REDUCTION OF MODULAR JACOBIANS AT THE BAD PRIME

SREEKAR M. SHASTRY

Abstract. The goal of these notes is to show that $\mathcal{J}^0 \otimes \mathbb{F}_p$ is a torus and to describe the action of Frobenius on it, where $\mathcal{J}$ is the Néron model over $\mathbb{Z}$ of the modular Jacobian $J_0(p)_{\mathbb{Q}}$.

1. Integral models of modular curves

1.1 Let $M_0(N)_{\mathbb{Z}[1/N]}$ be the "compactified coarse moduli scheme" associated to the problem of classifying pairs (E, C) where E is an elliptic curve over a $\mathbb{Z}[1/N]$–scheme and C is a cyclic étale subgroup scheme of order N. It is a smooth proper curve over $\mathbb{Z}[1/N]$ with geometrically connected fibers. One knows that $M_0(1) \simeq \mathbb{P}^1_{\mathbb{Z}}$ is "the j–line." There is a natural map $M_0(N)_{\mathbb{Z}[1/N]} \longrightarrow M_0(1)_{\mathbb{Z}[1/N]}$ gotten by forgetting the cyclic subgroup. We define $M_0(N)_{\mathbb{Z}}$ to be the normalization of $M_0(1)$ in $M_0(N)_{\mathbb{Z}[1/N]}$. Now we define $X_0(N)$ to be the minimal regular proper model of $M_0(N)$ over $\mathbb{Z}$—it is the unique scheme which is regular, proper, and flat over $\mathbb{Z}$ with generic fiber $M_0(N)_{\mathbb{Q}}$ such that for any other regular and proper scheme $\mathcal{C}$ flat over $\mathbb{Z}$ with generic fiber $M_0(N)_{\mathbb{Q}}$, the birational map $\mathcal{C} \longrightarrow X_0(N)$ is a morphism; cf. [4]. See Figure 1. We will not need $X_0(N)$ in the sequel.

Henceforth, we take N to be a prime number p. We have the following description of $M_0(p)$:

1.2 Theorem. *(a) $M_0(p)$ is smooth over $\mathbb{Z}$ away from the supersingular points in characteristic p.*

(b) $M_0(p)_{\mathbb{F}_p}$ is the union of two copies of $M_0(1)_{\mathbb{F}_p} = \mathbb{P}^1_{\mathbb{F}_p}$ crossing transversally at the supersingular points. Hence $M_0(p)$ has semi–stable reduction at p.

(c) Let $x = j(E)$ be a supersingular point in $M_0(1)(\overline{\mathbb{F}}_p)$. Then x on the first copy of $M_0(1)_{\overline{\mathbb{F}}_p}$ is glued to $x^{(p)}$ on the second copy. In fact, if we let w be the involution $(E, C) \mapsto (E/C, E[p]/C)$, $\Phi : M_0(1) \to M_0(p)$ be $E \mapsto (E, \ker(F : E \to E^{(p)}))$, and c be the contraction map $(E, C) \mapsto c(E)$ that forgets C and contracts into nodal cubics (=1–gons) those geometric fibers of E which are n–gons ($n > 1$), we have

$$\begin{tikzcd}
M_0(1)_{\mathbb{F}_p} \arrow[dr, "\Phi"] & & M_0(1)_{\mathbb{F}_p} \arrow[dl, "w\Phi"'] \\
& M_0(p)_{\mathbb{F}_p} \arrow[dl, "c"'] \arrow[dr, "cw"] & \\
M_0(1)_{\mathbb{F}_p} & & M_0(1)_{\mathbb{F}_p}
\end{tikzcd}$$

with Φ and $w\Phi$ closed immersions whose images are the two irreducible components of $M_0(p)_{\mathbb{F}_p}$.

