ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 40, Number 4, 2010

A NOTE ON ELLIPTIC CURVES WITH A RATIONAL 3-TORSION POINT

RINTARO KOZUMA

ABSTRACT. We determine reduction types and images of local connecting homomorphisms of elliptic curves with a rational 3-torsion point over a number field in which 3 is unramified. These results are shown to be useful for the explicit calculation of Selmer groups.

1. Introduction. Let E be an elliptic curve defined over a number field F with an F-rational 3-torsion point, and let $\phi : E \to \widehat{E}$ be an associated 3-isogeny over F with the dual elliptic curve $\widehat{E}/F$. Assume that 3 is unramified in F. We begin in Section 3 by calculating minimal Weierstrass forms and the number of irreducible components of Néron models for E, $\widehat{E}$ over the completion $F_{\mathfrak{p}}$ at a finite prime $\mathfrak{p}$. With these results, in Section 4 we determine the image of the local connecting homomorphisms (Theorem 4.1) that fit into the composed injection

$$\widehat{\delta}_{F_{\mathfrak{p}}} : E(F_{\mathfrak{p}})/\widehat{\phi}\big(\widehat{E}(F_{\mathfrak{p}})\big) \longrightarrow H^1(F,\, \widehat{E}[\widehat{\phi}]) \xrightarrow{e_{\widehat{\phi}}} H^1(F_{\mathfrak{p}},\, \mu_3) \longrightarrow F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*3},$$

where $e_{\widehat{\phi}}$ stands for a Weil $\widehat{\phi}$-pairing. This result enables us in Section 5 to explicitly calculate the Selmer groups of E/F associated with ϕ. As an application, we will consider Knight's problem in Section 6. We first introduce notation used in the present paper and recall some basic results of descent theory in Section 2.

2. Descent via isogenies. Let E be an elliptic curve defined over a number field F. The well known Mordell-Weil theorem states that the set of F-rational points on an elliptic curve E, often called a Mordell-Weil group, is a finitely generated abelian group. One problem of prime interest is the determination of the rank of the Mordell-Weil group $E(F)$. If one could calculate the finite quotient group $E(F)/mE(F)$ for some integer $m > 1$, one could thence find the rank of $E(F)$. Descent

Received by the editors on December 1, 2007, and in revised form on December 28, 2007.

DOI:10.1216/RMJ-2010-40-4-1227

theory gives an upper bound for the size of the group $E(F)/mE(F)$, which also often corresponds to the exact size of this group.

Now assume E admits an m-isogeny $\phi : E \to \widehat{E}$ over F with dual elliptic curve $\widehat{E}/F$, and let $\widehat{\phi} : \widehat{E} \to E$ be its dual isogeny. For a short exact sequence $0 \to E[\phi] \to E(\overline{F}) \xrightarrow{\phi} \widehat{E}(\overline{F}) \to 0$ as G_F-modules (G_F : the absolute Galois group of F), taking Galois cohomology yields the exact sequence

$$0 \longrightarrow \widehat{E}(F)/\phi\big(E(F)\big) \longrightarrow H^1(F,\, E[\phi]) \longrightarrow H^1(F,\, E)[\phi] \longrightarrow 0.$$

Considering the above F again locally, we also have a similar localized exact sequence. For the completion $F_{\mathfrak{p}}$ at each prime $\mathfrak{p}$ of F, fix an embedding $\overline{F} \hookrightarrow \overline{F_{\mathfrak{p}}}$ once and for all. Since the embedding $\overline{F} \hookrightarrow \overline{F_{\mathfrak{p}}}$ induces restriction maps of Galois cohomology, we obtain the following commutative diagram.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{\widehat{E}(F)}{\phi\left(E(F)\right)} & \xrightarrow{\delta} & H^1(F,\, E[\phi]) & \longrightarrow & H^1(F,\, E)[\phi] & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \mathrm{res}_{\mathfrak{p}}} & & \Big\downarrow{\scriptstyle \mathrm{res}_{\mathfrak{p}}} & & \Big\downarrow{\scriptstyle \mathrm{res}_{\mathfrak{p}}} & & \\
0 & \longrightarrow & \dfrac{\widehat{E}(F_{\mathfrak{p}})}{\phi\left(E(F_{\mathfrak{p}})\right)} & \xrightarrow{\delta_{\mathfrak{p}}} & H^1(F_{\mathfrak{p}},\, E[\phi]) & \longrightarrow & H^1(F_{\mathfrak{p}},\, E)[\phi] & \longrightarrow & 0
\end{array}$$

where δ, $\delta_{\mathfrak{p}}$ stands for connecting homomorphisms. Note that for an infinite prime $\mathfrak{p}$, if $2 \nmid \sharp E[\phi]$, then $H^1(F_{\mathfrak{p}},\, E[\phi])$ is trivial, and hence the map $\delta_{\mathfrak{p}}$ is also trivial. The ϕ-Selmer group of the elliptic curve E is a finite subgroup of $H^1(F,\, E[\phi])$ defined by

$$S^{(\phi)}(E/F) = \Big\{ \overline{\xi} \in H^1(F,\, E[\phi]) \;\Big|\; \mathrm{res}_{\mathfrak{p}}(\overline{\xi}) \in \mathrm{Im}\,\delta_{\mathfrak{p}} \quad \text{for any finite/infinite prime } \mathfrak{p} \text{ of } F \Big\}.$$

With reference to the above diagram, it is clear that the Selmer group $S^{(\phi)}(E/F)$ contains $\widehat{E}(F)/\phi\big(E(F)\big)$ as a subgroup. The gap between these groups is represented by the ϕ-kernel of the Shafarevich-Tate group, which fits into the exact sequence

$$0 \longrightarrow \widehat{E}(F)/\phi\big(E(F)\big) \longrightarrow S^{(\phi)}(E/F) \longrightarrow Ш(E/F)[\phi] \longrightarrow 0.$$

Conversely, one can define the $\widehat{\phi}$-Selmer group $S^{(\widehat{\phi})}(\widehat{E}/F)$, the $\widehat{\phi}$-kernel of the Shafarevich-Tate group $Ш(\widehat{E}/F)[\widehat{\phi}]$ by interchanging the role of the isogenies ϕ and $\widehat{\phi}$.

The relation between the finite groups $\widehat{E}(F)/\phi\big(E(F)\big)$ and $E(F)/\widehat{\phi}\big(\widehat{E}(F)\big)$ is described by the exact sequence

$$0 \longrightarrow \frac{\widehat{E}(F)[\widehat{\phi}]}{\phi\big(E(F)[m]\big)} \longrightarrow \frac{\widehat{E}(F)}{\phi\big(E(F)\big)} \xrightarrow{\widehat{\phi}} \frac{E(F)}{mE(F)} \longrightarrow \frac{E(F)}{\widehat{\phi}\big(\widehat{E}(F)\big)} \longrightarrow 0.$$

From this, when $m = p$ is a rational prime number, each term of the above sequence is a vector space over $\mathbf{F}_p$, and we thus have

$$\begin{aligned} \operatorname{rank}_{\mathbf{Z}} E(F) = {} & \dim_{\mathbf{F}_p} \frac{E(F)}{\widehat{\phi}\big(\widehat{E}(F)\big)} + \dim_{\mathbf{F}_p} \frac{\widehat{E}(F)}{\phi\big(E(F)\big)} \\ & - \dim_{\mathbf{F}_p} \frac{\widehat{E}(F)[\widehat{\phi}]}{\phi\big(E(F)[p]\big)} - \dim_{\mathbf{F}_p} E(F)[p]. \end{aligned} \tag{2.1}$$

Though it is straightforward to calculate the last two terms on the right-hand side, the first two terms on this side are, in general, particularly difficult to calculate. However, the Selmer groups can be calculated in principle and hence give an upper bound for the rank of $E(F)$.

Given an isogeny and its dual isogeny, it is known that Cassels' duality formula in [**3**] connects the order of a Selmer group with that of its dual Selmer group. Let $|\cdot|_{\mathfrak{p}}$ be the valuation of $F_{\mathfrak{p}}$ with the usual normalization $|\pi|_{\mathfrak{p}} = \sharp\mathbf{F}_{\mathfrak{p}}^{-1}$ ($\mathbf{F}_{\mathfrak{p}} := \mathfrak{O}_F/\mathfrak{p}$, $\mathfrak{O}_F$: the ring of integers of F) where π stands for a prime element in $F_{\mathfrak{p}}$, and let $E_0(F_{\mathfrak{p}})$ be the group of $F_{\mathfrak{p}}$-rational points on E with nonsingular reduction (of course, the Weierstrass form is taken to be minimal), which is isomorphic to the group of $\mathfrak{O}_{F_{\mathfrak{p}}}$-valued points on the identity component of a Néron model for $E/F_{\mathfrak{p}}$. Define $\widehat{E}_0(F_{\mathfrak{p}})$ similarly.

Theorem 2.1 [**3**]. *Let E be an arbitrary elliptic curve and $\phi : E \to \widehat{E}$ an isogeny, which are both defined over a number field F. Then*

$$\frac{\sharp S^{(\phi)}(E/F)}{\sharp S^{(\widehat{\phi})}(\widehat{E}/F)} = \frac{\sharp E(F)[\phi]}{\sharp \widehat{E}(F)[\widehat{\phi}]} \prod_{\mathfrak{p}} \frac{\int_{\widehat{E}(F_{\mathfrak{p}})} |\widehat{\omega}|_{\mathfrak{p}}}{\int_{E(F_{\mathfrak{p}})} |\omega|_{\mathfrak{p}}}$$

where $\mathfrak{p}$ varies through all the primes of F. Here ω is a global invariant differential on E/F, and $\widehat{\bullet}$ stands for the dual of the object $\bullet$.

We remark on the integrals in the above theorem. Since there is some $\alpha \in F^*$ such that $\phi^*\widehat{\omega} = \alpha\omega$, we calculate

(2.2)
$$\int_{E(F_\mathfrak{p})} |\omega|_\mathfrak{p} = |\alpha|_\mathfrak{p}^{-1} \cdot \sharp E(F_\mathfrak{p})[\phi] \cdot \left[\widehat{E}(F_\mathfrak{p}) : \phi\big(E(F_\mathfrak{p})\big)\right]^{-1} \cdot \int_{\widehat{E}(F_\mathfrak{p})} |\widehat{\omega}|_\mathfrak{p}.$$

This not only holds for global ω, $\widehat{\omega}$, but also for any local invariant differentials on E and $\widehat{E}$. The case for the dual is similar, but note that $\alpha\widehat{\alpha} = \deg\phi$ for $\widehat{\alpha} \in F^*$ with $\widehat{\phi}^*\omega = \widehat{\alpha}\widehat{\omega}$. Combining these facts with the product formula of the valuation $|\cdot|_\mathfrak{p}$ yields

$$\prod_\mathfrak{p} \frac{\int_{\widehat{E}(F_\mathfrak{p})} |\widehat{\omega}|_\mathfrak{p}}{\int_{E(F_\mathfrak{p})} |\omega|_\mathfrak{p}} = \prod_\mathfrak{p} \frac{\left[\widehat{E}(F_\mathfrak{p}) : \phi\big(E(F_\mathfrak{p})\big)\right]}{\sharp E(F_\mathfrak{p})[\phi]},$$

a result first derived by Cassels in [**3**].

