.

ELLIPTIC CURVES OVER THE RATIONAL NUMBERS WITH SEMI-ABELIAN REDUCTION AND TWO-DIVISION POINTS

STEFAN SCHRÖER

Revised Version, 18 August 2020

Abstract. We classify elliptic curves over the rationals whose Néron model over the integers is semi-abelian, with good reduction at $p = 2$, and whose Mordell–Weil group contains an element of order two that stays non-trivial at $p = 2$. Furthermore, we describe those curves where the element of order two is narrow, or where another element of order two exists, and also express our findings in terms of Deligne–Mumford stacks of pointed curves of genus one.

Contents

Introduction

Fontaine [4] proved that there are no abelian varieties $A_{\mathbb{Q}} \neq 0$ over the field of rationals that have good reduction everywhere. The case of elliptic curves $E_{\mathbb{Q}}$ is due to Ogg [14], who attributed the result to Tate. His proof proceeds by showing that any Weierstraß equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with integral coefficients has discriminant $\Delta \neq \pm 1$. Ogg actually classified, up to isomorphism, those $E_{\mathbb{Q}}$ where bad reduction occurs only at $p = 2$. It turns out that there are twelve cases, all of the form $y^2 = x^3 + mx^2 + nx$ with discriminant $\Delta = \pm 2^v$, for certain coefficients $-12 \leq m, n \leq 12$ and exponents $6 \leq v \leq 15$. One observes that there is always a 2-division point, that is, a non-zero rational point of order two, with coordinates $x = y = 0$.

Similar questions where treated in many subsequent papers. We just mention a few: Ogg himself analyzed elliptic curves with discriminant $\pm 2^\nu \cdot 3$ and $\pm 2^\nu \cdot 3^2$ in [15]. The case $\Delta = \pm 2^\nu \cdot p$ was studied by Ivorra [11], those with $\Delta = p_1p_2$ by Sadek [17]. Ogg's results where extended to imaginary quadratic number fields by Setzer [23], Stroecker [24] and Kida [12]. Zhao [30] studied elliptic curves E_K with good reduction everywhere over real quadratic number fields, and Takeshi [26]

2010 *Mathematics Subject Classification.* 14H52, 14G05, 14G25.

investigated the case of cubic number fields. The reduction behavior of an elliptic curve $E_{\mathbb{Q}}$ with a 2-division point was studied by Hadano [7].

The goal of this paper is to classify elliptic curves $E_{\mathbb{Q}}$ that have a 2-division point $P \in E(\mathbb{Z})$, and satisfy certain additional conditions. Here $E \to \operatorname{Spec}(\mathbb{Z})$ is the Néron model, and $E(\mathbb{Z}) = E(\mathbb{Q}) = E_{\mathbb{Q}}(\mathbb{Q})$ is the *Mordell–Weil group*, which is a finitely generated abelian group. My personal motivation is to study the arithmetic of families of elliptic surfaces, in particular Enriques surfaces [20], but the results seem to be of independent interest. The additional conditions considered here are as follows: *We stipulate that the relative group scheme E is semi-abelian, that good reduction occurs at $p = 2$, and that the 2-division point $P \in E(\mathbb{Z})$ stays non-trivial in $E(\mathbb{F}_2)$.*

It turns out that there are infinitely many isomorphism classes. We show that they correspond to pairs of integers (m, n) with n odd and $\gcd(4m + 1, n) = 1$, via the Weierstraß equations $y^2 + xy = x^3 + mx^2 + nx$ (see Theorem 2.1). We then describes the situation when there is further 2-division, which is our first main result:

Theorem. (See Theorem 3.8) *The following are equivalent:*

(i) *There is another element $Q \neq P$ of order two in $E(\mathbb{Z})$.*
(ii) *The relative group scheme $E[2]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mu_2$.*
(iii) *For every prime $p > 0$, the fiber $E \otimes \mathbb{F}_p$ has even Kodaira symbol.*
(iv) *We have $n = -d(4m + 1 + 16d)$ for some odd d with $\gcd(4m + 1, d) = 1$.*

I find it quit remarkable that the existence of $Q \neq P$ can be seen as a condition on relative group schemes, or Kodaira symbols, or the arithmetic of the numbers m and n.

Now recall that $P \subset E$ is called *narrow* it it passes through the same irreducible components of the closed fibers as the zero-section $O \subset E$, compare for example [21], Section 6.7. If we stipulate that our $P \subset E$ is narrow, the above list becomes finite. The second main results of the paper is:

Theorem. (See Theorem 5.1) *Up to isomorphism, there are exactly two elliptic curves $E_{\mathbb{Q}}$ such that its Néron model E has the following properties:*

(i) *The structure morphism $E \to \operatorname{Spec}(\mathbb{Z})$ is semi-abelian.*
(ii) *The closed fiber $E \otimes \mathbb{F}_2$ is an elliptic curve.*
(iii) *There is a narrow element $P \in E(\mathbb{Z})$ of order two whose image in $E(\mathbb{F}_2)$ is non-zero, and another element $Q \neq P$ of order two.*

These curves are given by $y^2 + xy = x^3 + 4nx^2 + nx$ for the coefficient $n = \pm 1$.

Taking the quotient by the subgroup scheme $\mu_2 \subset E$ yields two other elliptic curves, which must be of the form $y^2 + xy = x^3 + m'x^2 + n'x$. Somewhat surprisingly, they can be characterized via elements $R \in E(\mathbb{Z})$ of order four, which is the content of the third main result (see Theorem 5.2). We also reformulate some of our findings in terms of of $\mathbb{Z}$-valued objects in the Deligne–Mumford stack $\bar{\mathscr{M}}_{g,r}$ of stable pointed curves of genus $g = 1$.

The paper is organized as follows: Section 1 contains basic facts on Néron models of elliptic curves, and elementary computations with Weierstraß equations. In Section 2, we show how certain geometric assumptions on Néron models lead to our Weierstraß equations. A detailed analysis of the resulting Weierstraß models is

given in Section 3, which also contains the result on the existence of an additional element of order two. In Section 4 we apply Velu's formula to form some quotients by 2-division points. Section 5 contains our classification results that use additional narrowness assumptions. The final Section 6 gives reinterpretations in terms of Deligne–Mumford stacks.

Acknowledgement. I wish to thank the referee for valuable suggestions. This research was conducted in the framework of the research training group *GRK 2240: Algebro-geometric Methods in Algebra, Arithmetic and Topology*, which is funded by the Deutsche Forschungsgemeinschaft.

1. Preliminaries

Here we discuss basic facts on Néron models of elliptic curves and make some useful elementary computations with Weierstraß equations. We refer to the monograph of Bosch, Lütkebohmert and Raynaud for more details ([1], Section 1.5 in particular). Let R be a Dedekind ring, which we regard as a ground ring, $F = \mathrm{Frac}(R)$ its field of fractions, and

$$E_F: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

be an elliptic curve with coefficients $a_i \in F$. The homogenization of the Weierstraß equation yields a closed embedding $E_F \subset \mathbb{P}^2_F$, where the origin $O_F \in E_F$ corresponds to the point $(0:1:0) \in \mathbb{P}^2(F)$.

Let X' be the resolution of singularities for the closure of the subset $E_F \subset \mathbb{P}^2_R$, which we assume to exist. The closure of the origin defines a section $O' \subset X'$. Note that almost all closed fibers are irreducible. According to [18], Corollary 2.3 there is a contraction $X' \to Y$ that contracts the irreducible components of the closed fibers that are disjoint from O'. Then the image of $O' \subset X'$ on Y is an relatively ample effective Cartier divisor, and it follows that

$$Y = P(X', O') = \mathrm{Proj} \bigoplus_{t \geq 0} H^0(X', \mathscr{O}_{X'}(tO')).$$

This scheme is called the *Weierstraß model* of the elliptic curve $E_{\mathbb{Q}}$. Each fiber of $Y \to \mathrm{Spec}(R)$ is either an elliptic curves, or a twisted from of the rational nodal curve or the rational cuspidal curve. The *locus of non-smoothness* $\mathrm{Sing}(Y/R)$, which is defined by the first Fitting ideal for the sheaf $\Omega^1_{Y/R}$ (compare [3], Section 2), comprises finitely many closed points.

The minimal resolution of singularities $X \to Y$ is called the *minimal model* of the elliptic curve E_F. The locus of smoothness $E = \mathrm{Reg}(X/R)$ is the *Néron model* of the elliptic curve E_F. If the residue fields $R/\mathfrak{m}$ are perfect, this follows from [1], Section 1 in Section 1.5, together with Theorem 1 in Section 7.2. The general case follows from [25], Proposition 7.1.1. The Néron model has the property that the restriction map $E(R) \to E(\mathbb{Q})$ is bijective. The resulting abelian group

$$E(R) = E(F) = E_F(F)$$

is called the *Mordell–Weil group*. The Néron model $E \to \mathrm{Spec}(R)$ acquires in a canonical way the structure of a relative group scheme. We write $O \subset E$ for the zero-section. For each point $a \in \mathrm{Spec}(R)$, the fiber $E_a = E \otimes \kappa(a)$ is an algebraic

group scheme. We write $E_a^0 \subset E_a$ for the connected component of the origin, and $\Phi_a = E_a/E_a^0$ for the resulting group scheme of components. If the fiber E_a is an elliptic curve, one says that $E_{\mathbb{Q}}$ has *good reduction* at $a \in \mathrm{Spec}(R)$. If E_a^0 is a twisted form of $\mathbb{G}_m \otimes \kappa(a)$, one says that $E_{\mathbb{Q}}$ has *multiplicative reduction*. One says that the Néron model E is *semi-abelian* if the elliptic curve $E_{\mathbb{Q}}$ has good reduction or multiplicative reduction at all closed points.

