Mirror Congruence For Rational Points On Calabi-Yau Varieties

Lei Fu
Institute of Mathematics, Nankai University, Tianjin, P. R. China
leifu@nankai.edu.cn

Daqing Wan
Department of Mathematics, University of California, Irvine, CA 92697
dwan@math.uci.edu

0. Introduction

One of the basic problems in arithmetic mirror symmetry is to compare the number of rational points on a mirror pair of Calabi-Yau varieties. At present, no general algebraic geometric definition is known for a mirror pair. But an important class of mirror pairs comes from certain quotient construction. In this paper, we study the congruence relation for the number of rational points on a quotient mirror pair of varieties over finite fields. Our main result is the following theorem:

Theorem 0.1. Let X_0 be a smooth projective variety over the finite field $\mathbf{F}_q$ with q elements of characteristic p. Suppose X_0 has a smooth projective lifting X over the Witt ring $W = W(\mathbf{F}_q)$ such that the W-modules $H^r(X, \Omega^s_{X/W})$ are free. Let G be a finite group of W-automorphisms acting on the right of X. Suppose G acts trivially on $H^i(X, \mathcal{O}_X)$ for all i. Then for any natural number k, we have the congruence

$$\#X_0(\mathbf{F}_{q^k}) \equiv \#(X_0/G)(\mathbf{F}_{q^k}) \pmod{q^k},$$

where $\#X_0(\mathbf{F}_{q^k})$ (resp. $\#(X_0/G)(\mathbf{F}_{q^k})$) denotes the number of elements of the sets of $\mathbf{F}_{q^k}$-rational points of X_0 (resp. X_0/G).

The main application of the above theorem is to Calabi-Yau varieties. This gives the following theorem announced in [W], which was the main motivation of the present paper.

Theorem 0.2. Let X_0 be a geometrically connected smooth projective Calabi-Yau variety of dimension n over the finite field $\mathbf{F}_q$ with q elements of characteristic p. Suppose X_0 has a smooth projective lifting X over the Witt ring $W = W(\mathbf{F}_q)$ such that the W-modules $H^r(X, \Omega^s_{X/W})$ are free. Let G be a finite group of W-automorphisms acting on the right of X. Suppose G fixes a non-zero n-form on X. Then for any natural number k, we have the congruence

$$\#X_0(\mathbf{F}_{q^k}) \equiv \#(X_0/G)(\mathbf{F}_{q^k}) \pmod{q^k}.$$

Proof. If X is a Calabi-Yau scheme over W of dimension n, then $H^i(X, \mathcal{O}_X) = 0$ for $i \neq 0, n$ and G acts trivially on them. If the generic fiber of X is geometrically connected, then G acts trivially on $H^0(X, \mathcal{O}_X)$. By Serre duality, $H^n(X, \mathcal{O}_X)$ is dual to $H^0(X, \Omega^n_{X/W})$. Since X is Calabi-Yau, $\Omega^n_{X/W}$ is a trivial invertible sheaf. In order for G to act trivially on $H^n(X, \mathcal{O}_{X/W})$, it suffices for G to fix a nonzero n-form. Theorem 0.2 thus follows from Theorem 0.1.

In particular, we have the following corollary:

Corollary 0.3. Let X_0 be the smooth $(n-1)$-dimensional hypersurface

$$x_0^{n+1} + \cdots + x_n^{n+1} + \lambda x_0 \cdots x_n = 0$$

in $\mathbf{P}^n_{\mathbf{F}_q}$, where $\lambda \in \mathbf{F}_q$. Let

$$G = \{(\zeta_0, \ldots, \zeta_n) | \zeta_i \in \mathbf{F}_q, \zeta_i^{n+1} = 1, \prod_{i=0}^{n} \zeta_i = 1\}.$$

Consider the action $G \times X_0 \to X_0$ defined by

$$(\zeta_0, \ldots, \zeta_n) \times [x_0 : \ldots : x_n] \mapsto [\zeta_0 x_0 : \ldots : \zeta_n x_n].$$

We have $\#X_0(\mathbf{F}_{q^k}) \equiv \#(X_0/G)(\mathbf{F}_{q^k}) \pmod{q^k}$ for any natural number k.

