PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 139, Number 6, June 2011, Pages 1961–1969
S 0002-9939(2010)10621-4
Article electronically published on November 9, 2010

ON FIELDS OF DEFINITION OF TORSION POINTS OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

LUIS DIEULEFAIT, ENRIQUE GONZÁLEZ-JIMÉNEZ, AND JORGE JIMÉNEZ URROZ

(Communicated by Ken Ono)

Abstract. For any elliptic curve E defined over the rationals with complex multiplication (CM) and for every prime p, we describe the image of the mod p Galois representation attached to E. We deduce information about the field of definition of torsion points of these curves; in particular, we classify all cases where there are torsion points over Galois number fields not containing the field of definition of the CM.

1. Introduction

Elliptic curves defined over the rationals have been extensively studied for over a hundred years, mainly because we know that the set of rational points forms a finitely generated abelian group. In this paper we are interested in giving a description of the possible finite groups that can be realized in this way. If we focus on the torsion subgroup, the problem is solved: we know every possible group that appears as the rational torsion subgroup of an elliptic curve over the rationals.

However, when considering more general number fields, many questions about the torsion remain unsolved. Here we approach this problem from the following point of view: we are interested in studying how does the torsion subgroup of an elliptic curve change when we enlarge the field of definition. As a first step of this project, we are going to consider elliptic curves defined over $\mathbb{Q}$.

The first results on this problem dealt with the case of quadratic number fields. For this case, Kwon [3] has given results allowing us to compute the torsion subgroup over a quadratic field of an elliptic curve defined over the rationals that has all the 2-torsion subgroups defined over the rationals. First Qiu and Zhang [4] and then completed by Fujita [2] have generalized Kwon's result to the case of polyquadratic number fields.

We will focus on the complex multiplication (CM) case. We have proved results that give all the information about the field of definition of torsion points for CM elliptic curves defined over $\mathbb{Q}$. In particular, we have classified all cases where there are torsion points over Galois number fields not containing the field of definition of

Received by the editors March 16, 2010 and, in revised form, June 2, 2010.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80.

Key words and phrases. Elliptic curves, torsion, Galois representation.

The authors were partially supported by the grants MTM2006-04895 (Ministerio de Educación y Ciencia of Spain), MTM2009-07291 (Ministerio de Ciencia e Innovación of Spain), CCG08-UAM/ESP-3906 (Universidad Autónoma de Madrid and Comunidad de Madrid), and MTM2009-11068 (Ministerio de Ciencia e Innovación of Spain) respectively.

the CM. We also give a description of the image of the Galois representations on the p-torsion of all these curves for every prime p.

As is well-known, the mod p Galois representations attached to an elliptic curve behave in two very different ways depending on whether or not the curve has CM. Contrary to what happens in the CM case, in the non-CM case Serre [5] proved that the images of the mod p Galois representations are maximal, i.e., equal to $\mathrm{GL}_2(\mathbb{F}_p)$ for all but finitely many primes.

Notation. • Let F be a number field. We will denote by $\mathcal{O}_F$ the ring of integers of F.

• Let p be an odd prime. We will denote by ζ_p a primitive p^{th}-root of the unity and by $\mathbb{Q}^+(\zeta_p)$ the maximal real subfield of the p^{th}-cyclotomic field $\mathbb{Q}(\zeta_p)$, that is, $\mathbb{Q}^+(\zeta_p) = \mathbb{Q}(\zeta_p + \overline{\zeta}_p)$. Note that $\sqrt{-p}$ (respectively $\sqrt{p}$) belongs to $\mathbb{Q}(\zeta_p)$ if $p \equiv 3 (\bmod 4)$ (respectively $p \equiv 1 (\bmod 4)$).

• Let E be an elliptic curve defined over F. The m-torsion subgroup of $E(F)$ will be denoted by $E(F)[m] = \{P \in E(F) \mid [m]P = \mathcal{O}\}$ and by $E[m] = E(\overline{F})[m]$.

