ON THE DEGREE OF THE $p$-TORSION FIELD OF ELLIPTIC CURVES
OVER $\mathbb{Q}_\ell$ FOR $\ell \neq p$

NUNO FREITAS AND ALAIN KRAUS

Abstract. Let $\ell$ and $p \geq 3$ be distinct prime numbers. Let $E/\mathbb{Q}_\ell$ be an elliptic curve with $p$-torsion module $E_p$. Let $\mathbb{Q}_\ell(E_p)$ be the $p$-torsion field of $E$. We provide a complete description of the degree of the extension $\mathbb{Q}_\ell(E_p)/\mathbb{Q}_\ell$. As a consequence, we obtain a recipe to determine the discriminant ideal of the extension $\mathbb{Q}_\ell(E_p)/\mathbb{Q}_\ell$ in terms of standard information on $E$.

1. Introduction

Let $\ell$ and $p \geq 3$ be distinct prime numbers. Fix $\overline{\mathbb{Q}}_\ell$ an algebraic closure of $\mathbb{Q}_\ell$. Let $E/\mathbb{Q}_\ell$ be an elliptic curve with $p$-torsion module $E_p$. Let $\mathbb{Q}_\ell(E_p) \subset \overline{\mathbb{Q}}_\ell$ be the $p$-torsion field of $E$. The aim of this paper is to determine the degree $d$ of the extension $\mathbb{Q}_\ell(E_p)/\mathbb{Q}_\ell$.

Write $\pi$ for an uniformizer in $\mathbb{Q}_\ell(E_p)$ and $e$ for its ramification degree. The different ideal of $\mathbb{Q}_\ell(E_p)$ is $(\pi)$, where the integer $D$ is fully determined in [1]. The discriminant ideal $D$ of the extension $\mathbb{Q}_\ell(E_p)/\mathbb{Q}_\ell$ is generated by $\ell^{dD/e}$. The value of $e$ is given in [9] in terms of the standard invariants of a minimal Weierstrass model of $E$. Therefore, as a consequence of our results, we obtain a complete procedure to determine $D$ in terms of $\ell$, $p$ and invariants attached to $E$.

Part I. Statement of the results

Let $\ell$ and $p \geq 3$ be distinct prime numbers. Let $v$ be the valuation in $\mathbb{Q}_\ell$ such that $v(\ell) = 1$. Let $E/\mathbb{Q}_\ell$ be an elliptic curve and write $c_4$, $c_6$ and $\Delta$ for the standard invariants of a minimal Weierstrass model of $E/\mathbb{Q}_\ell$. Write $j = \frac{c_4}{c_6}$ for the modular invariant of $E$.

Write $E_p$ for the $p$-torsion module of $E$. Let $\mathbb{Q}_\ell(E_p) \subset \overline{\mathbb{Q}}_\ell$ be the $p$-torsion field of $E$ and denote by $d$ its degree

$$d = [\mathbb{Q}_\ell(E_p) : \mathbb{Q}_\ell].$$

Write $\mathbb{Q}_\ell^{\text{unr}}$ for the maximal unramified extension of $\mathbb{Q}_\ell$ contained in $\overline{\mathbb{Q}}_\ell$.

Let $r$ be the order of $\ell$ modulo $p$ and $\delta$ be the order of $-\ell$ modulo $p$.

Date: April 23, 2018.

2010 Mathematics Subject Classification. Primary 11G05.

Key words and phrases. Elliptic curves, $p$-torsion points, local fields.

The first-named author is supported by the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 747808 and the grant Proyecto RSME-FBBVA 2015 José Luis Rubio de Francia.
We will now state our results according to the type of reduction of $E$ and the prime $\ell$.

2. **The case of good reduction**

Let $M/\mathbb{Q}_\ell$ be a finite totally ramified extension and $E/M$ be an elliptic curve with good reduction. In this section we will write $d$ to denote $$d = [M(E_p) : M].$$

The residue field of $M$ is $\mathbb{F}_\ell$. Let $\tilde{E}/\mathbb{F}_\ell$ be the elliptic curve obtained from $E/M$ by reduction of a minimal model. Write $|\tilde{E}(\mathbb{F}_\ell)|$ for the order of its group of $\mathbb{F}_\ell$-rational points. Let $$a_E = \ell + 1 - |\tilde{E}(\mathbb{F}_\ell)| \quad \text{and} \quad \Delta_E = a_E^2 - 4\ell.$$ Note that the Weil bound implies $\Delta_E < 0$.

In the case of $E/M$ having good ordinary reduction i.e. $a_E \equiv 0 \pmod{\ell}$, the endomorphism ring of $\tilde{E}$ is isomorphic to an order of the imaginary quadratic field $\mathbb{Q}\left(\sqrt{\Delta_E}\right)$. The Frobenius endomorphism $\pi_{\tilde{E}}$ of $\tilde{E}$, generates a subring $\mathbb{Z}[\pi_{\tilde{E}}]$ of finite index of $\text{End}(\tilde{E})$. In this case, we define

$$b_E = \left[\text{End}(\tilde{E}) : \mathbb{Z}[\pi_{\tilde{E}}]\right].$$

The ratio $\frac{\Delta_E}{b_E}$ is the discriminant of $\text{End}(\tilde{E})$. The determination of $b_E$ has been implemented on Magma [11] by Centeleghe (cf. [2] and [3]). A method to obtain $b_E$ is also presented in [4].

Let $\alpha$ and $\beta$ be the roots in $\mathbb{F}_{p^2}$ of the polynomial in $\mathbb{F}_p[X]$ given by $$X^2 - a_E X + \ell \quad \pmod{p}.$$ 

**Theorem 1.** Let $n$ be the least common multiple of the orders of $\alpha$ and $\beta$ in $\mathbb{F}_{p^2}^\times$.

1) If $\Delta_E \not\equiv 0 \pmod{p}$, then $d = n$.

2) Suppose $\Delta_E \equiv 0 \pmod{p}$. Then $E/M$ has good ordinary reduction. We have $$d = \begin{cases} n & \text{if} \; b_E \equiv 0 \pmod{p}, \\ np & \text{otherwise}. \end{cases}$$

**Corollary 1.** Suppose $a_E = 0$. Then $d = 2\delta$.

3. **The case of multiplicative reduction**

Let $E/\mathbb{Q}_\ell$ be an elliptic curve with multiplicative reduction. In this case, we have $v(c_6) = 0$ and the Legendre symbol $\left(\frac{c_6}{\ell}\right) = \pm 1$. Let $$\tilde{j} = \frac{j}{L(2)}. $$

**Theorem 2.** We are in one of the following cases.

1) Suppose $\ell \geq 3$ and $\left(\frac{c_6}{\ell}\right) = 1$, or $\ell = 2$ and $c_6 \equiv 7 \pmod{8}$. 

1.1) If $\ell \not\equiv 1 \pmod{p}$, then
\[ d = \begin{cases} r & \text{if } v(j) \equiv 0 \pmod{p}, \\ pr & \text{otherwise}. \end{cases} \]

1.2) If $\ell \equiv 1 \pmod{p}$, then
\[ d = \begin{cases} 1 & \text{if } v(j) \equiv 0 \pmod{p} \text{ and } \frac{-\ell+1}{j^r} \equiv 1 \pmod{\ell}, \\ p & \text{otherwise}. \end{cases} \]

2) Suppose $\ell \geq 3$ and $\left(\frac{-c_6}{\ell}\right) = -1$, or $\ell = 2$ and $c_6 \not\equiv 7 \pmod{8}$.

2.1) If $r$ is even, then
\[ d = \begin{cases} r & \text{if } v(j) \equiv 0 \pmod{p}, \\ pr & \text{otherwise}. \end{cases} \]

2.2) Suppose $r$ odd.

2.2.1) If $\ell \not\equiv 1 \pmod{p}$, then
\[ d = \begin{cases} 2r & \text{if } v(j) \equiv 0 \pmod{p}, \\ 2pr & \text{otherwise}. \end{cases} \]

2.2.2) If $\ell \equiv 1 \pmod{p}$, then
\[ d = \begin{cases} 2 & \text{if } v(j) \equiv 0 \pmod{p} \text{ and } \frac{-\ell+1}{j^r} \equiv 1 \pmod{\ell}, \\ 2p & \text{otherwise}. \end{cases} \]

4. The case of additive potentially multiplicative reduction

Let us assume that $E/\mathbb{Q}_\ell$ has additive potentially multiplicative reduction.

**Theorem 3.** We are in one of the following cases.

1) If $\ell \not\equiv 1 \pmod{p}$, then
\[ d = \begin{cases} 2r & \text{if } v(j) \equiv 0 \pmod{p}, \\ 2pr & \text{otherwise}. \end{cases} \]

2) If $\ell \equiv 1 \pmod{p}$, then
\[ d = \begin{cases} 2 & \text{if } v(j) \equiv 0 \pmod{p} \text{ and } \frac{-\ell+1}{j^r} \equiv 1 \pmod{\ell}, \\ 2p & \text{otherwise}. \end{cases} \]
Let \( \ell \geq 5 \) and \( E/\mathbb{Q}_\ell \) be an elliptic curve with additive potentially good reduction. In this case, the triples \((v(c_4), v(c_6), v(\Delta))\) are given according to the following table.

| \(v(\Delta)\) | 2 | 3 | 4 | 6 | 8 | 9 | 10 |
|----------------|---|---|---|---|---|---|----|
| \(v(c_4)\)    | ≥1| 1 | ≥2| 2 | ≥3| 3 | ≥4 |
| \(v(c_6)\)    | 1 | ≥2| 2 | ≥3| 3 | 4 | ≥5|

Let \( e = e(E) \) be the semistability defect of \( E \), i.e. the degree of the minimal extension of \( \mathbb{Q}_\ell^{ur} \) over which \( E \) acquires good reduction.

From [9, Proposition 1] we know that

\[
(5.1) \quad e = \text{denominator of} \ \frac{v(\Delta)}{12}
\]

and, in particular, we have \( e \in \{2, 3, 4, 6\} \). The equation

\[
(5.2) \quad y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864},
\]

is a minimal model of \( E/\mathbb{Q}_\ell \).

5.1. Case \( e = 2 \). Suppose \( E \) satisfies \( e = 2 \). Let \( E'/\mathbb{Q}_\ell \) be the quadratic twist of \( E \) by \( \sqrt{\ell} \).

**Lemma 1.** The elliptic curve \( E'/\mathbb{Q}_\ell \) has good reduction.

Let \( \tilde{E}'/\mathbb{F}_\ell \) be the elliptic curve obtained by reduction of a minimal model for \( E' \). Write

\[
(5.3) \quad a_{E'} = \ell + 1 - |\tilde{E}'(\mathbb{F}_\ell)| \quad \text{and} \quad \Delta_{E'} = a_{E'}^2 - 4\ell.
\]

Let \( \alpha \) and \( \beta \) be the roots in \( \mathbb{F}_p^* \) of the polynomial in \( \mathbb{F}_p[X] \)

\[
X^2 - a_{E'}X + \ell \pmod{p}.
\]

Let \( n \) be the least common multiple of the orders of \( \alpha \) and \( \beta \) in \( \mathbb{F}_p^* \).

In case \( E'/\mathbb{Q}_\ell \) has good ordinary reduction, \( \pi_{E'} \) being the Frobenius endomorphism of \( \tilde{E}'/\mathbb{F}_\ell \), we will note

\[
b_{E'} = \left[ \text{End}(\tilde{E}') : \mathbb{Z}[\pi_{E'}] \right]
\]

the index of \( \mathbb{Z}[\pi_{E'}] \) in \( \text{End}(\tilde{E}') \).

**Theorem 4.** Let \( E/\mathbb{Q}_\ell \) satisfy \( e(E) = 2 \) and let \( E' \) be as above.

1) Suppose \( \Delta_{E'} \not\equiv 0 \pmod{p} \). We have

\[
d = \begin{cases} 
n & \text{if } n \text{ is even} \\
\frac{n}{2} & \text{otherwise}
\end{cases} \quad \text{and} \quad \alpha^2 = \beta^2 = -1,
\]

2) Suppose \( \Delta_{E'} \equiv 0 \pmod{p} \). Then \( E'/\mathbb{Q}_\ell \) has good ordinary reduction.
2.1) If \( n \) is even and \( \alpha_n = -1 \), then
\[
d = \begin{cases} 
  n & \text{if } b_{E'} \equiv 0 \pmod{p}, \\
  np & \text{otherwise}.
\end{cases}
\]

2.2) If \( n \) is odd or \( \alpha_n \neq -1 \), then
\[
d = \begin{cases} 
  2n & \text{if } b_{E'} \equiv 0 \pmod{p}, \\
  2np & \text{otherwise}.
\end{cases}
\]

5.2. Case \( e \in \{3, 4, 6\} \). Suppose \( E/\mathbb{Q}_\ell \) satisfies \( e \in \{3, 4, 6\} \). We define
\[
u = \ell^{\frac{e-2}{2}} \quad \text{and} \quad M = \mathbb{Q}_\ell(u).
\]

Let \( E'/M \) be the elliptic curve of equation
\[
Y^2 = X^3 - \frac{c_4}{48u^4}X - \frac{c_6}{864u^6}.
\]

**Lemma 2.** The elliptic curves \( E \) and \( E' \) are isomorphic over \( M \). Moreover, \( E'/M \) has good reduction.

The extension \( M/\mathbb{Q}_\ell \) is totally ramified of degree \( e \). Let \( \tilde{E}'/\mathbb{F}_\ell \) be the elliptic curve obtained from \( E' \) by reduction and denote
\[
a_{E'} = \ell + 1 - |\tilde{E}'(\mathbb{F}_\ell)| \quad \text{and} \quad \Delta_{E'} = a_{E'}^2 - 4\ell.
\]

Let \( \alpha \) and \( \beta \) be the roots in \( \mathbb{F}_{p^2}^* \) of the polynomial in \( \mathbb{F}_p[X] \) given by
\[
X^2 - a_{E'}X + \ell \pmod{p}.
\]

Let \( n \) be the least common multiple of the orders of \( \alpha \) and \( \beta \) in \( \mathbb{F}_{p^2}^* \).

When \( p \) does not divide \( e \), we denote by \( \zeta_e \) a primitive \( e \)-th root of unity in \( \mathbb{F}_{p^2}^* \). Note that when \( p \mid e \) we have \( p = 3 \) and \( e \in \{3, 6\} \).

**Theorem 5.** Suppose that \( e(E) = 3 \) and \( \ell \equiv 1 \pmod{3} \).

1) Assume also \( p \neq 3 \).

1.1) If \( \Delta_{E'} \equiv 0 \pmod{p} \), then
\[
d = \begin{cases} 
  n & \text{if } n \equiv 0 \pmod{3} \quad \text{and} \quad \{\alpha_n^{\frac{2}{3}}, \beta_n^{\frac{2}{3}}\} = \{\zeta_3, \zeta_3^{-1}\}, \\
  3n & \text{otherwise}.
\end{cases}
\]

1.2) If \( \Delta_{E'} \equiv 0 \pmod{p} \), then \( d = 3n \).

2) If \( p = 3 \), then \( d = 3n \).

**Theorem 6.** Suppose that \( e(E) = 4 \) and \( \ell \equiv 1 \pmod{4} \).

1) If \( \Delta_{E'} \equiv 0 \pmod{p} \), then
\[
d = \begin{cases} 
  n & \text{if } n \equiv 0 \pmod{4} \quad \text{and} \quad \{\alpha_n^{\frac{2}{4}}, \beta_n^{\frac{2}{4}}\} = \{\zeta_4, \zeta_4^{-1}\}, \\
  4n & \text{if } n \text{ is odd} \quad \text{or} \quad \{\alpha_n^{\frac{2}{4}}, \beta_n^{\frac{2}{4}}\} \neq \{-1\}, \\
  2n & \text{otherwise}.
\end{cases}
\]
2) If \( \Delta_{E'} \equiv 0 \pmod{p} \), then
\[
d = \begin{cases} 
2n & \text{if } n \text{ is even and } \alpha^2 = -1, \\
4n & \text{otherwise.}
\end{cases}
\]

**Theorem 7.** Suppose that \( e(E) = 6 \) and \( \ell \equiv 1 \pmod{3} \).

1) Assume also \( p \neq 3 \).

1.1) Suppose \( \Delta_{E'} \not\equiv 0 \pmod{p} \).