Furthermore, when $\mathfrak{p}$ is a finite prime, Tate pointed out in [**8**] that $\int_{E(F_\mathfrak{p})} |\omega|_\mathfrak{p} = [E(F_\mathfrak{p}) : E_0(F_\mathfrak{p})](\sharp E_\mathfrak{p}(\mathbf{F}_\mathfrak{p})_{\mathrm{ns}}/\sharp\mathbf{F}_\mathfrak{p})$ for an invariant differential ω on $E/F_\mathfrak{p}$ associated with a minimal Weierstrass form. Here the subscript ns stands for nonsingular points on the reduced curve $E_\mathfrak{p}$ of E at $\mathfrak{p}$. Upon deriving the corresponding expression for the dual, we have $\int_{\widehat{E}(F_\mathfrak{p})} |\widehat{\omega}|_\mathfrak{p} / \int_{E(F_\mathfrak{p})} |\omega|_\mathfrak{p} = [\widehat{E}(F_\mathfrak{p}) : \widehat{E}_0(F_\mathfrak{p})]/[E(F_\mathfrak{p}) : E_0(F_\mathfrak{p})]$ since $\sharp\widehat{E}_\mathfrak{p}(\mathbf{F}_\mathfrak{p})_{\mathrm{ns}} = \sharp E_\mathfrak{p}(\mathbf{F}_\mathfrak{p})_{\mathrm{ns}}$, which is an isogeny invariant. By equation (2.2), we have that

$$\begin{aligned} \frac{[\widehat{E}(F_\mathfrak{p}) : \widehat{E}_0(F_\mathfrak{p})]}{[E(F_\mathfrak{p}) : E_0(F_\mathfrak{p})]} &= |\alpha|_\mathfrak{p} \frac{\left[\widehat{E}(F_\mathfrak{p}) : \phi\big(E(F_\mathfrak{p})\big)\right]}{\sharp E(F_\mathfrak{p})[\phi]}, \\ \frac{[E(F_\mathfrak{p}) : E_0(F_\mathfrak{p})]}{[\widehat{E}(F_\mathfrak{p}) : \widehat{E}_0(F_\mathfrak{p})]} &= |\widehat{\alpha}|_\mathfrak{p} \frac{\left[E(F_\mathfrak{p}) : \widehat{\phi}\big(\widehat{E}(F_\mathfrak{p})\big)\right]}{\sharp\widehat{E}(F_\mathfrak{p})[\widehat{\phi}]}. \end{aligned} \tag{2.3}$$

If F has class number 1, then for any global invariant differentials ω, $\widehat{\omega}$,

$$\prod_\mathfrak{p} \frac{\int_{\widehat{E}(F_\mathfrak{p})} |\widehat{\omega}|_\mathfrak{p}}{\int_{E(F_\mathfrak{p})} |\omega|_\mathfrak{p}} = \prod_{\mathfrak{p}:\text{infinite}} \frac{\int_{\widehat{E}(F_\mathfrak{p})} |\widehat{\omega}_{\min}|_\mathfrak{p}}{\int_{E(F_\mathfrak{p})} |\omega_{\min}|_\mathfrak{p}} \prod_{\mathfrak{p}:\text{finite}} \frac{[\widehat{E}(F_\mathfrak{p}) : \widehat{E}_0(F_\mathfrak{p})]}{[E(F_\mathfrak{p}) : E_0(F_\mathfrak{p})]} \tag{2.4}$$

where $\omega_{\min}, \widehat{\omega}_{\min}$ are differentials associated with global minimal Weierstrass forms.

Henceforth we assume $E[\phi] \subset E(F)$.

2.1. On the Selmer group $S^{(\phi)}(E/F)$. For any finite group G, define the set of all Galois extensions over F whose Galois groups are isomorphic to a subgroup of G by

$$\mathfrak{Gal}(G/F) := \left\{ \left(\overline{F} \supset\right) K/F\text{: Galois extension} \;\middle|\; \mathrm{Gal}\,(K/F) \hookrightarrow G \right\} / \left\{\text{isomorphisms over } F\right\}.$$

Then the elements in $\mathfrak{Gal}(E[\phi]/F)$ come from the group $\mathrm{Hom}\,(G_F,\, E[\phi])$ by the surjection

$$\begin{aligned} \varrho : \mathrm{Hom}\,(G_F,\, E[\phi]) &\longrightarrow \mathfrak{Gal}(E[\phi]/F) \\ \xi &\longmapsto \overline{F}^{\mathrm{Ker}\,\xi} \end{aligned}$$

where $G_F := \mathrm{Gal}\,(\overline{F}/F)$. By the assumption $E[\phi] \subset E(F)$, we obtain the composed map

$$\begin{aligned} \delta_F : \widehat{E}(F)/\phi\big(E(F)\big) &\xrightarrow{\delta} H^1(F,\, E[\phi]) \\ &= \mathrm{Hom}\,(G_F,\, E[\phi]) \xrightarrow{\varrho} \mathfrak{Gal}(E[\phi]/F) \end{aligned}$$

which sends a point $P \in \widehat{E}(F)$ to an extension $F\big(\phi^{-1}(P)\big) \in \mathfrak{Gal}(E[\phi]/F)$ from the definitions.

Lemma 2.2. *For any $K \in \mathfrak{Gal}(E[\phi]/F)$, the fiber of the map ϱ at K is given by $\varrho^{-1}(K) = \{\xi = \iota \circ \mathrm{res}_K \mid \iota : \mathrm{Gal}\,(K/F) \hookrightarrow E[\phi]$; group injection$\}$. Here res_K stands for the restriction map $G_F \twoheadrightarrow \mathrm{Gal}\,(K/F)$. In particular, $\varrho^{-1}(F) = \{$the zero map$\}$, and for the case that the group $E[\phi]$ is cyclic, $\varrho(\xi) = \varrho(\eta)$ if and only if $\langle\xi\rangle = \langle\eta\rangle$ in $\mathrm{Hom}\,(G_F,\, E[\phi])$ for $\xi, \eta \in \mathrm{Hom}\,(G_F,\, E[\phi])$.*

Proof. For any $K \in \mathfrak{Gal}(E[\phi]/F)$, take the composed map $\xi : G_F \overset{\mathrm{res}}{\twoheadrightarrow} \mathrm{Gal}\,(K/F) \overset{\iota}{\hookrightarrow} E[\phi]$ with any injection ι. Then $\xi \in \mathrm{Hom}\,(G_F,\, E[\phi])$ and $\varrho(\xi) = K$, and hence ϱ is surjective. Since any $\xi \in \mathrm{Hom}\,(G_F,\, E[\phi])$

satisfying $\varrho(\xi) = K$ decomposes as above, the fiber $\varrho^{-1}(K)$ is identified with the set of injections $\iota : \mathrm{Gal}\,(K/F) \hookrightarrow E[\phi]$. The last statement then follows easily. □

Considering the above locally, we have the commutative diagram

$$\begin{array}{ccc} \widehat{E}(F)/\phi\big(E(F)\big) & \xrightarrow{\delta_F} & \mathfrak{Gal}(E[\phi]/F) \\ \big\downarrow{\scriptstyle \mathrm{res}_{\mathfrak{p}}} & & \big\downarrow{\scriptstyle \mathrm{res}_{\mathfrak{p}}} \\ \widehat{E}(F_{\mathfrak{p}})/\phi\big(E(F_{\mathfrak{p}})\big) & \xrightarrow{\delta_{F_{\mathfrak{p}}}} & \mathfrak{Gal}(E[\phi]/F_{\mathfrak{p}}). \end{array}$$

When $E[\phi]$ is cyclic of order m, by applying Lemma 2.2 we have that

$$\sharp S^{(\phi)}(E/F) = \sum_{K \in \mathcal{C}} \varphi\big([K : F]\big),$$

$$\mathcal{C} := \left\{ K \in \mathfrak{Gal}(C_m/F) \;\middle|\; \begin{array}{l} K/F \text{ is unramified outside } S_0 \\ K \cdot F_{\mathfrak{p}} \in \mathrm{Im}\,\delta_{F_{\mathfrak{p}}} \text{ for any } \mathfrak{p} \in S_0 \end{array} \right\}$$

where φ is the Euler function, C_m stands for the cyclic group of order m and S_0 the set of finite primes of F at which E has a bad reduction or dividing m.

2.2. On the Selmer group $S^{(\widehat{\phi})}(\widehat{E}/F)$. Assume that the group $E[\phi]$ is cyclic. Since $E[\phi] \subset E(F)$, the Weil pairing $e_{\hat{\phi}}(\cdot\,,\, T)$ with a fixed $T \in E[\phi]$ constructs injective homomorphisms $\widehat{\delta}_F$, $\widehat{\delta}_{F_{\mathfrak{p}}}$ that fit into the commutative diagram

$$\begin{array}{ccccc} \widehat{\delta}_F : \dfrac{E(F)}{\widehat{\phi}\big(\widehat{E}(F)\big)} & \xrightarrow{\widehat{\delta}} & H^1(F,\, \widehat{E}[\widehat{\phi}]) & \xrightarrow{e_{\hat{\phi}}(\cdot\,,\,T)} & H^1(F,\, \mu_m) \simeq F^*/F^{*m} \\ \big\downarrow & & \big\downarrow & & \\ \widehat{\delta}_{F_{\mathfrak{p}}} : \dfrac{E(F_{\mathfrak{p}})}{\widehat{\phi}\big(\widehat{E}(F_{\mathfrak{p}})\big)} & \xrightarrow{\widehat{\delta}_{\mathfrak{p}}} & H^1(F_{\mathfrak{p}},\, \widehat{E}[\widehat{\phi}]) & \xrightarrow{e_{\hat{\phi}}(\cdot\,,\,T)} & H^1(F_{\mathfrak{p}},\, \mu_m) \simeq F_{\mathfrak{p}}^*/F_{\mathfrak{p}}^{*m}. \end{array}$$

We can hence rewrite the $\widehat{\phi}$-Selmer group as

$$(2.5)\quad S^{(\widehat{\phi})}(\widehat{E}/F) = \Big\{ \overline{d} \in F^*/F^{*m} \;\Big|\; \overline{d} \in \operatorname{Im} \widehat{\delta}_{F_{\mathfrak{p}}} \text{ for any finite/infinite prime } \mathfrak{p} \text{ of } F \Big\}.$$

Further details of this argument can be found in [**6**].

3. Elliptic curves with a rational 3-torsion point. Let E/K be an elliptic curve defined over a perfect field K having a K-rational 3-torsion point. Then we can find a model of E/K as the form

$$(3.1)\quad y^2+axy+by = x^3 \quad \big(a,\, b \in K \text{ such that } \Delta := (a^3-27b)b^3 \neq 0\big),$$

with the 3-torsion point $(0,\, 0)$. The dual elliptic curve $\widehat{E} = E/\langle (0,\, 0)\rangle$ is then given by the form

$$(3.2)\quad y^2 + axy - 9by = x^3 - (a^3 + 27b)b \quad \big(\widehat{\Delta} := (a^3 - 27b)^3 b \neq 0\big),$$

while the 3-isogenies between them are

$$\begin{aligned} &\phi : E \longrightarrow \widehat{E}\,; \\ &(x,\, y) \longmapsto \left(\frac{x^3 + b(ax+b)}{x^2},\, \frac{x^3(y+4b) - b(ax+b)^2 + by(y-b)}{x^3} \right), \\ &\widehat{\phi} : \widehat{E} \longrightarrow E\,; \\ &(x,\, y) \longmapsto \left(\frac{(y-9b)(ax+y)}{(a^2+3x)^2},\, \left(\frac{y-9b}{a^2+3x} \right)^3 \right). \end{aligned}$$

These 3-isogenies have kernels and relations given by

$$(3.3)\quad \begin{aligned} &E[\phi] = \langle (0,\, 0)\rangle, && \phi^*\widehat{\omega} = \omega, \\ &\widehat{E}[\widehat{\phi}] = \left\langle \left(-\frac{a^2}{3},\, \frac{3(a^3+27b) + \sqrt{-3}(a^3-27b)}{18} \right) \right\rangle, && \widehat{\phi}^*\omega = 3\widehat{\omega}, \end{aligned}$$

where $\omega, \widehat{\omega}$ stand for the invariant differentials associated with the respective Weierstrass forms (3.1) and (3.2). Explicit formulae for general isogenies may be found in [**9**]. From the theory of the Weil pairing and descent (see [**6**]), the rational function $y \in K(E)$, whose

divisor is $3(0,\,0)-3(\mathcal{O})$ and satisfies $y\circ\widehat{\phi}\in K(\widehat{E})^{*3}$, describes the injection

$$\widehat{\delta}_K : E(K)/\widehat{\phi}\big(\widehat{E}(K)\big)\longrightarrow K^*/K^{*3} \tag{3.4}$$

in subsection 2.2 with $T=(0,\,0)$ as

$$\widehat{\delta}_K(P)=\begin{cases} yK^{*3} & \text{if } P=(x,\,y)\neq\mathcal{O},\,(0,\,0),\\ b^2K^{*3} & \text{if } P=(0,\,0),\\ K^{*3} & \text{if } P=\mathcal{O}.\end{cases} \tag{3.5}$$

In this paper we consider the case that K is a number field, F, or its $\mathfrak{p}$-adic completion, $F_\mathfrak{p}$. For the present case, there is no need to consider infinite primes $\mathfrak{p}$ since $H^1(F_\mathfrak{p},\,\widehat{E}[\widehat{\phi}])$ is trivial. For a finite prime $\mathfrak{p}$, let $\nu_\mathfrak{p}$ be the additive valuation of $F_\mathfrak{p}$ with the normalization $\nu_\mathfrak{p}(\pi)=1$. In order to determine the image of $\widehat{\delta}_{F_\mathfrak{p}}$, we first present simple, but useful, lemmas as follows:

Lemma 3.1. *Let $\mathfrak{p}$ be any finite prime of F. If $3\nu_\mathfrak{p}(a)\geq\nu_\mathfrak{p}(b)$ and $3\mid\nu_\mathfrak{p}(b)$, then* $\operatorname{Im}\widehat{\delta}_{F_\mathfrak{p}}\hookrightarrow\mathfrak{O}_{F_\mathfrak{p}}^*/\mathfrak{O}_{F_\mathfrak{p}}^{*3}$ $(\simeq\mathfrak{O}_{F_\mathfrak{p}}^*F_\mathfrak{p}^{*3}/F_\mathfrak{p}^{*3})$.

