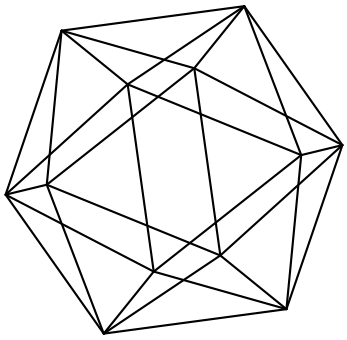
Max-Planck-Institut für Mathematik
Bonn

On 5-torsion of CM elliptic curves

by

Laura Paladino



Max-Planck-Institut für Mathematik
Preprint Series 2018 (45)

On 5-torsion of CM elliptic curves

Laura Paladino

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

University of Calabria
Ponte Bucci, Cubo 30B
87036 Arcavacata di Rende
Italy

MPIM 18-45

On 5-torsion of CM elliptic curves

Laura Paladino[1]

[1]Dipartimento di Matematica, Università della Calabria, Ponte Pietro Bucci, Cubo 30B - 87036 Arcavacata di Rende (CS), Italy, e-mail: paladino@mat.unical.it

Keywords: elliptic curves; complex multiplication; torsion points;

Mathematics subject classification: 11G05; 11F80; 11G18

Abstract

Let $\mathcal{E}$ be an elliptic curve defined over a number field K. Let m be a positive integer. We denote by $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$ and by $K_m := K(\mathcal{E}[m])$ the number field obtained by adding to K the coordinates of the points of $\mathcal{E}[m]$. We describe the fields K_5, when $\mathcal{E}$ is a CM elliptic curve defined over K, with Weiestrass form either $y^2 = x^3 + bx$ or $y^2 = x^3 + c$. In particular we classify the fields K_5 in terms of generators, degrees and Galois groups. Furthermore we show some applications of those results to the Local-Global Divisibility Problem, to modular curves and to Shimura curves.

1 Introduction

Let $\mathcal{E}$ be an elliptic curve defined over a number field K with algebraic closure $\bar{K}$. Let m be a positive integer. We denote by $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$ and by $K_m := K(\mathcal{E}[m])$ the number field generated by the 5-torsion points of $\mathcal{E}$, i.e. the field obtained by adding to K the coordinates of the points of $\mathcal{E}[m]$. Since K_m is the splitting field of the m-division polynomials, then K_m/K is a Galois extension, whose Galois group we denote by G. For every point $P \in \mathcal{E}$, we indicate by $x(P)$, $y(P)$ its coordinates. Furthermore, for every positive integer n, we indicate the n-th multiple of P simply by nP. It is well-known that $\mathcal{E}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$. Let $\{P_1\,, P_2\}$ be a $\mathbb{Z}$-basis for $\mathcal{E}[m]$; thus $K_m = K(x(P_1), x(P_2), y(P_1), y(P_2))$. To ease notation, we put $x_i := x(P_i)$ and $y_i := y(P_i)$ $(i = 1, 2)$. Knowing explicit generators for K_m could have a lot of interesting applications, for instance about Galois representations, local-global problems on elliptic curves (see [17], [18] and [19]), descent problems (see for example [22] and the particular cases [3] and [4]), points on modular curves (see [5], [6]) and points on Shimura curves. The Shimura curves are moduli spaces of abelian surfaces $\mathcal{A}$ and it turns out that $\mathcal{A}$ is simple with some extra structures or $\mathcal{A} = \mathcal{E} \times \mathcal{E}$, where $\mathcal{E}$ is a CM elliptic curve with some extra structures (see Subsection 8.3 for further details). So the elliptic curves with complex multiplication are particularly interesting since their squares (with some extra structures) correspond to points on certain Shimura curves. In the literature there are not many papers about the number fields generated by m-torsion points of elliptic curves (see also [1], [16] and [7]). A recent and very interesting paper about number fields $\mathbb{Q}(\mathcal{E}[m])$ is [14]. The discussion there is restricted to the case when $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is an abelian extension, even for CM elliptic curves. Among other results (see also Remark 5.1), in particular the authors prove that if $\mathcal{E}$ is an elliptic curve with complex multiplication and $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is abelian, then $m \in \{2, 3, 4\}$. In this paper we

will describe all possible extensions (even not abelian) $K(\mathcal{E}[5])/K$, for every K, when $\mathcal{E}$ is a CM elliptic curve. We will classify them in terms of generators, degree and Galois groups. By Artin's primitive element theorem, we know that the extension K_m/K is monogeneous and one can find a single generator for K_m/K by combining the above coordinates. Anyway, in general it is not easy to find this single generator. So, during the last few years we have searched for systems of generators easier to be found and to be used in applications. For every m, by the properties of the Weil pairing e_m, we have that the image $z_m := e_m(P_1, P_2) \in K_m$ is a primitive m-th root of unity and that $K(\zeta_m) \subseteq K_m$ (see for instance [24]). When m is odd, another generating set for K_m is showed in the following statement (see [6]).

Theorem 1.1. *In the notation as above, we have*

$$K_m = (x_1, \zeta_m, y_2), \tag{1}$$

for all odd integers m.

Of course, in general it is easier to work with the generating set as in (1). Furthermore, that generating set is often minimal among the subsets of $\{x_1, x_2, \zeta_m, y_1, y_2\}$ (for further details see [6]). For $m = 3$ and $m = 4$ there are explicit descriptions of all possible number fields K_3 and K_4, in terms of generators, degrees and Galois groups (see in particular [6] and also [5]). Here we give a similar classification of every possible number fields K_5, for all elliptic curves with complex multiplication, belonging to the families:

$$\mathcal{F}_1 : y^2 = x^3 + bx, \quad \text{with } b \in K \qquad \text{and} \qquad y^2 = x^3 + c, \quad \text{with } c \in K.$$

We will treat separately the case of the family $\mathcal{F}_1 : y^2 = x^3 + bx$, and of the family $\mathcal{F}_2 : y^2 = x^3 + c$, with $c \in K$. In the very last part of the paper, we show some applications (of those results) to the Local-Global Divisibility Problem, to K-rational CM points of modular curves and to K-rational CM points of Shimura curves.

2 Generators of $K(\mathcal{E}[5])$ for elliptic curves $y^2 = x^3 + bx$

If $\mathcal{E}$ is an elliptic curve defined over K, with Weierstrass form $y^2 = x^3 + bx + c$, then the abscissas of the points of order 5 of $\mathcal{E}$ are the roots of the polynomial

$$p_5(x) := -5x^{12} - 62bx^{10} - 380cx^9 + 105b^2x^8 - 240bcx^7 + (240c^2 + 300b^3)x^6 + 696b^2cx^5 +$$
$$(1920bc^2 + 125b^4)x^4 + (1600c^3 + 80b^3c)x^3 + (240b^2c^2 + 50b^5)x^2 + (640bc^3 + 100b^4c)x +$$
$$256c^4 + 32b^3c^2 - b^6.$$

If $\mathcal{E}_1 : y^2 = x^3 + c$ is an elliptic curve of the family $\mathcal{F}_1$, then the abscissas of the points of order 5 of $\mathcal{E}$ are the roots of the polynomial

$$q_5(x) := -5x^{12} - 62bx^{10} + 105b^2x^8 + 300b^3x^6 + 125b^4x^4 + 50b^5x^2 - b^6.$$

A factorization of $q_5(x)$ over $K(\zeta_5)$ is

$$q_5(x) = -5 \cdot (x^4 + (-8\zeta_5^3 - 8\zeta_5^2 + 2)bx^2 + (-8\zeta_5^3 - 8\zeta_5^2 + 5)b) \cdot (x^4 + \frac{2}{5}bx^2 + \frac{1}{5}b^2)$$

$$\cdot(x^4 + (8\zeta_5^3 + 8\zeta_5^2 + 10)bx^2 + (8\zeta_5^3 + 8\zeta_5^2 + 13)b)$$

and a factorization of $q_5(x)$ over $K(i, \zeta_5)$ is

$$q_5(x) = -5\cdot(x^2+((-4i+4)\zeta_5^3+4\zeta_5^2-4i\zeta_5-2i+5)b)\cdot(x^2+(-4\zeta_5^3+(-4i-4)\zeta_5^2-4i\zeta_5-2i+1)b)$$

$$\cdot(x^2 + ((4i + 4)\zeta_5^3 + 4\zeta_5^2 + 4i\zeta_5 + 2i + 5)b) \cdot (x^2 + (-4\zeta_5^3 + (4i - 4)\zeta_5^2 + 4i\zeta_5 + 2i + 1)b)$$

$$\cdot(x^2+ \tfrac{-2i+1}{5}\ b) \cdot (x^2+ \tfrac{2i+1}{5}\ \ b),$$

where as usual we denote by i a root of $x^2 + 1 = 0$.

