Pacific Journal of Mathematics

ELLIPTIC CURVES, RANDOM MATRICES AND ORBITAL INTEGRALS

JEFFREY D. ACHTER AND JULIA GORDON

WITH AN APPENDIX BY S. ALI ALTUĞ

Volume 286 No. 1 January 2017

PACIFIC JOURNAL OF MATHEMATICS
Vol. 286, No. 1, 2017
dx.doi.org/10.2140/pjm.2017.286.1

ELLIPTIC CURVES, RANDOM MATRICES AND ORBITAL INTEGRALS

JEFFREY D. ACHTER AND JULIA GORDON

WITH AN APPENDIX BY S. ALI ALTUĞ

An isogeny class of elliptic curves over a finite field is determined by a quadratic Weil polynomial. Gekeler has given a product formula, in terms of congruence considerations involving that polynomial, for the size of such an isogeny class (over a finite prime field). In this paper we give a new transparent proof of this formula; it turns out that this product actually computes an adelic orbital integral which visibly counts the desired cardinality. This answers a question posed by N. Katz and extends Gekeler's work to ordinary elliptic curves over arbitrary finite fields.

1. Introduction

The isogeny class of an elliptic curve over a finite field $\mathbb{F}_p$ of p elements is determined by its trace of Frobenius; calculating the size of such an isogeny class is a classical problem. Fix a number a with $|a| \leq 2\sqrt{p}$, and let $I(a, p)$ be the set of all elliptic curves over $\mathbb{F}_p$ with trace of Frobenius a. Further suppose that $p \nmid a$, so that the isogeny class is ordinary.

Gekeler [2003] proposed a random matrix model to compute the size of $I(a, p)$ (see also [Katz 2009]). For each rational prime $\ell \neq p$, let

(1-1)
$$\nu_\ell(a, p) = \lim_{n\to\infty} \frac{\#\{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^n) : \mathrm{tr}(\gamma) \equiv a \bmod \ell^n, \det(\gamma) \equiv p \bmod \ell^n\}}{\#\,\mathrm{SL}_2(\mathbb{Z}/\ell^n)/\ell^n}.$$

For $\ell = p$, let

(1-2)
$$\nu_p(a, p) = \lim_{n\to\infty} \frac{\#\{\gamma \in \mathrm{M}_2(\mathbb{Z}/p^n) : \mathrm{tr}(\gamma) \equiv a \bmod p^n, \det(\gamma) \equiv p \bmod p^n\}}{\#\,\mathrm{SL}_2(\mathbb{Z}/p^n)/p^n}.$$

Achter's research was partially supported by grants from the Simons Foundation (204164) and the NSA (H98230-14-1-0161 and H98230-15-1-0247). Gordon's research was supported by NSERC.
MSC2010: primary 11G20, 22E35; secondary 14G15.
Keywords: elliptic curve, orbital integral, isogeny class.

On average, the number of elements of $\mathrm{GL}_2(\mathbb{Z}/\ell^n)$ with a given characteristic polynomial is $\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^n)/(\#(\mathbb{Z}/\ell^n)^\times \cdot \ell^n)$. Thus, $\nu_\ell(a, p)$ measures the departure of the frequency of the event that a random matrix γ satisfies $f_\gamma(T) = T^2 - aT + p$ from the average (over all possible characteristic polynomials).

It turns out [Gekeler 2003, Theorem 5.5] that

$$\widetilde{\#} I(a, p) = \frac{1}{2}\sqrt{p}\,\nu_\infty(a, p) \prod_\ell \nu_\ell(a, p), \tag{1-3}$$

where

$$\nu_\infty(a, p) = \frac{2}{\pi}\sqrt{1 - \frac{a^2}{4p}},$$

$\widetilde{\#} I(a, p)$ is a count weighted by automorphisms (2-1), and we note that the term $H^*(a, p)$ of [Gekeler 2003] actually computes $2\widetilde{\#} I(a, p)$ (see [Gekeler 2003, (2.10) and (2.13); Katz 2009, Theorem 8.5, p. 451]). This equation is almost miraculous. An equidistribution assumption about Frobenius elements, which is so strong that it can't possibly be true, leads one to the correct conclusion.

In contrast to the heuristic, the proof of (1-3) is somewhat pedestrian. Let $\Delta_{a,p} = a^2 - 4p$, let $K_{a,p} = \mathbb{Q}(\sqrt{\Delta_{a,p}})$, and let $\chi_{a,p}$ be the associated quadratic character. Classically, the size of the isogeny class $I(a, \mathbb{F}_p)$ is given by the Kronecker class number $H(\Delta_{a,p})$. Direct calculation [Gekeler 2003] shows that, at least for unramified primes ℓ,

$$\nu_\ell(a, p) = \frac{1}{1 - \chi_{a,p}(\ell)/\ell}$$

is the term at ℓ in the Euler product expansion of $L(1, \chi_{a,p})$. More generally, a term by term comparison shows that the right-hand side of (1-3) computes $H(\Delta_{a,p})$.

Even though (1-3) is striking and unconditional, one might still want a pure thought derivation of it. (We are not alone in this desire; Katz calls attention to this question in [Katz 2009, Remark 8.7].) Our goal in the present paper is to provide a conceptual explanation of (1-3). We will show that Gekeler's random matrix model (i.e., the right-hand side of (1-3)) directly calculates $\widetilde{\#} I(a, p)$, *without* appeal to class numbers. A further payoff of our method is that we extend Gekeler's results to the case of ordinary elliptic curves over an arbitrary finite field $\mathbb{F}_q$.

Our method relies on the description, due to Langlands (for modular curves) and Kottwitz (in general), of the points on a Shimura variety over a finite field. A consequence of their study is that one can calculate the cardinality of an ordinary isogeny class of elliptic curves over $\mathbb{F}_q$ using orbital integrals on the finite adelic points of GL_2 (Proposition 2.1). Our main observation is that one can, without explicit calculation, relate each local factor $\nu_\ell(a,q)$ to an orbital integral

$$\int_{G_{\gamma_\ell}(\mathbb{Q}_\ell)\backslash \mathrm{GL}_2(\mathbb{Q}_\ell)} \mathbb{1}_{\mathrm{GL}_2(\mathbb{Z}_\ell)}(x^{-1}\gamma_\ell x)\,dx, \tag{1-4}$$

where γ_ℓ is an element of $\mathrm{GL}_2(\mathbb{Q}_\ell)$ of trace a and determinant q, G_{γ_ℓ} is its centralizer in $\mathrm{GL}_2(\mathbb{Q}_\ell)$, and $\mathbb{1}_{\mathrm{GL}_2(\mathbb{Z}_\ell)}$ is the characteristic function of the maximal compact subgroup $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Here the choice of the invariant measure dx on the orbit is crucial. On one hand, the measure that is naturally related to Gekeler's numbers is the so-called *geometric measure* (see [Frenkel et al. 2010]), which we review in Section 3A3. On the other hand, this measure is inconvenient for computing the global volume term that appears in the formula of Langlands and Kottwitz. The main technical difficulty is the comparison, which should be well-known but is hard to find in the literature, between the geometric measure and the so-called *canonical measure*.

We start in Section 2 by establishing notation and reviewing the Langlands–Kottwitz formula. We define the relevant natural measures in Section 3, and study the comparison factor between them in Section 4. Finally, in Section 5, we complete the global calculation.

It is perhaps not surprising that one can use a similar method to give an analogous product formula for the size of an isogeny class of simple ordinary principally polarized abelian varieties over a finite field. (The fact that the group controlling the moduli problem is GSp_{2g} rather than GL_2 means that, for example, conjugacy and stable conjugacy no longer coincide, the explicit invocation of the fundamental lemma is more involved, the comparison of measures (Proposition 4.5) is more difficult, the global volume calculation is less immediate, etc.) We take up this challenge in a companion work.

It turns out that [Frenkel et al. 2010, §3] has much of the information one needs for the crucial comparison of measures. This is explained in the Appendix by S. Ali Altuğ.

As we were finishing this paper, the authors of [David et al. 2016] shared their work with us, which takes Gekeler's random matrix model as its starting point; we invite the interested reader to consult that work.

Notation. Throughout, $\mathbb{F}_q$ is a finite field of characteristic p and cardinality $q = p^e$. Let $\mathbb{Q}_q$ be the unique unramified extension of $\mathbb{Q}_p$ of degree e, and let $\mathbb{Z}_q \subset \mathbb{Q}_q$ be its ring of integers. We use σ to denote both the canonical generator of $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and its lift to $\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$.

Typically, G will denote the algebraic group GL_2. While many of our results admit immediate generalization to other reductive groups, as a rule we resist this temptation unless the statement and its proof require no additional notation.

Shortly, we will fix a regular semisimple element $\gamma_0 \in G(\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Q})$; its centralizer will variously be denoted G_{γ_0} and T.

Conjugacy in an abstract group is denoted by $\sim$.

2. Preliminaries

Here we collect notation concerning isogeny classes (Section 2A) as well as basic information on Gekeler's ratios (Section 2C) and the Langlands–Kottwitz formula (Section 2D).

2A. ***Isogeny classes of elliptic curves.*** If $E/\mathbb{F}_q$ is an elliptic curve, then its characteristic polynomial of Frobenius has the form $f_{E/\mathbb{F}_q}(T) = T^2 - a_{E/\mathbb{F}_q}T + q$, where $|a_{E/\mathbb{F}_q}| \leq 2\sqrt{q}$. Moreover, E_1 and E_2 are $\mathbb{F}_q$-isogenous if and only if $a_{E_1/\mathbb{F}_q} = a_{E_2/\mathbb{F}_q}$. In particular, for a given integer a with $|a| \leq 2\sqrt{q}$, the set

$$I(a,q) = \{E/\mathbb{F}_q : a_{E/\mathbb{F}_q} = a\}$$

is a single isogeny class of elliptic curves over $\mathbb{F}_q$. Its weighted cardinality is

$$\widetilde{\#} I(a,q) := \sum_{E \in I(a,q)} \frac{1}{\#\,\mathrm{Aut}(E)}. \tag{2-1}$$

A member of this isogeny class is ordinary if and only if $p \nmid a$; henceforth, we assume this is the case.

Fix an element $\gamma_0 \in G(\mathbb{Q})$ with characteristic polynomial

$$f_0(T) = f_{a,q}(T) := T^2 - aT + q.$$

Newton polygon considerations show that exactly one root of $f_{a,q}(T)$ is a p-adic unit, and in particular $f_{a,q}(T)$ has distinct roots. Therefore, γ_0 is regular semisimple. Moreover, any other element of $G(\mathbb{Q})$ with the same characteristic polynomial is conjugate to γ_0. (Here and elsewhere, we use the fact that in a general linear group, two elements are conjugate if and only if they are stably conjugate.)

Let $K = K_{a,q} = \mathbb{Q}[T]/f(T)$; it is a quadratic imaginary field. If $E \in I(a,q)$, then its endomorphism algebra is $\mathrm{End}(E) \otimes \mathbb{Q} \cong K$. The centralizer G_{γ_0} of γ_0 in G is the restriction of scalars torus $G_{\gamma_0} \cong \mathrm{R}_{K/\mathbb{Q}}\mathbb{G}_m$.