Proof. We assume $3\nu_\mathfrak{p}(a)\geq\nu_\mathfrak{p}(b)$ and $3\mid\nu_\mathfrak{p}(b)$. Let $m:=3^{-1}\nu_\mathfrak{p}(b)\in\mathbf{Z}$. Then the substitution $(x,\,y)\mapsto(\pi^{2m}x,\,\pi^{3m}y)$ yields the Weierstrass form $y(y+\pi^{-m}ax+\pi^{-3m}b)=x^3$ of E/F with coefficients in $\mathfrak{O}_{F_\mathfrak{p}}$. If $\nu_\mathfrak{p}(y)>0$, then $\nu_\mathfrak{p}(y+\pi^{-m}ax+\pi^{-3m}b)=0$, and hence $3\mid\nu_\mathfrak{p}(y)$. If $\nu_\mathfrak{p}(y)<0$, then $3\mid\nu_\mathfrak{p}(y)$. Therefore, the image (3.5) of $\widehat{\delta}_{F_\mathfrak{p}}$ is of $\mathfrak{p}$-exponent divided by 3 for any point $(x,\,y)\in E(F_\mathfrak{p})$. This yields the lemma. □

Lemma 3.2. *If $\nu_\mathfrak{p}(b)\not\equiv 0\pmod 3$, then the group $\langle bF_\mathfrak{p}^{*3}\rangle\simeq\mathbf{Z}/3\mathbf{Z}$ is a subgroup of* $\operatorname{Im}\widehat{\delta}_{F_\mathfrak{p}}$.

Proof. Since $\nu_\mathfrak{p}(b)\not\equiv 0\pmod 3$, the image of the point $(0,\,-b)\in E(F_\mathfrak{p})$ is $\widehat{\delta}_{F_\mathfrak{p}}(0,\,-b)=bF_\mathfrak{p}^{*3}$, which generates a subgroup isomorphic to $\mathbf{Z}/3\mathbf{Z}$. □

Take a minimal Weierstrass form of $E/F_{\mathfrak{p}}$, and for each $r \in \mathbf{N}$, let

$$E_r(F_{\mathfrak{p}}) = \{(x,\, y) \in E(F_{\mathfrak{p}}) \mid \nu_{\mathfrak{p}}(y) \leq -3r\} \cup \{\mathcal{O}\},$$
$$U_{\mathfrak{p}}^{(r)} = \{d \in F_{\mathfrak{p}} \mid \nu_{\mathfrak{p}}(d-1) \geq r\}\,.$$

By a similar argument as in the proof of Lemma 3.1, we can prove the following lemma.

Lemma 3.3. *Let $\mathfrak{p}$ be any finite prime of F, Δ the discriminant for the Weierstrass form* (3.1) *of $E/F_{\mathfrak{p}}$, and $\Delta_{\mathfrak{p}}$ a minimal discriminant of $E/F_{\mathfrak{p}}$. Then, for any integer $r > \nu_{\mathfrak{p}}(\Delta/\Delta_{\mathfrak{p}})/12$,*

$$\widehat{\delta}_{F_{\mathfrak{p}}}\big(E_r(F_{\mathfrak{p}})\big) \hookrightarrow U_{\mathfrak{p}}^{(t)} F_{\mathfrak{p}}^{*3}/F_{\mathfrak{p}}^{*3} \text{ where } t := r - \frac{\nu_{\mathfrak{p}}(\Delta/\Delta_{\mathfrak{p}})}{12} + \nu_{\mathfrak{p}}(a).$$

Proof. Let $(x,\, y) \mapsto (x',\, y')$ be a substitution that transforms the Weierstrass form (3.1) to a minimal Weierstrass form. Note that this is $F_{\mathfrak{p}}$-linear, see [**6**] for further details. Then, for any $(x',\, y') \in E_r(F_{\mathfrak{p}})$, the corresponding point $(x,\, y)$ belonging to (3.1) satisfies $3\nu_{\mathfrak{p}}(x) = 2\nu_{\mathfrak{p}}(y) = -6m$ by the assumption $m := r - \nu_{\mathfrak{p}}(\Delta/\Delta_{\mathfrak{p}})/12$ is positive. Making the substitution $(x,\, y) \mapsto (\pi^{-2m}x,\, \pi^{-3m}y)$ yields the Weierstrass form $y^2 + \pi^m axy + \pi^{3m} by = x^3$, and hence $(x,\, y)$ must be of the form $(s^2 + \pi^m t,\, s^3 + \pi^m u)$ for some $s \in \mathfrak{O}_{F_{\mathfrak{p}}}^*$ and $t,\, u \in \mathfrak{O}_{F_{\mathfrak{p}}}$. The statement clearly holds for the case $\pi \nmid 3$, namely the image of $\widehat{\delta}_{F_{\mathfrak{p}}}$ is trivial by (3.5). We thus assume $\pi \mid 3$. Substituting for $(x,\, y)$ in this form into this Weierstrass form yields the congruence $u \equiv as^2 \pmod{\pi^m}$; therefore, we have $s^{-3}y = 1 + \pi^m as^{-1} \in U_{\mathfrak{p}}^{(m+\nu_{\mathfrak{p}}(a))}$, which implies the statement by relations (3.5). □

For each finite prime $\mathfrak{p}$, we next calculate the reduction type of the elliptic curves E, $\widehat{E}$ over $F_{\mathfrak{p}}$ and the group indices $[E(F_{\mathfrak{p}}) : E_0(F_{\mathfrak{p}})]$, $[\widehat{E}(F_{\mathfrak{p}}) : \widehat{E}_0(F_{\mathfrak{p}})]$ which appear in formula (2.3). The proof relies entirely on Tate's algorithm [**7, 8**], but it is wholly systematic. For simplicity, when $\mathfrak{p} \mid 3$, we make the assumption that 3 is unramified in $F_{\mathfrak{p}}$ in certain cases. To ease notation, let q, r be rational integers defined by

$$\min\{3\nu_{\mathfrak{p}}(a),\, \nu_{\mathfrak{p}}(b)\} = 3q + r, \quad 0 \leq r < 3, \tag{3.6}$$

and let $(a',\, b',\, D') := (\pi^{-q}a,\, \pi^{-3q}b,\, a'^3 - 27b')$, which lie in the ring of integers $\mathfrak{O}_{F_\mathfrak{p}}$ from the definition. We shall denote by $(\frac{-}{\mathfrak{p}})$ the Legendre symbol at $\mathfrak{p}$. We also quote Ogg's formula, which will often be used in the proof of the lemmas below. (See also [**7**, IV].)

Theorem 3.4 (Ogg's formula [**5**]). *For any elliptic curve E over a local field $F_\mathfrak{p}/\mathbf{Q}_p$, let $\mathfrak{f}_{E/F_\mathfrak{p}}$ be its conductor, $\Delta_\mathfrak{p}$ a minimal discriminant, and $m_{E/F_\mathfrak{p}}$ the number of irreducible components on the special fiber. Then $\mathfrak{f}_{E/F_\mathfrak{p}} = \nu_\mathfrak{p}(\Delta_\mathfrak{p}) - m_{E/F_\mathfrak{p}} + 1$.*

Proposition 3.5. *Let $\mathfrak{p}$ be an arbitrary finite prime of F. Assume that† 3 is unramified in $F_\mathfrak{p}$ when $\mathfrak{p} \mid 3$ (we shall indicate using the symbol $\dagger$ positions at which this assumption is used). Then the elliptic curve*

$$E : y^2 + axy + by = x^3 \quad \big(a,\, b \in F_\mathfrak{p} \text{ such that } \Delta = (a^3 - 27b)b^3 \neq 0\big)$$

has a minimal Weierstrass form given by

$$\text{(w)} \qquad y^2 + a'xy + b'y = x^3 \quad \big(\Delta' := (a'^3 - 27b')b'^3 = b'^3 D'\big).$$

The reduction type is determined as follows:

(*The box indicates* $\boxed{\text{Kodaira symbol} \,\|\, [E(F_\mathfrak{p}) : E_0(F_\mathfrak{p})]}$.)

$$3\nu_\mathfrak{p}(a) \leq \nu_\mathfrak{p}(b) \to \begin{cases} 3\nu_\mathfrak{p}(a) < \nu_\mathfrak{p}(b) \to \boxed{\mathrm{I}_{3\nu_\mathfrak{p}(b')} \,\|\, 3\nu_\mathfrak{p}(b')}, \\ 3\nu_\mathfrak{p}(a) = \nu_\mathfrak{p}(b) \to \begin{cases} \nu_\mathfrak{p}(D') > 0 \to \boxed{\mathrm{I}_{\nu_\mathfrak{p}(D')} \,\|\, \begin{array}{l}\nu_\mathfrak{p}(D') \text{ if } \zeta_3 \in F_\mathfrak{p} \\ 1 \text{ or } 2 \quad \text{if } \zeta_3 \notin F_\mathfrak{p}\end{array}}, \\ \nu_\mathfrak{p}(D') = 0 \to \boxed{\mathrm{I}_0 \,\|\, 1}, \end{cases} \end{cases}$$

$$3\nu_\mathfrak{p}(a) > \nu_\mathfrak{p}(b) \to \begin{cases} \nu_\mathfrak{p}(b) \equiv 0 \pmod 3 \to \begin{cases} \mathfrak{p} \mid 3 \to \boxed{\text{Lemma 3.6}}, \\ \mathfrak{p} \nmid 3 \to \boxed{\mathrm{I}_0 \,\|\, 1}, \end{cases} \\ \nu_\mathfrak{p}(b) \equiv 1 \pmod 3 \to \boxed{\mathrm{IV} \,\|\, 3}, \\ \nu_\mathfrak{p}(b) \equiv 2 \pmod 3 \to \boxed{\mathrm{IV}^* \,\|\, 3}. \end{cases}$$

Proof. The substitution $(x, y) \mapsto (\pi^{2q}x, \pi^{3q}y)$ yields the Weierstrass form

$$y^2 + a'xy + b'y = x^3 \tag{w}$$

which is defined over $\mathfrak{O}_{F_\mathfrak{p}}$ and has the discriminant $\Delta' = \pi^{-12q}\Delta$. First assume $3\nu_\mathfrak{p}(a) = \nu_\mathfrak{p}(b)$. Then $\nu_\mathfrak{p}(\Delta') = \nu_\mathfrak{p}(D')$. If $\nu_\mathfrak{p}(D') = 0$, then the reduction type is I_0. If $\nu_\mathfrak{p}(D') > 0$, then $\pi \nmid 3$, and so $a'^3 \equiv 3^3 b' \pmod{\pi}$. Using this, we find the singular point $(\overline{-3^{-2}a'^2}, \overline{b'})$ on the reduced curve of (w). Making the substitution $(x, y) \mapsto (x - 3^{-2}a'^2, y + b')$ yields a new Weierstrass form with the usual quantities in [**6**] as follows:

$$\begin{aligned}
a_1 &= a', & b_2 &= -3^{-1}a'^2,\\
a_2 &= -3^{-1}a'^2, & b_4 &= -3^{-3}a'D',\\
a_3 &= -3^{-2}D', & b_6 &= 3^{-6}(5a'^3 - 3^3b')D',\\
a_4 &= 3^{-3}a'D', & b_8 &= -3^{-7}a'^2(2a'^3 - 3^3b')D',\\
a_6 &= -3^{-6}(a'^3 - 2\,3^3b')D', & \Delta' &= b'^3D'.
\end{aligned}$$

From this we have $\pi \mid a_3, a_4, a_6$, $\pi \nmid b_2$ and the discriminant $-3^{-1}a'^2$ of the quadratic polynomial $T^2 + a_1T - a_2$. Therefore, by using Tate's algorithm, the reduction type is either split multiplicative or nonsplit multiplicative according to whether or not the condition $\zeta_3 \in F_\mathfrak{p}$ is satisfied, respectively. If one uses Tate's algorithm starting from the Weierstrass form (w), the other cases are easily verified except for the case $3\nu_\mathfrak{p}(a) > \nu_\mathfrak{p}(b)$, $\nu_\mathfrak{p}(b) \equiv 0 \pmod 3$, $\mathfrak{p} \mid 3$. So the precise proof is omitted. We will deal with the remaining case with the following lemma. □

Lemma 3.6. *We retain the notation of Proposition* 3.5. *Assume that*[†] $\nu_\mathfrak{p}(3) = 1$. *If the condition* $3\nu_\mathfrak{p}(a) > \nu_\mathfrak{p}(b)$, $\nu_\mathfrak{p}(b) \equiv 0 \pmod 3$ *holds, then*

$$y^2 + a'xy + b'y = x^3 \quad \big(\Delta' = (a'^3 - 27b')b'^3 = b'^3D'\big) \tag{w}$$

is a minimal Weierstrass form. The reduction type is determined as follows:

(*The box indicates* $\boxed{\text{Kodaira symbol}\,\|\,[E(F_\mathfrak{p}):E_0(F_\mathfrak{p})]}$.)

$$\nu_\mathfrak{p}(D')=\begin{cases} 3 \to \begin{cases} \left(\frac{\mathcal{D}'}{\mathfrak{p}}\right)=0 \to \boxed{\text{III}\,\|\,2}, \\ \left(\frac{\mathcal{D}'}{\mathfrak{p}}\right)\neq 0 \to \boxed{\text{II}\,\|\,1}, \end{cases} \\ 4 \to \boxed{\text{II}\,\|\,1}, \\ 5 \to \boxed{\text{IV}\,\|\,\begin{array}{l}3 \text{ if } \left(\mathcal{D}/\mathfrak{p}\right)=1 \\ 1 \text{ if } \left(\mathcal{D}/\mathfrak{p}\right)\neq 1\end{array}}, \\ 6 \overset{\dagger}{\to} \boxed{\text{I}_0^*\,\|\,1 \text{ or } 2 \text{ or } 4}, \\ \nu \overset{\dagger}{\to} \boxed{\text{I}_{\nu-6}^*\,\|\,2 \text{ or } 4} \quad (\nu>6), \end{cases}$$

where

$$\mathcal{D}:=b'\frac{D'}{3^3\pi^2},$$
$$\mathcal{D}':=\frac{D'}{\pi^3}\left(\frac{a'}{\pi}k^2-\frac{3}{\pi}b'+\frac{k^3-b'}{\pi}\right)\in\mathfrak{O}_{F_\mathfrak{p}}$$

for any $k\in\mathfrak{O}_{F_\mathfrak{p}}^*$ *with* $b'\equiv k^3 \pmod{\pi}$.

