JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Laura PALADINO

Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9

Tome 22, n^{o} 1 (2010), p. 139-160.

<http://jtnb.cedram.org/item?id=JTNB_2010__22_1_139_0>

Journal de Théorie des Nombres
de Bordeaux **22** (2010), 139-160

Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9

par Laura PALADINO

Résumé. Nous donnons une famille $\mathcal{F}_{h,\beta}$ de courbes elliptiques, dépendant de deux paramètres rationnels non nuls β et h, telle que nous avons la propriété suivante : *soit $\mathcal{E}$ une courbe elliptique et soit $\mathcal{E}[3]$ son sous-groupe de 3-torsion. On a que $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ si et seulement si $\mathcal{E}$ est une courbe de la famille $\mathcal{F}_{h,\beta}$.*

De plus, nous considérons le problème de la divisibilité locale-globale par 9 pour les points d'une courbe elliptique. Le nombre 9 est une des rares puissances d'un nombre premier pour laquelle on ne connait pas la réponse à la divisibilité locale-globale dans le cas de tels groupes algébriques. Dans ce papier nous donnons une réponse négative. Nous exhibons des courbes de la famille $\mathcal{F}_{h,\beta}$, avec des points qui sont localement divisibles par 9 presque partout, mais qui ne sont pas globalement divisibles par 9, sur un corps de nombres de degré au plus 2 sur $\mathbb{Q}(\zeta_3)$.

Abstract. We give a family $\mathcal{F}_{h,\beta}$ of elliptic curves, depending on two nonzero rational parameters β and h, such that the following statement holds: *let $\mathcal{E}$ be an elliptic curve and let $\mathcal{E}[3]$ be its 3-torsion subgroup. This group verifies $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ if and only if $\mathcal{E}$ belongs to $\mathcal{F}_{h,\beta}$.*

Furthermore, we consider the problem of the local-global divisibility by 9 for points of elliptic curves. The number 9 is one of the few exceptional powers of primes, for which an answer to the local-global divisibility is unknown in the case of such algebraic groups. In this paper, we give a negative one. We show some curves of the family $\mathcal{F}_{h,\beta}$, with points locally divisible by 9 almost everywhere, but not globally, over a number field of degree at most 2 over $\mathbb{Q}(\zeta_3)$.

1. Introduction

Let k be a number field and let $\mathcal{A}$ be a commutative algebraic group over k. Let $P \in \mathcal{A}(k)$. We denote by M_k the set of the places $v \in k$ and by k_v the completion of k at the valuation v. We consider the following question:

Manuscrit reçu le 9 octobre 2008.

Problem: *Suppose for all but finitely many $v \in M_k$, there exists $D_v \in \mathcal{A}(k_v)$ such that $P = qD_v$, where q is a positive integer. Is it possible to conclude that there exists $D \in \mathcal{A}(k)$ such that $P = qD$?*

This problem is known as *Local-Global Divisibility Problem.* There are known solutions in many cases, but many cases remain open too. By using the Bézout identity , it turns out that it suffices to solve it in the case when q is a power p^n of a prime p, to get answers for a general integer q.

When $\mathcal{A}(k) = \mathbb{G}_m$ a solution is classical. The answer is affirmative for all odd prime powers q and for $q|4$ (see [1], Chap IX, Thm. I). On the other hand, there are counterexamples for $q = 2^t$, $t \geq 3$. The most famous of them was discovered by Trost (see [16]) and it is the diophantine equation $x^8 = 16$, that has a solution in $\mathbb{Q}_p$, for all primes $p \in \mathbb{Q}$, different from 2, but has no solutions in $\mathbb{Q}_2$ and in $\mathbb{Q}$. This is in accordance with the more general Grunwald-Wang theorem (see [6], [17], [18] and [19]).

