Author: Pannekoek, Rene
Title: Topological aspects of rational points on K3 surfaces
Issue Date: 2013-09-17

Chapter 4

Refinements and computations

4.1 Introduction

We recall the following definition from chapter 3.

Definition 4.1. Let S be a set of primes.

(i) For $(d_p) \in \prod_{p \in S} \mathbb{Q}_p^*$ and $c \in \mathbb{Q}^*$, we call E^c a good twist of E with respect to (d_p) and S if for each $p \in S$ we have $c \in d_p \mathbb{Q}_p^{*2}$, and $E^c(\mathbb{Q})$ is dense in $\prod_{p \in S} E^c(\mathbb{Q}_p)$.

(ii) We say E has good twists if, for all $(d_p) \in \prod_{p \in S} \mathbb{Q}_p^*$, there is $c \in \mathbb{Q}^*$ such that E^c is a good twist of E with respect to (d_p) and S.

As before, if $S = \{p\}$ for some prime p, and if E has good twists with respect to (d_p) and S, we will also say that E has good twists with respect to d_p and p. If E has good twists with respect to S, we will also say that E has good twists with respect to p.

4.1.1 Goal of this chapter

In this chapter we will establish criteria for an elliptic curve E over $\mathbb{Q}$ to have good twists with respect to a prime p. In view of Theorem 3.20, the existence of good twists of E with respect to p implies that the rational points on $\mathrm{Km}(E \times E)$ lie p-adically dense. The crucial idea underlying all criteria established in this chapter is a construction of Jean-François Mestre [22], to be introduced in section 4.2.1. In section 4.7, we will use these criteria to perform a computer search for pairs (E, p) for which it is true that the rational points on $\mathrm{Km}(E \times E)$ lie p-adically dense.

4.1.2 Computer calculations

For an elliptic curve E over $\mathbb{Q}$ whose j-invariant is different from 0 and 1728, we will introduce the notion of a lucky prime number p for E in Definition 4.34. Prime numbers that are not lucky for E are called unlucky for E. The unlucky prime numbers include the prime numbers less than or equal to 7, and the primes for which E has bad reduction. It will be very easy to verify, using a Computer Algebra System, whether or not a prime number p is lucky for E. We will show in Proposition 4.35 that if p is lucky for E, and if $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ lies dense in $X(\mathbb{Q}_p)$. We have also created computer code (described in section 4.7) that computes the lucky prime numbers < 2000 for all elliptic curves E over $\mathbb{Q}$ given by $y^2 = x^3 + ax + b$, where a and b are integers such that $-5 \le a \le 5$ with $a \neq 0$, and $0 < b \le 5$. Doing this, we have obtained the following result.

Theorem 4.2. *Let $S_{5,5}$ be the set of elliptic curves E over $\mathbb{Q}$ given by $y^2 = x^3 + ax + b$, where a and b are integers such that $-5 \le a \le 5$ with $a \neq 0$, and $0 < b \le 5$. Then for all $E \in S_{5,5}$ there are at most 8 prime numbers p with $7 < p < 2000$ which are unlucky for E. Furthermore, for all prime numbers p such that $109 < p < 2000$ and all $E \in S_{5,5}$ we have that if p is unlucky for E, then p is a prime of bad reduction for E. If $E \in S_{5,5}$, and $X = \mathrm{Km}(E \times E)$, and p is a prime with $109 < p < 2000$ for which E has good reduction, then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$.*

The proof of Theorem 4.2 will be given at the end of section 4.7.

4.2 Definitions

Let k be a field of characteristic not equal to 2. Let a and b be elements of k such that

$$ab(4a^3 + 27b^2) \neq 0 \tag{4.1}$$

and define $f(x) = x^3 + ax + b$. Then the curve E over k given by $y^2 = f(x)$ is an elliptic curve with j-invariant not equal to 0 or 1728.

Remark 4.3. The assumption (4.1) also implies:

$$f(-b/a) = (-b/a)^3 + a(-b/a) + b = (-b/a)^3 \neq 0 \tag{4.2}$$

and

$$f(3b/a) = (3b/a)^3 + a(3b/a) + b = a^{-3}b\left(27b^2 + 4a^3\right) \neq 0; \tag{4.3}$$

in other words, $-b/a$ and $3b/a$ are not the x-coordinate of any 2-torsion point on E.

4.2.1 Mestre's construction

We now come to the construction by Mestre [22], which is of fundamental importance to the rest of this chapter. We shall denote

$$\phi(u) = -\frac{b}{a}\frac{u^4+u^2+1}{u^4+u^2}. \tag{4.4}$$

We will mostly interpret ϕ as a rational expression in whatever argument is given to it, but we will sometimes regard it as a morphism $\mathbb{P}^1_k \to \mathbb{P}^1_k$. Note that

$$u^2\phi(u) = \phi(u^{-1}).$$

For each $d \in k$, we define the smooth projective curve C^d over k as

$$C^d\colon dv^2 = f(\phi(u)).$$

For each $d \in k$, we have a morphism $\pi_1^d\colon C^d \to E^d$ sending (u,v) to $(\phi(u), v)$. It is clear from (4.4) that ϕ satisfies

$$a\phi(u)(u^4+u^2) = -b(u^4+u^2+1).$$

Multiplying both sides with (u^2-1), we get

$$a\phi(u)u^2(u^4-1) = b(1-u^6).$$

Rearranging this, we obtain

$$au^2\phi(u) + b = u^6(a\phi(u)+b).$$

Finally, from this it follows that we have

$$\begin{aligned} f(\phi(u^{-1})) = f(u^2\phi(u)) &= u^6\phi(u)^3 + au^2\phi(u) + b \\ &= u^6(\phi(u)^3 + a\phi(u) + b) = u^6 f(\phi(u)). \end{aligned}$$

For each $d \in k$ therefore, there exists the involution τ^d of C^d defined by

$$\begin{aligned} \tau^d\colon C^d &\to C^d \\ (u,v) &\mapsto (u^{-1}, u^3 v) \end{aligned}$$

We define a second morphism $\pi_2^d \colon C^d \to E^d$ for each $d \in k$, by setting $\pi_2^d = \pi_1^d \circ \tau^d$. The morphism π_2^d sends (u, v) to $(u^2\phi(u), u^3 v)$.

Summarizing, we have two morphisms for each $d \in k$

$$\begin{aligned} \pi_1 \colon C^d &\to E^d & \qquad \pi_2 \colon C^d &\to E^d \\ (u, v) &\mapsto (\phi(u), v) & (u, v) &\mapsto (u^2\phi(u), u^3 v) \end{aligned}$$

as well as the following diagram

$$\begin{tikzcd} C^d \arrow[rr, "\tau^d"] \arrow[dr, "\pi_1"'] & & C^d \arrow[dl, "\pi_2"] \\ & E^d & \end{tikzcd}$$

For brevity, we denote the curve C^1 by C, the automorphism τ^1 by τ, and the morphisms π_1^1 and π_2^1 from C to E by π_1 and π_2. This concludes the discussion of Mestre's construction.

Remark 4.4. Unless stated otherwise, when write (u_0, v_0) for a point on C, we will mean u_0 to be its u-coordinate, and v_0 to be its v-coordinate.

4.2.2 An affine model for C

We create an affine model for C that is smooth away from infinity. We introduce the change of variables $v' = u^3(u^2+1)^2 v$, resulting in a model for C of the form

$$v'^2 = g(u), \tag{4.5}$$

with $g(u)$ a polynomial of degree 14 equal to

$$g(u) = (u^2+1)\left(\left(-\frac{b}{a}\right)^3 (u^4+u^2+1)^3 - \right. \\ \left. b(u^4+u^2+1)(u^4+u^2)^2 + b(u^4+u^2)^3\right). \tag{4.6}$$

We will show that (4.5) defines a smooth affine curve in Proposition 4.8(ii). We have $g(0) = (-b/a)^3 \neq 0$. Relative to the model $v'^2 = g(u)$, the curve C has two points ∞_1 and ∞_2 at infinity. The maps $\pi_1 \colon C \to E$ and $\pi_2 \colon C \to E$ are now given by

$$\begin{aligned} \pi_1 \colon C &\to E & \qquad \pi_2 \colon C &\to E \\ (u, v') &\mapsto (\phi(u), u^{-3}v'(u^2+1)^{-2}) & (u, v') &\mapsto (u^2\phi(u), v'(u^2+1)^{-2}) \end{aligned}$$

while the automorphism $\tau\colon C \to C$ is given by

$$\begin{aligned}\tau\colon C &\to C\\ (u, v') &\mapsto (u^{-1}, u^{-7}v').\end{aligned}$$

4.3 Creating good twists

In this section, we take $k = \mathbb{Q}$. The conditions on a and b, which are now elements of $\mathbb{Q}$, are as in the previous section, and the rest of the notation introduced there remains valid. The lemmas 4.5 and 4.6 in this subsection will explain the relevance of the curves C^d and the morphisms π_i^d. They will be used to construct good twists of E.

Lemma 4.5. *Take $k = \mathbb{Q}$. Let $\alpha, \beta \in k$ with $\beta \neq 0$, and write $c = f(\phi(\alpha))/\beta^2$. The point*

$$(\alpha, \beta)$$

lies on the curve C^c, and the points

$$(\phi(\alpha), \beta) \quad \text{and} \quad (\alpha^2\phi(\alpha), \alpha^3\beta)$$

lie on the elliptic curve E^c.

Proof. It is obvious that (α, β) lies on C^c. The two points $(\phi(a), \beta)$ and $(\alpha^2\phi(\alpha), \alpha^3\beta)$ are its images on E^c under π_1^c and π_2^c. □

Lemma 4.6. *Suppose that there exists $P \in C^d(\mathbb{Q}_p)$ such that $\pi_1^d(P)$ and $\pi_2^d(P)$ generate $E^d(\mathbb{Q}_p)$ topologically. Then there exists a good twist of E with respect to d and p.*

Proof. By perturbing P if necessary, we may assume that $u_0 = u(P)$ and $v_0 = v(P)$ are both finite, and that v_0 is non-zero. Choose u_0' and $v_0' \in \mathbb{Q}$ with $v_0' \neq 0$ such that u_0' is close to u_0 and v_0' is close to v_0. Define $c = f(\phi(u_0'))/v_0'^2$; by possibly taking u_0' and v_0' closer to u_0 and v_0, we may assume that $c/d \in \mathbb{Q}_p^{*2}$. By Lemma 4.5, the curve C^c contains the rational point (u_0', v_0'), and E^c contains the rational points

$$Q_1' = (\phi(u_0'), v_0')) \quad \text{and} \quad Q_2' = (u_0'^2\phi(u_0'), u_0'^3v_0')).$$

Under the isomorphism defined over $\mathbb{Q}_p$

$$\begin{aligned}E^c &\to E^d\\ (x, y) &\mapsto (x, y\sqrt{c/d})\end{aligned}$$

the points $\pm Q_1'$ and $\pm Q_2'$ map to points lying arbitrarily close to $\pm Q_1$ and $\pm Q_2$, where $Q_1 = \pi_1^d(P)$ and $Q_2 = \pi_2^d(P)$. Hence, possibly after taking u_0' and v_0' closer to u_0 and v_0, we get that Q_1' and Q_2' are topological generators of $E^c(\mathbb{Q}_p)$. □

Lemma 4.6 provides the implication going from a purely p-adic statement to a statement about rational points. Therefore, after establishing some elementary properties of the curves C^d, we will restrict to $k = \mathbb{Q}_p$. Later on, in section 4.6, we will go back to assuming $k = \mathbb{Q}$, and we will use Lemma 4.6 to draw conclusions about the existence of good twists. In fact, the hypothesis of Lemma 4.6 is so important in this chapter, that we will make it into a definition.