Proof. We may start from the Weierstrass form

$$y^2+a'xy+b'y=x^3 \tag{w}$$

with the discriminant $\Delta'=\pi^{-12q}\Delta$ of $\mathfrak{p}$-exponent $\nu_\mathfrak{p}(D')$. From the condition we observe $\nu_\mathfrak{p}(D')\geq 3$. If $\nu_\mathfrak{p}(D')=3<12$, then the statement follows from Lemma 3.8 by using Ogg's formula and the fact that if two elliptic curves over a local field are isogenous over the ground field then those conductors coincide. Next we assume $\nu_\mathfrak{p}(D')>3$. Note that either of the cases $\nu_\mathfrak{p}(D')=4$ or 5 automatically implies $\nu_\mathfrak{p}(3)=1$; hence, we properly use the assumption $\nu_\mathfrak{p}(3)=1$ only for the case $\nu_\mathfrak{p}(D')>5$. For these cases we have the equivalence $3^{-3}a'^3\equiv b' \pmod{\pi}$, which yields the singular point $(\overline{-3^{-2}a'^2},\,\overline{b'})$ on the reduced curve of (w). Making the substitution $(x,\,y)\mapsto(x-3^{-2}a'^2,\,y+b')$ yields a new Weierstrass form with the same usual quantities as in the proof of Proposition 3.5. Since $\nu_\mathfrak{p}(D')>3$, we have further that $\pi\mid a_3,\,a_4,\,a_6,\,b_2$. The statement of the lemma is

then easily verified by using Tate's algorithm. However, note that in the case $\nu_{\mathfrak{p}}(D') = 5$ the discriminant of $T^2 + \pi^{-1}a_3T - \pi^{-2}a_6$ is equivalent to $b'(D'/3^3\pi^2)$ modulo π. This algorithm will terminate with equation (w); consequently, it is minimal. □

Proposition 3.7. *Let $\mathfrak{p}$ be an arbitrary finite prime of F. Assume that*† *3 is unramified in $F_{\mathfrak{p}}$ when $\mathfrak{p} \mid 3$. Then the elliptic curve*

$$\widehat{E} : y^2 + axy - 9by = x^3 - (a^3 + 27b)b$$
$$\big(a,\, b \in F_{\mathfrak{p}} \text{ such that } \widehat{\Delta} = (a^3 - 27b)^3 b \neq 0\big)$$

has a minimal Weierstrass form given by one of the following forms

$$(\widehat{\mathrm{w}}) \qquad y^2 + a'xy - 9b'y = x^3 - (a'^3 + 27b')b'$$
$$\big(\widehat{\Delta}' := (a'^3 - 27b')^3 b' = b'D'^3\big),$$

$$(\widehat{\mathrm{w}}') \quad y^2 + \frac{a'}{\pi}xy - \frac{9}{\pi^3}(3b' + a'k_\pi^2)y$$
$$= x^3 - \frac{9}{\pi^2}k_\pi^2 x^2 + \frac{3}{\pi^4}(3a'b' + a'^2k_\pi^2 + 9k_\pi^4)x$$
$$- \frac{1}{\pi^6}(a'^3b' + 7\,3^3b'^2 + 2^2 3^3 a'b'k_\pi^2 + 2\,3^2 a'^2 k_\pi^4 + 3^3 k_\pi^6)$$
$$\big(\widehat{\Delta}'' := \pi^{-12}(a'^3 - 27b')^3 b' = \pi^{-12}b'D'^3\big).$$

Here all the coefficients lie in $\mathfrak{O}_{F_{\mathfrak{p}}}$ while k_π denotes any integer in $\mathfrak{O}_F$ satisfying $k_\pi \equiv a'/3 \pmod{\pi}$. The reduction type is determined as follows: (*The box indicates*

minimal Weierstrass form	Kodaira symbol	$[\widehat{E}(F_{\mathfrak{p}}) : \widehat{E}_0(F_{\mathfrak{p}})]$

.)

$3\nu_{\mathfrak{p}}(a) \le \nu_{\mathfrak{p}}(b)$

$\to$ { $3\nu_{\mathfrak{p}}(a) < \nu_{\mathfrak{p}}(b) \to$ | $(\widehat{\mathrm{w}})$ | $\mathrm{I}_{\nu_{\mathfrak{p}}(b')}$ | $\nu_{\mathfrak{p}}(b')$ |,

$3\nu_{\mathfrak{p}}(a) = \nu_{\mathfrak{p}}(b)$

$\to$ { $\nu_{\mathfrak{p}}(D') > 0 \to$ | $(\widehat{\mathrm{w}})$ | $\mathrm{I}_{3\nu_{\mathfrak{p}}(D')}$ | $3\nu_{\mathfrak{p}}(D')$ if $\zeta_3 \in F_{\mathfrak{p}}$ / 1 or 2 if $\zeta_3 \notin F_{\mathfrak{p}}$ |,

$\nu_{\mathfrak{p}}(D') = 0 \to$ | $(\widehat{\mathrm{w}})$ | I_0 | 1 |,

$3\nu_{\mathfrak{p}}(a) > \nu_{\mathfrak{p}}(b)$

$$\longrightarrow \begin{cases} \nu_{\mathfrak{p}}(b) \equiv 0 \,(\mathrm{mod}\ 3) \to \begin{cases} \mathfrak{p} \mid 3 \to \boxed{\text{Lemma 3.8}}, \\ \mathfrak{p} \nmid 3 \to \boxed{(\widehat{\mathrm{w}})}\boxed{\mathrm{I}_0}\boxed{1}, \end{cases} \\ \nu_{\mathfrak{p}}(b) \equiv 1 \,(\mathrm{mod}\ 3) \\ \quad \to \begin{cases} \mathfrak{p} \mid 3 \to \begin{cases} \nu_{\mathfrak{p}}(a') = 1 \to \boxed{(\widehat{\mathrm{w}})}\boxed{\mathrm{IV}^*}\boxed{2 + (-a'b'^{-1}/\mathfrak{p})}, \\ \nu_{\mathfrak{p}}(a') \geq 2 \overset{\dagger}{\to} \boxed{(\widehat{\mathrm{w}})}\boxed{\mathrm{II}^*}\boxed{1}, \end{cases} \\ \mathfrak{p} \nmid 3 \to \boxed{(\widehat{\mathrm{w}})}\boxed{\mathrm{IV}}\boxed{\begin{array}{l} 3 \text{ if } \zeta_3 \in F_{\mathfrak{p}} \\ 1 \text{ if } \zeta_3 \notin F_{\mathfrak{p}} \end{array}}, \end{cases} \\ \nu_{\mathfrak{p}}(b) \equiv 2 \,(\mathrm{mod}\ 3) \\ \quad \to \begin{cases} \mathfrak{p} \mid 3 \to \begin{cases} \nu_{\mathfrak{p}}(a') = 1 \to \boxed{(\widehat{\mathrm{w}})}\boxed{\mathrm{II}^*}\boxed{1}, \\ \nu_{\mathfrak{p}}(a') \geq 2 \overset{\dagger}{\to} \boxed{(\widehat{\mathrm{w}}')}\boxed{\mathrm{II}}\boxed{1}, \end{cases} \\ \mathfrak{p} \nmid 3 \to \boxed{(\widehat{\mathrm{w}})}\boxed{\mathrm{IV}^*}\boxed{\begin{array}{l} 3 \text{ if } \zeta_3 \in F_{\mathfrak{p}} \\ 1 \text{ if } \zeta_3 \notin F_{\mathfrak{p}} \end{array}}. \end{cases} \end{cases}$$

Proof. The substitution $(x, y) \mapsto (\pi^{2q}x, \pi^{3q}y)$ yields the Weierstrass form

$$(\widehat{\mathrm{w}}) \qquad y^2 + a'xy - 9b'y = x^3 - (a'^3 + 27b')b',$$

which is defined over $\mathfrak{O}_{F_{\mathfrak{p}}}$ and has the discriminant $\widehat{\Delta}' = \pi^{-12q}\widehat{\Delta}$. First assume $3\nu_{\mathfrak{p}}(a) = \nu_{\mathfrak{p}}(b)$. Then $\nu_{\mathfrak{p}}(\Delta') = 3\nu_{\mathfrak{p}}(D')$. If $\nu_{\mathfrak{p}}(D') = 0$, then the reduction type is I_0. If $\nu_{\mathfrak{p}}(D') > 0$, then $\pi \nmid 3$, and so we have the equivalence $a'^3 \equiv 3^3 b' \pmod{\pi}$. With this equivalence, we find the singular point $(\overline{-3^{-1}a'^2}, \overline{3^2 b'})$ on the reduced curve of $(\widehat{\mathrm{w}})$. Making the substitution $(x, y) \mapsto (x - 3^{-1}a'^2, y + 3^2 b')$ yields a new Weierstrass

form with the usual quantities in [**6**] as follows:

$$\begin{aligned} a_1 &= a', & b_2 &= -3a'^2, \\ a_2 &= -a'^2, & b_4 &= 3^{-1}a'D', \\ a_3 &= -3^{-1}D', & b_6 &= -3^{-3}D'^2, \\ a_4 &= 3^{-1}a'D', & b_8 &= 0, \\ a_6 &= -3^{-3}D'^2, & \widehat{\Delta}' &= b'D'^3. \end{aligned}$$

From these we have $\pi \mid a_3,\ a_4,\ a_6,\ \pi \nmid b_2$ and the discriminant $-3a'^2$ of the quadratic polynomial $T^2 + a_1T - a_2$. Therefore, by applying Tate's algorithm, the reduction type is either split multiplicative or nonsplit multiplicative according to whether or not the condition $\zeta_3 \in F_\mathfrak{p}$ is satisfied, respectively. Starting from either of the Weierstrass forms $(\widehat{\mathrm{w}})$ or $(\widehat{\mathrm{w}}')$ given in the proposition, the other cases are easily verified except for the case $3\nu_\mathfrak{p}(a) > \nu_\mathfrak{p}(b),\ \nu_\mathfrak{p}(b) \equiv 0 \pmod 3,\ \mathfrak{p} \mid 3$. Note that the substitution $(x,\ y) \mapsto (\pi^2 x - 3k_\pi^2,\ \pi^3 y - 3(3b' + a'k_\pi^2))$ yields a transformation from $(\widehat{\mathrm{w}})$ to $(\widehat{\mathrm{w}}')$. We will deal with the remaining case with Lemma 3.8. □

Lemma 3.8. *We retain the notation of Proposition* 3.7. *Assume that*† $\nu_\mathfrak{p}(3) = 1$. *If the condition* $3\nu_\mathfrak{p}(a) > \nu_\mathfrak{p}(b),\ \nu_\mathfrak{p}(b) \equiv 0 \pmod 3$ *holds, then the reduction type is determined as follows*: (*The box indicates*

minimal Weierstrass form	Kodaira symbol	$[\widehat{E}(F_\mathfrak{p}) : \widehat{E}_0(F_\mathfrak{p})]$

.)

$$\nu_\mathfrak{p}(D') = \begin{cases} 3 \to \begin{cases} \left(\frac{\mathcal{D}'}{\mathfrak{p}}\right) = 0 \to \boxed{(\widehat{\mathrm{w}})}\boxed{\mathrm{III}^*}\boxed{2}, \\ \left(\frac{\mathcal{D}'}{\mathfrak{p}}\right) \neq 0 \to \boxed{(\widehat{\mathrm{w}})}\boxed{\mathrm{IV}^*}\begin{array}{|c|}\hline 3 \text{ if } \left(\mathcal{D}'/\mathfrak{p}\right) = 1 \\ \hline 1 \text{ if } \left(\mathcal{D}'/\mathfrak{p}\right) = -1 \\ \hline \end{array}, \end{cases} \\ 4 \to \boxed{(\widehat{\mathrm{w}})}\boxed{\mathrm{II}^*}\boxed{1}, \\ 5 \to \boxed{(\widehat{\mathrm{w}}')}\boxed{\mathrm{II}}\boxed{1}, \\ 6 \overset{\dagger}{\to} \boxed{(\widehat{\mathrm{w}}')}\boxed{\mathrm{I}_0^*}\boxed{1 \text{ or } 2 \text{ or } 4}, \\ \nu \overset{\dagger}{\to} \boxed{(\widehat{\mathrm{w}}')}\boxed{\mathrm{III}^*}\boxed{2} \text{ or } \boxed{(\widehat{\mathrm{w}}')}\boxed{\mathrm{I}_{3(\nu-6)}^*}\boxed{2 \text{ or } 4} \quad (\nu > 6), \end{cases}$$

where

$$\mathcal{D}' := \frac{D'}{\pi^3}\left(\frac{a'}{\pi}k^2 - \frac{3}{\pi}b' + \frac{k^3 - b'}{\pi}\right) \in \mathfrak{O}_{F_\mathfrak{p}}$$

for any $k \in \mathfrak{O}_{F_\mathfrak{p}}^*$ with $b' \equiv k^3 \pmod{\pi}$.