Remark 2.1. Let ϕ_1 denote the complex multiplication of $\mathcal{E}_2$, i. e. $\phi_1(x, y) = (-x, iy)$. As above, in many cases if P is a nontrivial m-torsion point, then $\phi_1(P)$ is an m-torsion point that is not a multiple of P. In this case a basis for $\mathcal{E}[m]$ is given by $\{P, \phi_1(P)\}$. Anyway, in a few special cases the point $\phi_1(P)$ is a multiple of P. For example, let $\omega_1 := -(1 + 2i)/5$, let $x_{1/2} = \pm\sqrt{\omega_1}$ and let P_1 and P_2 be the two 5-torsion points of $\mathcal{E}_1$, with abscissas respectively x_1 and x_2. Since $\phi_1(P_i) = 2P_i$ (for $i = 1, 2$), then $\{P_i, \phi_1(P_i)\}$ is not a basis of $\mathcal{E}[5]$. We would have not this problem by choosing a root of $q_5(x)$, different from x_1 and x_2.

Theorem 2.2. *Let*

$$\theta_1 := -((-4i + 4)z_5^3 + 4z_5^2 - 4iz_5 - 2i + 5).$$

Then $K_5 = K(\zeta_5, i, \sqrt{(\theta_1 + 1)b\sqrt{\theta_1 b}})$.

Proof. If $x_1 := \sqrt{\theta_1 b}$, then by the factorization of $q_5(x)$ showed above, we have that x_1 is the abscissas of a 5-torsion point of $\mathcal{E}$. Let $P_1 = (x_1, y_1)$, where $y_1 = \sqrt{(\theta_1 + 1)b\sqrt{\theta_1 b}}$. By calculating $\phi_1(P_1)$ and the powers of P_1, one sees that $\phi_1(P_1)$ is not a multiple of P_1. In addition observe that $\sqrt{\theta_1 b} \in K(\zeta_5, i, \sqrt{(\theta_1 + 1)b\sqrt{\theta_1 b}})$. Then the conclusion follows by Remark 2.1. □

Observe that $[K_5 : K] \leqslant 2 \cdot 4 \cdot 2 \cdot 2 = 32$, for every $b \in K$. This is in accordance with the fact that $\mathcal{E}$ has complex multiplication $(x, y) \mapsto (-x, -iy)$ and then the Galois representation

$$\rho_{\mathcal{E},5} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$$

is not surjective.

3 Degrees $[K_5 : K]$ for the curves of $\mathcal{F}_1$

Theorem 3.1. *Let $\mathcal{E} : y^2 = x^3 + bx$, with $b \in K$. Let θ_1 as above. Consider the conditions*

A. $i \notin K$;
B1. $\zeta_5 + \zeta_5^{-1} \notin K$;
B2. $\zeta_5 \notin K(\zeta_5 + \zeta_5^{-1})$;
C. $\sqrt{(\theta_1)b} \notin K(i, \zeta_5)$;
D. $\sqrt{(\theta_1 + 1)b\sqrt{\theta_1 b}} \notin K(i, \zeta_5, \sqrt{\theta_1 b})$.

The possible degrees of the extension K_5/K are the following

d	holding conditions	d	holding conditions
32	*5 among* **A**, **B1**, **B2**, **C**, **D**	4	*2 among* **A**, **B1**, **B2**, **C**, **D**
16	*4 among* **A**, **B1**, **B2**, **C**, **D**	2	*1 among* **A**, **B1**, **B2**, **C**, **D**
8	*3 among* **A**, **B1**, **B2**, **C**, **D**	1	*no holding conditions*

Table 2

Proof. Consider the tower of extensions

$$K \subseteq K(i) \subseteq K(i, \zeta_5 + \zeta_5^{-1}) \subseteq K(i, \zeta_5) \subseteq K(i, \zeta_5, \sqrt{(\theta_1)b}) \subseteq K(\zeta_3, \zeta_5, \sqrt{(\theta_1 + 1)b\sqrt{(\theta_1)b}}).$$

The degree of K_5/K is the product of the degrees of the intermediate extensions appearing in the tower. Clearly each of those extensions gives a contribution to the degree less than or equal to 2. The final computation is straightforward. □

4 Galois groups $\mathrm{Gal}(K_5/K)$ for the curves of $\mathcal{F}_1$

Let E_1 be a curve of the family $\mathcal{F}_1$, let $G := \mathrm{Gal}(K(\mathcal{E}_2[5])/K)$ and let $d := |G|$. Let θ_1 and ω_1 as above and let

$$\begin{aligned}
\theta_2 &:= -(-4z_5^3 + (-4i - 4)z_5^2 - 4iz_5 - 2i + 1);\\
\theta_3 &:= -((4i + 4)z_5^3 + 4z_5^2 + 4iz_5 + 2i + 5);\\
\theta_4 &:= -(-4z_5^3 + (4i - 4)z_5^2 + 4iz_5 + 2i + 1);\\
\omega_2 &:= -\frac{2i + 1}{5}b.
\end{aligned}$$

If $P = (x, y)$ is a point of $\mathcal{E}$, to ease notation, let us denote by iP the point $\phi_1(P) = (-x, iy)$. The 24 points of exact order 5 of $\mathcal{E}_2$ are the following:

$$\pm P_1 := (x_1, \pm y_1) = \left(\sqrt{\theta_1 b}, \pm\sqrt{(\theta_1+1)b\sqrt{\theta_1 b}}\right) \qquad \pm iP_1 := (-x_1, \pm iy_1);$$

$$\pm P_2 := (x_2, \pm y_2) = \left(\sqrt{\theta_2 b}, \pm\sqrt{(\theta_2+1)b\sqrt{\theta_2 b}}\right) \qquad \pm iP_2 := (-x_2, \pm iy_2);$$

$$\pm P_3 := (x_3, \pm y_3) = \left(\sqrt{\theta_3 b}, \pm\sqrt{(\theta_3+1)b\sqrt{\theta_3 b}}\right) \qquad \pm iP_3 := (-x_3, \pm iy_3);$$

$$\pm P_4 := (x_4, \pm y_4) = \left(\sqrt{\theta_4 b}, \pm\sqrt{(\theta_4+1)b\sqrt{\theta_4 b}}\right) \qquad \pm iP_4 := (-x_4, \pm iy_4);$$

$$\pm P_5 := (x_5, \pm y_5) = \left(\sqrt{\omega_1 b}, \pm\sqrt{(\omega_1+1)b\sqrt{\omega_1 b}}\right) \qquad \pm iP_5 := (-x_5, \pm iy_5);$$

$$\pm P_6 := (x_6, \pm y_6) = \left(\sqrt{\omega_2 b}, \pm\sqrt{(\omega_2+1)b\sqrt{\omega_2 b}}\right) \qquad \pm iP_6 := (-x_6, \pm iy_6).$$

By the observations made in the previous sections about the generators of K_5 and about the degree $[K_5 : K]$, we have that The Galois group is generated by the following 3 automorphisms.

i) The automorphism ϕ_1 of order 4 given by the complex multiplication. We have $\phi_1(x, y) = (-x, iy)$, for all $(x, y) \in K(\mathcal{E}[5])$. In particular, for every $1 \leqslant j \leqslant 6$, the automorphism ϕ_1 maps $\sqrt{\theta_j b}$ to $-\sqrt{\theta_j b}$ (i. e. x_j to $-x_j$) and y_1 to iy_1. Thus $\phi_1(P_j) = iP_j$, for all $1 \leqslant j \leqslant 6$. Observe that $\phi_1^2 = -\mathrm{Id}$.

ii) The automorphism ψ_1 of order 4 mapping ζ_5 to ζ_5^2. Observe that

$$P_1 \overset{\psi_1}{\longmapsto} P_2 \overset{\psi_1}{\longmapsto} P_3 \overset{\psi_1}{\longmapsto} P_4 \overset{\psi_1}{\longmapsto} P_1,$$

as well as

$$iP_1 \overset{\psi_1}{\longmapsto} iP_2 \overset{\psi_1}{\longmapsto} iP_3 \overset{\psi_1}{\longmapsto} iP_4 \overset{\psi_1}{\longmapsto} iP_1.$$

The other 5-torsion points are fixed by ψ_1.

iii) The automorphism ρ_1 of order 2 of the quadratic field of the complex multiplication, that maps i to $-i$. Observe that such an automorphism swaps P_1 and P_3 and swaps P_2 and P_4

$$P_1 \overset{\rho_1}{\longleftrightarrow} P_3 \qquad\qquad P_2 \overset{\rho_1}{\longleftrightarrow} P_4.$$