It is well known that the above hypersurface is Calabi-Yau. A G-equivariant nonzero $(n-1)$-form is $\frac{(-1)^i dx_0 \wedge \cdots \wedge \widehat{dx_i} \wedge \cdots \wedge dx_n}{1+\sum_{j\neq i} x_j^{n+1} - \lambda \prod_{j\neq i} x_j}$ on the affine space $x_i = 1$ of $\mathbf{P}^n$.

It is known that for the above hypersurface X_0, X_0/G is a strong singular mirror of X_0 if $(n+1)|(q-1)$. It is conjectured in [W] that for a strong mirror pair of Calabi-Yau varieties $\{X_0, X_0'\}$ over the finite field $\mathbf{F}_q$, we have $\#X_0(\mathbf{F}_{q^k}) \equiv \#X_0'(\mathbf{F}_{q^k}) \pmod{q^k}$ for any integer k. See [W] for a fuller discussion on this and other arithmetic mirror conjectures. In the situation of Theorem 0.2, if X/G is a singular mirror of X and if Y is a smooth crepant resolution of X/G, then the pair (X, Y) forms a strong mirror pair of smooth projective Calabi-Yau varieties. The congruence mirror conjecture in this case then reduces to showing the congruence

$$\#(X/G)(\mathbf{F}_{q^k}) \equiv \#Y(\mathbf{F}_{q^k}) \pmod{q^k}.$$

Another application of the theorem is to geometrically connected varieties with the property $H^i(X, \mathcal{O}_X) = 0$ for all $i \neq 0$. Again in this case, G acts trivially on $H^i(X, \mathcal{O}_X)$ for all i. Let $\overline{K}$ be the algebraic closure of the fraction field of $W = W(\mathbf{F}_q)$. By [E], if the l-adic cohomology group $H^i(X \otimes_W \overline{K}, \mathbf{Q}_l)$ satisfies the coniveau 1 condition for each $i \neq 0$, that is, if any cohomology class in $H^i(X \otimes_W \overline{K}, \mathbf{Q}_l)$ vanishes in $H^i(U, \mathbf{Q}_l)$ when restricted to some nonempty open $U \subset X \otimes_W \overline{K}$, then we have $H^i(X, \mathcal{O}_X) = 0$ for all $i \neq 0$. The converse is true if we assume the generalized Hodge conjecture. It turns out that in this case, we can prove a theorem stronger than Theorem 0.1. We don't need to assume X_0 can be lifted to W.

Theorem 0.4. Let X_0 be a smooth geometrically connected projective variety over the finite field $\mathbf{F}_q$. Suppose $H^i(X_0, \mathcal{O}_{X_0}) = 0$ for all $i \neq 0$. Then for any natural number k, we have

$$\#X_0(\mathbf{F}_{q^k}) \equiv 1 \pmod{q^k}.$$

Let G be a finite group of $\mathbf{F}_q$-automorphisms acting on the right of X_0. We have

$$\#(X_0/G)(\mathbf{F}_{q^k}) \equiv \#X_0(\mathbf{F}_{q^k}) \equiv 1 \pmod{q^k}.$$

The liftable condition in Theorem 0.1 cannot be dropped in general. However, if the order of G is prime to p, then the liftable condition can be dropped. This is given in the following general result of Berthelot-Bloch-Esnault, proved using their theory of Witt vector cohomology for singular varieties. In contrast, our method is based on crystalline cohomology and the Mazur-Ogus theorem.

Theorem 0.5 ([BBE]) Let X_0 be a proper scheme over $\mathbf{F}_q$, and G a finite group acting on X_0 so that each orbit is contained in an affine open subset of X_0. Suppose that the order of G is prime to the characteristic p and suppose that G acts trivially on $H^i(X_0, \mathcal{O}_{X_0})$ for all i. Then for any natural number k, we have the congruence

$$\#X_0(\mathbf{F}_{q^k}) \equiv \#(X_0/G)(\mathbf{F}_{q^k}) \pmod{q^k}.$$

Acknowledgements. The research of Lei Fu is supported by the Qiushi Science & Technologies Foundation, by the Fok Ying Tung Education Foundation, by the Transcentury Training Program Foundation, by the Project 973, and by the SRFDP. The research of Daqing Wan is partially supported by NSF. Part of this work is done while Lei Fu was visiting the University of California at Irvine. He would like to thank the Mathematics Department for its hospitality.

