Algebra & Number Theory

Volume 17
2023
No. 12

# On the variation of Frobenius eigenvalues in a skew-abelian Iwasawa tower

Asvin G.

msp

ALGEBRA AND NUMBER THEORY 17:12 (2023)
https://doi.org/10.2140/ant.2023.17.2151

# On the variation of Frobenius eigenvalues in a skew-abelian Iwasawa tower

Asvin G.

We study towers of varieties over a finite field such as $y^2 = f(x^{\ell^n})$ and prove that the characteristic polynomials of the Frobenius on the étale cohomology show a surprising $\ell$-adic convergence. We prove this by proving a more general statement about the convergence of certain invariants related to a skew-abelian cohomology group. The key ingredient is a generalization of Fermat's little theorem to matrices. Along the way, we will prove that many natural sequences of polynomials $(p_n(x))_{n\geq 1} \in \mathbb{Z}_\ell[x]^{\mathbb{N}}$ converge $\ell$-adically and give explicit rates of convergence.



**Notation 1.** We will work throughout over a fixed finite field $\mathbb{F}_q$. A curve $C$ over $\mathbb{F}_q$ refers to a smooth, projective, geometrically connected scheme of dimension 1. The base change to the algebraic closure $\bar{\mathbb{F}}_q$ is denoted by $\bar{C}$. We denote its étale cohomology with $\mathbb{Z}_\ell$ coefficients by $H^1_{\text{ét}}(\bar{C}, \mathbb{Z}_\ell)$. By standard functoriality arguments, it comes endowed with a linear action of the geometric Frobenius $\sigma_q$. We fix an auxiliary prime $\ell$ throughout and for simplicity assume that $\ell > 2$ and $q \equiv 1 \pmod{\ell}$.[1]

## 1. Introduction

The eigenvalues of the Frobenius on the étale cohomology of a smooth, projective variety over a finite field carry significant arithmetic information. By the Weil conjectures, these eigenvalues are algebraic integers and their absolute values under any complex embedding are understood.

We draw inspiration from Iwasawa theory to study the asymptotic behavior of these eigenvalues in an "Iwasawa tower" and in particular, we show that there is a strong $\ell$-adic convergence statement to be made in many natural examples. The Iwasawa algebras arising in this study are noncommutative due

*MSC2020:* primary 11R23; secondary 11G20.
*Keywords:* Iwasawa theory, $L$-functions over finite fields.

[1] As usual, the theorems go through if $\ell = 2$ with appropriately stronger hypothesis. For instance, if $\ell = 2$ then we need $q \equiv 1 \pmod{\ell^2}$.

to the nontrivial action of the Frobenius on this monodromy group and we hope that this perspective is interesting too. Let us begin with an example.

**Example 2.** Consider the smooth projective curves $C_n$ corresponding to the equations

$$Y^2 = X^{2^n} + 1 \text{ over } \mathbb{F}_5.$$

They define a tower $\cdots \to C_2 \to C_1$ with maps $C_{n+1} \to C_n$ defined by $(X, Y) \to (X^2, Y)$. The characteristic polynomial of $\sigma_5$ on $H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)$ is

$$f_n(x) := \det(1 - \sigma_2 x \mid H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)) = (1 - 2x + 5x^2) \prod_{i=1}^{n-2} (1 + x^{2^i} 5^{2^{i-1}})^2.$$

Note that $f_{n-1}(x)$ divides $f_n(x)$ and the inverse of the roots of $g_n(x) = f_n(x)/f_{n-1}(x)$ are of the form $\sqrt{5}\zeta$ for $\zeta$ a root of unity of order $2^{n-1}$ for $n \geq 3$. In Section 4, we show that for $n$ sufficiently large, the normalized (by $\alpha \to \alpha/|\alpha|$ so that the complex absolute value is 1) roots of $g_{n+1}(x)$ are exactly all possible $\ell$-th roots of the normalized roots of $g_n(x)$.[2]

In fact, we prove the same statement for towers of Fermat curves (from which the above follows) and Artin–Schreier curves. The proof of this statement follows from realizing the roots of $g_n(x)$ as Jacobi sums and using results of Coleman [1987] on identities for Gauss sums (coming from the Gross–Kubota $p$-adic Gamma function [Gross and Koblitz 1979]).

**1.1.** ***A congruence on characteristic polynomials.*** This prompts the question of what happens in a more general context. For instance, we could take a map $f : C \to \mathbb{P}^1$ or $f : C \to A$ for $A$ an abelian variety of dimension $d$ and pull back by the following diagrams:

$$\begin{tikzcd} C_n \arrow[r, "f_n"] \arrow[d, "\pi_n"] & \mathbb{P}^1 \arrow[d, "t \to t^{\ell^n}"] \\ C \arrow[r, "f"] & \mathbb{P}^1 \end{tikzcd} \quad \text{or} \quad \begin{tikzcd} C_n \arrow[r, "f_n"] \arrow[d, "\pi_n"] & A \arrow[d, "{[\ell^n]}"] \\ C \arrow[r, "f"] & A \end{tikzcd}$$

We denote the first family of examples by Case A and the second family by Case B. Note that in both the families, the $C_n \to C$ are geometrically (branched) Galois extensions with an abelian Galois group $G_n \cong (\mathbb{Z}/\ell^n\mathbb{Z})^b$ for $b = 1$ or $2d$ in Cases A and B respectively. Note that the $G_n$ themselves have an action of $\sigma_q$ and this will be crucial.

We define $M_n = H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)/H^1_{\text{ét}}(\overline{C}, \mathbb{Z}_\ell)$, $f_n(x)$ to be the characteristic polynomial of $\sigma_q$ on $M_n$ and $g_n$ to be the characteristic polynomial $\det(1 - \sigma_q x \mid M_n/M_{n-1})$. It does not seem to be true that $g_n$ determines $g_{n+1}$ as in Example 2. Nonetheless, the following weaker convergence statement is true.

Let $k_n$ be the order of $\sigma_q$ acting on $\mu_{\ell^n} = \mathbb{G}_m[\ell^n]$ in Case A while in Case B, $k_n$ is a close relative of the order of $\sigma_q$ acting on $A[\ell^n]$. In particular, it is independent of $C$ and can be made completely explicit. In either case $k_n$ is of the form $\max\{1, \ell^{n-n_0}\}$ with $n_0$ depending on which case we are considering.

[2] we note that the complex norm $|\alpha|$ is independent of the embedding to $\mathbb{C}$ by the Weil conjectures

**Theorem** (Theorem 19). *In the above set up (with some mild assumptions on $f$ and $q$):*

(1) *We have a factorization into monic polynomials*

$$f_m(x) = \prod_{n \le m} g_n(x)$$

*where the $g_n$ are independent of $m$.*

(2) *There exist polynomials $h_n(y), \tilde{h}_n(y) \in \mathbb{Z}[y]$ such that, **in Case A***

$$g_n(x) = h_n(x^{k_n}).$$

*while in **Case B***

$$g_n(x) = \tilde{h}_n(x^{k_n}).$$

(3) ***In Case A**, for $n$ sufficiently large so that $k_{n+1} = \ell k_n$ (Lemma 21), we have the $\ell$-adic convergence*

$$h_{n+1}(y) \equiv h_n(y) \pmod{\ell^n}.$$

*In particular, the following $\ell$-adic limit exists in $\mathbb{Z}_\ell[y]$:*

$$h_\infty(y) = \lim_{n \to \infty} h_n(y).$$

***In Case B**, for $n \ge n_0$ sufficiently large so that $k_{n+1} = \ell k_n$, we have the congruence*

$$\tilde{h}_{n+1}(y) \equiv \tilde{h}_n^{\ell(b-1)}(y) \pmod{\ell^n}.$$

*In particular, the following $\ell$-adic limit exists in $\mathbb{Z}_\ell[y]$ with* exp, log *defined formally as power series:*

$$\tilde{h}_\infty(y) = \exp\left( \lim_{n \to \infty} \frac{1}{\ell^{(n-n_0)(b-1)}} \log(\tilde{h}_n(y)) \right).$$

The first two properties of the theorem are fairly standard and follow from understanding the structure of $M_n$ as a module over $\mathbb{Z}_\ell[G_n, \sigma_q]$ and in particular, depends on $\sigma_q$ having "large" orbits when acting upon the characters of $G_n$.[3] The main body of the paper proves a more abstract statement (Theorem 26) about the convergence of certain invariants of a nonabelian cohomology group which implies the third part of the above theorem on the towers of curves.

We note that this more abstract statement can be applied to many more geometric contexts than just our two examples of towers of curves above although we do not pursue this in our paper. It applies to any tower of varieties with an action of an abelian group such that the Frobenius action on the cohomology has a "large" orbit. For instance, we could take hypersurfaces of the form

$$f(x_0^{\ell^n}, \ldots, x_n^{\ell^n}) = 0 \subset \mathbb{P}^n_{\mathbb{F}_q}.$$

[3] As a reviewer pointed out, part 2 has been "known for a long time and rediscovered several times", for instance see [Gordon 1979, Lemma 1.1]. For completeness, we give our own proof too.

All the interesting cohomology is concentrated in the middle dimensional cohomology and the above theorem holds for the characteristic polynomial of the Frobenius action on this middle dimensional cohomology group.

We will see in Section 3 that $M_\infty = \varprojlim_n M_n$ is a free module for a certain skew-abelian Iwasawa algebra and in particular, the characteristic polynomials we study are all determined by a Galois cohomology class with coefficients in matrices over a ring of power series. The bulk of this paper consists in studying the $\ell$-adic properties of these power series.

A key role in the study of the study of these algebraic properties is played by the following generalization of Fermat's little theorem (conjectured by Arnold [2006] and proven by Zarelua [2008]):

**Theorem** (Arnold and Zarelua, Theorem 29). *Let $A$ be a $r \times r$ matrix over $\mathbb{Z}_\ell$. Then, the congruence*

$$\operatorname{tr}(A^{\ell^{n+1}}) \equiv \operatorname{tr}(A^{\ell^n}) \pmod{\ell^{n+1}}$$

*holds for any prime $\ell$ and any $n \in \mathbb{N}$.*

Arnold's conjecture goes back to before Arnold (Jänichen [1921] and Schur [1937]). For a more recent expository survey and applications to topology and dynamics; see Zarelua [2008]. Arnold's conjecture has since been proven many times in the literature; for instance, see [Mazur and Petrenko 2010]. We give a new proof of a slightly refined statement since we will use a similar technique in proving our main theorem.[4]

To keep notation simple, we state a special (yet nontrivial) case of our general $\ell$-adic convergence theorem.

**Theorem** (Theorems 23 and 26). *Let $F(t)$ be a $r \times r$ matrix with entries in $\mathbb{Z}_\ell[t]$. Suppose that $q$ is a prime such that $q-1$ is divisible by $\ell$ but not $\ell^2$. For each $n \geq 1$, we define the matrix*

$$A_n = \prod_{i=1}^{\ell^{n-1}} F(\zeta_{\ell^n}^{q^i})$$

*with characteristic polynomial $p_n(x)$. Then, the limit $p_\infty(x) = \lim_n p_n(x)$ exists and we have the congruence*

$$p_{n+1}(x) \equiv p_n(x) \pmod{\ell^n}.$$

We note that even in the simplest case where $r = 1$, the above theorem is not obvious.

**1.2.** ***Some questions for future work.*** We pose a few questions suggested by this work.

**Question 3.** Our main theorem establishes the existence of $\ell$-adic limits $h_\infty(x), \tilde{h}_\infty(x)$ in the two cases. In some simple cases, the $h_n(x)$ are independent of $n$ for $n$ large enough and by the proof of the Weil conjectures, are known to in fact be polynomials over $\mathbb{Z}$ while a-priori $h_\infty(x)$ is only defined over $\mathbb{Z}_\ell$.

Are the roots of $h_\infty(x)$ always transcendental numbers (except in the cases where $h_n$ is eventually constant)?

[4] In the course of writing this paper, we found essentially the same proof by Qiaochu Yuan in a blog post from 2009.

**Question 4.** Even if the roots of $h_\infty(x)$ are transcendental, is it possible to describe them using simple $\ell$-adic transcendental functions?

**Question 5.** What information about the original morphism $f : C \to \mathbb{P}^1$ does $h_\infty(x)$ remember? In the classical Iwasawa theory set up, the limiting characteristic polynomials turn out to be equal to various $\ell$-adic $L$-functions up to a unit (by the main conjecture of Iwasawa theory), can we hope for something similar in this case?

**Question 6.** Let $(\Lambda, \sigma_q)$ be as in Section 3 and $M$ a finite, free $\Lambda$ module with a $\sigma_q$ semilinear endomorphism $\Phi : M \to M$. It might be possible and interesting to completely classify such endomorphisms $\Phi$ in the hope of a more conceptual proof of the main results. This question is reminiscent of Manin's classification of Dieudonne modules [Manin 1963]. Indeed, the $(M \otimes_\Lambda \Lambda_n(v), \Phi)$ form a "compatible" system of an "$\ell$-adic analogue of Dieudonne modules" over the "compatible" system of cyclotomic local rings with endomorphism $(\Lambda_n(v), \sigma_q)$ as $n$ varies - this final sentence is purely impressionistic!