• We will denote by $F(E[m])$ the number field obtained by adjoining the coordinates of the points of order m.

• Let p be a prime. We will denote by $\rho_{E,p}$ the mod p Galois representation attached to the p-torsion points of E.

• χ will denote the mod p cyclotomic character, where the prime p will be clear by the context.

• We will denote by $j(E)$ the j-invariant of the elliptic curve E.

2. Elliptic curve with complex multiplication over $\mathbb{Q}$

It is well known that there are 13 isomorphic classes of elliptic curves defined over $\mathbb{Q}$ with CM (cf. [7, A §3]). Table 1 gives a representative elliptic curve over $\mathbb{Q}$ for each class, that is, an elliptic curve over $\mathbb{Q}$ with CM by an order $R = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ of conductor $\mathfrak{f}$ in a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$, where $\mathcal{O}_K$ is the ring of integers of K. We will denote by $E_{D,\mathfrak{f}}$ this elliptic curve.

Table 1. Isomorphic classes of elliptic curves defined over $\mathbb{Q}$ with CM.

$-D$	$\mathfrak{f}$	Short Weierstrass model of $E_{D,\mathfrak{f}}$
-3	1	$y^2 = x^3 + 16$
-3	2	$y^2 = x^3 - 15x + 22$
-3	3	$y^2 = x^3 - 480x + 4048$
-4	1	$y^2 = x^3 + x$
-4	2	$y^2 = x^3 - 11x + 14$
-7	1	$y^2 = x^3 - 2835x - 71442$
-7	2	$y^2 = x^3 - 595x + 5586$
-8	1	$y^2 = x^3 - 4320x + 96768$
-11	1	$y^2 = x^3 - 9504x + 365904$
-19	1	$y^2 = x^3 - 608x + 5776$
-43	1	$y^2 = x^3 - 13760x + 621264$
-67	1	$y^2 = x^3 - 117920x + 15585808$
-163	1	$y^2 = x^3 - 34790720x + 78984748304$

Let E be an elliptic curve defined over $\mathbb{Q}$. We know that any $E'/\mathbb{Q}$ isomorphic to E over $\overline{\mathbb{Q}}$ is in fact $\mathbb{Q}$-isomorphic to a twist of E (cf. [6, X §5]). More precisely, let $E : y^2 = x^3 + ax + b$ be a Weierstrass model for E, and E' a curve isomorphic to E. We will denote once and for all

$$n(E) = \begin{cases} 2 & \text{if } j(E) \neq 0, 1728, \\ 4 & \text{if } j(E) = 1728, \\ 6 & \text{if } j(E) = 0. \end{cases}$$

T hen, $E' = E^d$ has a Weierstrass model of the form

$$\begin{array}{lll} \text{(i)} & E^d : y^2 = x^3 + d^2ax + d^3b & \text{if } j(E) \neq 0, 1728, \\ \text{(ii)} & E^d : y^2 = x^3 + dax & \text{if } j(E) = 1728, \\ \text{(iii)} & E^d : y^2 = x^3 + db & \text{if } j(E) = 0, \end{array}$$

where d is an integer in $\mathbb{Q}^*/(\mathbb{Q}^*)^{n(E)}$. In particular, any CM elliptic curve E defined over $\mathbb{Q}$ is in fact $\mathbb{Q}$-isomorphic to a curve $E^d_{D,\mathfrak{f}}$ for some D, f as in Table 1, and d an integer in $\mathbb{Q}^*/(\mathbb{Q}^*)^{n(E)}$.