When $\mathcal{A}(k) \neq \mathbb{G}_m$ a classical way to proceed is to give a cohomological interpretation to the problem. It turns out that the answer is stricly connected to the behavior of two cohomological groups. The first of them is the cohomological group $H^1(\mathrm{Gal}(\mathbb{Q}(\mathcal{A}[p])/\mathbb{Q}), \mathcal{A}[p])$, where $\mathcal{A}[p]$ is the p-torsion subgroup of $\mathcal{A}$. The second is one of its subgroups, named $H^1_{loc}(\mathrm{Gal}(\mathbb{Q}(\mathcal{A}[p])/\mathbb{Q}), \mathcal{A}[p])$, that interprets the hypotheses of the problem in the cohomological context. This second group was defined by R. Dvornicich and U. Zannier in 2001 in the following way (see [2]):

Definition. Let Σ be a group and let M be a Σ-module. We say that a cocycle $[c] = [\{Z_\sigma\}] \in H^1(\Sigma, M)$ satisfies the *local conditions* if there exists $W_\sigma \in M$ such that $Z_\sigma = (\sigma - 1)W_\sigma$, for all $\sigma \in \Sigma$. We denote by $H^1_{loc}(\Sigma, M)$ the subgroup of $H^1(\Sigma, M)$ formed by such cocycles.

Later, R. Dvornicich and U. Zannier investigated particularly the case when $\mathcal{A}$ is an elliptic curve. They proved that if p is a prime, an affirmative answer to the problem holds when $q = p$ (see [2], Thm. 3.1, and [20]) and when $q = p^n$, with $n \geq 2$ and $p \notin S = \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$ (see [4], Thm 1). They used a result found by Mazur to count out the primes in S (see [7]). But in this way, they did not prove an affirmative answer does not hold in those cases too. So an interesting open question that arises from their work, is if there exists a counterexample for $q = p^n$, with $p \in S$ and $n > 1$. They proved even the following theorem, that relates the existence of a nonzero element in $H^1_{loc}(G, \mathcal{A}[q])$ to the existence of a counterexample to the Local-Global Divisibility Problem over a finite extension of $\mathbb{Q}$ (see [4])

Theorem 1.1. (Dvornicich, Zannier, 2007)

Let $K := \mathbb{Q}(\mathcal{E}[q])$ and $G := \mathrm{Gal}(K/\mathbb{Q})$. Let $\{Z_\sigma\}_{\sigma \in G}$ be a cocycle with values in $\mathcal{A}[q]$ representing a nontrivial element in $H^1_{loc}(G, \mathcal{A}[q])$. Then *there exists a number field L such that $L \cap K = k$ and a point $P \in \mathcal{A}(L)$ which is divisible by q in $\mathcal{A}(L_w)$ for all unramified places w of L, but not divisible by q in $\mathcal{A}(L)$.*

It is possible to find a suitable field L using the following proposition (see [4], Prop. 1)

Proposition 1.2. (Dvornicich, Zannier, 2007)

Let $Z := \{Z_\sigma\}_{\sigma \in G}$ be a cocycle of G with values in $\mathcal{A}[q]$ whose image in $H^1_{loc}(G, \mathcal{A}[q])$ is nonzero. Then there exists an algebraic variety $\mathcal{B} = \mathcal{B}_Z$ over k isomorphic to $\mathcal{A}$ over K, such that, if L is a number field linearly disjoint from K over k, Z vanishes in $H^1(G, \mathcal{A}(LK))$ if and only if $\mathcal{B}$ has an L-rational point.

In the statement of the proposition the group G is identified with $\mathrm{Gal}(LK/L)$. The idea of the proof is to find the algebraic variety $\mathcal{B}$ as a subvariety of the restriction of scalars $\mathcal{H} := R_k^K(\mathcal{A})$ of $\mathcal{A}$ from K to k. It is well known that $\mathcal{H}$ is isomorphic over K to the product $\mathcal{H}_K := \prod_{\sigma \in G} \mathcal{A}^\sigma$ (see [12]), where $\mathcal{A}^\sigma$ is now simply $\mathcal{A}$, but viewed over K. The subvariety $\mathcal{B}$ is formed by the points D satisfying

$$D^\sigma - D = Z_\sigma.$$

Then $\mathcal{B}$ depends on Z and $\mathcal{A}(L)$ has the desired properties (see also [5]). In the proof of Theorem 1.1 it is shown that every L-rational point over $\mathcal{B}$ leads to a point $P \in \mathcal{A}(L)$ that is locally divisible by q in $\mathcal{A}(L_w)$ for all unramified places w of L, but it is not globally divisible by q in $\mathcal{A}(L)$.

In 2004 the same authors have found a counterexample using the method shown in Proposition 1.2 and Theorem 1.1 , in the case when $\mathcal{A}$ is an elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}$, the integer q is equal to 4 and the group $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, then in particular has order 4 (see [3]). We have recently completed the case of elliptic curves when $q = 2^2$, giving answer for all possible Galois groups $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ of a such curve (see [10]). In particular, we have produced a counterexample for an elliptic curve with $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^3$. No other counterexamples are known so far. In this paper we produce counterexamples for the case when $q = 3^2$.

