

NUMBER FIELDS GENERATED BY THE 3-TORSION POINTS OF AN ELLIPTIC CURVE

ANDREA BANDINI, LAURA PALADINO

ABSTRACT. Let $\mathcal{E}$ be an elliptic curve, m a positive number and $\mathcal{E}[m]$ the m -torsion subgroup of $\mathcal{E}$. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ form a basis of $\mathcal{E}[m]$. We prove that $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(x_1, x_2, \zeta_m, y_1)$ in general. For the case $m = 3$ we provide a description of all the possible extensions $\mathbb{Q}(\mathcal{E}[3])$ in terms of generators, degree and Galois groups.

Key-words: elliptic curves; torsion points.

Mathematics subject classification: 11G05; 12G05.

1. INTRODUCTION

Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where b and c are rational numbers. Let m be a positive integer. We denote by $\mathcal{E}[m]$ the m -torsion subgroup of $\mathcal{E}$, by $\mathbb{Q}(\mathcal{E}[m])$ the number field generated by the coordinates of the m -torsion points of $\mathcal{E}$ and by $\mathbb{Q}(\mathcal{E}_x[m])$ the field generated by the abscissas of the m -torsion points of $\mathcal{E}$. Let P_1 and P_2 be two of the m -torsion points of $\mathcal{E}$, forming a basis of $\mathcal{E}[m]$. It is well-known that $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(x_1, x_2, y_1, y_2)$. As usual, we denote by μ_m the group of m -th roots of unity and by ζ_m one of its generators. By the *Weil Pairing*, we have $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\mathcal{E}[m])$, for all m (see for example [15, III, 8.1.1]). In the first part of this paper we prove $\zeta_m \in \mathbb{Q}(\mathcal{E}_x[m])$ and $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(x_1, x_2, \zeta_m, y_1)$. Working on local-global divisibility problems for $\mathcal{E}$ (building on ideas and results provided in [4] and [5]) the second named author was naturally led to face the problem of describing the extension $\mathbb{Q}(\mathcal{E}[m])$ for $m = 3$ (to construct explicit counterexamples to local-global divisibility by 3). In [10] there is a description of the family of elliptic curves $\mathcal{E}$ such that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$. We now give a complete description of the extensions $\mathbb{Q}(\mathcal{E}[3])$, for all possible $b, c \in \mathbb{Q}$. Using the explicit expression of the generators x_1, x_2, y_1 and y_2 we get a further reduction step by showing that one has $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(x_2 - x_1, \zeta_3, y_1)$ (see Corollary 4.7). After that, in the final main theorem (Theorem 4.1), we provide a few details on all the possible extensions $\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}$: namely we give the generators, the degrees $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}]$ and the Galois groups $\text{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q})$. We recall that another nice and detailed description of the field $\mathbb{Q}(\mathcal{E}[3])$ (and of $\mathbb{Q}(\mathcal{E}[m])$ in general) in terms of the behaviour of the primes in the extension $\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}$ for the case $\text{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}) \simeq \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ can be found in [1] (see in particular Proposition 5.4.6 for the case $m = 3$).

In the final section we provide some remarks for the interpretation of our results in terms of rational points on the modular curves $X(3)$, $X_1(3)$ and $X_0(3)$.

Acknowledgements. We would like to thank U. Zannier and the anonymous referee for their remarks, especially the useful suggestion of adding a section about the consequences of our results in modular curves.

2. GENERATORS FOR $\mathbb{Q}(\mathcal{E}[m])$

Let m be a positive integer and let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ form a basis of $\mathcal{E}[m]$. We have $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(x_1, x_2, y_1, y_2)$. From now on, we will denote by L the field $\mathbb{Q}(x_1, x_2)$ and by K the field $\mathbb{Q}(\mathcal{E}[m])$. Let (x_3, y_3) be the coordinates of the point $P_3 := P_1 + P_2$ and let (x_4, y_4) be the coordinates of the point $P_4 := P_1 - P_2$. As usual, we denote by e_m the Weil Pairing

$$e_m : \mathcal{E}[m] \times \mathcal{E}[m] \longrightarrow \mu_m.$$

We first prove $\zeta_m \in \mathbb{Q}(\mathcal{E}_x[m])$, for every positive integer m .

Theorem 2.1. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $\mathcal{E} : y^2 = x^3 + bx + c$, where b and c are rational numbers. Let $\mathbb{Q}(\mathcal{E}_x[m])$ be the number field generated by the abscissas of the m -torsion points of $\mathcal{E}$. Then $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(x_1, \dots, x_4) \subseteq \mathbb{Q}(\mathcal{E}_x[m])$.*

Proof. There exist $S, T \in \mathcal{E}[m]$ such that $e_m(S, T) = \zeta_m$ (see [15, III, Corollary 8.1.1]). Let $L := \mathbb{Q}(x_1, x_2)$ and let $K := L(y_1, y_2) = \mathbb{Q}(\mathcal{E}[m])$. Clearly, the degree $\tilde{d} := [K : L]$ divides 4. If $\tilde{d} = 1$, we have the conclusion (this includes the case $m = 2$, where $y_1 = y_2 = 0$). If $\tilde{d} = 2$, we may suppose $K = \mathbb{Q}(x_1, x_2, y_1)$ (hence, from now on, $y_1 \neq 0$). Using the group law of an elliptic curve, we may express x_3 and x_4 in terms of x_1, x_2, y_1 and y_2 in the following way:

$$(1) \quad x_3 = \frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - x_1 - x_2$$

$$(2) \quad x_4 = \frac{(y_1 + y_2)^2}{(x_1 - x_2)^2} - x_1 - x_2$$

Thus $x_4 - x_3 = 4y_1y_2/(x_1 - x_2)^2$ and $y_1y_2 = (x_4 - x_3)(x_1 - x_2)^2/4$. Then $y_2 = \alpha_1 + \alpha_2y_1$, with $\alpha_1, \alpha_2 \in \mathbb{Q}(x_1, x_2)$. Hence $y_1y_2 = \alpha_1y_1 + \alpha_2y_1^2 = \alpha_1y_1 + \beta_1$, with $\alpha_1, \beta_1 \in \mathbb{Q}(x_1, x_2)$. Therefore $\alpha_1y_1 + \beta_1 = (x_4 - x_3)(x_1 - x_2)^2/4$. So, if $\alpha_1 \neq 0$, we have $y_1 \in \mathbb{Q}(x_1, x_2, x_3, x_4)$ and, by (1) and (2), $y_2 \in \mathbb{Q}(x_1, x_2, x_3, x_4)$ as well. If $\alpha_1 = 0$, then $y_2 = \alpha_2y_1$; so a generator τ of $\text{Gal}(K/L)$ sends y_i to $-y_i$ for $i = 1, 2$ and, in particular, $P_i^\tau = -P_i$ for $i = 1, 2$. Put $S = \gamma_1P_1 + \gamma_2P_2$ and $T = \delta_1P_1 + \delta_2P_2$ with $\gamma_1, \gamma_2, \delta_1, \delta_2 \in \{0, 1, 2, \dots, m-1\}$. Then

$$S^\tau = (\gamma_1P_1 + \gamma_2P_2)^\tau = \gamma_1P_1^\tau + \gamma_2P_2^\tau = -\gamma_1P_1 - \gamma_2P_2 = -S$$

and similarly, $T^\tau = -T$. The Weil pairing is Galois invariant (see [15, III, Proposition 8.1]), so we have

$$\zeta_m^\tau = e_m(S, T)^\tau = e_m(S^\tau, T^\tau) = e_m(-S, -T) = e_m(S, T) = \zeta_m,$$

i.e., $\zeta_m \in L$.

In both cases we can conclude $\zeta_m \in \mathbb{Q}(x_1, x_2, x_3, x_4) \subseteq \mathbb{Q}(\mathcal{E}_x[m])$.

Finally, let $\tilde{d} = 4$. In this case, we clearly have $\text{Gal}(K/L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then there exists a $\tau \in \text{Gal}(K/L)$ such that $\tau(y_i) = -y_i$ for $i = 1, 2$. As in the previous case, this leads to $\zeta_m^\tau = \zeta_m$. Therefore $\zeta_m \in K^\tau$ (the subfield of K fixed by τ). Moreover $y_1y_2 \in K^\tau$ as well and, since $[K^\tau : L] = |\text{Gal}(K/L)/\langle \tau \rangle| = 2$, one has $K^\tau = \mathbb{Q}(x_1, x_2, y_1y_2)$. From (1) and (2), we deduce $\mathbb{Q}(x_1, x_2, y_1y_2) = \mathbb{Q}(x_1, x_2, x_3, x_4)$. Then, we have proved $\zeta_m \in \mathbb{Q}(x_1, x_2, x_3, x_4) \subseteq \mathbb{Q}(\mathcal{E}_x[m])$. $\square$

Obviously, we have $\mathbb{Q}(x_1, x_2, y_1, y_2) = \mathbb{Q}(x_1, x_2, y_1y_2, y_1)$. By (1) and (2) it is clear that $\mathbb{Q}(\mathcal{E}[m])$ can be obtained by adding to $\mathbb{Q}(\mathcal{E}_x[m])$ the ordinate of one of the m -torsion points of $\mathcal{E}$. With the next theorem we will prove that $\mathbb{Q}(\mathcal{E}[m])$ can be obtained by adding to $\mathbb{Q}(x_1, x_2)$ an m -th root of unity and the ordinate of one of the m -torsion points of $\mathcal{E}$ with abscissas x_1 or x_2 .

Theorem 2.2. *With $\mathcal{E}$ as above, let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be generators of the m -torsion subgroup of $\mathcal{E}$. Then $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(x_1, x_2, \zeta_m, y_1)$.*

Proof. As above, we denote by L the number field $\mathbb{Q}(x_1, x_2)$ and by K the number field $\mathbb{Q}(\mathcal{E}[m])$. By Theorem 2.1, we know that $\zeta_m \in \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(x_1, x_2, y_1 y_2) = L(y_1 y_2)$. If $y_1 y_2 \in L$, we clearly have that $\zeta_m \in L$ too and, in particular, $L(\zeta_m) = L(y_1 y_2)$. Now, suppose $y_1 y_2 \notin L$. Therefore $[L(y_1 y_2) : L] = 2$ and there exists $\tau \in \text{Gal}(K/L)$ such that $(y_1 y_2)^\tau = -y_1 y_2$. Without loss of generality, we may suppose $y_1^\tau = -y_1$ and $y_2^\tau = y_2$ so that $P_1^\tau = -P_1$ and $P_2^\tau = P_2$. As in the proof of Theorem 2.1, let $S = \gamma_1 P_1 + \gamma_2 P_2$ and $T = \delta_1 P_1 + \delta_2 P_2$ be two m -torsion points of $\mathcal{E}$, such that $e_m(S, T) = \zeta_m$. An easy computation with the Weil pairing shows that

$$\zeta_m = e_m(S, T) = e_m(P_1, P_2)^{\gamma_1 \delta_2 - \gamma_2 \delta_1},$$

and that

$$\zeta_m^\tau = e_m(S, T)^\tau = e_m(P_1, P_2)^{-\gamma_1 \delta_2 + \gamma_2 \delta_1} = \zeta_m^{-1}.$$

We have proved that if $y_1 y_2 \notin L$, then $\zeta_m \notin L$. Hence

$$L \subsetneq L(\zeta_m) \subseteq L(y_1 y_2),$$

and, since $[L(y_1 y_2) : L] = 2$, we can conclude $L(\zeta_m) = L(y_1 y_2)$ in this case as well. Therefore $K = \mathbb{Q}(x_1, x_2, y_1 y_2, y_1) = \mathbb{Q}(x_1, x_2, \zeta_m, y_1)$, for every positive integer m . $\square$

In particular, for $m = 3$, we have $K = \mathbb{Q}(x_1, x_2, \zeta_3, y_1)$. In Section 4, we will prove $K = \mathbb{Q}(x_2 - x_1, \zeta_3, y_1)$.

