Full Level Structures on Elliptic Curves

June 7, 2018

Contents

Overview

Let p be a prime number, which we regard as fixed throughout this paper. For each $n > 0$, let $X(p^n)$ denote the modular curve parametrizing elliptic curves equipped with a full level-p^n structure, which we regard as a scheme defined over the cyclotomic field $\mathbf{Q}[\zeta_{p^n}]$. Each $X(p^n)$ determines a rigid-analytic curve $X(p^n)^{\mathrm{an}}$ over the local field $\mathbf{Q}_p[\zeta_{p^n}]$. These rigid-analytic curves can be organized into an inverse system

$$\cdots \to X(p^4)^{\mathrm{an}} \to X(p^3)^{\mathrm{an}} \to X(p^2)^{\mathrm{an}} \to X(p)^{\mathrm{an}}.$$

The starting point of this paper is the following result (which is a special case of Theorem III.1.2 of [4]):

Theorem 0.1 (Scholze)**.** *There is an essentially unique perfectoid space $X(p^\infty)^{\mathrm{an}}$ over the perfectoid field $\mathbf{Q}_p^{\mathrm{cyc}}$ such that $X(p^\infty)^{\mathrm{an}} \sim \varprojlim X(p^n)^{\mathrm{an}}$ (in the sense of [5], Definition 2.4.1).*

The primary goal of this paper is to prove an integral version of Theorem 0.1. For $p^n \neq 2$, we can identify $X(p^n)$ with the generic fiber a Deligne-Mumford stack $\overline{\mathrm{Ell}}(p^n)$ over the ring of integers $\mathbf{Z}[\zeta_{p^n}] \subseteq \mathbf{Q}[\zeta_{p^n}]$, which parametrize (generalized) elliptic curves equipped with a full level-p^n structure in the sense of Drinfeld (see [3] and [1]). These stacks can be organized into an inverse system

$$\cdots \to \overline{\mathrm{Ell}}(p^4) \to \overline{\mathrm{Ell}}(p^3) \to \overline{\mathrm{Ell}}(p^2) \to \overline{\mathrm{Ell}}(p)$$

with affine transition maps, and therefore admits an inverse limit $\overline{\mathrm{Ell}}(p^\infty)$ in the 2-category of Deligne-Mumford stacks which is defined over the ring $\mathbf{Z}[\zeta_{p^\infty}] = \varinjlim_n \mathbf{Z}[\zeta_{p^n}]$. For every positive integer n, let $\overline{\mathrm{Ell}}(p^\infty)_{\zeta_{p^n}=1}$ denote the closed substack of $\overline{\mathrm{Ell}}(p^\infty)$ given by the vanishing locus of $\zeta_{p^n} - 1$, so that we have a descending sequence of closed substacks

$$\cdots \subset \overline{\mathrm{Ell}}(p^\infty)_{\zeta_{p^3}=1} \subseteq \overline{\mathrm{Ell}}(p^\infty)_{\zeta_{p^2}=1} \subseteq \overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1}.$$

Note that $\overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1}$ is defined over the quotient ring $\mathbf{Z}[\zeta_p]/(\zeta_p - 1) \simeq \mathbf{F}_p$, and is therefore equipped with an (absolute) Frobenius map $\varphi : \overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1} \to \overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1}$. We will prove the following:

Theorem 0.2. *The absolute Frobenius map $\varphi : \overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1} \to \overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1}$ induces an isomorphism from $\overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1}$ to the closed substack $\overline{\mathrm{Ell}}(p^\infty)_{\zeta_{p^2}=1} \subseteq \overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1}$.*

It follows from Theorem 0.2 that the moduli stack $\overline{\mathrm{Ell}}(p^\infty)$ is étale locally integrally perfectoid (after p-adic completion). More precisely, we have the following:

Corollary 0.3. *For every étale map* $\mathrm{Spec}(R) \to \overline{\mathrm{Ell}}(p^\infty)$*, there exists a regular element* $\pi \in R$ *such that* π^p *divides* p *and the Frobenius map* $R/\pi R \to R/\pi^p R$ *is an isomorphism.*

Proof. Let us regard R as an algebra over the ring $\mathbf{Z}[\zeta_{p^\infty}]$. It follows from Theorem 0.2 that the Frobenius map induces an isomorphism $R/(\zeta_{p^2} - 1) \to R/(\zeta_p - 1)$. Since $(\zeta_{p^2} - 1)^p$ and $\zeta_p - 1$ differ by a unit, it follows that $\pi = \zeta_{p^2} - 1$ satisfies the requirements of Corollary 0.3. □

Remark 0.4. More generally, for every integer $n > 0$, the Frobenius map induces an isomorphism of Deligne-Mumford stacks $\overline{\mathrm{Ell}}(p^\infty)_{\zeta_{p^n}=1} \to \overline{\mathrm{Ell}}(p^\infty)_{\zeta_{p^{n+1}}=1}$. This is an immediate consequence of Theorem 0.2.

Remark 0.5. We will deduce Theorem 0.2 from slightly stronger assertion: the structure morphism $\overline{\mathrm{Ell}}(p^\infty) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^\infty}])$ becomes relatively perfect after extending scalars to $\mathbf{F}_p$ (see Theorems 1.15 and 8.5).

Remark 0.6. The conclusion of Corollary 0.3 is satisfied more generally for maps $f : \mathrm{Spec}(R) \to \overline{\mathrm{Ell}}(p^\infty)$ which are "log étale at infinity" (in particular, our result can be applied to the study of elliptic curves equipped with auxiliary "prime to p" level structures). This is a consequence of stronger version of Theorem 0.2, where we replace the moduli stack $\overline{\mathrm{Ell}}(p^\infty)$ by a certain enlargement $\mathrm{Ell}^+(p^\infty)$; see Remark 8.8.

Remark 0.7. In [6], Weinstein supplies an explicit description of the coordinate ring for Lubin-Tate space at infinite level (see Theorem 2.7.3 of [6]). From this description, one can immediately deduce that Corollary 0.3 holds after formal completion along the locus of supersingular elliptic curves.

Warning 0.8. For $p^n \neq 2$, the generic fiber of $\overline{\mathrm{Ell}}(p^n)$ is the modular curve $X(p^n)$, which is a scheme. However, the stack $\overline{\mathrm{Ell}}(p^n)$ itself is never a scheme: over a field of characteristic p, any supersingular elliptic curve E admits a unique full level-p^n structure, which is preserved by any automorphism of E. Consequently, there is a slight mismatch between the statements of Theorem 0.1 and Corollary 0.3: the first concerns the local structure of the inverse system $\{X(p^n)^{\mathrm{an}}\}$ with respect to the *analytic* topology, while the second concerns the local structure of the inverse system $\{\overline{\mathrm{Ell}}(p^n)\}$ with respect to the *étale* topology. Nevertheless, it is not difficult to deduce Theorem 0.1 formally from Corollary 0.3; we leave details to the interested reader.

Remark 0.9. Theorem 0.2 provides a moduli-theoretic interpretation of the tilt $X(p^\infty)^{\mathrm{an},\flat}$ of the perfectoid space of Theorem 0.1: it can be realized as the "generic fiber" of the formal Deligne-Mumford stack given by the direct limit of the system

$$\overline{\mathrm{Ell}}(p^\infty)_{p=0} \xrightarrow{\varphi} \overline{\mathrm{Ell}}(p^\infty)_{p=0} \xrightarrow{\varphi} \overline{\mathrm{Ell}}(p^\infty)_{p=0} \xrightarrow{\varphi} \cdots,$$

where the transition maps are given by the absolute Frobenius endomorphism of the product $\overline{\mathrm{Ell}}(p^\infty)_{p=0} = \overline{\mathrm{Ell}}(p^\infty) \times \mathrm{Spec}(\mathbf{F}_p)$.

Let us now outline our approach to Theorem 0.2. The map appearing in Theorem 0.2 can be realized as an inverse limit of Frobenius maps $\varphi : \overline{\mathrm{Ell}}(p^n)_{\zeta_p=1} \to \overline{\mathrm{Ell}}(p^n)_{\zeta_{p^2}=1}$ defined for $n \geqslant 2$. At finite level, these maps are not isomorphisms. However, we will show that they induce an isomorphism of pro-objects $\{\overline{\mathrm{Ell}}(p^n)_{\zeta_p=1}\}_{n\geqslant 2} \to \{\overline{\mathrm{Ell}}(p^n)_{\zeta_{p^2}=1}\}_{n\geqslant 2}$. This is a consequence of the following more precise assertion:

Theorem 0.10. *For each $n \geqslant 2$, the commutative diagram of Deligne-Mumford stacks*

$$\begin{array}{ccc} \overline{\mathrm{Ell}}(p^{n+1})_{\zeta_p=1} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^{n+1})_{\zeta_{p^2}=1} \\ \downarrow & \swarrow & \downarrow \\ \overline{\mathrm{Ell}}(p^n)_{\zeta_p=1} & \longrightarrow & \overline{\mathrm{Ell}}(p^n)_{\zeta_{p^2}=1} \end{array}$$

admits an extension as indicated; here the horizontal maps are given by the absolute Frobenius, and the vertical maps by "forgetting" level structure.

Remark 0.11. To fix ideas, let us give a rough description of the diagonal map appearing in Theorem 0.10. Working away from the cusp, we can think of points of $\overline{\mathrm{Ell}}(p^{n+1})_{\zeta_{p^2}=1}$ as elliptic curves E equipped with a full level-p^{n+1} structure (x, y) for which the Weil pairing $e_{p^{n+1}}(x, y)$ is a p^{n-1}st root of unity. The heuristic idea is that the degeneracy of the Weil pairing ensures that $p^n x$ and $p^n y$ "generate" a subgroup $S \subseteq E$ of order p. The diagonal map then carries the triple (E, x, y) to $(E/S, x', y')$, where x' and y' denote the images of x and y in the quotient elliptic curve E/S.

Let us now outline the contents of this paper. For most of this paper, we will be primarily concerned with the open substack $\mathrm{Ell}(p^\infty) \subseteq \overline{\mathrm{Ell}}(p^\infty)$ parametrizing *smooth* elliptic curves with a full level-p^∞ structure. In §1, we recall the definition of this stack (following [3]) and formulate a slightly stronger version of Theorem 0.2 for it (see Theorem 1.15). In §2, we reduce to proving a statement about about elliptic curves with a finite amount of level structure (Theorem 2.11), which asserts that a

certain map of moduli stacks $\rho : \mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} \to \mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$ is an isomorphism. This statement can be regarded as a precise articulation of the heuristic of Remark 0.11 (and implies a slightly stronger version of Theorem 0.10). In §3, we show that ρ induces an isomorphism over the locus of *ordinary* elliptic curves. In this case, our proof is conceptual: that is, it can be explained directly in terms of the functors represented by $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}$ and $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$. To extend this result over the supersingular locus, we resort to a calculation. First, we note that it suffices to prove that ρ induces an isomorphism of the reductions of the moduli stacks $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}$ and $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$ (which admit moduli-theoretic descriptions which we review in §4). These are reduced (stacky) curves over $\mathrm{Spec}(\mathbf{F}_p)$, whose failure to be smooth can be quantified by their *δ-invariants* (see §5). We will complete the proof by computing the δ-invariants on both sides (at each point of the supersingular locus) and showing that they agree. These calculations are carried out in §6 (for the moduli stack $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$) and in §7 (for the moduli stack $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}$) using the theory of Igusa curves $\mathrm{Ig}(p^n)$. In essence, the proof reduces to comparing intersection numbers between Igusa curves in two different settings: inside the (stacky) characteristic p surface $\mathrm{Ig}(p^{n+1})^2$, and inside the (stacky) arithmetic surface $\mathrm{Ell}(p^{n+1})$.

The remainder of this paper is devoted to extending our analysis to the compactified moduli stack $\overline{\mathrm{Ell}}(p^\infty)$ (and a bit further). We give a precise formulation in §8 and carry out the proof in §9, using an explicit calculation with the Tate curve and its cyclic covers.

Remark 0.12. Many of the results of this paper can be extended to a more general setting, where the (algebraic) moduli stack Ell of elliptic curves is replaced by the the (non-algebraic) moduli stack of 1-dimensional p-divisible groups. We will discuss such extensions in a sequel to this paper.

Acknowledgements

I would like to thank Bhargav Bhatt, Johan de Jong, Barry Mazur, and Peter Scholze for useful discussions related to the subject of this paper. I offer thanks also to the National Science Foundation, for supporting this work under grant number 1510417.

1 Level Structures on Elliptic Curves

In this section, we briefly review the theory of Drinfeld level structures on elliptic curves and formulate the first main result of this paper (Theorem 1.15). For a more comprehensive account, we refer the reader to [3].

Notation 1.1. Let E be an elliptic curve over a commutative ring R and let $x \in E(R)$ be an R-valued point of E. Then x determines a closed immersion of schemes $\mathrm{Spec}(R) \hookrightarrow E$, whose image is an effective Cartier divisor in E. We will denote this effective Cartier divisor by $[x]$.

Definition 1.2 (Drinfeld, Katz-Mazur)**.** Let E be an elliptic curve over a commutative ring R. A *full level-p^n structure on E* is a group homomorphism $\gamma : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E(R)$ for which there is an equality

$$\sum_{v \in (\mathbf{Z}/p\mathbf{Z})^2} [\gamma(v)] = E[p^n]$$

of effective Cartier divisors in E. Here $E[p^n]$ denotes the kernel of the map $p^n : E \to E$.

Remark 1.3. Let E be an elliptic curve over a commutative ring R. We will generally abuse notation by identifying group homomorphisms $(\mathbf{Z}/p^n\mathbf{Z})^2 \to E(R)$ with pairs of p^n-torsion points $x, y \in E(R)$. We will say that a pair of p^n-torsion points (x, y) is a *full level-p^n structure* if, under this identification, it corresponds to a full level-p^n structure $(\mathbf{Z}/p^n\mathbf{Z})^2 \to E(R)$ in the sense of Definition 1.2.

Example 1.4. In the situation of Definition 1.2, the datum of a group homomorphism $\gamma : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E(R)$ is equivalent to the datum of a map

$$\gamma' : (\underline{\mathbf{Z}/p^n\mathbf{Z}})^2 \to E[p^n]$$

in the category of finite flat group schemes over R; here $\underline{\mathbf{Z}/p^n\mathbf{Z}}$ denotes the constant group scheme associated to the finite group $\mathbf{Z}/p^n\mathbf{Z}$. If p is invertible in R, then γ is a full level-p^n structure (in the sense of Definition 1.2) if and only if γ' is an isomorphism of finite flat group schemes. Beware that if p is not invertible in R, then the latter condition is *never* satisfied (because the group scheme $E[p]$ is not étale over $\mathrm{Spec}(R)$).

Example 1.5. Let E be an elliptic curve over a separably closed field k. Then a map $\gamma : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E(k)$ is a full level-p^n structure on E if and only if every p^n-torsion element of $E(k)$ lies in the image of γ. It follows that the set of full level-p^n structures on E carries a transitive action of the group $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$.