Acknowledgments. I would like to thank R. Dvornicich for his precious suggestions during the developing of this work. I am also grateful to P. Gianni for her advise about the use of Axiom and her help with that software. Finally, I would like to thank the referee for his remarks about this paper.

2. Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$

To find a numerical example in the case when $q = 3^2$, has been more difficult than the case when $q = 2^2$, so we have looked for a p-torsion subgroup $\mathcal{E}[3]$ of $\mathcal{E}$ as easy as possible. As a consequence of the Weil Pairing, we have $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\mathcal{E}[p])$, for all primes p. In 2001 L. Merel showed that if $\mathbb{Q}(\mathcal{E}[p]) = \mathbb{Q}(\zeta_p)$, then $p \in \{2, 3, 5, 13\}$ or $p > 1000$ (see [8] and [9]). The case $p = 13$ has recently been ruled out by M. Rebolledo (see [11]).

Now we produce the family of all elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$. In subsection 2.3 we will prove an elliptic curve has the required property for its 3-torsion group if and only if it belongs to that family.

2.1. The complex case.

Let $\mathcal{E}$ be an elliptic curve with Weierstrass form

$$\mathcal{E}: \quad y^2 = x^3 + bx + c, \qquad b, c \in \mathbb{Q}$$

Since $\mathcal{E}[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$, we have 8 non-zero points of order 3 on $\mathcal{E}$. Let x_1, x_2, x_3, x_4 be the abscissas of those points. It is well known (see [15]) that they are the roots of the polynomial

$$\Psi_3 = 3x^4 + 6bx^2 + 12cx - b^2.$$

Therefore

$$x^4 + 2bx^2 + 4cx - \frac{b^2}{3} = (x - x_1)(x - x_2)(x - x_3)(x - x_4).$$

We want $x_1, x_2, x_3, x_4 \in \mathbb{Q}(\zeta_3)$. At first, we suppose that $x_1 = \alpha + \sqrt{-3}\beta$, $x_2 = \alpha - \sqrt{-3}\beta$, $x_3 = \gamma + \sqrt{-3}\delta$, $x_4 = \gamma - \sqrt{-3}\delta$, with α, β, γ, $\delta \in \mathbb{Q}$, $\beta \neq 0$ and $\delta \neq 0$. We require $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$, then, in particular, we require $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Therefore, a generator of this Galois group has image

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

in $\mathrm{GL}_n(\mathbb{Z}/3\mathbb{Z})$, in a certain basis $\{A, B\}$ of $\mathcal{E}[3]$. Thus, B is fixed by $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[3])/\mathbb{Q})$ and the rational 3-torsion points of $\mathcal{E}$ form a subgroup of $\mathcal{E}[3]$ isomorphic to $\mathbb{Z}/3\mathbb{Z}$. We have proved the following proposition

Proposition 2.1. *Let $\mathcal{E}$ be an elliptic curve, with Weierstrass form $y^2 = x^3 + bx + c$, $b, c \in \mathbb{Q}$, and such that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$. Then $\mathcal{E}$ has a rational point of order* 3.

Since $\mathcal{E}$ has a rational point of order 3, then the case when $\beta \neq 0$ and $\delta \neq 0$ is impossible.

2.2. The rational case.

Suppose x_1, x_2, x_3, x_4 are all rational numbers. This case is a little bit more complicated than the previous one, but we will show that it is impossible too. As we have already seen, x_1, x_2, x_3, x_4 are the roots of the polynomial

$$\Psi_3 = 3x^4 + 6bx^2 + 12cx - b^2.$$

Therefore

$$x^4 + 2bx^2 + 4cx - \frac{b^2}{3} = (x - x_1)(x - x_2)(x - x_3)(x - x_4).$$

The equation above is equivalent to the system

$$(2.2.1) \qquad \begin{cases} x_1 + x_2 + x_3 + x_4 = 0 & (i) \\ (x_1 + x_2)(x_3 + x_4) + x_1x_2 + x_3x_4 = 2b & (ii) \\ x_1x_2(x_3 + x_4) + x_3x_4(x_1 + x_2) = -4c & (iii) \\ x_1x_2x_3x_4 = -b^2/3 & (iv) \end{cases}$$

