THE NÉRON MODEL OVER THE IGUSA CURVES

CHRISTIAN LIEDTKE AND STEFAN SCHRÖER

Revised version, 14 March 2010

Abstract. We analyze the geometry of rational p-division points in degenerating families of elliptic curves in characteristic p. We classify the possible Kodaira symbols and determine for the Igusa moduli problem the reduction type of the universal curve. Special attention is paid to characteristic 2 and 3, where wild ramification and stacky phenomena show up.

Contents

Introduction 1
1. Twisted forms of μ_p and their torsors 4
2. Twisted forms of p-torsion in elliptic curves 9
3. The extension class 12
4. Néron models and sections of order p 14
5. Osculation numbers and Hasse invariant 16
6. Reduction types under quadratic twists 18
7. Reduction type under Frobenius pullback 20
8. p-torsion under quadratic twists 21
9. Decreasing osculation numbers 23
10. The elliptic curve over the Igusa curve 27
11. Elliptic curves with $\delta = 1$ 29
12. The Igusa curve in characteristic three 34
13. The Igusa stack in characteristic two 36
14. Other reduction types in characteristic two 40
15. Semistable reduction in characteristic two 42
References 43

Introduction

Let R be a discrete valuation ring of characteristic $p > 0$, with function field $R \subset K$ and residue field $k = R/\mathfrak{m}_R$, which for simplicity we assume to be algebraically closed. Suppose E_K is an elliptic curve containing a *rational p-division point* $z \in E_K$, that is a K-rational point of order p. The goal of this paper is to analyze the Néron model $E \to \operatorname{Spec}(R)$ and the geometry of the specialization $\overline{\{z\}} \subset E$. The corresponding problem for rational division points of order prime to p is classical and is basically answered by the Ogg-Shafarevich Criterion. For rational p-division points the situation turns out to be rather different.

2000 *Mathematics Subject Classification.* 14H52, 14H10, 14L15, 11G07.

Our point of departure are the following questions:

(i) When does there exist a rational p-division point $z \in E_K$ at all?
(ii) What are the possible *Kodaira symbols* describing the reduction types for E?
(iii) Can the specialization of z into the closed fiber E_k be nonzero?
(iv) And for characteristic two and three, which are somewhat special for our considerations, can the class of z in the *component group* Φ_k be nonzero as well?

Naturally these questions are closely related to the universal family $U \to \mathrm{Ig}(p)$ over the *Igusa curve*, which, roughly speaking, parametrizes elliptic curves endowed with a rational p-division point on the Frobenius pullback.

For the existence of a rational p-division point we analyze the kernel of the multiplication-by-p map. For ordinary elliptic curves, this is a twisted form of $\mu_p \oplus (\mathbb{Z}/p\mathbb{Z})$ and a rational p-division point exists if and only if this twisted form is trivial. We classify twisted forms of this group scheme in terms of nonabelian cohomology and relate this classification to the Hasse- and the j-invariant of an elliptic curve.

In characteristic $p \geq 5$ it turns out that the answer to the other questions depends on the congruence class of the characteristic modulo 12. Once we have an elliptic curve with additive reduction and a rational p-division point with nonzero specialization, Frobenius pullbacks provide elliptic curves with the same reduction type as before and zero specialization of arbitrary *osculation number*. Hence we are mainly interested in nonzero specialization of the p-division point and the first main result is:

Theorem. *Suppose $p \geq 5$. An elliptic curve E_K with additive reduction and containing a rational p-division point with nonzero specialization exists precisely for the following reduction types:*

congruence mod 12	reduction type
$p \equiv 1$	I_0^*
$p \equiv 5$	$\mathrm{II}, \mathrm{IV}, \mathrm{I}_0^*, \mathrm{IV}^*, \mathrm{II}^*$
$p \equiv 7$	$\mathrm{III}, \mathrm{I}_0^*, \mathrm{III}^*$
$p \equiv 11$	$\mathrm{II}, \mathrm{III}, \mathrm{IV}, \mathrm{I}_0^*, \mathrm{IV}^*, \mathrm{III}^*, \mathrm{II}^*$

In this case E_K has potentially supersingular reduction.

The same result holds if one demands that the rational point of order p exists only on the Frobenius pullback. We actually construct explicit examples of such curves in terms of Weierstrass equations. Note however, that we do not know the explicit coordinates for the rational p-division points. This existence of our examples has strong consequences for the universal elliptic curve over the Igusa curve: Let F be the function field of the Igusa curve $\mathrm{Ig}(p)$, and U_F the corresponding universal elliptic curve, and $x \in \mathrm{Ig}(p)$ be a supersingular point. Our second main result gives Weierstrass equations for U_F:

Theorem. *Suppose $p \geq 5$. Then for a suitable uniformizer $t \in \mathcal{O}^{\wedge}_{\mathrm{Ig}(p),x}$ the universal elliptic curve U_F over the completion at x is given by the following Weierstrass equations:*

$j(x)$	p	Weierstrass equation	U_F	$U_F^{(p)}$
0	$\equiv -1 \mod 3$	$y^2 = x^3 + t^{(p-5)/6}x + t^{-1}$	III^*	III
1728	$\equiv -1 \mod 4$	$y^2 = x^3 + t^{-1}x + t^{(p-7)/4}$	II^*	II
$\neq 0, 1728$	all p	$y^2 = x^3 + at^{-2p}x + (b + t^{(p-1)/2})t^{-3p}$	I_0^*	I_0^*

Here $a, b \in k$ are scalars so that the elliptic curve $y^2 = x^3 + ax + b$ has supersingular j-invariant $j = j(x)$.

Note that Ulmer [23] gave Weierstrass equations with coefficients in F for the universal curve U_F, which rely on relations between Eisenstein series and are of somewhat implicit nature. Our Weierstrass equations are explicit, but are defined only over various completions.

The situation in characteristic $p = 3$ and $p = 2$ is more complicated and, in some sense, entirely different. This comes from the fact that, besides the valuation of a minimal discriminant $\nu(\Delta)$, there is an additional numerical invariant $\delta \geq 0$, the *wild part of the conductor*.

Theorem. *Let $p = 3$. For the Kodaira symbols* II, II^*, III, III^*, IV, IV^*, I_0^*, *there is an elliptic curve E_K containing a rational 3-division point with nonzero specialization in E_k and the given reduction type. For* IV *and* IV^*, *there are such examples with nonzero specialization in Φ_k, and examples with zero specialization in Φ_k. In any case, the curve has potentially supersingular reduction.*

We show by example that the property of having a rational 3-division point with nonzero class in Φ_k might even be preserved under base changes of arbitrarily large degree. The universal elliptic curve over Ig(3) has already been determined by Ulmer [23] and we reprove this result in our setup.

In characteristic two, the Igusa moduli problem is not representable, such that stacky phenomena show up. Now, there is no restriction on the reduction type and the elliptic curve may have potentially ordinary and potentially multiplicative reduction.

Theorem. *Let $p = 2$. For all additive Kodaira symbols, there is an elliptic curve E_K containing a rational point of order two with nonzero specialization in E_k and having the given reduction type. For the Kodaira symbols* III, III^*, I_l^*, *$l \geq 0$, there are such examples where the specialization has nonzero class in Φ_k, and examples with zero class in Φ_k.*

To prove the preceding results, we analyze the behavior of the wild part of the conductor under small field extensions, and then apply Ogg's Formula $\nu(\Delta) = 2 + \delta + (m - 1)$ to determine the reduction type. It turns out that the numerical invariants have enough variation so that the Kodaira symbols listed above appear.

The article is organized as follows: In Section 1 we classify twisted forms of μ_p and describe their p-Lie algebras. In Section 2 we classify the twisted forms of $\mu_p \oplus (\mathbb{Z}/p\mathbb{Z})$ in terms of nonabelian cohomology. This preparatory work is used in Section 3 to describe the p-torsion subgroup scheme of an ordinary elliptic curve. In particular, we answer when an elliptic curve has a rational p-division point in this abstract setup and relate this to the Hasse- and the j-invariant of the curve. In Section 4 we prove that an elliptic curve with additive reduction has potentially supersingular reduction, provided that it contains a rational p-division point with

trivial specialization into the component group. This result restricts the possible additive reduction types depending on the congruence class of p modulo 12. In Section 5 we introduce the notion of osculation number, that is, the order of tangency of a rational p-division point with the zero section, and compute it in terms of the Hasse invariant. This allows us to decide when rational p-division points have nonzero specialization in the closed fiber of the Néron model without computing the coordinates of these points explicitly. In Section 6 we determine how the reduction type of an elliptic curve in characteristic $p \geq 5$ changes under twisting. This will be needed later on in the construction of examples. In Section 7 we determine how the reduction types in characteristic $p \geq 5$ change under Frobenius pullbacks, which we need for the analysis of the Igusa moduli problem. In Section 8 we construct elliptic curves with reduction of type I_0^* and having a rational p-division point with nonzero specialization in the special fiber. These curves are obtained as quadratic twists of certain pullbacks of the versal deformation of a given supersingular elliptic curve. In Section 9 we start from versal deformations of supersingular elliptic curves with $j = 0$ or $j = 1728$ and construct elliptic curves having rational p-division points and nonzero specialization in the special fiber for the remaining reduction types. At this point we have shown that all possibilities determined in Section 4 do exist in characteristic $p \geq 5$. In Section 10 we use our results to determine the degeneration behavior of the universal elliptic curve over the Igusa moduli problem in characteristic $p \geq 5$. We even determine equations of the Néron model over the Igusa curves around its supersingular points. In Section 11, we specialize to characteristic 2 and 3, where we analyze the Galois action on torsion points attached to elliptic curves whose wild part δ of the conductor is nontrivial yet as small as possible, namely $\delta = 1$. In Section 12 we use these results to establish existence of elliptic curves in characteristic 3 having a rational 3-division point with nonzero specialization in the closed fiber for all possible reduction types. Also, we determine the Néron model over the Igusa curve in characteristic 3. In Section 13 we specialize to characteristic 2 and introduce tautological families. Since the Igusa moduli problem is not representable in characteristic 2, these families are in some sense the best replacement for the universal object. We determine their reduction types and their behavior under Frobenius pullbacks. In Section 14 we construct the missing reduction types as pullbacks from tautological families. In Section 15 we classify reduction types in case we do not have potentially supersingular reduction.

Acknowledgement. We thank Matthias Schütt and the referee for helpful comments.

1. Twisted forms of μ_p and their torsors

Let S be a base scheme of characteristic $p > 0$, endowed with the fppf-topology. Consider the finite diagonalizable group scheme $\mu_p = \mathrm{Spec}(\mathcal{O}_S[\mathbb{Z}/p\mathbb{Z}])$, whose values on $\mathrm{Spec}(A) \to S$ are

$$\mu_p(A) = \{x \in A \mid x^p = 1\}\,.$$

In this section we shall discuss twisted forms $\widetilde{\mu}_p$ of μ_p and the corresponding group $H^1(S, \widetilde{\mu}_p)$ of isomorphism classes of $\widetilde{\mu}_p$-torsors. The former occur "in nature" as the kernel of the relative Frobenius on ordinary elliptic curves. The results will be used in the next section, which contains an analogous analysis for the group scheme $\mu_p \oplus \mathbb{Z}/p\mathbb{Z}$. Throughout, we assume for simplicity that $S = \mathrm{Spec}(R)$ is affine, and

that $\mathrm{Pic}(R) = 0$; for example, R could be a field, a local ring, or a polynomial ring over a field.

Let $\mathcal{A} = \underline{\mathrm{Aut}}(\mu_p)$ be the sheaf of automorphisms of μ_p. A twisted form $\widetilde{\mu}_p$ of μ_p determines an $\mathcal{A}$-torsor $\underline{\mathrm{Isom}}(\mu_p, \widetilde{\mu}_p)$. Conversely, an $\mathcal{A}$-torsor T yields a twisted form $\widetilde{\mu}_p = T \wedge^{\mathcal{A}} \mu_p = (T \times \mu_p)/\mathcal{A}$. Here the quotient is with respect to the diagonal action of $\mathcal{A}$ on the product. This establishes a canonical bijection between the cohomology set $H^1(S, \mathcal{A})$ and the set of isomorphism classes of twisted forms of μ_p. This correspondence has nothing in particular to do with μ_p; rather, it gives a general classification of twisted forms of sheaves (see [5], Chapter V, or [4], Chapter III, Section 2.3. An exposition in the context of Galois cohomology can be found in [12], Chapter I, §5).

Let us write down the sheaf of automorphism $\mathcal{A}$: We have a canonical map

$$(\underline{\mathbb{Z}/p\mathbb{Z}})^\times \longrightarrow \mathcal{A}, \quad \zeta \longmapsto (a \longmapsto a^\zeta),$$

and it follows from [6], Exposé VIII, Corollary 1.6 that this map is bijective. Since S is of characteristic $p > 0$, we have $\mu_{p-1} = (\underline{\mathbb{Z}/p\mathbb{Z}})^\times$ and so we may also write this bijection as $\mu_{p-1} \to \mathcal{A}$. Using the Kummer sequence $1 \to \mu_{p-1} \to \mathbb{G}_m \stackrel{p-1}{\to} \mathbb{G}_m \to 1$ and our assumption $\mathrm{Pic}(S) = 0$, we deduce that the coboundary map

$$R^\times / R^{\times(p-1)} \longrightarrow H^1(S, \mu_{p-1}) = H^1(S, \mathcal{A})$$

is bijective. In other words, the set of isomorphism classes of twisted forms of μ_p is the abelian group $R^\times/R^{\times(p-1)}$. We call $\tau \in R^\times$ the *twist parameter* for the corresponding twisted form $\widetilde{\mu}_p$. To write down these group schemes explicitly, we first determine their p-Lie algebras:

Write $\mu_p = \mathrm{Spec}(R[T]/(T^p - 1))$, and let $I \subset R[T]/(T^p - 1)$ be the principle ideal generated by $T - 1$. Then $\mathrm{Lie}(\mu_p)$ equals $(I/I^2)^\vee$, which is a free R-module of rank one, with basis $u \in \mathrm{Lie}(\mu_p)$ the residue class of $T - 1$. Using

$$T^\zeta - 1 = (T-1)(T^{\zeta-1} + T^{\zeta-2} + \ldots + 1) \equiv (T-1)\zeta \quad \text{modulo } I^2,$$

we see that the scalars $\zeta \in \mu_{p-1}$ act on $\mathrm{Lie}(\mu_p)$ by scalar multiplication with ζ. A straightforward computation shows that the p-fold composition of the derivation $(T-1)\frac{d}{d(T-1)}$ equals itself. In other words, the p-th power operation is given by $u^{[p]} = u$. We now view $H^1(S, \mathcal{A}) = R^\times/R^{\times(p-1)}$ as the set of isomorphism classes of twisted forms $\widetilde{\mathfrak{g}}$ of the p-Lie algebra $\mathfrak{g} = \mathrm{Lie}(\mu_p)$.

Proposition 1.1. *Let $\tau \in R^\times$. Then the corresponding twisted form $\widetilde{\mathfrak{g}}$ is the 1-dimensional p-Lie algebra with basis $\widetilde{u} \in \widetilde{\mathfrak{g}}$ so that $\widetilde{u}^{[p]} = \tau^{-1}\widetilde{u}$.*

Proof. By definition, the p-Lie algebra $\widetilde{\mathfrak{g}}$ is the invariant submodule of the R-module $\mathfrak{g} \otimes_R R[X]/(X^{p-1} - \tau)$, where the action of $\zeta \in \mu_{p-1}$ is induced by $X \mapsto \zeta X$ and $u \mapsto \zeta u$. Clearly, $\widetilde{u} = u \otimes X^{-1}$ is invariant, and a basis of the twisted form $\widetilde{\mathfrak{g}}$. Its p-th power is $\widetilde{u}^{[p]} = u^{[p]} \otimes X^{-p} = \tau^{-1} \cdot u \otimes X^{-1} = \tau^{-1}\widetilde{u}$. □

We finally regard $H^1(S, \mathcal{A}) = R^\times/R^{\times(p-1)}$ as the set of twisted forms $\widetilde{\mu}_p$ of the finite group scheme μ_p.

Proposition 1.2. *Let $\tau \in R^\times$. Then the corresponding twisted form $\widetilde{\mu}_p$ is the finite group scheme whose values on R-algebras A are $\widetilde{\mu}_p(A) = \{a \in A \mid a^p = 0\}$,*

with composition law

$$a \star b = a + b + \frac{1}{\tau} \sum_{i=1}^{p-1} \frac{a^i b^{p-i}}{i!(p-i)!}. \tag{1}$$

Proof. First observe that the functor $G \mapsto \mathrm{Lie}(G)$ induces an equivalence between the category of finite flat group schemes of height ≤ 1 and the category of p-Lie algebras whose underlying module is projective of finite rank. An inverse functor is $\mathfrak{g} \mapsto \mathrm{Spec}(U^{[p]}(\mathfrak{g})^\vee)$, where $U^{[p]}(\mathfrak{g})$ is the the universal enveloping algebra $U(\mathfrak{g})$ modulo the relations $x^p - x^{[p]}$, $x \in \mathfrak{g}$. Multiplication and comultiplication in the dual $U^{[p]}(\mathfrak{g})^\vee$ are induced by the diagonal $U^{[p]}(\mathfrak{g}) \to U^{[p]}(\mathfrak{g}) \otimes U^{[p]}(\mathfrak{g})$ and the multiplication in $U^{[p]}(\mathfrak{g})$, respectively.

The p-Lie algebra of $\widetilde{\mu}_p$ is $\widetilde{\mathfrak{g}} = Ru$ as in Proposition 1.1, and we merely have to spell out the general construction outlined in the preceding paragraph for this special case. Clearly, $1, u, \ldots, u^{p-1} \in U^{[p]}(\mathfrak{g})$ is an R-basis. Let $f_0, \ldots, f_{p-1} \in U^{[p]}(\mathfrak{g})^\vee$ be the dual basis. For $0 \leq r, s, n \leq p-1$ we compute

$$(f_r f_s)(u^n) = \langle f_r \otimes f_s, (u \otimes 1 + 1 \otimes u)^n \rangle = \sum_{i=0}^{n} \binom{n}{i} f_r(u^i) f_s(u^{n-i}) = \binom{n}{r} \delta_{s,n-r},$$

where $\delta_{s,n-r}$ is a Kronecker Delta, and consequently

$$f_r f_s = \begin{cases} \binom{r+s}{r} f_{r+s} & \text{if } r+s < p, \\ 0 & \text{else.} \end{cases} \tag{2}$$

Now set $f = f_1$. Formula (2) inductively gives $f^i = i! f_i$ for $0 \leq i \leq p-1$ and $f^p = 0$. The upshot is that $U^{[p]}(\mathfrak{g})^\vee = R[f]/(f^p)$ as R-algebra. It remains to compute the comultiplication map. Now recall that $u^p = \tau^{-1} u$; this implies

$$f_n(u^i \otimes u^j) = f_n(u^{i+j}) = \begin{cases} \tau^{-1} & \text{if } i+j = n+p-1, \\ 1 & \text{if } i+j = n, \\ 0 & \text{else.} \end{cases}$$

for all $0 \leq n, i, j \leq p-1$. Putting things together, we infer that the comultiplication in $U^{[p]}(\mathfrak{g})^\vee$ is given by

$$f_n \longmapsto \sum_{i+j=n} \frac{f^i \otimes f^j}{i!j!} + \frac{1}{\tau} \sum_{i+j=n+p-1} \frac{f^i \otimes f^j}{i!j!}, \tag{3}$$

where the summation indices satisfy $0 \leq i, j \leq p-1$. The special case $n = 1$ now yields our assertions. □

Remark 1.3. Formula (1) is due to Tate and Oort [14], page 9, who derived it, from a different perspective and in a more general setting, with methods of representation theory. They actually obtained a classification of group schemes of order p over rather general base rings. A discussion of their results is contained in [13]. For further generalizations, see [15].

Remark 1.4. Consider the special case $\tau = 1$, such that $\widetilde{\mu}_p = \mu_p$. At first glance, it seems strange that the Formula (1) gives a composition law $a \star b$ (on elements with $a^p = b^p = 0$) that looks astonishingly different from the original composition

law $x \cdot y$ (on elements with $x^p = y^p = 1$). Things clear up if one uses, instead of $f \in U^{[p]}(\mathfrak{g})^\vee$, the truncated exponential

$$e = f_0 + f_1 + \ldots + f_{p-1} = 1 + f + \frac{f^2}{2!} + \ldots + \frac{f^{p-1}}{(p-1)!}.$$

Then $e^p = 1$, and a direct computation using (3) shows that the comultiplication indeed satisfies $e \mapsto e \otimes e$.