Remark 1.6. Let E be an elliptic curve over a commutative ring R and suppose we are given a pair of p^n-torsion points $x, y \in E(R)$. Then there exists a finitely generated ideal $I \subseteq R$ with the following property: a ring homomorphism $R \to S$ annihilates the ideal I if and only if the images of x and y in $E(S)$ determine a full level-p^n structure on the elliptic curve $E \times_{\mathrm{Spec}(R)} \mathrm{Spec}(S)$.

Remark 1.7. Let E be an elliptic curve over a commutative ring R and let $\gamma : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E(R)$ be the zero map. The following conditions are equivalent:

- The map γ is a full level-p^n structure on E.
- The elliptic curve E is supersingular: that is, the prime number p vanishes in R and the subgroup $E[p] \subseteq E$ coincides with the kernel of the iterated Frobenius map $F^2 : E \to E^{(p^2)}$.

Notation 1.8. Let R be a commutative ring. We let $\mathrm{Ell}(R)$ denote the groupoid whose objects are elliptic curves over R and whose morphisms are isomorphisms of elliptic curves. If n is a positive integer, we let $\mathrm{Ell}(p^n)(R)$ denote the groupoid whose objects are pairs (E, γ), where E is an elliptic curve over R and $\gamma : (\mathbf{Z}/p^n)^2 \to E(R)$ is a full level-p^n structure on E; a morphism from (E, γ) to (E', γ') is an isomorphism of elliptic curves $f : E \to E'$ which carries γ to γ'. We regard the constructions $R \mapsto \mathrm{Ell}(R)$ and $R \mapsto \mathrm{Ell}(p^n)(R)$ as functors from the category of commutative rings to the 2-category of groupoids. We will refer to Ell as the *moduli stack of elliptic curves*, to $\mathrm{Ell}(p^n)$ as the *moduli stack of elliptic curves with a full level-p^n structure*.

The moduli stack Ell is a Deligne-Mumford stack which is smooth of dimension 1 over $\mathrm{Spec}(\mathbf{Z})$. Let $\mathcal{E}$ denote the universal elliptic curve over Ell and let $\mathcal{E}[p^n]$ denote its p^n-torsion subgroup, so that $\mathcal{E}[p^n]$ is finite flat of degree p^{2n} over Ell. It follows from Remark 1.3 that we can regard $\mathrm{Ell}(p^n)$ as a closed substack of the fiber product $\mathcal{E}[p^n] \times_{\mathrm{Ell}} \mathcal{E}[p^n]$. In particular, $\mathrm{Ell}(p^n)$ is also a Deligne-Mumford stack which is locally finite type over $\mathrm{Spec}(\mathbf{Z})$, and the projection map $\mathrm{Ell}(p^n) \to \mathrm{Ell}$ is finite. One can show that the Deligne-Mumford stack $\mathrm{Ell}(p^n)$ is regular (see Theorem 5.1.1 of [3]); we will give a proof here as Proposition 6.7. For the moment, we note the following weaker result:

Proposition 1.9. *For each $n > 0$, the Deligne-Mumford stack $\mathrm{Ell}(p^n)$ has pure Krull dimension 2.*

Proof. The moduli stack Ell is smooth of relative dimension 1 over $\mathrm{Spec}(\mathbf{Z})$, hence of Krull dimension 2. Since the projection map $\mathrm{Ell}(p^n) \to \mathrm{Ell}$ is finite, it follows that

$\mathrm{Ell}(p^n)$ has Krull dimension $\leqslant 2$ at each point. Let $|\mathrm{Ell}(p^n)|$ denote the underlying topological space of $\mathrm{Ell}(p^n)$ and let $K \subseteq |\mathrm{Ell}(p^n)|$ be the union of those irreducible components having dimension 2. Since the map $\mathrm{Ell}(p^n) \to \mathrm{Ell}$ is surjective, the set K is nonempty. It follows that the image of K is a nonempty closed subset of $|\mathrm{Ell}|$. Since the moduli stack Ell is irreducible, the map $K \to |\mathrm{Ell}|$ is surjective: that is, the set K intersects each fiber of the map $\mathrm{Ell}(p^n) \to \mathrm{Ell}$. Combining this observation with Remark 1.5, we deduce that $K = |\mathrm{Ell}(p^n)|$. □

The moduli stacks $\mathrm{Ell}(p^n)$ can be organized into an inverse system

$$\cdots \to \mathrm{Ell}(p^3) \to \mathrm{Ell}(p^2) \to \mathrm{Ell}(p),$$

where the transition maps are given by the construction $(E, x, y) \mapsto (E, px, py)$. We let $\mathrm{Ell}(p^\infty)$ denote the inverse limit of this system. Since each of the transition maps is affine (even finite), it follows that $\mathrm{Ell}(p^\infty)$ is also a Deligne-Mumford stack, which is affine over the moduli stack Ell of elliptic curves. Beware that the moduli stack $\mathrm{Ell}(p^\infty)$ is not Noetherian.

Notation 1.10 (The Weil Pairing)**.** Let E be an elliptic curve over a commutative ring R and let $x, y \in E(R)$ be a pair of p^n-torsion points of E. We let $e_{p^n}(x, y)$ denote the Weil pairing of x and y, which we regard as an element of the group

$$\mu_{p^n}(R) = \{u \in R : u^{p^n} = 1\}$$

of p^nth roots of unity in R.

Proposition 1.11. *Let E be an elliptic curve over a commutative ring R and let $x, y \in E(R)$ be a full level-p^n structure on R, Then the Weil pairing $e_{p^n}(x, y)$ is a primitive p^nth root of unity: that is, it is a root of the cyclotomic polynomial $u^{(p-1)p^{n-1}} + u^{(p-2)p^{n-1}} + \cdots + u^{p^{n-1}} + 1$.*

Proof. Replacing x and y by $p^{n-1}x$ and $p^{n-1}y$, we can reduce to the case $n = 1$. The triple (E, x, y) is then classified by a map $f : \mathrm{Spec}(R) \to \mathrm{Ell}(p)$. Working locally on $\mathrm{Spec}(R)$, we may assume that f factors through an étale map $\mathrm{Spec}(S) \to \mathrm{Ell}(p)$. Replacing R by S, we can reduce to the case where f is flat. Since $\mathrm{Ell}(p)$ is flat over $\mathrm{Spec}(\mathbf{Z})$ (see Remark 6.8), it follows that the commutative ring R is torsion-free. Consequently, to show that $e_p(x, y)$ is a primitive pth root of unity in R, we can replace R by $R[1/p]$ and thereby reduce to the case where p is invertible in R. Using Example 1.4, we see that x and y determine an isomorphism $(\underline{\mathbf{Z}/p\,\mathbf{Z}})^2 \to E[p]$. In

this case, the assertion that $e_p(x,y)$ is a primitive pth root of unity follows from the fact that the Weil pairing $e : E[p] \times_{\mathrm{Spec}(R)} E[p] \to \mu_p$ is nondegenerate (that is, it exhibits $E[p]$ as a Cartier dual of itself). $\square$

Construction 1.12. For each $n > 0$, let $\mathbf{Z}[\zeta_{p^n}]$ denote the ring of integers in the cyclotomic field $\mathbf{Q}[\zeta_{p^n}]$, which we can identify with the quotient $\mathbf{Z}[u]/(u^{(p-1)p^{n-1}} + u^{(p-2)p^{n-1}} + \cdots + u^{p^{n-1}} + 1)$. It follows that the spectrum $\mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}])$ can be identified with a closed subscheme of the group scheme μ_{p^n} of p^nth roots of unity. By virtue of Proposition 1.11, the construction $(E, x, y) \mapsto e_{p^n}(x,y)$ induces a map of Deligne-Mumford stacks $\theta_n : \mathrm{Ell}(p^n) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}])$, which we will refer to as the *Weil pairing map*. Passing to the limit over n, we obtain a map $\theta_\infty : \mathrm{Ell}(p^\infty) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^\infty}])$.

Remark 1.13 (Level Structures on Ordinary Elliptic Curves)**.** Let E be an elliptic curve over a commutative $\mathbf{F}_p$-algebra R, and assume that E is ordinary (that is, the map $E \to \mathrm{Spec}(R)$ has no supersingular fibers). Let n be a positive integer, so that the subgroup scheme $E[p^n] \subseteq E$ fits into an exact sequence

$$0 \to E[p^n]_{\mathrm{cn}} \to E[p^n] \to E[p^n]_{\text{ét}} \to 0$$

where the group scheme $E[p^n]_{\text{ét}}$ is étale over $\mathrm{Spec}(R)$ and the group scheme $E[p^n]_{\mathrm{cn}}$ has connected fibers. Let $x, y \in E(R)$ be a pair of p^n-torsion points, so that x and y determine a map of finite flat group schemes $\gamma : (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \to E[p^n]$. Then the pair (x,y) is a full level p^n-structure if and only if both of the following conditions are satisfied:

(a) The composite map $(\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \xrightarrow{\gamma} E[p^n] \to E[p^n]_{\text{ét}}$ is an epimorphism of finite flat group schemes over $\mathrm{Spec}(R)$.

(b) The Weil pairing $e_{p^n}(x,y)$ is a primitive p^nth root of unity in R.

Notation 1.14. For every Deligne-Mumford stack $\mathcal{X}$, we let $\mathcal{X}_{p=0}$ denote the product $\mathcal{X} \times \mathrm{Spec}(\mathbf{F}_p)$: that is, the closed substack of $\mathcal{X}$ given by the vanishing locus of p. We also let $\mathbf{F}_p[\zeta_{p^\infty}]$ denote the quotient $\mathbf{Z}[\zeta_{p^\infty}]/(p)$.

We can now state the first main result of this paper:

Theorem 1.15. *After extending scalars to $\mathbf{F}_p$, the morphism $\theta_\infty : \mathrm{Ell}(p^\infty) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^\infty}])$ is relatively perfect. In other words, the diagram of Deligne-Mumford*

stacks

$$\begin{array}{ccc} \mathrm{Ell}(p^\infty)_{p=0} & \xrightarrow{\varphi} & \mathrm{Ell}(p^\infty)_{p=0} \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^\infty}]) & \xrightarrow{\varphi} & \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^\infty}]) \end{array}$$

is a pullback square here the horizontal maps are given by the absolute Frobenius).

2 Reduction to Finite Level

Our goal in this section is give a precise formulation of the heuristic described in Remark 0.11 (Theorem 2.11), and to show that it implies Theorem 1.15. We begin by introducing some terminology.

Definition 2.1. Let R be a commutative ring, let n be a positive integer, and let E be an elliptic curve over R equipped with a full level-p^{n+1} structure, given by a pair of p^{n+1}-torsion points $x, y \in E(R)$. We will say that the level-p^{n+1}-structure (x, y) is *degenerate* if the Weil pairing $e_{p^{n+1}}(x, y)$ is a primitive p^nth root of unity in R.

We let $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$ denote the substack of $\mathrm{Ell}(p^{n+1})$ whose R-valued points are elliptic curves equipped with a degenerate full level-p^{n+1} structure, so that we have a pullback diagram

$$\begin{array}{ccc} \mathrm{Ell}(p^{n+1})_{\mathrm{deg}} & \longrightarrow & \mathrm{Ell}(p^{n+1}) \\ \downarrow & & \downarrow{\scriptstyle \theta_{n+1}} \\ \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}]) & \longrightarrow & \mu_{p^{n+1}}. \end{array}$$

It follows that the inclusion $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \hookrightarrow \mathrm{Ell}(p^{n+1})$ is a closed immersion, so that $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$ is a Deligne-Mumford stack of finite type over $\mathrm{Spec}(\mathbf{Z})$.

Remark 2.2. Let R be a commutative ring, let n be a positive integer, and let u be a primitive p^{n+1}st root of unity in R: that is, an element of R satisfying the equation $1 + u^{p^n} + u^{2p^n} + \cdots + u^{(p-1)p^n} = 0$. If u is also a p^nth root of unity, then we must have $p = 0$ in R. In particular, the existence of an elliptic curve E over R equipped with a degenerate full level-p^{n+1} structure implies that $p = 0$ in R. That is, we can regard $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$ as a closed substack of $\mathrm{Ell}(p^{n+1})_{p=0}$.

Example 2.3. Let E be an elliptic curve over a field k of characteristic p. Then every full level-p^{n+1} structure on E is degenerate (since every p^{n+1}st root of unity in k is equal to 1, which is also a primitive p^nth root of unity). Consequently, the inclusion map $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \hookrightarrow \mathrm{Ell}(p^{n+1})_{p=0}$ is an equivalence on field-valued points.

Example 2.4. Let R be a commutative $\mathbf{F}_p$-algebra, let E be an elliptic curve over R, and let $x, y \in E(R)$ determine a full level-p^{n+1} structure on E. Let $E^{(p)}$ denote the pullback of E along the Frobenius map $\varphi : \mathrm{Spec}(R) \to \mathrm{Spec}(R)$, and let $F : E \to E^{(p)}$ denote the relative Frobenius map. Then the elements $F(x), F(y) \in E^{(p)}(R)$ determine a degenerate full level-p^{n+1} structure on the elliptic curve $E^{(p)}$: this follows from the calculation

$$e_{p^{n+1}}(F(x), F(y)) = e_{p^{n+1}}(x, y)^p,$$

since $e_{p^{n+1}}(x, y)$ is a primitive p^{n+1}st root of unity (Proposition 1.11). In other words, the absolute Frobenius map $\mathrm{Ell}(p^{n+1})_{p=0} \to \mathrm{Ell}(p^{n+1})_{p=0}$ factors through the closed substack $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \subseteq \mathrm{Ell}(p^{n+1})_{p=0}$.

For every integer $n > 0$, we have a forgetful map $\mathrm{Ell}(p^{n+1}) \to \mathrm{Ell}(p^n)$, given by the construction $(E, x, y) \mapsto (E, px, py)$. If $n > 1$, then this map carries $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$ into $\mathrm{Ell}(p^n)_{\mathrm{deg}}$. We will deduce Theorem 1.15 from the following:

Theorem 2.5. *Let $n > 1$, and consider the commutative diagram of groupoid-valued functors*

$$\begin{array}{ccc} \mathrm{Ell}(p^{n+1})_{p=0} & \longrightarrow & \mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \\ \downarrow & \swarrow & \downarrow \\ \mathrm{Ell}(p^n)_{p=0} & \longrightarrow & \mathrm{Ell}(p^n)_{\mathrm{deg}}, \end{array}$$

where the vertical maps are given by forgetting level structure and the horizontal maps by the absolute Frobenius. Then there exists a dotted arrow as indicated, which renders the diagram commutative (up to canonical isomorphism).