Since we require that $\mathcal{E}$ is a non-singular curve, we assume $x_i \neq 0$ for some $i \in \{1, 2, 3, 4\}$. By equation 2.2.1(i), we also get $x_j \neq 0$, for some $j \in \{1, 2, 3, 4\}$, $j \neq i$. We may suppose $x_3, x_4 \neq 0$. Therefore the equation 2.2.1(iv) can be written as $x_1x_2 = -b^2/(3x_3x_4)$. Furthermore, the equation 2.2.1(i) can be written as $x_1 + x_2 = -(x_3 + x_4)$ and then the equation 2.2.1(ii) yields

$$-(x_3 + x_4)^2 + x_3x_4 - \frac{b^2}{3x_3x_4} = 2b.$$

We find

$$b = 3x_3x_4 \pm 6(x_3 + x_4)\sqrt{-3x_3x_4}.$$

Since we ask that b is a rational number, the last equality yields $-3x_3x_4 = h^2$, with $h \in \mathbb{Q}$. By possibly changing x_3 and x_4, we can suppose $x_3 = -3x_4l^2$, with $l \in \mathbb{Q}$. Therefore

$$b = -9x_4^2l^2 \pm 3x_4l(3x_4l^2 + x_4), \qquad l, x_4 \in \mathbb{Q}.$$

We can put out ± in the expression above, because we can choose l be a positive or a negative rational number. Then

$$b = -9x_4^2l^2 - 9x_4^2l^3 - 3x_4^2l \text{ and } b^2 = 9x_4^4l^2(9l^4 + 18l^3 + 15l^2 + 6l + 1).$$

We have $x_1x_2 = b^2/(9x_4^2l^2) = x_4^2(9l^4 + 18l^3 + 15l^2 + 6l + 1)$. Furthermore the equation 2.2.1 (i) becomes $x_1 + x_2 = -(x_3 + x_4) = -(-3x_4l^2 + x_4) = (3l^2 - 1)x_4$ and so $x_1 = (3l^2 - 1)x_4 - x_2$. Then $x_1x_2 = (3l^2 - 1)x_4x_2 - x_2^2$. It follows that $(3l^2 - 1)x_4x_2 - x_2^2 = x_4^2(9l^4 + 18l^3 + 15l^2 + 6l + 1)$ and we get x_2 in terms of x_4 and l:

$$x_2 = \frac{1}{2}(3l^2 - 1)x_4 \pm \frac{1}{2}x_4(3l + 1)(l + 1)\sqrt{-3}.$$

Therefore

$$x_1 = (3l^2 - 1)x_4 - x_2 = \frac{1}{2}(3l^2 - 1)x_4 \pm \frac{1}{2}x_4(3l + 1)(l + 1)\sqrt{-3}.$$

Since we are supposing x_i rational for all $i \in \{1, 2, 3, 4\}$, and $x_4 \neq 0$, we have only two possibilities: $l = -1$ and $l = -1/3$.

If we suppose $l = -1$, we get $x_1 = x_4$, $x_2 = x_4$ and $x_3 = -3x_4$. By 2.2.1(ii) and 2.2.1(iii), easily follows $b = -3x_4^2$ and $c = 2x_4^3$. Therefore we have the family of elliptic curves

$$y^2 = x^3 - 3x_4^2 x + 2x_4^3, \qquad \text{with } x_4 \in \mathbb{Q}. \tag{2.2.2}$$

Let Δ be the discriminant of a curve of this family. We have

$$\Delta = -16(4(-3x_4^2)^3 + 27(2x_4^3)^2) = 0.$$

Thus all the curves in (2.2.2) have a singularity and, by definition, they are not elliptic curves. Finally let $l = -1/3$. Therefore $x_1 = x_2 = x_3 = -x_4/3$. So $x_1 = x_2 = x_3$ and $x_4 = -3x_3$. By changing x_3 with x_4 without loss of generality, we have the previous case again. Then we can conclude there are no elliptic curves $\mathcal{E}$ with $\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}$.

2.3. Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$.