Furthermore

$$iP_1 \overset{\rho_1}{\longleftrightarrow} -iP_3 \qquad\qquad iP_2 \overset{\rho_1}{\longleftrightarrow} -iP_4;$$

$$P_5 \overset{\rho_1}{\longleftrightarrow} P_6 \qquad\qquad iP_6 \overset{\rho_1}{\longleftrightarrow} -iP_6.$$

By [25, Chapter II, Theorem 2.3], the extension $K_5/K(i)$ is abelian, thus $\langle \phi_1, \psi_1 \rangle \simeq \mathbb{Z}/4 \times \mathbb{Z}/4$, when all the conditions in the statement of Theorem 2.2 hold. Moreover, with a quick computation, one verifies that ψ_1 and ρ_1 commute. On the contrary ϕ_1 and ρ_1 do not commute in general, in fact

$$\rho_1\phi_1((x_1, y_1)) = \rho_1((-x_1, iy_1)) = (-x_3, -iy_3);$$

$$\phi_1\rho_1((x_1, y_1)) = \phi_1((x_3, y_3)) = (-x_3, iy_3).$$

Instead we have $\rho_1\phi_1((P_1)) = \phi_1^{-1}\rho((P_1))$ and $\rho_1\phi_1((iP_1)) = \phi_1^{-1}\rho_1((iP_1))$. Being $\{P_1, iP_1\}$ a generating set for K_5, we can conclude $\rho_1\phi_1 = \phi_1^{-1}\rho$. Thus, when all the condition hold, we have $\langle \phi_1, \rho_1 \rangle \simeq D_8$. We are going to describe the Galois groups $G = \mathrm{Gal}(K_5/K)$, with respect to the degrees $[K_5 : K]$.

$d = 32$ If the degree d of the extension K_5/K is 32, then all the conditions hold. We have $G = \langle \phi_1, \psi_1, \rho_1 | \phi_1^4 = \psi_1^4 = \rho_1^2 = \mathrm{Id}, \phi_1\psi_1 = \psi_1\phi_1, \rho_1\psi_1 = \psi_1\rho_1, \phi_1\rho_1 = \phi_1^{-1}\rho_1 \rangle \simeq D_8 \times \mathbb{Z}/4\mathbb{Z}$.

$d = 16$ If the degree d of the extension K_5/K is 16, then only one condition does not hold.

If **A** does not hold, then ρ_1 is the identity and we have an abelian group $G = \langle \phi_1, \psi_1 \rangle \simeq \mathbb{Z}/4 \times \mathbb{Z}/4$.

If one among **B1** and **B2** does not hold, then $G \simeq D_8 \times \mathbb{Z}/2\mathbb{Z}$.

If one among **C** and **D** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

$d = 8$ If the degree d of the extension K_5/K is 8, then two conditions do not hold among the ones as above.

If **B1** and **B2** do not hold, then $G\langle \phi_1, \rho_1 \rangle \simeq D_8$. This is the only case in which the Galois group G is not abelian.

If one among **B1** and **B2** does not hold and **A** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If one among **B1** and **B2** does not hold and one among **C** and **D** does not hold then $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

If one among **C** and **D** does not hold and **A** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ again.

$d = 4$ If the degree d of the extension K_5/K is 4, then three conditions do not hold. If both **B1** and **B2** hold or if both **C** and **D** hold, then $G \simeq \mathbb{Z}/4\mathbb{Z}$. Otherwise $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$d \leqslant 2$ If the degree d of the extension K_5/K is either 2 or 1, clearly the Galois group is respectively $\mathbb{Z}/2\mathbb{Z}$ or $\{\mathrm{Id}\}$.

5 Generators of $K(\mathcal{E}[5])$ for elliptic curves $y^2 = x^3 + c$

Let $\mathcal{E}_2 : y^2 = x^3 + c$ be an elliptic curve of the family $\mathcal{F}_2$.

Remark 5.1. Let ϕ_2 denote the complex multiplication of $\mathcal{E}_2$, i. e. $\phi_2(x, y) = (\zeta_3 x, y)$. In many cases, if P is a nontrivial m-torsion point, then $\phi_2(P)$ is an m-torsion point that is not a multiple of P. Therefore, in many cases a basis for $\mathcal{E}[m]$ is given by $\{P, \phi_2(P)\}$ and $K_m = K(x(P), y(P), \zeta_3)$. Anyway, in a few special cases, the point $\phi_2(P)$ is a multiple of P over the field $K(\zeta_3, \zeta_5)$. For example, the abscissas of the 3-torsion points of $\mathcal{E}_1$ are

$$\tilde{x_1} = 0; \quad \tilde{x_2} = \sqrt[3]{-4c}; \quad \tilde{x_3} = \zeta_3\tilde{x_2}; \quad \tilde{x_4} = \zeta_3^2\tilde{x_2}.$$

Let $\tilde{P_h}$ be a point of abscissas $\tilde{x_h}$, for $1 \leqslant h \leqslant 4$. Clearly $\phi_2(\tilde{P_1}) = \tilde{P_1}$ and then $\{\tilde{P_1}, \phi_2(\tilde{P_1})\}$ is not a basis of $\mathcal{E}[3]$. On the other hand, $\{\tilde{P_h}, \phi_2(\tilde{P_h})\}$ is a basis of $\mathcal{E}[3]$, for $2 \leqslant h \leqslant 4$. So we have to take care in our choice of P, when we use such a basis $\{P, \phi_2(P)\}$. For elliptic curves with complex multiplication ϕ_2, a generating set $\{x(P), y(P), \zeta_3\}$ is often easier to adopt than the one in (1).

The abscissas of the points of order 5 of $\mathcal{E}$ are the roots of the polynomial

$$r_5(x) := -5x^{12} - 380cx^9 + 240c^2x^6 + 1600c^3x^3 + 256c^4.$$

A factorization of φ_1 over $K(\zeta_5)$ is

$$r_5(x) = -5 \cdot (x^6 + (-36\zeta_5^3 - 36\zeta_5^2 + 20)cx^3 + \frac{-288\zeta_5^3 - 288\zeta_5^2 + 176}{5}c^2)$$

$$\cdot(x^6 + (36\zeta_5^3 + 36\zeta_5^2 + 56)cx^3 + \frac{288\zeta_5^3 - 288\zeta_5^2 + 464}{5}c^2)$$

and a factorization of $r_5(x)$ over $K(\zeta_3, \zeta_5)$ is

$$r_5(x) = -5 \cdot (x^3 + \frac{(-132\zeta_3 + 24)\zeta_5^3 + (36\zeta_3 + 108)\zeta_5^2 + (-96\zeta_3 - 48)\zeta_5 - 48\zeta_3 + 116}{5}c)$$

$$\cdot(x^3 + \frac{(-36\zeta_3 - 108)\zeta_5^3 + (-132\zeta_3 - 156)\zeta_5^2 + (-168\zeta_3 - 84)\zeta_5 - 84\zeta_3 + 8}{5}c)$$

$$\cdot(x^3 + \frac{(132\zeta_3 + 156)\zeta_5^3 + (-36\zeta_3 + 72)\zeta_5^2 + (96\zeta_3 + 48)\zeta_5 + 48\zeta_3 + 164}{5}c)$$

$$\cdot(x^3 + \frac{(36\zeta_3 - 72)\zeta_5^3 + (132\zeta_3 - 24)\zeta_5^2 + (168\zeta_3 + 84)\zeta_5 + 84\zeta_3 + 92}{5}c)$$

Let

$$\delta_1 := -(\frac{(-132\zeta_3 + 24)\zeta_5^3 + (36\zeta_3 + 108)\zeta_5^2 + (-96\zeta_3 - 48)\zeta_5 - 48\zeta_3 + 116}{5});$$
$$\delta_2 := -(\frac{(-36\zeta_3 - 108)\zeta_5^3 + (-132\zeta_3 - 156)\zeta_5^2 + (-168\zeta_3 - 84)\zeta_5 - 84\zeta_3 + 8}{5});$$
$$\delta_3 := -(\frac{(132\zeta_3 + 156)\zeta_5^3 + (-36\zeta_3 + 72)\zeta_5^2 + (96\zeta_3 + 48)\zeta_5 + 48\zeta_3 + 164}{5});$$
$$\delta_4 := -(\frac{(36\zeta_3 - 72)\zeta_5^3 + (132\zeta_3 - 24)\zeta_5^2 + (168\zeta_3 + 84)\zeta_5 + 84\zeta_3 + 92}{5}).$$

Then the 12 roots of $r_5(x)$, i. e. the abscissas of the 5-torsion points of $\mathcal{E}_1$, are $\sqrt[3]{\delta_1 c}$, $\sqrt[3]{\delta_1 c}\zeta_3$, $\sqrt[3]{\delta_1 c}\zeta_3^2$, $\sqrt[3]{\delta_2 c}$, $\sqrt[3]{\delta_2 c}\zeta_3$, $\sqrt[3]{\delta_2 c}\zeta_3^2$, $\sqrt[3]{\delta_3 c}$, $\sqrt[3]{\delta_3 c}\zeta_3$, $\sqrt[3]{\delta_3 c}\zeta_3^2$, $\sqrt[3]{\delta_4 c}$, $\sqrt[3]{\delta_4 c}\zeta_3$, $\sqrt[3]{\delta_4 c}\zeta_3^2$.

