ON A THEOREM OF TATE

FEDOR BOGOMOLOV AND YURI TSCHINKEL

Contents

1. Introduction

Let A be an abelian variety over a finite field k of characteristic p, and $A[\ell^n] \subset A(\bar{k})$ the subgroup of ℓ^n-torsion points on A. Let

$$T_\ell(A) := \varprojlim A[\ell^n], \;\; \ell \neq \mathrm{char}(k),$$

be the Tate module of A. It carries a natural action of the k-Frobenius automorphism. A classical theorem of Tate [6] linearizes the study of morphisms between abelian varieties defined over k:

$$\mathrm{Hom}_k(A, \tilde{A}) \otimes \mathbb{Z}_\ell = \mathrm{Hom}_{\mathbb{Z}[\mathrm{Fr}]}(T_\ell(A), T_\ell(\tilde{A})).$$

A far-reaching generalization of this result is the Tate conjecture, asserting algebraicity of *Tate classes*, i.e., ℓ-adic cohomology classes conformally invariant under the action of Frobenius.

In this note we provide an alternative condition for the existence of surjective morphisms between abelian varieties and, more generally, Tate classes in the cohomology of products of arbitrary algebraic varieties. It is formulated in terms of *divisibility* properties for the number of points over infinite sequences of finite field extensions.

Let X be a smooth projective algebraic variety of dimension d defined over k. Let

$$\mathfrak{F}_X := \cup_{i=1}^d \mathfrak{F}_{X,i},$$

Date: May 28, 2008.

where $\mathfrak{F}_{X,i} = \{\rho_{ij}\}$ is the set of Frobenius eigenvalues (roots of the characteristic polynomial) on the torsion-free part of the étale cohomology group $H^i_{et}(X, \mathbb{Z}_\ell)$. Let $\Gamma_X \subset \mathbb{C}^*$ be the multiplicative subgroup generated by $\mathfrak{F}_X$. Our main results are:

Theorem 1. *Let X, resp. $\tilde{X}$, be a smooth projective variety over a finite field k_1, resp. $\tilde{k}_1$. Let k_n/k_1, resp. $\tilde{k}_n/\tilde{k}_1$, be the unique extension of degree n. Assume that*

$$\#\tilde{X}(\tilde{k}_i) \mid \#X(k_i),$$

for infinitely many $n \in \mathbb{N}$. Then $\mathrm{char}(\tilde{k}_1) = \mathrm{char}(k_1)$ *and*

$$\Gamma_{\tilde{X}} \otimes \mathbb{Q} \subseteq \Gamma_X \otimes \mathbb{Q}. \tag{1.1}$$

Theorem 2. *Let X and $\tilde{X}$ be abelian varieties satisfying the conditions of Theorem 1. Then there exists a morphism $X \to \tilde{X}$, which induces the embedding* (1.1). *In particular, if* $\dim(X) = \dim(\tilde{X})$ *then X and $\tilde{X}$ are isogenous.*

Acknowledgments: The first author was partially supported by NSF grant DMS-0701578. The second author was partially supported by NSF grant DMS-0602333.

2. Recurrences and divisibility

A function $R : \mathbb{N} \to \mathbb{C}$ is called a *simple linear recurrence* if

$$R(n) = \sum_{\gamma \in \Gamma^0} c_\gamma \gamma^n,$$

where $c_\gamma \in \mathbb{C}^*$ and $\Gamma^0 \subset \mathbb{C}^*$ is a finite set of *roots* of R. Such a function satisfies a recurrence equation:

$$R(n+r) = \sum_{i=0}^{r-1} a_i R(n+i),$$

for some $a_i \in \mathbb{C}$ and all $n \in \mathbb{N}$.

Assume that the multiplicative group $\Gamma \subset \mathbb{C}^*$ generated by the set of roots Γ^0 is torsion-free. Fix a basis $\{\gamma_1, \dots, \gamma_r\}$ of Γ. Let $\mathbb{C}[\Gamma]$ be the corresponding algebra of Laurent polynomials, i.e., finite linear combinations of monomials $x^\gamma = \prod_{j=1}^r x_j^{g_j}$, where

$$\gamma = \sum_{i=1}^r g_i \gamma_i \in \Gamma.$$

Let $\mathfrak{R}_\Gamma$ be the ring of simple linear recurrences with roots in Γ. It is isomorphic to the unique factorization domain $\mathbb{C}[\Gamma]$ (see [2, Lemma 2.1]). The element in $\mathbb{C}[\Gamma]$ corresponding to a linear recurrence R will be denoted by F_R.

