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

Chapter 2

Density results for diagonal quartic surfaces

For $c \in \mathbb{Q}^*$, let V_c be the smooth quartic surface in $\mathbb{P}^3_{\mathbb{Q}}$ given by

$$x_0^4 + cx_1^4 = x_2^4 + cx_3^4. \tag{2.1}$$

Let $\mathbb{Q}_2$ denote the field of 2-adic numbers, let $\mathbb{Z}_2 \subset \mathbb{Q}_2$ denote the ring of 2-adic integers, and let $v\colon \mathbb{Q}_2 \to \mathbb{Z} \cup \{\infty\}$ denote the 2-adic valuation, using the convention $v(0) = \infty$. We will call a 2-adic integer a odd if $v(a) = 0$; otherwise we will call it even.

The main result discussed in this chapter is the following theorem, due to Sir Peter Swinnerton-Dyer.

Theorem 2.1 (Swinnerton-Dyer, 2010)**.** *Let c be 2 or 4. The set $V_c(\mathbb{Q})$ lies dense in $V_c(\mathbb{Q}_2)$, when this set is equipped with the 2-adic topology.*

The reasons for including a discussion of Swinnerton-Dyer's theorem in this thesis are twofold. Since this thesis is concerned with results concerning p-adic density of rational points on K3 surfaces, and since Swinnerton-Dyer's result was the first such result to appear for any K3 surface and for any p, it provides an important example of how such a result is arrived at. Secondly, we have striven to provide more details in our proof, and incorporate some minor improvements over the proof of Swinnerton-Dyer. For example, most of our results are stated for arbitrary values of c, whereas Swinnerton-Dyer restricts to $c \in \{2, 4, 8\}$ (although his methods clearly would have allowed him to go beyond this). Using this, we prove Theorem 2.1 for more values of c than Swinnerton-Dyer.

In our proof of Theorem 2.1, we will follow the arguments of Swinnerton-Dyer [38] in the main. The proof will be given in section 2.8.

2.1 Some open subsets of $V_c(\mathbb{Q}_2)$

We start by defining some open sets of $V_c(\mathbb{Q}_2)$. We use them to reduce the proof of density of $V_c(\mathbb{Q})$ in $V_c(\mathbb{Q}_2)$ to the proof of density of $V_c(\mathbb{Q})$ in many smaller open subsets.

Definition 2.2. For any $c \in \mathbb{Q}^*$, let $\mathcal{U}_c \subset V_c(\mathbb{Q}_2)$ be the open subset of 2-adic points that have representatives $(a_0 : a_1 : a_2 : a_3)$ where the a_i are 2-adic integers such that a_0 and a_2 are both odd.

Proposition 2.3. *Let $c \in \mathbb{Q}$ be such that $1 \leq v(c) \leq 3$. If the rational points on V_c lie dense in $\mathcal{U}_c$ and the rational points on $V_{16/c}$ lie dense in $\mathcal{U}_{16/c}$, then $V_c(\mathbb{Q})$ lies dense in $V_c(\mathbb{Q}_2)$ and $V_{16/c}(\mathbb{Q})$ lies dense in $V_{16/c}(\mathbb{Q}_2)$.*

Proof. Suppose that $(a_0 : a_1 : a_2 : a_3)$ defines a point in $V_c(\mathbb{Q}_2)$, where the a_i are 2-adic integers that do not all have positive valuation. Then it follows from (2.1) and the assumption on c that either a_0, a_2 are both odd, or a_0, a_2 are both even and a_1, a_3 are both odd. Moreover, there is an isomorphism between V_c and $V_{16/c}$ defined as follows

$$\begin{aligned} \psi_c \colon V_c &\to V_{16/c} \\ (x_0 : x_1 : x_2 : x_3) &\mapsto (x_1 : \frac{x_0}{2} : x_3 : \frac{x_2}{2}) \end{aligned}$$

We see from this that either a_0 and a_2 are both odd, or we have that $\psi_c(a_0 : a_1 : a_2 : a_3) \in V_{16/c}(\mathbb{Q}_2)$ has a representative $(a'_0 : a'_1 : a'_2 : a'_3)$ where the a'_i are 2-adic integers such that a'_0 and a'_2 are both odd. So for $P \in V_c(\mathbb{Q}_2)$ we have either $P \in \mathcal{U}_c$ or $\psi_c(P) \in \mathcal{U}_{16/c}$. This establishes the proposition. □

We partition the sets $\mathcal{U}_c$ into open subsets

$$\mathcal{U}'_c \cup \bigcup_{n=1}^{\infty} \mathcal{U}''_{c,n} \cup \bigcup_{n=1}^{\infty} \mathcal{U}'''_{c,n},$$

with the definition of these subsets included in the following definition.

Definition 2.4. We define various open subsets of $\mathcal{U}_c$.

- Let $\mathcal{U}'_c \subset \mathcal{U}_c$ be the open subset of 2-adic points that have representatives $(a_0 : a_1 : a_2 : a_3)$ such that the a_i are all odd 2-adic integers.

- Let $\mathcal{A}_c \subset \mathcal{U}'_c$ be the open subset of points $(a_0 : a_1 : a_2 : a_3)$ where the a_i additionally satisfy $v(a_0+a_2) = v(a_1-a_3) = 1$. Let $\mathcal{A}'_c \subset \mathcal{U}'_c$ be the open subset where instead the a_i satisfy $v(a_0 - a_2) = v(a_1 + a_3) = 1$.
- For $n \in \mathbb{Z}_{\geq 1}$, let $\mathcal{U}''_{c,n} \subset \mathcal{U}_c$ be the set of 2-adic points that have representatives $(a_0 : a_1 : a_2 : a_3)$ where the a_i are 2-adic integers such that a_0 and a_2 are both odd and $v(a_1) = v(a_3) = n$.
- For $n \in \mathbb{Z}_{\geq 1}$, let $\mathcal{B}_{c,n} \subset \mathcal{U}''_{c,n}$ be the open subset of points $(a_0 : a_1 : a_2 : a_3)$ where the a_i additionally satisfy $v(a_0 - a_2) = 1$ and $v(a_1 - a_3) = n+1$.
- For $n \in \mathbb{Z}_{\geq 1}$, let $\mathcal{U}'''_{c,n} \subset \mathcal{U}_c$ be the open subset of 2-adic points that have representatives $(a_0 : a_1 : a_2 : a_3)$ where the a_i are 2-adic integers such that a_0 and a_2 are both odd, and either $v(a_1) > v(a_3) = n$ or $v(a_3) > v(a_1) = n$.
- For $n \in \mathbb{Z}_{\geq 1}$, let $\mathcal{C}_{c,n} \subset \mathcal{U}'''_{c,n}$ be the open subset of points $(a_0 : a_1 : a_2 : a_3)$ where the a_i additionally satisfy $v(a_0+a_2) = 1$, and let $\mathcal{C}'_{c,n} \subset \mathcal{U}'''_{c,n}$ be the open subset of points $(a_0 : a_1 : a_2 : a_3)$ where the a_i additionally satisfy $v(a_0 - a_2) = 1$.

Clearly, to prove density of a certain subset of $\mathcal{U}_c$ it suffices to prove its density in each of the sets $\mathcal{U}'_c$, $\mathcal{U}''_{c,n}$ and $\mathcal{U}'''_{c,n}$. However, if we use some of the automorphisms of V_c, it suffices to restrict our attention to smaller open subsets $\mathcal{A}_c$, $\mathcal{A}'_c$, $\mathcal{B}_{c,n}$, $\mathcal{C}_{c,n}$ and $\mathcal{C}'_{c,n}$.

Throughout the chapter, we make frequent use of the following automorphisms of V_c.

Definition 2.5. For $0 \leq i \leq 3$, let ϕ_i denote the automorphism of V_c that acts on $(x_0 : x_1 : x_2 : x_3)$ by multiplying the x_i-coordinate by -1.

We observe that $\mathcal{U}'_c$ is the union of the images of $\mathcal{A}_c$ under the subgroup of $\mathrm{Aut}(V_c)$ generated by the ϕ_i. Note also that we have $\mathcal{A}'_c = \phi_2(\phi_3(\mathcal{A}_c))$ and $\mathcal{C}'_{c,n} = \phi_2(\mathcal{C}_{c,n})$ for each n. Also, each $\mathcal{U}''_{c,n}$ is the union of the images of $\mathcal{B}_{c,n}$ under the said subgroup of $\mathrm{Aut}(V_c)$ and each $\mathcal{U}'''_{c,n}$ is the union of the images of $\mathcal{C}_{c,n}$. Therefore, to prove density of the set of $V_c(\mathbb{Q})$ in $\mathcal{U}_c$, it suffices to prove its density in the sets $\mathcal{A}_c$, $\mathcal{B}_{c,n}$ for all integers $n \geq 1$ and in either $\mathcal{C}_{c,n}$ or $\mathcal{C}'_{c,n}$ for all integers $n \geq 1$.

2.1.1 Outline of the rest of the chapter

In sections 2.2 and 2.3, we introduce elliptic fibrations on V_c, and we investigate the fibres of these fibrations. In section 2.4, we explain the strategy of proving density of rational points using elliptic fibrations. Sections 2.5–2.7 form the core of the proof. We will prove in section 2.5 that the existence of any rational point on V_c that is in $\mathcal{C}_{c,1}$ implies the density of $V_c(\mathbb{Q})$ in $\mathcal{C}_{c,1}$; that the same fact implies the density of $V_c(\mathbb{Q})$ in $\mathcal{A}_c$ will be proven in section 2.6. In section 2.7, we will show that density of $V_c(\mathbb{Q})$ in $\mathcal{A}'_c = \phi_2(\phi_3(\mathcal{A}_c))$ implies the density of $V_c(\mathbb{Q})$ in $\mathcal{B}_{c,n}$ for all integers $n \geq 1$ and in $\mathcal{C}'_{c,n}$ for all integers $n \geq 2$. Therefore, in view of the arguments of the previous paragraph, sections 2.5–2.7 show that the existence of a rational point of V_c that is in $\mathcal{C}_{c,1}$ implies the density of $V_c(\mathbb{Q})$ in the set $\mathcal{U}_c$ defined at the start of this section. Furthermore, if we combine this with Proposition 2.3, we find that the existence of both a rational point of V_c that is in $\mathcal{C}_{c,1}$ and a rational point of $V_{16/c}$ that is in $\mathcal{C}_{16/c,1}$ implies the density of $V_c(\mathbb{Q})$ in $V_c(\mathbb{Q}_2)$.