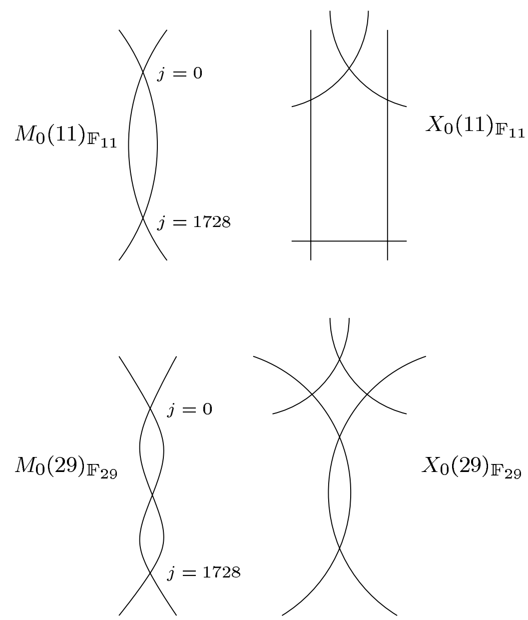

FIGURE 1. Special fibers of integral models and their minimal regular proper models.

(d) Let $x = j(E) \in M_0(p)(\overline{\mathbb{F}}_p)$ be a supersingular point (in fact all such are rational over $\mathbb{F}_{p^2}$; see [9], 12.5.4), and put $k := \frac{1}{2}\#\mathrm{Aut}E$. Then $X_0(p)_{\mathbb{F}_p}$ is obtained by gluing copies of $M_0(1)_{\mathbb{F}_p}$ at corresponding supersingular points as above, and then replacing a crossing by $k-1$ projective lines.

(e) The arithmetic genus of $M_0(p)_{\mathbb{F}_p}$ is

$$\#\{\text{supersingular } x \in M_0(1)(\overline{\mathbb{F}}_p)\} - 1.$$

See [5], pp. 144–148.

2. Review of the relative Picard functor

2.1 Fix $\pi : X \longrightarrow S$. Let

$$\mathrm{Pic}_{X/S} := R^1\pi_*\mathbb{G}_m$$

with respect to the fppf topology on S. It is the sheafification of the functor $P_{X/S}$ which associates to an S–scheme T the group $H^1(T, \mathscr{O}_T^\times)$. More concretely, if $\pi : X \longrightarrow S$ is proper, flat, finitely presented, has geometrically connected fibers, and we are given a section $\varepsilon : S \longrightarrow X$ then $\mathrm{Pic}_{X/S}(T)$ is the set of isomorphism classes of pairs $(\mathscr{L}, \lambda)$ such that $\mathscr{L}$ is an invertible sheaf on X_T and $\lambda : \mathscr{O}_T \longrightarrow (\varepsilon \times \mathrm{id}_T)^*\mathscr{L}$ is an isomorphism; λ is called a rigidification. The rigidification has the effects of killing invertible sheaves coming from T and eliminating automorphisms. It turns out that the set of isomorphism classes of such pairs $(\mathscr{L}, \lambda)$ is then equal to $\mathrm{Pic}(X_T)/\mathrm{Pic}(T)$. See [3], p. 204.

2.2 By 2.4(b) below, if X is a proper scheme over a field k then $\mathrm{Pic}_{X/k}$ is represented by a countable disjoint union of quasi–projective k–schemes; the identity component of this k–group is denoted $\mathrm{Pic}^0_{X/k}$. It is geometrically connected.

For a general base S, we define the relative identity component $\mathrm{Pic}^0_{X/S} \subset \mathrm{Pic}_{X/S}$ to be the subfunctor whose T–points are those $\xi \in \mathrm{Pic}_{X/S}(T)$ such that for all $s \in S$ and all geometric points $\bar{t} \to T$ whose image is s, $\xi_s \in \mathrm{Pic}^0_{X_s/k(s)}(k(\bar{t}))$.

If S is a proper and flat curve over a field k, then $\mathrm{Pic}^0_{X/k}$ consists of all elements of $\mathrm{Pic}_{X/k}$ whose restriction to every irreducible component of $X \otimes \bar{k}$ has degree zero. See [3], p. 239.