Definition 4.7. We will say that $P \in C^d(\mathbb{Q}_p)$ is a Mestre point if the points $\pi_1^d(P)$ and $\pi_2^d(P)$ generate $E^d(\mathbb{Q}_p)$ topologically.

4.4 Properties of the curve C

In this section, the field k is an arbitrary field of characteristic not equal to 2. We will collect some information on C (defined in section 4.2.1) and its maps to E. Let the assumptions and notation on the ground field k, the curve E, the curve C, and the maps π_1,π_2 and τ be as in section 4.2.

Proposition 4.8. *The following statements are true.*

(i) The branch locus of π_1 consists of the points on E with x equal to $-b/a$ or $3b/a$. The ramification loci of π_1 and π_2 are disjoint.

(ii) The polynomial g is separable. The genus of C is equal to 6.

Proof. We let C' be the smooth projective curve defined by

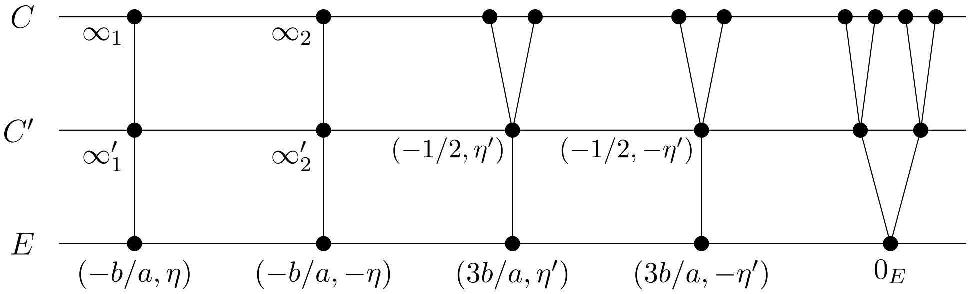
$$C' \colon v^2 = f\left(-\frac{b}{a}\frac{w^2+w+1}{w^2+w}\right).$$

Putting $v'' = v(w^2+w)^2$, we obtain for C' an affine model of the form $v''^2 = h(w)$ with $h(w)$ a polynomial of degree 8 with a simple zero at 0. Note that, relative to this model, the curve C' has two points ∞_1', ∞_2' at infinity. In terms of the coordinates (u, v') on C, and the coordinates (w, v'') on C', we define the maps

$$\begin{aligned} &\pi_1' \colon C \to C' & &\pi_1'' \colon C' \to E \\ &(u, v') \mapsto (u^2, uv') & &(w, v'') \mapsto \left(-\frac{b}{a}\frac{w^2+w+1}{w^2+w}, v''(w^2+w)^{-2}\right) \end{aligned}$$

With these definitions, we have factored the map π_1 as $\pi_1'' \circ \pi_1'$.

In view of (4.2) and (4.3), the points on E with x-coordinates $-b/a$ or $3b/a$ do not belong to the 2-torsion on E, and hence there are two of both.



We analyze the ramification of the degree-two map $\pi_1'' \colon C' \to E$. It is unramified above the identity 0_E of E, since the points with $w = 0$ or $w = -1$ map to 0_E. It is ramified at the two points (w, v) where $w = \infty$, which map to the points with $x = -b/a$. If w is finite, not equal to 0 or -1, and π_1'' is ramified at (w, v), then the equation

$$-\frac{b}{a}\frac{T^2 + T + 1}{T^2 + T} = -\frac{b}{a}\frac{w^2 + w + 1}{w^2 + w} =: x_0$$

must have a unique solution $T = w$; equivalently, the polynomial

$$T^2 + T + \frac{b}{ax_0 + b}$$

has its unique zero at $T = w$. Hence we must have $b/(ax_0 + b) = 1/4$. In that case, we must therefore have $x_0 = 3b/a$ and $w = -1/2$. Summarizing, we have found that π_1'' is ramified at the points (w, v) lying above the points where $x = -b/a$, which have $w = \infty$, and at the points (w, v) lying above the points where $x = 3b/a$, which have $w = -1/2$.

Next, we analyze the ramification of the degree-two map $\pi_1' \colon C \to C'$ that, in terms of the models constructed at the start of the proof, sends (u, v') to (u^2, uv'). It is certainly unramified above points where w is not 0 or ∞. It is also unramified above points where $w = 0$; indeed, there is a single point on C' where $w = 0$, which corresponds to the smooth point $(0, 0)$ on the model $v''^2 = h(w)$ for C' obtained before, whereas on C there are two points with $u = 0$. We claim further that π_1' is ramified above the points at infinity ∞_1' and ∞_2'. Indeed, it is clear that the preimage of $\{\infty_1', \infty_2'\}$ under π_1' is $\{\infty_1, \infty_2\}$.

Summarizing, we have shown, firstly, that π_1'' ramifies at ∞_1' and ∞_2', which map to the two points where $x = -b/a$, and at the two points where w equals $-1/2$, which map to the points where $x = 3b/a$; secondly, that π_1' ramifies at the two points ∞_1 and ∞_2, which map to ∞_1' and ∞_2'. This shows that π_1 is ramified at ∞_1 and ∞_2, each with ramification index 4, and at the four points where $u^2 = -1/2$, each with ramification index 2. Applying the automorphism τ, we get that π_2 is ramified at the two points where $u = 0$ with ramification index 4, and at the four points where $u^2 = -2$, each with ramification index 2. This shows that the ramification loci are disjoint.

Now we prove (ii). From (4.6), we see that the set of zeros of g is the union of the set of zeros of $u^2 + 1$, and the set of u with $u^4 + u^2 \neq 0$ such that

$$f(\phi(u)) = f\left(-\frac{b}{a}\frac{u^4 + u^2 + 1}{u^4 + u^2}\right) \tag{4.7}$$

is zero. We see from (4.2) and (4.3) that $f(\phi(u)) = 0$ implies $\phi(u) \neq -b/a$ and $\phi(u) \neq 3b/a$, hence π_1 is unramified above $E[2]$. This shows that there are exactly 12 values of u for which (4.7) vanishes. Hence g has 14 distinct zeros, and therefore it can have no repeated roots. This shows that C has genus 6, and ends the proof. □

Remark 4.9. Part (ii) of Proposition 4.8 was mentioned by Mestre [22].

We define the map

$$i\colon C \to E \times E \tag{4.8}$$

as the map given by (π_1, π_2). Also, we will use the letter Z to denote the (reduced) closed subscheme of C consisting of the points (u, v) with

$$u^4 + u^2 + 1 = 0 \quad \text{or} \quad v = 0.$$

Using (4.5) and (4.6), we see that $Z \times_k \overline{k}$ consists of the 8 points where $u^4 + u^2 + 1 = 0$, and the 14 points where $v = 0$, hence 22 points in total.

Proposition 4.10. *The restriction of i to $C - Z$ is an embedding.*

Proof. We resume the notation of the proof of Proposition 4.8. We first claim that $i|_{C-Z}$ is injective, and that $i(C - Z)$ and $i(Z)$ are disjoint; from this we will deduce that $i|_{C-Z}$ is a homeomorphism onto its image. Let P be a point on $C - Z$ and write (Q_1, Q_2) for the point on $E \times E$ that is the image of P under i. By definition of i, we have $Q_1 = \pi_1(P)$ and $Q_2 = \pi_2(P)$. We distinguish three pairwise exclusive possibilities for (Q_1, Q_2).

Case (a): we have $Q_1 = 0_E$ or $Q_2 = 0_E$. First suppose $P \notin Z$. If $Q_1 = 0_E$, we have that $u(P) = 0$ or $u(P)^2 + 1 = 0$; since $P \notin Z$, we must have $u(P) = 0$. We get that $u(\tau(P)) = u(P)^{-1} = \infty$, hence $\tau(P) = \infty_1$ or $\tau(P) = \infty_2$, and we have $Q_2 = \pi_1(\tau(P)) = (-b/a, \pm\eta)$, where $\eta^2 = f(-b/a)$. If $Q_2 = 0_E$, we can apply τ to the result of the previous calculation to find that $Q_1 = (-b/a, \pm\eta)$. Hence, there are four possibilities for P: the two points with $u(P) = 0$ and the two points with $u(P) = \infty$. The first pair maps to the two points $(0_E, (-b/a, \pm\eta))$, the second pair maps to the two points $((-b/a, \pm\eta), 0_E)$. Now suppose $P \in Z$. Reasoning as before, we find that $Q_1 = 0_E$ or $Q_2 = 0_E$ implies $u(P)^2 + 1 = 0$. One checks that i sends the points satisfying $u^2 + 1 = 0$ to $(0_E, 0_E)$.

Case (b): we have $x(Q_1) = 0$ or $x(Q_2) = 0$. Then we have either $\phi(u(P)) = 0$ or $u(P)^2\phi(u(P)) = 0$. In either case we have $u(P)^4 + u(P)^2 + 1 = 0$. Hence P lies in Z. Conversely, if P is such that $u(P)^4+u(P)^2+1 = 0$, then we have both $x(Q_1) = 0$ and $x(Q_2) = 0$.

Case (c): we have that $x_1 = x(Q_1)$ and $x_2 = x(Q_2)$ are both finite and non-zero. By the discussion of the previous case, we have $u(P)^4+u(P)^2+1 \neq 0$. Then since $x_1 = \phi(u(P))$ and $x_2 = u(P)^2\phi(u(P))$, we have that $u(P)$ is also finite and non-zero. If we further put $y_1 = y(Q_1)$ and $y_2 = y(Q_2)$, then from $y_1 = v(P)$ we get that y_1 is also finite. First assume that $y_1 = v(P)$ is zero. Then $P \in Z$. Assuming that $y_1 = v(P)$ is non-zero, then since we also had $u(P)^4 + u(P)^2 + 1 \neq 0$, we must have $P \notin Z$. Since we have $y_2 = u(P)^3v(P) = u(P)^3y_1$, we can find back $u(P)$ from x_1, x_2, y_1, y_2 as $u(P) = x_2y_2/(x_1y_1)$, and we can find $v(P)$ back as $v(P) = y_1$. Hence P is determined by Q_1 and Q_2 in case (c).

Clearly, cases (a) through (c) exhaust the possibilities for the pair (Q_1, Q_2). The discussion of the three cases above then establishes the claim that the restriction to $C - Z$ of i is injective, and that $i(C - Z)$ is disjoint from $i(Z)$. Since i is proper, it is closed and since $i(C - Z)$ is disjoint from $i(Z)$, we must have that the map $i|_{C-Z}$ is closed onto its image. Since $i|_{C-Z}$ is moreover injective and continuous, we get that it is a homeomorphism onto its image.

