On the number of irreducible mod ℓ rank 2 sheaves on curves over finite fields

GEBHARD BÖCKLE AND CHANDRASHEKHAR B. KHARE

Let X be a smooth, geometrically connected, projective curve of genus g over a finite field $\mathbb{F}_q$ of characteristic p. Consider primes ℓ different from p. We formulate some questions related to a well known counting formula of Drinfeld in [7]. Drinfeld counts rank 2, irreducible ℓ-adic sheaves on $X_n = X \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$ as n varies. We would like to count rank 2, irreducible mod ℓ sheaves on X_n as n varies. Drinfeld's ℓ-adic count gives an upper bound for the mod ℓ count. We conjecture that Drinfeld's count is the correct asymptotic for the count of rank 2, irreducible mod ℓ sheaves on X_n as n varies, and $(n, \ell) = 1$. The conjecture is an invitation to finding good lower bounds on the number of irreducible rank 2, mod ℓ sheaves on X_n.

We produce a lower bound on the mod ℓ count, which is weaker than the one conjectured, by counting "dihedral" mod ℓ sheaves. We make a deformation theoretic study of the number of ℓ-adic sheaves which lift the pull backs $\mathcal{F}_n$ to X_n, of a given mod ℓ sheaf $\mathcal{F}_{n_0}$ on X_{n_0}, as we ranger over n with $n_0 | n$.

1. Introduction

1.1. ℓ-adic representations of $\pi_1(X)$

Let X be a smooth, geometrically connected, projective curve of genus g over a finite field $\mathbb{F}_q$ of characteristic p. Consider primes ℓ different from p. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and we fix an embedding $\iota_\ell : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_\ell}$. In Theorem 1 of [7], a formula is given for the cardinality $T(X, 2, q^n, \ell)$ of the set of irreducible two dimensional ℓ-adic representations $\rho : \pi_1(\overline{X}) \to \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$ which are fixed by Frob_q^n, where $\overline{X} = X \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ is the base change of X to an algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$ and π_1 denotes the fundamental group.

Denote by $U(X)$ the set of (isomorphism classes of) irreducible representations $\pi_1(\overline{X}) \to \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$. It carries an action of the geometric Frobenius

Frob$_q$, and we let $T(X, 2, q^n, \ell)$ be the cardinality of $U(X)^{\mathrm{Frob}_q^n}$, the subset of fixed points of $U(X)$ under Frob$_q^n$. It is easy to see [5, 1.2] that the set $U(X)^{\mathrm{Frob}_q^n}$ is in natural bijection with equivalence classes under twisting by continuous characters $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^n}) \to \overline{\mathbb{Q}}_\ell^*$ of isomorphism classes of 2-dimensional ℓ-adic representations of $\pi_1(X_n)$, with $X_n = X \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$ the base change of X to $\mathbb{F}_{q^n}$, which remain irreducible on restriction to $\pi_1(\overline{X})$.

Recall that a q-Weil number α of weight $j \geq 0$ is an algebraic integer α such that for any embedding $\iota \colon \overline{\mathbb{Q}} \to \mathbb{C}$ one has $|\iota(\alpha)| = q^{j/2}$. As a corollary of [7, Theorem 1], Drinfeld deduces:

Theorem 1.1. *If $g > 1$, then there exists an integer k, and integers $m_1, \ldots, m_k$, and Weil numbers $\mu_1, \ldots, \mu_k$ of weights j in the range $0 \leq j/2 < 4g - 3$ such that*

$$T(X, 2, q^n, \ell) = q^{(4g-3)n} + \sum_{i=1}^{k} m_i \mu_i^n.$$

This is a Lefschetz like formula and suggests that one is actually counting $\mathbb{F}_{q^n}$-valued points of a geometrically irreducible variety M_X of dimension $4g - 3$ that is defined over $\mathbb{F}_q$. The number $4g - 3$ is suggestive as it is the dimension of the moduli space of irreducible two-dimensional unitary representations of the fundamental group of a compact Riemann surface of genus $g > 1$. Deligne in [5, 1.5 and Conj. 2.15] suggests instead that there may be a variety M_X in characteristic 0 and a suitable endomorphism V on its cohomology such that the Lefschetz fixed point point formula applied to the action of V^n on ℓ-adic cohomology gives the formula of Theorem 1.1.

Drinfeld's method of proof of Theorem 1.1 is to count everywhere unramified cuspidal automorphic representations of $\mathrm{GL}_2(\mathbb{A}_{X_n})$, where $\mathbb{A}_{X_n}$ is the adeles of the function field of X_n, via the trace formula. A theorem of Drinfeld shows that an irreducible representation $\pi_1(X_n) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ arises from an everywhere unramified cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_{X_n})$ with respect to the fixed embedding ι_ℓ. The leading term of Drinfeld's formula comes from the trivial (central) term, i.e. the orbital integral of the identity, of the geometric side of the trace formula.

1.2. Mod ℓ representations of $\pi_1(X)$

We would like to consider a similar counting problem for mod ℓ sheaves. Let $\overline{U(X)}$ be the set of (isomorphism classes of) irreducible representations $\pi_1(\overline{X}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, and consider the cardinality $\overline{T(X, 2, q^n, \ell)}$ of the subset of fixed points $\overline{U(X)}^{\mathrm{Frob}_q^n}$ of $\overline{U(X)}$. We again see that $\overline{T(X, 2, q^n, \ell)}$ is

the number of equivalence classes under twisting by continuous characters $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \overline{\mathbb{F}_\ell}^*$ of (isomorphism classes) of 2-dimensional representations of $\pi_1(X_n) \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ which remain irreducible on restriction to $\pi_1(\overline{X})$.

We also denote by $T'(X, 2, q^n, \ell)$ and by $\overline{T'(X, 2, q^n, \ell)}$ the cardinality of equivalence classes under twisting by continuous characters $\pi_1(X_n) \to \overline{\mathbb{Q}_\ell}^*$ and $\pi_1(X_n) \to \overline{\mathbb{F}_\ell}^*$, respectively, of isomorphism classes of 2-dimensional ℓ-adic and mod ℓ representations of $\pi_1(X_n)$ that remain irreducible on restriction to $\pi_1(\overline{X})$.

A. de Jong has shown in [4] that the deformation rings of mod ℓ representations of $\pi_1(X_n)$ that are absolutely irreducible when restricted to $\pi_1(\overline{X})$ are finite flat complete intersections over $\mathbb{Z}_\ell$. This implies a lifting result and one has:

Lemma 1.2 ([4, 3.6 Remark(c)]). *Every irreducible two dimensional mod ℓ representation $\bar{\rho} : \pi_1(\overline{X}) \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ which is fixed by Frob_q^n lifts to an (irreducible) representation $\bar{\rho} : \pi_1(\overline{X}) \to \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$ which is fixed by Frob_q^n.*

In particular, we have the inequality

$$\overline{T(X, 2, q^n, \ell)} \leq T(X, 2, q^n, \ell).$$

The following guess on the size of $\overline{T(X, 2, q^n, \ell)}$ is based on our expectation that asymptotically with n, the number of rank 2, mod ℓ sheaves on X_n, and the number of rank 2, ℓ-adic sheaves on X_n, is the same. In other words, we expect few congruences mod ℓ between representations in $U(X)^{\mathrm{Frob}_q^n}$ as we vary n. For any fixed ℓ, as $n \to \infty$ this would imply that everywhere unramified automorphic forms for $\mathrm{GL}_2(\mathbb{A}_{X_n})$ have Hecke field that is typically unramified the over prime ℓ. We refer to Subsection 4.2 for a classical analog.

Conjecture 1.3. *We have*

$$\lim_{n\to\infty} \frac{\overline{T(X, 2, q^n, \ell)}}{T(X, 2, q^n, \ell)} = 1,$$

where n runs through all positive integers prime to ℓ, and

$$\lim_{n\to\infty} \frac{\overline{T'(X, 2, q^n, \ell)}}{T'(X, 2, q^n, \ell)} = 1,$$

where n runs through all positive integers.

The difference in the two statements above is due to the fact that if n is allowed to be divisible by high powers of ℓ, there are mod ℓ congruences

between characters $\pi_1(X_n) \to \overline{\mathbb{Q}_\ell}^*$. We refer the reader to formulas (3.3) and (3.4) in Section 3 where quotients describing the asymptotics of counting mod ℓ versus ℓ-adic characters are made explicit in a comparable context (though with different constants).

The difficulty of the conjecture lies in the fact that we do not have a method to produce good lower bounds on $\overline{T(X, 2, q^n, \ell)}$. We explore two different paths towards Conjecture 1.3. As by de Jong's result we know that the reduction map $U(X)^{\mathrm{Frob}_q^m} \to \overline{U(X)}^{\mathrm{Frob}_q^m}$ is surjective, we could approach the conjecture by studying the orders of the fibers of this map. In §2 we make a modest beginning by studying the fiber of the maps $U(X)^{\mathrm{Frob}_q^m} \to \overline{U(X)}^{\mathrm{Frob}_q^m}$ at the restrictions of a fixed representation $\bar\rho : \pi_1(X_n) \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ to $\pi_1(X_m)$. Thus given a $\bar\rho : \pi_1(X_n) \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ which remains irreducible on restriction to $\pi_1(\overline{X})$ we make a qualitative (deformation theoretic) study in §2 of the cardinality $N_{\bar\rho,m}$ of the inverse image of $\bar\rho$ under the reduction map $U(X)^{\mathrm{Frob}_q^m} \to \overline{U(X)}^{\mathrm{Frob}_q^m}$, for varying $m \in \mathbb{N}$ such that $n|m$. We show that if we vary through m such that $\frac{m}{n}$ is prime to ℓ then $N_{\bar\rho,m}$ is bounded independently of m (cf. Theorem 2.3). We also analyze the case when $\frac{m}{n}$ is a power of ℓ where the answer is very different (see Theorem 2.7 for the precise statement). Our deformation theoretic methods do not yield any information about $N_{\bar\rho,m}$ as we vary over both m and $\bar\rho$, and thus do not directly address Conjecture 1.3.

The second approach we could take take towards the conjecture is to produce lower bounds on $\overline{U(X)}^{\mathrm{Frob}_q^m}$ by *explicitly* constructing elements of $\overline{U(X)}^{\mathrm{Frob}_q^m}$. This is the approach we take in §3. In Theorem 3.13 of §3 we count the number of dihedral representations in $\overline{U(X)}^{\mathrm{Frob}_q^m}$ for varying m which gives a weak lower bound towards the conjecture.

In §4 we compare counting rank 2, irreducible, mod ℓ sheaves over X_n, with counting 2-dimensional mod ℓ representations $\bar\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ that are irreducible, odd and unramified outside ℓ. This has been studied computationally in [2].

2. Asymptotic results on universal deformation rings

We use Mazur's article [15] as a general reference for the basics of deformation theory that we use in this section. Let G be a profinite group that satisfies Mazur's finiteness condition Φ_ℓ, i.e., for every open normal subgroup H of G, the maximal abelian quotient of exponent ℓ is a finite group. Let $\mathbb{F}$ be a finite field of characteristic ℓ. Let $\bar\rho\colon G \to \mathrm{GL}_m(\mathbb{F})$ be a continuous representation.