Lemma 3. *Assume that Γ is torsion-free. Let*

$$F(x) = \sum_{\gamma \in \Gamma_0} c_\gamma x^\gamma, \;\; \tilde{F}(x) = \sum_{\tilde{\gamma} \in \tilde{\Gamma}_0} \tilde{c}_{\tilde{\gamma}} x^{\tilde{\gamma}} \in \mathbb{C}[\Gamma]$$

be Laurent polynomials. Assume that

- *c_0 and $\tilde{c}_0$ are not equal to zero,*
- *$\tilde{F} \mid F$ in $\mathbb{C}[\Gamma]$.*

Then the $\mathbb{Q}$-subspace of $\Gamma \otimes \mathbb{Q}$ generated by $\tilde{\Gamma}_0$ is contained in the $\mathbb{Q}$-subspace generated by Γ_0.

Proof. Let $\Pi \subset \Gamma \otimes \mathbb{Q}$ be the $\mathbb{Q}$-subspace generated by $\gamma \in \Gamma_0$ and let $\bar{\Gamma} := \Pi \cap \Gamma$. Then F is a regular function on the torus $\mathsf{T} = \mathrm{Hom}(\Gamma, \mathbb{C}^*)$ which is lifted from the quotient torus $\bar{\mathsf{T}} = \mathrm{Hom}(\bar{\Gamma}, \mathbb{C}^*)$. In particular, F is constant on the fibers of projection $\mathsf{T} \to \bar{\mathsf{T}}$. The zero-divisor of $\tilde{F}$ is induced from $\bar{\mathsf{T}}$. Hence $\tilde{F}$ is a product of a unit in $\mathbb{C}[\Gamma]$ (a monomial) and an element of $\mathbb{C}[\bar{\Gamma}]$. Since both F and $\tilde{F}$ have nontrivial constant term it follows that $\tilde{F} \in \mathbb{C}[\bar{\Gamma}]$, contradiction. □

Lemma 4. [1, Lemma 6.2] *Assume that Γ is torsion-free and let $\gamma = \sum_{i=1}^r g_i \gamma_i$ be a primitive element in Γ, i.e., $\gcd(g_1, \dots, g_r) = 1$. Then $x^\gamma - \lambda$ is irreducible in $\mathbb{C}[\Gamma]$, for all $\lambda \in \mathbb{C}^*$. If γ, γ' generate a noncyclic subgroup in Γ then $x^\gamma - \lambda_\gamma$ and $x^{\gamma'} - \lambda_{\tilde{\gamma}}$ are coprime in $\mathbb{C}[\Gamma]$.*

Lemma 5. *Let R and $\tilde{R}$ be simple linear recurrences such that*

1. *$R(n), \tilde{R}(\tilde{n}) \neq 0$, for all sufficiently large positive integers $n, \tilde{n}$.*
2. *The subgroup $\Gamma \subset \mathbb{C}^*$ generated by the roots of R and $\tilde{R}$ is torsion-free.*
3. *There is a finitely-generated subring $\mathfrak{A} \subset \mathbb{C}$ with $R(n)/\tilde{R}(n) \in \mathfrak{A}$, for infinitely many $n \in \mathbb{N}$.*