If α is an invariant of an isogeny class, we will variously denote it as $\alpha(a,q)$, $\alpha(f_0)$, or $\alpha(\gamma_0)$, depending on the desired emphasis.

2B. ***The Steinberg quotient.*** We review the general definition of the Steinberg quotient. Let G be a split, reductive group of rank r, with simply connected derived group G^{der} and Lie algebra $\mathfrak{g}$; further assume that $G/G^{\mathrm{der}} \cong \mathbb{G}_m$. (In the case of interest for this paper, $G = \mathrm{GL}_2$, $r = 2$, and $G^{\mathrm{der}} = \mathrm{SL}_2$.)

Let T be a split maximal torus in G, $T^{\mathrm{der}} = T \cap G^{\mathrm{der}}$ (note that T^{der} is *not* the derived group of T), and W be the Weyl group of G relative to T. Let $A^{\mathrm{der}} = T^{\mathrm{der}}/W$ be the Steinberg quotient for the semisimple group G^{der}. It is isomorphic to the affine space of dimension $r-1$.

Let $A = A^{\mathrm{der}} \times \mathbb{G}_m$ be the analogue of the Steinberg quotient for the reductive group G, see [Frenkel et al. 2010]. We think of A as the space of "characteristic polynomials". There is a canonical map

$$G \xrightarrow{\mathfrak{c}} A. \tag{2-2}$$

Since $G/G^{\mathrm{der}} \cong \mathbb{G}_m$, we have

$$A \cong \mathbb{A}^{r-1} \times \mathbb{G}_m \subset \mathbb{A}^r.$$

2C. ***Gekeler numbers.*** We resume our earlier discussion of elliptic curves, and let $G = \mathrm{GL}_2$. As in Section 2A, fix data (a, q) defining an ordinary isogeny class over $\mathbb{F}_q$. Recall that, to each finite prime ℓ, Gekeler has assigned a local probability $\nu_\ell(a, q)$, see (1-1) and (1-2). We give a geometric interpretation of this ratio, as follows.

Since G is a group scheme over $\mathbb{Z}$, for any finite prime ℓ we have a well-defined group $G(\mathbb{Z}_\ell)$, which is a (hyperspecial) maximal compact subgroup of $G(\mathbb{Q}_\ell)$, as well as the "truncated" groups $G(\mathbb{Z}_\ell/\ell^n)$ for every integer $n \geq 0$.

Recall that, given the fixed data (a, q), we have chosen an element $\gamma_0 \in G(\mathbb{Q})$. Since the conjugacy class of a semisimple element of a general linear group is determined by its characteristic polynomial, γ_0 is well-defined up to conjugacy.

Let ℓ be any finite prime (we allow the possibility $\ell = p$); using the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_\ell$ we identify γ_0 with an element of $G(\mathbb{Q}_\ell)$. In fact, if $\ell \neq p$, then γ_0 is a regular semisimple element of $G(\mathbb{Z}_\ell)$.

For a fixed positive integer n, the average value of $\#\mathfrak{c}^{-1}(a)$, as a ranges over $A(\mathbb{Z}_\ell/\ell^n)$, is

$$\#G(\mathbb{Z}_\ell/\ell^n)/\#A(\mathbb{Z}_\ell/\ell^n).$$

Consequently, we set

$$\nu_{\ell,n}(a, q) = \nu_{\ell,n}(\gamma_0) = \frac{\#\{\gamma \in G(\mathbb{Z}_\ell/\ell^n) : \gamma \sim (\gamma_0 \bmod \ell^n)\}}{\#G(\mathbb{Z}_\ell/\ell^n)/\#A(\mathbb{Z}_\ell/\ell^n)}, \tag{2-3}$$

and rewrite (1-3) (and extend it to the case of $\mathbb{F}_q$) as

$$\nu_\ell(a, q) = \lim_{n\to\infty} \nu_{\ell,n}(a, q). \tag{2-4}$$

Again, we have exploited the fact that two semisimple elements of GL_2 are conjugate if and only if their characteristic polynomials are the same. Note that the denominator of (2-4) coincides with that of Gekeler's definition [2003, (3.7)]. Indeed,

$$\frac{\#G(\mathbb{Z}/\ell^n)}{\#A(\mathbb{Z}/\ell^n)} = \frac{\ell(\ell-1)(\ell^2-1)\ell^{4n-4}}{(\ell-1)\ell^{n-1}\ell^n} = (\ell^2-1)\ell^{2n-2}. \tag{2-5}$$

For $\ell = p$, γ_0 lies in $\mathrm{GL}_2(\mathbb{Q}_p) \cap \mathrm{Mat}_2(\mathbb{Z}_p)$. We make the apparently ad hoc definition

$$\nu_p(a,q) = \lim_{n\to\infty} \frac{\#\{\gamma \in \mathrm{Mat}_2(\mathbb{Z}_p/p^n) : \gamma \sim (\gamma_0 \bmod p^n)\}}{\#G(\mathbb{Z}_p/p^n)/\#A(\mathbb{Z}_p/p^n)}, \tag{2-6}$$

where we have briefly used $\sim$ to denote similarity of matrices under the action of $\mathrm{GL}_2(\mathbb{Z}_p/p^n)$. In the case where $q = p$, this recovers Gekeler's definition (1-2).

Finally, we follow [Gekeler 2003, (3.3)] and, inspired by the Sato–Tate measure, define an archimedean term

$$\nu_\infty(a,q) = \frac{2}{\pi}\sqrt{1-\frac{a^2}{4q}}. \tag{2-7}$$

2D. ***The Langlands and Kottwitz approach.*** For Shimura varieties of PEL type, Kottwitz [1992] proved Langlands's conjectural expression of the zeta function of that Shimura variety in terms of automorphic L-functions on the associated group. A key, albeit elementary, tool in this proof is the fact that the isogeny class of a (structured) abelian variety can be expressed in terms of an orbital integral. The special case where the Shimura variety in question is a modular curve, so that the abelian varieties are simply elliptic curves, has enjoyed several detailed presentations in the literature (e.g., [Clozel 1993; Scholze 2011] and, to a lesser extent, [Achter and Cunningham 2002]), and so we content ourselves here with the relevant statement.

As in Section 2A, fix data (a,q) which determines an isogeny class of ordinary elliptic curves over $\mathbb{F}_q$, and let $\gamma_0 \in G(\mathbb{Q})$ be a suitable choice. If $E \in I(a,q)$, then for each ℓ not dividing q there is an isomorphism

$$H^1(E_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell^{\oplus 2}$$

which takes the Frobenius endomorphism of E to γ_0.

There is an additive operator F on $H^1_{\mathrm{cris}}(E,\mathbb{Q}_q)$. It is σ-linear, in the sense that if $a \in \mathbb{Q}_q$ and $x \in H^1_{\mathrm{cris}}(E,\mathbb{Q}_q)$, then $F(ax) = a^\sigma F(x)$. To F corresponds some $\delta_0 \in G(\mathbb{Q}_q)$, well-defined up to σ-conjugacy. (Recall that δ and δ' are σ-conjugate if there exists some $h \in G(\mathbb{Q}_q)$ such that $h^{-1}\delta h^\sigma = \delta'$.) The two elements are related by $\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(\delta_0) \sim \gamma_0$.

Let G_{γ_0} be the centralizer of γ_0 in G. Let $G_{\delta_0\sigma}$ be the twisted centralizer of δ_0 in $G_{\mathbb{Q}_q}$; it is an algebraic group over $\mathbb{Q}_p$.

Finally, let $\mathbb{A}_f^p$ denote the prime-to-p finite adeles, and let $\hat{\mathbb{Z}}_f^p \subset \mathbb{A}_f^p$ be the subring of everywhere-integral elements. With these notational preparations, we have:

Proposition 2.1. *The weighted cardinality of an ordinary isogeny class of elliptic curves is given by*

$$\widetilde{\#}I(a,q) = \mathrm{vol}(G_{\gamma_0}(\mathbb{Q})\backslash G_{\gamma_0}(\mathbb{A}_f)) \cdot \int_{G_{\gamma_0}(\mathbb{A}_f^p)\backslash G(\mathbb{A}_f^p)} \mathbb{1}_{G(\hat{\mathbb{Z}}_f^p)}(g^{-1}\gamma_0 g)\,dg \cdot \int_{G_{\delta_0\sigma}(\mathbb{Q}_p)\backslash G(\mathbb{Q}_q)} \mathbb{1}_{G(\mathbb{Z}_q)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)G(\mathbb{Z}_q)}(h^{-1}\delta_0 h^{\sigma})\,dh. \tag{2-8}$$

Here, each group $G(\mathbb{Q}_\ell)$ has been given the Haar measure which assigns volume one to $G(\mathbb{Z}_\ell)$ (this is the so-called *canonical measure*, see Section 3A2). The choice of nonzero Haar measure on the centralizer $G_\gamma(\mathbb{Q}_\ell)$ is irrelevant, as long as the same choice is made for the global volume computation. Similarly, in the second, twisted orbital integral, $G(\mathbb{Q}_q)$ is given the Haar measure which assigns volume one to $G(\mathbb{Z}_q)$. Since we shall need to say something about the volume term later, we need to fix the measures on $G_{\gamma_0}(\mathbb{Q}_\ell)$ for every ℓ. We choose the canonical measures μ^{can} on both G and G_{γ_0} at every place. These measures are defined below in Section 3A2.

The idea behind Proposition 2.1 is straightforward. (We defer to [Clozel 1993] for details.) Fix an $E \in I(a,q)$ and $H^1(E_{\bar{\mathbb{F}}_q}, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell^{\oplus 2}$ as above. This singles out an integral structure

$$H^1(E_{\bar{\mathbb{F}}_q}, \mathbb{Z}_\ell) \subseteq \mathbb{Q}_\ell^{\oplus 2}.$$

If E' is any other member of $I(a,q)$, then the prime-to-p part of an $\mathbb{F}_q$-rational isogeny $E \to E'$ gives a new integral structure $H^1(E'_{\bar{\mathbb{F}}_q}, \mathbb{Z}_\ell)$ on $\mathbb{Q}_\ell^{\oplus 2}$. Similarly, p-power isogenies give rise to new integral structures on the crystalline cohomology $H^1_{\mathrm{cris}}(E, \mathbb{Q}_q)$. In this way, $I(a,q)$ is identified with $K^\times\backslash Y^p \times Y_p$, where Y^p ranges among γ_0-stable lattices in $Y^1(E_{\bar{\mathbb{F}}_q}, \mathbb{A}^p)$, and Y_p ranges among lattices in $H^1_{\mathrm{cris}}(E, \mathbb{Q}_q)$ stable under δ_0 and $p\delta_0^{-1}$. It is now straight forward to use an orbital integral to calculate the automorphism-weighted, or groupoid, cardinality of the quotient set $K^\times\backslash Y^p \times Y_p$ (e.g., [Hales 2012, §6]).

We remark that most expositions of Proposition 2.1 refer to a geometric context in which $\mathbb{1}_{G(\hat{\mathbb{Z}}_f^p)}$ is replaced with the characteristic function of an open compact subgroup which is sufficiently small that objects have trivial automorphism groups, so that the corresponding Shimura variety is a smooth and quasiprojective fine moduli space. However, this assumption is not necessary for the counting argument underlying (2-8); see, for instance, [Clozel 1993, Section 3(b)].