1.1.1) If \( n \equiv 0 \pmod{6} \) and \( \{\alpha^6, \beta^6\} = \{\zeta_6, \zeta_6^{-1}\} \), then \( d = n \).

1.1.2) Suppose \( n \not\equiv 0 \pmod{6} \) or \( \{\alpha^6, \beta^6\} \neq \{\zeta_6, \zeta_6^{-1}\} \). Then,
\[
d = \begin{cases} 
2n & \text{if } n \equiv 0 \pmod{3} \text{ and } \{\alpha^6, \beta^6\} = \{\zeta_6^2, \zeta_6^{-2}\}, \\
3n & \text{if } n \text{ is even and } \alpha^6 = \beta^6 = -1, \\
6n & \text{otherwise.}
\end{cases}
\]

1.2) If \( \Delta_{E'} \equiv 0 \pmod{p} \), then
\[
d = \begin{cases} 
3n & \text{if } n \text{ is even and } \alpha^6 = -1, \\
6n & \text{otherwise.}
\end{cases}
\]

2) If \( p = 3 \), then \( d = 6 \).

**Theorem 8.** Suppose that \( e = e(E) \in \{3, 4, 6\} \) and \( \ell \equiv -1 \pmod{e} \).

1) If \( e = 3 \), then \( d = 6\delta \).

2) If \( e \in \{4, 6\} \), then
\[
d = \begin{cases} 
er & \text{if } r \text{ is even,} \\
2er & \text{if } r \text{ is odd.}
\end{cases}
\]

6. The case of additive potentially good reduction with \( \ell = 3 \)

Let \( E/\mathbb{Q}_3 \) be an elliptic curve with additive potentially good reduction. We can find in [9] the value of \( e \) in terms of the triple \( (v(c_4), v(c_6), v(\Delta)) \). In particular, we have \( e \in \{2, 3, 4, 6, 12\} \).

When \( e = 2 \), we see from [9, p. 355, Cor.] that
\[
(v(c_4), v(c_6), v(\Delta)) \in \{(2, 3, 6), (3, 6, 6)\}.
\]

In this case, a minimal equation of \( E/\mathbb{Q}_3 \) is
\[
y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}
\]
and we let \( E'/\mathbb{Q}_3 \) be the elliptic curve obtained as the quadratic twist of \( E \) by \( \sqrt{3} \).

**Lemma 3.** The elliptic curve \( E'/\mathbb{Q}_3 \) has good reduction.
Let \( \tilde{E}'/\mathbb{F}_3 \) be the elliptic curve obtained from \( E'/\mathbb{Q}_3 \) by reduction and define
\[
a_{E'} = 4 - |\tilde{E}'(\mathbb{F}_3)| \quad \text{and} \quad \Delta_{E'} = a_{E'}^2 - 12.
\]
Let \( \alpha \) and \( \beta \) be the roots in \( \mathbb{F}_{p^2} \) of the polynomial in \( \mathbb{F}_p[X] \) given by
\[
X^2 - a_{E'}X + 3 \pmod{p}.
\]
Let \( n \) be the least common multiple of their orders in \( \mathbb{F}_{p^2}^* \).

**Theorem 9.** Let \( E/\mathbb{Q}_3 \) satisfy \( e(E) = 2 \) and let \( E' \) be as above.

1) Suppose \( \Delta_{E'} \not\equiv 0 \pmod{p} \). We have
\[
d = \begin{cases} n & \text{if } n \text{ is even} \quad \text{and} \quad \alpha^2 \beta^2 = -1, \\ 2n & \text{otherwise}. \end{cases}
\]

2) Suppose \( \Delta_{E'} \equiv 0 \pmod{p} \). Then \( p = 11 \) and \( d = 110 \).

**Theorem 10.** Suppose that \( e(E) \in \{3, 4, 6, 12\} \).

1) If \( e = 3 \), then \( d = 6\delta \).

2) If \( e \in \{4, 6, 12\} \), then
\[
d = \begin{cases} er & \text{if } r \text{ is even}, \\ 2er & \text{if } r \text{ is odd}. \end{cases}
\]

7. The case of additive potentially good reduction with \( \ell = 2 \)

Let \( E/\mathbb{Q}_2 \) be an elliptic curve with additive potentially good reduction. We can find in [9] the value of \( e \) in terms of the triple \( (v(c_4), v(c_6), v(\Delta)) \). In particular, \( e \in \{2, 3, 4, 6, 8, 24\} \).

When \( e = 2 \), we write \( t = (v(c_4), v(c_6), v(\Delta)) \), and [9, p. 357, Cor.] gives that
\[
t \in \{(\geq 6, 6, 6), (4, 6, 12), (\geq 8, 9, 12), (6, 9, 18)\}.
\]

The equation
\[
y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}
\]
is a minimal model of \( E/\mathbb{Q}_2 \). Define the quantity
\[
c'_6 = \frac{c_6}{2^w(c_6)}.
\]

**Lemma 4.** Suppose that \( E \) satisfies \( e = 2 \) and let \( u \in \{-2, -1, 2\} \) be defined as follows:
\[
u = \begin{cases} 2 & \text{if } t = (\geq 6, 6, 6) \quad \text{and} \quad c'_6 \equiv 1 \pmod{4}, \\ -2 & \text{if } t = (\geq 6, 6, 6) \quad \text{and} \quad c'_6 \equiv -1 \pmod{4}, \\ -1 & \text{if } t = (4, 6, 12) \quad \text{or} \quad t = (\geq 8, 9, 12), \\ 2 & \text{if } t = (6, 9, 18) \quad \text{and} \quad c'_6 \equiv -1 \pmod{4}, \\ -2 & \text{if } t = (6, 9, 18) \quad \text{and} \quad c'_6 \equiv 1 \pmod{4}. \end{cases}
\]

Then, the quadratic twist of \( E/\mathbb{Q}_2 \) by \( \sqrt{u} \) has good reduction.
Under the conditions of Lemma 4, we let $E'/\mathbb{Q}_2$ be the quadratic twist of $E/\mathbb{Q}_2$ by $\sqrt{u}$ and $\tilde{E}'/\mathbb{F}_2$ the elliptic curve obtained from $E'$ by reduction. Define also

$$a_{E'} = 3 - \left| \tilde{E}'(\mathbb{F}_2) \right| \quad \text{and} \quad \Delta_{E'} = a_{E'}^2 - 8.$$  

Let $\alpha$ and $\beta$ be the roots in $\mathbb{F}_{p^2}^*$ of the polynomial in $\mathbb{F}_p[X]$ given by

$$X^2 - a_{E'}X + 2 \pmod{p}.$$  

Let $n$ be the least common multiple of their orders in $\mathbb{F}_{p^2}^*$.

**Theorem 11.** Let $E/\mathbb{Q}_2$ satisfy $e(E) = 2$ and let $E'$ be as above.

1) Suppose $\Delta_{E'} \equiv 0 \pmod{p}$. We have,

$$d = \begin{cases} 
2n & \text{if } n \text{ is even} \quad \text{and} \quad \alpha^{\frac{n}{2}} = \beta^{\frac{n}{2}} = -1, \\
2n & \text{otherwise.}
\end{cases}$$

2) Suppose $\Delta_{E'} \equiv 0 \pmod{p}$. Then $p = 7$ and $d = 42$.

**Theorem 12.** Suppose that $E/\mathbb{Q}_2$ satisfies $e(E) \in \{3, 4, 6, 8, 24\}$.

1) If $e = 3$, then $d = 6\delta$.

2) If $e \in \{4, 6, 8, 24\}$, then

$$d = \begin{cases} 
er \cdot r & \text{if } r \text{ is even,} \\
2er & \text{if } r \text{ is odd.}
\end{cases}$$

### 8. Application of the Results

Before proceeding to the proofs of the results, let us give some examples of their application.

Consider the elliptic curve over $\mathbb{Q}$ with Cremona label 25920ba1 given by the minimal model

$$E : y^2 = x^3 - 432x - 864$$  

whose conductor is $N_E = 2^6 \cdot 3^4 \cdot 5$ and standard invariants are

$$c_4(E) = 2^8 \cdot 3^4, \quad c_6(E) = 2^{10} \cdot 3^6, \quad \Delta = 2^{14} \cdot 3^{10} \cdot 5.$$  

We will determine the degree $d_\ell$ of $\mathbb{Q}_\ell(E_p)/\mathbb{Q}_\ell$ for $\ell \in \{2, 3, 5, 7\}$ and $p \in \{3, 5, 7, 11\}$ with $\ell \neq p$. Recall that $\ell$ is the order of $\ell$ modulo $p$.

1) Let $\ell = 2$; from [9, p. 357, Cor.] we see that $e = 24$. From Theorem 12 we now conclude that

$$d_3 = 48, \quad d_5 = 96, \quad d_7 = 144, \quad d_{11} = 240,$$

since for $p = 3, 5, 7, 11$ we have $r = 2, 4, 3, 10$, respectively.

2) Let $\ell = 3$; from [9, p. 355, Cor.] we see that $e = 6$. From Theorem 10 we now conclude that

$$d_5 = 24, \quad d_7 = 36, \quad d_{11} = 110,$$

since for $p = 5, 7, 11$ we have $r = 4, 6, 5$, respectively.
3) Let $\ell = 5$; the curve $E$ has multiplicative reduction at 5 and the symbol $(-c_6/5) = 1$. Moreover, for $p = 3, 7, 11$, we have that $5 \not\equiv 1 \pmod{p}$, so by part 1.1) of Theorem 2 we conclude that
\[ d_3 = 6, \quad d_7 = 42, \quad d_{11} = 55, \]
since $r = 2, 6, 5$, respectively and $v_5(j) = 2 \not\equiv 0 \pmod{p}$ for all $p$.

4) Let $\ell = 7$; the curve $E$ has good reduction at 7 so we will apply Theorem 1. We have
\[ a_E = -2, \quad \Delta_E = -24. \]
For $p = 3$ we have $\Delta_E \equiv 0 \pmod{p}$ and $b_E = 1 \not\equiv 0 \pmod{3}$. Moreover,
\[ x^2 - a_E x + 7 \equiv (x + 1)^2 \pmod{3}, \]
so $n = 2$ and $d_3 = 6$ by Theorem 1 part 2). For $p = 5$, we have
\[ x^2 - a_E x + 7 \equiv (x + 3)(x + 4) \pmod{5}, \]
so $d_5 = n = 4$ by Theorem 1 part 1). For $p = 11$, we have
\[ x^2 - a_E x + 7 \equiv (x + 8)(x + 4) \pmod{11}, \]
so $d_{11} = n = 10$ by Theorem 1 part 1).

8.1. **Computing the discriminant of $\mathbb{Q}_\ell(E_p)$**. To finish we will determine the discriminant ideal of $K = \mathbb{Q}_\ell(E_p)$ for $(\ell, p) = (2, 3)$ and $(\ell, p) = (3, 5)$ where $E$ is the elliptic curve in the previous examples. Write $\pi$ for an uniformizer in $K$. The discriminant ideal $\mathcal{D}$ of $K / \mathbb{Q}_\ell$ is generated by $\ell^{d_{\mathcal{D}/\mathbb{Q}}}$, where $(\pi)^p$ is the different ideal of $K$.

1) Let $(\ell, p) = (2, 3)$. We have $e = 24$ and $d_3 = 48$ from the previous section. The valuations of $\nu_2(c_4)$ and $\nu_2(\Delta)$ together with [1, Théorème 4] tell us that $D = 50$, hence $\mathcal{D} = (2)^{100}$.

2) Let $(\ell, p) = (3, 5)$. In this case, we have $e = 6$ and $d_5 = 24$ and [1, Théorème 3] tell us that $D = 9$, hence $\mathcal{D} = (3)^{36}$.

**Part II. Proof of the statements**

9. **Proof of Theorem 1 and Corollary 1**

Let $E/M$ be as in the statement of Theorem 1 and recall that $d = [M(E_p) : M]$.

**Lemma 5.** Suppose $p$ divides $\Delta_E$. Then $E/M$ has good ordinary reduction.

**Proof.** We have to prove that $a_E \not\equiv 0 \pmod{\ell}$.

Recall that $\Delta_E = a_E^2 - 4\ell$. Since $\ell \neq p$ and $p \geq 3$, we have $a_E \neq 0$.

The Weil bound implies $|a_E| \leq 2\sqrt{\ell}$. So, for $\ell \geq 5$, it is clear that $\ell \nmid a_E$.

Suppose $\ell = 2$ or $\ell = 3$ and that $E/M$ has good supersingular reduction. In case $\ell = 2$, one has $a_E = \pm 2$ so $\Delta_E = -4$, which is not divisible by $p$. If $\ell = 3$, one has $a_E = \pm 3$ so $\Delta_E = -3$, which leads again to a contradiction, hence the assertion. \qed
Let $\tilde{E}_p$ be the group of $p$-torsion points of the reduced elliptic curve $\tilde{E}/\mathbb{F}_\ell$. From the work of Serre-Tate [15, Lemma 2], we have

\[(9.1)\quad d = [\mathbb{F}_\ell(\tilde{E}_p) : \mathbb{F}_\ell].\]

Let us note

$$\rho_{\tilde{E},p} : \text{Gal}(\mathbb{F}_\ell(\tilde{E}_p)/\mathbb{F}_\ell) \to \text{GL}_2(\mathbb{F}_p)$$

the representation giving the action of the Galois group $\text{Gal}(\mathbb{F}_\ell(\tilde{E}_p)/\mathbb{F}_\ell)$ on $\tilde{E}_p$ via a choice of a basis. Let $\sigma_\ell$ be the Frobenius element of $\text{Gal}(\mathbb{F}_\ell(\tilde{E}_p)/\mathbb{F}_\ell)$. The order of

$$\rho_{\tilde{E},p}(\sigma_\ell) \in \text{GL}_2(\mathbb{F}_p)$$

is equal to $d$. Let $f_E \in \mathbb{F}_p[X]$ be its characteristic polynomial, which is given by

$$f_E = X^2 - a_E X + \ell \pmod{p}.$$

1) Suppose $\Delta_E \not\equiv 0 \pmod{p}$.

If $\Delta_E$ is a square in $\mathbb{F}_p^*$, the roots $\alpha, \beta$ of $f_E$ belong to $\mathbb{F}_p^*$ and are distinct. So up to conjugation, one has

$$\rho_{\tilde{E},p}(\sigma_\ell) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},$$

which implies $d = n$ as stated.

If $\Delta_E$ is not a square in $\mathbb{F}_p^*$, then the roots of $f_E$ are $\alpha$ and $\alpha^p$ and belong to $\mathbb{F}_p^2$. So there exists a matrix $U \in \text{GL}_2(\mathbb{F}_p^2)$ such that

$$\rho_{\tilde{E},p}(\sigma_\ell) = U \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix} U^{-1},$$

which leads again $d = n$.

2) Suppose $\Delta_E \equiv 0 \pmod{p}$. We have $f_E = (X - \alpha)^2$ so, up to conjugation, we obtain

$$\rho_{\tilde{E},p}(\sigma_\ell) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \quad \text{or} \quad \rho_{\tilde{E},p}(\sigma_\ell) = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}.$$
10. Proof of Theorem 2 and Theorem 3

Suppose that $E$ has multiplicative reduction or additive potentially multiplicative reduction; in particular, one has $v(j) < 0$. Let us denote

$$L = \mathbb{Q}_\ell \left( \sqrt{-c_6} \right).$$

The elliptic curve $E/\mathbb{Q}_\ell$ is isomorphic over $L$ to the Tate curve $\mathbb{G}_m/q^Z$, with $q \in \mathbb{Z}_\ell$ the element defined by the equality ([14, p. 443] and [1, Lemme 1])

$$j = \frac{1}{q} + 744 + 196884q + \ldots. \quad (10.1)$$

Let $\varepsilon : \text{Gal} \left( \overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell \right) \to \{ \pm 1 \}$ be the character associated to the extension $L/\mathbb{Q}_\ell$. Note that $\varepsilon$ can be of order 1. The curves $E/\mathbb{Q}_\ell$ and $\mathbb{G}_m/q^Z$ are related by the quadratic twist by $\varepsilon$.

Let $\chi_p : \text{Gal} \left( \overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell \right) \to \mathbb{F}_p^\ast$ be the mod $p$ cyclotomic character. The representation giving the action of $\text{Gal} \left( \overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell \right)$ on $E_p$ is of the shape

$$\varepsilon \otimes \chi_p \left( \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right). \quad (10.2)$$

**Lemma 6.** The element $q$ is a $p$-th power in $\mathbb{Q}_\ell$ if and only if such is the case for $j$. In particular, one has $\mathbb{Q}_\ell \left( \mu_p, q^{\frac{j}{p}} \right) = \mathbb{Q}_\ell \left( \mu_p, j^{\frac{j}{p}} \right)$.