Then

$$\begin{array}{rccc} Q : & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & R(n)/\tilde{R}(n) \end{array}$$

is a simple linear recurrence. In particular, $F_Q \in \mathbb{C}[\Gamma]$ and

$$F_Q \cdot F_{\tilde{R}} = F_R.$$

Proof. See [2, p. 434] and [1, Proposition 6.1]. □

More generally, let $\Gamma' \subset \mathbb{C}^*$ be any finitely-generated group. Fix a splitting $\Gamma' = \Gamma \oplus \mathbb{Z}/m$, where $\mathbb{Z}/m = \{\zeta_m^j\}$ is the group of m-th roots of 1. A simple linear recurrence R with roots in Γ' defines m Laurent polynomials $F_{R,j} \in \mathbb{C}[\Gamma]$. Indeed, each root has the form

$$\gamma' = \zeta_m^{d(\gamma')}\gamma, \quad \text{for some } d(\gamma') \in \mathbb{N},$$

and we have

$$R(n) = \sum_{\gamma'} c_{\gamma'}\zeta_m^{nd(\gamma')}\gamma^n.$$

Put

$$c_{\gamma,j} := c_{\gamma'}\zeta_m^{jd(\gamma')}$$

and

$$R_j := \sum_{\gamma} c_{\gamma,j}\gamma^n, \quad j = 1, \dots, m.$$

This gives rise m recurrences and corresponding elements in $\mathbb{C}[\Gamma]$. We have $R_j(n) = R(n)$, for $n \equiv j \mod m$. Lemma 5 can be extented to R and $\tilde{R}$ as follows:

Lemma 6. *Let R, $\tilde{R}$ be simple linear recurrences satisfying the conditions (1) and (3) of Lemma 5. Assume that the subgroup $\Gamma' \subset \mathbb{C}^*$ generated by the roots of R and $\tilde{R}$ has torsion $\mathbb{Z}/m$. Fix a presentation $\Gamma' = \Gamma \oplus \mathbb{Z}/m$. Then there exists a $j \in \{1, \dots, m\}$ and subrecurrences R_j, resp. $\tilde{R}_j$, such that*

$$\tilde{R}_j(n) \mid R_j(n)$$

for infinitely many n. In particular,

$$F_{\tilde{R}_j} \mid F_{R_j}$$

in $\mathbb{C}[\Gamma]$.

Proof. If suffices to observe that at least one of the congruence classes mod m contains infinitely many n such that $\tilde{R}(n) \mid R(n)$ and to apply Lemma 5. □

3. Weil numbers

Let $\mathbb{Q}(\zeta_\infty)$ be the cyclotomic field containing all roots of 1. Let

$$\mathcal{W}_p \subset \bar{\mathbb{Q}}^*$$

be the multiplicative group $\mathbb{Q}$-generated by all eigenvalues of a p-Frobenius on ℓ-adic cohomology ($\ell \neq p$) of *all* algebraic varieties over finite fields of characteristic p. In particular, it contains all rational powers of p. The group $\mathcal{W}_p$ has the following properties:

- $\mathbb{Q}(\zeta_\infty) \subseteq \mathcal{W}_p$;

- it is preserved under the action of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$;
- it is $\mathbb{Q}$-generated by p-Frobenius eigenvalues on cohomology of abelian varieties defined over $\bar{\mathbb{F}}_p$ (by Honda's theorem [4], [7]);
- an algebraic integer ω is in $\mathcal{W}_p$ if and only if for every embedding $\iota : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$ one has $|\omega| = p^r$, for some $r \in \mathbb{Q}$ [3].

Let $L/\mathbb{Q}$ be the (unique) nontrivial quadratic extension of the maximal totally-real extension of $\mathbb{Q}$. Then $L/\mathbb{Q}$ is normal, with Galois group $\mathcal{G} := \mathrm{Gal}(L/\mathbb{Q})$. Note that $\mathcal{G}$ acts on $\mathcal{W}_p$, for each p.

Proposition 7. *Let $\alpha \in \bar{\mathbb{Q}}$ be such that $|\iota(\alpha)| = 1$, for all embeddings $\iota : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Then it can be factored*

$$\alpha = \prod_p \omega_p, \qquad \text{with } \omega_p \in \mathcal{W}_p.$$

Moreover, this representation is unique, modulo multiplication by elements in $\mathbb{Q}(\zeta_\infty)$.