Proof of Theorem 1.15 from Theorem 2.5. Using Theorem 2.5, we obtain a commutative diagram of Deligne-Mumford stacks

$$\begin{array}{ccc} \cdots & \longrightarrow & \cdots \\ \downarrow & \swarrow & \downarrow \\ \mathrm{Ell}(p^4)_{p=0} & \longrightarrow & \mathrm{Ell}(p^4)_{\mathrm{deg}} \\ \downarrow & \swarrow & \downarrow \\ \mathrm{Ell}(p^3)_{p=0} & \longrightarrow & \mathrm{Ell}(p^3)_{\mathrm{deg}} \\ \downarrow & \swarrow & \downarrow \\ \mathrm{Ell}(p^2)_{p=0} & \longrightarrow & \mathrm{Ell}(p^2)_{\mathrm{deg}}. \end{array}$$

Passing to the inverse limit in the vertical direction, the horizontal maps determine a morphism of algebraic stacks $\rho : \mathrm{Ell}(p^\infty)_{p=0} \to \varprojlim_n \mathrm{Ell}(p^n)_{\mathrm{deg}}$, whose codomain can be identified with the closed substack of $\mathrm{Ell}(p^\infty)_{p=0}$ given by the vanishing locus of $\pi = \zeta_{p^2}^{p-1} + \zeta_{p^2}^{p-2} + \cdots + \zeta_{p^2} + 1$. Theorem 1.15 now follows from the observation that the Frobenius homomorphism $\varphi : \mathbf{F}_p[\zeta_{p^\infty}] \to \mathbf{F}_p[\zeta_{p^\infty}]$ is a surjection whose kernel is generated by π. □

To prove Theorem 2.5, we will need an auxiliary construction.

Proposition 2.6. *Let R be a commutative $\mathbf{F}_p$-algebra, let E be an elliptic curve over R, and suppose we are given a pair of points $x, y \in E^{(p)}(R)$. Assume that the pair (Vx, Vy) is a full level-p^n structure on E, for some $n > 0$. Then the pair (x, y) is a degenerate full level-p^{n+1} structure on $E^{(p)}$.*

Proof. The assertion is local with respect to the fppf topology on $\mathrm{Spec}(R)$. We may therefore assume without loss of generality that $x = Fx'$ and $y = Fy'$ for some $x', y' \in E(R)$. Our assumption that $(Vx, Vy) = (px', py')$ is a full level-p^n structure on E guarantees that (x', y') is a full level-p^{n+1} structure on E, so that the desired result follows from Example 2.4. □

Remark 2.7. Let R be a commutative $\mathbf{F}_p$-algebra, let E be an elliptic curve over R, and suppose we are given a pair of points $x, y \in E^{(p)}(R)$ such that Vx and Vy are p^n-torsion elements of $E(R)$. Then x and y are p^{n+1}-torsion points of $E^{(p)}(R)$, and we have an equality of Weil pairings $e_{p^{n+1}}(x, y) = e_{p^n}(Vx, Vy)$. To prove this, we can work locally with respect to the fppf topology on $\mathrm{Spec}(R)$ and thereby reduce to the case where $x = Fx'$ for some $x' \in E(R)$. In this case, we compute

$$\begin{aligned} e_{p^{n+1}}(x, y) &= e_{p^{n+1}}(Fx_0, y) \\ &= e_{p^{n+1}}(x_0, Vy) \\ &= e_{p^n}(px_0, Vy) \\ &= e_{p^n}(Vx, Vy). \end{aligned}$$

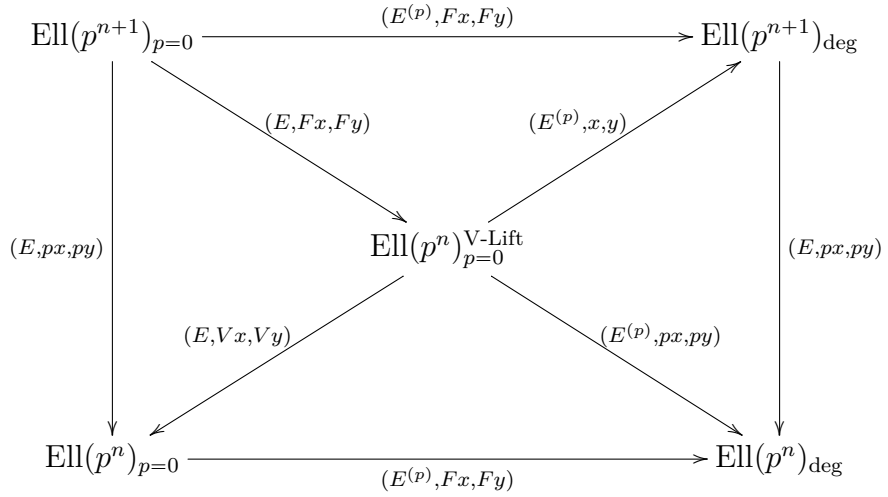
Notation 2.8. Let R be a commutative $\mathbf{F}_p$-algebra and let E be an elliptic curve over R. We let $V : E^{(p)} \to E$ denote the *Verschiebung map*: that is, the isogeny of elliptic curves which is dual to the relative Frobenius $F : E \to E^{(p)}$.

Construction 2.9. Let R be a commutative $\mathbf{F}_p$-algebra and let $n > 0$ be an integer. We let $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}(R)$ denote the groupoid whose objects are triples (E, x, y), where

E is an elliptic curve over R and $x, y \in E^{(p)}(R)$ have the property that the elements $Vx, Vy \in E(R)$ determine a full level-p^n structure on E. The construction $R \mapsto \mathrm{Ell}(p^n)^{\text{V-Lift}}(R)$ determines a functor from the category of commutative $\mathbf{F}_p$-algebras to the 2-category of groupoids, which we will denote by $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}$. By convention, we extend this functor to *all* commutative rings by setting $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}(R) = \varnothing$ when p does not vanish in R.

Remark 2.10. Let R be a commutative $\mathbf{F}_p$-algebra. Then we can identify the R-valued points of $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}$ with elliptic curves E over R equipped with a full level-p^n structure $\widetilde{x}, \widetilde{y} \in E(R)$, together with specified *Verschiebung lifts* $x, y \in E^{(p)}(R)$ of $\widetilde{x}$ and $\widetilde{y}$, respectively. Since the Verschiebung map $V : E^{(p)} \to E$ is finite flat of degree p, the construction $(E, x, y) \mapsto (E, V(x), V(y))$ determines a natural transformation $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} \to \mathrm{Ell}(p^n)_{p=0}$ which is finite flat of degree p^2. In particular, $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}$ is a Deligne-Mumford stack which is locally of finite type over $\mathrm{Spec}(\mathbf{F}_p)$.

Using Proposition 2.6, we see that the construction $(E, x, y) \mapsto (E^{(p)}, x, y)$ determines a map of Deligne-Mumord stacks $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} \to \mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$. For $n > 1$, this natural transformation fits into a diagram of Deligne-Mumford stacks



which commutes up to canonical isomorphism, where the outer square is the diagram of Theorem 2.5 (here each arrow has been labelled by its effect on a triple (E, x, y)). Consequently, to produce the extension required by Theorem 2.5, it will suffice to show that the diagonal map in the upper right is invertible. This is a consequence of the following converse to Proposition 2.6:

Theorem 2.11. *Let n be a positive integer. Then construction $(E, x, y) \mapsto (E^{(p)}, x, y)$ induces an isomorphism of Deligne-Mumford stacks $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} \to \mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$.*

Remark 2.12. For any positive integer n, we have a pullback diagram of Deligne-Mumford stacks

$$\begin{array}{ccc} \mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} & \xrightarrow{(E^{(p)},x,y)} & \mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \\ \downarrow{\scriptstyle (E,p^{n-1}x,p^{n-1}y)} & & \downarrow{\scriptstyle (E,p^{n-1}x,p^{n-1}y)} \\ \mathrm{Ell}(p)^{\text{V-Lift}}_{p=0} & \xrightarrow{(E^{(p)},x,y)} & \mathrm{Ell}(p^2)_{\mathrm{deg}}, \end{array}$$

where each arrow has been labelled by its effect on an object (E, x, y) of its domain. Consequently, to prove Theorem 2.11 in general, it suffices to treat the case $n = 1$. We will not make use of this observation, because it does not really simplify the proof.

Remark 2.13. More concretely, Theorem 2.11 asserts that if E is an elliptic curve over a commutative $\mathbf{F}_p$-algebra R equipped with a degenerate full level-p^{n+1} structure (x, y), then then there exists another elliptic curve E' over R and an isomorphism $\beta : E \simeq E'^{(p)}$ with the property that $(V\beta(x), V\beta(y))$ is a full level-p^n structure on E'; here $V : E'^{(p)} \to E'$ denotes the Verschiebung map for E'. Moreover, the pair (E', β) is well-defined up to unique isomorphism.

3 The Case of Ordinary Elliptic Curves

Let E be an elliptic curve over a commutative $\mathbf{F}_p$-algebra R. We will say that E is *ordinary* if each fiber of the map $E \to \mathrm{Spec}(R)$ is an ordinary elliptic curve. Let $\mathrm{Ell}_{\mathrm{ord}}$ denote the open substack of $\mathrm{Ell}_{p=0}$ whose R-valued points are given by ordinary elliptic curves over $\mathrm{Spec}(R)$. For each $n > 0$, we let $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\mathrm{ord}}$ denote the fiber product $\mathrm{Ell}(p^n)^{\text{V-Lift}} \times_{\mathrm{Ell}_{p=0}} \mathrm{Ell}_{\mathrm{ord}}$, and $\mathrm{Ell}(p^{n+1})_{\mathrm{deg,ord}}$ the fiber product $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \times_{\mathrm{Ell}} \mathrm{Ell}_{\mathrm{ord}}$. We regard $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\mathrm{ord}}$ and $\mathrm{Ell}(p^{n+1})_{\mathrm{deg,ord}}$ as open substacks of $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}$ and $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$, respectively.

Our goal in this section is to prove the following weak version of Theorem 2.11:

Theorem 3.1. *For each $n > 0$, the construction $(E, x, y) \mapsto (E^{(p)}, x, y)$ induces an isomorphism of Deligne-Mumford stacks $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\mathrm{ord}} \to \mathrm{Ell}(p^{n+1})_{\mathrm{deg,ord}}$.*

The proof is based on the following simple observation:

Lemma 3.2. *Let R be a commutative $\mathbf{F}_p$-algebra, let E be an ordinary elliptic curve over $\mathrm{Spec}(R)$, and suppose we are given a pair of points $x, y \in E(R)$ which determine a full level-p^n structure on E, which we identify with a map of group schemes*

$\gamma : (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \to E$. *Suppose that the Weil pairing* $e_{p^n}(x,y)$ *is equal to* 1. *Then the map* γ *factors (uniquely) as a composition* $(\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \to Q \hookrightarrow E$, *where* $Q \subseteq E$ *is an étale subgroup of degree* p^n.

Proof. Our assumption that E is ordinary guarantees that the p^n-torsion subgroup $E[p^n] \subseteq E$ fits into an exact sequence of finite flat group schemes

$$0 \to E[p^n]_{\mathrm{cn}} \to E[p^n] \xrightarrow{f} E[p^n]_{\text{ét}} \to 0,$$

where $E[p^n]_{\text{ét}}$ is étale over $\mathrm{Spec}(R)$ and $E[p^n]_{\mathrm{cn}}$ has connected fibers. Our assumption that x and y determine a level structure guarantees that the composite map $(\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \xrightarrow{\gamma} E[p] \to E[p]_{\text{ét}}$ is an epimorphism of étale group schemes over R (Remark 1.13). Let S denote its kernel and set $Q = (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2/S$, so that we have a diagram of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S & \longrightarrow & (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 & \xrightarrow{f\circ\gamma} & Q & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma_0} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \sim} & & \\ 0 & \longrightarrow & E[p^n]_{\mathrm{cn}} & \longrightarrow & E[p^n] & \xrightarrow{f} & E[p^n]_{\text{ét}} & \longrightarrow & 0. \end{array}$$

Note that the Weil pairing on $E[p^n]$ induces a perfect pairing of $E[p^n]_{\mathrm{cn}}$ with $E[p^n]_{\text{ét}}$. Our assumption that $e_{p^n}(x,y) = 1$ guarantees that the Weil pairing vanishes when restricted to $(\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2$, so that the map γ_0 vanishes. It follows that γ factors through a closed immersion $Q \hookrightarrow E[p^n] \hookrightarrow E$, whose image maps isomorphically onto $E[p^n]_{\text{ét}}$. □

Proof of Theorem 3.1. Let E be an ordinary elliptic curve over a commutative $\mathbf{F}_p$-algebra R and let $x, y \in E(R)$ be a degenerate full level-p^{n+1} structure on E. Then $e_{p^{n+1}}(x,y)$ is a p^nth root of unity. Applying Lemma 3.2 to the pair $(p^n x, p^n y)$, we deduce that there is a unique étale subgroup $Q \subseteq E$ of degree p which contains $p^n x$ and $p^n y$. Let E' denote the quotient E/Q, and let $f : E' \to E$ denote the dual of the quotient map $E \to E/Q$. Then f is an isogeny whose kernel can be identified with the Cartier dual of S. It follows that the Frobenius endomorphism of $\ker(f)$ vanishes: that is, $\ker(f)$ is contained in the kernel of the Frobenius isogeny $F : E' \to E'^{(p)}$. We can therefore factor F as a composition $E' \xrightarrow{f} E \xrightarrow{\beta} E'^{(p)}$. Since f and F have the same degree p, the map β is an isomorphism. Passing to duals, we conclude that the quotient map $E \to E/S$ factors as a composition $E \xrightarrow{\beta} E'^{(p)} \xrightarrow{V} E'$, where V is the Verschiebung map of E'. By construction, the map $V \circ \beta$ annihilates $p^n x$ and

$p^n y$, so that $\widetilde{x} = V\beta(x)$ and $\widetilde{y} = V\beta(y)$ are p^n-torsion points of E'. We will complete the proof by showing that the pair $(\widetilde{x}, \widetilde{y})$ is a full level-p^n structure on E' (note that the uniqueness of E' is clear from the construction, since any isogeny $E \to E''$ which annihilates $p^n x$ and $p^n y$ necessarily factors through $V \circ \beta$). Since E' is ordinary, it will suffice to show that the pair $(\widetilde{x}, \widetilde{y})$ satisfies the criteria of Remark 1.13:

(a) Let $\widetilde{\gamma} : (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \to E'[p^n]$ be the map of finite flat group schemes determined by the pair $(\widetilde{x}, \widetilde{y})$; we wish to show that the composite map $(\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \xrightarrow{\widetilde{\gamma}} E'[p^n] \to E'[p^n]_{\text{ét}}$ is an epimorphism. Let $Q^+ \subseteq E$ denote the inverse image of Q under the map $E \xrightarrow{p^n} E$, so that Q^+ is a finite flat subgroup of E of degree p^{2n+1}. We then have a commutative diagram of finite flat group schemes

$$\begin{array}{ccccc} (\underline{\mathbf{Z}/p^{n+1}\,\mathbf{Z}})^2 & \xrightarrow{(x,y)} & Q^+ & \longrightarrow & E[p^{n+1}]_{\text{ét}} \\ \downarrow & & \downarrow & & \downarrow \\ (\underline{\mathbf{Z}/p^{n}\,\mathbf{Z}})^2 & \xrightarrow{\widetilde{\gamma}} & E'[p^n] & \longrightarrow & E'[p^n]_{\text{ét}} \end{array}.$$

Since the right vertical map is an epimorphsim of finite flat group schemes over R, we are reduced to showing that the upper horizontal composition is an epimorphism. This follows from our assumption that the pair (x, y) determines a full level-p^{n+1} structure on E (Remark 1.13).