3. GENERATORS FOR $\mathbb{Q}(\mathcal{E}[3])$ AND THE CASE $bc = 0$

It is well known that the abscissas of the 3-torsion points of an elliptic curve are the roots of the polynomial

$$\varphi_3 = x^4 + 2bx^2 + 4cx - \frac{b^2}{3}$$

(see for example [16]). If $c \neq 0$ then the roots x_1, x_2, x_3 and x_4 of φ_3 are

$$\begin{aligned} x_1 &= -\frac{1}{2} \sqrt{\frac{-\sqrt[3]{432c^2 + 64b^3} - 8b}{3} - \frac{8c\sqrt{3}}{\sqrt{\sqrt[3]{432c^2 + 64b^3} - 4b}}} + \frac{\sqrt{\sqrt[3]{432c^2 + 64b^3} - 4b}}{2\sqrt{3}}, \\ x_2 &= \frac{1}{2} \sqrt{\frac{-\sqrt[3]{432c^2 + 64b^3} - 8b}{3} - \frac{8c\sqrt{3}}{\sqrt{\sqrt[3]{432c^2 + 64b^3} - 4b}}} + \frac{\sqrt{\sqrt[3]{432c^2 + 64b^3} - 4b}}{2\sqrt{3}}, \\ x_3 &= -\frac{1}{2} \sqrt{\frac{-\sqrt[3]{432c^2 + 64b^3} - 8b}{3} + \frac{8c\sqrt{3}}{\sqrt{\sqrt[3]{432c^2 + 64b^3} - 4b}}} + \frac{\sqrt{\sqrt[3]{432c^2 + 64b^3} - 4b}}{2\sqrt{3}}, \\ x_4 &= \frac{1}{2} \sqrt{\frac{-\sqrt[3]{432c^2 + 64b^3} - 8b}{3} + \frac{8c\sqrt{3}}{\sqrt{\sqrt[3]{432c^2 + 64b^3} - 4b}}} + \frac{\sqrt{\sqrt[3]{432c^2 + 64b^3} - 4b}}{2\sqrt{3}}. \end{aligned}$$

Note that the condition $c \neq 0$ is equivalent to the condition $\sqrt[3]{432c^2 + 64b^3} - 4b \neq 0$. Furthermore, observe that $-(432c^2 + 64b^3)$ is the discriminant of the elliptic curve $y^2 = x^3 + bx + c$. As usual, we denote that discriminant by Δ . Therefore, we have

$$\begin{aligned} x_1 &= -\frac{1}{2} \sqrt{\frac{(\sqrt[3]{\Delta} - 8b)}{3} - \frac{8c\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta} - 4b}}} + \frac{\sqrt{-\sqrt[3]{\Delta} - 4b}}{2\sqrt{3}}, \\ x_2 &= \frac{1}{2} \sqrt{\frac{(\sqrt[3]{\Delta} - 8b)}{3} - \frac{8c\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta} - 4b}}} + \frac{\sqrt{-\sqrt[3]{\Delta} - 4b}}{2\sqrt{3}}, \\ x_3 &= -\frac{1}{2} \sqrt{\frac{(\sqrt[3]{\Delta} - 8b)}{3} + \frac{8c\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta} - 4b}}} + \frac{\sqrt{-\sqrt[3]{\Delta} - 4b}}{2\sqrt{3}}, \end{aligned}$$

$$x_4 = \frac{1}{2} \sqrt{\frac{(\sqrt[3]{\Delta} - 8b)}{3} + \frac{8c\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta} - 4b}}} + \frac{\sqrt{-\sqrt[3]{\Delta} - 4b}}{2\sqrt{3}}$$

with $-\sqrt[3]{\Delta} - 4b \neq 0$. Let y_i be the ordinate of one of the two points of $\mathcal{E}$ with abscissas x_i ($i = 1, \dots, 4$). We may assume $y_i = \sqrt{x_i^3 + bx_i + c}$. We also show the expressions of y_1 and y_2 in terms of b and c :

$$(3) \quad y_1 = \sqrt{\frac{((\sqrt[3]{\Delta} + 4b)\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b} + 36c)\sqrt{\frac{(\sqrt[3]{\Delta} - 8b)\sqrt{-\sqrt[3]{\Delta} - 4b - 24c\sqrt{3}}}{3\sqrt{-\sqrt[3]{\Delta} - 4b}}} - 24c\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b} - \sqrt[3]{\Delta^2} + 4b\sqrt[3]{\Delta} + 32b^2}{12\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b}}},$$

$$(4) \quad y_2 = \sqrt{\frac{-((\sqrt[3]{\Delta} + 4b)\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b} + 36c)\sqrt{\frac{(\sqrt[3]{\Delta} - 8b)\sqrt{-\sqrt[3]{\Delta} - 4b - 24c\sqrt{3}}}{3\sqrt{-\sqrt[3]{\Delta} - 4b}}} - 24c\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b} - \sqrt[3]{\Delta^2} + 4b\sqrt[3]{\Delta} + 32b^2}{12\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b}}}.$$

Let $P_i = (x_i, y_i)$, since the 3-torsion subgroup of an elliptic curve is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$ and $2P_i = -P_i = (x_i, -y_i)$, the points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ generate $\mathcal{E}[3]$. Therefore, we have $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(x_1, x_2, y_1, y_2)$.

Now we focus on $\mathbb{Q}(\mathcal{E}[3])$ for the two (easy) cases $c = 0$ and $b = 0$, postponing the general case $bc \neq 0$ to the next section. For $c = 0$ we can easily provide a full description of $\mathbb{Q}(\mathcal{E}[3])$ via the following

Theorem 3.1. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx$, where $b \in \mathbb{Q}^*$. Then*

$$\mathbb{Q}(\mathcal{E}_x[3]) = \mathbb{Q}\left(\sqrt{\frac{-2b\sqrt{3} - 3b}{3}}, \zeta_3\right) \text{ with } [\mathbb{Q}(\mathcal{E}_x[3]) : \mathbb{Q}] = 8,$$

$$\mathbb{Q}(\mathcal{E}[3]) = \begin{cases} \mathbb{Q}\left(\zeta_3, \sqrt{\frac{-2b\sqrt{-2b\sqrt{3}-3b}}{3}}\right) & \text{if } b < 0 \\ \mathbb{Q}\left(\zeta_3, \sqrt{\frac{2b\sqrt{2b\sqrt{3}-3b}}{3}}\right) & \text{if } b > 0 \end{cases}$$

with $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = 16$.

Moreover $\text{Gal}(\mathbb{Q}(\mathcal{E}_x[3])/\mathbb{Q}) \simeq D_4$ (the dihedral group of order 8) and $\text{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}) \simeq SD_8$ (the semidihedral group of order 16).

Proof. The abscissas of the 3-torsion points of $\mathcal{E}$ are the roots of the polynomial

$$\hat{\varphi}_3 := x^4 + 2bx^2 - \frac{b^2}{3}.$$

We have

$$\hat{x}_1 := \sqrt{\frac{-2b\sqrt{3} - 3b}{3}}, \quad \hat{x}_2 := -\sqrt{\frac{-2b\sqrt{3} - 3b}{3}}, \quad \hat{x}_3 := \sqrt{\frac{2b\sqrt{3} - 3b}{3}}, \quad \hat{x}_4 := -\sqrt{\frac{2b\sqrt{3} - 3b}{3}}.$$

Clearly $\mathbb{Q}(\hat{x}_1, \hat{x}_2, \hat{x}_3, \hat{x}_4) = \mathbb{Q}(\hat{x}_1, \hat{x}_3) = \mathbb{Q}(\hat{x}_1, \zeta_3) = \mathbb{Q}(\hat{x}_3, \zeta_3)$ (since $\hat{x}_1\hat{x}_3 = \frac{b\sqrt{-3}}{3}$).

It is easy to verify that neither $\frac{-2b\sqrt{3}-3b}{3}$ nor $\frac{2b\sqrt{3}-3b}{3}$ is a square in $\mathbb{Q}(\sqrt{3})$, for all $b \in \mathbb{Q}^*$. Thus $[\mathbb{Q}(\hat{x}_1) : \mathbb{Q}] = [\mathbb{Q}(\hat{x}_3) : \mathbb{Q}] = 4$. Moreover if $b < 0$ (resp. $b > 0$), then $\frac{-2b\sqrt{3}-3b}{3} > 0$ and $\mathbb{Q}(\hat{x}_1) \subset \mathbb{R}$ (resp. $\frac{2b\sqrt{3}-3b}{3} > 0$ and $\mathbb{Q}(\hat{x}_3) \subset \mathbb{R}$). Hence, in any case, $[\mathbb{Q}(\mathcal{E}_x[3]) : \mathbb{Q}] = 8$. It is

easy to check that the Galois group is isomorphic to D_4 , generated by φ and ψ , where

$$\varphi \left\{ \begin{array}{l} \hat{x}_1 \mapsto \hat{x}_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \quad \text{and} \quad \psi \left\{ \begin{array}{l} \hat{x}_1 \mapsto \hat{x}_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. .$$

Obviously the field $\mathbb{Q}(\mathcal{E}[3])$ can be obtained by adding to $\mathbb{Q}(\mathcal{E}_x[3])$ one of the ordinates of the 3-torsion points of $\mathcal{E}$, i.e., $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\hat{x}_i, \zeta_3, \hat{y}_i)$ ($i = 1, \dots, 4$). If $b < 0$, then consider

$$\hat{y}_1 := \sqrt{\hat{x}_1^3 + b\hat{x}_1} = \sqrt{\frac{-2b\sqrt{-2b\sqrt{3}-3b}}{3}} .$$

Obviously $\sqrt{3} \in \mathbb{Q}(\hat{y}_1)$ and then $\hat{x}_1 = -\frac{\sqrt{3}}{2b}\hat{y}_1^2 \in \mathbb{Q}(\hat{y}_1)$ too, so $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\hat{y}_1, \zeta_3)$. To compute the degree, one notices that $\hat{y}_1 \in \mathbb{R}$ (so that $[\mathbb{Q}(\hat{y}_1, \zeta_3) : \mathbb{Q}(\hat{y}_1)] = 2$) and that

$$\hat{y}_1 = \sqrt[4]{\frac{-8b^3\sqrt{3}-12b^3}{9}}$$

where $\frac{-8b^3\sqrt{3}-12b^3}{9}$ is not a square in $\mathbb{Q}(\sqrt{3})$ (so that $[\mathbb{Q}(\hat{y}_1) : \mathbb{Q}(\sqrt{3})] = 4$).

If $b > 0$, one uses the same arguments but with $\hat{y}_3$. In any case we find $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = 16$.

The Galois group is a 2-Sylow subgroup of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$, hence isomorphic to SD_8 , generated by the elements

$$\varphi_1 \left\{ \begin{array}{l} \hat{y}_1 \mapsto \hat{y}_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \quad \text{and} \quad \psi_1 \left\{ \begin{array}{l} \hat{y}_1 \mapsto \hat{y}_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right.$$

of orders 8 and 2 respectively. Writing down the elements as extensions of the elements of $\text{Gal}(\mathbb{Q}(\mathcal{E}_x[3])/\mathbb{Q})$ and looking at their orders (in particular at the elements of order 2) one can also find a direct and explicit proof of $\text{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}) \simeq SD_8$ (see Appendix A for details). $\square$

For completeness we include here the (even easier) case $b = 0$ as well, but we remark that it is also included in the general case $c \neq 0$ which will be discussed in detail later on (we will point out where it can be found in the various Lemmas of Section 4).

