Full Level Structures on Elliptic Curves

April 30, 2020

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 (generalized) 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

$$\cdots \to X(p^4)^{\mathrm{an}} \to X(p^3)^{\mathrm{an}} \to X(p^2)^{\mathrm{an}} \to X(p)^{\mathrm{an}} \to X(1)^{\mathrm{an}}.$$

The starting point of this paper is the following result (which is a special case of Theorem III.1.2 of [7]):

Theorem 0.1 (Scholze)**.** *There exists a perfectoid space $X(p^\infty)^{\mathrm{an}}$ over the perfectoid field $\mathbf{Q}_p^{\mathrm{cyc}}$, characterized up to unique isomorphism by the requirement $X(p^\infty)^{\mathrm{an}} \sim \varprojlim X(p^n)^{\mathrm{an}}$ (in the sense of [8], 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 of 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 parametrizes (generalized) elliptic curves equipped with a full level-p^n structure in the sense of Drinfeld (see [5] and [3]). These stacks can be organized into an inverse system

$$\cdots \to \overline{\mathrm{Ell}}(p^4) \to \overline{\mathrm{Ell}}(p^3) \to \overline{\mathrm{Ell}}(p^2) \to \overline{\mathrm{Ell}}(p) \to \overline{\mathrm{Ell}}(1)$$

with affine transition maps, so that the inverse limit $\overline{\mathrm{Ell}}(p^\infty)$ is a Deligne-Mumford stack defined over the ring defined over the ring $\mathbf{Z}[\zeta_{p^\infty}] = \varinjlim_n \mathbf{Z}[\zeta_{p^n}]$. Let $\overline{\mathrm{Ell}}(p^\infty)_{p=0}$ denote the closed substack of $\overline{\mathrm{Ell}}(p^\infty)$ given by the vanishing locus of p, and let $\mathbf{F}_p[\zeta_{p^\infty}]$ denote the quotient ring $\mathbf{Z}[\zeta_{p^\infty}]/(p)$. The main result of this paper is the following:

Theorem 0.2. *The structure map $\overline{\mathrm{Ell}}(p^\infty)_{p=0} \to \mathrm{Spec}(\mathbf{F}_p[\zeta_{p^\infty}])$ is relatively perfect. That is, the commutative diagram of Deligne-Mumford stacks*

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

(in which the horizontal maps are given by the Frobenius) is a pullback square.

Note that the Frobenius map $\varphi : \mathbf{F}_p[\zeta_{p^\infty}] \to \mathbf{F}_p[\zeta_{p^\infty}]$ is a surjection, whose kernel is the ideal generated by the image of the element $\pi = (\zeta_{p^2} - 1)^{p-1} \in \mathbf{Z}[\zeta_{p^\infty}]$. We can therefore reformulate Theorem 0.2 more concretely as follows:

Theorem 0.3. *The absolute Frobenius map induces an isomorphism from* $\overline{\mathrm{Ell}}(p^\infty)_{p=0}$ *to the closed substack* $\overline{\mathrm{Ell}}(p^\infty)_{\pi=0} \subseteq \overline{\mathrm{Ell}}(p^\infty)$ *given by the vanishing locus of the element* $\pi = (\zeta_{p^2} - 1)^{p-1}$.

It follows from Theorem 0.3 that the moduli stack $\overline{\mathrm{Ell}}(p^\infty)$ is integral perfectoid (after p-adic completion). More precisely, we have the following:

Corollary 0.4. *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 *is a unit multiple of* p*, and the Frobenius map* $R/\pi R \to R/\pi^p R$ *is an isomorphism.*

Remark 0.5. The conclusion of Corollary 0.4 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).

Remark 0.6. In [10], Weinstein supplies an explicit description of the coordinate ring for Lubin-Tate space at infinite level (see Theorem 2.17 of [10]). From this description, one can immediately deduce that Corollary 0.4 holds after formal completion along the locus of supersingular elliptic curves.

Warning 0.7. For $p^n > 2$, 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 0.4: 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 0.4; we leave details to the interested reader.

Remark 0.8. 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.

Let us now outline the contents of this paper. We begin in §1 by reviewing the definition of the moduli stacks $\overline{\mathrm{Ell}}(p^n)$ (following Katz-Mazur [5]) and formulating a "finite-level" analogue of Theorem 0.3, which asserts the existence of a commutative diagram of Deligne-Mumford stacks

$$\begin{array}{ccc} \overline{\mathrm{Ell}}(p^n)_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^n)_{\pi=0} \\ \downarrow & \overset{\Theta}{\swarrow} & \downarrow \\ \overline{\mathrm{Ell}}(p^{n-1})_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^{n-1})_{\pi=0} \end{array} \tag{1}$$