1. Proof of the Theorems

First we introduce some notations. For any smooth proper scheme X_0 over $\mathbf{F}_q$, let $H^i(X_0/W)$ be the crystalline cohomology group of X_0. It is a finitely generated module over the Witt ring $W = W(\mathbf{F}_q)$. Denote by $F : X_0 \to X_0$ the Frobenius correspondence, that is, it is the identity map on the underlying topological space of X_0, and it maps a section of $\mathcal{O}_{X_0}$ to its q-th power.

Let κ be a field and let Z be a scheme over κ. Denote by $|Z|$ the set of Zariski closed points in Z. For any $z \in |Z|$, define $\deg(z) = [k(z) : \kappa]$, where $k(z)$ is the residue field at z. Let $f : Z \to Z$ be a κ-endomorphism with isolated fixed points. Set

$$Z^f = \{z \in |Z| \,|\, f(z) = z \text{ and } f \text{ induces identity on } k(z)\},$$

and define

$$\Lambda(f) = \sum_{z \in Z^f} \deg(z).$$

Let κ' be a field extending κ and let $f' : Z \otimes_\kappa \kappa' \to Z \otimes_\kappa \kappa'$ be the base change of f. Then we have $\Lambda(f) = \Lambda(f')$.

Lemma 1.1. Let X_0 be a smooth projective variety over the finite field $\mathbf{F}_q$, let $g : X_0 \to X_0$ be an $\mathbf{F}_q$-automorphism of finite order, and let $K = \mathrm{Frac}W$ be the fraction field of $W = W(\mathbf{F}_q)$. Then $\mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K)$ and $\mathrm{Tr}(gF^k, H^i(X_0/W) \otimes_W K)$ are algebraic integers for any positive integer k and any i, and

$$\begin{aligned}
\Lambda(F^k) &= \sum_{i=0}^{2\mathrm{dim}X_0} (-1)^i \mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K), \\
\Lambda(gF^k) &= \sum_{i=0}^{2\mathrm{dim}X_0} (-1)^i \mathrm{Tr}(gF^k, H^i(X_0/W) \otimes_W K).
\end{aligned}$$

Proof. Let l be a prime number distinct from p. By Deligne's theorem ([D] 3.3.9), $\mathrm{Tr}(F^k, H^i(X_0 \otimes_{\mathbf{F}_q} \overline{\mathbf{F}}_q, \overline{\mathbf{Q}}_l))$ are algebraic integers. By the comparison theorem of Katz-Messing ([KM]), we have

$$\mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) = \mathrm{Tr}(F^k, H^i(X_0 \otimes_{\mathbf{F}_q} \overline{\mathbf{F}}_q, \overline{\mathbf{Q}}_l)).$$

So $\mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K)$ are algebraic integers. The formula for $\Lambda(F^k)$ follows from the Lefschetz fixed point formula in crystalline cohomology theory ([B] Théorème VII 3.1.9).

We will reduce the statements about gF^k to the corresponding statements for F^k. Suppose $g : X_0 \to X_0$ has finite order m. Let $X_1 = X_0 \times_{\mathrm{Spec}\mathbf{F}_q} \mathrm{Spec}\mathbf{F}_{q^m}$, and let $\varphi \in \mathrm{Gal}(\mathbf{F}_{q^m}/\mathbf{F}_q)$ be the Frobenius substitution. For any $\sigma \in \mathrm{Gal}(\mathbf{F}_{q^m}/\mathbf{F}_q)$, we have $\sigma = \varphi^k$ for some integer k uniquely determined modulo m. Define

$$f_\sigma : X_1 \to X_1$$

to be the isomorphism of schemes

$$f_\sigma = (\mathrm{id}_{X_0} \times \sigma^*) \circ (g^{-k} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}) : X_0 \times_{\mathrm{Spec}\mathbf{F}_q} \mathrm{Spec}\mathbf{F}_{q^m} \to X_0 \times_{\mathrm{Spec}\mathbf{F}_q} \mathrm{Spec}\mathbf{F}_{q^m}.$$