2.2 Elliptic fibrations on V_c

We define rational maps $f, g\colon V_c \dashrightarrow \mathbb{P}^1$ as follows:

$$f(x_0 : x_1 : x_2 : x_3) = \frac{x_0 - x_2}{x_1 - x_3}, \quad g(x_0 : x_1 : x_2 : x_3) = \frac{x_0 + x_2}{x_1 - x_3}.$$

We observe that $g = f \circ \phi_2$. By considering the identities

$$-\frac{x_0 \pm x_2}{x_1 - x_3} = c\,\frac{(x_1 + x_3)(x_1^2 + x_3^2)}{(x_0 \mp x_2)(x_0^2 + x_2^2)}$$

in the function field of V_c, we see that f and g are actually morphisms from V_c to $\mathbb{P}^1$. For $\lambda \in \mathbb{P}^1$, the preimage $f^{-1}(\lambda)$ is the intersection of the cubic surface

$$(x_0 + x_2)(x_0^2 + x_2^2) = -\frac{c}{\lambda}(x_1 + x_3)(x_1^2 + x_3^2) \tag{2.2}$$

with the plane $x_0 - x_2 = \lambda(x_1 - x_3)$, with the understanding that the left-hand side is equated to zero if $\lambda = 0$, and the right-hand side is equated to zero if $\lambda = \infty$, with λ replaced by any finite value. For $\mu \in \mathbb{P}^1$, the preimage $g^{-1}(\mu)$ is the intersection of the cubic surface

$$(x_0 - x_2)(x_0^2 + x_2^2) = -\frac{c}{\mu}(x_1 + x_3)(x_1^2 + x_3^2),$$

with the plane $x_0 + x_2 = \mu(x_1 - x_3)$, with the understanding that the left-hand side is equated to zero if $\mu = 0$, and the right-hand side is equated to zero if $\mu = \infty$, with μ replaced by any finite value.

The morphisms $f, g\colon V_c \to \mathbb{P}^1$ endow the surface V_c with a fibration in curves of genus one (which is often abusively called an elliptic fibration). Note that f has the section $\lambda \mapsto P_\lambda$, where $P_\lambda = (\lambda : 1 : -\lambda : -1)$. The point P_λ is the intersection of $f^{-1}(\lambda)$ with the line $x_0 + x_2 = x_1 + x_3 = 0$. Applying ϕ_2, we see that g likewise has a section given by $\mu \mapsto P'_\mu$, where $P'_\mu = (\mu : 1 : \mu : -1)$. By taking P_λ to be the identity for the group law on $f^{-1}(\lambda)$, and P'_μ for the one on $g^{-1}(\mu)$, we may (and will) regard f and g as elliptic fibrations, i.e. fibrations whose generic fibres are elliptic curves.

2.2.1 The level of a point on a Weierstrass curve

Let $P \in V_c(\mathbb{Q}_2)$ and let $E = e^{-1}(e(P))$ be a fibre of an elliptic fibration $e\colon V_c \to \mathbb{P}^1$ passing through P. Then E is an elliptic curve over $\mathbb{Q}_2$. Suppose we are given a nice Weierstrass curve $\mathcal{E}$ over $\mathbb{Z}_2$ together with a morphism $i\colon E \to \mathcal{E}$ that is an isomorphism on generic fibres. On $\mathcal{E}(\mathbb{Q}_2)$, we have a filtration (see section 1.2)

$$\mathcal{E}(\mathbb{Q}_2) \supset \mathcal{E}_0(\mathbb{Q}_2) \supset \mathcal{E}_1(\mathbb{Q}_2) \supset \mathcal{E}_2(\mathbb{Q}_2) \supset \dots,$$

inducing an exhaustive filtration $\{E_n(\mathbb{Q}_2)\}_{n=0}^{\infty}$ on the subgroup of $E(\mathbb{Q}_2)$ that maps isomorphically to $\mathcal{E}_0(\mathbb{Q}_2)$. If P is not the identity of $E(\mathbb{Q}_2)$, and P lies in $E_0(\mathbb{Q}_2)$, then there exists a largest integer $n \geq 0$ such that $P \in E_n(\mathbb{Q}_2)$; we will call n the level of P on $\mathcal{E}$. If the image of P does not lie in $\mathcal{E}_0(\mathbb{Q}_2)$, we will say that the level of P is -1: this is the same as saying that the image of P has singular reduction. The choice of i is suppressed from the terminology; it is always clear from the context. Usually the choices of both i and $\mathcal{E}$ are clear: we will then speak of the level of P on E or along e, or write $\mathrm{level}_E(P)$.

2.3 Weierstrass models for the fibres of f

This section consists mainly of calculations, of which the aim is to find Weierstrass models for the fibres of f. We do this in order to be able to apply the results of chapter 1, which deal with Weierstrass curves. Moreover, with a Weierstrass equation at hand it is easier to compute j-invariants and division polynomials, as is done in the proof of Proposition 2.10. The Weierstrass models and the changes of variables from which they result are summarized in Propositions 2.6–2.8.

Throughout section 2.3, we assume $1 \leq v(c) \leq 3$. By $\overline{\mathbb{Z}}_2$ we denote the integral closure of $\mathbb{Z}_2$ in $\overline{\mathbb{Q}}_2$.

Proposition 2.6. *Let* $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ *be such that* $\lambda^8 \neq c^2$ *and* $v(\lambda) \geq 0$. *Then there exists an isomorphism from* $f^{-1}(\lambda)$ *to the generic fibre of the Weierstrass curve in* $\mathbb{P}^2_{\overline{\mathbb{Z}}_2}$ *with homogeneous coordinates* x, y, z *given by*

$$\mathcal{E}_\lambda\colon y^2 z = x^3 - 3\lambda^6 x^2 z - 3\lambda^4(c^2 - \lambda^8)xz^2 - \lambda^2(c^2 - \lambda^8)^2 z^3, \tag{2.3}$$

where this isomorphism is given by

$$x = -\frac{x_0 + x_2}{2c}, y = \frac{x_1 - x_3}{2}, z = \frac{x_1 + x_3 + \frac{\lambda^3}{c}(x_0 + x_2)}{2\lambda(c^2 - \lambda^8)}. \tag{2.4}$$

Proof. Let λ be as in the proposition. The preimage $f^{-1}(\lambda)$ of λ under the morphism $f\colon V_c \to \mathbb{P}^1$ is the cubic curve over $\overline{\mathbb{Q}}_2$

$$(x_0 + x_2)(x_0^2 + x_2^2) = -\frac{c}{\lambda}(x_1 + x_3)(x_1^2 + x_3^2), \quad x_0 - x_2 = \lambda(x_1 - x_3).$$

Note that it has the point P_λ defined in the previous section, which we take to be the identity for the group law, endowing $f^{-1}(\lambda)$ with the structure of an elliptic curve. We map $f^{-1}(\lambda)$ isomorphically to the cubic curve in $\mathbb{P}^3_{\overline{\mathbb{Q}}_2}(s_0, s_1, v_0, v_1)$ given by

$$s_0(s_0^2 + v_0^2) = -\frac{c}{\lambda}s_1(s_1^2 + v_1^2), \quad v_0 = \lambda v_1 \tag{2.5}$$

with the maps given by

$$s_0 = x_0 + x_2, \quad v_0 = x_0 - x_2, \quad s_1 = x_1 + x_3, \quad v_1 = x_1 - x_3. \tag{2.6}$$

If we project the image of $f^{-1}(\lambda)$ to $\mathbb{P}^2_{\overline{\mathbb{Q}}_2}(s_0, s_1, v_1)$, by eliminating v_0 in (2.5), its isomorphic copy in $\mathbb{P}^2_{\overline{\mathbb{Q}}_2}(s_0, s_1, v_1)$ is given by

$$s_0(s_0^2 + \lambda^2 v_1^2) = -\frac{c}{\lambda}s_1(s_1^2 + v_1^2). \tag{2.7}$$

The point P_λ maps to the flex point $(s_0 : v_1 : s_1) = (0 : 1 : 0)$, whose tangent is given by $\lambda^3 s_0 = -cs_1$. We introduce the variable

$$s_2 = s_1 + \frac{\lambda^3}{c}s_0.$$

With this substitution we arrive at the curve in $\mathbb{P}^2_{\overline{\mathbb{Q}}_2}(s_0, v_1, s_2)$

$$s_0^3 = \frac{c}{\lambda}\left(\frac{\lambda^9}{c^3}s_0^3 - 3\frac{\lambda^6}{c^2}s_0^2 s_2 + 3\frac{\lambda^3}{c}s_0 s_2^2 - s_2^3 - v_1^2 s_2\right),$$

isomorphic to the one given by (2.7). The effect of this last step is that the image of the point P_λ is $(s_0 : v_1 : s_2) = (0 : 1 : 0)$, with the tangent now given by $s_2 = 0$. Rearranging, we get

$$-\frac{c}{\lambda}v_1^2 s_2 = \left(1 - \frac{\lambda^8}{c^2}\right) s_0^3 + 3\frac{\lambda^5}{c} s_0^2 s_2 - 3\lambda^2 s_0 s_2^2 + \frac{c}{\lambda} s_2^3.$$