An element $P \in E(R)$ is called *narrow* if its images in Φ_a vanishes, for all closed points $a \in \mathrm{Spec}(R)$. In other words, the section $P, O \subset E$ pass through the same irreducible components inside each closed fiber E_a.

There is an open covering $D(f_1) \cup \ldots \cup D(f_n)$ of $\mathrm{Spec}(R)$ such that each restriction $Y \otimes R[1/f_i]$ is defined by some equation (1) with coefficients $a_i \in R[1/f_i]$ as a family of cubic curves in $\mathbb{P}^2 \otimes R[1/f_i]$. In general, it is impossible to find a global embedding $Y \subset \mathbb{P}^2$. However, making a substitution $x = u^2x'$ and $y = u^3y'$ with $u \in F^\times$ we obtain a Weierstraß equation (1) with coefficients $a_i \in R$. Such a Weierstraß equation is called *globally minimal* if the resulting family of cubics is isomorphic to $Y \to \mathrm{Spec}(R)$.

If the Dedekind ring R is local, that is, a discrete valuation ring, the *Tate Algorithm* [27] produces a minimal Weierstraß equation, at least if the residue field is perfect. Every round of the algorithm consists of twelve steps, each involving a change of coordinates $x = u^2x' + r$ and $y = u^3y' + su^2x' + t$, with $u \in R^\times$ and $r, s, t \in R$, to produces new equations. If the situation $\mathrm{val}(a_i) \geq i$ arises, one replaces the coefficients by a_i/π^i, where $\pi \in R$ is the uniformizer, and starts a new round. If not, the Weierstraß equation is minimal and indeed describes Y. It the ring R is factorial, one actually may run the Tate Algorithm locally and thus obtains a globally minimal Weierstraß equation.

Lemma 1.1. *Suppose the Weierstraß equation (1) has coefficients $a_i \in R$ and that the values $c_4, \Delta \in R$ generate the unit ideal. Then the Weierstraß equation is globally minimal, the Néron model $E \to \mathrm{Spec}(R)$ is semi-abelian, and the closed fibers E_a have Kodaira symbol I_v, with $v = \mathrm{val}_a(\Delta)$.*

Proof. The problem is local, so we may assume that R is a discrete valuation ring, say with uniformizer $\pi \in R$. Seeking a contradiction, we assume that the Weierstraß equation is not minimal. Then there is a change of coordinates $x = u^2x' + r$, $y = u^3y' + usx' + t$ over the field $F = \mathrm{Frac}(R)$ such that the new Weierstraß equation has coefficients in R, with $\mathrm{val}(\Delta') = \mathrm{val}(\Delta) - 12$. Then $\mathrm{val}(c_4') = \mathrm{val}(c_4) - 4$. In particular $\Delta, c_4 \in \mathfrak{m}_R$, contradiction. Thus the equation is minimal. According to [2], Proposition 5.1 the closed fiber is elliptic or multiplicative. In other words, the Kodaira symbol is I_v for some $v \geq 0$. By the first step in the Tate Algorithm, we actually have $v = \mathrm{val}(\Delta)$. □

We now state two observations for Weierstraß equations and the resulting families of cubics $Y \subset \mathbb{P}^2$ that are valid over arbitrary ground rings R.

Lemma 1.2. *For each Weierstraß equation of the form $y^2 + xy = x^3 + a_2x^2 + a_4x$, the two ideals (Δ, c_4) and $(4a_2 + 1, a_4)$ in the ring R have the same radical ideal.*

Proof. It suffices to treat the case that the ground ring $R = k$ is an algebraically closed field, say of characteristic $p \geq 0$. According to [2], Proposition 5.1 the cubic

$Y \subset \mathbb{P}^2$ is the rational cuspidal curve if and only if the $\Delta = c_4 = 0$. Using for example [9], we compute for our Weierstraß equation the values

$$\Delta = a_4^2((4a_2+1)^2 - 64a_4) \quad \text{and} \quad c_4 = (4a_2+1)^2 - 48a_4. \tag{2}$$

These two equations combined give the relation

$$\Delta = a_4^2(c_4 - 16a_4). \tag{3}$$

Obviously, the vanishing of $4a_2+1$ and a_4 implies the vanishing of Δ and c_4. Conversely, suppose that $\Delta = c_4 = 0$. We conclude $a_4 = 0$ in characteristic $p \neq 2$ from (3), and for $p = 2$ from the first equation in (2). The second equation finally gives $4a_2 + 1 = 0$. □

Lemma 1.3. *Let $a_2, a_4, a_2', a_4' \in R$. Suppose the two Weierstraß equations*

$$y^2 + xy = x^3 + a_2x^2 + a_4x \quad \text{and} \quad y^2 + xy = x^3 + a_2'x^2 + a_4'x$$

are related by a change of coordinates that respects $P = (0,0)$. Suppose the ring R has the property that $2 \in R$ is a regular element and $R^\times \cap (1+2R) = \{\pm 1\}$. Then the equations coincide, and the change of coordinates is either the identity or the sign involution $x = x'$, $y = -y' - x'$.

Proof. Write $x = u^2x' + r$ and $y = u^3y' + su^2x' + t$. Comparing coefficients for $a_1 = a_1' = 1$ gives $u = 1 + 2s$, which means $u = s = -1$ or $u = 1$, $s = 0$. Composing with the sign involution if necessary, we may assume that the latter holds. Since $P = (0,0)$ is fixed, we also have $r = t = 0$. □

2. From geometry to equations

Let $E_{\mathbb{Q}}$ be an elliptic curve over the field of rationals $\mathbb{Q}$, and $E \to S$ be the Néron model over $S = \operatorname{Spec}(\mathbb{Z})$. Write $O \subset E$ for the zero-section, $X \to S$ for the minimal model, and $Y \to S$ for the Weierstraß model. The goal of this section is to establish the following:

Theorem 2.1. *Suppose the elliptic curve $E_{\mathbb{Q}}$ satisfies the following three conditions:*

(i) *The Néron model $E \to \operatorname{Spec}(\mathbb{Z})$ is semi-abelian.*
(ii) *The closed fiber $E \otimes \mathbb{F}_2$ is an elliptic curve.*
(iii) *There is an element $P \in E(\mathbb{Z})$ of order two whose image in the group $E(\mathbb{F}_2)$ remains non-zero.*

Then there are integers $m, n \in \mathbb{Z}$ with n odd and $\gcd(4m+1, n) = 1$ such that the Weierstraß model is given by $y^2 + xy = x^3 + mx^2 + nx$, and the section $P \subset Y$ is defined by the equations $x = y = 0$. Moreover, these integers m, n are unique, and we have $P \cap O = \varnothing$.

The proof is given at the end of this section, after a few preparations. Since the ring $\mathbb{Z}$ is factorial, the Weierstraß model is a closed subscheme $Y \subset \mathbb{P}^2$, and the affine scheme $Y \smallsetminus O \subset \mathbb{A}^2$ is defined by a Weierstraß equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients $a_i \in \mathbb{Z}$. Any two such Weierstraß equations differ by a change of coordinates $x = u^2x' + r$, $y = u^3y' + usx' + t$, with $r, s, t \in \mathbb{Z}$ and $u = \pm 1$, as described in [27], Section 2.

Lemma 2.2. *If the closed fiber $E \otimes \mathbb{F}_2$ is an ordinary elliptic curve, there is a Weierstraß equation with $a_1 = 1$ and $a_3 = 0$.*

Proof. Let us recall from [10], Chapter 3, §6 that up to isomorphism, there are five elliptic curves $E_1, \ldots, E_5$ over the prime field $k = \mathbb{F}_2$. The groups $E_i(k)$ are cyclic, and all $1 \leq n \leq 5$ occur as orders. Let us choose indices in a natural fashion, so that $|E_i(k)| = i$. To be explicit, we write

$$E_1 : y^2 + y = x^3 + x^2 + 1, \quad E_3 : y^2 + y = x^3 \quad \text{and} \quad E_5 : y^2 + y = x^3 + x^2,$$

which are supersingular and have invariant $j = 0$. We are more interested in the ordinary elliptic curves, which have $j = 1$ and are given by

$$E_2 : y^2 + xy = x^3 + x^2 + x \quad \text{and} \quad E_4 : y^2 + xy = x^3 + x. \tag{4}$$

Since we are in characteristic $p = 2$ and the unit group $\mathbb{F}_2^\times$ is trivial, the coefficient $a_1 \in \mathbb{F}_2$ of the Weierstraß equations is invariant under every change of coordinates. For our Néron model $E \to \operatorname{Spec}(\mathbb{Z})$ of the elliptic curve $E_{\mathbb{Q}}$, this means that $a_1 \in \mathbb{Z}$ is odd. A change of coordinates $y = y' + sx'$ achieves $a_1 = 1$. A further change of coordinate $y = y' + t$ then yields $a_3 = 0$ as well. □