Note that f_σ is independent of the choice of k since g has order m. Since $g^{-k} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}$ is an $\mathbf{F}_{q^m}$-morphism of X_1, the following diagram commutes:

$$\begin{array}{ccc} X_1 & \stackrel{f_\sigma}{\to} & X_1 \\ \downarrow & & \downarrow \\ \mathrm{Spec}\mathbf{F}_{q^m} & \stackrel{\sigma^*}{\to} & \mathrm{Spec}\mathbf{F}_{q^m}. \end{array}$$

Moreover we have

$$f_\tau f_\sigma = f_{\sigma\tau}$$

for any $\sigma, \tau \in \mathrm{Gal}(\mathbf{F}_{q^m}/\mathbf{F}_q)$. By the theory of galois descent, ([S] Chapter V, No. 20, or Corollarie 7.7 in [SGA 1] Exposé VIII), there exists a scheme X_0' over $\mathrm{Spec}\mathbf{F}_q$ such that we have an $\mathbf{F}_{q^m}$-isomorphism

$$X_1 \cong X_0' \times_{\mathrm{Spec}\mathbf{F}_q} \mathrm{Spec}\mathbf{F}_{q^m}$$

and the following diagrams commute:

$$\begin{array}{ccc} X_1 & \stackrel{f_\sigma}{\to} & X_1 \\ \cong\downarrow & & \downarrow\cong \\ X_0' \times_{\mathrm{Spec}\mathbf{F}_q} \mathrm{Spec}\mathbf{F}_{q^m} & \stackrel{\mathrm{id}_{X_0'} \times \sigma^*}{\to} & X_0' \times_{\mathrm{Spec}\mathbf{F}_q} \mathrm{Spec}\mathbf{F}_{q^m}. \end{array}$$

For any scheme Z of characteristic p, let $F_Z : Z \to Z$ be the Frobenius correspondence, that is, F_Z is identity on the underlying topological space and the morphism of sheaves $F_Z^\sharp : \mathcal{O}_Z \to F_{Z*}\mathcal{O}_Z$ maps each section to its q-th power. On $X_1 = X_0 \times_{\mathrm{Spec}\mathbf{F}_q} \mathrm{Spec}\mathbf{F}_{q^m}$, we have

$$\begin{aligned} F_{X_1} &= (\mathrm{id}_{X_0} \times \varphi^*) \circ (F_{X_0} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}) = f_\varphi \circ (g \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}) \circ (F_{X_0} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}) \\ &= f_\varphi \circ (gF_{X_0} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}). \end{aligned}$$

Through the isomorphism $X_1 \cong X_0' \times_{\mathrm{Spec}\mathbf{F}_q} \mathrm{Spec}\mathbf{F}_{q^m}$, F_{X_1} is identified with $(\mathrm{id}_{X_0'} \times \varphi^*) \circ (F_{X_0'} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}})$. Moreover, the commutative diagram above shows that f_φ is identified with $\mathrm{id}_{X_0'} \times \varphi^*$. So the morphism $gF_{X_0} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}$ on $X_0 \times_{\mathbf{F}_q} \mathbf{F}_{q^m}$ is identified with the morphism $F_{X_0'} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}$ on $X_0' \times_{\mathrm{Spec}\mathbf{F}_q} \mathbf{F}_{q^m}$. So we have

$$\begin{aligned} & \mathrm{Tr}\Big(gF_{X_0} \times \mathrm{id}_{\mathbf{F}_{q^m}}, H^i\Big(X_0 \times_{\mathbf{F}_q} \mathbf{F}_{q^m}/W(\mathbf{F}_{q^m})\Big) \otimes_{W(\mathbf{F}_{q^m})} \mathrm{Frac}(W(\mathbf{F}_{q^m}))\Big) \\ = \; & \mathrm{Tr}\Big(F_{X_0'} \times \mathrm{id}_{\mathbf{F}_{q^m}}, H^i\Big(X_0' \times_{\mathbf{F}_q} \mathbf{F}_{q^m}/W(\mathbf{F}_{q^m})\Big) \otimes_{W(\mathbf{F}_{q^m})} \mathrm{Frac}(W(\mathbf{F}_{q^m}))\Big). \end{aligned}$$