Proof. If α is an integer satisfying the assumption then it is a root of 1. If α admits a real embedding, then $\alpha = \pm 1$, and there is nothing to prove. Same holds for the Galois-conjugates of α. In particular, the field $K := \mathbb{Q}(\alpha)$ has no real embeddings and $2d := [K : \mathbb{Q}]$. For every $\iota : K \hookrightarrow \mathbb{C}$, we have $1/\iota(\alpha) = c_\iota(\alpha)$, where c_ι is the corresponding complex conjugate. Im $m := [K : \mathbb{Q}]$ then $\{1, \alpha, \ldots, \alpha^{m-1}\}$ is a basis of the m-dimensional $\mathbb{Q}$-vector space $K = \mathbb{Q}(\alpha)$ and the $\mathbb{Q}$-linear map $K \to K$ that sends a basis element α^i to α^{-i} is an automorphism of the field K that coincides with the complex conjugation for every field embedding $K \hookrightarrow \mathbb{C}$. Let K^0 be the totally real subfield of K whose elements are fixed by σ. Let $\mathcal{O}_K$ be the ring of integers in K. The group $\mathcal{O}_K^*/\mathcal{O}_{K^0}^*$ is 2-torsion, modulo roots of 1. Let h be the class number of K and $\mathrm{N}_{K/\mathbb{Q}}$ the norm map.

Choose an $n \in \mathbb{N}$ so that $n\alpha \in \mathcal{O}_K$. Since n/α and $n\alpha$ are Galois conjugated, it follows that $n/\alpha \in \mathcal{O}_K$. We have $|\iota(n\alpha)| = n$, for all ι. The principal $\mathcal{O}_K$-ideal $(n\alpha)$ has norm n^{2d}. Let p be a prime dividing n and write $n = p^m\tilde{n}$, with $p \nmid \tilde{n}$. Put

$$(n\alpha) = \mathfrak{q} \cdot \tilde{\mathfrak{n}},$$

where $\mathfrak{q}, \tilde{\mathfrak{n}}$ are coprime $\mathcal{O}_K$-ideals and $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{q}) = p^{2dm}$. We have

$$\mathfrak{q}^h = (\phi_p), \quad \tilde{\mathfrak{n}}^h = (\tilde{\nu}),$$

principal $\mathcal{O}_K$-ideals with integral generators ϕ_p, and $\tilde{\nu}$, respectively. We have

$$(n\alpha)^h(\sigma(n\alpha))^h = (\phi_p)(\sigma(\phi_p))(\tilde{\nu})(\sigma(\tilde{\nu}))$$

and

$$(p)^{4dmh}(\tilde{n})^h = (\phi_p)(\sigma(\phi_p))(\tilde{\nu})(\sigma(\tilde{\nu})),$$

with coprime p and $\tilde{n}$, resp. $(\phi_p)(\sigma(\phi_p))$ and $(\tilde{\nu})(\sigma(\tilde{\nu}))$. It follows that we can write (modulo roots of 1)

$$\phi_p^2\sigma(\phi_p)^2 = p^{8dmh} \cdot u^2,$$

where u is a unit in $\mathcal{O}_K$. We may assume that $u \in \mathcal{O}_{K^0}^*$ (after raising both sides of the equation to a sufficiently high 2 power, if necessary). In particular, u is fixed by σ, and c_ι for all ι. Put $\omega_p := \phi_p^2/u$. Then

$$\omega_p\sigma(\omega_p) = p^{8dmh}.$$

The same holds for $\iota(\omega_p)$, in all embeddings $\iota : K \hookrightarrow \mathbb{C}$. Thus ω_p is an algebraic integer such that $|\iota(\omega_p)| = p^{4dmh}$, i.e., a p-Weil number.

Continuing inductively (over the prime divisors of n), we obtain a finite product decomposition

$$n^{2h}\alpha^{2h} = \prod_p \omega_p,$$

modulo roots of 1, where each ω_p is a p-Weil number. Thus $\alpha \in \prod_p \mathcal{W}_p$, as claimed.