Let $H \subset G$ be a normal open subgroup. Denote by ad the adjoint representation of G, respectively H, associated to $\bar{\rho}$, respectively $\bar{\rho}|_H$. The cohomology groups $H^i(G, \mathrm{ad})$ and $H^i(H, \mathrm{ad})$ for $i \geq$ are finite dimensional $\mathbb{F}$ vector spaces by our finiteness condition Φ_ℓ. Assume that the canonical homomorphism $\mathbb{F} \to \mathrm{End}_{\bar{\rho}(H)}(\mathbb{F}^m)$ is an isomorphism. For $? \in \{G, H\}$ denote by $R_?$ the universal deformation ring for deformations of $\bar{\rho}|_?$ in the sense of Mazur, which exists under the assumption just made.

Lemma 2.1. *Suppose that*

1) *the restriction map $H^1(G, \mathrm{ad}) \to H^1(H, \mathrm{ad})$ is an isomorphisms,*

2) *the restriction map $H^2(G, \mathrm{ad}) \to H^2(H, \mathrm{ad})$ is injective,*

Then the canonical homomorphism $\pi \colon R_H \to R_G$ is an isomorphism.

Proof. Observe first that by the injectivity in assumption 1, the map on mod ℓ cotangent spaces induced from π is surjective. Because R_H and R_G are complete noetherian local rings with residue field $\mathbb{F}$, it follows that π is surjective. Denote by I the kernel of π. If I is non-zero, we choose an ideal $\mathfrak{n}$ of R_H contained in I such that $I/\mathfrak{n} \cong \mathbb{F}$ and consider the induced short exact sequence

$$(2.1) \qquad\qquad 0 \to I/\mathfrak{n} \to R_H/\mathfrak{n} \to R_G \to 0.$$

There is an obstruction class θ in $H^2(G, \mathrm{ad})$ to lifting the universal deformation $\rho_G \colon G \to \mathrm{GL}_n(R_G)$ from R_G to $R_H/\mathfrak{n}$. Upon restriction to H this class vanishes, and so from assumption 2 we deduce $\theta = 0$. It follows that the sequence (2.1) is split. But then the homomorphism on cotangent spaces induced from π is not an isomorphism, contradicting assumption 1. Thus I is zero and π is an isomorphism. $\qquad\square$

Remark 2.2. If ℓ does not divide m, there is an obvious variant of Lemma 2.1 for deformations with fixed determinant, whose formulation, we leave to the reader.

Theorem 2.3. *Let $\bar{\rho} \colon \pi_1(X) \to \mathrm{GL}_m(\mathbb{F})$ be a continuous representation that is absolutely irreducible when restricted to $\pi_1(\overline{X})$. For each $n \geq 1$ denote by $\rho_n \colon \pi_1(X_n) \longrightarrow \mathrm{GL}_m(R_n)$ the universal deformation in the sense of Mazur of the restriction $\bar{\rho}|_{\pi_1(X_n)}$. Then there exists an n_0 prime to ℓ such that for any multiple n of n_0 with n prime to ℓ, the canonical homomorphism $R_n \to R_{n_0}$ is an isomorphism.*

Proof. We wish to apply Lemma 2.1 with $G = \pi_1(X_{n_0})$ and $H = \pi_1(X_n)$ for $n_0 | n$. Because ℓ is different from p, the group $\pi_1(\overline{X})$ satisfies Mazur's condition Φ_ℓ, and hence so does $\pi_1(X_n)$ for every n; this also implies that the groups $H^j(\pi_1(\overline{X}), \mathrm{ad})$ below are finite-dimensional vector spaces over $\mathbb{F}$. Since $\bar{\rho}|_{\pi_1(X_n)}$ is absolutely irreducible, it remains to verify assumptions 1 and 2 of Lemma 2.1, for n_0 chosen suitably.

We begin with an application of the Hochschild-Serre spectral sequence to $0 \to \pi_1(\overline{X}) \to \pi_1(X_n) \to G_{\mathbb{F}_{q^n}} \to 1$. Since $G_{\mathbb{F}_{q^n}} \cong \hat{\mathbb{Z}}$ has cohomological dimension 1, we obtain for all $j \geq 0$ a short exact sequence

$$0 \to H^1(G_{\mathbb{F}_{q^n}}, H^j(\pi_1(\overline{X}), \mathrm{ad}))$$
$$\to H^{j+1}(\pi_1(X_n), \mathrm{ad}) \to H^0(G_{\mathbb{F}_{q^n}}, H^j(\pi_1(\overline{X}), \mathrm{ad})) \to 0.$$

To have shorter formulas, we abbreviate $\Phi = \mathrm{Frob}_q$. Recall that for a $G_{\mathbb{F}_{q^n}}$-module M the cohomology $H^i(G_{\mathbb{F}_{q^n}}, M)$ for $i = 0, 1$ is isomorphic to the $G_{\mathbb{F}_{q^n}}$ invariants and covariants of M respectively. They are given as the Φ^n fixed points M^{Φ^n} of M and the quotient $M/(1 - \Phi^n) := M/(1 - \Phi^n)M$, respectively. Restriction from $G_{\mathbb{F}_{q^{n_0}}}$ to $G_{\mathbb{F}_{q^n}}$ on cohomology is then described by the following explicit diagram

$$0 \longrightarrow H^j(\pi_1(\overline{X}), \mathrm{ad})/(1 - \Phi^{n_0}) \longrightarrow H^{j+1}(\pi_1(X_{n_0}), \mathrm{ad}) \longrightarrow H^j(\pi_1(\overline{X}), \mathrm{ad})^{\Phi^{n_0}} \longrightarrow 0$$
$$\downarrow{\tau} \qquad\qquad\qquad \downarrow{\mathrm{res}} \qquad\qquad\qquad \downarrow{\iota}$$
$$0 \longrightarrow H^j(\pi_1(\overline{X}), \mathrm{ad})/(1 - \Phi^n) \longrightarrow H^{j+1}(\pi_1(X_n), \mathrm{ad}) \longrightarrow H^j(\pi_1(\overline{X}), \mathrm{ad})^{\Phi^n} \longrightarrow 0,$$

where ι is the inclusion homomorphism and τ is induced from the action of $1 + \Phi^{n_0} + \cdots + \Phi^{n_0(n/n_0 - 1)}$ on $H^j(\pi_1(\overline{X}), \mathrm{ad})$. The action of Φ on $H^j(\pi_1(\overline{X}), \mathrm{ad})$ is a linear automorphism. Since ad is finite of characteristic ℓ we may choose $n' \geq 1$ such that $\Phi^{n'}$ is unipotent. Let n_0 denote the minimal such choice. Suppose now that n/n_0 is not divisible by ℓ. Then the number of summands of τ is of order prime to ℓ, and since they are unipotent and commute with each other, we deduce that τ is an isomorphism. Observing further that $1 - \Phi^n = (1 - \Phi^{n_0})\tau$, we see that the kernels of $1 - \Phi^n$ and $1 - \Phi^{n_0}$ agree, and so also ι is an isomorphism. The assertion of Theorem 2.3 now follows from Lemma 2.1. $\square$

Remark 2.4. The above theorem is an affirmative solution to a question of Hida raised over number fields. He asks whether in prime-to-ℓ (cyclotomic) towers the deformation rings of residual representations stabilize. This question is being investigated by Geunho Gim in his UCLA PhD thesis.
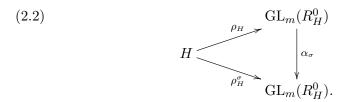
Corollary 2.5. *Suppose we are in the situation of Theorem 2.3. Denote by $L_{\bar{\rho},n}$ the set of lifts up to isomorphism of $\bar{\rho}$ to an ℓ-adic representation. Then $L_{\bar{\rho},n}$ is independent of n as long as $n_0|n$ and n/n_0 is not divisible by ℓ, i.e., restriction from $\pi_1(X_{n_0})$ to $\pi_1(X_n)$ defines a bijection $L_{\bar{\rho},n_0} \to L_{\bar{\rho},n}$ for any such n.*

Another way to rephrase the corollary is to say that the number of congruences to a fixed $\bar{\rho}$ is constant for all multiples n of n_0 as long as n/n_0 is of order prime to ℓ.

Theorem 2.3 concerns prime-to-ℓ towers. The following lemma prepares the analysis of the general situation.

Lemma 2.6. *Let $1 \to H \to G \xrightarrow{\pi} Z \to 1$ be a short exact sequence of profinite groups such that Z is procyclic, torsion free. There exists a continuous splitting $s\colon Z \to G$ of π. Suppose H satisfies Mazur's finiteness condition Φ_ℓ. Let $\bar{\rho}\colon G \to \mathrm{GL}_m(\mathbb{F})$ be a continuous representation of degree m prime to ℓ such that the natural map $\mathbb{F} \to \mathrm{End}_H(\mathbb{F}^m)$ is an isomorphism. For any closed subgroup H' of G containing H denote by $R^0_{H'}$ the universal ring for deformations of $\bar{\rho}|_{H'}$ whose determinant is the Teichmüller lift of $\det \bar{\rho}|_{H'}$. Then*

1) *The canonical homomorphism $\mathrm{can}_{H,G}\colon R^0_H \to R^0_G$ is surjective.*

2) *Let $\rho_H\colon H \to \mathrm{GL}_m(R^0_H)$ be the universal deformation represented by R^0_H. For $\sigma \in Z$ define $\rho^\sigma_H\colon H \to \mathrm{GL}_m(R^0_H), h \mapsto \rho_H(s(\sigma)hs(\sigma)^{-1})$. There is a unique homomorphism $\alpha_\sigma\colon R^0_H \to R^0_H$ such that*

(2.2)

$$
\begin{array}{ccc}
 & & \mathrm{GL}_m(R^0_H) \\
 & \overset{\rho_H}{\nearrow} & \\
H & & \downarrow \alpha_\sigma \\
 & \underset{\rho^\sigma_H}{\searrow} & \\
 & & \mathrm{GL}_m(R^0_H).
\end{array}
$$

commutes up to conjugation, and, if $I \subset R^0_H$ denotes the ideal generated by $\{r - \alpha_\sigma(r) \mid r \in R^0_H, \sigma \in Z\}$, then $R^0_H \to R^0_G$ factors via R^0_H/I and the induced map $R^0_H/I \to R^0_G$ is an isomorphism.