**Question 7.** Let $Q : \mathbb{Z}_\ell^n \to \mathbb{Z}_\ell^n$ be a linear automorphism and for $v \in \mathbb{Z}_\ell^n$, let $k_n(v)$ be the smallest positive integer so that $Q^{k_n(v)} v \equiv v \pmod{\ell^n}$. Let $\lambda : \mathbb{Z}_\ell^n \to \mathbb{Z}_\ell$ be an arbitrary linear form. Does the sequence

$$S_n(\lambda, v) := \sum_{j=1}^{k_n(v)} \zeta_{\ell^n}^{\lambda(Q^{-j} v)}$$

defined in Remark 32 converge to 0 as $n \to \infty$? If so, what is the rate of convergence and is it uniform as $v$ ranges over primitive vectors?

***Outline of the paper.*** For expository reasons, the paper is not presented in strictly logical order. Section 3 is independent of the rest of the paper and its main results (Theorems 23 and 26) are used in proving our main geometric result (Theorem 19). The reader interested in the geometry and willing to take the $\ell$-adic analysis on faith can skip Section 3. The reader interested only in the $\ell$-adic convergence results can skip Section 2.

## 2. On the cohomology of a tower of curves

In this section, we reduce Theorem 19 to an abstract statement about the convergence of characteristic polynomials of a sequence of matrices.

We fix an odd prime $\ell$ and a finite field $\mathbb{F}_q$ with $q$ large enough to be specified soon. For a variety $X/\mathbb{F}_q$, the notation $H^i_{\text{ét}}(\overline{X}, \mathbb{Z}_\ell)$ denotes as usual the étale cohomology of the variety $X \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ with $\mathbb{Z}_\ell$ coefficients. The Frobenius $\sigma_q$ acts on it through a linear automorphism.

### 2.1. *Two families of Iwasawa towers.*

**Definition 8.** Let $C/\mathbb{F}_q$ be a curve. We will be interested in the following two classes of towers:

Case A: Given a nonconstant map $f : C \to \mathbb{P}^1$, we can construct extensions $\pi_n : C_n \to C$ by the pull back diagram:

$$\begin{tikzcd} C_n \arrow[r, "f_n"] \arrow[d, "\pi_n"] & \mathbb{P}^1 \arrow[d, "t \to t^{\ell^n}"] \\ C \arrow[r, "f"] & \mathbb{P}^1 \end{tikzcd}$$

The $C_n$ form an inverse system with an action by the group

$$\Gamma_n = \mathbb{Z}/\ell^n\mathbb{Z} \rtimes \mathbb{Z}$$

where we denote a generator for the first factor by $\theta$ (corresponding to $\theta(t) = \zeta_{\ell^n} t$) and a generator for the second factor by $\sigma_q$ corresponding to the Frobenius operation. They satisfy the commutation identity

$$\sigma_q \theta = \theta^q \sigma_q.$$

We require the $\pi_n : C_n \to C$ to be totally ramified over the preimage $f^{-1}(\{0, \infty\})$ — for instance, this is satisfied if $f$ is unramified over $0, \infty$ or more generally, if the ramification indices of $f$ over $0, \infty$ are coprime to $\ell$. This guarantees that the $C_n$ are geometrically irreducible.

Case B: Given an abelian variety $A/\mathbb{F}_q$ of dimension $d$ and a map $f : C \to A$, we construct $\pi_n : C_n \to C$ by the pullback diagram:

$$\begin{tikzcd} C_n \arrow[r, "f_n"] \arrow[d, "\pi_n"] & A \arrow[d, "{[\ell^n]}"] \\ C \arrow[r, "f"] & A \end{tikzcd}$$

We require the $C_n$ to be geometrically irreducible, this is achieved for instance if the induced map $\pi_1^{\text{ét}}(f) : \pi_1^{\text{ét}}(C) \to \pi_1^{\text{ét}}(A)$ on the étale fundamental groups is surjective. In this case, the $C_n$ are acted upon by (with $b = 2d$)

$$\Gamma_n = (\mathbb{Z}/\ell^n\mathbb{Z})^b \rtimes \mathbb{Z}.$$

The first factor can be identified with $A[\ell^n]$ and we denote a basis of it by $\alpha_1, \ldots, \alpha_d, \beta_1, \ldots, \beta_d$ so that the Frobenius $\sigma_q$ (corresponding to the second factor) acts by a $b \times b$ matrix $Q$ as

$$\sigma_q v = Qv$$

for $v \in A[\ell^n]$. The congruence $Q \equiv \mathrm{I} \pmod{\ell}$ is equivalent to $\sigma_q$ acting as the identity on $A[\ell]$. This can always be achieved by a finite extension of the base field $\mathbb{F}_q$ and we suppose that $q$ is large enough so that $Q \equiv \mathrm{I} \pmod{\ell}$.[5] Note that 1 is not an eigenvalue of $Q$ since $\sigma_q - 1 : A \to A$ has finite degree equal to $A(\mathbb{F}_q)$.

[5] If $\ell = 2$, we would need $Q \equiv \mathrm{I} \pmod{\ell^2}$.

**Remark 9.** These aren't the only cases our main theorem applies to and in fact, we can even generalize to higher dimensions. What is important is that our tower of varieties has an action by a pro-$\ell$ abelian group as above and that the growth in cohomology is "regular" in the tower so that as a module over the group algebra, the rank of the cohomology groups are constant. For example, we could take Fermat hypersurfaces of the form

$$X_n : \sum_{j=0}^{d} x_j^{\ell^n} = 0 \subset \mathbb{P}^{b+1}$$

with action by $G_n = (\mathbb{Z}/\ell^n\mathbb{Z})^b$. The only interesting cohomology group is in degree $i = b$, in which case it is a rank 1 module over $\mathbb{Z}_\ell[G_n]$ ([Anderson 1987, Theorem 6] for instance) and a straightforward variant of Theorem 14 shows that growth in cohomology is regular.

**Remark 10.** Note that the automorphism groups $\Gamma_n$ aren't abelian but they are very close to being abelian, being the extension of an abelian group by the Frobenius action. Therefore one could view this as an example of skew-abelian Iwasawa theory.

In the remainder of this subsection we prove some basic results about the cohomology of these towers (ignoring the Frobenius action initially).

**Lemma 11.** *For a finite extension of curves $f : X \to Y$, $H^1_{\text{ét}}(\overline{Y}, \mathbb{Z}_\ell)$ is a direct factor of $H^1_{\text{ét}}(\overline{X}, \mathbb{Z}_\ell)$.*

*Proof.* Since $H^1_{\text{ét}}(\overline{Y}, \mathbb{Z}_\ell)$ is dual to the Tate module $T_\ell(Y)$, it suffices to show the corresponding fact for the Tate modules of $X$ and $Y$, i.e., we need to show that the natural map $f : T_\ell(X) \to T_\ell(Y)$ is surjective and that the kernel is torsion free.

One easily checks the following composite map

$$\mathrm{Jac}(Y) \xrightarrow{f^*} \mathrm{Jac}(X) \xrightarrow{f_*} \mathrm{Jac}(Y)$$

is simply multiplication by the degree of $f$, for instance by using an isomorphism $\mathrm{Jac}(X) \cong \mathrm{Pic}(X)$ and computing the map explicitly in terms of divisors supported away from the ramification locus. This shows that the second map is surjective which in turn implies that the map on Tate modules $T_\ell(f) : T_\ell(X) \to T_\ell(Y)$ is surjective.

Moreover, the kernel of $T_\ell(f)$ is torsion free since if $[P_n]_{n\ge 1} \in T_\ell(X)$ mapped to zero, then $P_n \in \ker(f)$ which would imply that $\deg(f) \ge \ell^n$ for all $n$ which is a contradiction. □

When the extension is generically Galois, we can say more.

**Lemma 12.** *Suppose $f : X \to Y$ is a generically Galois (branched) extension of (smooth, proper) curves with Galois group $G$. Then, $H^1_{\text{ét}}(\overline{Y}, \mathbb{Z}_\ell)$ is exactly the submodule of $H^1_{\text{ét}}(\overline{X}, \mathbb{Z}_\ell)$ fixed by the $G$ action.*

*Proof.* Let us first suppose that $X, Y$ are not necessarily proper but that $f : X \to Y$ is unramified. By the Hochschild–Serre spectral sequence,

$$H^r(G, H^s_{\text{ét}}(\overline{X}, \mathbb{Z}_\ell)) \Rightarrow H^{r+s}_{\text{ét}}(\overline{Y}, \mathbb{Z}_\ell).$$

If we want to let $r+s=1$, then we have either $r=0, s=1$ or $r=1, s=0$. But, $H^0_{\text{ét}}(\overline{X},\mathbb{Z}_\ell)=\mathbb{Z}_\ell$ with the trivial $G$ action and therefore

$$H^1(G, H^0_{\text{ét}}(\overline{X},\mathbb{Z}_\ell)) = \operatorname{Hom}(G,\mathbb{Z}_\ell)=0$$

since $G$ is torsion and $\mathbb{Z}_\ell$ is torsion free. This causes the spectral sequence to degenerate at the (1, 1) term and we have the required isomorphism

$$H^1_{\text{ét}}(\overline{Y},\mathbb{Z}_\ell)\cong H^0(G, H^1_{\text{ét}}(\overline{X},\mathbb{Z}_\ell)).$$

Now, for a general (branched) $f: X\to Y$, let $T\subset Y$ be the ramification divisor on $Y$ and $f^{-1}(T)=S\subset X$ its preimage in $X$ with $U=X-S$, $V=Y-T$. With this set-up, we have following commutative diagram:

$$\begin{tikzcd}
H^1_{\text{ét}}(\overline{X},\mathbb{Z}_\ell) \arrow[r, hook] & H^s_{\text{ét}}(\overline{U},\mathbb{Z}_\ell) \\
H^1_{\text{ét}}(\overline{Y},\mathbb{Z}_\ell) \arrow[r, hook] \arrow[u, hook] & H^1_{\text{ét}}(\overline{V},\mathbb{Z}_\ell) \arrow[u, hook]
\end{tikzcd}$$

Note that the cokernels along the horizontal rows have weight 2 (i.e., $\sigma_q$ acts by $q$ on the cokernel) as can be seen either from the excision long exact sequence or from the Lefschetz fixed point theorem for compactly supported cohomology along with Poincaré duality. On the other hand $H^1_{\text{ét}}(\overline{Y},\mathbb{Z}_\ell)$, $H^1_{\text{ét}}(\overline{Y},\mathbb{Z}_\ell)$ are both of weight 1 (by the Weil conjectures, for instance).

The above diagram is $G$-equivariant since $S, T$ are. Therefore, the $G$-invariants of $H^1_{\text{ét}}(\overline{X},\mathbb{Z}_\ell)$ are contained in $H^1_{\text{ét}}(\overline{V},\mathbb{Z}_\ell)$ but the above weight argument shows that it is in fact contained in $H^1_{\text{ét}}(\overline{Y},\mathbb{Z}_\ell)$ as required. □

Let us return to our specific towers above.

**Definition 13.** In *Case A*, let $G_n=\mathbb{Z}/\ell^n\mathbb{Z}$ with generator $\theta$ while in *Case B*, let $G_n=(\mathbb{Z}/\ell^n\mathbb{Z})^b$ with generators $\alpha_i$, $\beta_j$ as discussed before. We also define the group algebra $R_n=\mathbb{Z}_\ell[G_n]$.

By Lemma 11 and 12, $M_n=H^1_{\text{ét}}(\overline{C}_n,\mathbb{Z}_\ell)/H^1_{\text{ét}}(\overline{C},\mathbb{Z}_\ell)$ is a free $\mathbb{Z}_\ell$ module with an action of $R_n$ described by the following theorem with $g_0$ the genus of $C$.

**Theorem 14.** *Let us define*

$$r=\begin{cases} 2g_0+s-2 & \textit{in Case } A,\\ 2g_0-2 & \textit{in Case } B,\end{cases}$$

*where in Case $A$, $s$ is the number of preimages of* $0,\infty$ *for the defining map* $f: C\to\mathbb{P}^1$.

*As $R_n$ modules, we have an exact sequence*

$$0\to\mathbb{Z}_\ell^r\to R_n^r\to M_n\to 0,$$

*where $G_n$ acts trivially on the first term.*

As a preliminary to the above theorem, we use Riemann–Hurwitz to compute the dimensions of $M_n$.