**Proof.** From the equality (10.1), one has

$$j = \frac{u}{q} \quad \text{with} \quad u = 1 + 744q + 196884q^2 + \ldots.$$ 

Since $v(q) > 0$, we have $u \equiv 1 \pmod{\ell}$. The primes $\ell$ and $p$ being distinct, by Hensel’s Lemma we conclude that $u$ is a $p$-th power in $\mathbb{Q}_\ell$ and the result follows. \qed

**Lemma 7.** We have

$$\mathbb{Q}_\ell(E_p) = \mathbb{Q}_\ell \left( \sqrt{-c_6}, \mu_p, j^{\frac{j}{p}} \right).$$

**Proof.** The $\text{Gal} \left( \overline{\mathbb{Q}}_\ell/L \right)$-modules $E_p$ and $\left( \mu_p, q^{\frac{j}{p}} \right) q^Z/q^Z$ are isomorphic. So one has

$$L(E_p) = L \left( \mu_p, q^{\frac{j}{p}} \right).$$

The inequalities

$$[L(E_p) : \mathbb{Q}_\ell(E_p)] \leq 2 \quad \text{and} \quad p \geq 3,$$

imply that $q$ is a $p$-th power in $\mathbb{Q}_\ell(E_p)$. Moreover, from (10.2) it follows that for all element $\sigma \in \text{Gal} \left( \overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell \right)$ fixing $\mathbb{Q}_\ell(E_p)$, one has $\varepsilon(\sigma) = 1$, so $\sqrt{-c_6}$ belongs to $\mathbb{Q}_\ell(E_p)$. We obtain

$$L(E_p) = \mathbb{Q}_\ell \left( \sqrt{-c_6}, \mu_p, q^{\frac{j}{p}} \right) \subseteq \mathbb{Q}_\ell(E_p) \subseteq L(E_p),$$

which leads to $\mathbb{Q}_\ell(E_p) = \mathbb{Q}_\ell \left( \sqrt{-c_6}, \mu_p, q^{\frac{j}{p}} \right)$. The result now follows from Lemma 6. \qed

**Lemma 8.** Let $a$ be an element of $\mathbb{Q}_\ell^\ast$. 

1) If \( \ell \not\equiv 1 \pmod{p} \), then
\[
a \in \mathbb{Q}_\ell^p \iff v(a) \equiv 0 \pmod{p}.
\]

2) If \( \ell \equiv 1 \pmod{p} \), then
\[
a \in \mathbb{Q}_\ell^p \iff v(a) \equiv 0 \pmod{p} \quad \text{and} \quad \left( \frac{a}{\ell^{v(a)}} \right)^{\frac{\ell-1}{p}} \equiv 1 \pmod{\ell}.
\]

Proof. Let \( \mu_{\ell-1} \) be the group of \((\ell - 1)\)-th roots of unity and \( U^1 \) be the group of units of \( \mathbb{Z}_\ell \) which are congruent to 1 modulo \( \ell \). One has \( \mathbb{Q}_\ell^* = \mu_{\ell-1} \times U^1 \times \mathbb{Z}_\ell^2 \). Since \( p \neq \ell \), it follows from Hensel’s lemma that each unit in \( U^1 \) is a \( p \)-th power in \( \mathbb{Q}_\ell^* \).

In case \( \ell \not\equiv 1 \pmod{p} \), the map \( x \mapsto x^p \) is an automorphism of \( \mu_{\ell-1} \), hence the first assertion.

Suppose \( \ell \equiv 1 \pmod{p} \). There exists \( \zeta \in \mu_{\ell-1} \) such that \( a^{\frac{\ell-1}{p}} \equiv \zeta \pmod{\ell} \). Moreover, \( \zeta \) belongs to \( \mathbb{Q}_\ell^p \) if and only if \( \zeta^{\frac{\ell-1}{p}} = 1 \). This implies the result. \( \square \)

Let us recall the essential fact that
\[
r = [\mathbb{Q}_\ell(\mu_p) : \mathbb{Q}_\ell].
\]

We can now complete the proofs of Theorems 2 and 3.

10.1. Proof of Theorem 2. 1) Suppose \( \ell \geq 3 \) and \( \left( \frac{-c_6}{\ell} \right) = 1 \), or \( \ell = 2 \) and \( c_6 \equiv 7 \pmod{8} \).

From these assumptions, \(-c_6\) is a square in \( \mathbb{Q}_\ell \). So we have from Lemma 7 that
\[
\mathbb{Q}_\ell(E_p) = \mathbb{Q}_\ell \left( \mu_p, \sqrt{\frac{\mathbb{Q}_\ell}{\ell}} \right).
\]

If \( j \) is a \( p \)-th power in \( \mathbb{Q}_\ell \), it follows that \( d = r \), otherwise one has \( d = pr \). Moreover, if \( \ell \equiv 1 \pmod{p} \), one has \( r = 1 \). The assertions 1.1) and 1.2) of Theorem 2 are then a consequence of Lemma 8.

2) Suppose \( \ell \geq 3 \) and \( \left( \frac{-c_6}{\ell} \right) = -1 \), or \( \ell = 2 \) and \( c_6 \not\equiv 7 \pmod{8} \).

Suppose \( r \) is even. The elliptic curve \( E/\mathbb{Q}_\ell \) having multiplicative reduction, the extension \( L/\mathbb{Q}_\ell \) is unramified. Consequently, \( \sqrt{-c_6} \) belongs to \( \mathbb{Q}_\ell(\mu_p) \), so the equality (10.3) is again satisfied and the assertion 2.1) follows by Lemma 8. Suppose \( r \) is odd. Since \(-c_6\) is not a square in \( \mathbb{Q}_\ell \), it follows that \(-c_6\) is not a square in \( \mathbb{Q}_\ell(\mu_p) \). Now assertion 2.2) follows from Lemmas 7 and 8. This completes the proof of Theorem 2.

10.2. Proof of Theorem 3. Since \( E/\mathbb{Q}_\ell \) has additive reduction, the extension \( L/\mathbb{Q}_\ell \) is ramified. Therefore, if \( j \) is a \( p \)-th power in \( \mathbb{Q}_\ell \) one has \( d = 2r \), otherwise \( d = 2pr \). Lemma 8 now implies Theorem 3.
11. Proof of Lemmas 1, 2, 3, 4

11.1. **Proof of Lemma 1.** We have $\ell \geq 5$ and $e = 2$, so $v(\Delta) = 6$. The change of variables

$$
\begin{align*}
  x &= \ell X \\
  y &= \ell \sqrt{\ell} Y,
\end{align*}
$$

is an isomorphism from $E/\mathbb{Q}_\ell$ to its quadratic twist by $\sqrt{\ell}$, which is given by the equation

$$
Y^2 = X^3 - \frac{c_4}{48\ell^2} X - \frac{c_6}{864\ell^3}.
$$

It is an integral model whose discriminant is a unit of $\mathbb{Z}_\ell$, hence the lemma.

11.2. **Proof of Lemma 2.** Recall that

$$
u = \ell^{\frac{v(\Delta)}{12}} \quad \text{and} \quad M = \mathbb{Q}_\ell(u).
$$

The change of variables

$$
(11.1) \quad \begin{cases} 
  x = u^2 X \\
  y = u^3 Y,
\end{cases}
$$

is an isomorphism between the elliptic $E/\mathbb{Q}_\ell$ given by the equation (5.2) and the elliptic curve $E'/M$ given by the equation (5.5). The equation (5.5) is integral and the valuation of its discriminant is

$$
v(\Delta) - 12v(u) = 0,
$$

which proves the lemma.

11.3. **Proof of Lemma 3.** The change of variables

$$
\begin{align*}
  X &= 3x \\
  Y &= 3\sqrt{3} y,
\end{align*}
$$

realizes an isomorphism between the elliptic curve $E/\mathbb{Q}_3$ given by the equation (6.1) and its twist by $\sqrt{3}$ (denoted $E'/\mathbb{Q}_3$) of equation

$$
(W') : Y^2 = X^3 - \frac{3c_4}{16} X - \frac{c_6}{32}.
$$

Let $c_4(W')$, $c_6(W')$ and $\Delta(W')$ be the standard invariants associated to the model $(W')$. From the standard invariants for $E/\mathbb{Q}_3$ we conclude

$$
(v(c_4(W')), v(c_6(W')), v(\Delta(W'))) \in \{(4, 6, 12), (5, \geq 9, 12)\}.
$$

Moreover, the model $(W')$ is not minimal by [12, p. 126, Table II]; thus, $E'/\mathbb{Q}_3$ has good reduction over $\mathbb{Q}_3$, hence the lemma.
11.4. **Proof of Lemma 4.** We adopt here the notations used in [12].

1) Suppose $t = (6, 6, 6)$ and $c_6 \equiv 1 \pmod{4}$.

An integral model of $E'/\mathbb{Q}_2$, the quadratic twist of $E/\mathbb{Q}_2$ by $\sqrt{3}$, is

$$(W') : Y^2 = X^3 - \frac{c_4}{12}X - \frac{c_6}{108}.$$ 

It satisfies

$$(v(c_4(W')), v(c_6(W')), v(\Delta(W'))) = (8, 9, 12).$$

We shall prove that $(W')$ is not minimal, which implies that $E'/\mathbb{Q}_2$ has good reduction. For this, we use the Table IV and Proposition 6 of [12]. We have

$$b_8(W') = -a_4(W')^2,$$

hence the congruence

$$b_8(W') \equiv 0 \pmod{2^8}.$$ 

So we can choose $r = 0$ in Proposition 6 of *loc. cit.* Moreover, one has

$$b_6(W') = 4a_6(W') = -\frac{c_6}{27}.$$ 

Since $c_6 \equiv 1 \pmod{4}$, one has $-\frac{c_6}{27} \equiv 1 \pmod{4}$. The equality $v(c_6) = 6$ then implies

$$b_6(W') \equiv 2^6 \pmod{2^8},$$

and we obtain our assertion with $x = 8$.

2) Suppose $t = (6, 6, 6)$ and $c_6 \equiv -1 \pmod{4}$.

We proceed as above. An equation of $E'/\mathbb{Q}_2$, the quadratic twist of $E/\mathbb{Q}_2$ by $\sqrt{-2}$, is

$$(W') : Y^2 = X^3 - \frac{c_4}{12}X + \frac{c_6}{108}.$$ 

One has again $b_6(W') \equiv 2^6 \pmod{2^8}$, hence the result.

For the next two cases below, we will denote by $b_2$, $b_4$, $b_6$ and $b_8$ the standard invariants associated to the equation (7.2) of $E/\mathbb{Q}_2$.

3) Suppose $t = (4, 6, 12)$.

An equation of $E'/\mathbb{Q}_2$, the quadratic twist of $E/\mathbb{Q}_2$ by $\sqrt{-1}$, is

$$(W') : Y^2 = X^3 - \frac{c_4}{48}X + \frac{c_6}{864}.$$ 

We will use Table IV and Proposition 4 of [12] to prove that $(W')$ is not minimal, establishing that $E'/\mathbb{Q}_2$ has good reduction.

From the assumption made on $t$, the elliptic curve $E/\mathbb{Q}_2$ corresponds to the case 7 of Tate. One has $b_2 = 0$, $v(b_4) = 1$, $v(b_6) = 3$ and $v(b_8) = 0$. So there exists $r \in \mathbb{Z}_2$, with $v(r) = 0$, such that (conditions (a) and (b) of Proposition 4)

$$b_8 + 3rb_6 + 3r^2b_4 + 3r^4 \equiv 0 \pmod{32} \text{ and } r \equiv 1 \pmod{4}.$$ 

Furthermore,

$$b_2(W') = 0, \ b_4(W') = b_4, \ b_6(W') = -b_6, \ b_8(W') = b_8.$$
We conclude that the integer \(-r\) satisfies the condition (a) of the same Proposition 4 for the equation \((W')\). One has \(-3r \equiv 1 \pmod{4}\), so condition (b) of this proposition with \(s = 1\) implies the assertion.

4) Suppose \(t = (8, 9, 12)\).

Again an equation of \(E'/\mathbb{Q}_2\) is

\[
(W') : Y^2 = X^3 - \frac{c_4}{48}X + \frac{c_6}{864},
\]

We use Proposition 6 of [12]. The elliptic curve \(E/\mathbb{Q}_2\) corresponds to the case 10 of Tate. One has \(b_8 \equiv 0 \pmod{2^8}\), so \(r = 0\) satisfies the required condition of this proposition for the equation \((7.2)\). Since equation \((7.2)\) is minimal, we deduce (by [12, Prop 6]) that \(b_6\) is not a square modulo \(2^8\), so we have

\[
b_6 = -\frac{c_6}{216} = -\frac{2^6c_6'}{27} \equiv 2^6c_6' \equiv -2^6 \pmod{2^8},
\]

where the last congruence follows due to \(c_6' \equiv -1 \pmod{4}\). From the equality \(b_6(W') = -b_6\) it follows that \(b_6(W')\) is a square modulo \(2^8\), hence the \((W')\) is not minimal, as desired.

5) Suppose \(t = (6, 9, 18)\).

Let \(\varepsilon = \pm 1\), so that \(c_6' \equiv \varepsilon \pmod{4}\). An integral equation of the quadratic twist of \(E/\mathbb{Q}_2\) by \(\sqrt{-2\varepsilon}\), is

\[
(W') : Y^2 = X^3 - \frac{c_4}{2^6 \cdot 3}X + \varepsilon \frac{c_6}{2^8 \cdot 27}.
\]

It satisfies

\[
(v(c_4(W'))), v(c_6(W'))), v(\Delta(W')))) = (4, 6, 12).
\]

We will apply Proposition 4 of [12]. From the assumption on \(t\), we have \(c_4^3 \equiv c_6^2 \pmod{32}\), which implies

\[
c_4' \equiv 1, 9, 17, 25 \pmod{32}.
\]

Moreover, one has \(\varepsilon c_6' \equiv 1 \pmod{4}\), so from the condition (a) for \((W')\), there exists \(r \in \mathbb{Z}_2\) such that

\[
-c_4'^2 + 8r - 18c_4' r^2 + 27r^4 \equiv 0 \pmod{32}.
\]

For all the values of \(c_4'\) modulo 32, we then verify that this congruence is satisfied with \(r = -1\). The condition (b) then implies that \((W')\) is not minimal, so \(E'/\mathbb{Q}_2\) has good reduction, hence the lemma.

12. Proof of Theorems 4, 9, 11

Let \(\ell \geq 2\) and \(E/\mathbb{Q}_\ell\) satisfy \(e(E) = 2\). Let \(u \in \{\pm 1, -1\}\) be as defined in Lemma 4 and denote

\[
w = \begin{cases} 
\ell & \text{if } \ell \geq 3, \\
u & \text{if } \ell = 2.
\end{cases}
\]

From lemmas 1–4, the quadratic twist \(E'/\mathbb{Q}_\ell\) of \(E/\mathbb{Q}_\ell\) by \(\sqrt{w}\) has good reduction. Let \(\varepsilon : \text{Gal}(\mathbb{Q}_\ell(\sqrt{w})/\mathbb{Q}_\ell) \to \{\pm 1\}\) be the character associated to \(\mathbb{Q}_\ell(\sqrt{w})/\mathbb{Q}_\ell\). In suitable basis of \(E_p\) and \(E'_p\), the representations

\[
\rho_{E',p} : \text{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \text{GL}_2(\mathbb{F}_p) \quad \text{and} \quad \rho_{E,p} : \text{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \text{GL}_2(\mathbb{F}_p),
\]
giving the action of $\text{Gal}(\overline{Q}_\ell/Q_\ell)$ on $E'_p$ and $E_p$ satisfy the equality
\[
(12.1) \quad \rho_{E,p} = \varepsilon \cdot \rho_{E',p}.
\]

Let $H_0$ be the image of $\rho_{E',p}$. From the criterion of Néron-Ogg-Shafarevitch, since $\ell \neq p$ and $E'/Q_\ell$ has good reduction, the extension $Q_\ell(E'_p)/Q_\ell$ is unramified (see [14, p. 201, Thm 7.1]). So $H_0$ is cyclic. Let $\sigma_\ell \in \text{Gal}(\overline{Q}_\ell/Q_\ell)$ be a lift of the Frobenius element of the Galois group $\text{Gal}(Q_\ell(E'_p)/Q_\ell)$. Then $H_0$ is generated by $h_0 = \rho_{E',p}(\sigma_\ell)$.