for $n \geqslant 3$ (see Theorem 1.9 and Remark 1.10), where the horizontal maps are given by the Frobenius and the vertical maps by "forgetting" level structure. The difficulty is then to prove the existence of the morphism Θ in (1). Working away from the cusps, we can think of points of $\overline{\mathrm{Ell}}(p^n)_{\pi=0}$ as elliptic curves E equipped with a full level-p^n structure (x, y) for which the Weil pairing $e_{p^n}(x, y)$ is a primitive p^{n-1}st root of unity. The heuristic idea is that this property of the Weil pairing ensures that $p^{n-1}x$ and $p^{n-1}y$ "generate" a subgroup $S \subseteq E$ of order p. The morphism Θ then carries $(E, x, y) \mapsto (E/S, x', y')$, where x' and y' denote the images of x and y in the quotient elliptic curve E/S. In §2, we translate this heuristic into a precise mathematical construction in the case where E is an *ordinary* elliptic curve, and use this to construct a morphism $\mathrm{Ell}(p^n)^{\mathrm{ord}}_{\pi=0} \to \overline{\mathrm{Ell}}(p^{n-1})_{p=0}$ on the open substack $\mathrm{Ell}(p^n)^{\mathrm{ord}}_{\pi=0} \subseteq \overline{\mathrm{Ell}}(p^n)_{\pi=0}$ parametrizing *ordinary* elliptic curves (Proposition 1.11). We extend this construction to the supersingular locus (and to the cusps) using a descent argument together with the fact that Frobenius map $\varphi : \overline{\mathrm{Ell}}(p^n)_{p=0} \to \overline{\mathrm{Ell}}(p^n)_{\pi=0}$ is (faithfully) flat (Proposition 1.12). This follows from the regularity of the moduli stack $\overline{\mathrm{Ell}}(p^n)$ (Theorem 5.1.1 and Corollary 10.9.2 of [5]) together with a mixed-characteristic analogue of Kunz's characterization of regular $\mathbf{F}_p$-algebras, which we prove in §3 (Theorem 3.2).

Remark 0.9. 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 (non-algebraic) moduli stack of 1-dimensional p-divisible groups.

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, Preston Wake for offering corrections on an earlier version, and the anonymous referee for numerous

corrections and recommendations. Particular thanks are due to Ofer Gabber, who suggested Theorem 3.2 (thereby substantially simplifying the proof of Theorem 0.2). 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 give a more detailed outline of our proof of Theorem 0.3. For a more comprehensive account, we refer the reader to [5].

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.

Notation 1.4. 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 $\gamma : (\mathbf{Z}/p^n\mathbf{Z})^2 \to E(R)$ 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*.

Remark 1.5. Let $\mathcal{E} \to \mathrm{Ell}$ denote the universal elliptic curve, and let $\mathcal{E}[p^n]$ denote its p-torsion subgroup (so that $\mathcal{E}[p^n] \to \mathrm{Ell}$ is a finite flat map of degree p^{2n}). Then the construction $(E, x, y) \mapsto ((E, x), (E, y))$ determines a closed immersion of Deligne-Mumford stacks $\mathrm{Ell}(p^n) \to \mathcal{E}[p^n] \times_{\mathrm{Ell}} \mathcal{E}[p^n]$. In particular, the projection map

$$\mathrm{Ell}(p^n) \to \mathrm{Ell} \qquad (E, x, y) \mapsto E$$

is finite.

Notation 1.6. Let $\overline{\mathrm{Ell}}$ denote the Deligne-Mumford compactification of the moduli stack Ell and let $j : \mathrm{Ell} \hookrightarrow \overline{\mathrm{Ell}}$ denote the inclusion map. Let n be a nonnegative integer, and let $q : \mathrm{Ell}(p^n) \to \mathrm{Ell}$ denote the projection map. Then q is finite (Remark 1.5), and j is an affine open immersion (it is the inclusion of the complement of an effective Cartier divisor). Consequently, the composite map

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

is affine, determined by a quasi-coherent sheaf of algebras $(j \circ q)_* \mathcal{O}_{\mathrm{Ell}(p^n)}$ on the moduli stack $\overline{\mathrm{Ell}}$. Let $\mathscr{A}$ denote the integral closure of $\mathcal{O}_{\overline{\mathrm{Ell}}}$ in $(j \circ q)_* \mathcal{O}_{\mathrm{Ell}(p^n)}$, 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

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

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

Remark 1.7. The construction of Notation 1.6 is somewhat unsatisfying, because it does not *a priori* give a concrete description of the functor represented by the Deligne-Mumford stack $\overline{\mathrm{Ell}}(p^n)$. For a moduli-theoretic perspective, we refer the reader to [3].

Notation 1.8 (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. If (x, y) is a full level p^n-structure on E, then $e_{p^n}(x, y)$ is a primitive p^nth root of unity: that is, it is a root of the cyclotomic polynomial $\frac{u^{p^n}-1}{u^{p^{n-1}}-1}$.