Proposition 2.3. *If conditions (ii) and (iii) from Theorem 2.1 hold, one may choose a Weierstraß equation so that $P \subset Y$ is given by $P = (0, 0)$, and the coefficients satisfy $a_1 = 1$ and $a_3 = a_6 = 0$. Furthermore, $a_4 \in \mathbb{Z}$ then must be odd.*

Proof. We saw in the previous proof that the supersingular elliptic curves over $\mathbb{F}_2$ contain no element of order two, hence we may find a Weierstraß of the form $y^2 + xy = x^3 + a_2x^2 + a_4x + a_6$. This form is preserved under each change of coordinates $x = x' - 2t$, $y = y' + t$. Since the subscheme $P \subset Y$ is disjoint from the zero-section, it has coordinates $P = (m, n)$ for some integers $m, n \in \mathbb{Z}$. So after a change of coordinates, we may assume $n = 0$. The sign involution on E is given by $-(x, y) = (x, -y - x)$. For the element $P \in E(\mathbb{Z})$ of order two, this means $(m, 0) = (m, -m)$, thus $m = 0$. Summing up, $x = y = 0$ is a solution for our Weierstraß equation, and this means $a_6 = 0$. Seeking a contradiction, we suppose that a_4 is even. Then the fiber $Y \otimes \mathbb{F}_2$ is given by $y^2 + xy = x^3 + x^2$ or $y^2 + xy = x^3$. Both curves are singular at the point $(0, 0)$, contradiction. □

Proposition 2.4. *Suppose Y is given by a Weierstraß equation of the form $y^2 + xy = x^3 + mx^2 + nx$. Let $p > 0$ be a prime. Then the fiber $E \otimes \mathbb{F}_p$ is additive if and only if we have $p \mid \gcd(4m + 1, n)$.*

Proof. Consider the ideal $\mathfrak{a} = (4m+1, n)$. According to Lemma 1.2, the fiber $E \otimes \mathbb{F}_p$ is additive if and only if $\mathfrak{a} \subset (p)$, or equivalently $p \mid \gcd(4m + 1, n)$. □

Proof of Theorem 2.1: Suppose we have an elliptic curve $E_{\mathbb{Q}}$ whose Néron model $E \to \operatorname{Spec}(R)$ satisfies conditions (i)–(iii). According to Proposition 2.3, we may choose a Weierstraß equation of the form $y^2 + xy = x^3 + mx^2 + nx$. In light of Proposition 2.4 we have $\gcd(4m + 1, n) = 1$. The coefficients $m, n \in \mathbb{Z}$ are unique by Lemma 1.3. The Weierstraß model $Y \subset \mathbb{P}^2$ is the zero-locus for the homogeneous equation $Y^2Z + XYZ = X^3 + mX^2Z + nXZ^2$. The images of O and P on the Weierstraß model are given by the equations $X = Z = 0$ and $X = Y = 0$, which are clearly disjoint. Thus $O, P \subset E$ are disjoint. □

3. Analysis of the Weierstrass equation

Let $m, n \in \mathbb{Z}$ be two integers with n odd and $\gcd(4m+1, n) = 1$. We now consider the family of cubics $Y \subset \mathbb{P}^2$ defined by the Weierstraß equation

$$y^2 + xy = x^3 + mx^2 + nx. \tag{5}$$

The discriminant $\Delta = n^2((4m+1)^2 - 64n)$ is odd, in particular the generic fiber $E_{\mathbb{Q}} = Y_{\mathbb{Q}}$ is an elliptic curve. Combining Lemma 1.2 and Proposition 1.1, we obtain:

Proposition 3.1. *The Weierstraß equation (5) is globally minimal, and the family of cubics $Y \subset \mathbb{P}^2$ coincides with the Weierstraß model for the elliptic curve $E_{\mathbb{Q}}$.*

Let $E \to \operatorname{Spec}(\mathbb{Z})$ be the Néron model, with zero-section $O \subset E$. The section of the Weierstraß model Y given by $x = y = 0$ induces a section $P \subset E$. The following is an immediate converse for Theorem 2.1:

Proposition 3.2. *The relative group scheme $E \to \operatorname{Spec}(\mathbb{Z})$ is semi-abelian, the element $P \in E(\mathbb{Z})$ has order two, and the section $P \subset E$ is disjoint from the zero-section. The closed fiber $E \otimes \mathbb{F}_2$ is an ordinary elliptic curve, which contains two rational points if m is odd, and four rational points if m is even.*

Proof. The sign involution on E is given by $(x, y) \mapsto (x, -y - x)$, hence the element $P \in E(\mathbb{Z})$ has order two. Obviously, the images $(0 : 1 : 0)$ and $(0 : 0 : 1)$ on the Weierstraß model $Y \subset \mathbb{P}^2$ of the sections $O, P \subset E$ are disjoint, and the closed fiber $E \otimes \mathbb{F}_p$ belongs to the ordinary elliptic curves in (4). The Néron model E is semi-abelian by Proposition 2.4. Obviously, the close fiber $E \otimes \mathbb{F}_2$ occurs in our list of ordinary elliptic curves (4), and the assertion on $E(\mathbb{F}_2)$ is immediate. □

Proposition 3.3. *Let $p > 0$ be a prime. The element $P \in E(\mathbb{Z})$ has non-trivial class in the component group scheme Φ_p if and only if $p \mid n$.*

Proof. The image of $P \in E(\mathbb{Z})$ in the group $\Phi_p(\mathbb{F}_p)$ vanishes if and only if the image of the subscheme $P \subset E$ on the Weierstraß model Y is disjoint from the singular locus $\operatorname{Sing}(Y \otimes \mathbb{F}_p)$. The structure morphism $Y \to \operatorname{Spec}(\mathbb{Z})$ is smooth on some common open neighborhood of the zero-section $O \subset Y$ and the elliptic curve $Y \otimes \mathbb{F}_2$. Hence the locus of non-smoothness $\operatorname{Sing}(Y/\mathbb{Z})$ is the closed subscheme in $\mathbb{A}^2 \otimes \mathbb{Z}[1/2]$ defined by the Weierstraß equation (5) and its partial derivatives

$$2y + x = 0 \quad \text{and} \quad y = 3x^2 + 2mx + n. \tag{6}$$

For later use, we record that $\operatorname{Sing}(Y/\mathbb{Z})$ therefore equals the spectrum of the ring

$$\mathbb{Z}[1/2, x, y]/(2y + x, -8y^3 + (4m+1)y^2 - 2ny, 12y^2 - (4m+1)y + n), \tag{7}$$

which can be seen by substituting $x = -2y$ in the other two equations. By abuse of notation, we now identify the section $P \subset E$ with its image in the Weierstraß model Y, where it is is given by the equation $x = y = 0$. Thus the intersection $P \cap \operatorname{Sing}(Y/\mathbb{Z})$ is defined by the equations (5) and (6), together with $x = y = 0$. Clearly, the is the spectrum of $\mathbb{Z}[1/2]/(n)$, which coincides with $\mathbb{Z}/n\mathbb{Z}$ because n is odd. This shows that P intersects $\operatorname{Sing}(Y \otimes \mathbb{F}_p)$ if and only if $p \mid n$. The assertion follows. □

As an immediate consequence, we get:

Corollary 3.4. *The element $P \in E(\mathbb{Z})$ is narrow if and only if $n = \pm 1$.*

Fix some prime $p > 0$. The fiber $E \otimes \mathbb{F}_p$ has Kodaira symbol I_v for some integer $v \geq 0$. Let us make some general observations on the multiplicative case $v \geq 1$. The component of the origin G^0 of the algebraic group scheme $G = E \otimes \mathbb{F}_p$ is either the multiplicative group $\mathbb{G}_{m,\mathbb{F}_p}$ or its quadratic twist $\widetilde{\mathbb{G}}_{m,\mathbb{F}_p}$ with respect the involution $\lambda \mapsto 1/\lambda$ and the cyclic extension $\mathbb{F}_p \subset \mathbb{F}_{p^2}$. For the fibers of the Weierstraß model, this means the following:

Proposition 3.5. *Suppose $v \geq 1$ and $G^0 = \widetilde{\mathbb{G}}_{m,\mathbb{F}_p}$. Then the fiber $Y \otimes \mathbb{F}_p$ is obtained from the projective line $\mathbb{P}^1 \otimes \mathbb{F}_p$ by replacing an $\mathbb{F}_{p^2}$-valued point by some rational point.*

