On the division fields of an elliptic curve and an effective bound to the hypotheses of the local-global divisibility

Roberto Dvornicich[a], Laura Paladino[b]

Abstract

We investigate some aspects of the m-division field $K(\mathcal{E}[m])$, where $\mathcal{E}$ is an elliptic curve defined over a field K with $\mathrm{char}(K) \neq 2,3$ and m is a positive integer. When $m = p^r$, with $p \geq 5$ a prime and r a positive integer, we prove $K(\mathcal{E}[p^r]) = K(x_1, \zeta_p, y_2)$, where $\{(x_1, y_1), (x_2, y_2)\}$ is a generating system of $\mathcal{E}[p^r]$ and ζ_p is a primitive p-th root of the unity. If $\mathcal{E}$ has a K-rational point of order p, then $K(\mathcal{E}[p^r]) = K(\zeta_{p^r}, \sqrt[m_1]{a})$, with $a \in K(\zeta_{p^r})$ and $m_1 | p^r$. In addition, when K is a number field, we produce an upper bound to the logarithmic height of the discriminant of the extension $K(\mathcal{E}[m])/K$, for all $m \geq 3$. As a consequence, we give an explicit effective version of the hypotheses of the local-global divisibility problem in elliptic curves over number fields.

MSC: 11G05, 11G07

1 Introduction

Let $\mathcal{E}$ be an elliptic curve defined over a field K with $\mathrm{char}(K) \neq 2,3$. Let m be a positive integer. By $K(\mathcal{E}[m])/K$ we denote the m-th division field, i.e. the field generated over K by the coordinates of the m-torsion points of $\mathcal{E}$. Since the first serious study of the arithmetic of elliptic curves, the m-th division fields have played a vital rôle. Investigating the Galois representations on the total Tate module is the same as studying these fields. Iwasawa theory, modularity and even the proof of the Mordell-Weil theorem are related to the properties of $K(\mathcal{E}[m])/K$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two m-torsion points of $\mathcal{E}$, generating $\mathcal{E}[m]$. Then clearly $K(\mathcal{E}[m]) = K(x_1, x_2, y_1, y_2)$. It is well-known

[a]University of Pisa, Department of Mathematics, Pisa, Italy, e-mail address: roberto.dvornicich@unipi.it

[b]Corresponding author; ORCID ID: 0000-0003-4758-9775; University of calabria, Department of Mathematics and Computer Science, Rende, Italy, e-mail address: laura.paladino@unical.it

that as a consequence of the Weil pairing we have $K(\zeta_m) \subseteq K(\mathcal{E}[m])$, where ζ_m is a primitive m-th root of the unity. Recently there has been a growing interest in studying the possible cases when $K(\zeta_m) = K(\mathcal{E}[m])$ [21], [30], [25], [17] and more generally in producing new set of generators for $K(\mathcal{E}[m])/K$ involving ζ_m itself as a generator [2], [3]. In [3], in particular it was proved that, for every odd integer $m \geq 5$, we have $K(\mathcal{E}[m]) = K(x_1, \zeta_m, y_2)$. When $m = p^r$, for a prime $p \geq 5$ and a positive integer $r \geq 2$, we improve such a generating system, by showing $K(\mathcal{E}[p^r]) = K(x_1, \zeta_p, y_2)$, for every $r \geq 1$. Even if we substitute ζ_{p^r} with ζ_p, we still have that all the p^r-th roots of the unity are contained in $K(\mathcal{E}[p^r])$. We also show that, for every p^r-torsion point (x_1, y_1) of $\mathcal{E}$, the extension $K(\mathcal{E}[p^r])/K(x_1, y_1)$ is metacyclic. Let C_m denote the cyclic group of order m. If $F = K(x_1, y_1)$, then $K(\mathcal{E}[p^r])/F = F(\zeta_{p^r}, \sqrt[m_1]{a})$, where $a \in F(\zeta_{p^r})$, $m_1 | p^r$ and $\mathrm{Gal}(K(\mathcal{E}[p^r])/F) = C_{m_1}.C_{m_2}$, with m_2 dividing $p^{r-1}(p-1)$. Observe that this shows that if $\mathcal{E}$ has a $K(\zeta_{p^r})$-rational point of exact order p^r (and in particular if $\mathcal{E}$ has a K-rational point of exact order p^r), then $K(\mathcal{E}[p^r]) = K(\zeta_{p^r}, \sqrt[m_1]{a})$. We also give some remarks on the possible istances when $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p, \sqrt[p]{a})$, with $a \in \mathbb{Q}(\zeta_p)$.

In the second part of the paper, we concentrate in the case when K is a number field and $\mathcal{E} : y^2 = x^3 + bx + c$, with $b, c \in K$. For all $m \geq 3$ we produce an upper bound $B(m, b, c)$, depending on m, b and c, to the height of the discriminant of the extension $K(\mathcal{E}[m])/K$. As a consequence we give an explicit effective version to the hypotheses of the following local-global question, known as local-global divisibility problem.

Problem 1. *Let $P \in \mathcal{E}(K)$. Assume that for all but finitely many places $v \in K$, there exists $D_v \in \mathcal{E}(K_v)$ such that $P = mD_v$, where K_v is the completion of K at the place v. Is it possible to conclude that there exists $D \in \mathcal{E}(K)$ such that $P = mD$?*

This problem was originally stated by Dvornicich and Zannier in 2001, in the more general setting of a commutative algebraic group defined over K [9]. Many papers have been written about this question since its formulation. A solution to the problem for all powers of prime numbers implies a solution for every m. The question has been completely answered for elliptic curves over $\mathbb{Q}$. In particular the local-global divisibility holds for all m but the ones divided by the powers p^n, with $p \in \{2, 3\}$ and $n \geq 2$ (see [9], [29], [8] for further details). Moreover the question has been answered for all but finitely many primes p in elliptic curves over a general number field K [28]. Concerning the formulation of the problem in the setting of commutative algebraic groups defined over number fields, a classical anwer for algebraic tori of dimension 1 is given by the Grunwald-Wang Theorem and there are some partial answers in the case of algebraic tori of dimension $d > 1$ [15], in the case of abelian varieties [12], [13] and even in the general case [26]. In addition the problem has been connected with a classical question posed by Cassels on the divisibility of elements of the Tate-Shafarevic group $Ш(K, \mathcal{E})$ in the Weil-Châtelet group $H^1(\mathrm{Gal}(\overline{K}/K, \mathcal{E}(K))$, where $\overline{K}$ denotes the algebraic closure of K [7], [6]. In particular the mentioned results produced in [28] and [29] assure an affirmative answer to Cassels' question for all but finitely many primes p over K (for all $p \geq 5$ when $K = \mathbb{Q}$).

In this paper we deal with the hypotheses of Problem 1. They are not minimal, in fact it suffices to assume that the local divisibility holds for a *finite* number of places instead of all but finitely many places (see also [27]). Let $G := \mathrm{Gal}(K(\mathcal{E}[m])/K)$ with cardinality $|G|$. We will denote by v both a prime in K and the associate place and by $N_{K/\mathbb{Q}}(v)$ its norm. By $h(\alpha)$ we will denote the logarithmic height of $\alpha \in \overline{K}$. We will prove that the assumption of the validity of the local divisibility for all but finitely many places v in the statement of Problem 1, can be replaced by the assumption of the validity of the local divisibility for all v with $h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(m, b, c)$, but a finite number of them with density $\delta < \dfrac{1}{|G|}$, where $B(m, b, c)$ is an upper bound of the height of the discriminant of the extension L/K. If $K/\mathbb{Q}$ is a Galois extension, the condition $h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(m, b, c)$ is equivalent to $h(v) \leq 12577 \dfrac{B(m, b, c)}{[K : \mathbb{Q}]}$ and if $K = \mathbb{Q}$, this is nothing but $\log v \leq 12577 \cdot B(m, b, c)$ (see Section 5). In particular, if $K = \mathbb{Q}$ and m is not divisible by any power p^r, with $p \in \{2, 3\}$ and $r \geq 2$, then the validity of the local divisibility for all nonarchimedean v such that $\log v \leq 12577 \cdot B(m, b, c)$, but a finite number of them with density $\delta < \dfrac{1}{|G|}$, implies the global one. Even for some integers m divisible by powers 2^r or 3^r, with $r \geq 2$, for which the local-global divisibility does not hold in general, there are still examples of elliptic curves defined over $\mathbb{Q}$ for which this Hasse principle for divisibility holds as well (see [9] or [24] for examples for $m = 4$). So, regarding the bound $B(m, b, c)$, more generally we have that, when $K = \mathbb{Q}$, in all the cases when the Hasse principle for divisibility holds, the validity of the local divisibility by all v with $\log v \leq 12577 B(m, b, c)$, but a finite number of them with density $\delta < \dfrac{1}{|G|}$, implies the global one. In the last section of the paper, for $m = 4$, in a case when the Hasse principle for divisibility holds, we will produce an explicit example showing how to find points not satisfying those hypotheses that are locally divisible for infinitely many primes but not globally divisible. We will call them pseudodivisible points.

2 On the p^r-division field

We recall the following result given in [3] about the number fields $K(\mathcal{E}[m])$, for all odd integers $m \geq 5$.

Theorem 2.1. *Let $m \geq 5$ be an odd integer and let $\mathcal{E}$ be an elliptic curve defined over a field K with char$(K) \neq 2,3$. Let $P_1 = \{x_1, y_1\}$ and $P_2 = \{x_2, y_2\}$ be two m-torsion points of $\mathcal{E}$, generating $\mathcal{E}[m]$. Then $K(\mathcal{E}[m]) = K(x_1, \zeta_m, y_2)$.*

In particular, when $m = p^r$, with $p > 3$ and $r \geq 1$ we have

$$K(\mathcal{E}[p^r]) = K(x_1, \zeta_{p^r}, y_2).$$

We are going to show that, for all $r \geq 2$, we can replace ζ_{p^r} with ζ_p in this generating system.

Theorem 2.2. *Let $\mathcal{E}$ be an elliptic curve defined over a field K with char$(K) \neq 2,3$. Let $p > 3$ be a prime number and let $r \geq 1$. If $P_1 = \{x_1, y_1\}$ and $P_2 = \{x_2, y_2\}$ are two m-torsion points of $\mathcal{E}$, generating $\mathcal{E}[m]$, then*

$$K(\mathcal{E}[p^r]) = K(x_1, \zeta_p, y_2).$$

Proof. We first prove that $K[p^r] = K(x_1, x_2, \zeta_p, y_2)$. Let $\sigma \in \mathrm{Gal}(K[p^r]/K)$ fixing x_1, x_2, ζ_p and y_2. Since σ fixes x_1, x_2 and y_2, then σ has the form

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

We recall that $\sigma(\zeta_{p^r}) = \zeta_{p^r}^{\det(\sigma)}$ and, since $\zeta_p = \zeta_{p^r}^{p^{r-1}}$, consequently $\sigma(\zeta_p) = \zeta_p^{\det(\sigma)}$. If σ fixes ζ_p, then $\det(\sigma) \equiv 1 \pmod{p}$. We deduce

$$\sigma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and $K[p^r] = K(x_1, \zeta_p, x_2, y_2)$. Now let $\sigma \in \mathrm{Gal}(K[p^r]/K)$ fixing x_1, ζ_p and y_2. To prove $K[p^r] = K(x_1, \zeta_p, y_2)$, it suffices to show that σ is the identity. If σ fixes x_1, then σ has the form

$$\begin{pmatrix} \pm 1 & \alpha \\ 0 & \beta \end{pmatrix}.$$

As above, if σ fixes ζ_p, then $\det(\sigma) \equiv 1 \pmod p$. We deduce

$$\sigma = \begin{pmatrix} \pm 1 & \alpha \\ 0 & \pm 1 + kp \end{pmatrix},$$

with $0 \leq k \leq p^{r-1} - 1$. Moreover σ fixes y_2. Then the polynomial $x_2^3 + bx_2 + c - y_2^2 = 0$ has degree at most 3 over K and $[K[p^r] : K(x_1, \zeta_p, y_2)] \leq 3$. This implies that either σ^2 fixes x_2 or σ^3 fixes x_2. If $\sigma^2(x_2) = x_2$, then

$$\sigma^2 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p^r},$$

i.e.

$$\begin{pmatrix} 1 & \pm 2\alpha + \alpha kp \\ 0 & 1 \pm 2kp + k^2p^2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p^r}.$$

Thus

$$\begin{cases} \pm 2\alpha + \alpha kp & \equiv 0 \pmod{p^r} \\ 1 \pm 2kp + k^2p^2 & \equiv 1 \pmod{p^r} \end{cases}$$

$$\begin{cases} \alpha(\pm 2 + kp) & \equiv 0 \pmod{p^r} \\ kp(\pm 2 + kp) & \equiv 0 \pmod{p^r} \end{cases}$$

Since $p \neq 2$, then $\pm 2 + kp \not\equiv 0 \pmod{p^r}$, for every $0 \leq k \leq p^{r-1} - 1$. Therefore $\alpha \equiv 0 \pmod{p^r}$ and $kp \equiv 0 \pmod{p^r}$, implying $\sigma = \pm\mathrm{Id}$. Anyway $\sigma = -\mathrm{Id}$ is not possible, since σ fixes y_2. Therefore $\sigma = \mathrm{Id}$.