3) *The canonical map $R^0_H \to \varprojlim_U R^0_{\pi^{-1}(U)}$ is an isomorphism where $U \subseteq Z$ ranges over all open subgroups.*

4) *If for all open subgroups $U \subset Z$ the ring $R^0_{\pi^{-1}(U)}$ is flat over $\mathbb{Z}_\ell$ and reduced, then $\varinjlim_U \operatorname{Spec} R^0_{\pi^{-1}(U)}[1/\ell]$ is Zariski dense in $\operatorname{Spec} R^0_H$, the rings $R^0_H[1/\ell]$ and R^0_H are reduced, and R^0_H is flat over $\mathbb{Z}_\ell$.*

5) *The conjugation action of Z on $H/\operatorname{Ker}(\rho_H)$ via s factors via a virtual pro-ℓ quotient $\bar{Z}$ of Z.*

6) *If the conjugation action of Z on $H/\operatorname{Ker}(\rho_H)$ via s is trivial, then $R^0_H \to R^0_G$ is an isomorphism.*

Proof. Let us first observe that a continuous splitting $s\colon Z \to G$ exists. In the same way that one proves that the profinite completion $\hat{\mathbb{Z}}$ is isomorphic to $\prod_{\ell'} \mathbb{Z}_{\ell'}$ where ℓ' ranges over all prime numbers, one shows $Z \cong \prod_{\ell'} Z_{\ell'}$ for the procyclic group Z where $Z_{\ell'}$ is the pro-ℓ' completion of Z. Because Z is torsion free, each $Z_{\ell'}$ is either trivial or isomorphic to $\mathbb{Z}_{\ell'}$. Denote by g an element of G whose image in Z is a topological generator, and denote by Z' the profinite completion of $g^{\mathbb{Z}}$ in G. Then with similar notation as above we have $Z' \cong \prod_{\ell'} Z'_{\ell'}$, and moreover the surjective map $Z' \to Z$ is a surjection on each component. From the local shape of the Z_ℓ, we see that we can choose h inside $Z' \subset G$ such that the completion of $h^{\mathbb{Z}}$ maps isomorphically to Z. The inverse is a continuous section as wanted.

To prove part 1 it suffices to prove injectivity for the induced map on mod ℓ tangent spaces, i.e. for the restriction homomorphism $H^1(G, \operatorname{ad}^0) \to H^1(H, \operatorname{ad}^0)$, which is part of the inflation restriction sequence

$$(2.3) \qquad 0 \to H^1(G/H, H^0(H, \operatorname{ad}^0)) \to H^1(G, \operatorname{ad}^0)$$
$$\to H^1(H, \operatorname{ad}^0)^{G/H} \to H^2(G/H, H^0(H, \operatorname{ad}^0)).$$

Because ℓ is prime to m, the isomorphism $\mathbb{F} \to \operatorname{End}_H(\mathbb{F}^m)$ yields $H^0(H, \operatorname{ad}^0) = 0$, and part 1 follows.

We next prove part 2, which follows the proof of [4, 3.13 Lemma]. Let $\mathfrak{m}_H$ denote the maximal ideal of R^0_H. For each $\sigma \in Z$ choose $A_\sigma \in \operatorname{GL}_m(R^0_H)$ whose reduction modulo $\mathfrak{m}_H$ is equal to $\bar\rho(s(\sigma))$. Then $h \mapsto A_\sigma \rho^\sigma_H(h) A^{-1}_\sigma$, $H \to \operatorname{GL}_m(R^0_H)$, is a deformation of $\bar\rho|_H$ of determinant equal to the Teichmüller lift of $\det \bar\rho|_H$. Hence there exists a unique homomorphism $\alpha_\sigma \colon R^0_H \to R^0_H$ such that (2.2) commutes up to conjugacy with $A_\sigma \rho^\sigma_H(\_)A^{-1}_\sigma$ in place of ρ^σ_H. This proves the existence of α_σ. Its uniqueness is a consequence of the universality of R^0_H. Observe that α_σ is an isomorphism as can be checked on tangent spaces. Next we show that the canonical map $\operatorname{can}_{H,G}\colon R^0_H \to R^0_G$ factors via R^0_H/I: denote by $\rho_G\colon G \to \operatorname{GL}_m(R^0_G)$ the universal deformation for R^0_G. Then for all $\sigma \in Z$ one has $\rho^\sigma_G = B_\sigma \rho_G B^{-1}_\sigma$

with $B_\sigma = \rho_G(s(\sigma))$. One deduces that $\mathrm{can}_{H,G} \circ \alpha_\sigma = \mathrm{can}_{H,G}$, which shows that $\mathrm{can}_{G,H}$ factors via R_H^0/I. The map induced on tangent spaces from $R_H^0/I \to R_G^0$ is described by the central arrow in (2.3), which we know to be an isomorphism. To see that $R_H^0/I \to R_G^0$ is an isomorphism it thus suffices to construct a deformation $\hat\rho_H \colon G \to \mathrm{GL}_m(R_H^0/I)$ of $\bar\rho$ that extends ρ_H, since the latter yields a splitting of $R_H^0/I \to R_G^0$. For the details, we refer to the proof of [4, 3.13 Lemma]. Alternatively, one can obtain $\hat\rho_H$ by extending the results of [11, Subsec. 4.3.5] to a profinite setting: since $\bar\rho$ is given as a representation of G, the obstruction described in [11, Thm. 4.35(5)] will lie in $H^2(Z, 1 + \mathfrak{m}_H)$; the multiplicative group $1 + \mathfrak{m}_H$ is pro-ℓ and the mod ℓ cohomological dimension of the procyclic, torsion free group Z is at most 1.

For part 3, let I_U denote the ideal of R_H^0 defined in item 2 if one replaces G by $\pi^{-1}(U)$. By part 2, it remains to prove that $\bigcap_U I_U = 0$ where the intersection is over all open subgroups U of Z. For this it suffices to show that for all $t > 0$ there is a U such that $\mathfrak{m}_H^t \supset I_U$. To see the latter, we consider the quotient

$$\rho_H/\mathfrak{m}_H^t \colon H \to \mathrm{GL}_m(R_H/\mathfrak{m}_H^t).$$

This representation factors via a finite quotient, say H_t, of H. Because the action of Z on H_t via s and conjugation is continuous, there is an open subgroup U of Z such that U acts trivially on H_t. This implies that α_σ mod $\mathfrak{m}_t$ is the identity for all $z \in U$ and hence that I_U is contained in $\mathfrak{m}_H^t$.

To see part 4, let $J \subset R_H^0$ be the radical ideal such that the Zariski closure of $\varinjlim_U \mathrm{Spec}\, R_{\pi^{-1}(U)}^0[1/\ell]$ in $\mathrm{Spec}\, R_H^0$ agrees with $\mathrm{Spec}\, R_H^0/J$. Because each $R_{\pi^{-1}(U)}^0$ is reduced the kernel of the canonical map $R_H^0 \to R_{\pi^{-1}(U)}^0[1/\ell]$ contains J. But the map factors via $R_H^0 \to R_{\pi^{-1}(U)}^0 \to R_{\pi^{-1}(U)}^0[1/\ell]$, and by flatness of $R_{\pi^{-1}(U)}^0$ over $\mathbb{Z}_\ell$, the ideal J lies in the kernel of $R_H^0 \to R_{\pi^{-1}(U)}^0$. From the proof of part 3, we deduce that $J = 0$. This proves the density assertion as well as the reducedness of R_H^0 and $R_H^0[1/\ell]$. The vanishing of J also implies that $R_H^0 \to R_H^0[1/\ell]$ is injective, and this proves the flatness of R_H^0 over $\mathbb{Z}_\ell$.

To prove part 5, let P^ℓ be the kernel of the homomorphism from $\mathrm{Ker}(\bar\rho|_H)$ to its pro-ℓ completion. Then P^ℓ is a characteristic subgroup of H, that is closed. The quotient H/P^ℓ is thus a virtual pro-ℓ group that satisfies Mazur finiteness condition Φ_ℓ; moreover it surjects onto $\mathrm{Ker}(\rho_H)/H$. By [6, Ch. 5] the automorphism group $\mathrm{Aut}(H/P^\ell)$ is in a natural way a profinite group that is virtually pro-ℓ. Conjugation by elements of Z via s defines a closed subgroup of $\mathrm{Aut}(H/P^\ell)$, and from this part 5 is clear.

For the last assertion it suffices to show that under the hypothesis of part 6 one has $\alpha_\sigma = \mathrm{id}_{R_H^0}$ for all $\sigma \in Z$ for the maps in 3. This is clear, since the hypothesis implies that $\rho_H^\sigma = \rho_H$ for all $\sigma \in Z$. $\qquad\square$

For $n \geq 1$ define $\mathbb{F}_{q^{n\ell\infty}} = \varinjlim_t \mathbb{F}_{q^{n\ell^t}}$ and $X_{n\ell^\infty} = X \times_{\mathrm{Spec}\,\mathbb{F}_q} \mathrm{Spec}\,\mathbb{F}_{q^{n\ell\infty}}$.

Theorem 2.7. *Suppose that the representation $\bar\rho\colon \pi_1(X) \to \mathrm{GL}_m(\mathbb{F})$ is absolutely irreducible when restricted to $\pi_1(\overline{X})$. For an integer $n \geq 1$ and $t \in \{0, \infty\}$ denote by $\rho_{n\ell^t}\colon \pi_1(X_{n\ell^t}) \longrightarrow \mathrm{GL}_m(R_{n\ell^t}^0)$ the universal deformation in the sense of Mazur for deformations of the restriction $\bar\rho|_{\pi_1(X_{n\ell^t})}$ whose determinant is the Teichmüller lift of $\det \bar\rho|_{\pi_1(X_{n\ell^t})}$. Define similarly $\rho_\infty\colon \pi_1(\overline{X}) \longrightarrow \mathrm{GL}_m(R_\infty^0)$. Suppose that ℓ does not divide m and that $\ell > 2$ if $m > 2$. Let $n \geq 1$. Then the following hold:[1]*

1) *The ring R_n^0 is reduced and finite flat over $\mathbb{Z}_\ell$.*

2) *There is a canonical isomorphism $R_{n\ell^\infty}^0 \to \varprojlim_t R_{n\ell^t}^0$, and $\varinjlim_t \mathrm{Spec}\,R_{n\ell^t}^0$ is Zariski dense in $\mathrm{Spec}\,R_{n\ell^\infty}^0$.*

3) *There exists an n_0 such that for all multiples n of n_0 one has a canonical isomorphism $R_\infty^0 \to R_{n\ell^\infty}^0$.*

4) *If $g_{\overline{X}}$ denotes the genus of $\overline{X}$, then R_∞^0 is formally smooth over $W(\mathbb{F})$ of relative dimension*

$$(2.4) \qquad \dim H^1(\pi_1(\overline{X}), \mathrm{ad}^0) = (2g_{\overline{X}} - 2)(m^2 - 1) = (2g_{\overline{X}} - 2)\dim \mathrm{ad}^0.$$

Proof. Under the stated hypotheses on ℓ, the finite flatness in part 1 follows from [4, 1.3 Theorem] for $m \leq 2$ and [9] for $m > 2$. To see reducedness, observe that by finite flatness the ring $R_n^0[1/\ell]$ is a finite $\mathbb{Q}_\ell$-algebra. Let $\rho\colon \pi_1(X_n) \to \mathrm{GL}_m(\overline{\mathbb{Q}}_\ell)$ be any irreducible representation. Then by [12, Thm. 1], one has $H^2(\pi_1(X_n), \mathrm{ad}_\rho^0) = 0$ which in turn yields $H^1(\pi_1(X_n), \mathrm{ad}_\rho^0)$

---

[1]For $m > 2$, our proof makes use of [9]. It is stated in [9, 1.4], that [9] relies on two results whose proofs do not exist in the published literature: a derived theory of perverse étale sheaves with $\mathbb{F}_q((t))$-coefficients, and a sheaf-function correspondence compatible with inverse image, direct image and tensor product. We learned from [17] that the first result is known in the meanwhile by the theory of the pro-étale site of Bhatt and Scholze, cf. [1]. The second result about the geometric Satake isomorphism for the affine Grassmannian over finite fields and torsion coefficients is still unpublished. Over $\mathbb{C}$ the latter result is treated in [16] by Mirković and Vilonen.