Proof. Set $C = Y \otimes \mathbb{F}_p$ and let $\nu : C' \to C$ be the normalization map. Then C' is the projective line over $\mathbb{F}_p$, because this field is perfect and has trivial Brauer group. Let $B \subset C$ be the support of the coherent sheaf $\nu_*(\mathscr{O}'_C)/\mathscr{O}_C$ and $B' \subset C'$ be its preimage. Then there is an exact sequence $0 \to \mathscr{O}_C \to \mathscr{O}_{C'} \oplus \mathscr{O}_B \to \mathscr{O}_{B'} \to 0$, compare [19], Section 4. The long exact sequence reveals that $h^0(\mathscr{O}_B) = 1$ and $h^0(\mathscr{O}_{B'}) = 2$. Since the fiber is multiplicative, the scheme B' is étale. So it is either the spectrum of $A = \mathbb{F}_p \times \mathbb{F}_p$ or $A = \mathbb{F}_{p^2}$. In turn, the number of rational points in $G^0 = C \smallsetminus B = C' \smallsetminus B'$ is either $n = (p+1) - 2$ or $n = (p+1)$. The assertion follows from the fact that $\mathbb{G}_m(\mathbb{F}_p) = \mathbb{F}_p^\times$ has order $p - 1$. □

For the regular model X, the situation is as follows:

Proposition 3.6. *Suppose $v \geq 2$ and $G^0 = \widetilde{\mathbb{G}}_{m,\mathbb{F}_p}$. Then $C = X \otimes \mathbb{F}_p$ is a chain of curves $C_0, C_1, \ldots, C_w$, where the component C_0 of the origin is a projective line over $\mathbb{F}_p$, and the $C_1, \ldots, C_{w-1}$ are projective lines over $\mathbb{F}_{p^2}$. The intersections are $C_i \cap C_{i+1} \simeq \mathrm{Spec}(\mathbb{F}_{p^2})$ for $0 \leq i \leq w - 1$. If v is odd, we have $w = (v+1)/2$ and $C_w = \mathbb{P}^1 \otimes \mathbb{F}_p$. If v is even, we have $w = (v+2)/2$ and C_w arises from $\mathbb{P}^1 \otimes \mathbb{F}_{p^2}$ by replacing an $\mathbb{F}_{p^2}$-valued point by some rational point.*

Proof. According to the Tate Algorithm, the base-change $D = X \otimes \mathbb{F}_{p^2}$ is a cycle of smooth rational curves over $\mathbb{F}_{p^2}$, say with irreducible components $D_0, \ldots, D_{v-1}$ and intersections $D_j \cap D_{j+1} = \mathrm{Spec}(\mathbb{F}_{p^2})$, where we regard indices as congruence classes modulo v. The base-change comes with an action of the Galois group $\Gamma = \mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$, which is cyclic of order two, and the quotient is $C = X \otimes \mathbb{F}_p$. By assumption, the generator $\sigma \in \Gamma$ stabilizes $D_0 = C_0 \otimes \mathbb{F}_{p^2} = \mathrm{Spec}\, \mathbb{F}_{p^2}[t] \cup \mathrm{Spec}\, \mathbb{F}_{p^2}[t^{-1}]$, with induced action given by $t \mapsto t^{-1}$. It follows inductively that $\sigma(D_i) = D_{-i}$ for $0 \leq i \leq v - 1$.

If $v \geq 2$ is even, the Γ-action on the irreducible components of D reveals that $w = 1 + (v-2)/2 + 1 = (v+2)/2$. We have $D_i \cap D_{-i} = \varnothing$ for $1 \leq i \leq w - 1$, hence the projections $D_i \to C_i$ are isomorphisms. The Γ-action on D_w is free, so $C_w = D_w/\Gamma = \mathbb{P}^1 \otimes \mathbb{F}_p$. If $v \geq 3$ is odd, then $w = 1 + (v-1)/2 = (v+1)/2$. Now the projections $D_i \to C_i$ are isomorphisms for $1 \leq i \leq w - 1$. In contrast, $D_w \to C_w$ is only birational, and identifies the $\mathbb{F}_{p^2}$-valued point $D_w \cap D_{w+1}$ to a rational point. Finally, one easily computes $C_i \cap C_{i+1} \simeq \mathrm{Spec}(\mathbb{F}_{p^2})$. □

If $G^0 = \mathbb{G}_{m,\mathbb{F}_p}$, one says that $E_{\mathbb{Q}}$ has *split multiplicative reduction*, and the corresponding fibers of E, X and Y are called *untwisted*. On the other hand, if

$G^0 = \widetilde{\mathbb{G}}_{m,\mathbb{F}_p}$, one says that the elliptic curve has *non-split multiplicative reduction*, and the corresponding fibers are *twisted*.

Let us now unravel what this concretely means for our Weierstraß equation (5). Here the Legendre symbol $(\frac{d}{p}) = \pm 1$ is useful, which gives the class of of an integer d in $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$, where $p > 0$ is an odd prime not dividing d.

Proposition 3.7. *For each prime $p > 0$, the fiber $E \otimes \mathbb{F}_p$ has Kodaira symbol I_v with index $v = 2\,\mathrm{val}_p(n) + \mathrm{val}_p((4m+1)^2 - 64n))$. Moreover, in the multiplicative case $v \geq 1$, $p \neq 2$ the following holds:*

(i) *If $p \mid n$, the singularity on $Y \otimes \mathbb{F}_p$ has coordinates $x = y = 0$, and the fiber $E \otimes \mathbb{F}_p$ is untwisted if and only if $(\frac{4m+1}{p}) = 1$.*

(ii) *If $p \nmid n$, the singularity on $Y \otimes \mathbb{F}_p$ has coordinates $x = -(4m+1)/8$ and $y = (4m+1)/16$, and the fiber is untwisted if and only if the Legendre symbol satisfies $(\frac{4m+1}{p}) = (-1)^{(p^2+4p-5)/8}$.*

Proof. Our Weierstraß equation has discriminant $\Delta = n^2((4m+1)^2 - 64n)$. The assertion on the index $v \geq 0$ follows from the minimality of the Weierstraß equation and the Tate Algorithm. Now suppose that $v \geq 1$, such that $p \neq 2$. The change of coordinates $x = x'$ and $y = y' - \frac{1}{2}x'$ yields a Weierstraß equation in simplified form $y^2 = x^3 + \frac{4m+1}{4}x^2 + nx$. In case (i), the closed fiber $Y \otimes \mathbb{F}_p$ has an affine part given by the ring

$$A = \mathbb{F}_p[x,y]/(y^2 - x^2(x + \frac{4m+1}{4})).$$

Clearly, the singularity has coordinates $x = y = 0$. The fraction $t = 2y/x$ lies in the normalization $A \subset A'$, and satisfies the relation $t^2 = 4x + (4m+1)$. The fiber ring over the singularity is $L = k[t]/(t^2 - (4m+1))$, and we have $E \otimes \mathbb{F}_p = \mathbb{P}^1 \otimes \mathbb{F}_p \smallsetminus \mathrm{Spec}(L)$. The ring L a field if and only if $4m+1 \in \mathbb{F}_p^\times$ is not a square, and (i) follows.

Now suppose we are in case (ii), such that p divides $(4m+1)^2 - 64n$. Over $\mathbb{F}_p$, we get $x^2 + \frac{4m+1}{4}x + n = (x + \frac{4m+1}{8})^2$. In turn, the singular locus of $Y \otimes \mathbb{F}_p$ has coordinates $x' = -\frac{4m+1}{8}$, $y' = 0$ in the new coordinates, and $x = -\frac{4m+1}{8}$, $y = \frac{4m+1}{16}$ in the original coordinates. Arguing as in the previous paragraph, the element $t = y/(x + \frac{4m+1}{8})$ lies in the normalization, and the fiber ring becomes $L = k[t]/(t^2 + \frac{4m+1}{8})$. This is a field if and only if $-2(4m+1) \in \mathbb{F}_p^\times$ is not a square. According to [22], Chapter I, §3, Theorem 5, we have $(\frac{-2}{p}) = (-1)^d$ with exponent $d = (p-1)/2 + (p^2-1)/8 = (p^2+4p-5)/8$, and (ii) follows. □

Let us say that the fiber $E \otimes \mathbb{F}_p$ has *even Kodaira symbol* if the Kodaira symbol is I_v for some even integer $v \geq 0$. This means that either $E \otimes \mathbb{F}_p$ is an elliptic curve, or that the component group scheme Φ_p has even order. For each integer $r \geq 1$, write $E[r]$ for the kernel of the multiplication map $r : E \to E$, which is defined by the cartesian diagram

$$\begin{array}{ccc} E[r] & \longrightarrow & \mathrm{Spec}(\mathbb{Z}) \\ \downarrow & & \downarrow o \\ E & \xrightarrow[r]{} & E. \end{array}$$

Note that the formation of kernels commutes with base-change, because fiber products do so. Moreover, $E[r]$ inherits the structure of relative group scheme, whose structure morphism is separated and of finite type.

We now come to our first main result. Recall that m and n are integers, with n odd and relatively prime to $4m+1$.

