Lecture Notes in Mathematics

Edited by A. Dold and B. Eckmann

504

Serge Lang
Hale Trotter

Frobenius Distributions in GL_2-Extensions

Distribution of Frobenius Automorphisms in GL_2-Extensions of the Rational Numbers

Springer-Verlag
Berlin · Heidelberg · New York 1976

Authors
Serge Lang
Mathematics Department
Yale University
New Haven, Connecticut 06520
USA

Hale Freeman Trotter
Fine Hall
Princeton University
Princeton, New Jersey 08540
USA

Library of Congress Cataloging in Publication Data

Lang, Serge, 1927-
Frobenius distributions in GL_2-extensions.

(Lecture notes in mathematics ; 504)
Bibliography: p.
Includes index.
1. Probabilistic number theory. 2. Galois theory.
3. Field,extensions (Mathematics) 4. Numbers,
Rational. I. Trotter, Hale F., joint author. II. Title. III. Series: Lecture notes in mathematics
(Berlin) ; 504.
QA3.L28 no. 504 [QA241.7] 510'.8s [512'.7]
75-45242

AMS Subject Classifications (1970): 10K99, 12A55, 12A75, 33A25

ISBN 3-540-07550-X Springer-Verlag Berlin · Heidelberg · New York
ISBN 0-387-07550-X Springer-Verlag New York · Heidelberg · Berlin

Printed in Germany
Offsetdruck: Julius Beltz, Hemsbach/Bergstr.

ACKNOWLEDGMENTS

Both Lang and Trotter are supported by NSF grants. The final draft of this monograph was written while Lang was at the Institute for Advanced Study, whose hospitality we appreciated.

We also thank Mrs. Helen Morris for a superb job of varityping the final copy.

INTRODUCTION

We are interested in a distribution problem for primes related to elliptic curves, but which can also be described solely in terms of the distribution of Frobenius elements in certain Galois extensions of the rationals. We therefore first describe this situation, and then indicate its connection with elliptic curves.

Let K be a Galois (infinite) extension of the rationals, with Galois group G. We suppose given a representation

$$\rho : G \longrightarrow \prod GL_2(Z_\ell)$$

which we assume gives an embedding of G onto an open subgroup of the product, taken over all primes ℓ. We let

$$\rho_\ell : G \longrightarrow GL_2(Z_\ell)$$

be the projection of ρ on the ℓ-th factor. We assume that there is an integer Δ such that if p is a prime and $p \nmid \Delta\ell$, then p is unramified in ρ_ℓ, or in other words, the inertia group at a prime of K above p is contained in the kernel of ρ_ℓ. Then the Frobenius class σ_p is well defined in the factor group

$$G_\ell = G/\mathrm{Ker}\,\rho_\ell\ ,$$

and $\rho_\ell(\sigma_p)$ has a characteristic polynomial which we assume of the form

$$X^2 - t_p X + p\ .$$

We assume that t_p is an integer independent of ℓ, and call t_p the trace of Frobenius. Finally we assume that the roots of the characteristic polynomial have absolute value $\sqrt{p}$, and are complex conjugates of each other. Let π_p be such a root.

Let t_0 be a given integer. Let k be a given imaginary quadratic field. We let $N_{t_0,\rho}(x)$ be the number of primes $p \leqq x$ such that $t_p = t_0$. We let $N_{k,\rho}(x)$

be the number of primes $p \leqq x$ such that $Q(\pi_p) = k$. If $k = k_D$ is the field

$$k_D = Q(\sqrt{D})$$

with discriminant D, we also write $N_D(x)$, $N_{D,\rho}(x)$ or $N_k(x)$ instead of $N_{k,\rho}(x)$.

We conjecture that there are constants $C(t_0, \rho)$ and $C(k, \rho) > 0$ such that we have the asymptotic relations

$$N_k(x) \sim C(k,\rho)\frac{\sqrt{x}}{\log x} \qquad \text{and} \qquad N_{t_0}(x) \sim C(t_0,\rho)\frac{\sqrt{x}}{\log x}\,.$$

The constants depend on k, ρ or t_0, ρ respectively. If $C(t_0, \rho) = 0$ then the asymptotic relation is to be interpreted to mean that $N_{t_0}(x)$ is bounded. If $C(t_0, \rho) \neq 0$, then the asymptotic relation has the usual meaning. We shall also see that $C(0, \rho) \neq 0$. Cf. Part I, §4, Remark 1.