If $\sigma^3(x_2) = x_2$, then

$$\sigma^3 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p^r},$$

i.e.

$$\begin{pmatrix} \pm 1 & 3\alpha \pm 3\alpha kp + \alpha k^2p^2 \\ 0 & \pm 1 + 3kp \pm 3k^2p^2 + k^3p^3 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p^r}. \tag{2.1}$$

Immediately we deduce

$$\sigma = \begin{pmatrix} 1 & \alpha \\ 0 & \pm 1 + kp \end{pmatrix}.$$

Since $\det(\sigma) = \pm 1 + kp \equiv 1 \pmod{p}$, then

$$\sigma = \begin{pmatrix} 1 & \alpha \\ 0 & 1+kp \end{pmatrix}.$$

Moreover, from (2.1), we have

$$\begin{cases} 3\alpha + 3\alpha kp + \alpha k^2p^2 & \equiv 0 \pmod{p^r} \\ 1 + 3kp + 3k^2p^2 + k^3p^3 & \equiv 1 \pmod{p^r} \end{cases}$$

$$\begin{cases} \alpha(3 + 3kp + k^2p^2) & \equiv 0 \pmod{p^r} \\ kp(3 + 3kp + k^2p^2) & \equiv 0 \pmod{p^r}. \end{cases}$$

Owing to $3+3kp+k^2p^2 \not\equiv 0 \pmod{p^r}$, for all $0 \leq k \leq p^{r-1}-1$ (recall that $p > 3$), then $\alpha \equiv 0 \pmod{p^r}$ and $kp \equiv 0 \pmod{p^r}$, implying $\sigma = \mathrm{Id}$ and $K(\mathcal{E}[p^r]) = K(x_1, \zeta_p, y_2)$. $\square$

We keep the notation introduced in Section 1 and set $F := K(x_1, y_1)$. As usual we denote by $\mathbb{F}_p$ the field with p elements.

Theorem 2.3. *For all $p > 3$ and $r \geq 1$,*

1. *the degree $[K_{p^r} : K(x_1, \zeta_{p^r})]$ divides $2p^r$ and the Galois group $\mathrm{Gal}(K_{p^r}/K(x_1, \zeta_{p^r}))$ is cyclic, generated by a power of $\eta = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$.*

2. *The extension $K(\mathcal{E}[p^r])/F$ is metacyclic. In particular $K(\mathcal{E}[p^r])/F = F(\zeta_{p^r}, \sqrt[m_1]{a})$, with $a \in F(\zeta_{p^r})$ and $\mathrm{Gal}(K(\mathcal{E}[p^r])/F) = C_{m_1}.C_{m_2}$, where m_1, m_2 are positive integers such that $m_1|p^r$ and $m_2|p^{r-1}(p-1)$. The group C_{m_1} is generated by a power of $\omega = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.*

3. *If $\mathcal{E}$ has a $K(p^r)$-rational point of order p^r, then $K(\mathcal{E}[p^r]) = K(\zeta_{p^r}, \sqrt[m_1]{a})$, with $a \in K(\zeta_{p^r})$ and $m_1|p^r$, and the extension $K(\mathcal{E}[p^r])/K$ is metacyclic of order dividing $p^{2r-1}(p-1)$.*

Proof. **1.** By Theorem 2.1, we have $K_{p^r} = K(x_1, \zeta_{p^r}, y_2)$. Let $\sigma \in \mathrm{Gal}(K(\mathcal{E}[p^r])/K)$ fixing x_1 and ζ_{p^r}. Then $\sigma(P_1) = \pm P_1$ and $\det(\sigma) = 1$, i. e.

$$\sigma = \begin{pmatrix} \pm 1 & \alpha \\ 0 & \pm 1 \end{pmatrix},$$

for some $0 \leqslant \alpha \leqslant p^r - 1$. The powers of η are

$$\eta^n = \begin{cases} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} & \text{if } n \text{ is even} \\ \\ \begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix} & \text{if } n \text{ is odd} \end{cases}$$

and its order is $2p^r$. Clearly every power of σ is a power of η too. So the Galois group $\mathrm{Gal}(K_{p^r}/K(x_1,\zeta_{p^r}))$ is cyclic of order dividing $2p^r$ and it is generated by a power of η.

2. By Theorem 2.1, we have $K_{p^r}=K(x_1,\zeta_{p^r},y_2)$. In particular $K_{p^r}=K(x_1,y_1,\zeta_{p^r},y_2)$. Let $\sigma\in\mathrm{Gal}(K(\mathcal{E}[p^r]/K)$ fixing x_1, y_1 and ζ_{p^r}. Then $\sigma(P_1)=P_1$ and $\det(\sigma)=1$, i. e.

$$\sigma=\begin{pmatrix}1&\alpha\\0&1\end{pmatrix},$$

for some $0\leqslant\alpha\leqslant p^r-1$. Thus $\mathrm{Gal}(K(\mathcal{E}[p^r])/F(\zeta_{p^r})$ is cyclic of order m_1 dividing p^r and it is generated by a power of ω. Therefore $K(\mathcal{E}[p^r])/F=F(\zeta_{p^r},\sqrt[m_1]{a})$, with $a\in F(\zeta_{p^r})$. The extension $F(\zeta_{p^r})/F$ is cyclic of order dividing $p^{r-1}(p-1)$ (recall that $p\neq 2$). Therefore $\mathrm{Gal}(K(\mathcal{E}[p^r])/F)=C_{m_1}.C_{m_2}$, with $m_2|p^{r-1}(p-1)$.

3. This is a direct consequence of **2.**

□

Notice that in part **3.** of Theorem 2.3 we could have $\sqrt[m_1]{a}\in K(\zeta_{p^r})$ and $K(\mathcal{E}[p^r])=K(\zeta_{p^r})$. Of course an interesting case is when when $\mathbb{Q}(\mathcal{E}[p])=\mathbb{Q}(\zeta_p,\sqrt[p]{a})$. The istances when $\mathbb{Q}(\mathcal{E}[p])=\mathbb{Q}(\zeta_p)$ have been investigated in [21], [30], [24] and [17]. We are going to give some remarks on elliptic curves without complex multiplication (CM in the following) defined over $\mathbb{Q}$ such that $\mathbb{Q}(\mathcal{E}[p])\subsetneq\mathbb{Q}(\mathcal{E}[p])=\mathbb{Q}(\zeta_p,\sqrt[p]{a})$.

Proposition 2.4. *Let $\mathcal{E}$ be a non CM elliptic curve defined over $\mathbb{Q}$. If $p\in\{2,3,5,7\}$, then there exists an elliptic curve $\mathcal{E}/\mathbb{Q}$ such that $\mathbb{Q}(\mathcal{E}[p])/\mathbb{Q}=\mathbb{Q}(\zeta_p,\sqrt[p]{a})$, with $a\in\mathbb{Q}(\zeta_{p^r})\setminus(\mathbb{Q}(\zeta_p))^p$. If $p\geq 17$, $p\neq 37$, then $\mathbb{Q}(\mathcal{E}[p])\neq\mathbb{Q}(\zeta_p,\sqrt[p]{a})$, for all $a\in\mathbb{Q}(\zeta_p)$.*

Proof. If $\mathbb{Q}(\mathcal{E}[p])=\mathbb{Q}(\zeta_p,\sqrt[p]{a})$, with $a\in\mathbb{Q}(\zeta_p)\setminus(\mathbb{Q}(\zeta_p))^p$, then $|\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[p])/\mathbb{Q})|=p(p-1)$. By the classification of the maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ (see [32], in particular Proposition 15), we have that p divides $|\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[p])/\mathbb{Q})|$ if and only if either $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[p])/\mathbb{Q})$ is contained in a Borel subgroup, but it not contained in a split Cartan subgroup or $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[p])/\mathbb{Q})$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. If $p>17$ and $p\neq 37$, then the image of the representation

$$\rho_{\mathcal{E},p}:\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[p])/\mathbb{Q})\longrightarrow\mathrm{GL}_2(\mathbb{F}_p)$$

is either $\mathrm{GL}_2(\mathbb{F}_p)$ or it is contained in the normalizer of a non-split Cartan subgroup [33], [3]. Then $\mathbb{Q}(\mathcal{E}[p])\neq\mathbb{Q}(\zeta_p,\sqrt[p]{a})$. Therefore $\mathbb{Q}(\mathcal{E}[p])=\mathbb{Q}(\zeta_p,\sqrt[p]{a})$ implies $p\in\Omega=$

$\{2,3,5,7,11,13,17,37\}$. This proves the second part of the proposition. We are going to show explicit examples of curves $\mathcal{E}$ defined over $\mathbb{Q}$ and without CM, such that $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p, \sqrt[p]{a})$, with $a \in \mathbb{Q}(\zeta_p) \setminus (\mathbb{Q}(\zeta_p))^p$, for all $p \leq 7$. If $p = 2$, it suffices to take the curve

$$\mathcal{E} : y^2 = (x - \sqrt{\alpha})(x + \sqrt{\alpha})(x - \beta),$$

with $\alpha, \beta \in \mathbb{Q}$ and α not a rational square. In this case $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\sqrt{\alpha})$. For $p = 3$ consider the family of elliptic curves $\mathcal{F}_{b,a_0}$ in [2, Theorem 4.1, part 3.], with $a_0 = 2k^2$, $k \in \mathbb{Q}$. For every curve $\mathcal{E}_{b,2k^2}$ of

$$\mathcal{F}_{b,2k^2} : y^2 = x^3 + bx + \frac{16b^2 - 864k^2b - 3888k^4}{576k^2},$$

with $b, k \in \mathbb{Q}$, we have $\mathbb{Q}(\mathcal{E}_{b,2k^2}[3]) = \mathbb{Q}\left(\zeta_3, \sqrt[3]{\frac{k^2b}{3} + 4k^4}\right)$. So it suffices to take $\mathcal{F}_{b,2k^2}$, with $k \in \mathbb{Q}$ such that $\frac{k^2b}{3} + 4k^4$ is not a cube. By part **3.** of Theorem 2.3, if $\mathcal{E}$ has a $\mathbb{Q}(\zeta_p)$-rational point of exact order p, then $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p, \sqrt[p]{a})$, with $a \in \mathbb{Q}(\zeta_p)$. Since by Mazur's Theorem [20], there exist elliptic curves with a rational torsion point of exact order 5 or 7, then for those curves we have $\mathbb{Q}(\mathcal{E}[5]) = \mathbb{Q}(\zeta_5, \sqrt[5]{a})$, with $a \in \mathbb{Q}(\zeta_5)$ and, respectively $\mathbb{Q}(\mathcal{E}[7]) = \mathbb{Q}(\zeta_7, \sqrt[7]{a})$, with $a \in \mathbb{Q}(\zeta_7)$. For such curves there are two possibilities: either $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$ or $\mathbb{Q}(\zeta_p) \subsetneq \mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p, \sqrt[p]{a})$, $p \in \{5,7\}$. In [17] Gonzáles-Jiménes and Lozano-Robledo proved that if $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$, then $p \leq 5$ (see also [21], [30]). Therefore for every elliptic curve with a rational torsion point of order 7, we have $\mathbb{Q}(\mathcal{E}[7]) = \mathbb{Q}(\zeta_7, \sqrt[7]{a})$, with $a \in \mathbb{Q}(\zeta_7) \setminus \mathbb{Q}(\zeta_7)^7$. Examples of elliptic curves in short Weierstrass form with a rational torsion point of order 7 are

$$\mathcal{E} : y^2 = x^3 - 3483x + 121014,$$

$$\mathcal{E} : y^2 = x^3 - 1323x + 6395814.$$

For $p = 5$, examples of elliptic curves with a rational point of order 5 such that $\mathbb{Q}(\zeta_5) \subsetneq \mathbb{Q}(\mathcal{E}[5]) = \mathbb{Q}(\zeta_5, \sqrt[5]{a})$, with $a \in \mathbb{Q}(\zeta_5)$ are the curves

$$\mathcal{E} : y^2 = x^3 - 432x + 8208,$$

$$\mathcal{E} : y^2 = x^3 - 27x + 55350.$$

$\square$

There are no known examples of non CM elliptic curve defined over $\mathbb{Q}$ such that $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p, \sqrt[p]{a})$, for $p \in \{11, 13, 17, 37\}$. The curve 121a1 in Cremona label is a non CM elliptic curve defined over $\mathbb{Q}(\zeta_{11})$ with a torsion point of exact order 11 defined over $K = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$. For this curve we have $\mathbb{Q}(\mathcal{E}[11]) = \mathbb{Q}(\zeta_{11}, \sqrt[11]{a})$, for some $a \in \mathbb{Q}(\zeta_{11})$; anyway 121a1 is defined over $\mathbb{Q}(\zeta_{11})$ and not over $\mathbb{Q}$, as stated above. The curve 121b1 in Cremona label is defined over $\mathbb{Q}$ and it has a torsion point of exact order 11 defined over $K = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$, but it has CM too. In principle we can have non CM elliptic curves defined over $\mathbb{Q}$ with $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p, \sqrt[p]{a})$, for $p \in \{11, 13, 17, 37\}$. In fact, in principle we can have a non CM elliptic curve with a point of order 11 defined on a subfield of $\mathbb{Q}(\zeta_{11})$, since we can have a non CM elliptic curve with a point of order 11 defined on a field of degree 5 over $\mathbb{Q}$ [18]. Similarly a point of exact order 13 of a non CM elliptic curve can be defined on a number field of degree 3 or 4 or 6 or 12 over $\mathbb{Q}$ [18] and a point of exact order 17 (resp. 37) of a non CM elliptic curve can be defined on a number field of degree 8 or 16 (resp. 12 or 36 over $\mathbb{Q}$) [18]. Anyway, regarding the cases when $p \in \{13, 17, 37\}$, all the known Galois representations of $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[p])/\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{F}_p)$, that are not surjective are subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ of order $> (p-1)p$ (then in particular $\mathbb{Q}(\mathcal{E}[p]) \neq \mathbb{Q}(\zeta_p, \sqrt[p]{a})$ in all those examples) [35]. Therefore we can conjecture that if $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p, \sqrt[p]{a})$, with $a \in \mathbb{Q}(\zeta_p) \setminus (\mathbb{Q}(\zeta_p))^p$, then $p \in S = \{2, 3, 5, 7, 11\}$. It is also our guess that S can be shrunk to $\{2, 3, 5, 7\}$.

