqrt{q}) \sum_{t \in k^\times, t \neq 1} \psi((t + 1)/(t - 1))\chi(t)$$

as χ varies now over all *nontrivial* multiplicative characters of a finite field k of *odd* characteristic, cf. [**KRR**, Appendix A] for how these sums arose. For nontrivial χ, $T(\chi)$ is real, and (again by Weil) has absolute value at most 2. Rudnick found empirically that, for large $q = \#k$, these $q-2$ sums were approximately equidistributed for the same "Sato-Tate measure" $(1/2\pi)\sqrt{4 - x^2}dx$ on the closed interval $[-2, 2]$, and asked if this equidistribution could be proven.

[1]This is the measure which is the direct image of the total mass one Haar measure on the compact group $SU(2)$ by the trace map Trace : $SU(2) \to [-2, 2]$, i.e., it is the measure according to which traces of "random" elements of $SU(2)$ are distributed.

We will prove both of these equidistribution results. Let us begin by slightly recasting the original questions. Fixing the characteristic p of k, we choose a prime number $\ell \neq p$; we will soon make use of ℓ-adic étale cohomology. We denote by $\mathbb{Z}_\ell$ the ℓ-adic completion of $\mathbb{Z}$, by $\mathbb{Q}_\ell$ its fraction field, and by $\overline{\mathbb{Q}}_\ell$ an algebraic closure of $\mathbb{Q}_\ell$. We also choose a field embedding ι of $\overline{\mathbb{Q}}_\ell$ into $\mathbb{C}$. Any such ι induces an isomorphism between the algebraic closures of $\mathbb{Q}$ in $\overline{\mathbb{Q}}_\ell$ and in $\mathbb{C}$ respectively.[2] By means of ι, we can, on the one hand, view the sums $S(\chi)$ and $T(\chi)$ as lying in $\overline{\mathbb{Q}}_\ell$. On the other hand, given an element of $\overline{\mathbb{Q}}_\ell$, we can ask if it is real, and we can speak of its complex absolute value. This allows us to define what it means for a lisse sheaf to be ι-pure of some weight w (and later, for a perverse sheaf to be ι-pure of some weight w). We say that a perverse sheaf is pure of weight w if it is ι-pure of weight w for every choice of ι.

By means of the chosen ι, we view both the nontrivial additive character ψ of k and every (possibly trivial) multiplicative character χ of $k^\times$ as having values in $\overline{\mathbb{Q}}_\ell^\times$. Then, attached to ψ, we have the Artin-Schreier sheaf $\mathcal{L}_\psi = \mathcal{L}_{\psi(x)}$ on $\mathbb{A}^1/k := Spec(k[x])$, a lisse $\overline{\mathbb{Q}}_\ell$-sheaf of rank one on $\mathbb{A}^1/k$ which is pure of weight zero. And for each χ we have the Kummer sheaf $\mathcal{L}_\chi = \mathcal{L}_{\chi(x)}$ on $\mathbb{G}_m/k := Spec(k[x, 1/x])$, a lisse $\overline{\mathbb{Q}}_\ell$-sheaf of rank one on $\mathbb{G}_m/k$ which is pure of weight zero. For a k-scheme X and a k-morphism $f : X \to \mathbb{A}^1/k$ (resp. $f : X \to \mathbb{G}_m/k$), we denote by $\mathcal{L}_{\psi(f)}$ (resp. $\mathcal{L}_{\chi(f)}$) the pullback lisse rank one, pure of weight zero, sheaf $f^\star\mathcal{L}_{\psi(x)}$ (resp. $f^\star\mathcal{L}_{\chi(x)}$) on X.

In the question of Evans, we view $x - 1/x$ as a morphism from $\mathbb{G}_m$ to $\mathbb{A}^1$, and form the lisse sheaf $\mathcal{L}_{\psi(x-1/x)}$ on $\mathbb{G}_m/k$. In the question of Rudnick, we view $(x+1)/(x-1)$ as a morphism from $\mathbb{G}_m \setminus \{1\}$ to $\mathbb{A}^1$, and form the lisse sheaf $\mathcal{L}_{\psi((x+1)/(x-1))}$ on $\mathbb{G}_m \setminus \{1\}$. With

$$j : \mathbb{G}_m \setminus \{1\} \to \mathbb{G}_m$$

the inclusion, we form the direct image sheaf $j_\star\mathcal{L}_{\psi((x+1)/(x-1))}$ on $\mathbb{G}_m/k$ (which for this sheaf, which is totally ramified at the point 1, is the same as extending it by zero across the point 1).

The common feature of both questions is that we have a dense open set $U/k \subset \mathbb{G}_m/k$, a lisse, ι-pure of weight zero sheaf $\mathcal{F}$ on U/k, its extension $\mathcal{G} := j_\star\mathcal{F}$ by direct image to $\mathbb{G}_m/k$, and we are looking at the sums

$$-(1/\sqrt{q}) \sum_{t \in \mathbb{G}_m(k) = k^\times} \chi(t)\mathrm{Trace}(Frob_{t,k}|\mathcal{G})$$

[2]Such an ι need not be a field isomorphism of $\overline{\mathbb{Q}}_\ell$ with $\mathbb{C}$, but we may choose an ι which is, as Deligne did in [**De-Weil II**, 0.2, 1.2.6, 1.2.11].

$$= -(1/\sqrt{q}) \sum_{t \in \mathbb{G}_m(k)=k^\times} \mathrm{Trace}(Frob_{t,k}|\mathcal{G} \otimes \mathcal{L}_\chi).$$