(b) The degeneracy of the level structure (x, y) implies that the Weil pairing $e_{p^{n+1}}(x, y)$ is a primitive p^nth root of unity in R. Applying Remark 2.7, we deduce that $e_{p^n}(\widetilde{x}, \widetilde{y}) = e_{p^{n+1}}(x, y)$ is also a primitive p^nth root of unity in R.

□

We conclude this section by sketching some of the obstacles encountered when attempting to extend the proof of Theorem 3.1 to the case of supersingular elliptic curve. Note that proceeding proof can be broken into two steps:

(i) Using the assumption that the Weil pairing $e_{p^{n+1}}(x, y)$ was a p^nth root of unity, we constructed another elliptic curve E' and an isomorphism $\beta : E \simeq E'^{(p)}$ with the property that $V\beta(x)$ and $V\beta(y)$ are p^n-torsion points of E'.

(ii) Using the stronger assumption that $e_{p^{n+1}}(x, y)$ is a *primitive* p^nth root of unity, we showed that the pair $(V\beta(x), V\beta(y))$ determines a full level-p^n structure on E'.

It follows from (i) that there is a commutative diagram of moduli stacks

$$\begin{array}{ccc} \mathrm{Ell}(p^{n+1})_{\mathrm{deg,ord}} & \longrightarrow & \mathrm{Ell}(p^n)^{\text{V-Lift}}_{\mathrm{ord}} \\ \downarrow & & \downarrow \\ \mathrm{Ell}(p)_{\zeta_p=1,\mathrm{ord}} & \xrightarrow{\psi} & \mathrm{Ell}_{\mathrm{ord}}, \end{array}$$

where the upper horizontal map is inverse to the isomorphism of Theorem 3.1, and the vertical maps are given by "forgetting" level structure; here the map ψ carries a triple (E, x, y) to the quotient of E/Q, where $Q \subseteq E$ is the étale subgroup generated by x and y (Lemma 3.2). This construction does not extend to supersingular elliptic curves:

Counterexample 3.3. The map $\psi : \mathrm{Ell}(p)_{\zeta_p=1,\mathrm{ord}} \to \mathrm{Ell}_{\mathrm{ord}}$ cannot be extended to a map $\overline{\psi} : \mathrm{Ell}(p)_{\zeta_p=1} \to \mathrm{Ell}_{p=0}$.

Proof. We sketch a proof under the assumption that $p = 2$. We assume that the reader is familiar with the theory of Igusa curves, which we we review in §6. The moduli stack $\mathrm{Ell}(p)_{\zeta_p=1}$ can be written as a union of $(p+1)$ irreducible components $C_0, C_1, \ldots, C_p$, each of which is isomorphic to the Igusa curve $\mathrm{Ig}(p)$ (Corollary 6.9). When restricted to each C_i, the map ψ admits a (unique) extension $\overline{\psi}_i : C_i \to \mathrm{Ell}_{p=0}$, which can be identified with the tautological map $\mathrm{Ig}(p) \to \mathrm{Ell}_{p=0}$ and is therefore finite flat of degree $p-1$ (hence an isomorphism in the case $p = 2$). Let E be a supersingular elliptic curve over the finite field $\mathbf{F}_p$. Then E admits a unique full level-p structure (given by the pair $(0, 0)$), which determines an $\mathbf{F}_p$-valued point η of the moduli stack $\mathrm{Ell}(p)$ belonging to each of the curves C_i (and therefore also to $\mathrm{Ell}(p)_{\zeta_p=1}$). Let V denote the Zariski tangent space to $\mathrm{Ell}(p)$ at the point η. Since $\mathrm{Ell}(p)$ is regular of dimension 2 (Proposition 6.7), V is a vector space of dimension 2 over $\mathbf{F}_p$. Each C_i is smooth over $\mathbf{F}_p$, so the Zariski tangent space to C_i at the point η is a 1-dimensional subspace $V_i \subseteq V$. Since the curves C_i meet transversely at the point η (Lemma 6.11), we have $V_i \neq V_j$ for $i \neq j$. It follows that every $V_0, V_1, \ldots, V_p$ is the collection of all 1-dimensional subspaces of V.

Now suppose that there exists a map $\overline{\psi} : \mathrm{Ell}(p)_{\zeta_p=1} \to \mathrm{Ell}_{p=0}$ which extends ψ. Let W denote the Zariski tangent space to $\mathrm{Ell}_{p=0}$ at the point $\overline{\psi}(\eta)$, so that W is a 1-dimensional vector space over $\mathbf{F}_p$. It follows that the differential of $\overline{\psi}$ induces an $\mathbf{F}_p$-linear map $V \to W$ whose kernel is nonzero and therefore contains the subspace V_i for some i. We conclude that the map $\overline{\psi}_i : C_i \to \mathrm{Ell}_{p=0}$ must be ramified at the point η, contradicting our observation that $\overline{\psi}_i$ has degree $p - 1 = 1$. □

It follows from Counterexample 3.3 that our proof of Theorem 3.1 cannot be naively extended to the supersingular case: given an R-valued point (E, x, y) of $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$, the construction of the elliptic curve E' of Remark 2.13 must somehow use the fact the assumption that $e_{p^{n+1}}(x, y)$ is a *primitive* p^nth root of unity.

4 Passage to Reduced Fibers

Let n be a positive integer. Then the comparison map of Theorem 2.11 fits into a commutative diagram

$$\begin{array}{ccc} \mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} & \xrightarrow{(E,x,y)\mapsto(E^{(p)},x,y)} & \mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \\ & {\scriptstyle (E,x,y)\mapsto e_{p^n}(Vx,Vy)} \searrow \quad \swarrow {\scriptstyle (E',x,y)\mapsto e_{p^{n+1}}(x,y)} & \\ & \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^n}]), & \end{array}$$

where $\mathbf{F}_p[\zeta_{p^n}]$ denotes the quotient $\mathbf{Z}[\zeta_{p^n}]/(p)$ (see Remark 2.7). To prove Theorem 2.11, it will be convenient to pass to the fiber of this map over the (unique) residue field of $\mathbf{F}_p[\zeta_{p^n}]$. This is harmless, by virtue of the following:

Proposition 4.1. *Let n be a nonnegative integer. Then:*

(*a*) *The map $\theta_n : \mathrm{Ell}(p^n) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}])$ of Construction 1.12 is a local complete intersection morphism.*

(*b*) *The map $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \to \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^n}])$ is a local complete intersection morphism.*

(*c*) *The map $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} \xrightarrow{(E,x,y)\mapsto e_{p^n}(Vx,Vy)} \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^n}])$ is a local complete intersection morphism.*

Proof. Note that $\mathbf{Z}[\zeta_{p^n}]$ is a Dedekind ring. Consequently, to show that θ_n is a local complete intersection morphism, it suffices to observe that $\mathrm{Ell}(p^n)$ is regular (Proposition 6.7) and that $\mathrm{Ell}(p^n)$ is torsion-free as a module over $\mathbf{Z}[\zeta_{p^n}]$, or equivalently as a module over $\mathbf{Z}$ (Remark 6.8). This proves (*a*). To deduce (*b*) from (*a*), it will

suffice to show that the upper square in the diagram

$$\begin{array}{ccc} \mathrm{Ell}(p^{n+1})_{\mathrm{deg}} & \longrightarrow & \mathrm{Ell}(p^{n+1}) \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^n}]) & \longrightarrow & \mathrm{Spec}(\mathbf{Z}[\zeta_{p^{n+1}}]) \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}]) & \longrightarrow & \mu_{p^{n+1}} \end{array}$$

is a pullback diagram. This is clear, since the outer rectangle is a pullback by definition and the lower square is a pullback by virtue of Remark 2.2. To prove (c), we note that the relevant map admits a factorization

$$\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} \xrightarrow{f} \mathrm{Ell}(p^n)_{p=0} \xrightarrow{g} \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^n}])$$

where g is a pullback of θ_n (and therefore a local complete intersection morphism by virtue of (a)). We are therefore reduced to proving that f is a local complete intersection morphism. Fix a commutative ring R equipped with a map $\mathrm{Spec}(R) \to \mathrm{Ell}(p^n)_{p=0}$, classifying an elliptic curve E over R equipped with a full level-p^n structure $\overline{x}, \overline{y} \in E(R)$, and form a pullback diagram

$$\begin{array}{ccc} X & \xrightarrow{f_R} & \mathrm{Spec}(R) \\ \downarrow & & \downarrow \\ \mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} & \xrightarrow{f} & \mathrm{Ell}(p^n)_{p=0}; \end{array}$$

we wish to show that f_R is a local complete intersection morphism. Note that the map f_R fits into a pullback square

$$\begin{array}{ccc} X & \xrightarrow{f_R} & \mathrm{Spec}(R) \\ \downarrow & & \downarrow{\scriptstyle (\overline{x},\overline{y})} \\ E^{(p)} \times_{\mathrm{Spec}(R)} E^{(p)} & \xrightarrow{V \times V} & E \times_{\mathrm{Spec}(R)} E. \end{array}$$

We conclude by observing that the map $V \times V : E^{(p)} \times_{\mathrm{Spec}(R)} E^{(p)} \to E \times_{\mathrm{Spec}(R)} E$ is a local complete intersection morphism, because it is a flat map between smooth R-schemes. $\square$

Notation 4.2. For every positive integer n, we let $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ denote the closed substack of $\mathrm{Ell}(p^n)$ given by the vanishing locus of $\zeta_{p^n} - 1$: that is, the closed substack which parametrizes elliptic curves E equipped with a full level-p^n structure (x, y) for which the Weil pairing $e_{p^n}(x, y)$ is equal to 1. Note that $\mathrm{Ell}(p^n)_{\zeta_{p^n}} = 1$ is defined over the quotient ring $\mathbf{Z}[\zeta_{p^n}]/(\zeta_{p^n} - 1) \simeq \mathbf{F}_p$. In particular, $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ is contained in the closed substack $\mathrm{Ell}(p^n)_{p=0} \subseteq \mathrm{Ell}(p^n)$ given by the vanishing locus of p. If $n > 1$, we also have $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1} \subseteq \mathrm{Ell}(p^n)_{\mathrm{deg}}$.

We let $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}$ denote the fiber product $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} \times_{\mathrm{Ell}(p^n)_{p=0}} \mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$, which we regard a closed substack of $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}$.

Remark 4.3. Note that the closed substacks

$$\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1} \subseteq \mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0} \qquad \mathrm{Ell}(p^n)_{\zeta_{p^n}=1} \subseteq \mathrm{Ell}(p^n)_{p=0}$$

can be described as the vanishing locus of the element $\zeta_{p^n} - 1$, which is a nilpotent element of the local Artinian ring $\mathbf{F}_p[\zeta_{p^n}]$. We will later see that the stacks $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}$ and $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ are reduced (Theorems 5.4 and 5.5). It follows that they can be identified with the reductions of the Deligne-Mumford stacks $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{p=0}$ and $\mathrm{Ell}(p^n)_{p=0}$, respectively.

We will deduce Theorem 2.11 from the following more basic assertion:

Theorem 4.4. *For each $n > 0$, the construction $(E, x, y) \mapsto (E^{(p)}, x, y)$ induces an isomorphism of Deligne-Mumford stacks*

$$\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1} \to \mathrm{Ell}(p^{n+1})_{\zeta_{p^{n+1}}=1}.$$

Proof of Theorem 2.11 from Theorem 4.4. We wish to show that the horizontal map in the diagram

$$\begin{array}{ccc} \mathrm{Ell}(p^n)^{\text{V-Lift}} & \xrightarrow{(E,x,y)\mapsto(E^{(p)},x,y)} & \mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \\ & {\scriptstyle (E,x,y)\mapsto e_{p^n}(Vx,Vy)} \searrow \quad \swarrow {\scriptstyle (E',x,y)\mapsto e_{p^{n+1}}(x,y)} & \\ & \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^n}]) & \end{array}$$

is an isomorphism. Theorem 4.4 asserts that the horizontal map becomes an equivalence after pulling back along the closed immersion $i : \mathrm{Spec}(\mathbf{F}_p) \hookrightarrow \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^n}])$. The desired result now follows from the flatness of the vertical maps (Proposition 4.1), since the ideal sheaf associated to the closed immersion i is nilpotent. $\square$

5 Digression: The δ-Invariant of a Curve

Let X be a Noetherian Deligne-Mumford stack, let $|X|$ denote its underlying topological space, and let $\mathscr{F}$ be a coherent sheaf on X which is supported at the set of closed points of $|X|$. For each closed point $x \in X$, we can choose an étale map $f : \mathrm{Spec}(R) \to X$ and a maximal ideal $\mathfrak{m} \subseteq R$ lying over the point x. In this case, the stalk of the sheaf $f^* \mathscr{F}$ at the point $\mathfrak{m}$ is an $R_{\mathfrak{m}}$-module of finite length. We will denote this length by $\mathrm{len}_x(\mathscr{F})$ and refer to it as the *length of $\mathscr{F}$ at the point x*. Note that the quantity $\mathrm{len}_x(\mathscr{F})$ is independent of the choice of the map $f : \mathrm{Spec}(R) \to X$ and the maximal ideal $\mathfrak{m} \subseteq R$.

Definition 5.1. Let X be reduced Deligne-Mumford stack which is Noetherian of dimension 1, let $\pi : \widetilde{X} \to X$ denote its normalization, and assume that the map π is finite (this condition is satisfied, for example, if X is of finite type over a field). Then the cokernel of the unit map $\mathcal{O}_X \to \pi_* \mathcal{O}_{\widetilde{X}}$ is a coherent sheaf supported at the set of closed points of $|X|$. For each closed point $x \in |X|$, we let $\delta_x(X)$ denote the length $\mathrm{len}_x(\mathrm{coker}(\mathcal{O}_X \to \pi_* \mathcal{O}_{\widetilde{X}}))$. We will refer to $\delta_x(X)$ as the *δ-invariant of X at the point x*.

Example 5.2. Let Z be a Deligne-Mumford stack which is regular of Krull dimension 2 and let $D, D' \subseteq Z$ be reduced effective divisors having normalizations $\pi : \widetilde{D} \to D$ and $\pi' : \widetilde{D}' \to D'$. Assume that the maps π and π' are finite and that the intersection $D \times_Z D'$ has Krull dimension 0. Then the sum $D + D'$ is a reduced effective divisor in Z having normalization $\widetilde{D} \amalg \widetilde{D}'$. Moreover, for every closed point $x \in |Z|$ belonging to both D and D', we have an equality

$$\delta_x(D + D') = \delta_x(D) + \delta_x(D') + i_x(D, D'),$$

where $i_x(D, D')$ denotes the intersection number of D and D' at the point x (that is, the length $\mathrm{len}_x(\mathscr{F})$, where $\mathscr{F}$ denotes the structure sheaf of the intersection $D_i \times_Z D_j$).