3. Comparison of Gekeler numbers with orbital integrals

The calculation is based on the interplay between several G-invariant measures on the adjoint orbits in G. We start by carefully reviewing the definitions and the normalizations of all Haar measures involved.

3A. ***Measures on groups and orbits.*** Let $\pi_n : \mathbb{Z}_\ell \to \mathbb{Z}_\ell/\ell^n$ be the truncation map. For any $\mathbb{Z}_\ell$-scheme $\mathcal{X}$, we denote by $\pi_n^{\mathcal{X}}$ the corresponding map

$$\pi_n^{\mathcal{X}} : \mathcal{X}(\mathbb{Z}_\ell) \to \mathcal{X}(\mathbb{Z}_\ell/\ell^n)$$

induced by π_n.

Once and for all, fix the Haar measure on $\mathbb{A}^1(\mathbb{Q}_\ell)$ such that the volume of $\mathbb{Z}_\ell$ is 1. We will denote this measure by dx. For our calculations the key observation is that, with this normalization, the fibers of the standard projection $\pi_n^{\mathbb{A}^d} : \mathbb{A}^d(\mathbb{Z}_\ell) \to \mathbb{A}^d(\mathbb{Z}/\ell^n\mathbb{Z})$ have volume ℓ^{-nd}.

There are two fundamental approaches to normalizing a Haar measure on the set of $\mathbb{Q}_\ell$-points of an arbitrary algebraic group G. One can either fix a maximal compact subgroup and assign volume 1 to it, or one can fix a volume form ω_G on G with coefficients in $\mathbb{Z}$, and thus get the measure $|\omega_G|_\ell$ on each $G(\mathbb{Q}_\ell)$.

For the $\mathbb{Q}_\ell$-points of a general variety, one also has the Serre–Oesterlé measure; it is this measure which naturally arises in studying Gekeler-type ratios. In the case of GL_2, this measure comes from the volume form which Gross calls *canonical*.

We now review these constructions and the relations between them.

3A1. *Serre–Oesterlé measure.* Let $\mathcal{X}$ be a smooth scheme over $\mathbb{Z}_\ell$. Then there is the so-called Serre–Oesterlé measure on X, which we will denote by μ_X^{SO}. It is defined in [Serre 1981, §3.3], see also [Veys 1992] for an attractive equivalent definition. For a smooth scheme that has a nonvanishing gauge form this definition coincides with the definition of A. Weil [1982], and by Theorem 2.2.5 of that paper (extended by Batyrev [1999, Theorem 2.7]), this measure has the property that $\mathrm{vol}_{\mu_X^{\mathrm{SO}}}(\mathcal{X}(\mathbb{Z}_\ell)) = \#\mathcal{X}(\mathbb{F}_\ell)\ell^{-d}$, where d is the dimension of the generic fiber of $\mathcal{X}$. In particular, $\mu_{\mathbb{A}^1}^{\mathrm{SO}}$ is the Haar measure on the affine line such that $\mathrm{vol}_{\mu_{\mathbb{A}^1}^{\mathrm{SO}}}(\mathbb{A}^1(\mathbb{Z}_\ell)) = \ell\ell^{-1} = 1$, i.e., $\mu_{\mathbb{A}^1(\mathbb{Q}_\ell)}^{\mathrm{SO}}$ coincides with $|dx|_\ell$. Similarly, on any d-dimensional affine space $\mathbb{A}^d$, the Serre–Oesterlé measure gives $\mathbb{A}^d(\mathbb{Z}_\ell)$ volume 1.

The algebraic group GL_2 is a smooth group scheme defined over $\mathbb{Z}$. In particular, for every ℓ, $\mathrm{GL}_2 \times_{\mathbb{Z}} \mathbb{Z}_\ell$ is a smooth scheme over $\mathbb{Z}_\ell$, so μ^{SO} gives $\mathrm{GL}_2(\mathbb{Z}_\ell)$ volume

$$\mathrm{vol}_{\mu_{\mathrm{GL}_2}^{\mathrm{SO}}}(\mathrm{GL}_2(\mathbb{Z}_\ell)) = \frac{\#\,\mathrm{GL}_2(\mathbb{F}_\ell)}{\ell^d} = \frac{\ell(\ell-1)(\ell^2-1)}{\ell^4}.$$

3A2. *The canonical measures.* Let G be a reductive group over $\mathbb{Q}_\ell$; Gross [1997, Section 4] defines a canonical integral model $\underline{G}/\mathbb{Z}_\ell$. If G is unramified and connected, then $\underline{G}(\mathbb{Z}_\ell)$ is a hyperspecial maximal compact subgroup of $G(\mathbb{Q}_\ell)$. If T is a (possibly ramified) torus, then $\underline{T}$ is the identity component $\mathcal{T}^\circ$ of the weak Néron model $\mathcal{T}$ of T (discussed in more detail in Section 4A).

The measure most commonly used in orbital integrals, μ^{can}, is the Haar measure which assigns volume 1 to $\underline{G}(\mathbb{Z}_\ell)$.

In fact, Gross uses $\underline{G}$ to define a canonical volume form ω_G, which does not vanish on the special fiber $\underline{G}^\kappa$ of $\underline{G}$. If G is unramified over $\mathbb{Q}_\ell$, then ω_G recovers the Serre–Oesterlé measure, insofar as

$$\int_{\underline{G}(\mathbb{Z}_\ell)} |\omega_G|_\ell = \frac{\#\underline{G}^\kappa(\mathbb{F}_\ell)}{\ell^{\dim G}}$$

[Gross 1997, Proposition 4.7].

3A3. *The geometric measure.* We will use a certain quotient measure μ^{geom} on the orbits, which is called the geometric measure in [Frenkel et al. 2010]. This measure is defined using the Steinberg map $\mathfrak{c}$, (2-2). We return to the setting of Section 2B.

For a general reductive group G and $\gamma \in G(\mathbb{Q}_\ell)$ regular semisimple, the fiber over $\mathfrak{c}(\gamma)$ is the stable orbit of γ, which is a finite union of rational orbits. In our setting with $G = \mathrm{GL}_2$, the fiber $\mathfrak{c}^{-1}(\mathfrak{c}(\gamma))$ is a single rational orbit, which substantially simplifies the situation. From here onwards, we work only with $G = \mathrm{GL}_2$.

Consider the measure given by the form ω_G on G, and the measure on $A = \mathbb{A}^1 \times \mathbb{G}_m$ which is the product of the measures associated with the form dt on $\mathbb{A}^1$ and ds/s on $\mathbb{G}_m$, where we denote the coordinates on A by (t, s). We will denote this measure by $|d\omega_A|$.

The form ω_G is a generator of the top exterior power of the cotangent bundle of G. For each orbit $\mathfrak{c}^{-1}(t, s)$ (note that such an orbit is a variety) there is a unique generator $\omega^{\mathrm{geom}}_{\mathfrak{c}(\gamma)}$ of the top exterior power of the cotangent bundle on the orbit $\mathfrak{c}^{-1}(\mathfrak{c}(\gamma))$ such that

$$\omega_G = \omega^{\mathrm{geom}}_{\mathfrak{c}(\gamma)} \wedge \omega_A.$$

Then for any $\phi \in C_c^\infty(G(\mathbb{Q}_\ell))$,

$$\int_{G(\mathbb{Q}_\ell)} \phi(g)\,|d\omega_G| = \int_{A(\mathbb{Q}_\ell)} \int_{\mathfrak{c}^{-1}(\mathfrak{c}(\gamma))} \phi(g)\,|d\omega^{\mathrm{geom}}_{\mathfrak{c}(\gamma)}|\,|d\omega_A(t, s)|.$$

This measure also appears in [Frenkel et al. 2010], and it is discussed in detail in Section 4 below.

3A4. *Orbital integrals.* There are two kinds of orbital integrals that will be relevant for us; they differ only in the normalization of measures on the orbits. Let γ be a regular semisimple element of $G(\mathbb{Q}_\ell)$, and let ϕ be a locally constant compactly supported function on $G(\mathbb{Q}_\ell)$. Let T be the centralizer G_γ of γ. Since γ is regular (i.e., the roots of the characteristic polynomial of γ are distinct) and semisimple, T is a maximal torus in G.

First, we consider the orbital integral with respect to the geometric measure.

Definition 3.1. Define $O_\gamma^{\mathrm{geom}}(\phi)$ by

$$O_\gamma^{\mathrm{geom}}(\phi) := \int_{T(\mathbb{Q}_\ell)\backslash G(\mathbb{Q}_\ell)} \phi(g^{-1}\gamma g)\, d\mu_\gamma^{\mathrm{geom}},$$

where $\mu_\gamma^{\mathrm{geom}}$ is the measure on the orbit of γ associated with the corresponding differential form $\omega^{\mathrm{geom}}_{\mathfrak{c}^{-1}(\mathfrak{c}(\gamma))}$ as in Section 3A3 above.

Second, there is the canonical orbital integral over the orbit of γ, defined as follows. The orbit of γ can be identified with the quotient $T(\mathbb{Q}_\ell)\backslash G(\mathbb{Q}_\ell)$. Both $T(\mathbb{Q}_\ell)$ and $G(\mathbb{Q}_\ell)$ are endowed with canonical measures, as above in Section 3A2. Then there is a unique quotient measure on $T(\mathbb{Q}_\ell)\backslash G(\mathbb{Q}_\ell)$, which will be denoted $\mu_\gamma^{\mathrm{can}}$. The canonical orbital integral will be the integral with respect to this measure on the orbit (also considered as a distribution on the space of locally constant compactly supported functions on $G(\mathbb{Q}_\ell)$).

Definition 3.2. Define $O_\gamma^{\mathrm{can}}(\phi)$ by

$$O_\gamma^{\mathrm{can}}(\phi) := \int_{T(\mathbb{Q}_\ell)\backslash G(\mathbb{Q}_\ell)} \phi(g^{-1}\gamma g)\, d\mu_\gamma^{\mathrm{can}}.$$

By definition, the distributions O_γ^{geom} and O_γ^{can} differ by a multiple that is a function of γ. This ratio (which we feel should probably be well-known but was hard to find in the literature, see also [Frenkel et al. 2010] and the Appendix) is computed in Section 4 below.

We will first relate Gekeler's ratios to orbital integrals with respect to the geometric measure, in a natural way, and from there will get the relationship with the canonical orbital integrals, which are more convenient to use for the purposes of computing the global volume term appearing in the formula of Langlands and Kottwitz.

3B. ***Gekeler numbers and volumes, for ℓ not equal to p.*** From now on, $G = \mathrm{GL}_2$, $\gamma_0 = \gamma_{a,q}$, and ℓ is a fixed prime distinct from p. Our first goal is to relate the Gekeler number $\nu_\ell(a,q)$, (2-4), to an orbital integral $O_{\gamma_0}^{\mathrm{geom}}(\phi_0)$ of a suitable test function ϕ_0 with respect to $|d\omega^{\mathrm{geom}}_{\mathfrak{c}(\gamma)}|$. (Recall that γ_0 is the element of $G(\mathbb{Q}_\ell)$ determined by E, and in this case since $\ell \neq p$, it lies in $G(\mathbb{Z}_\ell)$.) In order to do this we define natural subsets of $G(\mathbb{Q}_\ell)$ whose volumes are responsible for this relationship.