Proof. We may start from the Weierstrass form

$$(\widehat{\mathrm{w}}) \qquad y^2 + a'xy - 9b'y = x^3 - (a'^3 + 27b')b'$$

with the usual quantities

$$\begin{aligned} a_1 &= a', & b_2 &= a'^2, \\ a_2 &= 0, & b_4 &= -3^2 a'b', \\ a_3 &= -3^2 b', & b_6 &= -b'(4a'^3 + 3^3 b'), \\ a_4 &= 0, & b_8 &= -a'^2 b'(a'^3 + 3^3 b'), \\ a_6 &= -b'(a'^3 + 3^3 b'), & \widehat{\Delta}' &= b'D'^3. \end{aligned}$$

From the condition we observe $\nu_\mathfrak{p}(D') \geq 3$. Assume $\nu_\mathfrak{p}(D') = 3$. Since $\pi \mid 3$, the cubic equation

$$T^3 + \pi^{-1}a_2 T^2 + \pi^{-2}a_4 T + \pi^{-3}a_6 \equiv 0 \pmod{\pi}$$

has a triple root $\pi^{-1}k(a' + 3k)$ modulo π, where k denotes an element in $\mathfrak{O}_{F_\mathfrak{p}}^*$ satisfying $b' \equiv k^3 \pmod{\pi}$. Note that such a k certainly exists by $\pi \mid 3$. It thus follows from Tate's algorithm that the possible reduction types are II*, III*, IV*, because equation $(\widehat{\mathrm{w}})$ is minimal by $\nu_\mathfrak{p}(\widehat{\Delta}') = 9 < 12$. However the case II* is impossible by Ogg's formula along with the fact that the $\mathfrak{p}$-exponent of a conductor is greater than or equal to 2 if and only if the reduction type is additive. We determine whether the reduction type is III* or IV*. Making the substitution $(x, y) \mapsto (x + k(a' + 3k), y)$ yields

$$\begin{aligned} a_3 &= a'k(a' + 3k) - 9b', \\ a_6 &= a'^3(k^3 - b') + 9a'^2k^4 + 27a'k^5 + 27(k^6 - b'^2), \end{aligned}$$

which are the usual quantities of the new Weierstrass form. Thus, the discriminant of $Y^2 + \pi^{-2}a_3 Y - \pi^{-4}a_6$ is equivalent to

$$\frac{D'}{\pi^3}\left(\frac{a'}{\pi}k^2 - \frac{3}{\pi}b' + \frac{k^3 - b'}{\pi}\right)$$

modulo π. The reduction type follows from this. Secondly, assume $\nu_{\mathfrak{p}}(D') = 4$, which automatically implies $\nu_{\mathfrak{p}}(3) = 1$. Then the elliptic curve $E/F_{\mathfrak{p}}$ has reduction type II from Lemma 3.6. Therefore, $\widehat{E}/F_{\mathfrak{p}}$ must also have a bad reduction. But the equality $\nu_{\mathfrak{p}}(\widehat{\Delta}') = 12$ implies that equation $(\widehat{\mathrm{w}})$ is minimal. Thus, Ogg's formula and Tate's algorithm tell us that $\widehat{E}/F_{\mathfrak{p}}$ has reduction type II*. Finally, assume $\nu_{\mathfrak{p}}(D') \geq 5$. Here the case $\nu_{\mathfrak{p}}(D') = 5$ automatically implies $\nu_{\mathfrak{p}}(3) = 1$; hence, we properly use the assumption $\nu_{\mathfrak{p}}(3) = 1$ only for the case $\nu_{\mathfrak{p}}(D') > 5$. Then $\nu_{\mathfrak{p}}(a') = \nu_{\mathfrak{p}}(3) = 1$ and $3^{-3}a'^3 \equiv b' \pmod{\pi^2}$. Let k_π be an integer in $\mathfrak{O}_F$ satisfying $k_\pi \equiv a'/3 \pmod{\pi}$. Making the substitution $(x, y) \mapsto \left(\pi^2 x - 3k_\pi^2,\ \pi^3 y - 3(3b' + a'k_\pi^2)\right)$ yields the Weierstrass form $(\widehat{\mathrm{w}}')$ with the usual quantities

$$
\begin{aligned}
a_1 &= \frac{a'}{\pi},\\
a_2 &= -\frac{3^2}{\pi^2}k_\pi^2,\\
a_3 &= -\frac{3^2}{\pi^3}(3b' + a'k_\pi^2),\\
a_4 &= \frac{3}{\pi^4}(3a'b' + a'^2k_\pi^2 + 9k_\pi^4),\\
a_6 &= -\frac{1}{\pi^6}(a'^3b' + 7\,3^3b'^2 + 2^2 3^3 a'b'k_\pi^2 + 2\,3^2 a'^2 k_\pi^4 + 3^3 k_\pi^6),\\
\widehat{\Delta}'' &= \pi^{-12}b'D'^3 \quad (= \pi^{-12}\widehat{\Delta}').
\end{aligned}
$$

It is straightforward to see that a_1, a_2, $a_3 \in \mathfrak{O}_{F_{\mathfrak{p}}}$, and a_4, $a_6 \in \mathfrak{O}_{F_{\mathfrak{p}}}$ by the equalities

$$
\begin{aligned}
a_4 &= \left(\frac{3}{\pi}\right)^3\left(-\frac{a'D'}{3^4\pi} + \left(\frac{a'}{3}\right)^2\frac{k_\pi^2 - (a'/3)^2}{\pi} + \frac{k_\pi^4 - (a'/3)^4}{\pi} + \frac{a'^4}{3^3\pi}\right),\\
a_6 &= \frac{D'}{\pi^5}\left(\frac{a'^3}{\pi} + 4\frac{a'}{\pi}\left(k_\pi^2 - \left(\frac{a'}{3}\right)^2\right) - 7\frac{D'}{3^3\pi}\right) - \left(\frac{3}{\pi}\right)^3\frac{k_\pi^2 - (a'/3)^2}{\pi}\\
&\quad \times\left(\left(\frac{k_\pi^2 - (a'/3)^2}{\pi}\right)^2 + \left(\frac{a'}{\pi}\right)^2 k_\pi^2 + 2\frac{a'^4}{3^2\pi^2}\right) - \left(\frac{a'}{\pi}\right)^6.
\end{aligned}
$$

Therefore, equation $(\widehat{\mathrm{w}}')$ is defined over $\mathfrak{O}_{F_{\mathfrak{p}}}$. If $\nu_{\mathfrak{p}}(D') > 5$, then the usual quantity $c_4 = a'D'/\pi^4 + (3^5/\pi^4)a'b'$ is of $\mathfrak{p}$-exponent 2, which is less than 4; that is, equation $(\widehat{\mathrm{w}}')$ is minimal. If $\nu_{\mathfrak{p}}(D') = 5$, then

$\nu_{\mathfrak{p}}(\widehat{\Delta}'') = 3 < 12$. Thus, equation $(\widehat{\mathrm{w}}')$ is minimal. The reduction types for the case $\nu_{\mathfrak{p}}(D') \geq 5$ now follow from Ogg's formula and Lemma 3.6. □

Remark 3.9. As we have seen in relations (3.3), if $E/F_{\mathfrak{p}}$ has the minimal Weierstrass form (w) and $\widehat{E}/F_{\mathfrak{p}}$ has the minimal Weierstrass form $(\widehat{\mathrm{w}})$, then the invariant differentials satisfy

$$\phi^*\widehat{\omega} = \omega, \qquad \widehat{\phi}^*\omega = 3\widehat{\omega}.$$

Here, the isogeny ϕ is defined from (w) to $(\widehat{\mathrm{w}})$. If $\widehat{E}/F_{\mathfrak{p}}$ has the minimal Weierstrass form $(\widehat{\mathrm{w}}')$, then the 3-isogeny $\Phi : (\mathrm{w}) \overset{\phi}{\to} (\widehat{\mathrm{w}}) \overset{\sim}{\to} (\widehat{\mathrm{w}}')$ between minimal Weierstrass forms satisfies

$$\Phi^*\widehat{\omega}' = \pi\omega, \qquad \widehat{\Phi}^*\omega = \frac{3}{\pi}\widehat{\omega}',$$

where $\widehat{\Phi}$ is the dual of Φ, and $\widehat{\omega}'$ is the differential associated with $(\widehat{\mathrm{w}}')$. This is a consequence of the transformation of the usual quantities of a Weierstrass form due to the change of coordinates. In the above case, $\widehat{\omega}' = \pi\widehat{\omega}$. More precise details may be found in [**6**].

Remark 3.10. Assume that F has class number 1, and 3 is unramified in F. Then we can find a global minimal Weierstrass form as follows. For the elliptic curve E/F (3.1), it is easily seen from Proposition 3.5 and Lemma 3.6 that one can take a global minimal Weierstrass form as

$$(\mathrm{w}_{\mathrm{gl}}) \qquad y^2 + a'xy + b'y = x^3 \quad \Big(\Delta_{\mathrm{gl}} := \Delta \prod_{\pi} \pi^{-12q_\pi}\Big),$$

where $a' = a\prod_\pi \pi^{-q_\pi}$, $b' = b\prod_\pi \pi^{-3q_\pi}$. Here q_π is the integer "q" defined by (3.6), which is determined exactly by a, b and π.

As for the dual elliptic curve $\widehat{E}/F$ (3.2), we first make a substitution to get the form $y^2 + a'xy - 9b'y = x^3 - (a'^3 + 27b')b'$ where a', b' are as described above. Next, let Ξ be the finite set of all distinct prime elements π in F above 3 at which the elliptic curve $\widehat{E}$ has the minimal Weierstrass form $(\widehat{\mathrm{w}}')$ over F_π. If $\Xi = \varnothing$, then the above form of $\widehat{E}/F$ is

already minimal. Assume that $\Xi \neq \varnothing$. For each $\pi \in \Xi$, there are some ε_π, $k_\pi \in \mathfrak{O}_F$ satisfying $(3/\pi)\varepsilon_\pi \equiv 1 \pmod{\pi}$, $k_\pi \equiv a'/3 \pmod{\pi}$. Let $\varpi := \prod_{\pi\in\Xi} \pi$ and $k_\varpi := \sum_{\pi\in\Xi}(3/\pi)\varepsilon_\pi k_\pi \in \mathfrak{O}_F$. Then for each $\pi \in \Xi$, the integer k_ϖ satisfies the condition $k_\varpi \equiv a'/3 \pmod{\pi}$ and the integer ϖ is a prime element in F_π. Thus, making the substitution $(x, y) \mapsto (\varpi^2 x - 3k_\varpi^2, \varpi^3 y - 3(3b' + a'k_\varpi^2))$ yields the global Weierstrass form

$$
\begin{aligned}
(\widehat{\mathrm{w}}_{\mathrm{gl}}) \quad & y^2 + \frac{a'}{\varpi}xy - \frac{9}{\varpi^3}(3b' + a'k_\varpi^2)y \\
& = x^3 - \frac{9}{\varpi^2}k_\varpi^2 x^2 + \frac{3}{\varpi^4}(3a'b' + a'^2k_\varpi^2 + 9k_\varpi^4)x \\
& \quad - \frac{1}{\varpi^6}(a'^3b' + 7\,3^3b'^2 + 2^2 3^3 a'b'k_\varpi^2 + 2\,3^2 a'^2 k_\varpi^4 + 3^3 k_\varpi^6) \\
& \qquad\qquad \Big(\widehat{\Delta}_{\mathrm{gl}} := \widehat{\Delta}\ \varpi^{-12}\prod_\pi \pi^{-12q_\pi}\Big),
\end{aligned}
$$

which has coefficients in $\mathfrak{O}_F$ and is minimal by Proposition 3.7 and Lemma 3.8.