The preceeding is a variant of a general definition of identity components for a smooth S–group scheme G: G^0 is defined to be the open subscheme $\bigcup_{s\in S} G^0_s$. See [EGA IV_3 15.6.5].

Before proceeding, let's give the

2.3 Definition. A *semi–stable curve of genus g over S* is a proper, flat, and finitely presented morphism $f : X \longrightarrow S$ such that

(i) The fibres $X_{\bar{s}}$ over geometric points $\bar{s}$ of S are reduced, connected, and one–dimensional,

(ii) $X_{\bar{s}}$ has only ordinary double points as singularities, and

(iii) $h^1(X_{\bar{s}}, \mathscr{O}_{X_{\bar{s}}}) = g$.

The importance of such curves in the theory of moduli is due to the "semi–stable reduction theorem" which we will not state here. See the article by Abbes in [1] for a relatively accessible treatment.

2.4 Concerning the representability of $\mathrm{Pic}_{X/S}$ we state only what we'll need later on as

Theorem. *(a) If $f : X \longrightarrow S$ is a smooth projective curve with geometrically connected fibers, then $\mathrm{Pic}_{X/S}$ is represented by a separated scheme, and moreover $\mathrm{Pic}^0_{X/S}$ is an abelian scheme.*

(b) If X is proper over a field k then $\mathrm{Pic}_{X/k}$ is represented by a countable disjoint union of quasi–projective k–schemes. If X is a proper curve over k, then $\mathrm{Pic}^0_{X/k}$ is a smooth k–group scheme.

(c) If X is a semi–stable curve over S then $\mathrm{Pic}^0_{X/S}$ is represented by a smooth and separated S–scheme which is, moreover, semi–abelian (i.e. all of its fibers are extensions of affine tori by abelian varieties).

(d) If $p > 3$ is a prime then $\mathrm{Pic}^0_{M_0(p)/\mathbb{Z}}$ is represented by a smooth and separated group scheme over $\mathbb{Z}$.

These are special cases of results due to Grothendieck, Murre–Oort, Deligne, and Raynaud, respectively. See [3], p. 210, p. 211, p. 232, p. 259, p. 288. For (d), also see [12]. In 4.2, we will prove the semi–abelian assertion of (c) as we will need the finer information that the proof provides.

2.5 Remark. When X is a proper curve over a field k, so that $\mathrm{Pic}^0_{X/S}$ is represented by a smooth group scheme, it will also be called the Jacobian of X.

2.6 Finally, let's recall Weil's restriction of scalars functor. Let $f : T \longrightarrow S$ be a morphism of schemes. For a T–scheme X, we define $f_*X = \mathrm{Res}_{T/S}X$ to be the functor on S–schemes

$$U \longmapsto X(U \times_S T).$$

A suitable adjunction formula tells us that there is a natural morphism of functors

$$X \longrightarrow \mathrm{Res}_{T/S}(X_T).$$

We pass over in silence all questions concerning representability. See [3], Ch. 7, §6. However, let's mention that if k'/k is a finite Galois extension of fields then for a k'–scheme X, $\mathrm{Res}_{k'/k}X$ is the Galois descent of the k'–scheme

$$\prod_{\sigma\in\mathrm{Gal}(k'/k)} X\otimes_\sigma k',$$

with respect to the evident descent data.

3. Comparison of the Picard scheme of $M_0(p)$ and the Néron model of the Jacobian $J_0(p)_{\mathbb{Q}}$

3.1 Fix the following notations:
$p > 3$ a prime number
$J_0(p)_{\mathbb{Q}}$ the Jacobian of $M_0(p)_{\mathbb{Q}}$
$P := \mathrm{Pic}_{M_0(p)/\mathbb{Z}}$
$P^0 := \mathrm{Pic}^0_{M_0(p)/\mathbb{Z}}$
$\mathcal{J}$ the Néron model over $\mathbb{Z}$ of $J_0(p)_{\mathbb{Q}}$
$\mathcal{J}^0$ its identity component.