Theorem 3.2. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + c$, where $c \in \mathbb{Q}^*$. Then $\mathbb{Q}(\mathcal{E}_x[3]) = \mathbb{Q}(\sqrt[3]{-4c}, \zeta_3)$ and $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\sqrt[3]{-4c}, \zeta_3, \sqrt{c})$.*

Proof. If $b = 0$, then the abscissas of the points of order 3 of $\mathcal{E}$ are the roots of the polynomial

$$\tilde{\varphi}_3 := x^4 + 4cx .$$

Clearly, these roots are

$$\tilde{x}_1 = 0, \quad \tilde{x}_2 = \sqrt[3]{-4c}, \quad \tilde{x}_3 = \zeta_3 \sqrt[3]{-4c}, \quad \tilde{x}_4 = \zeta_3^2 \sqrt[3]{-4c} .$$

Therefore $\tilde{y}_1 = \sqrt{c}$ and $\tilde{y}_2 = \sqrt{-3c}$. We have $\mathbb{Q}(\mathcal{E}_x[3]) = \mathbb{Q}(\sqrt[3]{-4c}, \zeta_3)$ and $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\sqrt[3]{-4c}, \zeta_3, \sqrt{c})$. $\square$

Clearly, by Theorem 3.2, if $b = 0$, then there are four possibilities for $d = [\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}]$. We list them in the following corollary.

Corollary 3.3. *One has:*

$$[\mathbb{Q}(\mathcal{E}_x[3]) : \mathbb{Q}] = \begin{cases} 6 & \text{if } c \not\equiv 2 \pmod{(\mathbb{Q}^*)^3} \text{ and } \text{Gal}(\mathbb{Q}(\mathcal{E}_x[3])/\mathbb{Q}) \simeq S_3 \\ 2 & \text{if } c \equiv 2 \pmod{(\mathbb{Q}^*)^3} \text{ and } \text{Gal}(\mathbb{Q}(\mathcal{E}_x[3])/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \end{cases}$$

and

$$[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = \begin{cases} 12 & \text{if } c \not\equiv 2 \pmod{(\mathbb{Q}^*)^3}, c \not\equiv 1, -3 \pmod{(\mathbb{Q}^*)^2} \\ 6 & \text{if } c \not\equiv 2 \pmod{(\mathbb{Q}^*)^3}, c \equiv 1, -3 \pmod{(\mathbb{Q}^*)^2} \\ 4 & \text{if } c \equiv 2 \pmod{(\mathbb{Q}^*)^3}, c \not\equiv 1, -3 \pmod{(\mathbb{Q}^*)^2} \\ 2 & \text{if } c \equiv 2 \pmod{(\mathbb{Q}^*)^3}, c \equiv 1, -3 \pmod{(\mathbb{Q}^*)^2} \end{cases}.$$

The above cases correspond (respectively) to the following Galois groups:

$$\text{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}) \simeq \begin{cases} S_3 \times \mathbb{Z}/2\mathbb{Z} \\ S_3 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \end{cases}.$$

Proof. By Lemma 3.2, we have $K = \mathbb{Q}(\sqrt[3]{-4c}, \zeta_3, \sqrt{c})$. So it is just a matter of checking whether the arguments under the roots are cubes or squares or generate the same extension of ζ_3 or not. Note also that $\Delta = -16 \cdot 27c^2$ and $\sqrt[3]{\Delta} = 6\sqrt[3]{-2c^2}$. Hence $\Delta \equiv -4c \pmod{(\mathbb{Q}^*)^3}$ so the conditions on $-4c$ being or not being a cube can also be expressed in terms of Δ (we are going to find similar conditions in the general case). The computations of the Galois groups are straightforward. $\square$

We end this section with an easy bound for $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}]$.

Since x_1 and x_2 are roots of a polynomial of degree 4, one has that x_2 has degree at most 3 over $\mathbb{Q}(x_1)$ so $[\mathbb{Q}(x_1, x_2) : \mathbb{Q}] \leq 12$. Each of the ordinates y_1 and y_2 is a root of a polynomial of degree 2 over $\mathbb{Q}(x_1, x_2)$. Therefore $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}(x_1, x_2)] \leq 4$ and finally

$$d = [\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = [\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}(x_1, x_2)] \cdot [\mathbb{Q}(x_1, x_2) : \mathbb{Q}] \leq 48.$$

Therefore, we have the following result

Proposition 3.4. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where b and c are rational numbers. Then $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] \leq 48$.*

Remark 3.5. Such a rough bound can be computed in the same way for $\mathbb{Q}(\mathcal{E}[n])$ using the division polynomials (see [15, Exercise 3.7]). If N is the degree of the polynomial having the abscissas of the points of order n as roots, one easily finds $[\mathbb{Q}(\mathcal{E}[n]) : \mathbb{Q}] \leq 4N(N-1)$. Another simple bound is provided by the well known embedding $\text{Gal}(\mathbb{Q}(\mathcal{E}[n])/\mathbb{Q}) \hookrightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ (which is a finite group). For p prime this yields $[\mathbb{Q}(\mathcal{E}[p]) : \mathbb{Q}] \leq (p^2 - 1)(p^2 - p)$ (which, for $p = 3$, gives again 48). Serre's celebrated "open image theorem" (see, for example, [15, Appendix C, Theorem 19.1]) tells us to expect equality for almost all primes p for elliptic curves without complex multiplication.

By the Weil Pairing $\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(\mathcal{E}[3])$. Then d is an even number that divides 48, i.e., $d \in \Omega := \{2, 4, 6, 8, 12, 16, 24, 48\}$. In Section 4, we will show that the set Ω is not minimal, because there exist no elliptic curves $\mathcal{E}$ such that $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = 24$. On the contrary, we will show that for all $d \in \Omega \setminus \{24\}$, there exists an elliptic curve $\mathcal{E}$ such that $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = d$, i.e., the set $\tilde{\Omega} := \Omega \setminus \{24\}$ is minimal.

4. NUMBER FIELDS $\mathbb{Q}(\mathcal{E}[3])$

In this section we shall list all the possibilities for $\mathbb{Q}(\mathcal{E}[3])$ and d , thus proving, in particular, that the set $\tilde{\Omega}$ is minimal. We will need several lemmas, which eventually will lead to the proof of the following

Theorem 4.1. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where b and c are rational numbers. Let $d := [\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}]$. Then $d \in \Omega = \{2, 4, 6, 8, 12, 16, 48\}$ and the set $\tilde{\Omega}$ is minimal. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ form a basis of $\mathcal{E}[3]$. Then $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(x_2 - x_1, \zeta_3, y_1)$ and, in particular, we have the following cases:*

1. *if Δ is not the cube of a rational number, and $(-\sqrt[3]{\Delta} - 4b)/3$ is not a square in $\mathbb{Q}(\sqrt[3]{\Delta})$, then $d = 48$;*
2. *if Δ is the cube of a rational number, and $(-\sqrt[3]{\Delta} - 4b)/3$ is not a rational square, then $d = 16$;*
3. *if Δ is not the cube of a rational number, and $(-\sqrt[3]{\Delta} - 4b)/3$ is a square in $\mathbb{Q}(\sqrt[3]{\Delta})$, then $\mathcal{E}$ belongs to one of the families*

$$\mathcal{F}_{b,a_0} : y^2 = x^3 + bx + \frac{16b^2 - 216a_0^2b - 243a_0^4}{288a_0},$$

$$\mathcal{F}_c : y^2 = x^3 + c,$$

with $b, a_0 \in \mathbb{Q}^*$ and $c \neq 0$, $c \not\equiv 2 \pmod{(\mathbb{Q}^*)^3}$. We have $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(x_2, \zeta_3, y_1) = \mathbb{Q}(\sqrt[3]{\Delta}, \zeta_3, y_1)$. In particular, if $\mathcal{E}$ belongs to $\mathcal{F}_{b,a_0}$, then $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(x_2, \zeta_3, y_1) = \mathbb{Q}(\sqrt[3]{4a_0b/3 + a_0^2}, \zeta_3, \sqrt{2a_0})$ and $d \in \{6, 12\}$. If $\mathcal{E}$ belongs to the family $\mathcal{F}_c$ then $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\sqrt[3]{-4c}, \zeta_3, \sqrt{c})$ and $d \in \{6, 12\}$ as well.

4. *if $\Delta = h^3$ and $(-h - 4b)/3 = \ell^2$ for some $h, \ell \in \mathbb{Q}^*$, then*

$$\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}\left(\sqrt{-\ell^2 - 4b - \frac{8c}{\ell}}, \zeta_3, \sqrt{-\ell^3 - 8b\ell - 16c + \left(-\ell^2 + \frac{4c}{\ell}\right)\sqrt{\gamma}}\right)$$

and we have $d \in \{2, 4, 8\}$.

5. *if $\Delta = h^3$, with $h \in \mathbb{Q}$, and $-h - 4b = 0$, then $c = 0$, $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(y_i, \zeta_3)$ for some i and $d = 16$.*

For many choices of nonzero rational b and c , we have that Δ is not the cube of a rational number and that $(-\sqrt[3]{\Delta} - 4b)/3$ is not a square in $\mathbb{Q}(\sqrt[3]{\Delta})$. We are going to prove that in this case $[L : \mathbb{Q}] = 12$.

Lemma 4.2. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where b and c are nonzero rational numbers. If $\Delta \notin (\mathbb{Q}^*)^3$ and $(-\sqrt[3]{\Delta} - 4b)/3 \notin \mathbb{Q}(\sqrt[3]{\Delta})^2$, then $[L : \mathbb{Q}] = 12$.*

Proof. By hypotheses, we have $[\mathbb{Q}(\sqrt{(-\sqrt[3]{\Delta} - 4b)/3}) : \mathbb{Q}] = 6$. Therefore $6 \mid [L : \mathbb{Q}]$. In Section 3 we showed $[L : \mathbb{Q}] \leq 12$, then $[L : \mathbb{Q}] \in \{6, 12\}$. Observe that under the hypothesis $c \neq 0$, we have

$$(5) \quad t := x_2 - x_1 = \sqrt{\frac{\sqrt[3]{\Delta} - 8b}{3} - 8c \frac{\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta} - 4b}}},$$

$$(6) \quad s := x_4 - x_3 = \sqrt{\frac{\sqrt[3]{\Delta} - 8b}{3} + 8c \frac{\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta} - 4b}}}.$$

Furthermore $x_1 + x_2 = x_3 + x_4 = \sqrt{(-\sqrt[3]{\Delta} - 4b)/3}$. Let $t := \sqrt{\gamma}$ and $s := \sqrt{\gamma'}$. Assume $[L : \mathbb{Q}] = 6$. Then $L = \mathbb{Q}\left(\sqrt{(-\sqrt[3]{\Delta} - 4b)/3}\right) = \mathbb{Q}(x_1 + x_2) = \mathbb{Q}(x_3 + x_4)$ and γ is a square in L . Therefore, there exist $a_0, b_0 \in \mathbb{Q}(\sqrt[3]{\Delta})$ such that

$$\gamma = \left(a_0 + b_0 \sqrt{\frac{-\sqrt[3]{\Delta} - 4b}{3}}\right)^2.$$

We get

$$\begin{cases} \frac{\sqrt[3]{\Delta} - 8b}{3} &= a_0^2 + b_0^2 \left(\frac{-\sqrt[3]{\Delta} - 4b}{3}\right) \\ -8c \left(\frac{3}{-\sqrt[3]{\Delta} - 4b}\right) &= 2a_0 b_0 \end{cases}$$

which yields

$$\gamma' = \left(a_0 - b_0 \sqrt{\frac{-\sqrt[3]{\Delta} - 4b}{3}}\right)^2.$$

Therefore $\mathbb{Q}(x_4 - x_3) = \mathbb{Q}(x_3 + x_4) = \mathbb{Q}(x_1 + x_2) = \mathbb{Q}(x_2 - x_1)$, i.e., $L = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(\sqrt{(-\sqrt[3]{\Delta} - 4b)/3})$. By Theorem 2.1, we have $\zeta_3 \in L$. Since $\sqrt[3]{\Delta} \in L$ too and $[L : \mathbb{Q}] = 6$, then $L = \mathbb{Q}(\sqrt[3]{\Delta}, \zeta_3)$. Observe that $(-\sqrt[3]{\Delta} - 4b)/3 > 0$, for all $c \in \mathbb{Q}^*$. In fact $-\sqrt[3]{\Delta} - 4b > 0$ if and only if $\sqrt[3]{64b^3 + 432c^2} > 4b$, if and only if $432c^2 > 0$. Then $L = \mathbb{Q}(\sqrt{(-\sqrt[3]{\Delta} - 4b)/3})$ is a real extension, a contradiction with $\zeta_3 \in L$. We can conclude $[L : \mathbb{Q}] = 12$. $\square$

Observe that with the same proof, we have the following statement too.