Finally, since $\lambda^8 \neq c^2$, we may define an isomorphism from the curve defined by the equation above to the Weierstrass curve given by

$$y^2 z = x^3 - 3\lambda^6 x^2 z - 3\lambda^4(c^2 - \lambda^8)xz^2 - \lambda^2(c^2 - \lambda^8)^2 z^3,$$

by setting

$$x = -\frac{s_0}{2c} = -\frac{x_0 + x_2}{2c}, y = \frac{v_1}{2} = \frac{x_1 - x_3}{2},$$
$$z = \frac{s_2}{2\lambda(c^2 - \lambda^8)} = \frac{x_1 + x_3 + \frac{\lambda^3}{c}(x_0 + x_2)}{2\lambda(c^2 - \lambda^8)}.$$

Here, the factors 2 in the denominators are introduced for our convenience at a later stage in this chapter. This ends the proof. □

Proposition 2.7. *Let $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ be such that $\lambda^8 \neq c^2$ and $v(\lambda) \geq v(c)$. There exists an isomorphism from $f^{-1}(\lambda)$ to the generic fibre of the Weierstrass curve in $\mathbb{P}^2_{\mathbb{Z}_2}$ with homogeneous coordinates $\widetilde{x}, \widetilde{y}, \widetilde{z}$ given by*

$$\widetilde{\mathcal{E}}_\lambda \colon \widetilde{y}^2 \widetilde{z} = \widetilde{x}^3 - \frac{3\lambda^6}{c^2}\widetilde{x}^2\widetilde{z} - \frac{3\lambda^4(c^2 - \lambda^8)}{c^4}\widetilde{x}\widetilde{z}^2 - \frac{\lambda^2(c^2 - \lambda^8)^2}{c^6}\widetilde{z}^3. \tag{2.8}$$

where this isomorphism is given by

$$\widetilde{x} = -\frac{x_0 + x_2}{2c^3}, \widetilde{y} = \frac{x_1 - x_3}{2c^3}, \widetilde{z} = \frac{x_1 + x_3 + \frac{\lambda^3}{c}(x_0 + x_2)}{2\lambda(c^2 - \lambda^8)}. \tag{2.9}$$

Proof. The new variables $\widetilde{x}, \widetilde{y}, \widetilde{z}$ are related to the x, y, z from Proposition 2.6 by $\widetilde{x} = x/c^2, \widetilde{y} = y/c^2, \widetilde{z} = z$. □

Proposition 2.8. *Let $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ be such that $\lambda^8 \neq c^2$ and $v(\lambda) < 0$. There exists an isomorphism from $f^{-1}(\lambda)$ to the generic fibre of the Weierstrass curve in $\mathbb{P}^2_{\mathbb{Z}_2}$ with homogeneous coordinates $\widehat{x}, \widehat{y}, \widehat{z}$ given by*

$$\widehat{\mathcal{E}}_\lambda \colon \widehat{y}^2 \widehat{z} = \widehat{x}^3 - 3\lambda^{-4}c^2\widehat{x}\widehat{z}^2 - \lambda^{-2}c^2(c^2\lambda^{-8} + 1)\widehat{z}^3. \tag{2.10}$$

where this isomorphism is given by

$$\widehat{x} = -\frac{x_0 + x_2}{2\lambda^4 c} - \frac{\lambda(x_1 + x_3) + \frac{\lambda^4}{c}(x_0 + x_2)}{2(c^2 - \lambda^8)}, \widehat{y} = \frac{x_1 - x_3}{2\lambda^6},$$
$$\widehat{z} = \frac{x_1 + x_3 + \frac{\lambda^3}{c}(x_0 + x_2)}{2\lambda(c^2 - \lambda^8)}. \tag{2.11}$$

Proof. Resuming the notation of Proposition 2.6, we set

$$u = x - \lambda^6 z = -\frac{x_0 + x_2}{2c} - \frac{\lambda^5(x_1 + x_3) + \frac{\lambda^8}{c}(x_0 + x_2)}{2(c^2 - \lambda^8)},$$

we get a morphism from $f^{-1}(\lambda)$ to the curve given by the short Weierstrass equation

$$y^2 z = u^3 - 3\lambda^4 c^2 u z^2 - \lambda^2 c^2 (c^2 + \lambda^8) z^3. \tag{2.12}$$

If we put $\widehat{z} = z$, and define scalings of u and y as follows

$$\widehat{x} = u/\lambda^4, \quad \widehat{y} = y/\lambda^6,$$

this defines an isomorphism from $f^{-1}(\lambda)$ to the curve (2.10). □

Remark 2.9. The above propositions can of course be used to give Weierstrass models for fibres of other elliptic fibrations on V_c. Let ϕ be any automorphism of V_c. Then $e = f \circ \phi$ is an elliptic fibration of V_c. For $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ such that $v(\lambda) \geq 0$, Proposition 2.6 can be used to give an embedding of $e^{-1}(\lambda)$ into the Weierstrass curve $E_\lambda \subset \mathbb{P}^2_{\mathbb{Z}_2}$ as defined by (2.3). This embedding is obtained by precomposing the morphism (2.4) with ϕ. Similarly, Propositions 2.7 and 2.8 can be used to obtain embeddings of $e^{-1}(\lambda)$ into the Weierstrass curves $\widetilde{E}_\lambda$ and $\widehat{E}_\lambda$ given by (2.8) and (2.10) for the appropriate values of $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$.

2.3.1 The group structure on the fibres

It will be important for us in what follows to know the structure of the topological groups $\mathcal{E}_\lambda(\mathbb{Q}_2)$, $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2)$, and $\widehat{\mathcal{E}}_\lambda(\mathbb{Q}_2)$, where the notation is as in Propositions 2.6–2.8, or at least the parts consisting of the points of good reduction.

Proposition 2.10. *Assume that* $1 \leq v(c) \leq 3$. *We have the following isomorphisms of topological groups.*

(i) For all $\lambda \in \mathbb{P}^1(\mathbb{Q}_2) - \{0, \infty\}$ *with* $v(\lambda) = 0$*, we have*

$$(\mathcal{E}_\lambda)_0(\mathbb{Q}_2) \cong \mathbb{Z}_2,$$

and the isomorphism can be chosen in such a way that $(\mathcal{E}_\lambda)_n(\mathbb{Q}_2)$ *is identified with* $2^n\mathbb{Z}_2$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

(ii) For all $\lambda \in \mathbb{P}^1(\mathbb{Q}_2) - \{0, \infty\}$ *with* $v(\lambda) \geq v(c)$*, we have*

$$(\widetilde{\mathcal{E}}_\lambda)_0(\mathbb{Q}_2) \cong \mathbb{Z}_2,$$

and the isomorphism can be chosen in such a way that $(\widetilde{\mathcal{E}}_\lambda)_n(\mathbb{Q}_2)$ *is identified with* $2^n\mathbb{Z}_2$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

(iii) For all $\lambda \in \mathbb{P}^1(\mathbb{Q}_2) - \{0, \infty\}$ *with* $v(\lambda) < 0$*, we have*

$$(\widehat{\mathcal{E}}_\lambda)_0(\mathbb{Q}_2) \cong \mathbb{Z}_2,$$

and the isomorphism can be chosen in such a way that $(\widehat{\mathcal{E}}_\lambda)_n(\mathbb{Q}_2)$ *is identified with* $2^n\mathbb{Z}_2$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

(iv) For all $\lambda \in \mathbb{P}^1(\mathbb{Q}_2) - \{0, \infty\}$ *with* $v(\lambda) = v(c) + 1$*, we have*

$$\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2) \cong 2^{-1}\mathbb{Z}_2,$$

where $2^{-1}\mathbb{Z}_2$ *is seen as an open subset of* $\mathbb{Q}_2$*, and the isomorphism can be chosen in such a way that* $(\widetilde{\mathcal{E}}_\lambda)_n(\mathbb{Q}_2)$ *is identified with* $2^n\mathbb{Z}_2$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

Proof. For (i)–(iii), it suffices to apply Theorem 1.28 of Chapter 1. Now part (iv). In view of (ii) and Corollary 1.17, it is enough to show that $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2) \cong 2^{-1}\mathbb{Z}_2$. Let $\lambda \in \mathbb{P}^1 - \{\infty\}$ be such that $v(\lambda) = v(c) + 1$. The j-invariant of the generic fibre of $\widetilde{\mathcal{E}}_\lambda$ equals

$$12^3 \cdot \frac{4\lambda^8 c^2}{4\lambda^8 c^2 - \lambda^8 - c^2},$$

which has positive 2-adic valuation. Therefore $\widetilde{\mathcal{E}}_\lambda$ has either good or additive reduction. However, the reduction must in fact be additive: the discriminant of $\widetilde{\mathcal{E}}_\lambda$ is equal to

$$16 \cdot 27 \cdot \lambda^4 c^{-8}(4\lambda^8 c^2 - (c^2 + \lambda^8)^2),$$

and so has valuation 8, hence $\widetilde{\mathcal{E}}_\lambda$ is minimal. We thus have a short exact sequence

$$0 \to (\widetilde{\mathcal{E}}_\lambda)_0(\mathbb{Q}_2) \to \widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2) \to G \to 0$$

where G is a group of order at most 4 [32, C.15]. It follows from Proposition 1.14(ii) that $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2)$ is isomorphic to $\mathbb{Z}_2$ if and only if it has no elements of order 2 or 3. We may prove that the 2- and 3-torsion of $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2)$ is trivial using the 2- and 3-division polynomials of $(\widetilde{\mathcal{E}}_\lambda)_{\mathbb{Q}_2}$. However, we may equally well work with the 2- and 3-division polynomials $\Phi_2, \Phi_3 \in \mathbb{Q}_2[u]$ of the generic fibre of the Weierstrass curve (2.12), which is isomorphic to $(\widetilde{\mathcal{E}}_\lambda)_{\mathbb{Q}_2}$; we will do this since this makes the computation easier. The polynomial Φ_2 is just the right-hand side of (2.12):

$$\Phi_2 = u^3 - 3\lambda^4 c^2 u - \lambda^2 c^2 (c^2 + \lambda^8).$$

For Φ_3 we have [32, III, Exercise 3.7]:

$$\Phi_3 = 3u^4 - 18\lambda^4 c^2 u^2 - 12\lambda^2 c^2 (c^2 + \lambda^8) u - 9\lambda^8 c^4.$$