Theorem 3.8. *For the Néron model $E \to \mathrm{Spec}(\mathbb{Z})$ of $y^2+xy = x^3+mx^2+nx$, and the section P defined by $x = y = 0$, the following are equivalent:*

(i) *There is another element $Q \neq P$ of order two in $E(\mathbb{Z})$.*
(ii) *The relative group scheme $E[2]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mu_2$.*
(iii) *For every prime $p > 0$, the fiber $E \otimes \mathbb{F}_p$ has even Kodaira symbol.*
(iv) *We have $n = -d(4m+1+16d)$ for some odd d with $\gcd(4m+1, d) = 1$.*

In this situation, the three elements of $E(\mathbb{Z})$ of order two are given by

$$P = (0,0), \quad Q = (4d, -2d) \quad \text{and} \quad P+Q = (-\frac{4m+1+16d}{4}, \frac{4m+1+16d}{8}).$$

Proof. The implication (ii)⇒(i) is trivial. For (iv)⇒(iii) we compute

$$(4m+1)^2 - 64n = (4m+1)^2 + 64d(4m+1+16d) = (4m+1+32d)^2.$$

In light of (2) the discriminant of our Weierstraß equation becomes

$$\Delta = d^2(4m+1+16d)^2(4m+1+32d)^2, \tag{8}$$

and we conclude with Proposition 3.7 that all closed fibers $E \otimes \mathbb{F}_p$ have even Kodaira symbol.

We now show (i)⇒(iv). Let $Q \neq P$ be another element of order two. Replacing Q by $Q+P$ if necessary, we may assume that its image in the group $E(\mathbb{F}_2)$ is non-zero. According to Theorem 2.1, the family of cubics $Y \subset \mathbb{P}^2$ admits a description with another Weierstraß equation

$$y'^2 + x'y' = x'^3 + m'x'^2 + n'x'$$

for some unique integers $m', n' \in \mathbb{Z}$ with n' odd and $\gcd(4m'+1, n') = 1$, where in the new coordinates the closed subscheme $Q \subset Y$ is defined by $x' = y' = 0$. The two Weierstraß equations are related by a change of variables $x = u^2x' + r$, $y = u^3y' + su^2x' + t$ with $u = \pm 1$ and $r, s, t \in \mathbb{Z}$. Composing with the sign involution if necessary, we may assume that $u = 1$. We now use [27], equations (2.2) to compare coefficients. The condition $a_1' = a_1 = 1$ yields $s = 0$, and $a_3' = a_3 = 0$ gives $r = -2t$. In turn, we get

$$n' = a_4' = a_4 + 2ra_2 - t + 3r^2 = n - 4tm - t + 12t^2.$$

In particular, t is a non-zero even integer, which we write as $t = -2d$. Comparing coefficients at $a_6' = a_6 = 0$ gives

$$0 = ra_4 + r^2a_2 + r^3 - t^2 - rt = 4dn + 16d^2m + 64d^3 + 4d^2.$$

Dividing by $4d \neq 0$ yields the desired equation $n + 4dm + 16d^2 + d = 0$. The integer d must be odd, because n is odd.

We now come to the implication (iii)⇒(ii). To simplify notation, write $G = E[2]$ and $S = \mathrm{Spec}(\mathbb{Z})$. Since E is semi-abelian, the multiplication map $r : E \to E$ is quasi-finite and flat for all integers $r \neq 0$, according to [1], Section 7.2, Lemma 2.

Being a base-change, the structure morphism $G \to S$ is quasi-finite and flat. Each geometric fiber for $E \to S$ is either an elliptic curve, or $\mathbb{G}_m \times \mathbb{Z}/v\mathbb{Z}$ with an even integer $v \geq 1$. It follows that the fibers $G \otimes \mathbb{F}_p$ are finite group schemes of constant order four. By Zariski's Main Theorem, G is an open subscheme of some finite $\mathbb{Z}$-scheme W. Replacing W by the closure of G me may assume that $G \subset W$ is schematically dense. Then the structure morphism $W \to S$, which is finite and flat, has $\deg(W/S) = 4$. Hence for each prime $p > 0$, the inclusion $G \otimes \mathbb{F}_p \subset W \otimes \mathbb{F}_p$ is an equality. The Nakayama Lemma gives $G = W$, so the structure morphism $G \to \operatorname{Spec}(\mathbb{Z})$ is finite and flat of degree four.

The section $P \subset E$ yields a homomorphism $\mathbb{Z}/2\mathbb{Z} \to E[2]$ of group schemes over S. This is a monomorphism, because the intersection $P \cap O$ is empty. The quotient H exists as a group scheme over $\mathbb{Z}$, its formation commutes with base-change, and the structure morphism $H \to S$ is free of rank two. By the Tate–Oort Classification ([28], Corollary to Theorem 3), we either have $H = \mu_2$ or $H = \mathbb{Z}/2\mathbb{Z}$. In the latter case, the group $G \otimes \mathbb{F}_2$ would be étale, contradicting the fact that multiplication by $r = 2$ on the elliptic curve $E \otimes \mathbb{F}_2$ is not étale. Thus we have a short exact sequence $0 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mu_2 \to 0$. By Lemma 3.9 below, such extensions split, such that (ii) follows.

It remains to verify the coordinates for the two-torsion sections, assuming that the equivalent conditions (i)–(iv) hold. By definition we have $P = (0, 0)$. In light of the equation $n = -d(4m + 1 + 16d)$ we make the change of coordinates

$$x = x' + 4d \quad \text{and} \quad y = y' - 2d,$$

which transforms the old Weierstraß equation into $y'^2 + x'y' = x'^3 + m'x'^2 + n'x'$, where

$$m' = m + 12d \quad \text{and} \quad n' = n + 8dm + 2d + 48d^2 = d(4m + 1 + 32d). \tag{9}$$

The two-torsion section $x' = y' = 0$ in the new Weierstraß equation corresponds to the two-torsion section $Q \subset Y$ defined by $x = 4d$ and $y = -2d$. In other words, $Q = (4d, -2d)$. The coordinates for $P + Q$ follow from the group law for elliptic curves. □

In the preceding proof, we have used a special case of the following observation:

Lemma 3.9. *Let N be a finite group, and write N_S for the corresponding constant group scheme over $S = \operatorname{Spec}(\mathbb{Z})$. Then every extension $1 \to N_S \to G \to \mu_2 \to 0$ of group schemes splits, and the resulting semidirect product $G = N_S \rtimes \mu_2$ is actually a direct product.*

Proof. The affine group scheme μ_2 is the spectrum of the ring $\mathbb{Z}[T]/(T^2 - 1)$, which sits in a cartesian diagram

$$\begin{array}{ccc} \mathbb{F}_2 \times \mathbb{F}_2 & \longleftarrow & \mathbb{Z} \times \mathbb{Z} \\ \uparrow & & \uparrow \\ \mathbb{F}_2 & \longleftarrow & \mathbb{Z}[T]/(T^2 - 1). \end{array}$$

Roughly speaking, the scheme μ_2 is a connected union $S_1 \cup S_2$ of two copies of S, where the two copies of $\operatorname{Spec}(\mathbb{F}_2)$ are identified.

According to Minkowski's Theorem ([13], Chapter III, Theorem 2.17), the scheme $S = \mathrm{Spec}(\mathbb{Z})$ is simply-connected, in the sense that for each finite étale morphism $S' \to S$, the scheme S' is the disjoint union of finitely many copies of S. In other words, the algebraic fundamental group $\pi_1^{\mathrm{alg}}(S, a)$ vanishes ([6], Exposé V), for any geometric point $a : \mathrm{Spec}(\Omega) \to S$.

Let $s_i : S_i \to G \times_{\mu_2} S_i$ be the unique sections passing through the origin of $G \otimes \mathbb{F}_2$. Then s_1 and s_2 coincide on $S_1 \cap S_2 = \mathrm{Spec}(\mathbb{F}_2)$, and thus define a section $s : \mu_2 \to G$. The expression $\psi(x, y) = s(xy)/s(x)s(y)$, where we write the group laws in multiplicative fashion, defines a morphism of schemes $\psi : \mu_2 \times \mu_2 \to N_S$. It factors over $\{n\} \times S \subset N_S$ for some group element $n \in N$, because both $\mu_2 \times \mu_2$ and S are connected. Base-changing to $\mathbb{F}_2$, we see that $n \in N$ must be the neutral element. In turn, the section of schemes $s : \mu_2 \to G$ is a homomorphism of group schemes, and thus splits the extension of group schemes.