**Lemma 15.** *Let $g_n$ be the genus of $C_n$. $M_n$ is a free $\mathbb{Z}_\ell$ module of rank $2(g_n - g_0)$ and in Case $A$, we have*

$$\dim_{\mathbb{Z}_\ell} M_n = (\ell^n - 1)(2g_0 + s - 2)$$

*while in Case $B$, we have*

$$\dim_{\mathbb{Z}_\ell} M_n = (\ell^{bn} - 1)(2g_0 - 2).$$

*Proof.* By Lemmas 11 and 12, $M_n$ is a free $\mathbb{Z}_\ell$ module. It remains to compute its $\mathbb{Z}_\ell$ rank ($= 2(g_n - g_0)$). In *Case A*, let $S_0, S_\infty \subset C(\bar{\mathbb{F}}_q)$ be the preimages of $0, \infty$ under $f$ so that $s = |S_0| + |S_\infty|$. Note that $\pi_n$ is only ramified over $S_0, S_\infty$ and by assumption, it is totally ramified to order $\ell^n$ over these points. By Riemann–Hurwitz, we then have

$$2g_n - 2 = \ell^n(2g_0 - 2) + s(\ell^n - 1) \Longrightarrow 2(g_n - g_0) = (\ell^n - 1)(2g_0 + s - 2).$$

In *Case B*, $\pi_n$ is unramified and of degree $\ell^{bn}$ and therefore, we simply have

$$2g_n - 2 = \ell^{bn}(2g_0 - 2) \Longrightarrow 2(g_n - g_0) = (\ell^{bn} - 1)(2g_0 - 2). \qquad \square$$

We finish the proof of Theorem 14 by using the Lefschetz fixed point theorem to compute the character of $M$ in terms of fixed points.

*Proof.* In *Case A*, let $g \in G_n$ be nontrivial. Since $g$ is not the identity, the only points it fixes on $C_n$ are the points lying over $0, \infty$ under the map $C_n \to \mathbb{P}^1$. In the notation of the previous lemma, there are $s$ such points in total and the local index at each point is $+1$. Moreover, $g$ acts trivially on the degree 0, 2 cohomology groups. Therefore, by the Lefschetz fixed point formula

$$\operatorname{tr}(g \mid H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)) = 2 - s$$

and since $G$ acts trivially on $C_0$,

$$\operatorname{tr}(g \mid H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)) - \operatorname{tr}(g \mid H^1_{\text{ét}}(\overline{C}, \mathbb{Z}_\ell)) = -(2g_0 + s - 2) = -r.$$

On the other hand, the identity $\mathrm{id} \in G_n$ of course acts trivially so that

$$\operatorname{tr}(\mathrm{id} \mid H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)) - \operatorname{tr}(\mathrm{id} \mid H^1_{\text{ét}}(\overline{C}, \mathbb{Z}_\ell)) = 2(g_n - g_0) = r(\ell^n - 1)$$

where the final equality is by the previous lemma.

In *Case B*, any $g \neq \mathrm{id} \in G_n$ acts on the abelian variety $A$ by a nontrivial translation and hence has no fixed points on either $C_n$ or $A$. As before, by the Lefschetz fixed point theorem

$$\operatorname{tr}(g \mid H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)) - \operatorname{tr}(g \mid H^1_{\text{ét}}(\overline{C}, \mathbb{Z}_\ell)) = 2 - 2g_0 = -r.$$

The identity element has trace equal to

$$\dim H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell) - \dim H^1_{\text{ét}}(\overline{C}, \mathbb{Z}_\ell) = 2(g_n - g_0) = r(\ell^{bn} - 1).$$

If we then examine the exact sequence

$$0 \to \mathbb{Z}_\ell^r \to R_n^r \to X \to 0,$$

we see that $X$ has the character we computed above in both cases for $M_n$ proving that $X \cong M_n$ as $G_n$ representations. □

**Remark 16.** As an immediate corollary of the above theorem, we notice that in both *Case A* and *B*, for every nontrivial character $\chi : G_n \to \bar{\mathbb{Z}}^\times$, the corresponding eigenspace $M_n(\chi)$ of $M_n \otimes \mathbb{Z}_\ell[\zeta_{\ell^n}]$ is of dimension $2g_0 + s - 2$ and $2g_0 - 2$ in the two cases respectively. In particular it is independent of $n$ and we call the characters appearing in $P_n = M_n/M_{n-1}$ "new" or "primitive" characters of level $n$.

We fix a set of generators $t_1, \dots, t_b$ for $G_n \cong (\mathbb{Z}/\ell^n\mathbb{Z})^b$ and identify characters $\chi$ of $G_n$ by vectors $v = (v_1, \dots, v_b) \in (\mathbb{Z}/\ell^n\mathbb{Z})^b$ by defining $\chi_v(t_i) = t_i^{v_i}$. Under this identification, primitive characters correspond exactly to primitive vectors as defined below in Definition 18. We denote the eigenspace of $\chi_v$ by $M_n(v)$.

The exact sequence in the above theorem implies that $M_n$ is not a free $R_n$ module but nevertheless, the inverse limit $M_\infty := \lim_n M_n$ is a free module over $\Lambda = \mathbb{Z}_\ell[[T_1, \dots, T_b]] = \lim_n R_n$.

**Lemma 17.** *Let $\theta_1, \dots, \theta_b$ be the generators of $G_n = (\mathbb{Z}/\ell^n\mathbb{Z})^b$ as above. Then the projective limit $M_\infty := \varprojlim_n M_n$ is a free module of rank $r$ over $\Lambda = \mathbb{Z}_\ell[[T_1, \dots, T_b]]$. The Frobenius $\sigma_q$ acts **semi**linearly on $M_\infty$, i.e., $\sigma_q$ is $\mathbb{Z}_\ell$ linear and satisfies*

$$\sigma_q \circ (1 + T_i) = \sigma_q(1 + T_i) \circ \sigma_q$$

*where we identify $1 + T_i$ with $\theta_i$ so that $\sigma_q$ acts on $1 + T_i$ through its action on $\varprojlim_n G_n$.*

*Proof.* By the above theorem, we have the following identification as $\mathbb{Z}_\ell[G_n]$-modules

$$M_n \cong \left( \frac{\mathbb{Z}_\ell[\theta_1, \dots, \theta_b]}{\theta_1^{\ell^n} = 1, \dots, \theta_b^{\ell^n} = 1, \prod_{i=1}^b \left(\sum_{j=0}^{\ell^n - 1} \theta_i^j\right)} \right)^r$$

since $\prod_{i=1}^b \left(\sum_{j=0}^{\ell^n-1} \theta_i^j\right)$ generates the unique 1-dimensional $\mathbb{Z}_\ell$ submodule of $\mathbb{Z}_\ell[G_n]$ with trivial $G_n$ action. Using this explicit presentation, we define a map

$$\Lambda^r = (\mathbb{Z}_\ell[[T_1, \dots, T_b]])^r \to M_\infty$$

by mapping, for each factor, the $T_i \to \theta_i - 1$ in each term in the projective limit. We will prove that this map is an isomorphism. Since the map is defined on each factor, we can assume henceforth that $r = 1$. The kernel of the induced map to $M_n$ is generated by the elements

$$(1 + T_i)^{\ell^n} - 1 = \sum_{j=1}^{\ell^n} \binom{\ell^n}{j} T_i^j \quad \text{for } i = 1, \dots, b$$

and
$$\prod_{i=1}^{b}\Big(\frac{(1+T_i)^{\ell^n}-1}{T_i}\Big)=\prod_{i=1}^{b}\Big(\sum_{j=1}^{\ell^n}\binom{\ell^n}{j}T_i^j\Big).$$

As $n \to \infty$, these elements tend to 0 in the $(\ell, T_1, \dots, T_b)$-adic topology of $\Lambda$ so that the map $\Lambda \to M_\infty$ is injective. On the other hand, surjectivity is also clear since the $\theta_i$ generate $G_n$, and consequently the $\theta_i - 1$ generate $\mathbb{Z}[G_n]$. The Frobenius action is induced through this morphism, thus completing the proof. □

**2.2. *On the distribution of Frobenius eigenvalues in towers of curves.*** In this subsection, we prove that the characteristic polynomials $f_n(x)$ of $\sigma_q$ on $H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)$ in our two cases satisfy some striking congruences. We will treat the cases uniformly by letting $Q = q$, $b = 1$ in Case A.

**Definition 18.** For $R$ a discretely valued ring (DVR) or a quotient of a DVR, we call $v \in R^b$ primitive if at least one of its coordinates is a unit. We denote the space of primitive vectors by $\mathcal{P}(R^b)$.

For a primitive vector $v \in H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)$, we define $k_n(v)$ to be the smallest positive integer such that $Q^{k_n(v)} v \equiv v \pmod{\ell^n}$. We define $k_n$ to be the minimum of $k_n(v)$ as $v$ ranges over primitive vectors. Lemma 21 shows the existence of a positive integer $\beta_v$ such that $k_n(v) = \ell^{n-\beta_v}$ for $n \geq \beta_v$. Moreover, $n_0 = \max_{v \text{ primitive}} \beta_v$ is finite so that $k_n = \ell^{n-n_0}$ for $n \geq n_0$.

**Theorem 19.** *Let $C_n$ be as in Case A or B of Definition 8 and*

$$f_n(x) = \det(1 - \sigma_q x \mid M_n)$$

*be the characteristic polynomial of the Frobenius $\sigma_q$ acting on $M_n = H^1_{\text{ét}}(\overline{C}_n, \mathbb{Z}_\ell)/H^1_{\text{ét}}(\overline{C}, \mathbb{Z}_\ell)$. It satisfies the following properties*:

(1) *We have a factorization into monic polynomials*
$$f_m(x) = \prod_{n \leq m} g_n(x) \tag{1}$$
*where the $g_n$ are independent of $m$.*

(2) *There exist polynomials $h_n(y)$, $\tilde{h}_n(y)$ such that, **in Case A***
$$g_n(x) = h_n(x^{k_n}). \tag{2}$$
*While **in Case B***
$$g_n(x) = \tilde{h}_n(x^{k_n}). \tag{3}$$

(3) ***In Case A**, for $n \geq n_0$ (Lemma 21), we have the $\ell$-adic convergence*
$$h_{n+1}(y) \equiv h_n(y) \pmod{\ell^n}. \tag{4}$$

*In particular, the following $\ell$-adic limit exists in $\mathbb{Z}_\ell[y]$:*

$$h_\infty(y) = \lim_{n\to\infty} h_n(y).$$

***In Case B**, for $n \geq n_0$, we have the congruence*

$$\tilde{h}_{n+1}(y) \equiv (\tilde{h}_n(y))^{\ell^{(b-1)}} \pmod{\ell^n}. \tag{5}$$

*In particular, the following $\ell$-adic limit exists in $\mathbb{Z}_\ell[y]$ with* exp, log *defined formally as power series:*

$$\tilde{h}_\infty(y) = \exp\left(\lim_{n\to\infty} \frac{1}{\ell^{(n-n_0)(b-1)}} \log(\tilde{h}_n(y))\right).$$

**Remark 20.** The Frobenius $\sigma_q$ is known to act semisimply on the étale cohomology of a curve and conjectured to act semisimply with rational coefficients on any variety over $\mathbb{F}_q$.[6] While the following proof simplifies slightly if we use the semisimplicity of $\sigma_q$ on $M_n$, we do not assume this so that the following proof can be adapted more easily to cases where semisimplicity is not known.

*Proof. Part* 1, i.e., equation (1) is an immediate consequence of Lemma 11 once we define $g_n(x)$ to be the characteristic polynomial of $\sigma_q$ on $P_n = M_n/M_{n-1}$.

*To prove Part* 2, i.e., equations (2) and (3), we treat the two cases simultaneously by taking $b = 1$, $Q = q$ in Case A. Recall the notation that, for $v \in \mathbb{Z}_\ell^b$, $M_n(v)$ is the eigenspace of $G_n$ for the character $\chi_v(t_i) = t_i^{v_i}$. The eigenspaces $M_n(v)$ get permuted by $\sigma_q$ in the following manner:

$$\sigma_q : M_n(v) \to M_n(Q^{-1}v)$$

and therefore $\sigma_q^{k_n(v)}$ is an automorphism of $M_n(v)$. We will prove that a Jordan block of $\sigma_q^{k_n(v)}$ acting on $M_n(v) \subset P_n$ (with eigenvalue $\lambda \neq 0$) corresponds to $k_n(v)$ distinct Jordan blocks of $\sigma_q$ acting on $P_n$ (with eigenvalues $\mu^{1/k_n(v)}$). Since this claim is independent of passing to an extension, we replace $P_n$ by $P_n \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell$.