Now fix a twisting parameter $\tau \in R^\times$, and let $\widetilde{\mu}_p$ be the corresponding twisted form of μ_p. We seek to understand the group $H^1(S, \widetilde{\mu}_p)$ of isomorphism classes of $\widetilde{\mu}_p$-torsors. There seems to be no obvious relation to the group $H^1(S, \mu_p)$, because the automorphisms of μ_p act via outer automorphisms, compare [12], Proposition 43. In case $\tau \in R^{\times(p-1)}$, we have $\widetilde{\mu}_p \simeq \mu_p$, and the Kummer sequence yields an isomorphism

$$R^\times / R^{\times p} \longrightarrow H^1(S, \mu_p). \tag{4}$$

In case $\tau \notin R^{\times(p-1)}$, however, there is no embedding of $\widetilde{\mu}_p$ into any iterated extension of the standard group schemes $\mathbb{G}_a$ or $\mathbb{G}_m$, because there is no homomorphism of p-Lie algebras from $\widetilde{\mathfrak{g}} = \mathrm{Lie}(\widetilde{\mu}_p)$ to $\mathrm{Lie}(\mathbb{G}_a)$ or $\mathrm{Lie}(\mathbb{G}_m)$. This destroys any hopes for an easy direct computations of $H^1(S, \widetilde{\mu}_p)$ such as (4).

However, there is an approach using Weil restriction. Set $R' = R[X]/(X^{p-1} - \tau)$, such that $T = \mathrm{Spec}(R')$ is the μ_p-torsor with $\widetilde{\mu}_p = T \wedge^{\mathcal{A}} \mu_p$. Let $f : T \to S$ be the structure morphism, and consider the *Weil restriction* $H = f_*(\mu_{p,T})$. This is a finite commutative group scheme on S whose values on R-algebras A are given by

$$H(A) = \left\{ x \in (A \otimes_R R')^\times \mid x^p = 1 \right\}. \tag{5}$$

To understand it, consider the twisted forms $H_i = T \wedge^{\mathcal{A}} \mu_p$ of μ_p, where the action of $\zeta \in \mu_{p-1} = \mathcal{A}$ on μ_p is given by $x \mapsto x^{\zeta^i}$, for $0 \leq i \leq p-2$. Clearly, $H_0 = \mu_p$ and $H_1 = \widetilde{\mu}_p$.

Proposition 1.5. *There is a direct sum decomposition $H = H_0 \oplus H_1 \oplus \ldots \oplus H_{p-2}$.*

Proof. It suffices to check this on the level of p-Lie algebras. Set $\mathfrak{h} = \mathrm{Lie}(H)$. Obviously, $\mathfrak{h} = \mathrm{Lie}(\mu_{p,T}) = R'u$, viewed as an R-module. Whence $u, Xu, \ldots, X^{p-2}u \in \mathfrak{h}$ constitutes an R-basis, and $(X^i u)^{[p]} = X^{ip} u^{[p]} = \tau^i (X^i u)$. Setting $\mathfrak{h}_i = RX^i u$, we obtain a direct sum decomposition of p-Lie algebras $\mathfrak{h} = \mathfrak{h}_0 \oplus \mathfrak{h}_1 \oplus \ldots \oplus \mathfrak{h}_{p-2}$. Using Proposition 1.1, we infer that $\mathfrak{h}_i = \mathrm{Lie}(H_i)$. □

This decomposition can also be viewed as an eigenspace decomposition: The abelian Galois group μ_{p-1} acts functorially on the $\mathbb{F}_p$-vector space $H(A)$ described in (5) via its action on R'. Whence the functor $H = H_{\chi^0} \oplus H_\chi \oplus \ldots \oplus H_{\chi^{p-2}}$ decomposes into eigenspaces, which are indexed by the characters $\chi^i : \mu_{p-1} \to \mu_{p-1}$, $0 \leq i \leq p-1$. Here χ is the tautological character $\chi(\zeta) = \zeta$, and $\chi^i(\zeta) = \zeta^i$.

Proposition 1.6. *We have $H_i = H_{\chi^i}$ for all $0 \leq i \leq p-2$.*

Proof. We first look at the p-Lie subalgebras $\mathfrak{h}_i \subset \mathfrak{h}$. Clearly, $\mathfrak{h}_i = RX^i u$ is μ_{p-1}-invariant, and $\zeta \in \mu_{p-1}$ acts via multiplication by $\zeta^i = \chi^i(\zeta)$. It follows that $H_i \subset H$ is μ_{p-1}-invariant, and $\zeta \in \mu_{p-1}$ acts via multiplication by $\zeta^i = \chi^i(\zeta)$. Whence $H_i \subset H_{\chi^i}$. Since the inclusion

$$H = H_0 \oplus \ldots \oplus H_{p-2} \subset H_{\chi^0} \oplus \ldots \oplus H_{\chi^{p-2}} = H$$

is an equality, we conclude $H_i = H_{\chi^i}$. □

The decomposition is inherited to the cohomology groups of $H = f_*(\mu_{p,T})$. This leads to the desired computation of $H^1(S, \widetilde{\mu}_p)$:

Theorem 1.7. *The cohomology group $H^1(S, \widetilde{\mu}_p)$ is the χ-eigenspace inside the cohomology group $H^1(S, f_*(\mu_{p,T})) = R'^{\times}/R'^{\times p}$ with respect to the Galois action of μ_{p-1}, where $\chi : \mu_{p-1} \to \mu_{p-1}$ is the tautological character $\chi(\zeta) = \zeta$.*

Proof. We have $\widetilde{\mu}_p = H_1 = H_\chi \subset H = f_*(\mu_{p,T})$, whence $H^1(S, \widetilde{\mu}_p)$ is the χ-eigenspace of $H^1(S, f_*(\mu_{p,T}))$. Since $f : T \to S$ is finite and flat and $T \times_S T$ is a disjoint sum of copies of T, it follows that $R^1 f_*(G) = 0$ for every abelian group scheme G on T. Now, the Leray–Serre spectral sequence shows that the canonical map $H^1(T, \mu_{p,T}) \to H^1(S, f_*(\mu_{p,T}))$ is bijective. Finally, the Kummer sequence gives $H^1(T, \mu_{p,T}) = R'^{\times}/R'^{\times p}$. □

Let us explicitly compute $H^1(S, \widetilde{\mu}_p)$ in the following special case: Suppose D' is a normal noetherian domain of characteristic $p > 0$ with function field $D' \subset F'$, endowed with a faithful μ_{p-1}-action. We make the assumptions that D' is factorial, and that $(D')^{\times p} = (D')^{\times}$; this holds, for example, for polynomial rings over perfect fields. Let $F \subset F'$ be the field of μ_{p-1}-invariants, and set $S = \operatorname{Spec}(F)$ and $T = \operatorname{Spec}(F')$, such that the projection $f : T \to S$ is a μ_{p-1}-torsor; we denote by $\widetilde{\mu}_p$ the corresponding twisted form of μ_p. Let I be the set of points of codimension one in $\operatorname{Spec}(D')$, or equivalently the set of prime elements in D' up to units. Then $F'^{\times}/D'^{\times}$ is the free abelian group generated by I, and the action of μ_{p-1} on the ring D' induces a permutation action on the set I.

Proposition 1.8. *Assumptions as above. Let $I_{\mathrm{free}} \subset I$ be the subset on which μ_{p-1} acts freely. Then $H^1(S, \widetilde{\mu}_p)$ is an $\mathbb{F}_p$-vector space whose dimension equals the cardinality of the quotient set $I_{\mathrm{free}}/\mu_{p-1}$.*

Proof. By Theorem 1.7, we may view $H^1(S, \widetilde{\mu}_p)$ as the χ-eigenspace of the Galois module $H^1(T, \mu_{p,T})$, where $\chi : \mu_{p-1} \to \mu_{p-1}$ is the tautological character. The factoriality of D' implies that the Galois module $H^1(T, \mu_{p,T}) = F'^{\times}/F'^{\times p}$ is the $\mathbb{F}_p$-vector space with basis I. In other words, we have to compute the χ-eigenspace of $\mathbb{F}_p[I] = \bigoplus_{i \in I} \mathbb{F}_p$. Using the algebra splitting of the group algebra $\mathbb{F}_p[\mu_{p-1}] = \prod_{i=0}^{p-2} \mathbb{F}_p$ into 1-dimensional eigenspaces, we see that each free orbit in I contributes a 1-dimensional subspace to the χ-eigenspace of $\mathbb{F}_p[I]$, whereas each nonfree orbit in I contributes only to eigenspaces for characters $\chi^i \neq \chi$. □

Example 1.9. Let $D' = k[X]$ be the polynomial ring over a perfect field k of characteristic $p > 0$, on which $\zeta \in \mu_{p-1}$ acts via $X \mapsto \zeta X$. Then $F' = k(X)$ and $F = k(X^{p-1})$, such that $\tau = X^{p-1} \in F$ is the twist parameter for the twisted form $\widetilde{\mu}_p$. The set I can be viewed as the set of irreducible polynomials $h \in k[X]$ up to invertible scalars. It is convenient to choose for every such h with $h(0) \neq 0$ a representant with $h(0) = 1$. Such polynomials then factor as

$$h(X) = (1 - \alpha_1 X)(1 - \alpha_2 X) \dots (1 - \alpha_d X)$$

with reciprocal roots $\alpha_1, \dots, \alpha_d \in \Omega$ in some algebraic closure $k \subset \Omega$. The Galois action is then given by $h(\zeta X) = (1 - \zeta\alpha_1 X) \dots (1 - \zeta\alpha_d X)$. It is easy to see that such a polynomial yields a free Galois orbit in I if and only if it is not contained in any of the subrings $k[X^i] \subset k[X]$, where $i > 1$ ranges over the divisors of $d - 1$.

2. Twisted forms of p-torsion in elliptic curves

Let S be a scheme of characteristic $p > 0$, endowed with the fppf-topology. Consider the finite abelian group scheme $G = \mu_p \oplus \mathbb{Z}/p\mathbb{Z}$ over S. It is endowed with the *Weil pairing*

$$\Phi : G \times G \longrightarrow \mu_p, \quad ((\mu, i), (\nu, j)) \longmapsto \mu^j/\nu^i,$$

which is obviously bilinear, alternating, and nondegenerate. We are interested in (G, Φ) because it or its twisted forms naturally occur as the group scheme of p-torsion of ordinary elliptic curves. The goal of this section is to determine the set of isomorphism classes of *twisted forms* $(\widetilde{G}, \widetilde{\Phi})$ of (G, Φ).

This set can be viewed as the set $H^1(S, \mathcal{A})$ of isomorphism classes of $\mathcal{A}$-torsors, where $\mathcal{A} = \underline{\mathrm{Aut}}(G, \Phi)$. Our first task is to compute this sheaf of automorphism groups. Let $U \to S$ be a faithfully flat morphism of finite presentation. Each local endomorphism of $G = \mu_p \oplus \mathbb{Z}/p\mathbb{Z}$ over U can be written as a matrix

$$\begin{pmatrix} \zeta & \nu \\ & \xi \end{pmatrix} \in \Gamma(U, \mathcal{A})$$

with ζ, ξ, ν local sections from $\underline{\mathrm{End}}(\mu_p)$, $\underline{\mathrm{End}}(\mathbb{Z}/p\mathbb{Z})$, $\underline{\mathrm{Hom}}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$, respectively. There is no term below the diagonal because $\underline{\mathrm{Hom}}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = 0$. Using the canonical identifications

$$\underline{\mathbb{Z}/p\mathbb{Z}} = \underline{\mathrm{End}}(\mu_p), \quad \underline{\mathbb{Z}/p\mathbb{Z}} = \underline{\mathrm{End}}(\mathbb{Z}/p\mathbb{Z}), \quad \text{and} \quad \underline{\mathrm{Hom}}(\mathbb{Z}/p\mathbb{Z}, \mu_p) = \mu_p,$$

we may view $\zeta, \xi : U \to \mathbb{Z}/p\mathbb{Z}$ as locally constant functions, and ν is an element from $\Gamma(U, \mathcal{O}_U)$ with $\nu^p = 1$. The action on $G = \mu_p \oplus \mathbb{Z}/p\mathbb{Z}$ is given by

$$\begin{pmatrix} \zeta & \nu \\ & \xi \end{pmatrix} \begin{pmatrix} \mu \\ n \end{pmatrix} = \begin{pmatrix} \mu^\zeta \nu^n \\ \xi n \end{pmatrix}, \tag{6}$$

and the composition law is

$$\begin{pmatrix} \zeta & \nu \\ & \xi \end{pmatrix} \circ \begin{pmatrix} \zeta' & \nu' \\ & \xi' \end{pmatrix} = \begin{pmatrix} \zeta\zeta' & \nu'^\zeta \nu^{\xi'} \\ & \xi\xi' \end{pmatrix}.$$

Obviously, an endomorphism is an automorphism if and only if we have $\zeta, \xi \in (\mathbb{Z}/p\mathbb{Z})^\times = \mu_{p-1}$. A straightforward argument shows that an automorphism respects the Weil pairing Φ if and only if $\zeta\xi = 1$. Summing up, we have

$$\Gamma(U, \mathcal{A}) = \left\{ \begin{pmatrix} \zeta & \nu \\ & \zeta^{-1} \end{pmatrix} \mid \zeta \in \Gamma(U, \mu_{p-1}) \text{ and } \nu \in \Gamma(U, \mu_p) \right\}. \tag{7}$$

We deduce that $\mathcal{A}$ sits inside an extension of groups

$$1 \longrightarrow \mu_p \longrightarrow \mathcal{A} \longrightarrow \mu_{p-1} \longrightarrow 1, \tag{8}$$

where the maps on the left and right are given by

$$\nu \longmapsto \begin{pmatrix} 1 & \nu \\ & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \zeta & \nu \\ & \zeta^{-1} \end{pmatrix} \longmapsto \zeta,$$

respectively. The surjection $\mathcal{A} \to \mu_{p-1}$ has an obvious splitting given by

$$s : \mu_{p-1} \longrightarrow \mathcal{A}, \quad \zeta \longmapsto \begin{pmatrix} \zeta & 1 \\ & \zeta^{-1} \end{pmatrix}.$$

Using this splitting, we may view $\mathcal{A}$ as a semidirect product $\mathcal{A} = \mu_p \rtimes_\phi \mu_{p-1}$, for some homomorphism $\phi : \mu_{p-1} \to \underline{\mathrm{Aut}}(\mu_p)$. The latter is given by $\zeta \mapsto (\mu \mapsto \mu^{\zeta^2})$, which follows from the formula for conjugation

$$\begin{pmatrix} \zeta & \nu \\ & \zeta^{-1} \end{pmatrix} \cdot \begin{pmatrix} \xi & \mu \\ & \xi^{-1} \end{pmatrix} \cdot \begin{pmatrix} \zeta & \nu \\ & \zeta^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} \xi & \mu^{\zeta^2} \nu^{\zeta(\xi^{-1}-\xi)} \\ & \xi^{-1} \end{pmatrix}. \tag{9}$$

Recall that $\underline{\mathrm{Aut}}(\mu_p) = \mu_{p-1}$, such that we may view ϕ as the map $\mu_p \to \mu_p$, $\zeta \mapsto \zeta^2$. Obviously, ϕ is trivial if and only if $p-1$, which is the order of the group μ_{p-1}, divides 2. Hence:

Proposition 2.1. *The sheaf of groups $\mathcal{A}$ is commutative if and only if $p = 2$ or $p = 3$. In this case, we have $H^1(S, \mathcal{A}) = H^1(S, \mu_p) \oplus H^1(S, \mu_{p-1})$.*

For $p = 2$ and $p = 3$ it is thus easy to compute the cohomology group $H^1(S, \mathcal{A})$ with Kummer sequences.

From now on, we assume that $p \geq 5$ and shall apply the theory of nonabelian cohomology to compute the cohomology set $H^1(S, \mathcal{A})$. Care has to be taken because the extension in (8) is noncentral. In any case, we have an exact sequence of pointed sets

$$H^0(S, \mathcal{A}) \longrightarrow H^0(S, \mu_{p-1}) \longrightarrow H^1(S, \mu_p) \longrightarrow H^1(S, \mathcal{A}) \longrightarrow H^1(S, \mu_{p-1}).$$

The outer maps are surjective, because $\mathcal{A} \to \mu_{p-1}$ has a section. In other words:

Proposition 2.2. *The canonical map $H^1(S, \mu_p) \to H^1(S, \mathcal{A})$ is injective, the canonical map $H^1(S, \mathcal{A}) \to H^1(S, \mu_{p-1})$ is surjective, and $H^1(S, \mu_p)$ is the fiber over the class of the trivial torsor in $H^1(S, \mu_{p-1})$.*

To understand the other fibers of the surjection $H^1(S, \mathcal{A}) \to H^1(S, \mu_{p-1})$, it is necessary to twist the groups in (8). Let T be an $\mathcal{A}$-torsor. The sheaf of groups $\mathcal{A}$ acts on itself by conjugation $a \mapsto (x \mapsto axa^{-1})$. Whence we obtain a new sheaf of groups $\widetilde{\mathcal{A}} = T \wedge^{\mathcal{A}} \mathcal{A}$, which is a twisted form of $\mathcal{A}$. The conjugation action leaves $\mu_p \subset \mathcal{A}$ stable, and is trivial on the quotient μ_{p-1}. Hence we obtain a twisted form $\widetilde{\mu}_p$ and an extension of groups

$$1 \longrightarrow \widetilde{\mu}_p \longrightarrow \widetilde{\mathcal{A}} \longrightarrow \mu_{p-1} \longrightarrow 1. \tag{10}$$

It turns out that this extension does not necessarily split. Note that in our situation the notions of schematically split and group-theoretically split coincide:

Proposition 2.3. *If the morphism of schemes $\widetilde{\mathcal{A}} \to \mu_{p-1}$ admits a section, then there is also a section that is a homomorphism of group schemes. In any case, there is at most one section that is a homomorphism.*

Proof. Suppose there is a section of schemes, and choose a generator $\zeta \in \mu_{p-1}$. Let $a \in \widetilde{\mathcal{A}}(S)$ be the image of ζ under the section. Then $a^{p-1} \in \widetilde{\mathcal{A}}(S)$ lies over $1 \in \mu_{p-1}$, in other words, $a^{p-1} \in \widetilde{\mu}_p(S)$. Since p annihilates the group scheme $\widetilde{\mu}_p$, there is some $b \in \widetilde{\mu}_p(S)$ with $b^{1-p} = a^{p-1}$, namely $b = a^{p-1}$. Replacing a by ba we obtain $a^{p-1} = 1$. Whence a defines a section that is also a homomorphism of group schemes.

If a, a' are two sections that are homomorphisms, then a/a' defines a homomorphism of group schemes $\mu_{p-1} \to \widetilde{\mu}_p$. Such homomorphism must be trivial because $p-1$ annihilates the domain of definition and p annihilates the range. The uniqueness statement follows. □

Let $S' \to S$ be the total space of the μ_{p-1}-torsor induced from the $\mathcal{A}$-torsor T via the homomorphism $\mathcal{A} \to \mu_{p-1}$. According to Proposition 2.2, the pullback of T along $S' \to S$ is induced form a unique $\mu_{p,S'}$-torsor, which we call T'.

Proposition 2.4. *The extension of groups in (10) splits if and only if the $\mu_{p,S'}$-torsor T' is trivial.*

Proof. The condition is sufficient: Suppose that T' has a section. Our task is to see that the surjection $\widetilde{\mathcal{A}} \to \mu_{p-1}$ has a section that is a homomorphism of groups. We may check this after replacing S by a finite Galois covering, because if such a section exist, it is unique by Proposition 2.3, and whence descends. Replacing S by the total space S' of the induced μ_{p-1}-torsor, we may assume that the $\mathcal{A}$-torsor T is induced by some $\widetilde{\mu}_p$-torsor T', which is trivial by assumption. Now we are twisting with the trivial $\mathcal{A}$-torsor T, and the resulting group extension is obviously split.