Recall (2-3), the definition of $\nu_{\ell,n}(\gamma_0)$. For each positive integer n, consider the subset V_n of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ defined as

$$\begin{aligned} V_n = V_n(\gamma_0) &:= \{\gamma \in \mathrm{GL}_2(\mathbb{Z}_\ell) \mid f_\gamma(T) \equiv f_0(T) \bmod \ell^n\} \\ &= \{\gamma \in \mathrm{GL}_2(\mathbb{Z}_\ell) \mid \pi_n^A(\mathfrak{c}(\gamma)) = \pi_n^A(\mathfrak{c}(\gamma_0))\}, \end{aligned} \tag{3-1}$$

and set

$$V(\gamma_0) := \bigcap_{n\geq 1} V_n(\gamma_0).$$

We define an auxiliary ratio

$$v_n(\gamma_0) := \frac{\mathrm{vol}_{\mu^{\mathrm{SO}}_{GL_2}}(V_n(\gamma_0))}{\ell^{-2n}}. \tag{3-2}$$

Now we would like to relate the limit of these ratios $v_n(\gamma_0)$ both to the limit of Gekeler ratios $\nu_{\ell,n}(\gamma_0)$ and to an orbital integral.

Let $\phi_0 = \mathbb{1}_{\mathrm{GL}_2(\mathbb{Z}_\ell)}$ be the characteristic function of the maximal compact subgroup $\mathrm{GL}_2(\mathbb{Z}_\ell)$ in $\mathrm{GL}_2(\mathbb{Q}_\ell)$.

Proposition 3.3. *We have*

$$\lim_{n\to\infty} v_n(\gamma_0) = O^{\mathrm{geom}}_{\gamma_0}(\phi_0).$$

Proof. Because equality of characteristic polynomials is equivalent to conjugacy in $\mathrm{GL}_2(\mathbb{Q}_\ell)$, $V(\gamma_0)$ is the intersection of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ with the orbit $\mathcal{O}(\gamma_0)$ of γ_0 in $G = \mathrm{GL}_2(\mathbb{Q}_\ell)$. Then the orbital integral $O^{\mathrm{geom}}_{\gamma_0}(\phi_0)$ is nothing but the volume of the set $V(\gamma_0)$, as a subset of $\mathcal{O}(\gamma_0)$, with respect to the measure $d\mu^{\mathrm{geom}}_{\gamma_0}$.

Let $a_0 = \mathfrak{c}(\gamma_0) = (a, q) \in \mathbb{A}^1 \times \mathbb{G}_m(\mathbb{Q}_\ell)$, and let $U_n(a_0)$ be its $\ell^{-n} \times \ell^{-n}$-neighborhood. Its Serre–Oesterlé volume is $\mathrm{vol}_{\mu^{\mathrm{SO}}_A}(U_n(\gamma_0)) = \ell^{-2n}$.

Moreover, $V_n(\gamma_0) = \mathfrak{c}^{-1}(U_n(\gamma_0)) \cap \mathrm{GL}_2(\mathbb{Z}_\ell)$. Consequently,

$$\begin{aligned}\lim_{n\to\infty} v_n(\gamma_0) &= \lim_{n\to\infty} \frac{\mathrm{vol}_{\mu^{\mathrm{SO}}_{\mathrm{GL}_2}}\big(\mathfrak{c}^{-1}(U_n(\gamma_0)) \cap \mathrm{GL}_2(\mathbb{Z}_\ell)\big)}{\mathrm{vol}_{\mu^{\mathrm{SO}}_A}(U_n(\gamma_0))} \\ &= \lim_{n\to\infty} \frac{\mathrm{vol}_{|d\omega_G|}\big(\mathfrak{c}^{-1}(U_n(\gamma_0)) \cap \mathrm{GL}_2(\mathbb{Z}_\ell)\big)}{\mathrm{vol}_{|d\omega_A|}(U_n(\gamma_0))} \\ &= \mathrm{vol}_{\mu^{\mathrm{geom}}_{\gamma_0}}(V(\gamma_0)),\end{aligned} \tag{3-3}$$

by definition of the geometric measure. □

Next, let us relate the ratios v_n to the Gekeler ratios.

Proposition 3.4. *The ratios $v_n(\gamma_0)$ (and thus, also $\nu_{\ell,n}(\gamma_0)$) stabilize, in the sense that when n is large enough, $v_n(\gamma_0) = \lim_{n\to\infty} v_n(\gamma_0)$, and we have*

$$\begin{aligned}\lim_{n\to\infty} v_n(\gamma_0) &= \frac{\#\,\mathrm{SL}_2(\mathbb{F}_\ell)}{\ell^3} \cdot \lim_{n\to\infty} \nu_{\ell,n}(\gamma_0) \\ &= \frac{\ell^2-1}{\ell^2} \cdot \nu_\ell(a, q).\end{aligned}$$

Remark 3.5. We do not need the claim that Gekeler's ratios $\nu_{\ell,n}$ stabilize for large n in order to relate them to the orbital integrals. However, we have included this claim in order to point out that this behavior (also proved by Gekeler by direct computation) is a special case of a very general phenomenon (which can be thought of as a multivariable version of Hensel's lemma) that has appeared in the work of Igusa, Serre, and later Veys, Denef, and others, and was at the foundation of the theory of motivic integration (see [Veys 2006] for related results), but does not appear to be widely known. We provide more specific references in the proof of the proposition.

Proof. Let $\pi_n = \pi_n^{\mathrm{GL}_2} : \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n)$. To ease notation slightly, let $V_n = V_n(\gamma_0)$. Let $S_n \subset \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ be the set that appears in the numerator of (2-3),

$$S_n := \{\gamma \in \mathrm{GL}_2(\mathbb{Z}/\ell^n) \mid f_\gamma(T) \equiv f_0(T) \bmod \ell^n\}.$$

First, observe that for all $n \geq 1$, we have $V_n = \pi_n^{-1}(S_n)$. Indeed, taking characteristic polynomials commutes with reduction $\bmod \ell^n$, since the coefficients of the characteristic polynomial are themselves polynomial in the matrix entries of γ, and reduction $\bmod \ell^n$ is a ring homomorphism. We claim that, for large enough n (with the restriction depending on the discriminant of f), the following hold:

(i) $\pi_n|_{V_n} : V_n \to S_n$ is surjective.

(ii) We have the equality

$$\mathrm{vol}_{\mu^{\mathrm{SO}}_{\mathrm{GL}_2}}(V_n) = \ell^{-4n} \# S_n. \tag{3-4}$$

(iii) The number $\ell^{2n}\, \mathrm{vol}_{\mu^{\mathrm{SO}}_{\mathrm{GL}_2}}(V_n)$ does not depend on n.

We only need the second and third claims to establish the Proposition; we have singled out the first claim since it is key to the proof of claims (ii) and (iii). First, let us finish the proof of the Proposition assuming (ii) holds. Handling the denominator of Gekeler's ratio as in (2-5) above, we get

$$v_n(\gamma_0) = \frac{\ell^{-4n}\# S_n}{\ell^{-2n}} = \frac{\# S_n}{\ell^{2n}} = \frac{\# S_n \# \mathrm{SL}_2(\mathbb{F}_\ell)}{\# \mathrm{SL}_2(\mathbb{F}_\ell)\ell^{3(n-1)}\ell^{-n}\ell^3} = \frac{\# \mathrm{SL}_2(\mathbb{F}_\ell)}{\ell^3}\nu_{\ell,n}(\gamma_0), \tag{3-5}$$

as required.

Thus, it remains to address the three claims. The set $V(\gamma_0)$ is the subset of $\mathbb{A}^4(\mathbb{Z}_\ell)$ cut out by the algebraic equations $\mathrm{tr}(\gamma) = \mathrm{tr}(\gamma_0)$ and $\det(\gamma) = \det(\gamma_0)$. Since γ_0 is a regular semisimple element, these equations define a 2-dimensional ℓ-adic analytic submanifold of $\mathbb{A}^4$ (namely, the orbit of γ_0). For such submanifolds, all three claims were proved by J.-P. Serre in [Serre 1981] (see Theorem 9 in §3.3 and the remarks following it; see also [Veys 1992, Proposition 0.1], and the discussion before Corollary 1.8.2 in the survey [Denef 2000]). We note that (i) is key, and the other two claims follow easily. Indeed, since GL_2 is smooth over the residue field $\mathbb{F}_\ell$, all fibers of π_n have volume equal to ℓ^{-4n}. The set V_n is a disjoint union of fibers of π_n, and by (i), the number of these fibers is $\#\pi_n(V_n) = \#S_n$. Thus, the volume of V_n is exactly ℓ^{-4n} times the number of points in the image of the set in the numerator under this projection. Claim (iii) follows in a similar fashion by considering $\pi_{n+1}(V_n) = S_{n+1}$ as a fibration over S_n. $\square$

Combining Propositions 3.3 and 3.4, we immediately obtain:

Corollary 3.6. *The Gekeler numbers relate to orbital integrals via*

$$\nu_\ell(a, q) = \frac{\ell^3}{\#\,\mathrm{SL}_2(\mathbb{F}_\ell)} O_{\gamma_0}^{\mathrm{geom}}(\phi_0).$$

3C. *ℓ = p revisited.* We now consider $\nu_p(a, q)$ in a similar light. Since $\det(\gamma_0) = q$, γ_0 lies in $\mathrm{Mat}_2(\mathbb{Z}_p) \cap \mathrm{GL}_2(\mathbb{Q}_p)$ but *not* in $\mathrm{GL}_2(\mathbb{Z}_p)$, and we must consequently modify the argument of Section 3B.

For integers m and n, let $\lambda_{m,n} = \left(\begin{smallmatrix} p^m & 0 \\ 0 & p^n \end{smallmatrix}\right)$, and let $C_{m,n} = \mathrm{GL}_2(\mathbb{Z}_p)\lambda_{m,n}\,\mathrm{GL}_2(\mathbb{Z}_p)$. The Cartan decomposition for GL_2 asserts that $\mathrm{GL}_2(\mathbb{Q}_p)$ is the disjoint union

$$\mathrm{GL}_2(\mathbb{Q}_p) = \bigcup_{m \geq n} C_{m,n},$$

so that

$$\mathrm{Mat}_2(\mathbb{Z}_p) \cap \mathrm{GL}_2(\mathbb{Q}_p) = \bigcup_{0 \leq n \leq m} C_{m,n}.$$

We now express $\nu_p(a, q)$ as an orbital integral. Recall that $q = p^e$. Since we consider an ordinary isogeny class, the element $\gamma_0 \in \mathrm{GL}_2(\mathbb{Q}_p)$ actually can be chosen to have the form $\gamma_0 = \left(\begin{smallmatrix} u_1 p^e & 0 \\ 0 & u_2 \end{smallmatrix}\right)$, where $u_1, u_2 \in \mathbb{Z}_p$ are units and thus, in particular, $\gamma_0 \in C_{e,0}$.