Corollary 4.3. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where b and c are nonzero rational numbers. If $\Delta \in (\mathbb{Q}^*)^3$ and $(-\sqrt[3]{\Delta} - 4b)/3 \notin \mathbb{Q}^2$, then $[L : \mathbb{Q}] = 4$.*

Proof. Let $\Delta = h^3$, with $h \in \mathbb{Q}$. Then (5) and (6) become

$$(7) \quad t := \sqrt{\gamma} := x_2 - x_1 = \sqrt{\frac{h - 8b}{3} - 8c \frac{\sqrt{3}}{\sqrt{-h - 4b}}},$$

$$(8) \quad s := \sqrt{\gamma'} := x_4 - x_3 = \sqrt{\frac{h - 8b}{3} + 8c \frac{\sqrt{3}}{\sqrt{-h - 4b}}}.$$

Since $\sqrt{(-h - 4b)/3} \notin \mathbb{Q}$, a priori we have $[L : \mathbb{Q}] \in \{2, 4\}$. By repeating the same argument of Lemma 4.2, we have $\mathbb{Q}(t) \neq \mathbb{Q}(\sqrt{(-h - 4b)/3})$, otherwise $\mathbb{Q}(t) = \mathbb{Q}(s) = L = \mathbb{Q}(\mathcal{E}_x[3])$ would be a real extension, contradicting $\zeta_3 \in \mathbb{Q}(\mathcal{E}_x[3])$. Then $[L : \mathbb{Q}] = 4$. $\square$

Remark 4.4. During the proofs of Lemma 4.2 and of Corollary 4.3 we have basically proved that, if $(-\sqrt[3]{\Delta} - 4b)/3 \notin \mathbb{Q}(\sqrt[3]{\Delta})^2$, then

$$\gamma, \gamma' \notin \mathbb{Q} \left(\sqrt{\frac{-\sqrt[3]{\Delta} - 4b}{3}} \right)^2 = \mathbb{Q}(\gamma)^2 = \mathbb{Q}(\gamma')^2$$

(this will be useful later).

With the following statement we are going to treat the case when Δ is not the cube of a rational number and $(-\sqrt[3]{\Delta} - 4b)/3$ is a square in $\mathbb{Q}(\sqrt[3]{\Delta})$.

Lemma 4.5. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where c is a nonzero rational number. If $\Delta \notin (\mathbb{Q}^*)^3$ and $(-\sqrt[3]{\Delta} - 4b)/3 \in \mathbb{Q}(\sqrt[3]{\Delta})^2$, then $\mathcal{E}$ belongs to one of the families*

$$(9) \quad \mathcal{F}_{b,a_0} : y^2 = x^3 + bx + \frac{16b^2 - 216a_0^2b - 243a_0^4}{288a_0},$$

$$(10) \quad \mathcal{F}_c : y^2 = x^3 + c,$$

with $b, a_0, c \in \mathbb{Q}^*$. We have $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(x_2, \zeta_3, y_1) = \mathbb{Q}(\sqrt[3]{\Delta}, \zeta_3, y_1)$. In particular, if $\mathcal{E}$ belongs to $\mathcal{F}_{b,a_0}$, then $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(x_2, \zeta_3, y_1) = \mathbb{Q}(\sqrt[3]{4a_0b/3 + a_0^3}, \zeta_3, \sqrt{2a_0})$ and $d \in \{6, 12\}$. If $\mathcal{E}$ belongs to the family $\mathcal{F}_c$ then $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\sqrt[3]{-4c}, \zeta_3, \sqrt{c})$ and $d \in \{6, 12\}$ as well.

Proof. We have $\sqrt{(-\sqrt[3]{\Delta} - 4b)/3} \in \mathbb{Q}(\sqrt[3]{\Delta})$ if and only if there exist $a_0, a_1, a_2 \in \mathbb{Q}$, such that

$$(11) \quad \frac{-\sqrt[3]{\Delta} - 4b}{3} = \left(a_0 + a_1 \sqrt[3]{\Delta} + a_2 \sqrt[3]{\Delta^2} \right)^2.$$

Equation (11) is equivalent to the following system

$$\begin{cases} 2a_0a_2 + a_1^2 &= 0 \\ 3\Delta a_2^2 + 6a_0a_1 + 1 &= 0 \\ 4b + 6\Delta a_1a_2 + 3a_0^2 &= 0 \end{cases}.$$

With a bit of computation we can see that there exists a solution of that system if and only if

$$a_0 \neq 0 \text{ and } c = \pm \frac{16b^2 - 216a_0^2b - 243a_0^4}{288a_0} \quad \text{or} \quad a_0 = b = 0.$$

Note that, in both cases $c \neq 0$, indeed one can easily see that $16b^2 - 216a_0^2b - 243a_0^4 \neq 0$ for every choice of rational $a_0 \neq 0$. Since a_0 varies in $\mathbb{Q}^*$, we may put out the minus sign in the expression of c above. Therefore, we get the families

$$\mathcal{F}_{b,a_0} : y^2 = x^3 + bx + \frac{16b^2 - 216a_0^2b - 243a_0^4}{288a_0}, \quad \text{with } a_0 \in \mathbb{Q}^* ;$$

$$\mathcal{F}_c : y^2 = x^3 + c, \quad \text{with } c \in \mathbb{Q}^*.$$

For every curve $\mathcal{E}_{b,a_0}$ in $\mathcal{F}_{b,a_0}$, we have that one of the abscissas of the points of order 3 is $x_1 = 3a_0/2$ and another one is

$$x_2 = \frac{6\sqrt[3]{(\frac{4}{3}a_0b + a_0^3)^2} - 3a_0\sqrt[3]{\frac{4}{3}a_0b + a_0^3} - 4b - 3a_0^2}{6\sqrt[3]{\frac{4}{3}a_0b + a_0^3}}.$$

Since $x_1 \in \mathbb{Q}$, then $L = \mathbb{Q}(x_2)$ and $[L : \mathbb{Q}] \leq 3$. We are assuming $\sqrt[3]{\Delta} \notin \mathbb{Q}$, thus $[L : \mathbb{Q}] = 3$ and $L = \mathbb{Q}\left(\sqrt[3]{\frac{4}{3}a_0b + a_0^3}\right) = \mathbb{Q}(\sqrt[3]{\Delta})$. In fact, observe that for every curve in $\mathcal{F}_{b,a_0}$, we have

$$\Delta = -\frac{(4b + 3a_0^2)^2(4b + 27a_0^2)^3}{3 \cdot 4^3 a_0^2} \quad \text{and} \quad \left(\frac{4}{3}a_0b + a_0^3\right) \cdot \frac{1}{\Delta} \in (\mathbb{Q}^*)^3.$$

One of the ordinates of the points in $\mathcal{E}_{b,a_0}$ with abscissas x_1 is

$$y_1 = \frac{4b + 27a_0^2}{12\sqrt{2a_0}}.$$

Therefore, by Theorem 2.2, $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\sqrt[3]{4a_0b/3 + a_0^3}, \zeta_3, \sqrt{2a_0}) = \mathbb{Q}(\sqrt[3]{\Delta}, \zeta_3, \sqrt{2a_0})$. If $a_0 \equiv 2, -6 \pmod{(\mathbb{Q}^*)^2}$, then $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\sqrt[3]{4a_0b/3 + a_0^3}, \zeta_3)$ and $d = 6$, otherwise $d = 12$. The Galois groups are isomorphic to S_3 or $S_3 \times \mathbb{Z}/2\mathbb{Z}$ respectively.

For the family $\mathcal{F}_c$ see Theorem 3.2 and Corollary 3.3. $\square$

Remark 4.6. The previous Lemma includes some (but not all) of the cases with $b = 0$. It misses the cases with $b = 0$ and $\Delta = -432c^2 \in (\mathbb{Q}^*)^3$, i.e., the cases in which $c \equiv 2 \pmod{(\mathbb{Q}^*)^3}$. One readily checks that those are exactly the curves arising from the family $\mathcal{F}_{b,a_0}$ when b is allowed to be 0.

As a consequence of Lemma 4.2 and Lemma 4.5, we can restrict the set of generators of $\mathcal{E}[3]$ showed in Theorem 2.2.

Corollary 4.7. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $\mathcal{E} : y^2 = x^3 + bx + c$, where b and c are rational numbers. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be generators of the 3-torsion subgroup of $\mathcal{E}$. Then $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(x_2 - x_1, \zeta_3, y_1)$.*

Proof. If $c = 0$, the conclusion follows by Theorem 3.1. We now assume that $c \in \mathbb{Q}^*$. Then let $t := x_2 - x_1$ as in (5). If $\Delta \notin (\mathbb{Q}^*)^3$ and $(-\sqrt[3]{\Delta} - 4b)/3 \notin \mathbb{Q}(\sqrt[3]{\Delta})^2$, then, by Lemma 4.2 (more precisely, by its proof), $L = \mathbb{Q}(t) = \mathbb{Q}(x_2 - x_1)$. If $\Delta \notin (\mathbb{Q}^*)^3$ and $(-\sqrt[3]{\Delta} - 4b)/3 \in \mathbb{Q}(\sqrt[3]{\Delta})^2$, then, by Lemma 4.5, we have $x_1 \in \mathbb{Q}$. Thus, in particular $L = \mathbb{Q}(x_2 - x_1) = \mathbb{Q}(x_2)$. If $\sqrt[3]{\Delta} = h$, with $h \in \mathbb{Q}$, then recall equation (7), i.e.,

$$(12) \quad x_2 - x_1 = \sqrt{\frac{h - 8b}{3} - 8c \frac{\sqrt{3}}{\sqrt{-h - 4b}}}.$$

By the expressions of x_1 and x_2 showed in Section 3, we get

$$x_1 + x_2 = \frac{\sqrt{3}}{\sqrt{-h - 4b}}.$$

Therefore $L = \mathbb{Q}(x_2, x_1) = \mathbb{Q}(x_2 - x_1, x_1 + x_2) = \mathbb{Q}(x_2 - x_1)$. Theorem 2.2 provides the conclusion. $\square$

To complete the description of the cases considered until now, we have to investigate the extension K/L .