Theorem 5.2. *Let δ_1 as above. We have $K_5 = K(\sqrt[3]{\delta_1 c}, \zeta_3, \sqrt{(\delta_1 + 1)c})$.*

Proof. If $x_1 := \sqrt{\delta_1 c}$, then by the factorization of $r_5(x)$ showed above, we have that x_1 is the abscissas of a 5-torsion point of $\mathcal{E}$. Let $y_1 := \sqrt{(\delta_1+1)c}$. Then $P_1 = (x_1, y_1)$ is a 5-torsion point of $\mathcal{E}$. By calculating $\phi_2(P_1)$ and the powers of P_1, one sees that $\phi_2(P_1)$ is not a multiple of P_1. In fact $\phi_2(P_1) = (x_1\zeta_3, y_1) = (\sqrt{\delta_1 c}\zeta_3, y_1)$ and $x(2P_1) = x(3P_1) = ((\zeta_3+2)\zeta_5^3 + (-\zeta_3+1)\zeta_5^2 + 1)\sqrt[3]{\delta_1 c}$. Thus $x(\phi_2(P_1)) \neq x(nP_1)$, for all $1 \leqslant n \leqslant 4$ (recall that $x(4P_1) = x(P_1)$). By Remark 5.1, then $\{P_1, \phi_1(P_1)\}$ form a basis of $\mathcal{E}[5]$ and the conclusion is straightforward. □

Observe that $[K_5 : K] \leqslant 3 \cdot 2 \cdot 4 \cdot 2 = 48$, for every $c \in K$. This is in accordance with the fact that $\mathcal{E}$ has complex multiplication $\phi_1 : (x, y) \mapsto (\zeta_3 x, y)$ and then the Galois representation

$$\rho_{\mathcal{E},5} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$$

is not surjective.

6 Degrees $[K_5 : K]$ for the curves of $\mathcal{F}_2$

As above, let K be a number field and let $\mathcal{E}$ be an elliptic curve defined over K.

Theorem 6.1. *Let $\mathcal{E} : y^2 = x^3 + c$, with $c \in K$. Let δ_1 as above. Consider the conditions*

A. $\zeta_3 \notin K$;
B1. $\zeta_5 + \zeta_5^{-1} \notin K(\zeta_3)$;
B2. $\zeta_5 \notin K(\zeta_3, \zeta_5 + \zeta_5^{-1})$;
C. $\sqrt[3]{(\delta_1)c} \notin K(\zeta_3, \zeta_5)$;
D. $\sqrt{(\delta_1+1)c} \notin K(\zeta_3, \zeta_5)$.

The possible degrees of the extension K_5/K are the following

d	holding conditions	d	holding conditions
48	**A**, **B1**, **B2**, **C**, **D**	6	**C** *and 1 among* **A**, **B1**, **B2**, **D**
24	**C** *and 3 among* **A**, **B1**, **B2**, **D**	4	*2 among* **A**, **B1**, **B2**, **D**
16	**A**, **B1**, **B2**, **D**	3	**C**
12	**C** *and 2 among* **A**, **B1**, **B2**, **D**	2	*1 among* **A**, **B1**, **B2**, **D**
8	*3 among* **A**, **B1**, **B2**, **D**	1	*no holding conditions*

Table 1

Proof. Consider the tower of extensions

$$K \subseteq K(\zeta_3) \subseteq K(\zeta_3, \zeta_5+\zeta_5^{-1}) \subseteq K(\zeta_3, \zeta_5) \subseteq K(\zeta_3, \zeta_5, \sqrt[3]{(\delta_1)c}) \subseteq K(\zeta_3, \zeta_5, \sqrt[3]{(\delta_1)c}, \sqrt{(\delta_1+1)c}).$$

The degree of K_5/K is the product of the degrees of the intermediate extensions appearing in the tower. Each of those extension gives a contribution to the degree that is less than or equal to 2, except the extension $K(\zeta_3, \zeta_5, \sqrt[3]{(\delta_1)c})/K(\zeta_3, \zeta_5)$ that gives a contribution equal to 1 or 3. The final computation is straightforward. □

7 Galois groups $\mathrm{Gal}(K_5/K)$ for the curves of $\mathcal{F}_2$

Let $\mathcal{E}_1$ be a curve of the family $\mathcal{F}_1$ and let $d := |\mathrm{Gal}(K(\mathcal{E}_1[5])/K)|$. To study the Galois group $G := \mathrm{Gal}(K(\mathcal{E}_1[5])/K)$, we have to understand better the shapes of the coordinates of the 5-torsion points of $\mathcal{E}_1$. Let $\delta_1, \delta_2, \delta_3, \delta_4$ as in Section 5. The 24 torsion points of $\mathcal{E}$ with exact order 5 are:

$$
\begin{aligned}
\pm P_1 &= (x_1, \pm y_1) &&= \left(\sqrt[3]{\delta_1 c}, \pm\sqrt{(\delta_1+1)c}\right);\\
\pm\phi_2(P_1) &= (\zeta_3 x_1, \pm y_1) &&= \left(\sqrt[3]{\delta_1 c}\,\zeta_3, \pm\sqrt{(\delta_1+1)c}\right);\\
\pm\phi_2^2(P_1) &= (\zeta_3^2 x_1, \pm y_1) &&= \left(\sqrt[3]{\delta_1 c}\,\zeta_3^2, \pm\sqrt{(\delta_1+1)c}\right);\\
\pm P_2 &= (x_2, \pm y_2) &&= \left(\sqrt[3]{\delta_2 c}, \pm\sqrt{(\delta_2+1)c}\right);\\
\pm\phi_2(P_2) &= (\zeta_3 x_2, \pm y_2) &&= \left(\sqrt[3]{\delta_2 c}\,\zeta_3, \pm\sqrt{(\delta_2+1)c}\right);\\
\pm\phi_2^2(P_2) &= (\zeta_3^2 x_2, \pm y_2) &&= \left(\sqrt[3]{\delta_2 c}\,\zeta_3^2, \pm\sqrt{(\delta_2+1)c}\right);\\
\pm P_3 &= (x_3, \pm y_3) &&= \left(\sqrt[3]{\delta_3 c}, \pm\sqrt{(\delta_3+1)c}\right);\\
\pm\phi_2(P_3) &= (\zeta_3 x_3, \pm y_3) &&= \left(\sqrt[3]{\delta_3 c}\,\zeta_3, \pm\sqrt{(\delta_3+1)c}\right);\\
\pm\phi_2^2(P_3) &= (\zeta_3^2 x_3, \pm y_3) &&= \left(\sqrt[3]{\delta_3 c}\,\zeta_3^2, \pm\sqrt{(\delta_3+1)c}\right);\\
\pm P_4 &= (x_4, \pm y_4) &&= \left(\sqrt[3]{\delta_4 c}, \pm\sqrt{(\delta_4+1)c}\right);\\
\pm\phi_2(P_4) &= (\zeta_3 x_4, \pm y_4) &&= \left(\sqrt[3]{\delta_4 c}\,\zeta_3, \pm\sqrt{(\delta_4+1)c}\right);\\
\pm\phi_2^2(P_4) &= (\zeta_3^2 x_4, \pm y_4) &&= \left(\sqrt[3]{\delta_4 c}\,\zeta_3^2, \pm\sqrt{(\delta_4+1)c}\right).
\end{aligned}
$$

Thus we have the following four generating automorphisms of the Galois group G.

i) The automorphism ϕ_2 of the complex multiplication permuting the abscissas as follows

$$\sqrt[3]{\delta_i c} \mapsto \sqrt[3]{\delta_i c}\zeta_3 \mapsto \sqrt[3]{\delta_i c}\zeta_3^2 \mapsto \sqrt[3]{\delta_i c},$$

for all $1 \leqslant i \leqslant 4$, and fixing all the ordinates. Clearly ϕ_2 has order 3.

ii) The automorphism φ_1 of order 4 mapping ζ_5 to ζ_5^2,, that consequentely maps

$$\delta_1 \mapsto \delta_2 \mapsto \delta_3 \mapsto \delta_4 \mapsto \delta_1,$$

i. e.