We find the valuation of the three zeros of Φ_2 by inspecting its Newton polygon. The coefficient of u^0 has valuation $6v(c) + 2$, that of u^1 has valuation $6v(c) + 4$, and that of u^3 has valuation 0: each zero of Φ_2 therefore has valuation $2v(c) + \frac{2}{3}$, and therefore does not lie in $\mathbb{Q}_2$. We consider the Newton polygon of Φ_3: the coefficient of u^0 has valuation $12v(c) + 8$, that of u^1 has valuation $6v(c)+4$, that of u^2 has valuation $6v(c)+5$, and that of u^4 has valuation 0. From this, we see that Φ_3 has a unique root in $\mathbb{Q}_2$, and this root has valuation $6v(c) + 4$. However, there is no 2-adic point (u_0, y_0) on the curve (2.12) such that $v(u_0) = 6v(c) + 4$, since then it would follow from (2.12) and from the valuations of the coefficients of Φ_2 we have just computed that we would have

$$y_0^2 \equiv -\lambda^2 c^2 (c^2 + \lambda^8) \pmod{2^{12v(c)+8}}.$$

However, the right-hand side cannot be a square in $\mathbb{Q}_2$, since $\lambda^2 c^2 (c^2 + \lambda^8) = \lambda^2 c^4 (1 + \lambda^8/c^2)$ is a square in $\mathbb{Q}_2$. Therefore $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2)$ has no 2- or 3-torsion. This concludes the proof. □

Section 2.3.2 will illustrate how Proposition 2.10 can be used to prove that, locally in $V_c(\mathbb{Q}_2)$, one has 2-adic density of rational points.

2.3.2 The bad fibres

We will describe the bad (non-smooth) fibres of f.

Lemma 2.11. *The geometric fibre of $f\colon V_c \to \mathbb{P}^1$ above $\lambda = 0$ is the union of the line*

$$x_0 - x_2 = x_1 + x_3 = 0$$

and two lines whose field of definition contains a square root of -1. The geometric fibre of f above $\lambda = \infty$ is the union of the line

$$x_0 + x_2 = x_1 - x_3 = 0$$

and two lines whose field of definition contains a square root of -1. The fibres of f above $\lambda = 0$ and $\lambda = \infty$ both consist of three lines meeting in one point.

Proof. If $\lambda = 0$, then from (2.2) we get that the fibre $f^{-1}(\lambda)$ is given by

$$(x_1 + x_3)(x_1^2 + x_3^2) = 0,\ x_0 - x_2 = 0.$$

If $\lambda = \infty$, then the fibre $f^{-1}(\lambda)$ is given by

$$(x_0 + x_2)(x_0^2 + x_2^2) = 0,\ x_1 - x_3 = 0.$$

The last assertion is clear from these equations. $\square$

Lemma 2.12. *Let $\lambda \in \overline{\mathbb{Q}}$ be such that $\lambda^8 = c^2$. The geometric fibres of $f\colon V_c \to \mathbb{P}^1$ above λ are unions of a line and a smooth conic.*

Proof. Let λ be as in the statement of the lemma. From (2.2) we get that the fibre $f^{-1}(\lambda)$ is given by

$$(x_0 + x_2)(x_0^2 + x_2^2) = \pm\lambda^3(x_1 + x_3)(x_1^2 + x_3^2),\ x_0 - x_2 = \lambda(x_1 - x_3),$$

for some change of sign. Changing variables to

$$s_0 = x_0 + x_2,\ v_0 = x_0 - x_2,\ s_1 = \lambda(x_1 + x_3),\ v_1 = \lambda(x_1 - x_3),$$

we find that $f^{-1}(\lambda)$ is isomorphic to the curve given by

$$s_0(s_0^2 + v_0^2) = \pm s_1(s_1^2 + v_1^2),\ v_0 = v_1.$$

By projecting onto the coordinates (s_0, s_1, v_1), and slightly rearranging the resulting equation, we get that $f^{-1}(\lambda)$ is isomorphic to the curve given by

$$(s_0 \mp s_1)(s_0^2 + s_1^2 \pm s_0 s_1 + v_1^2) = 0.$$

This clearly consists of a line and a non-singular conic. $\square$

We will show that there are no other bad fibres than the ones described in Lemmas 2.11–2.12.

Proposition 2.13. *The non-smooth fibres of* $f\colon V_c \to \mathbb{P}^1$ *are exactly the fibres above* $\lambda = 0$, $\lambda = \infty$ *and the* λ *with* $\lambda^8 = c^2$.

Proof. Let $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ be such that $\lambda^8 \neq c^2$. We will see that $f^{-1}(\lambda)$ is an elliptic curve. It follows from the proof of Proposition 2.8 that (2.11) defines an isomorphism from $f^{-1}(\lambda)$ to the curve E_λ over $\overline{\mathbb{Q}}_2$ defined by

$$\widehat{y}^2\widehat{z} = \widehat{x}^3 - 3\lambda^{-4}c^2\widehat{x}\widehat{z}^2 - \lambda^{-2}c^2(c^2\lambda^{-8}+1)\widehat{z}^3.$$

(The restriction $v(\lambda) < 0$ in Proposition 2.8 is there just to ensure that (2.10) defines a Weierstrass curve over $\overline{\mathbb{Z}}_2$.) We claim that the Weierstrass curve E_λ is non-singular. In order to see this, it suffices to check that its discriminant, which is

$$16 \cdot 27 \cdot \lambda^{20}c^{-8}(4c^2\lambda^{-8} - (c^2\lambda^{-8}+1)^2) = -16 \cdot 27 \cdot \lambda^{20}c^{-8}(c^2\lambda^{-8}-1)^2,$$

is non-zero, which is clearly the case. The proposition now follows from Lemmas 2.11–2.12. □

Corollary 2.14. *Let* $P \in V_c(\mathbb{Q}_2)$ *be a point lying on a bad fibre of* f.

(i) We have $f(P) = 0$ *or* $f(P) = \infty$*, and* P *lies on the line* $x_0 - x_2 = x_1 + x_3 = 0$ *if* $f(P) = 0$*, and on the line* $x_0 + x_2 = x_1 - x_3 = 0$ *if* $f(P) = \infty$.

(ii) Assume that $P \in \mathcal{U}_c$. *If* $f(P) = 0$*, then* $P \in \mathcal{A}_c$ *or* $P \in \phi_3(\mathcal{B}_{c,n})$ *for some* $n \geq 1$. *If* $f(P) = \infty$*, then* $P \in \mathcal{A}'_c$ *or* $P \in \phi_2(\mathcal{B}_{c,n})$ *for some* $n \geq 1$.

Proof. Let P be as in the statement, and let $\lambda = f(P) \in \mathbb{P}^1(\mathbb{Q}_2)$. The point P is defined over $\mathbb{Q}_2$, so we cannot have $\lambda^8 = c^2$, since the valuation of c is not a multiple of four. Hence λ is either 0 or ∞ by Proposition 2.13.

Assuming that $f(P) = 0$, then by Lemma 2.11, the point P lies on the line $x_0 - x_2 = x_1 + x_3 = 0$. Assume moreover $P \in \mathcal{U}_c$. Then if P is given by $(a_0 : a_1 : a_2 : a_3)$ with the a_i in $\mathbb{Z}_2$ and $v(a_0) = v(a_2) = 0$, we have $v(a_0 - a_2) = \infty$ and $v(a_0 + a_2) = v(2a_0) = 1$, and $v(a_1 + a_3) = \infty$ and $v(a_1 - a_3) = v(2a_1)$. Hence, if $v(a_1) = 0$, then P lies in $\mathbb{A}_c$, if $v(a_1) > 0$, then P lies in $\phi_2(\mathcal{B}_{c,n})$ with $n = v(a_1)$.

Assuming that $f(P) = \infty$, then by Lemma 2.11, the point P lies on the line $x_0 + x_2 = x_1 - x_3 = 0$. Assume moreover $P \in \mathcal{U}_c$. Then if P is given by $(a_0 : a_1 : a_2 : a_3)$ with the a_i in $\mathbb{Z}_2$ and $v(a_0) = v(a_2) = 0$, we have $v(a_0 + a_2) = \infty$ and $v(a_0 - a_2) = v(2a_0) = 1$, and $v(a_1 - a_3) = \infty$ and $v(a_1 + a_3) = v(2a_1)$. Hence, if $v(a_1) = 0$, then P lies in $\mathbb{A}'_c$; if $v(a_1) > 0$, then P lies in $\phi_3(\mathcal{B}_{c,n})$ with $n = v(a_1)$. □

2.4 Using elliptic fibrations to prove density

We will show how the elliptic fibrations on V_c can be exploited to show that, locally around a certain point in $V_c(\mathbb{Q}_2)$, the rational points lie dense. The main result of this section, Lemma 2.16, is almost trivial, but it neatly captures the basic ideas of this chapter.

2.4.1 One elliptic fibration

Assume that $e\colon V_c \to \mathbb{P}^1$ is an elliptic fibration. Let P and P' be elements of $V_c(\mathbb{Q}_2)$ lying on the same smooth fibre of e, and let $E = e^{-1}(e(P))$. Assume that we have a Weierstrass curve $\mathcal{E}$ over $\mathbb{Z}_2$, and an isomorphism $i\colon E \to \mathcal{E}_{\mathbb{Q}_2}$ of elliptic curves over $\mathbb{Q}_2$. Suppose furthermore that we have an isomorphism $\phi\colon \mathcal{E}_n(\mathbb{Q}_2) \xrightarrow{\sim} 2^n\mathbb{Z}_2$ for some $n \geq -1$, where we write $\mathcal{E}_{-1}(\mathbb{Q}_2) = \mathcal{E}(\mathbb{Q}_2)$, and that ϕ identifies $\mathcal{E}_k(\mathbb{Q}_2)$ with $2^k\mathbb{Z}_2$ for all $k \geq n$. (Note that Proposition 2.10 asserts that there (many) triples (e, P, P') for which these conditions are all satisfied.) In this setup, we have the following lemma.