Lemma 3.7. *Let ϕ_q be the characteristic function of $C_{e,0} = \mathrm{GL}_2(\mathbb{Z}_p)\left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right)\mathrm{GL}_2(\mathbb{Z}_p)$. Then*

$$\nu_p(a, q) = \frac{p^3}{\#\,\mathrm{SL}_2(\mathbb{F}_p)} O_{\gamma_0}^{\mathrm{geom}}(\phi_q).$$

Proof. The proof is similar to the case $\ell \neq p$, with one key modification. There, we use the reduction $\bmod \ell^n$ map π_n defined on $G(\mathbb{Z}_\ell)$. Here, we need to extend the map π_n to a set that contains γ_0.

Let $\pi_n^{\mathrm{M}} : \mathrm{Mat}_2(\mathbb{Z}_p) \to \mathrm{Mat}_2(\mathbb{Z}_p/p^n)$ be the projection map, and let $\mathfrak{c} : \mathrm{GL}_2(\mathbb{Q}_p) \to A(\mathbb{Q}_p)$ be the characteristic polynomial map. As in Section 3B, we define the sets

$$\begin{aligned} U_n &:= \{a = (a_0, a_1) \in A(\mathbb{Z}_p) \mid a_i \equiv a_i(\gamma_0) \bmod p^n, i = 0, 1\}, \\ S_n &:= \{\gamma \in \mathrm{Mat}_2(\mathbb{Z}_p/p^n) : \gamma \sim \pi_n^{\mathrm{M}}(\gamma_0)\}, \\ V_n &:= (\pi_n^{\mathrm{M}})^{-1}(S_n) \subset \mathrm{Mat}_2(\mathbb{Z}_p) \cap \mathrm{GL}_2(\mathbb{Q}_p). \end{aligned}$$

As before, informally, we think of U_n as a neighborhood of the point given by the coefficients of the characteristic polynomial of γ_0 in the Steinberg–Hitchin base, and we think of V_n as the intersection of the corresponding neighborhood of the orbit of γ_0 in $\mathrm{GL}_2(\mathbb{Q}_p)$ with $\mathrm{Mat}_2(\mathbb{Z}_p)$. In the case $\ell \neq p$ we had $\mathrm{GL}_2(\mathbb{Z}_\ell)$ in the place of $\mathrm{Mat}_2(\mathbb{Z}_p)$ in this description, and so it was clear that the evaluation of the volume of V_n would lead to the orbital integral of ϕ_0, the characteristic function of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Here, we need to make the connection between the set V_n and our function ϕ_q.

We claim that if $n > e$, then $V_n \subset C_{e,0}$. Indeed, suppose $\gamma \in V_n$. Then, since the characteristic polynomial of γ is congruent to that of γ_0, the trace of γ is a p-adic unit. Then γ cannot lie in any double coset $C_{m,n}$ with both m, n positive, because if it did, its trace would have been divisible by $p^{\min(m,n)}$. Then γ has to lie in a double coset of the form $C_{e+m,-m}$ for some $m \geq 0$, but if $m > 0$, then such a double coset has empty intersection with $\mathrm{Mat}_2(\mathbb{Z}_p)$, so $m = 0$ and the claim is proved.

As in the proof of Proposition 3.4 (iii), the volume of the set V_n equals $p^{-4n}\#S_n$. The rest of the proof repeats the proofs of Proposition 3.4 and Corollary 3.6. We again set $V(\gamma_0) = \bigcap_{n\geq 1} V_n \subset C_{e,0}$. Since π_n^{M} is surjective, $V(\gamma_0) = O(\gamma_0) \cap C_{e,0}$. By (3-3),

$$O_{\gamma_0}^{\mathrm{geom}}(\phi_q) = \lim_{n\to\infty} \frac{\mathrm{vol}_{\mu^{\mathrm{SO}}_{\mathrm{GL}_2}} V_n(\gamma_0)}{\mathrm{vol}_{\mu_A^{\mathrm{SO}}}(U_n)} = \lim_{n\to\infty} \frac{\#S_n(\gamma_0)p^{-4n}}{p^{-2n}},$$

and the statement follows by (3-5), which does not require any modification. $\square$

Recall that, in terms of the data (a, q), we have also computed a representative δ_0 for a σ-conjugacy class in $\mathrm{GL}_2(\mathbb{Q}_q)$. It is characterized by the fact that, possibly after adjusting γ_0 in its conjugacy class, we have $\mathrm{N}_{\mathbb{Q}_q/\mathbb{Q}_p}(\delta_0) = \gamma_0$. (Here we exploit the fact that, in a general linear group, conjugacy and stable conjugacy coincide.)

The twisted centralizer $G_{\delta_0\sigma}$ of δ_0 is an inner form of the centralizer G_{γ_0} [Kottwitz 1982, Lemma 5.8]; since γ_0 is regular semisimple, G_{γ_0} is a torus, and thus $G_{\delta_0\sigma}$ is isomorphic to G_{γ_0}. Using this, any choice of Haar measure on $G_{\delta_0\sigma}(\mathbb{Q}_p)$ induces one on $G_{\gamma_0}(\mathbb{Q}_p)$.

If ϕ is a function on $G(\mathbb{Q}_q)$, denote its twisted (canonical) orbital integral along the orbit of δ_0 by

$$TO_{\delta_0}^{\mathrm{can}}(\phi) = \int_{G_{\delta_0\sigma}(\mathbb{Q}_p)\backslash G(\mathbb{Q}_q)} \phi(h^{-1}\delta_0 h^\sigma)\, d\mu^{\mathrm{can}}.$$

Lemma 3.8. *Let $\phi_{p,q}$ be the characteristic function of* $\mathrm{GL}_2(\mathbb{Z}_q)\lambda_{0,1}\,\mathrm{GL}_2(\mathbb{Z}_q)$. *Then*

$$TO_{\delta_0}^{\mathrm{can}}(\phi_{p,q}) = O_{\gamma_0}^{\mathrm{can}}(\phi_q).$$

Proof. The asserted matching of twisted orbital integrals on $\mathrm{GL}_2(\mathbb{Q}_q)$ with orbital integrals on $\mathrm{GL}_2(\mathbb{Q}_p)$ is one of the earliest known instances of the fundamental lemma ([Langlands 1980]; see also [Laumon 1996, Section 4; Getz and Goresky 2012, (E.4.9)] or even [Achter and Cunningham 2002, Section 2.1]]). Indeed, the base change homomorphism of the Hecke algebras matches the characteristic function of $\mathrm{GL}_2(\mathbb{Z}_q)\lambda_{1,0}\,\mathrm{GL}_2(\mathbb{Z}_q)$ with $\phi_q+\phi$, where ϕ is a linear combination of the characteristic functions of $C_{a,b}$ with $a+b=e$ and $a, b>0$. As shown in the proof of the previous lemma, the orbit of γ_0 does not intersect the double cosets $C_{a,b}$ with $a, b>0$, and thus the only nonzero term on the right-hand side is $O^{\mathrm{can}}_{\gamma_0}(\phi_q)$. □

4. Canonical measure versus geometric measure

Finally, we need to relate the orbital integral with respect to the geometric measure as above to the canonical orbital integrals. A very similar calculation is discussed in [Frenkel et al. 2010] (and as the authors point out, surprisingly, it seemed impossible to find in earlier literature). Since our normalization of local measures seems to differ by an interesting constant from that of [Frenkel et al. 2010] at ramified finite primes, we carry out this calculation in our special case.

4A. ***Canonical measure and L-functions.*** Here we briefly review the facts that go back to the work of Weil, Langlands, Ono, Gross, and many others, that show the relationship between convergence factors that can be used for Tamagawa measures and various Artin L-functions. Our goal is to introduce the Artin L-factors that naturally appear in the computation of the canonical measures. To any reductive group G over $\mathbb{Q}_\ell$, Gross [1997] attaches a motive $M=M_G$; following his notation, we consider $M^\vee(1)$ — the Tate twist of the dual of M. For any motive M we let $L_\ell(s, M)$ be the associated local Artin L-function. We will write $L_\ell(M)$ for the value of $L_\ell(s, M)$ at $s=0$. The value $L_\ell(M^\vee(1))$ is always a positive rational number, related to the canonical measure reviewed in Section 3A2. In particular, if G is quasisplit over $\mathbb{Q}_\ell$, then

$$\mu^{\mathrm{can}}_G = L_\ell(M^\vee(1))|\omega_G|_\ell \tag{4-1}$$

[Gross 1997, Proposition 4.7 and (5.1)].

We shall also need a similar relation between volumes and Artin L-functions in the case when $G=T$ is an algebraic torus which is not necessarily anisotropic. Here we follow [Bitan 2011]. Suppose that T splits over a finite Galois extension L of $\mathbb{Q}_\ell$; let κ_L be the residue field of L, and let I be the inertia subgroup of the Galois group $\mathrm{Gal}(L/\mathbb{Q}_\ell)$. Let $X^*(T)$ be the group of rational characters of T. Let $\mathcal{T}$ be the Néron model of T over $\mathbb{Z}_\ell$, with the connected component of the identity denoted by $\mathcal{T}^\circ$. This is the canonical model for T referred to in Section 3A2.

Let Fr_L be the Frobenius element of $\mathrm{Gal}(\kappa_L/\mathbb{F}_\ell)$. The Galois group of the maximal unramified subextension of L, which is isomorphic to $\mathrm{Gal}(\kappa_L/\mathbb{F}_\ell)$, acts naturally on the I-invariants $X^*(T)^I$, giving rise to a representation which we will denote by ξ_T (and which is denoted by h in [Bitan 2011]),

$$\xi_T : \mathrm{Gal}(\kappa_L/\mathbb{F}_\ell) \to \mathrm{Aut}(X^*(T)^I) \simeq \mathrm{GL}_{d_I}(\mathbb{Z}),$$

where $d_I = \mathrm{rank}(X^*(T)^I)$. Then the associated local Artin L-factor is defined as

$$L_\ell(s, \xi_T) := \det\Big(1_{d_I} - \frac{\xi_T(\mathrm{Fr}_L)}{\ell^s}\Big)^{-1}.$$

Proposition 4.1 [Bitan 2011, Proposition 2.14].

$$L_\ell(1, \xi_T)^{-1} = \#\mathcal{T}^\circ(\mathbb{F}_\ell)\ell^{-\dim(T)} = \int_{\mathcal{T}^\circ(\mathbb{Z}_\ell)} |\omega_T|_\ell.$$

We observe that by definition [Gross 1997, § 4.3], since $G = T$ is an algebraic torus, the canonical parahoric $\underline{T}^\circ$ is $\mathcal{T}^\circ$; the canonical volume form ω_T is the same as the volume form denoted by $\omega_{\mathfrak{p}}$ in [Bitan 2011].

We also note that the motive of the torus T is the Artin motive $M = X^*(T) \otimes \mathbb{Q}$. If T is anisotropic over $\mathbb{Q}_\ell$, by the formula (6.6) (see also (6.11)) in [Gross 1997], we have

$$L_\ell(M^\vee(1)) = L_\ell(1, \xi_T).$$

As in the first paragraph of Section 3A3, let G be a reductive group over $\mathbb{Q}_\ell$ with simply connected derived group G^{der} and connected center Z, and assume that $G/G^{\mathrm{der}} \cong \mathbb{G}_m$.