$$P_1 \overset{\varphi_1}{\longmapsto} P_2 \overset{\varphi_1}{\longmapsto} P_3 \overset{\varphi_1}{\longmapsto} P_4 \overset{\varphi_1}{\longmapsto} P_1;$$

$$\phi_2 P_1 \overset{\varphi_1}{\longmapsto} \phi_2 P_2 \overset{\varphi_1}{\longmapsto} \phi_2 P_3 \overset{\varphi_1}{\longmapsto} \phi_2 P_4 \overset{\varphi_1}{\longmapsto} \phi_2 P_1;$$

$$\phi_2^2 P_1 \overset{\varphi_1}{\longmapsto} \phi_2^2 P_2 \overset{\varphi_1}{\longmapsto} \phi_2^2 P_3 \overset{\varphi_1}{\longmapsto} \phi_2^2 P_4 \overset{\varphi_1}{\longmapsto} \phi_2^2 P_1.$$

iii) The automorphism -Id of order 2, mapping $\sqrt{(\delta_i+1)c}$ to $-\sqrt{(\delta_i+1)c}$, for all $1 \leqslant i \leqslant 4$, such that

$$P \overset{-\mathrm{Id}}{\longmapsto} -P,$$

for all $P \in \mathcal{E}[5]$.

iv) The automorphism φ_2 of order 2 of the quadratic field of the complex multiplication mapping ζ_3 to ζ_3^2, and then swapping δ_1 and δ_3 and also δ_2 and δ_4. In particular

$$P_1 \overset{\varphi_2}{\longleftrightarrow} P_3 \qquad P_2 \overset{\varphi_2}{\longleftrightarrow} P_4;$$

$$\phi_2(P_1) \overset{\varphi_2}{\longleftrightarrow} \phi_2^2(P_3) \qquad \phi_2(P_2) \overset{\varphi_2}{\longleftrightarrow} \phi_2^2(P_4);$$

$$\phi_2^2(P_1) \overset{\varphi_2}{\longleftrightarrow} \phi_2(P_3) \qquad \phi_2^2(P_2) \overset{\varphi_2}{\longleftrightarrow} \phi_2(P_4).$$

One easily verifies that all these authomorphisms commute, except ϕ_2 and φ_2.

Observe that $\psi_2 := \phi_2 \circ \varphi_1$ form an homomorphism of order 12 and that $G = \langle \psi_2, \varphi_2, -\mathrm{Id} \rangle$. The automorphism ψ_2 and φ_2 does not commute, since ϕ_2 does not commute with φ_2, instead one can verify that $\varphi_2 \circ \psi_2 = \psi_2^{-1} \circ \varphi_2$.

Thus the group $\langle \psi_2, \varphi_2 \rangle$ has a presentation $\langle \psi_2, \varphi_2 | \psi_2^{12} = \varphi_2^2 = \mathrm{Id}, \varphi_2\psi_2 = \psi_2^{-1}\varphi_2 \rangle \simeq D_{24}$. If all the conditions as in Table 1 hold, then we have a Galois group of order 48 $G = \langle \psi_2, \varphi_2 \rangle \times \langle -\mathrm{Id} \rangle \simeq D_{24} \times \mathbb{Z}/2\mathbb{Z}$. By [25, Chapter II, Theorem 2.3], the extension $K_5/K(\zeta_3)$ is abelian. Thus, if condition **A** does not hold, then we have an abelian group. In all cases the group G is isomorphic to a subgroup of $D_{24} \times \mathbb{Z}/2\mathbb{Z}$ as follows.

$d = 48$ If the degree d of the extension K_5/K is 48, then all the conditions hold. We have $G \simeq D_{24} \times \mathbb{Z}/2\mathbb{Z}$ as above.

$d = 24$ If the degree d of the extension K_5/K is 24, then condition **C** holds.

If **A** does not hold, then we have an abelian group. In this case $G = \langle \psi_2, -\mathrm{Id} \rangle \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If **A**, **B1**, **B2** and **C** hold and **D** does not hold, then $G = \langle \varphi_2, \psi_2 \rangle \simeq D_{24}$.

If **A**, **C** and **D** hold and one among the conditions **B1** and **B2** does not hold, then $G = \langle \varphi_2, \psi_2, -\mathrm{Id} \rangle$, where ψ now has order 6 and $\langle \varphi_2, \psi_2 \rangle$ is isomorphic to D_{12}. We have $G \simeq D_{12} \times \langle \mathbb{Z}/2\mathbb{Z} \rangle$.

$d = 16$ If the degree d of the extension K_5/K is 16, then all the conditions hold but **C**. Thus ϕ_2 is the identity. We have an abelian extension and an abelian Galois group $G = \langle \varphi_1, \varphi_2, -\mathrm{Id} \rangle \simeq \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

$d = 12$ If the degree d of the extension K_5/K is 12, then condition **C** holds.

If **A** does not hold, then we have an abelian group $G = \langle \psi_2, -\mathrm{Id} \rangle \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If **A** and **C** hold, **D** does not hold and only one condition among **B1** and **B2** hold, then $G = \langle \varphi_2, \psi_2 \rangle \simeq D_{12}$ (now ψ_2 has order 6).

If **A**, **C** and **D** hold, then $G \simeq D_6 \times \mathbb{Z}/2\mathbb{Z} \simeq S_3 \times \mathbb{Z}/2\mathbb{Z}$, where S_3 is the symmetric group of order 6.

$d = 8$ If the degree d of the extension K_5/K is 8, then **C** does not hold and we have again an abelian extension.

If **D** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If **A** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If one among **B1** and **B2** does not holds, then $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

$d = 6$ If the degree d of the extension K_5/K is 6, then **C** holds.

If **A** holds as well, then $G \simeq D_6 \simeq S_3$.

If **A** does not hold, then $G \simeq \mathbb{Z}/6\mathbb{Z}$.

$d = 4$ If the degree d of the extension K_5/K is 4, then **C** does holds. If both **B1** and **B2** hold, then $G \simeq \mathbb{Z}/4\mathbb{Z}$, otherwise G is isomorphic to the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$d \leqslant 3$ If the degree d of the extension K_5/K is 3 or 2 or 1, clearly the Galois group is respectively $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ or $\{\mathrm{Id}\}$.

8 Some applications

We are going to show some applications of the results achieved in the previous sections. In particular we will show an application to the local-global divisibility problem, an immediate application to modular curves and another one to Shimura curves.

8.1 A minimal bound for the local-global divisibility by 5

We recall the statement of the Local-Global Divisibility Problem and some key facts about the cohomology group that gives the obstruction to its validity in order to maintain the paper more self-contained. For further details one can see [11], [10] and [20].

Problem 8.1 (Dvornicich, Zannier, 2001)**.** *Let K be a number field, M_K the set of the places v of K and K_v the completion of K at v. Let $\mathcal{G}$ be a commutative algebraic group defined over k. Fix a positive integer m and assume that there exists a K-rational point P in $\mathcal{G}$, such that $P = mD_v$, for some $D_v \in \mathcal{G}(K_v)$, for all but finitely many $v \in M_K$. Does there exist $D \in \mathcal{G}(K)$ such that $P = mD$?*

The classical question is considered for all commutative algebraic groups, but in our situation, we can confine the discussion only to elliptic curves $\mathcal{E}$ over K. Let $P \in \mathcal{E}[m]$ and let $D \in \mathcal{E}(\bar{K})$ be a m-divisor of P, i. e. $P = mD$. For every $\sigma \in G = \mathrm{Gal}(K_5/K)$, we have

$$m\sigma(D) = \sigma(mD) = \sigma(P) = P.$$

Thus $\sigma(D)$ and D differ by a point in $\mathcal{E}[m]$ and we can construct a cocycle $\{Z_\sigma\}_{\sigma \in G}$ of G with values in $\mathcal{E}[m]$ by

$$Z_\sigma := \sigma(D) - D. \tag{2}$$

Such a cocycle vanishes in $H^1(G, \mathcal{E}[m])$, if and only if there exists a K-rational m-divisor of P (see for example [11] or [10]). In particular, the hypotheses about the validity of the local-dividibility in Problem 8.1 imply that the cocyle $\{Z_\sigma\}_{\sigma \in G}$ vanishes in $H^1(\mathrm{Gal}((K_m)_v/K_v), \mathcal{E}[m])$, for all but finitely many $v \in M_K$. Let G_v denote the group $\mathrm{Gal}((K_m)_v/K_v)$ and let Σ be the subset of M_K containing all the $v \in M_K$, that are unramified in K_m. Then G_v is a cyclic subgroup of G, for all $v \in \Sigma$. Moreover, in [11] Dvornicich and Zannier observe that by the Chebotarev Density Theorem, the local Galois group G_v varies over *all* cyclic subgroups of G as v varies in Σ. Thus, they state the following definition about a subgroup of $H^1(G, \mathcal{E}[m])$ which portrays the hypotheses of the problem in this cohomological context and essentially gives the obstruction to the validity of such Hasse principle (see also [12]).