Lemma 2.15. *Suppose that we have*

$$\mathrm{level}_E(P') \geq \mathrm{level}_E(P) \geq n.$$

Then the multiples of P on E lie dense around P'. Moreover, if there exists a sequence $\{Q_i\}_{i=0}^{\infty}$ of rational points converging to P, then there exists a sequence $\{Q'_i\}_{i=0}^{\infty}$ of rational points converging to P'.

Proof. Let $k = \mathrm{level}_E(P)$ and $k' = \mathrm{level}_E(P')$. Then $\phi(i(P)) \in 2^n\mathbb{Z}_2$ has valuation k and $\phi(i(P')) \in 2^n\mathbb{Z}_2$ has valuation $k' \geq k$. Hence the multiples of $\phi(i(P))$ are dense around $\phi(i(P'))$. Since $\phi \circ i$ is a homeomorphism from $\mathcal{E}_n(\mathbb{Q}_2)$ to $2^n\mathbb{Z}_2$, the multiples of P are dense around P'. For any integer m, we have the rational map $[m]\colon V_c \dashrightarrow V_c$ that is multiplication by m along fibres of e; it is a morphism when restricted to the smooth locus of e. Let $\{Q_i\}_{i=0}^{\infty}$ be as in the statement of the lemma. If $\{m_i\}_{i=0}^{\infty}$ is a sequence of integers such that $[m_i]P$ converges to P', then $\{[m_i]Q_i\}_{i=0}^{\infty}$ converges to P', by continuity of $[m_i]$ near smooth fibres. We may thus take $Q'_i = [m_i]Q_i$ for all i. □

2.4.2 Two elliptic fibrations

We continue with the assumptions of section 2.4.1. If we employ not just one elliptic fibration e, but also a second one e', we obtain a method for proving density in an open subset of $V_c(\mathbb{Q}_2)$. Let $e' \colon V_c \to \mathbb{P}^1$ be an elliptic fibration, and suppose that P'' is an element of $V_c(\mathbb{Q}_2)$ such that P' and P'' lie on the same smooth fibre of e'. Let us denote $E' = (e')^{-1}(e'(P'))$.

Assume, analogously to what we assumed for E, that we have a Weierstrass curve $\mathcal{E}'$ over $\mathbb{Z}_2$, and an isomorphism $i' \colon E' \to \mathcal{E}'_{\mathbb{Q}_2}$ of elliptic curves over $\mathbb{Q}_2$. Suppose furthermore that we have an isomorphism $\phi' \colon \mathcal{E}'_m(\mathbb{Q}_2) \xrightarrow{\sim} 2^m\mathbb{Z}_2$ for some $m \geq -1$, where we again write $\mathcal{E}'_{-1}(\mathbb{Q}_2) = \mathcal{E}'(\mathbb{Q}_2)$, and that ϕ' identifies $\mathcal{E}'_k(\mathbb{Q}_2)$ with $2^k\mathbb{Z}_2$ for all $k \geq m$.

Lemma 2.16. *Suppose that we have both*

$$\mathrm{level}_E(P') \geq \mathrm{level}_E(P) \geq n$$

and

$$\mathrm{level}_{E'}(P'') \geq \mathrm{level}_{E'}(P') \geq m.$$

Then if there exists a sequence $\{Q_i\}_{i=0}^\infty$ of rational points converging to P, then there exists a sequence $\{Q''_i\}_{i=0}^\infty$ of rational points converging to P''. In particular, the rational points are dense around P''.

Proof. For any integer m, we have the rational maps $[m]_e \colon V_c \dashrightarrow V_c$ and $[m]_{e'} \colon V_c \dashrightarrow V_c$ that are multiplication by m along fibres of e and e'; the rational maps $[m]_e$ and $[m]_{e'}$ give morphisms when restricted to the smooth loci of e and e'. Lemma 2.15 applied to P and P' yields the existence of a sequence $\{m_i\}_{i=0}^\infty$ of integers such that $([m_i]_e P)_i$ converges to P'. By restricting to a subsequence if necessary, we can assume that all $[m_i]_e P$ lie on smooth fibres of e'. Applying Lemma 2.15 to P' and P'', we get the existence of a sequence $\{m'_i\}_{i=0}^\infty$ of integers such that $([m'_i]_{e'} P')_i$ converges to P''. If we put

$$Q''_i = [m'_i]_{e'}[m_i]_e Q_i,$$

then $\{Q''_i\}_{i=0}^\infty$ is a sequence of rational points converging to P''. □

Lemma 2.16 shows the strategy that we will follow to prove density of $V_c(\mathbb{Q})$ in $V_c(\mathbb{Q}_2)$. Continuing with the assumptions on e and e' and the notation established earlier in this section, one starts from a point $P \in V_c(\mathbb{Q}_2)$ and a sequence $\{Q_i\}_{i=0}^\infty$ of rational points converging to P (this is especially easy if P is itself rational), then one looks for an open subset U of

$V_c(\mathbb{Q}_2)$ such that, for all $P'' \in U$, there exists an auxiliary point $P' \in V_c(\mathbb{Q}_2)$ with $e(P') = e(P)$ and $e'(P') = e'(P'')$ such that both

$$\mathrm{level}_E(P') \geq \mathrm{level}_E(P) \geq n$$

and

$$\mathrm{level}_{E'}(P'') \geq \mathrm{level}_{E'}(P') \geq m.$$

It follows from Lemma 2.16 that the rational points are then dense in U.

This is the strategy that will be followed in sections 2.5 and 2.6, where density in $\mathcal{C}_{c,1}$ and $\mathcal{A}_c$ is established. The roles of e and e' will be taken by the elliptic fibrations f, g and $f \circ \phi_3$. The arguments in section 2.7, which covers density in $\mathcal{B}_{c,n}$ for $n \geq 1$ and $\mathcal{C}_{c,n}$ for $n \geq 2$, are similar, but apply Lemma 2.15 instead of Lemma 2.16.

2.5 Density in $\mathcal{C}_{c,1}$

From this point in the chapter on, we will assume that $c \in \mathbb{Q}^*$ is such that $1 \leq v(c) \leq 3$.

We will show that the rational points on V_c are dense in $\mathcal{C}_{c,1}$. In this section and the next, we will frequently use the fact that the equation (2.1) defining V_c can be rewritten as

$$(x_0 - x_2)(x_0 + x_2)(x_0^2 + x_2^2) = -c(x_1 - x_3)(x_1 + x_3)(x_1^2 + x_3^2). \qquad (2.13)$$

Lemma 2.17. *Let $P = (a_0 : a_1 : a_2 : a_3)$ be a point in $\mathcal{C}_{c,1}$, where the a_i are 2-adic integers at least one of which is a unit. Write $\lambda = f(P)$ and $\pi = (f \circ \phi_3)(P)$. Then the following statements are true.*

(i) We have

$$v(a_0 + a_2) = 1, v(a_0 - a_2) = v(c) + 2, v(a_0^2 + a_2^2) = 1$$

as well as

$$v(a_1 + a_3) = 1, v(a_1 - a_3) = 1, v(a_1^2 + a_3^2) = 2.$$

(ii) We have $v(\lambda) = v(\pi) = v(c) + 1$.

Proof. The first equality is by definition of $\mathcal{C}_{c,1}$. The third equality follows from the fact that the square of an element $a \in \mathbb{Z}_2^*$ is 1 (mod 8). The second row of equalities all follow from the definition of $\mathcal{C}_{c,1}$. Now from (2.13), we get

$$\begin{aligned} v(a_0 - a_2) = v(c) + v(a_1 - a_3) + v(a_1 + a_3) + v(a_1^2 + a_3^2) \\ - v(a_0 + a_2) - v(a_0^2 + a_2^2) = v(c) + 2, \end{aligned} \tag{2.14}$$

which concludes the proof of (i). Part (ii) is a direct consequence of part (i). □

We have the following converse of Lemma 2.17(ii).

Lemma 2.18. *Let $\lambda_0, \pi_0 \in \mathbb{Q}_2$ satisfy $v(\lambda_0) = v(\pi_0) = v(c)+1$. Then there exists a unique point $P \in \mathcal{C}_{c,1}$ such that $f(P) = \lambda_0$ and $(f \circ \phi_3)(P) = \pi_0$. Moreover, the dependence of P on λ_0 and π_0 is continuous.*

Proof. We rewrite (2.13) in terms of the homogeneous coordinates $s_0 = x_0 + x_2, v_0 = x_0 - x_2, s_1 = x_1 + x_3, v_1 = x_1 - x_3$:

$$s_0 v_0 (s_0^2 + v_0^2) = -c s_1 v_1 (s_1^2 + v_1^2). \tag{2.15}$$

The hypotheses imply that in (2.15) we have $v_0 = \lambda_0 v_1$ and $v_0 = \pi_0 s_1$. If we set $w = s_0/v_0$, we obtain the following equation for w:

$$w^3 + w + b_0 = 0,$$

where

$$b_0 = c\frac{\lambda_0^2 + \pi_0^2}{\lambda_0^3 \pi_0^3}.$$

The conditions on the valuations of λ_0 and π_0 give $v(b_0) = -3v(c) - 3$. (Here, we use that if $\kappa \in \mathbb{Z}_2$, then $\kappa^2 \equiv 2^{2v(\kappa)} \pmod{2^{2v(\kappa)+3}}$.) Setting $w = w'/2c$, we find that w' satisfies

$$w'^3 + 4c^2 w' + 8b_0 c^3 = 0. \tag{2.16}$$

By Hensel's lemma, this has a solution $w_0' \in \mathbb{Q}_2$ with $v(w_0') = 0$. Moreover, the three roots w_0', w_1', w_2' of (2.16) in $\overline{\mathbb{Q}}_2$ reduce to the three zeros of X^3+1 in $\overline{\mathbb{F}}_2$, only one of which lies in $\mathbb{F}_2$; therefore, w_0' is the unique solution to (2.16) in $\mathbb{Q}_2$. It gives rise to the point

$$P_0 = P(\lambda_0, \pi_0) = (w_0' + 2c : 2c/\lambda_0 + 2c/\pi_0 : w_0' - 2c : -2c/\lambda_0 + 2c/\pi_0),$$

of which one checks that it indeed lies in $\mathcal{C}_{c,1}$. For the P whose existence was asserted in the lemma we may thus take $P = P_0$.