By the base change theorem in crystalline cohomology theory ([B] Corollaire V 3.5.7), we have

$$\begin{aligned} & \mathrm{Tr}(gF_{X_0}, H^i(X_0/W) \otimes_W K) \\ = \; & \mathrm{Tr}\Big(gF_{X_0} \times \mathrm{id}_{\mathbf{F}_{q^m}}, H^i\Big(X_0 \times_{\mathbf{F}_q} \mathbf{F}_{q^m}/W(\mathbf{F}_{q^m})\Big) \otimes_{W(\mathbf{F}_{q^m})} \mathrm{Frac}(W(\mathbf{F}_{q^m}))\Big), \\ & \mathrm{Tr}(F_{X_0'}, H^i(X_0'/W) \otimes_W K) \\ = \; & \mathrm{Tr}\Big(F_{X_0'} \times \mathrm{id}_{\mathbf{F}_{q^m}}, H^i\Big(X_0' \times_{\mathbf{F}_q} \mathbf{F}_{q^m}/W(\mathbf{F}_{q^m})\Big) \otimes_{W(\mathbf{F}_{q^m})} \mathrm{Frac}(W(\mathbf{F}_{q^m}))\Big). \end{aligned}$$

So we have

$$\mathrm{Tr}(gF_{X_0}, H^i(X_0/W) \otimes_W K) = \mathrm{Tr}(F_{X_0'}, H^i(X_0'/W) \otimes_W K).$$

In particular, $\mathrm{Tr}(gF_{X_0}, H^i(X_0/W) \otimes_W K)$ are algebraic integers for all i. Moreover, we have

$$\begin{aligned} \Lambda(gF_{X_0}) &= \Lambda(gF_{X_0} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}) \\ &= \Lambda(F_{X_0'} \times \mathrm{id}_{\mathrm{Spec}\mathbf{F}_{q^m}}) \\ &= \Lambda(F'_{X_0}) \\ &= \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(F_{X_0'}, H^i(X_0'/W) \otimes_W K) \\ &= \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(gF_{X_0}, H^i(X_0/W) \otimes_W K). \end{aligned}$$

This proves the statements for gF. To prove the statements for gF^k, we use the base change from $\mathbf{F}_q$ to $\mathbf{F}_{q^k}$.

Lemma 1.2. Under the condition of Theorem 0.1, we have

$$\mathrm{Tr}(gF^k, H^i(X_0/W)\otimes_W K) \equiv \mathrm{Tr}(F^k, H^i(X_0/W)\otimes_W K) \pmod{q^k}$$

for all i.

Proof. Let $H^i = H^i(X_0/W)$. Recall that H^i can be identified with the de Rham cohomology of the lifting X of X_0 to $W = W(\mathbf{F}_q)$. (Confer [B] Théorème V 2.3.2). On H^i, we have the Hodge filtration

$$H^i = F^0H^i \supset F^1H^i \supset \cdots$$

and this filtration is G stable. By a result of Mazur (the property (8.2) on page 65 of [M]), we have

$$F(F^1H^i) \subset qH^i.$$

We have

$$H^i/F^1H^i = F^0H^i/F^1H^i \cong H^i(X, \mathcal{O}_X).$$

Choose a basis $\{e_1, \ldots, e_s\}$ of F^1H^i and extend it to a basis $\{e_1, \ldots, e_s, e_{s+1}, \ldots, e_{s+t}\}$ of H^i. Since $F^k(F^1H^i) \subset q^kH^i$, the matrix of F^k on H^i with respect to the above basis is of the form

$$\begin{pmatrix} q^kA & q^kB \\ C & D \end{pmatrix},$$

where A is an $s\times s$ matrix, B is an $s\times t$ matrix, C is a $t\times s$ matrix, and D is a $t\times t$ matrix. Since G acts trivially on $H^i/F^1H^i \cong H^i(X, \mathcal{O}_X)$ and G preserves the Hodge filtration, the matrix of $g\in G$ on H^i with respect to the above basis is of the form