To prove that $i|_{C-Z}$ is an embedding in the sense of algebraic geometry, it is enough by the proof of [12, Lemma II.7.4] to show that it separates tangent vectors, i.e., that, for each $P \in C$, the map

$$T_PC \to T_{i(P)}(E \times E) = T_{\pi_1(P)}(E) \times T_{\pi_2(P)}(E)$$

induced by i is an injection. By dualizing, this is equivalent to showing that the pull-back map

$$i_P^*\colon T^*_{\pi_1(P)}(E) \times T^*_{\pi_2(P)}(E) \to T^*_P C \tag{4.9}$$

on cotangent spaces is surjective for all $P \in C$. Let ω be the invariant differential

$$\omega = \frac{dx}{y} \in H^0(E, \Omega^1_E)$$

on E. Since $T^*_P C$ is a one-dimensional k-vector space, it suffices to check that for each $P \in C$, at least one of the everywhere-regular differential forms $\pi_1^*\omega$ and $\pi_2^*\omega$ on C is non-zero at P. One easily computes that

$$\pi_1^*\omega = \frac{1}{v} d\left(-\frac{b}{a}\frac{u^4+u^2+1}{u^4+u^2}\right) = \frac{2b}{a}\frac{2u^2+1}{u^3v(u^2+1)^2}du = \frac{2b}{a}\frac{2u^2+1}{v'}du$$

and

$$\pi_2^*\omega = \frac{1}{v} d\left(-\frac{b}{a}\frac{u^4+u^2+1}{u^2+1}\right) = -\frac{2b}{a}\frac{u^2+2}{(u^2+1)^2 v}du = -\frac{2b}{a}\frac{u^3(u^2+2)}{v'}du.$$

One computes that the zero-locus of $\pi_1^*\omega$ consists of $\{\infty_1, \infty_2\}$ as well as the points where $u^2 = -1/2$, while the zero-locus of $\pi_2^*\omega$ consists of the points where $u^2 = 0$ or $u^2 = -2$. Hence (4.9) is surjective for all $P \in C$, and so $i\colon C \to E \times E$ separates tangent vectors. This concludes the proof of the proposition. □

The following lemma will be used in the proof of Proposition 4.12. We keep the assumption that k is a field of characteristic not equal to 2.

Lemma 4.11. *Let e_1, e_2, e_3 be the roots of $f = x^3 + ax + b$ in $\overline{k}$, and let $\{\lambda, \mu, \nu\} = \{1, 2, 3\}$. Then the roots in $\overline{k}$ of the polynomial*

$$T^2 + T + \frac{b}{ae_\lambda + b} \tag{4.10}$$

are e_μ/e_λ and e_ν/e_λ. If furthermore k is a p-adic field with $p \neq 2$, and e_1, e_2 and e_3 are of equal valuation in k, then one of the elements

$$\frac{e_1}{e_2}, \frac{e_2}{e_3}, \text{ and } \frac{e_3}{e_1}$$

is a square in $k(e_1, e_2, e_3)$.

Proof. Without loss of generality, we assume that we have $\lambda = 1, \mu = 2, \nu = 3$. Long division gives $f = (x - e_1)g$ with

$$g = (x^2 + e_1 x + a + e_1^2),$$

so that we have

$$(x - e_2/e_1)(x - e_3/e_1) = e_1^{-2} g(e_1 x) = x^2 + x + \frac{a + e_1^2}{e_1^2} = x^2 + x + \frac{-b/e_1}{(-ae_1 - b)/e_1},$$

from which the first claim follows. The second one is clear. □

Proposition 4.12. *Let ϕ_1 denote ϕ and let ϕ_2 denote the function $u \mapsto u^2\phi(u)$. Let k be a finite extension of $\mathbb{Q}_p$ for some prime number p with $p \neq 2$, and assume that the zeros of f in $\overline{k}$ have the same valuation.*

(i) Let i be either 1 or 2. If f has three roots in k, then at least two of the roots of f are contained in $\phi_i(\mathbb{P}^1(k))$.

(ii) Let e_1, e_2, e_3 be the roots of f in $\overline{k}$, and let $\{\lambda, \mu, \nu\} = \{1, 2, 3\}$. Then

$$\phi_2(\phi_1^{-1}(e_\lambda)) = \{e_\mu, e_\nu\}.$$

Proof. We first prove assertion (i) for $i = 1$. For any $e \in k$, we have $e \in \phi_1(\mathbb{P}^1(k))$ if and only if there exists $u \in k$ such that

$$\phi_1(u) = -\frac{b}{a}\frac{u^4 + u^2 + 1}{u^4 + u^2} = e. \tag{4.11}$$

Let e_1, e_2, e_3 be the zeros of f. If for example $e = e_1$, Lemma 4.11 shows that the solutions to this equation are $u = \pm\sqrt{e_2/e_1}$ and $u = \pm\sqrt{e_3/e_1}$. For the cases where $e = e_2$ and $e = e_3$, the solutions follow from this by symmetry.

By the identity $(e_1/e_2) \cdot (e_2/e_3) \cdot (e_3/e_1) = 1$ and the fact that e_1, e_2, e_3 have equal valuation in k, we can choose λ, μ and ν such that $\{\lambda, \mu, \nu\} = \{1, 2, 3\}$ in such a way that e_λ/e_μ is a square in k. Therefore equation (4.11) has the solution $u_\lambda = \sqrt{e_\mu/e_\lambda}$ in k if $e = e_\lambda$, and the solution $u_\mu = 1/u_\lambda$ in k if $e = e_\mu$. Hence we find that u_λ is a preimage in k of e_λ under ϕ_1, and u_μ is a preimage in k of e_μ under ϕ_1. Hence assertion (i) is proven for $i = 1$. For $i = 2$, we need only observe

$$\phi_2(u_\lambda) = u_\lambda^2 \phi(u_\lambda) = (e_\mu/e_\lambda) \cdot e_\lambda = e_\mu \tag{4.12}$$

and

$$\phi_2(u_\mu) = u_\mu^2 \phi(u_\mu) = (e_\lambda/e_\mu) \cdot e_\mu = e_\lambda.$$

We now prove (ii). We define $u'_\lambda = \sqrt{e_\nu/e_\lambda}$. The preimages of e_λ under ϕ_1 are $\pm u_\lambda$ and $\pm u'_\lambda$. We get $\phi_2(\pm u_\lambda) = e_\mu$ by (4.12), as well as

$$\phi_2(\pm u'_\lambda) = (e_\nu/e_\lambda) \cdot \phi(\pm u'_\lambda) = (e_\nu/e_\lambda) \cdot e_\lambda = e_\nu.$$

This concludes the proof of (ii). □

4.5 Existence criteria for Mestre points

In this section we will establish various criteria for the existence of Mestre points on C in the sense of Definition 4.7.

Definition 4.13. By a smooth curve (resp. surface) over $\mathbb{Z}_p$ we shall mean a scheme equipped with a smooth morphism to $\mathbb{Z}_p$ whose fibres are of dimension one (resp. two).

4.5.1 Assumptions and definitions

For the rest of this section, we assume that $p > 2$ is a prime, that $k = \mathbb{Q}_p$ and that a and b are elements of $\mathbb{Z}_p$ such that

$$ab(4a^3 + 27b^2) \in \mathbb{Z}_p^*. \tag{4.13}$$

The elliptic curve E over $\mathbb{Q}_p$ is defined as at the start of section 4.2, and we let $\mathcal{E}$ be the Weierstrass model of E defined by $y^2 = x^3 + ax + b$. By (4.13), we have that $\mathcal{E}$ is a smooth curve over $\mathbb{Z}_p$. In particular, the elliptic curve E has good reduction, and $\mathcal{E}$ is a minimal Weierstrass model of it. By $\mathcal{C}$ we denote the closure of $i(C)$ in $\mathcal{E} \times \mathcal{E}$, where i is as in (4.8), and by $\mathcal{Z}$ we denote the closure of $i(Z)$ in $\mathcal{E} \times \mathcal{E}$, both considered with their reduced subscheme structures. We further define $\mathcal{C}^\circ = \mathcal{C} - \mathcal{Z}$. We have that $\mathcal{C}$ is a proper curve over $\mathbb{Z}_p$. Moreover, since $\mathcal{C}$ is the scheme-theoretic image of the morphism $C \to \mathcal{E} \times \mathcal{E}$ by [12, ex. II.3.11(d)], it is flat over $\mathbb{Z}_p$ by [3, 1.1]. Since $\mathcal{C}^\circ \subset \mathcal{C}$ is an open subscheme of the proper flat scheme $\mathcal{C}$ over $\mathbb{Z}_p$, and its fibres over $\mathbb{Z}_p$ are smooth, it is itself smooth over $\mathbb{Z}_p$. The automorphism of $\mathcal{E} \times \mathcal{E}$ that interchanges both factors will be denoted by τ. On $i(C)$, the map τ induces the same map as the automorphism τ of C. The maps π_1 and π_2 from C to E extend to morphisms $\mathcal{C} \to \mathcal{E}$, which we will denote by the same symbols.

By $\Gamma_n \subset \mathcal{E} \times \mathcal{E}$, we denote the graph of multiplication by n, in the following sense

$$\Gamma_n = \{(e, ne) : e \in \mathcal{E}\} .$$

We have that the curve $\Gamma_n \subset \mathcal{E} \times \mathcal{E}$ is smooth over $\mathbb{Z}_p$ for all n. By the valuative criterion of properness, we have

$$E(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Z}_p), \quad C(\mathbb{Q}_p) = \mathcal{C}(\mathbb{Q}_p) = \mathcal{C}(\mathbb{Z}_p)$$

and via these identifications the subgroups $E_n(\mathbb{Q}_p)$ and $\mathcal{E}_n(\mathbb{Q}_p)$, as defined in section 1.2, coincide for all integers $n \geq 0$.

4.5.2 The case where p does not divide $\#\mathcal{E}(\mathbb{F}_p)$

The following proposition shows that if $\#\mathcal{E}(\mathbb{F}_p)$ is coprime to p, we may reduce the problem of finding a P as in Lemma 4.6 to a problem involving only the reductions $\mathcal{C}_{\mathbb{F}_p}$ and $\mathcal{E}_{\mathbb{F}_p}$.

Proposition 4.14. *Assume that the order of $\mathcal{E}(\mathbb{F}_p)$ is coprime to p. Let $\overline{P} \in \mathcal{C}(\mathbb{F}_p)$. Then the following conditions are equivalent.*

(i) The points $\pi_1(\overline{P})$ and $\pi_2(\overline{P})$ generate $\mathcal{E}(\mathbb{F}_p)$.

(ii) There exists a Mestre point $P \in \mathcal{C}(\mathbb{Q}_p)$ with $P_{\mathbb{F}_p} = \overline{P}$.

Proof. The implication (ii) ⇒ (i) is clear: if $P \in \mathcal{C}(\mathbb{Q}_p)$ is such that $P_{\mathbb{F}_p} = \overline{P}$, and $\pi_1(\overline{P})$ and $\pi_2(\overline{P})$ do not generate $\mathcal{E}(\mathbb{F}_p)$, then certainly $\pi_1(P)$ and $\pi_2(P)$ do not generate $E(\mathbb{Q}_p)$ topologically.

Since the ramification loci of the π_i are disjoint by Proposition 4.8(i), without loss of generality we may assume $(\pi_1)_{\mathbb{F}_p}$ to be unramified, and hence étale, at $\overline{P}$. Write $\overline{Q} = \pi_1(\overline{P})$.