Definition 8.2. A cocycle $\{Z_\sigma\}_{\sigma\in G} \in H^1(G, \mathcal{E}[m])$ satisfies the *local conditions* if, for every $\sigma \in G$, there exists $A_\sigma \in \mathcal{E}[m]$ such that $Z_\sigma = (\sigma - 1)A_\sigma$. The subgroup of $H^1(G, \mathcal{E}[m])$ formed by all the cocycles satisfying the local conditions is the first local cohomology group $H^1_{\mathrm{loc}}(G, \mathcal{E}[m])$.

Thus

$$H^1_{\mathrm{loc}}(G, \mathcal{E}[m]) = \bigcap_{v\in\Sigma} (\ker H^1(G, \mathcal{E}[m]) \xrightarrow{res_v} H^1(G_v, \mathcal{E}[m])). \tag{3}$$

The triviality of $H^1_{\mathrm{loc}}(G, \mathcal{E}[m])$ assures the validity of the local-global divisibility by m in $\mathcal{E}$ over K.

Theorem 8.3 (Dvornicich, Zannier, 2001)**.** *If $H^1_{loc}(G, \mathcal{E}[m]) = 0$, then the local-global divisibility by m holds in $\mathcal{E}$ over k.*

In [11] the authors showed that the local-global divisibility by 5 holds in $\mathcal{E}$ over k, for all $l \geqslant 1$ (see also [27]). Anyway in that paper, as well as in all the other papers (of various authors) about the topic, there is no information about the minimal number of places v for which the validity of the local divisibility by a prime p in $\mathcal{E}$ over K_v is sufficient to have the global divisibility by p in $\mathcal{E}$ over K.

For the first time, here we show such a lower bound for the number of places v when $p = 5$, in the case of the curves belonging to the families $\mathcal{F}_1$ and $\mathcal{F}_2$.

By Theorem 8.3, the triviality of the first cohomology group $H^1_{\mathrm{loc}}(G, \mathcal{E}[m])$ is a sufficient condition to have an affirmative answer to Problem 8.1. We have already recalled that by the Tchebotarev Density Theorem, the group G_v varies over all the cyclic subgroups of G, as v varies among all the places of K, that are unramified in K_m. Observe that in fact we have

$$H^1_{\mathrm{loc}}(G, \mathcal{E}[m]) = \bigcap_{v\in S} (\ker H^1(G, \mathcal{E}[m]) \xrightarrow{res_v} H^1(G_v, \mathcal{E}[m])),$$

where S is a subset of Σ such that, for all $v, w \in S$, with $v \neq w$, the groups G_v and G_w correspond to distinct cyclic subgroups of G. If we are able to find such an S and to prove that the local-global divisibility by 5 holds in $\mathcal{E}(K_v)$, for all $v \in S$, then we get $H^1_{\mathrm{loc}}(G, \mathcal{E}[m]) = 0$ (and consequently the validity of the Hasse principle for disivibility by 5 in $\mathcal{E}$ over K). Observe that in particular the set S is finite (on the contrary Σ is not finite). So it suffices to have the local-global divisibility by 5 for a finite number of suitable places to get the global divisibility by 5.

In view of the results achieved for the Galois groups $\mathrm{Gal}(K_5/K)$ for elliptic curves of the families $\mathcal{F}_1$ and $\mathcal{F}_2$, we can prove that S could be chosen as a subset of S with a cardinality surprisingly small.

Theorem 8.4. *Let m be a positive integer. Let $\mathcal{E}$ be an elliptic curves defined over a number field K, with Weierstrass equation $y^2 = x^2 + bx$, for some $b \in K$. Let S be a subset of M_K of places v unramified in K_m, with cardinality $|S| = 7$, such that G_v varies among all the cyclic subgroups of G, as v varies in S. Let $P \in \mathcal{E}(K)$ such that $P = mD_v$, for some $D_v \in \mathcal{E}(K_v)$, for all $v \in S$. Then there exists $D \in \mathcal{E}(K)$ such that $P = mD$.*

Proof. Let s be the number of distinct cyclic subgroups of G. Since the group G_v varies over all the cyclic subgroups of G, as v varies in M_k, we can choose S as a subset of M_k with cardinality s, such that G_v and G_w are pairwise distinct cyclic subgroups of G, for all $v, w \in S$,

$v \neq w$. We have just to show that $s = 7$. We have proved in Section 4, that for every $\mathcal{E} \in \mathcal{F}_1$, the Galois group G is isomorphic to a subgroup of $D_8 \times \mathbb{Z}/4\mathbb{Z}$. The group D_8 has 5 cyclic subgroups, namely $\langle \phi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$, $\langle \phi_1^2 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \rho \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \phi_1\rho \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \phi_1^2\rho \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. In addition we have the cyclic subgroups $\langle \psi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ and $\langle \psi_1^2 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Thus G has at most 7 cyclic subgroups and we get the conclusion. □

Theorem 8.5. *Let m be a positive integer. Let $\mathcal{E}$ be an elliptic curves defined over a number field K, with Weierstrass equation $y^2 = x^2 + c$, for some $c \in K$. Let S be a subset of M_K of places v unramified in K_m, with cardinality $|S| = 13$, such that G_v varies among all the cyclic subgroups of G, as v varies in S. Let $P \in \mathcal{E}(K)$ such that $P = mD_v$, for some $D_v \in \mathcal{E}(K_v)$, for all $v \in S$. Then there exists $D \in \mathcal{E}(K)$ such that $P = mD$.*

Proof. Let s be the number of distinct cyclic subgroups of G. As in the proof of Theorem 8.4 we can choose S as a subset with cardinality s, such that G_v and G_w are pairwise distinct cyclic subgroups of G, for all $v, w \in S$, with $v \neq w$. We have just to show that $s = 13$. We have proved in Section 7, that for every $\mathcal{E} \in \mathcal{F}_2$, the Galois group G is isomorphic to a subgroup of $D_{24} \times \mathbb{Z}/2\mathbb{Z}$. The group D_{24} has 11 cyclic subgroups, namely $\langle \psi_1 \rangle \simeq \mathbb{Z}/12\mathbb{Z}$, $\langle \psi_1^2 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$, $\langle \psi_1^3 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$, $\langle \psi_1^4 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$, $\langle \psi_1^6 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \varphi_2 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \psi_1\varphi_2 \rangle \simeq \mathbb{Z}/12\mathbb{Z}$, $\langle \psi_1^2\varphi_2 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$, $\langle \psi_1^3\varphi_2 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$, $\langle \psi_1^4\varphi_2 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$, $\langle \psi_1^6\varphi_2 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. In addition, we have the cyclic subgroups $\langle -\mathrm{Id} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ and $\langle \psi_1^4, \rangle \times \langle -\mathrm{Id} \rangle \simeq \mathbb{Z}/6\mathbb{Z}$. Thus G has at most 13 cyclic subgroups and we get the conclusion. □

8.2 Remarks on modular curves

We recall some basic definitions about modular curves; for further details one can see for instance [13] and [23]. As usual, we denote by $\mathcal{H} = \{z \in \mathbb{C} : Im\, z > 0\}$ the complex upper half plane. It is well-known that the group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ via the Möbius trasformations

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

For every positive integer N, the *principal congruence group of level N* is the set

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

A *congruence group* is a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$, for some N. When N is minimal, the congruence group is said to be *of level N*. For every N, the most important congruence groups of level N are $\Gamma(N)$ itself and the groups:

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

and

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

The quotient $\mathcal{H}/\Gamma$ of $\mathcal{H}$ by the action of Γ, equipped with the analytic structure induced by $\mathcal{H}$, is a Riemann surface, that is denoted by Y_Γ. The modular curve X_Γ, associated to Γ, is the compactification of Y_Γ by the addition of a finite set of rational points corresponding to the orbits of $\mathbb{P}^1(\mathbb{Q})$ under Γ, i. e. the *cusps*.
The modular curves associated to the groups $\Gamma_0(N)$ and $\Gamma_1(N)$ are denoted respectively by $X_0(N)$ and $X_1(N)$. The modular curve associated to $\Gamma(N)$ is denoted by $X(N)$.

The curves $X(N)$, $X_1(N)$ and $X_0(N)$ are spaces of moduli of families of elliptic curves with an extra structure of level N as follows (for further details see for example [13], [15] and [23]).

Theorem 8.6. *Let N be a positive integer and let $X(N)$, $X_1(N)$ and $X_0(N)$ as above. Then*

i) *non cuspidal points in $X(N)$ correspond to triples $(\mathcal{E}, P, Q)$, where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and P, Q are points of order N generating $\mathcal{E}[N]$;*

ii) *non cuspidal points in $X_1(N)$ correspond to pairs $(\mathcal{E}, P)$, where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and P is a point of order N;*

iii) *non cuspidal points in $X_0(N)$ correspond to couples $(\mathcal{E}, C_N)$, where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and C_N is a cyclic subgroup of $\mathcal{E}[N]$ of order N.*

A point on a modular curve, which corresponds to an elliptic curve with complex multiplication is called a *CM-point*.