Consequently, the extension is given by a semidirect product $G = N_S \rtimes \mu_2$, formed with respect to some homomorphism $\varphi : \mu_2 \to \mathrm{Aut}(N_S) = \mathrm{Aut}(N)_S$. Arguing as above, we see that φ is trivial, hence $G = N_S \times \mu_2$. □

4. Quotients by 2-division points

We keep the notation as in the previous section, and study the Néron model E for the Weierstraß equation $y^2 + xy = x^3 + mx^2 + nx$, where $n = -d(4m + 1 + 16d)$ for some odd integer d with $\gcd(4m + 1, d) = 1$. We saw in Theorem 3.8 that there are two elements $P, Q \in E(\mathbb{Z})$ of order two whose images in $E(\mathbb{F}_2)$ keep order two. Moreover, the sum $P + Q$ generates a copy of the multiplicative group scheme $\mu_2 \subset E$. The quotient E/μ_2 is a relative group scheme over the ring $\mathbb{Z}$ whose structure morphism is separated and of finite type. It comes with a canonical section of order two that is disjoint from the zero-section, because $E[2]/\mu_2 = \mathbb{Z}/2\mathbb{Z}$. From this one may deduce that Theorem 2.1 applies to the generic fiber $(E/\mu_2)_{\mathbb{Q}}$. In fact, it is possible to infer directly the equation for its Weierstraß model:

Proposition 4.1. *The elliptic curve $(E/\mu_2)_{\mathbb{Q}}$ is given by the globally minimal Weierstraß equation $y^2 + xy = x^3 + (m + 6d)x^2 + d^2x$.*

Proof. Applying Velu's Formula [29] with the subgroup in $(E/\mu_2)_{\mathbb{Q}}$ generated by the 2-division point

$$P + Q = (-\frac{4m + 1 + 16d}{4}, \frac{4m + 1 + 16d}{8}),$$

we get a Weierstraß equation $y^2 + xy = x^3 + mx^2 + a_4x^2 + a_6$ with new coefficients

$$a_4 = -5m^2 + 64md - \frac{5}{2}m - 176d^2 + 16d - \frac{5}{16},$$

$$a_6 = 3m^3 - 64m^2d + \frac{9}{4}m^2 + 432md^2 - 32md + \frac{9}{16}m - 896d^3 + 108d^2 - 4d + \frac{3}{64}.$$

A change of coordinates $x = x' - 2t$, $y = y' + t$ with $t = -\frac{1}{2}m - 4d - \frac{1}{8}$ transforms this into $y^2 + xy = x^3 + (4m + 24d + \frac{3}{4})x^2 + 16d^2x$. A further change of coordinates with $x = x'$, $y = y' + \frac{1}{2}x'$ gives $y^2 + 2xy = x^3 + (4m + 24d)x^2 + 16d^2x$, which immediately leads to the desired Weierstraß equation. □

The elements $P, Q \in E(\mathbb{Z})$ may pass through different components of the fibers $E \otimes \mathbb{F}_p$. We may easily unravel the situation, by considering their difference, which is also their sum:

Lemma 4.2. *The element $P + Q \in E(\mathbb{Z})$ has non-trivial class in the component group scheme Φ_p if and only if the prime p divides $(4m + 1 + 16d)(4m + 1 + 32d)$.*

Proof. The assertion is trivial for $p = 2$. Assume now that p is odd. Clearly, the element $P + Q$ has non-trivial class in Φ_p if and only if its image on the Weierstraß model passes through the singularity of the fiber $Y \otimes \mathbb{F}_p$. This image has coordinates $x = -(4m+1+16d)/4$ and $y = (4m+1+16d)/8$ by Theorem 3.8, and the singular locus is given by $12y^2 - (4m + 1)y + n = 0$ and $x = -2y$, according to (7). We see $P + Q \not\equiv 0$ in Φ_p if and only if p divides

$$16m^2 + 192md + 8m + 512d^2 + 48d + 1 = (4m + 1 + 16d)(4m + 1 + 32d),$$

and the result follows. □

The translation action of μ_2 on the Néron model E extends to an action of the minimal model X. The induced action on the fibers $X \otimes \mathbb{F}_p$ may or may not be free.

Proposition 4.3. *The induced action of $\mu_2 \otimes \mathbb{F}_2$ on the fiber $X \otimes \mathbb{F}_p$ is not free if and only if $p \mid d$. In this case, the locus of fixed points coincides with* $\mathrm{Sing}(X \otimes \mathbb{F}_p)$. *Moreover, the minimal resolution of singularities for the quotient scheme X/μ_2 is the minimal model of the elliptic curve $(E/\mu_2)_{\mathbb{Q}}$.*

Proof. The action is non-free if and only if $E \otimes \mathbb{F}_p$ is multiplicative, and $P + Q \equiv O$ in the component group scheme Φ_p. In this case, the μ_2-action stabilizes every irreducible component and fixes precisely the singularities on $X \otimes \mathbb{F}_p$. According to equations (8), the discriminant Δ of our Weierstraß equation is the square of $d(4m+1+16d)(4m+1+32d)$. Thus the fiber $E \otimes \mathbb{F}_p$ is multiplicative if and only if p divides this number. By Lemma 4.2, we have $P + Q \equiv 0$ in the component group scheme Φ_p if and only if p does not divide $(4m + 1 + 16d)(4m + 1 + 32d)$. The first assertion follows.

The fixed points $a \in X$ for the μ_2-action yield rational double points of type A_1 on the quotient scheme X/μ_2. Let $X' \to X/\mu_2$ be the resolution of singularities. The three schemes in $X \to X/\mu_2 \leftarrow X'$ are Gorenstein. The dualizing sheaf $\omega_{X/\mathbb{Z}}$ is trivial, hence the dualizing sheaves on X/μ_2 and X' are numerically trivial. It follows that $X' \to \mathrm{Spec}(\mathbb{Z})$ contains no (-1)-curve, thus X' is the minimal model of $(E/\mu_2)_{\mathbb{Q}}$. □

5. Classification of curves with additional sections

We now classify elliptic curves $E_{\mathbb{Q}}$ whose Néron model E is semi-abelian and whose Mordell–Weil group $E(\mathbb{Z})$ has certain elements of order two. Our first result is:

Theorem 5.1. *Up to isomorphism, there are exactly two elliptic curves $E_{\mathbb{Q}}$ such that its Néron model E has the following properties:*

(i) *The structure morphism $E \to \mathrm{Spec}(\mathbb{Z})$ is semi-abelian.*
(ii) *The closed fiber $E \otimes \mathbb{F}_2$ is an elliptic curve.*

(iii) *There is a narrow element $P \in E(\mathbb{Z})$ of order two whose images in $E(\mathbb{F}_2)$ are non-zero, and another element $Q \neq P$ of order two.*

These elliptic curve are given by the global minimal Weierstraß equation

$$y^2 + xy = x^3 - 4x^2 - x \quad \text{and} \quad y^2 + xy = x^3 + 4x^2 + x,$$

The former has invariant $j = 20346417/289$ and the only singular fiber occurs at $p = 17$. The latter has $j = 13997521/225$, with singular fibers at $p = 3$ and $p = 5$. All these singular fibers have Kodaira symbol I_2.

Proof. Suppose $E_{\mathbb{Q}}$ satisfies the conditions (i)–(iii). According to Theorem 2.1, the Weierstraß model Y is given by the equation $y^2+xy = x^3+mx^2+nx$ where n is odd and $\gcd(4m+1, n) = 1$, and the element $P \in E(\mathbb{Z})$ is given by $x = y = 0$. Since this element is narrow, we must have $n = \pm 1$, by Corollary 3.4. Since there is another 2-division point $Q \neq P$, Theorem 3.8 tells us that $n = -d(4m + 1 + 16d)$ for some integer d. We thus have $d = \pm 1$ and $4m + 16d = 0$, thus $m = -4d$. Consequently the only solutions are $n = -1$, $d = 1$, $m = -4$ and $n = 1$, $d = -1$, $m = 4$. This gives our two Weierstraß equations.

Conversely, we have to check that the two equations have the stated properties. The equations are relatively minimal by Proposition 3.1, and the Néron model E satisfies conditions (i)–(iii) according to Proposition 3.2. The description of the singular fibers follow from Proposition 3.7. One may compute their j-invariant with [9]. □

Let E be the Néron model for the Weierstraß equation $y^2 + xy = x^3 + 4nx^2 + nx$ with $n = \pm 1$ as in the preceding theorem. After replacing Q by $Q + P$, we may assume that both $P, Q \in E(\mathbb{Z})$ stay non-trivial in $E(\mathbb{F}_2)$. Consider the subgroup scheme $\mu_2 \subset E$ generated by the sum $P+Q$. The induced μ_2-action on the minimal model X is free, according to Proposition 4.3, and the quotient X/μ_2 arises from the Weierstraß equation $y^2 + xy = x^3 \pm 2x^2 + x$, by Proposition 4.1. It is somewhat surprising that these two curves can be characterize in terms of 4-division points:

Theorem 5.2. *Up to isomorphism, there are exactly two elliptic curves $E_{\mathbb{Q}}$ such that its Néron model E has the following properties:*

(i) *The structure morphism $E \to \mathrm{Spec}(\mathbb{Z})$ is semi-abelian.*
(ii) *The fiber $E \otimes \mathbb{F}_2$ is an ordinary elliptic curve.*
(iii) *There is a narrow element $R \in E(\mathbb{Z})$ of order four whose image in $E(\mathbb{F}_2)$ keeps order four.*

These elliptic curve are given by the global minimal Weierstraß equation

$$y^2 + xy = x^3 + 2x^2 + x \quad \text{and} \quad y^2 + xy = x^3 - 2x^2 + x.$$

The former has invariant $j = 35937/17$, and the only singular fiber appears at $p = 17$. The latter has $j = -1/15$, with singular fibers at $p = 3$ and $p = 5$. All these singular fibers have Kodaira symbol I_1

Proof. Suppose first that $E_{\mathbb{Q}}$ satisfies conditions (i)–(iii). The element $P = 2R$ in $E(\mathbb{Z})$ is narrow, has order two, and remains non-zero in $E(\mathbb{F}_2)$. Consider the group $G = \mathbb{Z}/2\mathbb{Z}$. It acts via translation by P on the Néron model E, with induced actions on the minimal model X and the Weierstraß model Y. The G-action on is free on the open subset $E \subset X$, and fixes the complement $\mathrm{Sing}(X/\mathbb{Z}) = X \smallsetminus E$. This

complement is finite, because $E \to \mathrm{Spec}(\mathbb{Z})$ is semi-abelian, and disjoint from the fiber $X \otimes \mathbb{F}_2$, because $E \otimes \mathbb{F}_2$ is an elliptic curve. It follows that for each point $a \in \mathrm{Sing}(X/\mathbb{Z})$, the image $b \in X/G$ yields a rational double point of type A_1. Let $X' \to X/G$ be the minimal resolution of singularities. As in the proof for Proposition 4.3, one sees that X' is the minimal model of the elliptic curve $(E/G)_{\mathbb{Q}}$. Write E' for its Néron model.