**Lemma 9.** Let $H$ be the subgroup of $\text{GL}_2(F_p)$ generated by $-1$ and $h_0$. Then, $H$ is the image of $\rho_{E,p}$. In particular, one has
\[
d = \begin{cases} |H_0| & \text{if } -1 \in H_0, \\ 2|H_0| & \text{otherwise}. \end{cases}
\]

**Proof.** The equality (12.1) implies that the image of $\rho_{E,p}$ is contained in $H$.

Conversely, by assumption the inertia subgroup of $\text{Gal}(Q_\ell(E_p)/Q_\ell)$ has order 2. Noting $\tau \in \text{Gal}(\overline{Q}_\ell/Q_\ell)$ a lift of its generator, $\rho_{E,p}(\tau)$ belongs to $\text{SL}_2(F_p)$, so one has
\[
(12.2) \quad \rho_{E,p}(\tau) = -1.
\]

Moreover, the extension $Q_\ell(\sqrt{w})/Q_\ell$ being ramified, it is not contained in $Q_\ell(E'_p)$. So the restriction map induces an isomorphism between
\[
\text{Gal}(Q_\ell(\sqrt{w})(E_p)/Q_\ell(\sqrt{w})) \quad \text{and} \quad \text{Gal}(Q_\ell(E'_p)/Q_\ell).
\]

We deduce there exists $\sigma \in \text{Gal}(\overline{Q}_\ell/Q_\ell)$ such that $\sigma(\sqrt{w}) = \sqrt{w}$ and the restriction of $\sigma$ and $\sigma_\ell$ to $Q_\ell(E'_p)$ are equal. From (12.1), we obtain $\rho_{E,p}(\sigma) = h_0$ which shows that $H$ is contained in the image of $\rho_{E,p}$, hence the lemma. \[\]

Recall that the characteristic polynomial in $F_p[X]$ of $h_0$ is
\[
f_{E'} = X^2 - a_{E'} X + \ell \pmod{p}.
\]

**12.1. Proof of the assertion 1 in theorems 4, 9, 11.** We assume $\Delta_{E'} \not\equiv 0 \pmod{p}$. Up to conjugation by a matrix in $\text{GL}_2(F_p)$, we have
\[
h_0 = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},
\]
so $|H_0| = n$. Recall that $d = [Q_\ell(E_p) : Q_\ell]$. It follows from Lemma 9 that
\[
d = \begin{cases} n & \text{if } -1 \in H_0, \\ 2n & \text{otherwise}. \end{cases}
\]

We will prove that $-1$ belongs to $H_0$ if and only if $n$ is even and $\alpha^{\frac{p-1}{2}} = \beta^{\frac{p-1}{2}} = -1$. This will establish the assertion 1 of the theorems.
Suppose $-1$ belongs to $H_0$. Then there exists $k \in \{1, \ldots, n\}$, such that
\[(12.3) \quad \begin{pmatrix} \alpha^k & 0 \\ 0 & \beta^k \end{pmatrix} = -1.\]
One has $\alpha^{2k} = \beta^{2k} = 1$, so $n$ divides $2k$. Since $k \leq n$, one has $2k = n$ or $k = n$. Since $\alpha^n = \beta^n = 1$ and $p \neq 2$, we have $k \neq n$, so $n$ is even and we obtain $\alpha^{\frac{n}{2}} = \beta^{\frac{n}{2}} = -1$. Conversely, if $n$ even and $\alpha^{\frac{n}{2}} = \beta^{\frac{n}{2}} = -1$, we have $-1 = h_0^{\frac{n}{2}} \in H_0$, as desired.

12.2. **Proof of the assertion 2 in theorems 4, 9, 11.** We assume $\Delta_{E'} \equiv 0 \pmod{p}$. The elliptic curve $E'/\mathbb{Q}_\ell$ has good ordinary reduction by Lemma 5. Moreover, the polynomial $f_{E'}$ has a single root
\[\alpha = \frac{a_{E'}}{2} \pmod{p}.\]
From [2, Theorem 2] there exists a suitable basis of $E'_p$ in which
\[h_0 = \begin{pmatrix} \alpha & 0 \\ b_{E'} & \alpha \end{pmatrix}.\]
We conclude that
\[|H_0| = \begin{cases} n & \text{if } b_{E'} \equiv 0 \pmod{p}, \\ np & \text{otherwise}. \end{cases}\]
For all integers $k \geq 1$, one has
\[h_0^k = \begin{pmatrix} \alpha^k & 0 \\ kb_{E'}\alpha^{k-1} & \alpha^k \end{pmatrix}.\]

**Lemma 10.** One has $-1 \in H_0$ if and only if $n$ is even and $\alpha^{\frac{n}{2}} = -1$.

**Proof.** Suppose $-1 \in H_0$ i.e. there exists an integer $k$ such that $-1 = h_0^k$. Then
\[\alpha^k = -1 \quad \text{and} \quad kb_{E'}\alpha^{k-1} = 0.\]
Since $p \neq 2$, $n$ being the order of $\alpha$ in $\mathbb{F}_p^*$, by considering the value of $k$ modulo $p$, we have inequalities
\[1 \leq k \leq n \leq p - 1.\]
Moreover, $\alpha^{2k} = 1$, so $n$ divides $2k$. Then $2k = n$ or $2k = 2n$, which leads to $n = 2k$, hence the implication.

Conversely, suppose $n$ even and $\alpha^{\frac{n}{2}} = -1$. One has $\alpha^{\frac{2n}{2}} = -1$, which implies $h_0^{\frac{2n}{2}} = -1 \in H_0$ and proves the lemma.

The assertions 2.1) and 2.2) of Theorem 4 are now a direct consequence of lemmas 9 and 10.

Suppose $\ell = 2$. Since $E'/\mathbb{Q}_2$ has good ordinary reduction, we have $a_{E'} = \pm 1$, so $\Delta_{E'} = -7$ and we obtain $p = 7$. Moreover, $b_{E'}^2$ divides $\Delta_{E'}$, so $b_{E'} = 1$. If $a_{E'} = 1$ one has $n = 3$ and if $a_{E'} = -1$ one has $n = 6$. In both cases, lemmas 9 and 10 imply $d = 42$ as stated.

Suppose $\ell = 3$. One has $a_{E'} \in \{-1, \pm 2\}$, so $\Delta_{E'} \in \{-11, -8\}$. Since $p$ divides $\Delta_{E'}$, this implies $a_{E'} = \pm 1$ and $\Delta_{E'} = -11$. In particular, $p = 11$. One has again $b_{E'} = 1$. Furthermore, if $a_{E'} = 1$ one has $n = 10$ and if $a_{E'} = -1$ one has $n = 5$. This leads to $d = 110$ (by lemmas 9 and 10).
This completes the proofs of theorems 4, 9, 11.

13. Notation for the proof of theorems 5, 6, 7, 8

We have \( \ell \geq 5 \) and the elliptic curve \( E/\mathbb{Q}_\ell \) has additive potentially good reduction, with a semistability defect \( e \in \{3, 4, 6\} \). Let \( M \) and the elliptic curve \( E'/M \) be defined as in (5.4) and (5.5). We will write

\[
K = \mathbb{Q}_\ell(E_p), \quad G = \text{Gal}(K/\mathbb{Q}_\ell), \quad G' = \text{Gal}(M(E'_p)/M) \quad \text{and} \quad d_0 = [M(E'_p) : M].
\]

The elliptic curve \( E'/M \) has good reduction (Lemma 2), so the extension \( M(E'_p)/M \) is unramified and cyclic. Since \( M/\mathbb{Q}_\ell \) is totally ramified, the value of \( d_0 \) can be determined from Theorem 1.

Let \( \text{Frob}_M \in G' \) be the Frobenius element of \( G' \). Recall that \( \text{Frob}_M \) is a generator of \( G' \). We have \( M(E'_p) = MK \) and the extension \( K/\mathbb{Q}_\ell \) is Galois, so the Galois groups \( \text{Gal}(K/M \cap K) \) and \( G' \) are isomorphic via the restriction morphism. Let \( \text{Frob}_K \in G \) be the restriction of \( \text{Frob}_M \) to \( K \). It is a generator of \( \text{Gal}(K/M \cap K) \). In particular, \( \text{Frob}_K \) and \( \text{Frob}_M \) have the same order.

Recall that the inertia subgroup of \( G \) is cyclic of order \( e \). We let \( \tau \) be one of its generators.

Let \( \mathcal{B} \) be a basis of \( E_p \). Let \( \mathcal{B}' \) be the basis of \( E'_p \) which is the image of \( \mathcal{B} \) by the isomorphism from \( E_p \) to \( E'_p \) given by the change of variables (11.1). Denote by

\[
\rho_{E,p} : G \to \text{GL}_2(\mathbb{F}_p) \quad \text{and} \quad \rho_{E',p} : G' \to \text{GL}_2(\mathbb{F}_p)
\]

the faithful representations giving the actions of \( G \) and \( G' \) on \( E_p \) and \( E'_p \) in the basis \( \mathcal{B} \) and \( \mathcal{B}' \), respectively. We have

\[
(13.1) \quad \rho_{E,p}(\text{Frob}_K) = \rho_{E',p}(\text{Frob}_M).
\]

Since the determinant of \( \rho_{E,p} \) is the mod \( p \) cyclotomic character, we also have

\[
(13.2) \quad \rho_{E,p}(\tau) \in \text{SL}_2(\mathbb{F}_p).
\]

Finally, let also

\[
\sigma_{E,p} : G \to \text{PGL}_2(\overline{\mathbb{F}}_p) \quad \text{and} \quad \sigma_{E',p} : G' \to \text{PGL}_2(\overline{\mathbb{F}}_p)
\]

be the associated projective representations extended to \( \overline{\mathbb{F}}_p \).

We write \( F \) for the fixed field by the kernel of \( \sigma_{E,p} \).

14. Proof of Theorem 5 and assertion 1 of Theorem 8

In this case, we have \( e = [M : \mathbb{Q}_\ell] = 3 \), so either \( M \subset K \) or \( M \cap K = \mathbb{Q}_\ell \).

Lemma 11. The degree \( d = [K : \mathbb{Q}_\ell] \) satisfies

\[
d = \begin{cases} 
3d_0 & \text{if } M \subset K, \\
d_0 & \text{otherwise.}
\end{cases}
\]
Proof. Suppose $M$ is contained in $K$. Since $E$ and $E'$ are isomorphic over $M$ (Lemma 2), we have $K = M(E'_p)$. Therefore, $d_0 = [K : M]$ and
\[ d = [K : M][M : \mathbb{Q}_\ell] = 3d_0. \]
In case $M$ is not contained in $K$, the Galois groups $G$ and $G'$ are isomorphic, so $d = d_0$, hence the lemma. \(\square\)

14.1. Assertion 1) of Theorem 8. The field $M$ is contained in $K$ ([8, Lemma 5]), so $d = 3d_0$ by Lemma 11. From the assumption $\ell \equiv 2 \pmod{3}$ and [10, Lemme 1] it follows that $E'/M$ has good supersingular reduction. Since $\ell \geq 5$ we must have $a_{E'} = 0$. Now by Corollary 1 we obtain $d_0 = 2\delta$ and assertion 1 of Theorem 8 follows.

14.2. Assertion 1) of Theorem 5. Assume $p \neq 3$.

Since 3 divides $\ell - 1$, the group $G$ is abelian by [8, Corollary 3]. So there exists $U \in \text{GL}_2(\mathbb{F}_p^2)$ and $a \in \mathbb{F}_p^*$ such that
\[ (14.1) \quad U_{\rho_{E,p}}(\text{Frob}_K)U^{-1} = \begin{pmatrix} \alpha & a \\ 0 & \beta \end{pmatrix} \quad \text{and} \quad U_{\rho_{E,p}}(\tau)U^{-1} = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}. \]

Lemma 12. We have $a = 0$. In particular, $d_0 = n$.

Proof. Using the fact that Frob$_K$ and $\tau$ commute, we obtain the equality $a(1 - \zeta) = 0$, so $a = 0$. We deduce that Frob$_K$ has order $n$. Moreover, Frob$_K$ and Frob$_M$ have the same order and the latter has order $d_0$. \(\square\)

Lemma 13. We have that $M \not\subset K$ if and only if
\[ (14.2) \quad n \equiv 0 \pmod{3} \quad \text{and} \quad \{\alpha^\frac{n}{3}, \beta^\frac{n}{3}\} = \{\zeta, \zeta^2\}. \]
If this condition is satisfied then $d = n$, otherwise $d = 3n$.

Proof. Suppose that $M$ is not contained in $K$. Then $G$ and $G'$ are isomorphic, so $G$ is cyclic generated by Frob$_K$. Consequently, there exist $k \in \{1, \cdots, n\}$ such that
\[ \alpha^k = \zeta \quad \text{and} \quad \beta^k = \zeta^2. \]
We have $k \neq n$ and $\alpha^{3k} = \beta^{3k} = 1$, so $n$ divides $3k$. Since $3k \leq 3n$, this implies $3k \in \{n, 2n\}$, so $3$ divides $n$ and $k = \frac{n}{3}$ or $k = \frac{2n}{3}$. If $\alpha^\frac{n}{3} = \zeta$, then $\alpha^\frac{2n}{3} = \alpha^\frac{n}{3} = \zeta^2$ and similarly $\beta^\frac{n}{3} = \zeta$, hence the condition (14.2).

Conversely, suppose $M \subset K$. We shall prove that, for all $k \geq 1$, we have
\[ (14.3) \quad \{\alpha^k, \beta^k\} \neq \{\zeta, \zeta^2\}. \]
This implies (14.2) is not satisfied, completing the proof of the first statement.

From our assumption, one has $K = M(E'_p)$ and Frob$_K$ is a generator of Gal($K/M$). The fixed field by $\tau$ is an unramified extension of $\mathbb{Q}_\ell$. In particular, $\tau$ does not fix $M$. We deduce that for all $k \geq 1$, one has Frob$_K^k \neq \tau$, which implies (14.3).

The last statement now follows from lemmas 11 and 12. \(\square\)

Lemma 14. Suppose that $p \mid \Delta_{E'}$. Then $M \subset K$ and $d = 3n$. 

Proof. From our assumption, one has \( \alpha = \beta \). Suppose that \( M \) is not contained in \( K \). Then \( \text{Frob}_K \) is a generator of \( G \). The eigenvalues of \( \rho_{E,p}(\tau) \) are distinct, so the condition (14.1) leads to a contradiction. The result follows from lemmas 11 and 12.

This completes the proof of the first assertion of Theorem 5.

14.3. Assertion 2) of Theorem 5. Suppose \( p = 3 \).

There exist \( U \in \text{GL}_2(\mathbb{F}_9) \) and \( a \in \mathbb{F}_9 \) such that \( U\rho_{E,p}(\text{Frob}_K)U^{-1} = \begin{pmatrix} \alpha & a \\ 0 & \beta \end{pmatrix} \). Moreover, the image of \( \rho_{E,3} \) being a subgroup of \( \text{GL}_2(\mathbb{F}_3) \), one has \( d \not\equiv 0 \pmod{9} \).

Suppose \( M \) is not contained in \( K \). The group \( G \) and \( G' \) are isomorphic, so \( G \) is generated by \( \text{Frob}_K \). Since 3 divides \( d \) (because \( e = 3 \)), the order of \( a \in \mathbb{F}_9 \) is equal to 3, so \( d = 3n \).

Suppose \( M \) is contained in \( K \). Then one has \( d = 3[K : M] \). One deduces that 3 does not divide \( [K : M] \). The group \( \text{Gal}(K/M) \) being generated by \( \text{Frob}_K \), this implies \( a = 0 \), so \( [K : M] = n \) and \( d = 3n \) as stated.

This completes the proof of Theorem 5.

15. Proof of Theorem 6

In this case, we have \( e = [M : \mathbb{Q}_\ell] = 4 \). Recall that \( \zeta_4 \) is a primitive 4th root of unity.

The extension \( M/\mathbb{Q}_\ell \) is cyclic, so \( M \cap K = \mathbb{Q}_\ell, \mathbb{Q}_\ell(\sqrt{\ell}) \) or \( M \).