As we mentioned, in order to study the torsion of the elliptic curve, we will be using the mod p Galois representation of the elliptic curve, for any prime p. It is then important to note that, for $j(E) \neq 0, 1728$, if $\rho_{E_{D,\mathfrak{f}},p}$ is the representation associated to $E_{D,\mathfrak{f}}$, then

$$\rho_{E^d_{D,\mathfrak{f}},p} = \rho_{E_{D,\mathfrak{f}},p} \otimes \psi(d) \tag{1}$$

is the twisted representation by the Legendre symbol $\psi(d) = \left(\frac{d}{p}\right)$. For the general case, we can look at the number of points of the reduced curve to get information about the trace of the Frobenius at p, a splitting prime in the CM field. It is well known that the following formula holds in general:

$$|E^d_{D,\mathfrak{f}}(\mathbb{F}_p)| = p + 1 + \pi\psi_{n(E)}(d) + \overline{\pi\psi_{n(E)}(d)},$$

where π is a primary prime above p and $\psi_{n(E)}(\cdot)$ is the $n(E)$-power residue symbol.

3. Statements of the main results

Theorem 1 (2-torsion)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ with CM by an order of $K = \mathbb{Q}(\sqrt{-D})$ of conductor $\mathfrak{f}$ and let F be a Galois number field not containing K. Then*

- *$j(E) \neq 0, 1728$:*
  - *If $D \neq 8$ and $\mathfrak{f}$ is odd, then $E(F)[2] = E(\mathbb{Q})[2]$.*
  - *Otherwise, $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{p})$, where $p|D$; in particular, there are 2-torsion points in a quadratic field different from K.*
- *$j(E) = 1728$: In this case, $E = E^d_{4,1}$ for $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^4$ and $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-d})$; in particular, for $d \neq 1$ there are 2-torsion points in a quadratic field different from K.*
- *$j(E) = 0$: In this case, $E = E^d_{3,1}$ for $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^6$ and $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2d})$. Moreover, $E(F)[2] = E(\mathbb{Q})[2]$.*

Theorem 2. *Let E be an elliptic curve defined over $\mathbb{Q}$ with CM by an order of $K = \mathbb{Q}(\sqrt{-D})$ and p an odd prime not dividing D. Let F be a Galois number field not containing K. Then $E(F)[p]$ is trivial.*

Theorem 3. *Let E be an elliptic curve defined over $\mathbb{Q}$ with CM by an order of $K = \mathbb{Q}(\sqrt{-D})$ of conductor $\mathfrak{f}$. We know that $E = E^d_{D,\mathfrak{f}}$ for some integer $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^{n(E)}$. Let p be an odd prime dividing D.*

- *If $p > 7$, then there are p-torsion points of E defined over $\mathbb{Q}(\zeta_p + \overline{\zeta}_p, \sqrt{d})$. Furthermore, $d = -p$ is the only case where any Galois number field containing p-torsion points contains K.*
- *If $D = 7$:*
  - *Case $\mathfrak{f} = 1$. There are 7-torsion points of E defined over $\mathbb{Q}(\zeta_7 + \overline{\zeta}_7, \sqrt{-7d})$. Furthermore, $d = 1$ is the only case where any Galois number field containing 7-torsion points contains K.*
  - *Case $\mathfrak{f} = 2$. There are 7-torsion points of E defined over $\mathbb{Q}(\zeta_7 + \overline{\zeta}_7, \sqrt{7d})$. Furthermore, $d = -1$ is the only case where any Galois number field containing 7-torsion points contains K.*
- *If $D = 3$:*
  - *Case $\mathfrak{f} = 1$. $\mathbb{Q}(E[3]) = \mathbb{Q}(d^{1/6}, \sqrt{-3})$. There is a 3-torsion point in the field $\mathbb{Q}(\sqrt{d})$ and, except for $d = -3$, this quadratic field is different from K. Moreover, if $d = e^3$, there is a 3-torsion point on $\mathbb{Q}(\sqrt{-3e})$ which, except when e is a square, is different from K.*
  - *Case $\mathfrak{f} \neq 1$. There are 3-torsion points in the field $\mathbb{Q}(\sqrt{d})$. Except for $d = -3$ this quadratic field is different from K.*

Remark. $p = 3$ is the only odd prime where there are p-torsion points defined over $\mathbb{Q}$. For example, in the last item of the previous theorem $\mathfrak{f} = 1$ with $e = 1$ or $e = -3$, when $d = e^3$, and $\mathfrak{f} \neq 1$ with $d = 1$ are the only cases where the curve has rational 3-torsion.