For completeness we bound the degree $[K(\mathcal{E}[p^r]) : K(x_1, \zeta_p)]$ and describe the Galois group $\mathrm{Gal}(K(\mathcal{E}[p^r])/K(x_1, \zeta_p))$.

Proposition 2.5. *Let $p \geq 5$ and $r \geq 1$. Then the degree $[K(\mathcal{E}[p^r]) : K(x_1, \zeta_p)]$ divides $2p^{2r-1}$ and the extension $K(x_1, \zeta_p, y_2)/K(x_1, \zeta_p)$ is a metacyclic extension with Galois group $C_{m_3}.C_{m_4}$, where m_3, m_4 are positive integers such that $m_3 | 2p^r$ and $m_4 | p^{r-1}$.*

Proof. In part **1.** of Theorem 2.3 we have proved that $[K(\mathcal{E}[p^r])/K(x_1, \zeta_{p^r})]$ is a cyclic extension of order dividing $2p^r$. The extension $K(\zeta_{p^r})/K(\zeta_p)$ is cyclic of order dividing p^{r-1} (recall $p \neq 2$). Since $K(\mathcal{E}[p^r]) = K(x_1, \zeta_p, y_2)$ by Theorem 2.2, then $[K(\mathcal{E}[p^r]) : K(x_1, \zeta_p)] | 2p^{2r-1}$ and $\mathrm{Gal}(K(\mathcal{E}[p^r])/K(x_1, \zeta_p)) = C_{m_3}.C_{m_4}$, with $m_3 | 2p^r$ and $m_4 | p^{r-1}$. $\square$

3 On the height of the abscissas of the m-torsion points of $\mathcal{E}$

From now on let K be a number field and $m \geq 3$. Let M_K be the set of places v of K. For every $v \in M_K$, we denote by $|\ .\ |_v$ the associate absolute value. As in Section 1, by K_v we denote the completion of K at v. We briefly recall some basic facts about the height of a rational number and of a polynomial (for further details see [14] and [5]). We also show how to get a bound for the height of the abscissas of a m-torsion point of $\mathcal{E}$, for every m.

Definition 3.1. Let $\alpha \in K$. We define the height of α as

$$H(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{\frac{d_v}{d}},$$

where $d = [K : \mathbb{Q}]$ and $d_v = [K_v : \mathbb{Q}_{\tilde{v}}]$, with $\tilde{v} \in M_{\mathbb{Q}}$ and $v|\tilde{v}$.

Observe that $H(v) = v^{\frac{d_v}{d}}$, for every prime v of K. In particular $H(v) = v$, when $K = \mathbb{Q}$. In many cases it is more useful to work with the logarithm of $H(\alpha)$, instead of $H(\alpha)$ itself. For this reason we have the following definition.

Definition 3.2. Let K be a number field and let $\alpha \in K$. We define the logarithmic height (or Weil height) of α as

$$h(\alpha) := \log^+ H(\alpha) = \sum_{v \in M_k} \frac{d_v}{d} \log^+ |\alpha|_v.$$

We recall that $\log^+ 0 := 0$ and $\log^+ \beta := \max\{0, \log \beta\}$ for every $\beta \in \mathbb{R}^+$ (see for instance [5]). In particular we have $h(\alpha) \geq 0$, for all α. Let ∞ denote the archimedean place of $\mathbb{Q}$ and $|\ .\ |$ denote the classical absolute value associated to ∞. If $\alpha \in \mathbb{Q}$, $\alpha = \frac{\alpha_1}{\alpha_2}$, with $\alpha_1 \in \mathbb{Z}$, $\alpha_2 \in \mathbb{Z} \setminus \{0\}$ and $\gcd(\alpha_1, \alpha_2) = 1$, then $h(\alpha) = \log^+ \max\{|\alpha_1|, |\alpha_2|\}$. If $\alpha \in \mathbb{Z}$, then $h(\alpha) = \log^+ |\alpha|$ and if $\alpha \in \mathbb{Z} \setminus \{0\}$, then $h(\alpha) = \log|\alpha|$. There are some basic properties of the logarithmic height that we list below (see also [16] and [5]).

Proposition 3.3. *Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let r be a positive integer and let $\alpha, \beta, \alpha_1, \alpha_2, ..., \alpha_r \in \overline{\mathbb{Q}}$. Then*

i. $h(\alpha\beta) \leq h(\alpha) + h(\beta)$;

ii. $h(\alpha_1 + \alpha_2 + ... + \alpha_r) \leq h(\alpha_1) + h(\alpha_2) + ... + h(\alpha_r) + \log r$;

iii. $h(\alpha^r) = rh(\alpha)$;

iv. $h(\sigma(\alpha)) = h(\alpha)$.

There is a classical way of defining the height of a polynomial too.

Definition 3.4. Let K be a number field and let $f(x) \in K[x]$, such that

$$f(x) = \sum_{i=0}^{r} a_i x^i.$$

We define the height of f as

$$H(f) = \prod_{v \in M_k} (\max_i |a_i|_v)^{\frac{d_v}{d}}$$

and the logarithmic height of f as

$$h(f) = \log^+ H(f) = \sum_{v \in M_k} \frac{d_v}{d} \log^+(\max_i |a_i|_v).$$

For every algebraic integer $\alpha \in K$, we denote by f_α its minimal polynomial and by $\widetilde{f_\alpha}$ the multiple of f_α with integer coprime coefficients. Observe that for $\widetilde{f_\alpha}$, we have $\max_i |a_i|_v = 1$, for every non-archimedean place v of K; otherwise all the coefficients of $\widetilde{f_\alpha}$ would be divisible by v, which is a contraddiction. Then

$$h(\widetilde{f_\alpha}) = \log^+(\max_i |a_i|) = \log(\max_i |a_i|). \tag{3.1}$$

We recall the following relation between the logarithmic height of α and the logarithmic height of f_α.

Proposition 3.5. *Let K be a number field and $\alpha \in \overline{K}$ be algebraic over K, with minimal polynomial f_α. Then*

$$h(\alpha) \leq h(f_\alpha) + \log 2. \tag{3.2}$$

Proof. Let $f_\alpha = \sum_{i=1}^{n} a_i x^i$, with $a_n = 1$. We prove that $|\alpha|_v \leq 2 \max_i |a_i|_v$, for every $v \in M_K$. Obviously $\max_i |a_i|_v \geq 1$, because of $a_n = 1$. Therefore, if $|\alpha|_v \leq 1$, then $|\alpha|_v \leq \max_i |a_i|_v \leq 2 \max_i |a_i|_v$. Assume $|\alpha|_v > 1$. Since α is a root of f_α, then $\alpha^n = -\sum_{i=1}^{n-1} a_i \alpha^i$. If v is nonarchimedean, then, by the strong triangle inequality,

$$|\alpha|_v^n \leq \max_i |a_i|_v |\alpha|_v^{n-1}$$

(recall that we are assuming $|\alpha|_v > 1$, which implies $|\alpha|_v^{n-1} > |\alpha|_v^i$, for every $1 \leq i \leq n-2$). Thus $|\alpha|_v \leq \max_i |a_i|_v$. If $v = \infty$ is archimedean, then we use the triangle inequality

$$\begin{aligned}|\alpha|^n &\leq \sum_{i=1}^{n-1} |a_i||\alpha|^i \leq \max_i |a_i| \sum_{i=1}^{n-1} |\alpha|^i = \max_i |a_i| \cdot |\alpha|^{n-1} \left(1 + \sum_{i=1}^{n-2} \frac{1}{|\alpha|^i}\right) \\ &\leq \max_i |a_i| \cdot |\alpha|^{n-1} \left(1 + \sum_{i=1}^{n-2} \frac{1}{2^i}\right) \leq 2 \max_i |a_i| \cdot |\alpha|^{n-1}\end{aligned}$$

Therefore $|\alpha| \leq 2 \max_i |a_i|$. We deduce

$$\log^+ |\alpha|_v \leq \log^+ |2|_v + \log^+ \max_i |a_i|_v,$$

for all $v \in M_K$, and then

$$\sum_{v \in M_k} \frac{d_v}{d} \log^+ |\alpha|_v \leq \sum_{v \in M_k} \frac{d_v}{d} \log^+ |2|_v + \sum_{v \in M_k} \frac{d_v}{d} \log^+ \max_i |a_i|_v,$$

i.e.

$$h(\alpha) = h(f_\alpha) + \log 2.$$

□

In the case when α is one of the abscissas of the m-torsion points of $\mathcal{E}$, the minimal polynomial of α divides the m-th division polynomial Ψ_m of $\mathcal{E}$ (i.e. the polynomial whose roots are the abscissas of the m-torsion points of $\mathcal{E}$). We recall that

$$\deg \Psi_m = \begin{cases} \dfrac{m^2-1}{2}, & \text{if } m \text{ is odd;} \\ \dfrac{m^2-4}{2}, & \text{if } m \text{ is even;} \end{cases}$$

(see for instance [23]) and that Ψ_m has integer coefficients. We denote by b_i, with $0 \leq i \leq \deg \Psi_m$, the coefficients of Ψ_m. We can deduce an uniform bound for the absolute value $|b_i|$, for every $0 \leq i \leq \deg \Psi_m$, by the following result (see [23, equation (6), pag. 769]).

Proposition 3.6 (McKee, 2010)**.** *Let* $\Psi_m = \sum_{i=0}^{\deg \Psi_m} b_i x^i$ *be the* m*-th division polynomial of* $\mathcal{E}$*, where* $b_i = \sum_{2r+3s=\deg \Psi_m - i} a_{r,s} b^r c^s$*. Then*

$$|a_{r,s}| \leq \frac{m^{m^2}(m^2-\frac{1}{2})!}{[(\frac{m^2-1}{2})!]^2(\frac{m^2}{2}+1)!} \sim \frac{2^{\frac{3m^2+1}{2}}e^{\frac{m^2}{2}}}{\pi m^3}, \tag{3.3}$$

for all r, s.

Observe that the bound in (3.3) does not depend on r, s. So, in particular, it holds for $\max|a_{r,s}|$. For m small we have

$$\frac{m^{m^2}(m^2-\frac{1}{2})!}{[(\frac{m^2-1}{2})!]^2(\frac{m^2}{2}+1)!} \leq \frac{2^{\frac{3m^2+1}{2}}e^{\frac{m^2}{2}}}{\pi m^3};$$

when m grows, the bound of $|a_{r,s}|$ is asintothically equivalent to $\frac{2^{\frac{3m^2+1}{2}}e^{\frac{m^2}{2}}}{\pi m^3}$. Therefore

$$\log^+|a_{r,s}| \leq \frac{3m^2+1}{2}\log 2 + \frac{m^2}{2} - 3\log m - \log\pi, \tag{3.4}$$

for every r, s and, in particular,

$$\log^+\max|a_{r,s}| \leq \frac{3m^2+1}{2}\log 2 + \frac{m^2}{2} - 3\log m - \log\pi.$$

By $b_i = \sum_{2r+3s=\deg\Psi_m - i} a_{r,s}b^rc^s$, one can deduce the following statement.

Corollary 3.7. *Let $\Psi_m = \sum_{i=0}^{\deg\Psi_m} b_ix^i$ be the m-th division polynomial of $\mathcal{E}$, where*

$$\deg\Psi_m = \begin{cases} \dfrac{m^2-1}{2}, & \text{if } m \text{ is odd;} \\[2ex] \dfrac{m^2-4}{2}, & \text{if } m \text{ is even.} \end{cases}$$

Then

$$\log^+\max_i|b_i| \leq \deg\Psi_m\left(\frac{3m^2+1}{2}\log 2 + \frac{m^2}{2} - 3\log m - \log\pi + h(b) + h(c)\right). \tag{3.5}$$

Notice that the last bound holds for the coefficients of $\widetilde{f_\alpha}$ too (and for the coefficients of f_α itself). With the next statement we give a bound to the height of the abscissas of a m-torsion point of $\mathcal{E}$, that we will use in the following.