Denote the set of points in $C(\mathbb{Q}_p)$ that reduce to $\overline{P}$ with $C(\mathbb{Q}_p)_{\overline{P}}$. If $P' \in C(\mathbb{Q}_p)_{\overline{P}}$, then by the assumption of the proposition, the points $Q'_1 = \pi_1(P')$ and $Q'_2 = \pi_2(P')$ together with $E_1(\mathbb{Q}_p)$ generate $E(\mathbb{Q}_p)$. Therefore it suffices to show that we can choose P' in such a way that some $\mathbb{Z}$-linear combination of Q'_1 and Q'_2 lies in $E_1(\mathbb{Q}_p) - E_2(\mathbb{Q}_p)$. By the fact that π_1 is étale at $\overline{P}$ and by Hensel's lemma, the restriction of π_1 to $C(\mathbb{Q}_p)_{\overline{P}}$ surjects to the set $E(\mathbb{Q}_p)_{\overline{Q}}$ of points $Q' \in E(\mathbb{Q}_p)$ such that $(Q')_{\mathbb{F}_p} = \overline{Q}$. We have $E(\mathbb{Q}_p)_{\overline{Q}} = \pi_1(P') + E_1(\mathbb{Q}_p)$ for any $P' \in C(\mathbb{Q}_p)_{\overline{P}}$. Hence, for any $P' \in C(\mathbb{Q}_p)_{\overline{P}}$, there exists $P'' \in C(\mathbb{Q}_p)_{\overline{P}}$ with $\pi_1(P') - \pi_1(P'') \notin E_2(\mathbb{Q}_p)$.

Now we use the fact that the order of $\mathcal{E}(\mathbb{F}_p)$ is coprime to p. We have $\ell\pi_1(\overline{P}) = 0$ for some integer ℓ coprime to p. Let $P' \in C(\mathbb{Q}_p)_{\overline{P}}$ be arbitrary.

The fact $\ell\pi_1(\overline{P}) = 0$ implies that $\ell\pi_1(P') \in E_1(\mathbb{Q}_p)$. If $\ell\pi_1(P') \notin E_2(\mathbb{Q}_p)$, we are done. Otherwise, there exists $P'' \in C(\mathbb{Q}_p)_{\overline{P}}$ such that $\pi_1(P') - \pi_1(P'') \notin E_2(\mathbb{Q}_p)$. We have $\ell\pi_1(P') - \ell\pi_1(P'') \notin E_2(\mathbb{Q}_p)$, since $E_2(\mathbb{Q}_p)$ has index p in $E_1(\mathbb{Q}_p)$, and $p \nmid \ell$, and therefore $\ell\pi_1(P'') \notin E_2(\mathbb{Q}_p)$. Hence in this case we can take P'' instead of P', and we are again done. □

4.5.3 The case of anomalous reduction

The most notable case to which Proposition 4.14 does not apply is the case where $\mathcal{E}(\mathbb{F}_p)$ has order p. Indeed, when we have $p > 5$ the Hasse–Weil bound implies that if $\mathcal{E}(\mathbb{F}_p)$ is divisible by p, then it must be equal to p.

Definition 4.15. We say that E has anomalous reduction if $\mathcal{E}(\mathbb{F}_p)$ is cyclic of order p.

In this section, we establish two criteria for the existence of Mestre points on C in the anomalous reduction case.

Remark 4.16. Assume that E has anomalous reduction at p, and that $p > 7$. We have the usual short exact sequence

$$0 \to E_1(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \to \mathcal{E}(\mathbb{F}_p) \to 0$$

as well as the topological isomorphism $E_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$ [32, IV.6.4(b)]. Then according to Proposition 1.14(iii), we have either $E(\mathbb{Q}_p) \cong \mathbb{Z}_p$ or $E(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$. In the first case, we have that $E(\mathbb{Q}_p)$ is procyclic, and the results of chapter 3 give that E has good twists. Therefore, the results from this section are only needed in the second case.

Lemma 4.17. *Assume that E has anomalous reduction. Let P_1 and P_2 be elements of $\mathcal{E}(\mathbb{Q}_p)$. Consider the following three statements.*

(i) The points P_1 and P_2 generate $\mathcal{E}(\mathbb{Q}_p)$ topologically.

(ii) The points P_1 are P_2 are not both contained in $\mathcal{E}_1(\mathbb{Q}_p)$.

(iii) There exists $n \in \mathbb{Z}$ such that $(P_1, P_2)_{\mathbb{F}_p}$ is contained in $\Gamma_n(\mathbb{F}_p)$, but $(P_1, P_2)_{\mathbb{Z}/p^2\mathbb{Z}}$ is not contained in $\Gamma_n(\mathbb{Z}/p^2\mathbb{Z})$.

Then (ii)+(iii) implies (i).

Proof. Assume that assumption (ii) and (iii) hold. In view of (ii), we only have to prove that $\langle P_1, P_2\rangle$ lies dense in $\mathcal{E}_1(\mathbb{Q}_p)$. Since we had assumed $p > 2$, we have $\mathcal{E}_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$; therefore it suffices to show that some integer linear combination of P_1 and P_2 lies in $\mathcal{E}_1(\mathbb{Q}_p) - \mathcal{E}_2(\mathbb{Q}_p)$. We let n be as in (iii). Then we have $P_2 - nP_1 \in \mathcal{E}_1(\mathbb{Q}_p) - \mathcal{E}_2(\mathbb{Q}_p)$. □

Anomalous reduction: a transversality criterion

To establish the first criterion for the existence of a Mestre point on C in the case of anomalous reduction, we reinterpret condition (iii) of Lemma 4.17 as the statement that a certain intersection is transversal.

Proposition 4.18. *Let $\mathcal{S}$ be a smooth surface over $\mathbb{Z}_p$, and let $\mathcal{D}_1, \mathcal{D}_2 \subset \mathcal{S}$ be smooth curves over $\mathbb{Z}_p$. Let $P \in \mathcal{S}(\mathbb{Z}_p)$. The following conditions are equivalent.*

(i) We have the following equality between subsets of $\mathcal{S}(\mathbb{Z}/p^2\mathbb{Z})$:

$$\left\{P' \in \mathcal{D}_1(\mathbb{Z}/p^2\mathbb{Z}) : (P')_{\mathbb{F}_p} = P_{\mathbb{F}_p}\right\} = \left\{P' \in \mathcal{D}_2(\mathbb{Z}/p^2\mathbb{Z}) : (P')_{\mathbb{F}_p} = P_{\mathbb{F}_p}\right\}.$$

(ii) The curves $(\mathcal{D}_1)_{\mathbb{F}_p}$ and $(\mathcal{D}_2)_{\mathbb{F}_p}$ are tangent to each other in $P_{\mathbb{F}_p}$.

Proof. The result can be seen as a variant of the multi-variable Hensel's lemma. A difference here is that we are only interested in lifting $\mathbb{F}_p$-points to $\mathbb{Z}/p^2\mathbb{Z}$-points.

By the fact that $\mathcal{S}$ is locally of finite type, we have that $\mathcal{S}$ is of the following form locally around $P_{\mathbb{F}_p}$

$$\operatorname{Spec} \mathbb{Z}_p[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$$

for $f_1, \ldots, f_r \in \mathbb{Z}_p[x_1, \ldots, x_n]$, where we may identify P with the section $\mathbf{0} = (0, \ldots, 0)$. Let $i \in \{1, 2\}$. Since $\mathcal{D}_i$ is smooth along P of relative dimension 1, there exist

$$g_{1,1}, \ldots, g_{1,n-1}, g_{2,1}, \ldots, g_{2,n-1} \in \mathbb{Z}_p[x_1, \ldots, x_n]$$

such that $\mathcal{D}_i$ is given as the zero-set $\mathcal{V}_i$ of

$$g_{i,1}, \ldots, g_{i,n-1}$$

locally around $\mathbf{0}$, where the $g_{i,j}$ are such that the matrix

$$\mathbf{T}_i = \begin{pmatrix} \frac{\partial g_{i,1}}{\partial x_1} & \cdots & \frac{\partial g_{i,1}}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial g_{i,n-1}}{\partial x_1} & \cdots & \frac{\partial g_{i,n-1}}{\partial x_n} \end{pmatrix}_{(0,\ldots,0)}$$

has an $(n-1)$-by-$(n-1)$ minor whose determinant is contained in $\mathbb{Z}_p^*$. As usual, the tangent space of $(\mathcal{D}_i)_{\mathbb{F}_p}$ at $\mathbf{0}_{\mathbb{F}_p}$ may be identified with the kernel of the matrix

$$\mathbf{T}_{i,\mathbb{F}_p}\Big|_{(0,\ldots,0)}$$

where $\mathbf{T}_{i,\mathbb{F}_p}$ denotes the entry-wise reduction modulo p of the matrix $\mathbf{T}_i$.

Since $\mathbb{Z}/p^2\mathbb{Z}$ is a local ring and $\mathcal{D}_i$ and $\mathcal{V}_i$ agree on open subsets containing P and $\mathbf{0}$ respectively, the $\mathbb{Z}/p^2\mathbb{Z}$-points of $\mathcal{D}_i$ reducing to $P_{\mathbb{F}_p}$ are in bijection with the $\mathbb{Z}/p^2\mathbb{Z}$-points of $\mathcal{V}_i$ reducing to $\mathbf{0}_{\mathbb{F}_p}$. It thus suffices to show that equality

$$\{P' \in \mathcal{V}_1(\mathbb{Z}/p^2\mathbb{Z}) : P'_{\mathbb{F}_p} = \mathbf{0}_{\mathbb{F}_p}\} = \{P' \in \mathcal{V}_2(\mathbb{Z}/p^2\mathbb{Z}) : P'_{\mathbb{F}_p} = \mathbf{0}_{\mathbb{F}_p}\} \tag{4.14}$$

is equivalent to

$$\ker(\mathbf{T}_{1,\mathbb{F}_p}) = \ker(\mathbf{T}_{2,\mathbb{F}_p}). \tag{4.15}$$

Let $Z_i = \{P' \in \mathcal{V}_i(\mathbb{Z}/p^2\mathbb{Z}) : P'_{\mathbb{F}_p} = \mathbf{0}_{\mathbb{F}_p}\}$. We can describe Z_i explicitly in terms of $\mathbf{T}_{i,\mathbb{F}_p}$: any $P' \in Z_i$ must be of the form

$$(\delta_1 p, \ldots, \delta_n p)$$

with $\delta_1, \ldots, \delta_n \in \mathbb{F}_p$. Let $P' = (\delta_1 p, \ldots, \delta_n p)$. By expanding the equations

$$g_{i,1}(\delta_1 p, \ldots, \delta_n p) = \ldots = g_{i,n-1}(\delta_1 p, \ldots, \delta_n p) = 0,$$

we find that for P' to be contained in Z_i, it is necessary and sufficient that

$$\mathbf{T}_i|_{(0,\ldots,0)} \cdot \begin{pmatrix} \delta_1 p \\ \vdots \\ \delta_n p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{in } (\mathbb{Z}/p^2\mathbb{Z})^{n-1}.$$

This shows that (4.14) and (4.15) are indeed equivalent. This finishes the proof. □

In order to be able to keep track of tangent directions on $(\mathcal{E} \times \mathcal{E})_{\mathbb{F}_p}$, we introduce the following definition.

Definition 4.19. Let κ be $\mathbb{Q}_p$ or $\mathbb{F}_p$, and denote by $\mathcal{E}_\kappa$ the base-change of $\mathcal{E}$ to κ. Let $\omega = \frac{dx}{y}$ be the standard invariant differential on $\mathcal{E}_\kappa$. Let D be a smooth curve on $(\mathcal{E} \times \mathcal{E})_\kappa$. If $P \in D(\kappa)$, then the tangent direction to D at P is

$$\left(\frac{i_2^*\omega}{i_1^*\omega}\right)(P) \in \mathbb{P}^1(\kappa), \tag{4.16}$$

where

$$(i_1, i_2) \colon D \to (\mathcal{E} \times \mathcal{E})_\kappa, \tag{4.17}$$

is the closed embedding of D into $(\mathcal{E} \times \mathcal{E})_\kappa$, and where the left-hand side of (4.16) denotes the value of the function $\frac{i_2^*\omega}{i_1^*\omega} \in \kappa(D)$ at P.