Let $\mathbf{Z}[\zeta_{p^n}] \simeq \mathbf{Z}[u]/(\frac{u^{p^n}-1}{u^{p^{n-1}}-1})$ denote the ring of integers in the cyclotomic field $\mathbf{Q}[\zeta_{p^n}]$, so that the construction $(E, x, y) \mapsto e_{p^n}(x, y)$ induces a morphism of Deligne-Mumford stacks $\mathrm{Ell}(p^n) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}])$. Since $\mathbf{Z}[\zeta_{p^n}]$ is integral over $\mathbf{Z}$, this extends uniquely to a morphism $\overline{\mathrm{Ell}}(p^n) \to \mathrm{Spec}(\mathbf{Z}[\zeta_{p^n}])$. For $n \geqslant 2$, we let $\overline{\mathrm{Ell}}(p^n)_{\pi=0}$ denote the vanishing locus of the element $\pi = (\zeta_{p^2} - 1)^{p-1} \in \mathbf{Z}[\zeta_{p^2}] \subseteq \mathbf{Z}[\zeta_{p^n}]$. Note that π^p is a unit multiple of p, so the Frobenius induces a morphism of Deligne-Mumford stacks $\varphi : \overline{\mathrm{Ell}}(p^n)_{p=0} \to \overline{\mathrm{Ell}}(p^n)_{\pi=0}$.

Theorem 1.9. *For each $n \geqslant 2$, there is an essentially unique commutative diagram of*

$$\begin{array}{ccc} \overline{\mathrm{Ell}}(p^n)_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^n)_{\pi=0} \\ \downarrow & \swarrow^{\Theta} & \downarrow \\ \overline{\mathrm{Ell}}(p^{n-1})_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^{n-1})_{p=0}, \end{array}$$

where the horizontal maps are given by the absolute Frobenius and the vertical maps by forgetting level structure.

Remark 1.10. If $n \geqslant 3$, then the absolute Frobenius of $\overline{\mathrm{Ell}}(p^{n-1})_{p=0}$ factors through the closed substack $\overline{\mathrm{Ell}}(p^{n-1})_{\pi=0} \subseteq \overline{\mathrm{Ell}}(p^{n-1})$. In this case, Theorem 1.9 supplies a commutative diagram

$$\begin{array}{ccc} \overline{\mathrm{Ell}}(p^n)_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^n)_{\pi=0} \\ \downarrow & \swarrow^{\Theta} & \downarrow \\ \overline{\mathrm{Ell}}(p^{n-1})_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^{n-1})_{\pi=0}. \end{array}$$

Proof of Theorem 0.3 from Theorem 1.9. By virtue of Theorem 1.9 (and Remark 1.10), we have a commutative diagram of Deligne-Mumford stacks

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

Passing to the inverse limit in the vertical directions, we conclude that the Frobenius map $\varphi : \overline{\mathrm{Ell}}(p^\infty)_{p=0} \to \overline{\mathrm{Ell}}(p^\infty)_{\pi=0}$ is an isomorphism. $\square$

Let $\mathrm{Ell}^{\mathrm{ord}}_{p=0}$ denote the open substack of $\mathrm{Ell}_{p=0}$ classifying *ordinary* elliptic curves (over commutative rings of characteristic p). For each $n \geqslant 2$, we let $\mathrm{Ell}(p^n)^{\mathrm{ord}}_{p=0}$ and $\mathrm{Ell}(p^n)^{\mathrm{ord}}_{\pi=0}$ denote the inverse image of $\mathrm{Ell}^{\mathrm{ord}}_{p=0}$ in the moduli stacks $\overline{\mathrm{Ell}}(p^n)_{p=0}$ and $\overline{\mathrm{Ell}}(p^n)_{\pi=0}$, respectively. In §2, we will prove the following weaker version of Theorem 1.9:

Proposition 1.11. *For each $n \geqslant 2$, there exists an essentially unique commutative diagram of Deligne-Mumford stacks*

$$\begin{array}{ccc} \mathrm{Ell}(p^n)^{\mathrm{ord}}_{p=0} & \xrightarrow{\varphi} & \mathrm{Ell}(p^n)^{\mathrm{ord}}_{\pi=0} \\ \downarrow & \overset{\Theta^{\mathrm{ord}}}{\swarrow} & \downarrow \\ \overline{\mathrm{Ell}}(p^{n-1})_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^{n-1})_{p=0}, \end{array}$$

where the horizontal maps are given by the absolute Frobenius and the vertical maps by forgetting level structure.

We will deduce Theorem 1.9 from Proposition 1.11 together with the following result:

Proposition 1.12. *For $n \geqslant 2$, the Frobenius morphism $\varphi : \overline{\mathrm{Ell}}(p^n)_{p=0} \to \overline{\mathrm{Ell}}(p^n)_{\pi=0}$ is flat.*

Our proof of Proposition 1.12 will use a mixed-characteristic analogue of Kunz's characterization of regular rings of characteristic p (Theorem 3.2), which we establish in §3.