Lemma 4.8. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where b and c are rational numbers and $c \neq 0$. Assume that $(\sqrt[3]{\Delta} - 4b)/3 \notin \mathbb{Q}(\sqrt[3]{\Delta})^2$, then $y_1 \in \mathbb{Q}(x_1, x_2)$ if and only if $y_2 \in \mathbb{Q}(x_1, x_2)$.*

Proof. Let t be as in (5). By Corollary 4.7, we have $L = \mathbb{Q}(x_1, x_2) = \mathbb{Q}(x_2 - x_1) = \mathbb{Q}(t)$. Let

$$\begin{aligned} \lambda &= \frac{-24c\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b} - \sqrt[3]{\Delta}^2 + 4b\sqrt[3]{\Delta} + 32b^2}{12\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b}}, \\ \mu &= \frac{(\sqrt[3]{\Delta} + 4b)\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b} + 36c}{12\sqrt{3}\sqrt{-\sqrt[3]{\Delta} - 4b}}, \\ \gamma &= \frac{(\sqrt[3]{\Delta} - 8b)}{3} - 8c \frac{\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta} - 4b}}. \end{aligned}$$

Then, by (3), we may write $y_1 = \sqrt{\lambda + \mu\sqrt{\gamma}}$ and $y_2 = \sqrt{\lambda - \mu\sqrt{\gamma}}$ and recall that $t = \sqrt{\gamma}$. Suppose that $y_1 \in \mathbb{Q}(x_1, x_2) = \mathbb{Q}(x_2 - x_1) = \mathbb{Q}(\sqrt{\gamma})$. Thus, $\lambda + \mu\sqrt{\gamma}$ is a square in $\mathbb{Q}(\sqrt{\gamma})$, i.e.,

$\lambda + \mu\sqrt{\gamma} = (a_0 + b_0\sqrt{\gamma})^2$, for some $a_0, b_0 \in \mathbb{Q}(\gamma) = \mathbb{Q}\left(\sqrt{\frac{-\sqrt[3]{\Delta} - 4b}{3}}\right)$. Therefore $\lambda + \mu\sqrt{\gamma} = a_0^2 + b_0^2\gamma + 2a_0b_0\sqrt{\gamma}$ and, since, by Remark 4.4, $[\mathbb{Q}(\sqrt{\gamma}) : \mathbb{Q}(\gamma)] = 2$, that implies

$$\lambda = a_0^2 + b_0^2\gamma \quad \text{and} \quad \mu = 2a_0b_0.$$

Then $y_2 = \lambda - \mu\sqrt{\gamma} = a_0^2 + b_0^2\gamma - 2a_0b_0\sqrt{\gamma} = (a_0 - b_0\sqrt{\gamma})^2$. Since $a_0, b_0 \in \mathbb{Q}(\gamma)$, we have $y_2 \in \mathbb{Q}(\sqrt{\gamma}) = \mathbb{Q}(x_1, x_2)$. By interchanging y_1 and y_2 and proceeding in the same way, we clearly obtain the other implication. $\square$

Lemma 4.9. *Let $c \neq 0$. If $(\sqrt[3]{\Delta} - 4b)/3 \notin \mathbb{Q}(\sqrt[3]{\Delta})^2$, then $[K : L] = 4$.*

Proof. Suppose $[K : L] < 4$, i.e., $[K : L] \in \{1, 2\}$. If $[K : L] = 1$, then $y_1, y_2 \in L$ and, in particular, we have $y_1y_2 \in L$. If $[K : L] = 2$, then we may assume $K = L(y_1)$. Since $[L(y_1) : L] = 2$, in particular we have $y_2 = a_0 + a_1y_1$, with $a_0, a_1 \in L$. Let λ, μ, γ be as in the proof of the previous lemma. We have $y_2y_1 = \sqrt{\lambda^2 - \mu^2\gamma}$. On the other hand $y_1y_2 = a_0y_1 + a_1y_1^2$. We get $\lambda^2 - \mu^2\gamma = a_0^2y_1^2 + a_1^2y_1^4 + 2a_0a_1y_1^3$. Since $\lambda^2 - \mu^2\gamma \in L$ and $a_0, a_1, y_1^2, y_1^4 \in L$ too, that equality implies $a_0a_1 = 0$. If $a_1 = 0$, then $y_2 = a_0 \in L$. By Lemma 4.8 we have $y_1 \in L$ too, which contradicts our hypothesis on y_1 . Therefore $a_0 = 0$, and $y_2 = a_1y_1$. We get $y_1y_2 = a_1y_1^2 \in L$. As in the previous case $y_1y_2 \in L$. Thus, by (1) and (2), we have $x_3, x_4 \in L$ too. By Lemma 4.2, then $L = \mathbb{Q}(x_2 - x_1) = \mathbb{Q}(t)$. By replacing x_1 and x_2 with x_3 and x_4 in the proof of Lemma 4.2 and Corollary 4.3, we may also prove $[\mathbb{Q}(x_4 - x_3) : \mathbb{Q}(\sqrt[3]{\Delta})] = 4$. Since $\mathbb{Q}(x_4 - x_3) \subseteq L$, we get $L = \mathbb{Q}(x_4 - x_3) = \mathbb{Q}(x_2 - x_1)$. But then $s = \sqrt{\gamma'} \in \mathbb{Q}(\sqrt{\gamma})$ and one can write $\sqrt{\gamma'} = b_0 + b_1\sqrt{\gamma}$ for some $b_0, b_1 \in \mathbb{Q}(\gamma)$ (note that $b_1 \neq 0$ because of Remark 4.4). Therefore

$$\gamma' = b_0^2 + b_1^2\gamma + 2b_0b_1\sqrt{\gamma}$$

which yields $b_0b_1 = 0$, so that $b_0 = 0$. Hence we obtain $\gamma' = b_1^2\gamma$ which is an equality in $\mathbb{Q}(\gamma) = \mathbb{Q}\left(\sqrt{\frac{-\sqrt[3]{\Delta}-4b}{3}}\right)$. Writing it in terms of the basis $\left\{1, \left(\sqrt{\frac{-\sqrt[3]{\Delta}-4b}{3}}\right)^{-1}\right\}$ over the field $\mathbb{Q}(\sqrt[3]{\Delta})$ one gets

$$\frac{\sqrt[3]{\Delta} - 8b}{3} + 8c \left(\sqrt{\frac{-\sqrt[3]{\Delta} - 4b}{3}} \right)^{-1} = b_1^2 \left(\frac{\sqrt[3]{\Delta} - 8b}{3} - 8c \left(\sqrt{\frac{-\sqrt[3]{\Delta} - 4b}{3}} \right)^{-1} \right),$$

which is clearly impossible since it yields $b_1^2 = 1$ and $b_1^2 = -1$. The contradiction shows that $[K : L] \neq 1, 2$ hence $[K : L] = 4$. $\square$

Corollary 4.10. *One has*

- i. *in the setting of Lemma 4.2, $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = 48$ and $\text{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}) \simeq \text{GL}_2(\mathbb{Z}/3\mathbb{Z})$;*
- ii. *in the setting of Corollary 4.3, $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = 16$ and $\text{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}) \simeq SD_8$.*

Proof. Part i is a direct consequence of Lemmas 4.2 and 4.9 and the fact that $|\text{GL}_2(\mathbb{Z}/3\mathbb{Z})| = 48$. Part ii follows from Corollary 4.3 and Lemma 4.9. The Galois group is a 2-Sylow subgroup of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$, hence it is conjugated (and isomorphic) to SD_8 , the 2-Sylow appearing in Theorem 3.1 (and computed in Appendix A). $\square$

With the next (final) lemma, we will investigate the case when Δ is the cube of a rational number and $(-\sqrt[3]{\Delta} - 4b)/3$ is a nonzero rational square.

Lemma 4.11. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where c is a nonzero rational number. Suppose that $\Delta \in (\mathbb{Q}^*)^3$ and that $(-\sqrt[3]{\Delta} - 4b)/3 \in (\mathbb{Q}^*)^2$. Then we have $\mathbb{Q}(\mathcal{E}_x[3]) = \mathbb{Q}(\zeta_3, \sqrt{\gamma})$ and $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = 2, 4$ or 8 with Galois groups $\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$ or D_4 respectively.*

Proof. Let $\Delta = h^3$ and $(-h - 4b)/3 = \ell^2$ with $h, \ell \in \mathbb{Q}^*$ (note that $\ell \neq 0$ because of the hypothesis $c \neq 0$). From the explicit expressions of the x_i 's it is easy to see that $\mathbb{Q}(\mathcal{E}_x[3]) = \mathbb{Q}(\sqrt{\gamma}, \sqrt{\gamma'})$ (with our usual notations for γ and γ'). Moreover we know that $\zeta_3 \in \mathbb{Q}(\mathcal{E}_x[3])$,

hence $[\mathbb{Q}(\mathcal{E}_x[3]) : \mathbb{Q}] \in \{2, 4\}$.

If $[\mathbb{Q}(\mathcal{E}_x[3]) : \mathbb{Q}] = 2$ then $\mathbb{Q}(\mathcal{E}_x[3]) = \mathbb{Q}(\zeta_3)$ and $\mathcal{E}$ belongs to the family

$$(13) \quad \mathcal{F}_{\alpha, \beta} : \quad y^2 = x^3 + (-3m^2 + 6\beta m)x + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m ,$$

with $\alpha, \beta, m \in \mathbb{Q}$, $\beta \neq 0$ and $m^2 = \alpha^2 + 3\beta^2$ (see [10]). In this case one has $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3, \sqrt{-2(\alpha + m)})$ and therefore

$$[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = \begin{cases} 2 & \text{if } -2(\alpha + m) \equiv 1, -3 \pmod{(\mathbb{Q}^*)^2} \\ 4 & \text{otherwise} \end{cases} ,$$

with Galois groups isomorphic to $(\mathbb{Z}/2\mathbb{Z})^i$, $i = 1, 2$. We remark that in the already cited [10] one finds that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ only for the curves of the following family

$$(14) \quad \mathcal{F}_{\beta, \tilde{h}} : \quad y^2 = x^3 + b_{\beta, \tilde{h}}x + c_{\beta, \tilde{h}} \quad \beta, \tilde{h} \in \mathbb{Q}^* ,$$

with

$$b_{\beta, \tilde{h}} = -27\frac{\beta^4}{\tilde{h}^4} + 18\frac{\beta^3}{\tilde{h}^2} - 9\frac{\beta^2}{2} + 3\frac{\beta\tilde{h}^2}{2} - 3\frac{\tilde{h}^4}{16}$$

and

$$c_{\beta, \tilde{h}} = 54\frac{\beta^6}{\tilde{h}^6} - 54\frac{\beta^5}{\tilde{h}^4} + 45\frac{\beta^4}{2\tilde{h}^2} - 15\frac{\beta^2\tilde{h}^2}{8} - 3\frac{\beta\tilde{h}^4}{8} - \frac{1}{32\tilde{h}^6} .$$

Now we assume that $[\mathbb{Q}(\mathcal{E}_x[3]) : \mathbb{Q}] = 4$, so that $\mathbb{Q}(\mathcal{E}_x[3]) = \mathbb{Q}(\sqrt{\gamma}, \sqrt{\gamma'}) = \mathbb{Q}(\sqrt{\gamma}, \zeta_3)$. Noting that $\gamma = -\ell^2 - 4b - \frac{8c}{\ell}$ one easily computes

$$y_1 = \frac{1}{2}\sqrt{-\ell^3 - 8b\ell - 16c + \left(-\ell^2 + \frac{4c}{\ell}\right)\sqrt{\gamma}} .$$