$= 0$, and hence that ρ has no non-trivial deformations. This shows that $R_n^0[1/\ell]$ is a product of fields, and hence is reduced.

The proof of part 2 is a direct consequence of Lemma 2.6, part 4, where for the short exact sequence $1 \to H \to G \to Z \to 1$ one takes $1 \to \pi_1(\overline{X}) \to \pi_1(X) \to G_{\mathbb{F}_q} \to 1$. Next, by Lemma 2.6, part 5, there exists $n_0 > 1$ such that $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{n_0\ell^\infty})$ acts trivially on $\pi_1(\overline{X})/\mathrm{Ker}(\rho_\infty)$. If one applies Lemma 2.6, part 6, to the sequence $1 \to \pi_1(\overline{X}) \to \pi_1(X_{n\ell^\infty}) \to \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{n\ell^\infty}) \to 1$ for any n with $n_0 | n$, part 3 follows.

We finally prove part 4. The proof of the relative formal smoothness is given in [4, 3.11 Lemma]. To compute the relative dimension one first observes that $\dim H^1(\pi_1(\overline{X}), \mathrm{ad}^0)$ is equal to the Euler-Poincaré characteristic of ad^0 as a sheaf on $\pi_1(\overline{X})$, because the relevant H^0 and H^2 terms vanish; the former by absolute irreducibility, the latter by Poincaré duality. The Euler-Poincaré characteristic is then evaluated to the number given in (2.4) by the Theorem of Grothendieck-Ogg-Shafarevich, [18], using that ad^0 is lisse on $\overline{X}$. $\square$

To give a concrete interpretation of Theorem 2.7, fix a representation $\bar{\rho} \colon \pi_1(X) \to \mathrm{GL}_m(\mathbb{F}_q)$ whose restriction to $\pi_1(\overline{X})$ is absolutely irreducible. Because of part 1 of the theorem, for every n and t, the ring $R_{n\ell^t}^0[\frac{1}{\ell}]$ is a product of fields. By the Theorem of Lafforgue, [14, Théorème (p. 2), Théorème. VI.9], each factor corresponds to a cuspidal automorphic representation of $\mathrm{GL}_m(\mathbb{A}_{X_{n\ell^t}})$. By parts 2–4, the number of such factors tends to ∞ as $t \to \infty$. This means that the number of cuspidal automorphic representations for $\mathrm{GL}_m(\mathbb{A}_{X_{n\ell^t}})$ of fixed central character the Teichmüller lift of $\det \bar{\rho}$ that are congruent modulo ℓ to the given $\bar{\rho}$ also converges to ∞ for $t \to \infty$. However the theorem makes no quantitative assertions. For instance it sheds no light on the $\mathbb{Q}_\ell$-dimension of $R_{n\ell^t}^0[\frac{1}{\ell}]$.

3. Dihedral representations

In the following, we denote by E an algebraically closed field of characteristic different from 2 and from p. Unless indicated otherwise, E will carry the discrete topology. We call a continuous representation ρ of a profinite group G over E dihedral, if there exists an index 2 subgroup H of G and a character $\chi \colon H \to E^*$ such that $\rho = \mathrm{Ind}_H^G \chi$ where χ satisfies $\chi \neq \chi^c$; here c is any element in $G \setminus H$ and $\chi^c \colon H \to E^*$ is the character $h \mapsto \chi(chc^{-1})$ (which is independent of the chosen c). We note right away that ρ is induced from exactly two such characters, namely χ and χ^c. The condition $\chi \neq \chi^c$ implies that the image of G under ρ is non-abelian. Without further mentioning, we

assume in the following that all representations are continuous. Because E is discrete, all representations we consider have image of finite order. In the following we write $\operatorname{Hom}(\cdot, \cdot)$ for the group of homomorphisms between abelian groups and $\operatorname{Hom}_{\mathrm{cts}}(\cdot, \cdot)$ for the subgroup of continuous homomorphisms, if both groups carry a topology.

The aim of this section is to deduce asymptotic formulas for the number of dihedral representations of $\pi_1(X_n)$, that remain dihedral after restriction to $\pi_1(\overline{X})$, as n varies, up to certain twist that we shall specify below. Such representations are induced from characters $\chi : \pi_1(Y_n) \to E^*$ for geometrically irreducible double covers $Y \to X$, and we shall count the latter up to twisting. As recalled from [5, 1.2] in the introduction, this number is the same as the number of dihedral representations of $\overline{X}$ that are fixed by the n-th power of the q-Frobenius.

3.1. ℓ-power torsion of abelian varieties

Let A be an abelian variety over $\mathbb{F}_q$ of dimension g_A. We collect some simple facts on the behavior of the size of the ℓ-power torsion of $A(\mathbb{F}_{q^n})$ for $n \to \infty$. The results below are inspired by the behavior of $|q^n - 1|_\ell^{-1}$ for $n \to \infty$, where $q^n - 1$ is the cardinality of the set of $\mathbb{F}_{q^n}$-rational points of the multiplicative scheme $\mathbb{G}_m$. The results are probably well-known, but we could not locate a reference. For background on abelian varieties, we refer to the forthcoming book [8], and there in particular to Chapter 12.

By π_A we denote the Frobenius of A relative to $\mathbb{F}_q$. We regard π_A as an element of the $\mathbb{Q}$-endomorphism ring $D = \operatorname{End}_\mathbb{Q}(A)$. We write ch_A for the characteristic polynomial of π_A. It is the unique monic polynomial in $\mathbb{Z}[T]$ of degree $2g_A$ such that for all $n \in \mathbb{N}$ one has $\mathrm{ch}_A(n) = \deg([n]_A - \pi_A)$, where $[n]_A$ is the multiplication by n map on A and $\deg$ the degree of an endomorphism, with the convention that the degree is zero if the endomorphism is not finite. For any prime number $\ell \neq p$, the polynomial ch_A is also the characteristic polynomial of the endomorphism on the ℓ-adic Tate module of A induced by π_A. The roots of ch_A in $\overline{\mathbb{Q}}$ we denote by α_i, $i = 1, \ldots, 2g_A$. They are q-Weil numbers of weight one.

The group $A(\mathbb{F}_{q^n})$ is the kernel of the isogeny $\mathrm{id} - \pi_A^n : A \to A$. The degree of this isogeny is

$$\#A(\mathbb{F}_{q^n}) = \deg(\mathrm{id} - \pi_A^n) = \prod_{i=1}^{2g_A}(1 - \alpha_i^n).$$

Denote by K the splitting field of ch_A over $\mathbb{Q}$. We fix a prime ℓ different from p and a place λ of K above ℓ. By K_λ we denote the completion of K at λ, by k_λ the residue field of K_λ, by ϖ_λ a uniformizer of K_λ and by $|\ |_\lambda$ the valuation on K_λ that extends the valuation $|\ |_\ell$ on $\mathbb{Q}_\ell$ with $|\ell|_\ell = \frac{1}{\ell}$. The field K_λ is unramified over $\mathbb{Q}_\ell$ for almost all ℓ. If this holds for ℓ, one may take $\varpi_\lambda = \ell$. Choosing λ enables us to analyze the factors $(1 - \alpha_i^n)$ separately because $|\prod_i(1 - \alpha_i^n)|_\ell = \prod_i |1 - \alpha_i^n|_\lambda$.

We have $\alpha_i^{\#k_\lambda - 1} \equiv 1 \pmod{\varpi_\lambda}$ for all $i = 1, \ldots, 2g_A$. We denote by h_ℓ the smallest divisor of $\#k_\lambda - 1$ such that

$$\alpha_i^{h_\ell} \equiv 1 \pmod{\varpi_\lambda} \text{ for all } i = 1, \ldots, 2g_A.$$

It follows that $\alpha_i^{h_\ell \ell^j} \to 1$ for $j \to \infty$. Let $j_\ell \geq 0$ be the smallest integer such that

$$\left| \alpha_i^{h_\ell \ell^{j_\ell}} - 1 \right|_\lambda < \ell^{\frac{-1}{\ell-1}} < 1 \text{ for all } i = 1, \ldots, 2g_A.$$

Note that $j_\ell = 0$ whenever $K/\mathbb{Q}$ is unramified above ℓ and $\ell > 2$.

For each divisor d of h_ℓ and each $j \geq 0$ we define $N_{\ell,d,j}$ as $\#A[\ell^\infty](\mathbb{F}_{q^{d\ell^j}})$, and g_d as the number of $i \in \{1, \ldots, 2g_A\}$ such that $\alpha_i^d \equiv 1 \pmod{\varpi_\lambda}$. Then $g_{h_\ell} = 2\dim A \geq g_d$ for all d.

Proposition 3.1. *For $n \in \mathbb{N}$ define $j = -\log_\ell |n|_\ell$, i.e., as the largest integer j such that $\ell^j | n$. Then*

$$\#A[\ell^\infty](\mathbb{F}_{q^n}) = \left| \prod_{i=1}^{2g_A}(1 - \alpha_i^n) \right|_\lambda^{-1} = N_{\ell, \gcd(n, h_\ell), j}.$$

Moreover for $j \geq j_\ell$ one has $N_{\ell, \gcd(n, h_\ell), j+k} = \ell^{k g_{\gcd(n, h_\ell)}} N_{\ell, \gcd(n, h_\ell), j}$.

Proposition 3.1 means that $\#A[\ell^m](\mathbb{F}_{q^n})$ depends only on the subgroup of $\mathbb{Z}/(h_\ell)$ generated by n and the ℓ-divisibility of n, and the contribution of the ℓ-divisibility behaves regularly for $|n|_\ell^{-1}$ sufficiently large.

Proof of Proposition 3.1. The two points that require proof are:

1) For $j \geq 0$ and $n \geq 1$ prime to ℓ one has $|1 - \alpha_i^{n\ell^j}|_\lambda = |1 - \alpha_i^{\gcd(n, h_\ell)\ell^j}|_\lambda$.

2) For n a divisor of h_ℓ and $j \geq j_\ell$ one has

$$|1 - \alpha_i^{n\ell^j}|_\lambda = \begin{cases} \left(\frac{1}{\ell}\right)^{j - j_\ell} \cdot |1 - \alpha_i^{n\ell^{j_\ell}}|_\lambda, & \text{if } |1 - \alpha_i^n| < 1, \\ 1, & \text{if } |1 - \alpha_i^n| = 1. \end{cases}$$

If $\alpha_i^n \not\equiv 1 \pmod{\varpi_\ell}$, then the left and right hand sides above take the value 1, and so the equalities are clear. So let us assume from now on that $\alpha_i^n \equiv 1 \pmod{\varpi_\ell}$. Then the left and right and sides take values in the open interval $(0,1)$; the value 0 is impossible since α_i is a q-Weil number of weight 1, and in particular not a root of unity.