Lemma 4.2. *Let $T \subset G$ be a maximal torus and let $T^{\mathrm{der}} = T \cap G^{\mathrm{der}}$. Then*

$$\frac{L_\ell(M_G^\vee(1))}{L_\ell(1, \xi_T)} = \frac{L_\ell(M_{G^{\mathrm{der}}}^\vee(1))}{L_\ell(1, \xi_{T^{\mathrm{der}}})}. \tag{4-2}$$

Proof. The motive M_H of a reductive group H, and thus $L_\ell(M_H^\vee(1))$, depends on H only up to isogeny [Gross 1997, Lemma 2.1]. Since G is isogenous to $Z \times G^{\mathrm{der}}$,

$$L_\ell(M_G^\vee(1)) = L_\ell(M_Z^\vee(1)) L_\ell(M_{G^{\mathrm{der}}}^\vee(1)).$$

Because $G^{\mathrm{der}} \cap Z$ is finite [Frenkel et al. 2010, (3.1)], so is $T^{\mathrm{der}} \cap Z$. Therefore, the natural map $T^{\mathrm{der}} \to T/Z$ is an isogeny onto its image. For dimension reasons it is an actual isogeny, and induces an isomorphism $X^*(T^{\mathrm{der}}) \otimes \mathbb{Q} \cong X^*(T/Z) \otimes \mathbb{Q}$ of $\mathrm{Gal}(\mathbb{Q}_\ell)$-modules. Therefore, $L(s, \xi_{T^{\mathrm{der}}}) = L(s, \xi_{T/Z})$, and thus

$$L(s, \xi_T) = L(s, \xi_{T/Z}) L(s, \xi_Z) = L(s, \xi_{T^{\mathrm{der}}}) L(s, \xi_Z).$$

Identity (4-2) is now immediate. □

4B. ***Weyl discriminants and measures.*** Our next immediate goal is to find an explicit constant $d(\gamma)$ such that $\mu_\gamma^{\mathrm{can}} = d(\gamma)\mu_\gamma^{\mathrm{geom}}$. We note that a similar calculation is carried out in [Frenkel et al. 2010]. However, the notation there is slightly different, and the key proof in [Frenkel et al. 2010] only appears for the field of complex numbers; hence, we decided to include this calculation here.

Let G be a split reductive group over $\mathbb{Q}_\ell$. Choose a split maximal torus and associated root system R and set of positive roots R^+.

Definition 4.3. Let $\gamma \in G(\mathbb{Q}_\ell)$, let T be the centralizer of γ, and let $\mathfrak{t}$ be the Lie algebra of T. Then the discriminant of γ is

$$D(\gamma) = \prod_{\alpha \in R} (1 - \alpha(\gamma)) = \det(I - \mathrm{Ad}(\gamma^{-1})|_{\mathfrak{g}/\mathfrak{t}}).$$

4B1. *Weyl integration formula, revisited.* As pointed out in [Frenkel et al. 2010, the paragraph above equation (3.28)], since both $\mu_\gamma^{\mathrm{can}}$ and $\mu_\gamma^{\mathrm{geom}}$ are invariant under the center, it suffices to consider the case $G = G^{\mathrm{der}}$. So for the moment, let us assume that the group G is semisimple and simply connected. Let $\phi \in C_c^\infty(\mathbb{Q}_\ell)$.

On one hand, the Weyl integration formula (we write a group-theoretic version of the formulation for the Lie algebra in [Kottwitz 2005, §7.7]) asserts that

(4-3)
$$\int_{G(\mathbb{Q}_\ell)} \phi(g)|d\omega_G| = \sum_T \frac{1}{|W_T|} \int_{T(\mathbb{Q}_\ell)} |D(\gamma)| \int_{T(\mathbb{Q}_\ell)\backslash G(\mathbb{Q}_\ell)} \phi(g^{-1}\gamma g)|d\omega_{T\backslash G}||d\omega_T|,$$

by our definition of the measure $|d\omega_{T\backslash G}|$. (Here, the sum ranges over a set of representatives for $G(\mathbb{Q}_\ell)$-conjugacy classes of maximal $\mathbb{Q}_\ell$-rational tori in G, and W_T is the finite group $W_T = N_G(T)(\mathbb{Q}_\ell)/T(\mathbb{Q}_\ell)$.)

On the other hand we have, by definition of the geometric measure,

$$\int_{G(\mathbb{Q}_\ell)} \phi(g)|d\omega_G| = \int_{A(\mathbb{Q}_\ell)} \int_{\mathfrak{c}^{-1}(a)} \phi(g)|d\omega_\gamma^{\mathrm{geom}}(g)||d\omega_A|.$$

To compare the two measures, we need to match the integration over $A(\mathbb{Q}_\ell)$ with the sum of integrals over tori.

Up to a set of measure zero, $A(\mathbb{Q}_\ell)$ is a disjoint union of images of $T(\mathbb{Q}_\ell)$, as T ranges over the same set as in (4-3); and for each such T, the restriction of $\mathfrak{c}$ to T is $|W_T|$-to-one.

It remains to compute the Jacobian of this map for a given T. Over the algebraic closure of $\mathbb{Q}_\ell$ this calculation is done, for example, in [Kottwitz 2005, § 14]; over $\mathbb{Q}_\ell$, this only applies to the split torus T^{spl}. The answer over the algebraic closure is $c_T \prod_{\alpha>0}(\alpha(x) - 1)$, where $c_T \in \bar{F}^\times$ is a constant (which depends on the torus T). We compute $|c_T|_\ell$ in the special case where T comes from a restriction of scalars in GL_2.

Lemma 4.4. *Let T be a torus in $\mathrm{GL}_2(\mathbb{Q}_\ell)$, and let c_T be the constant defined above. Then $|c_T|_\ell = 1$ if T is split or splits over an unramified extension, and $|c_T| = \ell^{-1/2}$ if T splits over a ramified quadratic extension. In particular, if $\gamma_0 \in \mathrm{GL}_2(\mathbb{Q})$ and $T = \mathrm{R}_{K/\mathbb{Q}}\mathbb{G}_m$ is the centralizer of γ_0 as in Section 2A, then $|c_T| = |\Delta_K|_\ell^{-1/2}$.*

Proof. We prove the lemma by direct calculation for GL_2. First, let us compute $|c_T|$ for the split torus. Here we can just compute the Jacobian of the map $T^{\mathrm{der}} \to T^{\mathrm{der}}/W$ by hand. Since we are working with invariant differential forms, we can just do the Jacobian calculation on the Lie algebra; it suffices to compute the Jacobian of the map from $\mathfrak{t}$ to $\mathfrak{t}/W$. Choose coordinates on the split torus in $\mathrm{SL}_2 = \mathrm{GL}_2^{\mathrm{der}}$ so that elements of $\mathfrak{t}$ are diagonal matrices with entries $(t, -t)$, then the canonical measure on $\mathfrak{t}$ is nothing but dt. Now, the coordinate on $\mathfrak{t}/W$ is $y = -t^2$ and the form $\omega_{\mathbb{A}^1}$ is dx. The Jacobian of the change of variables from $\mathfrak{t}/W$ to $\mathbb{A}^1$ is $-2t$. Thus, for the split torus $c = -1$. Note that $2t$ is the product of positive roots (on the Lie algebra). Thus, $|c_T| = 1$.

Now, consider a general maximal torus T in GL_2. Let T^{spl} be a split maximal torus; we have shown that $|c_{T^{\mathrm{spl}}}| = 1$. The torus T is conjugate to T^{spl} over a quadratic field extension L. Let us briefly denote this conjugation map by ψ. Then the map $\mathfrak{c}|T$ can be thought of as the conjugation $\psi : T \to T^{\mathrm{spl}}$ (defined over L) followed by the map $\mathfrak{c}|T^{\mathrm{spl}}$. Then

$$c_T = c_{T^{\mathrm{spl}}} \frac{\omega_T}{\psi^*(\omega_{T^{\mathrm{spl}}})},$$

where $\psi^*(\omega_{T^{\mathrm{spl}}})$ is the pullback of the canonical volume form on T^{spl} under ψ and the ratio $\omega_T/(\psi^*(\omega_{T^{\mathrm{spl}}}))$ is a constant in L. We thus have

$$c_T = \left| \frac{\omega_T}{\psi^*(\omega_{T^{\mathrm{spl}}})} \right|_L, \tag{4-4}$$

where $|\cdot|_L$ is the unique extension of the absolute value on $\mathbb{Q}_\ell$ to L.

At this point this is just a question about two tori, no longer requiring Steinberg section, and so we pass back to working with the group GL_2 rather than SL_2. Now T is obtained by restriction of scalars from $\mathbb{G}_m$, and so we can compute $\psi^*(\omega_{T^{\mathrm{spl}}})$ by hand. By definition, $T = \mathrm{R}_{L/\mathbb{Q}_\ell} \mathrm{G}_m$ and $T^{\mathrm{spl}} = \mathbb{G}_m \times \mathbb{G}_m$. The form $\omega_{T^{\mathrm{spl}}}$ is

$$\omega_{T^{\mathrm{spl}}} = \frac{du}{u} \wedge \frac{dv}{v},$$

where we denote the coordinates on $\mathbb{G}_m \times \mathbb{G}_m$ by (u, v). Let $L = \mathbb{Q}_\ell(\sqrt{\epsilon})$, where ϵ is nonsquare in $\mathbb{Q}_\ell$ (assume for the moment that $\ell \neq 2$). Then every element of T is conjugate in $\mathrm{GL}_2(\mathbb{Q}_\ell)$ to $\left(\begin{smallmatrix} x & \epsilon y \\ y & x \end{smallmatrix}\right)$, and using (x, y) as the coordinates on T, the map ψ can be written as $\psi(x, y) = (x + \sqrt{\epsilon} y, x - \sqrt{\epsilon} y)$. Then one can simply compute

$$\psi^*\Big(\frac{du}{u} \wedge \frac{dv}{v}\Big) = 2\sqrt{\epsilon} \frac{dx \wedge dy}{x^2 - \epsilon y^2} = 2\sqrt{\epsilon}\, \omega_T.$$

Thus we get (for $\ell \neq 2$),

$$|c_T|_\ell = |2\sqrt{\epsilon}|_L = \begin{cases} 1 & \text{if } L \text{ is unramified,} \\ \sqrt{\ell} & \text{if } L \text{ is ramified,} \end{cases}$$

which completes the proof of the lemma in the case $\ell \neq 2$.