4. On the division polynomials for small or bad reduction primes

In this section we are going to study the p-division polynomial of the elliptic curves $E_{D,\mathfrak{f}}$, where $p = 2, 3$ or a bad reduction prime (i.e. $p = D$ with $2, 3 \nmid D$). This study has been done computing explicitly the factorization of the p-division polynomial for the 13 curves in Table 1.

Let E be an elliptic curve defined over a number field F given by a short Weierstrass equation of the form $y^2 = x^3 + ax + b$, where $a, b \in \mathcal{O}_F$. Define the m-division polynomial Ψ_m, attached to E, recursively as follows:

$$\begin{aligned}
&\psi_1 = 1,\\
&\psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,\\
&\psi_4 = (2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8bax - 2a^3 - 16b^2)\Psi_2,\\
&\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3,\ k \geq 2,\\
&\psi_{2k} = \psi_k(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2)/\psi_2,\ k \geq 2.
\end{aligned}$$

Now, for $m > 2$ define

$$\Psi_m = \begin{cases} \psi_m & m \text{ odd},\\ \psi_m/\psi_2 & m \text{ even}, \end{cases}$$

and $\Psi_2 = x^3 + ax + b$. We have $\Psi_m \in \mathcal{O}_F[x]$. Then $P \in E[m]$ if and only if $\Psi_m(x(P)) = 0$. In particular, $P \in E(F)[m]$ if and only if $\Psi_m(x(P)) = 0$ and $P \in E(F)$.

Remark. Let E be an elliptic curve defined over a number field F with $j(E) \neq 0, 1728$ and E^d its d-twist, for some $d \in F$. Then it is a straightforward computation to check that $\Psi^d_m(dx) = d^{\deg \Psi_m} \Psi_m(x)$, where Ψ_m (respectively Ψ^d_m) denotes the m-division polynomial of E (respectively E^d). Therefore the study of the behavior of the roots of $\Psi^d_m(x)$ could be done on $\Psi_m(x)$ instead.

Let E be an elliptic curve defined over $\mathbb{Q}$, p a prime and $g(x) \in \mathbb{Z}[x]$ be a factor of the p-division polynomial of E. We denote by

$$\mathbb{Q}[E, g] = \mathbb{Q}(\{\alpha, \beta \in \overline{\mathbb{Q}} \mid (\alpha, \beta) \in E[p]\,, g(\alpha) = 0\}).$$

Thus, $\mathbb{Q}(E[m]) = \mathbb{Q}[E, \Psi_m]$.

Lemma 4. *Let $-D \in \{-7, -11, -19, -43, -67, -163\}$ and $E = E_{D,\mathfrak{f}}$ be an elliptic curve in Table* 1*. Let $p = D$ and $\Psi_p(x)$ be the p-division polynomial of E. Then the irreducible factorization of $\Psi_p(x)$ over $\mathbb{Z}[x]$ is given by*

$$\Psi_p(x) = g_p(x) h_p(x), \ \textit{where} \begin{cases} \deg g_p = \ \ \ (p-1)/2\,, \\ \deg h_p = p(p-1)/2\,. \end{cases}$$

Let us denote by $F'_p = \mathbb{Q}(\{\alpha \in \overline{\mathbb{Q}} \mid g_p(\alpha) = 0\})$. Then $F'_p = \mathbb{Q}^+(\zeta_p)$. Moreover, if we denote by $F_p = \mathbb{Q}[E, g_p]$, then:

(i) *If $p \neq 7$, then $F_p = F'_p$. Therefore, $\mathbb{Q}(\zeta_p) = F'_p(\sqrt{-p}) = F'_p \cdot \mathbb{Q}(\sqrt{-D})$.*
(ii) *If $p = 7$ and $\mathfrak{f} = 1$, then $F_7 = \mathbb{Q}(\zeta_7)$. Thus, $\mathbb{Q}(\sqrt{-7}) \subset F_7$.*
(iii) *If $p = 7$ and $\mathfrak{f} = 2$, then $F_7 = \mathbb{Q}^+(\zeta_7)(\sqrt{7})$. Thus, $\mathbb{Q}(\zeta_7) \neq F_7$ and $\mathbb{Q}(\sqrt{-7}) \not\subset F_7$.*

Lemma 5. *Let $E = E_{D,\mathfrak{f}}$ be an elliptic curve in Table* 1*, $K = \mathbb{Q}(\sqrt{-D})$ and $g(x) \in \mathbb{Z}[x]$ be a nonlinear irreducible factor of the* 3*-division polynomial of E. Then $K(\sqrt{-3}) \subset \mathbb{Q}[E, g]$. Furthermore:*

(i) *If $D = 3$, then $\mathbb{Q}(E_{D,\mathfrak{f}}[3]) = K(\sqrt[3]{\mathfrak{f}})$.*
(ii) *If $D \neq 3$, then $\#\mathrm{Gal}(\mathbb{Q}(E_{D,\mathfrak{f}}[3])/\mathbb{Q}) = 8$ or* 16.

Table 2

$-D$	$\mathfrak{f}$	$\mathbb{Q}(E_{D,\mathfrak{f}}[2])$
-3	1	$K(\sqrt[3]{2})$
-3	2	$\mathbb{Q}(\sqrt{3})$
-3	3	$K(\sqrt[3]{2})$
-4	1	K
-4	2	$\mathbb{Q}(\sqrt{2})$
-7	1	K
-7	2	$\mathbb{Q}(\sqrt{7})$
-8	1	$\mathbb{Q}(\sqrt{2})$
-11	1	$K(\alpha)$, $\alpha^3 + \alpha^2 + \alpha - 1 = 0$
-19	1	$K(\alpha)$, $\alpha^3 - \alpha^2 + 3\alpha - 1 = 0$
-43	1	$K(\alpha)$, $\alpha^3 - 3\alpha^2 + 7\alpha - 1 = 0$
-67	1	$K(\alpha)$, $\alpha^3 - \alpha^2 + 7\alpha - 9 = 0$
-163	1	$K(\alpha)$, $\alpha^3 - 9\alpha^2 + 85\alpha - 227 = 0$

Lemma 6. *Let $E = E_{D,\mathfrak{f}}$ be an elliptic curve in Table* 1 *and $K = \mathbb{Q}(\sqrt{-D})$. Then:*

(i) *If $D \neq 8$ and $\mathfrak{f}$ is odd, then $K \subset \mathbb{Q}(E[2])$.*
(ii) *Otherwise, $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{p})$, where $p|D$.*

Moreover, Table 2 *shows $\mathbb{Q}(E[2])$.*

The proof of the above lemmas is a straightforward computation that has been done by using Magma and Sage (cf. respectively [1], [8]). All the sources are available from http://www.uam.es/enrique.gonzalez.jimenez/research/tables/CM/. Note that the case with more computer cost was the factorization of the 163-division polynomial of $E_{163,1}$. This polynomial is of degree 13284 with huge coefficients. The file that stores it is around 280 MB. Then the factorization was done using the functionality PARI on Sage.