The condition is also necessary: Suppose that T' is nontrivial. Let $\widetilde{f} : \widetilde{\mathcal{A}} \to \mu_{p-1}$ be the canonical projection, and fix a generator $\xi \in \mu_{p-1}$. We shall show that the $\widetilde{\mu}_p$-torsor $\widetilde{f}^{-1}(\xi)$ is nontrivial. Making a base change as in the preceding paragraph, we may assume that the $\mathcal{A}$-torsor T is induced by the nontrivial μ_p-torsor T'. Let $f : \mathcal{A} \to \mu_p$ be the original projection. Then the fiber is $\widetilde{f}^{-1}(\xi) = T' \wedge^{\mu_p} f^{-1}(\xi)$. According to the formula for conjugation (9), the $\nu \in \mu_p$ act on $f^{-1}(\xi)$ via

$$\begin{pmatrix} \xi & \mu \\ & \xi^{-1} \end{pmatrix} \longmapsto \begin{pmatrix} \xi & \mu\nu^n \\ & \xi^{-1} \end{pmatrix},$$

where $n = \xi^{-1} - \xi$ is an element from $\mathbb{Z}/p\mathbb{Z}$. Since $p \geq 5$, we have $n \neq 0$, such that $\nu \mapsto \nu^n$ is an automorphism of μ_p. Set $m = 1/n$, and let T'' be the μ_p-torsor obtained from T' via pulling back along the automorphism $\nu \mapsto \nu^m$. Then $\widetilde{f}^{-1}(\xi)$ is obtained from $f^{-1}(\xi)$ by twisting with the nontrivial μ_p-torsor T'' with respect to the multiplication action of μ_p on $f^{-1}(\xi) \simeq \mu_p$. Consequently, $f^{-1}(\xi) \simeq T''$ does not admit a section over S. □

The preceding proof actually gives the following information:

Proposition 2.5. *Suppose S is connected, and that the $\mu_{p,S'}$-torsor T' is nontrivial. Then the image of $H^0(S, \widetilde{\mathcal{A}}) \to H^0(S, \mu_{p-1})$ is the subgroup $\{\pm 1\}$.*

Proof. The condition that the fiber $\widetilde{f}^{-1}(\xi) \subset \widetilde{\mathcal{A}}$, $\xi \in \mu_{p-1}$ admits a section is equivalent to the vanishing of $n = \xi^{-1} - \xi$, that is, $\xi = \pm 1$. □

We now have everything to compute the set of isomorphism classes of $\mathcal{A}$-torsors: Fix an $\mathcal{A}$-torsor T, and consider the exact sequence (10) obtained by twisting with T with respect to the conjugation action. According to [5], Section 5.6, we have:

Theorem 2.6. *The pointed set of isomorphism classes of $\mathcal{A}$-torsors in $H^1(S, \mathcal{A})$ with the same image in $H^1(S, \mu_{p-1})$ as T is in canonical bijection to the group $H^1(S, \widetilde{\mu}_p)$ modulo the permutation action of $H^0(S, \mu_{p-1})$ coming from the twisted extension $1 \to \widetilde{\mu}_p \to \widetilde{\mathcal{A}} \to \mu_{p-1} \to 1$.*

Remark 2.7. The permutation action of the subgroup $\{\pm 1\} \subset H^0(S, \mu_{p-1})$ on $H^1(S, \widetilde{\mu}_p)$ is trivial. This follows from [5], Proposition 5.4.1, because its conjugation action on $\widetilde{\mu}_p$ is trivial, and its image in $H^1(S, \widetilde{\mu}_p)$ under the coboundary map is trivial.

3. The extension class

Let K be a field of characteristic $p > 0$ and E_K an elliptic curve over K. In order to decide when E_K has a *rational p-division point*, that is, a K-rational point of order p, we shall analyze the multiplication-by-p map. We recall that the *Frobenius pullback* $E_K^{(p)}$ is defined by the cartesian diagram

$$\begin{array}{ccc} E_K^{(p)} & \longrightarrow & E_K \\ \downarrow & & \downarrow \\ \operatorname{Spec}(K) & \xrightarrow[F]{} & \operatorname{Spec}(K). \end{array}$$

We obtain a factorization

$$\begin{array}{ccccc} E_K & & \xrightarrow{\quad p \quad} & & E_K \\ & \searrow^{F} & & \nearrow_{V} & \\ & & E_K^{(p)} & & \end{array}$$

of the multiplication-by-p into the relative Frobenius followed by the *Verschiebung*. The kernels $\ker(F)$ and $\ker(V)$ are finite and flat group schemes of order p over K, where $\ker(F)$ is infinitesimal. We recall that E_K is *ordinary* if $\ker(V)$ is étale, that is, a twisted form of $\mathbb{Z}/p\mathbb{Z}$. In any case, the kernel $E_K[p]$ of the multiplication-by-p map sits inside a short exact sequence

$$1 \longrightarrow \ker(F) \longrightarrow E_K[p] \longrightarrow \ker(V) \longrightarrow 1, \tag{11}$$

and we conclude from this discussion:

Proposition 3.1. *There exists a rational p-division point on E_K if and only if the following two conditions are satisfied:*

(i) *the group scheme* $\ker(V)$ *is isomorphic to* $\mathbb{Z}/p\mathbb{Z}$*, and*
(ii) *the extension (11) splits.*

As explained in [10], Section 2.8 there exists a canonical pairing between the kernel of an isogeny and the kernel of its dual isogeny. This implies that $E_K[p]$ isomorphic to its own Cartier dual and hence $\ker(F)$ is the Cartier dual of $\ker(V)$. In particular, $\ker(V)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ if and only if $\ker(F)$ is isomorphic to μ_p.

We recall from [10], Section 12.4 that the *Hasse invariant* h of E_K is defined as the induced linear mapping on Lie algebras

$$h = \operatorname{Lie}(V) : \operatorname{Lie}(E_K^{(p)}) \to \operatorname{Lie}(E_K).$$

Using the identification $\operatorname{Lie}(E_K^{(p)}) = \operatorname{Lie}(E_K)^{\otimes p}$, we may regard the Hasse invariant as an element in the one-dimensional K-vector space $\operatorname{Lie}(E)^{\otimes(1-p)}$. From this we derive more explicit invariants: Choose a basis $u \in \operatorname{Lie}(E_K)$, such that $h = \lambda u^{\otimes(1-p)}$ for some scalar $\lambda \in K$, which is unique up to $(p-1)$.st powers.

The Hasse invariant determines the p-Lie algebra $\mathfrak{g} = \operatorname{Lie}(E_K) = Ku$ up to isomorphism via $u^{[p]} = \lambda u$, and consequently $\ker(F) = \operatorname{Spec}(U^{[p]}(\mathfrak{g})^\vee)$. Clearly, E_K is ordinary if and only if $\lambda \neq 0$. In turn, the Cartier dual is given as a scheme by

$$\ker(V) = \underline{\operatorname{Hom}}(\ker(F), \mathbb{G}_m) = \operatorname{Spec} k[u]/(u^p - \lambda u).$$

Applying Proposition 1.1 we conclude

Proposition 3.2. *If $\lambda \neq 0$, then $\ker(F)$ is the twisted form of μ_p corresponding to the twist parameter $\lambda^{-1} \in K$. In particular, the group scheme $\ker(V)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ if and only if λ lies in $K^{\times(p-1)}$.*

Proposition 3.3. *Let E_K be an ordinary elliptic curve over K. Then the following are equivalent:*

(i) *$j(E_K) \in K^p$,*
(ii) *there exists an elliptic curve X_K over K, so that $X_K^{(p)} \simeq E_K$, and*
(iii) *the extension (11) splits.*

For supersingular elliptic curves (i) and (ii) are always true, whereas (iii) never holds.

Proof. Let E_K be ordinary. To prove $(i) \Rightarrow (iii)$, choose an elliptic curve Y_K over K with $j(Y_K)^p = j(E_K)$. The separable isogeny $V : Y_K^{(p)} \to Y_K$ shows that the extension (11) splits for $Y_K^{(p)}$ and the splitting is given by the subgroup scheme $G = \ker(V)$. To proceed, note that E_K is a twisted form of $Y_K^{(p)}$. In order to establish existence of an étale subgroup scheme of $E_K[p]$ it thus suffices to check that G is invariant under the automorphism group scheme of $Y_K^{(p)}$. To check the latter, we may assume that K is algebraically closed. Now the invariance is clear because the automorphism group scheme is reduced and G is the reduction of the p-torsion subgroup scheme.

To prove $(iii) \Rightarrow (ii)$, let $G_K \subset E_K[p]$ be the subgroup scheme defining the splitting of (11), and set $X_K = E_K/G_K$. Consider the following commutative diagram

$$\begin{array}{ccc} E_K & \xrightarrow{\times p} & E_K \\ {\scriptstyle \mathrm{pr}}\downarrow & \nearrow & \uparrow \\ X_K & \xrightarrow{F} & X_K^{(p)} \end{array}$$

The diagonal dotted arrow exists because $G_K \subset E_K[p]$ and the vertical dotted arrow exists because $X_K \to E_K$ is purely inseparable. Then $X_K(p) \to E_K$ has degree one, hence is an isomorphism. The implication $(ii) \Rightarrow (i)$ is trivial.

Now let E_K be supersingular. Then (11) never splits because otherwise the embedding dimension of $E_K[p]$ would be too large. As explained in the proof of [10], Theorem 12.4.3, the multiplication by p-map induces a canonical isomorphism $E_K \simeq E_K^{(p^2)}$ from which (i) and (ii) follow immediately. □

We have seen that $E_K[p]$ is a twisted form of $G = \mu_p \oplus (\mathbb{Z}/p\mathbb{Z})$ over $S = \operatorname{Spec} K$ that respects the Weil pairing Φ. As explained in Section 2, $E_K[p]$ defines an $\mathcal{A} = \underline{\mathrm{Aut}}(G, \Phi)$-torsor. By Proposition 2.2 there is a surjective homomorphism of pointed sets

$$H^1(S, \mathcal{A}) \longrightarrow H^1(S, \mu_{p-1}) \longrightarrow 1$$

mapping the class of $E_K[p]$ to the class of $\ker(F)$. This latter cohomology group and the class of $\ker(F)$ have been analyzed in Section 1 and their relation to the Hasse invariant is described in Proposition 3.2. To determine the fiber over the class of $\ker(F)$ we proceed as in Section 2 and consider the $\mathcal{A}$-torsor $T = \ker F \oplus \underline{\mathrm{Hom}}(\ker(F), \mathbb{G}_m)$. The twisted form $\widetilde{\mathcal{A}} = T \wedge^{\mathcal{A}} \mathcal{A}$ of $\mathcal{A}$ is an extension of μ_{p-1} by a

twisted form $\widetilde{\mu}_p$ of μ_p as in (10). For this specific choice of $\widetilde{\mathcal{A}}$ the general machinery developed in Section 2 simplifies:

Theorem 3.4. *The pointed set of isomorphism classes of $\mathcal{A}$-torsors with image $\ker(F)$ in $H^1(S,\mu_{p-1})$ is in bijection with $H^1(S,\widetilde{\mu}_p)$. Moreover we have canonical isomorphisms of groups*

$$H^1(S,\widetilde{\mu}_p) \simeq H^1(S,\underline{\mathrm{Hom}}(\ker V,\ker F)) \simeq \mathrm{Ext}^1(\ker V,\ker F),$$

identifying this pointed set with the group of twisted splittings of (11), as well as the group classifying all extensions of $\ker(V)$ by $\ker(F)$.

Proof. Let $S' \to S$ be the total space of the μ_{p-1}-torsor induced from the $\mathcal{A}$-torsor T via the homomorphism $\mathcal{A} \to \mu_{p-1}$ as in Section 2. The pullback of T along $S' \to S$ yields $\mu_{p,S'} \oplus (\mathbb{Z}/p\mathbb{Z})_{S'}$, which is induced from the trivial $\mu_{p,S'}$-torsor. By Proposition 2.4 the sequence (10) for $\widetilde{\mathcal{A}}$ is split. In particular, the map from $H^1(S,\widetilde{\mu}_p)$ to $H^1(S,\widetilde{\mathcal{A}})$ is injective.

By construction, we have $\widetilde{\mu}_p = \underline{\mathrm{Hom}}(\ker V,\ker F)$, so that $H^1(S,\widetilde{\mu}_p)$ classifies twists of splittings of (11). The identification of the group of twisted splittings with the group of all extensions follows from the discussion in [2], Chapter III, §6.3.5 and [2], Chapter III, §6, Corollaire 4.9. □

We stress that this result is due to the specific choice of the $\mathcal{A}$-torsor T. In this case, the distinguished element of $H^1(S,\widetilde{\mathcal{A}})$ corresponds to the split extension of $\ker(F)$ by $\ker(V)$. In particular, the class of $E_K[p]$ in $H^1(S,\widetilde{\mathcal{A}})$ equals this distinguished element if and only if $j(E_K) \in K^p$ thanks to Proposition 3.3. Moreover, in the proof we have seen that if $f : S' \to S$ trivializes the μ_{p-1}-torsor $\ker(F)$ then $\widetilde{\mu}_p$ becomes isomorphic to μ_p. Hence we obtain $\widetilde{\mu}_p$ as a subgroup scheme of the Weil restriction $f_*(\mu_{p,S'})$ and Theorem 1.7 applies.

4. Néron models and sections of order p

Throughout, we shall work in the following set-up: Let R be a henselian discrete valuation ring of characteristic $p > 0$, whose residue field $k = R/\mathfrak{m}_R$ is algebraically closed, with field of fraction $R \subset K$. Let us also fix a uniformizer $t \in R$. Given an elliptic curve E_K over K, we denote by $E \to \mathrm{Spec}(R)$ its *Néron model*, and by $E_k \subset E$ the closed fiber. Let $\Phi_k = E_k/E_k^0$ be the group of connected components of the closed fiber E_k. Note that if E_K has additive reduction, then the possible orders for Φ_k are $1, 2, 3, 4$. We refer to [1] as general reference for the theory of Néron models.

Suppose there is a rational p-division point $z \in E_K$. Let $G_K \subset E_K$ be the subgroup scheme generated by z, and consider its schematic closure $G \subset E$.

Lemma 4.1. *The subscheme $G \subset E$ is a subgroup scheme, and the structure morphism $G \to \mathrm{Spec}(R)$ is flat and finite of degree p.*

Proof. Clearly, G is reduced and the structure morphism $G \to \mathrm{Spec}(R)$ is flat. The Néron mapping property yields a morphism of group schemes $\varphi : (\mathbb{Z}/p\mathbb{Z}) \to E$ with $1_K \mapsto z$. Hence G is the schematic image of φ, whence finite because $E \to \mathrm{Spec}(R)$ is separated. Its degree must be p, because the generic fiber has length p.

To see that $G \subset E$ is a subgroup scheme, it suffices to check that the multiplication map $\mu : G \times G \to E$ factors through $G \subset E$, according to [19]. Since $G \times G \to \mathrm{Spec}(R)$ is flat and finite, the inclusion $G_K \times G_K \subset G \times G$ is dense. Since

$E \to \mathrm{Spec}(R)$ is separated, the multiplication map $\mu : G \times G \to E$ is finite, and in particular closed. Whence

$$\mu(G \times G) = \mu(\overline{G_K \times G_K}) = \overline{\mu(G_K \times G_K)} = \overline{G_K} = G,$$

such that μ factors through $G \subset E$ set-theoretically. Using that $G \times G$ is reduced, we conclude that the schematic image $\mu(G \times G) \subset E$ is reduced as well, and infer that μ factors through $G \subset E$ scheme-theoretically. □

In the preceding situation, it is convenient to consider the Cartier dual $H = \underline{\mathrm{Hom}}(G, \mathbb{G}_m)$, which is actually easier to describe than G. Note that the group scheme $H \to \mathrm{Spec}(R)$ is finite flat of degree p, and recall that $t \in R$ denotes a uniformizer.

Proposition 4.2. *Both fibers of $H \to \mathrm{Spec}(R)$ are infinitesimal group schemes. If G_k is connected, then $G_k \simeq H_k \simeq \alpha_p$. Moreover, the Lie algebra $\mathfrak{h} = \mathrm{Lie}(H)$ is a free R-module of rank one, and admits a basis $b \in \mathfrak{h}$ satisfying $b^{[p]} = t^n b$ for some integer $n \geq 0$.*

Proof. By construction, the generic fiber is $H_K = \mu_{p,K}$. Since $H_K \subset H$ is dense, it follows that the closed fiber H_k is connected. Over the algebraically closed field k, there are only two connected group schemes of length p, namely α_p and μ_p. Only the former has a connected Cartier dual. So if G_k is connected, we must have $H_k \simeq \alpha_{p,k}$.

The Lie algebra $\mathfrak{h}$ is a free module of rank one, because the fibers of $H \to \mathrm{Spec}(R)$ are infinitesimal of length p. Choose an arbitrary basis $b \in \mathfrak{h}$. Then $b^{[p]} = fb$ for some $f \in R$, which is nonzero because $H_K = \mu_{p,K}$. Write $f = t^n g$ for some unit $g \in R$. Since R is strictly henselian, there exists an $h \in R$ with $h^{p-1} = g$. Replacing b by $h^{-1}b$, we find the desired basis. □

Now back to our elliptic curve E_K and its Néron model $E \to \mathrm{Spec}(R)$. If $K \subset K'$ is a finite field extension, we denote by $R' \subset K'$ the integral closure of $R \subset K'$. Then R' is a henselian discrete valuation ring with field of fraction $R' \subset K'$ and algebraically closed residue field $k = R/\mathfrak{m}_R = R'/\mathfrak{m}_{R'}$. We shall denote by $E_{K'} = E_K \otimes_K K'$ the induced elliptic curve over K', and by $E' \to \mathrm{Spec}(R')$ its Néron model. Note that the canonical map $E \otimes_R R' \to E'$ coming from the Néron mapping property is, in general, not an isomorphism.

The preceding Proposition yields a first restriction on Néron models in presence of rational p-division points:

Theorem 4.3. *Let E_K be an elliptic curve over K. Suppose the Frobenius pullback $E_K^{(p)}$ contains a rational p-division point whose class in Φ_k is zero, and that E_K has additive reduction. Then E_K has potentially supersingular reduction.*

Proof. For characteristic $p \neq 2$, this easily follows from the representability of the Igusa moduli problem. The following argument works in general: Replacing E_K by $E_K^{(p)}$, we may assume that the rational p-division point already lies on E_K. Choose a finite field extension $K \subset K'$ over which $E_{K'}$ acquires semistable reduction. The Néron mapping property yields a morphism $f : E \otimes_R R' \to E'$, which is the identity over K'. Since all homomorphisms from $\mathbb{G}_a$ into $\mathbb{G}_m$ or elliptic curves are zero, f maps the connected component of the closed fiber of $E \otimes_R R'$ to the origin.

Fix a rational p-division point $z \in E_K$ and let $S_z \subset E$ be its closure. Then the schematic image $f(S_z \otimes_R R') \subset E'$ is a section inducing a point of order p

over K' and passing through the origin of the closed fiber. Let $G' \subset E'$ be the closed subscheme generated by this section. Its generic fiber is cyclic of order p, whereas the closed fiber is connected. According to Proposition 4.2, the closed fiber is isomorphic to α_p. Now suppose that E_K has either potentially ordinary or potentially multiplicative reduction. Then the connected component of the origin in E'_k would be an ordinary elliptic curve or $\mathbb{G}_m$. But these group schemes do not contain α_p, a contradiction. □

Remark 4.4. If a rational p-division point has non-zero specialization into Φ_k, then p divides the order of Φ_k. In case of additive reduction Φ_k is of order at most 4. In particular, the assumption of the theorem on Φ_k is automatically fulfilled for $p \geq 5$.

Using information from tables of reduction types (for example in [21], Chapter IV, §9), we obtain the following more specific consequences:

Corollary 4.5. *Let E_K be an elliptic curve over K. Suppose that $E_K^{(p)}$ contains a rational p-division point, and that $p \geq 3$. Then the reduction type of E_K is not I_l^* with $l \geq 1$.*

Proof. If the reduction type is I_l^* with $l \geq 1$, then the j-invariant of E_K is not contained in R. Consequently E_K has potentially multiplicative reduction, in contradiction to Theorem 4.3. □

Corollary 4.6. *Let E_K be an elliptic curve over K. Suppose that $E_K^{(p)}$ contains a rational p-division point. If $p \geq 5$ and if the reduction type is* II, IV, IV* *or* II*, *then we have $p \equiv -1$ modulo 3. If $p \geq 3$ and if the reduction type is* III *or* III*, *then $p \equiv -1$ modulo 4.*

Proof. Let $j_k \in R/\mathfrak{m}_R$ be the residue class of the j-invariant of E_K, which must be a supersingular j-value by Theorem 4.3. If the reduction type is III or III*, then $j_k = 1728$ by the tables of reduction type. According to [20], Chapter V, Example 4.5 this j-value is supersingular if and only if $p \equiv -1$ modulo 4. If the reduction type is II, IV, IV* or II*, then $j_k = 0$, and this is supersingular if and only if $p \equiv -1$ modulo 3, according to loc. cit. Example 4.4. □

Corollary 4.7. *Let E_K be an elliptic curve over K. Suppose that $E_K^{(p)}$ contains a rational p-division point, that E_K has additive reduction, and that $p \equiv 1$ modulo 12. Then E_K has reduction type I_0^*.*

Proof. In light of Corollary 4.5 and Corollary 4.6, the only remaining possibility for an additive reduction type is I_0^*. □

5. Osculation numbers and Hasse invariant

Let E_K be an elliptic curve and $E \to \mathrm{Spec}(R)$ be its Néron model, say given by a minimal Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. The group $E(K)$ comes along with a *decreasing filtration* defined as follows [22]: The subgroup $E_1(K) \subset E(K)$ comprises those $z \in E$ with vanishing specialization in E_k. The coordinates of such points $z = (\lambda, \mu)$ have valuations $\nu(\lambda) = -2m$ and $\nu(\mu) = -3m$, and one defines

$$E_m(K) = \{z \in E_1(K) \mid z = 0 \text{ or } \nu(\lambda) \leq -2m\}\,.$$

Let us check that this is independent of the chosen Weierstrass equation: Given a rational point $z \in E_K$, we write $S_z = \overline{\{z\}}$ for its closure in E. For each nonzero $z \in E_1(K)$, the scheme $S_z \cap S_0$ is a local Artin scheme, and it is convenient to call its length the *osculation number* of $z \in E_0(K)$.