The Néron mapping property gives us a unique morphism $c : P^0 \longrightarrow \mathcal{J}^0$ which extends the identity map on generic fibers. The following theorem reduces the study of $\mathcal{J}^0_{\mathbb{F}_p}$ to the study of $P^0_{\mathbb{F}_p}$.

3.2 Theorem. *The map c is an isomorphism.*

Proof. The statement is obvious over $\mathbb{Z}[1/p]$ as $M_0(p)$ is a smooth proper curve over $\mathbb{Z}[1/p]$. Hence, by "chasing denominators" [EGA IV$_3$ 8.10.5] we may work over $\mathbb{Z}_{(p)}$. By 1.2(b) and 4.2, $P^0_{\mathbb{F}_p}$ is a semi–abelian variety. Now use the following proposition. □

3.3 Proposition. *Let R be a discrete valuation ring with field of fractions K and residue field k. Let A_K be an abelian variety with Néron model A and let B be a smooth and separated R–group with generic fiber A_K. Assume that B_k is a semi–abelian variety. Then the canonical morphism $B \longrightarrow A$ is an open immersion and is an isomorphism on identity components.*

For the proof see [3], p. 182.

4. The toric part of the Jacobian of a semi–stable curve

4.1 Given a semi–stable curve X over a field k, write S for the set of non–smooth points of $X \otimes \overline{k}$ and I for the set of irreducible components of $X \otimes \overline{k}$. Define a graph $\Gamma(X)$ with I as the set of vertices and S as the set of edges: a singular point s lying on the irreducible components X_i, X_j ($i = j$ is allowed) defines an edge in the graph. It is a general fact in the theory of semi–stable curves that all $s \in S$ are rational over a separable extension of k.

4.2 Proposition. *Let X be a semi–stable curve over a field k with normalization $\pi : \widetilde{X} \longrightarrow X$. Then $\mathrm{Pic}^0_{X/k}$ is canonically an extension of an abelian variety by a torus:*

$$1 \longrightarrow T \longrightarrow \mathrm{Pic}^0_{X/k} \xrightarrow{\pi^*} \mathrm{Pic}^0_{\widetilde{X}/k} \longrightarrow 1.$$

Furthermore, the rank of T equals the first Betti number of the graph $\Gamma(X)$.

PROOF. Let $X = \bigcup X_i$ be a decomposition of X into irreducibles, so the normalization is

$$\widetilde{X} = \coprod \widetilde{X}_i \xrightarrow{\pi} X.$$

Then $\mathrm{Pic}^0_{\widetilde{X}/k}$ is an abelian variety over k since the $\widetilde{X}_i$ are proper and smooth.

We have the exact sequence of sheaves on $X_{\text{ét}}$

$$1 \longrightarrow \mathbb{G}_{m/X} \longrightarrow \pi_* \mathbb{G}_{m/\widetilde{X}} \longrightarrow \mathscr{Q} \longrightarrow 1. \tag{1}$$

Write S_k for the finite set of singular points of X as a k–curve, so that $\mathscr{Q}$ is supported on S_k. Fix $x \in S_k$. Naïvely, one expects that the pullback of (1) along $\operatorname{Spec} k(x) \longrightarrow X$ would give rise to the sequence on $(\operatorname{Spec} k(x))_{\text{ét}}$

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathrm{Res}_{k(\widetilde{x})/k(x)} \mathbb{G}_m \times \mathrm{Res}_{k(\widetilde{x}')/k(x)} \mathbb{G}_m \longrightarrow \mathscr{Q}_x \longrightarrow 1$$

where $\widetilde{x}, \widetilde{x}'$ are the two points of $\widetilde{X}$ lying over x (see 4.3). Proceeding formally, we have that $k(x) = k(\widetilde{x}) = k(\widetilde{x}')$ by [6], p. 184, so that this sequence is just

$$1 \longrightarrow \mathbb{G}_m \xrightarrow{\text{diag.}} \mathbb{G}_m \times \mathbb{G}_m \longrightarrow \mathscr{Q}_x \longrightarrow 1. \tag{2}$$

Let $f : X \longrightarrow \operatorname{Spec} k$ be the structure map. Then we have that

$$f_* \mathscr{Q} \simeq \prod_{x \in S_k} \mathrm{Res}_{k(x)/k} \mathbb{G}_m$$

is a k–torus of rank $\sum [k(x) : k] = \# S$. This isomorphism is not canonical as it depends on an ordering of the points $\{\widetilde{x}, \widetilde{x}'\}$ for each $x \in S_k$.