We see that $E' \to \mathrm{Spec}(\mathbb{Z})$ is semi-abelian, and for each closed fiber $E \otimes \mathbb{F}_p$ with Kodaira symbol I_v, the closed fiber $E' \otimes \mathbb{F}_p$ has Kodaira symbol I_{2v}. Moreover, the image $P' \subset E'$ of $R \subset E$, which is the quotient of the closed subscheme $R \cup (R+P) \subset E$ by the G-action, defines a narrow element $P' \in E'(\mathbb{Z})$ of order two whose image in $E'(\mathbb{F}_2)$ is non-zero. According to Theorem 5.1, we may assume that E' is given by a Weierstraß equations of the form

$$y^2 + xy = x^3 + 4nx^2 + nx$$

for some sign $n = \pm 1$, such that $P' \subset E'$ is given by the equations $x = y = 0$. According to Theorem 3.8, we have another element $Q' \in E'(\mathbb{Z})$ of order two that is disjoint from the zero-section, namely $Q' = (-4d, 2d)$ with the value $d = -n$. In turn, $P' + Q'$ is the third element of order two, which must hit the zero-section, and generates a subgroup scheme $\mu_2 \subset E'$. Since $R \subset E$ is disjoint from the zero-section, we infer that $\mu_2 = E[2]/G$. In turn, we get an identification of elliptic curves $E_{\mathbb{Q}} = (E/E[2])_{\mathbb{Q}} = (E'/\mu_2)_{\mathbb{Q}}$. The latter quotient can be computed with Proposition 4.1, and is given by the Weierstraß equation $y^2 + xy = x^3 + a_2x^2 + x$ with coefficient $a_2 = 4n + 6d = -2n$.

Conversely, if $E_{\mathbb{Q}}$ is given by one of the Weierstraß equation $y^2 + xy = x^3 + 2nx^2 + nx$ with $n = \pm 1$, then conditions (i)–(ii) hold by Proposition 3.2. One easily sees that $R = (-n, n)$ has order four in in the groups $E(\mathbb{Q})$ and $E(\mathbb{F}_2)$. The statements on the singular fibers follow from Proposition 3.7. Since all fibers are irreducible, every element in $E(\mathbb{Z})$ is narrow. The j-invariant is easily computed with [9]. □

6. Reinterpretation in terms of stacks

In this final section we reformulate our main results in terms of stacks. For details on the theory of stacks, we refer to the monographs of Laumon and Moret-Bailly [8] and Olsson [16].

Let $g, r \geq 0$ be integers with $g + r \geq 2$, and $\mathscr{M}_{g,r}$ be the Deligne–Mumford stack over the base ring $\mathbb{Z}$ whose fiber categories $\mathscr{M}_{g,r}(R)$ are tuples $(C, \sigma_1, \ldots, \sigma_r)$ as follows: C is a finitely presented flat proper R-scheme whose fibers are smooth curves with $h^0(\mathscr{O}_{C_a}) = 1$ and $h^1(\mathscr{O}_{C_a}) = g$, and $\sigma_1, \ldots, \sigma_n$ are pairwise disjoint sections for the structure morphism $f : C \to \mathrm{Spec}(R)$. This has a natural compactification $\bar{\mathscr{M}}_{g,r}$, where the fibers C_a have at most normal crossing singularities, the sections pass through the smooth locus, and the automorphism group is finite. The structure morphism $\bar{\mathscr{M}}_{g,r} \to \mathrm{Spec}(\mathbb{Z})$ is proper, and the inclusion $\mathscr{M}_{g,r} \subset \bar{\mathscr{M}}_{g,r}$ is open. By abuse of notation, we write $\mathscr{O}_C(\sigma_i)$ for the invertible sheaf attached to the image of the section $\sigma_i : \mathrm{Spec}(R) \to C$, which is an effective Cartier divisor.

We are mainly interested in the case $g = 1$ and $r \geq 1$. Note that the objects (C, σ_1) from $\mathscr{M}_{1,1}$ can be regarded as *families of elliptic curves* $E \to \mathrm{Spec}(R)$, where the zero-section $O \subset E$ is the image of σ_1. Likewise, objects from $\bar{\mathscr{M}}_{1,1}$ can

be regarded as families $Y \to \mathrm{Spec}(R)$ of cubic curves with a zero-section $O \subset Y$, locally given by Weierstraß equations where Δ, c_4 generate the unit-ideal. Given an object $(C, \sigma_1, \ldots, \sigma_r) \in \bar{\mathscr{M}}_{1,r}(R)$, the invertible sheaf $\mathscr{O}_C(\sigma_1)$ is semiample, and the homogeneous spectrum

$$P = P(C, \sigma_1) = \mathrm{Proj}\, H^0(C, \bigoplus \mathscr{O}_C(t\sigma_1))$$

together with the induced section $\sigma_1 : \mathrm{Spec}(R) \to Y$ passing through $\mathrm{Reg}(Y/\mathbb{Z})$ defines an object (P, σ_1). The construction $(C, \sigma_1, \ldots, \sigma_r) \mapsto (P, \sigma_1)$ actually yields a morphism of stacks $\bar{\mathscr{M}}_{1,r} \to \bar{\mathscr{M}}_{1,1}$, and composition with the j-invariant gives $\bar{\mathscr{M}}_{1,r} \xrightarrow{j} \mathbb{P}^1$. By abuse of notation, we write $j(C) \in \mathbb{P}^1(R)$ for the image of an object $(C, \sigma_1, \ldots, \sigma_r)$. If $R = k$ is a field, this may be interpreted as a number $j(C) \in k \cup \{\infty\}$.

Now let $m, n \in \mathbb{Z}$ be integers with n odd and $\gcd(4m+1, n) = 1$, and consider our Weierstraß equation $y^2 + xy = x^4 + mx^2 + nx$. The Weierstraß model Y of the ensuing elliptic curve $E_{\mathbb{Q}}$ together with its zero-section $O \subset Y$ can be regarded as an object in $\bar{\mathscr{M}}_{1,1}(\mathbb{Z})$. This defines a map

$$\Psi \longrightarrow \bar{\mathscr{M}}_{1,1}(\mathbb{Z}), \quad (m, n) \longmapsto (Y, O),$$

defined on the set $\Psi = \{(m, n) \in \mathbb{Z}^2 \mid n \text{ odd and } \gcd(4m+1, n) = 1\}$. The equations $x = y = 0$ define an element $P \in E(\mathbb{Z})$ of order two. The strict transforms of $O \cup P \subset E$ on the minimal model X yields a relatively semi-ample invertible sheaf $\mathscr{L}$ on X. The homogeneous spectrum $Y' = P(X, \mathscr{L}) = \mathrm{Proj} \bigoplus_{t \geq 0} H^0(X, \mathscr{L}^{\otimes t})$ defines a partial resolution $X \to Y' \to Y$. Write $O', P' \subset Y'$ for the strict transforms of $O, P \subset Y$. Each geometric fiber for the structure morphism $Y \to \mathrm{Spec}(R)$ is either an elliptic curve or a cycle of rational curves with one or two irreducible components, and P', Q' are contained in $\mathrm{Reg}(Y'/\mathbb{Z})$. This gives a map

$$\Psi \longrightarrow \bar{\mathscr{M}}_{1,2}(\mathbb{Z}), \quad (m, n) \longmapsto (Y', O', P').$$

If the element $P \in E(\mathbb{Z})$ is narrow, which means $n = \pm 1$ according to Proposition 3.4, the partial desingularization coincides with the Weierstraß model, and the map becomes $(m, n) \mapsto (Y, O, P)$.

Proposition 6.1. *The above map induces a bijection between* $\{(m, n) \mid n = \pm 1\}$ *and the set of isomorphism classes of objects* $(C, \sigma_1, \sigma_2) \in \bar{\mathscr{M}}_{1,2}(\mathbb{Z})$ *with the properties* $\mathscr{O}_C(2\sigma_2) \simeq \mathscr{O}_C(2\sigma_1)$ *and* $j(C \otimes \mathbb{F}_2) \neq \infty$.