To deal with the factor $1/\sqrt{q}$, we choose a square root of the ℓ-adic unit p in $\overline{\mathbb{Q}}_\ell$, and use powers of this chosen square root as our choices of $\sqrt{q}$. [For definiteness, we might choose that $\sqrt{p}$ which via ι becomes the positive square root, but either choice will do.] Because $\sqrt{q}$ is an ℓ-adic unit, we may form the "half"-Tate twist $\mathcal{G}(1/2)$ of $\mathcal{G}$, which for any finite extension field E/k and any point $t \in \mathbb{G}_m(E)$ multiplies the traces of the Frobenii by $1/\sqrt{\#E}$, i.e.,

$$\mathrm{Trace}(Frob_{t,E}|\mathcal{G}(1/2)) = (1/\sqrt{\#E})\mathrm{Trace}(Frob_{t,E}|\mathcal{G}).$$

As a final and apparently technical step, we replace the middle extension sheaf $\mathcal{G}(1/2)$ by the same sheaf, but now placed in degree -1, namely the object

$$M := \mathcal{G}(1/2)[1]$$

in the derived category $D^b_c(\mathbb{G}_m/k, \overline{\mathbb{Q}}_\ell)$. It will be essential in a moment that the object M is in fact a perverse sheaf, but for now we need observe only that this shift by one of the degree has the effect of changing the sign of each Trace term. In terms of this object, we are looking at the sums

$$S(M, k, \chi) := \sum_{t \in \mathbb{G}_m(k)=k^\times} \chi(t)\mathrm{Trace}(Frob_{t,k}|M).$$

So written, the sums $S(M, k, \chi)$ make sense for *any* object $M \in D^b_c(\mathbb{G}_m/k, \overline{\mathbb{Q}}_\ell)$. If we think of M as fixed but χ as variable, we are looking at the Mellin (:= multiplicative Fourier) transform of the function $t \mapsto \mathrm{Trace}(Frob_{t,k}|M)$ on the finite abelian group $\mathbb{G}_m(k) = k^\times$. It is a standard fact that the Mellin transform turns multiplicative convolution of functions on $k^\times$ into multiplication of functions of χ.

On the derived category $D^b_c(\mathbb{G}_m/k, \overline{\mathbb{Q}}_\ell)$, we have a natural operation of !-convolution

$$(M, N) \to M \star_! N$$

defined in terms of the multiplication map

$$\pi : \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m, \quad (x, y) \to xy$$

and the external tensor product object

$$M \boxtimes N := pr_1^\star M \otimes pr_2^\star M$$

in $D^b_c(\mathbb{G}_m \times \mathbb{G}_m/k, \overline{\mathbb{Q}}_\ell)$ as

$$M \star_! N := R\pi_!(M \boxtimes N).$$

It then results from the Lefschetz Trace formula [**Gr-Rat**] and proper base change that, for any multiplicative character χ of $k^\times$, we have the product formula

$$S(M \star_! N, k, \chi) = S(M, k, \chi)S(N, k, \chi);$$

more generally, for any finite extension field E/k, and any multiplicative character ρ of $E^\times$, we have the product formula

$$S(M \star_! N, E, \rho) = S(M, E, \rho)S(N, E, \rho).$$

At this point, we must mention two technical points, which will be explained in detail in the next chapter, but which we will admit here as black boxes. The first is that we must work with perverse sheaves N satisfying a certain supplementary condition, $\mathcal{P}$. This is the condition that, working on $\mathbb{G}_m/\overline{k}$, N admits no subobject and no quotient object which is a (shifted) Kummer sheaf $\mathcal{L}_\chi[1]$. For an N which is geometrically irreducible, $\mathcal{P}$ is simply the condition that N is not geometrically a (shifted) Kummer sheaf $\mathcal{L}_\chi[1]$. Thus any geometrically irreducible N which has generic rank ≥ 2, or which is not lisse on $\mathbb{G}_m$, or which is not tamely ramified at both 0 and ∞, certainly satisfies $\mathcal{P}$. Thus for example the object giving rise to the Evans sums, namely $\mathcal{L}_{\psi(x-1/x)}(1/2)[1]$, is wildly ramified at both 0 and ∞, and the object giving rise to the Rudnick sums, namely $j_\star\mathcal{L}_{\psi((x+1)/(x-1))}(1/2)[1]$, is not lisse at $1 \in \mathbb{G}_m(\overline{k})$, so both these objects satisfy $\mathcal{P}$. The second technical point is that we must work with a variant of ! convolution $\star_!$, called "middle" convolution $\star_{mid}$, which is defined on perverse sheaves satisfying $\mathcal{P}$, cf. the next chapter.

In order to explain the simple underlying ideas, we will admit four statements, and explain how to deduce from them equidistribution theorems about the sums $S(M, k, \chi)$ as χ varies.

(1) If M and N are both perverse on $\mathbb{G}_m/k$ (resp. on $\mathbb{G}_m/\overline{k}$) and satisfy $\mathcal{P}$, then their middle convolution $M \star_{mid} N$ is perverse on $\mathbb{G}_m/k$ (resp. on $\mathbb{G}_m/\overline{k}$) and satisfies $\mathcal{P}$.

(2) With the operation of middle convolution as the "tensor product," the skyscraper sheaf δ_1 as the "identity object," and $[x \mapsto 1/x]^\star DM$ as the "dual" $M^\vee$ of M (DM denoting the Verdier dual of M), the category of perverse sheaves on $\mathbb{G}_m/k$ (resp. on $\mathbb{G}_m/\overline{k}$) satisfying $\mathcal{P}$ is a neutral Tannakian category, in which the "dimension" of an object M is its Euler characteristic $\chi_c(\mathbb{G}_m/\overline{k}, M)$.

(3) Denoting by

$$j_0 : \mathbb{G}_m/\overline{k} \subset \mathbb{A}^1/\overline{k}$$