We can use Definition 5.1 to give a numerical criterion for showing that a map between curves is an isomorphism:

Proposition 5.3. *Let $f : X \to Y$ be a finite morphism between reduced Deligne-Mumford stacks which are of finite type and relative dimension 1 over a field k. Suppose that:*

(*a*) *There exists a dense open substack $U \subseteq Y$ for which the projection $X \times_Y U \to U$ is an isomorphism.*

(*b*) *For each point $y \in |Y|$ which does not belong to U, we can choose some point $x \in |X|$ lying over Y which satisfies $\delta_x(X) = \delta_y(Y)$.*

Then f is an isomorphism.

Proof. The assertion is local with respect to the étale topology on Y. We may therefore assume without loss of generality that $Y = \mathrm{Spec}(R)$, where R is a reduced k-algebra of Krull dimension 1, and that $U \subseteq Y$ is the complement of a single point corresponding to some maximal ideal $\mathfrak{m} \subseteq R$. Since f is finite, we can write $X = \mathrm{Spec}(S)$, where S is a finite R-algebra. Let $\widetilde{R}$ denote the normalization of R. It follows from (a) that we can also identify $\widetilde{R}$ with the normalization of S, so that we can regard S as an R-subalgebra of $\widetilde{R}$. We have an exact sequence of finite length R-modules

$$0 \to S/R \to \widetilde{R}/R \to \widetilde{R}/S \to 0.$$

The length of $\widetilde{R}/S$ as an R-module is at least as large as the length of $\widetilde{R}/S$ as an S-module, which (by virtue of (b)) is the same as the length of $\widetilde{R}/R$ as an R-module. It follows that the quotient S/R is trivial, so that f is an isomorphism as desired. □

We will deduce Theorem 4.4 from the following pair of results, which we prove in §6 and §7.

Theorem 5.4. *Let n be a positive integer. Then:*

(1) *The moduli stack $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ is reduced.*

(2) *For each supersingular point $z \in |\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}|$, we have*

$$\delta_z(\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}) = (1/2)(p^{3n-1} + p^{3n-2})$$

.

Theorem 5.5. *Let n be a positive integer. Then:*

(1) *The moduli stack $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}$ is reduced.*

(2) *For each supersingular point $z \in |\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}|$, we have*

$$\delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}) = (1/2)(p^{3n+2} + p^{3n+1})$$

.

Proof of Theorem 4.4. It follows from Theorem 3.1 that the map

$$u : \mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1} \to \mathrm{Ell}(p^{n+1})_{\zeta_{p^{n+1}}=1} \qquad (E, x, y) \mapsto (E^{(p)}, x, y)$$

is an isomorphism over the ordinary locus

$$\mathrm{Ell}(p^{n+1})_{\zeta_{p^{n+1}}=1,\mathrm{ord}} = \mathrm{Ell}(p^{n+1})_{\zeta_{p^{n+1}}=1g} \times_{\mathrm{Ell}} \mathrm{Ell}_{\mathrm{ord}} .$$

It follows from Theorems 5.4 and 5.5 that each supersingular point of $\mathrm{Ell}(p^{n+1})_{\zeta_{p^{n+1}}=1}$ can be lifted uniquely to a supersingular point of $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}$ having the same δ-invariant, so that u is an isomorphism by the criterion of Proposition 5.3. □

6 Igusa Curves

For each $n > 0$, the moduli stack $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ is an effective Cartier divisor in the moduli stack $\mathrm{Ell}(p^n)$ (given as the vanishing locus of the regular function $\zeta_{p^n} - 1$). In this section, we review the description of $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ as a sum of regular divisors, meeting nontransversely at the supersingular points of $\mathrm{Ell}(p^n)$ (Corollary 6.9 below), and use this description to compute the δ-invariants of $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$. For a more detailed discussion, we refer the reader to [3].

Notation 6.1. Let n be a positive integer and let $S \subseteq (\mathbf{Z}/p^n\,\mathbf{Z})^2$ be a subgroup. We let $\mathrm{Ell}(p^n)_S$ denote the closed substack of $\mathrm{Ell}(p^n)$ whose R-valued points are given by pairs (E, γ), where E is an elliptic curve over $\mathrm{Spec}(R)$ and $\gamma : (\mathbf{Z}/p^n\,\mathbf{Z})^2 \to E(R)$ is a full level-p^n structure on E satisfying $\gamma|_S = 0$.

In the case where the subgroup S is cyclic of order p^n (which is the only case we will consider), the substack $\mathrm{Ell}(p^n)_S$ is contained in $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$. In particular, it is contained in the vanishing locus of p.

It will be useful to have an alternate description of the closed substacks $\mathrm{Ell}(p^n)_S \subseteq \mathrm{Ell}(p^n)$.

Notation 6.2. Let R be a commutative $\mathbf{F}_p$-algebra and let E be an elliptic curve over R. For each integer $n \geqslant 0$, let $V^n : E^{(p^n)} \to E$ denote the iterated Verschiebung map, and regard the kernel $\ker(V^n)$ as a relative effective divisor of degree p^n in the elliptic curve $E^{(p^n)}$. If $n > 0$, then the map V^n factors as a composition

$$E^{(p^n)} \xrightarrow{V^{n-1}} E^{(p)} \xrightarrow{V} E,$$

where V^{n-1} denotes the $(n-1)$st iterate of the Verschiebung map of $E^{(p)}$. It follows that $\ker(V^{n-1}) \subseteq \ker(V^n)$, so we can write $\ker(V^n) = \ker(V^{n-1}) + D$ for some uniquely determined relative effective divisor $D \subseteq E^{(p^n)}$ of degree $p^n - p^{n-1}$. We say that a point $x \in E^{(p^n)}(R)$ is a *cyclic generator of* $\ker(V^n)$ if it belongs to the subset $D(R) \subseteq E^{(p^n)}(R)$.

Remark 6.3. In the situation of Notation 6.2, let x be an R-valued point of $\ker(V^n)$, which we can identify with a map of finite flat group schemes $\underline{\mathbf{Z}/p^n\,\mathbf{Z}} \xrightarrow{\alpha} \ker(V^n) \subseteq E^{(p^n)}$. If E is ordinary, then x is a cyclic generator of $\ker(V^n)$ if and only if α is an isomorphism. Beware that if E has supersingular fibers, then α is never an isomorphism (since $\ker(V^n)$ is not an étale group scheme over R).

Definition 6.4. Let n be a positive integer. If R is a commutative $\mathbf{F}_p$-algebra, we let $\mathrm{Ig}(p^n)(R)$ denote the category whose objects are pairs (E, x), where E is an elliptic curve over R and x is a cyclic generator of $\ker(V^n) \subseteq E^{(p^n)}$; a morphism from (E, x) to (E', x') is an isomorphism of elliptic curve $E \simeq E'$ for which the induced map $E^{(p^n)} \simeq E'^{(p^n)}$ carries x to x'. The construction $R \mapsto \mathrm{Ig}(p^n)(R)$ determines a groupoid-valued functor on category of commutative $\mathbf{F}_p$-algebras, which we extend formally to all commutative rings by setting $\mathrm{Ig}(p^n)(R) = \varnothing$ if $p \neq 0$ in R. We will refer to $\mathrm{Ig}(p^n)$ as the *nth Igusa curve*.

Remark 6.5. In the situation of Definition 6.4, the construction $(E, x) \mapsto E$ determines a map $\mathrm{Ig}(p^n) \to \mathrm{Ell} \times \mathrm{Spec}(\mathbf{F}_p)$ which is finite flat of degree $p^n - p^{n-1}$. In particular, the Igusa curve $\mathrm{Ig}(p^n)$ is a Deligne-Mumford stack which is of finite type over $\mathrm{Spec}(\mathbf{F}_p)$.

Remark 6.6. Let $\mathrm{Ig}(p^n)_{\mathrm{ord}}$ denote the open substack of $\mathrm{Ig}(p^n)$ given by the inverse image of $\mathrm{Ell}_{\mathrm{ord}}$. Then the projection map $\mathrm{Ig}(p^n)_{\mathrm{ord}} \to \mathrm{Ell}_{\mathrm{ord}}$ is finite étale of degree $p^n - p^{n-1}$. It follows that the Igusa curve $\mathrm{Ig}(p^n)_{\mathrm{ord}}$ is smooth of dimension 1 over $\mathrm{Spec}(\mathbf{F}_p)$.

Proposition 6.7 (Katz-Mazur, Theorems 5.1.1 and 13.7.6)**.** *Let n be a positive integer. Then:*

(1) *The moduli stack $\mathrm{Ell}(p^n)$ is regular of dimension 2.*

(2) *Let $S \subseteq (\mathbf{Z}/p^n\,\mathbf{Z})^2$ be a subgroup which is isomorphic to $\mathbf{Z}/p^n\,\mathbf{Z}$. Then the closed substack $\mathrm{Ell}(p^n)_S \subseteq \mathrm{Ell}(p^n)$ is smooth of dimension 1 over $\mathrm{Spec}(\mathbf{F}_p)$.*

(3) *Let* $\alpha : (\mathbf{Z}/p^n\mathbf{Z})^2 \to \mathbf{Z}/p^n\mathbf{Z}$ *be a surjection of abelian groups with kernel* $S \subseteq (\mathbf{Z}/p^n\mathbf{Z})^2$. *Then there is canonical isomorphism of Deligne-Mumford stacks* $\theta : \mathrm{Ig}(p^n) \to \mathrm{Ell}(p^n)_S$, *given on* R*-valued points by the construction* $(E, x) \mapsto (E^{(p^n)}, \gamma)$, *where* $\gamma : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E^{(p^n)}(R)$ *is given by the formula* $\gamma(v) = \alpha(v)x$.

(4) *The Igusa curve* $\mathrm{Ig}(p^n)$ *is smooth of dimension* 1 *over* $\mathrm{Spec}(\mathbf{F}_p)$.

Remark 6.8. It follows from Proposition 6.7 that the map $\mathrm{Ell}(p^n) \to \mathrm{Spec}(\mathbf{Z})$ is flat.

Proof of Proposition 6.7. We first show that the map θ of (3) is an isomorphism over the ordinary locus $\mathrm{Ell}(p^n)_{S,\mathrm{ord}} = \mathrm{Ell}(p^n)_S \times_{\mathrm{Ell}} \mathrm{Ell}_{\mathrm{ord}}$. Let R be a commutative $\mathbf{F}_p$-algebra and let E' be an ordinary elliptic curve over R equipped with a full level-p^n structure $\gamma : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E'(R)$ which annihilates S. Then γ factors as a composition $(\mathbf{Z}/p^n\mathbf{Z})^2 \xrightarrow{\alpha} \mathbf{Z}/p^n\mathbf{Z} \xrightarrow{\gamma'} E'(R)$. Applying Lemma 3.2, we see that γ' induces an isomorphism from $\underline{\mathbf{Z}/p^n\mathbf{Z}}$ onto an étale subgroup $S' \subseteq E'$. Setting $E = E'/S'$, we obtain an isomorphism $E' \simeq E^{(p^n)}$ carrying $\gamma'(1)$ to a cyclic generator of $\ker(V^n)$. It is easy to see that the construction $(E', \gamma) \mapsto (E, \gamma'(1))$ is an inverse of θ over the ordinary locus $\mathrm{Ell}(p^n)_{S,\mathrm{ord}}$.

We now prove (2). We first note that the closed substack $\mathrm{Ell}(p^n)_S \subseteq \mathrm{Ell}(p^n)$ is given locally as the vanishing locus of a single regular function. Since $\mathrm{Ell}(p^n)$ is of pure dimension 2 (Proposition 1.9), each irreducible component of $\mathrm{Ell}(p^n)_S$ has Krull dimension $\geqslant 1$. Let $X \subseteq \mathrm{Ell}(p^n)_S$ be the closed substack whose R-valued points are pairs (E, γ), where E is an elliptic curve over R and $\gamma : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E(R)$ is a full level-p^n structure which is identicially zero. It follows from Remark 1.7 that the projection map $\mathrm{Ell}(p^n) \to \mathrm{Ell}$ induces an isomorphism of Deligne-Mumford stacks $X \to \mathrm{Ell}^{\mathrm{ss}}$, where $\mathrm{Ell}^{\mathrm{ss}} \subseteq \mathrm{Ell}$ is the reduced closed substack parametrizing supersingular elliptic curves in characteristic p (which is étale over $\mathrm{Spec}(\mathbf{F}_p)$). Since X can be described locally as the vanishing locus of a regular function on $\mathrm{Ell}(p^n)_S$, it follows that $\mathrm{Ell}(p^n)_S$ is smooth of dimension 1 over $\mathrm{Spec}(\mathbf{F}_p)$ at the points of X. It will therefore suffice to show that $\mathrm{Ell}(p^n)_S$ is smooth of dimension 1 over $\mathrm{Spec}(\mathbf{F}_p)$ at every closed point which does not belong to X. Since every such point belongs to the open substack $\mathrm{Ell}(p^n)_{S,\mathrm{ord}} \subseteq \mathrm{Ell}(p^n)_S$, we are reduced (by the first part of the proof) to showing that the stack $\mathrm{Ig}(p^n)_{\mathrm{ord}}$ is smooth of dimension 1 over $\mathrm{Spec}(\mathbf{F}_p)$, which follows from Remark 6.6.

We now prove (1). Suppose we are given a geometric point $\eta : \mathrm{Spec}(k) \to \mathrm{Ell}(p^n)$, corresponding to an elliptic curve E over k equipped with a full level-p^n structure

$\gamma : (\mathbf{Z}/p^n\,\mathbf{Z})^2 \to E(k)$; we wish to show that $\mathrm{Ell}(p^n)$ is regular at the image of η. If the field k has characteristic different from p, then the map $\mathrm{Ell}(p^n) \to \mathrm{Ell}$ is étale in a neighborhood of η, so the desired result follows from the regularity of the moduli stack Ell. We may therefore assume that k has characteristic p. In this case, the map γ must annihilate a subgroup $S \subseteq (\mathbf{Z}/p^n\,\mathbf{Z})^2$ which is isomorphic to $\mathbf{Z}/p^n\,\mathbf{Z}$, so that we can regard (E, γ) as a k-valued point of the closed substack $\mathrm{Ell}(p^n)_S \subseteq \mathrm{Ell}(p^n)$. Since $\mathrm{Ell}(p^n)_S$ is regular of dimension 1 and is given locally as the vanishing locus of a single function on $\mathrm{Ell}(p^n)$, it follows that $\mathrm{Ell}(p^n)$ is regular of dimension 2 near the point η (recall that $\mathrm{Ell}(p^n)$ is of pure Krull dimension 2 by virtue of Proposition 1.9).