With these observations, we have in particular that

$$
\frac{\Phi^*\widehat{\omega}_{\min}}{\omega_{\min}} = \varpi, \qquad \frac{\widehat{\Phi}^*\omega_{\min}}{\widehat{\omega}_{\min}} = \frac{3}{\varpi}, \tag{3.7}
$$

where $\Phi : (\widehat{\mathrm{w}}_{\mathrm{gl}}) \xrightarrow{\sim} (3.1) \xrightarrow{\phi} (3.2) \xrightarrow{\sim} (\widehat{\mathrm{w}}_{\mathrm{gl}})$ is a refined 3-isogeny for ϕ, and $\widehat{\Phi}$ its dual isogeny. This follows from relations (3.3) and the relation $\omega_{\min}/\omega = \prod_\pi \pi^{q_\pi}$, $\widehat{\omega}_{\min}/\widehat{\omega} = \varpi\prod_\pi \pi^{q_\pi}$. (See [**6**].)

4. The image of the local connecting homomorphism $\widehat{\delta}_{F_\mathfrak{p}}$. We retain the notation of the previous section. We are now ready to determine the image of local connecting homomorphisms.

Theorem 4.1. *Let $\mathfrak{p}$ be an arbitrary finite prime of F. Assume that*[†] *3 is unramified in $F_\mathfrak{p}$ when $\mathfrak{p} \mid 3$. The image of $\widehat{\delta}_{F_\mathfrak{p}}$ under mapping* (3.4) *and the ratio of the numbers of irreducible components of Néron models for $E/F_\mathfrak{p}$ and $\widehat{E}/F_\mathfrak{p}$ are determined as follows*:

$\Big($*The box indicates* $\boxed{\mathrm{Im}\,\widehat{\delta}_{F_\mathfrak{p}} \,\Big\|\, \dfrac{[\widehat{E}(F_\mathfrak{p}) : \widehat{E}_0(F_\mathfrak{p})]}{[E(F_\mathfrak{p}) : E_0(F_\mathfrak{p})]}}$.$\Big)$

$3\nu_\mathfrak{p}(a) \le \nu_\mathfrak{p}(b)$

$$\longrightarrow \begin{cases} 3\nu_\mathfrak{p}(a) < \nu_\mathfrak{p}(b) \to \boxed{F_\mathfrak{p}^*/F_\mathfrak{p}^{*3} \,\|\, 1/3}, \\ 3\nu_\mathfrak{p}(a) = \nu_\mathfrak{p}(b) \\ \quad \to \begin{cases} \nu_\mathfrak{p}(D') > 0 \to \boxed{\{e\} \,\Big\|\, \dfrac{3 \text{ if } \zeta_3 \in F_\mathfrak{p}}{1 \text{ if } \zeta_3 \notin F_\mathfrak{p}}}, \\ \nu_\mathfrak{p}(D') = 0 \to \boxed{\mathfrak{O}_{F_\mathfrak{p}}^*/\mathfrak{O}_{F_\mathfrak{p}}^{*3} \,\|\, 1} \text{ (good reduction)}, \end{cases} \end{cases}$$

$3\nu_\mathfrak{p}(a) > \nu_\mathfrak{p}(b)$

$$\longrightarrow \begin{cases} \nu_\mathfrak{p}(b) \equiv 0(3) \to \begin{cases} \mathfrak{p} \mid 3 \to \begin{cases} \nu_\mathfrak{p}(D') = 3 \to \boxed{\text{Lemma 4.2}}, \\ \nu_\mathfrak{p}(D') = 4 \to \boxed{\mathfrak{O}_{F_\mathfrak{p}}^*/\mathfrak{O}_{F_\mathfrak{p}}^{*3} \,\|\, 1}, \\ \nu_\mathfrak{p}(D') = 5 \to \boxed{\text{Lemma 4.3}}, \\ \nu_\mathfrak{p}(D') > 5 \overset{\dagger}{\to} \boxed{\{e\} \,\|\, 1}, \end{cases} \\ \mathfrak{p} \nmid 3 \to \boxed{\mathfrak{O}_{F_\mathfrak{p}}^*/\mathfrak{O}_{F_\mathfrak{p}}^{*3} \,\|\, 1} \text{ (good reduction)}, \end{cases} \\ \nu_\mathfrak{p}(b) \equiv 1(3) \to \begin{cases} \mathfrak{p} \mid 3 \to \begin{cases} \nu_\mathfrak{p}(a') = 1 \to \boxed{\text{Lemma 4.4}}, \\ \nu_\mathfrak{p}(a') \ge 2 \overset{\dagger}{\to} \boxed{F_\mathfrak{p}^*/{F_\mathfrak{p}}^{*3} \,\|\, 1/3}, \end{cases} \\ \mathfrak{p} \nmid 3 \to \boxed{\langle bF_\mathfrak{p}^{*3}\rangle \,\Big\|\, \dfrac{1 \quad \text{if } \zeta_3 \in F_\mathfrak{p}}{1/3 \text{ if } \zeta_3 \notin F_\mathfrak{p}}}, \end{cases} \\ \nu_\mathfrak{p}(b) \equiv 2(3) \to \begin{cases} \mathfrak{p} \mid 3 \to \begin{cases} \nu_\mathfrak{p}(a') = 1 \to \boxed{F_\mathfrak{p}^*/{F_\mathfrak{p}}^{*3} \,\|\, 1/3}, \\ \nu_\mathfrak{p}(a') \ge 2 \overset{\dagger}{\to} \boxed{\langle bF_\mathfrak{p}^{*3}\rangle \,\|\, 1/3}, \end{cases} \\ \mathfrak{p} \nmid 3 \to \boxed{\langle bF_\mathfrak{p}^{*3}\rangle \,\Big\|\, \dfrac{1 \quad \text{if } \zeta_3 \in F_\mathfrak{p}}{1/3 \text{ if } \zeta_3 \notin F_\mathfrak{p}}}. \end{cases} \end{cases}$$

Proof. All the materials we need have been prepared in Section 3. In particular, the proof can be easily verified by applying formula (2.3) along with Propositions 3.5, 3.7, Lemmas 3.1, 3.2, 3.6, 3.8, Remark 3.9 and invariants (3.3) depending on the isogenies ϕ, $\widehat{\phi}$. □

Lemma 4.2. *Assume that* $3\nu_{\mathfrak{p}}(a) > \nu_{\mathfrak{p}}(b)$, $\nu_{\mathfrak{p}}(b) \equiv 0 \pmod 3$, $\mathfrak{p} \mid 3$, $\nu_{\mathfrak{p}}(D') = 3$, *and assume that*† 3 *is unramified in* $F_{\mathfrak{p}}$. *Let* k *be an integer satisfying* $b' \equiv k^3 \pmod{\pi}$ (*such an integer always exists since* $\mathfrak{p} \mid 3$), *and let*

$$R := \left\{ r \in \{ a \text{ complete representative system for } \mathbf{F}_{\mathfrak{p}} \} \mid r \not\equiv k \pmod{\pi} \right\}.$$

Then $\left| \operatorname{Im} \widehat{\delta}_{F_{\mathfrak{p}}} \right| \left| \dfrac{[\widehat{E}(F_{\mathfrak{p}}) : \widehat{E}_0(F_{\mathfrak{p}})]}{[E(F_{\mathfrak{p}}) : E_0(F_{\mathfrak{p}})]} \right|$ *are*

$$\begin{cases} \left| \left\langle b' F_{\mathfrak{p}}^{*3}, \left\{ 1 + \dfrac{\pi}{(k-r)^3} \left(r(r+k) \left(\dfrac{a'}{\pi} - \dfrac{3}{\pi} k \right) + \dfrac{b' - k^3}{\pi} \right) \right\} F_{\mathfrak{p}}^{*3} \,\middle|\, r \in R \right\rangle \right| \left| 3 \right|^{\dagger}, \\ \qquad \text{if } \left(\dfrac{\mathcal{D}'}{\mathfrak{p}} \right) = 1, \\ \left| \mathfrak{O}_{F_{\mathfrak{p}}}^{*} / \mathfrak{O}_{F_{\mathfrak{p}}}^{*3} \right| \left| 1 \right| \qquad \text{otherwise.} \end{cases}$$

Furthermore, if $(\mathcal{D}'/\mathfrak{p}) = 1$, *then the group* $\operatorname{Im} \widehat{\delta}_{F_{\mathfrak{p}}}$ *is of order* $\sharp \mathbf{F}_{\mathfrak{p}}/3$. *In particular, for the case* $F = \mathbf{Q}$, *we have* $\operatorname{Im} \widehat{\delta}_{\mathbf{Q}_3} = \{e\}$ *or* $\mathbf{Z}_3^*/\mathbf{Z}_3^{*3}$ *according to whether or not* $(\mathcal{D}'/\mathfrak{p}) = 1$, *respectively.*

Proof. Under the assumption, in the case $(\mathcal{D}'/\mathfrak{p}) \neq 1$, the statement follows from formula (2.3) with the results of Section 3. Consider the case $(\mathcal{D}'/\mathfrak{p}) = 1$. Let (x, y) be an $F_{\mathfrak{p}}$-rational point satisfying the minimal Weierstrass form (w). Under the assumption, since $\widehat{\delta}_{F_{\mathfrak{p}}}(E_1(F_{\mathfrak{p}}))$ is trivial by Lemma 3.3, it suffices to consider the case $\nu_{\mathfrak{p}}(x) \geq 0$. When $\nu_{\mathfrak{p}}(x) > 0$, we have either $\nu_{\mathfrak{p}}(y + a'x + b') > 0$ or $\nu_{\mathfrak{p}}(y) > 0$ from equation (w). In the former case, the point (x, y) is of the form $(\pi r, -b' + \pi s)$ for some $r, s \in \mathfrak{O}_{F_{\mathfrak{p}}}$. Substituting for (x, y) in this form into equation (w) modulo π^2 yields $\pi \mid s$, and hence $\widehat{\delta}_{F_{\mathfrak{p}}}(x, y) = b' F_{\mathfrak{p}}^{*3}$ upon using $U_{\mathfrak{p}}^{(2)} \subset F_{\mathfrak{p}}^{*3}$, which follows from $\nu_{\mathfrak{p}}(3) = 1$. Consider the

latter case. Let $m := \nu_{\mathfrak{p}}(x)$. Then $(x, y) = (\pi^m r, \pi^{3m} s)$ for some $r, s \in \mathfrak{O}_{F_{\mathfrak{p}}}^*$ since $m > 0$ and $\nu_{\mathfrak{p}}(y + a'x + b') = 0$. Substituting for (x, y) in this form into equation (w) modulo π^{4m+1} yields $\pi^{3m} b' s \equiv \pi^{3m} r^3 \pmod{\pi^{4m+1}}$, and hence $\widehat{\delta}_{F_{\mathfrak{p}}}(x, y) = b'^2 F_{\mathfrak{p}}^{*3}$. Secondly, we assume $\nu_{\mathfrak{p}}(x) = 0$. Then $\nu_{\mathfrak{p}}(y) = 0$ from equation (w). In this case, since every integer in $\mathfrak{O}_{F_{\mathfrak{p}}}$ is a cubic residue modulo $\mathfrak{p}$, the point (x, y) must be written as $(r(r+k) + \pi s, r^3 + \pi t)$ for some $r, s, t \in \mathfrak{O}_{F_{\mathfrak{p}}}$. Substituting for (x, y) in this form into equation (w) modulo π^2 yields

$$\pi t(b' + 2r^3) + (a' - 3k)r^4(r + k) + r^3(b' - k^3) \equiv 0 \pmod{\pi^2}.$$

Upon using $\nu_{\mathfrak{p}}(a' - 3k) = 1$ from the assumption $\nu_{\mathfrak{p}}(D') = 3$, we have

$$t \equiv \left(\frac{r}{k - r}\right)^3 \left(\left(\frac{a'}{\pi} - \frac{3}{\pi}k\right) r(r + k) + \frac{b' - k^3}{\pi}\right) \pmod{\pi}.$$

Since any smooth point on the reduced curve can be lifted to an $F_{\mathfrak{p}}$-rational point, the form of the image of $\widehat{\delta}_{F_{\mathfrak{p}}}$ given in the statement of the present lemma now follows from Lemma 3.6, which states $E(F_{\mathfrak{p}}) = E_0(F_{\mathfrak{p}})$. □