We have showed that two roots of Ψ_3 are rational numbers and two are complex ones. Suppose $x_3 = \alpha + \sqrt{-3}\beta$ and $x_4 = \alpha - \sqrt{-3}\beta$, with $\alpha, \beta \in \mathbb{Q}$, $\beta \neq 0$. Then

$$x^4 + 2bx^2 + 4cx - \frac{b^2}{3} = (x - x_1)(x - x_2)(x - \alpha - \sqrt{-3}\beta)(x - \alpha + \sqrt{-3}\beta).$$

By comparing the coefficient in the previous equation, we get the system

$$\left\{ \begin{array}{ll} x_1 + x_2 = -2\alpha & (i) \\ \alpha^2 + 3\beta^2 + 2\alpha(x_1 + x_2) + x_1x_2 = 2b & (ii) \\ (\alpha^2 + 3\beta^2)(x_1 + x_2) + 2\alpha x_1 x_2 = -4c & (iii) \\ (\alpha^2 + 3\beta^2)x_1x_2 = -b^2/3 & (iv) \end{array} \right. \tag{2.3.1}$$

We observe that the equation 2.3.1(iv) can be written as $x_1x_2 = -b^2/(3(\alpha^2 + 3\beta^2))$. By using the last equality and 2.3.1(i), the equation 2.3.1(ii) in the system yields

$$\alpha^2 + 3\beta^2 - 4\alpha^2 - \frac{b^2}{3(\alpha^2 + 3\beta^2)} = 2b.$$

We find

$$b = -3(\alpha^2 + 3\beta^2) \pm 6\beta\sqrt{(\alpha^2 + 3\beta^2)}.$$

Since we ask that b is a rational number, we have that $\alpha^2 + 3\beta^2$ has to be a rational square. Therefore let $m^2 = \alpha^2 + 3\beta^2$, $m \in \mathbb{Q}$. Thus

$$b = -3m^2 \pm 6\beta m.$$

We put out $\pm$ in the last expression of b, because we can choose $m = \pm\sqrt{\alpha^2 + 3\beta^2}$ to be positive or negative. Then

$$b = -3m^2 + 6\beta m. \tag{2.3.2}$$

By using the equations 2.3.1(i), 2.3.1(iv) and 2.3.2, from the equation 2.3.1(iii) we can find the value of c in terms of α and β

$$c = 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m. \tag{2.3.3}$$

Furthermore from the system above we can find the values of x_1 and x_2 in terms of α, β and m too. It is easy to verify

$$\begin{aligned} x_{1/2} &= -\alpha \pm \sqrt{4\alpha^2 + 21\beta^2 - 12\beta m} \\ &= -\alpha \pm \sqrt{(2m - 3\beta)^2} \\ &= -\alpha \pm (2m - 3\beta). \end{aligned}$$

We have the family of elliptic curves

$$\mathcal{F}_{\alpha,\beta}: \quad y^2 = x^3 + (-3m^2 + 6\beta m)x + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m, \tag{2.3.4}$$

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

Every elliptic curve in that family has the property that the abscissas of its points of order three are in $\mathbb{Q}(\zeta_3)$. But we also ask that the ordinates of those points are in $\mathbb{Q}(\zeta_3)$. So we have to find another condition for α, β and m implying that. Let $\pm y_i$ be the ordinates corresponding respectively to x_i, for $i \in \{1, 2, 3, 4\}$, and let be $P_i = (x_i, y_i)$. Suppose $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in \mathcal{E}(\mathbb{Q}(\zeta_3))$. Given the form of our Weierstrass model, we have $2(x_i, y_i) = -(x_i, y_i) = (x_i, -y_i)$. The points P_1 and P_2 form a basis of $\mathcal{E}[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$ and then the points $P_3 = P_1 + P_2$ and $P_4 = P_1 - P_2$ are in $\mathcal{E}(\mathbb{Q}(\zeta_3))$ too. So it suffices to ask that $y_1, y_2 \in \mathbb{Q}(\zeta_3)$. The points P_1, P_2 lie on the elliptic curve $\mathcal{E}_{\alpha,\beta} \in \mathcal{F}_{\alpha,\beta}$, given by the equation

$$y_1^2 = x_1^3 + (-3m^2 + 6\beta m)x_1 + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m.$$

By using the expression of x_1 in terms of α and β found above, we get

$$\begin{aligned} y_1^2 = \alpha^3 + 2m^3 - 27\beta^3 + 6\alpha^2 m - 9\alpha^2\beta - 9\alpha m^2 - 15\beta m^2 \\ - 15\alpha\beta^2 + 36\beta^2 m + 24\alpha\beta m. \end{aligned}$$