We now prove (3). Note first that the map $\theta : \mathrm{Ig}(p^n) \to \mathrm{Ell}(p^n)_S$ is relatively representable (since every nontrivial automorphism of an elliptic curve E over an $\mathbf{F}_p$-algebra R is also nontrivial on the iterated Frobenius pullback $E^{(p^n)}$). Since $\mathrm{Ell}(p^n)_S$ is smooth of dimension 1 over $\mathrm{Spec}(\mathbf{F}_p)$ and θ is an isomorphism over a dense open set, it will suffice to show that the stack $\mathrm{Ig}(p^n)$ is reduced. Note that $\mathrm{Ig}(p^n)$ can be realized as an effective Cartier divisor in a Deligne-Mumford stack which is smooth of dimension 2 over $\mathrm{Spec}(\mathbf{F}_p)$, and is therefore a local complete intersection. Consequently, to show that $\mathrm{Ig}(p^n)$ is reduced, it will suffice to show that $\mathrm{Ig}(p^n)$ is reduced at each generic point, which follows from Remark 6.6.

Assertion (4) follows immediately from (2) and (3). □

Corollary 6.9 (Katz-Mazur, Theorem 13.7.6)**.** *For each $n > 0$, the moduli stack $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ can be identified with the sum $\sum_S \mathrm{Ell}(p^n)_S$ as an effective Cartier divisor in $\mathrm{Ell}(p^n)$; here the sum is taken over all subgroups $S \subseteq (\mathbf{Z}/p^n\,\mathbf{Z})^2$ which are isomorphic to $\mathbf{Z}/p^n\,\mathbf{Z}$.*

Proof. It follows from Proposition 6.7 that each $\mathrm{Ell}(p^n)_S$ is an effective Cartier divisor in $\mathrm{Ell}(p^n)$, so that $D = \sum_S \mathrm{Ell}(p^n)_S$ is well-defined as an effective Cartier divisor in $\mathrm{Ell}(p^n)$. Moreover, the substack $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1} \subseteq \mathrm{Ell}(p^n)$ is an effective Cartier divisor by construction. By virtue of Lemma 3.2, these Cartier divisors agree outside of the supersingular locus of $\mathrm{Ell}(p^n)$, and therefore coincide (since the supersingular locus has codimension 2). □

Lemma 6.10. *Let $0 \leqslant m < n$, and let D denote the closed substack of $\mathrm{Ig}(p^n)$ parametrizing those pairs (E, x) where x is a cyclic generator of $\ker(V^n) \subseteq E^{(p^n)}$ satisfying $p^m x = 0$. Then D has multiplicity p^{2m} at each supersingular point of $\mathrm{Ig}(p^n)$.*

Proof. The Igusa curve $\mathrm{Ig}(p^{n-m})$ parametrizes pairs (E, y), where y is a cyclic generator of $\ker(V^{n-m}) \subseteq E^{(p^{n-m})}$. Let $D_0 \subseteq \mathrm{Ig}(p^{n-m})$ be the closed substack parametrizing

such pairs where $y = 0$. The proof of Proposition 6.7 shows that D_0 has multiplicity 1 at each supersingular point of $\mathrm{Ig}(p^{n-m})$. Unwinding the definitions, we see that D can be identified with the inverse image of D_0 under the composition

$$\mathrm{Ig}(p^n) \xrightarrow{(E,x) \mapsto (E, V^m x)} \mathrm{Ig}(p^{n-m}) \xrightarrow{\varphi^m} \mathrm{Ig}(p^{n-m})$$

where φ denotes the absolute Frobenius map of $\mathrm{Ig}(p^{n-m})$. Since $\mathrm{Ig}(p^{n-m})$ is smooth of dimension 1 over $\mathrm{Spec}(\mathbf{F}_p)$, the pullback $\varphi^{m*} D_0$ has multiplicity p^m at each supersingular point of $\mathrm{Ig}(p^{n-m})$. We complete the proof by observing that the map $\mathrm{Ig}(p^n) \xrightarrow{(E,x) \mapsto (E, V^m x)} \mathrm{Ig}(p^{n-m})$ has degree p^m and is totally ramified over each supersingular point of $\mathrm{Ig}(p^{n-m})$. □

Lemma 6.11. *[Katz-Mazur, Corollary 13.8.5] Let S and T be distinct subgroups of $(\mathbf{Z}/p^n \mathbf{Z})^2$, each isomorphic to $\mathbf{Z}/p^n \mathbf{Z}$, and regard $\mathrm{Ell}(p^n)_S$ and $\mathrm{Ell}(p^n)_T$ as effective divisors in $\mathrm{Ell}(p^n)$. Then, at each supersingular point of $\mathrm{Ell}(p^n)$, the intersection multiplicity of $\mathrm{Ell}(p^n)_S$ and $\mathrm{Ell}(p^n)_T$ is equal to $|(\mathbf{Z}/p^n \mathbf{Z})^2/(S+T)|^2$.*

Proof. Without loss of generality, we may assume that S and T are the cyclic subgroups of $(\mathbf{Z}/p^n \mathbf{Z})^2$ generated by $(1,0)$ and $(1, p^m)$, for some $m < n$. Under the isomorphism $\mathrm{Ig}(p^n) \simeq \mathrm{Ell}(p^n)_S$ of Proposition 6.7, the intersection $\mathrm{Ell}(p^n)_S \times_{\mathrm{Ell}(p^n)} \mathrm{Ell}(p^n)_T$ corresponds to the divisor $D \subseteq \mathrm{Ig}(p^n)$ described in Lemma 6.10, which has multiplicity p^{2m} at each supersingular point. □

Proof of Theorem 5.4. Corollary 6.9 supplies an identification

$$\mathrm{Ell}(p^n)_{\zeta_{p^n}=1} = \sum_S \mathrm{Ell}(p^n)_S$$

of effective Cartier divisors in $\mathrm{Ell}(p^n)$. In particular, $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ is smooth away from the locus of supersingular elliptic curves, and therefore generically reduced. Since it is an effective Cartier divisor in the regular Deligne-Mumford stack $\mathrm{Ell}(p^n)$, it is a local complete intersection, and is therefore everywhere reduced. At each supersingular point z of $|\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}|$, repeated application of Example 5.2 gives the identity

$$\delta_z(\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}) = \frac{1}{2} \sum_{S \neq T} i_z(\mathrm{Ell}(p^n)_S, \mathrm{Ell}(p^n)_T),$$

where $i_z(\mathrm{Ell}(p^n)_S, \mathrm{Ell}(p^n)_T)$ denotes the intersection multiplicity of $\mathrm{Ell}(p^n)_S$ and $\mathrm{Ell}(p^n)_T$ at the point x and is therefore given by $|(\mathbf{Z}/p^n \mathbf{Z})^2/(S+T)|^2$ (Lemma 6.11). Here there are $p^n + p^{n-1}$ choices for the cyclic subgroup $S \subseteq (\mathbf{Z}/p^n \mathbf{Z})^2$. For

every such subgroup S, there are exactly p^n subgroups T for which $S + T = (\mathbf{Z}/p^n\,\mathbf{Z})^2$, and for each $0 < m < n$ there are exactly $p^{n-m} - p^{n-m-1}$ subgroups T satisfying $|(\mathbf{Z}/p^n\,\mathbf{Z})^2/(S+T)| = p^m$. We therefore have

$$\begin{aligned}
\delta_z(\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}) &= \frac{1}{2}\sum_{S \neq T} i_z(\mathrm{Ell}(p^n)_S, \mathrm{Ell}(p^n))_T \\
&= \frac{p^n + p^{n-1}}{2}(p^n + \sum_{0<m<n}(p^{n-m} - p^{n-m-1})p^{2m}) \\
&= \frac{p^n + p^{n-1}}{2}(p^n + \sum_{0<m<n}(p^{n+m} - p^{n+m-1})) \\
&= \frac{p^n + p^{n-1}}{2}p^{2n-1} \\
&= \frac{p^{3n-1} + p^{3n-2}}{2}.
\end{aligned}$$

□

7 Ramification of Igusa Curves

For each $n > 0$, the construction $(E, x) \mapsto (E, Vx)$ determines a map of Igusa curves $\mathrm{Ig}(p^{n+1}) \to \mathrm{Ig}(p^n)$. It follows from Remark 6.6 that this map is étale over the ordinary locus $\mathrm{Ig}(p^n)_{\mathrm{ord}} \subseteq \mathrm{Ig}(p^n)$. However, it is totally ramified at each supersingular point. We will need the following more quantitative assertion:

Proposition 7.1. *Let $n > 0$ and let $y \in |\mathrm{Ig}(p^{n+1}) \times_{\mathrm{Ig}(p^n)} \mathrm{Ig}(p^{n+1})|$ be a point lying over the supersingular locus $|\mathrm{Ell}^{\mathrm{ss}}| \subseteq |\mathrm{Ell}|$. Then we have an equality*

$$\delta_y(\mathrm{Ig}(p^{n+1}) \times_{\mathrm{Ig}(p^n)} \mathrm{Ig}(p^{n+1})) = (1/2)(p^{2n+2} - p^{2n+1}).$$

Remark 7.2. The map $\mathrm{Ig}(p^{n+1}) \to \mathrm{Ig}(p^n)$ is a finite and generically étale map between Deligne-Mumford stacks which are smooth of dimension 1 over $\mathrm{Spec}(\mathbf{F}_p)$. To any such map, we can associate a *different ideal sheaf* $\mathfrak{D}_{\mathrm{Ig}(p^{n+1})/\mathrm{Ig}(p^n)} \subseteq \mathcal{O}_{\mathrm{Ig}(p^{n+1})}$, defined as the annihilator ideal of the sheaf of relative Kähler differentials $\Omega_{\mathrm{Ig}(p^{n+1})/\mathrm{Ig}(p^n)}$. Proposition 7.1 is equivalent to the statement that the different $\mathfrak{D}_{\mathrm{Ig}(p^{n+1})/\mathrm{Ig}(p^n)}$ has multiplicity $p^{2n+2} - p^{2n+1}$ at each supersingular point of $\mathrm{Ig}(p^{n+1})$.

Proof of Proposition 7.1. Choose a scheme C and an étale map $f : C \to \mathrm{Ig}(p^n)$, classifying an elliptic curve E over C together with a cyclic generator $\ker(V^n) \subseteq E^{(p^n)}$.

Then C is smooth of dimension 1 over $\mathrm{Spec}(\mathbf{F}_p)$ (Proposition 6.7). Set $\widetilde{C} = C \times_{\mathrm{Ig}(p^n)} \mathrm{Ig}(p^{n+1})$ and $D = \widetilde{C} \times_C \widetilde{C}$. Then f induces an étale map $D \to \mathrm{Ig}(p^{n+1}) \times_{\mathrm{Ig}(p^n)} \mathrm{Ig}(p^{n+1})$. Note that, if c is a closed point of $|C|$ for which the fiber E_c is supersingular, then the map $\widetilde{C} \to C$ is totally ramified at the point c. Consequently, we can lift c uniquely to closed points $\widetilde{c} \in |\widetilde{C}|$ and $y \in |D|$. We will prove Proposition 7.1 by verifying the equality $\delta_y(D) = (1/2)(p^{2n+2} - p^{2n+1})$. To prove this, we are free to replace C by an open neighborhood of c and may therefore assume that c is the *only* point of C for which the elliptic curve E_c is supersingular.

Let us regard D as an effective Cartier divisor in the algebraic surface $\widetilde{C} \times_{\mathrm{Spec}(\mathbf{F}_p)} \widetilde{C}$. Let G denote the collection of all elements $\lambda \in \mathbf{Z}/p^{n+1}\mathbf{Z}$ satisfying $\lambda \equiv 1 \pmod{p^n}$. We regard G as a group under multiplication (so that G is isomorphic to the cyclic group $\mathbf{Z}/p\mathbf{Z}$). The construction $(E, x) \mapsto (E, \lambda x)$ determines an action of G on $\mathrm{Ig}(p^{n+1})$ which fixes the projection map $\mathrm{Ig}(p^{n+1}) \to \mathrm{Ig}(p^n)$. We therefore also obtain an action of G on the curve $\widetilde{C}$, which we will denote by $(\lambda \in G) \mapsto (u_\lambda : \widetilde{C} \to \widetilde{C})$. Since the elliptic curve E is ordinary away from the point c, this action exhibits $\widetilde{C} - \{\widetilde{c}\}$ as a G-torsor over the curve $C - \{c\}$. For each $\lambda \in G$, the pair $(\mathrm{id}_{\widetilde{C}}, u_\lambda)$ determines a closed immersion $\widetilde{C} \to \widetilde{C} \times_{\mathrm{Spec}(\mathbf{F}_p)} \widetilde{C}$, whose image is a (smooth) divisor D_λ which is contained in D. Moreover, in the punctured surface $(\widetilde{C} \times_{\mathrm{Spec}(\mathbf{F}_p)} \widetilde{C}) - \{y\}$, the divisor $D - \{y\}$ is given by the *disjoint* union of the divisors $D_\lambda - \{y\}$. It follows that we have an equality of effective Cartier divisors $D = \sum_\lambda D_\lambda$. Since each D_λ is smooth over $\mathrm{Spec}(\mathbf{F}_p)$, iterated application of Example 5.2 gives the equality

$$\delta_y(D) = \frac{1}{2} \sum_{\lambda \neq \lambda'} i_y(D_\lambda, D_{\lambda'}).$$

Here the sum is taken over all ordered pairs of *distinct* elements of the group G, so there are $p^2 - p$ summands. We will complete the proof by showing that each summand $i_y(D_\lambda, D_{\lambda'})$ is equal to p^{2n}. By symmetry, we may assume that $\lambda' = 1$. In this case, the scheme-theoretic $D_\lambda \cap D_{\lambda'}$ can be identified with the closed subscheme of $\widetilde{C}$ given by the fixed points of u_λ. Consequently, the projection map $\widetilde{C} \to \mathrm{Ig}(p^{n+1})$ induces an étale map $D_\lambda \cap D_{\lambda'} \to Y$, where Y denotes the closed substack of $\mathrm{Ig}(p^{n+1})$ given by pairs (E, x) satisfying the condition $\lambda x = x$, or equivalently the condition $p^n x = 0$. It follows from Lemma 6.10 that Y is an effective Cartier divisor having degree p^{2n} at each supersingular point of $\mathrm{Ig}(p^{n+1})$. □

Proof of Theorem 5.5. By virtue of Proposition 4.1, the algebraic stack $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}$ is a local complete intersection of dimension 1. Moreover, it has a dense open substack (given by the inverse image of $\mathrm{Ell}_{\mathrm{ord}}$) which is isomorphic to an open substack of

$\mathrm{Ell}(p^{n+1})_{\zeta_{p^{n+1}}=1}$ (Theorem 3.1), and is therefore reduced (Theorem 5.4). It follows that $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}$ is everywhere reduced. The construction $(E,x,y) \mapsto (E,Vx,Vy)$ determines a morphism of stacks $\rho : \mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1} \to \mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ which is finite flat of degree p^2 (and totally ramified over the supersingular points of $\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$).

