REDUCTION AND ISOGENIES OF ELLIPTIC CURVES

MENTZELOS MELISTAS

Abstract. Let R be a complete discrete valuation ring with fraction field K and perfect residue field k of characteristic $p > 0$. Let E/K be an elliptic curve with a K-rational isogeny of prime degree ℓ. In this article, we study the possible Kodaira types of reduction that E/K can have. We also prove some related results for elliptic curves over $\mathbb{Q}$.

1. Introduction

Let K be a number field and let E/K be an elliptic curve. A K-rational isogeny ϕ of E/K is an isogeny $\phi : E \longrightarrow E'$ which is defined over K, for some elliptic curve E'/K. The study of K-rational isogenies of elliptic curves (and their possible degrees) for different number fields K is a rich topic with a long history (see e.g. [10], [14], [6], [13]). In this paper we are interested in answering the following related question; Given an elliptic curve E/K with a cyclic K-rational isogeny of prime degree, then can we say anything about the reduction properties of E/K? To be more precise, if E/K is an elliptic curve with a K-rational isogeny of prime degree $\ell > 3$, then we are interested in the possible Kodaira types of reduction that can occur. The reduction properties of elliptic curves with complex multiplication and of elliptic curves with torsion points have been previously studied by the author in [11] and [12], respectively.

Since determining the reduction type of an elliptic curve is a problem of local nature, we can consider elliptic curves over complete discrete valuation rings. Our main result is the following theorem, proved in the next section.

Theorem 1.1. *Let R be a complete discrete valuation ring with fraction field K and perfect residue field k of characteristic $p > 3$. Let E/K be an elliptic curve with a K-rational isogeny of prime degree $\ell > 3$ such that $p \neq \ell$.*

(i) If $\ell - 1 \equiv 2$ or $10 \,(mod\ 12)$, then E/K has either semi-stable reduction or reduction of type I_n^* for some $n \geq 0$.

(ii) If $\ell - 1 \equiv 4$ or $8 \,(mod\ 12)$, then E/K has either semi-stable reduction or reduction of type III, III*, or I_n^* for some $n \geq 0$.

(iii) If $\ell - 1 \equiv 6 \,(mod\ 12)$, then E/K cannot have reduction of type III or III*.

We present some examples (see Examples 2.5, 2.6, as well as the paragraph before them) showing that all Kodaira types that appear in Parts (i) and (ii) Theorem 1.1 do indeed occur. We also prove a partial analog (see Theorem 2.8 below) of Theorem 1.1 when $p = 2$ or 3 and we explain, in Remark 2.4, why the restriction that $\ell > 3$ is natural in the context of Theorem 1.1. We note that Theorem 1.1 is false when $\ell = p$. Indeed, in Example 2.9 below we present examples of elliptic curves $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational isogeny of degree $\ell = 5$ that have modulo 5 reduction of type II, II*, III, III*, IV, IV*, I_0^*, I_1^*, and I_1.

Date: October 25, 2023.

We now turn our attention to elliptic curves over $\mathbb{Q}$. In this case, a celebrated theorem of Mazur (see [10, Theorem 1]) provides a classification for the possible prime degrees of $\mathbb{Q}$-rational isogenies. Namely, if $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational isogeny of prime degree ℓ, then $\ell \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$. A selection of our results from Section 3 concerning elliptic curves over $\mathbb{Q}$ is the following theorem (See Theorems 3.3, 3.4. 3.6, and 3.7 below).

Theorem 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational isogeny of prime degree ℓ.*

(i) If $\ell = 11, 19, 43, 67,$ or 163, and p is a prime such that $p \neq 2, \ell$, then $E/\mathbb{Q}$ has either good reduction or reduction of type I_0^* modulo p.

(ii) If $\ell = 19, 43, 67,$ or 163, then $E/\mathbb{Q}$ has reduction of type III or III* modulo ℓ.

(iii) If $\ell = 11, 19, 37, 43, 67,$ or 163, then $E/\mathbb{Q}$ has either good redcution or reduction of type II or II* modulo 2.

(iv) If $\ell = 17$ or 37 and $p \neq 2, 5, 7, 17$ is a prime, then $E/\mathbb{Q}$ has either good reduction or reduction of type III, III*, or I_0^* modulo p.

For the prime numbers ℓ treated in Theorem 1.2 we also classify the possible reduction types modulo 2 and modulo ℓ in Section 3. Moreover, by following the proof of each part of Theorem 1.2, which involves the computation of the possible Kodaira types of elliptic curves with a fixed j-invariant, we can see that in fact all allowed Kodaira types do indeed occur.

This article is organized as follows. In Section 2, after recalling some background material, we prove Theorem 1.1. Then we present some examples showing that all Kodaira types that appear in Parts (*i*) and (*ii*) Theorem 1.1 do indeed occur. Finally, Section 3 is devoted to elliptic curves over $\mathbb{Q}$ and Theorem 1.2 is proved.

Acknowledgement. The author was supported by Czech Science Foundation (GAČR) grant 21-00420M and by Charles University Research Center program No.UNCE/SCI/022.