$$\begin{pmatrix} P & O \\ Q & I \end{pmatrix},$$

where P is an $s\times s$ matrix, O is the $s\times t$ zero matrix, Q is a $t\times s$ matrix, and I is the $t\times t$ identity matrix. So the matrix of gF^k is

$$\begin{pmatrix} q^kA & q^kB \\ C & D \end{pmatrix}\begin{pmatrix} P & O \\ Q & I \end{pmatrix} = \begin{pmatrix} q^kAP + q^kBQ & q^kB \\ CP + DQ & D \end{pmatrix}.$$

We have

$$\mathrm{Tr}(gF^k, H^i) = \mathrm{Tr}(q^kAP + q^kBQ) + \mathrm{Tr}(D).$$

On the other hand, we have

$$\mathrm{Tr}(F^k, H^i) = \mathrm{Tr}(q^k A) + \mathrm{Tr}(D).$$

So we have

$$\mathrm{Tr}(gF^k, H^i) \equiv \mathrm{Tr}(F^k, H^i) \pmod{q^k}.$$

This finishes the proof of Lemma 1.2.

Lemma 1.3. Let X_0 be a quasi-projective scheme over $\mathbf{F}_q$, let G be a finite group acting on the right of X_0. Then for any natural number k, we have

$$\#(X_0/G)(\mathbf{F}_{q^k}) = \frac{1}{\#G} \sum_{g \in G} \Lambda(gF^k).$$

Proof. This result is well known. We include a proof here for completeness. Let $Y_0 = X_0/G$, and let $|X_0|$ (resp. $|Y_0|$) be the set of Zariski closed point in X_0 (resp. Y_0). For any $x \in |X_0|$, define the decomposition subgroup at x by

$$G_d(x) = \{g \in G | gx = x\}$$

and the inertia subgroup at x by

$$G_i(x) = \{g \in G_d(x) | g \text{ induces identity on the residue field } k(x) \text{ at } x\}.$$

Let y be the image of x in Y_0. By Proposition 1.1 in Exposé V of [SGA 1], we have an isomorphism

$$G_d(x)/G_i(x) \cong \mathrm{Gal}(k(x)/k(y)),$$

and for any $y \in |Y_0|$, there are exactly $\frac{\#G}{\#G_d(x)}$ Zariski closed points in X_0 above y and each of these closed points has degree $\deg(y)\frac{\#G_d(x)}{\#G_i(x)}$. We have

$$\begin{aligned}
\#Y_0(\mathbf{F}_{q^k}) &= \sum_{y \in |Y_0|,\, \deg(y)|k} \deg(y) \\
&= \frac{1}{\#G} \sum_{y \in |Y_0|,\, \deg(y)|k} \frac{\#G}{\#G_d(x)} \frac{\#G_d(x)}{\#G_i(x)} \#G_i(x) \deg(y) \\
&= \frac{1}{\#G} \sum_{y \in |Y_0|,\, \deg(y)|k} \sum_{x \in |X_0|,\, x \mapsto y} \deg(x) \#G_i(x).
\end{aligned}$$

Let $y \in |Y_0|$ be a Zariski closed point with $\deg(y)|k$, let $x \in |X_0|$ be a point above y, and let $\phi_y \in \mathrm{Gal}(k(x)/k(y))$ be the Frobenius substitution. Suppose $g \in G_d(x)$ and $g^{-1} \mapsto \phi_y^{\frac{k}{\deg(y)}}$ under the canonical homomorphism $G_d(x) \to \mathrm{Gal}(k(x)/k(y))$. Then $gF^k(x) = x$ and gF^k induces identity on $k(x)$. Conversely, if x is a Zariski closed point in X_0 such that $gF^k(x) = x$ and gF^k induces identity on $k(x)$, then $g \in G_d(x)$, $\deg(y)|k$, and $g^{-1} \mapsto \phi_y^{\frac{k}{\deg(y)}}$, where y is the image of x in Y_0. On the other hand, there are exactly $\#G_i(x)$ elements g in $G_d(x)$ such that $g^{-1} \mapsto \phi_y^{\frac{k}{\deg(y)}}$. So we finally get

$$\begin{aligned}
\#Y_0(\mathbf{F}_{q^k}) &= \frac{1}{\#G} \sum_{y\in|Y_0|,\ \deg(y)|k} \ \sum_{x\in|X_0|,\ x\mapsto y} \deg(x)\#G_i(x) \\
&= \frac{1}{\#G} \sum_{g\in G} \Lambda(gF^k).
\end{aligned}$$

This proves Lemma 1.3.