The above definition can be given in a dual form that is a little more involved, but shows more clearly the relationship between Definition 4.19 and tangent vectors.

Lemma 4.20. *Let κ be $\mathbb{Q}_p$ or $\mathbb{F}_p$, and denote by $\mathcal{E}_\kappa$ the base-change of $\mathcal{E}$ to κ. Let $\omega = \frac{dx}{y}$ as in Definition 4.19. For every $Q \in \mathcal{E}(\kappa)$, there is a unique tangent vector $\omega_Q^* \in T_Q\mathcal{E}_\kappa$ such that $\omega(\omega_Q^*) = 1$. Let D, i_1 and i_2 be as in Definition 4.19, and let $P \in D(\kappa)$ be a smooth point with $i_1(P) = Q_1$ and $i_2(P) = Q_2$. Choose a non-zero element $\eta \in T_P D$. Then the tangent direction to D at P is the image of η under the composite map*

$$T_P D \xrightarrow{(i_1,i_2)_*} T_{Q_1}\mathcal{E}_\kappa \times T_{Q_2}\mathcal{E}_\kappa \dashrightarrow \mathbb{P}^1(\kappa),$$

where the last arrow is the partially-defined map that sends $(t_1\omega_{Q_1}, t_2\omega_{Q_2})$ to $(t_2 : t_1)$ for all $t_1, t_2 \in \kappa$ that are not both zero.

Proof. We have that ω is a basis for the cotangent space $T_Q^*\mathcal{E}_\kappa$ for every $Q \in \mathcal{E}_\kappa$, so for each $Q \in \mathcal{E}(\kappa)$ there exists a unique tangent vector $\omega_Q^* \in T_Q\mathcal{E}_\kappa$ such that $\omega(\omega_Q^*) = 1$. Furthermore, ω_Q^* is a basis of $T_Q\mathcal{E}_\kappa$ for each Q, which shows that the map $T_{Q_1}\mathcal{E}_\kappa \times T_{Q_2}\mathcal{E}_\kappa \dashrightarrow \mathbb{P}^1(\kappa)$ is defined everywhere except at 0. Suppose that $t_1, t_2 \in \kappa$ are such that $(i_1, i_2)_*(\eta) = (t_1\omega_{Q_1}, t_2\omega_{Q_2})$. Then we have $i_1^*(\omega)(\eta) = \omega(i_{1*}(\eta)) = \omega(t_1\omega_{Q_1}) = t_1$, and likewise $i_2^*(\omega)(\eta) = t_2$. This shows that $i_2^*(\omega)/i_1^*(\omega)$ evaluated at P gives t_2/t_1, which is what we had to show. □

The following lemma is due to J. F. Voloch, to whom I am very grateful for mentioning it to me in a discussion about this chapter.

Lemma 4.21. *Assume that $\mathcal{E}(\mathbb{F}_p)$ is cyclic of order p. Write*

$$f(x)^{(p-1)/2} = U(x) + Ax^{p-1} + x^p V(x)$$

for some $U(x)$ of degree at most $p-2$ and $V(x)$ of degree $(p-3)/2$. Then the map

$$\begin{aligned} \mathcal{E}(\mathbb{F}_p) &\to \mathbb{F}_p \\ (x, y) &\mapsto yV(x) \end{aligned}$$

is an isomorphism of groups.

Proof. Let $\phi\colon \mathcal{E}'_{\mathbb{F}_p} \to \mathcal{E}_{\mathbb{F}_p}$ the isogeny dual to the Frobenius. Since $\mathcal{E}(\mathbb{F}_p)[p] \neq 0$, we have that ϕ is separable and its image equals $p\mathcal{E}(\mathbb{F}_p) = 0$. The result now follows from Proposition 1.3 in [40]. □

The proof of the following proposition makes essential use of the smoothness of $\mathcal{C}^\circ$.

Proposition 4.22. *Suppose that E has anomalous reduction. Write*

$$f(x)^{(p-1)/2} = U(x) + Ax^{p-1} + x^p V(x) \tag{4.18}$$

for some $U(x)$ of degree at most $p-2$ and $V(x)$ of degree $(p-3)/2$. Write $\omega = dx/y$ for the standard invariant differential on $\mathcal{E}_{\mathbb{F}_p}$. Assume that there exists a point $P \in \mathcal{C}^\circ(\mathbb{F}_p)$ such that

$$\left(\frac{\pi_2^*\omega}{\pi_1^*\omega}\right)(P) \neq \left(\frac{\pi_2^* yV(x)}{\pi_1^* yV(x)}\right)(P), \tag{4.19}$$

where the value infinity is allowed for both sides. Then C has a Mestre point.

Proof. Recall that we denote by τ the automorphism of $\mathcal{E} \times \mathcal{E}$ that interchanges both factors. Replacing P by $\tau(P)$ amounts to replacing both sides of (4.19) by their inverses. Possibly after replacing P by $\tau(P)$, we may assume that $\pi_1(P) \neq 0$, so there exists an integer n such that $\pi_2(P) = n\pi_1(P)$, which is equivalent to $P \in \Gamma_n(\mathbb{F}_p)$.

The left-hand side of (4.19) is the tangent direction to $\mathcal{C}^\circ_{\mathbb{F}_p} \subset (\mathcal{E} \times \mathcal{E})_{\mathbb{F}_p}$ at P. For the right-hand side, we have

$$\left(\frac{\pi_2^* yV(x)}{\pi_1^* yV(x)}\right)(P) = n$$

by Proposition 4.21 and the definition of n. We claim that the tangent direction to $(\Gamma_n)_{\mathbb{F}_p}$ at P is n. The curve Γ_n arises as the image of the closed immersion

$$(i_1, i_2)\colon \mathcal{E} \to \mathcal{E} \times \mathcal{E}$$

defined on points by $e \mapsto (e, ne)$. Using Definition 4.19, we see that the tangent direction to $(\Gamma_n)_{\mathbb{F}_p}$ at any point P' is

$$\left(\frac{i_2^*\omega}{i_1^*\omega}\right)(P') = n.$$

(This uses the fact that $[n]^*\omega = n\omega$, where $[n]\colon \mathcal{E}_{\mathbb{F}_p} \to \mathcal{E}_{\mathbb{F}_p}$ is multiplication by n; see [32, III.5.3].) Hence the statement (4.19) is equivalent to the tangent direction to $\mathcal{C}^\circ$ at P not being equal to the tangent direction to Γ_n at P. Then by Proposition 4.18, there exists a point $P' \in \mathcal{C}^\circ(\mathbb{Z}/p^2\mathbb{Z})$

with $(P')_{\mathbb{F}_p} = P$, but $P' \notin \Gamma_n(\mathbb{Z}/p^2\mathbb{Z})$. By Hensel's lemma, there exists $P'' \in \mathcal{C}^\circ(\mathbb{Z}_p) \subset C(\mathbb{Q}_p)$ so that P'' satisfies $(P'')_{\mathbb{Z}/p^2\mathbb{Z}} = P'$. Let $Q_1 = \pi_1(P'')$ and $Q_2 = \pi_2(P'')$. The condition $(P'')_{\mathbb{Z}/p^2\mathbb{Z}} \notin \Gamma_n(\mathbb{Z}/p^2\mathbb{Z})$ implies that $Q_2 - nQ_1 \in E_1(\mathbb{Q}_p) - E_2(\mathbb{Q}_p)$, and hence by Lemma 4.17 we have that Q_1 and Q_2 are topological generators of $E(\mathbb{Q}_p)$. This concludes the proof. □

Remark 4.23. By expanding, we can make the inequality (4.19) more explicit. It says that, for a point $P = (u_0, v_0) \in \mathcal{C}(\mathbb{F}_p)$, we have

$$-\frac{u_0^3(u_0^2+2)}{2u_0^2+1} \neq \frac{u_0^3 V(-b/a \cdot (u_0^4+u_0^2+1)/(u_0^2+1))}{V(-b/a \cdot (u_0^4+u_0^2+1)/(u_0^4+u_0^2)))}$$

with V defined as in (4.18). It seems difficult in general to prove that there exists a point $P = (u_0, v_0) \in \mathcal{C}(\mathbb{F}_p)$ for which this inequality is satisfied. For instance, the degree of the rational function on the right-hand side grows linearly with p, so that the naive estimate comparing the number of zeros of a rational function on $\mathcal{C}$ with the number of points in $\mathcal{C}(\mathbb{F}_p)$ will not work.

Anomalous reduction: an explicit criterion

Proposition 4.24. *Suppose that E has anomalous reduction. Assume that $-ab \in \mathbb{Q}_p^{*2}$. Then C has a Mestre point.*

Proof. We assume $-ab \in \mathbb{Q}_p^{*2}$. We will prove the existence of $P \in C(\mathbb{Q}_p)$ such that $Q_1 = \pi_1(P)$ is contained in $E_1(\mathbb{Q}_p) - E_2(\mathbb{Q}_p)$ and $Q_2 = \pi_2(P)$ is contained in $E(\mathbb{Q}_p) - E_1(\mathbb{Q}_p)$. Since $E(\mathbb{Q})$ is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$, where in the latter case the subgroup $\mathbb{Z}_p$ corresponds to $E_1(\mathbb{Q}_p)$, the points Q_1 and Q_2 generate $E(\mathbb{Q}_p)$ topologically.

Let $Q_1 = (x_0, y_0) \in E_1(\mathbb{Q}_p) - E_2(\mathbb{Q}_p)$ be arbitrary. Observe that we have $v_p(x_0) = -2$. Also, since $y_0^2 = x_0^3 + ax_0 + b$, we have $x_0 \in \mathbb{Q}_p^{*2}$. Then, for $u_0 \in \mathbb{Q}_p$, the statement that $P = (u_0, y_0)$ is contained in $C(\mathbb{Q}_p)$ and is such that $\pi_1(P) = Q_1$ is equivalent to

$$x_0 = \phi(u_0) = -\frac{b}{a}\frac{w_0^2 + w_0 + 1}{w_0^2 + w_0}, \tag{4.20}$$

where we have put $w_0 = u_0^2$. Solving this equation for w_0, we get

$$w_+ = -\frac{1}{2} + \frac{1}{2}\sqrt{1 - \frac{4b}{ax_0 + b}} \quad \text{and} \quad w_- = -\frac{1}{2} - \frac{1}{2}\sqrt{1 - \frac{4b}{ax_0 + b}} \tag{4.21}$$

Since $v_p(4b/(ax_0+b)) = 2$, we have $w_+ \in \mathbb{Q}_p$. Moreover, by p-adically expanding the square roots in the expressions (4.21), we obtain

$$w_+ = -\frac{1}{2} + \frac{1}{2}\left(1 - \frac{1}{2}\frac{4b}{ax_0+b} + O(p^4)\right) = -\frac{b}{ax_0+b} + O(p^4) \qquad (4.22)$$

and

$$w_- = -\frac{1}{2} - \frac{1}{2}\left(1 - \frac{1}{2}\frac{4b}{ax_0+b} + O(p^4)\right) = -1 + \frac{b}{ax_0+b} + O(p^4)$$

We have that x_0 and $-b/a$ are both contained in $\mathbb{Q}_p^{*2}$, so that w_+ is a p-adic square. Therefore, there exists $u_0 \in \mathbb{Q}_p$ that satisfies (4.20), and equation (4.22) shows that $v_p(w_+) = -v_p(x_0) = 2$. We have that $P = (u_0, y_0)$ maps to $Q_1 \in E_1(\mathbb{Q}_p)$. Moreover, $Q_2 = \pi_2(u_0, y_0)$ is equal to $Q_2 = (u_0^2\phi(u_0), u_0^3 y_0) = (u_0^2 x_0, u_0^3 y_0)$, which is obviously contained in $E(\mathbb{Q}_p) - E_1(\mathbb{Q}_p)$. This proves the proposition. (Note that we couldn't have used w_- even if $-1 \in \mathbb{Q}_p^{*2}$, since in that case both $\pi_1(\sqrt{w_-}, y_0)$ and $\pi_2(\sqrt{w_-}, y_0)$ would lie in $E_1(\mathbb{Q}_p)$.) □

4.5.4 Good points over ramified twists

For $d \in \mathbb{Q}_p^*$, recall that a twist E^d of E is called ramified if the valuation of d is odd. For such d, the existence of Mestre points on C^d is guaranteed by Proposition 4.26 in the case where E^d has the full 2-torsion over $\mathbb{Q}_p$. (In the other cases we will have that $E^d(\mathbb{Q}_p)$ is procyclic, so we can apply the results of the previous chapter.)