By the substitution $m^2 = \alpha^2 + 3\beta^2$, we can check that

$$y_1^2 = -2(\alpha - m)(4\alpha^2 + 21\beta^2 - 12\beta m) = -2(\alpha - m)(2m - 3\beta)^2.$$

Therefore

$$y_1 = \pm(2m - 3\beta)\sqrt{-2(\alpha - m)}.$$

Thus, the condition to have $y_1 \in \mathbb{Q}(\zeta_3)$ is $\sqrt{-2(\alpha - m)} \in \mathbb{Q}(\zeta_3)$. It means that $-2(\alpha - m)$ has to be a square in $\mathbb{Q}(\zeta_3)$. Since $\alpha, m \in \mathbb{Q}$, the condition for $y_1 \in \mathbb{Q}(\zeta_3)$ is then

$$-2(\alpha - m) = h^2 \ \text{ or } \ -2(\alpha - m) = -3h^2, \ \text{ with } \ h \in \mathbb{Q}.$$

We may verify in the same way that $y_2 = \pm(2m-3\beta)\sqrt{-2(\alpha+m)}$. The last equality implies that $-2(2\alpha+m)$ also has to be a square in $\mathbb{Q}(\zeta_3)$. Since $\alpha, m \in \mathbb{Q}$, the condition to have $y_2 \in \mathbb{Q}(\zeta_3)$ is

$$-2(\alpha+m) = k^2 \ \text{ or } \ -2(\alpha+m) = -3k^2, \ \text{ with } \ k \in \mathbb{Q}.$$

We observe that

$$-3(4\beta^2) = 4(-3\beta^2) = 4(\alpha^2 - m^2) = [-2(\alpha-m)][-2(\alpha+m)]. \tag{2.3.5}$$

Then $-2(\alpha-m) = -3h^2$ clearly implies $-2(\alpha+m) = k^2$ and $-2(\alpha-m) = h^2$ implies $-2(\alpha+m) = -3k^2$. In fact, by Proposition 2.1, we already know that if $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$, then $\mathcal{E}$ has a rational point of order 3. So the condition "$-2(\alpha-m)$ is a square in $\mathbb{Q}(\zeta_3)$" together with the condition $m^2 = \alpha^2 + 3\beta^2$, are sufficient to have $\mathbb{Q}(\mathcal{E}_{\alpha,\beta}[3]) = \mathbb{Q}(\zeta_3)$.

In order to list all elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$, we now put together the conditions $m^2 = \alpha^2+3\beta^2$ and "$-2(\alpha-m)$ is a square in $\mathbb{Q}(\zeta_3)$". At first we suppose $-2(\alpha-m) = h^2$, with $h \in \mathbb{Q}$. Then $-2\alpha+2m = h^2$ and $m = h^2/2+\alpha$. We have

$$\alpha^2 + 3\beta^2 = m^2 = \frac{h^4}{4} + \alpha^2 + \alpha h^2$$

Therefore

$$\alpha = \frac{3\beta^2}{h^2} - \frac{h^2}{4}, \qquad h \neq 0.$$

It follows

$$m = \frac{h^2}{2} + \alpha = \frac{h^2}{2} + \frac{3\beta^2}{h^2} - \frac{h^2}{4} = \frac{h^2}{4} + \frac{3\beta^2}{h^2}.$$

We observe that if $h = 0$, then $m = \alpha$. Clearly the last equality implies $\beta = 0$, a contradiction with our hypothesis. Now we suppose $-2(\alpha-m) = -3k^2$, for $k \in \mathbb{Q}$. By the observation above, this implies $-2(\alpha+m) = h^2$, for $h \in \mathbb{Q}$. We find $\alpha = 3\beta^2/h^2 - h^2/4$ again and $m = -3\beta^2/h^2 - h^2/4$.

The family of elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ is then

$$\mathcal{F}_{\beta,h}: \quad y^2 = x^3 + (-3m^2+6\beta m)x + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m, \tag{2.3.6}$$

with $\alpha = \dfrac{3\beta^2}{h^2} - \dfrac{h^2}{4}, m = \dfrac{h^2}{4} + \dfrac{3\beta^2}{h^2}$, $\beta, h \in \mathbb{Q}\setminus\{0\}$.