Finally, we check that $P(\lambda_0, \pi_0)$ depends on λ_0 and π_0 in a continuous way. This comes down to the claim that if $((\lambda_i, \pi_i))_{i=1}^{\infty} \subset \mathbb{Q}_2^2$ is a sequence of pairs converging to (λ_0, μ_0), then if w_i' is a solution to

$$w'^3 + 4c^2 w' + 8b_i c^3 = 0 \tag{2.17}$$

where

$$b_i = c\frac{\lambda_i^2 + \pi_i^2}{\lambda_i^3 \pi_i^3}.$$

then the sequence $(w_i')_i$ tends to w_0'. We now prove this claim. From (2.17) we deduce

$$\begin{aligned} 8(b_i - b_{i-1})c^3 &= (w_{i-1}'^3 + 4c^2 w_{i-1}') - (w_i'^3 + 4c^2 w_i') \\ &= -(w_i' - w_{i-1}')(w_i'^2 + w_i' w_{i-1}' + w_{i-1}'^2 + 4c^2). \end{aligned}$$

As i tends to infinity, we have that $b_i - b_{i-1}$ tends to 0, while $v(w_i'^2 + w_i' w_{i-1}' + w_{i-1}'^2 + 4c^2) = 0$ since $v(w_{i-1}') = v(w_i') = 0$. Hence $w_i' - w_{i-1}'$ tends to 0, and we are done. □

For each $P \in \mathcal{C}_{c,1}$, we will identify the fibre through P of f with the generic fibre of the curve $\widetilde{\mathcal{E}}_{f(P)}$ given by (2.8) via (2.9); the fibre through P of $f \circ \phi_3$ we will identify with the generic fibre of the curve $\widetilde{\mathcal{E}}_{(f\circ\phi_3)(P)}$ in the same way. It follows from Lemma 2.17(ii) that these identifications can be made. With these conventions, it makes sense to speak of the levels of the points in $\mathcal{C}_{c,1}$ along f and $f \circ \phi_3$.

Lemma 2.19. *Let P be a point in $\mathcal{C}_{c,1}$. The level of P along f is equal to -1. The level of P along $f \circ \phi_3$ is equal to -1.*

Proof. The proof uses Lemma 2.17 throughout. We write $P = (a_0 : a_1 : a_2 : a_3)$ and $\lambda = f(P)$. We obtain a representative $(\widetilde{\xi} : \widetilde{\eta} : \widetilde{\zeta})$ of the image of P on $\widetilde{E}_\lambda$ by substituting $x_i = a_i$ into the equations (2.9). Using (2.9), we get

$$v(\widetilde{\xi}) = v(a_0 + a_2) - 3v(c) - 1 = -3v(c), \;\; v(\widetilde{\eta}) = v(a_1 - a_3) - 3v(c) - 1 = -3v(c),$$

where we have used the definition of $\mathcal{C}_{c,1}$. To compute the valuation of

$$\widetilde{\zeta} = \frac{a_1 + a_3 + \frac{\lambda^3}{c}(a_0 + a_2)}{2\lambda(c^2 - \lambda^8)} \tag{2.18}$$

note that Lemma 2.17(i) implies $v(a_1+a_3) = 1 < 2v(c)+4 = v(\frac{\lambda^3}{c}(a_0+a_2))$; hence the valuation of the numerator is equal to 1. Therefore

$$v(\widetilde{\zeta}) = 1 - v(2\lambda(c^2 - \lambda^8)) = 1 - (1 + v(c) + 1 + 2v(c)) = -3v(c) - 1.$$

It follows that we have $v(\widetilde{\xi}/\widetilde{\zeta}) = v(\widetilde{\eta}/\widetilde{\zeta}) = 1$. Therefore the point P reduces to the singular point on the special fibre of $\widetilde{E}_\lambda$. Thus we have shown that the level of P along f is -1.

The calculations for the level along $f \circ \phi_3$ go in exactly the same way as the calculations for the level along f. □

Proposition 2.20. *Assume that there exists a rational point $P_0 \in \mathcal{C}_{c,1}$. Then $V_c(\mathbb{Q})$ is dense in $\mathcal{C}_{c,1}$.*

Proof. Let $P_2 \in \mathcal{C}_{c,1}$ be an arbitrary 2-adic point. Define $\lambda_0 = f(P_0)$ and $\pi_2 = (f \circ \phi_3)(P_2)$. It follows from Lemma 2.17(ii) and 2.18 that there exists a unique $P_1 \in \mathcal{C}_{c,1}$ such that $f(P_1) = \lambda_0$ and $(f \circ \phi_3)(P_1) = \pi_2$. These conditions express exactly that P_1 lies on the same f-fibre as P_0, and on the same $(f \circ \phi_3)$-fibre as P_2. The levels of P_0 and P_1 along f are both equal to -1 by Lemma 2.19. The levels of P_1 and P_2 along $f \circ \phi_3$ are both equal to -1 by Lemma 2.19. By Corollary 2.14, the points P_0 and P_1 lie on a smooth fibre of f, and P_1 and P_2 lie on a smooth fibre of $f \circ \phi_3$. By Lemma 2.16, the rational points lie dense around P_2. □

2.6 Density in $\mathcal{A}_c$

Assuming there is a rational point in $\mathcal{C}_{c,1}$, we will show density of the rational points in $\mathcal{A}_c$.

Lemma 2.21. *Let $P = (a_0 : a_1 : a_2 : a_3)$ be a point in $\mathcal{A}_c$. Write $\lambda = f(P)$ and $\mu = g(P)$. Then the following statements are true.*

(i) We have

$$v(a_0 + a_2) = 1, v(a_0 - a_2) = v(\lambda) + 1, v(a_0^2 + a_2^2) = 1,$$

as well as

$$v(a_1 + a_3) = v(\lambda) + 1 - v(c), v(a_1 - a_3) = 1, v(a_1^2 + a_3^2) = 1.$$

(ii) We have $v(\lambda) \geq v(c) + 1$ and $v(\mu) = 0$.

Proof. Since P is in $\mathcal{A}_c$ we have $v(a_0 + a_2) = v(a_1 - a_3) = 1$ by definition of $\mathcal{A}_c$, and this implies

$$v(a_0^2 + a_2^2) = v(a_1^2 + a_3^2) = 1,$$

since the square of the 2-adic unit a_i is 1 (mod 8) for each i. This shows (i) except for the second and fourth equality. Using (2.13) as in the proof of Lemma 2.17, we get

$$v(a_0 - a_2) = v(a_1 + a_3) + v(c), \tag{2.19}$$

which shows that $v(\lambda) = v((a_0 - a_2)/(a_1 - a_3)) = v(a_0 - a_2) - 1$, which shows the second equality. If we combine this with (2.19), we get $v(\lambda) = v(a_1 + a_3) + v(c) - 1$. This concludes the proof of the fourth equality and therefore that of (i). Part (ii) is a direct consequence of part (i). □

We have the following converse of Lemma 2.21(ii).

Lemma 2.22. *Let $\lambda_0, \mu_0 \in \mathbb{Q}_2$ satisfy $v(\lambda_0) \geq v(c)+1$ and $v(\mu_0) = 0$. Then there exists a unique point $P \in \mathcal{A}_c$ such that $f(P) = \lambda_0$ and $g(P) = \mu_0$. Moreover, the dependence of P on λ_0 and μ_0 is continuous.*

Proof. We rewrite (2.13) in terms of the homogeneous coordinates $s_0 = x_0 + x_2, v_0 = x_0 - x_2, s_1 = x_1 + x_3, v_1 = x_1 - x_3$:

$$s_0 v_0 (s_0^2 + v_0^2) = -c s_1 v_1 (s_1^2 + v_1^2).$$

We are looking for a point with $f(P) = \lambda_0$ and $g(P) = \mu_0$. We thus have $v_0 = \lambda_0 v_1$ and $s_0 = \mu_0 v_1$. In terms of $w = s_1/v_1$ we have to solve the equation

$$\lambda_0 \mu_0 (\lambda_0^2 + \mu_0^2) = -cw(1 + w^2).$$

Defining

$$a = \frac{\lambda_0 \mu_0}{c} (\lambda_0^2 + \mu_0^2),$$

we can rewrite the equation as

$$w^3 + w + a = 0.$$

Given a solution $w_0 \in \mathbb{Q}_2$ to this equation, we get the point in $V_c(\mathbb{Q}_2)$ represented by the four-tuple

$$P_0 = (\lambda_0 + \mu_0 : w_0 + 1 : -\lambda_0 + \mu_0 : w_0 - 1). \tag{2.20}$$

Note that we have $v(a) > 0$. By considering the Newton polygon of $w^3 + w + a$, we see that two of its zeros in $\overline{\mathbb{Q}}_2$ have valuation 0. These do not give rise to points in $\mathcal{U}'_c$. The remaining zero w_0 has positive valuation. By Galois theory, we have $w_0 \in \mathbb{Q}_2$. By the assumptions on λ_0, μ_0 and the fact that $v(w_0) > 0$, the four-tuple (2.20) represents a point in $\mathcal{U}'_c$. One can check that it in fact lies in $\mathcal{A}_c$. For the P whose existence was asserted in the lemma we may thus take $P = P_0$. Finally, the fact that P depends continuously on λ_0 and μ_0 is shown exactly as in the proof of Lemma 2.18. □

For each $P \in \mathcal{A}_c$, we will identify $f^{-1}(f(P))$ with the generic fibre of (2.8) via (2.9). Note that this is the same choice that we made in section 2.5 for $P \in \mathcal{C}_{c,1}$, so that it makes sense to compare levels along f of points in $\mathcal{A}_c$ and $\mathcal{C}_{c,1}$. We will identify the fibre $g^{-1}(g(P))$ with the generic fibre of (2.3) via (2.4). It follows from Lemma 2.21(ii) that these identifications can be made. With these conventions, it makes sense to speak of the levels of the points in $\mathcal{A}_c$ along f and g.