To that end, let $m_1, \ldots, m_s \in M_n(v)$ be some generalized eigenvectors of $\sigma_q^{k_n}$ corresponding to a pure Jordan block of eigenvalue $\lambda$ (possibly defined over an extension $\mathbb{Z}_\ell$) so that

$$\sigma_q^{k_n}(m_{i+1}) = \lambda m_{i+1} + m_i$$

(with the convention that $m_0 = 0$). We will first show that the eigenvector $m_1$ for $\sigma_q^{k_n(v)}$ corresponds to $k_n(v)$ distinct eigenvectors for $\sigma_q$. For $m_i \in M_n(v)$, let $m_{i,j} = \sigma_q^{j-1}(m_i)$ for $j = 1, \ldots, k_n(v)$. Note that

$$\sigma_q(m_{i+1,k_n(v)}) = \sigma_q^{k_n(v)}(m_{i+1}) = \lambda m_{i+1,1} + m_{i,1}.$$

For each $\mu$ a $k_n$ root of $\lambda$, $n_\mu = \sum_{j=1}^{k_n(v)} \mu^{-j} m_{1,j}$ is an eigenvector of $\sigma_q$. Indeed, we have

$$\sigma_q(n_\mu) = \sum_{j=1}^{k_n(v)-1} \mu^{-j} m_{1,j+1} + \lambda\mu^{-k_n(v)} m_{1,1} = \mu n_\mu.$$

[6] Semisimplicity for abelian varieties.

Therefore, the $n_\mu$ are each an eigenvector of $\sigma_q$ and the subspace $N = \mathrm{span}(n_\mu : \mu^{k_n(v)} = \lambda)$ is stable under $\sigma_q$ and contains

$$m_{1,j} = \frac{1}{k_n(v)} \sum_{\mu^{k_n(v)}=\lambda} \mu^j n_\mu \quad \text{for } j = 1, \ldots, k_n(v).$$

Passing to the quotient $P_n/N$ therefore corresponds to replacing the $m_1, \ldots, m_s$ by $m_2, \ldots, m_s$ (with $m_2$ now an eigenvalue of $\sigma_q^{k_n(v)}$) and we continue inductively to show that each $m_i$ corresponds to $k_n(v)$ distinct generalized eigenvectors $n_{i,\mu}$ with eigenvalue $\mu$.

Let $g_{n,v}(x) = \det(\mathrm{I} - \sigma_q x)$ be the characteristic polynomial of $\sigma_q$ on $N_n(v) = \bigoplus_{i=0}^{k_n(v)-1} M_n(Q^i(v))$. This module has dimension exactly $k_n(v)$ times the dimension of $M_n(v)$ and since for each generalized eigenvector $m_i$ of $M_n(v)$, we have constructed $k_n(v)$ distinct generalized eigenvectors $n_{i,\mu}$ of $N_n(v)$ corresponding to the $k_n(v)$ distinct roots of $\lambda$, the $n_{i,\mu}$ together in fact span $N_n(v)$.

The identity

$$\prod_{j=1}^{k_n(v)} (1 - x\mu\zeta_{k_n(v)}^j) = 1 - x^{k_n(v)}\mu^{k_n(v)}$$

then shows that $g_{n,v}(x) = h_{n,v}(x^{k_n(v)})$ for some polynomial $h_{n,v}(y)$ with roots $y = \lambda = \mu^{k_n(v)}$. We note that the above proof in fact computes the $h_{n,v}(x)$ to be exactly the characteristic polynomial of $\sigma_q^{k_n(v)}$ on $M_n(v)$. Since

$$g_n(x) = \prod_{v \in \mathcal{P}(\mathbb{Z}/\ell^n\mathbb{Z})/\sim} g_{n,v}(x)$$

where the product is over a set of representatives for the $\sigma_q$ action on primitive vectors, the proof of part (2) in Case A is completed by defining

$$h_n(y) = \prod_{v \in \mathcal{P}(\mathbb{Z}/\ell^n\mathbb{Z})/\sim} h_{n,v}(y)$$

and setting $y = x^{k_n}$.

For Case B, we define (again as a product over a similar set of representatives for the $\sigma_q$ action on primitive vectors)

$$\tilde{h}_n(y) = \prod_{v \in \mathcal{P}(\mathbb{Z}/\ell^n\mathbb{Z})^b/\sim} h_{n,v}(y^{k_n(v)/k_n})$$

so that (with $y = x^{k_n}$)

$$g_n(x) = \prod_{v \in \mathcal{P}(\mathbb{Z}/\ell^n\mathbb{Z})^b/\sim} g_{n,v}(x) = \prod_{v \in \mathcal{P}(\mathbb{Z}/\ell^n\mathbb{Z})^b/\sim} h_{n,v}(x^{k_n(v)}) = \tilde{h}_n(x^{k_n}).$$

*Finally, we prove Part* (3), i.e., equations (4) and (5). Let us fix a generating set $m_1, \ldots, m_r$ for $M_n$ over $\mathbb{Z}_\ell[G_n] \cong \mathbb{Z}_\ell[t_1, \ldots, t_b]/(t_i^{\ell^n} - 1 : i = 1, \ldots, b)$. Since $M_n$ is not a free $\mathbb{Z}_\ell[G_n]$ module, it might not be completely clear what a generating set should mean. For our purposes, it suffices to choose $m_1, \ldots, m_r$ so that under any specialization that maps the $t_i$ to $\ell^n$ roots of unity, the $m_i$ specialize to a genuine basis over the induced specialization of $M_n$. That this is indeed possible follows from the explicit description of the $M_n$ as $G_n$ modules in Lemma 17. Such a specialization corresponds to a representation $\chi_v : G_n \to \overline{\mathbb{Q}}$ for $v \in \mathbb{Z}_\ell^b$ and we denote the induced specialization also by $\chi_v : M_n \to M_n(v)$

In terms of the $m_1, \ldots, m_r$, $\sigma_q$ acting on $M_n$ can be represented by some invertible matrix $F(t_1, \ldots, t_b)$. From this point on, *we will be concerned only with this matrix* $F(t_1, \ldots, t_b)$. Since $\sigma_q$ skew commutes with the $t_i$, we have

$$\sigma_q^{k_n(v)} = \prod_{i=1}^{k_n(v)} F(t^{Q^{k_n(v)-i}v}).$$

Therefore, with respect to the basis $\chi_v(m_1), \ldots, \chi_v(m_r)$ of $M_n(v)$, the action of $\sigma_q^{k_n(v)}$ corresponds to evaluating the above product using the character $\chi_v$ and is represented by the matrix

$$A_n(v) = \prod_{i=1}^{k_n(v)} F(\zeta_{\ell^n}^{Q^{k_n(v)-i}v})$$

of Section 3 (and we note that $A_n(v)$ is independent of our choice of $F$ or the $m_1, \ldots, m_r$). As noted above, the $h_{n,v}(y)$ are the characteristic polynomials of $\sigma_q^{k_n(v)}$ on $M_n(v)$ and therefore, correspond to the $p_{n,v}(y)$ in Section 3. We further see that the $\tilde{h}_n(y)$ correspond to the polynomials $r_n(y)$ of Theorem 26 and by this theorem, we have the required congruence:

$$\tilde{h}_{n+1}(y) \equiv \tilde{h}_n(y) \pmod{\ell^n}. \qquad \square$$

## 3. On the convergence of a skew-abelian Iwasawa theoretic invariant

In this section, we prove a general, abstract result about the convergence of a certain cohomological invariant defined for a skew commutative Iwasawa algebra. The set up is as follows.

We fix an odd prime $\ell$ and positive integers $b, r$ throughout this section.[7] All cohomology groups in this section represent group cohomology unless indicated otherwise. All congruences in this paper are in $\mathbb{Z}_\ell$ (and hence only concerned with the $\ell$-adic valuation) unless explicitly mentioned otherwise.

Let $\Lambda = \mathbb{Z}_\ell[[T_1, \ldots, T_b]]$ be the $b$ dimensional Iwasawa algebra and set $t_i = 1 + T_i$. It is a local ring with maximal ideal $\mathfrak{m} = (\ell, T_1, \ldots, T_b)$. Note that for $\lambda \in \mathbb{Z}_\ell$, the expression

$$t_i^\lambda = (1 + T_i)^\lambda = \sum_{k \geq 0} \binom{\lambda}{k} T_i^k$$

converges in $\Lambda$. For $v = (v_1, \ldots, v_b) \in (\mathbb{Z}_\ell)^b$, we define $t^v = (t_1^{v_1}, \ldots, t_b^{v_b})$. We suppose that $\Lambda$ has an endomorphism $\sigma_q$ acting through a matrix $Q = Q_{ij} \in \mathrm{GL}_b(\mathbb{Z}_\ell)$ in the following way:

$$\sigma_q(t^v) = t^{Qv} \iff \sigma_q(T_i) = \left[\prod_j (1 + T_j)^{Q_{ji}}\right] - 1 \text{ for all } i.$$

[7] As usual, the arguments of this paper go through if $\ell = 2$ with minor, standard modifications.

We note that the action is well defined since $\sigma_q(T_i) \in \mathfrak{m}$. For $v \in \mathbb{Z}_\ell^b$, we denote the size of the orbit of $v$ under $Q$ in $(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^b$ by $k_n(v)$.[8] We also define

$$k_n = \min_{v \text{ primitive}} k_n(v).$$

**Assumption.** We suppose henceforth that $Q \equiv \mathrm{I} \pmod{\ell}$ and that $Q$ fixes no vectors.[9]

**Lemma 21.** *Let $v$ be a primitive vector. Then there exist integers $\alpha \geq 1$, $\beta_v \geq 0$ so that*

$$k_n(v) = \begin{cases} \ell^{n-\alpha-\beta_v} & \text{if } n \geq \alpha + \beta_v, \\ 1 & \text{otherwise.} \end{cases}$$

*Moreover, there is some (minimal) $\beta_0$ such that $\beta_v \leq \beta_0$ for all primitive $v$.*

*In particular, we have*

$$k_n = \begin{cases} \ell^{n-\alpha-\beta_0} & \text{if } n \geq n_0 := \alpha + \beta_0, \\ 1 & \text{otherwise.} \end{cases}$$

*Proof.* Since $Q \equiv \mathrm{I} \pmod{\ell}$, we have $\log Q = \ell^\alpha X$ for $\alpha \geq 1$ with $X \in M_b(\mathbb{Z}_\ell)$ not divisible by $\ell$. Since $\ell \geq 3$,

$$(Q^m - \mathrm{I})v = \exp(m \log Q)v - v = m\ell^\alpha Xv + \frac{(m\ell^\alpha)^2}{2} X^2 v + \cdots .$$

Since $Q$ does not fix any vectors, $Xv \neq 0$ so let $\beta_v$ be the largest value such that $Xv \equiv 0 \pmod{\ell^{\beta_v}}$. We see that $k_n(v)$ is the smallest $m$ so that $(Q^m - \mathrm{I})v$ is divisible by $\ell^n$. Since $X^k v \equiv 0 \pmod{\ell^{\beta_v}}$ for any $k \geq 1$ too, the $\ell$-adic valuation of $(Q^m - \mathrm{I})v$ is determined by the leading term $m\ell^\alpha Xv$ so that

$$k_n(v) = \begin{cases} \ell^{n-\alpha-\beta_v} & \text{if } n \geq \alpha + \beta_v, \\ 1 & \text{otherwise.} \end{cases}$$

It remains to show that there is a uniform upper bound on $\beta_v$.

Let $\pi : \mathbb{Z}_\ell^b \to \mathbb{F}_\ell^b$ be the reduction map. The primitive vectors correspond to the subspace $\mathcal{P} = \pi^{-1}(\mathbb{F}_\ell^b - \{0\})$ which is a closed (and open) subset of $\mathbb{Z}_\ell^b$. Therefore $\mathcal{P}$ is compact and by continuity of multiplication by $X$,

$$X\mathcal{P} = \{Xv : v \in \mathcal{P}\} \subset \mathbb{Z}_\ell^b$$

is compact and closed too. By assumption on $Q$, $X\mathcal{P}$ does not contain 0 (since this would correspond to a fixed point of $Q$). This implies that $X\mathcal{P}$ is in fact bounded away from 0, i.e, there is some minimal $\beta_0$ so that the image of $X\mathcal{P}$ in $(\mathbb{Z}/\ell^{\beta_0+1}\mathbb{Z}_\ell)^b$ does not contain 0 so that $\beta_v \leq \beta_0$ for every primitive $v$ (and $\beta_0 = \beta_v$ for some primitive $v$). □

**Remark 22.** It is easy to see why we need to restrict to $v$ primitive and to $Q$ not having any fixed vectors. If $Qv = v$, then $k_n(v) = 1$ and if $v = \ell^s v_0$, then $k_n(v) = 1$ for $n \leq s$ which is an obstruction to a uniform bound on $n$.

[8] i.e., $Q^{k_n(v)} v \equiv v \pmod{\ell^n}$ and $k_n(v)$ is the least such positive integer.

[9] If $\ell = 2$, then we would need to assume that $Q \equiv 1 \pmod 4$.