Proof of Proposition 1.12. Fix an étale morphism $\mathrm{Spec}(R) \to \overline{\mathrm{Ell}}(p^n)$, and let us abuse notation by identifying the element $\pi = (\zeta_{p^2} - 1)^{p-1} \in \mathbf{Z}[\zeta_{p^2}]$ with its image in R. We wish to show that the Frobenius map

$$\varphi : R/\pi R \to R/\pi^p R = R/pR$$

is flat. Since R is a regular Noetherian ring (Theorem 5.1.1 and Corollary 10.9.2 of [5]), this is a special case of Theorem 3.2. $\square$

Proof of Theorem 1.9. Fix an integer $n \geqslant 2$, so we have a commutative diagram

$$\begin{array}{ccc} \overline{\mathrm{Ell}}(p^n)_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^n)_{\pi=0} \\ \downarrow{\scriptstyle \theta} & & \downarrow \\ \overline{\mathrm{Ell}}(p^{n-1})_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^{n-1})_{p=0} \end{array}$$

in the category $\mathcal{C}$ of Deligne-Mumford stacks equipped with an affine morphism to $\overline{\mathrm{Ell}}(p^{n-1})_{p=0}$. We wish to show that, in the category $\mathcal{C}$, the morphism θ factors uniquely as a composition

$$\overline{\mathrm{Ell}}(p^n)_{p=0} \xrightarrow{\varphi} \overline{\mathrm{Ell}}(p^n)_{\pi=0} \xrightarrow{\Theta} \overline{\mathrm{Ell}}(p^{n-1})_{p=0}.$$

Note that the Frobenius map $\varphi : \overline{\mathrm{Ell}}(p^n)_{p=0} \to \overline{\mathrm{Ell}}(p^n)_{\pi=0}$ is a flat surjection (Proposition 1.12), and is therefore an epimorphism in the category $\mathcal{C}$; this proves the uniqueness of Θ. To prove existence, it will suffice (by faithfully flat descent) to show that $\theta \circ q_+ = \theta \circ q_-$, where

$$q_-, q_+ : \overline{\mathrm{Ell}}(p^n)_{p=0} \times_{\overline{\mathrm{Ell}}(p^n)_{\pi=0}} \overline{\mathrm{Ell}}(p^n)_{p=0} \to \overline{\mathrm{Ell}}(p^n)_{p=0}$$

are the two projection maps. Note that the fiber product $\overline{\mathrm{Ell}}(p^n)_{p=0} \times_{\overline{\mathrm{Ell}}(p^n)_{\pi=0}} \overline{\mathrm{Ell}}(p^n)_{p=0}$ is flat over the moduli stack $\overline{\mathrm{Ell}}(p^n)_{p=0}$ (by Proposition 1.12), and therefore also over $\overline{\mathrm{Ell}}_{p=0}$ (since $\overline{\mathrm{Ell}}(p^n)$ is finite flat over $\overline{\mathrm{Ell}}$). It follows that the ordinary locus $\mathrm{Ell}(p^n)^{\mathrm{ord}}_{p=0} \times_{\mathrm{Ell}(p^n)^{\mathrm{ord}}_{\pi=0}} \mathrm{Ell}(p^n)^{\mathrm{ord}}_{p=0}$ is schematically dense in the fiber product $\mathrm{Ell}(p^n)_{p=0} \times_{\mathrm{Ell}(p^n)_{\pi=0}} \mathrm{Ell}(p^n)_{p=0}$, so it suffices to prove that $\theta \circ q_+$ and $\theta \circ q_-$ agree on the ordinary locus. This follows from the existence of the morphism $\Theta^{\mathrm{ord}} : \mathrm{Ell}(p^n)^{\mathrm{ord}}_{\pi=0} \to \overline{\mathrm{Ell}}(p^{n-1})_{p=0}$ supplied by Proposition 1.11. $\square$

2 The Ordinary Locus

Let E be an elliptic curve over a commutative $\mathbf{F}_p$-algebra R. We say that E is *ordinary* if each fiber of the map $E \to \mathrm{Spec}(R)$ is an ordinary elliptic curve. In this case, the subgroup scheme $E[p^n] \subseteq E$ fits into a short exact sequence of finite flat group schemes

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

here $E[p^n]_{\mathrm{conn}}$ is the connected component of the identity in $E[p^n]$ (given by the kernel of the nth power of the Frobenius morphism on E), and $E[p^n]_{\text{ét}}$ is an étale group scheme which is Cartier dual to $E[p^n]_{\mathrm{conn}}$ (via the Weil pairing)

Remark 2.1 (Level Structures on Ordinary Elliptic Curves)**.** Let $E \to \mathrm{Spec}(R)$ be an ordinary elliptic curve over an $\mathbf{F}_p$-algebra R. Then a pair of p^n-torsion points $x, y \in E(R)$ determines a full level-p^n structure on E if and only if the following two conditions are satisfied:

- The induced map of finite flat group schemes $(\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \to E[p^n]$ induces an epimorphism of étale group schemes $(\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \twoheadrightarrow E[p^n]_{\text{ét}}$.
- The Weil pairing $e_{p^n}(x, y) \in \mu_{p^n}(R)$ is a *primitive* p^nth root of unity: that is, it satisfies the cyclotomic polynomial $\frac{u^{p^n}-1}{u^{p^{n-1}}-1}$.