Lemma 4.25. *Let $d \in \mathbb{Q}_p^*$ be an element of valuation 1. Then the quadratic twist E^d of E has Kodaira type I_0^*, and $E^d(\mathbb{Q}_p)[2]$ contains no non-zero points of good reduction.*

Proof. The 2-torsion of E^d is defined over any extension of $\mathbb{Q}_p$ that contains the roots of the polynomial

$$x^3 + ad^2x + bd^3 = d^3 f(x/d). \qquad (4.23)$$

As (4.23) shows, the same is true over any extension of $\mathbb{Q}_p$ that contains the roots of f. Since $f \pmod p$ is separable over $\mathbb{F}_p$, the roots of f are contained in an unramified extension of $\mathbb{Q}_p$. The 2-torsion of E^d is therefore defined over the maximal unramified extension $\mathbb{Q}_p^{\mathrm{un}}$ of $\mathbb{Q}_p$. Equation (4.23) shows that for any $x_0 \in \mathbb{Q}_p^{\mathrm{un}}$, we have that x_0 is a root of f if and only if $(dx_0, 0)$ is a point in $E^d(\mathbb{Q}_p^{\mathrm{un}})$. Since $y^2 = x^3 + ad^2x + bd^3$ defines a minimal Weierstrass model of E^d, the non-trivial 2-torsion of $E^d(\mathbb{Q}_p^{\mathrm{un}})$ is of bad reduction, which shows that $E^d(\mathbb{Q}_p^{\mathrm{un}})/E_0^d(\mathbb{Q}_p^{\mathrm{un}})$ contains the Klein four-group. The only Kodaira type for which the component group contains the Klein four-group is I_0^* (see [32, C.15]), so this must be the Kodaira type of E^d. □

Proposition 4.26. *Let $d \in \mathbb{Q}_p^*$ be an element of valuation 1. Assume furthermore that either $p > 7$ or $E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$, and assume furthermore that $\#E^d(\mathbb{Q}_p)[2] = 4$. Then there exists a Mestre point $P \in C^d(\mathbb{Q}_p)$.*

Proof. The assumption that either $p > 7$ or $E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$ is there to guarantee $E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$. (See Theorem 1.1; note that E^d has additive reduction.) Putting $\Phi = E^d(\mathbb{Q}_p)/E_0^d(\mathbb{Q}_p)$, we have the usual short exact sequence

$$0 \to \mathbb{Z}_p \to E^d(\mathbb{Q}_p) \to \Phi \to 0,$$

with Φ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ by Lemma 4.25. Proposition 1.14(iv) shows that $E^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p \times (\mathbb{Z}/2\mathbb{Z})^2$.

When denoting points on E^d, we shall be using the equation $dy^2 = f(x)$ for it. By performing Tate's algorithm on a Weierstrass model for E^d, we find that the three non-trivial cosets of $E_0^d(\mathbb{Q}_p)$ in $E^d(\mathbb{Q}_p)$ are of the following form:

$$S_e = \left\{(x_0, y_0) \in E^d(\mathbb{Q}_p) : x_0 \equiv e \pmod{p}\right\},$$

where $e \in \mathbb{Z}_p^*$ is one of the three roots of f. We may apply Proposition 4.12 to $\overline{f}$, using $\phi_2(u) = \phi_1(u^{-1})$, to find that there exist two distinct roots e_1 and e_2 of f, such that if we put $\alpha_1 = \overline{e_1}$ and $\alpha_2 = \overline{e_2}$, there exist elements β_1 and β_2 of $\mathbb{F}_p$ such that

$$\overline{\phi}(\beta_1) = \alpha_1, \quad \overline{\phi}(\beta_2) = \alpha_2$$

and

$$\overline{\phi}(\beta_1^{-1}) = \alpha_2, \quad \overline{\phi}(\beta_2^{-1}) = \alpha_1,$$

where we use $\overline{\cdot}$ to denote reduction modulo p. These identities imply that for any point $P' = (u_1, v_1)$ in $C^d(\mathbb{Q}_p)$ such that $\overline{u_1} = \beta_1$, if we write $\pi_1(P') = (x_1, y_1)$ and $\pi_2(P') = (x_2, y_2)$, then we have $\overline{x_1} = \alpha_1$ and $\overline{x_2} = \alpha_2$ in $\mathbb{F}_p$.

Let $Q_1 = (x_1, y_1)$ be an arbitrary point in $E^d(\mathbb{Q}_p) - E_0^d(\mathbb{Q}_p)$ with $x_1 \equiv e_1 \pmod{p}$. We will construct a point $P = (u_1, v_1)$ in $C^d(\mathbb{Q}_p)$ such that $\pi_1(P) = Q_1$. Such a P may be constructed from a solution $u = u_1$ to the equation

$$-\frac{b}{a}\frac{u^4 + u^2 + 1}{u^4 + u^2} = x_1, \tag{4.24}$$

since for a solution u_1 to (4.24), the morphism π_1 maps $P = (u_1, y_1)$ to Q_1. Over $\mathbb{F}_p$, the reduction modulo p of (4.24) has 4 distinct solutions, since the right-hand side reduces to α_1, and we know from Proposition 4.8(i) that π_1 is unramified above the point $(\alpha_1, 0)$ on the smooth curve $\mathcal{E}_{\mathbb{F}_p}$. We may thus apply Hensel's lemma to find a solution u_1 such that $\overline{u_1} = \beta_1$. We define $P = (u_1, y_1)$. Then we have $\pi_1(P) = Q_1$, as desired. Moreover, by the previous paragraph, we also have $\pi_2(P) = (x_2, y_2)$, with x_2 an element of $\mathbb{Z}_p$ such that $\overline{x_2} = \alpha_2$.

Now take $Q_1 = (x_1, y_1)$ to be a point in $E^d(\mathbb{Q}_p)$ such that $x_1 \equiv e_1 \pmod{p}$ and such that some multiple of Q_1 lies in $E_0^d(\mathbb{Q}_p) - E_1^d(\mathbb{Q}_p)$. (We know that such a Q_1 exists by the fact that the points (x_1, y_1) satisfying $x_1 \equiv e_1 \pmod{p}$ make up a coset of $E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$ in $E^d(\mathbb{Q}_p) \cong \mathbb{Z}_p \times (\mathbb{Z}/2\mathbb{Z})^2$.) Then by the previous paragraph, there exists P in $C^d(\mathbb{Q}_p)$ such that $Q_1 = \pi_1(P)$ and $Q_2 = \pi_2(P)$ lie in different non-trivial cosets of $E_0^d(\mathbb{Q}_p)$ in $E^d(\mathbb{Q}_p)$. Since in addition some multiple of Q_1 lies in $E_0^d(\mathbb{Q}_p) - E_1^d(\mathbb{Q}_p)$, it is clear that Q_1 and Q_2 generate $E^d(\mathbb{Q}_p)$ topologically. □

4.6 Existence criteria for good twists

We let $p > 2$ be a prime number and a and b rational numbers of non-negative p-adic valuation such that

$$ab(4a^3 + 27b^2)$$

is a p-adic unit. We let E be the elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 + ax + b$. In this section, we will combine the results of section 4.5 with Lemma 4.6 to give existence results on good twists, given $d \in \mathbb{Q}_p^*$, of E with respect to d and p.

4.6.1 Unramified twists

The following definitions are made in order to apply the results of section 4.5 to (unramified) twists E^d of E, instead of just E itself. Instead of the curves E^d, given by $dy^2 = x^3 + ax + b$, we consider the curves E'^d, which are given by $y^2 = x^3 + ad^2x + bd^3$. The curves E^d and E'^d are isomorphic for each d, but the E'^d have the advantage that they are given by Weierstrass equations.

Definition 4.27. For $d \in \mathbb{Z}_p^*$, we let E'^d be the elliptic curve given by $y^2 = x^3 + ad^2x + bd^3$ and $\mathcal{E}'^d$ the smooth Weierstrass curve over $\mathbb{Z}_p$ given by the same equation. Note that E'^d is isomorphic to E^d and that $\mathcal{E}'^d$ is a smooth Weierstrass model of E'^d. We let C'^d be the curve arising from the construction in section 4.2.1 applied to the case where E is replaced by the elliptic curve E'^d. Note that C'^d is isomorphic to C^d as defined in section 4.2.1. We define $Z'^d \subset C'^d$ in the same way as we defined Z for C (see the start of section 4.4). As in section 4.2.1, we have maps

$$\pi_1'^d \colon C'^d \to E'^d, \quad \pi_2'^d \colon C'^d \to E'^d,$$

and we define the notion of a Mestre point on C'^d in the same way we did for C^d. We denote by $i'^d \colon C'^d \to E'^d \times E'^d$ the map $i'^d = (\pi_1'^d, \pi_2'^d)$. We let $\mathcal{C}'^d \subset \mathcal{E}'^d \times \mathcal{E}'^d$ be the closure of $i'^d(C'^d)$. The morphisms $\pi_1'^d$ and $\pi_2'^d$ extend to morphisms $\pi_1'^d, \pi_2'^d \colon \mathcal{C}'^d \to \mathcal{E}'^d$. We let $\mathcal{Z}'^d \subset \mathcal{E}'^d \times \mathcal{E}'^d$ be the closure of $i'^d(Z'^d)$. Finally, the smooth subscheme $\mathcal{C}'^d - \mathcal{Z}'^d$ of $\mathcal{E}'^d \times \mathcal{E}'^d$ we will denote by $\mathcal{C}'^d_{\text{smooth}}$.

Remark 4.28. One checks that the isomorphisms between E'^d and E^d and between C^d and C'^d can be chosen in such a way that, for $d \in \mathbb{Z}_p^*$ and $i \in \{1, 2\}$, the diagram

$$\begin{tikzcd}
C^d \arrow[r, "\sim"] \arrow[d, "\pi_i^d"] & C'^d \arrow[d, "\pi_i'^d"] \\
E^d \arrow[r, "\sim"] & E'^d
\end{tikzcd}$$

commutes. Thus C'^d has a Mestre point if and only if C^d does.

Unramified twists: the non-anomalous reduction case

Let $d \in \mathbb{Q}_p^*$ be an element with $v_p(d) = 0$.