Lemma 5.1. *The point $z \in E_1(K)$ has osculation number m if and only if $z \in E_m(K) - E_{m+1}(K)$.*

Proof. Suppose $z = (\lambda, \mu)$ has osculation number m and $\nu(\lambda) = -2n$. By [22], Theorem 4.2, the fraction $-x/y$, viewed as a variable, yields a uniformizer along the zero section for E. The intersection scheme $S_z \cap S_0$ has length m, and is defined by $R[z]/(z, z - \lambda/\mu)$, which has length $\nu(\lambda/\mu) = n$. We conclude $n = m$, and the result follows. □

Now we are interested in the osculation number for rational p-division points. It turns out that this is closely related to the Hasse invariant. Suppose for simplicity that E_K has good reduction and consider the factorization of the multiplication-by-p morphism of Néron models

$$\begin{array}{ccc} E & \xrightarrow{\;p\;} & E \\ & {\scriptstyle F}\searrow \quad \nearrow{\scriptstyle V} & \\ & E^{(p)} & \end{array}$$

As in Section 3, the *Hasse invariant* h of E is defined as the induced linear mapping on Lie algebras

$$h = \mathrm{Lie}(V) : \mathrm{Lie}(E^{(p)}) \to \mathrm{Lie}(E).$$

Using the identification $\mathrm{Lie}(E^{(p)}) = \mathrm{Lie}(E)^{\otimes p}$, we may regard the Hasse invariant as an element in the invertible R-module $\mathrm{Lie}(E)^{\otimes(1-p)}$. From this we derive more explicit invariants: Choose a basis $u \in \mathrm{Lie}(E)$, such that $h = \omega u^{\otimes(1-p)}$ for some scalar $\omega \in R$. Then the *vanishing order* $\nu(h) = \nu(\omega) \geq 0$ and the *residue class* $[h] = [\omega] \in R/R^{\times(p-1)}$ do not depend on the choice of the basis.

The Hasse invariant determines the p-Lie algebra $\mathfrak{g} = \mathrm{Lie}(E) = Ru$ up to isomorphism via $u^{[p]} = \omega u$, and consequently $\ker(F) = \mathrm{Spec}(U^{[p]}(\mathfrak{g})^\vee)$. It turn, the Cartier dual is given as a scheme by

$$\ker(V) = \underline{\mathrm{Hom}}(\ker(F), \mathbb{G}_m) = \mathrm{Spec}\, k[u]/(u^p - \omega u).$$

This leads to the following observation:

Proposition 5.2. *Suppose that E_K has good reduction and that the Hasse invariant of E has vanishing order $\nu(h) = p - 1$. Then the Frobenius pullback contains a rational p-division point $z \in E_K^{(p)}$ with osculation number one. Its coordinates $z = (\lambda, \mu)$ in the Weierstrass model have valuations $\nu(\lambda) = -2$ and $\nu(\mu) = -3$.*

Proof. Since R is strictly henselian, we may represent the Hasse invariant h by the scalar $\omega = t^{p-1}$ for some uniformizer $t \in R$. Clearly, $z \in \ker(V)$, and we just saw $\ker(V) = \mathrm{Spec}\, k[u]/(u^p - t^{p-1}u)$. Now the decomposition

$$u^p - t^{p-1}u = u \prod_{\zeta \in \mu_{p-1}(R)} (u - \zeta t)$$

shows that the intersection $S_z \cap S_0$ has length one, and the statement follows from Lemma 5.1. □

Remark 5.3. There is actually an explicit formula, of a somewhat implicit nature, for the x-coordinate of p-division points discovered by Gunji [8].

6. Reduction types under quadratic twists

In this section we shall analyze the behavior of reduction types under quadratic twists. Let E_K be an elliptic curve over K, and $W \to \mathrm{Spec}(R)$ be its Weierstrass model, that is, the relative cubic defined by a minimal Weierstrass equation. Choose a separable quadratic field extension $K \subset K'$, and let $R \subset R'$ be the corresponding extension of discrete valuation rings. Then the group $\{\pm 1\}$ acts on W via the sign involution, and on R' via the Galois involution. Now consider the diagonal action on the product

$$W' = W \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R') = W \otimes_R R',$$

and let $Y = W'/\{\pm 1\}$ be the quotient, which exists as a scheme because W' carries an ample invertible sheaf. All our actions are via R-morphisms, so Y is an R-scheme. The scheme Y is normal, the morphism $Y \to \mathrm{Spec}(R)$ is proper, and the canonical map $R \to H^0(Y, \mathcal{O}_Y)$ is bijective.

Taking quotients commutes with passing to invariant open subsets, so $Y_K = E_{K'}/\{\pm 1\}$ is nothing but the *quadratic twist* of E_K with respect to the field extension $K \subset K'$. More abstractly, $Y_K = \mathrm{Spec}(K') \wedge^{\{\pm 1\}} E_K$, where we view $\mathrm{Spec}(K')$ as a $\{\pm 1\}$-torsor. To emphasize this aspect, we write $\widetilde{E}_K = Y_K$ for this elliptic curve. Note that $K \subset K'$ is unique up to isomorphism if $p \neq 2$, because R is assumed to be strictly henselian.

Proposition 6.1. *If E_K has good reduction and $p \neq 2$, then the quadratic twist $\widetilde{E}_K$ has reduction type I_0^*.*

Proof. First note that the Weierstrass model coincides with the Néron model E, which is a relative elliptic curve. The fixed schemes for the action on E and $\mathrm{Spec}(R)$ are given by the 2-torsion scheme and the closed point, respectively. Whence the fixed points on $E' = E \otimes_R R'$ are the 2-torsion points in the closed fiber E'_k. If $p \neq 2$, then there are four such fixed points, whose images on Y are four rational double points of type A_1, which comprise $\mathrm{Sing}(Y)$. Let $X \to Y$ be the minimal resolution of singularities. Since Y is Gorenstein and Y_k is irreducible, the relative canonical class $K_{X/R}$ is trivial. It follows that X is the regular model of $\widetilde{E}_K$. The closed fiber Y_k has multiplicity two, because it is birational to the quotient of the double curve $E \otimes_R (R'/tR')$. We infer that $\widetilde{E}_K$ has reduction type I_0^*. □

It is not difficult to determine the behavior under twists for arbitrary reduction types without geometry, by merely using Weierstrass equations and Ogg's Formula, at least if $p \neq 2, 3$, which we assume for the rest of this section. Then, Ogg's formula [21], Chapter IV, Formula 11.1 tells us that

$$\nu(\Delta) = \varepsilon + (m - 1),$$

where $\nu(\Delta)$ is the valuation of a minimal discriminant, m denotes the number of irreducible components of the closed fiber of E and ε is equal to $0, 1, 2$, depending on whether E_K has good, multiplicative or additive reduction.

Proposition 6.2. *For $p \geq 5$ the reduction types of E_K and its quadratic twists $\widetilde{E}_K$ are related as in the following table:*

E_K	I_m	II	III	IV	IV^*	III^*	II^*	I_m^*
$\widetilde{E}_K$	I_m^*	IV^*	III^*	II^*	II	III	IV	I_m

Proof. Choose a minimal Weierstrass equation

$$y^2 = x^3 + a_4 x + a_6 \tag{12}$$

for E_K with coefficients $a_4, a_6 \in R$. According to [20], Chapter X, §6, Proposition 5.4, the quadratic twist $\widetilde{E}_K$ has Weierstrass equation

$$y^2 = x^3 + t^2 a_4 x + t^3 a_6, \tag{13}$$

whose discriminant is $t^6\Delta$. Let $j \in K$ be the j-invariant of E_K. We first consider the case $\nu(j) \geq 0$. Suppose that $\nu(\Delta) = 0, 2, 3, 4$, such that the reduction type of E_K is I_0, II, III, IV, respectively. Then the Weierstrass equation (13) is minimal, and Ogg's Formula implies that the reduction type of the quadratic twist $\widetilde{E}_K$ is I_0^*, IV^*, III^*, II^*. Now suppose that $\nu(\Delta) = 6, 8, 9, 10$, such that E_K has reduction type I_0^*, IV^*, III^*, II^*, respectively. According to Lemma 6.5, the change of coefficients $x = t^2 x'$ and $y = t^3 y'$ yields another integral Weierstrass equation

$$y^2 = x^3 + t^{-2} a_4 x + t^{-3} a_6, \tag{14}$$

which has discriminant $\widetilde{\Delta} = t^{-6}\Delta$, and is therefore minimal. Ogg's Formula implies that the quadratic twist has reduction type I_0, II, III, IV, respectively.

It remains to treat the case $\nu(j) < 0$. Suppose that E_K has reduction type I_m, $m \geq 1$. Then $\nu(j) = -m$, and $a_4, a_6 \in R$ are invertible, by the table after [1], Chapter 1, Section 1.5, Lemma 4. It follows from the Tate algorithm ([22], see also [21], Chapter 4, Section 9) that the Weierstrass equation (13) is minimal and has reduction of type I_l^* for some $l \geq 0$. Then, Ogg's formula yields $l = m$. Conversely, if E_K has reduction type I_m^*, then the Weierstrass equation (14) is minimal, with invertible coefficients, and the quadratic twist has reduction type I_m. □

If $j(E_K) = 0$, then the automorphism scheme of E_K is isomorphic to μ_6, and we may also perform a *sextic twist* with respect to the generator

$$u \in H^1(K, \mu_6) = K^\times / K^{\times 6}.$$

If E_K has Weierstrass equation $y^2 = x^3 + a_6$, then the sextic twist is given by the Weierstrass equation $y^2 = x^3 + ua_6$, by [20], Chapter X, §6, Proposition 5.4. Using u^2 instead of the generator $u \in H^1(K, \mu_6)$, we obtain the *cubic twist*, which is given by the Weierstrass equation $y^2 = x^3 + u^2 a_6$.

Proposition 6.3. *Suppose that $j(E_K) = 0$ and $p \geq 5$. Then the reduction types of E_K and its cubic and sextic twists are related as in the following table:*

E_K	I_0	II	IV	I_0^*	IV^*	II^*
cubic twist	IV	I_0^*	IV^*	II^*	I_0	II
sextic twist	II	IV	I_0^*	IV^*	II^*	I_0

If $j(E_K) = 1728$, then the automorphism scheme of E_K is isomorphic to μ_4, and we may also perform a *quartic twist* with respect to the generator

$$u \in H^1(K, \mu_4) = K^\times / K^{\times 4}.$$

If E_K has Weierstrass equation $y^2 = x^3 + a_4 x$, then the quartic twist is given by the Weierstrass equation $y^2 = x^3 + ua_4 x$, by [20], Chapter X, §6, Proposition 5.4.

Proposition 6.4. *Suppose that $j(E_K) = 1728$ and $p \geq 5$. Then the reduction types of E_K and its quartic twist are related as in the following table:*

E_K	I_0	III	I_0^*	III^*
quartic twist	III	I_0^*	III^*	I_0

The proofs for the preceding two propositions are as for Proposition 6.2; we leave the actual computations to the reader. In the proof of Proposition 6.2, we have used the following fact:

Lemma 6.5. *Suppose $y^2 = x^3 + a_4x + a_6$ is a minimal Weierstrass equation. If $\nu(\Delta) \geq 6$, then $\nu(a_4) \geq 2$ and $\nu(a_6) \geq 3$.*

Proof. Using the formulas $\Delta = -16(4a_4^3 + 27a_6^2)$ and $j = 1728(4a_4)^3/\Delta$ for the discriminant and j-invariant, together with Ogg's Formula, one obtains the following table, which gives $\nu(\Delta)$ and the reduction type in dependence on the valuations of $a_4, a_6 \in R$:

$\nu(a_4)$	0	0	≥ 1	1	≥ 1	≥ 2
$\nu(a_6)$	0	≥ 1	0	≥ 2	1	2
$\nu(\Delta)$	$-n$	0	0	3	2	4
reduction type	I_n	I_0	I_0	III	II	IV

The statement follows from this table. □

7. Reduction type under Frobenius pullback

Let E_K be an elliptic curve over K, and consider its Frobenius pullback $E_K^{(p)}$. In this section we describe the reduction type of the Frobenius pullback in terms of the reduction type of the original elliptic curve. Since an additive reduction type changes to a semistable reduction type only after a nontrivial Galois extension by [17], Corollary 3 to Theorem 2, the following fact holds:

Lemma 7.1. *The Frobenius pullback $E_K^{(p)}$ has semistable reduction if and only if E_K has semistable reduction.*

Let $j \in K$ be the j-invariant of E, such that $j^p \in K$ is the j-invariant of the Frobenius pullback.

Proposition 7.2. *If E_K has reduction type I_m for some $m \geq 0$, then the Frobenius pullback $E_K^{(p)}$ has reduction type I_{pm}.*

Proof. We have $\nu(j) = -m$ and $\nu(j^p) = -pm$. Using Lemma 7.1 we infer that the Frobenius pullback has reduction type I_{pm}. □

Proposition 7.3. *If E_K has reduction type I_m^* for some $m \geq 0$ and $p \geq 3$, then the Frobenius pullback $E_K^{(p)}$ has reduction type I_{pm}^*.*

Proof. It is easy to see that quadratic twists commute with Frobenius pullbacks. So for $p \geq 5$ the statement follows from Proposition 6.2 and Proposition 7.2. Also, if $m \geq 1$, we can argue for all $p \geq 3$ as follows: then $\nu(j) = -m$ and $\nu(j^p) = -pm$, and we infer that the Frobenius pullback has reduction type I_{pm}^*. It remains to treat the case $p = 3$ and $m = 0$. Then $\nu(\Delta) = 6$ and the Tate algorithm reveals that a minimal Weierstrass equation exists with $\nu(a_1) \geq 1$, $\nu(a_2) \geq 1$, $\nu(a_3) \geq 2$, $\nu(a_4) \geq 2$ and $\nu(a_6) \geq 3$. Obviously, this equation is no longer minimal after

Frobenius pullback and we infer that the discriminant of a minimal Weierstrass equation has $\nu(\Delta^{(p)}) = 3 \cdot 6 - 12 = 6$. From [21], Chapter IV, §9, Table 4.1. we get the reduction type I_0^*. □

As we shall see in Section 14, this does not hold true in characteristic two.

Proposition 7.4. *Suppose $p \geq 5$. Then the reduction type of E_K is related to the reduction type of its Frobenius pullback as described the following table, according to the congruence class of p modulo 12:*

E_K	I_m	I_m^*	II	III	IV	IV*	III*	II*
$E_K^{(p)}$ for $p \equiv 1$	I_{pm}	I_{pm}^*	II	III	IV	IV*	III*	II*
$E_K^{(p)}$ for $p \equiv 5$	I_{pm}	I_{pm}^*	II*	III	IV*	IV	III*	II
$E_K^{(p)}$ for $p \equiv 7$	I_{pm}	I_{pm}^*	II	III*	IV	IV*	III	II*
$E_K^{(p)}$ for $p \equiv 11$	I_{pm}	I_{pm}^*	II*	III*	IV*	IV	III	II

Proof. We already verified the first two columns of the table. Suppose now that E_K has reduction type of the form $\mathrm{II}, \mathrm{III}, \ldots, \mathrm{II}^*$. Then the reduction type is entirely determined by $1 \leq \nu(\Delta) \leq 11$ via Ogg's Formula, and we have $\nu(\Delta^{(p)}) \equiv p\nu(\Delta)$ modulo 12 by Tate's Algorithm. Reducing modulo 3 and 4, we see that the possible congruence classes for the prime p are $1, 5, 7, 11$. A direct computation now yields the entries of the table. □

Remark 7.5. Let $T \in \{\mathrm{II}, \mathrm{III}, \mathrm{IV}\}$ be a Kodaira symbol. The change on the Kodaira symbols in passing from E_K to $E_K^{(p)}$ is not difficult to remember: If $p \equiv 1$ modulo 12, nothing changes. If $p \equiv -1$, then $T \leftrightarrow T^*$. If $p \equiv 5$ then $T \leftrightarrow T^*$ for the "even" Kodaira symbols, and nothing else changes. If $p \equiv -5$, then $T \leftrightarrow T^*$ for the "odd" Kodaira symbols, and nothing else changes.

8. p-torsion under quadratic twists

We keep the notation as in the preceding section. Let E_K be an elliptic curve over K. Choose a separable quadratic field extension $K \subset K'$ and let $\widetilde{E}_K$ be the corresponding quadratic twist. Passing to the quadratic twist may turn closed points into rational points. This relies on a useful fact from Galois theory:

Lemma 8.1. *Let $F \subset L$ be a finite abelian field extension with Galois group H. The quotient of $\mathrm{Spec}(L) \times_{\mathrm{Spec}(F)} \mathrm{Spec}(L)$ by the diagonal action of H is isomorphic to the disjoint sum of $|H|$ copies of $\mathrm{Spec}(F)$.*

Proof. Set $A = \prod_{\sigma \in H} L$. Under the isomorphism $L \otimes_F L \to A$, $x \otimes y \mapsto (x\sigma(y))_\sigma$, the diagonal tensor product action of H on $L \otimes_F L$ corresponds to the diagonal product action on A given by $\tau \cdot (z_\sigma)_\sigma = (\tau(z_\sigma))_\sigma$. The corresponding invariant ring is $A^H = \prod_{\sigma \in H} F$, which gives our statement. □

Now suppose $z \in E_K$ is a closed point, so that the corresponding closed subscheme $\mathrm{Spec}\, \kappa(z) \subset E_K$ is invariant under the sign involution, and whose residue field extension $K \subset \kappa(z)$ is isomorphic to $K \subset K'$. Set $E_{K'} = E_K \otimes K'$, and let

$$r : E_{K'} \to E_K \quad \text{and} \quad q : E_{K'} \to \widetilde{E}_K$$

be the canonical morphisms. Then, by the preceding Lemma, the closed subscheme $q(r^{-1}(z)) \subset \widetilde{E}_K$ is the disjoint union of two rational points $y_1, y_2 \in \widetilde{E}_K$. This leads to the following result:

Proposition 8.2. *Suppose there is a étale subgroup scheme $G_K \subset E_K$ of length p, containing a closed point $z \in G_K$ so that the field extension $K \subset \kappa(z)$ is of degree two. Then $\widetilde{E}_K$ contains a rational p-division point.*

Proof. First note that G_K is a twisted form of $\mathbb{Z}/p\mathbb{Z}$. For $p = 2$, all such twisted forms are trivial, such that all points of G_K are rational. Our assumptions thus imply $p \geq 3$. Then the two field extensions $K \subset \kappa(z)$ and $K \subset K'$ are isomorphic, because R is strictly henselian. We now check that $z \in G_K$, viewed as a closed subscheme, is invariant under the sign involution. Write G_K as the spectrum of $K[T]/(T^p - \tau T)$ for some $\tau \in K^\times$. Then the sign involution acts via $T \mapsto -T$. The closed point $z \in G_K$ corresponds to an irreducible quadratic factor in $K[T]$ of $T^{p-1} - \tau = \prod_{\zeta \in \mu_{p-1}} (T - \zeta\alpha)$, where $\alpha \in \Omega$ is a root of this polynomial. The quadratic factors are of the form

$$(T - \zeta\alpha)(T - \zeta'\alpha) = T^2 - (\zeta + \zeta')\alpha T + \zeta\zeta'\alpha^2,$$

whence $\zeta' = -\zeta$, and the quadratic factor is invariant under $T \mapsto -T$. In light of the discussion preceding the Proposition, the image $q(r^{-1}(z)) \subset \widetilde{E}_K$ is the disjoint union of two rational points, which are necessarily of order p. □

It is easy to see that quadratic twisting is compatible with isogenies: If $E_K \to E'_K$ is an isogeny, we obtain an isogeny $\widetilde{E}_K \to \widetilde{E}'_K$ of the same degree between the corresponding quadratic twists. We now apply this to the inseparable isogeny $F : E_K \to E_K^{(p)}$ of degree p. Clearly, the induced isogeny on quadratic twists is also inseparable, and it follows that the quadratic twist of a Frobenius pullback is the Frobenius pullback of the quadratic twist. We simply write $\widetilde{E}_K^{(p)}$ for this elliptic curve.

Proposition 8.3. *Suppose $p \geq 3$, that E_K has good reduction, and that the Hasse invariant of $E \to \operatorname{Spec}(R)$ has vanishing order $(p-1)/2$. Then the quadratic twist $\widetilde{E}_K^{(p)}$ contains a rational p-division point. Its specialization in the closed fiber of the Néron model is nonzero and lies in the connected component of the origin, that is, its class in Φ_k is zero.*

Proof. Let $E^{(p)}$ be the Néron model of $E_K^{(p)}$. According to Lemma 4.1, there is a subgroup scheme $G \subset E^{(p)}$ of order p that is generically étale. Let $t \in R$ be a uniformizer. Then $t^{(p-1)/2} \in R$ represents the Hasse invariant of E, and G is isomorphic to the spectrum of $R[T]/(T^p - t^{(p-1)/2}T)$. Now let $R' \subset K'$ be the integral closure of $R \subset K'$, and choose a uniformizer $t' \in R'$ with $t'^2 = t$. Using the decomposition

$$T^p - t'^{p-1}T = T \prod_{\zeta \in \mu_{p-1}} (T - \zeta t'),$$

we infer that $G' = G \otimes_R R'$ decomposes into p sections for $E' = E \otimes_R R'$, which are invariant under the diagonal $\{\pm 1\}$-action and intersect pairwise transversally in the fixed point $0 \in E'_k$. We conclude that $\widetilde{E}_K^{(p)}$ contains a rational p-division point. It remains to determine its specialization behavior.