To show uniqueness, assume that there are distinct representations

$$\prod_p \omega_p = \prod_{\tilde{p}} \omega_{\tilde{p}}.$$

Since each $\mathcal{W}_p$ is a multiplicative group we can combine elements corresponding to the same p and obtain

$$\alpha_S := \prod_{p \in S} \omega_p = \prod_{\tilde{p} \in \tilde{S}} \omega_{\tilde{p}} =: \alpha_{\tilde{S}},$$

where $S, \tilde{S}$ are (nonempty) disjoint finite sets of primes. We can choose coprime $n_S, n_{\tilde{S}} \in \mathbb{N}$ (e.g., divisible only by primes in S, resp. $\tilde{S}$), such that both $n_S\alpha_S$ and $n_{\tilde{S}}\alpha_{\tilde{S}}$ are algebraic integers. Let $c_S, c_{\tilde{S}} \in \mathbb{N}$ be such that $c_S n_S - c_{\tilde{S}} n_{\tilde{S}} = 1$. It follows that α_S is also an algebraic integer, necessarily a root of 1. This proves uniqueness. □

4. Tate lattices

Let X be a smooth projective algebraic variety of dimension d over a finite field k of characteristic p. Let k_n/k be the unique extension of degree n. Then

$$\#X(k_n) = \mathrm{tr}(\mathrm{Fr}^n) = \sum_{i=1}^{d}(-1)^i c_{ij}\rho_{ij}^n,$$

where $c_{ij} \in \mathbb{C}^*$ and $\mathfrak{F}_{X,i} = \{\rho_{ij}\}$ is the set of eigenvalues of Fr on the étale cohomology $H^i_{et}(X, \mathbb{Q}_\ell)$, with $\ell \neq p$. We have $\#X(k_n) \neq 0$, for all $n \gg 0$. This gives a simple linear recurrence R_X as in Section 2.

Put $\mathfrak{F}_X := \cup_i \mathfrak{F}_{X,i}$ and let $\Gamma_X \subset \mathbb{C}^*$ be the multiplicative subgroup generated by $\mathfrak{F}_X$. This group was introduced and studied in [8]. It contains a cyclic subgroup $q^{\mathbb{Z}}$ generated by q (arising from the polarization). For $\gamma \in \mathfrak{F}_{X,i}$ define

$$\iota(\gamma) := q^i/\gamma \in \mathfrak{F}_{X,i}.$$

This involution extends to Γ_X. Let $\Lambda_X \subset \Gamma_X$ be the monoid generated by $\mathfrak{F}_X$. This monoid is preserved by the Galois group $\mathcal{G}$ of the nontrivial quadratic extension of the totally-real closure of $\mathbb{Q}$, in particular, by ι. The cone $\Lambda_{X,\mathbb{R}} \subset \Gamma_X \otimes \mathbb{R}$ is strictly convex, rational and polyhedral.

Lemma 8. *We have a natural isomorphism*

$$\Gamma_{X^n} \otimes \mathbb{Q} = \Gamma_X \otimes \mathbb{Q}.$$

Moreover,

$$\Lambda_X = \Lambda_{X^n}.$$

Theorem 9. *Let X and $\tilde{X}$ be smooth projective varieties over a finite field k_1, resp. $\tilde{k}_1$. Assume that*

$$\#\tilde{X}(\tilde{k}_n) \mid \#X(k_n)$$

for infinitely many $n \in \mathbb{N}$. Then $\mathrm{char}(k_1) = \mathrm{char}(\tilde{k}_1)$ *and*

$$\Gamma_{\tilde{X}} \otimes \mathbb{Q} \subseteq \Gamma_X \otimes \mathbb{Q}.$$

Proof. Let $\Gamma' \subset \mathbb{C}^*$ be the group generated by Frobenius eigenvalues on the cohomology of X and $\tilde{X}$. Applying Lemma 6 and considering n confined to an arithmetic progression, if necessary, we arrive at two recurrences R_X and $R_{\tilde{X}}$ such that

- the group Γ generated by the roots of R_X and $\tilde{R}_X$ is torsion-free;
- $R_{\tilde{X}}(n) = \#\tilde{X}(\tilde{k}_n) \mid \#X(k_n) = R_X(n)$, for infinitely many n.

By Lemma 5, we obtain the divisibility in $\mathbb{C}[\Gamma]$ of the corresponding Laurent polynomials

$$F_{\tilde{X}} \mid F_X.$$

Now we can apply Lemma 3.