Actually, define

$$\pi_{\frac{1}{2}}(x) = \sum_{p \leqq x} \frac{1}{2\sqrt{p}}\,.$$

This is essentially

$$\int^{x} \frac{1}{2\sqrt{x}}\, d\pi(x) \sim \int^{x} \frac{1}{2\sqrt{x}}\, \frac{dx}{\log x}\,,$$

which can be integrated by parts with $u = 1/\log x$ and $dv = \dfrac{dx}{2\sqrt{x}}$ to show that

$$\pi_{\frac{1}{2}}(x) \sim \frac{\sqrt{x}}{\log x}\,.$$

Both in the theoretical analysis and in the numerical computations, it is the asymptotic relations

$$N_k(x) \sim C(k,\rho)\pi_{\frac{1}{2}}(x) \qquad \text{and} \qquad N_{t_0}(x) \sim C(t_0,\rho)\pi_{\frac{1}{2}}(x)$$

which arise. Therefore it is more natural to deal with $\pi_{\frac{1}{2}}(x)$, rather than with the elementary form

$$\frac{\sqrt{x}}{\log x}\,,$$

which converges asymptotically only slowly to $\pi_{\frac{1}{2}}(x)$.

Our arguments to make the conjecture plausible involve only the Galois representation ρ, the Tchebotarev and Hecke distribution theorems in finite Galois extensions, and a conjectured distribution function for the angles of Frobenius elements. One may view our study as a first attempt to formulate for certain infinite extensions distribution laws for Frobenius elements. On the other hand, the motivation also arises from the theory of elliptic curves as follows.

Let A be an elliptic curve over the rationals. Let $K = \mathbf{Q}(A_{tor})$ be the field obtained by adjoining the coordinates of its torsion points. Then the Galois group admits a natural representation in $\prod GL_2(\mathbf{Z}_\ell)$. We assume that A has no complex multiplication. We then know from Serre's work [S 2] that the representation is open in the product. It is also known that the other properties mentioned above are satisfied (especially that the roots of the characteristic polynomial are complex conjugates of each other, which is none other than the Riemann Hypothesis, Hasse's Theorem). When the representation arises from an elliptic curve, we then write also $N_{k,A}(x)$, etc., replacing ρ by A in the notation. We note that the constants $C(k, A)$ and $C(t_0, A)$ are obviously isogeny invariants of A. (Isogenies over the algebraic closure of $\mathbf{Q}$ are allowed.)

A prime p is called **supersingular** when $t_p = 0$. This is a standard interesting case in the theory of elliptic curves. There are numerous other characterizations of this case, which are however irrelevant for us here (cf. for instance Appendix 2 of [L 1]). Serre had already observed that the densities of supersingular primes, or those for which $\mathbf{Q}(\pi_p) = k$, are zero ([S 1] for the supersingular case, private communication in the other). Mazur emphasized the importance of the case when $t_p = 1$ for the arithmetic of elliptic curves (see [Ma], Propositions 8.5 and 8.14) and called the prime p anomalous when $t_p = 1$. In the case of complex multiplication, if a prime is anomalous, then it lies in a quadratic progression, and the conjectured distribution of such primes can be reduced to a conjecture of Hardy-Littlewood, that it is of the form

$$C \frac{\sqrt{x}}{\log x}$$

for some constant C. The Galois group of a curve with complex multiplication is of course not a GL_2-group, and our situation is more complicated.

(Strictly speaking, one should define supersingular (resp. anomalous) by the condition $t_p \equiv 0$ (resp. $t_p \equiv 1$) mod p, but since $|t_p| < 2\sqrt{p}$, this amounts to the same thing for primes > 5, so the distinction is irrelevant for our purpose, which is to count primes asymptotically.)

The axiomatization of the distribution properties only in terms of the Galois group is important for eventual applications to representations arising from modular forms other than those associated with elliptic curves. One knows from the work of Swinnerton-Dyer [SwD] that they give rise to (essentially) GL_2-extensions of the rational numbers. (Cf. also Ribet [R].) The characteristic polynomial of a Frobenius element is of the form

$$X^2 - t_p X + p^{k-1} = 0 .$$

The analogue of our $\sqrt{p}$ is then $p^{(k-1)/2}$. This leads us to think that when $k \geqq 4$, there is only a finite number of primes such that the Frobenius element belongs to the given quadratic field, or such that $t_p = 0$. This would be in line with the Lehmer conjecture that $\tau_p \neq 0$ for all p, where τ_p is the trace of Frobenius for the best known cusp form Δ from the theory of elliptic functions. For $k = 3$, one gets an intermediate asymptotic behavior, and for $k = 1$ one gets back to the oldest situation of actual densities, since the associated Galois group is finite. The case with $k > 2$ introduces enough perturbations in our arguments that we shall handle it elsewhere.