See Proposition 1.11.2 of [5].

Proposition 2.2. *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 p-torsion points $x, y \in E(R)$ which determine a full level-p structure on E, which we identify with a morphism of group schemes $\gamma : (\underline{\mathbf{Z}/p\,\mathbf{Z}})^2 \to E$. If the Weil pairing $e_p(x, y)$ is equal to* 1*, then γ factors uniquely as a composition $(\underline{\mathbf{Z}/p\,\mathbf{Z}})^2 \twoheadrightarrow S \hookrightarrow E$, where $S \subseteq E$ is an étale subgroup of degree p.*

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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & (\underline{\mathbf{Z}/p\,\mathbf{Z}})^2 & \longrightarrow & S & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma_0} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \sim} & & \\ 0 & \longrightarrow & E[p]_{\text{conn}} & \longrightarrow & E[p] & \longrightarrow & E[p]_{\text{ét}} & \longrightarrow & 0. \end{array}$$

Since the Weil pairing on $E[p]$ induces a perfect pairing of $E[p]_{\text{conn}}$ with $E[p]_{\text{ét}}$, the equation $e_p(x, y) = 1$ guarantees that the morphism γ_0 vanishes. It follows that γ factors through a unique homomorphism $S \to E[p]$, which splits the epimorphism $E[p] \twoheadrightarrow E[p]_{\text{ét}}$ and therefore identifies S with a closed subgroup of $E[p] \subset E$. □

Remark 2.3. In the situation of Proposition 2.2, let E/S denote the quotient of E by the subgroup $S \subset E$, let $(E/S)^{(p)}$ denote its pullback along the Frobenius map $\mathrm{Spec}(R) \to \mathrm{Spec}(R)$, and let $F : E/S \to (E/S)^{(p)}$ be the relative Frobenius map. Then the composite map $E \twoheadrightarrow E/S \xrightarrow{F} (E/S)^{(p)}$ is an isogeny of degree p^2, whose

kernel is the p-torsion subgroup $E[p] \subset E$. It follows that there exists a unique isomorphism of elliptic curves $\alpha : E \to (E/S)^{(p)}$ for which the diagram

$$\begin{array}{ccc} E & \longrightarrow & E/S \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle F} \\ E & \xrightarrow[\sim]{\alpha} & (E/S)^{(p)} \end{array}$$

is commutative.

Corollary 2.4. *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 p-torsion points $x, y \in E(R)$ which determine a full level-p^n structure on E for some $n \geqslant 1$, which we identify with a morphism of group schemes $\gamma : (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 \to E$.*

(*a*) *If the Weil pairing $e_{p^n}(x, y)$ is a p^{n-1}st root of unity, then there exists a diagram of group schemes (which is unique up to unique isomorphism)*

$$\begin{array}{ccc} (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 & \longrightarrow & (\underline{\mathbf{Z}/p^{n-1}\,\mathbf{Z}})^2 \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \gamma'} \\ E & \xrightarrow{\quad f \quad} & E', \end{array}$$

where f is an étale isogeny of degree p.

(*b*) *If $n \geqslant 2$ and the Weil pairing $e_{p^n}(x, y)$ is a primitive p^{n-1}st root of unity, then the map $\gamma' : (\underline{\mathbf{Z}/p^{n-1}\,\mathbf{Z}})^2 \to E'$ is a full level-p^{n-1} structure on the elliptic curve E'.*

Proof. If $e_{p^n}(x, y)$ is a p^{n-1}st root of unity, then $e_p(p^{n-1}x, p^{n-1}y) = 1$. Applying Proposition 2.2, we see that there is a unique étale subgroup $S \subseteq E$ of degree p containing the points $p^{n-1}x$ and $p^{n-1}y$. To prove (*a*), we take $E' = E/S$ and $f : E \twoheadrightarrow E'$ to be the tautological map. Note that we have a commutative diagram of étale group schemes

$$\begin{array}{ccc} (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 & \longrightarrow & (\underline{\mathbf{Z}/p^{n-1}\,\mathbf{Z}})^2 \\ \downarrow & & \downarrow \\ E[p^n]_{\text{ét}} & \longrightarrow & E'[p^{n-1}]_{\text{ét}}, \end{array}$$

where the left vertical map and bottom horizontal map are epimorphisms; it follows that the right vertical map is also an epimorphism. Invoking Remark 2.1, we deduce that γ' is a full level-p^{n-1} structure on the elliptic curve E' if and only if $e_{p^{n-1}}(f(x), f(y)) = e_{p^n}(x, y)$ is a primitive p^{n-1}st root of unity, which proves (*b*). □