For the equality in part 1 observe that $n' := n/\gcd(n, h_\ell)$ is prime to ℓ. Since $\alpha_i^{\gcd(n,h_\ell)\ell^j} \equiv 1 \pmod{\varpi_\ell}$ raising the element $\alpha_i^{\gcd(n,h_\ell)}$ to the power n' does not change its distance to 1, and this proves part 1.

Regarding equality in part 2, observe first, that by the just discussed part 1, we can on both sides replace n by h_ℓ without changing the valuations. By the definition of j_ℓ we have $|\alpha_i^{h_\ell \ell^{j_\ell}} - 1|_\lambda < \left(\frac{1}{\ell}\right)^{\frac{1}{\ell-1}}$. By induction on $j - j_\ell \geq 0$ one easily deduces the equality in 2: for the induction one shows by the binomial theorem that $|(1 + \epsilon)^\ell - 1|_\lambda = |(1 + \ell\epsilon) - 1|_\lambda = |\ell|_\ell|\epsilon|_\lambda$ if $\epsilon \in K_\lambda$ satisfies $|\epsilon|_\lambda < \left(\frac{1}{\ell}\right)^{\frac{1}{\ell-1}}$, i.e., $|\epsilon^\ell|_\lambda < |\epsilon\ell|_\lambda$. $\qquad\square$

3.2. Counting dihedral representations up to twisting

In this subsection, we fix the following abstract setting: G is a profinite group and $H \subset G$ is an index 2 subgroup such that one has commutative diagram with exact rows

$$(3.1) \qquad \begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & H^{\mathrm{ab}} & \longrightarrow & \hat{\mathbb{Z}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & M & \longrightarrow & G^{\mathrm{ab}} & \xrightarrow{\kappa} & \hat{\mathbb{Z}} & \longrightarrow & 0, \end{array}$$

in which M and M' are finite abelian groups. We shall give elementary formulas and estimates for the number of non-abelian dihedral representations ρ over E of G induced from H in terms of M and M'. Recall that dihedral means that $\rho = \mathrm{Ind}_H^G \chi$, where $\chi \colon H \to E^*$ is a character such that $\chi \neq \chi^c$, and where c is a fixed element of $G \setminus H$. By κ we also denote the composite $G \to G^{\mathrm{ab}} \xrightarrow{\kappa} \hat{\mathbb{Z}}$.

Definition 3.2. *Let ρ and ρ' be representations of G (or of H) over E.*

We call ρ and ρ' strongly twist-equivalent over G (over H), and write $\rho \approx \rho'$, if there is a character $\chi_0 \colon G \to E^*$ (or $\chi_0 \colon H \to E^*$) that is trivial on $\operatorname{Ker} \kappa$ (or $\operatorname{Ker} \kappa|_H$) such that $\rho' \cong \rho \otimes \chi_0$.

We call ρ stably irreducible if the restriction ρ to the kernel of $\kappa : G \to \hat{\mathbb{Z}}$ is irreducible.

Lemma 3.3. *Let $\chi\colon H \to E^*$ be a character and set $\rho = \operatorname{Ind}_H^G \chi$.*

1) *The order of $\operatorname{Im}(\rho)$ is invertible in E and hence ρ is semisimple.*

2) *The representation ρ is stably irreducible if and only if $\chi|_{M'} \neq \chi^c|_{M'}$.*

3) *The restriction map $\chi \mapsto \chi|_{M'}$ defines a bijection*

$$\{characters\ \chi\colon H \to E^*\}/\approx\ \to\ \{characters\ \chi_1\colon M' \to E^*\}.$$

4) *Suppose ρ is stably irreducible. Then for any character $\chi'\colon H \to E^*$ one has the following equivalences*

$$\operatorname{Ind}_H^G \chi \approx \operatorname{Ind}_H^G \chi'\ over\ G \iff \chi' \approx \chi\ or\ \chi' \approx \chi^c\ over\ H$$
$$\iff \chi'|_{M'} = \chi|_{M'}\ or\ \chi'|_{M'} = \chi^c|_{M'}.$$

5) *The strong twist-equivalence classes of stably irreducible dihedral representations of G over E are in bijection with (unordered) pairs $\{\chi_1, \chi_1^c\}$ of characters $\chi_1\colon M' \to E^*$ such that $\chi_1 \neq \chi_1^c$.*

Proof. Because E is discrete, $\operatorname{Im}(\chi) \subset E^*$ is a finite subgroup. As such its order is prime to char E. Since also char $E \neq 2 = [G : H]$, the first half of part 1 holds. The second half follows from Maschke's theorem.

For part 2, let G_0 and H_0 be the kernels of $G \to \hat{\mathbb{Z}}$ and $H \to \hat{\mathbb{Z}}$ from (3.1), respectively. Then the restriction of $\operatorname{Ind}_H^G \chi$ to G_0 is isomorphic to $\operatorname{Ind}_{H_0}^{G_0}(\chi|_{H_0})$, and the latter is irreducible if and only if $\chi|_{H_0} \neq \chi|_{H_0}^c$. Because χ is abelian, the restriction $\chi|_{H_0}$ factors via the quotient M' of H_0, and part 2 follows.

The surjectivity in part 3 is clear, since the horizontal sequences in (3.1) are split. The injectivity is straightforward from the definitions.

The left expression in part 4 is equivalent to the existence of a character $\chi_0\colon \hat{\mathbb{Z}} \to E^*$ such that $\operatorname{Ind}_H^G \chi \approx \operatorname{Ind}_H^G \chi' \otimes (\chi_0 \circ \kappa)$. This is equivalent to $\chi' \otimes (\chi_0 \circ \kappa|_H)$ being equal to χ or χ^c, which is defined to mean $\chi' \approx \chi$ or $\chi' \approx \chi^c$. The second equivalence in part 4 follows from part 3. Finally part 5 is immediate from parts 3 and 4. □

One has a short exact sequence $1 \to H^{\mathrm{ab}} \to G/[H, H] \to \mathbb{Z}/2 \to 1$. The element c chosen above maps to the generator of $\mathbb{Z}/2$, and conjugation by c acts on H^{ab} as an endomorphism of order 2. For any subgroup $H' \subset H^{\mathrm{ab}}$, we denote by $[c, H']$ the subgroup of H^{ab} generated by the commutators $[c, h']$, $h' \in H'$. Note that $[c, H^{\mathrm{ab}}]$ maps to 0 under κ and hence $[c, H^{\mathrm{ab}}]$ is a subgroup of M'. We let M'^- be the subgroup of M' on which c acts by

multiplication with -1. For the next three results, we introduce the index

$$(3.2) \qquad\qquad e = [[c, H^{\mathrm{ab}}] : [c, M']].$$

Lemma 3.4. *Let* $\chi_1 \colon M' \to E^*$ *be a character.*

1) $\chi_1 = \chi_1^c$ *if and only if* $[c, M']$ *lies in the kernel of* χ_1.

2) χ_1 *extends to a character of* $G/[H, H]$*, i.e., of* M*, if and only if* $[c, H^{\mathrm{ab}}]$ *lies in the kernel of* χ_1.

3) *One has* $2M'^{-} \subset [c, M'^{-}] \subset [c, M'] \subset [c, H^{\mathrm{ab}}] \subset M'^{-}$.

4) *The index* e *from (3.2) is* 1 *or* 2.

5) *The map* $\mathrm{Hom}(M, E^*) \to \{\chi_1 \in \mathrm{Hom}(M', E^*) \mid \chi_1^c = \chi_1\}, \chi \mapsto \chi|_{M'}$ *has kernel of order* 2 *and image of index* e*, with* e *from part 4.*

Proof. For part 1 note that $\chi_1^c \cdot \chi_1^{-1} = \mathrm{id}$ if and only if for all $h \in M'$ we have $\chi_1(chc^{-1}h^{-1}) = 1$, and the latter is equivalent to $[c, M'] \subset \mathrm{Ker}\,\chi_1$. To see part 2, note that since c generates $G/H \cong \mathbb{Z}/(2)$, and since $H^{\mathrm{ab}} = H/[H, H]$ is abelian, the commutator subgroup of $G/[H, H]$ is $[c, H^{\mathrm{ab}}]$, and now part 2 is immediate.

For part 3, let $h \in H^{\mathrm{ab}}$ and note that $c^2 \in H^{\mathrm{ab}}$. The inclusion on the right now follows from $c[c, h]c^{-1} = cchc^{-1}h^{-1}c^{-1} = hch^{-1}c^{-1} = [h, c] = [c, h]^{-1}$; note that $[c, H^{\mathrm{ab}}] \subset M'$ had been observed right before the lemma. It remains to show the inclusion on the left. Let $m' \in M'^{-}$, so that $cm'c^{-1} = m'^{-1}$. Then $[c, m'^{-1}] = cm'^{-1}c^{-1}m' = (m')^2$, which completes part 3.

To see part 4, note that by part 3 the quotient $\bar{M} := [c, H^{\mathrm{ab}}]/[c, M']$ is a finite elementary abelian 2 group. Now if $h \in H^{\mathrm{ab}}$ maps to 1 in $\mathbb{Z}$ under κ, then it follows that $[c, h]$ is a generator of $\bar{M}$, and this gives part 4.

Regarding part 5, note first that the map is well-defined, since conjugation by c acts trivially on $G^{\mathrm{ab}} \supset M$. Next observe that the kernel of the map in part 5 consists of inflated homomorphisms from M modulo the image of M'. The latter quotient is isomorphic to $G/H \cong \mathbb{Z}/(2)$, and so the kernel in part 5 has order 2. The assertion on the cokernel is immediate from parts 1, 2 and 4. $\qquad\square$

Combining Lemmas 3.3 and 3.4 directly gives the following result.

Corollary 3.5. *The number of strong twist-equivalence classes of stably irreducible dihedral representations of* G *over* E *is*

$$\frac{1}{2}(\# \mathrm{Hom}(M', E^*) - \frac{e}{2} \# \mathrm{Hom}(M, E^*)).$$

Specializing Corollary 3.5 to $E = \overline{\mathbb{Q}}_\ell$ and to $E = \overline{\mathbb{F}}_\ell$, and using the duality between a finite abelian group and its group of characters, as well as $\ell \neq 2$, yields the following consequence.

Corollary 3.6. *The number of strong twist-equivalence classes of stably irreducible dihedral representations of G over $\overline{\mathbb{Q}}_\ell$ is $\frac{1}{2}(\#M' - \frac{e}{2}\#M)$.*
The number of strong twist-equivalence classes of stably irreducible dihedral representations of G over $\overline{\mathbb{F}}_\ell$ is $\frac{1}{2}(\#M'/M'_\ell - \frac{e}{2}\#M/M_\ell)$, where for a finite abelian group A by A_ℓ we denote its ℓ-primary part.

The last lemma in this section concerns the number of lifts to $\overline{\mathbb{Q}}_\ell$ of a given dihedral representation of G over $\overline{\mathbb{F}}_\ell$. Let $\overline{\mathbb{Z}}_\ell$ be the ring of integers of $\overline{\mathbb{Q}}_\ell$. We begin with the following well-known result:

Proposition 3.7. *Any representation $\rho\colon G \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ is conjugate to a representation ρ' whose image lies in $\mathrm{GL}_n(\overline{\mathbb{Z}}_\ell)$. The semisimplification of the reduction of ρ' to $\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ is independent of the chosen ρ'.*

By $\bar{\rho}$ we will denote the semisimplification of a reduction of a representation $\rho\colon G \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$.