**3.1.** ***A cohomological interpretation.*** Let $M$ be a free $\Lambda$ module of rank $r$ with a $\Lambda$-linear endomorphism $\Phi : M \to M$. Upon picking a basis $m_1, \ldots, m_r$ for $M$, we express $\Phi$ as a matrix $F(T_1, \ldots, T_b)$ with entries in $\Lambda$. We suppose that $\Phi$ skew commutes with $\sigma_q$ in the following sense:

$$\sigma_q \circ F = F(\sigma_q(T_1), \ldots, \sigma_q(T_b)) \circ \sigma_q.$$

Note that $\sigma_q$ acts on $\mathrm{GL}_r(\Lambda)$ through its action on $\Lambda$. This data of $M$ and the endomorphism $\Phi$ as above gives rise to an element $\eta$ in the nonabelian cohomology group $H^1(\mathbb{Z}\sigma_q, \mathrm{GL}_r(\Lambda))$ in the following way:

Given a $F$ as above, we can define a cocycle representative by $\eta(\sigma_q) = F \in \mathrm{GL}_r(\Lambda)$. A change of basis by a matrix $P \in \mathrm{GL}_r(\Lambda)$ corresponds to $F \to P(\sigma_q(T_1), \ldots, \sigma_q(T_b))FP^{-1}$ which is exactly the boundary action. Therefore, the cohomology class $\eta \in H^1(\mathbb{Z}\sigma_q, \mathrm{GL}_r(\Lambda))$ depends only on $(M, \Phi)$.

For a positive integer $n$ and $v = (v_1, \ldots, v_b) \in \mathbb{Z}_\ell^b$, note that since $T_i = \zeta_{\ell^n}^{v_i} - 1$ is in the maximal ideal of $\mathbb{Z}_\ell[\zeta_{\ell^n}]$, we can define the quotient

$$\Lambda_n(v) = \frac{\mathbb{Z}_\ell[\![T_1, \ldots, T_b]\!]}{(t_1 = \zeta_{\ell^n}^{v_1}, \ldots, t_b = \zeta_{\ell^n}^{v_b})}.$$

We note that $\sigma_q^{k_n(v)}$ fixes the ideal $(t_1 - \zeta_{\ell^n}^{v_1}, \ldots, t_b - \zeta_{\ell^n}^{v_b}) \subset \mathbb{Z}_\ell[\![T_1, \ldots, T_b]\!]$ and thus descends to an endomorphism of $\Lambda_n(v)$.

Henceforth, we fix $\eta \in H^1(\mathbb{Z}\sigma_q, \mathrm{GL}_r(\Lambda))$, $v \in \mathbb{Z}_\ell^b$ and define the following sequence of invariants (implicitly depending on $\eta$) taking values in polynomials in one variable:

$$p_{n,-}(y) : v \in H^1(\mathbb{Z}\sigma_q, \mathrm{GL}_r(\Lambda)) \xrightarrow{\text{restriction}} H^1(\mathbb{Z}\sigma_q^{k_n(v)}, \mathrm{GL}_r(\Lambda_n(v))) \xrightarrow{\text{char poly}} \Lambda_n(v)[y] \ni p_{n,v}(y)$$

where for the first map, we restrict along $\mathbb{Z}\sigma_q^{k_n(v)} \subset \mathbb{Z}\sigma_q$ and push forward along the quotient $\mathrm{GL}_r(\Lambda) \to \mathrm{GL}_r(\Lambda_n(v))$ and for the second map, since $\sigma_q^{k_n(v)}$ acts trivially on $\mathrm{GL}_r(\Lambda_n(v))$, we have

$$H^1(\mathbb{Z}\sigma_q^{k_n(v)}, \mathrm{GL}_r(\Lambda_n(v))) = \mathrm{Hom}(\mathbb{Z}\sigma_q^{k_n(v)}, \mathrm{GL}_r(\Lambda_n(v)))/\text{conjugacy} = \mathrm{GL}_r(\Lambda_n(v))/\text{conjugacy}$$

which shows that the characteristic polynomial is a well defined invariant. Tracing through the definition in terms of the value of $F = \eta(\sigma_q)$ for $\eta \in H^1(\mathbb{Z}\sigma_q, \mathrm{GL}_r(\Lambda))$, $p_{n,v}(y)$ has the following explicit formula. For $v \in \mathbb{Z}_\ell^b$, we denote $F(t_1 = \zeta_{\ell^n}^{v_1}, \ldots, t_b = \zeta_{\ell^n}^{v_b})$ by $F(\zeta_{\ell^n}^{v})$ and define

$$A_n(v) := F(\zeta_{\ell^n}^{Q^{k_n(v)-1}v}) \cdots F(\zeta_{\ell^n}^{v}) = \prod_{i=1}^{k_n} F(\zeta_{\ell^n}^{Q^{-i}v}) \tag{6}$$

where we implicitly use that $Q^{k_n(v)}v \equiv v \pmod{\ell^n}$ for the second equality. The characteristic polynomial of $A_n(v)$ is exactly

$$p_{n,v}(y) = \det(\mathrm{I} - yA_n(v)).$$

Equivalently, it is the characteristic polynomial of $\sigma_q^{k_n(v)}$ acting on $\Lambda_n(v)$.

As the main results of this section, we will prove two $\ell$-adic convergence results regarding the sequence of polynomials $p_{n,v}(y)$ as $n \to \infty$.

**Theorem 23.** *Suppose that $Q = q\,\mathrm{I}$ is a scalar matrix. For $n$ sufficiently large so that $k_{n+1} = \ell k_n$, the characteristic polynomials satisfy the congruence*

$$p_{n+1,v}(y) \equiv p_{n,v}(y) \pmod{k_{n+1}}.$$

**Remark 24.** Unfortunately, this strong congruence is not true in general if $Q$ is not scalar (even if $r = 1$) as the following example shows. Take $\ell = 5$, $q_1 = 6$, $q_2 = 11$ and let $Q$ be the diagonal matrix with entries $q_1, q_2$. Take $F(t_1, t_2) = 1 + t_1^3 t_2$ and $v = (1, 1) \in \mathbb{Z}_\ell^2$. Computation shows that $A_3(v) = 49$, $A_2(v) = 7$ so that the difference is only divisible by 7 and not $k_3 = 49$ as the above theorem would suggest. Nevertheless, the computational evidence also suggests that the $A_n(v)$ still converge, just with a slower rate of convergence. As we will see in Remark 32, this will be related to the vanishing of certain sums of roots of unity.

For our geometric applications, the following statement is sufficient. Recall that $\mathcal{P}((\mathbb{Z}/\ell^n\mathbb{Z})^b)$ denotes the space of primitive vectors. It is acted upon by $Q$ and we denote a set of representatives for the orbits of $Q^{\mathbb{Z}}$ acting on $\mathcal{P}((\mathbb{Z}/\ell^n\mathbb{Z})^b)$ by $\mathcal{P}((\mathbb{Z}/\ell^n\mathbb{Z})^b)/\sim$. For $v' = Qv$, we note that $p_{n,v} \equiv p_{n,v'}$ so that $p_{n,v}$ is independent of the choice of representative. The following polynomial depends only on the class $\eta$.

**Definition 25.** With $A_n(v)$ and $p_{n,v}$ as before, define

$$r_n(y) := \prod_{v \in \mathcal{P}((\mathbb{Z}/\ell^n\mathbb{Z})^b)/\sim} p_{n,v}(y^{k_n(v)/k_n}).$$

**Theorem 26.** *Let $Q$ be any matrix in the kernel of $\mathrm{GL}_b(\mathbb{Z}_\ell) \to \mathrm{GL}_b(\mathbb{F}_\ell)$. For $n \geq n_0$ so that $k_{n+1} = \ell k_n$, We have*

$$r_{n+1}(y) \equiv r_n^{\ell^{b-1}}(y) \pmod{\ell^n}.$$

*If $Q = q\,\mathrm{I}$, we have the stronger congruence*

$$r_{n+1}(y) \equiv r_n^{\ell^{b-1}}(y) \pmod{\ell^{nb}}.$$

**Remark 27.** When $b = 1$, the two bounds agree since all matrices are scalar! Note that Theorem 23 only implies the following weaker congruence for $b = 1$:

$$r_{n+1}(y) \equiv r_n(y) \pmod{k_{n+1}}.$$

**Remark 28.** Numerical evidence shows that these congruences are in fact sharp and the bounds in Theorems 23 and 26 are realized in most cases (but not always!). For instance, with $r = 1$, $b = 2$, $\ell = 3$ and $Q = (1 + \ell^2)\,\mathrm{I}$ a scalar matrix, the computation

$$A_3\left(\frac{1}{1-\ell}, \frac{1}{1-\ell}\right) - A_2\left(\frac{1}{1-\ell}, \frac{1}{1-\ell}\right) = 70\ell$$

shows the sharpness of Theorem 23. The same example also shows the sharpness of part 2 of Theorem 26. Let $d \geq 1$ and $\tau_3, \tau_2 \in \mathbb{Z}_\ell$ so that $r_3(y) = 1 - \tau_3 y + \cdots$ and $r_2^\ell(y) = 1 - \tau_2 y + \ldots$. Then

$$\tau_3 - \ell\tau_2 = 560\ell^4.$$

Both the theorems above will depend on the following generalization of Fermat's little theorem to matrices to deal with the case when $r \geq 1$. This generalization of Fermat's little theorem can be seen as the degenerate case of Theorem 23 when $F(T_1, \dots, T_b) = F_0$ is constant in the $T_i$.

**3.2. *A generalization of Fermat's little theorem to matrices.*** In this subsection we state and prove a generalization of Fermat's little theorem to the case of matrices. As noted in the introduction, this generalization was conjectured by Arnold [2006] and proved by Zarelua [2008] (and many other following works). Our proof is short and apparently new and therefore we present it here.[10]

**Theorem 29** (Arnold and Zarelua). *Let $A \in M_r(\mathbb{Z}_\ell)$. Then*

$$\operatorname{tr} A^{\ell^{n+1}} \equiv \operatorname{tr} A^{\ell^n} \pmod{\ell^{n+1}}.$$

*In fact, we also have*

$$\det(1 - xA^{\ell^{n+1}}) \equiv \det(1 - xA^{\ell^n}) \pmod{\ell^{n+1}}.$$

*Proof.* We fix a $n$. Since we are proving a congruence modulo $\ell^{n+1}$, we can replace $A$ by a $r \times r$ matrix with nonnegative integer entries. Let $G$ be the directed multigraph with adjacency matrix $A$, i.e it has $r$ vertices labeled from 1 to $r$ and there are $a_{ij}$ many edges from $i$ to $j$.

A closed path of length $n$ on the graph corresponds to a sequence of edges $e_1, \dots, e_{n-1}$ such that the in-vertex of $e_{i+1}$ is the out-vertex of $e_i$ and the path starts and ends at the same vertex. The quantity $\operatorname{tr} A^n$ has the graph theoretic interpretation of being the number of closed paths of length $n$ on $G$.

Now, consider a closed path $P$ of length $\ell^{n+1}$. The cyclic group of order $\ell^{n+1}$ acts on the path by permuting

$$(e_1, \dots, e_{n-1}) \to (e_2, \dots, e_{n-1}, e_1).$$

Since we are working modulo $\ell^{n+1}$, we can ignore those paths $P$ where the orbit by this action has size $\ell^{n+1}$. The remaining paths $P$ are exactly those which are concatenations of $\ell$ copies of a path of length $\ell^n$. These are exactly counted by $\operatorname{tr}(A^{\ell^n})$ and therefore we have shown the required congruence

$$\operatorname{tr}(A^{\ell^{n+1}}) \equiv \operatorname{tr}(A^{\ell^n}) \pmod{\ell^{n+1}}.$$

To prove the corresponding congruence for characteristic polynomials, we use the well known determinant to trace exponential identity (as formal power series in $x$)

$$\det(1 - xB) = \exp\left(-\sum_{d \geq 1} \frac{\operatorname{tr}(B^d)x^d}{d}\right). \tag{7}$$

Let $d = d_0\ell^e$ for $d_0$ coprime to $\ell$. The congruence above on powers of $A^{d_0}$ then implies that

$$\operatorname{tr}(A^{d\ell^{n+1}}) \equiv \operatorname{tr}(A^{d\ell^n}) \pmod{d\ell^{n+1}}.$$

Since $\ell > 2$, $\alpha \equiv \beta \pmod{\ell^n}$ for $n \geq 1$ implies that $\exp(\alpha) \equiv \exp(\beta) \pmod{\ell^n}$.

[10] In the course of writing this paper, we found essentially the same proof by Qiaochu Yuan in a blog post from 2009.

To see this, let $t \in \mathbb{Z}_\ell$ such that $\ell^n \mid t$. We will show that $e^t \equiv 1 \pmod{\ell^n}$. Supposing this, we see that

$$\alpha \equiv \beta \pmod{\ell^n} \Longrightarrow e^{\alpha-\beta} \equiv 1 \pmod{\ell^n} \Longrightarrow e^{\alpha} \equiv e^{\beta} \pmod{\ell^n}$$

since $e^\beta \in \mathbb{Z}_\ell[\![x]\!]$ in our case.