Now we are ready to prove Theorem 0.1. By Lemmas 1.3 and 1.1, we have

$$\begin{aligned}
\#(X_0/G)(\mathbf{F}_{q^k}) &= \frac{1}{\#G} \sum_{g\in G} \Lambda(gF^k) \\
&= \frac{1}{\#G} \sum_{g\in G} \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(gF^k, H^i(X_0/W) \otimes_W K).
\end{aligned}$$

By Lemmas 1.1 and 1.2, $\mathrm{Tr}(gF^k, H^i(X_0/W) \otimes_W K)$ and $\mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K)$ are algebraic integers, and

$$\mathrm{Tr}(gF^k, H^i(X_0/W) \otimes_W K) \equiv \mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) \pmod{q^k}.$$

From now on, we work over the integral closure of p-adic integers. Let $\mathrm{ord}_q(\#G) = c$, a non-negative rational number. For each $k \geq c$, we have

$$\begin{aligned}
\#(X_0/G)(\mathbf{F}_{q^k}) &= \frac{1}{\#G} \sum_{g\in G} \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(gF^k, H^i(X_0/W) \otimes_W K) \\
&\equiv \frac{1}{\#G} \sum_{g\in G} \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) \pmod{q^{k-c}}
\end{aligned}$$

$$
\begin{aligned}
&\equiv \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) \pmod{q^{k-c}} \\
&\equiv \#X_0(\mathbf{F}_{q^k}) \pmod{q^{k-c}}.
\end{aligned}
$$

Let $Z(X_0, T)$ and $Z(X_0, T)$ be the zeta-functions of X_0 and X_0/G, respectively. They are rational functions. Recall that we have

$$
\begin{aligned}
\frac{d}{dT} \log Z(X_0, T) &= \sum_{k=1}^{\infty} \#X_0(\mathbf{F}_{q^k}) T^{k-1}, \\
\frac{d}{dT} \log Z(X_0/G, T) &= \sum_{k=1}^{\infty} \#(X_0/G)(\mathbf{F}_{q^k}) T^{k-1}.
\end{aligned}
$$

Take a factorization

$$
\frac{Z(X_0, T)}{Z(X_0/G, T)} = \prod_{i=1}^{m} (1 - \alpha_i T)^{-n_i}, \ \alpha_i \neq 0
$$

where the α_i's are distinct and the n_i's are non-zero integers. Taking logarithmic derivative on both sides, we get

$$
\sum_{k=1}^{\infty} (\#X_0(\mathbf{F}_{q^k}) - \#(X_0/G)(\mathbf{F}_{q^k})) T^{k-1} = \sum_{i=1}^{m} \frac{n_i \alpha_i}{1 - \alpha_i T}.
$$

Using the congruence

$$
\#(X_0/G)(\mathbf{F}_{q^k}) \equiv \#X_0(\mathbf{F}_{q^k}) \pmod{q^{k-c}}
$$

for all $k \geq c$, one deduces that the above power series is p-adic analytic in the open disk $\mathrm{ord}_q(T) > -1$. This implies that each α_i satisfies $\mathrm{ord}_q(\alpha_i) \geq 1$, that is, each α_i is divisible by q. We conclude that

$$
\#X_0(\mathbf{F}_{q^k}) - \#(X_0/G)(\mathbf{F}_{q^k}) = \sum_{i=1}^{m} n_i \alpha_i^k \equiv 0 \pmod{q^k}.
$$

This finishes the proof of Theorem 0.1.