2. Proof of Theorem 1.1

Let R be a complete discrete valuation ring with valuation v, fraction field K, and perfect residue field k of characteristic $p > 0$. Let K^{s} be a fixed separable closure of K and let $G_K = \mathrm{Gal}(K^{\mathrm{s}}/K)$. Assume that E/K has a cyclic K-rational isogeny ϕ of prime degree $\ell > 3$ with kernel denoted by C. We assume that $\ell \neq p$ throughout this section. Let $P \in E[\ell]$ be a generator for C. Write L/K for the minimal field of definition of the point P, i.e., L is the field obtained by adjoining the coordinates of P to the field K. Extend P to a basis $\{P, Q\}$ of $E[\ell]$ and denote $\bar{\rho}_{E,\ell} : G_K \longrightarrow \mathrm{GL}(\mathbb{F}_\ell)$ the mod ℓ representation of E/K with respect to the basis $\{P, Q\}$. Let B be the Borel subgroup of $\mathrm{GL}(\mathbb{F}_\ell)$, i.e.,

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{F}_\ell \text{ and } ad \neq 0 \right\},$$

and let B_1 be the subgroup

$$B_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} : b, d \in \mathbb{F}_\ell \text{ and } d \neq 0 \right\}.$$

Using Galois theory we can prove the following (see also [2, Lemma 3.1]).

Lemma 2.1. *The degree of the extension L/K divides $\ell - 1$.*

Proof. Since the isogeny ϕ is defined over K, we have that $\bar{\rho}_{E,\ell}(G_K)$ is a subgroup of B. Therefore, it follows from Galois theory that

$$[L:K] = [B \cap \bar{\rho}_{E,\ell}(G_K) : B_1 \cap \bar{\rho}_{E,\ell}(G_K)] = [\bar{\rho}_{E,\ell}(G_K) : B_1 \cap \bar{\rho}_{E,\ell}(G_K)],$$

which divides $[B : B_1] = \ell - 1$.

□

Denote by E_L/L the base extension of E/K to L. The following lemma will be useful in our proofs below.

Lemma 2.2. *Then the curve E_L/L has semi-stable reduction.*

Proof. Assume that E_L/L does not have semi-stable reduction and we will find a contradiction. Consequently, we assume from now on that E_L/L has additive reduction. Let R_L be the integral closure of R in L, which is again a discrete valuation ring because R is complete, and denote by k_L its residue field. Pick a minimal Weierstrass equation for E_L/L and denote by $\widetilde{E_L}/k_L$ the corresponding reduction. Denote also by $(E_L)_0(L)$ the set of points with nonsingular reduction and by $(E_L)_1(L)$ the kernel of the reduction map.

It follows from [19, Proposition VII.2.1], that there exists a short exact sequence of abelian groups

$$0 \longrightarrow (E_L)_1(L) \longrightarrow (E_L)_0(L) \longrightarrow (\widetilde{E_L})_{\mathrm{ns}}(k_L) \longrightarrow 0,$$

where $(\widetilde{E_L})_{\mathrm{ns}}(k_L)$ is the set of non-singular points of $\widetilde{E_L}/k_L$ and the right-hand map is the reduction map. Consider now the point $P \in E_L(L)$, which has order ℓ. We will first show that $P \notin (E_L)_0(L)$. Suppose that $P \in (E_L)_0(L)$, and we will find a contradiction. Since ℓ is coprime to p and P has order ℓ, we find, using [19, Proposition VII.3.1], that $P \notin (E_L)_1(L)$. Therefore, if $P \in (E_L)_0(L)$, then we must have that the reduction of P must have order ℓ in $(\widetilde{E_L})_{\mathrm{ns}}(k_L)$. However, by [19, Exercise III.3.5] we see that $(\widetilde{E_L})_{\mathrm{ns}}(k_L)$ is the additive group $\mathbb{G}_{\mathrm{a}}(k_L)$, where $\mathbb{G}_{\mathrm{a}}/k_L$ is the additive group scheme over k_L. Since $\mathbb{G}_{\mathrm{a}}(k_L)$ has no points of order ℓ, we see that $P \notin (E_L)_0(L)$.

Finally, if E_L/L has additive reduction, then, using [18, Corollary IV.9.2] (or [20]), we find that the group $E_L(L)/(E_L)_0(L)$ has order at most 4. However, since $P \notin (E_L)_0(L)$, we must have that $E_L(L)/(E_L)_0(L)$ has order divisible by the prime ℓ, which is bigger than 3. This is a contradiction and, hence, E_L/L has semi-stable reduction. This completes the proof of our claim.

□

Theorem 2.3. *Let R be a complete discrete valuation ring with valuation v, fraction field K, and perfect residue field k of characteristic $p > 0$. Let E/K be an elliptic curve with potentially good reduction and a K-rational isogeny of prime degree $\ell > 3$ with $\ell \neq p$. Denote by $\Delta_{E/K}$ the discriminant of a minimal Weierstrass equation for E/K. Then*

$$12 \text{ divides } (\ell - 1)v(\Delta_{E/K}).$$

Proof. Assume that E/K has a cyclic K-rational isogeny of degree ℓ with kernel denoted by C. Let $P \in E[\ell]$ be a generator for C. Write L/K for the minimal field of definition of the point P.

Let R_L be the integral closure of R in L, which is again a discrete valuation ring because R is complete. We denote by v_L the associated (normalized) valuation of R_L. Note that the restriction $v_L|K$ of v_L to K satisfies $v_L|_K = ev$ where e is the ramification index of L/K. By Lemma 2.2 the curve E_L/L has semi-stable reduction. Therefore, since we assume that E/K has potentially good reduction, we find that E_L/L has good reduction. Thus, if $\Delta_{E_L/L}$ is the discriminant of a minimal Weierstrass equation of E_L/L, then we must have that $v_L(\Delta_{E_L/L}) = 0$.