For every subgroup $S \subseteq (\mathbf{Z}/p^n\mathbf{Z})^2$ which is isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$, let $\mathrm{Ell}(p^n)_S \subseteq \mathrm{Ell}(p^n)_{\zeta_{p^n}=1}$ be the closed substack introduced in Notation 6.1, and set

$$\mathrm{Ell}(p^n)^{\text{V-Lift}}_S = \mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1} \times_{\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}} \mathrm{Ell}(p^n)_S.$$

Note that if z is a closed point of $|\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}|$ lying over the supersingular locus of Ell, then z belongs to each of the closed substacks $\mathrm{Ell}(p^n)^{\text{V-Lift}}_S$. Moreover, the canonical map $\coprod_S \mathrm{Ell}(p^n)^{\text{V-Lift}}_S \to \mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}$ is an isomorphism over the ordinary locus, so the normalization of $\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}$ can be identified with the disjoint union of the normalizations of the closed substacks $\mathrm{Ell}(p^n)^{\text{V-Lift}}_S$. Letting $\overline{z}$ denote the image of z in $|\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}|$, we compute

$$\begin{aligned}
\delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}) &= \mathrm{len}_z(\bigoplus_S \mathcal{O}_{\mathrm{Ell}(p^n)^{\text{V-Lift}}_S} / \mathcal{O}_{\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}}) + \sum_S \delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_S) \\
&= \mathrm{len}_z(\rho^*(\bigoplus_S \mathcal{O}_{\mathrm{Ell}(p^n)_S} / \mathcal{O}_{\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}}) + \sum_S \delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_S) \\
&= p^2 \,\mathrm{len}_{\overline{z}}(\bigoplus_S \mathcal{O}_{\mathrm{Ell}(p^n)_S} / \mathcal{O}_{\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}}) + \sum_S \delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_S) \\
&= p^2 \delta_{\overline{z}}(\mathrm{Ell}(p^n)_{\zeta_{p^n}=1}) + \sum_S \delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_S) \\
&= \frac{p^{3n+1}+p^{3n}}{2} + \sum_S \delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_S),
\end{aligned}$$

where the last equality follows from Theorem 5.4. Note that there are $p^n + p^{n-1}$ summands appearing in the sum $\sum_S \delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_S)$. Consequently, to establish the identity $\delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_{\zeta_{p^n}=1}) = (1/2)(p^{3n+2}+p^{3n+1})$, it will suffice to establish the identity $\delta_z(\mathrm{Ell}(p^n)^{\text{V-Lift}}_S) = (1/2)(p^{2n+2}-p^{2n+1})$ for each S. Without loss of generality, we may assume that S is the antidiagonal subgroup, given by the kernel of the map

$$\alpha : (\mathbf{Z}/p^n\mathbf{Z})^2 \to \mathbf{Z}/p^n\mathbf{Z} \qquad \alpha(i,j) = i+j.$$

According to Proposition 6.7, the construction $(E,x) \mapsto (E^{(p^n)}, x, x)$ induces an isomorphism of stacks $\mathrm{Ig}(p^n) \to \mathrm{Ell}(p^n)_S$. Under this isomorphism, we can identify $\mathrm{Ell}(p^n)^{\text{V-Lift}}_S$ with the fiber product $\mathrm{Ig}(p^{n+1}) \times_{\mathrm{Ig}(p^n)} \mathrm{Ig}(p^{n+1})$, so that the desired identity follows from Proposition 7.1. $\square$

8 Extension to the Cusps

In this section, we formulate a generalization of Theorem 1.15 which incorporates information about modular curves at the cusps. We begin by reviewing some definitions. Let $\overline{\mathrm{Ell}}$ denote the Deligne-Mumford compactification of the moduli stack Ell of elliptic curves (so that the R-valued points of $\overline{\mathrm{Ell}}$ are given by stable curves of genus 1 over $\mathrm{Spec}(R)$, equipped with a section).

Construction 8.1. Let n be a positive integer, let $\pi : \mathrm{Ell}(p^n) \to \mathrm{Ell}$ denote the projection map, and let $j : \mathrm{Ell} \hookrightarrow \overline{\mathrm{Ell}}$ be the inclusion. The map π is finite, and the map j is an affine open immersion (it is the inclusion of the complement of an effective Cartier divisor). Consequently, the composite map

$$(j \circ \pi) : \mathrm{Ell}(p^n) \to \overline{\mathrm{Ell}}$$

is affine, determined by a quasi-coherent sheaf of algebras $(j \circ \pi)_* \mathcal{O}_{\mathrm{Ell}(p^n)}$ on the moduli stack $\overline{\mathrm{Ell}}$. Let $\mathscr{A}$ denote the integral closure of $\mathcal{O}_{\overline{\mathrm{Ell}}}$ in $(j \circ \pi)_* \mathcal{O}_{\mathrm{Ell}(p^n)}$, and let $\overline{\mathrm{Ell}}(p^n)$ denote the relative spectrum of $\mathscr{A}$. By construction, we have a pullback diagram of Deligne-Mumford stacks

$$\begin{array}{ccc} \mathrm{Ell}(p^n) & \longrightarrow & \overline{\mathrm{Ell}}(p^n) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \overline{\pi}} \\ \mathrm{Ell} & \xrightarrow{j} & \overline{\mathrm{Ell}}, \end{array}$$

where the vertical maps are finite and the horizontal maps are open immersions.

Remark 8.2. Construction 8.1 is somewhat unsatisfying; the definition of $\overline{\mathrm{Ell}}(p^n)$ as a normalization does not *a priori* give a concrete description of its functor of points. For a moduli-theoretic perspective, we refer the reader to [1].

The map $\overline{\pi} : \overline{\mathrm{Ell}}(p^n) \to \overline{\mathrm{Ell}}$ of Construction 8.1 is characterized, up to isomorphism, by the following universal property:

($*$) For every commutative diagram of Deligne-Mumford stacks

$$\begin{array}{ccc} \mathrm{Ell}(p^n) & \longrightarrow & \mathcal{X} \\ \downarrow & & \downarrow{\scriptstyle \psi} \\ \overline{\mathrm{Ell}}(p^n) & \xrightarrow{\pi^+} & \overline{\mathrm{Ell}} \end{array}$$

where the map ψ is finite, there exists an essentially unique extension to a commutative diagram

$$\begin{array}{ccc} \mathrm{Ell}(p^n) & \longrightarrow & \mathcal{X} \\ \downarrow & \nearrow & \downarrow \psi \\ \overline{\mathrm{Ell}}(p^n) & \xrightarrow{\overline{\pi}} & \overline{\mathrm{Ell}}. \end{array}$$

Example 8.3. Let n be a positive integer. Applying $(*)$ to the outer rectangle of the diagram

$$\begin{array}{ccccc} \mathrm{Ell}(p^{n+1}) & \longrightarrow & \mathrm{Ell}(p^n) & \longrightarrow & \overline{\mathrm{Ell}}(p^n) \\ \downarrow & & & & \downarrow \\ \overline{\mathrm{Ell}}(p^{n+1}) & & \longrightarrow & & \overline{\mathrm{Ell}}, \end{array}$$

we obtain a map of Deligne-Mumford stacks $\overline{\mathrm{Ell}}(p^{n+1}) \to \overline{\mathrm{Ell}}(p^n)$ which extends the forgetful map

$$\mathrm{Ell}(p^{n+1}) \to \mathrm{Ell}(p^n) \qquad (E, x, y) \mapsto (E, px, py).$$

These maps can be arranged into a tower

$$\cdots \to \overline{\mathrm{Ell}}(p^3) \to \overline{\mathrm{Ell}}(p^2) \to \overline{\mathrm{Ell}}(p)$$

We will denote the inverse limit of this tower by $\overline{\mathrm{Ell}}(p^\infty)$. Since the transition maps $\overline{\mathrm{Ell}}(p^{n+1}) \to \overline{\mathrm{Ell}}(p^n)$ are affine (in fact, they are finite), it follows that $\overline{\mathrm{Ell}}(p^\infty)$ is a (non-Noetherian) Deligne-Mumford stack, which contains $\mathrm{Ell}(p^\infty)$ as an open substack.

Example 8.4. For every positive integer n, we can apply $(*)$ to the diagram

$$\begin{array}{ccc} \mathrm{Ell}(p^n) & \longrightarrow & \overline{\mathrm{Ell}} \times \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}]) \\ \downarrow & & \downarrow \\ \overline{\mathrm{Ell}}(p^n) & \longrightarrow & \overline{\mathrm{Ell}}, \end{array}$$

where the upper horizontal map is given by the construction $(E, x, y) \mapsto (E, e_{p^n}(x, y))$. It follows that the Weil pairing map

$$\mathrm{Ell}(p^n) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}]) \qquad (E, x, y) \mapsto e_{p^n}(x, y)$$

admits an essentially unique extension to a map $\overline{\theta}_n : \overline{\mathrm{Ell}}(p^n) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}])$. Passing to the inverse limit over n, we obtain a map $\overline{\theta}_\infty : \overline{\mathrm{Ell}}(p^\infty) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^\infty}])$, whose restriction to the open substack $\mathrm{Ell}(p^\infty)$ agrees with the map θ_∞ of Construction 1.12.

Theorem 1.15 admits the following refinement:

Theorem 8.5. *After extending scalars to $\mathbf{F}_p$, the morphism*

$$\overline{\theta}_\infty : \overline{\mathrm{Ell}}(p^\infty) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^\infty}])$$

is relatively perfect. In other words, the diagram of Deligne-Mumford stacks

$$\begin{array}{ccc} \overline{\mathrm{Ell}}(p^\infty)_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^\infty)_{p=0} \\ \downarrow{\scriptstyle \overline{\theta}_\infty} & & \downarrow{\scriptstyle \overline{\theta}_\infty} \\ \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^\infty}]) & \xrightarrow{\varphi} & \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^\infty}]) \end{array}$$

is a pullback square (where the horizontal maps are given by the absolute Frobenius).

Proof of Theorem 0.2. We have a commutative diagram

$$\begin{array}{ccccc} \overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1} & \longrightarrow & \overline{\mathrm{Ell}}(p^\infty)_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^\infty)_{p=0} \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbf{Z}_p[\zeta_{p^\infty}]/(\zeta_p - 1)) & \longrightarrow & \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^\infty}]) & \xrightarrow{\varphi} & \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^\infty}]) \end{array}$$

where the left square is a pullback by definition and the right square is a pullback by Theorem 8.5. It follows that the outer rectangle in the diagram

$$\begin{array}{ccccc} \overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^\infty)_{\zeta_{p^2}=1} & \longrightarrow & \overline{\mathrm{Ell}}(p^\infty)_{p=0} \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbf{Z}_p[\zeta_{p^\infty}]/(\zeta_p - 1)) & \xrightarrow{\varphi} & \mathrm{Spec}(\mathbf{Z}_p[\zeta_{p^\infty}]/(\zeta_{p^2} - 1)) & \longrightarrow & \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^\infty}]) \end{array}$$

is also a pullback square. Since the right square in this second diagram is also a pullback, and the lower left horizontal map is an isomorphism, we conclude that the Frobenius map $\varphi : \overline{\mathrm{Ell}}(p^\infty)_{\zeta_p=1} \to \overline{\mathrm{Ell}}(p^\infty)_{\zeta_{p^2}=1}$ is also an isomorphism. □

Our proof of Theorem 8.5 is a mild embellishment of our proof of Theorem 1.15.

Notation 8.6. For every positive integer n, we let $\overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}}$ denote the closed substack of $\overline{\mathrm{Ell}}(p^{n+1})$ given by the fiber product

$$\overline{\mathrm{Ell}}(p^{n+1}) \times_{\mu_{p^{n+1}}} \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}]).$$

Note that $\overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}}$ contains the moduli stack $\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}$ of Definition 2.1 as an open substack.

By virtue of Remark 2.2, we can regard $\overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}}$ as a closed substack of the special fiber $\overline{\mathrm{Ell}}(p^{n+1})_{p=0}$. Moreover, the absolute Frobenius map on $\overline{\mathrm{Ell}}(p^{n+1})_{p=0}$ factors through $\overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}}$. We will deduce Theorem 8.5 from the following stronger version of Theorem 2.5:

Theorem 8.7. *Let $n > 1$ be an integer, and consider the commutative diagram of Deligne-Mumford stacks*

$$\begin{array}{ccc} \overline{\mathrm{Ell}}(p^{n+1})_{p=0} & \longrightarrow & \overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}} \\ \downarrow & \swarrow & \downarrow \\ \overline{\mathrm{Ell}}(p^{n})_{p=0} & \longrightarrow & \overline{\mathrm{Ell}}(p^{n})_{\mathrm{deg}}, \end{array}$$

where the vertical maps are as in Example 8.3 and the horizontal maps are given by the absolute Frobenius. Then there exists a dotted arrow as indicated, which renders the diagram commutative (up to canonical isomorphism).

Proof of Theorem 8.5 from Theorem 8.7. Using Theorem 8.7, we obtain a commutative diagram of Deligne-Mumford stacks

$$\begin{array}{ccc} \cdots & \longrightarrow & \cdots \\ \downarrow & \swarrow & \downarrow \\ \overline{\mathrm{Ell}}(p^{4})_{p=0} & \longrightarrow & \overline{\mathrm{Ell}}(p^{4})_{\mathrm{deg}} \\ \downarrow & \swarrow & \downarrow \\ \overline{\mathrm{Ell}}(p^{3})_{p=0} & \longrightarrow & \overline{\mathrm{Ell}}(p^{3})_{\mathrm{deg}} \\ \downarrow & \swarrow & \downarrow \\ \overline{\mathrm{Ell}}(p^{2})_{p=0} & \longrightarrow & \overline{\mathrm{Ell}}(p^{2})_{\mathrm{deg}}. \end{array}$$

Passing to the inverse limit in the vertical direction, we obtain a map of algebraic stacks

$$\rho : \overline{\mathrm{Ell}}(p^{\infty})_{p=0} \to \varprojlim_{n} \overline{\mathrm{Ell}}(p^{n})_{\mathrm{deg}},$$

which we can identify with the relative Frobenius for the map $\overline{\theta}_{\infty} : \overline{\mathrm{Ell}}(p^{\infty})_{p=0} \to \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^\infty}])$. Consequently, Theorem 8.5 is equivalent to the assertion that ρ is an isomorphism. An explicit homotopy inverse is given by the dotted arrows in the preceding diagram. $\square$

Remark 8.8. For every commutative ring R, let $\mathrm{Ell}^+(R)$ denote the groupoid whose objects are generalized elliptic curves $E \to \mathrm{Spec}(R)$ (in the sense of [2]) which satisfy the following additional condition:

($*$) For every point $x \in \mathrm{Spec}(R)$, the characteristic of the residue field $\kappa(x)$ does not divide the number of irreducible components of the fiber $E_x = E \times_{\mathrm{Spec}(R)} \mathrm{Spec}(\kappa(x))$.

The construction $R \mapsto \mathrm{Ell}^+(R)$ determines a Deligne-Mumford stack Ell^+, which contains the Deligne-Mumford compactification $\overline{\mathrm{Ell}}$ as an open substack (namely, the open substack whose R-valued points are generalized elliptic curves $E \to \mathrm{Spec}(R)$ with irreducible fibers); in fact, Ell^+ is precisely the "Deligne-Mumford locus" of the algebraic stack parametrizing *all* generalized elliptic curves. All of the statements formulated in this section remain valid if we replace $\overline{\mathrm{Ell}}$ by the larger moduli stack Ell^+. We leave the details to the reader.