Lemma 3.8. *Let $\mathcal{E}$ be an elliptic curve defined over a number field K, with Weierstrass form $\mathcal{E} : y^2 = x^3 + bx + c$. Let α be the abscissas of a m-torsion of $\mathcal{E}$ and let $h(\alpha)$ denote its logarithmic height. Then*

$$h(\alpha) \leq \begin{cases} (m^2-1)^2\log m + \dfrac{m^2-1}{2}\left(h(b)+h(c)\right) + \log 2, & \textit{if } m \geq 3 \textit{ is odd;} \\[2ex] (m^2-4)^2\log m + \dfrac{m^2-4}{2}\left(h(b)+h(c)\right) + \log 2, & \textit{if } m \geq 4 \textit{ is even.} \end{cases} \tag{3.6}$$

Proof. By equation (3.1) and equation (3.5) the height of $\widetilde{f_\alpha}$ can be bounded as follows:

$$h(\widetilde{f_\alpha}) \leq \deg \Psi_m \left(\frac{3m^2+1}{2}\log 2 + \frac{m^2}{2} - 3\log m - \log \pi + h(b) + h(c)\right). \tag{3.7}$$

By the Gelfand's inequality [14, B.7.3], we have that

$$h(f_\alpha) \leq h(\widetilde{f_\alpha}) + \deg(\widetilde{f_\alpha}).$$

Since $\deg(\widetilde{f_\alpha}) \leq \deg(\Psi_m)$, then by equation (3.7) and equation (3.2), we deduce

$$h(\alpha) \leq \begin{cases} \dfrac{m^2-1}{2}\left(\dfrac{3m^2+1}{2}\log 2 + \dfrac{m^2}{2} - 3\log m - \log \pi + h(b) + h(c)\right) & +\dfrac{m^2-1}{2} + \log 2, \\ & \text{if } m \geq 3 \text{ is odd;} \\[2ex] \dfrac{m^2-4}{2}\left(\dfrac{3m^2+1}{2}\log 2 + \dfrac{m^2}{2} - 3\log m - \log \pi + h(b) + h(c)\right) & +\dfrac{m^2-4}{2} + \log 2, \\ & \text{if } m \geq 4 \text{ is even.} \end{cases} \tag{3.8}$$

Suppose that $m \geq 3$ is odd. Observe that $\dfrac{3m^2+1}{2}\log 2 < \dfrac{3m^2+1}{2}\log m$ and $\dfrac{m^2}{2} - \log \pi < \dfrac{m^2-1}{2}\log m$. Applying these inequalities, equation (3.8) becomes

$$\begin{aligned} h(\alpha) \leq& \frac{m^2-1}{2}\left(\frac{3m^2+1}{2}\log m + \frac{m^2-1}{2}\log m - 3\log m + h(b) + h(c)\right) + \frac{m^2-1}{2} + \log 2 \\ =& \frac{m^2-1}{2}\left(\frac{3m^2+1+m^2-1-6}{2}\log m + h(b) + h(c)\right) + \frac{m^2-1}{2} + \log 2 \\ =& \frac{m^2-1}{2}\left((2m^2-3)\log m + h(b) + h(c)\right) + \frac{m^2-1}{2} + \log 2 \end{aligned}$$

To give a bound in a more condensed form, we also observe that $\dfrac{m^2-1}{2} \leq \dfrac{m^2-1}{2}\log m$ (recall that $m \geq 3$). Thus for $m \geq 3$ odd, we have

$$h(\alpha) \leq (m^2-1)^2\log m + \frac{m^2-1}{2}\left(h(b)+h(c)\right) + \log 2.$$

Now suppose that $m \geq 4$ is even. With the aim to get a bound similar to the one obtained for odd m, we observe that

$$\frac{3m^2+1}{2}\log 2 + \frac{m^2}{2} - 3\log m - \log \pi \leq (2m^2-9)\log m.$$

Then equation (3.8) becomes

$$h(\alpha) \leq \frac{m^2-4}{2}\big((2m^2-9)\log m + h(b) + h(c)\big) + \frac{m^2-4}{2} + \log 2.$$

Again, to have a bound in a more condensed form notice that $\frac{m^2-4}{2} \leq \frac{m^2-4}{2}\log m$, for all $m \geq 4$. Thus

$$h(\alpha) \leq (m^2-4)^2 \log m + \frac{m^2-4}{2}(h(b)+h(c)) + \log 2.$$

□

4 A bound for the height of the discriminant of a m-division field

For every extension L/K of number fields, we denote by $D_{L/K}$ its discriminant. We recall that given a tower of extensions $L \subseteq F \subseteq K$, the discriminant of L/K is equal to

$$D_{L/K} = D_{F/K}^{[L:F]} N_{F/K}(D_{L/F}). \tag{4.1}$$

(see for instance [19] or [4]). If $L = EF$ is the compositum of two fields linearly disjoint over K, then

$$D_{L/K} = D_{E/K}^{[F:K]} D_{F/K}^{[E:K]} \tag{4.2}$$

(see for instance [22]).

Remark 4.1. Obviously we can rewrite equation (4.1) as

$$D_{L/K} = D_{F/K}^{[L:F]} \prod_{\sigma \in \mathrm{Gal}(F/K)} \sigma(D_{L/F}).$$

Consider the logarithmic height of $|D_{L/K}|$ in the last equation. By the properties recalled in Proposition 3.3, we have

$$h(D_{L/K}) \leq [L:F]h(D_{F/K}) + [F:K]h(D_{L/F}). \tag{4.3}$$

On the other hand, if we consider the logarithmic height of $D_{E/K}$ in equation (4.2), then we get

$$h(D_{E/K}) \leq [F:K]h(D_{E/K}) + [E:K]h(D_{F/K}). \tag{4.4}$$

Since E and F are linearly disjoint over K, then both $[L:F] = [EF:F] = [E:K]$ and $D_{L/F} = D_{E/K}$. Therefore (4.4) is nothing but (4.3) again

$$h(D_{E/K}) \leq [F:K]h(D_{L/F}) + [L:F]h(D_{F/K}).$$

Then, when we calculate the height of the discriminant on an extension EF/K, we can assume without loss of generality that E and F are linearly disjoint over K.

We also recall that $disc(f_1(x))$ divides $disc(f_1(x)f_2(x))$, for every $f_1(x), f_2(x) \in K[x]$. From here on out we will consider the extension L/K with $L = K(\mathcal{E}[m])$. We are going to give a bound to the height of its discriminant. Such a computation can be obtained by using one of the generating systems of $K(\mathcal{E}[m])/K$ mentioned above. Anyway, it turns out that the orders of the bounds got by using different generating systems are similar and then there is no much improvement in changing the generating system in this case. For this reason we are going to use the classical generating system $\{x_1, x_2, y_1, y_2\}$ which has the advantage of holding for all m.

Theorem 4.2. *Let $\mathcal{E}: y^2 = x^3 + bx + c$ be an elliptic curve defined over a number field K. Consider the extension $L := K(\mathcal{E}[m])$, where $m \geq 3$ is a positive integer. Then*

$$h(D_{L/K}) \leq \begin{cases} 5(m^2-1)^3(m^2-3)(\log m + h(b) + h(c)), & \text{if } m \geq 3 \text{ is odd;} \\ 5(m^2-4)^3(m^2-6)(\log m + h(b) + h(c)), & \text{if } m \geq 4 \text{ is even.} \end{cases} \tag{4.5}$$

Proof. As in the previous sections, let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be a generating set for $\mathcal{E}[m]$. Then $K(\mathcal{E}[m]) = K(x_1, x_2, y_1, y_2)$. To extimate $|D_{L/K}|$, we use the equalities (4.1) and (4.2). We denote by F_1 and F_2 the fields $K(x_1)$ and respectively $K(x_2)$.

By F_3 we denote the field $K(x_1, x_2, y_1) = F_1F_2(y_1)$. First of all we have to bound the discriminant of the extension F_1/K. Since this extension is monogeneous, we have to bound the discriminant of the minimal polynomial of x_1, which divides the m-th division polynomial Ψ_m of $\mathcal{E}$. Let $Disc(\Psi_m)$ be the discriminant of Ψ_m and let $\Delta = -16(4b^3 + 27c^2)$ be the discriminant of $\mathcal{E}$. In [31], where Ψ_m is denoted by B_n^*, Schmidt shows

$$Disc(\Psi_m) = \begin{cases} (-1)^{\frac{m-1}{2}} m^{\frac{m^2-3}{2}} \Delta^{\frac{(m^2-1)(m^2-3)}{24}}, & \text{if } m \text{ is odd;} \\ (-1)^{\frac{m-2}{2}} m^{\frac{m^2}{2}} 2^{2-m^2} \Delta^{\frac{m^2(m^2+2)}{24}}, & \text{if } m \text{ is even.} \end{cases}$$

(see also [34]). Thus

$$D_{F_1/K} \leq \begin{cases} (-1)^{\frac{m-1}{2}} m^{\frac{m^2-3}{2}} \Delta^{\frac{(m^2-1)(m^2-3)}{24}}, & \text{if } m \text{ is odd;} \\ (-1)^{\frac{m-2}{2}} m^{\frac{m^2}{2}} 2^{2-m^2} \Delta^{\frac{m^2(m^2+2)}{24}}, & \text{if } m \text{ is even.} \end{cases} \tag{4.6}$$

Similarly, we have

$$D_{F_2/K} \leq \begin{cases} (-1)^{\frac{m-1}{2}} m^{\frac{m^2-3}{2}} \Delta^{\frac{(m^2-1)(m^2-3)}{24}}, & \text{if } m \text{ is odd;} \\ (-1)^{\frac{m-2}{2}} m^{\frac{m^2}{2}} 2^{2-m^2} \Delta^{\frac{m^2(m^2+2)}{24}}, & \text{if } m \text{ is even.} \end{cases} \tag{4.7}$$

Since we aim to bound the height of the discriminant of the extension F_1F_2/K, by Remark 4.1, we can assume, without loss of generality that F_1 and F_2 are linearly disjoint over K and that

$$D_{F_1F_2/K} = D_{F_1/K}^{[F_2:K]} D_{F_2/K}^{[F_1:K]}.$$

Both $[F_1 : K]$ and $[F_2 : K]$ are less or equal than $\deg(\Psi_m)$. As in the statement of Proposition 3.6, we have

$$\deg(\Psi_m) = \begin{cases} \dfrac{m^2-1}{2} \text{ if } m \text{ is odd;} \\ \\ \dfrac{m^2-4}{2} \text{ if } m \text{ is even.} \end{cases}$$

By (4.6) and (4.7), we get

$$D_{F_1F_2/K} \leq \begin{cases} \left[(-1)^{\frac{m-1}{2}} m^{\frac{m^2-3}{2}} \Delta^{\frac{(m^2-1)(m^2-3)}{24}}\right]^{m^2-1} & \text{if } m \text{ is odd;} \\ \left[(-1)^{\frac{m-2}{2}} m^{\frac{m^2}{2}} 2^{2-m^2} \Delta^{\frac{m^2(m^2+2)}{24}}\right]^{m^2-4} & \text{if } m \text{ is even.} \end{cases}$$

Thus

$$h(D_{F_1F_2/K}) \le \begin{cases} \dfrac{m^2-1}{2}(h(D_{F_1/K})+h(D_{F_2/K})), & \text{if } m \text{ is odd;} \\ \dfrac{m^2-4}{2}(h(D_{F_1/K})+h(D_{F_2/K})), & \text{if } m \text{ is even;} \end{cases}$$

and

$$h(D_{F_1F_2/K}) \le \begin{cases} (m^2-1)\left(\dfrac{m^2-3}{2}\log m + \dfrac{(m^2-1)(m^2-3)}{24}h(\Delta)\right), & \text{if } m \text{ is odd;} \\ (m^2-4)\left(\dfrac{m^2}{2}\log m + (m^2-2)\log 2 + \dfrac{m^2(m^2+2)}{24}h(\Delta)\right), & \text{if } m \text{ is even.} \end{cases} \tag{4.8}$$

We must extimate the norm of D_{F_3/F_1F_2} and the norm of D_{L/F_1F_2}. Since F_3 contains x_1, then $[F_3 : F_1F_2] \le 2$. If $F_3 \ne F_1F_2$, then a basis of F_3/F_1F_2 is $\mathfrak{B} = \{1, y_1\}$. The Galois group $\mathrm{Gal}(F_3/F_1F_2)$ is generated by the automorphism of the m-torsion points of $\mathcal{E}$ sending y_1 to $-y_1$ (and fixing x_1). Therefore

$$Disc(\mathfrak{B}) = \left[\det\begin{pmatrix} 1 & y_1 \\ 1 & -y_1 \end{pmatrix}\right]^2 = (2y_1)^2 = 4y_1^2 = 4(x_1^3+bx_1+c). \tag{4.9}$$