On the other hand, $\Delta_{E/K}$ is the discriminant of a (not necessarily minimal) Weierstrass equation for E_L/L. Since when we perform a change of variable the valuation of the discriminant changes by a factor of 12, we see that 12 divides $v_L(\Delta_{E_L/L}) - v_L(\Delta_{E/K})$. However, from the previous paragraph we have that $v_L(\Delta_{E_L/L}) = 0$ and, hence, 12 divides $v_L(\Delta_{E/K}) = ev(\Delta_{E/K})$. Moreover, it follows from Lemma 2.1 that the degree of the extension L/K divides $\ell - 1$. Therefore, we find that e divides $\ell - 1$ and, hence, we see that 12 divides $(\ell - 1)v(\Delta_{E/K})$. □

We are now ready to proceed to the proof of Theorem 1.1.

Proof of Theorem 1.1. Assume that E/K has a cyclic K-rational isogeny of degree p with kernel denoted by C. Let $P \in E[\ell]$ be a generator for C. Write L/K for the minimal field of definition of the point P. Lemma 2.1 tells us that $[L : K]$ divides $\ell - 1$ while Lemma 2.2 tells us that the base extension E_L/L of E/K to L has semi-stable reduction.

If E_L/L has multiplicative reduction, then using Tate's algorithm [20], since $p > 3$, we find that that E/K has either multiplicative reduction or reduction of type I_n^*, for some $n \geq 0$. We assume from now on that E_L/L has good reduction.

Proof of (i)*:* Assume that $\ell - 1 \equiv 2$ or $10 \pmod{12}$. Denote by $\Delta_{E/K}$ the discriminant of a minimal Weierstrass equation for E/K. Theorem 2.3 tells us that 12 divides $(\ell - 1)v(\Delta_{E/K})$. Since $\ell - 1 \equiv 2$ or $10 \pmod{12}$, we find that

$$0 \equiv (\ell - 1)v(\Delta_{E/K}) \equiv 2v(\Delta_{E/K}) \text{ or } 10v(\Delta_{E/K}) \pmod{12}.$$

Since $p > 3$, this is only possible when $v(\Delta_{E/K}) = 0$ or 6. Therefore, using [18, Page 365], we see that E/K has either good reduction or reduction of type I_0^*. This proves part (i).

Proof of (ii)*:* Assume that $\ell - 1 \equiv 4$ or $8 \pmod{12}$. Denote by $\Delta_{E/K}$ the discriminant of a minimal Weierstrass equation for E/K. Theorem 2.3 tells us that 12 divides $(\ell - 1)v(\Delta_{E/K})$. Since $\ell - 1 \equiv 4$ or $8 \pmod{12}$, we find that

$$0 \equiv (\ell - 1)v(\Delta_{E/K}) \equiv 4v(\Delta_{E/K}) \text{ or } 8v(\Delta_{E/K}) \pmod{12}.$$

Since $p > 3$, this is only possible when $v(\Delta_{E/K}) = 0, 3, 6,$ or 9. Therefore, using [18, Page 365], we find that E/K has either good reduction or reduction of type III, III*, or I_0^*. This proves part (ii).

Proof of (iii)*:* Assume now that $\ell - 1 \equiv 6 \pmod{12}$. Denote by $\Delta_{E/K}$ the discriminant of a minimal Weierstrass equation for E/K. Theorem 2.3 tells us that 12 divides $(\ell - 1)v(\Delta_{E/K})$. Since $\ell - 1 \equiv 6 \pmod{12}$, we find that

$$0 \equiv (\ell - 1)v(\Delta_{E/K}) \equiv 6v(\Delta_{E/K}) \pmod{12}.$$

From this we obtain that $v(\Delta_{E/K}) \neq 3$ or 9. Therefore, using [18, Page 365], we find that E/K cannot have reduction of type III or III*. This completes the proof of our theorem. □

Remark 2.4. We explain in this remark why the restriction that $\ell > 3$ is natural in the context of Theorem 1.1. First, for an elliptic curve E/K having a K-rational isogeny of degree 2 is the same as having a K-rational torsion point of order 2. Thus, studying elliptic curves with an isogeny of degree 2 is the same as studying elliptic curves with a K-rational point of order 2.

On the other hand, it is not hard to show that if an elliptic curve E/K has a K-rational isogeny of degree 3, then a quadratic twist of E/K has a K-rational point of order 3 (see also [17, Exercise 2.6]). Therefore, studying elliptic curves with an isogeny of degree 3 is the same as studying elliptic curves whose twists have a K-rational point of order 3. We note that when the absolute ramification index of K is 1, the possible Kodaira types of reduction of elliptic curves E/K that have a K-rational point of order 3 have been described by Kozuma in [5, Proposition 3.5] and [5, Lemma 3.6].

Let now K be a number field and let E/K be an elliptic curve that has a K-rational isogeny of prime degree $\ell > 3$. Let $\mathfrak{p}$ be a prime of K which lies above a rational prime $p > 3$ with $\ell \neq p$. Assume that E/K has reduction of Kodaira type I_n, for some $n \geq 0$, modulo $\mathfrak{p}$. By performing an appropriate quadratic twist we can construct an elliptic curve E'/K with a K-rational isogeny of degree ℓ and reduction of Kodaira type I_n^* modulo $\mathfrak{p}$ (see [1] for background on Kodaira types of quadratic twists). Thus, the Kodaira types I_n^* that appear in Parts (i) and (ii) of Theorem 1.1 do indeed occur.