9 Analysis of the Tate Curve

We will prove Theorem 8.7 by combining Theorem 2.5 with a local analysis around the cusp of the moduli stack $\overline{\mathrm{Ell}}$. We begin by introducing some notation. For every Deligne-Mumford stack $\mathcal{X}$ equipped with a map equipped with affine map $\pi : \mathcal{X} \to \overline{\mathrm{Ell}}_{p=0}$, let $\mathcal{A}(\mathcal{X})$ denote the direct image $\pi_* \mathcal{O}_{\mathcal{X}}$, regarded as a quasi-coherent sheaf of algebras on the stack $\overline{\mathrm{Ell}}_{p=0}$. The diagram

$$\begin{array}{ccc} \overline{\mathrm{Ell}}(p^{n+1})_{p=0} & \longrightarrow & \overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}} \\ \downarrow & & \downarrow \\ \overline{\mathrm{Ell}}(p^{n})_{p=0} & \longrightarrow & \overline{\mathrm{Ell}}(p^{n})_{\mathrm{deg}} \end{array}$$

appearing in the statement of Theorem 8.7 then determines a commutative square of $\mathcal{O}_{\overline{\mathrm{Ell}}_{p=0}}$-algebras, indicated by the solid arrows in the diagram

$$\begin{array}{ccc} \varphi_* \mathcal{A}(\overline{\mathrm{Ell}}(p^{n+1})_{p=0}) & \longleftarrow & \mathcal{A}(\overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}}) \\ \uparrow & \overset{\psi}{\nearrow} & \uparrow \\ \varphi_* \mathcal{A}(\overline{\mathrm{Ell}}(p^{n})_{p=0}) & \longleftarrow & \mathcal{A}(\overline{\mathrm{Ell}}(p^{n})_{\mathrm{deg}}), \end{array}$$

where φ denotes the (absolute) Frobenius endomorphism of $\overline{\mathrm{Ell}}_{p=0}$. We wish to show that there exists a map ψ which renders the diagram commutative. Theorem 2.5

guarantees that such an arrow exists after restricting to the open substack $\mathrm{Ell} \subseteq \overline{\mathrm{Ell}}$. In other words, we can choose a map $\psi_0 : \varphi_* \mathcal{A}(\mathrm{Ell}(p^n)_{p=0}) \to \mathcal{A}(\mathrm{Ell}(p^{n+1})_{\mathrm{deg}})$ for which the diagram

$$\begin{array}{ccc} \mathcal{A}(\mathrm{Ell}(p^{n+1})_{p=0}) & \longleftarrow & \mathcal{A}(\mathrm{Ell}(p^{n+1})_{\mathrm{deg}}) \\ \uparrow & \overset{\psi_0}{\nearrow} & \uparrow \\ \varphi_* \mathcal{A}(\mathrm{Ell}(p^n)_{p=0}) & \longleftarrow & \mathcal{A}(\mathrm{Ell}(p^n)_{\mathrm{deg}}), \end{array}$$

commutes. To complete the proof, it will suffice to verify the following:

(a) The canonical maps

$$\mathcal{A}(\overline{\mathrm{Ell}}(p^{n+1})_{p=0}) \to \mathcal{A}(\mathrm{Ell}(p^{n+1})_{p=0}) \qquad \mathcal{A}(\overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}}) \to \mathcal{A}(\mathrm{Ell}(p^{n+1})_{\mathrm{deg}})$$

are monomorphisms.

(b) The composite map

$$\varphi_* \mathcal{A}(\overline{\mathrm{Ell}}(p^n)_{p=0}) \to \varphi_* \mathcal{A}(\mathrm{Ell}(p^n)_{p=0}) \xrightarrow{\psi_0} \mathcal{A}(\mathrm{Ell}(p^{n+1})_{\mathrm{deg}})$$

factors through the monomorphism $\mathcal{A}(\overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}}) \to \mathcal{A}(\mathrm{Ell}(p^{n+1})_{\mathrm{deg}})$.

Let E_{Tate} denote the Tate curve, which we regard as an elliptic curve over the commutative ring $\mathbf{Z}((q))$, classified by a map $\rho : \mathrm{Spec}(\mathbf{Z}((q))) \to \mathrm{Ell}$ which admits a canonical extension $\overline{\rho} : \mathrm{Spec}(\mathbf{Z}[[q]]) \to \overline{\mathrm{Ell}}$. The maps

$$\mathrm{Spec}(\mathbf{Z}[[q]]) \xrightarrow{\overline{\rho}} \overline{\mathrm{Ell}} \hookleftarrow \mathrm{Ell}$$

determine a covering with respect to the fpqc topology. Since assertions (a) and (b) can be tested locally with respect to the fpqc topology and are tautologically satisfied over the open substack $\mathrm{Ell} \subseteq \overline{\mathrm{Ell}}$, it will suffice to show that they hold after restriction to $\mathrm{Spec}(\mathbf{Z}[[q]])$. We are therefore reduced to proving the following more concrete statements:

(a') The open immersions

$$j : \mathrm{Ell}(p^{n+1})_{p=0} \times_{\mathrm{Ell}} \mathrm{Spec}(\mathbf{Z}((q))) \hookrightarrow \overline{\mathrm{Ell}}(p^{n+1})_{p=0} \times_{\overline{\mathrm{Ell}}} \mathrm{Spec}(\mathbf{Z}[[q]])$$

$$j' : \mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \times_{\mathrm{Ell}} \mathrm{Spec}(\mathbf{Z}((q))) \hookrightarrow \overline{\mathrm{Ell}}(p^{n+1})_{\mathrm{deg}} \times_{\overline{\mathrm{Ell}}} \mathrm{Spec}(\mathbf{Z}[[q]])$$

are schematically dense.

(b') The composite map

$$\begin{aligned} \mathrm{Ell}(p^{n+1})_{\mathrm{deg}} \times_{\mathrm{Ell}} \mathrm{Spec}(\mathbf{Z}((q))) &\xrightarrow{\psi_0} \mathrm{Ell}(p^n)_{p=0} \times_{\mathrm{Ell}} \mathrm{Spec}(\mathbf{Z}((q))) \\ &\hookrightarrow \overline{\mathrm{Ell}}(p^{n+1})_{p=0} \times_{\overline{\mathrm{Ell}}} \mathrm{Spec}(\mathbf{Z}[[q]]) \end{aligned}$$

factors (uniquely) over the open immersion j'.

To prove (a') and (b'), we need an explicit analysis of the schemes $\overline{\mathrm{Ell}}(p^n) \times_{\overline{\mathrm{Ell}}} \mathrm{Spec}(\mathbf{Z}[[q]])$. Recall that the p^n-torsion subscheme of the Tate curve E_{Tate} fits into a short exact sequence of finite flat group schemes

$$0 \to \mu_{p^n} \to E_{\mathrm{Tate}}[p^n] \xrightarrow{v} \underline{\mathbf{Z}/p^n\,\mathbf{Z}} \to 0.$$

over the commutative ring $\mathbf{Z}((q))$. Moreover, the fiber of the map v over the element $1 \in \mathbf{Z}/p^n\,\mathbf{Z}$ can be identified with $\mathrm{Spec}(\mathbf{Z}((q^{1/p^n})))$ as a μ_{p^n}-torsor over $\mathrm{Spec}(\mathbf{Z}((q)))$. For every surjective map $\alpha : (\mathbf{Z}/p^n\,\mathbf{Z})^2 \to (\mathbf{Z}/p^n\,\mathbf{Z})$, let $\mathrm{Ell}(p^n, \alpha)$ denote the closed and open subscheme of $\mathrm{Ell}(p^n) \times_{\mathrm{Ell}} \mathrm{Spec}(\mathbf{Z}((q)))$ classifying level structures $\gamma : (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \to E_{\mathrm{Tate}}[p^n]$ for which the composition $(v \circ \gamma) : (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \to \underline{\mathbf{Z}/p^n\,\mathbf{Z}}$ is given by α. We then have decompositions

$$\mathrm{Ell}(p^n) \times_{\mathrm{Ell}} \mathrm{Spec}(\mathbf{Z}((q))) \simeq \coprod_{\alpha} \mathrm{Ell}(p^n, \alpha)$$

$$\mathrm{Ell}(p^{n+1}) \times_{\mathrm{Ell}} \mathrm{Spec}(\mathbf{Z}((q))) \simeq \coprod_{\widetilde{\alpha}} \mathrm{Ell}(p^{n+1}, \widetilde{\alpha}),$$

where the decomposition on the left is indexed by the collection of all surjections $\alpha : (\mathbf{Z}/p^n\,\mathbf{Z})^2 \to \mathbf{Z}/p^n\,\mathbf{Z}$, and the decomposition the right is indexed by the collection of all surjections $\widetilde{\alpha} : (\mathbf{Z}/p^{n+1}\,\mathbf{Z})^2 \to \mathbf{Z}/p^{n+1}\,\mathbf{Z}$. This induces decompositions

$$\overline{\mathrm{Ell}}(p^n) \times_{\overline{\mathrm{Ell}}} \mathrm{Spec}(\mathbf{Z}[[q]]) \simeq \coprod_{\alpha} \overline{\mathrm{Ell}}(p^n, \alpha)$$

$$\overline{\mathrm{Ell}}(p^{n+1}) \times_{\overline{\mathrm{Ell}}} \mathrm{Spec}(\mathbf{Z}[[q]]) \simeq \coprod_{\widetilde{\alpha}} \overline{\mathrm{Ell}}(p^{n+1}, \widetilde{\alpha}).$$

Fix a surjection $\widetilde{\alpha} : (\mathbf{Z}/p^{n+1}\,\mathbf{Z})^2 \to \mathbf{Z}/p^{n+1}\,\mathbf{Z}$, let $\overline{\mathrm{Ell}}(p^{n+1}, \widetilde{\alpha})$ denote the fiber product $\overline{\mathrm{Ell}}(p^{n+1}, \widetilde{\alpha}) \times_{\mu_{p^{n+1}}} \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}])$, and define $\mathrm{Ell}(p^{n+1}, \widetilde{\alpha})_{\mathrm{deg}}$ similarly. To deduce (a') and (b'), it will suffice to prove the following:

(a'') The open immersions

$$j_{\widetilde{\alpha}} : \mathrm{Ell}(p^{n+1}, \widetilde{\alpha})_{p=0} \hookrightarrow \overline{\mathrm{Ell}}(p^{n+1}, \widetilde{\alpha})_{p=0} \qquad j'_{\widetilde{\alpha}} : \mathrm{Ell}(p^{n+1}, \widetilde{\alpha})_{\mathrm{deg}} \hookrightarrow \overline{\mathrm{Ell}}(p^{n+1}, \widetilde{\alpha})_{\mathrm{deg}}$$

are schematically dense.

(b'') The composite map

$$\mathrm{Ell}(p^{n+1}, \widetilde{\alpha})_{\deg} \xrightarrow{\psi_0} \mathrm{Ell}(p^n, \alpha)_{p=0} \hookrightarrow \overline{\mathrm{Ell}}(p^n, \alpha)$$

factors (uniquely) over the open immersion $j'_{\widetilde{\alpha}}$; here $\alpha : (\mathbf{Z}/p^n\,\mathbf{Z})^2 \to \mathbf{Z}/p^n\,\mathbf{Z}$ denotes the surjection obtained from $\widetilde{\alpha}$ by reduction modulo p^n.

To prove (a'') and (b''), we may assume without loss of generality that the map $\widetilde{\alpha}$ is given by projection onto the second factor. In this case, R-valued points of the $\mathbf{Z}((q))$-scheme $\mathrm{Ell}(p^n, \alpha)$ are given by pairs of p^n-torsion points $x, y \in E_{\mathrm{Tate}}(R)$ for which x is the image of a primitive p^nth root of unity under the closed immersion

$$\mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}]) \times \mathrm{Spec}(\mathbf{Z}((q))) \hookrightarrow \mu_{p^n} \times \mathrm{Spec}(\mathbf{Z}((q))) \hookrightarrow E_{\mathrm{Tate}}[p^n],$$

and y is an arbitrary R-valued point of the μ_{p^n}-torsor $\mathrm{Spec}(\mathbf{Z}((q^{1/p^n})))$. This analysis supplies an isomorphism of $\mathbf{Z}((q))$-schemes

$$\mathrm{Ell}(p^n, \alpha) \simeq \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}]) \times \mathrm{Spec}(\mathbf{Z}((q^{1/p^n}))) \simeq \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}]((q^{1/p^n}))).$$

Passing to the integral closure of $\mathbf{Z}[[q]]$ in the ring of functions on $\mathrm{Ell}(p^n, \alpha)$, this extends to an isomorphism $\overline{\mathrm{Ell}}(p^n, \alpha) \simeq \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}][[q^{1/p^n}]])$. Similarly, we have isomorphisms

$$\mathrm{Ell}(p^{n+1}, \widetilde{\alpha}) \simeq \mathrm{Spec}(\mathbf{Z}[\zeta_{p^{n+1}}]((q^{1/p^{n+1}})))$$
$$\overline{\mathrm{Ell}}(p^{n+1}, \widetilde{\alpha}) \simeq \mathrm{Spec}(\mathbf{Z}[\zeta_{p^{n+1}}][[q^{1/p^{n+1}}]]).$$

Assertion (a'') now follows from the observation that the canonical map $S[[q^{1/p^{n+1}}]] \to S((q^{1/p^{n+1}}))$ is a monomorphism for the commutative rings $S = \mathbf{F}_p[\zeta_{p^n}]$ and $S = \mathbf{F}_p[\zeta_{p^{n+1}}]$. To prove ($b''$), it suffices to observe that the commutative square of rings

$$\begin{array}{ccc} \mathbf{F}_p[\zeta_{p^{n+1}}][[q^{1/p^{n+1}}]] & \longleftarrow & \mathbf{F}_p[\zeta_{p^n}][[q^{1/p^{n+1}}]] \\ \uparrow & \nearrow & \uparrow \\ \mathbf{F}_p[\zeta_{p^n}][[q^{1/p^n}]] & \longleftarrow & \mathbf{F}_p[\zeta_{p^{n-1}}][[q^{1/p^n}]] \end{array}$$

admits an extension as indicated, where the vertical maps are the evident inclusions and the horizontal maps are given by $q \mapsto q^p$. The desired extension is given by the construction $q^{1/p^n} \mapsto q^{1/p^{n+1}}$.

References

[1] Conrad, B. *Arithmetic moduli of generalized elliptic curves*. J. Inst. Math. Jussieu 6 (2007), no. 2, 209–278.

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

[3] Katz, N., and B. Mazur. *Arithmetic moduli of elliptic curves*. Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985.

[4] Scholze, P. *On the torsion in the cohomology of locally symmetric varieties*. Ann. of Math. (2) 182 (2015), no. 3, 945–1066.

[5] Scholze, P., and J. Weinstein. *Moduli of p-divisible groups*. Camb. J. Math. 1 (2013), no. 2, 145–237.

[6] Weinstein, J. *Semistable models for modular curves of arbitrary level*. Invent. Math. 205 (2016), no. 2, 459–526.