Proof. By [13, Remark 9.0.7] the image of ρ lies in $\mathrm{GL}_n(F)$ for some finite extension F of $\mathbb{Q}_\ell$. If $\mathcal{O}_F$ is its ring of integers, then by [11, p. 37] a conjugate of ρ takes values in $\mathrm{GL}_n(\mathcal{O}_F)$. The independence of the reduction follows from [3, Thm. 30.16], a result due to Brauer and Nesbitt. $\qquad\square$

For the following lemma, we remark that any finite order character χ to $\overline{\mathbb{Q}}_\ell^*$ can be written uniquely as a product $\chi = \chi_\ell \chi^\ell$, where χ_ℓ has order a power of ℓ and χ^ℓ has order prime to ℓ.

Lemma 3.8.   1) *The map $\mathrm{Hom}(M', \overline{\mathbb{Q}}_\ell^*) \longrightarrow \mathrm{Hom}(M', \overline{\mathbb{F}}_\ell^*)$, $\chi \longmapsto \bar{\chi}$, is an epimorphism of abelian groups with kernel $\{\chi \in \mathrm{Hom}(M', \overline{\mathbb{Q}}_\ell^*) \mid \chi = \chi_\ell\}$. We have $\overline{\chi} = \overline{\chi^\ell}$.*

   2) *The reduction of $\mathrm{Ind}_H^G \chi$ is $\mathrm{Ind}_H^G \bar{\chi}$. The map*

$$\{\mathrm{Ind}_H^G \chi \mid \chi \in \mathrm{Hom}_{\mathrm{cts}}(H, \overline{\mathbb{Q}}_\ell^*)\}/\approx$$
$$\longrightarrow \{\mathrm{Ind}_H^G \bar{\chi} \mid \bar{\chi} \in \mathrm{Hom}_{\mathrm{cts}}(H, \overline{\mathbb{F}}_\ell^*)\}/\approx, \ \rho \mapsto \bar{\rho},$$

   between strong twist-equivalence classes is surjective. The fibers of stably irreducible representations $\mathrm{Ind}_H^G \bar{\chi}$ have cardinality $\#M_\ell$.

Proof. Part 1 is obvious. For the first claim of part 2, let χ be in $\mathrm{Hom}_{\mathrm{cts}}(H, \overline{\mathbb{Q}}_\ell^*)$. By compactness of H the image of χ lies in $\mathbb{Z}_\ell^*$. Now $\mathrm{Ind}_H^G \chi$ can be described explicitly by

$$h \mapsto \begin{pmatrix} \chi(h) & 0 \\ 0 & \chi^c(h) \end{pmatrix} \subset \mathrm{GL}_2(\mathbb{Z}_\ell) \qquad c \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

for $h \in H$. It is then clear that $\mathrm{Ind}_H^G \chi$ maps to $\mathrm{Ind}_H^G \bar{\chi}$ under reduction. The explicit description also makes it apparent that without passing to strong twist-equivalence classes, the map in part 2 is surjective. Moreover, for a homomorphism $\chi_0 \colon \hat{\mathbb{Z}} \to \mathbb{Z}_\ell^*$ the twist $(\mathrm{Ind}_H^G \chi) \otimes \chi_0$ is isomorphic to $\mathrm{Ind}_H^G (\chi \otimes \chi_0)$, and so reduction preserves strong-twist equivalence classes. This completes the proof of the second assertion of part 2.

Let finally $\bar{\chi} \in \mathrm{Hom}_{\mathrm{cts}}(H, \overline{\mathbb{F}}_\ell^*)$ be such that $\mathrm{Ind}_H^G \bar{\chi}$ is stably irreducible. Then any lift $\chi \in \mathrm{Hom}_{\mathrm{cts}}(H, \overline{\mathbb{Q}}_\ell^*)$ is also stably irreducible. Furthermore, any two lifts differ by multiplication by a continuous character $G \to \overline{\mathbb{Q}}_\ell^*$ of ℓ-power order. After passing to twist equivalence classes, the fiber of $\mathrm{Ind}_H^G \bar{\chi}$ will be in bijection with the characters from M to $\overline{\mathbb{Q}}_\ell^*$ of ℓ-power order, and hence (non-canonically) with the ℓ-primary part M_ℓ of M. This completes the proof. $\square$

Remark 3.9. Observe that the two numbers in Corollary 3.6 do not differ by a factor of $\#M_\ell$. This is so because the mod ℓ reduction of a dihedral representation may become a sum of characters.

3.3. Growth of ℓ-adic and mod ℓ-systems of dihedral representations

Suppose in the following that ℓ is a prime different from 2, and that the genus g of X is at least 2.

We begin by recalling the main theorem of unramified geometric class field theory for X first formulated by Lang and Weil.

Theorem 3.10 ([20, Ch. VI]). *There is a commutative diagram*

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Pic}^0(X)(\mathbb{F}_q) & \longrightarrow & \mathrm{Pic}(X)(\mathbb{F}_q) & \xrightarrow{\ \deg\ } & \mathbb{Z} & \longrightarrow & 0 \\
& & \Big\downarrow{\simeq} & & \Big\downarrow{[x]\mapsto\mathrm{Frob}_x} & & \Big\downarrow{n\mapsto\mathrm{Frob}_{\mathbb{F}_q}^n} & & \\
0 & \longrightarrow & \mathrm{Ker}(s^*) & \longrightarrow & \pi_1^{\mathrm{ab}}(X) & \xrightarrow{\ s^*\ } & G_{\mathbb{F}_q} & \longrightarrow & 0,
\end{array}
$$

where the left vertical map is an isomorphism, the central and right vertical maps are injective with dense image, the central homomorphism is characterized by sending any (Weil) divisor $[x]$, for $x \in |X|$, to the well-defined Frobenius automorphism $\mathrm{Frob}_x \in \pi_1^{\mathrm{ab}}(X)$, and the homomorphism s^* arises from the structure morphism $s\colon X \to \mathrm{Spec}\,\mathbb{F}_q$ by functoriality of étale fundamental groups.

We call a character of $\pi_1(X)$ a *character of the base* if it is the inflation of a character of $G_{\mathbb{F}_q}$ under s^*. Then the above theorem has the following immediate consequence.

Corollary 3.11. *The homomorphism $\mathrm{Pic}(X)(\mathbb{F}_q) \to \pi_1^{\mathrm{ab}}(X)$ of the previous theorem induces a bijection*

$$\left\{ \begin{array}{c} \textit{finite order characters} \\ \mathrm{Pic}^0(X)(\mathbb{F}_q) \to \mathbb{Q}_\ell^* \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{characters of } \pi_1(X)^{\mathrm{ab}} \to \mathbb{Q}_\ell^* \\ \textit{up to twists by characters of the base.} \end{array} \right\}$$

Let $f\colon X' \to X$ be an unramified degree 2 Galois cover of X by a smooth projective curve X' that is again geometrically connected over $\mathbb{F}_q$. Note that the genus of X' is $2g-1$. We write $\{1,c\}$ for $\mathrm{Aut}_X(X')$. The automorphism c induces an involution c^* on the Jacobian $\mathrm{Pic}^0(X')$ of X'. To relate the above to the axiomatic setting of 3.2, we display the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Pic}^0(X')(\mathbb{F}_{q^n}) & \longrightarrow & \pi_1(X'_n)^{\mathrm{ab}} & \longrightarrow & G_{\mathbb{F}_{q^n}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \mathrm{Pic}^0(X)(\mathbb{F}_{q^n}) & \longrightarrow & \pi_1(X_n)^{\mathrm{ab}} & \longrightarrow & G_{\mathbb{F}_{q^n}} & \longrightarrow & 0. \end{array}$$

Before we state results on counting dihedral representation of $\pi_1(X_n)$ over $\overline{\mathbb{Q}}_\ell$ and $\overline{\mathbb{F}}_\ell$ for $n \to \infty$, we collect some basic results on the number of unramified degree 2 Galois covers $f\colon X'_n \to X_n$, when n varies: From Theorem 3.10 it follows that for each n the set of degree 2 unramified Galois covers of X is in bijection with the index 2 subgroups of

$$\mathrm{Pic}^0(X)(\mathbb{F}_{q^n}) \otimes \mathbb{Z}/2 \oplus \mathrm{Gal}(\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^n}) \cong \pi_1^{\mathrm{ab}}(X_n) \otimes \mathbb{Z}/2.$$

Let $X_n^{(i)} \to X_n$, $i=1,2$ be two such covers, and suppose that $\chi_i\colon \pi_1(X_n^{(i)}) \to E^*$ are two characters, such that

$$\mathrm{Ind}_{\pi_1(X_n^{(1)})}^{\pi_1(X_n)} \chi_1 \approx \mathrm{Ind}_{\pi_1(X_n^{(2)})}^{\pi_1(X_n)} \chi_2.$$

Then there is an isomorphism $X_{2n}^{(1)} \cong X_{2n}^{(2)}$ as coverings of X_n. Hence if we wish to count unramified dihedral representation of $\pi_1(X_n)$ up to (strong) twist equivalence, then the relevant quadratic covers of X_n are labelled by the index two subgroups of $\mathrm{Pic}^0(X)(\mathbb{F}_{q^n}) \otimes \mathbb{Z}/2$. The number of such labels is this equal to $\# \mathrm{Pic}^0(X)[2](\mathbb{F}_{q^n}) - 1$.