Consider the normal surface $Y = E^{(p)}_{R'}/\{\pm 1\}$, and let $q : E^{(p)}_{R'} \to Y$ be the quotient map. Let $X \to Y$ be the blowing-up of the four rational double points of type A_1 on Y. As explained in the proof for Proposition 6.1, the Néron model $\widetilde{E}$ of $\widetilde{E}_K$ is obtained from X by removing the strict transform of the closed fiber $Y_k \subset Y$. Choose a rational p-division point $z \in \widetilde{E}^{(p)}_K$ and consider the closures $S_z, S_0 \subset \widetilde{E}^{(p)}_K$. If the Artin scheme $q(S_z) \cap q(S_0)$ is of length one, the strict transforms of $q(S_z)$ and $q(S_0)$ on X will be disjoint and must pass through the same irreducible component of the closed fiber. So the following Lemma concludes the proof. □

Lemma 8.4. *Let $S = \mathrm{Spec}(A)$ be a regular local 2-dimensional scheme in characteristic $p \neq 2$ endowed with a $\{\pm 1\}$-action whose only fixed point is the closed point. Let $C_1, C_2 \subset S$ be invariant regular curves intersecting transversely, and $q : S \to S/\{\pm 1\}$ be the quotient map. Then $q(C_1) \cap q(C_2)$ has length one.*

Proof. Without loss of generality we may assume that $A = k[[x, y]]$, and that the action is given by $x \mapsto -x$ and $y \mapsto -y$ (see, for example, [16], Lemma 5.4). The invariant ring is then $k[[x^2, xy, y^2]]$. Set $D_i = q(C_i)$, and let $a \in S/\{\pm 1\}$ be the closed point. Then $q^{-1}(a)$ has length three, and the projections $C_i \to D_i$ have degree two. If the integral curve D_i were nonnormal, then $q^{-1}(a) \cap C_i$ would have length ≥ 4. This is impossible, so the D_i are regular. Let $n \geq 1$ be the length of $D_1 \cap D_2$. The Nakayama Lemma implies that $q^{-1}(D_1 \cap D_2)$ has length $\leq 3n$. On the other hand, $q^{-1}(D_1 \cap D_2) \cap (C_1 \cup C_2)$ has length $4n - 1$. This gives us the estimate $4n - 1 \leq 3n$, and consequently $n = 1$. □

It remains to find a discrete valuation ring R and an elliptic curve E_K over the function field $R \subset K$ whose Néron model $E \to \mathrm{Spec}(R)$ meets the assumptions of the Proposition 8.3.

Theorem 8.5. *Let k be an algebraically closed field of characteristic $p \geq 3$, and $j_k \in k$ be a supersingular j-value. Then there is an elliptic curve E_K over the field $K = k(t)$ with reduction type I^*_0 so that $E^{(p)}_K$ contains a rational p-division point whose specialization in the closed fiber of the Néron model is nonzero and lies in the connected component of the origin. Moreover, the j-invariant of E_K lies in R and has residue class j_k.*

Proof. Let V_k be the supersingular elliptic curve with the given j-invariant j_k. Set $A = k[u]_{(u)}$ and choose a versal deformation $V \to \mathrm{Spec}(A)$ of V_k. According to Igusa's Theorem ([10], Theorem 12.4.3), the Hasse invariant of V has vanishing order one. Now set $R = k[t]_{(t)}$ with $t = u^{(p-1)/2}$. The Hasse invariant of the induced family $V \otimes_R R'$ has vanishing order $(p-1)/2$. Let E be the quadratic twist of $V \otimes_R R'$. According to Proposition 6.1 and Proposition 8.3, the elliptic curve E has all desired properties. □

Remark 8.6. Here and the the sequel we are concerned with the *existence* of rational p-division points. It might be interesting to compute their coordinates *explicitly*.

9. Decreasing osculation numbers

In this section we develop a method to produce rational p-division points by passing from one Weierstrass equation to another that is defined over a smaller field. The set-up is as follows: Let R' be a henselian discrete valuation ring in

characteristic $p \geq 5$ with algebraically closed residue field $k = R'/\mathfrak{m}_{R'}$ and field of fractions $R' \subset K'$. We also fix a uniformizer $t' \in R'$.

Let $E_{K'}$ be an elliptic curve over K' with good reduction and Néron model $E' \to \operatorname{Spec}(R')$. Choose a Weierstrass equation of the form

$$y'^2 = x'^3 + a'_4 x' + a'_6 \tag{15}$$

with coefficients $a'_4, a'_6 \in R'$, such that the discriminant $\Delta' \in R'$ is invertible. Making the substitutions $x' = t'^{-2}x$ and $y' = t'^{-3}y$ over K', we obtain a new Weierstrass equation

$$y^2 = x^3 + a_4 x + a_6, \tag{16}$$

for $E_{K'}$. Note that its coefficients $a_i = t'^i a'_i$ remain integral, such that the new Weierstrass equation still defines a relative cubic $C' \to \operatorname{Spec}(R')$. This cubic, however, is not the Weierstrass model of its generic fiber, because its discriminant $t'^{12}\Delta'$ is not invertible. Now suppose there is a subring $R \subset R'$ with $a_4, a_6 \in R$ so that the extension $R \subset R'$ is finite and separable. Replacing R by its normalization, we conclude that R is another henselian discrete valuation ring, and the residue field extension $R/\mathfrak{m}_R \subset R'/\mathfrak{m}_{R'}$ is bijective. Let $R \subset K$ be the field of fractions.

Our new Weierstrass equation (16) defines a relative cubic $C \to \operatorname{Spec}(R)$ with $C \otimes_R R' \simeq C'$. Let E_K be its generic fiber, such that $E_K \otimes_K K' = E_{K'}$, and $E \to \operatorname{Spec}(R)$ be its Néron model.

Proposition 9.1. *Under the preceding assumptions, the degree $d = [K' : K]$ satisfies the divisibility condition $d \mid 12$. If furthermore $d \neq 1$, then E_K has additive reduction and the relative cubic $C \to \operatorname{Spec}(R)$ is its Weierstrass model. If $d = 6, 4, 3, 2$, then the reduction type of E_K is* II, III, IV, I_0^*, *respectively.*

Proof. Let $\Delta \in R$ be the discriminant for (16). Since $C \otimes_R R' = C'$ by construction, we have $d\nu(\Delta) = 12$. Now suppose that $d \neq 1$, such that $\nu(\Delta) < 12$. By Tate's Algorithm, the Weierstrass equation (16) must be minimal, such that $C \to \operatorname{Spec}(R)$ is the Weierstrass model of its generic fiber. Since $\Delta \in \mathfrak{m}_R$, the elliptic curve E_K has bad reduction. Since E_K has potentially good reduction, the reduction type must be additive. Ogg's Formula $\nu(\Delta) = 2 + (m-1)$ implies the statement on the reduction types. □

We now examine the behavior of rational p-division points in our construction:

Proposition 9.2. *Under the preceding assumptions, suppose the field extension $K \subset K'$ has degree $d > 1$. Assume furthermore that $E_{K'}$ contains a rational p-division point with osculation number one. Then E_K contains a rational p-division point whose specialization into E_k is nonzero.*

Proof. Choose a rational p-division point $z \in E_{K'}$, say with coordinates $z = (\lambda, \mu)$ with $\lambda, \mu \in K'$. According to Proposition 5.1, the coordinates have valuations $\nu(\lambda) = -2$ and $\nu(\mu) = -3$. Consequently $u'^2\lambda, u'^3\mu \in R'$, and the closure $S_z \subset C'$ of $z \in E_{K'}$ in the relative cubic defined by the new Weierstrass equation (16) is a section over R' disjoint from the zero section. Since $u'^2\lambda$ is invertible, it is also disjoint from the singularity in C'.

Suppose for the moment that the j-invariant $j \in K$ of the elliptic curve E_K is a p-th power. According to Proposition 3.3, there is an étale subgroup scheme $G_K \subset E_K$ of order p. Let $A_K = G_K - 0$ be the complement of the origin, and $A \subset C$ be its closure in the Weierstrass model $C \to \operatorname{Spec}(R)$ of E_K. Since $d \geq 1$,

this Weierstrass model is defined by the Weierstrass equation (16), according to Proposition 9.1. We saw in the preceding paragraph that $A \otimes_R R' \subset C' = C \otimes_R R'$ is disjoint from the zero section and the singularity in C', so the same holds for $A \subset C$. We infer that $A \cup \{0\}$ coincides with the closure $G \subset E$ of G_K in the Néron model $E \to \mathrm{Spec}(R)$, such that G is a relative group scheme whose closed fiber is reduced at the origin. But R is strictly henselian, so $G = (\mathbb{Z}/p\mathbb{Z})_R$. Restricting to the generic fiber yields the desired rational p-division point on E_K.

It remains to verify that the j-invariant $j \in K$ of E_K is a p-th power. By assumption, $E_{K'}$ contains a rational p-division point, whence $j \in K'$ is a p-th power by Proposition 3.3. The following Lemma ensures that $j \in K$ is already a p-th power. □

Lemma 9.3. *Let $F \subset E$ be a field extension in characteristic $p > 0$. If this extension is separable, then the inclusion $F^p \subset E^p \cap F$ is a bijection.*

Proof. It suffices to show that the canonical map $F^\times/F^{\times p} \to E^\times/E^{\times p}$ is injective. Via the Kummer sequence, we may regard this map as $H^1(F, \mu_p) \to H^1(E, \mu_p)$. Let T be a nontrivial μ_p-torsor over F, such that T is a reduced scheme. Since $F \subset E$ is separable, the induced torsor $T \otimes_F E$ remains a reduced scheme, hence is a nontrivial torsor. Consequently, the map in question is injective. □

Proposition 9.4. *Suppose $p \equiv -1$ modulo 3. Fix an integer $1 \leq n \leq 5$, and let E_K be the elliptic curve over K defined by the Weierstrass equation*

$$y^2 = x^3 + t^{n(p-5)/6}x + t^{-n}. \tag{17}$$

Then $E_K^{(p)}$ contains a rational p-division point whose specialization in the closed fiber of the Néron model is nonzero. The j-invariant of E_K lies in R and reduces to $0 \in k$. The reduction types are given by the following table:

n	1	2	3	4	5
E_K	II^*	IV^*	I_0^*	IV	II
$E_K^{(p)}$	II	IV	I_0^*	IV^*	II^*

Proof. We first treat the case $n = 1$. Let t' be an indeterminate, and consider the family of elliptic curves $y^2 = x^3 + t'x + 1$ over $R' = k[[t']]$, which is a versal deformation for the supersingular elliptic curve $y^2 = x^3 + 1$ with j-invariant $j_k = 0$. The base change $t' \mapsto t'^{p-1}$ yields the family of elliptic curves $y^2 = x^3 + t'^{p-1}x + 1$, whose Hasse invariant has vanishing order $p-1$, according to Igusa's Theorem ([10], Theorem 12.4.3). Whence the Frobenius pullback $y^2 = x^3 + t'^{p(p-1)}x + 1$ contains a rational p-division point, which has osculation number one by Proposition 5.2. Making the substitution $x = t'^{-2}x'$, $y = t'^{-3}y'$, we obtain the new Weierstrass equation $y^2 = x^3 + t'^{p(p-1)+4}x + t'^6$, which defines a relative cubic over $k[[t']]$. Since $p \equiv -1$ modulo 3, this cubic is already defined over the subring $k[[t]] \subset k[[t']]$, where $t = t'^6$. According to Proposition 9.2, the elliptic curve

$$y^2 = x^3 + t^{(p(p-1)+4)/6}x + t$$

over $K = k((t))$ contains a rational p-division point whose specialization in the Néron model is nonzero. Its reduction type is II by Proposition 9.1.

It remains to identify this elliptic curve as the Frobenius pullback of E_K. To do this, write $p = 6d - 1$ for some integer $d \geq 1$. Making the substitution $x = t^{2d}x'$,

$y = t^{3d}y'$, we obtain the Weierstrass equation

$$y^2 = x^3 + t^{(p(p-1)+4)/6-4d}x + t^{1-6d},$$

which is indeed the Frobenius pullback of (17) in the case $n = 1$ at hand. According to Proposition 7.4, the curve E_K has reduction type II^*.

The elliptic curves for $n > 1$ are obtained from the elliptic curve with $n = 1$ via the base change $t \mapsto t^n$, and their reduction types easily follow from Ogg's Formula. □

Proposition 9.5. *Suppose $p \equiv -1$ modulo 4. Fix an integer $1 \leq n \leq 3$, and let E_K be the elliptic curve over K defined by the Weierstrass equation*

$$y^2 = x^3 + t^{-n}x + t^{n(p-7)/4}. \tag{18}$$

Then E_K contains a rational p-division point whose specialization in the closed fiber of the Néron model is nonzero. Its j-invariant lies in R and reduces to $1728 \in k$, and the reduction type is given by the following table:

n	1	2	3
E_K	III^*	I_0^*	III
$E_K^{(p)}$	III	I_0^*	III^*

Proof. This is analogous to the proof for Proposition 9.4. Consider the family of elliptic curves $y^2 = x^3 + x + t'$ over $R' = k[[t']]$, which is a versal deformation for the supersingular elliptic curve $y^2 = x^3 + x$ with j-invariant $j_k = 1728$. The base change $t' \mapsto t'^{p-1}$ yields the family of elliptic curve $y^2 = x^3 + x + t'^{p-1}$, and its Frobenius pullback $y^2 = x^3 + x + t'^{p(p-1)}$ contains a rational p-division point with osculation number one. Making the substitution $x = t'^{-2}x'$, $y = t'^{-3}y'$, we obtain the new Weierstrass equation $y^2 = x^3 + t'^4x + t'^{p(p-1)+6}$, which defines a relative cubic over $k[[t']]$. Since $p \equiv -1$ modulo 4, this cubic is already defined over the subring $k[[t]] \subset k[[t']]$, where $t = t'^4$. According to Proposition 9.2, the elliptic curve

$$y^2 = x^3 + tx + t^{(p(p-1)+6)/4}$$

over $K = k((t))$ contains a rational p-division point whose specialization in the Néron model is nonzero. Its reduction type is III according to Proposition 9.1

Write $p = 4d - 1$ for some integer $d \geq 1$. Making the substitution $x = t^{2d}x'$, $y = t^{3d}y'$, we obtain the Weierstrass equation

$$y^2 = x^3 + t^{1-4d}x + t^{(p(p-1)+6)/4-6d},$$

which is the Frobenius pullback of (18) in the case $n = 1$. According to Proposition 7.4, the curve E_K has reduction type III^*. The elliptic curves for $n > 1$ are obtained from the elliptic curve with $n = 1$ via the base change $t \mapsto t^n$, and Ogg's Formula gives the reduction type. □

Now let $j_k \in \overline{\mathbb{F}}_p \subset R$ be an arbitrary supersingular j-value. Choose $a, b \in \mathbb{F}_{p^2}$ so that $y^2 = x^3 + ax + b$ defines a supersingular elliptic curve with j-invariant j_k.

Proposition 9.6. *Assumptions as above. Let E_K be the elliptic curve over K defined by the Weierstrass equation*

$$y^2 = x^3 + at^{-2p}x + (b + t^{(p-1)/2})t^{-3p}. \tag{19}$$

Then E_K contains a rational p-division point whose specialization in the closed fiber of the Néron model is nonzero. Its reduction type is I_0^*, and its j-invariant lies in R and reduces to $j_k \in k$.

Proof. This is analogous to the proof for Proposition 9.4. Consider the family of elliptic curves $y^2 = x^3 + ax + b + t'$ over $R' = k[[t']]$, which is a versal deformation for the supersingular elliptic curve $y^2 = x^3 + ax + b$ with j-invariant j_k. The base change $t' \mapsto t'^{p-1}$ yields the family of elliptic curves $y^2 = x^3 + ax + b + t'^{p-1}$, so its Frobenius pullback $y^2 = x^3 + a^p x + b^p + t'^{p(p-1)}$ contains a rational p-division point with osculation number one. Making the substitution $x = t'^{-2}x'$, $y = t'^{-3}y'$, we obtain the new Weierstrass equation $y^2 = x^3 + t'^4 a^p x + (b^p + t'^{p(p-1)})t'^6$, which defines a relative cubic over $k[[t']]$. This cubic is already defined over the subring $k[[t]] \subset k[[t']]$, where $t = t'^2$. According to Proposition 9.2, the corresponding elliptic curve

$$y^2 = x^3 + t^2 a^p x + (b^p + t^{p(p-1)/2})t^3$$

over $K = k((t))$ contains a rational p-division point whose specialization in the Néron model is nonzero. Its reduction type is I_0^* by Proposition 9.1.

Write $p = 1-2d$ for some integer d. Making the substitution $x = t^{2d}x'$, $y = t^{3d}y'$, we obtain the Weierstrass equation

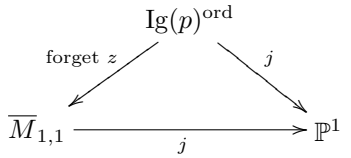
$$y^2 = x^3 + t^{2-4d} a^p x + (b^p + t^{p(p-1)/2})t^{3-6d},$$

which is the Frobenius pullback of (19). According to Proposition 7.4, the curve E_K has reduction type I_0^*. □

Remark 9.7. In the proofs of Propositions 9.4, 9.5 and 9.6 we constructed our examples from the base change $t' \mapsto t'^{p-1}$ from a versal deformation of a supersingular elliptic curve. If we apply an n-fold Frobenius pullback to this base change and carry out the constructions explained in the proofs of these propositions, we obtain all the examples of this section, but now with osculation number n. In particular, Frobenius pullbacks from the curves constructed in this section give all possible reduction types with arbitrary osculation numbers. We leave it to the reader to determine explicit Weierstrass equations.

10. The elliptic curve over the Igusa curve

Let $p > 0$ be a prime number, and consider the ordinary part of the *Igusa stack* $\mathrm{Ig}(p)^{\mathrm{ord}}$, whose objects over a k-algebra A are pairs (E, z), where $E \to \mathrm{Spec}(A)$ is a family of ordinary elliptic curves, and $z : \mathrm{Spec}(A) \to E^{(p)}$ is a section whose fibers are points of order p. We have a commutative diagram of algebraic stacks



where the map on the left maps is $(E, z) \mapsto (E, 0)$, which is a cyclic Galois covering of degree $p - 1$, and the map on the right is $(E, z) \mapsto j(E)$, which has degree $(p - 1)/2$. Note that the horizontal map of algebraic stacks has degree $1/2$, and that the image of the j-map $\mathrm{Ig}(p)^{\mathrm{ord}} \to \mathbb{A}^1$ is precisely the ordinary locus on the j-line.

This moduli problem has been first studied by Igusa [9]. For $p \geq 3$, the Igusa stack is representable by [10], Corollary 12.6.3, and we shall assume $p \geq 3$ in this section. Abusing notation we write $\mathrm{Ig}(p)^{\mathrm{ord}}$ for the corresponding algebraic curve, and denote by $\mathrm{Ig}(p)$ its normal compactification. Let $U^{\mathrm{ord}} \to \mathrm{Ig}(p)^{\mathrm{ord}}$ be the universal elliptic curve, and $U \to \mathrm{Ig}(p)$ be its Néron model. We now give a complete description of the universal curve around supersingular points. Let $F = \mathcal{O}_{\mathrm{Ig}(p),\eta}$ be the function field of the Igusa curve.

Theorem 10.1. *Suppose $p \geq 5$. Let $x \in \mathrm{Ig}(p)$ be a supersingular point. Then a Weierstrass equation for U_F over the completion at $x \in \mathrm{Ig}(p)$, as well as the reduction type for U_F and its Frobenius pullback are as in the following table:*

$j(x)$	p	Weierstrass equation	U_F	$U_F^{(p)}$
0	$\equiv -1 \mod 3$	$y^2 = x^3 + t^{(p-5)/6}x + t^{-1}$	II^*	II
1728	$\equiv -1 \mod 4$	$y^2 = x^3 + t^{-1}x + t^{(p-7)/4}$	III^*	III
$\neq 0, 1728$	all p	$y^2 = x^3 + at^{-2p}x + (b + t^{(p-1)/2})t^{-3p}$	I_0^*	I_0^*

Here $t \in \mathcal{O}^{\wedge}_{\mathrm{Ig}(p),x}$ is a suitable uniformizer, and the scalars $a, b \in k$ in the last row are so that the elliptic curve $y^2 = x^3 + ax + b$ has j-invariant $j(x)$. Moreover, the rational p-division points in $U_F^{(p)}$ have nonzero specialization in the Néron model.