Finally, if $p = \mathrm{char}(k_1) \neq \mathrm{char}(\tilde{k}_1)$ then the group $p^a \subset \mathbb{C}^*$, with $a \in \mathbb{Q}$, is contained in Γ_X but not in $\Gamma_{\tilde{X}}$, contradiction. □

Remark 10. Assume that $\Gamma_{\tilde{X}} \otimes \mathbb{Q} \subseteq \Gamma_X \otimes \mathbb{Q}$. Let $\gamma \in \Lambda_{\tilde{X}} \cap \Lambda_X$. Then there exist $m, i, j \in \mathbb{N}$ and classes $c_m \in H^i_{et}(X^m, \mathbb{Z}_\ell)$, $\tilde{c}_m \in H^i_{et}(\tilde{X}^m, \mathbb{Z}_\ell)$, both with eigenvalue γ^j. Let $\iota(\tilde{c}_m) \in H^i_{et}(\tilde{X}^m, \mathbb{Z}_\ell)$ be a cohomology class with eigenvalue q^i/γ^j.

The classes c_m and $\iota(\tilde{c}_m)$ define minimal Frobenius-invariant $\mathbb{Z}_\ell$-subspaces in the corresponding cohomology groups. The tensor product of these subspaces in $H^{2i}_{et}(X^m \times \tilde{X}^m, \mathbb{Z}_\ell)$ contains a nontrivial subspace of Tate classes.

5. Abelian varieties

In this section we prove Theorem 2, following an argument in [1].

Let A be an abelian variety of dimension g defined over a finite field k_1 of characteristic p, and let $\{\rho_j\}_{j=1,\dots,2\mathsf{g}}$ be the set of eigenvalues of Frobenius on $H^1_{et}(A, \mathbb{Q}_\ell)$, for $\ell \neq p$. Let k_n/k_1 be the unique extension of degree n. The sequence

$$R(n) := \#A(k_n) = \prod_{j=1}^{2\mathsf{g}} (\rho_j^n - 1). \tag{5.1}$$

is a simple linear recurrence. Assume that the group $\Gamma' \subset \mathbb{C}^*$ generated by $\{\rho_j\}_{j=1,\dots,2\mathsf{g}}$ has torsion of order m. Choose a splitting $\Gamma' = \Gamma \oplus \mathbb{Z}/m$ as in Section 2, with Γ torsion-free. Let R_j be a subrecurrence as in Lemma 6. The corresponding Laurant polynomial has the form

$$F_{R_j} = \prod_{u=1}^{2\mathsf{g}} (z_u x^{\alpha_u} - 1),$$

where z_u are m-th roots of 1, and $\alpha_u \in \Gamma$. The ρ_j are q-Weil numbers, i.e., all Galois-conjugates have absolute value $\sqrt{q}$. Same holds for all x^{α_u}. Thus, for $u \neq u'$ we have either $\alpha_u = \alpha_{u'}$ or $\alpha_u, \alpha_{u'}$ generate a sublattice of rank 2 (since Γ is torsion-free). We get a subdivision of the sequence of α_u

$$\{\alpha_u\} = \sqcup_{s=1}^t I_s, \quad t \leq 2\mathsf{g},$$

into subsets of equal elements. Put $d_s = \#I_S$ and let $\alpha_s \in I_S$.

Theorem 11. *Let A and $\tilde{A}$ be abelian varieties of dimension g, respectively $\tilde{\mathsf{g}}$, over finite fields k_1, respectively $\tilde{k}_1$. Let R and $\tilde{R}$ be simple linear recurrences as in equation* (5.1)*. Assume that $\tilde{R}(n) \mid R(n)$ for infinitely many $n \in \mathbb{N}$. Then $\mathrm{char}(k_1) = \mathrm{char}(\tilde{k}_1)$ and there exists a morphism $A \to \tilde{A}$. In particular, if $\mathsf{g} = \tilde{\mathsf{g}}$ then A and $\tilde{A}$ are isogenous.*