To organize the above, for a non-trivial homomorphism $\beta \colon \pi_1(\overline{X}) \to \{\pm 1\}$ we denote by n_β the smallest n such β has an extension to $\pi_1(X_{n_\beta}) \to \{\pm 1\}$. Note that all n such that β extends to $\pi_1(X_n)$ are multiples of n_β. By $f_\beta \colon X_{n_\beta}^{(\beta)} \to X_{n_\beta}$ we denote the corresponding unramified degree 2 cover. The number of such β is $2^{2g} - 1$ where g is the genus of X. For positive integers n, m we define $\delta_{m|n}$ to be 1 if m divides n and 0 otherwise. For each β define $e_\beta \in \{1, 2\}$ according to Lemma 3.4 part 4. Then we deduce from Corollary 3.6:

Proposition 3.12. *Let ℓ be an odd prime. The number of stably irreducible dihedral representation of $\pi_1(X_n)$ over $\overline{\mathbb{Q}}_\ell^*$ up to twist by characters of the base is*

$$\sum_\beta \frac{\delta_{n_\beta|n}}{2} \Big(\# \mathrm{Pic}^0(X_{n_\beta}^{(\beta)})(\mathbb{F}_{q^n}) - \frac{e_\beta}{2} \# \mathrm{Pic}^0(X)(\mathbb{F}_{q^n}) \Big).$$

The number of stably irreducible dihedral representation of $\pi_1(X_n)$ over $\overline{\mathbb{F}}_\ell^*$ up to twist by characters of the base is

$$\sum_\beta \frac{\delta_{n_\beta|n}}{2} \Big(\# \frac{\mathrm{Pic}^0(X_{n_\beta}^{(\beta)})(\mathbb{F}_{q^n})}{\mathrm{Pic}^0(X_{n_\beta}^{(\beta)})(\mathbb{F}_{q^n})_\ell} - \frac{e_\beta}{2} \frac{\# \mathrm{Pic}^0(X)(\mathbb{F}_{q^n})}{\# \mathrm{Pic}^0(X)(\mathbb{F}_{q^n})_\ell} \Big).$$

From the Weil conjecture for curves we obtain sequences of real constants (c_n) and $(c_{\beta,n})$ for $n \in \mathbb{N}$ that satisfy $|c_n| \leq q^{-n/2}$ and $|c_{\beta,n}| \leq q^{-n/2}$, respectively, such that

$$\# \mathrm{Pic}^0(X)(\mathbb{F}_{q^n}) = q^{gn}(1 - c_n)^{2g} \quad \text{and}$$
$$\# \mathrm{Pic}^0(X_{n_\beta}^{(\beta)})(\mathbb{F}_{q^n}) = q^{(2g-1)n}(1 - c_{\beta,n})^{4g-2}.$$

From Proposition 3.1 we obtain

- integers $h_\ell > 0$ and $h_{\beta,\ell} > 0$,

- for every divisor d of h_ℓ or $h_{\beta,\ell}$ integers $g_d \geq 0$ and $g_{\beta,d} \geq 0$ such that $g_{h_\ell} = 2g > g_d$ for d a proper divisor of h_ℓ and $g_{\beta,h_{\beta,\ell}} = 4g - 2 > g_d$ for d a proper divisor of $h_{\beta,\ell}$,

- for any d and $j \geq 0$ let $N_{d,j} = \ell^{-g_d j} \# \operatorname{Pic}^0(X)[\ell^\infty](\mathbb{F}_{q^{d\ell j}})$ and $N_{\beta,d,j} = \ell^{-g_{\beta,d} j} \# \operatorname{Pic}^0(X_{n_\beta}^{(\beta)})(\mathbb{F}_{q^{d\ell j}})$,

- some $j_\ell \geq 0$ such that for all $j \geq j_\ell$ one has[2]

$$N_{d,j} = N_{d,j_\ell} \quad \text{and } N_{\beta,d,j} = N_{\beta,d,j_\ell},$$

such that for any $n \geq 0$ and $j(= j(n)) = -\log_\ell |n|_\ell$ one has

$$\# \operatorname{Pic}^0(X)[\ell^\infty](\mathbb{F}_{q^n}) = N_{\gcd(n,h_\ell),j} \ell^{g_d j},$$
$$\# \operatorname{Pic}^0(X_{n_\beta}^{(\beta)})[\ell^\infty](\mathbb{F}_{q^n}) = N_{\beta,\gcd(n,h_{\beta,\ell}),j} \ell^{g_{\beta,d} j}.$$

Theorem 3.13. *Let ℓ be an odd prime.*

1) *The number of stably irreducible dihedral representation of $\pi_1(X_n)$ over $\overline{\mathbb{Q}}_\ell^*$ up to twist by characters of the base is*

$$q^{(2g-1)n} \cdot \sum_\beta \frac{\delta_{n_\beta|n}}{2} \left((1 - c_{\beta,n})^{4g-2} - \frac{e_\beta}{2} q^{-n(g-1)} (1 - c_n)^{2g} \right).$$

2) *The number of stably irreducible dihedral representation of $\pi_1(X_n)$ over $\overline{\mathbb{F}}_\ell^*$ up to twist by characters of the base is*

$$q^{(2g-1)n} \cdot \sum_\beta \frac{\delta_{n_\beta|n}}{2} \left(\frac{(1 - c_{\beta,n})^{4g-2}}{N_{\beta,\gcd(n,h_{\beta,\ell}),j}} q^{-j g_{\gcd(n,h_{\beta,\ell})} \log_q \ell} \right.$$
$$\left. - \frac{e_\beta}{2} \frac{(1 - c_n)^{2g}}{N_{\gcd(n,h_\ell),j}} q^{-j g_{\gcd(n,h_\ell)} \log_q \ell} \right),$$

where as before $j = -\log_\ell |n|_\ell$ is the largest integer such that $\ell^j | n$ – in particular $0 \leq j \leq \log_\ell n$.

Remark 3.14. We make some remarks that may help to better parse the expressions in Theorem 3.13 parts 1 and 2: Let us note first that some of the constants introduced above depend on ℓ. We did not want to add this extra term into the notation. The constants in formula 1, c_n, n_β, e_β, $c_{\beta,n}$ and $\tilde{c}_{\beta,n}$ do not depend on ℓ. The constants $h_{...}$, $g_{...}$ and $N_{...}$ from Proposition 3.1 do depend on ℓ.

---

[2]The constants $N_{...}$ as defined here differ by some ℓ-powers from those in Proposition 3.1.

The expression in part 1 is independent of ℓ. The coefficient of its leading term $q^{(2g-1)n}$ is $\frac{1}{2} \sum_\beta \delta_{n_\beta | n}$. It depends on the non-vanishing of $\delta_{n_\beta | n}$, where n_β is the minimal n, so that a certain 2-torsion subgroup of $\mathrm{Pic}^0(X)$ is defined over $\mathbb{F}_{q^{n_\beta}}$. There are $2^{2g} - 1$ choices for β; say the set of such is B. For each divisor d of $n_B = \mathrm{lcm}(n_\beta, \beta \in B)$ one obtains a different coefficient C_d of the leading term. So asymptotically for $n \to \infty$ and fixed $d = \gcd(n, n_B)$, the expression in 1 behaves like

$$C_d q^{n(2g-1)}(1 + O(q^{-n/2})).$$

If $\min(n_\beta, \beta \in B) > 1$, then $C_1 = 0$, and in fact the entire expression is zero for all n such that $\gcd(n, n_B) = 1$. I.e., within the so defined congruence classes, the expression is also zero asymptotically for $n \to \infty$. Note also the expression in part 1 is a Lefschetz like formula in the sense of Definition 4.1.

The second expression is more involved. There are finitely many structural constants since the $N_{d,j}$ and $N_{\beta,d,j}$ become constant for $j \to \infty$. This allows one to group all n again into finitely many congruence classes (that depend on n_B, h_ℓ and $h_{\beta,\ell}$ and j_ℓ) within which these structural constants are in fact constant. Within such a congruence class for n (that is in fact of the form $\gcd(n, n_{B,\ell}) = d$), one can write the expression in 2 as

$$C_d' q^{(2g-1)(n - 2j \log_q \ell) + j g_d' \log_q \ell}(1 + O(q^{-n/2 + c_d' \log_\ell n})),$$

where j is the largest integer such that ℓ^j divides n. The quantity g_d' lies between 0 and $4g - 2$, and for certain d it does assume the value $4g - 2$. This simply corresponds to the fact that (for all β and all dihedral representations counted for that β) a given mod ℓ representation has roughly $\ell^{2j(2g-1-g_d')}$ distinct lifts.

If one fixes $j = j_0$ and considers $n \to \infty$ (within the fixed congruence class), then the growth in part 2 is slightly but consistently slower than that in part 1. Asymptotically the quotient of the two expressions is

$$(3.3) \qquad \frac{C_d}{C_d'} \ell^{j_0(4g-2-g_d')}$$

This is in line with Theorem 2.3 and Corollary 2.5.

If on the other hand one considers a sequence of the form $n = n_0 \ell^k$ with $k \to \infty$, the quotient above takes the form

$$(3.4) \qquad \frac{C_d}{C_d'} \ell^{k(4g-2-g_d')} = \frac{C_d}{C_d'} q^{(4g-2-g_d') \log_q(n/n_0)},$$

i.e., it grows logarithmically in n in the exponent, or polynomially in n. This can be seen as a quantitative refinement of Theorem 2.7.

The effect of changing ℓ does not qualitatively change the behavior of the expression in part 2 for $n \to \infty$. For $\ell \gg 0$, the constants $N_{...}$ simplify as explained before Proposition 3.1: for all but finitely many ℓ one has $j_\ell = 0$. However the quantities $h_{?,\ell}$ typically grow with ℓ, and for each ℓ, the $g_?$ will be new constants about which we cannot say anything.

Corollary 3.15. *Given any prime ℓ there are infinitely many n such that*

$$\overline{T(X, 2, q^n, \ell)} < T(X, 2, q^n, \ell).$$

Proof. This is a consequence of Lemma 1.2 and Theorem 3.13. □

4. Miscellaneous remarks

We end with some remarks and by comparing the situation to counting mod ℓ eigenforms of level one.

4.1. Lefschetz like formulas

Definition 4.1. *We say that the counting function $n \mapsto \overline{T(X, 2, q^n, \ell)}$ satisfies a Lefschetz-like formula if there exist complex numbers $m_{i,\ell}$ and $\mu_{i,\ell}$ for i between 1 and k_ℓ, with $m_{i,\ell}, \mu_{i,\ell}$ independent of n but may be dependent on ℓ, such that $\overline{T(X, 2, q^n, \ell)} = \sum_{i=1}^{k_\ell} m_{i,\ell} \mu_{i,\ell}^n$ for all $n \geq 1$.*

We show that there cannot be a Lefschetz-like formula for $\overline{T(X, 2, q^n, \ell)}$ for infinitely many ℓ with the number k_ℓ in the formula bounded independently of ℓ. A Lefschetz like formula of this sort should mean roughly that $\overline{T(X, 2, q^n, \ell)}$ is counting the number of $\mathbb{F}_{q^n}$ points of a variety X_ℓ which might depend on ℓ but whose dimension and dimensions of cohomologies is bounded as ℓ varies.

Proposition 4.2. *There is no infinite set X of primes $\ell \neq p$, such that we have a Lefschetz like formula for $n \mapsto \overline{T(X, 2, q^n, \ell)}$ for all $\ell \in X$ with k_ℓ bounded independently of ℓ.*

Proof. Assume on the contrary that there is an infinite set X which violates the statement of the proposition. Let $k' \geq k + 1$, with k from Theorem 1.1

be a constant, such that for all $\ell \in X$ we have a Lefschetz like formula

$$\overline{T(X, 2, q^n, \ell)} = \sum_{i=1}^{k_\ell} m_{i,\ell} \mu_{i,\ell}^n \quad \text{for all } n \geq 1,$$

for suitable complex numbers $m_{i,\ell}, \mu_{i,\ell}, i = 1, \ldots, k_\ell$, independent of n, but possibly dependent on ℓ, such that $\mu_{1,\ell}, \ldots, \mu_{k_\ell,\ell}$ are pairwise distinct and non-zero, and $k_\ell \leq k'$. The sequence $n \mapsto a_\ell(n) := \sum_{i=1}^{k_\ell} m_{i,\ell} \mu_{i,\ell}^n$ is what is called a generalized power sum. The numbers $m_{i,\ell}$ and $\mu_{i,\ell}$ are uniquely determined by this sequence; this follows from the asymptotics for the difference of two sequences for $n \to \infty$.