Lemma 4.3. *Assume that* $3\nu_{\mathfrak{p}}(a) > \nu_{\mathfrak{p}}(b)$, $\nu_{\mathfrak{p}}(b) \equiv 0 \pmod 3$, $\mathfrak{p} \mid 3$, $\nu_{\mathfrak{p}}(D') = 5$. *Then* $\begin{array}{|c||c|}\hline \mathrm{Im}\,\widehat{\delta}_{F_{\mathfrak{p}}} & [\widehat{E}(F_{\mathfrak{p}}) : \widehat{E}_0(F_{\mathfrak{p}})] \\ \hline & [E(F_{\mathfrak{p}}) : E_0(F_{\mathfrak{p}})] \\ \hline \end{array}$ *are*

$$\begin{cases} \begin{array}{|c||c|}\hline \langle (1 + \pi r) F_{\mathfrak{p}}^{*3} \rangle & 1/3 \\ \hline \end{array} & \text{if } {}^{\exists} r \in \mathfrak{O}_{F_{\mathfrak{p}}}^* \text{ s.t. } r^2 \equiv b'^{-1}(D'/3^3\pi^2) \pmod{\pi}, \\ \begin{array}{|c||c|}\hline \{e\} & 1 \\ \hline \end{array} & \text{otherwise.} \end{cases}$$

In particular, for the case $F = \mathbf{Q}$, *we have* $\mathrm{Im}\,\widehat{\delta}_{\mathbf{Q}_3} = \mathbf{Z}_3^*/\mathbf{Z}_3^{*3}$ *or* $\{e\}$ *according to whether or not* $b' \equiv 3^{-5} D' \pmod 3$, *respectively.*

Proof. The condition $\nu_{\mathfrak{p}}(D') = 5$ automatically implies $\nu_{\mathfrak{p}}(a') = \nu_{\mathfrak{p}}(3) = 1$, and in particular $b' \equiv 3^{-3} a'^3 \pmod{\pi^2}$. By applying the results in Section 3 to formula (2.3), we observe $\sharp \mathrm{Im}\,\widehat{\delta}_{F_{\mathfrak{p}}} = [E(F_{\mathfrak{p}}) : E_0(F_{\mathfrak{p}})]$. If there is no element $r \in \mathfrak{O}_{F_{\mathfrak{p}}}^*$ such that $r^2 \equiv b'^{-1}(D'/3^3\pi^2) \pmod{\pi}$, then $[E(F_{\mathfrak{p}}) : E_0(F_{\mathfrak{p}})] = 1$ by Lemma 3.6; that is, $\mathrm{Im}\,\widehat{\delta}_{F_{\mathfrak{p}}}$

is trivial. Assume that there is such an $r \in \mathfrak{O}_{F_\mathfrak{p}}^*$. Then $[E(F_\mathfrak{p}) : E_0(F_\mathfrak{p})] = 3$ and the set $E(F_\mathfrak{p}) \setminus E_0(F_\mathfrak{p})$ is nonempty. Equation (w) is minimal and $(\overline{-3^{-2}a'^2}, \overline{3^{-3}a'^3})$ is a unique singular point on the reduced curve. Thus any element in $E(F_\mathfrak{p}) \setminus E_0(F_\mathfrak{p})$ has the form $(-3^{-2}a'^2 + \pi s, 3^{-3}a'^3 + \pi t)$ for some $s, t \in \mathfrak{O}_{F_\mathfrak{p}}$. Substituting for (x, y) in this form into the minimal equation (w) modulo π^3 yields

$$\pi^2 t^2 \equiv \left(\frac{a'}{3}\right)^3 \frac{D'}{3^3} \pmod{\pi^3},$$

and hence $\widehat{\delta}_{F_\mathfrak{p}}(P) = (1 \pm \pi(3/a')^3 t) F_\mathfrak{p}^{*3} (\neq F_\mathfrak{p}^{*3})$. This implies the required result. □

Lemma 4.4. *Assume that* $\nu_\mathfrak{p}(a') = \nu_\mathfrak{p}(b') = 1$, $\mathfrak{p} \mid 3$, *and assume that*† 3 *is unramified in* $F_\mathfrak{p}$. *Let* $\{r_1, r_2, \ldots, r_{(m-1)/2}\} \amalg \{-r_1, -r_2, \ldots, -r_{(m-1)/2}\}$ $(\subset \mathfrak{O}_{F_\mathfrak{p}}^*)$ *be a complete representative system for the multiplicative group* $\mathbf{F}_\mathfrak{p}^*$ *with* $m = \sharp \mathbf{F}_\mathfrak{p}$, *and let* $R := \{r_1, r_2, \ldots, r_{(m-1)/2}\}$. *Then*

$\mathrm{Im}\,\widehat{\delta}_{F_\mathfrak{p}}$	$[\widehat{E}(F_\mathfrak{p}) : \widehat{E}_0(F_\mathfrak{p})]$
	$[E(F_\mathfrak{p}) : E_0(F_\mathfrak{p})]$

are

$$\begin{cases} \left\langle bF_\mathfrak{p}^{*3},\ \left(1 + r^{-3}(a'r^2 + b')\right)F_\mathfrak{p}^{*3} \;\middle|\; r \in R \right\rangle \quad \Big| \quad 1 \quad \Big|^\dagger & \text{if } (-a'b'^{-1}/\mathfrak{p}) = 1, \\ F_\mathfrak{p}^*/F_\mathfrak{p}^{*3} \quad \Big| \quad 1/3 & \text{if } (-a'b'^{-1}/\mathfrak{p}) = -1. \end{cases}$$

Furthermore, if $(-a'b'^{-1}/\mathfrak{p}) = 1$, *then the group* $\mathrm{Im}\,\widehat{\delta}_{F_\mathfrak{p}}$ *is of order* m. *In particular, for the case* $F = \mathbf{Q}$, *we have* $\mathrm{Im}\,\widehat{\delta}_{\mathbf{Q}_3} = \langle b\,\mathbf{Q}_3^{*3}\rangle$ *or* $\mathbf{Q}_3^*/\mathbf{Q}_3^{*3}$ *according to whether or not* $-a'b'^{-1} \equiv 1 \pmod 3$, *respectively.*

Proof. Under the assumption, for the case $(-a'b'^{-1}/\mathfrak{p}) = -1$, the statement follows from formula (2.3) with the results in Section 3. When $(-a'b'^{-1}/\mathfrak{p}) = 1$, the Weierstrass form (w) is minimal from Proposition 3.5, and the group $E(F_\mathfrak{p})/E_0(F_\mathfrak{p})$ is of order 3 and is generated by the class of the representative $(0, 0)$. It is thus verified that the image $\mathrm{Im}\,\widehat{\delta}_{F_\mathfrak{p}}$ is $\langle bF_\mathfrak{p}^{*3}\rangle \cdot \widehat{\delta}_{F_\mathfrak{p}}(E_0(F_\mathfrak{p}))$. Further, since $\widehat{\delta}_{F_\mathfrak{p}}(E_1(F_\mathfrak{p}))$ is trivial from Lemma 3.3, it suffices to consider the image of $E_0(F_\mathfrak{p}) \setminus E_1(F_\mathfrak{p})$. From equation (w) we observe that any point

$P \in E_0(F_\mathfrak{p}) \setminus E_1(F_\mathfrak{p})$ can be written as the form $(r^2+\pi s,\, r^3+\pi t)$ for some $r \in \mathfrak{O}_{F_\mathfrak{p}}^*$ and $s,\, t \in \mathfrak{O}_{F_\mathfrak{p}}$, which implies $\widehat{\delta}_{F_\mathfrak{p}}(E_0(F_\mathfrak{p})) \hookrightarrow U_\mathfrak{p}^{(1)}/U_\mathfrak{p}^{(2)}$ by the identity $(U_\mathfrak{p}^{(1)})^3 = U_\mathfrak{p}^{(2)}$ under $\nu_\mathfrak{p}(3) = 1$. The substitution $(x,\, y) = (r^2+\pi s,\, r^3+\pi t)$ into equation (w) yields

$$t \equiv \frac{a'}{\pi} r^2 + \frac{b'}{\pi} \pmod{\pi},$$

and hence

$$r^{-3} y \equiv 1 + r^{-3}(a' r^2 + b') \pmod{\pi^2}.$$

Therefore, we have $\widehat{\delta}_{F_\mathfrak{p}}(E_0(F_\mathfrak{p})) = \langle (1 + r^{-3}(a'r^2+b'))F_\mathfrak{p}^{*3} \mid r \in \mathfrak{O}_{F_\mathfrak{p}}^* \rangle$, since any smooth point on the reduced curve can be lifted to an $F_\mathfrak{p}$-rational point. It is sufficient to vary r through R because $(1 + r^{-3}(a'r^2+b'))^2$ is equivalent to $1 + (-r)^{-3}(a'(-r)^2 + b')$ modulo π^2. The latter statement of the lemma is a consequence of the results of Section 3 together with formula (2.3). □

Proposition 4.5. *For an arbitrary number field F, the converse statement of Lemma* 3.1 *is true; namely, the following two conditions are equivalent for any finite prime $\mathfrak{p}$ of F:*

- $3\nu_\mathfrak{p}(a) \geq \nu_\mathfrak{p}(b)$ *and* $3 \mid \nu_\mathfrak{p}(b)$.
- $\operatorname{Im} \widehat{\delta}_{F_\mathfrak{p}} \hookrightarrow \mathfrak{O}_{F_\mathfrak{p}}^*/\mathfrak{O}_{F_\mathfrak{p}}^{*3}$ $(\simeq \mathfrak{O}_{F_\mathfrak{p}}^* F_\mathfrak{p}^{*3}/F_\mathfrak{p}^{*3})$.

Proof. If $\operatorname{Im} \widehat{\delta}_{F_\mathfrak{p}} \hookrightarrow \mathfrak{O}_{F_\mathfrak{p}}^*/\mathfrak{O}_{F_\mathfrak{p}}^{*3}$, then by applying Theorem 4.1 and Lemma 3.2, we must have $3\nu_\mathfrak{p}(a) \geq \nu_\mathfrak{p}(b)$ and $3 \mid \nu_\mathfrak{p}(b)$. □

Let S be the set of all finite primes of F satisfying $3\nu_\mathfrak{p}(a) < \nu_\mathfrak{p}(b)$ or $3 \nmid \nu_\mathfrak{p}(b)$. From the above proposition, the $\widehat{\phi}$-Selmer group (2.5) $(m = 3)$ is a subgroup of the multiplicative group

$$R_S := \{\overline{d} \in F^*/F^{*3} \mid \nu_\mathfrak{p}(d) \equiv 0 \pmod 3 \text{ for any finite prime } \mathfrak{p} \text{ of } F \text{ outside } S\}$$

which corresponds to the group of S-units and S-ideal classes with the exact sequence

$$0 \longrightarrow \mathfrak{O}_{F,S}^* F^{*3}/F^{*3} \longrightarrow R_S \longrightarrow \mathrm{Cl}_{F,S}[3] \longrightarrow 0. \tag{4.1}$$

Here

$$\mathfrak{O}_{F,S} := \{d \in F \mid \nu_{\mathfrak{p}}(d) \geq 0 \text{ for any finite prime } \mathfrak{p} \text{ of } F \text{ outside } S\},$$
$$\mathrm{Cl}_{F,S} := \{\text{nonzero fractional ideals of } \mathfrak{O}_{F,S}\}/F^*\mathfrak{O}_{F,S}$$

are the ring of S-integers and the group of S-ideal classes, respectively. We thus have the following estimate.

Proposition 4.6. $\dim_{\mathbf{F}_3} S^{(\widehat{\phi})}(\widehat{E}/F) \leq \dim_{\mathbf{F}_3} \mathrm{Cl}_{F,S}[3] + \mathrm{rank}_{\mathbf{Z}}\mathfrak{O}_{F,S}^* + \dim_{\mathbf{F}_3}\mu_3(F)$. *Here $\mu_3(F)$ stands for the group of all cube roots of unity in F.*

Proof. This follows immediately from sequence (4.1) with the equality $\dim_{\mathbf{F}_3}\mathfrak{O}_{F,S}^*F^{*3}/F^{*3} = \dim_{\mathbf{F}_3}\mathfrak{O}_{F,S}^*/\mathfrak{O}_{F,S}^{*3} = \mathrm{rank}_{\mathbf{Z}}\mathfrak{O}_{F,S}^* + \dim_{\mathbf{F}_3}\mu_3(F)$. Note that $\mathrm{rank}_{\mathbf{Z}}\mathfrak{O}_{F,S}^* = |S| + r - 1$ from Dirichlet's S-units theorem. Here r denotes the number of all the infinite primes of F. □

Remark 4.7. If $F_{\mathfrak{p}}$ contains a primitive cube root of unity, then the elliptic curve $\widehat{E}/F_{\mathfrak{p}}$ is isomorphic over $F_{\mathfrak{p}}$ to

$$y^2 + 3axy + (a^3 - 27b)y = x^3$$

by making a substitution

$$(x,\, y) \longmapsto \left(-3x - a^2,\, 3\sqrt{-3}\frac{-1-\sqrt{-3}}{2}ax - 3\sqrt{-3}y + a^3 - 27\frac{-1-\sqrt{-3}}{2}b\right).$$

We can thus apply the flow chart in Theorem 4.1 to determine the image of $\delta_{F_{\mathfrak{p}}}$ for finite primes $\mathfrak{p}$ not lying over 3. When $\mathfrak{p} \mid 3$, additional argument might be required in certain cases.