The following two examples show that the Kodaira types III and III* allowed by Part (ii) of Theorem 1.1 also occur.

Example 2.5. Consider the elliptic curve $E/\mathbb{Q}$ given by the following Weierstrass equation

$$E \,:\, y^2 + xy + y = x^3 - 190891x - 36002922.$$

This curve has LMFDB [7] label 14450.b1. Using LMFDB it is easy to see that $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational isogeny of degree 17 and that it has reduction of Kodaira type III modulo 5.

Example 2.6. Consider the elliptic curve $E/\mathbb{Q}$ given by the following Weierstrass equation

$$E \,:\, y^2 + xy = x^3 - 16513x - 916983.$$

This curve has LMFDB [7] label 14450.w2 and is a quadratic twist of the elliptic curve with label 14450.b1 considered in the previous example. It is easy to see that $E/\mathbb{Q}$ has a $\mathbb{Q}$-rational isogeny of degree 17 and that it has reduction of Kodaira type III* modulo 5.

The following example illustrates two important aspects related to Theorem 1.1. Firstly, the assumption that $\ell \neq p$ in Theorem 1.1 is necessary as more reduction types can occur. Secondly, when $\ell - 1 \equiv 6 \pmod{12}$ (as is the case for $\ell = 19$ below) then the reduction types II and IV* can indeed occur.

Example 2.7. Consider the elliptic curve $E/\mathbb{Q}(\sqrt{-3})$ given by the following Weierstrass equation

$$E \,:\, y^2 + xy + y = x^3 + (184a - 12)x + 101a + 872,$$

where $a = \frac{1+\sqrt{-3}}{2}$. This curve has LMFDB [7] label 2.0.3.1-61009.7-b1 and has a $\mathbb{Q}(\sqrt{-3})$-rational isogeny of order 19. Denote by $\mathfrak{p}$ and $\mathfrak{q}$ the prime ideals $(4a - 3)$ and $(-5a + 3)$ of the ring of integers of $\mathbb{Q}(\sqrt{-3})$, respectively. Note that $\mathfrak{p}$ lies above 13 and $\mathfrak{q}$ lies above 19. Using the database it is easy to see that $E/\mathbb{Q}(\sqrt{-3})$ has a $\mathbb{Q}(\sqrt{-3})$-rational isogeny of degree 19, bad reduction of Kodaira type IV* modulo $\mathfrak{p}$, and reduction of Kodaira type III modulo $\mathfrak{q}$.

Let $d_1 = 4a - 3$ and $d_2 = -5a + 3$. It follows from [1, Proposition 1] that the quadratic twist $E^{d_1}/\mathbb{Q}(\sqrt{-3})$ of $E/\mathbb{Q}(\sqrt{-3})$ has bad reduction of Kodaira type II modulo $\mathfrak{p}$. Moreover, it follows from [1, Proposition 1] that the quadratic twist $E^{d_2}/\mathbb{Q}(\sqrt{-3})$ of $E/\mathbb{Q}(\sqrt{-3})$ has reduction of Kodaira type III* modulo $\mathfrak{q}$.

Theorem 2.8. *Let R be a complete discrete valuation ring with valuation v, fraction field K of characteristic 0, and perfect residue field k of characteristic $p > 0$. Let E/K be an elliptic curve with a K-rational isogeny of prime degree $\ell > 3$. Assume that $v(p) = 1$.*

(i) If $\ell - 1 \equiv 2, 4, 8,$ or $10 \,(mod\ 12)$ and $p = 2$, then E/K cannot have reduction of type IV or IV.*

(ii) If $\ell - 1 \equiv 2$ or $10\ (mod\ 12)$ and $p = 3$, then E/K has either semi-stable reduction, reduction of type IV or II, or reduction of type I_n^* for some $n \geq 0$.*

Proof. The proof is similar to the proof of Theorem 1.1, using [15] instead of [18, Page 365]. We include all the details here for completeness. Assume that E/K has a cyclic K-rational isogeny of degree p with kernel denoted by C. Let $P \in E[\ell]$ be a generator for C. Write L/K for the minimal field of definition of the point P. Exactly as in the proof of Theorem 1.1, Lemma 2.1 tells us that $[L : K]$ divides $\ell - 1$. Moreover, Lemma 2.2 tells us that the base extension E_L/L of E/K to L has semi-stable reduction. We denote by $\Delta_{E/K}$ the discriminant of a fixed minimal Weierstrass equation for E/K.

Proof of (i)*:* We assume for contradiction that E/K has reduction of type IV or IV*. This implies that E_L/L has good reduction. Assume first that $\ell - 1 \equiv 2$ or $10\,(\text{mod } 12)$. Theorem 2.3 tells us that 12 divides $(\ell - 1)v(\Delta_{E/K})$. Since $\ell - 1 \equiv 2$ or 10 (mod 12), we find that

$$0 \equiv (\ell - 1)v(\Delta_{E/K}) \equiv 2v(\Delta_{E/K}) \text{ or } 10v(\Delta_{E/K}) \text{ (mod 12)}.$$

On the other hand, since $v(2) = 1$ and E/K has reduction of type IV or IV*, by [15, Tableau IV] we have that $v(\Delta_{E/K}) = 4$ or 8, which is a contradiction.