5. 2-torsion

Proof of Theorem 1. Let E be an elliptic curve defined over $\mathbb{Q}$ with CM by an order $R = \mathbb{Z} + \mathfrak{f}\mathcal{O}_K$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. Then if $j(E) \neq 0, 1728$, E is $\mathbb{Q}$-isomorphic to $E^d_{D,\mathfrak{f}}$ for some square-free integer d. We have $\Psi^d_2(dx) = d^3\Psi_2(x)$, where Ψ_2 (respectively Ψ^d_2) denotes the 2-division polynomial of $E_{D,\mathfrak{f}}$ (respectively $E^d_{D,\mathfrak{f}}$). That is, if $E_{D,\mathfrak{f}} : y^2 = x^3+ax+b$, then $\Psi_2(x) = x^3+ax+b$ and $\Psi^d_2(x) = x^3 + d^2ax + d^3b$. Now, since the points of order 2 are the ones that have ordinate zero we have that the field of definition of a point of order 2 on $E^d_{D,\mathfrak{f}}$ is the same as the one on $E_{D,\mathfrak{f}}$. Now, thanks to Lemma 6, we have that if F is a Galois field not containing K and $D \neq 8$ and $\mathfrak{f}$ is odd, then $E(F)[2]$ does not increase with respect to the 2-torsion defined over $\mathbb{Q}$. For the case $D = 8$ or $\mathfrak{f}$ even, we have that $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{p})$, where $p|D$.

Now let E be such that $j(E) = 1728$. Then $E = E^d_{4,1} : y^2 = x^3 + dx$ for some fourth powerfree integer d. Then it is trivial to realize that $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-d})$. The case $j(E) = 0$ is similar to the above case. □

6. Primes not dividing the discriminant

Theorem 7. *Let E be an elliptic curve defined over $\mathbb{Q}$ with CM by an order of $K = \mathbb{Q}(\sqrt{-D})$. Then, for every odd prime $p \nmid D$, the Galois representation corresponding to the p-torsion points of E is irreducible.*

Proof. Since E has CM, half of the traces of $\rho_{E,p}$ will be 0; more precisely, for every prime q inert on K and of good reduction, the trace $a_q = 0$.

Suppose that $\rho_{E,p}$ is reducible. This means that, after semi-simplifying, we have $\rho_{E,p} = \mu_1 \oplus \mu_2$, with μ_1, μ_2 characters. It is well-known that these characters will take values on $\mathbb{F}^*_p$ (this follows from the fact that the Galois representations attached to an elliptic curve are odd). The determinant of $\rho_{E,p}$ is χ; thus we can write $\mu_2 = \chi \cdot \mu_1^{-1}$.

Thus $\rho_{E,p}$ is isomorphic to the sum of the two characters $\chi\mu_1^{-1}$ and μ_1. Comparing traces for the image of Frob q for any prime q inert in K and of good reduction for E, we obtain

$$a_q = 0 \equiv q\mu_1(q)^{-1} + \mu_1(q) \pmod{p}\,. \tag{2}$$

Since, by assumption, p is not ramified in K, if we fix a nonzero residue class t modulo p, the Cebotarev density theorem implies that there are infinitely many primes q that are inert in K and also congruent to t modulo p. We can also assume that these primes q are of good reduction for E. We fix the following residue class modulo p: take w to be any quadratic nonresidue modulo p and let $t = -w$. Thus, there are infinitely many primes q inert in K, of good reduction for E, and congruent to $t = -w$ modulo p. For these primes q, congruence in (2) gives

$$w \equiv -q \equiv \mu_1(q)^2 \qquad \pmod{p}.$$

Since $-q \equiv w \pmod{p}$, which is a nonsquare, this is a contradiction (recall that we know the character μ_1 to take values on $\mathbb{F}_p^*$). This proves the theorem. □

Proof of Theorem 2. We have shown that the representation is irreducible. On the other hand, by the theory of complex multiplication the restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ has an abelian image. Therefore the image contains an abelian normal subgroup of index 2; it has a dihedral projectivization such as

$$\left\langle \begin{pmatrix} * & \\ & * \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle, \tag{3}$$

where the element T of order 2 comes from the conjugation $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q})$. Hence, for any field $K \subsetneq F \subset E[p]$, $\mathrm{Gal}\,(F/\mathbb{Q})$ will be a quotient of $\mathrm{Gal}\,(E[p]/\mathbb{Q})$ containing T and, in particular, will again be irreducible. The conclusion follows since it is obvious that a torsion point defined over F will produce a subspace invariant by $\mathrm{Gal}\,(F/\mathbb{Q})$ which would then give a reducible representation. □

The following proposition describes the image of the mod p Galois representation obtained in this section.