Let's prove Theorem 0.4. By Ogus' generalization of Mazur's theorem ([BO] Theorem 8.39), the Newton polygon of the Frobenius correspondence F on $H^i(X_0/W) \otimes_W$

K lies on or above the Hodge polygon of X_0. For any $i \neq 0$, we have $H^i(X_0, \mathcal{O}_{X_0}) = 0$. So the slope of each line segment on the Newton polygon is at least 1, that is, all the eigenvalues of F^k on $H^i(X_0/W) \otimes_W K$ are divisible by q^k (as p-adic integers). So we have

$$\mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) \equiv 0 \pmod{q^k}$$

for all $i \neq 0$. Since X_0 is geometrically connected, we have

$$\mathrm{Tr}(F^k, H^0(X_0/W) \otimes_W K) = 1.$$

So by Lemma 1.1, we have

$$\begin{aligned} \#X_0(\mathbf{F}_{q^k}) &= \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) \\ &\equiv 1 \pmod{q^k}. \end{aligned}$$

Now let G be a finite group acting on the right of X_0. For any $g \in G$, since g has finite order, the action of g on $H^i(X_0/W) \otimes_W K$ is diagonalizable and all its eigenvalues are roots of unity. Combining with the fact that F commutes with g, we see that all the eigenvalues of gF^k on $H^i(X_0/W) \otimes_W K$ are also divisible by q^k for any $i \neq 0$. So we have

$$\mathrm{Tr}(gF^k, H^i(X_0/W) \otimes_W K) \equiv \mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) \equiv 0 \pmod{q^k}$$

for all $i \neq 0$. Since X_0 is geometrically connected, we have

$$\mathrm{Tr}(gF^k, H^0(X_0/W) \otimes_W K) = \mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) = 1.$$

Again let $\mathrm{ord}_q(\#G) = c$. For each $k \geq c$, by Lemmas 1.1, 1.3, and the above discussion, we have

$$\begin{aligned} \#(X_0/G)(\mathbf{F}_{q^k}) &= \frac{1}{\#G} \sum_{g \in G} \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(gF^k, H^i(X_0/W) \otimes_W K) \\ &\equiv \frac{1}{\#G} \sum_{g \in G} \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) \pmod{q^{k-c}} \\ &\equiv \sum_{i=0}^{2\dim X_0} (-1)^i \mathrm{Tr}(F^k, H^i(X_0/W) \otimes_W K) \pmod{q^{k-c}} \\ &\equiv \#X_0(\mathbf{F}_{q^k}) \pmod{q^{k-c}}. \end{aligned}$$

As in the proof of Theorem 0.1, this implies that

$$\#(X_0/G)(\mathbf{F}_{q^k}) \equiv \#X_0(\mathbf{F}_{q^k}) \pmod{q^k}.$$

This finishes the proof of Theorem 0.4.

References.

[B] P. Berthelot, *Cohomologie Cristalline des Schémas de Carastéristique* $p > 0$, Lecture Notes in Mathematics 407, Springer-Verlag 1974.

[BO] P. Berthelot and A. Ogus, *Notes on Crystalline Cohomology*, Princeton University Press 1978.

[BBE] P. Berthelot, S. Bloch and H. Esnault, *On Witt vector cohomology for singular varieties*, preprint, October, 2005.

[D] P. Deligne, *La Conjecture de Weil II*, Publ. Math., IHES, 52(1980), 137-252.

[E] H. Esnault, *Deligne's Integrality Theorem in Unequal Characteristic and Rational Points over Finite Fields*, Ann. Math., to appear.

[KM] N. Katz and W. Messing, *Some Consequences of the Riemann Hypothesis for Varieties over Finite Fields*, Invent. Math., 23(1974), 73-77.

[S] J.-P. Serre, *Algebraic Groups and Class Fields*, translation of the French edition, Springer-Verlag, 1988.

[SGA 1] A. Grothendieck, *Revêtements Étales et Groupe Fondamental*, Lecture Notes in Mathematics 224, Springer-Verlag (1971).

[W] D. Wan, *Mirror Symmetry for Zeta Functions*, arXiv:math.AG/0411464, 21 Nov 2004. To appear in Mirror Symmetry V.