Proof. Suppose first that (C, σ_1, σ_2) arises from a pair (m, n) with $n = \pm 1$. Then $C = Y$, and the closed fiber at $p = 2$ has invariant $j = 1$. Moreover, all geometric fibers of the structure morphism $C \to \mathrm{Spec}(\mathbb{Z})$ are integral. Thus the Picard scheme $\mathrm{Pic}_{C/\mathbb{Z}}$ exists ([5], Theorem 3.1), and we have an identification $E = \mathrm{Pic}^0_{C/\mathbb{Z}}$ of relative group schemes, given by $D \mapsto \mathscr{O}_C(D - O)$. Since P has order two in $E(\mathbb{Z})$, the invertible sheaf $\mathscr{O}_C(2\sigma_1 - 2\sigma_2)$ has trivial class in $\mathrm{Pic}_{C/\mathbb{Z}}(\mathbb{Z})$. The Leray–Serre spectral sequence gives an exact sequence

$$\mathrm{Pic}(\mathbb{Z}) \longrightarrow \mathrm{Pic}(C) \longrightarrow \mathrm{Pic}_{C/\mathbb{Z}}(\mathbb{Z}),$$

and the factoriality of the ring $\mathbb{Z}$ ensures that $\mathscr{O}_C(2\sigma_1 - 2\sigma_2)$ is trivial.

Conversely, suppose that (C, σ_1, σ_2) has the stated properties. Then $j(C \otimes \mathbb{F}_2) = 1$, and this ensures that the generic fiber $E_{\mathbb{Q}} = C_{\mathbb{Q}}$ becomes an elliptic curve, with

origin given by σ_1. Let E be its Néron model. Write X and Y for the minimal model and Weierstraß model, respectively. From $\mathscr{O}_C(2\sigma_2) \simeq \mathscr{O}_C(2\sigma_1)$ we infer that $\sigma_1, \sigma_2 : \mathrm{Spec}(R) \to C$ pass through the same irreducible component, in all fibers for $C \to \mathrm{Spec}(\mathbb{Z})$. It follows that the fibers are irreducible. Moreover, using that the sections pass through $\mathrm{Reg}(C/\mathbb{Z})$ we infer $C = Y$. The image of σ_2 defines a section $P \subset E$ that is disjoint from the zero-section $O \subset E$. Moreover, the element $P \in E(\mathbb{Z})$ has order two and is narrow. From Theorem 2.1 and Proposition 3.4 we see that $C = Y$ is given by a Weierstraß equation $y^2 + xy = x^3 + mx^2 \pm x$. The equation is unique by Lemma 1.3. □

Now consider the situation of Theorem 5.2, such that we have a narrow element $R \in E(\mathbb{Z})$ of order four whose image in $E(\mathbb{F}_2)$ also has order four. The resulting narrow element $P = 2R$ has order two in both $E(\mathbb{Q})$ and $E(\mathbb{F}_2)$, and the three sections O, R, P are pairwise disjoint. This gives a map

$$\{(4,1),(-4,-1)\} \longrightarrow \bar{\mathscr{M}}_{1,3}(\mathbb{Z}), \quad (m,n) \longmapsto (Y, O, R, P).$$

Proposition 6.2. *The above map induces a bijection between* $\{(4,1),(-4,-1)\}$ *and the set of isomorphism classes of objects* $(C, \sigma_1, \sigma_2, \sigma_3) \in \bar{\mathscr{M}}_{1,3}(\mathbb{Z})$ *with the properties*

$$\mathscr{O}_C(4\sigma_2) \simeq \mathscr{O}_C(4\sigma_1), \quad \mathscr{O}_C(2\sigma_2) \simeq \mathscr{O}_C(\sigma_3) \quad \textit{and} \quad j(C \otimes \mathbb{F}_2) \neq \infty.$$

Proof. It follows from Theorem 5.2 that $m = 4n$ and $n = \pm 1$ gives a family of pointed stable curves $(C, \sigma_1, \sigma_2, \sigma_3)$ with the stated properties. The two Weierstraß equations have different j-invariants, so the map in question is injective.

Conversely, suppose that we have an object $(C, \sigma_1, \sigma_2, \sigma_3)$ with the properties at hand. Then C and σ_1 define an elliptic curve $E_{\mathbb{Q}}$. Write E for its Néron model, and let $R, P \in E(\mathbb{Z})$ be the elements corresponding to σ_2, σ_3. Set $S = \mathrm{Spec}(\mathbb{Z})$. The conditions on the invertible sheaves $\mathscr{O}_C(\sigma_i)$ ensure $4R = O$ and $2R = P$. If a geometric fiber for $C \to \mathrm{Spec}(\mathbb{Z})$ contains a copy of $\mathbb{P}^1$, it must intersect some image $\sigma_i(S)$, by stability. Again by the condition on the invertible sheaves $\mathscr{O}_C(\sigma_i)$ we infer that all geometric fibers are irreducible. It follows that C coincides with the Weierstraß model Y of the elliptic curve $E_{\mathbb{Q}}$. This ensures that the structure morphism $E \to S$ is semi-abelian. Moreover, the subschemes $O, R, P \subset E$ map to the $\sigma_i(S) \subset Y$ under the canonical morphism $E \to Y$. It follows that O, R, P are pairwise disjoint. Hence R has order four in both $E(\mathbb{Q})$ and $E(\mathbb{F}_2)$. Applying Theorem 5.2, we see that the family of cubics $Y = C$ is define by the Weierstraß equation $y^2 + xy = x^3 + 4nx^2 + nx$ with either $n = 1$ or $n = -1$. □

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud: Néron models. Springer, Berlin, 1990.

[2] P. Deligne: Courbes elliptiques: Formulaire. In: B. Birch, W. Kuyk (eds.), Modular functions of one variable IV, pp. 53–73. Springer, Berlin, 1975.

[3] A. Fanelli, S. Schröer: Del Pezzo surfaces and Mori fiber spaces in positive characteristic. Trans. Amer. Math. Soc. 373 (2020), 1775–1843.

[4] J.-M. Fontaine: Il n'y a pas de variété abélienne sur Z. Invent. Math. 81 (1985), 515–538.

[5] A. Grothendieck: Technique de descente et théorèmes d'existence en géométrie algébrique. V. Les schémas de Picard: théorèmes d'existence. Séminaire Bourbaki, Vol. 7, Exp. 232, 143–161. Soc. Math. France, Paris, 1995.

[6] A. Grothendieck: Revêtements étales et groupe fondamental (SGA 1). Société Mathématique de France, Paris, 2003.

[7] T. Hadano: On the conductor of an elliptic curve with a rational point of order 2. Nagoya Math. J. 53 (1974), 199–210.
[8] G. Laumon, L. Moret-Bailly: Champs algebriques. Springer, Berlin, 2000.
[9] W. Bosma, J. Cannon, C. Fieker, A. Steel (eds.): Handbook of Magma functions, Edition 2.16 (2010).
[10] D. Husemöller: Elliptic curves. Springer, New York, 1987.
[11] W. Ivorra: Courbes elliptiques sur $\mathbb{Q}$, ayant un point d'ordre 2 rationnel sur Q, de conducteur $2^N p$. Dissertationes Math. 429 (2004).
[12] M. Kida: Good reduction of elliptic curves over imaginary quadratic fields. J. Théor. Nombres Bordeaux 13 (2001), 201–209.
[13] J. Neukirch: Algebraic number theory. Springer, Berlin, 1999.
[14] A. Ogg: Abelian curves of 2-power conductor. Proc. Cambridge Philos. Soc. 62 (1966), 143–148.
[15] A. Ogg: Abelian curves of small conductor. J. Reine Angew. Math. 226 (1967), 204–215.
[16] M. Olsson: Algebraic spaces and stacks. American Mathematical Society, Providence, RI, 2016.
[17] M. Sadek: On elliptic curves whose conductor is a product of two prime powers. Math. Comp. 83 (2014), 447–460.
[18] S. Schröer: A characterization of semiampleness and contractions of relative curves. Kodai Math. J. 24 (2001), 207-213.
[19] S. Schröer, B. Siebert: Toroidal crossings and logarithmic structures. Adv. Math. 202 (2006), 189–231.
[20] S. Schröer: There is no Enriques surface over the integers. Preprint, arXiv:2004.07025.
[21] M. Schütt, T. Shioda: Mordell–Weil lattices. Springer, Singapore, 2019.
[22] J.-P. Serre: A course in arithmetic. Springer, New York-Heidelberg, 1973.
[23] B. Setzer: Elliptic curves over complex quadratic fields. Pacific J. Math. 74 (1978), 235–250.
[24] R. Stroeker: Reduction of elliptic curves over imaginary quadratic number fields. Pacific J. Math. 108 (1983), 451–463.
[25] M. Szydlo: Elliptic fibers over non-perfect residue fields. J. Number Theory 104 (2004), 75–99.
[26] N. Takeshi: Elliptic curves with good reduction everywhere over cubic fields. Int. J. Number Theory 11 (2015), 1149–1164.
[27] 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. Springer, Berlin, 1975.
[28] J. Tate, F. Oort: Group schemes of prime order. Ann. Sci. Éc. Norm. Supér. 3 (1970), 1–21.
[29] J. Vélu: Isogénies entre courbes elliptiques. C. R. Acad. Sci. Paris Sér. A-B 273 (1971), A238–A241.
[30] Y. Zhao: Elliptic curves over real quadratic fields with everywhere good reduction and a non-trivial 3-division point. J. Number Theory 133 (2013), 2901–2913.

Mathematisches Institut, Heinrich-Heine-Universität, 40204 Düsseldorf, Germany

Email address: schroeer@math.uni-duesseldorf.de