Thus

$$[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = \begin{cases} 4 & \text{if } -\ell^3 - 8b\ell - 16c + \left(-\ell^2 + \frac{4c}{\ell}\right)\sqrt{\gamma} \in \mathbb{Q}(\sqrt{\gamma}, \zeta_3)^2 \\ 8 & \text{otherwise} \end{cases}$$

and the Galois groups are $(\mathbb{Z}/2\mathbb{Z})^2$ or D_4 . The D_4 case comes from the fact that when $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = 8$ one has $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3, y_1)$ and the Galois group is generated by

$$\varphi \begin{cases} y_1 \mapsto \frac{1}{2}\sqrt{-\ell^3 - 8b\ell - 16c - \left(-\ell^2 + \frac{4c}{\ell}\right)\sqrt{\gamma}} \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{cases} \quad \text{and} \quad \psi \begin{cases} y_1 \mapsto y_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{cases} .$$

□

Remark 4.12. *The case $b = 0$.*

If $b = 0$, then $\mathbb{Q}(\sqrt[3]{\Delta}) = \mathbb{Q}(\sqrt[3]{2c^2})$ and

$$\frac{-\sqrt[3]{\Delta} - 4b}{3} = 2\sqrt[3]{2c^2} = \left(\pm\sqrt[3]{4c}\right)^2 \in \mathbb{Q}(\sqrt[3]{\Delta})^2 .$$

Then the curves $\mathcal{E} : y^2 = x^3 + c$ have the features of the cases treated in Lemma 4.5 and Lemma 4.11 (a little shift in the notations has to be taken into account: when $b = 0$ the $\tilde{x}_1 = 0$ of Theorem 3.2 is represented by the “general” x_3). We have already observed that $\Delta \in (\mathbb{Q}^*)^3$ if and only if $c \equiv 2 \pmod{(\mathbb{Q}^*)^3}$, if this is not the case then we have the description given in Lemma 4.5. Otherwise $\mathcal{E} : y^2 = x^3 + 2h^3$, with $h \in \mathbb{Q}^*$. Then $(-\sqrt[3]{\Delta} - 4b)/3 = 576h^6$ is a rational square and we are in the situation described by Lemma 4.11.

Remark 4.13. *No elliptic curves with $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}] = 24$.*

Since $[K : L] \in \{1, 2, 4\}$ and $[L : \mathbb{Q}] \mid 12$ (see Section 3), we only have the following possibilities:

- i) $[L : \mathbb{Q}] = 12$ and $[K : L] = 2$,
- ii) $[L : \mathbb{Q}] = 6$ and $[K : L] = 4$.

We have proved that $[L : \mathbb{Q}] = 12$ only when $\Delta \notin (\mathbb{Q}^*)^3$ and $(-\sqrt[3]{\Delta} - 4b)/3 \notin \mathbb{Q}(\sqrt[3]{\Delta})^2$. By Lemma 4.9, under those hypotheses we have $[K : L] = 4$ and $[K : \mathbb{Q}] = 48$ (see Corollary 4.10). So i) is impossible. We have also proved that $[L : \mathbb{Q}]$ can be 6 only when $\mathcal{E}$ belongs to the families of Lemma 4.5. But then we have $[K : L] \in \{1, 2\}$ and ii) is impossible too.

We can now conclude with a brief summary on how the previous Lemmas provide the proof of the various cases stated in Theorem 4.1 (for each case we point out an example as well).

Proof. (**Theorem 4.1**)

1. See Lemma 4.2, Lemma 4.9 and Corollary 4.10. An example of an elliptic curve with the features of that case is $y^2 = x^3 + x + 1$, with $b = c = 1$.
2. See Corollary 4.3, Lemma 4.9 and Corollary 4.10. An example of an elliptic curve with those properties is

$$y^2 = x^3 - \frac{1}{3}x + \frac{2}{9}.$$

In fact, we have $\Delta = (-8/3)^3$ and $(\sqrt[3]{\Delta} - 4b)/3 = 4/3$. In this case $t = \frac{2\sqrt{-2\sqrt{3}}}{3}$ and

$$\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}\left(\sqrt{-2\sqrt{3}}, \zeta_3, \sqrt{-\zeta_3\sqrt{-2\sqrt{3}} - 3}\right).$$

3. See Lemma 4.5. An example of an elliptic curve with those properties and $d = 6$ is the curve $y^2 = x^3 + x - 74/9$, obtained by choosing $b = 1$ and $a_0 = 2$. In fact, we have $\sqrt[3]{\Delta} = \sqrt[3]{20/3}$ and $y_1 = \sqrt{2a_0} = 2$. An example of an elliptic curve with those properties and $d = 12$ is the curve, $y^2 = x^3 + x - 443/288$, obtained by choosing $b = 1$ and $a_0 = 1$. In fact, we have $\sqrt[3]{\Delta} = \sqrt[3]{1/3}$ and $y_1 = \sqrt{2a_0} = \sqrt{2}$. As already remarked, other examples are the curves of the family $y^2 = x^3 + c$, with $c \neq 2\ell^3$, for all $\ell \in \mathbb{Q}^*$. The curves $y^2 = x^3 + 3$ and $y^2 = x^3 + 1$ belongs to that family and give, respectively, $d = 12$ and $d = 6$.
4. See Lemma 4.11. For the cases $d = 2, 4$ we can find examples among the curves with $b = 0$: just take $y^2 = x^3 + 2$ for $d = 4$ and $y^2 = x^3 + 16$ for $d = 2$. For $d = 8$ consider the curve $y^2 = x^3 - \frac{3}{2}x + 1$. One gets $\Delta = -6^3 = h^3$ and $(-h - 4b)/3 = 4 = \ell^2$. With $\ell = 2$ one finds $\gamma = -2$ (note that $\ell = -2$ provides $\gamma = 6 = (-3)(-2)$) and $y_1 = \sqrt{-2\sqrt{-2}}$ which is easily seen not to be a square in $\mathbb{Q}(\sqrt{-2}, \zeta_3)$.
5. As we have already remarked, this case is equivalent to the case when $c = 0$. For the proof see Lemma 3.1. The examples are the curves of the family $y^2 = x^3 + bx$.

□

5. REMARKS ON MODULAR CURVES

The results of the previous sections provide informations on rational points of classical modular curves. There is a vast literature on modular curves so here we simply recall the basic definitions and properties we are interested in; more details can be found, for example, in [6], [7] and [14].

Let $\mathcal{H} = \{z \in \mathbb{C} : \text{Im } z > 0\}$ be the complex upper half plane and consider the action of $\text{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ given by the Möbius transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}.$$

The *principal congruence group of level N* is the set

$$\Gamma(N) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

A congruence group in $\mathrm{SL}_2(\mathbb{Z})$ is any subgroup containing $\Gamma(N)$ for some N (if N is minimal then the congruence group is said to be *of level N*). For any congruence subgroup Γ one defines Y_Γ to be the quotient of $\mathcal{H}$ by the action of Γ , equipped with the analytic structure induced by $\mathcal{H}$. Then Y_Γ is a Riemann surface and it can be compactified by adjoining a finite set of (rational) points corresponding to the orbits of $\mathbb{P}^1(\mathbb{Q})$ under Γ (the *cusps*). This compactification is the modular curve associated to Γ and will be denoted by X_Γ .

The main examples of congruence groups (together with $\Gamma(N)$ itself) are:

$$\Gamma_1(N) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

and

$$\Gamma_0(N) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

Those are all of level N and the corresponding modular curves will be denoted, respectively, by $X_1(N)$ and $X_0(N)$ (we write $X(N)$ for the modular curve associated to $\Gamma(N)$).

The modular curves $X(N)$, $X_1(N)$ and $X_0(N)$ parametrize families of elliptic curves with some extra *level N structure* via their moduli interpretation. Namely

- non cuspidal points in $X(N)$ correspond to triples $(\mathcal{E}, P, Q)$ where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and P, Q are points of order N generating the whole group $\mathcal{E}[N]$;
- non cuspidal points in $X_1(N)$ correspond to couples $(\mathcal{E}, P)$ where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and P is a point of order N ;
- non cuspidal points in $X_0(N)$ correspond to couples $(\mathcal{E}, C_N)$ where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and C_N is a cyclic subgroup of $\mathcal{E}[N]$ of order N ,

(all these correspondences have to be considered modulo the natural isomorphisms).

Let K be a number field, the points of a modular curve X_Γ which are rational over K will be denoted by $X_\Gamma(K)$. Obviously a point is in $X_\Gamma(K)$ (i.e., is *defined over K*) if and only if it is $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ -invariant (so that, in particular, with the representation provided above one needs an elliptic curve $\mathcal{E}$ defined over K). The $\mathbb{Q}$ -rational points of modular curves have been studied quite extensively since the pioneering work of B. Mazur (see [8], [9], [13] and many others): for example $X_0(3)(\mathbb{Q})$ is known to be infinite but, in general, the sets $X_0(N)(\mathbb{Q})$ and $X_1(N)$ are finite (almost always equal to the set of rational cusps).

Now, with this basic definitions and the results of the previous sections, we look for non cuspidal rational points in the modular curves $X(3)$, $X_1(3)$ and $X_0(3)$.

We shall study the cases listed in Theorem 4.1, providing the minimal degree for the fields K_0 (resp. K_1) over which the elliptic curve $\mathcal{E}$ defines a point in $X_0(3)$ (resp. $X_1(3)$). We recall the following easy result.

Lemma 5.1. *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{Q}$, let $P = (x_P, y_P)$ be a point of order 3 and let $\langle P \rangle$ the subgroup generated by P . Then*

- the couple $(\mathcal{E}, \langle P \rangle)$ defines a point in $X_0(3)(K) \iff K \supseteq \mathbb{Q}(x_P)$;*
- the couple $(\mathcal{E}, P)$ defines a point in $X_1(3)(K) \iff K \supseteq \mathbb{Q}(P)$;*
- $[K_0 : \mathbb{Q}] \leq [K_1 : \mathbb{Q}] \leq 2[K_0 : \mathbb{Q}]$.*

Proof. Everything is straightforward observing that, since $-P = (x_P, -y_P)$ and y_P is at most quadratic over $\mathbb{Q}(x_P)$, the set $\langle P \rangle = \{O, P, -P\}$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(x_P))$ -invariant and $K_1 = K_0(y_P)$. $\square$

Now we proceed case by case.

Case 1: Δ is not the cube of a rational number, and $(-\sqrt[3]{\Delta} - 4b)/3$ is not a square in $\mathbb{Q}(\sqrt[3]{\Delta})$. Then $\sqrt{-\frac{\sqrt[3]{\Delta}-4b}{3}}$ has degree 6 over $\mathbb{Q}$ and, by Remark 4.4, $x_i \notin \mathbb{Q}\left(\sqrt{-\frac{\sqrt[3]{\Delta}-4b}{3}}\right)$ for any i : therefore these curves define points in $X_0(3)(K_0)$ with $[K_0 : \mathbb{Q}] = 12$. Moreover, by Lemma 4.9, y_1 (and y_2) have degree 2 over $\mathbb{Q}(\mathcal{E}_x[3])$; hence $[K_1 : \mathbb{Q}] = 24$.

Case 2: Δ is the cube of a rational number, and $(-\sqrt[3]{\Delta} - 4b)/3$ is not a rational square. By Corollary 4.3 one has that $[K_0 : \mathbb{Q}] = 4$ and, as above, Lemma 4.9 shows that $[K_1 : \mathbb{Q}] = 8$.