There is, however, a better argument, which also covers the case $\ell = 2$. Namely, to find the ratio $|\omega_T/\psi^*(\omega_{T^{\mathrm{spl}}})|_L$ of (4-4), we just need to find the ratio of the volume of $\mathcal{T}^\circ(\mathbb{Z}_\ell)$ with respect to the measure $|d\omega_T|$ to its volume with respect to $|d\psi^*(\omega_{T^{\mathrm{spl}}})|$. This is, in fact, the same calculation as the one carried out in [Weil 1982, p. 22 (before Theorem 2.3.2)], and the answer is that the convergence factors for the pull-back of the form $\omega_{T^{\mathrm{spl}}}$ to the restriction of scalars is $(\sqrt{|\Delta_K|_\ell})^{\dim(\mathbb{G}_m)}$, in this case. $\square$

Finally, summarizing the above discussion, we obtain

Proposition 4.5. *Let $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ be a regular element. Let T be the centralizer of γ, and let K be as in Section 2A. Abusing notation, we also denote by γ the image of γ in $\mathrm{GL}_2(\mathbb{Q}_\ell)$ for every finite prime ℓ. Then for every finite prime ℓ,*

$$\mu_\gamma^{\mathrm{geom}} = \frac{L_\ell(1, \xi_T)}{L_\ell(M_G^\vee(1))} |\Delta_K|_\ell^{-1/2} |D(\gamma)|_\ell^{1/2} \mu_\gamma^{\mathrm{can}}$$

as measures on the orbit of γ.

5. The global calculation

In this section, we put all the above local comparisons together, and thus show that Gekeler's formula reduces to a special case of the formula of Langlands and Kottwitz. In the process we will need a formula for the global volume term that arises in that formula. We are now in a position to give a new proof of Gekeler's theorem, and of its generalization to arbitrary finite fields.

Theorem 5.1. *Let q be a prime power, and let a be an integer with $|a| \leq 2\sqrt{q}$ and $\gcd(a, p) = 1$. The number of elliptic curves over $\mathbb{F}_q$ with trace of Frobenius a is*

$$\widetilde{\#}I(a, q) = \frac{\sqrt{q}}{2} \nu_\infty(a, q) \prod_\ell \nu_\ell(a, q). \tag{5-1}$$

Here, $\nu_\ell(a, q)$ (for $\ell \neq p$), $\nu_p(a, q)$, and $\nu_\infty(a, q)$ are defined, respectively, in (2-4), (2-6), and (2-7), and the weighted count $\widetilde{\#}I(a, q)$ is defined in (2-1).

Proof. Recall the notation surrounding γ_0 and δ_0 established in Section 2A. Given Proposition 2.1, it suffices to show that the right-hand side of (5-1) calculates the right-hand side of (2-8).

Let $G = \mathrm{GL}_2$. First, let

$$\phi^p = \otimes_{\ell \neq p} \mathbb{1}_{G(\mathbb{Z}_\ell)}$$

be the characteristic function of $G(\hat{\mathbb{Z}}_f^p)$ in $G(\mathbb{A}_f^p)$. The first integral appearing in (2-8) is equal to

$$O_{\gamma_0}(\phi^p) = \int_{G(\mathbb{A}^p)} \phi^p |d\omega_G| = \prod_{\ell \neq p} O^{\mathrm{can}}(\mathbb{1}_{G(\mathbb{Z}_\ell)}).$$

Combining Corollary 3.6, relation (4-2), and Proposition 4.5 we get, for $\ell \neq p$,

$$\begin{aligned} \nu_\ell(a,q) &= \frac{\ell^3}{\#G^{\mathrm{der}}(\mathbb{F}_\ell)} O_{\gamma_0}^{\mathrm{geom}}(\mathbb{1}_{G(\mathbb{Z}_\ell)}) \\ &= \frac{\ell^3}{\#G^{\mathrm{der}}(\mathbb{F}_\ell)} \frac{L_\ell(1,\xi_{T^{\mathrm{der}}})}{L_\ell(M^\vee_{G^{\mathrm{der}}}(1))} |\Delta_K|_\ell^{-1/2} |D(\gamma_0)|_\ell^{1/2} O_{\gamma_0}^{\mathrm{can}}(\mathbb{1}_{G(\mathbb{Z}_\ell)}) \\ &= L_\ell(1,\xi_{T^{\mathrm{der}}}) |D(\gamma_0)|_\ell^{1/2} |\Delta_K|_\ell^{-1/2} O_{\gamma_0}^{\mathrm{can}}(\mathbb{1}_{G(\mathbb{Z}_\ell)}). \end{aligned}$$

Second, let ϕ_q be the characteristic function of $G(\mathbb{Z}_p)\left(\begin{smallmatrix}1&0\\0&q\end{smallmatrix}\right)G(\mathbb{Z}_p)$ in $G(\mathbb{Q}_p)$, and let $\phi_{p,q}$ be the characteristic function of $G(\mathbb{Z}_q)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)G(\mathbb{Z}_q)$ in $G(\mathbb{Q}_q)$. Using Lemmas 3.7 and 3.8, we find that

$$\begin{aligned} \nu_p(a,q) &= \frac{p^3}{\#G^{\mathrm{der}}(\mathbb{F}_p)} O_{\gamma_0}^{\mathrm{geom}}(\phi_q) \\ &= \frac{p^3}{\#G^{\mathrm{der}}(\mathbb{F}_p)} \frac{L_p(1,\xi_{T^{\mathrm{der}}})}{L_p(M^\vee_{G^{\mathrm{der}}}(1))} |\Delta_K|_p^{-1/2} |D(\gamma_0)|_p^{1/2} O_{\gamma_0}^{\mathrm{can}}(\phi_q) \\ &= \frac{p^3}{\#G^{\mathrm{der}}(\mathbb{F}_p)} \frac{L_p(1,\xi_{T^{\mathrm{der}}})}{L_p(M^\vee_{G^{\mathrm{der}}}(1))} |\Delta_K|_p^{-1/2} |D(\gamma_0)|_p^{1/2} T O_{\delta_0}^{\mathrm{can}}(\phi_{p,q}). \end{aligned}$$

Taking a product over all finite primes, we obtain

$$\prod_{\ell<\infty} \nu_\ell(a,q) = L(1,\xi_{T^{\mathrm{der}}}) \sqrt{\frac{|\Delta_K|}{|D(\gamma_0)|}} T O_{\delta_0\sigma}^{\mathrm{can}}(\phi_{p,q}) O_{\gamma_0}^{\mathrm{can}}(\phi^p). \tag{5-2}$$

Recall that $f_0(T)$, the characteristic polynomial of γ_0, is $f_0(T) = T^2 - aT + q$. The (polynomial) discriminant of $f_0(T)$ and the (Weyl) discriminant of γ_0 are related by $|D(\gamma_0)\det(\gamma_0)| = |\mathrm{disc}(f_0)| = 4q - a^2$. Consequently,

$$\sqrt{q}\,\nu_\infty(a,q) = \frac{1}{\pi}\sqrt{|D(\gamma_0)|}.$$

Since $L(1,\xi_{T^{\mathrm{der}}}) = L(1,\xi_{T/Z})$ (Lemma 4.2), to deduce (5-1) from (5-2) it suffices to show that

$$\frac{\sqrt{|\Delta_K|}}{2\pi} L(1,\xi_{T/Z}) = \mathrm{vol}(T(\mathbb{Q})\backslash T(\mathbb{A}_f)). \tag{5-3}$$

On one hand $L(s,\xi_{T/Z})$ coincides with $L(s,K/\mathbb{Q})$, the Dirichlet L-function attached to the quadratic character of K. Therefore, the analytic class number formula implies that the left-hand side of (5-3) is h_K/w_K, the ratio of the class number of K to the number of roots of unity in K. On the other hand, the right-hand side of (5-3) is also well-known to be h_K/w_K (e.g., [Weil 1973, Proposition VII.6.12]); we defer to Lemma A.4 in the Appendix for details. □

Appendix: Orbital integers and measure conversions

by S. Ali Altuğ

In this appendix, we explain how to deduce the comparison factor of Proposition 4.5 from [Frenkel et al. 2010] and certain computations in [Langlands 2013] as well as calculate the volume factor that goes into the proof of Theorem 5.1. We also remark that the same measure comparison also appears in [Altuğ 2015] (although implicitly) in the passage from equation (2) to (3).

Comparison of measures. Let $G = \mathrm{GL}_2$. Let ω_G be the same volume form as in Section 3A2. For a torus $T \subset G$, let ω_T be as in Proposition 4.1. Recall that $\mathcal{T}^\circ$ is the connected component of the identity in the Néron model of T.

Lemma A.1. *Let ℓ be a finite prime, let $\gamma \in G(\mathbb{Q}_\ell)$ be regular semisimple, and let $T = G_\gamma$ be its centralizer. Let μ_G and μ_T be nonzero Haar measures on $G(\mathbb{Q}_\ell)$ and $T(\mathbb{Q}_\ell)$, respectively. Then*

$$\mu^{\mathrm{geom}}_{\gamma,\ell} = \sqrt{|D(\gamma)|_\ell}\,\frac{\mathrm{vol}(|\omega_G|_\ell)\,\mathrm{vol}(\mu_{T,\ell})}{\mathrm{vol}(|\omega_T|_\ell)\,\mathrm{vol}(\mu_{G,\ell})}\,\bar{\mu}_{T\backslash G,\ell},$$

where $|D(\gamma)| = |\mathrm{tr}(\gamma)^2 - 4\det(\gamma)|$ and $\bar{\mu}_\ell = \mu^{\mathrm{can}}_{\mathrm{GL}_2,\ell}/\mu_{T\ell}$.

Proof. By equation (3.30) of [Frenkel et al. 2010], we have

$$\mu^{\mathrm{geom}}_{\gamma,\ell} = \sqrt{|D(\gamma)|_\ell}\,|\omega_{T\backslash G}|_\ell,$$

where we note that the left hand side of (3.30) of loc. cit. is what we denoted by $\mu^{\mathrm{geom}}_\gamma$. Since the Haar measure is unique up to a constant we have $|\omega_G|_\ell = c_\ell(G)d\mu_{G,\ell}$ and $|\omega_T|_\ell = c_\ell(T)d\mu_{T,\ell}$. The constants can be calculated easily by comparing the volumes of the integral points

$$c_\ell(G) = \frac{\mathrm{vol}_{|\omega_G|}(G(\mathbb{Z}_\ell))}{\mathrm{vol}_{\mu_{G,\ell}}(G(\mathbb{Z}_\ell))} \quad \text{and} \quad c_\ell(T) = \frac{\mathrm{vol}_{|\omega_T|}(\mathcal{T}^\circ(\mathbb{Z}_\ell))}{\mathrm{vol}_{\mu_{T,\ell}}(\mathcal{T}^\circ(\mathbb{Z}_\ell))}.$$

Therefore, the quotient measures $\bar{\mu}_{T\backslash G,\ell}$ and $|\omega_{T\backslash G}|_\ell$ are related by

$$|\omega_{T\backslash G}|_\ell = \frac{c_\ell(G)}{c_\ell(T)}\bar{\mu}_{T\backslash G,\ell}.$$

The lemma follows. □

As an immediate corollary to Lemma A.1 we get:

Corollary A.2. *Let $\mu^{\mathrm{can}}_{G,\ell}$ and $\mu^{\mathrm{can}}_{T,\ell}$ be normalized to give measure* 1 *to $G(\mathbb{Z}_\ell)$ and $\mathcal{T}^\circ(\mathbb{Z}_\ell)$ respectively, and let the rest of the notation be as in Lemma A.1. Then*

$$\mu^{\mathrm{geom}}_{\gamma,\ell} = \sqrt{|D(\gamma)|_\ell}\,\frac{\mathrm{vol}_{|\omega_G|_\ell}(G(\mathbb{Z}_\ell))}{\mathrm{vol}_{|\omega_T|_\ell}(\mathcal{T}^\circ(\mathbb{Z}_\ell))}\,\bar{\mu}_{T\backslash G,\ell}.$$

We now quote a result of [Langlands 2013]. Let $\zeta_\ell(s) = 1/(1-\ell^{-s})$.