Assume now that $\ell - 1 \equiv 4$ or 8 (mod 12). Theorem 2.3 tells us that 12 divides $(\ell - 1)v(\Delta_{E/K})$. Since $\ell - 1 \equiv 4$ or 8 (mod 12), we find that

$$0 \equiv (\ell - 1)v(\Delta_{E/K}) \equiv 4v(\Delta_{E/K}) \text{ or } 8v(\Delta_{E/K}) \text{ (mod 12)}.$$

On the other hand, since $v(2) = 1$ and E/K has reduction of type IV or IV*, by [15, Tableau IV] we have that $v(\Delta_{E/K}) = 4$ or 8, which is again a contradiction.

Proof of (iii)*:* Proceeding exactly in in part (i) we find that

$$0 \equiv (\ell - 1)v(\Delta_{E/K}) \equiv 2v(\Delta_{E/K}) \text{ or } 10v(\Delta_{E/K}) \text{ (mod 12)}.$$

Therefore, since $v(3) = 1$, by [15, Tableau II] we see that E/K has either semi-stable reduction, reduction of type IV or II*, or reduction of type I_n^* for some $n \geq 0$. This proves our theorem. □

We end this section by explaining why an analog of Theorem 1.1 for $\ell = p$ does not seem to exist. Concerning the case where the characteristic of the field K is 0, even for $K = \mathbb{Q}$ such a pattern does not seem to hold. This is because in Example 2.9 below among other examples we exhibit elliptic curves $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational isogeny of degree $\ell = 5$ that have modulo 5 reduction of type II, II*, III, III*, IV, IV*, I_0^*, I_1^*, and I_1. Thus, we do not see any pattern concerning their reduction types modulo 5.

Example 2.9. Consider the curves with LMFDB labels 75.a2, 50.b1, 175.a2, 150.a1, 50.a1, 50.a2, 275.b1, 550.f1, and 110.b1. Those curves have $\mathbb{Q}$-rational isogeny of degree 5 and reduction modulo 5 of type II, II*, III, III*, IV, IV*, I_0^*, I_1^*, and I_1, respectively.

Suppose now that the characteristic of K is p. Let E/K be any elliptic curve. Extending scalars using the absolute Frobenius $Fr : \mathrm{Spec}(K) \longrightarrow \mathrm{Spec}(K)$, we obtain an elliptic curve $E^{(p)}/K$ and a purely inseparable isogeny $F : E \longrightarrow E^{(p)}$ of degree p. Thus every elliptic curve defined over K has an isogeny of degree p, and, hence, we cannot have any restrictions on the reduction properties of elliptic curves with an isogeny of degree p. To remedy this problem one could restrict to separable isogenies. However, we note that given any isogeny ϕ of degree p and dual isogeny $\hat{\phi}$, the facts that $\phi \circ \hat{\phi} = [p]$ and that $[p]$ is inseparable in characteristic p combined imply that either ϕ or $\hat{\phi}$ is inseparable.

3. Elliptic curves over $\mathbb{Q}$

In this section, we focus on elliptic curves over $\mathbb{Q}$ and we prove Theorem 1.2. Before we proceed to our proofs we briefly explain our general strategy. A similar strategy has been employed by Trbović in [21] to compute Tamagawa numbers of elliptic curves with isogenies. Let $\ell \geq 11$ be a prime and consider the modular curve $X_0(\ell)/\mathbb{Q}$ parametrizing elliptic curves together with an isogeny of degree ℓ (see [3] and [16] for general background on modular curves). In [9, Table 4], we can find the j-invariants corresponding to non-cuspidal $\mathbb{Q}$-rational points of $X_0(\ell)/\mathbb{Q}$, i.e., the j-invariants of elliptic curves defined over $\mathbb{Q}$ that have a $\mathbb{Q}$-rational isogeny of degree ℓ.

Moreover, according to [19, Corollary X.5.4.1] all elliptic curves having the same j-invariant are twists of each other. Since all these j-invariants coming from [9, Table 4], are not equal to 0 or 1728, we need to consider only quadratic twists. Finally, we will use results on reduction types of quadratic twists of elliptic curves.

If $E/\mathbb{Q}$ is an elliptic curve and d is a square-free integer, then we will denote by $E^d/\mathbb{Q}$ the quadratic twist of $E/\mathbb{Q}$ by d. We recall now some of the results from [1] for future reference.

Lemma 3.1. *(See* [1, Proposition 1]*) Let $E/\mathbb{Q}$ be an elliptic curve and d a square-free integer. If $p \neq 2$ is a prime with $p \mid d$, then the reduction types of $E/\mathbb{Q}$ and $E^d/\mathbb{Q}$ modulo p are related as follows*

Reduction type of $E/\mathbb{Q}$ modulo p	*Reduction type of $E^d/\mathbb{Q}$ modulo p*
I_0	I_0^*
I_n	I_n^*
II	IV^*
III	III^*
IV	II^*
I_0^*	I_0
II^*	IV
III^*	III
IV^*	II

Keeping the same notation as in the previous lemma, it is well known that if $p \neq 2$ and $p \nmid d$, then the reduction types of $E/\mathbb{Q}$ and $E^d/\mathbb{Q}$ modulo p are the same. We will also need the following lemma.