Lemma 2.23. *Let P be a point in $\mathcal{A}_c$ and write $\lambda = f(P)$. The level of P along f is equal to 0. The level of P along g is equal to $v(\lambda) - v(c)$.*

Proof. We write $P = (a_0 : a_1 : a_2 : a_3)$. We obtain a representative $(\widetilde{\xi} : \widetilde{\eta} : \widetilde{\zeta})$ of the image of P on $\widetilde{\mathcal{E}}_\lambda$ by substituting $x_i = a_i$ into the equations (2.9). Using (2.9), we get

$$v(\widetilde{\xi}) = v(a_0+a_2)-3v(c)-1 = -3v(c),\ \ v(\widetilde{\eta}) = v(a_1-a_3)-3v(c)-1 = -3v(c),$$

where we have used the definition of $\mathcal{A}_c$. To compute the valuation of

$$\widetilde{\zeta} = \frac{a_1 + a_3 + \frac{\lambda^3}{c}(a_0 + a_2)}{2\lambda(c^2 - \lambda^8)}, \tag{2.21}$$

note that Lemma 2.21(i) implies $v(a_1 + a_3) = v(\lambda) + 1 - v(c) < 3v(\lambda) + 1 - v(c) = v(\frac{\lambda^3}{c}(a_0 + a_2))$; hence the valuation of the numerator is equal to $v(a_1 + a_3)$. Therefore

$$v(\widetilde{\zeta}) = v(a_1+a_3)-v(2\lambda(c^2-\lambda^8)) = (v(\lambda)+1-v(c))-(v(\lambda)+1+2v(c)) = -3v(c).$$

It follows that we have $v(\widetilde{\xi}/\widetilde{\zeta}) = v(\widetilde{\eta}/\widetilde{\zeta}) = 0$. Therefore the point P reduces to a non-singular point different from the identity on the special fibre of $\widetilde{E}_\lambda$. Thus we have shown that the level of P along f is 0.

Set $\mu = g(P)$. We obtain a representative $(\xi : \eta : \zeta)$ of the image of P on $\mathcal{E}_\mu$ by substituting $x_i = a_i$ for $i \neq 2$ and $x_2 = -a_2$ into the equations (2.4), and replacing λ by μ. We get

$$v(\xi) = v(a_0 - a_2) - 1 - v(c) = v(\lambda) - v(c) \geq 1$$

and

$$v(\eta) = v(a_1 - a_3) - 1 = 0.$$

From $v(\mu) = 0$ and (2.19) we deduce

$$v(a_1 + a_3) = v\left(\frac{\mu^3}{c}(a_0 - a_2)\right),$$

hence we have, by formula (2.4),

$$v(\zeta) > v(a_1 + a_3) - v(2\mu(c^2 - \mu^8)) = v(a_1 + a_3) - 1 > 0.$$

Since $v(\eta) < v(\zeta)$, the point P is mapped to $(\mathcal{E}_\mu)_1(\mathbb{Q}_p)$, and its level is therefore $v(\xi/\eta) = v(\lambda) - v(c)$. □

Proposition 2.24. *Assume that there is a rational point $P_0 \in V_c(\mathbb{Q})$ such that $P_0 \in \mathcal{C}_{c,1}$. Then $V_c(\mathbb{Q})$ is dense in $\mathcal{A}_c$.*

Proof. Let P_0 be as in the statement of the proposition, and let $P_2 \in \mathcal{A}_c$ be an arbitrary 2-adic point. Define $\lambda_0 = f(P)$ and $\mu_2 = g(P_2)$. We have $v(\lambda_0) = v(c) + 1$ by Lemma 2.17(ii) and $v(\mu_2) = 0$ by Lemma 2.21(ii). It follows from Lemma 2.22 that there exists a unique $P_1 \in \mathcal{A}_c$ such that $f(P_1) = \lambda_0$ and $g(P_1) = \mu_2$.

By Lemma 2.19 we have that the level of P along f is -1 and, by Lemma 2.23, the level of P_1 along f is 0. Also by Lemma 2.23, the level of P_1 along g equals $v(f(P_1)) - v(c) = 1$ and level of P_2 along g is $v(f(P_2)) - v(c)$, which is at least 1 by Lemma 2.21. The f-fibre through P_1 is smooth since it equals the f-fibre through P_0, which is smooth by Corollary 2.14. Moreover, we may assume that the g-fibre through P_1 is smooth, since we may otherwise replace P_2 by a point lying arbitrarily close to it by Lemma 2.22. By Lemma 2.16, the rational points lie dense around P_2. □

2.7 Density in $\mathcal{B}_{c,n}$ for all n and in $\mathcal{C}'_{c,n}$ for $n \geq 2$

Assuming density of $V_c(\mathbb{Q})$ in $\mathcal{A}'_c$, we show that the rational points on V_c are dense in $\mathcal{B}_{c,n}$ for all $n \geq 1$ and in $\mathcal{C}'_{c,n}$ for all $n \geq 2$.

Lemma 2.25. *The following statements are true.*

(i) Let $P = (a_0 : a_1 : a_2 : a_3)$ be a point in $\mathcal{A}'_c$, where the a_i are 2-adic integers at least one of which is a unit. Write $\lambda = f(P)$. We have

$$v(a_0 + a_2) = v(c) + 1 - v(\lambda), v(a_0 - a_2) = 1, v(a_0^2 + a_2^2) = 1$$

as well as

$$v(a_1 + a_3) = 1, v(a_1 - a_3) = 1 - v(\lambda), v(a_1^2 + a_3^2) = 1.$$

(ii) Let $P \in \mathcal{A}'_c$ and write $\lambda = f(P), \mu = g(P)$. Then we have $v(\lambda) < 0$ and $v(\mu) = v(c)$.

(iii) Let $P = (a_0 : a_1 : a_2 : a_3)$ be a point in $\mathcal{B}_{c,n}$ for some integer $n \geq 1$, where the a_i are 2-adic integers at least one of which is a unit. We have

$$v(a_0 - a_2) = 1, v(a_0^2 + a_2^2) = 1$$

as well as

$$v(a_1+a_3) = v(a_0+a_2)-3n-v(c), v(a_1-a_3) = n+1, v(a_1^2+a_3^2) = 2n+1.$$

(iv) Let $P \in \mathcal{B}_{c,n}$ for some integer $n \geq 1$. Write $\lambda = f(P)$. Then we have $v(\lambda) = -n$.

(v) Let $P = (a_0 : a_1 : a_2 : a_3) \in \mathcal{C}'_{c,n}$ for some integer $n \geq 2$, where the a_i are 2-adic integers at least one of which is a unit. We have

$$v(a_0 + a_2) = v(c) + 4n - 2, v(a_0 - a_2) = 1, v(a_0^2 + a_2^2) = 1$$

as well as

$$v(a_1 + a_3) = n, v(a_1 - a_3) = n, v(a_1^2 + a_3^2) = 2n.$$

(vi) Let $P \in \mathcal{C}'_{c,n}$ for some integer $n \geq 2$. Write $\lambda = f(P)$. Then we have $v(\lambda) = 1 - n$.

Proof. Part (i) follows directly from Lemma 2.21(i). Part (ii) follows from part (i). In part (iii), the first and fourth equality follow directly from the definition of $\mathcal{B}_{c,n}$. For the second and fifth, one uses that if $a \in \mathbb{Z}_2$, then $a^2 \equiv 2^{2v(a)} \pmod{2^{2v(a)+3}}$. The third equality follows from the others and from (2.13). Part (iv) follows from part (iii). In part (v), the only non-obvious equation is the first one: it follows from the others and (2.13). Part (vi) follows from part (v). □

We have the following converse of Lemma 2.25(ii).