Proof. Let $\Gamma' \subset \mathbb{C}^*$ be the group generated by $\{\rho_j\}_{j=1,\dots,2\mathsf{g}} \cup \{\tilde{\rho}_j\}_{j=1,\dots,2\tilde{\mathsf{g}}}$. Choose a splitting $\Gamma' = \Gamma \oplus \mathbb{Z}/m$ as in Section 2, with Γ torsion-free of rank r. Let R_j, resp. $\tilde{R}_j$ be subrecurrences as in Lemma 6, i.e.,

$R_j(n) = R(n)$ and $\tilde{R}_j = \tilde{R}(n)$ for infinitely many $n = j \mod m$. It follows that

$$F_{\tilde{R}_j} \mid F_{R_j} \quad \text{in } \mathbb{C}[\Gamma].$$

The Laurent polynomials have the form

$$F_{\tilde{F}_j} = \prod_{\tilde{s}=1}^{\tilde{t}} (z_{\tilde{s}} \prod_{i=1}^{r} x_i^{\tilde{a}_{i\tilde{s}}} - 1)^{d_{\tilde{s}}}, \quad F_{R_j} = \prod_{s=1}^{t} (z_s \prod_{i=1}^{r} x_i^{a_{is}} - 1)^{d_s},$$

where $z_s, z_{\tilde{s}}$ are some m-th roots of 1. Observe, that

$$\gcd(z_s \prod_{i=1}^{r} x_i^{a_{is}} - 1, z_{s'} \prod_{i=1}^{r} x_i^{a_{is'}} - 1) \in \mathbb{C}^*,$$

for $s \neq s'$, by Lemma 4. The same holds for $\tilde{R}$. We conclude that $\tilde{t} \leq t$, that we can order the indices so that $\#I_s \leq \#\tilde{I}_s$, for $s = 1, \dots, \tilde{t}$; and so that the multiplicative groups generated by $\alpha_s \in I_s$ and $\tilde{\alpha}_s \in \tilde{I}_s$ have rank 1, for each $s = 1, \dots, \tilde{t}$. For these s we have $\tilde{\alpha}_s = \alpha_s^u$, where $u \in \mathbb{Q}$ depends only on k_1 and $\tilde{k}_1$. It follows that there exists $N, \tilde{N} \in \mathbb{N}$ such that the $\tilde{N}$th power of each Frobenius eigenvalue of $\tilde{\mathrm{Fr}}$ is an Nth power of a Frobenius eigenvalue of Fr, with equal multiplicities of the corresponding eigenvalues. We get a homomorphism of Frobenius modules, and it suffices to apply Tate's Theorem to conclude that $A \to \tilde{A}$. □

Remark 12. This result can be made effective. Although we ask for divisibilty of infinitely many terms in the recurrence sequences, in fact, results in [2] imply that divisibility of *finitely many* terms, depending on $A, \tilde{A}$, will suffice. Actually, it suffices to bound from below greatest common divisors between finitely many elements of the recurrence sequences. Applications of these ideas to elliptic curves can be found in [5].

References

[1] Fedor Bogomolov, Michael Korotiaev, and Yuri Tschinkel. A torelli theorem for curves over finite fields. `arXiv:0802.3708`, 2008.

[2] Pietro Corvaja and Umberto Zannier. Finiteness of integral values for the ratio of two linear recurrences. *Invent. Math.*, 149(2):431–451, 2002.

[3] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[4] Taira Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20:83–95, 1968.

[5] Carlo Magagna. A lower bound for the r-order of a matrix modulo N. *Monatsh. Math.*, 153(1):59–81, 2008.

[6] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[7] John Tate. Classes d'isogénie des variétés abéliennes sur un corps fini, (d'aprés T. Honda). In *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*, Lecture Notes in Mathematics, Vol. 179, pages 95–110. Springer-Verlag, Berlin, 1971.

[8] Yuri G. Zarhin. Abelian varieties, l-adic representations and Lie algebras. Rank independence on l. *Invent. Math.*, 55(2):165–176, 1979.

Courant Institute, NYU, 251 Mercer Str., New York, NY 10012
E-mail address: `bogomolo@cims.nyu.edu`

Courant Institute, NYU, 251 Mercer Str., New York, NY 10012, and Mathematisches Institut, Bunsenstr. 3-5, 37073 Göttingen, Germany
E-mail address: `tschinkel@cims.nyu.edu`