To show that $e^t \equiv 1 \pmod{\ell^n}$, we argue by cases. The terms appearing in the Taylor expansion of $\exp(t)$ are of the form $t^r/r!$. If $r=1$, then $\ell^n \mid t$. In general, Legendre's formula shows that $t^r/r$ is divisible by $\ell^{\delta_{n,r}}$ for $\delta_{n,r} := nr - r/(\ell-1)$. For $r \geq 2$, note that

$$\delta_{n,r} \geq n \Longleftarrow nr - \frac{r}{2} - n \geq 0 \Longleftrightarrow 2n \geq \frac{r}{r-1} \text{ which is always true for } n \geq 1.$$

We finish our proof now by noting that the congruences on the traces implies (by the exponential identity)

$$\det(1 - xA^{\ell^{n+1}}) \equiv \det(1 - xA^{\ell^n}) \pmod{\ell^{n+1}}. \qquad \square$$

**3.3.** ***A proof of the main congruences.*** In this subsection, we prove Theorems 23 and 26. It will help to set up some notation and make some easy reductions first.

Recall that $F(T_1, \dots, T_b)$ is a power series in the $T_i$ and to define $A_{n+1}(v)$, we are required to evaluate $F$ at $T_i = \zeta_{\ell^{n+1}}^{v_i} - 1$ (for $i = 1, \dots, b$) which is in the maximal ideal for the local ring $\mathbb{Z}_\ell[\zeta_{\ell^{n+1}}]$. Since we are interested in a congruence modulo $k_{n+1}(v)$ (or $k_{n+1}$), we can truncate the $F$ at some finite degree $d$ so that $(\zeta_{\ell^{n+1}} - 1)^d \equiv 0 \pmod{k_{n+1}(v)}$ and suppose that it is a polynomial in the $t_i = T_i + 1$ of the form

$$F = \sum_{I \in \mathbb{N}^b} F_I t_1^{i_1} \cdots t_b^{t_b}$$

where the $F_I$ are $r \times r$ matrices over $\mathbb{Z}_\ell$.

Let $\rho \geq 1$ and for a tuple $J = (I_1, \dots, I_\rho) \in (N^b)^\rho$, we define $F_J = \prod_{j=1}^{\rho} F_{I_j}$. Using the standard notation $\langle \cdot, \cdot \rangle$ for inner products (and considering $\mathbb{N}^b \subset \mathbb{Z}_\ell^b$), we also define the linear form

$$\lambda_J(v) = \sum_{j=1}^{\rho} \langle I_j, Q^{-j} v \rangle.$$

In terms of this notation, we see that

$$A_{n+1}^d(v) = \sum_{J \in (N^b)^{dk_{n+1}(v)}} F_J \zeta_{\ell^{n+1}}^{\lambda_J(v)}$$

where we have implicitly used that $Q^{k_{n+1}(v)} v \equiv v \pmod{\ell^{n+1}}$. We denote cyclic permutations by

$$\tau(J) = (I_2, I_3, \dots, I_\rho, I_1)$$

and if $k_n(v) \mid \rho$, we note that

$$\lambda_{\tau J}(v) \equiv \lambda_J(Qv) \pmod{\ell^n}. \tag{8}$$

**Notation 30.** We will argue by considering each tuple along with its cyclic permutations. To that end, we fix some notation that we will use repeatedly. Let $K = (I_1, \dots, I_\rho)$ be a tuple of length $\rho$ such that it is nonperiodic.[11] For any $\delta = r\rho \in \mathbb{N}$, we define $J_K(\delta) = (I_1, \dots, I_\delta) := (K, \dots, K)$ to be the tuple of length $\delta$ where $K$ is concatenated to itself $r$ times. We suppose that $r = r_0\ell^s$ with $r_0$ coprime to $\ell$.

We need one more lemma (which will in fact control the rate of congruence) before the proof of Theorem 23.

**Lemma 31.** *For $n \geq 0$, suppose $\rho$ is an integer multiple of $k_n$. For any $w \in \mathbb{Z}_\ell$,*

$$S_{\rho,n}(w) := \sum_{i=1}^{\rho} \zeta_{\ell^n}^{q^i w} \equiv 0 \pmod{\rho}.$$

*Proof.* Let $w = \ell^m w_0$ with $w_0$ a unit. Since $q^{k_n} \equiv 1 \pmod{\ell^n}$ and $\rho/k_n \in \mathbb{Z}$, we see that

$$S_{\rho,n}(w) = \sum_{i=1}^{\rho} \zeta_{\ell^{n-m}}^{q^i w_0} = \frac{\rho}{k_{n-m}} S_{k_{n-m},n-m}(w_0)$$

where we use the convention that $\zeta_{-m} = 1$ if $m \geq 0$. Therefore, we can suppose that $w$ is a unit and $\rho = k_n$ without loss of generality. Let $\log q = \ell^\alpha x$ with $x$ a unit so that $q^i - 1 = i\ell^\alpha x \pmod{\ell^{\alpha+1}}$. We now have two cases to consider. Either $\alpha \geq n$ in which case $\zeta_{\ell^n}^{q^i w} = \zeta_{\ell^n}^{w}$ and

$$S_{\rho,n}(w) = \rho\zeta_{\ell^n}^{w} \equiv 0 \pmod{\rho}$$

or $\alpha < n$. In this second case, note that the $\zeta_{\ell^n}^{q^i w}$ are all pairwise distinct for $i \leq k_n = \ell^{n-\alpha}$.

If $1 \leq j < i \leq \ell^{n-\alpha}$, then

$$i - j < \ell^{n-\alpha} \Longrightarrow \zeta_{\ell^n}^{(q^i - q^j)w} = \zeta_{\ell^n}^{(i-j)w\ell^\alpha x + \cdots} \neq 1.$$

In fact, the $\zeta_{\ell^n}^{q^i w}$ are a complete set of roots for the polynomial $z^{\ell^{n-\alpha}} = \zeta_{\ell^\alpha}^{w}$ and $S_{\rho,n}(w)$ is equal to the linear term of this polynomial which is 0 thus completing the proof. □

*Proof of Theorem 23.* For this proof, recall that $Q = q\,\mathrm{I}$ is a scalar matrix so that $k_n(v) = k_n$ for all primitive $v$. We reduce the congruence on the characteristic polynomials $p_{n,v}$ to a congruence on traces using the exponential identity (7)

$$p_{n,v}(y) = \exp\left(-\sum_{d \geq 0} \mathrm{tr}(A_n^d(v))\frac{y^d}{d}\right)$$

as in the proof of Theorem 29. Upon fixing $n$ such that $k_{n+1} = \ell k_n$, it suffices to show the congruence

$$t_n := \mathrm{tr}(A_{n+1}^d(v)) - \mathrm{tr}(A_n^d(v)) \equiv 0 \pmod{dk_{n+1}}.$$

[11] i.e., the tuples $\tau^i J$ are pairwise distinct for $1 \leq i < \rho$.

We will consider the contributions to $t_n$ from each tuple and its cyclic permutations. In the notation of Notation 30, we take $\delta = dk_{n+1}$ and $J = J_K(dk_{n+1})$ and if $\ell \mid r$, $J_0 = J_K(dk_n)$. Note that

$$\lambda_J(v) = \sum_{i=1}^{\rho} \langle I_i, q^{-i}(1+q^{-\rho}+\cdots+q^{-(r-1)\rho})v\rangle = \frac{q^{-r\rho}-1}{q^{-\rho}-1}\lambda_K(v).$$

Since $q^i - 1 = i\log(q) + \frac{1}{2}(i\log(q))^2 + \cdots$ is exactly divisible by $i\log(q)$, there exists some $w \in \mathbb{Z}_\ell$ so that

$$\frac{q^{-r\rho}-1}{q^{-\rho}-1} = \frac{\ell^s\rho}{\rho} w = \ell^s w \Longrightarrow \lambda_J(v) = \ell^s w \lambda_K(v). \tag{9}$$

Moreover, there exists some $y \in \mathbb{Z}_\ell$ so that $q^{-dk_n} \equiv 1 + \ell^n y \pmod{\ell^{n+1}}$ and therefore

$$\sum_{i=1}^{\ell-1} q^{-idk_n} \equiv \ell + \ell^n y \sum_{i=0}^{\ell-1} i \equiv \ell + \ell^{n+1} y \frac{\ell-1}{2} \pmod{\ell^{n+1}} \Longrightarrow \lambda_J(v) \equiv \ell\lambda_{J_0}(v) \pmod{\ell^{n+1}}. \tag{10}$$

We now have to consider two cases:

*First, suppose* $s = 0$. In this case, the only contributions from tuples that are repetitions of $K$ and its cyclic permutations comes from $\operatorname{tr}(A^d_{n+1}(v))$ and is of the form

$$\sum_{i=1}^{\rho} \operatorname{tr}(F_{\tau^i J})\zeta_{\ell^{n+1}}^{\lambda_{\tau^i J}(v)} = \operatorname{tr}(F_J)\sum_{i=1}^{\rho}\zeta_{\ell^{n+1}}^{\lambda_J(q^i v)} = \operatorname{tr}(F_J)\sum_{i=1}^{\rho}\zeta_{\ell^{n+1}}^{q^i w\lambda_K(v)}$$

where for the first equality, we use that the trace is invariant under cyclic permutations and (8) while for the second equality, we use (9) above and that $s = 0$ by assumption. Now, $r\rho = dk_{n+1}$ and since $r$ is coprime to $\ell$, $k_{n+1}$ being a $\ell$-power necessarily divides $\rho$. In fact, $\rho$ and $dk_{n+1}$ have the same $\ell$-adic valuation. Thus, we can apply Lemma 31 to conclude

$$\sum_{i=1}^{\rho} \operatorname{tr}(F_{\tau^i J})\zeta_{\ell^{n+1}}^{\lambda_{\tau^i J}(v)} \equiv 0 \pmod{\rho} \Longleftrightarrow \sum_{i=1}^{\rho} \operatorname{tr}(F_{\tau^i J})\zeta_{\ell^{n+1}}^{\lambda_{\tau^i J}(v)} \equiv 0 \pmod{dk_{n+1}}.$$

*Next, suppose* $s > 0$. In this case, we will have contributions from both $\operatorname{tr}(A^d_{n+1}(v))$ and $\operatorname{tr}(A^d_n(v))$ and they are of the form

$$\begin{aligned}\sum_{i=1}^{\rho} \operatorname{tr}(F_{\tau^i J})\zeta_{\ell^{n+1}}^{\lambda_{\tau^i J}(v)} - \sum_{i=1}^{\rho} \operatorname{tr}(F_{\tau^i J_0})\zeta_{\ell^{n}}^{\lambda_{\tau^i J_0}(v)} &= (\operatorname{tr}(F_K^r) - \operatorname{tr}(F_K^{r/\ell}))\sum_{i=1}^{\rho}\zeta_{\ell^n}^{\lambda_J(q^i v)} \\ &= (\operatorname{tr}(F_K^r) - \operatorname{tr}(F_K^{r/\ell}))\sum_{i=1}^{\rho}\zeta_{\ell^{n+1}}^{q^i\ell^s w\lambda_K(v)} \\ &\equiv 0 \pmod{r\rho = dk_{n+1}}\end{aligned}$$

where the first equality follows from invariance of trace under cyclic permutations and (10) while the second equation follows from (9). For the last congruence, Theorem 29 implies that

$$\operatorname{tr}(F_K^r) - \operatorname{tr}(F_K^{r/\ell}) \equiv 0 \pmod{r}.$$

Moreover, since $dk_{n+1} = r\rho$, we see that $\rho$ is divisible by $dk_{n+1}\ell^{-s}$ and in particular by $k_{n+1-s}$. Therefore, we can apply Lemma 31 to conclude

$$\sum_{i=1}^{\rho} \zeta_{\ell^{n+1-s}}^{q^i w \lambda_K(v)} \equiv 0 \pmod{\rho}. \qquad \square$$

**Remark 32.** We remark that the failure of this proof for the general case (see Remark 24) happens exactly at Lemma 31. If $Q$ is not scalar, it is no longer true that $\lambda_J(Qv) = Q\lambda_J(v)$ and consequently, there exist examples (with $\lambda$ a linear form) such that

$$S_n(\lambda; v) := \sum_{j=1}^{k_n(v)} \zeta_{\ell^n}^{\lambda(Q^{-j}v)} \not\equiv 0 \pmod{k_n(v)}.$$

Nevertheless, the above proof shows that if the $S_n(\lambda_J; v) \to 0$ as $n \to \infty$, then the characteristic polynomials $p_{n,v}(y)$ will also converge as $n \to \infty$. If $\lambda_J(\log(Q)v) \neq 0$, a variation of Lemma 31 still applies to $S_n(\lambda_J; v)$. In fact, numerical evidence supports the vanishing of the limit (for $\lambda_J$ an arbitrary linear form) but we do not know how to prove it.