We can deduce the following facts from what showed in the previous sections (see in particular Theorem 5.2 and Theorem 2.2).

Proposition 8.7. *Let K be a number field. Let $\mathcal{E}_1 \in \mathcal{F}_1$ and let $P \in \mathcal{E}_1[5]$ such that $\{P, \phi_1(P)\}$ is a basis of $\mathcal{E}_1[5]$ (as above ϕ_1 denotes the complex multiplication of $\mathcal{E}_1$). Then*

the pair $(\mathcal{E}_1, \langle P \rangle)$ defines a non-cuspidal K-rational CM-point of $X_0(5)$,
if and only if $(\mathcal{E}_1, P)$ defines a non-cuspidal K-rational CM-point of $X_1(5)$,
if and only if $(\mathcal{E}_1, P, \phi_1(P))$ defines a K-rational CM-point of $X(5)$.

Proposition 8.8. *Let K be a number field. Let $\mathcal{E}_2 \in \mathcal{F}_2$ and let $P \in \mathcal{E}_2[5]$ such that $\{P, \phi_1 2P)\}$ is a basis of $\mathcal{E}_2[5]$ (as above ϕ_2 denotes the complex multiplication of $\mathcal{E}_2$). Then*

the pair $(\mathcal{E}_2, \langle P \rangle)$ defines a non-cuspidal K-rational CM-point of $X_0(5)$,
if and only if $(\mathcal{E}_2, P)$ defines a non-cuspidal K-rational CM-point of $X_2(5)$,
if and only if $(\mathcal{E}_2, P, \phi_2(P))$ defines a K-rational CM-point of $X(5)$.

8.3 Remarks on Shimura curves

We are going to describe two curves, the Shimura curves named $\mathcal{X}_0(N)$ and $\mathcal{X}_1(N)$, which are generalizations of the modular curves $X_0(N)$ and $X_1(N)$, i. e. they are moduli spaces of certain abelian varieties of dimension 2, with some N-level structures.

We firstly recall that a central K-algebra is an algebra over K with center K. Furthermore a simple K-algebra is an algebra over K with nontrivial two-sided ideals. A division K-algebra is an algebra $\mathfrak{A}$ over the field K, in which for every $a_1, a_2 \in \mathfrak{A}$, with $a_2 \neq 0$, there exists $b \in \mathfrak{A}$ such that $a_1 = a_2 b$.

Definition 8.9. A quaternion algebra over K is a central simple algebra over K of dimension 4.

By Wedderburn's Theorem (see [26]), every central simple K-algebra is a matrix algebra over a central division K-algebra. The division central K-algebra are classified by the Brauer group $\mathrm{Br}(K) = H^2(\mathrm{Gal}(\bar{K}/K), \bar{K})$.

One of the simplest example of a quaternion K-algebra is the set $M_2(K)$ of 2×2 matrices with entries in K. The quaternion algebra $\mathfrak{B} = M_2(\mathbb{Q})$ over $\mathbb{Q}$ is important in the definition of Shimura curves.

Definition 8.10. Let R be the ring of integers of K. An order of a quaternion K-algebra $\mathfrak{A}$ is a R-lattice, which is also a subring. A maximal order of a quaternion K-algebra $\mathfrak{A}$ is an order that is not contained in any other order, i. e. it is a R-lattice of rank 4, which is also a subring. An Eichler order is given by the intersection of two maximal orders.

For example, the set $M_2(R)$ of 2×2 matrices with entries in R is a maximal order of $M_2(K)$. In particular $M_2(\mathbb{Z})$ is a maximal order of $M_2(\mathbb{Q})$. Let N be a positive integer. Observe that the subgroup $\mathcal{O}'_N$ of $M_2(\mathbb{Q})$, formed by the matrices

$$\begin{pmatrix} a & Nb \\ N^{-1}c & d \end{pmatrix}$$

is conjugate to $M_2(\mathbb{Z})$ by

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus $\mathcal{O}'_N$ is a maximal order too and $\mathcal{O}_N := M_2(\mathbb{Z}) \cap \mathcal{O}'_N$ is an Eichler order. We have that $\mathcal{O}_N$ is the subset of $M_2(\mathbb{Z})$, formed by the matrices of the form

$$\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}.$$

Observe that $\mathcal{O}_N$ is an analogous in $M_2(\mathbb{Z})$ of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ in the case of modular curves.

Definition 8.11. For every order $\mathcal{O}$, we denote by $\mathcal{O}^1$ the subset of its, formed by the elements of norm 1.

Definition 8.12. The quotient $\mathcal{X}(\mathcal{O}) := \mathcal{H}/\mathcal{O}^1$ is called a Shimura curve. In particular we denote by $\mathcal{X}(1)$ the Shimura curve obtained by the order $\mathcal{O} = M_2(\mathbb{Z})$ of $\mathfrak{B}$.

In the literature, the curve $\mathcal{X}(1)$ is also denoted by $\mathcal{M}^{\mathfrak{B}}$ or simply by $\mathcal{M}$. It turns out that the Shimura curves are connected and compact. So we do not need to add cusps as in the case of modular curves. Indeed, we have such a moduli interpretation of the curve $\mathcal{X}(1)$ (see for example [8] and see also [23]).

Theorem 8.13. *The curve $\mathcal{X}(1)$ is the moduli space of the couples $(\mathcal{A}, \iota)$, where $\mathcal{A}$ is an abelian surface principally polarized such that either A is simple with $End \otimes \mathbb{Q} = M_2(\mathbb{Q})$ or $A = \mathcal{E} \times \mathcal{E}$, where $\mathcal{E}$ is a CM elliptic curve defined over K, and $\iota : \mathcal{O} \to \mathrm{End}(\mathcal{A})$ is an embedding.*

When an abelian surface $\mathcal{A}$ admits an embedding $\iota : \mathcal{O} \to \mathrm{End}(\mathcal{A})$, one says that $\mathcal{A}$ has a quaternion multiplication or that $\mathcal{A}$ is a QM-abelian surface. Sometimes A is also said a $\mathcal{O} - QM$-abelian surface, to underline that the quaternion multiplication is given by the order $\mathcal{O}$.

By Theorem 8.13, it is clear the strong relation between CM elliptic curves and Shimura curves. The points on Shimura curves parametrizing squares of CM elliptic curves are often called CM points.

For a positive integer N, the Shimura curve $\mathcal{X}(\mathcal{O}_N) := \mathcal{H}/\mathcal{O}_N^1$ is similar to the Shimura curve $\mathcal{X}(1)$, but with an extra structure of level N. Because of the connection between $\mathcal{O}_N$ and $\Gamma_0(N)$, the curve $\mathcal{X}(\mathcal{O}_N)$ is often denoted by $\mathcal{X}_0(N)$ (and sometimes by $M_0^{\mathfrak{B}}(N)$, as for instance in [2]). We recall the moduli interpretation for $\mathcal{X}_0(N)$ (see again [8] and also [23]).

Theorem 8.14. *Let $\mathcal{O} = M_2(\mathbb{Z})$. The curve $\mathcal{X}_0(N)$ is the moduli space of the triples $(\mathcal{A}, \iota, W)$, where $\mathcal{A}$ is a QM-abelian surface principally polarized such that either A is simple with End$\otimes \mathbb{Q} = M_2(\mathbb{Q})$ or $A = \mathcal{E} \times \mathcal{E}$, where $\mathcal{E}$ is a CM elliptic curve defined over K, the quaternionic multiplication is given by $\iota : \mathcal{O} \to \mathrm{End}(\mathcal{A})$ and $W \in \mathcal{A}[N]$ is a cyclic $\mathcal{O}$-submodule of order N^2, which is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$ as an abelian group.*

In a similar way as for $\mathcal{O}_N$, one can take the Eichler order

$$\mathcal{O}_{1,N} := \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

which is an analogous of $\Gamma_1(N)$. In this case we get the Shimura curve $\mathcal{X}(\mathcal{O}_{1,N})$, that is denoted by $\mathcal{X}_1(N)$ (and sometimes by $M_1^{\mathfrak{B}}(N)$). Let e_1, e_2 denote two standard idempotents for $M_2(\mathbb{Z}/N\mathbb{Z})$. The moduli interpretation for $\mathcal{X}_1(N)$ is the following (see [8] and see also [23]).