Apply f_* to (1) and consider the resulting sequence of higher direct images:

$$\begin{array}{l} 1 \longrightarrow f_* \mathbb{G}_{m/X} \longrightarrow f_* \pi_* \mathbb{G}_{m/\widetilde{X}} \longrightarrow f_* \mathscr{Q} \\ \qquad \longrightarrow R^1 f_* \mathbb{G}_{m/X} \longrightarrow (R^1 f_*) \pi_* \mathbb{G}_{m/\widetilde{X}} \longrightarrow R^1 f_* \mathscr{Q} \longrightarrow \cdots \end{array}$$

Now note that:—

(a) $f_* \mathbb{G}_{m/X} = \mathbb{G}_{m/k}$ since X is proper and geometrically connected.

(b) $R^1 f_* \mathscr{Q} = 0$ since the support of $\mathscr{Q}$ is zero dimensional.

(c) $(R^1 f_*) \pi_* \mathbb{G}_{m/\widetilde{X}} = \mathrm{Pic}_{\widetilde{X}/k}$ by the conjunction of the Leray spectral sequence and the fact that if $f : X' \longrightarrow X$ is any finite morphism and $\mathscr{F}$ is an abelian sheaf on $X_{\text{ét}}$ then $R^i f_* \mathscr{F} = 0 \ \forall i \geqslant 1$ [6], p. 32.

Hence we may rewrite the above as

$$1 \longrightarrow \mathbb{G}_{m/k} \longrightarrow f_* \pi_* \mathbb{G}_{m/\widetilde{X}} \longrightarrow f_* \mathscr{Q} \longrightarrow T \longrightarrow 1 \tag{3}$$

$$1 \longrightarrow T \longrightarrow \mathrm{Pic}^0_{X/k} \longrightarrow \mathrm{Pic}^0_{\widetilde{X}/k} \longrightarrow 1,$$

where we have restricted to the identity component. Thus T, being a quotient of a torus, is a torus.

For the second assertion of the proposition, we claim that by extending scalars to k_s, the exact sequence (3) becomes

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \prod_{i \in I} \mathbb{G}_m \longrightarrow \prod_{x \in S} \mathbb{G}_m \longrightarrow T \longrightarrow 1 \tag{4}$$

As Pic commutes with base change, the only point to be checked is that we may still label the product on the left by I. This will be the case if $(\widetilde{X})_{k_s} = (X_{k_s})^{\sim}$, i.e. if normalization commutes with étale base change. This is so by [EGA IV$_4$ 18.12.15].

By (4), the rank of T is $\#S - \#I + 1 = \#\text{edges} - \#\text{vertices} + 1$. This is the first Betti number of $\Gamma(X)$ by elementary topology. □

4.3 Remark. The above proof is incomplete. The reason is as follows. Suppose we have a morphism $f : Y \longrightarrow X$ and a commutative group scheme G_X over X. As usual, we obtain a group scheme $G_Y := G \times_X Y$ on Y. Hence, by means of their functors of points, we obtain abelian sheaves again denoted G_X, G_Y on $X_{\text{ét}}, Y_{\text{ét}}$, respectively. On the other hand, we also have the abelian sheaf f^*G_X on $Y_{\text{ét}}$. There is a canonical morphism $\phi : f^*G_X \longrightarrow G_Y$. It is *not* in general an isomorphism. However, it is an isomorphism if either f or G_X is étale, neither of which is the case in the above proof. For example, the sheaf $G := \mathbb{G}_m$ on $(\operatorname{Spec}\mathbb{C})_{\text{ét}}$ is isomorphic to the constant sheaf $\underline{\mathbb{C}}^{\times}$ on $(\operatorname{Spec}\mathbb{C})_{\text{ét}}$. If $f : \operatorname{Spec}\mathbb{C}(t) \longrightarrow \operatorname{Spec}\mathbb{C}$ is the obvious map, then f^*G is isomorphic to the constant sheaf $\underline{\mathbb{C}}^{\times}$ on $(\operatorname{Spec}\mathbb{C}(t))_{\text{ét}}$. This is of course not the same as $\mathbb{G}_m$ on $(\operatorname{Spec}\mathbb{C}(t))_{\text{ét}}$. See [11], pp. 68–69.