Lemma 2.26. *Let $\lambda_0, \mu_0 \in \mathbb{Q}_2$ satisfy $v(\lambda_0) < 0$ and $v(\mu_0) = v(c)$. Then there exists a unique point $P \in \mathcal{A}'_c$ such that $f(P) = \lambda_0$ and $g(P) = \mu_0$. Moreover, the dependence of P on λ_0 and μ_0 is continuous.*

Proof. As in the proof of Lemma 2.22, we define

$$a = \frac{\lambda_0 \mu_0}{c}(\lambda_0^2 + \mu_0^2).$$

Still as in the proof of Lemma 2.22, given a solution w_0 to the equation

$$w^3 + w + a = 0, \tag{2.22}$$

we get the point in $V_c(\mathbb{Q}_2)$ represented by the four-tuple

$$(\lambda_0 + \mu_0 : w_0 + 1 : -\lambda_0 + \mu_0 : w_0 - 1). \tag{2.23}$$

Under the assumptions of the lemma, we have $v(a) = 3v(\lambda_0) < 0$. If we put $w = \lambda_0 w'$, equation (2.22) transforms to

$$w'^3 + \lambda_0^{-2} w' + a\lambda_0^{-3} = 0, \tag{2.24}$$

where $a\lambda_0^{-3} \in \mathbb{Z}_2^*$. By Hensel's lemma, this has a solution $w'_0 \in \mathbb{Z}_2^*$. Moreover, the three roots w'_0, w'_1, w'_2 of (2.24) in $\overline{\mathbb{Q}}_2$ reduce to the three zeros of $X^3 + 1$ in $\overline{\mathbb{F}}_2$, only one of which lies in $\mathbb{F}_2$; therefore, w'_0 is the unique solution to (2.24) in $\mathbb{Q}_2$. We then have $w_0 = \lambda_0 w'_0$ with $v(w_0) = v(\lambda_0) < 0$. The four-tuple (2.23) that we obtain has non-integral coordinates. Scaling by λ_0^{-1}, we obtain the four-tuple

$$(\mu_0/\lambda_0 + 1 : w'_0 + \lambda_0^{-1} : \mu_0/\lambda_0 - 1 : w'_0 - \lambda_0^{-1}),$$

which defines a point in $\mathcal{U}'_c$, and one checks that it lies in $\mathcal{A}'_c$. For the P whose existence was asserted in the lemma we may thus take $P = P_0$. Finally, the fact that P depends continuously on λ_0 and μ_0 follows as in the proof of Lemma 2.18. □

For a point $P \in V_c(\mathbb{Q}_2)$ that is contained in $\mathcal{A}'_c$, in $\mathcal{B}_{c,n}$ for some $n \geq 1$, or in $\mathcal{C}_{c,n}$ for some $n \geq 2$, we will identify $f^{-1}(f(P))$ with the generic fibre of the curve $\widehat{\mathcal{E}}_{f(P)}$ given by (2.10) via (2.11). Since Lemma 2.25 shows that $v(f(P)) < 0$ in each case, these identifications may be made. Accordingly, the level along f of such a point P is well-defined.

Lemma 2.27. *Let $P = (a_0 : a_1 : a_2 : a_3) \in V_c(\mathbb{Q}_2)$ be a point, where the a_i are 2-adic integers at least one of which is a unit.*

(i) Assume that $P \in \mathcal{A}'_c$. The level of P along f is equal to 0.
(ii) Assume that $P \in \mathcal{B}_{c,n}$ for some $n \geq 1$. The level of P along f is equal to $v(a_1 + a_3) - 1$, which is an integer at least 2.
(iii) Assume that $P \in \mathcal{C}'_{c,n}$ for some $n \geq 2$. The level of P along f is equal to $n - 1$.

Proof. We write $\lambda = f(P)$. In all cases (i)–(iii), we obtain a representative $(\widehat{\xi} : \widehat{\eta} : \widehat{\zeta})$ of the image of P on $\widehat{\mathcal{E}}_\lambda$ by substituting $x_i = a_i$ into the equations (2.11). We have

$$v(\widehat{\xi}) = v\left(-\frac{a_0 + a_2}{2\lambda^4 c} - \frac{\lambda(a_1 + a_3) + \frac{\lambda^4}{c}(a_0 + a_2)}{2(c^2 - \lambda^8)}\right). \tag{2.25}$$

We will only need to compute this valuation for case (ii). We have $v\left(-\frac{a_0+a_2}{2\lambda^4 c}\right) = v(a_0 + a_2) - 1 - v(c) + 4n = v(a_1 + a_3) + 7n - 1$ by Lemma 2.25(iii)–(iv). Both the terms $\lambda(a_1 + a_3)$ and $\frac{\lambda^4}{c}(a_0 + a_2)$ have valuation equal to $v(a_1 + a_3) - n$ by Lemma 2.25(iii)–(iv). Hence the second fraction in (2.25) has valuation greater than or equal to $v(a_1 + a_3) + 7n$. Hence in case (ii) we have $v(\widehat{\xi}) = v(a_1 + a_3) + 7n - 1$.

For

$$v(\widehat{\eta}) = v\left(\frac{a_1 - a_3}{2\lambda^6}\right),$$

we have in case (i) that $v(\widehat{\eta}) = -7v(\lambda)$. In case (ii) we find $v(\widehat{\eta}) = n + 1 - (1 - 6n) = 7n$. In case (iii) we get $v(\widehat{\eta}) = n - (1 + 6(1 - n)) = 7n - 7$.

Finally, we consider

$$v(\widehat{\zeta}) = v\left(\frac{a_1 + a_3 + \frac{\lambda^3}{c}(a_0 + a_2)}{2\lambda(c^2 - \lambda^8)}\right).$$

In case (i), we have $v(a_1 + a_3) = 1$ and $v(\frac{\lambda^3}{c}(a_0 + a_2)) = 2v(\lambda) + 1 < 1$; therefore, we have that $v(\widehat{\zeta}) = 2v(\lambda) + 1 - (1 + 9v(\lambda)) = -7v(\lambda)$. In case (ii), both the terms $a_1 + a_3$ and $\frac{\lambda^3}{c}(a_0 + a_2)$ have valuation equal to $v(a_1 + a_3)$, hence we have that $v(\widehat{\zeta}) \geq v(a_1 + a_3) + 9n$. In case (iii), we have $v(a_1 + a_3) = n$ and $v(\frac{\lambda^3}{c}(a_0 + a_2)) = 3(1 - n) - v(c) + v(c) + 4n - 2 = n + 1$; therefore, we have that $v(\widehat{\zeta}) = n - (10 - 9n) = 10n - 10$.

We finish the proof for case (i) by observing that, in that case, we have $v(\widehat{\eta}/\widehat{\zeta}) = 0$. Therefore, in view of equation (2.10), we must have that the level of P is 0. In case (ii) we see that $v(\widehat{\eta}/\widehat{\zeta}) \leq -2n - v(a_1 + a_3)$, which implies that the level of P is equal to $v(\widehat{\xi}/\widehat{\zeta}) = v(a_1 + a_3) - 1 \geq 2$, where the last inequality follows from $v(a_1 + a_3) \geq 3$. Finally, in case (iii), we have $v(\widehat{\eta}/\widehat{\zeta}) = -3n + 3$, which shows that the level of P is equal to $n - 1$. □

Proposition 2.28. *Assume the density of $V_c(\mathbb{Q})$ in $\mathcal{A}'_c$. The rational points on V_c are dense in $\mathcal{B}_{c,n}$ for all integers $n \geq 1$ and in $\mathcal{C}'_{c,n}$ for all integers $n \geq 2$.*

Proof. Let P_1 be any point in either $\mathcal{B}_{c,n}$ or $\mathcal{C}'_{c,n}$, where n is as in the proposition. Then if $\lambda_1 = f(P_1)$, we have $v(\lambda_1) < 0$ by Lemma 2.25(iv)+(vi). By Lemma 2.26, there exists $P_0 \in \mathcal{A}'_c$ such that $f(P_0) = \lambda_1$ and $g(P_0) = c$. Note that P_0 and P_1 lie on the same fibre of f. Since the rational points on V_c are dense in $\mathcal{A}'_c$, there is a sequence $\{P'_i\}_{i=0}^{\infty} \subset V_c(\mathbb{Q})$ that converges to P_0. By Lemma 2.27, the level of P_0 along f is 0 and the level of P_1 along f is at least 1. By Corollary 2.14, the f-fibre through P_0 and P_1 is smooth. Hence we are done by Lemma 2.15. □

2.8 Proof of the main theorem

Theorem 2.29. *Let c be an element of the set*

$$S = \{2, 4, 6, 10, 12, 14, 18, 20, 22, 2/3, 2/5, 2/7, 2/9, 2/11\}.$$

Then the set $V_c(\mathbb{Q})$ lies dense in the set $V_c(\mathbb{Q}_2)$, when this set is equipped with the 2-adic topology.

Proof. In view of the discussion in section 2.1, it suffices to exhibit an element $P_c \in V_c(\mathbb{Q})$ that lies in $\mathcal{C}_{c,1}$ for each c such that either c or $16/c$ lies in S. This is done in the table below.

Value of c	Point P_c in $V_c(\mathbb{Q}) \cap \mathcal{C}_{c,1}$
2	$P_2 = (489 : 684 : 577 : 662)$
4	$P_4 = (61 : 168 : 237 : 58)$
6	$P_6 = (67 : 16 : -37 : 42)$
8	$P_8 = (257 : 22 : -223 : 124)$
10	$P_{10} = (1 : 4 : -7 : 2)$
12	$P_{12} = (359 : 112 : -361 : 106)$
14	$P_{14} = (11 : 4 : 3 : 6)$
18	$P_{18} = (9 : 16 : 33 : 2)$
20	$P_{20} = (309 : 132 : 37 : 166)$
22	$P_{22} = (347 : 76 : -269 : 146)$
24	$P_{24} = (11 : 308 : -533 : 274)$
40	$P_{40} = (29 : 12 : -3 : 14)$
56	$P_{56} = (43 : 68 : 139 : 62)$
72	$P_{72} = (269 : 52 : 109 : 94)$
88	$P_{88} = (1333 : 172 : 1109 : 374)$
2/3	$P_{2/3} = (39 : 4 : 31 : 38)$
2/5	$P_{2/5} = (31 : 8 : -25 : 34)$
2/7	$P_{2/7} = (349 : 124 : -347 : 194)$
2/9	$P_{2/9} = (3 : 16 : 11 : 2)$
2/11	$P_{2/11} = (179 : 76 : -53 : 274)$
4/3	$P_{4/3} = (171 : 88 : -101 : 158)$
4/5	$P_{4/5} = (79 : 452 : 415 : 262)$
8/3	$P_{8/3} = (19 : 4 : -13 : 14)$
8/5	$P_{8/5} = (5 : 24 : -27 : 2)$
8/7	$P_{8/7} = (599 : 2732 : 1591 : 2662)$
8/9	$P_{8/9} = (269 : 156 : 109 : 282)$
8/11	$P_{8/11} = (391 : 152 : -281 : 394)$

□

Proof of Theorem 2.1. This follows from Theorem 2.29. □