Proposition 4.29. *Assume that the order of $\mathcal{E}'^d(\mathbb{F}_p)$ is coprime to p. Let $P \in \mathcal{C}'^d(\mathbb{F}_p)$. If the points $\pi_1'^d(P)$ and $\pi_2'^d(P)$ generate $\mathcal{E}'^d(\mathbb{F}_p)$, then there exists a good twist of E with respect to d and p.*

Proof. Proposition 4.14, with E replaced by E'^d, implies that C'^d has a Mestre point. By Remark 4.28, so does C^d. The result now follows from Lemma 4.6. □

The following proposition deals with the special case of cyclic non-anomalous reduction. It is partly a corollary of the results from the previous chapter.

Proposition 4.30. *Assume that $\mathcal{E}'^d(\mathbb{F}_p)$ is cyclic of order coprime to p. Then there exists a good twist of E with respect to d and p.*

Proof. We have that $E'^d(\mathbb{Q}_p)$ sits inside a short exact sequence with continuous maps, and with the second map an embedding

$$0 \to E_1'^d(\mathbb{Q}_p) \to E'^d(\mathbb{Q}_p) \to \mathcal{E}'^d(\mathbb{F}_p) \to 0,$$

where $E_1'^d(\mathbb{Q}_p)$ is procyclic and $\mathcal{E}'^d(\mathbb{F}_p)$ is cyclic of order coprime to p. By Proposition 1.14(ii), we have that $E'^d(\mathbb{Q}_p)$ is procyclic, and therefore so is $E^d(\mathbb{Q}_p)$. By Proposition 3.27 we find that E has a good twist with respect to d and p. □

Unramified twists: the anomalous reduction case

Again, we let $d \in \mathbb{Q}_p^*$ be an element with $v_p(d) = 0$.

Proposition 4.31. *Assume that the order of $\mathcal{E}'^d(\mathbb{F}_p)$ is equal to p. Write*

$$\left(x^3 + ad^2x + bd^3\right)^{(p-1)/2} = U(x) + Ax^{p-1} + x^pV(x) \tag{4.25}$$

for some $U(x)$ of degree at most $p-2$ and $V(x)$ of degree $(p-3)/2$. Write

$$\omega = \frac{dx}{y} \tag{4.26}$$

for the standard invariant differential on $(\mathcal{E}'^d)_{\mathbb{F}_p}$. Assume that there exists a point $P \in \mathcal{C}'^d_{\text{smooth}}(\mathbb{F}_p)$ such that

$$\left(\frac{\pi_2^*\omega}{\pi_1^*\omega}\right)(P) \neq \left(\frac{\pi_2^*yV(x)}{\pi_1^*yV(x)}\right)(P), \tag{4.27}$$

where the value infinity is allowed for both sides. Then E has a good twist with respect to d and p.

Proof. From Proposition 4.22, with E replaced by E'^d, it follows that C'^d has a Mestre point. By Remark 4.28, so does C^d. The result follows from Lemma 4.6. □

Proposition 4.32. *Suppose that E^d has anomalous reduction at p. Assume that $-abd \in \mathbb{Q}_p^{*2}$. Then E has a good twist with respect to d and p.*

Proof. From Proposition 4.24, with E replaced by E'^d, it follows that C'^d has a Mestre point. By Remark 4.28, so does C^d. The result follows from Lemma 4.6. □

4.6.2 Ramified twists

If $d \in \mathbb{Q}_p^*$ is such that $v_p(d) = 1$, and p is greater than 7, it is very easy to prove that E has good twists with respect to d and p.

Proposition 4.33. *Let $d \in \mathbb{Q}_p^*$ be an element of valuation one. Assume also that either $p > 7$ or $E_0^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$. Then E has a good twist with respect to d and p.*

Proof. We know from Lemma 4.25 that E^d has Kodaira type I_0^*, so that $E^d(\mathbb{Q}_p)$ fits inside an exact sequence

$$0 \to E_0^d(\mathbb{Q}_p) \to E^d(\mathbb{Q}_p) \to \Phi \to 0,$$

with $E_0^d(\mathbb{Q}_p)$ topologically isomorphic to $\mathbb{Z}_p$, and Φ isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2$. Proposition 1.14(iv) shows that we have

$$E^d(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \Phi \tag{4.28}$$

as topological groups. By (4.28) and since Φ is isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2$, we have that Φ is isomorphic to the torsion subgroup of $E^d(\mathbb{Q}_p)[2]$. If Φ is not isomorphic to the full $(\mathbb{Z}/2\mathbb{Z})^2$, then $E^d(\mathbb{Q}_p)$ is a product of two procyclic groups of coprime order, hence procyclic, and we may apply Proposition 3.27 to find that E has good twists with respect to d and p. If $\Phi \cong (\mathbb{Z}/2\mathbb{Z})^2$, we may apply Proposition 4.26 to find that C^d has a Mestre point, and the result follows from Lemma 4.6 again. □

4.7 A computer experiment

Propositions 4.29–4.33 provide five criteria implying the existence of good twists of E, and hence the p-adic density of rational points on $\mathrm{Km}(E \times E)$ by Theorem 3.20. These criteria are all formulated in terms of elliptic curves over finite fields, and hence are well-suited to do a computer search. In this section, we list the results of a computer search we have performed using the open-source Computer Algebra System `sage` [35].

For the purpose of this section only, we will introduce the notion of a lucky prime for E. Very loosely speaking, a prime p will be called lucky for E if we can deduce from Propositions 4.29–4.33 and Theorem 3.20 that E has good twists with respect to p. We keep the notation introduced in Definition 4.27.

Definition 4.34. We will call a prime p lucky (for E) if p is greater than 7, the elliptic curve E can be given by a short Weierstrass equation

$$y^2 = x^3 + ax + b \tag{4.29}$$

with a and b in $\mathbb{Q}^*$ such that $v_p(a) = v_p(b) = v_p(ab(4a^3 + 27b^2)) = 0$, and for all $d \in \mathbb{Q}_p^*$ with $v_p(d) \in \{0, 1\}$ at least one of the following criteria is satisfied:

(C1) we have $v_p(d) = 0$, the order of $\mathcal{E}'^d(\mathbb{F}_p)$ is coprime to p, and there exists $\overline{P} \in \mathcal{C}'^d(\mathbb{F}_p)$ such that $\pi_1'^d(\overline{P})$ and $\pi_2'^d(\overline{P})$ generate $\mathcal{E}'^d(\mathbb{F}_p)$;

(C2) we have $v_p(d) = 0$, and $\mathcal{E}'^d(\mathbb{F}_p)$ is cyclic of order coprime to p;

(C3) we have $v_p(d) = 0$, the order of $\mathcal{E}'^d(\mathbb{F}_p)$ is equal to p, and for some $\overline{P} \in \mathcal{C}'^d_{\text{smooth}}(\mathbb{F}_p)$ we have

$$\left(\frac{\pi_2^*\omega}{\pi_1^*\omega}\right)(P) \neq \left(\frac{\pi_2^* yV(x)}{\pi_1^* yV(x)}\right)(P), \tag{4.30}$$

where ω is as in (4.26) and V is as in (4.25);

(C4) we have $v_p(d) = 0$, the order of $\mathcal{E}'^d(\mathbb{F}_p)$ equals p, and $-abd \in \mathbb{Q}_p^{*2}$;

(C5) we have $v_p(d) = 1$.

If p is not lucky for E, then we will call it unlucky (for E). Note that the set of primes that are unlucky for E include the primes p for which E has bad reduction.

The ultimate use of the above definition is recorded in the following proposition.

Proposition 4.35. *Let p be a lucky prime for E. If $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$.*

Proof. By Theorem 3.20, it suffices to show that if $d \in \mathbb{Q}_p^*$, then E has a good twist with respect to d and p. Obviously, we may assume that $v_p(d) = 0$ or $v_p(d) = 1$. Choose an arbitrary d with $v_p(d) = 0$ or $v_p(d) = 1$. One proceeds in a manner depending on d: if (C1) is satisfied, apply Proposition 4.29; if (C2) is satisfied, apply Proposition 4.30; if (C3) is satisfied, apply Proposition 4.31; if (C4) is satisfied, apply Proposition 4.32; if (C5) is satisfied, apply Proposition 4.33. □

Remark 4.36. In fact, to verify whether p is a lucky prime for E, we only need to check the conditions (C1)–(C5) for d running through a set of coset representatives of $\mathbb{Q}_p^{*2}$ in $\mathbb{Q}_p^*$, which has only four elements. In fact, since (C5) automatically holds for the two coset representatives for which $v_p(d) = 1$, it suffices to check the conditions (C1)–(C4) for a single d such that $d \in \mathbb{Z}_p^{*2}$, and a single d for which $d \in \mathbb{Z}_p^* - \mathbb{Z}_p^{*2}$.

4.7.1 Results of the experiment

In our search, we consider the set $S_{5,5}$ of all elliptic curves $E_{a,b}$ over $\mathbb{Q}$ given by a short Weierstrass equation

$$E_{a,b}\colon y^2 = x^3 + ax + b$$

with $-5 \leq a \leq 5$, where $a \neq 0$, and $0 < b \leq 5$, as well as the 299 prime numbers p such that $7 < p < 2000$. For each of the curves $E_{a,b}$ and each prime p in the sets just described, we have let the computer decide the question whether p is lucky for $E_{a,b}$.

From the results of our experiments, it seems that the criteria developed in this thesis always seem to yield the existence of good twists with respect to p, roughly speaking, once p is large enough. The following table shows this more precisely. For each of the 49 elliptic curves E in our search space, we list the set of unlucky primes p with $7 < p < 2000$, along with its cardinality $N_{a,b}$. The asterisks denote primes of bad reduction.

(a,b)	Set of unlucky primes for $E_{a,b}$	$N_{a,b}$
$(-5,1)$	$\{11^*, 43^*, 73\}$	3
$(-5,2)$	$\{17, 23, 47\}$	3
$(-5,3)$	$\{257^*\}$	1
$(-5,4)$	$\{13, 17^*, 19, 43, 53, 67\}$	6
$(-5,5)$	$\{53\}$	1
$(-4,1)$	$\{37, 229^*\}$	2
$(-4,2)$	$\{37^*\}$	1
$(-4,3)$	$\{13^*, 17, 23, 29, 43\}$	5
$(-4,4)$	$\{11^*, 47\}$	2
$(-4,5)$	$\{43, 419^*\}$	2
$(-3,1)$	$\{17, 19, 37\}$	3
$(-3,3)$	$\emptyset$	0
$(-3,4)$	$\{13, 53, 67\}$	3
$(-3,5)$	$\{23, 29\}$	2
$(-2,1)$	$\{11, 19, 29, 41\}$	4
$(-2,2)$	$\{19^*, 23\}$	2
$(-2,3)$	$\{11, 53, 109, 211^*\}$	4
$(-2,4)$	$\{13, 17, 29, 37\}$	4
$(-2,5)$	$\{643^*\}$	1
$(-1,1)$	$\{23^*\}$	1
$(-1,2)$	$\{13^*\}$	1
$(-1,3)$	$\{239^*\}$	1

(a, b)	set of unlucky primes for $E_{a,b}$	$N_{a,b}$
$(-1, 4)$	$\{13, 29, 107^*\}$	3
$(-1, 5)$	$\{11^*, 17, 43, 61^*\}$	4
$(1, 1)$	$\{31^*\}$	1
$(1, 2)$	$\{11, 23, 37, 43\}$	4
$(1, 3)$	$\{13^*, 17, 19^*\}$	3
$(1, 4)$	$\{109^*\}$	1
$(1, 5)$	$\{11, 97^*\}$	2
$(2, 1)$	$\{17, 59^*\}$	2
$(2, 2)$	$\{17\}$	1
$(2, 3)$	$\{11^*, 23, 31, 37, 47, 53, 67, 71\}$	8
$(2, 4)$	$\{19, 29^*\}$	2
$(2, 5)$	$\{101^*\}$	1
$(3, 1)$	$\{47, 73\}$	2
$(3, 2)$	$\{11, 29, 79\}$	3
$(3, 3)$	$\{11, 13^*, 41\}$	3
$(3, 4)$	$\{17, 19, 23, 53\}$	4
$(3, 5)$	$\{29^*\}$	1
$(4, 1)$	$\{71, 283^*\}$	1
$(4, 2)$	$\{13^*\}$	1
$(4, 3)$	$\{499^*\}$	1
$(4, 4)$	$\{11, 13, 43^*, 47\}$	4
$(4, 5)$	$\{11, 17, 19^*, 23, 43, 47, 61\}$	7
$(5, 1)$	$\{11, 17^*, 19, 29, 31^*\}$	5
$(5, 2)$	$\{19^*, 37, 47\}$	3
$(5, 3)$	$\{37, 743^*\}$	2
$(5, 4)$	$\{11, 233^*\}$	2
$(5, 5)$	$\{37, 47^*, 53, 61\}$	4

Proof of Theorem 4.2. This follows from the table above. □

4.8 sage code

This section lists the `sage` source code that was used to perform the computations described in section 4.7.