From a naive approach, one already suspects that the asymptotic behavior has something to do with $\pi_{\frac{1}{2}}(x)$. Indeed, the trace of Frobenius t_p must lie in the interval $|t_p| < 2\sqrt{p}$. Under equal probability that it hits any integer in this interval, this probability is $\frac{1}{4\sqrt{p}}$. Summing for $p \leqq x$ yields the $\pi_{\frac{1}{2}}(x)$. In reality, the probabilities of hitting the different integers in the interval are not equal, but depend in a fairly complicated way on the Galois representation. In the imaginary quadratic case one wants the probability of coincidence of t_p with the trace of some integer of the field k with norm p. This probability involves an interaction between the field of division points and the maximal abelian extension of k, and becomes especially complicated when the intersection of these two fields is larger (as it may be, by a finite extension) than the field of all roots of unity over the rationals. The effect that this last complication can have on the probabilistic factor is one of the more interesting things we have encountered in the present study.

Tuskina [Tu] already conjectured an equivalent asymptotic formula for the distribution of supersingular primes, purely on the basis of empirical evidence (but without making any conjecture as to the value of the constant).

The computation of the constant makes it necessary to have an exact description of the Galois groups. This can be an arduous task. We obviously rely heavily on Serre [S 2], and also use ideas of Shimura [Sh], especially in determining the group of $X_0(11)$.

Our heuristic method is to consider probabilistic models in which we consider the sequence of traces of Frobenius $\{t_p\}$ to be a random sequence. We choose the simplest model for which almost all sequences have asymptotic properties consistent with the density theorems of Tchebotarev and Hecke, concerning the distribution of primes with given element of the Galois group, and in sectors of the plane, and also consistent with the Sato-Tate conjecture. We show that for this model, almost all sequences have an asymptotic behavior of the form mentioned (a constant times $\pi_{\frac{1}{2}}(x)$), and we compute this constant explicitly in terms of the Galois group. Our conjecture is that the sequence of Frobenius elements has this behavior. More precisely, say in the supersingular case, this amounts to saying that the probability that p is supersingular is asymptotic to $C(0,\rho)\cdot\frac{1}{2\sqrt{p}}$, and similarly in the other cases, using $C(k,\rho)$ instead of $C(0,\rho)$.

In the case of the quadratic field k with discriminant D, the constant is inversely proportional to $\sqrt{|D|}$, and can be expressed as a product of local factors depending on ℓ and D for almost all primes ℓ, as well as a factor depending on the special position of the Galois group in the product at a finite number of exceptional primes depending on ρ, and D. There is also a factor at infinity, derived from the Sato-Tate distribution.

The factors at finite primes can be expressed as integrals over ℓ-adic sets of certain functions which are Harish transforms. We develop ab ovo the theory of Harish transforms, which can be formulated completely naively in terms of the direct image of Haar measure under the trace-determinant map (i.e. the map which associates with each matrix the coefficients of its characteristic polynomial). The theory of this transform has independent interest, and is given in Part II, §7 and §8.

Our axiomatization involving only a GL_2-Galois extension of the rationals gives rise to various questions.

1. Are there such extensions (all of elliptic type, see §1 below) other than those arising from the division points of an elliptic curve?

This question does not seem to fit exactly in the general Langlands framework, since no assumption is made here about the associated zeta function of the GL_2-extension.

2. Cusp forms do not appear in the present work. Can the conjecture be even remotely approached for the case of elliptic curves by using explicit formulas for the coefficients of the associated cusp form, e.g. formulas as in Manin [Man]?

How do the congruence conditions and the finite part of the constant arising from the Galois representation translate into conditions on the coefficients of the associated cusp form? How can one describe only in terms of these coefficients the conditions which determine the "fixed trace progression," or the "given imaginary quadratic field progression"?

In some sense what we are about is to reconstruct the arithmetic of an elliptic curve without complex multiplication by piecing together the totality of elliptic curves with complex multiplication in a certain way. There should be something like a reciprocity law which bears to our conjectured asymptotic behavior a relationship analogous to that which the Artin reciprocity law bore to the Frobenius conjectured density properties, proved by Tchebotarev.

3. Again in the case of elliptic curves, can one give a condition on the analytic behavior of the associated Dirichlet series (zeta function) which implies our conjectured asymptotic property? In particular, is there significance to the partial Euler products taken over those p which are supersingular, or which correspond to a given imaginary quadratic field, and is there an L-series formalism attached to such products? The Hardy-Littlewood paper [H – L] is in two parts. The first shows how various Riemann Hypotheses imply distribution results. The second, including the conjecture on primes in quadratic progressions, limits itself to heuristic arguments. Therefore, even in that case, it would be interesting to see what analytic properties of zeta functions imply the conjectured asymptotic behavior.