As explained in [21, § 2], the sequence $(a_\ell(n))_{n \geq 0}$ is a recurrence sequence with minimal polynomial $s_\ell(X) = \prod_{i=1}^m (X - \mu_{i,\ell})$; and in fact the argument indicated there shows that $s_\ell(X)$ is the minimal polynomial of the sequence. In particular it is determined by $(a_\ell(n))_{1 \leq n \leq 2k_\ell}$. Knowing the $\mu_{i,\ell}$, one can solve for the $m_{i,\ell}$ by using the values $(a_\ell(n))_{1 \leq n \leq k_\ell}$, and hence these $k_\ell + k_\ell$ structural constants are determined by $(a_\ell(n))_{1 \leq n \leq 2k_\ell}$. In particular, if we have $\overline{T(X, 2, q^n, \ell)} = T(X, 2, q^n, \ell)$ for all $n \leq 2k_\ell$, then from the above we deduce that $k_\ell = k + 1$, $m_{i,\ell} = m_i$ and $\mu_{i,\ell} = \mu_i$ for m_i, μ_i as in Theorem 1.1 and $i = 1, \ldots, k_\ell$, and $m_{k+1,\ell} = 1$ and $\mu_{k+1,\ell} = q^{4g-3}$.

Now from de Jong's lifting result Lemma 1.2 any representation in $\overline{T(X, 2, q^n, \ell)}$ lifts to a representation in $T(X, 2, q^n, \ell)$. Since clearly for any fixed n, there are only finitely many ℓ for which two distinct representation in $T(X, 2, q^n, \ell)$ can have isomorphic reductions, there exists an ℓ_0 such that for all $\ell > \ell_0$ and all $n \leq 2k'$ we have the equality $\overline{T(X, 2, q^n, \ell)} = T(X, 2, q^n, \ell)$ required in the previous paragraph. But then the Lefschetz like formula with structural constants as in Theorem 1.1 shows that for almost all $\ell \in X$ we have $\overline{T(X, 2, q^n, \ell)} = T(X, 2, q^n, \ell)$ for all $n \geq 1$. This however contradicts Corollary 3.15 deduced from our explicit formulas on the number of dihedral representations. □

The proposition and its proof do not rule out the possibility

$$\overline{T(X, 2, q^n, \ell)} = T(X, 2, q^n, \ell)$$

for $\ell \gg 0$ and all n with $(n, \ell) = 1$.

4.2. Analogy with mod ℓ modular forms

Let us recall an analogous situation studied by T. Centeleghe in [2]. He counts the number $N(G_{\mathbb{Q}}, 2, \ell)$ of irreducible mod ℓ representations $\bar{\rho} : G_{\mathbb{Q}} \to$

$\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ that are odd and unramified outside ℓ. By Serre's conjecture these arise from newforms of level 1 and weight between 2 and $\ell + 1$, up to twisting by powers of the mod ℓ cyclotomic character χ.

Thus $N(G_{\mathbb{Q}}, 2, \ell)$ is finite and is bounded above by

$$(\ell - 1) \left(\sum_{k=2}^{\ell+1} \dim_{\mathbb{C}}(S_k(\mathrm{SL}_2(\mathbb{Z}))) \right)$$

and this number is roughly $\ell^3/48$. The conjecture here is that this is the correct asymptotic with ℓ. Something in fact stronger should be true to reflect the hypothesis that the number of congruences mod ℓ is negligible.

By an argument due to Serre, one can prove a lower bound like $\ell^2/8$, using roughly the fact that by bounds of Carlitz, at most $\ell/4$ of the Bernoulli numbers B_k (k between 2 and $\ell + 1$) are divisible by ℓ. For weights k with $2 \leq k \leq \ell + 1$, and such that ℓ does not divide B_k, it is not hard to see that all newforms in $S_k(\mathrm{SL}_2(\mathbb{Z}))$ give rise to irreducible mod ℓ representations. This together with the fact that at most two twists of irreducible mod ℓ representations arising from cusp forms can have Serre weight $\leq \ell + 1$ shows that $N(G_{\mathbb{Q}}, 2, \ell) \geq \ell^2/48$.

Note that a more constructive proof using induced dihedral representations may sometimes give no lower bounds when ℓ is 1 mod 4 (there are no unramified outside ℓ, odd, 2-dimensional mod ℓ dihedral representations when ℓ is 1 mod 4), or poor lower bounds like $\ell^{3/2}/2$ when ℓ is 3 mod 4 (as the class group of $\mathbb{Q}(\sqrt{(-\ell)})$ has order around $\sqrt{\ell}$). Serre's non-constructive proof does better, but still falls well short of the conjectured asymptotic.

Question 4.3. *Is there an analog of Serre's lower bound, and his style of argument, in the present geometric case which improves the lower bound on $\overline{T(X, 2, q^n, \ell)}$ (for fixed ℓ and varying n) that we have obtained via counting dihedral representations in Theorem 3.13?*

4.3. Congruences between cusp forms and Eisenstein series

We pose a question related to producing irreducible liftings of reducible Galois representations $\bar{\rho} : \pi_1(X) \to \mathrm{GL}_2(\mathbb{F})$.

It is known that given any pair of characters $\chi_1, \chi_2 : G_{\mathbb{Q}} \to \mathbb{F}^*$ such that $\chi_1 \chi_2$ is odd, there is a newform f of weight $k \geq 2$ and level N, the prime to ℓ part of the product of the conductors of χ_1 and χ_2, such that the ℓ-adic representation $\rho_{f,\iota} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ attached to f has reduction whose semi simplification is $\chi_1 \oplus \chi_2$. This is proved by using Ramanujan's Θ-operator on

mod ℓ modular forms whose effect on q-expansions of mod ℓ modular forms is given by $\Theta(\sum_n a_n q^n) = \sum_n n a_n q^n$. The proof, cf. Theorem 1 of [10] for instance, is to start with a mod ℓ Eisenstein series $E = E_{\chi_1, \chi_2}$ which is an eigenform for Hecke operators T_r for primes r, $(r, N\ell) = 1$, with eigenvalue $\chi_1(r) + \chi_2(r)$ and observe that $f = \Theta^{\ell-1} E$ is a mod ℓ cuspidal form with the same Hecke eigenvalues. Note that the weight of f can be as large as $\ell^2 - 1$.

Motivated by this we can ask for analogs in our present function field case. Let $\chi : \pi_1(X) \to \overline{\mathbb{F}_\ell}^*$ be a character that factors thorough the Galois group of a geometric cover of X.

Given an irreducible ℓ-adic representation $\rho : \pi_1(X) \to \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$ such that the semi simplification of a reduction of it is given by $1 \oplus \chi$. Then a standard argument using lattices and going back to Ribet [19, Prop. 2.1] shows that $H^1(\pi_1(X), \overline{\mathbb{F}_\ell}(\chi))$ and $H^1(\pi_1(X), \overline{\mathbb{F}_\ell}(\chi^{-1}))$ are both non-zero. Conversely:

Question 4.4. *Suppose $H^1(\pi_1(X), \overline{\mathbb{F}_\ell}(\chi))$ and $H^1(\pi_1(X), \overline{\mathbb{F}_\ell}(\chi^{-1}))$ are both non-zero. Then is there an irreducible ℓ-adic representation $\rho : \pi_1(X) \to \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$ such that the semisimplification of a reduction of an integral model of it is given by $1 \oplus \chi$?*

Acknowledgements

References

[1] B. Bhatt and P. Scholze, *The pro-étale topology for schemes*, Astérisque (2015), no. 369, 99–201.

[2] T. G. Centeleghe, *Computing the number of certain Galois representations mod p*, J. Théor. Nombres Bordeaux **23** (2011), no. 3, 603–627.

[3] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers, a division of John Wiley & Sons, New York-London (1962).

[4] A. J. de Jong, *A conjecture on arithmetic fundamental groups*, Israel J. Math. **121** (2001), 61–84.

[5] P. Deligne, *Comptage de faisceaux l-adiques*, Astérisque (2015), no. 369, 285–312.

[6] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, Vol. 61 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, second edition (1999), ISBN 0-521-65011-9.

[7] V. G. Drinfel'd, *The number of two-dimensional irreducible representations of the fundamental group of a curve over a finite field*, Funktsional. Anal. i Prilozhen. **15** (1981), no. 4, 75–76.

[8] B. Edixhoven, G. van der Geer, and B. Moonen, *Abelian Varieties* (2014). (preliminary version of the first chapters), http://gerard.vdgeer.net/AV.pdf.

[9] D. Gaitsgory, *On de Jong's conjecture*, Israel J. Math. **157** (2007), 155–191.

[10] A. Ghitza, *All Siegel Hecke eigensystems (mod p) are cuspidal*, Math. Res. Lett. **13** (2006), no. 5-6, 813–823.

[11] H. Hida, *Modular forms and Galois cohomology*, Vol. 69 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge (2000), ISBN 0-521-77036-X.

[12] U. Jannsen, *On the l-adic cohomology of varieties over number fields and its Galois cohomology*, in: Galois groups over **Q** (Berkeley, CA, 1987), Vol. 16 of Math. Sci. Res. Inst. Publ., 315–360, Springer, New York (1989).

[13] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Vol. 45 of American Mathematical Society Colloquium Publications, American Mathematical Society, Providence, RI (1999), ISBN 0-8218-1017-0.

[14] L. Lafforgue, *Chtoucas de Drinfeld et correspondance de Langlands*, Invent. Math. **147** (2002), no. 1, 1–241.

[15] B. Mazur, *Deforming Galois representations*, in: Galois groups over **Q** (Berkeley, CA, 1987), Vol. 16 of Math. Sci. Res. Inst. Publ., 385–437, Springer, New York (1989).

[16] I. Mirković and K. Vilonen, *Geometric Langlands duality and representations of algebraic groups over commutative rings*, Ann. of Math. (2) **166** (2007), no. 1, 95–143.

[17] S. Morel, *Note sur les foncteurs de déformations dérivés et la conjecture de de Jong*, preprint, (2016).

[18] M. Raynaud, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*, in: Séminaire Bourbaki 1964/65, Vol. 9, Exp. No. 286, 129–147, Soc. Math. France, Paris (1995).

[19] K. A. Ribet, *A modular construction of unramified p-extensions of $Q(\mu_p)$*, Invent. Math. **34** (1976), no. 3, 151–162.

[20] J.-P. Serre, *Algebraic groups and class fields*, Vol. 117 of Graduate Texts in Mathematics, Springer-Verlag, New York (1988), ISBN 0-387-96648-X. Translated from the French.

[21] A. J. van der Poorten, *Some facts that should be better known, especially about rational functions*, in: Number theory and applications (Banff, AB, 1988), Vol. 265 of NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 497–528, Kluwer Acad. Publ., Dordrecht (1989).

INTERDISCIPLINARY CENTER FOR SCIENTIFIC COMPUTING
UNIVERSITÄT HEIDELBERG, 69120 HEIDELBERG, GERMANY
E-mail address: boeckle@uni-hd.de

DEPARTMENT OF MATHEMATICS, UCLA
BOX 951555, LOS ANGELES, CA 90095-1555, USA
E-mail address: shekhar@math.ucla.edu