Proposition 8. *Let E be an elliptic curve defined over $\mathbb{Q}$ with CM by an order of $K = \mathbb{Q}(\sqrt{-D})$ and p an odd prime not dividing D. Then the projectivization of $\rho_{E,p}$ has dihedral image.*

7. Primes dividing the discriminant

Proof of Theorem 3. We consider a curve $E = E_{D,\mathfrak{f}}$ as in Table 1 and $p = D > 3$, which is a bad reduction prime. We will use Lemma 4 together with the information that the curve has CM defined over K to give a precise description of the Galois number field generated by the p-torsion points of E.

The image of $\rho_{E,p}$ is contained in $\mathrm{GL}_2(\mathbb{F}_p)$ and since the curve has CM over K, it is well-known that the restriction to the Galois group of K is reducible since the p-torsion points generate an abelian extension of K. Thus, the image of $\rho_{E,p}$ is a group containing an abelian normal subgroup with index at most 2.

We know by Lemma 4 that the order of the Galois number field generated by the p-torsion of E is divisible by p (in fact, a factor h_p of the p-division polynomial has degree divisible by p). This Galois number field is the one corresponding to the image of $\rho_{E,p}$. If we apply Dickson's classification (cf. [5, Prop. 15]) of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ we conclude that the representation is either reducible or surjective (we know that the determinant is surjective). But since we also know that it contains an abelian normal subgroup of index at most 2, it has to be reducible. Since its order is divisible by p it is reducible but not decomposable. Thus, the image of $\rho_{E,p}$ can be described as follows:

$$\rho_{E,p} \cong \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}, \tag{4}$$

where $* \neq 0$ and ϕ_1, ϕ_2 are characters of $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ satisfying $\phi_1 \cdot \phi_2 = \chi$. It is known that these two characters must have values in $\mathbb{F}_p^*$, because the representation $\rho_{E,p}$ is odd and therefore if it is reducible it must reduce over $\mathbb{F}_p$. In this case, precisely because the representation is reducible, either there are torsion points defined over $\mathbb{Q}$ (but it is well-known that there are no such points since $p > 3$) or there is a nontrivial Galois invariant 1-dimensional subspace, the character ϕ_1 corresponding to the action of $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ on this subspace. In Lemma 4 we observe that there is an abelian extension generated by some of the torsion points (the one corresponding to points of torsion whose x-coordinates are roots of g_p); this abelian extension must clearly correspond to the Galois invariant subspace with character ϕ_1. In Lemma 4 this is the extension that we have called F_p. Then we can recover the character ϕ_1 which corresponds to F_p, and also $\phi_2 = \chi \cdot \phi_1^{-1}$, in each case. From Lemma 4, the character ϕ_1 is:

If $D = p > 7$, prime: $\phi_1 = \chi^2$.
If $D = 7$, $\mathfrak{f} = 1$: $\phi_1 = \chi$.
If $D = 7$, $\mathfrak{f} = 2$: $\phi_1 = \mu$, where μ corresponds to the extension $\mathbb{Q}(\zeta_7 + \overline{\zeta}_7, \sqrt{7})$.