5. Computing the Selmer groups. The purpose of the current section is to explain how to calculate an upper bound for the rank of the elliptic curve (3.1) over a number field F by using Selmer groups. Recall the account of Section 2. Assume that F has class number 1, and 3 is unramified in F. It is then observed by applying formula (2.1) that

$$\mathrm{rank}_{\mathbf{Z}}E(F) \leq \dim_{\mathbf{F}_3} S^{(\widehat{\phi})}(\widehat{E}/F) + \dim_{\mathbf{F}_3} S^{(\phi)}(E/F) - 1. \tag{5.1}$$

Combining Cassels' formula in Section 2 with equalities (2.2), (2.4) and (3.7) yields

(5.2)
$$\sharp S^{(\phi)}(E/F) = 3 \cdot \sharp S^{(\widehat{\phi})}(\widehat{E}/F) \prod_{\mathfrak{p}:\text{infinite}} \frac{|\varpi|_{\mathfrak{p}}}{3} \prod_{\mathfrak{p}:\text{finite}} \frac{[\widehat{E}(F_{\mathfrak{p}}) : \widehat{E}_0(F_{\mathfrak{p}})]}{[E(F_{\mathfrak{p}}) : E_0(F_{\mathfrak{p}})]}.$$

Here ϖ is as in Remark 3.10 (let $\varpi := 1$ in the case $\Xi = \varnothing$) and each $[\widehat{E}(F_{\mathfrak{p}}) : \widehat{E}_0(F_{\mathfrak{p}})]/[E(F_{\mathfrak{p}}) : E_0(F_{\mathfrak{p}})]$ has been determined by the flow chart of Theorem 4.1. From sequence (4.1), the Selmer group $S^{(\widehat{\phi})}(\widehat{E}/F)$ is a subgroup of the finite group

(5.3)
$$\mathfrak{O}_{F,S}^* F^{*3}/F^{*3} = \left\{ \varepsilon \prod_{\pi \in S} \pi^{m_\pi} \in F^* \;\middle|\; \varepsilon \in \mathfrak{O}_F^*,\ m_\pi = 0 \text{ or } 1 \text{ or } 2 \right\} \Big/ F^{*3}.$$

Hence, from definition (2.5), we only have to verify whether every element in this group lies locally in $\operatorname{Im} \widehat{\delta}_{F_{\mathfrak{p}}}$ for every finite prime $\mathfrak{p}$ by again using the flow chart of Theorem 4.1. Summarizing these procedures:

- Compute $S^{(\widehat{\phi})}(\widehat{E}/F)$ by searching all the elements in (5.3) lying in $\operatorname{Im} \widehat{\delta}_{F_{\mathfrak{p}}}$ for every $\mathfrak{p}$.
- Compute (5.2) to obtain the upper bound (5.1).

Example 5.1. Assume that the class number of F is equal to 1 and $\zeta_3 \notin F$. Consider the elliptic curve $E : y^2 + rxy + y = x^3$, $r \in \mathfrak{O}_F$. From Proposition 4.6, $\dim_{\mathbf{F}_3} S^{(\widehat{\phi})}(\widehat{E}/F) \leq \operatorname{rank}_{\mathbf{Z}} \mathfrak{O}_F^*$. In particular, for the case $F = \mathbf{Q}$ and $3 \nmid r$, the $\widehat{\phi}$-Selmer group $S^{(\widehat{\phi})}(\widehat{E}/\mathbf{Q})$ is trivial and $\dim_{\mathbf{F}_3} S^{(\phi)}(E/\mathbf{Q}) = n$ where n is the number of primes $p \mid r^3 - 27$ satisfying $p \equiv 1 \pmod 3$. We thus have the upper bound $\operatorname{rank}_{\mathbf{Z}} E(\mathbf{Q}) \leq n - 1$.

6. An application: Knight's problem. In their paper [**2**], Bremner, Guy and Nowakowski considered Knight's problem:

Which integers n are of the form

$$n = (a+b+c)\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right), \quad a, b, c \in \mathbf{Z} \; ? \tag{6.1}$$

To the author's knowledge, the solutions to this problem in the range $-1000 \le n \le 1000$ have been found, with most of these solutions discussed in [**2**]. When $n \neq 0, 1, 9, 10$, Bremner, Guy and Nowakowski's first observation is the one-to-one correspondence:

$$\begin{aligned}\big\{[a, b, c] \in \mathbf{P}^2(\mathbf{Q}) \mid \ (a, b, c) \text{ satisfies } (6.1)\big\} \\ \xrightarrow{\theta} E_n(\mathbf{Q}) \setminus E_n(\mathbf{Q})[6];\\ [a, b, c] \longmapsto \left(-\frac{(a+c)(b+c)}{c^2}, \frac{a(a+c)(b+c)^2}{bc^3}\right),\\ \theta^{-1} : (x, y) \longmapsto \left[-\frac{(x+1)y}{x^2+y}, -\frac{x(x+1)}{x-y}, 1\right].\end{aligned}$$

Here E_n is an elliptic curve defined by the Weierstrass form

$$\begin{aligned}E_n : y^2 + (n-3)xy + (n-1)y = x^3\\ \big(n \in \mathbf{Z} \text{ such that } \Delta := n^2(n-1)^3(n-9) \neq 0\big).\end{aligned} \tag{6.2}$$

However, the original equation that they considered is $y^2 = x(x^2 + (n^2 - 6n - 3)x + 16n)$, which is isomorphic over $\mathbf{Q}$ to form (6.2) and is appropriate for descent via 2-isogenies. Equation (6.2) is appropriate for descent via 3-isogenies, as has been discussed in the preceding sections. Note that the torsion subgroup is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ for $n = 10$ (in fact $\operatorname{rank}_{\mathbf{Z}} E_{10}(\mathbf{Q}) = 0$), and $\mathbf{Z}/6\mathbf{Z}$ for $n \in \mathbf{Z} \setminus \{0, 1, 9, 10\}$. For the case $n \in \{0, 1, 9, 10\}$, one can easily verify that n is representable in the form (6.1). Hence, from the above correspondence the problem (6.1) may be generally reduced to that of finding rational points on $E_n/\mathbf{Q}$ of infinite order, that is, for any $n \in \mathbf{Z} \setminus \{0, 1, 9, 10\}$,

(6.3) the integer n is representable in the form (6.1) if and only if $\operatorname{rank}_{\mathbf{Z}} E_n(\mathbf{Q}) > 0$.

Notice that, for $n \in \mathbf{Z} \setminus \{0, 1, 9, 10\}$, the contribution of the torsion subgroup $E_n(\mathbf{Q})[6] = \langle (n-1, n-1) \rangle \simeq \mathbf{Z}/6\mathbf{Z}$ to the solution of problem (6.1) is described by

$$\begin{aligned}\theta\left(\left[\frac{1}{b}, \frac{1}{c}, \frac{1}{a}\right]\right) = \theta([a, b, c]) + (n-1, n-1),\\ \theta([b, a, c]) = -\theta([a, b, c]),\end{aligned}$$

whenever there is a triple $[a, b, c]$ representing n in the form (6.1). Therefore, the torsion points generate no essential solutions. The latter also implies the contribution of the inverse law for the Mordell-Weil group $E_n(\mathbf{Q})$.

Since $E_n/\mathbf{Q}$ has the rational 3-torsion point $(0, 0)$, one can state a criterion for problem (6.1) by using the argument of the preceding sections, which is as follows:

Proposition 6.1. *If an integer n satisfies the following two conditions, then n is not representable in the form* (6.1).

- *n is of the form $\pm q^r + 1$ with prime q, positive integer $r \in \mathbf{N}$ and satisfies $9 \nmid n \neq 10$.*
- *Every prime p dividing $n(n-9)$ satisfies $p \not\equiv 1 \pmod 3$.*

Proof. It is observed that $n \in \mathbf{Z} \setminus \{0, 1, 9, 10\}$ under the assumption. Thus, we have only to prove $\operatorname{rank}_{\mathbf{Z}} E_n(\mathbf{Q}) = 0$ by (6.3). The proof is easily deduced from the following flow chart with computation in Section 5. □

Proposition 6.2. *For any rational prime p, the image of the local connecting homomorphism $\widehat{\delta}_{\mathbf{Q}_p}$ for $E_n/\mathbf{Q}$ is determined as follows*:

$$\left(\textit{The box indicates } \boxed{\operatorname{Im}\widehat{\delta}_{\mathbf{Q}_\mathfrak{p}} \;\Big\|\; \begin{array}{|c|}\hline [\widehat{E}_n(\mathbf{Q}_\mathfrak{p}) : \widehat{E}_{n,0}(\mathbf{Q}_\mathfrak{p})] \\ \hline [E_n(\mathbf{Q}_\mathfrak{p}) : E_{n,0}(\mathbf{Q}_\mathfrak{p})] \\ \hline \end{array}}.\right)$$

$n \not\equiv 3 \pmod p$

$$\longrightarrow \begin{cases} p = 2 \to \boxed{\mathbf{Z}_2^*/\mathbf{Z}_2^{*3} \;\|\; 1}, \\ p \neq 2 \\ \quad \to \begin{cases} n \equiv 1 \pmod p \to \boxed{\mathbf{Q}_p^*/\mathbf{Q}_p^{*3} \;\|\; 1/3}, \\ n \not\equiv 1 \pmod p \to \begin{cases} p \mid n(n-9) \to \boxed{\{1\} \;\Big\|\; \begin{array}{|c|}\hline 3 \text{ if } p \equiv 1 \pmod 3 \\ \hline 1 \text{ if } p \not\equiv 1 \pmod 3 \\ \hline \end{array}}, \\ p \nmid n(n-9) \to \boxed{\mathbf{Z}_p^*/\mathbf{Z}_p^{*3} \;\|\; 1}, \end{cases} \end{cases} \end{cases}$$

$$
\begin{array}{l}
n \equiv 3 \pmod{p} \\
\quad \to \begin{cases}
p = 2 & \\
\quad \to \begin{cases}
n \equiv 9 \pmod{16} \to \boxed{\mathbf{Z}_2^*/\mathbf{Z}_2^{*3} \,\|\, 1}, \\
n \not\equiv 9 \pmod{16} \to \boxed{\mathbf{Q}_2^*/\mathbf{Q}_2^{*3} \,\|\, 1/3},
\end{cases} \\
p \neq 2 & \\
\quad \to \begin{cases}
p = 3 \to \begin{cases}
n \equiv 3, 6 \pmod{9} \to \boxed{\mathbf{Z}_3^*/\mathbf{Z}_3^{*3} \,\|\, 1}, \\
n \equiv 0 \pmod{9} \to \boxed{\{1\} \,\|\, 1},
\end{cases} \\
p \neq 3 \to \boxed{\mathbf{Z}_p^*/\mathbf{Z}_p^{*3} \,\|\, 1}.
\end{cases}
\end{cases}
\end{array}
$$

Proof. Apply Theorem 4.1 to the elliptic curve $E_n/\mathbf{Q}$ (6.2). □

REFERENCES

1. V.G. Berkovič, *On the division by an isogeny of the points of an elliptic curve*, Math. USSR Sbor. **22** (1974), 473–492.

2. A. Bremner, R.K. Guy and R.J. Nowakowski, *Which integers are representable as the product of the sum of three integers with the sum of their reciprocals?*, Math. Comp. **61** (1993), 117–130.

3. J.W.S. Cassels, *Arithmetic on curves of genus* 1. VIII. *On conjectures of Birch and Swinnerton-Dyer*, J. reine Angew. Math. **217** (1965), 180–199.

4. ———, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

5. A.P. Ogg, *Elliptic curves and wild ramification*, Amer. J. Math. **89** (1967), 1–21.

6. J.H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts Math. **106**, Springer-Verlag, 1986.

7. ———, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts Math. **151**, Springer-Verlag, 1994.

8. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in *Modular functions of one variable* IV, Lecture Notes Math. **476** Springer-Verlag, 1975.

9. J. Vélu, *Isogénies entre courbes elliptiques*, C.R. Acad. Sci. Paris **273** (1971), 238–241.

Graduate School of Mathematics, Kyushu University, Fukuoka 812-8581, Japan

Email address: rinrin@math.kyushu-u.ac.jp