Similarly the discriminant of a basis of the extension $F_1F_2(y_2)$ is $4(x_2^3+bx_2+c)$. Because of Remark 4.1 again, we can assume without loss of generality that F_3 and $F_1F_2(y_2)$ are linearly disjoint over F_1F_2. Then by the equality (4.2) we have $D_{L/F_1F_2} \le 2^8(x_1^3+bx_1+c)^2(x_2^3+bx_2+c)^2$. By the equality (4.1), there is such a relation between the discriminant of L/K and the ones of F_1F_2/K and of L/F_1F_2

$$D_{L/K} = D_{F_1F_2/K}^{[L:F_1F_2]} N_{F_1F_2/K}(D_{L/F_1F_2}).$$

We have

$$N_{F_1F_2/K}(D_{L/F_1F_2}) = \prod_{\sigma\in\mathrm{Gal}(F_1F_2/K)} 2^8\sigma(x_1^3+bx_1+c)^2\sigma(x_2^3+bx_2+c)^2.$$

Since both x_1 and x_2 are roots of Ψ_m, then $[F_1F_2 : K] \le \deg\Psi_m(\deg\Psi_m - 1)$, i.e.

$$[F_1F_2 : K] \le \begin{cases} \dfrac{(m^2-1)(m^2-3)}{4}, & \text{if } m \text{ is odd;} \\ \dfrac{(m^2-4)(m^2-6)}{4}, & \text{if } m \text{ is even.} \end{cases}$$

For all odd $m \ge 3$, by Proposition 3.3 we get

$$\begin{aligned}h(N_{F_1F_2/K}(D_{L/F_1F_2})) &\leq [F_1F_2:K][8\log 2+2h(x_1^3+bx_1+c)+2h(x_2^3+bx_2+c)]\\ &\leq [F_1F_2:K][8\log 2+2(3h(x_1)+h(x_1)+h(b)+h(c)+\log 3)\\ &\qquad +2(3h(x_2)+h(x_2)+h(b)+h(c)+\log 3)].\end{aligned}$$

Then

$$h(N_{F_1F_2/K}(D_{L/F_1F_2})) \leq \begin{cases} \dfrac{(m^2-1)(m^2-3)}{4}[8\log 2+8h(x_1)+8h(x_2) \\ \qquad +4h(b)+4h(c)+4\log 3], & \text{if } m\geq 3 \text{ is odd;}\\ \dfrac{(m^2-4)(m^2-6)}{4}[8\log 2+8h(x_1)+8h(x_2) \\ \qquad +4h(b)+4h(c)+4\log 3], & \text{if } m\geq 3 \text{ is even.}\end{cases} \tag{4.10}$$

We are going to treat separately the case when m is odd and the case when m is even. Firstly assume $m\geq 3$ odd. By inequality (3.6), for $i=1,2$, we get

$$\begin{aligned}h(N_{F_1F_2/K}(D_{L/F_1F_2})) \leq &\frac{(m^2-1)(m^2-3)}{4}\Bigg[8\log 2+16\bigg((m^2-1)^2\log m+\\ &\frac{m^2-1}{2}(h(b)+h(c))+\log 2\bigg)+4h(b)+4h(c)+4\log 3\Bigg]\\ =&(m^2-1)(m^2-3)\Bigg[2\log 2+4\bigg((m^2-1)^2\log m+\\ &\frac{m^2-1}{2}(h(b)+h(c))+\log 2\bigg)+h(b)+h(c)+\log 3\Bigg].\end{aligned}$$

In order to give a more elegant bound, we observe that $\log 2\leq\log m$ and $\log 3\leq\log m$, for every $m\geq 3$. Then

$$\begin{aligned}h(N_{F_1F_2/K}(D_{L/F_1F_2})) \leq &(m^2-1)(m^2-3)\Bigg[2\log m+4\bigg((m^2-1)^2\log m\\ &+\frac{m^2-1}{2}(h(b)+h(c))+\log m\bigg)+h(b)+h(c)+\log m\Bigg]\\ =&(m^2-1)(m^2-3)\Bigg[(4(m^2-1)^2+7)\log m+(2m^2-1)\left(h(b)+h(c)\right)\Bigg].\end{aligned}$$

In addition $4(m^2-1)^2+7\leq\frac{9}{2}(m^2-1)^2$ and $2m^2-1\leq\frac{9}{2}(m^2-1)^2$. Thus

$$h(N_{F_1F_2/\mathbb{Q}}(D_{L/F_1F_2})) \leq \frac{9}{2}(m^2-1)^3(m^2-3)(\log m+h(b)+h(c)). \tag{4.11}$$

Putting together all those considerations and using equation (4.1), we deduce, for $m\geq 3$ odd,

$$\begin{aligned} h(D_{L/K}) \leq & 4\frac{(m^2-1)(m^2-3)}{2}\log m + 4\frac{(m^2-1)^2(m^2-3)}{24}h(\Delta) \\ & + \frac{9}{2}(m^2-1)^3(m^2-3)(\log m + h(b) + h(c)) \\ = & 2(m^2-1)(m^2-3)\log m + \frac{(m^2-1)^2(m^2-3)}{6}h(\Delta) \\ & + \frac{9}{2}(m^2-1)^3(m^2-3)(\log m + h(b) + h(c)). \end{aligned}$$

Observe that

$$\begin{aligned} h(\Delta) \leq & 6\log 2 + 3h(b) + 3\log 3 + 2h(c) + \log 2 \\ & = 7\log 2 + 3\log 3 + 3h(b) + 2h(c) \\ & \leq 10\log m + 3h(b) + 2h(c). \end{aligned} \tag{4.12}$$

Thus

$$\begin{aligned} h(D_{L/K}) \leq & 2(m^2-1)(m^2-3)\log m + \frac{(m^2-1)^2(m^2-3)}{6}(10\log m + 3h(b) + 2h(c)) \\ & + \frac{9}{2}(m^2-1)^3(m^2-3)(\log m + h(b) + h(c)) \\ = & (m^2-1)(m^2-3)\left(\left(2 + \frac{5}{3}(m^2-1)\right)\log m + \frac{m^2-1}{2}h(b) + \frac{m^2-1}{3}h(c)\right) \\ & + \frac{9}{2}(m^2-1)^3(m^2-3)(\log m + h(b) + h(c)) \\ = & (m^2-1)(m^2-3)\left(\frac{5m^2+5}{3}\log m + \frac{m^2-1}{2}h(b) + \frac{m^2-1}{3}h(c)\right) \\ & + \frac{9}{2}(m^2-1)^3(m^2-3)(\log m + h(b) + h(c)) \\ = & (m^2-1)(m^2-3)\left[\left(\frac{5m^2+5}{3} + \frac{9}{2}(m^2-1)^2\right)\log m \right. \\ & \left. + \left(\frac{m^2-1}{2} + \frac{9}{2}(m^2-1)^2\right)h(b) + \left(\frac{m^2-1}{3} + \frac{9}{2}(m^2-1)^2\right)h(c).\right] \end{aligned}$$

Observe that $\left(\frac{5m^2+5}{3} + \frac{9}{2}(m^2-1)^2\right) \leq 5(m^2-1)^2$, for all $m \geq 3$. Moreover $\left(\frac{m^2-1}{2} + \frac{9}{2}(m^2-1)^2\right) \leq 5(m^2-1)^2$ and $\left(\frac{m^2-1}{3} + \frac{9}{2}(m^2-1)^2\right) \leq 5(m^2-1)^2$, for all $m \geq 3$. Then

$$h(D_{L/K}) \leq 5(m^2-1)^3(m^2-3)(\log m + h(b) + h(c)).$$

Assume that $m \geq 4$ is even. By equation (4.10) and equation (3.6), we get

$$\begin{aligned} h(N_{F_1F_2/K}(D_{L/F_1F_2})) \leq & \frac{(m^2-4)(m^2-6)}{4}\left[8\log 2 + 16\left((m^2-4)^2\log m + \right.\right. \\ & \left.\left.\frac{m^2-4}{2}(h(b)+h(c)) + \log 2\right) + 4h(b) + 4h(c) + 4\log 3\right] \\ = & (m^2-4)(m^2-6)\left[2\log 2 + 4\left((m^2-4)^2\log m + \right.\right. \\ & \left.\left.\frac{m^2-4}{2}(h(b)+h(c)) + \log 2\right) + h(b) + h(c) + \log 3\right]. \end{aligned}$$

Again, in order to give a more elegant bound, we use that $\log 2 \leq \log m$ and $\log 3 \leq \log m$, for every $m \geq 4$. Then

$$\begin{aligned} h(N_{F_1F_2/K}(D_{L/F_1F_2})) \leq & (m^2-4)(m^2-6)\left[2\log m + 4\left((m^2-4)^2\log m + \right.\right. \\ & \left.\left.\frac{m^2-4}{2}(h(b)+h(c)) + \log m\right) + h(b) + h(c) + \log m\right]. \\ = & (m^2-4)(m^2-6)\left[(4(m^2-4)^2+7)\log m + (2m^2-7)(h(b)+h(c))\right] \end{aligned}$$

We have $4(m^2-4)^2+7 \leq \frac{9}{2}(m^2-4)^2$ and $2m^2-7 \leq \frac{9}{2}(m^2-4)^2$. Thus

$$h(N_{F_1F_2/\mathbb{Q}}(D_{L/F_1F_2})) \leq \frac{9}{2}(m^2-4)^3(m^2-6)(\log m + h(b) + h(c)). \tag{4.13}$$

We can repeat the same arguments as above, by using the bound (4.8) for m even, i.e.

$$h(D_{F_1F_2/K}) \leq (m^2-4)\left[\frac{m^2}{2}\log m + (m^2-2)\log 2 + \frac{m^2(m^2+2)}{24}h(\Delta)\right]. \tag{4.14}$$

By equation (4.1), we get

$$\begin{aligned} h(D_{L/K}) \leq & 4(m^2-4)\left[\frac{m^2}{2}\log m + (m^2-2)\log 2 + \frac{m^2(m^2+2)}{24}h(\Delta)\right] \\ & + \frac{9}{2}(m^2-4)^3(m^2-6)(\log m + h(b) + h(c)). \end{aligned}$$

We use again $\log 2 \leq \log m$. Then

$$\begin{aligned}
h(D_{L/K}) \leq & 4(m^2-4)\left[\frac{m^2}{2}\log m + (m^2-2)\log m + \frac{m^2(m^2+2)}{24}h(\Delta)\right] \\
& + \frac{9}{2}(m^2-4)^3(m^2-6)(\log m + h(b) + h(c)) \\
= & 4(m^2-4)\left[\frac{3m^2-4}{2}\log m + \frac{m^2(m^2+2)}{24}h(\Delta)\right] \\
& + \frac{9}{2}(m^2-4)^3(m^2-6)(\log m + h(b) + h(c)) \\
= & (m^2-4)\left[(6m^2-8)\log m + \frac{m^2(m^2+2)}{6}h(\Delta)\right] \\
& + \frac{9}{2}(m^2-4)^3(m^2-6)(\log m + h(b) + h(c)).
\end{aligned}$$

Because of equation (4.12), i.e. $h(\Delta) \leq 10\log m + 3h(b) + 2h(c)$, we get

$$\begin{aligned}
h(D_{L/K}) \leq & (m^2-4)\left[(6m^2-8)\log m + \frac{(m^2+2)m^2}{6}(10\log m + 3h(b) + 2h(c))\right] \\
& + \frac{9}{2}(m^2-4)^3(m^2-6)(\log m + h(b) + h(c)) \\
= & \left[\left(6m^2 - 8 + \frac{5}{3}(m^2+2)m^2\right)(m^2-4) + \frac{9}{2}(m^2-4)^3(m^2-6)\right]\log m \\
& + \left(\frac{m^2+2}{2}(m^2-4)m^2 + \frac{9}{2}(m^2-4)^3(m^2-6)\right)h(b) \\
& + \left(\frac{m^2+2}{3}(m^2-4)m^2 + \frac{9}{2}(m^2-4)^3(m^2-6)\right)h(c).
\end{aligned}$$

We have $\left(6m^2 - 8 + \frac{5}{3}(m^2+2)m^2\right)(m^2-4) + \frac{9}{2}(m^2-4)^3(m^2-6) \leq 5(m^2-4)^3(m^2-6)$, for all $m \geq 4$. In addition $\frac{m^2+2}{2}(m^2-1)m^2 + \frac{9}{2}(m^2-4)^3(m^2-6) \leq 5(m^2-4)^3(m^2-6)$ and $\frac{m^2+2}{3}(m^2-1)m^2 + \frac{9}{2}(m^2-4)^3(m^2-6) \leq 5(m^2-4)^3(m-6)$, for all $m \geq 4$. Then

$$h(D_{L/K}) \leq 5(m^2-4)^3(m-6)(\log m + h(b) + h(c)).$$

$\square$

We will use the bounds (4.5) in the next section to give an explicit effective version of the hypotheses of Problem 1, in elliptic curves over $\mathbb{Q}$.