Lemma 15. The degree \( d = [K : \mathbb{Q}_\ell] \) satisfies

\[
\begin{align*}
\text{d} & = \begin{cases} 
4d_0 & \text{if } M \not\subseteq K, \\
2d_0 & \text{if } M \cap K = \mathbb{Q}_\ell(\sqrt{\ell}), \\
d_0 & \text{if } M \cap K = \mathbb{Q}_\ell.
\end{cases}
\end{align*}
\]

Proof. The Galois groups \( G' \) and \( \text{Gal}(K/M \cap K) \) are isomorphic and \( |G'| = d_0 \), hence the result.

Since 4 divides \( \ell - 1 \), the Galois group \( G \) is abelian by [8, Cor. 3]. So there exist \( U \in \text{GL}_2(\mathbb{F}_{p^2}) \) and \( a \in \mathbb{F}_{p^2} \) such that

\[
U \rho_{E,p}(\text{Frob}_K)U^{-1} = \begin{pmatrix} \alpha & a \\ 0 & \beta \end{pmatrix} \quad \text{and} \quad U \rho_{E,p}(\tau)U^{-1} = \begin{pmatrix} \zeta_4 & 0 \\ 0 & \zeta_4^{-1} \end{pmatrix}.
\]

Lemma 16. We have \( a = 0 \). In particular, \( d_0 = n \).

Proof. Using the fact that \( \text{Frob}_K \) and \( \tau \) commute, we obtain the equality \( a(\zeta_4 - \zeta_4^{-1}) = 0 \), so \( a = 0 \). Moreover, the orders of \( \text{Frob}_K \) and \( \text{Frob}_M \) are equal, so \( d_0 \) is the order of \( \text{Frob}_K \), hence the assertion.

Lemma 17. We have \( M \cap K = \mathbb{Q}_\ell \) if and only if

\[
\begin{align*}
n & \equiv 0 \pmod{4} \quad \text{and} \quad \{\alpha^2, \beta^2\} = \{\zeta_4, \zeta_4^{-1}\}.
\end{align*}
\]

If this condition is fulfilled, then \( d = n \).
Proof. Suppose \( M \cap K = \mathbb{Q}_\ell \). Then, \( G \) are \( G' \) isomorphic and \( \text{Frob}_K \) generates \( G \). From (15.1) and Lemma 16, we deduce that there exists \( k \in \{1, \cdots, n\} \) such that
\[
\{\alpha^k, \beta^k\} = \{\zeta_4, \zeta_4^{-1}\}.
\]
One has \( \alpha^{4k} = \beta^{4k} = 1 \), so \( n \) divides \( 4k \). One has \( k \neq n \). Moreover, if \( 4k = 2n \), then \( k = \frac{n}{2} \) so \( \alpha^n = \beta^n = -1 \) which is not. As in the proof of Lemma 13, we conclude \( n = 4k \) or \( 3n = 4k \), which implies (15.2).

Conversely, suppose the condition (15.2) is satisfied. We deduce that \( \tau \) belongs to the subgroup of \( G \) generated by \( \text{Frob}_K \). Furthermore, the fixed field by \( \tau \) is an unramified extension of \( \mathbb{Q}_\ell \). In particular, the extension \( M \cap K/\mathbb{Q}_\ell \) must be unramified, hence \( M \cap K = \mathbb{Q}_\ell \).

Now lemmas 15 and 16 imply \( d = n \), as desired. \( \square \)

Lemma 18. The field \( M \) is contained in \( K \) if and only if
\[
n \equiv 1 \pmod{2} \quad \text{or} \quad \{\alpha^{\frac{n}{2}}, \beta^{\frac{n}{2}}\} \neq \{-1\}.
\]
If this condition is fulfilled, then \( d = 4n \).

Proof. The order of \( \tau^2 \) is equal to 2. From (13.2), one has
\[
\rho_{E,p}(\tau^2) = -1.
\]
Suppose \( M \) is contained in \( K \). Then, \( \tau^2 \) does not fix \( M \), because the extension \( K/M \) is unramified. Since \( \text{Gal}(K/M) \) is generated by \( \text{Frob}_K \), for all \( k \in \{1, \cdots, n\} \), one has \( \text{Frob}_K^k \neq -1 \). The condition (15.1) then implies (15.3).

Conversely, suppose that the condition (15.3) is satisfied. From Lemma 17, we conclude that \( \mathbb{Q}_\ell(\sqrt{7}) \) is contained in \( K \). So \( \tau^2 \) belongs to \( \text{Gal}(K/\mathbb{Q}_\ell(\sqrt{7})) \). Suppose \( M \cap K = \mathbb{Q}_\ell(\sqrt{7}) \). Then the Galois groups \( \text{Gal}(K/\mathbb{Q}_\ell(\sqrt{7})) \) and \( G' \) are isomorphic. Consequently, \( \text{Gal}(K/\mathbb{Q}_\ell(\sqrt{7})) \) is generated by \( \text{Frob}_K \) and there exists \( k \in \{1, \cdots, n\} \) such that \( \text{Frob}_K^k = \tau^2 \). This means that \( \alpha^k = \beta^k = -1 \), which implies \( n \) even and \( \alpha^{\frac{n}{2}} = \beta^{\frac{n}{2}} = -1 \). This leads to a contradiction, hence \( M \) is contained in \( K \).

If (15.3) is satisfied, we then obtain \( d = 4n \) from lemmas 15 and 16. \( \square \)

Lemma 19. We have \( M \cap K = \mathbb{Q}_\ell(\sqrt{7}) \) if and only if the conditions (15.2) and (15.3) are not satisfied. In such case, we have \( d = 2n \).

Proof. It follows directly from the previous lemmas. \( \square \)

This completes the proof of part 1) of Theorem 6.

Lemma 20. Suppose \( p \nmid \Delta_{E'} \). Then \( \mathbb{Q}_\ell(\sqrt{7}) \) is contained in \( K \). Moreover, we have \( d = 2n \) if and only if the condition (15.3) is not fulfilled; otherwise, \( d = 4n \).

Proof. Under this assumption, one has \( \alpha = \beta \). Suppose \( \mathbb{Q}_\ell(\sqrt{7}) \) is not contained in \( K \). Then \( G' \) and \( \text{Gal}(K/\mathbb{Q}_\ell) \) are isomorphic, so \( \tau \) is a power of \( \text{Frob}_K \). The condition (15.1) implies a contradiction because the eigenvalues of \( \rho_{E,p}(\tau) \) are distinct.

Consequently, \( d = 4n \) or \( d = 2n \) by Lemma 15. The result now follows from lemmas 18, 19. \( \square \)

Finally, part 2) of Theorem 6 follows from Lemma 20.
In this case, we have \( e = [M : \mathbb{Q}_\ell] = 6 \). Recall that \( \zeta_6 \) is a primitive 6-th root of unity. The extension \( M/\mathbb{Q}_\ell \) is cyclic, so \( M \cap K = \mathbb{Q}_\ell, \mathbb{Q}_\ell(\sqrt{7}), \mathbb{Q}_\ell(\sqrt{17}) \) or \( M \).

Recall that \( d_0 = [M(E'_p) : M] \).

**Lemma 21.** The degree \( d = [K : \mathbb{Q}_\ell] \) satisfies
\[
d = \begin{cases} 
6d_0 & \text{if } M \subseteq K, \\
3d_0 & \text{if } M \cap K = \mathbb{Q}_\ell(\sqrt{7}), \\
2d_0 & \text{if } M \cap K = \mathbb{Q}_\ell(\sqrt{17}), \\
d_0 & \text{if } M \cap K = \mathbb{Q}_\ell.
\end{cases}
\]

**Proof.** The Galois groups \( G \) and \( \text{Gal}(K/M \cap K) \) are isomorphic, hence the result. \( \square \)

### 16.1. Proof of part 1)

Assume \( p \neq 3 \).

After taking the quadratic twist of \( E/\mathbb{Q}_\ell \) by \( \sqrt{7} \), the semistability defect is of order 3. Moreover, taking quadratic twist does not change the fact that the image of \( \rho_{E,p} \) is abelian or not. So, as in the case \( e = 3 \), we conclude that \( G \) is abelian (by \([8, \text{Cor. 3}]\)). Consequently, there exist \( U \in \text{GL}_2(\mathbb{F}_p^2) \) and \( a \in \mathbb{F}_p^2 \) such that
\[
U \rho_{E,p}(\text{Frob}_K)U^{-1} = \begin{pmatrix} \alpha & a \\ 0 & \beta \end{pmatrix} \quad \text{and} \quad U \rho_{E,p}(\tau)U^{-1} = \begin{pmatrix} \zeta_6 & 0 \\ 0 & \zeta_6^{-1} \end{pmatrix}.
\]

**Lemma 22.** We have \( a = 0 \). In particular, \( d_0 = n \).

**Proof.** This follows as Lemma 12. \( \square \)

**Lemma 23.** We have \( M \cap K = \mathbb{Q}_\ell \) if and only if
\[
n \equiv 0 \pmod{6} \quad \text{and} \quad \{\alpha^\frac{n}{6}, \beta^\frac{n}{6}\} = \{\zeta_6, \zeta_6^{-1}\}.
\]

If this condition is fulfilled, then \( d = n \).

**Proof.** Suppose \( M \cap K = \mathbb{Q}_\ell \). Then, \( G \) are \( G' \) isomorphic and \( \text{Frob}_K \) generates \( G \). From (16.1) and Lemma 23 there exists \( k \in \{1, \ldots, n\} \) such that \( \{\alpha^k, \beta^k\} = \{\zeta_6, \zeta_6^{-1}\} \). We have \( \alpha^{6k} = \beta^{6k} = 1 \), so \( n \) divides \( 6k \). As in the proof of Lemma 17, we conclude that (16.2) holds.

Conversely, if (16.2) is satisfied, \( \tau \) belongs to the subgroup of \( G \) generated by \( \text{Frob}_K \). The fixed field by \( \tau \) being an unramified extension of \( \mathbb{Q}_\ell \), this implies \( M \cap K = \mathbb{Q}_\ell \).

Finally, when (16.2) is satisfied, we then obtain \( d = n \) from lemmas 21 and 22. \( \square \)

**Lemma 24.** We have \( M \cap K = \mathbb{Q}_\ell(\sqrt{7}) \) if and only if the two following conditions are satisfied:

1) \( n \not\equiv 0 \pmod{6} \) or \( \{\alpha^\frac{n}{6}, \beta^\frac{n}{6}\} \neq \{\zeta_6, \zeta_6^{-1}\} \).

2) \( n \equiv 0 \pmod{3} \) and \( \{\alpha^\frac{n}{6}, \beta^\frac{n}{6}\} = \{\zeta_6^2, \zeta_6^{-2}\} \).

Moreover, if these conditions are fulfilled, then \( d = 2n \).
Proof. Suppose \( M \cap K = \mathbb{Q}_\ell(\sqrt[3]{d}) \). From lemma 24 the first condition is satisfied. The order of \( \tau^2 \) is equal to 3, hence \( \tau^2 \) belongs to \( \text{Gal}(K/\mathbb{Q}_\ell(\sqrt[3]{d})) \), which is isomorphic to \( G' \). So there exists \( k \in \{1, \ldots, n\} \) such that \( \tau^2 = \text{Frob}_K^k \) and (16.1) leads to \( \{\alpha^k, \beta^k\} = \{\zeta_6^2, \zeta_6^{-2}\} \). One has \( \alpha^{3k} = \beta^{3k} = 1 \), so \( n \) divides \( 3k \), and since \( n \neq k \), this implies the second condition.

Conversely, suppose that the two conditions of the statement are satisfied. Then \( M \cap \mathbb{Q}_\ell \neq \mathbb{Q}_\ell \). By condition 1 and Lemma 24. The second condition implies that \( \tau^2 \) belongs to the subgroup \( \text{Gal}(K/M \cap K) \) of \( G \) generated by \( \text{Frob}_K \). In particular, the ramification index of the extension \( K/M \cap K \) is at least 3, hence \( M \cap K = \mathbb{Q}_\ell(\sqrt[3]{d}) \).

The last statement follows from lemmas 22 and 23. \( \square \)

Lemma 25. We have \( M \cap K = \mathbb{Q}_\ell(\sqrt[3]{d}) \) if and only if the following conditions are satisfied:

1) \( n \not\equiv 0 \pmod{6} \) or \( \{\alpha^\frac{n}{6}, \beta^\frac{n}{6}\} \neq \{\zeta_6, \zeta_6^{-1}\} \).

2) \( n \equiv 0 \pmod{2} \) and \( \alpha^\frac{n}{2} = \beta^\frac{n}{2} = -1 \).

Moreover, if these conditions are fulfilled, then \( d = 3n \).

Proof. Suppose \( M \cap K = \mathbb{Q}_\ell(\sqrt[3]{d}) \). The first condition is satisfied (lemma 24). The order of \( \tau^3 \) is equal to 2, so \( \tau^3 \) belongs to \( \text{Gal}(K/\mathbb{Q}_\ell(\sqrt[3]{d})) \), which is isomorphic to \( G' \). So there exists \( k \in \{1, \ldots, n\} \) such that \( \tau^3 = \text{Frob}_K^k \) and (16.1) leads to \( \{\alpha^k, \beta^k\} = \{\zeta_6^2, \zeta_6^{-3}\} \). One has \( \alpha^{2k} = \beta^{2k} = 1 \) hence the second condition.

Conversely, one has \( M \cap \mathbb{Q}_\ell \neq \mathbb{Q}_\ell \) (condition 1 and lemma 24). Moreover, 3 does not divide \( n \). Otherwise, from the second condition, it follows that the first one is not satisfied. We deduce that \( M \cap \mathbb{Q}_\ell \neq \mathbb{Q}_\ell(\sqrt[3]{d}) \) (lemma 25). Moreover, the second condition implies that \( \tau^3 \) belongs to the \( \text{Gal}(K/M \cap K) \). So the ramification index of the extension \( K/M \cap K \) is at least 2, hence \( M \cap K = \mathbb{Q}_\ell(\sqrt[3]{d}) \) and the lemma.

The last statement follows from lemmas 22 and 23. \( \square \)

The assertion 1.1) of Theorem 7 is now a consequence of the previous lemmas.

Lemma 26. Suppose that \( p \mid \Delta_{E^p} \). Then \( \mathbb{Q}_\ell(\sqrt[3]{d}) \) is contained in \( K \). One has \( d = 3n \) if and only if the two conditions of Lemma 25 are satisfied; otherwise, \( d = 6n \).

Proof. Note that \( p \mid \Delta_{E^p} \) implies \( \alpha = \beta \). Suppose \( \mathbb{Q}_\ell(\sqrt[3]{d}) \) is not contained in \( K \). Then \( G' \) is either isomorphic to \( \text{Gal}(K/\mathbb{Q}_\ell) \) or \( \text{Gal}(K/\mathbb{Q}_\ell(\sqrt[3]{d})) \). So \( \tau \) or \( \tau^2 \) is a power of \( \text{Frob}_K \). The condition (16.1) implies a contradiction because the eigenvalues of \( \rho_{E,p}(\tau) \) and \( \rho_{E,p}(\tau^2) \) are distinct.

Consequently, one has \( d = 3n \) or \( d = 6n \) by lemma 21; Lemma 25 now completes the proof. \( \square \)

We can now conclude part 1.2) as follows. Since \( M \cap \mathbb{Q}_\ell \neq \mathbb{Q}_\ell \) (Lemma 26), it follows from Lemma 24 that condition 1 of Lemma 25 is satisfied. So if \( n \) is even and \( \alpha^\frac{n}{2} = -1 \), then \( d = 3n \) (Lemma 26 since \( \alpha = \beta \)). Otherwise, \( d = 6n \) (by Lemma 26), as desired.
16.2. **Assertion 2.** The group $G$ is abelian ([8, Cor. 3]). Let $\Phi$ be the inertia subgroup of $G$. Up to conjugation, there exists only one cyclic subgroup of order 6 in $GL_2(\mathbb{F}_3)$. So we can suppose that $\rho_{E,p}(\Phi)$ is generated by the matrix $\begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$. We deduce that the normalizer of $\rho_{E,p}(\Phi)$ is the standard Borel subgroup $B$ of $GL_2(\mathbb{F}_3)$. Since $\Phi$ is a normal subgroup of $G$, this implies that $\rho_{E,p}(G)$ is contained in $B$. The group $B$ is non-abelian of order 12. Since 6 divides $|\rho_{E,p}(G)|$, one deduces that $|\rho_{E,p}(G)| = 6$, hence $d = 6$.