4.8.1 Looking for two-element sets of generators

This procedure takes as input two elements of an abelian group isomorphic to $\mathbb{Z}/mZ \oplus \mathbb{Z}/n\mathbb{Z}$ with $m \mid n$, and decides whether or not they generate it.

```
# Given a list of two elements P, Q of an abelian group A
# isom. to Z/m + Z/n, with m | n, check whether <P,Q> = A.

def isSetOfGenerators(A,elements):
    P = elements[0]; Q = elements[1]
    m = A.invariants()[0]; n = A.invariants()[1]
    # we take n to be at least m
    if m > n:
        r = m
        m = n
        n = r

    # if ord(P) < ord(Q), switch P and Q.
    if P.order() != n:
        R = P
        P = Q
        Q = R

    # if ord(P) < n still holds, then <P,Q> != A.
    if P.order() != n:
        return false

    # order of Q has to be multiple of m.
    Q_order = Q.order()
    if Q_order % m != 0:
        return false

    P_multiples = set([i*P for i in range(n)])
    Q_multiples = set([j*Q for j in range(1,m)])

    # check if {i*P} and {j*Q : 0<j<m} have empty int'n
    return (P_multiples.intersection(Q_multiples) == set([]))
```

4.8.2 Finding pairs in the image of $\mathcal{C}(\mathbb{F}_p)$

The following procedure takes an elliptic curve over $\mathbb{F}_p$ as input, and finds the pairs $(Q_1, Q_2) \in \mathcal{E}(\mathbb{F}_p) \times \mathcal{E}(\mathbb{F}_p)$ such that $Q_1 = \pi_1(P)$ and $Q_2 = \pi_2(P)$ for some $P \in \mathcal{C}(\mathbb{F}_p)$.

```
# given an elliptic curve E over F_p as input
# find the elements in the image of C(F_p) -> E(F_p) x E(F_p).

def findPairs(E):
    a = E.a4(); b = E.a6()

    K = a.base_ring()
    R.<u> = PolynomialRing(K)
    S.<x> = PolynomialRing(K)

    p = K.characteristic()
    alpha = K.multiplicative_generator()

    gamma = -b/a
    phi = gamma*(u^4+u^2+1)/(u^4+u^2)
    f = x^3+a*x+b

    # don’t need to consider u with u^4 + u^2 = 0
    # (maps to infinity)
    # also use the fact that u, u^-1, -u, -u^-1 all
    # give the same pair of points on E: therefore
    # u only needs to range up to (p-1)/4.

    alpha_range = range(1,(p-1)/4)
    u_list = [alpha^i for i in alpha_range]
    pairsList = []

    for u_0 in u_list:

        x_0 = phi(u_0)
        # is x_0 the x-coordinate of a point in E(F_p)?
        f_0 = f(x_0)
        if f_0.is_square() == false:
            continue
        y_0 = f_0.sqrt()

        # append the pair of points that was found
        pairsList.append([[E.point([x_0,y_0]),E.point(
        [u_0^2*x_0,u_0^3*y_0])],u_0])

    return pairsList
```

4.8.3 The criteria involving anomalous reduction

The procedure `checkAnomalousCurve` takes an elliptic curve over $\mathbb{F}_p$ as input, and determines whether either of Propositions 4.31–4.32 applies to it. It returns 2 if this is the case, and 3 otherwise. The procedure `computeV` computes the polynomial V from Lemma 4.21.

```
# given f in F_p[x], compute V
# such that x^p*V + A*x^(p-1) + U(x) = f(x)^((p-1)/2)
# with deg(U) < p-1

def computeV(f):

    K = f.base_ring()
    R.<x> = PolynomialRing(K)
    p = K.characteristic()

    g = f^((p-1)/2)
    coeff_list = g.coeffs()

    V = 0
    for i in range(p,len(coeff_list)):
        V += coeff_list[i]*x^(i-p)

    return V

# input: elliptic curve E over GF(p) with j != 0 or 1728 and
# E.order() == p
# output: 2 if a good twist was found, 3 otherwise

def checkAnomalousCurve(E):
    a = E.a4(); b = E.a6()
    K = a.base_ring()
    p = K.characteristic()

    if E.order() != p:
        print("Number of points is wrong:",E.order())
        return False

    if a*b == 0:
        return False

    gamma = -b/a

    # explicit criterion
    if (gamma).is_square():
        return 2

    # Voloch’s criterion: need to enumerate points on C

    R.<x> = PolynomialRing(K)
    f = x^3 + a*x + b
    phi = gamma*(x^4+x^2+1)/(x^4+x^2)

    V = computeV(f)

    alpha = K.multiplicative_generator()
    alpha_range = range(1,(p-1)/4)
    if (p-1) % 6 == 0 and p > 7:
        alpha_range.remove((p-1)/6)

    u_list = [alpha^i for i in alpha_range]

    for u_0 in u_list:
        x_0 = phi(u_0)

        # is x_0 the x-coordinate of a point in E(F_p)?
        # if yes, see if Voloch’s criterion holds there.
        if f(x_0).is_square():

            # we have found a point, namely (u_0,v_0):

            v_0 = f(x_0).sqrt()

            # now check to see if (5.27) holds:

            num_1   = u_0^3*(u_0^6 - 3*u_0^2 + 2)
            denom_1 = -2*u_0^6 + 3*u_0^4 - 1
            num_2   = u_0^3*v_0*V(u_0^2*phi(u_0))
            denom_2 = v_0*V(phi(u_0))

            if num_1*denom_2 != num_2*denom_1:
                if not(num_1 == 0 and denom_1 == 0) and not(
                num_2 == 0 and denom_2 == 0):
                    return 2

    return 3
```

4.8.4 Wrapper code

The rest of the procedures are mainly non-mathematical in nature. The procedure checkManyPrimes takes as input an elliptic curve E over $\mathbb{Q}$ and upper and lower prime bounds max_p and min_p, and outputs a table listing, among others, the primes of anomalous reduction that are lucky for E, the primes of anomalous reduction that are lucky for the twist of E, the set of primes that are unlucky for E, and the set of primes that are unlucky for its twist.

```
# return e with
# e = 0 if E has bad reduction;
# e = 1 if E(F_p) has order 1;
# e = 2 if E is anomalous and satisfies C3 or C4;
# e = 3 if E is anomalous and can’t be dealt
# with by one of these criteria;
# e = 5 if E is non-anomalous and satisfies C1
# e = 6 if E is non-anomalous and can’t be dealt
# with by that criterion;
# e = 7 if E(F_p) is cyclic non-anomalous (C2).

def checkSingleCurve(Ep,p):

    A = Ep.abelian_group()
    gen_orders = A.generator_orders()

    if len(gen_orders) == 0:
        return 1

    n = gen_orders[0]

    if len(gen_orders)==1:
        if n == p:
            return checkAnomalousCurve(Ep)
        if (n % p) == 0 and n != p:
            return 4
        if (n % p) != 0:
            return 7

    pairsList = findPairs(Ep)

        # check whether some pair is a set of generators;
        # keep track of how many pairs

    if pairsList == false:
        return 8

    else:
        for pair in pairsList:
            if isSetOfGenerators(A,pair[0]):
                return 5
        return 6


def checkManyPrimes(E,min_p,max_p):

    counter   = [0,0,0,0,0,0,0,0,0]
    counter_t = [0,0,0,0,0,0,0,0,0]
```

```
results   = [range(1,500) for i in range(0,9)]
results_t = [range(1,500) for i in range(0,9)]

# p <= 7 is not allowed
min_p = max(11,min_p)

Delta = E.discriminant()*E.a4()*E.a6()

for p in prime_range(min_p,max_p):

    F = GF(p)
    alpha = F.multiplicative_generator()

    if (Delta % p) == 0:
        results[0][counter[0]] = p
        counter[0] += 1
        continue

    Ep = E.change_ring(GF(p))
    e = checkSingleCurve(Ep,p)
    results[e][counter[e]] = p
    counter[e] += 1

    Ept = Ep.quadratic_twist(alpha)
    e_t = checkSingleCurve(Ept,p)
    results_t[e_t][counter_t[e_t]] = p
    counter_t[e_t] += 1

badList = results[0][0:counter[0]]
oneList = results[1][0:counter[1]]
pGoodList = results[2][0:counter[2]]
pBadList = results[3][0:counter[3]]
two_pList = results[4][0:counter[4]]
lGoodList = results[5][0:counter[5]]
lBadList = results[6][0:counter[6]]
cyclicList = results[7][0:counter[7]]

oneList_t = results_t[1][0:counter_t[1]]
pGoodList_t = results_t[2][0:counter_t[2]]
```

```
pBadList_t = results_t[3][0:counter_t[3]]
two_pList_t = results_t[4][0:counter_t[4]]
lGoodList_t = results_t[5][0:counter_t[5]]
lBadList_t = results_t[6][0:counter_t[6]]
cyclicList_t = results_t[7][0:counter_t[7]]

print(str([E.a4(),E.a6()])+":")
print("Primes of ’bad reduction’: "+str(badList))
print("Good anomalous primes: "+str(pGoodList))
print("Good anom. primes (twist): "+str(pGoodList_t))
print("Bad anomalous primes: "+str(pBadList))
print("Bad non-anomalous primes: "+str(lBadList))
print("Bad anom. primes (twist): "+str(pBadList_t))
print("Bad non-anom. primes (twist): "+str(lBadList_t))

badSet = list(set(badList).union(set(pBadList))
.union(set(lBadList)).union(set(pBadList_t))
.union(set(lBadList_t)))
badSet.sort()
howManyBad = len(badSet)

print("Set of bad primes / total number of primes: ")
print("("+E.a4().str()+","+E.a6().str()+") &"),
if howManyBad > 0:
    print("\\{"),
    for i in range(0,howManyBad-1):
        print(str(badSet[i])+","),
    print(badSet[howManyBad-1]),
    print("\\}"),
else:
    print("\\emptyset"),
print("& "+str(howManyBad)+" \\\\")
print(RR(100*(1-howManyBad/164)))
```