Lemma 3.2. *Let $E/\mathbb{Q}$ be an elliptic curve and d be a squarefree number.*

(i) If $E/\mathbb{Q}$ has good reduction modulo 2, then $E^d/\mathbb{Q}$ has either good reduction or reduction of type I_4^*, I_8^*, II, or II^* modulo 2.

(ii) If $E/\mathbb{Q}$ has modulo 2 reduction of type I_n for some $n \geq 0$, then $E^d/\mathbb{Q}$ has modulo 2 either reduction of type I_n or reduction of type I_m^*, where m is equal to either $n+4$ or $n+8$.

Proof. Both of these statements are well known to the experts. We include some references here for completeness. Part (i) follows from either [1, Table I] and [1, Table II], or, alternatively, by [4, Table 3] and keeping in mind that $E^d/\mathbb{Q}$ acquires good reduction after at most a quadratic extension. On the other hand, Part (ii) follows from a theorem of Lorenzini [8, Theorem 2.8]) □

We are now ready to proceed with our proofs.

Theorem 3.3. *Let ℓ be equal to $19, 43, 67$, or 163. Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational isogeny of prime degree ℓ.*

(i) If $p \neq 2, \ell$ is a prime, then $E/\mathbb{Q}$ has either good reduction or reduction of type I_0^* modulo p.
(ii) The curve $E/\mathbb{Q}$ has reduction of type III or III* modulo ℓ.
(iii) The curve $E/\mathbb{Q}$ has either good reduction or reduction of type I_4^*, I_8^*, II, or II* modulo 2.

Proof. Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree ℓ and let $p \neq 2, \ell$ be a prime number. We will proceed with a case by case analysis.

Assume first that $\ell = 19$. From [9, Table 4] we see that if $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 19, then its j-invariant is equal to $-2^{15} \cdot 3^3$. The curve E_1 with LMFDB label 361.a2 is a curve with the smallest conductor in the twist class with j-invariant $-2^{15}3^3$. Using the LMFDB database it is easy to see that $E_1/\mathbb{Q}$ has good reduction away from 19 and that it has reduction of type III modulo 19. Let now $E/\mathbb{Q}$ be an elliptic curve with $j(E) = -2^{15} \cdot 3^3$. Since $j(E) = -2^{15} \cdot 3^3 \neq 0, 1728$, it follows from [19, Corollary X.5.4.1] that there exists a square-free d such that $E/\mathbb{Q}$ is isomorphic over $\mathbb{Q}$ to $E_1^d/\mathbb{Q}$.

If now $p \nmid d$, then $E_1^d/\mathbb{Q}$ and, hence, $E/\mathbb{Q}$ has good reduction modulo p. On the other hand, if $p \mid d$, then it follows from Lemma 3.1 that $E/\mathbb{Q}$ has reduction of type I_0^* modulo p. Moreover, if $19 \nmid d$, then $E/\mathbb{Q}$ has reduction of type III modulo 19 while if $19 \mid d$, then, by Lemma 3.1, we obtain that $E/\mathbb{Q}$ has reduction of type III* modulo 19. Finally, since the curve $E_1/\mathbb{Q}$ has good reduction modulo 2, using Part (i) of Lemma 3.2, we find that $E/\mathbb{Q}$ has either good reduction or reduction of type I_4^*, I_8^*, II, or II* modulo 2.

Assume that $\ell = 43$. From [9, Table 4] we see that if $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 43, then its j-invariant is equal to $-2^{18} \cdot 3^3 \cdot 5^3$. The curve E_1 with LMFDB label 1849.b2 is a curve with the smallest conductor in the twist class with j-invariant $-2^{18} \cdot 3^3 \cdot 5^3$. Using the LMFDB database it is easy to see that $E_1/\mathbb{Q}$ has good reduction away from 43 and that it has reduction of type III modulo 43. Since $j(E) = -2^{18} \cdot 3^3 \cdot 5^3 \neq 0, 1728$, it follows from [19, Corollary X.5.4.1] that there exists a square-free d such that $E/\mathbb{Q}$ is $\mathbb{Q}$-isomorphic to $E_1^d/\mathbb{Q}$.

If now $p \nmid d$, then $E/\mathbb{Q}$ has good reduction modulo p. On the other hand, if $p \mid d$, then it follows from Lemma 3.1 that $E/\mathbb{Q}$ has reduction of type I_0^* modulo p. Moreover, if $43 \nmid d$, then $E/\mathbb{Q}$ has reduction of type III modulo 43 while if $43 \mid d$, then, by Lemma 3.1, we find that $E/\mathbb{Q}$ has reduction of type III* modulo 43. Finally, the curve $E_1/\mathbb{Q}$ has good reduction modulo 2 and we find on the LMFDB database a minimal Weierstrass equation. Since the

b_2 invariant is even, using Part (i) of Lemma 3.2 we find that $E/\mathbb{Q}$ has either good reduction or reduction of type I_4^*, I_8^*, II, or II* modulo 2.

Assume that $\ell = 67$. From [9, Table 4] we see that if $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 67, then its j-invariant is equal to $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$. The curve E_1 with LMFDB label 4489.b2 is a curve with the smallest conductor in the twist class with j-invariant $-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$. Using the LMFDB database it is easy to see that $E_1/\mathbb{Q}$ has good reduction away from 67 and that it has reduction of type III modulo 67. The rest of the proof from the previous case carries over verbatim in this case. We will not reproduce the details.