17. **Proof of assertion 2 of Theorem 8**

Recall that one has $e \in \{4, 6\}$. Since $\ell \equiv -1 \pmod{e}$, the group $G$ is not abelian ([8, Cor. 3]). Let $\Phi$ be the inertia subgroup of $G$.

17.1. **Case** $(p, e) = (3, 6)$. As in section 16.2, we can suppose that $\rho_{E,p}(G)$ is contained in the standard Borel subgroup $B$ of $GL_2(\mathbb{F}_3)$, which is of order 12. Since $G$ is not abelian and $\Phi$ is cyclic of order 6, this implies $\rho_{E,p}(G) = B$, hence $d = 12$. Moreover, one has $\ell \equiv 2 \pmod{3}$, so $r = 2$ and we obtain $d = er$, as desired.

17.2. **Case** $p \geq 5$ or $(p, e) = (3, 4)$. We will use for our proof the results established in [5] and [6] and we will adopt the notations and terminology used in these papers.

The group of the $e$-th roots of unity is not contained in $\mathbb{Q}_\ell$. Since $p \geq 5$ or $(p, e) = (3, 4)$, we deduce from [6, Proposition 0.3], that the representation $\sigma_{E,p} : G \to PGL_2(\overline{\mathbb{F}}_p)$ is of type $\mathbf{V}$. Denote by $\Phi$ the inertia subgroup of $G$. Recall that $F$ is the field fixed by the kernel of $\sigma_{E,p}$ and write $H = \text{Gal}(K/F)$ and $d' = [K : F]$.

Recall also that $r = [\mathbb{Q}_\ell(\mu_p) : \mathbb{Q}_\ell]$.

For all $\sigma \in H$, $\rho_{E,p}(\sigma)$ is a scalar matrix in $GL_2(\overline{\mathbb{F}}_p)$. So there exists a character $\varphi : H \to \overline{\mathbb{F}}_p^*$ such that

$$\rho_{E,p}|_H \simeq \begin{pmatrix} \varphi & 0 \\ 0 & \varphi \end{pmatrix}.$$ 

The order of $\varphi$ is $d'$. Moreover, $\chi_p|_H : H \to \text{Aut}(\mu_p)$ being the cyclotomic character giving the action of $H$ on $\mu_p$, one has

$$\varphi^2 = \chi_p|_H.$$ 

We then deduce the equality

$$d' = \frac{\gcd(d', 2)}{[\overline{\mathbb{F}}(\mu_p) : F]}.$$ 

Moreover, since $\Phi$ is cyclic of order $e$, one has

$$|\sigma_{E,p}(\Phi)| = e.$$

Furthermore, the assumption $\ell \equiv -1 \pmod{e}$ implies that $\mathbb{Q}_\ell(\zeta_e)$ is the quadratic unramified extension of $\mathbb{Q}_\ell$.

**Lemma 27.** We have $F = \mathbb{Q}_\ell(\zeta_e, \ell^\times)$. In particular, $d = ed'$. 
**Proof.** The Galois group $\text{Gal}(F/\mathbb{Q}_\ell)$ is isomorphic to the dihedral group of order $e$ (see condition 3 in [5, Proposition 2.3] and (17.2)). The group $\Phi$ fixes an unramified extension of $\mathbb{Q}_\ell$. From (17.2) it follows the extension $F/\mathbb{Q}_\ell$ is not totally ramified, hence the result in case $e = 4$. If $e = 6$, since $\ell \equiv 2 \pmod{3}$, then [13, Theorem 7.2] implies the result. □

1) Suppose $r$ even. Then $\zeta_e$ belongs to $\mathbb{Q}_\ell(\mu_p)$. Lemma 27 implies $F \cap \mathbb{Q}_\ell(\mu_p) = \mathbb{Q}_\ell(\zeta_e)$. So the Galois groups $\text{Gal}(F(\mu_p)/F)$ and $\text{Gal}(\mathbb{Q}_\ell(\mu_p)/\mathbb{Q}_\ell(\zeta_e))$ are isomorphic, and we obtain

$$[F(\mu_p) : F] = \frac{r}{2}.$$ 

The ramification index of $K/F$ is equal to $\frac{e}{2}$, so 2 divides $d'$. From (17.1) we then deduce $d' = r$, which leads to $d = er$ by Lemma 27, as desired.

2) Suppose $r$ odd. Then $\zeta_e$ does not belong to $\mathbb{Q}_\ell(\mu_p)$. This implies $F \cap \mathbb{Q}_\ell(\mu_p) = \mathbb{Q}_\ell$, so $[F(\mu_p) : F] = r$, i.e. the order of $\chi_p|_H$ is $r$. We deduce that $\varphi^{2r} = 1$, so $d'$ divides $2r$. Since $F(\mu_p)$ is contained in $K$, $r$ divides $d'$. So we have $d' = r$ or $d' = 2r$. One has $d' \neq r$, otherwise $K = F(\mu_p)$ and this contradicts the fact that the ramification index of $K/\mathbb{Q}_\ell$ is $e$ and the one of $F(\mu_p)/\mathbb{Q}_\ell$ is $\frac{e}{2}$. So $d' = 2r$ and we obtain $d = 2er$, hence the result.

This completes the proof of Theorem 8.

18. **Proof of Theorem 10**

Let $E/\mathbb{Q}_3$ be an elliptic curve with additive potentially good reduction with $e \neq 2$.

Let $\rho_{E,p} : \text{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3) \rightarrow \text{GL}_2(\mathbb{F}_p)$ be the representation arising on the $p$-torsion points of $E$.

Write $K = \mathbb{Q}_3(E_p)$ for the field fixed by the kernel of $\rho_{E,p}$ whose degree is $d = [K : \mathbb{Q}_3]$.

Let the projective representation obtained from $\rho_{E,p} \otimes \overline{\mathbb{F}}_p$ be denoted by

$$\sigma_{E,p} : \text{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3) \rightarrow \text{PGL}_2(\overline{\mathbb{F}}_p)$$

and write $F$ for the field fixed by its kernel.

A minimal equation of $E/\mathbb{Q}_3$ is (see [9, p. 355])

$$(18.1) \quad y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}.$$ 

Let $\Delta^{\frac{1}{4}}$ be a 4th root of $\Delta$ in $\overline{\mathbb{Q}}_3$ and $E_2$ be the group of 2-torsion points of $E(\overline{\mathbb{Q}}_3)$. From the corollary in [9, p. 362], the smallest extension of $\mathbb{Q}_3^{\text{unr}}$ over which $E/\mathbb{Q}_3^{\text{unr}}$ acquires good reduction is

$$(18.2) \quad L = \mathbb{Q}_3^{\text{unr}}(E_2, \Delta^{\frac{1}{4}}).$$

In particular, we have

$$(18.3) \quad [L : \mathbb{Q}_3^{\text{unr}}] = e.$$ 

We will divide the proof according to the value of $e \in \{3, 4, 6, 12\}$. 

18.1. Case $e = 3$. We have (cf. loc.cit., cor. p. 355)

\[
(v(c_4), v(c_6), v(\Delta)) \in \{(2, 3, 4), (5, 8, 12)\}.
\]

Let $x_0$ be the $x$-coordinate of a point of $E_2$ in the model (18.1). Let us denote

\[ M = \mathbb{Q}_3(x_0). \]

**Lemma 28.** The extension $M/\mathbb{Q}_3$ is totally ramified of degree 3 and $E/M$ has good supersingular reduction.

*Proof.* Since 4 divides $v(\Delta)$, $\Delta$ is a 4th power in $\mathbb{Q}_3^{unr}$. So from (18.2) one has $L = \mathbb{Q}_3^{unr}(E_2)$ and $E/L$ acquires good reduction. Since we have $e = 3$, we deduce from (18.3) the equality $[\mathbb{Q}_3^{unr}(E_2) : \mathbb{Q}_3^{unr}] = 3$. This implies $\mathbb{Q}_3^{unr}(E_2) = \mathbb{Q}_3^{unr}(x_0)$. So the extension $M/\mathbb{Q}_3$ is totally ramified of degree 3 and $E/M$ has good reduction. One has $2v(c_6) \neq v(\Delta)$, so $E/M$ has good supersingular reduction by [10, p. 21, Lemme 7].

Let $E'/M$ be an elliptic curve with good reduction isomorphic over $M$ to $E/M$ and $\tilde{E}'/\mathbb{F}_3$ be the elliptic curve obtained from $E'/M$ by reduction. Let also

\[ a_{E'} = 4 - |\tilde{E}'(\mathbb{F}_3)|. \]

**Lemma 29.** We have $a_{E'} = 0$.

*Proof.* The elliptic curve $E'/M$ has a rational point of order 2 rational over $M$ (Lemma 28). It follows $\tilde{E}'/\mathbb{F}_3$ has also a rational point of order 2 rational over $\mathbb{F}_3$. Since $E'/M$ has good supersingular reduction, up to an $\mathbb{F}_3$-isomorphism, an equation of $\tilde{E}'/\mathbb{F}_3$ is $Y^2 = X^3 - X$ or $Y^2 = X^3 + X$, which implies the result.

1) Suppose that the extension $K/\mathbb{Q}_3$ is non-abelian. The Galois group Gal($M(E_p)/M$) being cyclic, implies that $M$ is contained in $K$. So $M(E'_p) = K$. From Corollary 1 and Lemma 29, one has $[K : M] = 2\delta$, so $d = 6\delta$ as stated.

2) Let us assume that extension $K/\mathbb{Q}_3$ is abelian. One has $p \neq 3$. Let $\zeta \in \mathbb{F}_9$ be a primitive cubic root of unity and $\alpha \in \mathbb{F}_9$ such that $\alpha^2 = -3$. Let $n$ the least common multiple of the orders of $\alpha$ and $-\alpha$ in $\mathbb{F}_9$.

**Lemma 30.** We have $d = 3n$.

*Proof.* The same arguments of Lemma 13 allow to conclude that $M$ is not contained in $K$ if and only if one has

(18.4) \[ n \equiv 0 \pmod{3} \quad \text{and} \quad \{\alpha^{2\zeta}, (-\alpha)^{2\zeta}\} = \{\zeta, \zeta^2\}. \]

Moreover, if this condition is fulfilled one has $d = n$, otherwise $d = 3n$. If 3 divides $n$, one has $(-\alpha)^{2\zeta} = \pm \alpha^{2\zeta}$, but $\zeta \neq \zeta^2$. So the condition (18.4) is not satisfied, hence the lemma.

**Lemma 31.** We have $n = 2\delta$.

*Proof.* Let $s$ be the order of $\alpha$. We have $s = \delta \gcd(2, s)$. If $s = 2\delta$, we have $n = s$ and the assertion. If $s = \delta$, then $s$ must be odd, so the order of $-\alpha$ is $2s$, hence $n = 2\delta$.

Lemmas 30 and 31 imply the first part of the theorem in case $K/\mathbb{Q}_3$ is abelian, which completes the proof of Theorem 10 for $e = 3$. 26
18.2. Case $e = 4$. The same proof as in section 17.2 for $e = 4$ gives the result.

18.3. Case $e = 6$. We have ([9, p. 355, Cor])
\[(v(c_4), v(c_6), v(\Delta)) \in \{(3, 5, 6), (4, 6, 10)\}.
\]

Lemma 32. The group $\text{Gal}(K/\mathbb{Q}_3)$ is abelian if and only if one has $\frac{\Delta}{3v(\Delta)} \equiv 1 \pmod{3}$.

Proof. Let $E'/\mathbb{Q}_3$ be the quadratic twist of $E/\mathbb{Q}_3$ by $\sqrt{3}$. The elliptic curve $E'/\mathbb{Q}_3$ has additive potentially good reduction with a semi-stability defect of order 3 (cf. loc.cit.). Moreover, the extension $\mathbb{Q}_3(E'_p)/\mathbb{Q}_3$ is abelian if and only if such is the case of $K/\mathbb{Q}_3$. The result now follows from [8, Proposition 5].

18.4. Case $e = 6$ with $K/\mathbb{Q}_3$ is abelian. Let $x_0$ be the $x$-coordinate of a point of $E_2$ in the model (18.1). Let us denote
\[(18.5) \quad M = \mathbb{Q}_3\left(x_0, \sqrt{3}\right).
\]

Lemma 33. Suppose $\text{Gal}(K/\mathbb{Q}_3)$ abelian. Then the extension $M/\mathbb{Q}_3$ is totally ramified of degree 6 and $E/M$ has good supersingular reduction.

Proof. Since 2 divides $v(\Delta)$, we deduce from Lemma 32 that $\Delta$ is a square in $\mathbb{Q}_3$. Moreover, $\frac{\Delta}{3v(\Delta)}$ is a 4-th power in $\mathbb{Q}_3$, so one has $L = \mathbb{Q}_{3}^{\text{unr}}(E_2, \sqrt{3})$ (equality (18.2)). Furthermore, $\Delta$ being a square in $\mathbb{Q}_3$, and 3 dividing $[\mathbb{Q}_{3}^{\text{unr}}(E_2) : \mathbb{Q}_3^{\text{unr}}]$, one has $\mathbb{Q}_{3}^{\text{unr}}(E_2) = \mathbb{Q}_{3}^{\text{unr}}(x_0)$. In particular, $L = \mathbb{Q}_{3}^{\text{unr}}(x_0, \sqrt{3})$. Since $[L : \mathbb{Q}_{3}^{\text{unr}}] = 6$ (equality (18.3)), we deduce that $M/\mathbb{Q}_3$ is totally ramified of degree 6 and $E/M$ has good reduction. The fact that $2v(c_6) \neq v(\Delta)$ implies that the reduction is supersingular [10, p. 21, lemme 7].

Let $E'/M$ be an elliptic curve with good reduction isomorphic over $M$ to $E/M$ and $\tilde{E}'/\mathbb{F}_3$ be the elliptic curve obtained from $E'/M$ by reduction. Let $a_{E'} = 4 - |\tilde{E}'(\mathbb{F}_3)|$. Using Lemma 33, the same proof as the one establishing Lemma 29 leads to the equality $a_{E'} = 0$. Let $\alpha \in \mathbb{F}_9$ such that $\alpha^2 = -3$ and $n$ be the least common multiple of the orders of $\alpha$ and $-\alpha$ in $\mathbb{F}_9$. Let $\zeta$ be a primitive 6-th root of unity in $\mathbb{F}_9$. Using exactly the same arguments, lemmas 22-25 are also valid with $\ell = 3$ and the field $M$ defined by (18.5). Since one has $\zeta \neq \pm \zeta^{-1}$ and $\zeta^2 \neq \pm \zeta^{-2}$, we get
\[d = \begin{cases} 3n & \text{if } n \equiv 0 \pmod{2} \text{ and } \alpha^{\frac{n}{2}} = (-\alpha)^{\frac{n}{2}} = -1, \\ 6n & \text{otherwise.} \end{cases}\]

Lemma 34. We have
\[d = \begin{cases} 6\delta & \text{if } \delta \equiv 0 \pmod{2}, \\ 12\delta & \text{if } \delta \equiv 1 \pmod{2}. \end{cases}\]

Proof. As in the proof of Lemma 31, we have $n = 2\delta$.

Suppose $\delta$ even. Let $\delta = 2\delta'$. One has $(-\alpha)^{\frac{\delta'}{2}} = \alpha^{\frac{\delta'}{2}} = \alpha^{2\delta'} = (-3)^{\delta'} = -1$, hence $d = 3n = 6\delta$. If $\delta$ is odd, one has $(-\alpha)^{\frac{\delta'}{2}} \neq \alpha^{\frac{\delta'}{2}}$, so $d = 6n = 12\delta$, hence the result.

To end this section, let us give the link between $\delta$ and $r$ for any prime number $\ell$. We will use this lemma several times.
Lemma 35. We have
\[
\delta = \begin{cases} 
    r & \text{if } r, \delta \text{ are both even}, \\
    \frac{r}{2} & \text{if } r \text{ is even and } \delta \text{ is odd}, \\
    2r & \text{if } r \text{ is odd}. 
\end{cases}
\]

Proof. If \( r \) is odd, the equality \(-\ell = (-1)\ell \) implies \( \delta = 2r \). If both \( \delta \) and \( r \) are even, one has \( \ell^r = (-\ell)^r = 1 \) and \( \ell^\delta = (-\ell)^\delta = 1 \) so that \( \delta \mid r \) and \( r \mid \delta \), thus \( r = \delta \). Suppose \( r \) even and \( \delta \) odd. One has \( (-\ell)^\delta = (-1)^\delta \ell^\delta = 1 \), so \( \ell^{2\delta} = 1 \), and \( r \) divides \( 2\delta \). Moreover, \( \ell^r = (-\ell)^r = 1 \), so \( \delta \) divides \( r \). We obtain \( r = \delta \) or \( r = 2\delta \). This leads to \( r = 2\delta \) because \( r \) and \( \delta \) have not the same parity, hence the result. \( \square \)

Lemmas 34 and 35 now imply Theorem 10 for \( e = 6 \) and \( K \) abelian.