Theorem 8.15. *Let $\mathcal{O} = M_2(\mathbb{Z})$. The curve $\mathcal{X}_1(N)$ is the moduli space of the 4-tuples $(\mathcal{A}, \iota, W, P)$, where $\mathcal{A}$ is a QM-abelian surface principally polarized such that either A is simple with End $\otimes \mathbb{Q} = M_2(\mathbb{Q})$ or $A = \mathcal{E} \times \mathcal{E}$, where $\mathcal{E}$ is a CM elliptic curve defined over K, the quaternionic multiplication is given by $\iota : \mathcal{O} \to \mathrm{End}(\mathcal{A})$, $W \in \mathcal{A}[N]$ is a stable $\mathcal{O}$-module and $P = e_1 W$ is a point of order N.*

Observe that if $(\mathcal{A}, \iota, W, P)$ corresponds to a CM point of $\mathcal{X}_1(N)$, then $\mathcal{A} = \mathcal{E} \times \mathcal{E}$ (for some CM elliptic curve) and $W = P \times Q \in \mathcal{E}^2[N]$, with $P = e_1 W \in \mathcal{E}[N]$ and $Q \in \mathcal{E}[N]$.

For some Shimura varieties and certain fields F it is known that the set of F-rational points is empty (see for instance [21] and [9]). For $j \in \{0, 1\}$, let $\mathcal{X}_j(5)(K)$ denote the sets of the K-rational points of the Shimura curve $\mathcal{X}_j(5)$. Let θ_1 as in Section 2 and δ_1 as in Section 5. We have that the sets $\mathcal{X}_0(5)(K)$ and $\mathcal{X}_1(5)(K)$ are nonempty whenever $K = K_5$ is one of the fields $\mathbb{Q}(\zeta_5, i, \sqrt{(\theta_1 + 1)b\sqrt{\theta_1 b}})$ and $\mathbb{Q}(\sqrt[3]{\delta_1 c}, \zeta_3, \sqrt{(\delta_1 + 1)c})$.

More precisely, by the results achieved about the fields K_5 for elliptic curves of the families $\mathcal{F}_1$ and $\mathcal{F}_2$, we can make the following remarks about the points of the curves $\mathcal{X}_0(5)$ and $\mathcal{X}_1(5)$.

Proposition 8.16. *Let K be a number field, let $\mathcal{E}_1 \in \mathcal{F}_1$ and let $P_1 = \left(\sqrt{\theta_1 b}, \pm\sqrt{(\theta_1 + 1)b\sqrt{\theta_1 b}}\right)$. In particular $(P_1, \phi_1(P_1)) \in \mathcal{E}_1 \times \mathcal{E}_1$. Let $\mathcal{O} = M_2(\mathbb{Z})$ and let $\iota : \mathcal{O} \to \mathrm{End}(\mathcal{E}_1 \times \mathcal{E}_1)$. Then*

i) *the triple* $(\mathcal{E}_1 \times \mathcal{E}_1,\ \iota,\ (P_1, \phi_1(P_1))$ *corresponds to a CM-point of* $\mathcal{X}_0(5)$*;*

ii) *the 4-tuple* $(\mathcal{E}_1 \times \mathcal{E}_1,\ \iota,\ (P_1, \phi_1(P_1)),\ P_1)$ *corresponds to a CM-point of* $\mathcal{X}_1(5)$*.*

Proposition 8.17. *Let* K *be a number field, let* $\mathcal{E}_2 \in \mathcal{F}_2$ *and let* $P_1 = \left(\sqrt[3]{\delta_1 c}, \pm\sqrt{(\delta_1+1)c}\right)$*. In particular* $(P_1, \phi_2(P_1)) \in \mathrm{End}\mathcal{E}_2 \times \mathcal{E}_2$*. Let* $\mathcal{O} = M_2(\mathbb{Z})$ *and let* $\iota : \mathcal{O} \to \mathrm{End}(\mathcal{E}_2 \times \mathcal{E}_2)$*. Then*

i) *the triple* $(\mathcal{E}_2 \times \mathcal{E}_2,\ \iota,\ (P_1, \phi_1(P_1))$ *corresponds to a CM-point of* $\mathcal{X}_0(5)$*;*

ii) *the 4-tuple* $(\mathcal{E}_1 \times \mathcal{E}_1,\ \iota,\ (P_1, \phi_1(P_1)),\ P_1)$ *corresponds to a CM-point of* $\mathcal{X}_1(5)$*.*

Acknowledgments. I would like to thank Andrea Bandini for useful discussions and for some precious remarks about a preliminary version of this paper. I produced part of this work when I was a guest at the Max Planck Institute for Mathematics in Bonn. I am grateful to all people there for their kind hospitality and for the excellent work conditions.

References

[1] C. Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics **1761**, Springer-Verlag, Berlin, 2001.

[2] K. Arai, F. Momose, Algebraic points on Shimura curves of $\Gamma_0(p)$-type, *J. Reine Angew. Math.* **690** (2014) 179-202.

[3] A. Bandini, Three-descent and the Birch and Swinnerton-Dyer conjecture, *Rocky Mount. J. of Math.* **34** (2004), 13–27.

[4] A. Bandini, 3-Selmer groups for curves $y^2 = x^3 + a$, *Czechoslovak Math. J.* **58** (2008), 429–445.

[5] A. Bandini and L. Paladino, Number fields generated by the 3-torsion poins of an elliptic curve, *Monatsh. Math.* **168** no. 2 (2012), 157–181.

[6] A. Bandini and L. Paladino, Fields generated by torsion poins of elliptic curves, *J. Number Theory*, 169, 103-133.

[7] B. M. Bekker, Y. G. Zarhin, The divisibility by 2 of rational points on elliptic curves, arXiv:1702.02255.

[8] P. Clark, Rational points on Atkin-Lehner quotients of Shimura curves, Phd Thesis, Harvard University Cambridge, Massachusset, 2003.

[9] P. Clark, X. Xarles, Local bounds for torsion points on abelian varieties, *Canad. J. Math.*, 60 (2008), 532-555.

[10] R. Dvornicich and A. Paladino, Local-global questions for divisibility in commutative algebraic groups, https://arxiv.org/pdf/1706.03726.pdf

[11] R. Dvornicich and U. Zannier, Local-global divisibility of rational points in some commutative algebraic groups, *Bull. Soc. Math. France* **129**, no. 3 (2001), 317–338.

[12] R. Dvornicich, U. Zannier, On local-global principle for the divisibility of a rational point by a positive integer, *Bull. Lon. Math. Soc.*, no. **39** (2007), 27-34.

[13] N.M. Katz - B. Mazur, Arithmetic moduli of elliptic curves, *Annals of Math. Studies* **108**, Princeton Univ. Press, Princeton, 1985.

[14] E. González-Jiménez, Á. Lozano-Robledo, Elliptic curves with abelian division fields, *Math. Z.*, **283** no. 3-4 (2016), 835-859.

[15] A.W. Knapp, Elliptic curves, Princeton Univ. Press, Princeton, 1992.

[16] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.* **124** (1996), 437–449.

[17] L. Paladino, Local-global divisibility by 4 in elliptic curves defined over $\mathbb{Q}$, *Annali di Matematica Pura e Applicata* **189** no. 1 (2010), 17-23.

[18] L. Paladino, Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9, *J. Théor. Nombres Bordeaux* **22** (2010), no. 1, 138–160.

[19] L. Paladino, On local-global divisibility in commutative algebraic groups, *Acta Arithmetica* **148** no. 1 (2011), pp. 21-29.

[20] Paladino L., Ranieri G., Viada E., On minimal set for counterexamples to the local-global principle, *Journal of Algebra*, **415** (2014), 290-304.

[21] V. Rotger, C. de Vera-Piquero, Galois representations over fields of moduli and rational points on Shimura curves, *Canadian J. Math.* **66** (2014), 1167-1200.

[22] E.F. Schaefer and M. Stoll, How to do a p-descent on an elliptic curve, *Trans. Amer. Math. Soc.* **356** (2004), 1209-1231.

[23] G. Shimura, Construction of Class Fields and Zeta Functions of Algebraic Curves, *Ann. of Math.*, **85** no. 1 (1967), 58-159.

[24] J.H. Silverman, The arithmetic of elliptic curves, 2-nd edition, **GTM 106** Springer-Verlag, New York, 2009.

[25] J.H. Silverman, Advanced Topic in Elliptic Curves, **GTM 151** Springer-Verlag, New York, 1994.

[26] Wedderburn J.H.M., On Hypercomplex Numbers, *Proc. London Math. Soc.*, **6** (1908), 77-118.

[27] Wong S., Power residues on abelian variety, *Manuscripta Math.*, no. **102** (2000), 129-137.

Laura Paladino

University of Calabria
Ponte Bucci, Cubo 30B
87036 Arcavacata di Rende
Italy
e-mail address: paladino@mat.unical.it