Assume that $\ell = 163$. From [9, Table 4] we see that if $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 163, then its j-invariant is equal to $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$. The curve E_1 with LMFDB label 26569.a2 is a curve with the smallest conductor in the twist class with j-invariant $-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$. Using the LMFDB database it is easy to see that $E_1/\mathbb{Q}$ has good reduction away from 163 and that it has reduction of type III modulo 163. The rest of the proof from the previous case carries over verbatim in this case so we will not reproduce the details. This completes the proof of our theorem. □

Theorem 3.4. *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree* 11.

(i) If $p \neq 2, 11$ is a prime, then $E/\mathbb{Q}$ has either good reduction or reduction of type I_0^* modulo p.

(ii) The curve $E/\mathbb{Q}$ has reduction of type II, II*, III, III*, IV, or IV* modulo 11.

(iii) The curve $E/\mathbb{Q}$ has either good reduction or reduction of type I_4^*, I_8^*, II, or II* modulo 2.

Proof. Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 11 and let $p \neq 2, 11$ be a prime number. From [9, Table 4] we see that if $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 11, then its j-invariant is equal to $-11 \cdot 131^3$, -2^{15}, or -11^2. The curves with LMFDB labels, denoted by $E_1/\mathbb{Q}$, $E_2/\mathbb{Q}$, $E_3/\mathbb{Q}$, respectively, 121.a2, 121.b2, 121.c2 are curves with the smallest conductors in each twist class corresponding to j-invariant $-11\cdot 131^3$, -2^{15}, and -11^2, respectively. It is easy to check, using the LMFDB database, that all these curves have good reduction away from 11. It follows from [19, Corollary X.5.4.1] that there exists a square-free d such that $E/\mathbb{Q}$ is $\mathbb{Q}$-isomorphic to either $E_1^d/\mathbb{Q}$, $E_2^d/\mathbb{Q}$, or $E_3^d/\mathbb{Q}$. If $p \nmid d$, then $E/\mathbb{Q}$ has good reduction modulo p. On the other hand, if $p \mid d$, then it follows from [1, Proposition 1] that $E/\mathbb{Q}$ has reduction of type I_0^* modulo p.

Moreover, the curves $E_1/\mathbb{Q}$, $E_2/\mathbb{Q}$, and $E_3/\mathbb{Q}$ have reduction of type II, III, and IV modulo 11, respectively. Therefore, we see from Lemma 3.1 that $E/\mathbb{Q}$ has reduction of type II, II*, III, III*, IV, or IV* modulo 11. Finally, since $E_1/\mathbb{Q}$, $E_2/\mathbb{Q}$, and $E_3/\mathbb{Q}$ all have good reduction modulo 2, using Lemma 3.2 we find that $E/\mathbb{Q}$ has either good reduction or reduction of type I_4^*, I_8^*, II, or II* modulo 2. □

Example 3.5. Consider the elliptic curves with LMFDB labels 121.a2, 121.a1, 121.b2, 121.b1, 1089.c2, and 1089.c1. Those curves have $\mathbb{Q}$-rational isogeny of degree 11 and reduction modulo 11 of type II, II*, III, III*, IV, and IV*, respectively.

Theorem 3.6. *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree* 17.

(i) If $p \neq 2, 5, 17$ is a prime, then $E/\mathbb{Q}$ has either good reduction or reduction of type I_0^* modulo p.

(ii) The curve $E/\mathbb{Q}$ has reduction of type I_1, I_{17}, I_5^*, I_9^*, I_{21}^*, or I_{25}^* modulo 2.
(iii) The curve $E/\mathbb{Q}$ has reduction of type III or III* modulo 5.
(iv) The curve $E/\mathbb{Q}$ has reduction of type II, II*, IV, or IV* modulo 17.

Proof. Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 17. From [9, Table 4] we see that if $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 17, then its j-invariant is equal to $-\frac{17^2 \cdot 101^3}{2}$ or $-\frac{17 \cdot 373^3}{2^{17}}$. The curves with LMFDB labels 14450.b2 and 14450.b1, denoted by $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$, respectively, are curves with the smallest conductors in each twist class corresponding to j-invariant $-\frac{17^2 \cdot 101^3}{2}$ and $-\frac{17 \cdot 373^3}{2^{17}}$, respectively. Using the LMFDB database it is easy to see that each of those curves has good reduction away from $2, 5$ and 17. Therefore, proceeding similarly as in the proofs of the previous theorems in this section, we can show that $E/\mathbb{Q}$ has either good reduction or reduction of type I_0^* modulo p, for p a prime such that $p \neq 2, 5, 17$. The curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have reduction of type III modulo 5. Therefore, $E/\mathbb{Q}$ can only have reduction of type III or III* modulo 5.

Moreover, using the LMFDB database we see that the curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have reduction of type IV and IV* modulo 17, respectively. Thus, using Lemma 3.1 we find that the curve $E/\mathbb{Q}$ has reduction of type II, II*, IV, or IV* modulo 17. Finally, the curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have reduction of type I_1 and I_{17} modulo 2, respectively. Therefore, using Lemma 3.2 we find that $E/\mathbb{Q}$ has reduction of type I_1, I_{17}, I_5^*, I_9^*, I_{21}^*, or I_{25}^* modulo 2. □

Theorem 3.7. *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree* 37.