18.5. Case \( e = 6 \) with \( K/Q_3 \) is non-abelian. We have \( j - 1728 = \frac{a^3}{c} \). In particular, \( v(j - 1728) \) is even. From our assumption and Lemma 32, this implies that \( j - 1728 \) is not a square in \( Q_3 \). We conclude the representation \( \sigma_{E,p} : G \to \text{PGL}_2(F_p) \) is of type \( V \) (by [6, Cor. 0.5]). Since \( \Phi \) is cyclic of order 6, one has \( |\sigma_{E,p}(\Phi)| = 3 \), so the extension \( F/Q_3 \) is dihedral of degree 6 ([5], prop. 2.3). This extension is not totally ramified, so the unramified quadratic extension \( \Omega_3(\sqrt{2}) \) of \( Q_3 \) is contained in the field \( F \) fixed by the kernel of \( \sigma_{E,p} \).

The end of the proof is now the same as the one used in section 17.2. Let \( d' = [K : F] \). One has \( d = 6d' \). In case \( r \) is even, \( \sqrt{2} \) belongs to \( Q_3(\mu_p) \), so \( [F(\mu_p) : F] = \frac{r}{2} \). The ramification index of \( K/F \) is equal to 2, consequently 2 divides \( d' \). The equality (17.1) then leads to \( d' = r \), and \( d = 6r \) as stated. If \( r \) odd, then \( \sqrt{2} \) does not belong to \( Q_3(\mu_p) \). This implies \( F \cap Q_3(\mu_p) = Q_3 \) and \( [F(\mu_p) : F] = r \). We then conclude that \( d' = 2r \) and \( d = 12r \), hence the result.

18.6. Case \( e = 12 \). Recall that \( K = Q_3(E_p) \). Let
\[
M = Q_3\left(E_2, \Delta^{\frac{1}{2}}\right).
\]
Recall that we have \( Q_3(E_2) = Q_3\left(\sqrt{\Delta}, x_0\right) \) with \( x_0 \) being a root of the 2-division polynomial of \( E/Q_3 \). In particular, \( [M : Q_3] \leq 12 \).

Lemma 36. The extension \( M/Q_3 \) is totally ramified of degree 12 and \( E/M \) has good supersingular reduction.

Proof. We have \( [L : Q_3^{\text{num}}] = 12 \) (equality (18.3)), so \( M/Q_3 \) is totally ramified of degree 12 and \( E/M \) has good reduction. We have \( 2v(c_0) = 2v(\Delta) \) (see [9, cor. p. 355]) so the reduction is supersingular (see [10, p. 21, lemme 7]). \( \square \)

Lemma 37. We have \( [K \cap M : Q_3] \in \{6, 12\} \).

Proof. Let \( E'/M \) be an elliptic curve with good reduction isomorphic over \( M \) to \( E/M \) and \( E'/\mathbb{F}_3 \) be the curve obtained from \( E'/M \) by reduction. Let \( a_{E'} = 4 - |E'(\mathbb{F}_3)| \). The points of order 2 of \( E'/M \) are rational over \( M \), so 4 divides \( a_{E'} \), and the Weil bound implies \( a_{E'} = 0 \). From Corollary 1, we conclude
\[
[M(E_p) : M] = 2\delta.
\]
From Lemma 35 we have \( \delta \in \{ \frac{r}{2}, r, 2r \} \), so
\[
d = [K \cap M : \mathbb{Q}_3]u \quad \text{with} \quad u \in \{ r, 2r, 4r \}.
\]
Moreover, \( 12r \) divides \( d \), hence \( [K \cap M : \mathbb{Q}_3] \neq 1, 2, 4 \).

Suppose \( [K \cap M : \mathbb{Q}_3] = 3 \). Then \( K \cap M \) is contained in \( \mathbb{Q}_3(E_2) \), otherwise \( M/K \cap M \) would be an extension of degree divisible by 3, hence 9 would divide \( [M : \mathbb{Q}_3] \), a contradiction. Since \( K/\mathbb{Q}_3 \) is Galois, this implies that \( K \cap M = \mathbb{Q}_3(E_2) \) which leads to a contradiction, hence the lemma.

The representation \( \sigma_{E,p} : G \to \text{PGL}_2(\overline{\mathbb{F}}_p) \) is of type \( \text{H} \) by [6, Prop. 0.4]. From [5, Proposition 2.4], we see that \( \sigma_{E,p}(\Phi) \) is dihedral of order 6. Furthermore, \( F \) being the fixed field by the kernel of \( \sigma_{E,p} \), implies \( [F : \mathbb{Q}_3] = 6 \) or \( [F : \mathbb{Q}_3] = 12 \) (loc. cit.).

Let \( d' = [K : F] \). We have \( d \in \{ 6d', 12d' \} \) and, furthermore, (17.1) is still true.

**Lemma 38.** If \( [F : \mathbb{Q}_3] = 6 \), then \( d = 12r \).

**Proof.** Since \( |\sigma_{E,p}(\Phi)| = 6 \), our assumption implies that the extension \( F/\mathbb{Q}_3 \) is totally ramified. We have \( e = 12 \), so 2 divides \( d' \) and (17.1) leads to \( d' = 2r \), hence the lemma.

**Lemma 39.** If \( r \) is even, then \( d = 12r \).

**Proof.** From Lemma 38 we can suppose \( [F : \mathbb{Q}_3] = 12 \). Since \( r \) is even, the quadratic unramified extension of \( \mathbb{Q}_3 \) is contained in \( \mathbb{Q}_3(\mu_p) \). It is also contained in \( F \) because the ramification index of \( F/\mathbb{Q}_3 \) is 6. So we have \( [F \cap \mathbb{Q}_3(\mu_p) : \mathbb{Q}_3] = 2 \), hence \( [F(\mu_p) : F] = 2 \).

Using (17.1), the ramification index of \( K/F \) being equal to 2, we conclude \( d' = r \), so \( d = 12r \), as desired.

**Lemma 40.** Suppose \( r \) is odd. We have \( [K \cap M : \mathbb{Q}_3] = 6 \) and \( d = 24r \).

**Proof.** Suppose \( [K \cap M : \mathbb{Q}_3] = 12 \). Then \( M \subseteq K \), so \( d = 12(2\delta) = 24\delta \) by Corollary 1. Since \( r \) is odd, one has \( \delta = 2r \) (Lemma 35), so \( d = 48r \). Moreover, from Lemma 38, we deduce that \( [F : \mathbb{Q}_3] = 12 \) and (17.1) implies \( d' \leq 2r \), so \( d \leq 24r \), hence a contradiction. We so obtain \( [K \cap M : \mathbb{Q}_3] = 6 \) (Lemma 37) and we deduce that \( d = 6(2\delta) = 6(4r) = 24r \) as stated.

This concludes the proof of Theorem 10.

19. **Proof of Theorem 12.**

Let \( E/\mathbb{Q}_2 \) be an elliptic curve with additive potentially good reduction with \( e \neq 2 \).

Let \( \rho_{E,p} : \text{Gal}(\overline{\mathbb{Q}_2}/\mathbb{Q}_2) \to \text{GL}_2(\overline{\mathbb{F}}_p) \) be the representation arising on the \( p \)-torsion points of \( E \).

Write \( K = \mathbb{Q}_2(E_p) \) for the field fixed by the kernel of \( \rho_{E,p} \) whose degree is \( d = [K : \mathbb{Q}_2] \).

Let the projective representation obtained from \( \rho_{E,p} \otimes \overline{\mathbb{F}}_p \) be denoted by
\[
\sigma_{E,p} : \text{Gal}(\overline{\mathbb{Q}_2}/\mathbb{Q}_2) \to \text{PGL}_2(\overline{\mathbb{F}}_p)
\]
and write \( F \) for the field fixed by its kernel.

We will write \( \Phi \) for both the inertia subgroups of \( \text{Gal}(\overline{\mathbb{Q}_2}/\mathbb{Q}_2) \) and \( G = \text{Gal}(K/\mathbb{Q}_2) \).
19.1. Case $e = 3$. Suppose that $E / \mathbb{Q}_2$ satisfies $e = 3$. Let $\pi \in \overline{\mathbb{Q}}_2$ be a cubic root of 2. Write $M = \mathbb{Q}_2(\pi)$. The extension $M / \mathbb{Q}_2$ is totally ramified of degree 3.

**Lemma 41.** The elliptic curve $E / \mathbb{Q}_2$ acquires good supersingular reduction over $M$.

*Proof.* The field $\mathbb{Q}_2^{unr}(\pi)$ is the unique extension of degree 3 of $\mathbb{Q}_2^{unr}$. Since $e = 3$, the elliptic curve $E / M$ has good reduction. Since $v(j) > 0$ (see [9]), so the $j$ invariant modulo 2 is 0, which is supersingular in characteristic 2. \[ \square \]

We have $\ell = 2 \equiv -1 \pmod{e}$. It follows from [8, Corollary 3 and Lemma 5] that $K / \mathbb{Q}_2$ in non-abelian and $M$ is contained in $K$. We conclude that

\begin{equation}
(19.1) \quad d = 3[M(E_\pi) : M].
\end{equation}

Let $E'/M$ be an elliptic curve with good reduction isomorphic over $M$ to $E/M$. Since $E'/M$ has supersingular reduction, its trace of Frobenius satisfies $a_{E'} \in \{-2, 0, 2\}$.

**Lemma 42.** We have $a_{E'} = 0$.

*Proof.* The residue field of $M$ is $\mathbb{F}_2$, so $a_{E'} = 3 - |\tilde{E}'(\mathbb{F}_2)|$, where $\tilde{E}'$ is the reduction of $E'$. We will show $E/M$ has a rational 3-torsion point over $M$. Together with the Weil bound, this gives the desired result. Let $\chi_3 : \Gal(\overline{\mathbb{Q}}_2 / \mathbb{Q}_2) \to \mathbb{F}_3^*$ be the mod 3 cyclotomic character. From [8, Proposition 8], the representation $\rho_{E,3}$ is of one of the following types

\[ \begin{pmatrix} 1 & * \\ 0 & \chi_3 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \chi_3 & * \\ 0 & 1 \end{pmatrix}, \]

in particular its image is of order 6. So the restriction of $\rho_3$ to $\Gal(\overline{\mathbb{Q}}_2 / M)$ is of the shape

\[ \begin{pmatrix} 1 & 0 \\ 0 & \chi_3 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \chi_3 & 0 \\ 0 & 1 \end{pmatrix}, \]

hence the result. \[ \square \]

From Lemma 41 and Corollary 1 we conclude $[M(E_\pi) : M] = 2\delta$. Now equation (19.1) gives $d = 6\delta$, as desired.

19.2. Case $e = 4$. Suppose that $E / \mathbb{Q}_2$ satisfies $e = 4$. We consider the 3-torsion field $M = \mathbb{Q}_2(E_3)$.

**Lemma 43.** We have $[M : \mathbb{Q}_2] = 8$ and $E / M$ has good supersingular reduction.

*Proof.* It follows from $e = 4$ and Table 1 and Proposition 4 of [7] that $[M : \mathbb{Q}_2] = 8$. Since $v(j) > 0$ (see [9]), so the $j$ invariant modulo 2 is 0, which is supersingular in characteristic 2. \[ \square \]

Let $E'/M$ be an elliptic curve of good reduction isomorphic over $M$ to $E/M$. The residue field of $M$ is $\mathbb{F}_4$ and $\tilde{E}' / \mathbb{F}_4$ has full 3-torsion over $\mathbb{F}_4$. It follows from $a_{E'} = 5 - |\tilde{E}'(\mathbb{F}_4)|$ and the Weil bound that $|\tilde{E}'(\mathbb{F}_4)| = 9$ and $a_{E'} = -4$. Moreover, $\Delta_{E'} = a_{E'}^2 - 4 \cdot 2^2 = 0$ so (by [2,
Theorem 2]) the Frobenius element $\text{Frob}_M$ of the extension $M(E_p)/M$ is representable by
the matrix $\begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}$. It is the homothety of ratio $-2$. Consequently, one has

\begin{equation}
[M(E_p) : M] = \delta.
\end{equation}

Lemma 44. We have $K \cap M \neq \mathbb{Q}_2$.

Proof. Suppose $K \cap M = \mathbb{Q}_2$. Then the Galois groups of $K/\mathbb{Q}_2$ and $M(E_p)/M$ are isomorphic.
Let $\sigma$ be a generator of the inertia subgroup of $\text{Gal}(K/\mathbb{Q}_2)$. The element $\rho_{E,p}(\sigma)$ belongs to
$\text{SL}_2(\mathbb{F}_p)$ and is of order 4. Consequently, there exists $U \in \text{GL}_2(\mathbb{F}_p)$ such that

$$U \rho_{E,p}(\sigma) U^{-1} = \begin{pmatrix} \zeta_4 & 0 \\ 0 & -\zeta_4 \end{pmatrix}.$$  

The restriction of the Frobenius $\text{Frob}_M \in \text{Gal}(M(E_p)/M)$ to $K$ is the homothety of ratio $-2$
and it is a generator of $\text{Gal}(K/\mathbb{Q}_2)$. So there exists $k = 1, \ldots, \delta$ such that

$$\begin{pmatrix} \zeta_4 & 0 \\ 0 & -\zeta_4 \end{pmatrix} = \begin{pmatrix} (-2)^k & 0 \\ 0 & (-2)^k \end{pmatrix},$$

which leads to a contradiction, hence the result. \qed

Lemma 45. Suppose $K/\mathbb{Q}_2$ is abelian. Then $\text{Gal}(M/\mathbb{Q}_2)$ is cyclic of order 8.

Proof. From [8, Proposition 6] it follows that $M/\mathbb{Q}_2$ is abelian and [7, Table 1] gives the conclusion, since $M/\mathbb{Q}_3$ is of degree 8. \qed

Lemma 46. We have $\mu_3 \subseteq K$.

Proof. From Lemma 44 we know $[K \cap M : \mathbb{Q}_2] \geq 2$.

1) Suppose $K/\mathbb{Q}_2$ is abelian. Then Lemma 45 implies that $K \cap M/\mathbb{Q}_2$ contains the quadratic
unramified extension (the ramification degree of $M$ is $e = 4$), as desired.

2) Suppose $K/\mathbb{Q}_2$ is non-abelian. Because $\Phi$ is cyclic of order 4, the representation $\rho_{E,p}$ is
of type $V$ (by [5, Proposition 2.3]). Since $|\sigma_{E,p}(\Phi)| = 2$, we conclude from condition 3 of [5,
Proposition 2.3] that the image of $\sigma_{E,p}$ is dihedral of order 4. We have $F \subseteq K$ and $F/\mathbb{Q}_2$ is
not totally ramified. Thus $\mu_3 \subseteq F \subseteq K$. \qed

Lemma 47. The field $\mathbb{Q}_2(\mu_3)$ is strictly contained in $K \cap M$. In particular,

\begin{equation}
[K \cap M : \mathbb{Q}_2] \in \{4, 8\}.
\end{equation}

Proof. Since $\mu_3 \subseteq M$ by Lemma 46 we have $\mu_3 \subseteq K \cap M$. Suppose $K \cap M = \mathbb{Q}_2(\mu_3)$. Then
$\mu_3$ is fixed by the generator $\sigma$ of the inertia subgroup of $\text{Gal}(K/\mathbb{Q}_2)$. Up to conjugation, we
have $\rho_{E,p}(\sigma) = \begin{pmatrix} \zeta_4 & 0 \\ 0 & -\zeta_4 \end{pmatrix}$. The Galois groups $K/\mathbb{Q}_2(\mu_3)$ and $M(E_p)/M$ are isomorphic, so
there exist (as in Lemma 44) an integer $k = 1, \ldots, \delta$ such that

$$\begin{pmatrix} \zeta_4 & 0 \\ 0 & -\zeta_4 \end{pmatrix} = \begin{pmatrix} (-2)^k & 0 \\ 0 & (-2)^k \end{pmatrix},$$

which gives a contradiction. Now Lemma 43 implies (19.3). \qed
Lemma 48. There exists \( k = 1, \ldots, \delta \) such that
\[
\begin{pmatrix}
(-2)^k & 0 \\
0 & (-2)^k
\end{pmatrix} = -1
\]
if and only if \( \delta \) is even.