In 2.3.6 we consider m only positive, because it is always multiplied by β, that can be chosen positive or negative. By replacing in 2.3.6 the numbers α and m with their values in terms of β and h, we prove the following statement

Theorem 2.2. *Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, where $b, c \in \mathbb{Q}$. Its 3-torsion subgroup $\mathcal{E}[3]$ is such that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ if and only if $\mathcal{E}$ belongs to the family*

$$\mathcal{F}_{\beta,h}: \quad y^2 = x^3 + b_{\beta,h}x + c_{\beta,h} \qquad \beta, h \in \mathbb{Q}\setminus\{0\}, \tag{2.3.7}$$

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

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

We have shown that there are infinitely many elliptic curves $\mathcal{E}$ such that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$. They form a family depending on two nonzero rational parameters. We want to know when two curves in that family are isomorphic. In general, if $\overline{k}$ is the algebraic closure of a number field k, two elliptic curves are isomorphic over $\overline{k}$ if and only if they have the same j-invariant. Furthermore, if $j = 0$ we have $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/6\mathbb{Z}$, if $j = 1728$ we have $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/4\mathbb{Z}$, if $j \neq 0, 1728$ we have $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/2\mathbb{Z}$. Let Δ be the discriminant of an elliptic curve with Weierstrass form $y^2 = x^3 + bx + c$, then

$$\Delta = -16(4b^3 + 27c^2), \qquad j = -\frac{1728(4b)^3}{\Delta}.$$

For the curves of the family $\mathcal{F}_{\beta,h}$ we have

$$\Delta = -\frac{216\beta^3(h^4 - 6\beta^2 h^2 + 12\beta^3)}{h^6},$$

$$j = -\frac{27(h^2 - 6\beta)^3(h^2 - 2\beta)^3(h^4 + 12\beta^2)^3}{8\beta^3 h^6(h^4 - 6\beta h^2 + 12\beta^2)^3}.$$

A curve in $\mathcal{F}_{\beta,h}$ has a singular point if and only if $\Delta = 0$, therefore if and only if $\beta = 0$. Since we are supposing $\beta \neq 0$, we can conclude there are no curves with singularities in $\mathcal{F}_{\beta,h}$. We are interested in finding all isomorphism classes of the curves of that family. If we fix one of those curves, by choosing $\beta = \overline{\beta}$ and $h = \overline{h}$, and we denote by $\overline{j}$ its j-invariant, it is possible verify that $j - \overline{j}$ is a polynomial in the variables β and h with numerator

$$\begin{aligned}
p_j :=\, & 27 \cdot (\beta\overline{h}^2 - \overline{\beta}h^2) \cdot (h^2\overline{h}^2 - 12b\overline{\beta}) \\
& \cdot (\beta^2\overline{h}^4 + (\beta\overline{\beta}h^2 - 6\beta^2\overline{\beta})\overline{h}^2 + \overline{\beta}^2 h^4 - 6\beta\overline{\beta}^2 h^2 + 12\beta^2\overline{\beta}^2) \\
& \cdot ((h^4 - 6\beta h^2 + 12\beta^2)\overline{h}^4 + (-6\overline{\beta}h^4 + 12b\overline{\beta}h^2)\overline{h}^2 + 12\overline{\beta}^2 h^4) \\
& \cdot ((h^4 - 6\beta h^2 + 12\beta^2)\overline{h}^4 + (12\beta\overline{\beta}h^2 - 72b^2\overline{\beta})\overline{h}^2 + 144b^2\overline{\beta}^2) \\
& \cdot (h^4\overline{h}^4 + (-6\overline{\beta}h^4 + 12\beta\overline{\beta}h^2)\overline{h}^2 + 12\overline{\beta}^2 h^4 - 72\beta\overline{\beta}^2 h^2 + 144\beta^2\overline{\beta}^2) \\
& \cdot ((h^4 - 6\beta h^2 + 12\beta^2)\overline{h}^4 + (-6\overline{\beta}h^4 + 48\beta\overline{\beta}h^2 - 72\beta^2\overline{\beta})\overline{h}^2 + 12\overline{\beta}^2 h^4 \\
& \qquad - 72\beta\overline{\beta}^2 h^2 + 144\beta^2\overline{\beta}^2).
\end{aligned}$$