To repair the proof of 4.2, consider the divisor $D := \sum_{P \in S_k} P$ supported on the singular locus and let $i : D \longrightarrow X$ be the inclusion. Then, for any scheme S over k, one considers the following variant of (1):

$$1 \longrightarrow \mathbb{G}_{m/X_S} \longrightarrow (\pi_S)_* \mathbb{G}_{m/\widetilde{X}_S} \longrightarrow (i_S)_* \mathbb{G}_{m/D_S} \longrightarrow 1.$$

One must then show that $(i_S)_*\mathbb{G}_{m/D_S}$ coincides on $S_{\text{ét}}$ with the points of a torus, compatibly as S varies through (**schemes**/k). We will not do this. For the details, see the notes in the margin on page 246 of Professor Conrad's copy of [3].

4.4 Apply $\mathbf{X}(\,\cdot\,) := \operatorname{Hom}_{k-\text{grp}}(\,\cdot\,, \mathbb{G}_m)$ to the exact sequence (2) to obtain

$$1 \longrightarrow \mathbb{Z}'(x) \longrightarrow \mathbb{Z}^{B_x} \longrightarrow \mathbb{Z} \longrightarrow 1$$

where $\mathbb{Z}'(x) := \mathbf{X}(\mathscr{Q}_x)$ and B_x is the (two element) set of analytic branches of X at x. Then (4) becomes

$$0 \longrightarrow \mathbf{X}(T) \longrightarrow \bigoplus_{x \in S} \mathbb{Z}'(x) \longrightarrow \bigoplus_{i \in I} \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow 0$$

where the middle arrow sends a branch to the irreducible component containing it. The Galois action on $\mathbf{X}(T)$ coincides with the action induced by the natural Galois actions on the sets S, I, and the B_x for $x \in S$.

In particular, just as the proof of 4.2 shows that there is a Galois–equivariant isomorphism

$$T_{k_s} \simeq H^1(\Gamma(X), \mathbb{Z}) \otimes \mathbb{G}_m, \tag{5}$$

we also have

$$\mathbf{X}(T) \simeq H_1(\Gamma(X), \mathbb{Z})$$

compatibly with Galois actions.

4.5 Explicitly in the case of the curve $M_0(p)_{\mathbb{F}_p}$, it follows from 1.2(a) that its Jacobian is a torus, and in fact the proof of 4.2 shows that

$$P^0_{\mathbb{F}_p} \simeq \left(\prod_{x \in S_{\mathbb{F}_p}} \mathrm{Res}_{\mathbb{F}_p(x)/\mathbb{F}_p} \mathbb{G}_m \right) \Big/ \mathbb{G}_m$$

where the $\mathbb{G}_m$ is diagonally embedded. Moreover, the restrictions of scalars are from at worst quadratic extensions by 1.2(d).

5. The action of Frobenius

5.1 Let S be a scheme of characteristic p, i.e. the canonical map $S \longrightarrow \mathrm{Spec}\,\mathbb{Z}$ factors through $\mathrm{Spec}\,\mathbb{F}_p$. Let $F : S \longrightarrow S$ be the absolute Frobenius morphism. It is defined to be the identity on the underlying topological space and the p–th power on $\mathscr{O}_S$. Let X be a scheme over S. We define the relative Frobenius $F_{X/S}$, as well as $X^{(p)}$, by the diagram

$$\begin{tikzcd} X \arrow[r, "F_{X/S}"] \arrow[rr, bend left, "F"] \arrow[dr] & X^{(p)} \arrow[r, "\mathrm{pr}"] \arrow[d] \arrow[dr, phantom, "\square"] & X \arrow[d] \\ & S \arrow[r, "F"'] & S \end{tikzcd}$$

For $x \in X$, we also write $x^{(p)}$ for $F_{X/S}(x)$.