Example 2.5. Let E be an ordinary elliptic curve over an $\mathbf{F}_p$-algebra R, let $E^{(p)}$ denote the pullback of E along the Frobenius map $\varphi : \mathrm{Spec}(R) \to \mathrm{Spec}(R)$, and let $F : E \to E^{(p)}$ be the relative Frobenius map. Let $x, y \in E(R)$ be a pair of points which supply a full level-p^n structure on E, for some $n \geqslant 2$. Then (Fx, Fy) is a full level-p^n structure on $E^{(p)}$, and the Weil pairing $e_{p^n}(Fx, Fy) = e_{p^n}(x, y)^p$ is a primitive p^{n-1}st root of unity (since $e_{p^n}(x, y)$ is a primitive p^nth root of unity). Applying Corollary 2.4 to the triple $(E^{(p)}, Fx, Fy)$, we obtain the commutative diagram

$$\begin{array}{ccc} (\underline{\mathbf{Z}/p^n\,\mathbf{Z}})^2 & \longrightarrow & (\underline{\mathbf{Z}/p^{n-1}\,\mathbf{Z}})^2 \\ \downarrow{\scriptstyle (Fx,Fy)} & & \downarrow{\scriptstyle (px,py)} \\ E^{(p)} & \xrightarrow{\quad V \quad} & E, \end{array}$$

where $V : E^{(p)} \to E$ is the Verschiebung morphism.

Proof of Proposition 1.11. Fix $n \geqslant 2$ and let R be a commutative $\mathbf{F}_p$-algebra, so that we can identify R-valued points of $\mathrm{Ell}(p^n)^{\mathrm{ord}}_{p=0}$ with triples (E, x, y) where E is an ordinary elliptic curve over $\mathrm{Spec}(R)$ and (x, y) is a full level-p^n structure on E. Set $\pi = (\zeta_{p^2} - 1)^{p-1} \in \mathbf{Z}[\zeta_{p^n}]$. Using the identity

$$\pi \equiv 1 + \zeta_{p^2} + \cdots + \zeta_{p^2}^{p-1} = 1 + \zeta_{p^n}^{p^{n-2}} + \cdots + \zeta_{p^n}^{(p-1)p^{n-2}} \pmod{p}.$$

It follows that (E, x, y) is an R-valued point of the closed substack $\mathrm{Ell}(p^n)^{\mathrm{ord}}_{\pi=0} \subseteq \mathrm{Ell}(p^n)^{\mathrm{ord}}_{p=0}$ if and only if the Weil pairing $e_{p^n}(x, y)$ is a primitive p^{n-1}st root of unity. In this case, Corollary 2.4 supplies an étale isogeny $f : E \twoheadrightarrow E'$ of degree p such that $(f(x), f(y))$ is a full level-p^{n-1} structure on E'. This construction depends functorially on R and therefore determines a map of moduli stacks $\Theta^{\mathrm{ord}} : \mathrm{Ell}(p^n)^{\mathrm{ord}}_{\pi=0} \to \mathrm{Ell}(p^{n-1})_{p=0}$. It follows from Remark 2.3 and Example 2.5 that this map fits into a commutative diagram of Deligne-Mumford stacks

$$\begin{array}{ccc} \mathrm{Ell}(p^n)^{\mathrm{ord}}_{p=0} & \xrightarrow{\varphi} & \mathrm{Ell}(p^n)^{\mathrm{ord}}_{\pi=0} \\ \downarrow & \overset{\Theta^{\mathrm{ord}}}{\swarrow} & \downarrow \\ \overline{\mathrm{Ell}}(p^{n-1})_{p=0} & \xrightarrow{\varphi} & \overline{\mathrm{Ell}}(p^{n-1})_{p=0}. \end{array}$$

□

3 Kunz's Theorem in Mixed Characteristic

We refer the reader to [6] for a proof of the following classical result:

Theorem 3.1 (Kunz)**.** *Let R be a Noetherian $\mathbf{F}_p$-algebra. Then R is regular if and only if the Frobenius morphism $\varphi_R : R \to R$ is flat.*

Our goal in this section is to prove the following mixed-characteristic variant of Theorem 3.1, which was suggested to us by Gabber (see [2] for a closely related result):

Theorem 3.2. *Let R be a Noetherian ring and let $\pi \in R$ be a regular element for which π^p divides p. The following conditions are equivalent:*

(1) *For every maximal ideal $\mathfrak{m} \subseteq R$ containing π, the local ring $R_{\mathfrak{m}}$ is regular.*

(2) *The Frobenius morphism $\varphi : R/\pi R \to R/\pi^p R$ is flat.*

Remark 3.3. For the purpose of proving Theorem 1.9, we will need only the "easy" implication (1) $\Rightarrow$ (2) of Theorem 3.2. However, since the converse implication may be of independent interest, we include a proof here.