Proof. Note that the entries for the Frobenius pullback $U_F^{(p)}$ are determined by those for U_F and vice versa, according to Proposition 7.4. We now give a complete proof for the case $j(x) = 0$, the other cases being analogous and left to to the reader. So suppose $j(x) = 0$. Obviously, this j-value must be supersingular, whence $p \equiv -1$ modulo 3. According to Proposition 9.4, there is an elliptic curve E_K over the function field $K = k((t))$ of $R = k[[t]]$, with reduction type II^* and Weierstrass equation as in the table. Moreover, the Frobenius pullback $E_K^{(p)}$ contains a rational p-division point whose specialization in the closed fiber of the Néron model is nonzero. Let $\varphi : \mathrm{Spec}(K) \to \mathrm{Ig}(p)$ be the corresponding classifying morphism, such that $E_K = U \otimes_F K$ and $E_K^{(p)} = U_F^{(p)} \otimes K$. By the valuation criterion, the morphism extends uniquely to a morphism $\varphi : \mathrm{Spec}(R) \to \mathrm{Ig}(p)$. By Igusa's result [10], Corollary 12.6.2 the morphism $j : \mathrm{Ig}(p) \to \mathbb{P}^1$ is totally ramified over the supersingular j-values and hence the point x lies in the image of φ. We thus obtain an extension of discrete valuation rings $R' \subset R$, say with ramification index $e \geq 1$, where $R' = \mathcal{O}_{\mathrm{Ig}(p),x}$. We claim that $e = 1$. To see this, denote by $\nu \geq 2$ the valuation of a minimal discriminant for $U_F^{(p)}$ at x. Since $E_K^{(p)}$ has reduction type II, Lemma 10.2 below tells us that $2 = e\nu$, and whence $e = 1$. Since Néron models are preserved under extensions with ramification index $e = 1$, the curve U_F has reduction type II^* at x, and the statement about the specialization of the rational point on $E_K^{(p)}$ follows in a similar way. □

We have used the following observation: Suppose $R' \subset R$ is an extension of discrete valuation rings of arbitrary characteristic $p > 0$, with the same residue field $k = R/\mathfrak{m}_R = R'/\mathfrak{m}_{R'}$, and function fields $K' \subset K$. Suppose $E_{K'}$ is an elliptic curve containing a rational p-division point. Set $E_K = E_{K'} \otimes K$, and let $E \to \mathrm{Spec}(R)$ and $E' \to \mathrm{Spec}(R')$ be the Néron models of E_K and $E_{K'}$, respectively.

Lemma 10.2. *Suppose the rational p-division point on $E_{K'}$ specializes into ${E'}_k^0$, and that the induced point on E_K specializes into a nonzero element of E_k^0. Let ν*

and ν' be the valuations of minimal discriminants for E_K and $E_{K'}$, respectively, and $e \geq 1$ be the ramification index of $R \subset R'$. Then we have $\nu = e\nu'$.

Proof. We have $\nu = e\nu' - 12c$, where $c \geq 0$ is the number of cycles needed in the Tate Algorithm before termination. Consider the canonical homomorphism of relative group schemes $E' \otimes_{R'} R \to E$. If $c \geq 1$, then the connected component of the origin in E'_k is mapped to the origin in E_k, whence the rational p-division point on E_K specializes to zero, contradiction. □

It remains to determine the Néron model over the cusps of $\mathrm{Ig}(p)$, that is, the points where the j-invariant has a pole [10], Section 8.6.3.

Theorem 10.3. *Suppose $p \geq 3$. Then the scheme of cusps of $\mathrm{Ig}(p)$ is finite étale of length $(p-1)/2$ with a transitive action of the Galois group of $j : \mathrm{Ig}(p) \to \mathbb{P}^1$. The Néron model over a cusp of $\mathrm{Ig}(p)$ has multiplicative reduction of type I_1 and its Frobenius pullback has multiplicative reduction of type I_p.*

Proof. Since the j-invariant has negative valuation, U_F has potentially multiplicative reduction. If U_F had additive reduction then we would have reduction of type I^*_ℓ for some $\ell \geq 1$. However, this is excluded by Corollary 4.5 and U_F has already multiplicative reduction.

Let $K = k((t))$ and $q = t^p$. Then there exists an elliptic curve E_K over and a homomorphism $K^* \to E_K(K)$ with kernel $q^{\mathbb{Z}}$, namely the Tate curve ([21], Chapter V, §3). In particular, $t \in K^*$ maps to a rational p-division point of E_K and since $\nu(j) = -\nu(q) = -p$ this elliptic curve has multiplicative reduction of type I_p.

This curve is the Frobenius pullback of a curve induced from U_F around a cusp $x \in \mathrm{Ig}(p)$. Hence $\nu(j(x)) = -1$ for this cusp x, which implies that U_F has multiplicative reduction of type I_1 at x. Hence $j : \mathrm{Ig}(p) \to \mathbb{P}^1$ is étale around x and since j is a Galois morphism the same is true for every cusp. In particular, the scheme of cusps is étale of length $(p-1)/2$ and I_1 is the reduction type of the Néron model for every cusp of $\mathrm{Ig}(p)$. □

Let E be the Néron model of an elliptic curve E_K and assume that it has multiplicative reduction. If there exists a rational p-division point on E_K then it generates a group scheme $G \subset E$ with generic fiber $(\mathbb{Z}/p\mathbb{Z})_K$, which can specialize to α_p or $\mathbb{Z}/p\mathbb{Z}$ only. Since $E^0_k \simeq \mathbb{G}_m$ neither of these latter group schemes is contained in E^0_k and so the rational p-division point specializes non-trivially into Φ_k.

Remark 10.4. Note that Ulmer [23], Section 2 gave Weierstrass equations with coefficients in F for the universal curve U_F, which rely on relations between Eisenstein series and are of somewhat implicit nature. There it is also shown that the universal family over $\mathrm{Ig}(p)$ descends to the j-line if and only if $p \equiv -1$ modulo 4. In this case, the reduction type of the Néron model of the descended family has been determined in loc. cit., Section 6. It is interesting to note that the universal family over $\mathrm{Ig}(p)$ has good reduction over $j = 0$ if $p \equiv 1$ modulo 3, whereas the descended family acquires additive reduction.

11. Elliptic curves with $\delta = 1$

The Igusa stack in characteristic two and three has entirely new features because wild ramification shows up. In this section we briefly recall some relevant facts from ramification theory and analyze the Galois representation on torsion points attached to elliptic curves whose wild part of the conductor is nontrivial yet as small

as possible, namely $\delta = 1$. These results will be applied to universal families over Igusa curves in the next sections. For more background on ramification groups, we refer to the monographs [18] and [7] and the survey article [3].

Suppose k is an algebraically closed field of characteristic $p > 0$ and set $R = k[[t]]$ and $K = k((t))$. Let $K \subset L$ be a finite Galois extension, with Galois group $G = \mathrm{Gal}(L/K)$, and $R_L \subset L$ be the integral closure of R. The *higher ramification groups*

$$G_0 \supset G_1 \supset G_2 \supset \dots$$

are defined as the subgroups $G_i \subset G$ that act trivially on the i-th infinitesimal neighborhood $\mathrm{Spec}(R_L/\mathfrak{m}_L^{i+1})$. Then $G = G_0$, the $G_i \subset G$ are normal, $G_1 \subset G$ is the Sylow p-subgroup, and G/G_1 is cyclic of order prime to p. Using the existence of Sylow subgroups in G for the prime divisors of $[G : G_1]$, we infer that $G \simeq G_1 \rtimes C_m$ for some integer prime to p. Here and throughout, C_m denotes a cyclic group of order m.

Choose a prime $l \neq p$. The *Swan representation* P attached to the Galois group G is the projective $\mathbb{Z}_l[G]$-module whose character is given by $b(\sigma) = -\max\{i \mid \sigma \in G_i\}$, $\sigma \neq e$, and $\sum_{\sigma \in G} b(\sigma) = 0$. If V is a $\mathbb{F}_l[G]$-module, one defines an integer invariant $\delta(V) = \dim_{\mathbb{F}_l} \mathrm{Hom}_G(P, V)$, which does not depend on the choice of $K \subset L$. It also satisfies the formula

$$\delta(V) = \sum_{i \geq 1} \frac{1}{[G : G_i]} \dim_{\mathbb{F}_l} V/V^{G_i}. \tag{20}$$

Now let E_K be an elliptic curve and E be its Néron model. Choose a Galois extension $K \subset L$ so that the $\mathbb{F}_l$-vector space $E[l](L)$ becomes 2-dimensional. The invariant $\delta = \delta(E[l](L))$ is called the *wild part of the conductor*. It does not depend on l. If E_K has additive reduction, Ogg's formula tells us $\nu(\Delta) = 2 + \delta + (m - 1)$, where m denotes the number of irreducible components in the closed fiber of the minimal model.

By construction, the Galois group G comes along with a representation on the vector space $E[l](L)$, which we regard as a homomorphism $G \to \mathrm{GL}(2, \mathbb{F}_l)$. The linear G-action respects the Weil pairing $\Phi : E[l] \times E[l] \to \mu_l(K)$ in the sense that $\Phi(a^\sigma, b^\sigma) = \Phi(a, b)^\sigma$. Since k is algebraically closed, the G-action on $\mu(K)$ is trivial, such that we have a factorization $G \to \mathrm{SL}(2, \mathbb{F}_l)$. We remark in passing that this factorization holds for $l = 2$ without any assumption on k. Note that saying that $G \to \mathrm{SL}(2, \mathbb{F}_l)$ is surjective means that the scheme of nonzero l-torsion $E_K[l] - 0$ is connected, and stays so under base extension as long as possible.

It is often convenient to replace G by its image in $\mathrm{SL}(2, \mathbb{F}_l)$, such that $K \subset L$ becomes the smallest Galois extension so that $E[l](L)$ is 2-dimensional. But it is useful to work with the general situation when it comes to base change:

Lemma 11.1. *Let $K \subset K'$ be a field extension of degree d prime to p. Then the wild part of the conductor for the induced elliptic curve $E_{K'}$ is $\delta' = d\delta$.*

Proof. Enlarging L, we may assume that $K \subset K' \subset L$, and set $G' = \mathrm{Gal}(L/K')$. Obviously $G'_i = G' \cap G_i$ are the ramification groups for $K' \subset L$. By Puiseux's Theorem, $K \subset K'$ is cyclic, hence corresponds to a surjection $G \to C_d$, whose kernel equals G', and contains G_1 because d is prime to p. We conclude $G'_i = G_i$ for $i \geq 1$, and the statement follows from Formula (20). □

Lemma 11.2. *Let $K \subset K'$ be a finite and purely inseparable field extension. Then the wild part of the conductor for the induced elliptic curve $E_{K'}$ is $\delta' = \delta$.*

Proof. Choose a R_K-algebra generator $x \in R_L$. Given $\sigma \in G$ we have $\sigma \in G_i$ if and only if $\nu_L(\sigma(x) - x) \geq i + 1$ by [18], Chapter IV, §1, Lemma 1. Recall that $K = k((t))$ so that $K' = K^{1/p^n}$ for some $n \geq 1$. It suffices to treat the case $n = 1$. Then $L' = L \otimes_K K'$ and a straightforward argument shows that $x^{1/p}$ is a $R_{K'}$-algebra generator of $R_{L'}$. Now

$$\nu_{L'}(\sigma(x^{1/p}) - x^{1/p}) = \frac{1}{p}\nu_{L'}(\sigma(x) - x) = \frac{p}{p}\nu_L(\sigma(x) - x).$$

Using this equation we conclude that the higher ramification groups and their indices for L/K and L'/K' coincide. The statement now follows from Formula (20). □

The group $\mathrm{SL}(2, \mathbb{F}_2) = \mathrm{GL}(2, \mathbb{F}_2)$ has order 6, consequently $\delta = 0$ for characteristic $p \geq 5$. For the rest of the section, we work in characteristic two and three and examine the Galois representation $G \to \mathrm{SL}(2, \mathbb{F}_l)$ for elliptic curves with $\delta = 1$.

We start with the case $p = 3$ and choose $l = 2$. Note that the action on $\mathbb{P}^1(\mathbb{F}_2)$ gives a bijection $\mathrm{GL}(2, \mathbb{F}_2) \to S_3$, and these groups are isomorphic to the nontrivial semidirect product $C_3 \rtimes C_2$. Let E_K be an elliptic curve, and choose a Galois extension $K \subset L$ so that $E[2](L)$ becomes a 2-dimensional $\mathbb{F}_2$-vector space. Let δ be the wild part of the conductor for E_K and g be the order of the Galois group $G = \mathrm{Gal}(L/K)$.

Proposition 11.3. *If $\delta = 1$, then the homomorphism $G \to \mathrm{SL}(2, \mathbb{F}_2)$ is surjective. If moreover $9 \nmid g$, then G is isomorphic to the nontrivial semidirect product $G = C_3 \rtimes C_{g/3}$, and the ramification groups are $G_0 = G$ and $G_1 = \ldots = G_m = C_3$ and $G_{m+1} = 1$ with $m = g/6$.*

Proof. Suppose that the homomorphism in question is not surjective. Replacing G by its image, we may assume that $G \subsetneq \mathrm{SL}(2, \mathbb{F}_2)$ is a subgroup. If g is prime to $p = 3$ then $\delta = 0$, contradiction. Suppose $g = 3$. Since each matrix in $\mathrm{GL}(2, \mathbb{F}_2)$ of order three is conjugate to $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, we have $E[2](L)^{G_i} = 0$ for every nontrivial G_i, and Formula (20) yields $1 = \delta \geq 1/1 \cdot 2$, again a contradiction. We conclude that $G \to \mathrm{SL}(2, \mathbb{F}_2)$ is surjective.

Now suppose that $9 \nmid g$, so that $G_1 = C_3$ is the unique Sylow 3-subgroup. Then $G = C_3 \rtimes C_{g/3}$ is a semidirect product, which must be the nontrivial one because $G \to \mathrm{GL}(2, \mathbb{F}_2)$ is surjective. It remains to determine the orders of the ramification groups: We have $g_0 = g$ and $g_1 = g_2 = \ldots = g_m = 3$ and $g_{m+1} = 1$ for some $m \geq 1$. Formula (20) yields $\delta = m \cdot \frac{1}{g/3} \cdot 2$, and the result follows. □

Now choose a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for the elliptic curve E_K, and let $K \subset K'$ be the field extension obtained by adjoining a root of the cubic $x^3 + (a_1^2 + a_2)x^2 + (a_4 - a_1a_3)x + (a_3^2 + a_6)$.

Corollary 11.4. *Notation as above. If the elliptic curve E_K has $\delta = 1$, then $K \subset K'$ is a non-Galois extension of degree three, the induced elliptic curve $E_{K'}$ has $\delta' = 0$, and the $\mathbb{F}_2$-vector space $E[2](K')$ is 1-dimensional.*

Proof. We may chose $K \subset L$ so that its Galois group is $G = \mathrm{GL}(2, \mathbb{F}_2)$, by Proposition 11.3. By the inversion formula ([20], III.2.3.) the scheme of nonzero 2-torsion on E_K is given by $y = a_1x + a_3$ together with the Weierstrass equation, whence by the cubic in question. The Galois correspondence implies that $K' \subset L$, and that

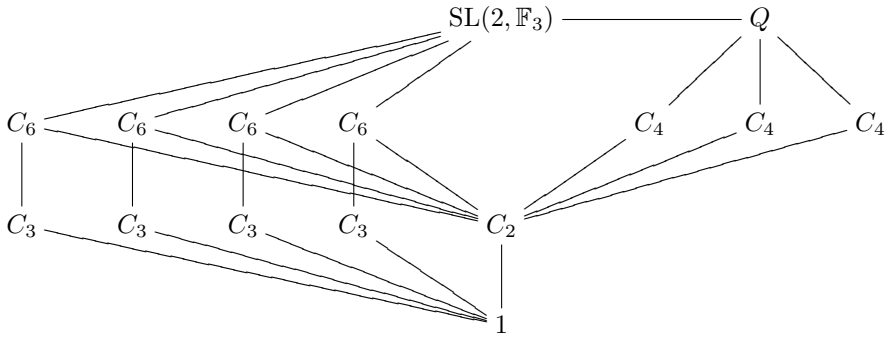
$K \subset K'$ is non-Galois of degree three. Using that $K' \subset L$ has degree two, we infer that $\delta' = 0$ and that $E[2](K')$ is 1-dimensional. □

For the rest of this section we work in characteristic $p = 2$ and choose $l = 3$. This case is more challenging. To start with, let us briefly recall some well-known facts on the group $\mathrm{SL}(2, \mathbb{F}_3)$. We have a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C_2 & \longrightarrow & \mathrm{GL}(2,\mathbb{F}_3) & \longrightarrow & S_4 & \longrightarrow & 1 \\
 & & = \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & C_2 & \longrightarrow & \mathrm{SL}(2,\mathbb{F}_3) & \longrightarrow & A_4 & \longrightarrow & 1 \\
 & & = \uparrow & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & C_2 & \longrightarrow & Q & \longrightarrow & V & \longrightarrow & 1,
\end{array}$$

where $\mathrm{GL}(2, \mathbb{F}_3) \to S_4$ is given by the action on $\mathbb{P}^1(\mathbb{F}_3)$. The group $V \subset A_4$ is the Klein four group, and $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is the quaternion group. Its six elements of order four correspond to the traceless matrices in $\mathrm{SL}(2, \mathbb{F}_3)$.

Since $A_4 = V \rtimes C_3$ it follows that $V \subset A_4$ is the commutator subgroup, and $S_4/V = S_3$ implies that $A_4 \subset S_4$ is the commutator subgroup. Using that $-1 \in Q$ is a commutator, we infer that $1 \subset C_2 \subset Q \subset \mathrm{SL}(2, \mathbb{F}_3) \subset \mathrm{GL}(2, \mathbb{F}_3)$ is the derived series. Let us depict the lattice of subgroups in $\mathrm{SL}(2, \mathbb{F}_3)$:



The normal subgroups in $\mathrm{SL}(2, \mathbb{F}_3)$ are precisely $1 \subset C_2 \subset Q \subset \mathrm{SL}(2, \mathbb{F}_3)$. Note that the $C_6 \subset \mathrm{SL}(2, \mathbb{F}_3)$ are the four Borel subgroups, that is, conjugate to the group $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$.

Now suppose E_K is an elliptic curve. Choose a Galois extension $K \subset L$ so that $E_K[3](L)$ becomes 2-dimensional, and let $G = \mathrm{Gal}(L/K) \to \mathrm{SL}(2, \mathbb{F}_3)$ be the associated representation on $E_K[3](L)$. The lattice of subgroups in $\mathrm{SL}(2, \mathbb{F}_3)$ is related to a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ as follows: The subgroups $C_6 \subset \mathrm{SL}(2, \mathbb{F}_3)$ correspond to the field extensions of K obtained by adding one of the four roots of the quartic $x^4 + b_2x^3 + b_4x^2 + b_6x + b_8$, which defines the x-coordinate for one of the four lines of points of order three (compare with the duplication formula [20], III.3.2.). The normal subgroup $Q \subset \mathrm{SL}(2, \mathbb{F}_3)$ corresponds to the Galois extension of K obtained by splitting the *resolvent cubic* $x^3 + b_4x^2 + b_2b_6x + b_2^2b_8 + b_6^2$ (compare [11], Section III.13). Note that the quartic has Galois group contained in $V = Q/C_2$ after splitting the resolvent cubic. The normal subgroup C_2 corresponds to splitting the quartic. The inclusion $1 \subset C_2$ finally corresponds to adding the y-coordinates of the 3-torsion points.

Proposition 11.5. *Suppose the elliptic curve E_K has $\delta = 1$. Then $G \to \mathrm{SL}(2, \mathbb{F}_3)$ is surjective. If moreover $16 \nmid g$, then G is isomorphic to the nontrivial semidirect product $Q \rtimes C_{g/8}$, and the ramification groups are $G_0 = G$ and $G_1 = ... = G_s = Q$, $G_{s+1} = \ldots = G_{3s} = C_2$ with $s = g/24$ and $G_m = 1$ for $m \geq 1 + g/8$.*

Proof. For the first statement, we may assume $G \subset \mathrm{SL}(2, \mathbb{F}_3)$, and our task is to show that G has order $g = 24$. Note first that $2 \mid g$, because otherwise $\delta = 0$. We observe that $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in G_i$ and whence $E[3](L)^{G_i} = 0$ for every nontrivial G_i. Second, we have $3 \mid g$. Otherwise G would be a 2-group, and Formula (20) gives $\delta \geq 1/1 \cdot 2$, contradiction. Third, we have $g \neq 6$. Otherwise the orders of the ramification groups are $g_1 = \ldots = g_m = 2$ and $g_{m+1} = 1$ for some $m \geq 1$, and thus $\delta = m \cdot 1/3 \cdot 2$, contradiction. Fourth and last, we have $g \neq 12$, because $\mathrm{SL}(2, \mathbb{F}_3)$ contains no subgroup of order 12; such a group would be normal, and whence define a splitting for $\mathrm{SL}(2, \mathbb{F}_3) \to A_4$, which is absurd. Thus, G is equal to $\mathrm{SL}(2, \mathbb{F}_3)$.