Remark 4.3. As recalled in Section 3, if $b = \frac{b_1}{b_2}$, $c = \frac{c_1}{c_2}$, with $b_1, c_1 \in \mathbb{Z}$, $b_2, c_2 \in \mathbb{Z} \setminus \{0\}$, $\gcd(b_1, b_2) = 1$ and $\gcd(c_1, c_2) = 1$, then $h(b) = \log^+ \max\{|b_1|, |b_2|\}$ and $h(c) =$

$\log^+ \max\{|c_1|, |c_2|\}$. If $b, c \in \mathbb{Z}$, then $h(b) = \log^+ |b|$ and $h(c) = \log^+ |c|$. In particular, if $b, c \in \mathbb{Z} \setminus \{0\}$, then $h(b) + h(c) = \log |bc|$. In this last case the bound (4.5) can also be expressed in the following more elegant form

$$|h(D_{L/K})| \leq \begin{cases} (m^2-1)^3(m-3)\log m^5|bc|, & \text{if } m \geq 3 \text{ is odd;} \\ (m^2-4)^3(m-6)\log m^5|bc|, & \text{if } m \geq 4 \text{ is even.} \end{cases}$$

5 An explicit effective version of the hypotheses of Problem 1

We briefly recall the definition of the cohomology group which gives an obstruction to the validity of the Hasse principle for divisibility of points in $\mathcal{E}/K$. Let $P \in \mathcal{E}(K)$ and let $D \in \mathcal{E}(\overline{K})$ be a m-divisor of P, i.e. $P = mD$. For every $\sigma \in G = \mathrm{Gal}(K(\mathcal{E}[m])/K)$, we have

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

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

$$Z_\sigma := \sigma(D) - D. \tag{5.1}$$

Such a cocycle vanishes in $H^1(G, \mathcal{E}[m])$, if and only if there exists a K-rational m-divisor of P [9]. In particular, the hypotheses about the validity of the local-divisibility in Problem 1, assuring the existence of a K_v-rational m-divisor of P, imply that the cocycle $\{Z_\sigma\}_{\sigma\in G}$ vanishes in $H^1(\mathrm{Gal}((K(\mathcal{E}[m]))_w/K_v), \mathcal{E}[m])$, for all but finitely many $v \in M_K$, where w denotes a place of $K(\mathcal{E}[m])$ extending v. This fact motivates the following definition (5.2), given by Dvornicich and Zannier in [9], of a subgroup of $H^1(G, \mathcal{E}[m])$ which encodes the hypotheses of the problem in this cohomological context and gives an obstruction to the validity of this Hasse principle [11]. Let G_v denote the group $\mathrm{Gal}((K(\mathcal{E}[m]))_w/K_v)$ and let Σ be the subset of M_K containing all the $v \in M_K$, that are unramified in $K(\mathcal{E}[m])$. Then

$$H^1_{\mathrm{loc}}(G, \mathcal{E}[m]) := \bigcap_{v\in\Sigma} (\ker H^1(G, \mathcal{E}[m]) \xrightarrow{res_v} H^1(G_v, \mathcal{E}[m])), \tag{5.2}$$

where res_v is the usual restriction map.

Since every $v \in \Sigma$ is unramified in $K(\mathcal{E}[m])$, then G_v is a cyclic subgroup of G, for all $v \in \Sigma$. By the Chebotarev Density Theorem, the local Galois group G_v varies over *all* cyclic subgroups of G as v varies in Σ (see Theorem 5.2 and Theorem 5.3 below for further details). Then we have the following equivalent definition of the group $H^1_{\text{loc}}(G, \mathcal{E}[m])$.

Definition 5.1. 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* $H^1_{\text{loc}}(G, \mathcal{E}[m])$.

The triviality of $H^1_{\text{loc}}(G, \mathcal{E}[m])$ assures the validity of the local-global divisibility by m in $\mathcal{E}$ over K [9, Proposition 2.1]. The condition $H^1_{\text{loc}}(G, \mathcal{E}[m]) = 0$ is also necessary, not exactly over K, but over a finite extension of K [11, Theorem 3]. So the nontriviality of the first cohomology group $H^1_{\text{loc}}(G, \mathcal{E}[m])$ is an obstruction to the validity of the Hasse principle.

As stated above, the validity of the Hasse principle for divisibility of points in $\mathcal{E}$ has been proved for many integers m. Anyway in all the other papers (of various authors) about this topic, there is no information about the minimal number of places v for which the validity of the local divisibility over K_v is sufficient to have the global divisibility in $\mathcal{E}$ over K, for a general m. Only when $m = 5$ and $\mathcal{E}$ is an elliptic curve with Weierstrass form $y^2 = x^3 + bx$ or $y^2 = x^3 + c$, with $b, c \in \mathbb{Q}$, minimal bounds were produced in [27]. For the first time, here we show for every $m \geq 3$, an explicit upper bound to the number of places v for which the validity of the local divisibility by m implies the global one in all the cases when the Hasse principle for divisibility holds, in elliptic curves defined over $\mathbb{Q}$. As recalled in Section 1, this in particular happens in all $\mathcal{E}$ over $\mathbb{Q}$, for every m not divisible by any power p^n, with $p \in \{2, 3\}$ and $n \geq 2$, but there are also examples of elliptic curves $\mathcal{E}$ over $\mathbb{Q}$ for which the local-global principle for divisibility holds when m is divisible by powers of 2 or 3 (with $n \geq 2$).

We have already mentioned that by the Chebotarev 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 $K(\mathcal{E}[m])$. Therefore in fact we have

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

where S is a subset of Σ such that G_v varies over all cyclic subgroups of G as v varies in S.

If we are able to find such a set S, then we can replace the hypotheses of Problem 1 about the validity of the local divisibility for all but finitely many $v \in M_K$ with the assumption of the validity of the local divisibility for every $v \in S$. Observe that in particular S is finite (on the contrary Σ is not finite). So it suffices to have that the local divisibility by m holds for a finite number of suitable places to get the global divisibility by m. Of course S varies with respect to m and $\mathcal{E}$. In [27] the minimal possible cardinality of the set S is showed when $m = 5$ and $\mathcal{E}$ is an elliptic curve with Weierstrass form $y^2 = x^3 + bx$ or $y^2 = x^3 + c$, with $b, c \in \mathbb{Q}$. In particular the maximum number N of cyclic subgroups of $\mathrm{Gal}(K(\mathcal{E}[5])/K)$ is calculated. Then N is used as a lower bound for the cardinality of S. In principle, for every m, we can have a set S, as above, with cardinality N equal to the maximum number of cyclic subgroups of $\mathrm{Gal}(K(\mathcal{E}[m])/K)$. Anyway it is not immediate to define a proper set S, by using only this information about its cardinality. In fact, we are not sure that the validity of the local divisibility for the first N rational primes, implies the validity of the global divisibility. A priori two different primes among the first N ones, can correspond to the same cyclic Galois group G_v. For a general $\mathcal{E} : y = x^3 + bx + c$ and for every $m \geq 3$, we are going to show that we can take

$$S = \{v \in M_K \setminus \{\infty\} | h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(m, b, c)\} \setminus S', \tag{5.3}$$

where $B(m, b, c)$ is the bound for $h(D_{L/K})$ appearing in Theorem 4.2 (respectively for $m \geq 3$ odd and $m \geq 4$ even) and S' is a subset of

$$\{v \in M_K \setminus \{\infty\} | h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(m, b, c)\}$$

with cardinality $|S'| < \frac{1}{|G|}$. In particular, we are going to see that for every cyclic subgroup C of G, there exists a place v with $h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(m, b, c)$, such that $G_v = C$.

Theorem 5.2 (Chebotarev Density Theorem, 1926)**.** *Let L/K be a finite Galois extension. For every prime v of K, unramified in L, let $\left(\frac{L|K}{v}\right)$ denote the Artin symbol of v. For every conjugacy class C in $\mathrm{Gal}(L/K)$ the density of the primes v such that $\left(\frac{L|K}{v}\right) = C$ is $\frac{\#C}{\#\mathrm{Gal}(L/K)}$.*

Since the smallest among the cardinalities of a coniugacy class C in $G = \mathrm{Gal}(L/K)$ is 1, by the Chebotarev Density Theorem, the density $\delta(C)$ of primes v such that $G_v = C$ is boundend in the following way

$$\frac{1}{|G|} \leq \delta(C) \leq 1. \tag{5.4}$$

In 1979 Lagarias, Montgomery and Odlyzko gave an effective version of Chebotarev Density Theorem.

Theorem 5.3 (Lagarias, Montgomery and Odlyzko, 1979)**.** *There exists an effectively computable positive absolute constant c_1 such that for any number field K, any finite Galois extension L/K and any conjugacy class C in $\mathrm{Gal}(L/K)$, there exists a prime v of K which is unramified in L, for which $\left(\frac{L|K}{v}\right) = C$ and the norm $N_{K/\mathbb{Q}}(v)$ is a rational prime satisfying the bound*

$$N_{K/\mathbb{Q}}(v) \leq 2|D_{L/\mathbb{Q}}|^{c_1}. \tag{5.5}$$

In addition, in their recent paper [1], Ahn and Kwon show this more explicit result.

Theorem 5.4 (Ahn, Kwon, 2019)**.** *For any number field K, any finite Galois extension L/K, with $L \neq \mathbb{Q}$ and any conjugacy class C in $\mathrm{Gal}(L/K)$, there exists a prime v of K which is unramified in L, for which $\left(\frac{L|K}{v}\right) = C$ and the norm $N_{K/\mathbb{Q}}(v)$ is a rational prime satisfying the bound*

$$N_{K/\mathbb{Q}}(v) \leq |D_{L/\mathbb{Q}}|^{12577}. \tag{5.6}$$

Since $\mathbb{Q}(\zeta_m) \subseteq K(\mathcal{E}[m])$, then $L = K(\mathcal{E}[m]) \neq \mathbb{Q}$, for all K, $\mathcal{E}$ and $m \geq 3$. Thus we can apply Theorem 5.4 with $L = K(\mathcal{E}[m])$ (and in particular with $L = \mathbb{Q}(\mathcal{E}[m])$), for every $m \geq 3$. It suffices that the local divisibility is satisfied for all nonarchimedean places v of K with norm $N_{K/\mathbb{Q}}(v) \leq |D_{L/\mathbb{Q}}|^{12577}$, to have the global one in the case when the Hasse principle for divisibility holds. Then we can take a set S as

$$\{v \in M_K \setminus \{\infty\} | h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(m, b, c)\}.$$

Moreover, as a consequence of inequality (5.4), we can restrict this set still, as in (5.3).

$$S = \{v \in M_K \setminus \{\infty\} | h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(m, b, c)\} \setminus S'.$$

Remark 5.5. Observe that when $K/\mathbb{Q}$ is a Galois extension, then $N_{K/\mathbb{Q}}(v) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(v)$ and by Proposition 3.3, the hypothesis that $h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(m,b,c)$ in Problem 1' is equal to $h(v) \leq 12577 \frac{B(m,b,c)}{[K:\mathbb{Q}]}$. In particular, when $K = \mathbb{Q}$, we have $N_{K/\mathbb{Q}}(v) = v$ and $h(v) = \log v$ and it suffices to assume that $\log v \leq 12577 \cdot B(m,b,c)$, as in Corollary 5.6.

Therefore, by the results produced about the local-global divisibility in elliptic curves over $\mathbb{Q}$ mentioned in Section 1, together with Theorem 5.4, the inequality (5.4) and Remark 5.5 the bound produced in Theorem 4.2 implies the following result.

Corollary 5.6. *Let $\mathcal{E} : y^2 = x^3 + bx + c$ be an elliptic curve defined over $\mathbb{Q}$ and let $L = \mathbb{Q}(\mathcal{E}[m])$, where $m \geq 3$ is a fixed positive integer not divisible by any power p^n, with $p \in \{2,3\}$ and $n \geq 2$. Set*

$$B(m,b,c) := \begin{cases} 5(m^2-1)^3(m^2-3)(\log m + h(b) + h(c)), & \text{if } m \geq 3 \text{ is odd;} \\ 5(m^2-4)^3(m^2-6)(\log m + h(b) + h(c)), & \text{if } m \geq 4 \text{ is even.} \end{cases}$$

Let $P \in \mathcal{E}(\mathbb{Q})$ and assume that for all nonarchimedean places $v \in \mathbb{Q}$, such that $h(v) \leq 12577 \cdot B(m,b,c)$, but at most some of them with density $\delta < \frac{1}{[L:\mathbb{Q}]}$, there exists $D_v \in \mathcal{E}(\mathbb{Q}_v)$ such that $P = mD_v$. Then there exists $D \in \mathcal{E}(\mathbb{Q})$ such that $P = mD$.

As a consequence of Theorem 4.2, together with Theorem 5.4 and the inequality (5.4), we can reformulate the statement of Problem 1 as follows.

Problem 1'. *Let K be a number field, let $\mathcal{E} : y^2 = x^3 + bx + c$ be an elliptic curve defined over K and let $L = K(\mathcal{E}[m])$, where $m \geq 3$ is a fixed positive integer. Set*

$$B(m,b,c) := \begin{cases} 5(m^2-1)^3(m^2-3)(\log m + h(b) + h(c)), & \text{if } m \geq 3 \text{ is odd;} \\ 5(m^2-4)^3(m^2-6)(\log m + h(b) + h(c)), & \text{if } m \geq 4 \text{ is even.} \end{cases}$$

Let $P \in \mathcal{E}(K)$. Assume that for all nonarchimedean places $v \in M_K$, such that $h(N_{K/\mathbb{Q}}(v)) \leq 12577 \cdot B(m,b,c)$, but at most some of them with density $\delta < \frac{1}{[L:K]}$, there exists $D_v \in \mathcal{E}(K_v)$ such that $P = mD_v$. Is it possible to conclude that there exists $D \in \mathcal{E}(K)$ such that $P = mD$?