Warning 3.4. In the statement of Theorem 3.2, the assumption that π is regular cannot be omitted (note that the ring $\mathbf{F}_p[\pi]/(\pi^p)$ satisfies condition (2) of Theorem 3.2, but does not satisfy (1)).

Proof of (1) $\Rightarrow$ (2). Let R be a Noetherian ring containing a regular element π for which π^p divides p. To show that the Frobenius map $\varphi : R/\pi R \to R/\pi^p R$ is flat, it will suffice to show that it becomes flat after localizing with respect to every prime ideal of $R/(\pi)$. We may therefore assume without loss of generality that R is a local ring whose maximal ideal $\mathfrak{m}$ contains π. Choose a faithfully flat map $R \to S$, where S is a complete regular local ring with perfect residue field. We then have a commutative diagram

$$\begin{array}{ccc} R/\pi R & \xrightarrow{\varphi} & R/\pi^p R \\ \downarrow & & \downarrow \\ S/\pi S & \xrightarrow{\varphi} & S/\pi^p S, \end{array}$$

where the vertical maps are faithfully flat. Consequently, to show that the upper horizontal map is flat, it will suffice to show that the lower horizontal map is flat. We may therefore replace R by S and thereby reduce to the case where R is a complete regular local ring with perfect residue field $k = R/\mathfrak{m}$.

Choose a regular system of parameters $x_1, x_2, \ldots, x_n \in \mathfrak{m}$, and let $\overline{R}$ denote the power series ring $W(k)[[X_1, \ldots, X_n]]$, so that there is a unique surjective ring homomorphism $\rho : \overline{R} \to R$ lifting the identity map id_k on residue fields and satisfying

$\rho(X_i) = x_i$. Choose a ring homomorphism $\varphi_{\overline{R}} : \overline{R} \to \overline{R}$ lifting the Frobenius map on $\overline{R}/p\overline{R}$ (for example, we can choose $\varphi_{\overline{R}}$ to carry each generator X_i to its pth power); note that $\varphi_{\overline{R}}$ automatically restricts to the Witt vector Frobenius on $W(k)$. We then have a commutative diagram

$$\begin{array}{ccc} \overline{R} & \twoheadrightarrow & R/\pi R \\ \downarrow{\scriptstyle \varphi_{\overline{R}}} & & \downarrow{\scriptstyle \varphi} \\ \overline{R} & \twoheadrightarrow & R/\pi^p R, \end{array} \tag{2}$$

where the left vertical map is flat. We will complete the proof by showing that this diagram is a pushout square of commutative rings.

Since the element $p \in R$ belongs to $\mathfrak{m}$, we can choose a power series $f = f(X_1, \ldots, X_n)$ with vanishing constant term satisfying $\rho(f) = p$, so that ρ induces an isomorphism $\overline{R}/(p-f) \simeq R$. Similarly, we can choose a power series $\overline{\pi} = \overline{\pi}(X_1, \ldots, X_n)$ with vanishing constant term which satisfies $\rho(\overline{\pi}) = \pi$. It follows that the homomorphism $\overline{R} \xrightarrow{\rho} R \twoheadrightarrow R/\pi R$ is a surjection with kernel ideal $(p - f, \overline{\pi})$, and that the homomorphism $\overline{R} \xrightarrow{\rho} R \twoheadrightarrow R/\pi^p R$ is a surjection with kernel ideal $(p - f, \overline{\pi}^p)$. Let I denote the ideal of $\overline{R}$ generated by the elements $\varphi_{\overline{R}}(p - f)$ and $\varphi_{\overline{R}}(\overline{\pi})$, so that the commutativity of diagram (2) guarantees that we have an inclusion $I \subseteq (p - f, \overline{\pi}^p)$. To complete the proof, it will suffice to show that the reverse inclusion holds: that is, that $p - f$ and $\overline{\pi}^p$ belong to I.