(i) If $p \neq 2, 5, 7$ is a prime, then $E/\mathbb{Q}$ has either good reduction or reduction of type I_0^* modulo p.
(ii) The curve $E/\mathbb{Q}$ has either good reduction or reduction of type I_4^*, I_8^*, II, or II* modulo 2.
(iii) The curve $E/\mathbb{Q}$ has reduction of type III or III* modulo 5.
(iv) The curve $E/\mathbb{Q}$ has reduction of type II or IV* modulo 7.

Proof. Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 37. From [9, Table 4] we see that if $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 37, then its j-invariant is equal to $-7 \cdot 11^3$ or $-7 \cdot 137^3 \cdot 2083^3$. The curves with LMFDB labels 1225.b2 and 1225.b1, denoted by $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$, respectively, are curves with the smallest conductors in each twist class corresponding to j-invariant $-7 \cdot 11^3$ and $-7 \cdot 137^3 \cdot 2083^3$, respectively. Using the LMFDB database it is easy to see that each of those curves has good reduction away from 5 and 7. Therefore, proceeding similarly as in the proofs of the previous theorems in this section, we can show that $E/\mathbb{Q}$ has either good reduction or reduction of type I_0^* modulo p, for p a prime such that $p \neq 5, 7$.

On the other hand, the curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have reduction of type III modulo 5. Therefore, $E/\mathbb{Q}$ can only have reduction of type III or III* modulo 5. Finally, both curves $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ have reduction of type II modulo 7. Therefore, $E/\mathbb{Q}$ can only have reduction of type II or IV* modulo 7. Finally, since $E_1/\mathbb{Q}$ has good reduction modulo 2, using Lemma 3.2 we find that $E/\mathbb{Q}$ has either good reduction or reduction of type I_4^*, I_8^*, II, or II* modulo 2. □

Remark 3.8. Given any primes p, ℓ with $p \neq 2$ and any reduction type T that appears in Theorem 3.3, 3.4. 3.6, or 3.7, then by using an appropriate quadratic twist one can find an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree ℓ and reduction type T modulo p. For example, suppose we are looking for an elliptic curve $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational isogeny of degree 17 and reduction of Kodaira type III* modulo 5. The curve $E_1/\mathbb{Q}$ with LMFDB label 14450.b2, which appears in the proof of Theorem 3.6, is an elliptic curve with a $\mathbb{Q}$-rational isogeny of degree 17 and reduction of Kodaira type III modulo 5. Therefore, it follows from Lemma 3.1 that the quadratic twist $E_1^5/\mathbb{Q}$ is an elliptic curve with reduction of Kodaira type III* modulo 5 and it has a $\mathbb{Q}$-rational isogeny of degree 17. Thus we have found an example with the required properties. We can proceed in a similar way for the other choices of primes p, ℓ, and Kodaira types T.

References

[1] S. Comalada. Twists and reduction of an elliptic curve. *J. Number Theory*, 49(1):45–62, 1994. 5, 6, 7, 8, 9

[2] J. E. Cremona and F. Najman. $\mathbb{Q}$-curves over odd degree number fields. *Res. Number Theory*, 7(4):30, 2021. 2

[3] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985. 7

[4] M. Kida. Variation of the reduction type of elliptic curves under small base change with wild ramification. *Cent. Eur. J. Math.*, 1(4):510–560, 2003. 8

[5] R. Kozuma. A note on elliptic curves with a rational 3-torsion point. *Rocky Mountain J. Math.*, 40(4):1227–1255, 2010. 5

[6] E. Larson and D. Vaintrob. Determinants of subquotients of Galois representations associated with abelian varieties. *J. Inst. Math. Jussieu*, 13(3):517–559, 2014. With an appendix by Brian Conrad. 1

[7] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2019. [Online; accessed 11 November 2022]. 5

[8] D. Lorenzini. Models of curves and wild ramification. *Pure Appl. Math. Q.*, 6(1, Special Issue: In honor of John Tate. Part 2):41–82, 2010. 8

[9] Á. Lozano-Robledo. On the field of definition of p-torsion points on elliptic curves over the rationals. *Math. Ann.*, 357(1):279–305, 2013. 7, 8, 9, 10

[10] B. Mazur. Rational isogenies of prime degree. (With an appendix by D. Goldfeld). *Invent. Math.*, 44:129–162, 1978. 1, 2

[11] M. Melistas. Reduction types of CM curves. Preprint. 1

[12] M. Melistas. Purely additive reduction of abelian varieties with torsion. *J. Number Theory*, 239:21–39, 2022. 1

[13] P. Michaud-Jacobs. On elliptic curves with p-isogenies over quadratic fields. *Can. J. Math.*, 75(3):945–964, 2023. 1

[14] F. Momose. Isogenies of prime degree over number fields. *Compos. Math.*, 97(3):329–348, 1995. 1

[15] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *J. Number Theory*, 44(2):119–152, 1993. 6

[16] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publ. Math. Soc. Japan*. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971. 7

[17] S. Siksek. Explicit arithmetic of modular curves. `https://homepages.warwick.ac.uk/~maseap/teaching/modcurves/l` Notes for the 2019 CMI-HIMR summer school in computational number theory. 5

[18] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. 3, 4, 6

[19] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009. 3, 7, 8, 9

[20] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476, 1975. 3, 4

[21] A. Trbović. Tamagawa numbers of elliptic curves with prescribed torsion subgroup or isogeny. *J. Number Theory*, 234:74–94, 2022. 7

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 18600 Praha 8, Czech Republic

University of Twente, Department of Applied Mathematics, Drienerlolaan 5, 7522 NB Enschede, The Netherlands