Proof. If \( \delta \) is even, one has \((-2)^\delta = -1\). Conversely, suppose there exists \( k = 1, \ldots, \delta \) such that \((-2)^k = -1\). One has \((-2)^{2k} = 1\), so \( \delta \) divides \( 2k \). If \( \delta \) is odd, then \( \delta \) divides \( k \), so \( k = \delta \) which is false, so \( \delta \) is even, hence the lemma.

\( \square \)

Lemma 49. We have the following equivalence
\[
M \subseteq K \iff \delta \equiv 1 \pmod{2}.
\]

Proof. Let \( \tau \) be the element of order 2 of the inertia subgroup of \( \text{Gal}(K/\mathbb{Q}_2) \). Its image \( \rho_{E,p}(\tau) \) is in \( \text{SL}_2(\mathbb{F}_p) \) and is of order 2, so
\[
\rho_{E,p}(\tau) = -1.
\]
Suppose \( M \not\subseteq K \). Then, Lemma 47 implies both \([K \cap M : Q_2] = 4\) and the ramification index of the extension \( K \cap M / Q_2 \) is equal to 2. We conclude that \( \tau \in \text{Gal}(K/K \cap M) \). Since the Frobenius \( \text{Frob}_M \in \text{Gal}(M(E_p)/M) \) restricts to a generator of \( \text{Gal}(K/K \cap M) \), there exists \( k = 1, \ldots, \delta \), such that \((-2)^k = -1\). Thus \( \delta \) is even by Lemma 48.

Conversely, suppose \( M \subseteq K \); then \( K/M \) is unramified. In particular, \( \tau \) does not belong to \( \text{Gal}(K/M) \), which is generated by \( \text{Frob}_M \) (because \( M(E_p) = K \)). From (19.5), it follows there does not exist \( k = 1, \ldots, \delta \) such that \((-2)^k = -1\); thus \( \delta \) is odd by Lemma 48.

\( \square \)

Corollary 2. The degree \( d = [K : \mathbb{Q}_2] \) satisfies
\[
d = \begin{cases} 
4\delta & \text{if } \delta \text{ is even}, \\
8\delta & \text{if } \delta \text{ is odd}.
\end{cases}
\]

Proof. If \( \delta \) is even, \( M \) is not contained in \( K \) (Lemma 49) so \([K \cap M : \mathbb{Q}_2] = 4\) (Lemma 47). The equality (19.2) then implies \( d = 4\delta \).

If \( \delta \) is odd, \( M \) is contained in \( K \), so \( d = 8\delta \), as desired.

\( \square \)

Corollary 2 and Lemma 35 complete the proof of Theorem 12 for \( e = 4 \).

19.3. Case \( e = 6 \). Suppose that \( E/\mathbb{Q}_2 \) satisfies \( e = 6 \). After a suitable quadratic twist we have \( e = 3 \) and since \( \ell = 2 \equiv -1 \pmod{3} \) we conclude that \( K \) is non-abelian ([8, Corollary 3]). A similar argument to the case \( e = 6 \) in the proof of Theorem 8 part 2) gives the result.
19.4. **Case** \( e = 8 \). Suppose that \( E/Q_2 \) satisfies \( e = 8 \). We consider the fields

\[
M = Q_2(E_3), \quad K = Q_2(E_p), \quad L = K \cap M
\]

which are three Galois extensions of \( Q_\ell \).

Since \( e = 8 \), it is well known that \( \Phi \subset \text{Gal}(K/Q_2) \) is isomorphic to quaternion group.

**Lemma 50.** The image \( \sigma_{E,p}(\Phi) \) is non-cyclic of order 4 and the Galois group \( \text{Gal}(F/Q_2) \) is dihedral of order dividing 8.

**Proof.** Since \( \Phi \) is isomorphic to quaternion group, its center \( C \) is of order 2 and \( \Phi/C \) is isomorphic to the Klein group of order 4. The result now follows from condition 3 of [5, Proposition 2.4]. \( \square \)

**Lemma 51.** The degree \( d = [K : Q_2] \) satisfies \( d \in \{8r, 16r\} \).

**Proof.** We have \( r = [Q_2(\mu_p) : Q_2] \) and the unramified extension \( Q_2(\mu_p)/Q_2 \) is contained in \( K \); moreover, the inertia subgroup \( \Phi \subset \text{Gal}(K/Q_2) \) is of order 8. Then \( 8r \mid d \).

Write \( H = \text{Gal}(K/F) \). There exists a character \( \varphi : H \to \mathbb{F}_p^* \) such that

\[
\rho_{E,p}|_H = \begin{pmatrix} \varphi & 0 \\ 0 & \varphi \end{pmatrix} \quad \text{and} \quad \varphi^2 = \chi_p|_H.
\]

The order of \( \varphi \) is \( d' = [K : F] \) and the order of \( \chi_p|_H \) is \( \frac{d'}{\gcd(d', 2)} \) and it divides \( r \). Hence \( d' \leq 2r \) and from Lemma 50, we have \( [F : Q_2] \leq 8 \). Thus \( d \leq 16r \) and the lemma follows. \( \square \)

**Lemma 52.** The Galois group \( \text{Gal}(M/Q_2) \) is semidihedral of order 16.

**Proof.** This follows from Table 1 in [7]. \( \square \)

**Lemma 53.** We have \( [L : Q_2] \in \{4, 8, 16\} \).

**Proof.** The same argument leading to equality (19.2) shows that here we also have

\[
[M(E_p) : M] = \delta.
\]

Thus \( d = \delta[L : Q_2] \). From Lemma 35 we conclude that \( [L : Q_2] = 4, 8, 16 \) or 32. Note the last case is impossible due to Lemma 52, completing the proof. \( \square \)

Let us denote by \( SD_{16} \) the semidihedral group of order 16.

**Corollary 3.** We have \( \mu_3 \subseteq K \).

**Proof.** This is clear if \( [L : Q_2] = 16 \) i.e. \( L = M \) (because \( \mu_3 \subseteq M \)).

Suppose \( [L : Q_2] = 8 \). The only normal subgroup of \( SD_{16} \) of order 2 is its center and its quotient is dihedral. Thus \( L/Q_2 \) is a dihedral extension of order 8. Consequently, \( L/Q_2 \) is not totally ramified, because \( \Phi \) is the quaternion group, hence \( Q_2(\mu_3) \subset L \).

Suppose \( [L : Q_2] = 4 \). We will again show that \( L/Q_2 \) is not totally ramified, which gives the result. The Galois group \( \text{Gal}(M/L) \) is a normal subgroup of order 4 of \( \text{Gal}(M/Q_2) \). There is only one normal subgroup of order 4 of \( SD_{16} \), and it is cyclic (its derived subgroup). Moreover, \( SD_{16} \) has exactly three cyclic subgroups of order 4 and one subgroup isomorphic
to $H_8$. The group $H_8$ has also exactly three cyclic subgroups of order 4. We deduce that the cyclic subgroups of order 4 of $\text{Gal}(M/Q_2)$ are contained in its inertia subgroup. This implies that $L/Q_2$ is not totally ramified, hence the result.

We can now complete the proof of Theorem 12 in the case $e = 8$.

1) Suppose $r$ odd. Then $\mu_3 \notin Q_2(\mu_p)$. Since $Q_2(\mu_3) \subseteq K$ by Corollary 3, we deduce that the degree of the maximal unramified subfield of $K$ is at least $2r$. This implies $d \geq 16r$, so $d = 16r$ by Lemma 51.

2) Suppose $r$ even. Then $\mu_3 \in Q_2(\mu_p)$. From Lemma 50 we have that $F/Q_2$ is dihedral with ramification index 4 and of degree $[F : Q_2] = 8$ or $[F : Q_2] = 4$. Write $d' = [K : F]$.

Suppose $[F : Q_2] = 8$. We have $Q_2(\mu_p) \cap F = Q_2(\mu_3)$. The Galois groups $\text{Gal}(F(\mu_p)/F)$ and $\text{Gal}(Q_2(\mu_p)/Q_2(\mu_p) \cap F)$ being isomorphic, we deduce that

$$[F(\mu_p) : F] = \frac{r}{2}.$$ 

Using the notations in the proof of Lemma 51, we have that the order of $\chi_p|_H$ is $\frac{r}{2}$, which leads to the equality

$$\frac{d'}{\gcd(d', 2)} = \frac{r}{2}.$$ 

Since the ramification index of $K/F$ is 2, we have $2 \mid d'$. Thus $d' = r$ and $d = 8r$.

Suppose $[F : Q_2] = 4$. We have

$$\frac{d'}{\gcd(d', 2)} = [F(\mu_p) : F] \leq r.$$ 

So $d' \leq 2r$, which implies $d \leq 8r$. Then $d = 8r$ by Lemma 51, as desired.

19.5. **Case** $e = 24$. Suppose that $E/Q_2$ satisfies $e = 24$. We consider the fields

$$M = Q_2(E_3), \quad K = Q_2(E_p), \quad L = K \cap M$$

which are three Galois extensions of $Q_2$. Since $e = 24$, it is well known that $\Phi \in \text{Gal}(K/Q_2)$ is isomorphic to $\text{SL}_2(\mathbb{F}_3)$ and $\text{Gal}(M/Q_2) \simeq \text{GL}_2(\mathbb{F}_3)$.

**Lemma 54.** The image $\sigma_{E,p}(\Phi)$ is of order 12 isomorphic to $A_4$. Moreover, the Galois group $\text{Gal}(F/Q_2)$ is isomorphic to $A_4$ or $S_4$.

**Proof.** The only scalar matrices in $\text{SL}_2(\mathbb{F}_p)$ are $\pm 1$, therefore $\sigma_{E,p}(\Phi) \simeq \text{SL}_2(\mathbb{F}_3)/\{\pm 1\} \simeq A_4$, proving the first statement. Now, the condition 3 of [5, Proposition 2.4] implies the second statement.

**Lemma 55.** The degree $d = [K : Q_2]$ satisfies $d \in \{24r, 48r\}$.

**Proof.** We have $[F : Q_2] = 12$ or 24 by Lemma 54. Since $Q_2(\mu_p) \subseteq K$ we have $24r \mid d$. Now, a similar argument to Lemma 51 shows that $[K : F] \leq 2r$. Then $d \leq 48r$ and the result follows.

**Lemma 56.** We have $[L : Q_2] \in \{24, 48\}$. 

34
we conclude $[L : Q_2] \geq 12$. We have $[L : Q_2] \neq 16$, otherwise $d$ would be $8r$, $16r$ or $32r$ by Lemma 35, which is false by Lemma 52. Finally, $[L : Q_2] \neq 12$, because $\text{GL}_2(F_3)$ has not normal subgroups of order 4. The result follows.

\begin{proof}
The result is clear when $[L : Q_2] = 48$ i.e. if $L = M$.

Suppose $[L : Q_2] = 24$. The only normal subgroup of order 2 of $\text{GL}_2(F_3)$ is its center $C$. It is contained in $\text{SL}_2(F_3)$ and $\text{GL}_2(F_3)$ contains a unique subgroup isomorphic to $\text{SL}_2(F_3)$. We deduce that $C$ is contained in the inertia subgroup of $\text{Gal}(M/Q_2)$, so the extension $M/L$ is ramified. Therefore, $L/Q_2$ is not totally ramified, which implies $\mu_3 \subseteq L \subseteq K$.

We can now complete the proof in the case $e = 24$.

1) Suppose $r$ odd. Then $\mu_3 \nsubseteq Q_2(\mu_p)$. Since $Q_2(\mu_3) \subseteq K$ by Corollary 4, we deduce that the degree of the maximal unramified subfield of $K$ is at least $2r$. This implies $d \geq 48r$, so $d = 48r$ by Lemma 55.

2) Suppose $r$ even. Then $\mu_3 \subseteq Q_2(\mu_p)$. From Lemma 54 we have that $F/Q_2$ has ramification index 12 and degree $[F : Q_2] = 12$ or $[F : Q_2] = 24$. Write $d' = [K : F]$.

Suppose $[F : Q_2] = 24$. Let us show that $d' = r$. The Galois group of $F/Q_2$ is isomorphic to $S_4$ by Lemma 54. This extension is not totally ramified, thus $Q_2(\mu_p) \cap F = Q_2(\mu_3)$. The Galois groups $\text{Gal}(F(\mu_p)/F)$ and $\text{Gal}(Q_2(\mu_p)/Q_2(\mu_p) \cap F)$ being isomorphic, we conclude that

$$[F(\mu_p) : F] = \frac{r}{2}.$$  

This leads to the equality

$$\frac{d'}{\gcd(d', 2)} = \frac{r}{2}.$$  

The ramification index of $K/F$ is equal to 2, so 2 divides $d'$. We obtain $d' = r$, thus $d = 24d' = 24r$.

Suppose $[F : Q_2] = 12$. We have

$$\frac{d'}{\gcd(d', 2)} = [F(\mu_p) : F] \leq r.$$  

So $d' \leq 2r$, which implies $d \leq 24r$. Then, by Lemma 55, $d = 24r$, completing the proof.

\section*{References}

[1] É. Cali and A. Kraus, \textit{Sur la p-différente du corps des points de ℓ-torsion des courbes elliptiques, ℓ ≠ p}, Acta Arithm. \textbf{104} (2002) 1–21.

[2] T. Centeleghe, \textit{Integral Tate modules and splitting of primes in torsion fields of elliptic curves}, Int. J. Number Theory \textbf{12} (2016), no. 1, 237–248.

[3] T. Centeleghe and P. Tsaknias, \textit{Integral Frobenius}, Magma package available at \url{http://math.uni.lu/~tsaknias/swfware.html}

[4] W. Duke and Á. Tóth, \textit{The splitting of primes in division fields of elliptic curves} Experimental Math. \textbf{11} (2002) 555–665.
[5] F. Diamond, *An extension of Wiles’ results*, Modular forms and Fermat’s Last theorem (Boston, MA, 1995), 475–489, Springer, New York, 1997. 17.2, 17.2, 18.5, 18.6, 19.2, 19.4, 19.5

[6] F. Diamond and K. Kramer, *Appendix: Classification of $\bar{\rho}_{E,\ell}$ by the $j$-invariant of $E$*, Modular forms and Fermat’s Last theorem (Boston, MA, 1995), 491–498, Springer, New York, 1997. 17.2, 18.5, 18.6

[7] T. Dokchitser and V. Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bull. London Math. Soc. 40 (2008), 516–524. 19.2, 19.2, 19.4

[8] N. Freitas and A. Kraus, *On the symplectic type of isomorphisms of the $p$-torsion of elliptic curves*, arXiv:1607.01218v3 (2017). 9, 14.1, 14.2, 15, 16.1, 16.2, 17, 18.3, 19.1, 19.1, 19.2, 19.3

[9] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta. Math., 69 (1990), 353–385. 1, 5, 6, 7, 8, 18, 18, 18.3, 18.6, 19.1, 19.2

[10] A. Kraus, *Détermination du poids et du conducteur associés aux représentations des points de $p$-torsion des courbes elliptiques*, Dissertationes Math. (1997). 14.1, 18.1, 18.4, 18.6

[11] W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, J. Symb. Comp. 24 (1997), 235–265. (See also http://magma.maths.usyd.edu.au/magma/) 2

[12] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3*, J. Number Theory, 44 (1993), 119–152. 11.3, 11.4

[13] S. Pauli and X-F Roblot, *On the computation of all extensions of a $p$-adic field of a given degree* Math. Comp., 70 number 236, (2001), 1641–1659. 17.2

[14] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition, Graduate Texts in Mathematics 106, Springer, 2009. 10, 12

[15] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Math. 88 (1968), no. 2, 492–517. 9

Mathematics Institute, University of Warwick, CV4 7AL, United Kingdom

E-mail address: nunobfreitas@gmail.com

Université Pierre et Marie Curie - Paris 6, Institut de Mathématiques de Jussieu, 4 Place Jussieu, 75005 Paris, France

E-mail address: alain.kraus@imj-prg.fr