Since the quotient ring $\overline{R}/(p-f, \overline{\pi}) \simeq R/\pi R$ is an $\mathbf{F}_p$-algebra, the ideal $(p-f, \overline{\pi}) \subseteq \overline{R}$ contains p. Applying the ring homomorphism $\varphi_{\overline{R}}$, we deduce that the ideal I also contains p. The congruence $\overline{\pi}^p \equiv \varphi_{\overline{R}}(\overline{\pi}) \pmod{p}$ shows that $\overline{\pi}^p$ also belongs to I. Our assumption that π^p divides p in R guarantees that we can write $p = a\overline{\pi}^p + b(p - f)$ for some elements $a, b \in \overline{R}$. Evaluating at $X_1 = X_2 = \cdots = X_n = 0$, we see that the power series b must have constant term equal to 1, and is therefore an invertible element of $\overline{R}$. We then have

$$p - f = b^{-1}(p - a\overline{\pi}^p) \in (p, \overline{\pi}^p) \subseteq I,$$

as desired. □

Proof of (2) ⇒ (1). Fix a Noetherian ring R, a regular element $\pi \in R$ such that π^p divides p, and assume that the Frobenius homomorphism $\varphi : R/\pi R \to R/\pi^p R$ is flat. We wish to show that, for every maximal ideal $\mathfrak{m} \subseteq R$ containing π, the local ring $R_{\mathfrak{m}}$ is regular. Replacing R by its localization $R_{\mathfrak{m}}$, we may assume that R is a local ring whose maximal ideal $\mathfrak{m}$ contains π. Let $\mathfrak{n}$ denote the maximal ideal of the

quotient ring $R/\pi R$, and let $x_1, \ldots, x_d \in \mathfrak{m}$ be a collection of elements whose images form a basis of the quotient $\mathfrak{n}/\mathfrak{n}^2$ (as a vector space over the residue field $R/\mathfrak{m}$). Let $c = \ell(R/(\pi^p, x_1^p, \ldots, x_d^p))$ denote the length of the Artinian ring $R/(\pi^p, x_1^p, \ldots, x_d^p)$.

Let I denote the ideal of $R/\pi^p R$ generated by the images of the elements x_i^p. Invoking the flatness of the Frobenius map $\varphi : R/\pi R \to R/\pi^p R$, we see that I/I^2 is a free module of rank d over the quotient ring $R/(\pi^p, x_1^p, \ldots, x_d^p)$, with basis given by the images of the elements x_i^p. Applying [9, Tag 0EBY], we conclude that $c = p^d \ell(R/(\pi^p, x_1, \ldots, x_d))$. In particular, we have $c \geqslant p^d$, and equality holds if and only if $\mathfrak{m} = (\pi^p, x_1, \ldots, x_d)$.

Let $\chi : \mathbf{Z}_{\geqslant 0} \to \mathbf{Z}_{\geqslant 0}$ be the Hilbert-Samuel function $\chi(t) = \ell(R/(\pi R + \mathfrak{m}^t))$. For $t \gg 0$, $\chi(t)$ is a polynomial function of n, whose degree D is equal to the Krull dimension of $R/\pi R$ (so that $D+1$ is the Krull dimension of R, since the element π is not a zero divisor). Using flatness of the Frobenius map $\varphi : R/\pi R \to R/\pi^p R$, we obtain

$$\begin{aligned}
\chi(t) &= \ell(R/(\pi R + (x_1, \ldots, x_d)^t)) \\
&= \frac{1}{c} \ell(R/(\pi^p R + (x_1^p, \ldots, x_d^p)^t)) \\
&\leqslant \frac{1}{c} \ell(R/(\pi^p R + (x_1, \ldots, x_d)^{pt+(p-1)d})) \\
&\leqslant \frac{p}{c} \ell(R/(\pi R + (x_1, \ldots, x_d)^{pt+(p-1)d})) \\
&= \frac{p}{c} \chi(pt + (p-1)d).
\end{aligned}$$

Evaluating at $t \gg 0$, we deduce that $p^{D+1} \geqslant c$.

We now consider two cases:

- Suppose that $c > p^d$. It follows that the Krull dimension $\dim(R) = D+1$ is strictly larger than d. Then the maximal ideal $\mathfrak{m} = (\pi, x_1, \ldots, x_d)$ can be generated by $d+1 \leqslant \dim(R)$ elements, so R is regular.
- Suppose that $c = p^d$, so that $\mathfrak{m} = (\pi^p, x_1, \ldots, x_d)$. Applying Nakayama's lemma, we deduce that $\mathfrak{m} = (x_1, \ldots, x_d)$ can be generated by $d \leqslant D+1 = \dim(R)$ elements, so R is regular. □

References

[1] Bhatt, B., Morrow, M., and P. Scholze. *Integral p-adic Hodge Theory.* Publ. Math. Inst. Hautes Études Sci. 128 (2018), 219–397.

[2] Bhatt, B., Iyengar, S. and L. Ma. *Regular rings and perfect(oid) algebras.* Comm. Algebra 47 (2019), no. 6, 2367–2383.

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

[4] 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.

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

[6] Kunz, E. *On Noetherian rings of characteristic p.* Amer. J. Math. 98 (1976), no. 4, 999–1013.

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

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

[9] *The Stacks Project.* `https://stacks.math.columbia.edu`.

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