Case 3: Δ is not the cube of a rational number, and $(-\sqrt[3]{\Delta} - 4b)/3$ is a square in $\mathbb{Q}(\sqrt[3]{\Delta})$. The curves of the family

$$\mathcal{F}_{b,a_0} : y^2 = x^3 + bx + \frac{16b^2 - 216a_0^2b - 243a_0^4}{288a_0}$$

$(b, a_0 \in \mathbb{Q}^*)$ have a point of order 3 with abscissa $3a_0/2$ (see Lemma 4.5), whose ordinate is $\frac{4b+27a_0^2}{12\sqrt{2a_0}}$. Therefore $K_0 = \mathbb{Q}$ and

$$[K_1 : \mathbb{Q}] = \begin{cases} 1 & \text{if } a_0 \equiv 2 \pmod{(\mathbb{Q}^*)^2} \\ 2 & \text{otherwise} \end{cases}.$$

The other family

$$\mathcal{F}_c : y^2 = x^3 + c,$$

$(c \neq 0 \text{ and } c \not\equiv 2 \pmod{(\mathbb{Q}^*)^3})$ behaves in a similar way. We always have a $\mathbb{Q}$ -rational subgroup of order 3, namely $\{O, (0, \sqrt{c}), (0, -\sqrt{c})\}$ (see Theorem 3.2), so that $K_0 = \mathbb{Q}$. Finally

$$[K_1 : \mathbb{Q}] = \begin{cases} 1 & \text{if } c \equiv 1 \pmod{(\mathbb{Q}^*)^2} \\ 2 & \text{otherwise} \end{cases}.$$

Case 4: $\Delta = h^3$ and $(-h - 4b)/3 = \ell^2$ for some $h, \ell \in \mathbb{Q}^*$.

As seen in Lemma 4.11, $\mathbb{Q}(\mathcal{E}_x[3])$ has degree 2 or 4 and is generated by $\sqrt{\gamma}$ and $\sqrt{\gamma'}$ (which, summed with a rational, are the abscissas of the 3-torsion points). Therefore one has a rational abscissa if and only if $\mathbb{Q}(\mathcal{E}_x[3])$ has degree 2, i.e., if and only if the curve belongs to the family

$$\mathcal{F}_{\alpha,\beta} : y^2 = x^3 + (-3m^2 + 6\beta m)x + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m,$$

with $\alpha, \beta, m \in \mathbb{Q}$, $\beta \neq 0$ and $m^2 = \alpha^2 + 3\beta^2$. In all other cases $[K_0 : \mathbb{Q}] = 2$.

With the notations of Lemma 4.11 one has that

$$[K_1 : \mathbb{Q}] = \begin{cases} [K_0 : \mathbb{Q}] & \text{if } \sqrt{-\ell^3 - 8b\ell - 16c + (-\ell^2 + \frac{4c}{\ell})\sqrt{\gamma}} \in \mathbb{Q}(\sqrt{\gamma})^2 \\ 2[K_0 : \mathbb{Q}] & \text{otherwise} \end{cases}.$$

Case 5: $\Delta = h^3$, with $h \in \mathbb{Q}$, and $-h - 4b = 0$, i.e., $c = 0$.

In the proof of Theorem 3.1 we showed that $[K_0 : \mathbb{Q}] = 4$ and that $\hat{y}_i$ does not belong to $\mathbb{Q}(\mathcal{E}_x[3])$: hence $[K_1 : \mathbb{Q}] = 8$.

We summarize the results (and extend them to $X(3)$) in the following

Theorem 5.2. *An elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}$ provides a non cuspidal rational point in $X_0(3)(\mathbb{Q})$ if and only if*

- it belongs to the family

$$\mathbf{A1}: y^2 = x^3 + bx + \frac{16b^2 - 216a_0^2b - 243a_0^4}{288a_0}$$

$(b, a_0 \in \mathbb{Q}^*)$;

- or it belongs to the family

$$\mathbf{A2}: y^2 = x^3 + c;$$

- or it belongs to the family

$$\mathbf{A3}: y^2 = x^3 + (-3m^2 + 6\beta m)x + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m,$$

with $\alpha, \beta, m \in \mathbb{Q}$, $\beta \neq 0$ and $m^2 = \alpha^2 + 3\beta^2$.

An elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}$ provides a non cuspidal rational point in $X_1(3)(\mathbb{Q})$ if and only if

- it belongs to the family **A1** with $a_0 \equiv 2 \pmod{(\mathbb{Q}^*)^2}$;
- or it belongs to the family **A2** with $c \equiv 1 \pmod{(\mathbb{Q}^*)^2}$;
- or it belongs to the family **A3** and

$$\gamma, -\ell^3 - 8b\ell - 16c + \left(-\ell^2 + \frac{4c}{\ell}\right) \sqrt{\gamma} \in (\mathbb{Q}^*)^2$$

or

$$\gamma', -\ell^3 - 8b\ell - 16c + \left(-\ell^2 + \frac{4c}{\ell}\right) \sqrt{\gamma'} \in (\mathbb{Q}^*)^2.$$

An elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}$ provides a non cuspidal rational point in $X(3)(\mathbb{Q})$ if and only if

- it belongs to the family **A2** with $c \equiv 1 \pmod{(\mathbb{Q}^*)^2}$ and $c \equiv 2 \pmod{(\mathbb{Q}^*)^3}$;
- it belongs to the family

$$\mathbf{A4}: y^2 = x^3 + b_{\beta, \tilde{h}}x + c_{\beta, \tilde{h}}$$

described in (14) of Lemma 4.11.

Proof. The results for $X_0(3)$ and $X_1(3)$ are in the above case by case analysis. Because of the natural projections $X(N) \rightarrow X_1(N) \rightarrow X_0(N)$ (coming from the inclusions $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$) we look for points in $X(3)(\mathbb{Q})$ only among the curves with $K_1 = \mathbb{Q}$, i.e., the ones providing points in $X_1(3)(\mathbb{Q})$. Note that if one has a rational point P of order 3, then P cannot be a part of a rational triple $(\mathcal{E}, P_1, P_2)$ (with $\langle P_1, P_2 \rangle = \mathcal{E}[3]$) because there is no elliptic curve with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}$. Therefore we have to find non rational points P_1 and P_2 which are permuted by the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

By Lemma 4.5 no curve of the family **A1** can provide such points.

For the curves $y^2 = x^3 + c$ with $c \equiv 1 \pmod{(\mathbb{Q}^*)^2}$ and $c \equiv 2 \pmod{(\mathbb{Q}^*)^3}$ one has $(\mathcal{E}, (\zeta_3 \sqrt[3]{-4c}, \sqrt{-3c}), (\zeta_3^2 \sqrt[3]{-4c}, -\sqrt{-3c})) \in X(3)(\mathbb{Q})$.

For the remaining case assume that $\gamma \in (\mathbb{Q}^*)^2$ so that, since $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\mathcal{E}_x[3]) = \mathbb{Q}(\sqrt{\gamma}, \sqrt{\gamma'})$, one has $\gamma' \equiv -3 \pmod{(\mathbb{Q}^*)^2}$. The points with non rational abscissas are $x_3 = \frac{1}{2}(\ell - \sqrt{\gamma'})$ and $x_4 = \frac{1}{2}(\ell + \sqrt{\gamma'})$ and are permuted by $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The corresponding ordinates are (we only consider the positive ones since the sign is not important here)

$$y_3 = \sqrt{\ell^3 + 3\ell\gamma' + b\ell + c - (3\ell^2 + \gamma' + b)\sqrt{\gamma'}}, y_4 = \sqrt{\ell^3 + 3\ell\gamma' + b\ell + c + (3\ell^2 + \gamma' + b)\sqrt{\gamma'}}$$

and they are permuted by $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ only if

$$\ell^3 + 3\ell\gamma' + b\ell + c - (3\ell^2 + \gamma' + b)\sqrt{\gamma'} \in \mathbb{Q}(\sqrt{\gamma'})^2.$$

Note that this final case gives $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\sqrt{\gamma'}) = \mathbb{Q}(\zeta_3)$, so these curves are exactly the ones of the family **A4**. We remark that the curves $y^2 = x^3 + c$, with $c \equiv 1 \pmod{(\mathbb{Q}^*)^2}$ and

$c \equiv 2 \pmod{(\mathbb{Q}^*)^3}$, are included in the family **A4**, we kept the cases separated (and omitted the usual “or” in the statement) to maintain some symmetry with the previous cases and to provide an easy example. $\square$

Remark 5.3. As is well known the presence of a rational subgroup C_3 of order 3 in $\mathcal{E}[3]$ is equivalent to the existence of a rational isogeny $\varphi : \mathcal{E} \rightarrow \mathcal{E}'$ whose kernel is exactly C_3 . This isogeny can be useful to approach various questions. For example in descent procedures to compute 3-Selmer groups and the 3-part of the Tate-Shafarevich group (some computations of this kind for the curves $y^2 = x^3 + c$ are provided in [2] and [3]). Another example is the local global problem: in [5] the authors prove that if there is no K -rational 3-isogeny for $\mathcal{E}$, then the local global divisibility problem (for $p=3$) has an affirmative answer (see the lines immediately below the statement of [5, Theorem 1]). Therefore the local global divisibility holds for $p=3$ over $\mathbb{Q}$ for all the curves not included in the families **A1**, **A2** and **A3** of Theorem 5.2 and, looking at the fields K_0 described above, one can find many more examples of this phenomenon. The same conclusions and many generalizations arise also from [11] and [12]; in particular, [12, Theorem 10] assures that the local global divisibility holds for $p=3$ over $\mathbb{Q}$ for all the curves not included in the family **A4**.

APPENDIX A. GALOIS GROUP FOR $c = 0$

We maintain the notations of Section 3, in particular of Theorem 3.1. Recall that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\hat{y}_1, \zeta_3)$, so we are basically looking for the Galois group of the splitting field of the minimal polynomial of $\hat{y}_1$ which is $X^8 + \frac{8b^3}{3}X^4 - \frac{16b^6}{27}$. From the generators given in Theorem 3.1 it is easy to compute the elements of the group $\text{Gal}(\mathbb{Q}(\mathcal{E}_x[3])/\mathbb{Q})$: one has

$$\begin{aligned} \varphi_1 &= id & \varphi_5 &\begin{cases} \hat{x}_1 \mapsto \hat{x}_3 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{cases} \\ \varphi_2 &\begin{cases} \hat{x}_1 \mapsto \hat{x}_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{cases} & \varphi_6 &\begin{cases} \hat{x}_1 \mapsto \hat{x}_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{cases} \\ \varphi_3 &\begin{cases} \hat{x}_1 \mapsto \hat{x}_2 = -\hat{x}_1 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{cases} & \varphi_7 &\begin{cases} \hat{x}_1 \mapsto \hat{x}_4 = -\hat{x}_3 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{cases} \\ \varphi_4 &\begin{cases} \hat{x}_1 \mapsto \hat{x}_2 = -\hat{x}_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{cases} & \varphi_8 &\begin{cases} \hat{x}_1 \mapsto -\hat{x}_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{cases} \end{aligned}$$

(the φ and ψ of Theorem 3.1 correspond to φ_6 and φ_2 respectively) with $\varphi_2\varphi_6\varphi_2 = \varphi_8 = \varphi_6^3$. Using the equations

$$\hat{x}_1\hat{x}_3 = \frac{b}{3}\sqrt{-3} \quad ; \quad \hat{x}_1^2 - \hat{x}_3^2 = -\frac{4b}{3}\sqrt{3} \quad ; \quad i = \frac{\sqrt{3}\sqrt{-3}}{3}$$

one computes

$$(15) \quad \varphi_1(\hat{x}_3) = \varphi_4(\hat{x}_3) = \hat{x}_3 \quad ; \quad \varphi_2(\hat{x}_3) = \varphi_2(\hat{x}_3) = \hat{x}_4 = -\hat{x}_3 ;$$

$$(16) \quad \varphi_5(\hat{x}_3) = \varphi_8(\hat{x}_3) = \hat{x}_1 \quad ; \quad \varphi_6(\hat{x}_3) = \varphi_7(\hat{x}_3) = \hat{x}_2 = -\hat{x}_1 ,$$

and

$$(17) \quad \varphi_1(i) = \varphi_3(i) = \varphi_6(i) = \varphi_8(i) = i \quad ; \quad \varphi_2(i) = \varphi_4(i) = \varphi_5(i) = \varphi_7(i) = -i .$$