Let us determine the higher ramification groups for the special case $G = \mathrm{SL}(2, \mathbb{F}_3)$. Since C_4 is not normal in Q, it cannot be among the ramification groups. We obtain $G_1 = Q$, $G_2 = G_3 = C_2$ and $G_m = 1$ for $m \geq 4$ as in the proof for Proposition 11.3.

Now let G be arbitrary with $16 \nmid g$ and denote by G' the kernel of the surjective homomorphism $G \to \mathrm{SL}(2, \mathbb{F}_3)$. The lower filtration on ramification groups does not behave well with respect to passing to quotients. But the so-called *upper filtration* $G^x = G_{\psi(x)}$ has precisely the property $(G/G')^x = G^x G'/G'$, see [18] Section IV.§3, Proposition 14. Here $\psi : [0, \infty] \to [0, \infty]$ is a convex piecewise linear homeomorphism called the *Hasse–Herbrand* function. Its inverse $\varphi : [0, \infty] \to [0, \infty]$ can be defined in terms of the indices of the ramification groups by

$$\varphi(x) = 1/[G_0 : G_1] + \ldots + 1/[G_0 : G_n] + (x - n)/[G_0 : G_{n+1}], \quad n \leq x \leq n + 1.$$

Knowing the ramification groups of $G/G' = \mathrm{SL}(2, \mathbb{F}_3)$ already, and using the Hasse–Herbrand function, one computes the desired ramification groups for G as in the statement. □

We now can compute the behavior of the wild part of the conductor under base changes contained in L:

Proposition 11.6. *Suppose the wild part of the conductor for E_K is $\delta = 1$. Let $G' \subset \mathrm{SL}(2, \mathbb{F}_3)$ be a subgroup, and $K' \subset L$ be the fixed field of the preimage of G' in G. Then the wild part of the conductor for the induced elliptic curve $E_{K'}$ is given by the following table:*

G'	$\mathrm{SL}(2, \mathbb{F}_3)$	C_6	Q	C_4	C_3	C_2	1
δ'	1	2	3	4	0	6	0

Proof. We may assume $G = \mathrm{SL}(2, \mathbb{F}_3)$. The ramification groups for G' are $G'_i = G' \cap G_i$, and the statement follows by an elementary computation from Proposition 11.5 together with the formula (20). Consider, for example, the case $G' = C_4$. Then we have $G'_0 = C_4$ and $G'_1 = C_4$, $G'_2 = G'_3 = C_2$ and $G'_4 = 0$, consequently $\delta' = 1/1 \cdot 2 + 1/2 \cdot 2 + 1/2 \cdot 2 = 4$. □

Now let $G' \subset G \subset \mathrm{SL}(2, \mathbb{F}_3)$ be two subgroups so that $G' \subset G$ has index two. Then the extension of fixed fields $F \subset F'$ is cyclic of degree two. Let $R_F \subset R_{F'}$ be the corresponding extension of discrete valuation rings. To control Weierstrass equations, it will later be useful to express the uniformizer of R_F in terms of the uniformizer of $R_{F'}$. Luckily, the situation is as simple as possible:

Proposition 11.7. *Suppose that E_K has $\delta = 1$, and let $u \in R_F$ be a uniformizer. Then there is a uniformizer $s \in R_{F'}$ and a nonzero scalar $\lambda \in k$ with $u = s^2/(\lambda - s)$.*

Proof. The isomorphism class of $F \subset F'$ corresponds to an element from the cohomology group $H^1(F, \mathbb{Z}/2\mathbb{Z}) = F/\wp(F)$, $\wp(g) = g^2 - g$, which we identify with the group of odd polynomials f in u^{-1}. Let $f = \lambda_{1-2n}u^{1-2n} + \ldots + \lambda_{-1}u^{-1}$ be the odd polynomial for $F \subset F'$, with $n \geq 1$ and $\lambda_{1-2n} \neq 0$. Then $R_{F'} = R_F[s]/(s^2 - u^n s - u^{2n} f)$, and the Galois involution is $s \mapsto s + u^n$. Since $u = s^2 + O(3)$, the ramification groups for G/G' are

$$(G/G')_0 = \ldots = (G/G')_{2n-1} = C_2 \quad \text{and} \quad (G/G')_{2n} = 1.$$

We have to show $n = 1$, or, equivalently $(G/G')_2 = 1$. As explained in the proof of Proposition 11.5, we have to pass to the upper filtration and determine the Hasse–Herbrand function. In our situation, the Hasse–Herbrand function for G/G' has a unique break point at $x = 2n - 1$.

We now make the computation in the case $G = C_4$, $G' = C_2$, and leave the other cases to the reader. By Proposition 11.5, the ramification groups for G are $G_0 = C_4$, $G_1 = G_2 = G_3 = C_2$ and $G_4 = 1$. We infer that the Hasse–Herbrand function for G/G' has its break point at $x = 1$, and consequently $n = 1$. □

12. The Igusa curve in characteristic three

In this section, we shall analyze the the Néron model $U \to \mathrm{Ig}(3)$ and the resulting possibilities for rational points of order three with nonzero specialization in the Néron model. First note that the j-map $j : \mathrm{Ig}(3) \to \mathbb{P}^1$, having degree $1 = (3-1)/2$, is an isomorphism. Second note that there is only one supersingular point $x \in \mathrm{Ig}(3)$, which has j-value $j(x) = 0$. So we may identify $\mathrm{Ig}(3)^{\mathrm{ord}} = \mathbb{A}^1 - \{0\} = \mathrm{Spec}(A)$, where $A = k[t^{\pm 1}]$ is the ring of Laurent polynomials, and t is a uniformizer at $j = 0$. Since $\mathrm{Pic}(A) = 0$, the universal elliptic curve U^{ord} must admit a global Weierstrass equation over A:

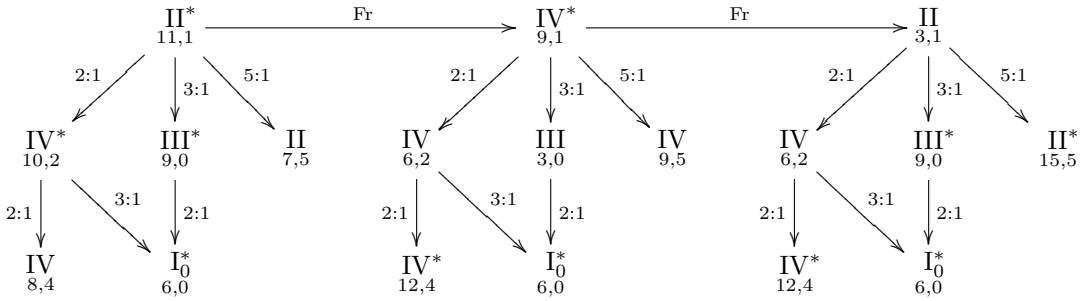
Proposition 12.1. *The universal elliptic curve U^{ord} has as global Weierstrass equation $y^2 + xy = x^3 - 1/t$ over A. At the supersingular point $x \in \mathrm{Ig}(3)$, the reduction type is II^*, the valuation of a minimal discriminant is $\nu(\Delta) = 11$, and the wild part of the conductor is $\delta = 1$.*

Proof. The given Weierstrass equation has j-invariant $j = t$ and discriminant $1/t$. Whence it differs from the universal elliptic curve by a quadratic twist. Using inversion and duplication formula, we see that the Frobenius pullback $y^2 + txy = x^3 - t^3$ admits a rational point of order three, namely $x = t$, $y = 0$. Since a nontrivial quadratic twist destroys this rational point, we conclude that U^{ord} is actually given by this Weierstrass equation. The remaining statements follow from the Tate Algorithm and Ogg's Formula. □

Remark 12.2. The universal curve over $\mathrm{Ig}(3)$ has already been determined in [23], Proposition 2.3. For the sake of completeness we decided to include a proof in our setup.

Now set $R = k[[t]]$ and consider the induced elliptic curve U_K over $K = k((t))$. Since $\delta = 1$, our results form the preceding section apply. The goal now is to construct elliptic curves so that the rational points of order three on the Frobenius pullbacks have nonzero specialization in the Néron model. We can compute

the behavior of $U_{K'} = U_K \otimes K'$ for various base changes $K \subset K'$ of successive degrees $d = 2, 3, 5$. using Lemma 11.1 and Proposition 11.6. Our findings are best summarized in a family tree:



Here the two numbers below the Kodaira symbols denote the valuation of a minimal discriminant $\nu(\Delta)$ and the wild part of the conductor δ, and the $3:1$ extensions are obtained by adjoining the root of the cubic $x^3 + t^2x^2 - t^5$ (compare Corollary 11.4). Note that $s = t^2/x$, which satisfies the integral equation $s^3 - ts - t$ or equivalently $t = s^3/(s+1)$, is a uniformizer for the corresponding discrete valuation ring.

It turns out that the rational 3-division points occurring in the Frobenius pullbacks have nonzero specialization in the Néron models. To verify this, we compute the minimal Weierstrass equations for the $U_{K'} = U_K \otimes K'$, using the substitutions $t = t'^2$, $t = t'^5$ or $t = t'^3/(1+t')$:

minimal Weierstrass equation	$\nu(\Delta)$	δ	type	j
$y^2 + txy = x^3 - t^5$	11	1	II*	t
$y^2 + txy = x^3 - t^4$	10	2	IV*	t^2
$y^2 + txy = x^3 - t^2$	8	4	IV	t^4
$y^2 + txy = x^3 - t$	7	5	II	t^5
$y^2 + txy = x^3 - t^3(1+t)$	9	0	III*	$t^3/(1+t)$
$y^2 + txy = x^3 - t^2x$	6	0	I_0^*	$t^6/(1+t^2)$
$y^2 + txy + t^2y = x^3$	9	1	IV*	t^3
$y^2 + txy + ty = x^3$	6	2	IV	t^6
$y^2 + t^2xy + t^2y = x^3$	12	4	IV*	t^{12}
$y^2 + t^2xy + ty = x^3$	9	5	IV	t^{15}
$y^2 + txy + (1+t)y = x^3$	3	0	III	$t^9/(1+t)^3$
$y^2 + t^2xy + (1+t^2)y = x^3$	6	0	I_0^*	$t^{18}/(1+t^2)^3$
$y^2 + txy + y = x^3$	3	1	II	t^9
$y^2 + t^2xy + y = x^3$	6	2	IV	t^{18}
$y^2 + t^4xy + y = x^3$	12	4	IV*	t^{36}
$y^2 + t^5xy + y = x^3$	15	5	II*	t^{45}
$y^2 + t^3xy + (1+t)^3y = x^3$	9	0	III*	$t^{27}/(1+t^9)$
$y^2 + t^5xy = x^3 - t^2x$	6	0	I_0^*	$t^{54}/(1+t^{18})$

For such families, it is easy to determine the specialization behavior of points of order three:

Proposition 12.3. *Let E_A be an elliptic curve over an arbitrary ring A of characteristic three. Then E_A admits a section whose fibers are rational 3-division points if and only if it admits a global Weierstrass equation of the form $y^2 + a_1xy + a_3y = x^3$*

for some units $a_1, a_3 \in A$. One such section of order three is then given by $x = y = 0$.

Proof. The condition is necessary, because the Frobenius pullback of U^{ord} admits the Weierstrass equation $y^2 + txy + t^2y = x^3$. The sufficiency follows from the duplication and the inversion formula. □

As an immediate consequence:

Corollary 12.4. *Suppose $y^2 + a_1xy + a_3y = x^3$ is a minimal Weierstrass equation with nonzero $a_1, a_3 \in R$. Then the rational 3-division points on E_K have nonzero specialization in the closed fiber of the Néron model. Moreover, we have $a_3 \in \mathfrak{m}_R$ if and only if the rational 3-division points have nonzero class in Φ_k.*

Proof. Clearly, the point $z = (0, 0) \in E_K$ of order three does not specialize to infinity in the Weierstrass model, whence has nonzero specialization into the Néron model. Moreover, z has nonzero class in Φ_k if and only if it specializes into the singularity of the Weierstrass model. The latter is given by $x = 0$, $y = -a_3$, and the result follows. □

Examining our table above, we obtain the following result:

Theorem 12.5. *For the Kodaira symbols* II, II^*, III, III^*, IV, IV^*, I_0^*, *there is an elliptic curve E_K containing a rational 3-division point with nonzero specialization in E_k and the given reduction type. For* IV *and* IV^*, *there are such examples with nonzero specialization in Φ_k, and examples with zero specialization in Φ_k.*

We close this section by discussing the elliptic curves

$$E_{n,K} : y^2 + t^{2^n}xy + t^{2^{n+1}}y = x^3, \quad n \geq 0$$

which contain a rational 3-divsion point. They are obtained from the Frobenius pullback of the universal elliptic curve by the base change of degree 2^n. Let $\nu(\Delta)$ be the valuation of a minimal discriminant for $E_{n,K}$

Proposition 12.6. *If n is odd, then $\nu(\Delta) = 2^n + 4$ and the reduction type of $E_{n,K}$ is* IV. *If n is even, then $\nu(\Delta) = 2^n + 8$, and the reduction type is* IV^*. *In any case, $\delta = 2^n$, and the rational 3-division points have nonzero specialization in Φ_k.*

Proof. We have $\delta = 2^n$ by Lemma 11.1. Suppose n is odd. Then $3 \mid 2^{n+1} - 1$, and E_K is given by the integral Weierstrass equation $y^2 + t^{2^n-(2^{n+1}-1)/3}xy + ty = x^3$, whose discriminant has valuation $2^n + 4$. Ogg's Formula implies that the latter Weierstrass equation is minimal, and that the reduction type is IV. Corollary 12.4 shows that the rational 3-division points have nonzero class in Φ_k. The argument for n even is similar. □

We see that the property of having a rational 3-division point with nonzero class in Φ_k can be preserved under base changes of arbitrarily large degree.

13. The Igusa stack in characteristic two

In this section, $A = k[t^{\pm 1}]$ denotes the ring of Laurent polynomials over an algebraically closed field k of characteristic $p = 2$. We shall analyze the Igusa stack $\mathrm{Ig}(2) \to \mathrm{Spec}(A)$, and in particular the reduction types of tautological families.

Here a family of elliptic curves E_A over A is called a *tautological family* if $j(E_A) = t$. For example, the Weierstrass equation

$$y^2 + xy = x^3 + a_2x^2 + t^{-1} \tag{21}$$

has j-invariant $j = t$ and discriminant $\Delta = 1/t$, and hence yields a tautological family. Note that this is independent of the coefficient $a_2 \in A$.

When we regard a tautological family as an object in the Igusa stack, we also call it a *tautological object*. The existence of tautological objects shows that the $\{\pm 1\}$-gerbe $\mathrm{Ig}(2) \to \mathrm{Spec}(A)$ is trivial, that is, isomorphic to the classifying stack $B(\mathbb{Z}/2\mathbb{Z})$. In some sense, tautological objects are the best replacement, in a stack theoretical context, for the universal object. To understand the set of tautological objects, consider the map

$$\tau : A \longrightarrow \mathrm{Ig}(2)_A, \quad a_2 \longmapsto E : y^2 + xy = x^3 + a_2x^2 + t^{-1}$$

from the group of polynomials into the set of tautological objects of the Igusa stack. Let $A_{\mathrm{odd}} \subset A$ be the vector space of all odd Laurent polynomials.

Proposition 13.1. *The map τ induces a bijection between the group A_{odd} of odd Laurent polynomials and the set of isomorphism classes of tautological objects in the stack* $\mathrm{Ig}(2)$.

Proof. Consider the additive map $\wp : A \to A$, $f \mapsto f^2 - f$. Using that k is algebraically closed, we easily see that the canonical projection

$$A_{\mathrm{odd}} \longrightarrow H^1(A, \mathbb{Z}/2\mathbb{Z}) = A/\wp(A)$$

is bijective. To proceed, let E_A be the tautological family given by the Weierstrass equation (21). It remains to see that given $a_2 \in A_{\mathrm{odd}}$, the corresponding quadratic twist of E_A is given by the Weierstrass equation $y^2 + xy = x^3 + a_2x^2 + t^{-1}$. We sketch the argument: The sign involution acts on E_A via $y \mapsto y + x$, and the Galois involution acts on $A[u]/(u^2 - u - a_2)$ via $u \mapsto u + 1$. Whence $y' = y + xu$ and $x' = x$ are invariant under the diagonal action, and indeed yield the desired Weierstrass equation. □

Our next task is to determine the reduction types at $t = 0$. Let $a_2 \in A_{\mathrm{odd}}$ be an odd Laurent polynomial, and write its vanishing order at $t = 0$ in the form $\nu(a_2) = -2d - 1$. In other words, we have

$$a_2 = t^{-2d-1}f^2$$

for some integer d and some polynomial $f \in k[t]$ that has nonzero constant term or is the zero polynomial. In the latter case we take it that $d = -\infty$.

Proposition 13.2. *Let E_A be the tautological family $y^2 + xy = x^3 + a_2x^2 + t^{-1}$.*

(i) *If $d < 0$, then the reduction type of E_A at $t = 0$ is II^*, the valuation of a minimal discriminant is $\nu(\Delta) = 11$, and the wild part of the conductor is $\delta = 1$.*

(ii) *If $d \geq 0$, then the reduction type at $t = 0$ is I^*_{8d+3}, the valuation of a minimal discriminant is $\nu(\Delta) = 12d+11$, and the wild part of the conductor is $\delta = 4d + 2$.*

Proof. We may replace the ring of Laurent polynomials by the field of formal Laurent series $K = k((t))$. Suppose that $d < 0$, such that $a_2 \in k[[t]]$. Since all power series vanish in $H^1(K, \mathbb{Z}/2\mathbb{Z}) = K/\wp(K)$, $\wp(f) = f^2 - f$, we may as well assume

that $a_2 = 0$. Then $y^2 + txy = x^3 + t^5$ is a minimal Weierstrass equation for E_K, and statement (i) immediately follows from the Tate Algorithm.

Now suppose $d \geq 0$. Then $f \in k[[t]]$ is a unit; set $g = 1/f$. Starting with the original Weierstrass equation, we make the substitution $x = (gt^{d+1})^{-2}x' + gt^d$, and obtain a new Weierstrass equation

$$y^2 + (gt^{d+1})xy + (g^4t^{4d+3})y = x^3 + (t + g^3t^{3d+2})x^2 + (g^6t^{6d+4})x + (g^9t^{9d+6}).$$

The coefficients of this Weierstrass equation satisfy the assumption of Lemma 13.6 below, which tells us that the last Weierstrass equation is minimal, and that the reduction type is I^*_{8d+3}. The remaining statements follow from Ogg's Formula. □

We next consider Frobenius pullbacks of our tautological families:

Proposition 13.3. *Let E_A be the tautological family $y^2 + xy = x^3 + a_2x^2 + t^{-1}$. Then the 2-torsion section on the Frobenius pullback $E_A^{(2)}$ has nonzero specialization in the component group Φ_k at $t = 0$. Moreover:*

(i) *If $d < 0$, then the reduction type is III^*, the valuation of a minimal discriminant is $\nu(\Delta) = 10$, and the wild part of the conductor is $\delta = 1$.*

(ii) *If $d \geq 0$, then the reduction type is I^*_{8d+2}, the valuation of the minimal discriminant is $\nu(\Delta) = 12d + 10$, and the wild part of the conductor is $\delta = 4d + 2$.*

Proof. To check (i), it suffices to treat the case $a_2 = 0$. Then the Weierstrass equation $y^2 + txy = x^3 + t^4$ for $E_A^{(2)}$ must be minimal, because $\nu(\Delta) = 10$, and the result follows from the Tate Algorithm.

We next verify (ii). The Weierstrass equation for the Frobenius pullback is

$$y^2 + xy = x^3 + f^4t^{2(-2d-1)}x^2 + t^{-2}.$$

Again we may replace the ring of Laurent polynomials by the field of formal Laurent series $K = k((t))$, and set $g = 1/f$. Applying successively the substitutions

$$y = y' + f^2t^{-2d-1}x \quad \text{and} \quad x = (gt^{d+1})^{-2}x' \quad \text{and} \quad y = y' + g^3t^{3d+2},$$

we simplify the coefficient of x^2, make the Weierstrass equation integral, and remove the constant term, respectively. The outcome is the new Weierstrass equation

$$y^2 + gt^{d+1}xy = x^3 + tx^2 + t^{4d+3}g^4x.$$

Now Lemma 13.7 below yields (ii).

It remains to prove the statement about the section of order 2. Using that all our minimal Weierstrass equations have $a_3 = a_6 = 0$, we infer that the section of order 2 is given by $x = y = 0$, and hence specializes into the singularity of the Weierstrass model. It follows that its specialization into the component group Φ_k of the Néron model is nontrivial. □

Our final task is to compute the reduction types at $t = \infty$. Changing notation, we write the vanishing order of a_2 at $t = \infty$ in the form $\nu(a_2) = -2d - 1$ for some integer d. In other words, we have $a_2 = t^{2d+1}f^2$ for some integer d and some polynomial $f \in k[t^{-1}]$ that has nonzero constant term or is the zero polynomial.