Let us now consider the case $p = 3$, $\mathfrak{f} > 1$ and $E = E_{3,\mathfrak{f}}$. These elliptic curves have rational 3-torsion points, and therefore the representation $\rho_{E,3}$ is reducible as in (4) with $\phi_1 = 1$ and $\phi_2 = \chi$, but, by Lemma 5, $\rho_{E,3}$ do not decompose as the sum of these two characters. For the general case of a CM curve E, we will use again the fact that $E = E^d_{D,\mathfrak{f}}$ and $\rho_{E,p} = \rho_{E_{D,\mathfrak{f}},p} \otimes \psi$, where ψ is quadratic. Therefore we have for the image of $\rho_{E,p}$ that again it is contained in a Borel set as in (4):

$$\rho_{E,p} \cong \begin{pmatrix} \phi_1 \cdot \psi & * \\ 0 & \phi_2 \cdot \psi \end{pmatrix}, \tag{5}$$

where $* \neq 0$.

For $p = 3$, $\mathfrak{f} = 1$, we just have to consider the 3-division polynomial of $E^d_{3,1}$, $\psi_3(x) = 3x(x^3 + 2^6 d)$, to conclude that the coordinates of the 3-torsion points are $(0, \pm 4\sqrt{d})$, $(4\alpha d^{1/3}, \pm 4\sqrt{-3d})$, where α is any cubic root of -1. From here, (4) and (5), Theorem 3 follows easily. □

The description of the image of the mod p Galois representation just obtained can be summarized as follows:

Proposition 9. *Let $E = E^d_{D,\mathfrak{f}}$ and $p = D$ be a prime greater than 3. Then the image of $\rho_{E,p}$ is*

$$\rho_{E,p} \cong \begin{pmatrix} \phi_1 \cdot \psi & * \\ 0 & \phi_2 \cdot \psi \end{pmatrix},$$

where

$$\phi_1 = \begin{cases} \chi & \text{if } p = 7 \text{ and } \mathfrak{f} = 1, \\ \mu & \text{if } p = 7 \text{ and } \mathfrak{f} = 2, \\ \chi^2 & \text{if } p > 7, \end{cases}$$

where μ corresponds to the extension $\mathbb{Q}(\zeta_7 + \overline{\zeta}_7, \sqrt{7})$, $\phi_2 = \chi \cdot \phi_1^{-1}$, ψ is the quadratic character of $\mathbb{Q}(\sqrt{d})$ and $* \neq 0$.

Acknowledgements

The authors are grateful to John Cremona for useful comments at the beginning of this work. The authors also thank William Stein for computational facilities on the Sage server. Finally, the authors thank the anonymous referee for useful comments.

References

[1] J. J. Cannon, W. Bosma (eds.), *Handbook of Magma Functions*, Edition 2.15 (2008).

[2] Y. Fujita, Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$, *Acta Arith.* **115** (2004), 29–45. MR2102804 (2005j:11041)

[3] S. Kwon, Torsion subgroups of elliptic curves over quadratic extensions, *Journal of Number Theory* **62** (1997) 144–162. MR1430007 (98e:11068)

[4] D. Qiu and X. Zhang, Elliptic curves and their torsion subgroups over number fields of type $(2, 2, \dots, 2)$, *Sci. China Ser. A* **44** (2001), 159–167. MR1824316 (2002d:11065)

[5] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), no. 4, 259–331. MR0387283 (52:8126)

[6] J. H. Silverman, The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986. MR817210 (87g:11070)

[7] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994. MR1312368 (96b:11074)

[8] W. Stein et al., *Sage: Open Source Mathematical Software (Version 3.4)*, The Sage Group, 2009, `http://www.sagemath.org`.

Departament d'Algebra i Geometria, Universitat de Barcelona, G. V. de les Corts Catalanes 585, 08007 Barcelona, Spain
E-mail address: `ldieulefait@ub.edu`

Departamento de Matemáticas, Universidad Autónoma de Madrid and Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM), 28049 Madrid, Spain
E-mail address: `enrique.gonzalez.jimenez@uam.es`

Departament de Matemàtica Aplicada IV, Universitat Politecnica de Catalunya, 08034 Barcelona, Spain
E-mail address: `jjimenez@ma4.upc.edu`