From now on, we again let $Q \equiv \mathrm{I} \pmod{\ell}$ be a general matrix. We recall some notation before the proof of Theorem 26. We let $V = \mathbb{Z}_\ell^b$ be a free $\mathbb{Z}_\ell$ module, $V_n = V/\ell^n V$, $\mathcal{P}(V_n)$ to be the primitive vectors in $V_n$ and $\mathcal{P}(V_n)/\sim$ to be a set of representatives under the action by $Q$. The characteristic polynomials we are interested in are

$$r_n(y) = \prod_{v \in \mathcal{P}((\mathbb{Z}/\ell^n\mathbb{Z})^b)/\sim} p_{n,v}(y^{k_n(v)/k_n}).$$

We also fix $n$ sufficiently large and define (in the notation of Lemma 21)

$$V_e = \left\{ v \in V : \frac{k_n(v)}{k_n} \;\middle|\; \ell^e \iff \beta_v \geq \beta_0 - e \iff Xv \equiv 0 \pmod{\ell^{\beta_0 - e}} \right\} \subset V.$$

By the last equivalent condition, we see that $V_e$ is a (nonempty) submodule of $V$. Since $Q$ commutes with $\log(Q)$ and hence also $X$, we see that $Q$ preserves $V_e$. When $Q = q\,\mathrm{I}$, $V_e = V$ since $\beta_v = \beta_0$ for all primitive $v$. Also define $V_{e,n}$ to be the image of $V_e$ in $V/\ell^n V$ under the reduction map. Note that, in general, $V_e \not\cong (\mathbb{Z}/\ell^n\mathbb{Z})^c$ for some $c$ and is only a-priori a finite $\mathbb{Z}/\ell^n\mathbb{Z}$ module.

So, let $M$ be an arbitrary finite $\mathbb{Z}_\ell$ module and $n \geq 0$ be the smallest value such that $\ell^n M = 0$. An element $v \in M$ is said to be primitive (generalizing our usual notion) when $\ell^{n-1}v \neq 0$ and the set of primitive elements is denoted $\mathcal{P}(M)$. Our two definitions of primitive are compatible in the sense that

$$\mathcal{P}(V_{e,n}) = \mathcal{P}(V/\ell^n V) \cap V_{e,n}.$$

We need one more lemma (analogous to Lemma 31 and also the determining factor for the rate of convergence) before the proof of Theorem 26.

**Lemma 33.** *Let $M$ be as above with*

$$\chi : M \to \bar{\mathbb{Z}}_\ell^\times$$

*a character. Then, we have the congruence*

$$\sum_{v \in \mathcal{P}(M)} \chi(v) \equiv 0 \pmod{\ell^{n-1}}.$$

*If $M = (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^b$, we have the stronger congruence*

$$\sum_{v \in \mathcal{P}(M)} \chi(v) \equiv 0 \pmod{\ell^{(n-1)b}}.$$

*Proof.* Let $|M| = m$, note that $S_M := \sum_{v \in M} \chi(v) \equiv 0 \pmod{m}$. There are two cases to consider: First, if $\chi$ is the trivial character, then $S_M = m$ and the congruence is clear. Second, if $\chi$ is not trivial, we can find some $m_0 \in M$ so that $\chi(m_0) \neq 1$ and $S_M = \chi(m_0) S_M \implies S_M = 0 \equiv 0 \pmod{m}$.

Define

$$N = \{v \in M : \ell^{n-1} v = 0\} \subset M$$

so that $\mathcal{P}(M) = M - N$. The module $M$ has size at least $\ell^n$ and the module $N$ has size at least $\ell^{n-1}$. Therefore, we have

$$\sum_{v \in \mathcal{P}(M)} \chi(v) = \sum_{v \in M} \chi(v) - \sum_{w \in N} \chi(w) = S_M - S_N \equiv 0 \pmod{\ell^{n-1}}$$

since $|M| \equiv |N| \equiv 0 \pmod{\ell^{n-1}}$.

If $M = (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^b$ so that $N = (\mathbb{Z}_\ell/\ell^{n-1}\mathbb{Z}_\ell)^b$, then the above argument shows the stronger congruence

$$\sum_{v \in \mathcal{P}(M)} \chi(v) = \sum_{v \in M} \chi(v) - \sum_{w \in N} \chi(w) = S_M - S_N \equiv 0 \pmod{\ell^{(n-1)b}}. \qquad \square$$

We now prove Theorem 26, along the same general lines as the proof of Theorem 23.

*Proof of Theorem 26.* By the exponential identity (7), we have

$$r_n(y) = \exp\Bigg( - \sum_{v \in \mathcal{P}(V/\ell^n V)/\sim} \sum_{f \geq 0} \frac{\operatorname{tr} A_n^f(v)}{f} y^{f k_n(v)/k_n} \Bigg).$$

Let us fix some $d = d_0 \ell^e$ (with $d_0$ coprime to $\ell$) and collect the terms corresponding to $y^d$ so that with

$$C_{d,n} = \sum_{v \in \mathcal{P}(V_{e,n})/\sim} \frac{k_n(v)}{d k_n} \operatorname{tr} A_n^{d k_n / k_n(v)}(v), \quad \text{we have } r_n(y) = \exp\Bigg( - \sum_{d \geq 0} C_{d,n} y^d \Bigg).$$

As in the proof of Theorem 29, the congruence

$$r_{n+1}(y) \equiv r_n^{\ell^{b-1}}(y) \pmod{\ell^n},$$

is reduced to the congruence

$$C_{d,n+1} \equiv \ell^{b-1} C_{d,n} \pmod{\ell^n}.$$

Since a representative $v \in \mathcal{P}(V_{e,n})/\sim$ represents $k_n(v)$ many vectors in $\mathcal{P}(V_{e,n})$ and $A_n(Qv)$ is conjugate to $A_n(v)$ so that their powers have the same traces, we can express $C_{d,n}$ as a sum over *all* primitive vectors by

$$C_{d,n} = \sum_{v \in \mathcal{P}(V_{e,n})} \frac{1}{dk_n} \operatorname{tr} A_n^{dk_n/k_n(v)}(v).$$

Therefore we are reduced to proving the congruence

$$t_n := \sum_{v \in \mathcal{P}(V_{e,n+1})} \frac{1}{dk_{n+1}} \operatorname{tr} A_{n+1}^{dk_{n+1}/k_{n+1}(v)}(v) - \sum_{v \in \mathcal{P}(V_{e,n})} \frac{\ell^b}{dk_{n+1}} \operatorname{tr} A_n^{dk_n/k_n(v)}(v) \equiv 0 \pmod{\ell^n}$$

where we have implicitly used the assumption that $n$ is sufficiently large so that $k_{n+1} = \ell k_n$. Since every vector in $\mathcal{P}(V_{e,n})$ has $\ell^b$ many lifts to $\mathcal{P}(V_{e,n+1})$, we also have

$$t_n = \frac{1}{dk_{n+1}} \sum_{v \in \mathcal{P}(V_{e,n+1})} \left( \operatorname{tr} A_{n+1}^{dk_{n+1}/k_{n+1}(v)}(v) - \operatorname{tr} A_n^{dk_n/k_n(v)}(v) \right).$$

Note that in the expansion

$$\operatorname{tr} A_n^{dk_n/k_n(v)}(v) = \sum_{J \in (\mathbb{N}^b)^{dk_n}} \operatorname{tr}(F_J) \zeta_{\ell^n}^{\lambda_J(v)},$$

the tuples all have size $dk_n$ independent of $v$. As before, we will argue by fixing a tuple $K$ and considering the contributions from tuples that are multiples of $K$ and their cyclic permutations. In the notation of Notation 30, let $J = J_K(dk_{n+1})$ and when $\ell \mid r$, $J_0 = J_K(dk_n)$.

*First, we suppose that* $s = 0$. In this case, the only contribution to $t_n$ from $K$ will be through $J$ and will be of the form

$$\frac{1}{dk_{n+1}} \sum_{v \in \mathcal{P}(V_{e,n+1})} \operatorname{tr}(F_J) \zeta_{\ell^{n+1}}^{\lambda_J(v)}.$$

We note that $\zeta_{\ell^{n+1}}^{\lambda_J(v)}$ is a character on $V_{e,n+1}$ and therefore, by Lemma 33, there exists some $T_{\lambda_J} \in \mathbb{Z}_\ell$ such that

$$\frac{1}{dk_{n+1}} \sum_{v \in \mathcal{P}(V_{e,n+1})} \operatorname{tr}(F_J) \zeta_{\ell^{n+1}}^{\lambda_J(v)} = \frac{\ell^n}{dk_{n+1}} T_{\lambda_J}.$$

Moreover, for any cyclic permutation $\tau^i J$ of $J$, the corresponding contribution is of the same form as before since $Q^i$ permutes $\mathcal{P}(V_{e,n+1})$

$$\frac{1}{dk_{n+1}} \sum_{v \in \mathcal{P}(V_{e,n+1})} \operatorname{tr}(F_{\tau^i J}) \zeta_{\ell^{n+1}}^{\lambda_J(Q^i v)} = \frac{1}{dk_{n+1}} \sum_{v \in \mathcal{P}(V_{e,n+1})} \operatorname{tr}(F_J) \zeta_{\ell^{n+1}}^{\lambda_J(v)} = \frac{\ell^n}{dk_{n+1}} T_{\lambda_J}.$$

Therefore, the contribution from all the cyclic permutations of $J$ is together equal to

$$\frac{\rho \ell^n}{dk_{n+1}} \operatorname{tr}(F_J) T_{\lambda_J} \equiv 0 \pmod{\ell^n}$$

since the $\ell$-adic valuation of $\rho$ is equal to the $\ell$-adic valuation of $dk_{n+1}$.

*Next, suppose* $s > 0$. In this case, the contribution from $K$ will be through $J$ and $J_0$. Since $v \in V_e$, $dk_{n+1}$ is divisible by $k_{n+1}(v)$ so that $Q^{-idk_n} v = v + i\ell^n Y v$ for some $Y \in M_b(\mathbb{Z}_\ell)$ and

$$(\mathrm{I} + Q^{-dk_n} + \cdots + Q^{-(\ell-1)dk_n})v = \ell v + i\ell^n \sum_{i=0}^{\ell-1} Y v = \ell v + \ell^{n+1}\frac{\ell-1}{2} Y v \equiv \ell v \pmod{\ell^{n+1}}.$$

This implies that

$$\lambda_J(v) = \sum_{i=1}^{dk_n} \langle I_i, q^{-i}(1 + Q^{-dk_n} + \cdots + Q^{-(\ell-1)dk_n})v\rangle \equiv \ell\lambda_{J_0}(v) \pmod{\ell^{n+1}}$$

which is equivalent to $\zeta_{\ell^{n+1}}^{\lambda_J(v)} = \zeta_{\ell^n}^{\lambda_{J_0}(v)}$. Therefore, the contribution from $J$, $J_0$ in $t_n$ is of the form

$$\frac{1}{dk_{n+1}}(\mathrm{tr}(F_k^r) - \mathrm{tr}(F_k^{r/\ell})) \sum_{v \in \mathcal{P}(V_{e,n+1})} \zeta_{\ell^{n+1}}^{\lambda_J(v)} = \frac{\ell^n}{dk_{n+1}}(\mathrm{tr}(F_k^r) - \mathrm{tr}(F_k^{r/\ell}))T_{\lambda_J}.$$

As above, the cyclic permutations of $K$ give rise to exactly the same contribution so that the total contribution from all cyclic permutations of $K$ is

$$\frac{\rho\ell^n}{dk_{n+1}}(\mathrm{tr}(F_k^r) - \mathrm{tr}(F_k^{r/\ell}))T_{\lambda_J} \equiv 0 \pmod{\ell^n}$$

since $(\mathrm{tr}(F_k^r) - \mathrm{tr}(F_k^{r/\ell}))$ is divisible by $r$ by Theorem 29 and $r\rho = dk_{n+1}$.

When $Q = q\,\mathrm{I}$, the proof is exactly the same as above except that we have the stronger congruence

$$\sum_{v \in \mathcal{P}(V_{e,n+1})} \mathrm{tr}(F_J)\zeta_{\ell^{n+1}}^{\lambda_J(v)} \equiv 0 \pmod{\ell^{nb}}.$$

This follows from the second part of Lemma 33 since $V_e = V = \mathbb{Z}_\ell^b$ in this case and $V_{e,n+1} = (\mathbb{Z}_\ell/\ell^{n+1}\mathbb{Z}_\ell)^b$. □

**Remark 34.** As one sees from the proof, the modulus of the congruence in Theorem 26 depends on the structure of $V_{e,n+1}$.

## 4. Explicit examples

In this section, we prove that the normalized eigenvalues of the characteristic polynomials $h_{n,v}(x)$ defined in the proof of Theorem 19 are independent of $n$ for $n$ sufficiently large in the following two examples:

- *Fermat Curves*: This is the family of curves defined by the equation

  $$C_n : x^{\ell^n} + y^{\ell^n} + z^{\ell^n} = 0 \subset \mathbb{P}^2.$$

  We have maps

  $$\cdots \to C_n \to C_{n-1} \to \cdots \to C_1 \cong \mathbb{P}^1$$

  with $G_n = \mathrm{Aut}(C_n/C_1) = (\mu_{\ell^n})^2$ and the element $(\zeta_1, \zeta_2)$ acts by $[x : y : z] \to [x\zeta_1 : y\zeta_2 : z]$.