6 An example

In this section we will produce an example of an elliptic curve in Weiestrass form

$$\mathcal{E} : y^2 = (x-\alpha)(x-\beta)(x-\gamma), \tag{6.1}$$

where $\alpha, \beta, \gamma \in \mathbb{Q}$ and $\alpha+\beta+\gamma = 0$, with a point P, locally divisible by 4 for infinitely many primes but not globally divisible by 4. Similar examples have been given in [10] and in [24] for curves such that the Hasse principle for divisibility does not work, but here we instead consider a curve for which the local-global divisibility by 4 holds and give a method to find points failing the hypotheses of the local-global principle even if they are locally divisible for infinitely many places. For what we have discussed in the previous sections, it suffices that the local divisibility holds for a finite number of places that should be distribuited with a certain density; in our example we have the local divisibility for infinitely many primes but they are not distribuited with the necessary density. In particular the density of prime numbers for which the local divisibility fails is indeed $\delta > \frac{1}{[\mathbb{Q}(\mathcal{E}[4]):\mathbb{Q}]}$ (contradicting the hypotheses of Problem 1'). We call those points pseudodivisible since they apparently satisfy the hypotheses of the local-global principle for divisibility (being locally divisible for infinitely many places), but indeed they fail them (and then they fail the local-global principle). Let G_p be the p-Sylow subgroup of the image of the representation of the Galois group $G = \mathrm{Gal}(\mathbb{Q}(K(E[4])/\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and let G_0 be the kernel of the reduction modulo 2 of the matrices in G. Let G be the subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ generated by the matrices

$$\sigma_1 = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad \sigma_4 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus

$$G = \left\langle \sigma(x,y,z,w) \,\middle|\, \mathrm{Id} + 2\begin{pmatrix} x+w & y \\ x+y+z & x+y \end{pmatrix}, \text{ with } x,y,z,w \in \mathbb{Z}/4\mathbb{Z} \right\rangle.$$

We have $\sigma_1 = \sigma(1,0,0,0), \sigma_2 = \sigma(0,1,0,0), \sigma_3 = \sigma(0,0,1,0), \sigma_4 = \sigma(0,0,0,1)$. One can easily verify that $G \simeq (\mathbb{F}_2)^4 = G_p \cap G_0$. In particular $G_0 \cap G_p$ has dimension 4 as vector space over $\mathbb{F}_2$ and then, by [9, Proposition 3.2, Case (iii)], we have that the local-global divisibility by 4 holds in $\mathcal{E}$ over $\mathbb{Q}$. Thus, by the results produced in Section 5, if the local divisibility holds for every nonarchimedean place $v \in M_{\mathbb{Q}}$ such that

$$\log v \leq 5 \cdot 12^3 \cdot 10 \cdot (\log 4 + h(\alpha\beta + \beta\gamma + \alpha\gamma) + h(\alpha\beta\gamma)),$$

but at most some of them with density $\delta < \frac{1}{16}$, then the global divisibility holds as well. Of course, for explicit nonzero integers $\alpha\beta+\beta\gamma+\alpha\gamma$ and $\alpha\beta\gamma$, such bound can be written in a more elegant form as in Remark 4.3. Let $\{Z_\sigma\}_{\sigma\in G}$ be the cocycle of G with values in $\mathcal{E}[4]$, defined by

$$Z_{\sigma(x,y,z,w)} := \begin{pmatrix} 2w \\ 0 \end{pmatrix}.$$

For $i \in \{1,2,3,4\}$ we have that Z_{σ_i} satisfies the local conditions. Anyway there are some $\sigma \in G$ such that Z_σ does not satisfy the local conditions. For instance

$$\sigma(1,0,0,1) = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}$$

and

$$(\sigma(1,0,0,1)-1)\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \neq \begin{pmatrix} 2 \\ 0 \end{pmatrix},$$

for every $(\alpha,\beta) \in \mathbb{Z}/4\mathbb{Z}$. Thus $\sigma(1,0,0,1)$ does not satisfy the local conditions and $\{\mathbb{Z}_\sigma\}_{\sigma\in G}$ does not define a class in $H^1_{\mathrm{loc}}(G,\mathcal{E}[4])$. In a similar way one can verify that $Z_{\sigma(0,1,0,1)}, Z_{\sigma(0,0,1,1)}$, and $Z_{\sigma(1,0,1,1)}$ are the only other images of the cocycle Z that do not satisfy the local conditions. In any case, since Z_{σ_i} satisfies the local conditions, for every $i \in \{1,2,3,4\}$, then we search for a point $D \in \mathcal{E}(\overline{\mathbb{Q}})$, such that $Z_{\sigma_i} = \sigma_i(D) - D$, for every $i \in \{1,2,3,4\}$. We will find a point $P = 4D$ which is locally divisible by 4 in infinitely many p-adic fields (this is assured by the validity of the local conditions for σ_i, with $i = 1,...,4$). Anyway, we expect that the local-global divisibility should fail for such a point P arising from this cocycle, even if P is locally divisible for an infinite number of primes. We will show that this is indeed the case. Notice that the density of primes for which the local divisibility fails is about $\frac{4}{16} = 0,25$, since the local conditions are not satisfied only by the following 4 images of the cocycle Z:

$$Z_{\sigma(1,0,0,1)}, Z_{\sigma(0,1,0,1)}, Z_{\sigma(0,0,1,1)} \text{ and } Z_{\sigma(1,0,1,1)}.$$

A generating set of $\mathbb{Q}(\mathcal{E}[4])$ is given by the points

$$A' = (\alpha + \sqrt{(\alpha-\beta)(\alpha-\gamma)}, (\alpha-\beta)\sqrt{\alpha-\gamma} + (\alpha-\gamma)\sqrt{\alpha-\beta}),$$

$$B' = (\beta + \sqrt{(\beta-\alpha)(\beta-\gamma)}, (\beta-\alpha)\sqrt{\beta-\gamma} + (\beta-\gamma)\sqrt{\beta-\alpha}),$$

with $2A' = A = (\alpha,0)$ and $2B' = B = (\beta,0)$ [10], [24]. To find a suitable elliptic curve $\mathcal{E}$, with $G = \langle\sigma_1,\sigma_2,\sigma_3,\sigma_4\rangle$, we require that the columns of σ_i are $\sigma_i(A')$ and $\sigma_i(B')$, for

$i = 1, ..., 4$. Thus we request $\sigma_1(A') = -A' + 2B' = B - A'$ and $\sigma_2(B') = -B'$. By a bit of calculations, one can see that $B - A' = (\alpha - \sqrt{(\alpha-\beta)(\alpha-\gamma)}, (\alpha-\beta)\sqrt{\alpha-\gamma} - (\alpha-\gamma)\sqrt{\alpha-\beta})$. We deduce

$$\begin{array}{llll} \textbf{1)} & \sigma_1(\sqrt{\alpha-\beta}) = -\sqrt{\alpha-\beta}; & \textbf{3)} & \sigma_1(\sqrt{-1}) = \sqrt{-1}; \\ \textbf{2)} & \sigma_1(\sqrt{\beta-\gamma}) = -\sqrt{\beta-\gamma}; & \textbf{4)} & \sigma_1(\sqrt{\alpha-\gamma}) = \sqrt{\alpha-\gamma}. \end{array}$$

Furthermore we should have $\sigma_2(A') = A' + 2B' = A' + B$ and $\sigma_2(B') = 2A' - B' = A - B'$. Observe that $-B = B$ and $A' + B = -(-B - A') = -(B - A') = (\alpha - \sqrt{(\alpha-\beta)(\alpha-\gamma)}, -(\alpha-\beta)\sqrt{\alpha-\gamma} + (\alpha-\gamma)\sqrt{\alpha-\beta})$. Moreover one can verify that $A - B' = (\beta - \sqrt{(\beta-\alpha)(\beta-\gamma)}, (\beta-\alpha)\sqrt{\beta-\gamma} - (\beta-\gamma)\sqrt{\beta-\alpha})$. We deduce

$$\begin{array}{llll} \textbf{5)} & \sigma_2(\sqrt{\alpha-\beta}) = \sqrt{\alpha-\beta}; & \textbf{7)} & \sigma_2(\sqrt{-1}) = -\sqrt{-1}; \\ \textbf{6)} & \sigma_2(\sqrt{\beta-\gamma}) = \sqrt{\beta-\gamma}; & \textbf{8)} & \sigma_2(\sqrt{\alpha-\gamma}) = -\sqrt{\alpha-\gamma}. \end{array}$$

Regarding σ_3, we require $\sigma_3(A') = A' + 2B' = A' + B$ and $\sigma_3(B') = B'$, i. e.

$$\begin{array}{llll} \textbf{9)} & \sigma_3(\sqrt{\alpha-\beta}) = \sqrt{\alpha-\beta}; & \textbf{11)} & \sigma_3(\sqrt{-1}) = \sqrt{-1}; \\ \textbf{10)} & \sigma_3(\sqrt{\beta-\gamma}) = \sqrt{\beta-\gamma}; & \textbf{12)} & \sigma_3(\sqrt{\alpha-\gamma}) = -\sqrt{\alpha-\gamma}. \end{array}$$

Finally we should have $\sigma_4(A') = -A'$ and $\sigma_4(B') = B'$, implying

$$\begin{array}{llll} \textbf{13)} & \sigma_4(\sqrt{\alpha-\beta}) = -\sqrt{\alpha-\beta}; & \textbf{15)} & \sigma_4(\sqrt{-1}) = -\sqrt{-1}; \\ \textbf{14)} & \sigma_4(\sqrt{\beta-\gamma}) = \sqrt{\beta-\gamma}; & \textbf{16)} & \sigma_4(\sqrt{\alpha-\gamma}) = -\sqrt{\alpha-\gamma}. \end{array}$$

Since

$$Z_{\sigma_i} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

for every $i \in \{1, 2, 3\}$, then $\sigma_i(D) = D$, for every $i \in \{1, 2, 3\}$. Thus $D \in \mathcal{E}(K_4^{\langle\sigma_1,\sigma_2,\sigma_3\rangle})$, where $K_4^{\langle\sigma_1,\sigma_2,\sigma_3\rangle}$ denotes the field fixed by $\langle\sigma_1, \sigma_2, \sigma_3\rangle$. We have

$$K_4^{\langle\sigma_1,\sigma_2,\sigma_3\rangle} = \mathbb{Q}\left(\sqrt{(\alpha-\beta)(\beta-\gamma)}\right).$$

Let $(\alpha-\beta)(\beta-\gamma) = \delta\omega^2$, with $\delta, \omega \in \mathbb{Q}$ and δ squarefree. Therefore $D = (u, v)$, with $u = u_0 + u_1\sqrt{\delta}$ and $v = v_0 + v_1\sqrt{\delta}$. By a computation showed in [10], every such point D corresponds to a point (s, t) satisfying the equation

$$\mathcal{B} : \delta s^2 = \delta^2 t^4 - 6\alpha\delta t^2 - (\beta-\gamma)^2, \tag{6.2}$$

by $u_1 = s/2$, $u_0 = (t^2\delta - \alpha)/2$ and $v = t\sqrt{\delta}(u - \alpha)$. Now we have to choose α, β, γ such that $[K_4 : \mathbb{Q}] = 16$. We set $\alpha = 9$, $\beta = 6$ and $\gamma = -15$. Then $\alpha - \beta = 3$, $\beta - \gamma = 21$,

$\alpha - \gamma = 24$ and $K_4 = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{-1}, \sqrt{7})$. Moreover $\delta = 7$. Thus the curve $\mathcal{E}$ has equation

$$y^2 = x^3 - 171x + 810$$

and (6.2) becomes

$$\mathcal{B} : s^2 = 7t^4 - 54t^2 + 63.$$

A rational point of $\mathcal{B}$ is $(s,t) = (4,1)$ (other rational points are for instance $(12,3)$ and $(204,9)$). The point $(s,t) = (4,1)$ corresponds to $D = (-1 + 2\sqrt{7}, 14 - 10\sqrt{7})$. Observe that $D^{\sigma_4} - D = (-1 - 2\sqrt{7}, 14 + 10\sqrt{7}) + (-1 + 2\sqrt{7}, -14 + 10\sqrt{7}) = A$, i.e.