5.2 Let X and X' be proper curves over a field k of characteristic p. For a morphism $f : X \longrightarrow X'$ over k, write $\mathrm{Pic}(f)$ for the induced map $\mathrm{Pic}^0_{X'/k} \longrightarrow \mathrm{Pic}^0_{X/k}$. Also, we write $F_{\mathrm{Pic}/k}$ for the relative Frobenius on $\mathrm{Pic}^0_{X/k}$.

5.3 Proposition. *Let X be a generically smooth, geometrically connected, and proper curve over a field k of characteristic p. Then*

$$F_{\mathrm{Pic}/k} \circ \mathrm{Pic}(F_{X/k}) = [p]$$

on $(\mathrm{Pic}^0_{X/k})^{(p)} = \mathrm{Pic}^0_{X^{(p)}/k}$.

Proof. We may assume without loss that $k = \overline{k}$ (cf. [5] I.7.4). As $\mathrm{Pic}^0_{X/k}$ is smooth it suffices to check the identity on k–points (the k–points are dense; [3] p. 42). We use the fact that every invertible sheaf $\mathscr{L}$ on X has the form $\mathscr{O}_X(D)$ for a Cartier divisor D such that $\mathrm{supp}(D)$ is contained in the smooth locus X^{sm} of X (see the discussion after Theorem 7, p. 258 of [3]).

Let $\mathscr{L}$ be an invertible sheaf on $X^{(p)}$ of degree zero on each irreducible component. We may assume by additivity that $\mathscr{L}$ is of the form $\mathscr{O}_X(x_1^{(p)} - x_0^{(p)})$ where $x_0^{(p)}, x_1^{(p)} \in X^{(p)}(k)$ actually lie in the smooth locus of a common irreducible component $C^{(p)}$ of $X^{(p)}$.

Let $i_{x_0} : C^{\mathrm{sm}} \longrightarrow \mathrm{Pic}_{X/k}$ be the k–morphism $x \longmapsto \mathscr{O}_X(x - x_0)$. Since C^{sm} is irreducible and $i_{x_0}(x_0) = 0$, i_{x_0} factors through $\mathrm{Pic}^0_{X/k}$.

Before proceeding any further, let's note that

(a) $i_{x_0^{(p)}} = i_{x_0}^{(p)}$, i.e. the following diagram commutes

$$\begin{tikzcd}
 & (\mathrm{Pic}^0_{X/k})^{(p)} \arrow[dd, equal] \\
(C^{\mathrm{sm}})^{(p)} \arrow[ur, "(i_{x_0})^{(p)}"] \arrow[dr, "i_{x_0^{(p)}}"'] & \\
 & \mathrm{Pic}^0_{X^{(p)}/k}
\end{tikzcd}$$

For the proof, we have that

$$i_{x_0^{(p)}} : x^{(p)} \longmapsto [x^{(p)} - x_0^{(p)}]$$
$$(i_{x_0})^{(p)} : x^{(p)} \longmapsto \mathrm{pr}^*[x - x_0]$$

where pr is as in 5.1. But $\mathrm{pr}^*[x] = [x^{(p)}]$ so that $[x^{(p)} - x_0^{(p)}] = \mathrm{pr}^*[x - x_0]$, as claimed.

(b) Since raising to the p–th power commutes with any ring map we have the commutativity of

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "F_{X/k}"'] & Y \arrow[d, "F_{Y/k}"] \\
X^{(p)} \arrow[r, "f^{(p)}"'] & Y^{(p)}
\end{tikzcd}$$

for any morphism of $f : X \longrightarrow Y$ of schemes of characteristic p.