- *Artin–Schreier Curves*: This is the family of curves defined by the projective closure of the equation

$$C_n : y^q - y = x^{\ell^n} \subset \mathbb{P}^2/\mathbb{F}_q.$$

  The automorphism group in this case is $G_n = \mathbb{F}_q \times \mu_{\ell^n}$. An element $(a, \zeta)$ in this group acts on the curve by $(x, y) \to (\zeta x, y + a)$.

**Remark 35.** The results of this section work in somewhat greater generality, for instance we don't need to restrict to Fermat or Artin–Schreier curves of degree a power of $\ell$. The results also work for various quotients of these curves such as the superelliptic curves $y^m = x^{\ell^n} + a$.

Since the computations in other cases are exactly analogous, we only deal with the above two cases.

Throughout this section, we identify characters $\chi : \mu_{\ell^n} \to \bar{\mathbb{Z}}_\ell$ with vectors $v \in \mathbb{Z}_\ell$ by $\chi(v) : \zeta_{\ell^n} \to \zeta_{\ell^n}^v$. We also fix a compatible family of additive characters $\psi_n : \mathbb{F}_{q^n} \to \bar{\mathbb{Z}}_\ell$ that satisfy $\psi_n = \mathrm{tr}(\mathbb{F}_{q^n}/\mathbb{F}_q) \circ \psi_1$.

In both of the above families of curves, we can decompose $M_n = H^1_{\text{ét}}(\bar{C}_n, \mathbb{Z}_\ell)$ into one dimensional eigenspaces $M_n(\chi)$ indexed by characters $\chi$ of $G_n$. In the Fermat curve case, the characters are naturally indexed by $v \in (\mathbb{Z}/\ell^n\mathbb{Z})^2$ while in the second case, the characters are indexed by $(\psi, v)$ where $\psi$ is an additive character of $\mathbb{F}_q$ and $v \in \mathbb{Z}/\ell^n\mathbb{Z}$.

Given a character $\chi : \mu_{\ell^n} \to \bar{\mathbb{Z}}_\ell$ and $q \equiv 1 \pmod{\ell^n}$, we can define a multiplicative character of $\mathbb{F}_q^\times$ since the map $x \to x^{(q-1)/\ell^n}$ induces a surjection

$$\mathbb{F}_q^\times \to \mu_{\ell^n}(\mathbb{F}_q) \cong \mu_{\ell^n}$$

and we compose this surjection with $\chi$. By a slight abuse of notation, we also denote this character by $\chi$.

The following well-known theorem [Katz 1981, Corollary 2.2 and Lemma 2.3] identifies the eigenvalues of the Frobenius $\sigma_q$ on $M(\chi)$ with Gauss and Jacobi sums respectively.

**Theorem 36.** *We assume that* $q \equiv 1 \pmod{\ell^n}$:

- *For the Fermat curves $C_n$, let $\eta = (\chi, \chi_2)$ be a character of $G_n = (\mu_{\ell^n})^2$. The eigenvalues of $\sigma_q$ on the eigenspace $M_n(\eta)$ are given by the Jacobi sum*

$$-J_q(\chi_1, \chi_2) = -\sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1 - x).$$

- *For the Artin–Schreier curves, let $\eta = (\psi, \chi)$ be a character of $G_n = \mathbb{F}_q \times \mu_{\ell^n}$. The eigenvalues of $\sigma_q$ on the eigenspace $M_n(\eta)$ are given by the Gauss sums*

$$-g_q(\psi, \chi) = -\sum_{x \in \mathbb{F}_q} \psi(x)\chi(x).$$

*Proof.* We sketch the proof for completeness. In the case of Fermat curves, we would like to count points on the affine curve $x^{\ell^n} + y^{\ell^n} = -1$ while in the case of Artin–Schreier curves, we would like to count points on $y^q - y = x^{\ell^n}$.

We have the identities

$$\sum_{\chi:\mathbb{F}_q^\times\to\mu_{\ell^n}} \chi(x) = \begin{cases} \ell^n & \text{if } x = y^{\ell^n}, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\sum_{\psi:\mathbb{F}_q\to\mu_q} \psi(x) = \begin{cases} q & \text{if } x = y^q - y, \\ 0 & \text{otherwise.} \end{cases}$$

We can use these identities to test if an element $x \in \mathbb{F}_q$ is a $\ell^n$-th power or of the form $y^q - y$ and therefore use it to count points.

For the Fermat curve, we have

$$C_n(F_q) = \sum_{z+w=-1} \sum_{\chi_1,\chi_2:\mathbb{F}_q^\times\to\mu_{\ell^n}} \chi_1(x)\chi_2(y)$$

while for Artin–Schreier curves

$$C_n(\mathbb{F}_q) = \sum_{z\in\mathbb{F}_q} \sum_{\psi,\chi} \psi(z)\chi(z).$$

Exchanging the summation, this shows that the point counts on the two curves can be expressed in terms of Jacobi and Gauss sums respectively. Finally, we use the Weil-conjectures to identify eigenvalues of the Frobenius action with Jacobi/Gauss sums by varying over all powers of $q$. □

Let us return to the set-up of Theorem 19. The roots of the characteristic polynomial $h_{n,v}(x)$ therefore correspond to $(-J_q(\chi_1,\chi_2))^{k_n} = -J_{q^{k_n}}(\chi_1,\chi_2)$ with $v$ corresponding to the character $\chi_1$, $\chi_2$ and similarly for the Gauss sum in the two cases we are interested in. Put another way, we choose the minimal $q$ so that $q-1$ is exactly divisible by $\ell^n$ and we are looking for a relation between these values for varying $n$.

Luckily, the exact statement we need is a result of Coleman [1987] proved using the $p$-adic Gamma function of Gross and Koblitz [1979]. Stated in our notation and specialized to our needs, [Coleman 1987, Theorem 11] takes the following form:

**Theorem 37** (Coleman). *Let $v \in \mathbb{Z}_\ell$, $q = p^f$ be such that $\ell^n$ exactly divides $q-1$. In the notation of the previous theorem, we have*

$$g_{q^\ell}(\psi, \chi_{q^\ell}(v)) = g_q(\psi, \chi_q(v))\chi_q(v)(\ell)c_q$$

*for $c_q = c_p^f$ and $c_p = (-1)^r p^{(\ell-1)/2}$ where $r$ depends only on $\ell$.*

*Proof.* In Theorem 11 of [loc. cit.], take $b = v/\ell^{n+1}$, $d = \ell$. Note that there is exactly one orbit of size $\ell$ and $c = (\sqrt{-p}^{\,\ell-1}\phi_d(0))^f$, $r = r_\ell + (\ell-1)/2$ in the notation of that paper. □

The following theorem is an immediate consequence of Coleman's theorem and is the required relation.

**Theorem 38.** *Suppose that $q$ is such that $\ell^n$ exactly divides $q-1$. Let $v_1, v_2 \in \mathbb{Z}_\ell$, $\chi_{q^m}(v_i)$ multiplicative characters of $\mu_{\ell^\infty}(\mathbb{F}_{q^m})$ corresponding to $v_i$ and $\psi_n : \mathbb{F}_{q^n} \to \bar{\mathbb{Z}}_\ell$ a compatible series of additive characters as above.*

*Then, we have the following identities*:

$$\frac{J_q(\chi_q(v_1), \chi_q(v_2))}{q^{1/2}} = \frac{J_{q^\ell}(\chi_{q^\ell}(v_1), \chi_{q^\ell}(v_2))}{q^{\ell/2}} \tag{11}$$

*and*

$$\frac{g_q(\psi, \chi_q(v))\chi_q(v)(\ell)}{q^{1/2}} = \frac{g_{q^\ell}(\psi, \chi_{q^\ell}(v))}{q^{\ell/2}}. \tag{12}$$

*Proof.* We first prove (11). We have the well known identity

$$J_q(\chi_1, \chi_2) g_q(\psi, \chi_1\chi_2) = g_q(\psi, \chi_1) g_q(\psi, \chi_2).$$

By Theorem 37, we then have

$$\begin{aligned}
J_{q^\ell}(\chi_{q^\ell}(v_1), \chi_{q^\ell}(v_2)) &= \frac{g_{q^\ell}(\psi, \chi_{q^\ell}(v_1)) g_{q^\ell}(\psi, \chi_{q^\ell}(v_2))}{g_{q^\ell}(\psi, \chi_1\chi_2)} \\
&= \frac{g_q(\psi, \chi_q(v_1)) g_q(\psi, \chi_q(v_2)) c_q}{g_q(\psi, \chi_1\chi_2)} \\
&= J_q(\chi_q(v_1), \chi_q(v_2)) c_q
\end{aligned}$$

where $q = p^f$. Since $c_q = \pm q^{(\ell-1)/2}$, we recover (11) *up to a sign* by dividing by $q^{\ell/2}$. Finally, upon reducing Theorem 23 $\pmod{\ell}$, we note that the normalized eigenvalues are all congruent $\pmod{\ell}$ and therefore the sign has to be $+1$.

Equation (12) follows in exactly the same manner from Theorem 37. □

**Remark 39.** We note that the above theorem is in exact accord with Case A, Theorem 19 since in the notation of that theorem, it shows that the roots of $h_{n+1}(y)$ are equal to the roots of $h_n(y)$. In other words, we not only have a congruence $h_{n+1}(y) \equiv h_n(y) \pmod{\ell^n}$, we have an equality $h_{n+1}(y) = h_n(y)$ in the two cases considered in this section.

## Acknowledgements

I would like to thank my advisor Jordan Ellenberg for posing a question that led to this paper, feedback on the writing of this paper and many other useful discussions, Douglas Ulmer for many helpful discussions and useful feedback on the writing of the paper, John Yin for helping with some computer calculations.

I am also very grateful to the anonymous referee for helpful expository suggestions and spotting an error in an earlier version of the proof of Lemma 12 and to Yifan Wei for helping me fix the error.

## References

[Anderson 1987] G. W. Anderson, "Torsion points on Fermat Jacobians, roots of circular units and relative singular homology", *Duke Math. J.* **54**:2 (1987), 501–561. MR Zbl

[Arnold 2006] V. I. Arnold, "On the matricial version of Fermat–Euler congruences", *Jpn. J. Math.* **1**:1 (2006), 1–24. MR Zbl

[Coleman 1987] R. F. Coleman, "The Gross–Koblitz formula", pp. 21–52 in *Galois representations and arithmetic algebraic geometry* (Kyoto, 1985/Tokyo, 1986), edited by Y. Ihara, Adv. Stud. Pure Math. **12**, North-Holland, Amsterdam, 1987. MR Zbl

[Gordon 1979] W. J. Gordon, "Linking the conjectures of Artin–Tate and Birch–Swinnerton-Dyer", *Compositio Math.* **38**:2 (1979), 163–199. MR Zbl

[Gross and Koblitz 1979] B. H. Gross and N. Koblitz, "Gauss sums and the $p$-adic $\Gamma$-function", *Ann. of Math.* (2) **109**:3 (1979), 569–581. MR Zbl

[Janichen 1921] W. Janichen, "Uber die Verallgemeinerung einer Gaussschen Formel aus der Theorie der hohern Kongruenzen", *Sitzungsber. Berlin. Math. Ges.* **20** (1921), 23–29. Zbl

[Katz 1981] N. M. Katz, "Crystalline cohomology, Dieudonné modules, and Jacobi sums", pp. 165–246 in *Automorphic forms, representation theory and arithmetic* (Bombay, 1979), Tata Inst. Fundam. Res. Stud. Math. **10**, Springer, 1981. MR Zbl

[Manin 1963] Y. I. Manin, "Theory of commutative formal groups over fields of finite characteristic", *Uspehi Mat. Nauk* **18**:6 (1963), 3–90. In Russian; translated in *Russ. Math. Surv.* **18** (1963), 1–83. MR Zbl

[Mazur and Petrenko 2010] M. Mazur and B. V. Petrenko, "Generalizations of Arnold's version of Euler's theorem for matrices", *Jpn. J. Math.* **5**:2 (2010), 183–189. MR Zbl

[Schur 1937] I. Schur, "Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung", *Compositio Math.* **4** (1937), 432–444. MR Zbl

[Zarelua 2008] A. V. Zarelua, "On congruences for the traces of powers of some matrices", *Tr. Mat. Inst. Steklova* **263** (2008), 85–105. MR Zbl

Communicated by Bjorn Poonen
Received 2022-03-30 Revised 2023-01-12 Accepted 2023-03-20

gasvinseeker94@gmail.com Department of Mathematics, University of Wisconsin-Madison, WI, United States

Algebra & Number Theory

msp.org/ant



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

The subscription price for 2023 is US $485/year for the electronic version, and $705/year (+$65, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

**mathematical sciences publishers**

**nonprofit scientific publishing**

http://msp.org/

# Algebra & Number Theory

Volume 17 No. 12 2023