Lemma A.3. *We have*

$$\mathrm{vol}(|\omega_G|_\ell) = \zeta_\ell(1)^{-1}\zeta_\ell^{-1}(2),$$
$$\mathrm{vol}(|\omega_T|_\ell) = \sqrt{|\Delta_K|_\ell}\begin{cases}\zeta_\ell(1)^{-2} & \text{if } K/\mathbb{Q} \text{ is split at } \ell,\\ \zeta_\ell(2)^{-1} & \text{if } K/\mathbb{Q} \text{ is unramified at } \ell,\\ \zeta_\ell(1)^{-1} & \text{if } K/\mathbb{Q} \text{ is ramified at } \ell,\end{cases}$$

where $K/\mathbb{Q}$ is the quadratic extension which splits T and Δ_K is the discriminant of K.

Proof. The result for odd primes ℓ is given on pages 41 and 42 of [Langlands 2013]. The case for $\ell = 2$ follows the same lines. The only point to keep in mind is the extra factor of 2 that appears in the calculation of the differential form on page 42 of [Langlands 2013]; we leave the details to the reader. □

Corollary A.2 and Lemma A.3 then give the conversion factor between the two measures.

***Calculation of* $\mathbf{vol}(K^\times\backslash\mathbb{A}_K^{\times,\mathrm{fin}})$.** Let (a, p) be such that $a^2 - 4p < 0$. Let $d\mu^{\mathrm{can}}_{T,\ell}$ be the Haar measure normalized to give measure 1 to $T(\mathbb{Z}_\ell)$ and set

$$d\mu^{\mathrm{can}}_{T,\mathrm{fin}} := \otimes_{l\neq\infty} d\mu^{\mathrm{can}}_{T,\ell}.$$

Lemma A.4. *We have*

$$\mu^{\mathrm{can}}_{T,\mathrm{fin}}(T(\mathbb{Q})\backslash T(\mathbb{A}^{\mathrm{fin}})) = \frac{h_K}{\omega_K},$$

where $K/\mathbb{Q}$ is the quadratic extension which splits T, ω_K is the number of roots of unity in K, and h_K is its class number.

Proof. By identifying $T = G_\gamma$ with $\mathbb{G}_m$ over the quadratic extension K we have

$$\mathrm{M}^{\mathrm{can}}_{T,\mathrm{fin}}(T(\mathbb{Q})\backslash T(\mathbb{A}^{\mathrm{fin}})) = \mu^{\mathrm{can}}_{K,\mathrm{fin}}(K^\times\backslash\mathbb{A}_K^{\times,\mathrm{fin}}),$$

where the measure on the right is such that $\mu^{\mathrm{can}}_{K,\mathrm{fin}}(O_v^\times) = 1$ for each place v. Let $\hat{\mathcal{O}}_K^\times = \prod_v \mathcal{O}_v^\times$. Recall that

$$1 \to (K^\times \cap \hat{\mathcal{O}}_K^\times)\backslash\hat{\mathcal{O}}_K^\times \to K^\times\backslash\mathbb{A}_K^{\times,\mathrm{fin}} \to \mathrm{Cl}(K) \to 1,$$

which implies that $\mu(K^\times\backslash\mathbb{A}_K^{\times,\mathrm{fin}}) = h_K\mu(K^\times \cap \hat{\mathcal{O}}_K^\times)\backslash\hat{\mathcal{O}}_K^\times) = h_K/\omega_K$. □

Acknowledgments

We have benefited from discussions with Bill Casselman, Clifton Cunningham, David Roe, William Sawin, and Sug-Woo Shin, as well as from suggestions from the referee. We are particularly grateful to Luis Garcia for sharing his insights. It is a great pleasure to thank these people.

References

[Achter and Cunningham 2002] J. D. Achter and C. L. R. Cunningham, "Isogeny classes of Hilbert–Blumenthal abelian varieties over finite fields", *J. Number Theory* **92**:2 (2002), 272–303. MR Zbl

[Altuğ 2015] S. A. Altuğ, "Beyond endoscopy via the trace formula, 1: Poisson summation and isolation of special representations", *Compos. Math.* **151**:10 (2015), 1791–1820. MR Zbl

[Batyrev 1999] V. V. Batyrev, "Birational Calabi–Yau n-folds have equal Betti numbers", pp. 1–11 in *New trends in algebraic geometry* (Warwick, 1996), edited by K. Hulek et al., London Math. Soc. Lecture Note Ser. **264**, Cambridge Univ. Press, 1999. MR Zbl

[Bitan 2011] R. A. Bitan, "The discriminant of an algebraic torus", *J. Number Theory* **131**:9 (2011), 1657–1671. MR Zbl

[Clozel 1993] L. Clozel, "Nombre de points des variétés de Shimura sur un corps fini (d'après R. Kottwitz)", exposé no. 766, 121–149 in *Séminaire Bourbaki,* 1992/93, Astérisque **216**, Société Mathématique de France, Paris, 1993. MR Zbl

[David et al. 2016] C. David, D. Koukoulopoulos, and E. Smith, "Sums of Euler products and statistics of elliptic curves", *Mathematische Annalen* (October 2016), 1–68.

[Denef 2000] J. Denef, "Arithmetic and geometric applications of quantifier elimination for valued fields", pp. 173–198 in *Model theory, algebra, and geometry*, edited by D. Haskell et al., Math. Sci. Res. Inst. Publ. **39**, Cambridge Univ. Press, 2000. MR Zbl

[Frenkel et al. 2010] E. Frenkel, R. Langlands, and B. C. Ngô, "Formule des traces et fonctorialité: Le début d'un programme", *Ann. Sci. Math. Québec* **34**:2 (2010), 199–243. MR Zbl

[Gekeler 2003] E.-U. Gekeler, "Frobenius distributions of elliptic curves over finite prime fields", *Int. Math. Res. Not.* **2003**:37 (2003), 1999–2018. MR Zbl

[Getz and Goresky 2012] J. Getz and M. Goresky, *Hilbert modular forms with coefficients in intersection homology and quadratic base change*, Progress in Mathematics **298**, Springer, 2012. MR Zbl

[Gross 1997] B. H. Gross, "On the motive of a reductive group", *Invent. Math.* **130**:2 (1997), 287–313. MR Zbl

[Hales 2012] T. C. Hales, "The fundamental lemma and the Hitchin fibration [after Ngô Bao Châu]", exposé no. 1035, 233–263 in *Séminaire Bourbaki,* 2010/2011, Astérisque **348**, Société Mathématique de France, Paris, 2012. MR Zbl

[Katz 2009] N. M. Katz, "Lang–Trotter revisited", *Bull. Amer. Math. Soc.* (*N.S.*) **46**:3 (2009), 413–457. MR Zbl

[Kottwitz 1982] R. E. Kottwitz, "Rational conjugacy classes in reductive groups", *Duke Math. J.* **49**:4 (1982), 785–806. MR Zbl

[Kottwitz 1992] R. E. Kottwitz, "Points on some Shimura varieties over finite fields", *J. Amer. Math. Soc.* **5**:2 (1992), 373–444. MR Zbl

[Kottwitz 2005] R. E. Kottwitz, “Harmonic analysis on reductive p-adic groups and Lie algebras”, pp. 393–522 in *Harmonic analysis, the trace formula, and Shimura varieties*, edited by J. Arthur et al., Clay Math. Proc. **4**, Amer. Math. Soc., Providence, RI, 2005. MR Zbl

[Langlands 1980] R. P. Langlands, *Base change for* GL(2), Annals of Mathematics Studies **96**, Princeton University Press, 1980. MR Zbl

[Langlands 2013] R. P. Langlands, “Singularités et transfert”, *Ann. Math. Qué.* **37**:2 (2013), 173–253. MR Zbl

[Laumon 1996] G. Laumon, *Cohomology of Drinfeld modular varieties, Part I: Geometry, counting of points and local harmonic analysis*, Cambridge Studies in Advanced Mathematics **41**, Cambridge University Press, 1996. MR Zbl

[Scholze 2011] P. Scholze, “The Langlands–Kottwitz approach for the modular curve”, *Int. Math. Res. Not.* **2011**:15 (2011), 3368–3425. MR Zbl

[Serre 1981] J.-P. Serre, “Quelques applications du théorème de densité de Chebotarev”, *Inst. Hautes Études Sci. Publ. Math.* 54 (1981), 323–401. MR Zbl

[Veys 1992] W. Veys, “Reduction modulo p^n of p-adic subanalytic sets”, *Math. Proc. Cambridge Philos. Soc.* **112**:3 (1992), 483–486. MR Zbl

[Veys 2006] W. Veys, “Arc spaces, motivic integration and stringy invariants”, pp. 529–572 in *Singularity theory and its applications*, edited by S. Izumiya et al., Adv. Stud. Pure Math. **43**, Math. Soc. Japan, Tokyo, 2006. MR Zbl

[Weil 1973] A. Weil, *Basic number theory*, 2nd ed., Grundlehren der Math. Wissenschaften **144**, Springer, Berlin, 1973. MR Zbl

[Weil 1982] A. Weil, *Adeles and algebraic groups*, Progress in Mathematics **23**, Birkhäuser, Boston, 1982. MR Zbl

Received July 15, 2016.

JEFFREY D. ACHTER
DEPARTMENT OF MATHEMATICS
COLORADO STATE UNIVERSITY
WEBER BUILDING
FORT COLLINS, CO 80523-1874
UNITED STATES

achter@math.colostate.edu

JULIA GORDON
UNIVERSITY OF BRITISH COLUMBIA
VANCOUVER, BC V6T 1Z2
CANADA

gor@math.ubc.ca

S. ALI ALTUĞ
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE, MA 02139-4307
UNITED STATES

altug@mit.edu

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2017 is US $450/year for the electronic version, and $625/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 286 No. 1 January 2017

Elliptic curves, random matrices and orbital integrals 1
JEFFREY D. ACHTER and JULIA GORDON

On the absolute continuity of p-harmonic measure and surface measure in Reifenberg flat domains 25
MURAT AKMAN

On the geometry of gradient Einstein-type manifolds 39
GIOVANNI CATINO, PAOLO MASTROLIA, DARIO D. MONTICELLI and MARCO RIGOLI

On the Fourier–Jacobi model for some endoscopic Arthur packet of $U(3) \times U(3)$: the nongeneric case 69
JAEHO HAAN

A Kirchberg-type tensor theorem for operator systems 91
KYUNG HOON HAN

Remarks on quantum unipotent subgroups and the dual canonical basis 125
YOSHIYUKI KIMURA

Scalar invariants of surfaces in the conformal 3-sphere via Minkowski spacetime 153
JIE QING, CHANGPING WANG and JINGYANG ZHONG

Action of intertwining operators on pseudospherical K-types 191
SHIANG TANG

Local symmetric square L-factors of representations of general linear groups 215
SHUNSUKE YAMANA

0030-8730(201701)286:1;1-Z