4. Adapting to the present situation the classical view point of characterizing Galois extensions by those primes that split completely, it is reasonable to expect that two elliptic curves over the rationals are isogenous if they have the same set of supersingular primes, except possibly for a subset having an asymptotic order of magnitude strictly smaller than $\sqrt{x}/\log x$. Further comments are made on this in §4, when we have more precise definitions to discuss the matter technically.

For simplicity of expression, the conjecture may be weakened by requiring that the two curves have the same sets of supersingular primes, except for a finite number. In §4 we shall see that it may be strengthened by supposing merely that the common set of supersingular primes not be $O(\log \log x)$.

The elliptic curve A has a rational invariant j_A. For all non-exceptional primes p, we have

> $\mathbf{Q}(\pi_p) = k$ *if and only if* $j_A \equiv j(\mathfrak{o}) \pmod{\mathfrak{p}}$ *for some order* $\mathfrak{o}$ *in* k *and some prime* $\mathfrak{p}$ *over* p *in* $k(j(\mathfrak{o}))$.

According to a theorem of Deuring (cf. [L 1], Chapter 13, §4, Theorem 13), we can pick $\mathfrak{o}$ such that p splits completely in $k(j(\mathfrak{o}))$, and the above congruence condition has to be satisfied. It is standard (cf. [L 1], Chapter 8, §1, Corollary of Theorem 7) that there is only a finite number of imaginary quadratic orders $\mathfrak{o}$ such that $j(\mathfrak{o})$ lies in a given number field. However this approach through an increasing tower of orders and congruence conditions did not seem to lead towards a determination of the asymptotic behavior of the distribution of Frobenius elements belonging to the given quadratic field k.

Finally we observe that in the light of Yoshida's proof of the analogue of the Sato conjecture in the function field case [Y], it is possible that enough is known about the distribution of Frobenius elements in that case to be able to give a proof of the analogue of our conjecture. Of course, there is no question of having infinitely many supersingular values of j, which are necessarily finite, and in characteristic p one can only have imaginary quadratic fields as algebras of endomorphisms in which p splits completely, by Deuring's theorems. Cf. [L 1], Chapter 13 and 14. Except for these limitations, one expects a similar theory to hold. The approach through the congruence values $j(\mathfrak{o})$ as $\mathfrak{o}$ ranges over orders of k with conductor prime to p may in fact work in this case, in line with Ihara's ideas [I] which were used by Yoshida [Y].

There remains to say a few words about the logistics of this paper. In Part I, we discuss the fixed trace case In Part II, we treat the imaginary quadratic distribution. While the finite part of the constant stabilizes at finite level in Part I, it does not in Part II, and its theoretical analysis, as well as practical computation requires a more elaborate discussion. Finally, in Part III, we put together special computations dealing with the quadratic fields for which the GL_2-extension has an intersection with the maximal abelian extension of k which is strictly bigger than the field of all roots of unity. These cases are the most interesting.

For instance, the exceptionally large number of occurrences of $Q(\sqrt{-11})$ for $X_0(11)$ must be reflected in a correspondingly large prediction. (It occurs 88 times, when most other fields occur at most one-fourth this many times.) This requires a description of the field of 4-division points. Other cases require a similar description of the 3-division points. Since we felt that our computations should be checkable by anyone else interested to do so, we have included the full details in all cases.

In Part IV we present and discuss the numerical results for five curves and the first 5,000 primes. For one of the curves, $X_0(11)$, the calculation was pushed to include almost 190,000 primes. On the whole, the fit between actual and predicted values is good. We feel that the data are compatible with the conjecture. There are discrepancies, but they seem to lie within the range of reasonable statistical fluctuations.

PART I

SUPERSINGULAR AND FIXED TRACE DISTRIBUTION

PRELIMINARIES

THE DISTRIBUTION FOR FIXED TRACE

EXAMPLES

PART II

IMAGINARY QUADRATIC DISTRIBUTION

THE FIXED TRACE CASE

THE MODEL FOR THE MIXED CASE

COMPUTATIONS OF HARISH TRANSFORMS

PART III

SPECIAL COMPUTATIONS

GENERAL LEMMAS

$k = \mathbf{Q}(\sqrt{-3})$

$k = \mathbf{Q}(i)$

$k = \mathbf{Q}(\sqrt{\Delta})$

PART IV

NUMERICAL RESULTS

SUPERSINGULAR AND FIXED TRACE DISTRIBUTION

IMAGINARY QUADRATIC DISTRIBUTION

EXTENDED RESULTS FOR $X_0(11)$