We write down the elements of $\text{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q})$ according to their restriction to $\mathbb{Q}(\mathcal{E}_x[3])/\mathbb{Q}$, i.e., providing $2 = [\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}(\mathcal{E}_x[3])]$ extensions to any of the previous φ_j 's. Here they are

$$\begin{array}{ll}
\varphi_1 \left\{ \begin{array}{l} \varphi_{1,1} = id \\ \varphi_{1,2} \left\{ \begin{array}{l} \hat{y}_1 \mapsto -\hat{y}_1 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{array} \right. \end{array} \right. & \varphi_5 \left\{ \begin{array}{l} \varphi_{5,1} \left\{ \begin{array}{l} \hat{y}_1 \mapsto \hat{y}_3 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{array} \right. \\ \varphi_{5,2} \left\{ \begin{array}{l} \hat{y}_1 \mapsto -\hat{y}_3 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{array} \right. \end{array} \right. \\
\varphi_2 \left\{ \begin{array}{l} \varphi_{2,1} \left\{ \begin{array}{l} \hat{y}_1 \mapsto \hat{y}_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \\ \varphi_{2,2} \left\{ \begin{array}{l} \hat{y}_1 \mapsto -\hat{y}_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \end{array} \right. & \varphi_6 \left\{ \begin{array}{l} \varphi_{6,1} \left\{ \begin{array}{l} \hat{y}_1 \mapsto \hat{y}_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \\ \varphi_{6,2} \left\{ \begin{array}{l} \hat{y}_1 \mapsto -\hat{y}_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \end{array} \right. \\
\varphi_3 \left\{ \begin{array}{l} \varphi_{3,1} \left\{ \begin{array}{l} \hat{y}_1 \mapsto \hat{y}_2 = i\hat{y}_1 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{array} \right. \\ \varphi_{3,2} \left\{ \begin{array}{l} \hat{y}_1 \mapsto -\hat{y}_2 = -i\hat{y}_1 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{array} \right. \end{array} \right. & \varphi_7 \left\{ \begin{array}{l} \varphi_{7,1} \left\{ \begin{array}{l} \hat{y}_1 \mapsto \hat{y}_4 = i\hat{y}_3 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{array} \right. \\ \varphi_{7,2} \left\{ \begin{array}{l} \hat{y}_1 \mapsto -\hat{y}_4 = -i\hat{y}_3 \\ \sqrt{-3} \mapsto \sqrt{-3} \end{array} \right. \end{array} \right. \\
\varphi_4 \left\{ \begin{array}{l} \varphi_{4,1} \left\{ \begin{array}{l} \hat{y}_1 \mapsto \hat{y}_2 = i\hat{y}_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \\ \varphi_{4,2} \left\{ \begin{array}{l} \hat{y}_1 \mapsto -\hat{y}_2 = -i\hat{y}_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \end{array} \right. & \varphi_8 \left\{ \begin{array}{l} \varphi_{8,1} \left\{ \begin{array}{l} \hat{y}_1 \mapsto \hat{y}_4 = i\hat{y}_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \\ \varphi_{8,2} \left\{ \begin{array}{l} \hat{y}_1 \mapsto -\hat{y}_4 = -i\hat{y}_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{array} \right. \end{array} \right.
\end{array}$$

(note that $\varphi_j(\hat{x}_1) = \hat{x}_k$ yields $\varphi_j(\hat{y}_1^2) = \hat{y}_k^2$ which gives the two extensions $\varphi_{j,h}(\hat{y}_1) = \pm \hat{y}_k$, $h = 1, 2$). Since the image of $\hat{y}_3$ depends on the image of $\hat{x}_3$, from equations (15) and (16), one gets

$$\begin{aligned}
\varphi_{1,h}(\hat{y}_3) &= \pm \hat{y}_3 ; \varphi_{2,h}(\hat{y}_3) = \pm i\hat{y}_3 ; \varphi_{3,h}(\hat{y}_3) = \pm i\hat{y}_3 ; \varphi_{4,h}(\hat{y}_3) = \pm \hat{y}_3 ; \\
\varphi_{5,h}(\hat{y}_3) &= \pm \hat{y}_1 ; \varphi_{6,h}(\hat{y}_3) = \pm i\hat{y}_1 ; \varphi_{7,h}(\hat{y}_3) = \pm i\hat{y}_1 ; \varphi_{8,h}(\hat{y}_3) = \pm \hat{y}_1 .
\end{aligned}$$

With these informations it is easy to check the orders of some elements:

$$o(\varphi_{1,1}) = 1 ; o(\varphi_{1,2}) = o(\varphi_{2,1}) = o(\varphi_{2,2}) = 2 ; o(\varphi_{3,1}) = o(\varphi_{3,2}) = 4 .$$

Moreover the elements $\varphi_{6,1}$ has order 8 and it generates the subgroup

$$\langle \varphi_{6,1} \rangle = \{ \varphi_{1,1}, \varphi_{6,1}, \varphi_{3,1}, \varphi_{8,1}, \varphi_{1,2}, \varphi_{6,2}, \varphi_{3,2}, \varphi_{8,2} \}$$

where $o(\varphi_{6,2}) = o(\varphi_{8,1}) = o(\varphi_{8,2}) = 8$ (the ambiguity on the sign of $\varphi_{6,1}(\hat{y}_3)$ does not alter these results). Looking at the non abelian groups of order 16, there are only two of them with this type of elements: D_8 (dihedral) and SD_8 (semidihedral). To choose between them one has to compute the orders of $\varphi_{5,h}$ and $\varphi_{7,h}$ ($h = 1, 2$) but here the ambiguity on the sign of $\varphi_{5,h}(\hat{y}_3)$ and $\varphi_{7,h}(\hat{y}_3)$ allows them to have order 2 or 4: if they are all of order 2 we have D_8

otherwise they are all of order 4 and we get SD_8 .

Assume, for example, that $o(\varphi_{7,1}) = 2$: this comes from the choice $\varphi_{7,1}(\widehat{y}_3) = i\widehat{y}_1$. Then (recalling also equations (17))

$$\varphi_{7,1}(\widehat{y}_1 + i\widehat{y}_3) = i\widehat{y}_3 + \widehat{y}_1.$$

Moreover

$$\widehat{y}_1 + i\widehat{y}_3 = \left(\sqrt{-\frac{2b}{3}\sqrt{3}} \right) (\sqrt{\widehat{x}_1} + \sqrt{\widehat{x}_3}).$$

Using the equations

$$\widehat{y}_1 = \sqrt{-\frac{2b}{3}\widehat{x}_1\sqrt{3}} \quad \text{and} \quad \widehat{y}_3 = \sqrt{\frac{2b}{3}\widehat{x}_3\sqrt{3}},$$

one computes

$$\begin{aligned} \varphi_{7,1}(\sqrt{\widehat{x}_1} + \sqrt{\widehat{x}_3}) &= \varphi_{7,1}(\widehat{y}_1)\varphi_{7,1}\left(\sqrt{-\frac{3}{2b\sqrt{3}}}\right) + \varphi_{7,1}(\widehat{y}_3)\varphi_{7,1}\left(\sqrt{\frac{3}{2b\sqrt{3}}}\right) \\ &= \varphi_{7,1}\left(\sqrt{\frac{3}{2b\sqrt{3}}}\right) [\varphi_{7,1}(\widehat{y}_1)\varphi_{7,1}(i) + \varphi_{7,1}(\widehat{y}_3)] \\ &= \varphi_{7,1}\left(\sqrt{\frac{3}{2b\sqrt{3}}}\right) [i\widehat{y}_3(-i) + i\widehat{y}_1] \\ &= \varphi_{7,1}\left(\sqrt{\frac{3}{2b\sqrt{3}}}\right) [(-i)(i\widehat{y}_3 - \widehat{y}_1)] \\ &= \varphi_{7,1}\left(\sqrt{\frac{3}{2b\sqrt{3}}}\right) [\varphi_{7,1}(i)(i\widehat{y}_3 - \widehat{y}_1)] \\ &= \varphi_{7,1}\left(\sqrt{-\frac{3}{2b\sqrt{3}}}\right) (i\widehat{y}_3 - \widehat{y}_1) \end{aligned}$$

But this yields

$$\begin{aligned} i\widehat{y}_3 - \widehat{y}_1 &= \varphi_{7,1}(\sqrt{\widehat{x}_1} + \sqrt{\widehat{x}_3})\varphi_{7,1}\left(\sqrt{-\frac{2b}{3}\sqrt{3}}\right) \\ &= \varphi_{7,1}\left((\sqrt{\widehat{x}_1} + \sqrt{\widehat{x}_3})\sqrt{-\frac{2b}{3}\sqrt{3}}\right) \\ &= \varphi_{7,1}(\widehat{y}_1 + i\widehat{y}_3) = i\widehat{y}_3 + \widehat{y}_1 \end{aligned},$$

which provides a contradiction.

Therefore $\varphi_{7,1}$ has order 4 and $\text{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}) \simeq SD_8$.

REFERENCES

- [1] C. ADELMANN, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, 1761. Springer-Verlag, Berlin, 2001.
- [2] A. BANDINI, *3-descent and the Birch and Swinnerton-Dyer conjecture*, Rocky Mt. J. Math **34** (2004), 13–27.
- [3] A. BANDINI, *3-Selmer groups for curves $y^2 = x^3 + a$* , Czechoslovak Math. J. **58** (2008), 429–445.
- [4] R. DVORNICICH - U. ZANNIER, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France **129**, no. 3 (2001), 317–338.
- [5] R. DVORNICICH - U. ZANNIER, *On a local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lond. Math. Soc. **39**, no. 1 (2007), 27–34.
- [6] N.M. KATZ - B. MAZUR, *Arithmetic moduli of elliptic curves*, Annals of Math. Studies **108**, Princeton Univ. Press, Princeton, 1985.
- [7] A.W. KNAPP, *Elliptic curves*, Princeton Univ. Press, Princeton, 1992.
- [8] B. MAZUR, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33–186.
- [9] B. MAZUR, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
- [10] L. PALADINO, *Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9*, J. Théor. Nombres Bordeaux, **22** no. 1 (2010), 139–160.
- [11] L. PALADINO, G. RANIERI, E. VIADA, *On Local-Global Divisibility by p^n in elliptic curves*, arXiv:1104.4762.

- [12] L. PALADINO, G. RANIERI, E. VIADA, *On the minimal set for counterexamples to the local-global principle*, arXiv:1107.3431.
- [13] J.P. SERRE, *Points rationnels des courbes modulaires $X_0(N)$* , Seminaire Bourbaki, Vol. 1977/78, Exposé No. 511, Lect. Notes Math. **710** (1979), 89–100.
- [14] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, 1971.
- [15] J.H. SILVERMAN, *The arithmetic of elliptic curves, 2nd edition*, **GTM 106** Springer-Verlag, Heidelberg, 2009.
- [16] J.H. SILVERMAN, J. TATE, *Rational points on elliptic curves*, Springer-Verlag, Heidelberg, 1992.

Andrea Bandini, e-mail: andrea.bandini@unipr.it
Dipartimento di Matematica - Università degli Studi di Parma
Parco Area delle Scienze, 53/A - 43124 Parma - Italy

Laura Paladino, e-mail: paladino@mat.unical.it
Dipartimento di Matematica - Università della Calabria
Ponte Pietro Bucci - Cubo 31 B - 87036 Arcavacata di Rende (CS) - Italy