Proposition 13.4. *Let E_A be the tautological family $y^2 + xy = x^3 + a_2x^2 + t^{-1}$.*

(i) *If $d < 0$, then the reduction type of E_A at $t = \infty$ is I_1, the valuation of a minimal discriminant is $\nu(\Delta) = 1$, and the wild part of the conductor is $\delta = 0$.*

(ii) *If $d \geq 0$, then the reduction type at $t = \infty$ is I^*_{8d+5}, the valuation of a minimal discriminant is $\nu(\Delta) = 12d+13$, and the wild part of the conductor is $\delta = 4d + 2$.*

Proof. The arguments are as in the proof for Proposition 13.2. In case $d \geq 0$, one has to use the substitution $x = (gt^{-d-1})^{-2}x' + gt^{-d-1}$, where $g = f^{-1}$, which yields the minimal Weierstrass equation

$$y^2 + gt^{-d-1}xy + g^4t^{-4d-4}y = x^3 + (t^{-1} + g^3t^{-3d-3})x^2 + g^6t^{-6d-6}x + g^9t^{-9d-9},$$

and Lemma 13.6 yields the result; details are left to the reader. □

With the techniques presented in the proofs of Proposition 13.4 and Proposition 13.3 we obtain:

Proposition 13.5. *Let E_A be the tautological family $y^2 + xy = x^3 + a_2x^2 + t^{-1}$. Then the 2-torsion section on the Frobenius pullback $E_A^{(2)}$ has nonzero specialization in the component group at $t = \infty$. Moreover*

(i) *If $d < 0$, then the reduction type is I_2, the valuation of a minimal discriminant is $\nu(\Delta) = 2$, and the wild part of the conductor is $\delta = 0$.*
(ii) *If $d \geq 0$, then the reduction type is I^*_{8d+6}, the valuation of a minimal discriminant is $\nu(\Delta) = 12d + 14$, and the wild part of the conductor is $\delta = 4d + 2$.*

We summarize our results about tautological families in the following table

around t	d	E_A			$E_A^{(2)}$		
		$\nu(\Delta)$	δ	type	$\nu(\Delta)$	δ	type
$t = 0$	< 0	11	1	II^*	10	1	III^*
	≥ 0	$12d + 11$	$4d + 2$	I^*_{8d+3}	$12d + 10$	$4d + 2$	I^*_{8d+2}
$t = \infty$	< 0	1	0	I_1	2	0	I_2
	≥ 0	$12d + 13$	$4d + 2$	I^*_{8d+5}	$12d + 14$	$4d + 2$	I^*_{8d+6}

In particular, we see that reduction of type I_l^* plays a special role. Note that in characteristic $p \geq 3$ this type of reduction does not appear at all if the Frobenius pullback has a rational p-division point by Corollary 4.5. We will come back to this point in Section 15.

We end the section by the following two technical observations, which are very useful in handling reduction type I_l^*, and have been used in preceding proofs:

Lemma 13.6. *Let E_K be an elliptic curve with Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Set $n = \nu(a_3)$, and assume*

$$\nu(a_1) \geq 1, \quad \nu(a_2) = 1, \quad n = \nu(a_3) \geq 2, \quad \nu(a_4) \geq n, \quad \text{and} \quad \nu(a_6) \geq 2n - 1.$$

Then the Weierstrass equation is minimal, and E_K has reduction type I^*_{2n-3}.

Proof. The Tate Algorithm reveals that the Weierstrass equation is minimal and has reduction type I_l^* for some $l \geq 0$. To determine l, one first blows up the ideal (x, y, t), which defines the reduced singular point, and then the ideal $(y/t, t)$, which defines the reduced fiber. In the chart with coordinate $x/t, y/t^2, t$, the Weierstrass equation transforms into

$$t(y/t^2)^2 + a_1(x/t)(y/t^2) + t^{-1}a_3(y/t^2) = t^3(x/t)^3 + t^{-2}a_4(x/t) + t^{-3}a_6,$$

and the reduced fiber becomes a configuration of 4 copies of $\mathbb{P}^1$ with intersection graph D_4, containing one rational double point. To proceed, one successively blows up the ideals

$$(x/t,t), \quad (y/t^2,t), \quad (x/t^2,t), \quad (y/t^2,t), \quad \dots \quad (y/t^{n-1},t), \quad (x/t^{n-1},t).$$

In other words, one blows up reduced fibers $2n-3$ times. In all but the last blowing ups this introduces on additional copy of $\mathbb{P}^1$ into the fiber, whereas the last blowing up adds two disjoint copies of $\mathbb{P}^1$. In each blowing ups, the coefficients a_i' of the successive equations acquire factors, which are given by the following table:

coefficients	a_1'	a_3'	a_2'	a_4'	a_6'
blowing up of $(x/t^i,t)$	1	$1/t$	t	1	$1/t$
blowing up of $(y/t^{i+1},t)$	1	1	$1/t$	$1/t$	$1/t$

According to our assumptions on the original coefficients a_i, it is indeed possible to carry out the sequence of blowing ups. After the last blowing up, the resulting scheme is regular, and we infer that the reduction type of E_K is I_l^*, where the number of irreducible components is $4 + (2n-4) + 2 = 2n+2$, and therefore $l = 2n-3$. □

Similar arguments yield the next result, whose proof is left to the reader:

Lemma 13.7. *Let E_K be an elliptic curve over the field K with Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Set $n = \nu(a_4)$, and suppose that*

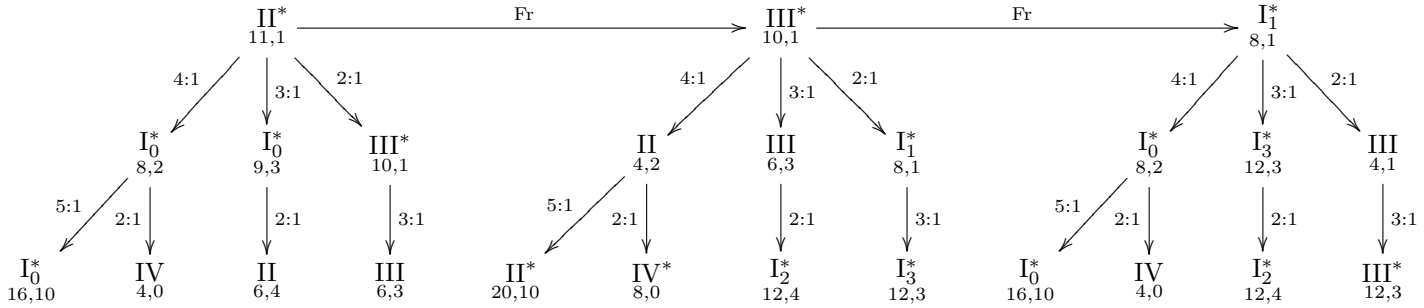
$$\nu(a_1) \geq 1, \quad \nu(a_2) = 1, \quad \nu(a_3) \geq n-1, \quad n = \nu(a_4) \geq 2, \quad \nu(a_6) \geq 2n-1.$$

Then the Weierstrass equation is minimal, and E_K has reduction type I_{2n-4}^*.

14. Other reduction types in characteristic two

We continue to work in characteristic $p = 2$, with $R = k[[t]]$ and $K = k((t))$. In this section, we shall construct elliptic curves whose Frobenius pullbacks have various reduction types and whose rational 2-division point has nonzero specialization.

The starting point is the tautological curve E_K given by $y^2 + xy = x^3 + t^{-1}$, which has minimal Weierstrass equation $y^2 + txy = x^3 + t^5$, numerical invariants $\nu(\delta) = 11$, $\delta = 1$, and reduction type II^*. Applying the results from Section 11, we now examine various pullbacks for successive field extensions of degree $d = 2, 3, 4, 5$. We depict our relevant findings in a family tree:



Here the two numbers below the Kodaira symbols denote the valuation of a minimal discriminant $\nu(\Delta)$ and the wild part of the conductor δ. The quadratic extensions are given by $t = s^2/(1-s)$, and the quartic extension is given by adjoining one root of the quartic $x^4 + t^2x^3 + t^7$, which defines the x-coordinate for one line of points

of order three on E_K. Note that $s = t^2/x$, which satisfies the integral equation $s^4 + ts + t = 0$ or equivalently $t = s^4/(1-s)$ is a uniformizer for the corresponding discrete valuation ring.

The behavior of δ follows from Proposition 11.1, except for the branches starting with an initial base change of degree two; for those, δ must be computed via the Tate Algorithm. We now can tabulate the minimal Weierstrass equations for the induced elliptic curves $E_{K'} = E_K \otimes K'$, using successively the substitutions $t = t'^2/(1-t')$, $t = t'^3$, $t = t'^4/(1-t')$, and $t = t'^5$:

minimal Weierstrass equation	$\nu(\Delta)$	δ	type	j
$y^2 + txy = x^3 + t^5$	11	1	II^*	t
$y^2 + txy = x^3 + t^2(1+t)$	8	2	I_0^*	$t^4/(1+t)$
$y^2 + t^3xy + t^4y = x^3 + t^3$	16	10	I_0^*	$t^{20}/(1+t^5)$
$y^2 + txy + ty = x^3 + x^2 + tx + t^3$	4	0	IV	$t^8/(1+t)^3(1+t+t^2)$
$y^2 + txy = x^3 + t^3$	9	3	I_0^*	t^3
$y^2 + txy = x^3 + (1+t)^3$	6	4	II	$t^6/(1+t^3)$
$y^2 + txy = x^3 + t^4(1+t)$	10	1	III^*	$t^2/(1+t)$
$y^2 + txy = x^3 + tx + t^3$	6	3	III	$t^6/(1+t^3)$
$y^2 + txy = x^3 + t^3x$	10	1	III^*	t^2
$y^2 + txy = x^3 + (1+t)x$	4	2	II	$t^8/(1+t)^2$
$y^2 + t^5xy = x^3 + (1+t^5)x$	20	10	II^*	$t^{40}/(1+t^5)^2$
$y^2 + t^2xy = x^3 + (1+t)^2(1+t^3)x$	8	0	IV^*	$t^{16}/(1+t)^6(1+t+t^2)^2$
$y^2 + txy = x^3 + tx$	6	3	III	t^6
$y^2 + t^2xy = x^3 + t^2(1+t)^3x$	12	4	I_2^*	$t^{12}/(1+t)^6$
$y^2 + txy = x^3 + t^2x$	8	1	I_1^*	$t^4/(1+t^2)$
$y^2 + t^2xy = x^3 + t^2x$	12	8	I_3^*	$t^{12}/(1+t^6)$
$y^2 + txy = x^3 + t^2x$	8	1	I_1^*	t^4
$y^2 + t^2xy = x^3 + (1+t^2)x$	8	2	I_0^*	$t^{16}/(1+t^4)$
$y^2 + t^8xy + t^4y = x^3 + t^6x^2 + t^7x + t^3$	16	10	I_0^*	$t^{80}/(1+t^{20})$
$y^2 + t^3xy + ty = x^3 + t^2x^2 + t^6x + t^4$	4	0	IV	$t^{32}/(1+t)^{12}(1+t+t^2)^4$
$y^2 + t^2xy = x^3 + t^2x$	12	3	I_3^*	t^{12}
$y^2 + t^3xy = x^3 + (1+t)^6x^2$	12	4	I_2^*	$t^{24}/(1+t)^{12}$
$y^2 + txy = x^3 + (1+t^2)x$	4	1	III	$t^8/(1+t^4)$
$y^2 + t^3xy = x^3 + (1+t^6)x$	12	3	III^*	$t^{24}/(1+t^{12})$

For most of these curves, it is easy to determine the behavior of the rational 2-division point. As in Section 12, one proves:

Proposition 14.1. *Let E_A be an elliptic curve over an arbitrary ring A of characteristic two. Then E_A admits a section whose fibers are rational points of order two if and only if it admits a global Weierstrass equation of the form $y^2 + a_1xy = x^3 + a_2x^2 + a_4x$ for some $a_1, a_3, a_4 \in A$ with a_1, a_4 invertible. The section of order two is then given by $x = y = 0$.*

Corollary 14.2. *Suppose $y^2 + a_1xy = x^3 + a_2x^2 + a_4x$ is a minimal Weierstrass equation with nonzero $a_1, a_4 \in R$. Then the rational 2-division point on E_K has nonzero specialization in the closed fiber of the Néron model. Moreover, we have $a_4 \in \mathfrak{m}_R$ if and only if this rational point has nonzero class in Φ_k.*

Theorem 14.3. *For all additive Kodaira symbols, there is an elliptic curve E_K containing a rational point of order two with nonzero specialization in E_k and having the given reduction type. For the Kodaira symbols* III, III*, I$_l^*$, $l \geq 0$, *there are such examples where the specialization has nonzero class in Φ_k, and examples with zero class in Φ_k.*

Proof. For the Kodaira symbols II, II*, III, III*, IV*, the desired examples appear in the table above. To achieve IV, consider the elliptic curve

$$y^2 + txy = x^3 + a_2x^2 + (1+t)x.$$

This has reduction type II for $a_2 = 0$. For $a_2 = t$, the Tate algorithm shows that the reduction type is IV, with $\nu(\Delta) = 4$ and $\delta = 0$.

It remains to treat the cases I$_l^*$. Lemmas 13.6 and 13.7 easily give the following examples, where $n \geq 2$:

minimal Weierstrass equation	type	2-torsion
$y^2 + t^{n-1}xy = x^3 + tx^2 + t^nx$	I^*_{2n-4}	$(0,0)$
$y^2 + t^{n-1}xy + t^{n-1}(1+t)y = x^3 + t(1+t+t^{n-1})x^2 + t^n(1+t)x$	I^*_{2n-4}	$(1+t,(1+t)^2)$
$y^2 + t^{n-1}xy + t^ny = x^3 + tx^2$	I^*_{2n-3}	$(t,0)$
$y^2 + t^nxy + t^n(1+t)y = x^3 + tx^2$	I^*_{2n-3}	$(1+t,1+t)$

□

15. Semistable reduction in characteristic two

Let R be a henselian discrete valuation ring of characteristic $p > 0$, whose residue field $k = R/\mathfrak{m}_R$ is algebraically closed, and with field of fraction $R \subset K$. Let E_K be an elliptic curve with additive reduction so that $E_K^{(p)}$ has a rational p-division point. If $p \geq 3$ then we have seen in Theorem 4.3 and in Section 12 that E_K has potentially supersingular reduction. Although this is not true in characteristic 2, we see that only additive reduction of type I_l^* is possible if the curve is not potentially supersingular.

Proposition 15.1. *Let $p = 2$ and let E_K be an elliptic curve with additive and potentially ordinary reduction. We denote by $\nu(\Delta)$ the valuation of a minimal discriminant and by δ the wild part of the conductor. Then there is an integer $d \geq 0$ and*

E_K			$E_K^{(2)}$		
$\nu(\Delta)$	δ	*type*	$\nu(\Delta)$	δ	*type*
$12d+12$	$4d+2$	I^*_{8d+4}	$12d+12$	$4d+2$	I^*_{8d+4}

and the rational 2-division point on $E_K^{(2)}$ has nonzero specialization into Φ_k.

Proof. We may and will assume $R = k[[t]]$. Since E_K has potentially ordinary reduction, its j-invariant $j = j(E_K)$ lies in $R^\times$ and E_K itself is ordinary. In particular, $X_K : y^2 + xy = x^3 + j^{-1}$ defines an elliptic curve with $j(X_K) = j(E_K)$ and good ordinary reduction. Since E_K is ordinary, its automorphism group is $\{\pm 1\}$ and hence X_K and E_K differ by a quadratic twist. As in the proof of Proposition 13.1 we conclude that E_K is isomorphic to

$$y^2 + xy = x^3 + t^{-2d-1}f^2x^2 + j^{-1}$$

where f is a power series with nonzero constant term. We have $d \geq 0$ because otherwise this curve would have good reduction. For $E_K^{(2)}$ we obtain the reduction type, $\nu(\Delta)$ and δ analogous to Proposition 13.3. The specialization behavior of the 2-torsion point is given by Corollary 14.2. For E_K the Tate Algorithm shows that we have reduction of type I_l^* and $\nu(\Delta) = 12d + 12$. Since $\delta(E_K) = \delta(E_K^{(2)})$, we use Ogg's formula to determine the precise reduction type. □

We leave the remaining case to the reader, which is also a generalization of Proposition 13.4 and Proposition 13.5.

Proposition 15.2. *Let $p = 2$ and let E_K be an elliptic curve with additive and potentially multiplicative reduction. We denote by $\nu(\Delta)$ the valuation of a minimal discriminant and by δ the wild part of the conductor. Then there is an integer $d \geq 0$ and*

E_K			$E_K^{(2)}$		
$\nu(\Delta)$	δ	*type*	$\nu(\Delta)$	δ	*type*
$12d + 12 - \nu(j)$	$4d + 2$	$I^*_{8d+4-\nu(j)}$	$12d + 12 - 2\nu(j)$	$4d + 2$	$I^*_{8d+4-2\nu(j)}$

and the rational 2-division point on $E_K^{(2)}$ has nonzero specialization into Φ_k.

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud: Néron models. Ergeb. Math. Grenzgebiete (3) 21. Springer, Berlin, 1990.

[2] M. Demazure, P. Gabriel: Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs. North-Holland Publishing Co., Amsterdam, 1970.

[3] M. du Sautoy, I. Fesenko: Where the wild things are: ramification groups and the Nottingham group, Progr. Math. 184, 287-328, Birkhäuser, Boston, 2000.

[4] J. Giraud: Cohomologie non abélienne. Grundlehren Math. Wiss. 179. Springer, Berlin, 1971.

[5] A. Grothendieck: A general theory of fibre spaces with structure sheaf. University of Kansas, Department of Mathematics, Report No. 4, 1955.

[6] M. Demazure, A. Grothendieck (eds.): Schémas en groupes II. Lect. Notes Math. 152. Springer, Berlin, 1970.

[7] I. Fesenko, S. Vostokov: Local fields and their extensions. Translations of Mathematical Monographs 121. American Mathematical Society, Providence, RI, 1993.

[8] H. Gunji: The Hasse invariant and p-division points of an elliptic curve. Arch. Math. 27 (1976), 148–158.

[9] J.-I. Igusa: On the algebraic theory of elliptic modular functions. J. Math. Soc. Japan 20 (1968) 96–106.

[10] N. Katz, B. Mazur: Arithmetic moduli of elliptic curves. Annals of Mathematics Studies 108. Princeton University Press, Princeton, 1985.

[11] P. Morandi: Field and Galois theory. Graduate Texts in Mathematics 167. Springer, New York, 1996.

[12] J.-P. Serre: Cohomologie galoisienne. Fifth edition. Lect. Notes Math. 5. Springer, Berlin, 1994.

[13] S. Shatz: Group schemes, formal groups, and p-divisible groups. In: G. Cornell, J. Silverman (eds.), Arithmetic geometry, pp. 29-78. Springer, New York, 1986.

[14] J. Tate, F. Oort: Group schemes of prime order. Ann. Sci. Éc. Norm. Supér. 3, 1–21 (1970).

[15] M. Raynaud: Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. Fr. 102 (1974), 241–280.

[16] S. Schröer: Some Calabi–Yau threefolds with obstructed deformations over the Witt vectors. Compositio Math. 140 (2004), 1579–1592.

[17] J.-P. Serre, J. Tate: Good reduction of abelian varieties. Ann. Math. 88 (1968), 492–517.

[18] J.-P. Serre: Local fields. Grad. Texts Math. 67. Springer, Berlin, 1979.

[19] S. Shatz:. Finite subschemes of group schemes. Canad. J. Math. 22 (1970), 1079–1081.
[20] J. Silverman: The arithmetic of elliptic curves. Grad. Texts Math. 106. Springer, Berlin, 1986.
[21] J. Silverman: Advanced topics in the arithmetic of elliptic curves. Grad. Texts Math. 151. Springer, New York etc., 1994.
[22] J. Tate: Algorithm for determining the type of a singular fiber in an elliptic pencil. In: B. Birch, W. Kuyk (eds.), Modular functions of one variable, IV, pp. 33–52. Lecture Notes in Math. 476. Springer, Berlin, 1975.
[23] D. Ulmer: On universal elliptic curves over Igusa curves. Invent. Math. 99 (1990), 377–391.

Mathematisches Institut, Heinrich-Heine-Universität, Universitätsstr. 1, 40225 Düsseldorf, Germany

Current address: Department of Mathematics, Stanford University, 450 Serra Mall, Stanford CA 94305, USA

E-mail address: liedtke@math.stanford.edu

Mathematisches Institut, Heinrich-Heine-Universität, Universitätsstr. 1, 40225 Düsseldorf, Germany

E-mail address: schroeer@math.uni-duesseldorf.de