Returning to the proof of the proposition, we have

$$\begin{aligned}(F_{\mathrm{Pic}/k} \circ \mathrm{Pic}(F_{X/k}))(\mathscr{L}) &= F_{\mathrm{Pic}/k}(F^*_{X/k}(\mathscr{L})) \\ &= F_{\mathrm{Pic}/k}(\mathscr{O}_X(F^*_{X/k}(F_{X/k}(x_1) - F_{X/k}(x_0))))\end{aligned}$$

Now using the fact that $F_{X/k}$ is finite flat and purely inseparable of degree p *over the smooth locus*, the last term above equals $F_{\mathrm{Pic}/k}(\mathscr{O}_X(p(x_1 - x_0)))$. Then we have

$$\begin{aligned}F_{\mathrm{Pic}/k}(\mathscr{O}_X(p(x_1 - x_0))) &= [p] \circ F_{\mathrm{Pic}/k} i_{x_0}(x_1) \\ &= [p] \circ i_{x_0^{(p)}}(F_{X/k}(x_1)) \\ &= [p] \circ i_{x_0^{(p)}}(x_1^{(p)}) \\ &= \mathscr{O}_X(x_1^{(p)} - x_0^{(p)})^{\otimes p} \\ &= \mathscr{L}^{\otimes p}\end{aligned}$$

as required. □

5.4 Put $X := M_0(p)_{\mathbb{F}_p}$. Then by 1.2, $\Gamma(X)$ has two vertices and an edge for each geometric supersingular point. See Figure 2.

The following is Theorem A.1.(a) of [10].

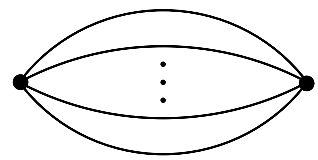

FIGURE 2. $\Gamma(M_0(p)_{\mathbb{F}_p})$.

5.5 THEOREM. $F_{\mathrm{Pic}/\mathbb{F}_p} = -pw$.

PROOF. If we could show that $\mathrm{Pic}(F_{X/\mathbb{F}_p}) = -w$ then $F_{\mathrm{Pic}/\mathbb{F}_p} \circ (-w) = p$ by 5.3. The theorem would follow since w is an involution.

Let E be an ordinary elliptic curve over $\overline{\mathbb{F}}_p$, so that $E[p] \simeq \mathbb{Z}/p\mathbb{Z} \times \boldsymbol{\mu}_p$ and put $C := \ker(F_{E/\mathbb{F}_p} : E \to E^{(p)})$. C is the unique connected subgroup of E of order p; it is isomorphic to $\boldsymbol{\mu}_p$. Also, $F_{E/\mathbb{F}_p}$ induces an isomorphism $E/C \simeq E^{(p)}$ and $E[p]/C$ is étale. See [5], p. 27. Hence $w\Phi(E) = w(E, C) = (E/C, E[p]/C) \simeq (E^{(p)}, C')$ for some étale $C' \hookrightarrow E^{(p)}$. It now follows from 1.2(c) that w exchanges the vertices of $\Gamma(X)$ and sends an edge x to the edge $x^{(p)}$.

On the other hand, $F_{X/\mathbb{F}_p}$ fixes the vertices and sends an edge x to the edge $x^{(p)}$. We are done by (5). $\square$

REFERENCES

[1] *Courbes semi-stables et groupe fondamental en géométrie algébrique*, volume 187 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2000.

[2] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.

[3] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1990.

[4] Brian Conrad. *Minimal Models for Elliptic Curves*. Unpublished.

[5] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[6] Eberhard Freitag and Reinhardt Kiehl. *Étale cohomology and the Weil conjecture*, volume 13 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1988.

[7] Alexandre Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. Troisième partie. *Inst. Hautes Études Sci. Publ. Math.*, (28):255, 1966.

[8] Alexandre Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. Quatrième partie. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.

[9] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[10] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[11] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[12] Michel Raynaud. Jacobienne des courbes modulaires et opérateurs de Hecke. *Astérisque*, (196-197):9–25 (1992), 1991.