$$Z_{\sigma_4} = \begin{pmatrix} 2 \\ 0 \end{pmatrix},$$

as expected. We have $P = 4D = (10, 10)$. By the software of computational algebra AXIOM (that is also implemented in SAGE), we calculated all the 4-divisor of P. The abscissas of the 4-divisors of P are the roots of the polynomial

$$\begin{aligned} \varphi_4(x) := \ & x^{16} - 160x^{15} + 6840x^{14} - 139680x^{13} + 4862268x^{12} - 134693280x^{11} \\ & + 2294454600x^{10} - 32425103520x^9 + 300976938918x^8 \\ & + 1203164578080x^7 - 68296345025400x^6 + 695993396274720x^5 \\ & - 1996085493644292x^4 - 14987477917513440x^3 + 146812808536034040x^2 \\ & - 478587272134802400x + 570463955816032161, \end{aligned}$$

which on K_4 factors as

$$\begin{aligned} & (x + 2\sqrt{7} + 1)(x - 2\sqrt{7} + 1)(x + 6\sqrt{7} - 27)(x - 6\sqrt{7} - 27) \cdot \\ & (x + 6\sqrt{-3} + 6\sqrt{3} + 12\sqrt{-1} + 3)(x - 6\sqrt{-3} - 6\sqrt{3} + 12\sqrt{-1} + 3) \cdot \\ & (x + 6\sqrt{-3} - 6\sqrt{3} - 12\sqrt{-1} + 3)(x - 6\sqrt{-3} + 6\sqrt{3} - 12\sqrt{-1} + 3) \cdot \\ & (x - 3\sqrt{-6} + 6\sqrt{-3} - 3\sqrt{2} - 3)(x + 3\sqrt{-6} - 6\sqrt{-3} - 3\sqrt{2} - 3) \cdot \\ & (x - 3\sqrt{-6} - 6\sqrt{-3} + 3\sqrt{2} - 3)(x + 3\sqrt{-6} + 6\sqrt{-3} + 3\sqrt{2} - 3) \cdot \\ & (x - 3\sqrt{42} - 6\sqrt{21} - 21\sqrt{2} - 27)(x + 3\sqrt{42} + 6\sqrt{21} - 21\sqrt{2} - 27) \cdot \\ & (x - 3\sqrt{42} + 6\sqrt{21} + 21\sqrt{2} - 27)(x + 3\sqrt{42} - 6\sqrt{21} + 21\sqrt{2} - 27) \end{aligned}$$

The 16 abscissas of the 4-divisors of P are the following:

$$\begin{array}{ll}
x_1 = -1 + 2\sqrt{7}; & x_2 = -1 - 2\sqrt{7}; \\
x_3 = 27 - 6\sqrt{7}; & x_4 = 27 + 6\sqrt{7}; \\
x_5 = -3 + 6\sqrt{-3} + 6\sqrt{3} - 12\sqrt{-1}; & x_6 = 6\sqrt{-3} - 6\sqrt{3} + 12\sqrt{-1} - 3; \\
x_7 = -3 - 6\sqrt{-3} + 6\sqrt{3} + 12\sqrt{-1}; & x_8 = -3 - 6\sqrt{-3} - 6\sqrt{3} - 12\sqrt{-1}; \\
x_9 = 3 + 3\sqrt{-6} + 6\sqrt{-3} - 3\sqrt{2}; & x_{10} = 3 + 3\sqrt{-6} - 6\sqrt{-3} + 3\sqrt{2}; \\
x_{11} = 3 - 3\sqrt{-6} + 6\sqrt{-3} + 3\sqrt{2}; & x_{12} = 3 - 3\sqrt{-6} - 6\sqrt{-3} - 3\sqrt{2}; \\
x_{13} = 27 - 3\sqrt{42} + 6\sqrt{21} - 21\sqrt{2}; & x_{14} = 27 - 3\sqrt{42} - 6\sqrt{21} + 21\sqrt{2}; \\
x_{15} = 27 + 3\sqrt{42} + 6\sqrt{21} + 21\sqrt{2}; & x_{16} = 27 + 3\sqrt{42} - 6\sqrt{21} - 21\sqrt{2};
\end{array}$$

and the ordinates corresponding to x_i, for every $1 \leq i \leq 16$ are respectively the following

$$\begin{array}{ll}
y(x_1) = \pm(14 - 10\sqrt{7}); & y(x_2) = \pm(14 + 10\sqrt{7}); \\
y(x_3) = \pm(126 - 54\sqrt{7}); & y(x_4) = \pm(126 + 54\sqrt{7}); \\
y(x_5) = \pm(72 - 6\sqrt{-3} - 42\sqrt{3}); & y(x_6) = \pm(72 - 6\sqrt{-3} + 42\sqrt{3}); \\
y(x_7) = \pm(72 + 6\sqrt{-3} - 42\sqrt{3}); & y(x_8) = \pm(72 + 6\sqrt{-3} + 42\sqrt{3}); \\
y(x_9) = \pm(36 + 27\sqrt{2} - 15\sqrt{-6} - 12\sqrt{-3}); & y(x_{10}) = \pm(36 - 27\sqrt{2} - 15\sqrt{-6} + 12\sqrt{-3}); \\
y(x_{11}) = \pm(36 - 27\sqrt{2} + 15\sqrt{-6} - 12\sqrt{-3}); & y(x_{12}) = \pm(36 + 27\sqrt{2} + 15\sqrt{-6} + 12\sqrt{-3}); \\
y(x_{13}) = \pm(252 - 39\sqrt{42} + 60\sqrt{21} - 189\sqrt{2}); & y(x_{14}) = \pm(252 - 39\sqrt{42} - 60\sqrt{21} + 189\sqrt{2}); \\
y(x_{15}) = \pm(252 + 39\sqrt{42} + 60\sqrt{21} + 189\sqrt{2}); & y(x_{16}) = \pm(252 + 39\sqrt{42} - 60\sqrt{21} - 189\sqrt{2}).
\end{array}$$

Thus

i) four among the 4-divisors of P have coordinates in $\mathbb{Q}(\sqrt{7})$;

ii) four among the 4-divisors of P have coordinates in $\mathbb{Q}(\sqrt{-1}, \sqrt{-3})$;

iii) four among the 4-divisors of P have coordinates in $\mathbb{Q}(\sqrt{-3}, \sqrt{2})$;

iv) four among the 4-divisors of P have coordinates in $\mathbb{Q}(\sqrt{2}, \sqrt{21})$.

None of the 4-divisors of P has coordinates in $\mathbb{Q}$. Thus P is not globally divisible by 4 over $\mathbb{Q}$.

Anyway, as stated above, P is divisible by 4 in $\mathbb{Q}_p$ for infinitely many prime numbers p. Just to have an idea of the distribution of primes for which the locally divisibility does not hold we will describe the situation for all $p < 1000$. To know if a 4-divisor of P has coordinates in $\mathbb{Q}_p$, for any prime number p, we can use the quadratic reciprocity law or we can factor $\varphi_4(x)$ on $\mathbb{Q}_p$, by the use of a software of computational algebra. By using the software PARI, we verified that the equation $\varphi_4(x) = 0$ has a solution in $\mathbb{Q}_p$ for the following 123 primes $p < 1000$:

3, 7, 13, 17, 19, 29, 31, 37, 41, 47, 53, 59, 61, 73, 79, 83, 89, 97, 103, 109, 113, 127, 131, 137, 139, 149, 151, 157, 167, 181, 193, 197, 199, 223, 227, 229, 233, 241, 251, 257, 271, 277, 281, 283, 307, 311, 313, 317, 337, 349, 353, 367, 373, 383, 389, 397, 401, 409, 419, 421, 433, 439, 449, 457, 463, 467, 479, 487, 503, 521, 523, 541, 557, 563, 569, 577, 587, 593, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 661, 673, 691, 701, 709, 719, 727, 733, 751, 757, 761, 769, 787, 809, 811, 821, 823, 829, 839, 853, 857, 859, 877, 881, 887, 919, 929, 937, 953, 967, 971, 977, 983, 991, 997.

In the same way we verified that instead the equation $\varphi_4(x) = 0$ has no solution in $\mathbb{Q}_p$ for the following 45 primes $p < 1000$:

2, 5, 11, 23, 43, 67, 71, 101, 107, 163, 173, 179, 191, 211, 239, 263, 269, 293, 331, 347, 359, 379, 431, 443, 461, 491, 499, 509, 547, 571, 599, 659, 677, 683, 739, 743, 773, 797, 827, 863, 883, 907, 911, 941, 947.

Notice that the density of primes $p < 1000$ for which we have no solution is $\frac{45}{168} \sim 0,26$. Even if calculated just for a finite number of primes, instead of all but finitely many primes, this density corresponds to the expected density $\frac{4}{16} = 0,25$ calculated by the number of cocycles not satisfying the local conditions and it is greater than $\frac{1}{|G|} = \frac{1}{16} = 0,0625$, which is the maximum density required by the hypotheses Problem 1'.

Acknowledgments. The idea of investigating about pseudodivisible points and giving an explicit effective version of the hypotheses of the local-global divisibility in elliptic curves over $\mathbb{Q}$ was originally conceived when Laura Paladino and Igor Shparlinski were both guests at the Max Planck Institute for Mathematics in Bonn. The authors are grateful to Igor Shparlinski for suggesting the idea of studying these topics and for useful discussions. Laura Paladino is also grateful to MPIM for the hospitality and the excellent work conditions. The authors thank Joseph H. Silverman for some suggestions about the introduction of this paper.

References

[1] J.-H. Ahn, S.-H. Kwon, *An explicit upper bound for the least prime ideal in the Chebotarev Density Theorem*, Ann. Inst. Fourier, **69** no. 3, (2019), 1411-1458.

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

[3] A. Bandini, L. Paladino, *Fields generated by torsion points of elliptic curves.*, J. Number Theory, **169** (2016), 103-133.

[4] W. D. Banks, F. Luca, I. E. Shparlinski, H. Stichtenoth, *On the value set of $n!$ modulo a prime.*, Turk. J. Math., **29** (2005), 169-174.

[5] E. Bombieri, W. Gubler, *Heights in diophantine geometry*, Cambridge University Press, Cambridge, 2006.

[6] M. Çiperiani, J. Stix, *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels*, J. Reine Angew. Math., **700** (2015), 175-207.

[7] B. Creutz, *Locally trivial torsors that are not Weil-Châtelet divisible*, Bull. London Math. Soc., **45** (2013), 935-942.

[8] B. Creutz, *On the local-global principle for divisibility in the cohomology of elliptic curves*, Math. Res. Lett., **23** no. 2 (2016), 377-387.

[9] R. Dvornicich, U. Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France, **129** (2001), 317-338.

[10] R. Dvornicich, U. Zannier, *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Acad. Sci. Paris, Ser. I **338** (2004), 47-50.

[11] R. Dvornicich, Zannier U., *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lon. Math. Soc., **39** (2007), 27-34.

[12] F. Gillibert, G. Ranieri, *On the local-global divisibility over abelian varieties*, Annales de l'Institut Fourier, **68** no. 2 (2018), 847-873.

[13] F. Gillibert, G. Ranieri, *On the local-global divisibility over* GL_2*-type varieties* https://arxiv.org/pdf/1703.06235.pdf

[14] M. Hindry, J. H. Silverman, *Diophantine geometry. An introduction*, Springer-Verlag, New York, 2000.

[15] M. Illengo, *Cohomology of integer matrices and local-global divisibility on the torus*, Le Journal de Théorie des Nombres de Bordeaux, **20** (2008), 327-334.

[16] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, New York, 1983.

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

[18] E. Gonzáles-Jiménez, F. Najman, *Growth of torsion groups of elliptic curves upon base change*, arXiv:1609.02515

[19] D. A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.

[20] B. Mazur, *Modular curves and the Eiseinstein ideal*, Publ. Math. Inst. Hautes Études Sci., **47** (1977), 33–186.

[21] L. Merel, W. Stein, *The field generated by the points of small prime order on an elliptic curve*, Int. Math. Res. Not. **20** (2001), 1075-1082.

[22] J. Neukirch, *Algebraic Number Theory*, Springer, Heidelberg, 1999.

[23] J. McKee, *Computing division polynomials*, Mathematics of Computations, **63** no. 208, (2010), 17-23.

[24] L. Paladino, *Local-global divisibility by* 4 *in elliptic curves defined over* $\mathbb{Q}$, Annali di Matematica Pura e Applicata, **189** no. 1, (1994), 767-761.

[25] L. Paladino, *Elliptic curves with* $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ *and counterexamples to local-global divisibility by 9*, Le Journal de Théorie des Nombres de Bordeaux, Vol. **22**, n. 1 (2010), 138-160.

[26] L. Paladino, *Divisibility questions in commutative algebraic groups*, 2019, Journal of Number Theory, **205** (2019), 210-245.

[27] L. Paladino, *On 5-torsion of CM elliptic curves*, Riv. Mat. Univ. Parma, **9** (2018), 329-350.

[28] L. Paladino, G. Ranieri, E. Viada, *On Local-Global Divisibility by* p^n *in elliptic curves*, Bulletin of the London Mathematical Society, **44** no. 5 (2012), 789-802.

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

[30] M. Rebolledo Hauchert, *Corps engendré par les points de 13-torsion des courbes elliptiques*, Acta Arith. **109** no.3 (2003), 219-230.

[31] H. Schmidt, *Resultants and discriminats of multiplication polynomials for elliptic curves*, J. Number Theory **149** (2015), 70-91.

[32] J.-P. Serre, *Proprietes Galoissiennes des points d'ordre fini des courbes elliptiques*, Inventiones Math. **15** (1972), 259-331.

[33] J.-P. Serre, *Quelques applications du théor 'eme de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323-401.

[34] H. M. Stark *The Coates-Wiles theorem revisited. Number theory related to Fermat's last theorem (Cambridge, Mass., 1981)*, pp. 349-362, Progr. Math., **26**, Birkhäuser, Boston, 1982.

[35] A. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum of Mathematics, Sigma **4** e4 (2016), 1-79.