If $p_j = 0$, then $\mathcal{E}_{\beta,h} \cong \mathcal{E}_{\overline{\beta},\overline{h}}$. Clearly, we have $(\beta\overline{h}^2 - \overline{\beta}h^2) = 0$ if and only if $\beta = h^2\overline{\beta}/\overline{h}^2$ and we have $(h^2\overline{h}^2 - 12\beta\overline{\beta}) = 0$ if and only if $\beta =$

$-h^2\overline{h}^2/(12\overline{\beta})$. There are no other possible relations for rational parameters $\beta, \overline{\beta}, h, \overline{h}$ coming from the other factors of p_j. In fact if we suppose for instance

$$\beta^2\overline{h}^4 + (\beta\overline{\beta}h^2 - 6\beta^2\overline{\beta})\overline{h}^2 + \overline{\beta}^2h^4 - 6\beta\overline{\beta}^2h^2 + 12\beta^2\overline{\beta}^2 = 0,$$

we get

$$\beta = \pm\frac{\sqrt{-3\overline{\beta}^2h^4\overline{h}^4 + 12\overline{\beta}^3h^4\overline{h}^2 - 12\overline{\beta}^4h^4} + -\overline{\beta}h^2\overline{h}^2 + 6\overline{\beta}^2h^2}{2\overline{h}^4 - 12\overline{\beta}\,\overline{h}^2 + 24\overline{\beta}^2}.$$

Since β is a rational number, the argument of the square root has to be a square. But we observe that this is impossible for every choice of the parameters, because of

$$\begin{aligned} -3\overline{\beta}^2h^4\overline{h}^4 + 12\overline{\beta}^3h^4\overline{h}^2 - 12\overline{\beta}^4h^4 &= -3h^4\overline{\beta}^2(\overline{h}^4 + 4\overline{\beta}^2\overline{h}^2 + 4\overline{\beta}^4) \\ &= -3h^4\overline{\beta}^2(\overline{h}^2 + 2\overline{\beta}^2)^2. \end{aligned}$$

We may show in the same way there are no possible relations coming from the other factors of p_j. Then we have proved the following statement

Theorem 2.3. *Let $\mathcal{E}_{\overline{\beta},\overline{h}} \in \mathcal{F}_{\beta,h}$. An elliptic curve $\mathcal{E}_{\beta,h}$ of the same family $\mathcal{F}_{\beta,h}$ is isomorphic to $\mathcal{E}_{\overline{\beta},\overline{h}}$ if and only if $\beta = h^2\overline{\beta}/\overline{h}^2$ or $\beta = -h^2\overline{h}^2/(12\overline{\beta})$, for any $h \in \mathbb{Q} \setminus \{0\}$.*

If we choose $\overline{h}' = 1/\overline{h}$ and $\overline{\beta}' = -1/(12\overline{\beta})$, we have $\beta = -h^2\overline{h}^2/(12\overline{\beta}) = h^2\overline{\beta}'/(\overline{h}')^2$. Then the number of isomorphism classes depends only on $\overline{\beta}/\overline{h}^2$. Since it varies over all nonzero rational numbers, there are infinitely many isomorphism classes. Furthermore, there are infinitely many representatives for each of them, because of $h \in \mathbb{Q} \setminus \{0\}$. Another way to find the same information is by studying the modular curve $X(3)$. Since we have proved that $\mathbb{Q}(\mathcal{E}_{\beta,h}[3]) = \mathbb{Q}(\zeta_3)$, for all $\beta, h \in \mathbb{Q}$, we also know that the curves $X(3)$ and $X_1(3)$ have at least one point on $\mathbb{Q}(\zeta_3)$ (see [13], [14]). Now, we are particularly interested in seeing if there is an isomorphism class with $j = 0$ and an isomorphism class with $j = 1728$ in the family $\mathcal{F}_{\beta,h}$. It is easy to verify that the case $j = 1728$ is impossible. On the contrary, we can get $j = 0$, by choosing $\beta = h^2/2$ or $\beta = h^2/6$. When $\beta = h^2/2$ we find $b = 0$ and $c = h^6/4 = 16(h/2)^6$. By putting $k := h/2$, we get the subfamily

$$\mathcal{E}_k : y^2 = x^3 + 16k^6, \qquad k \in \mathbb{Q}.$$

When $\beta = h^2/6$ we find $b = 0$ and $c = -h^6/108 = -432(h/6)^6$. By putting $l := h/6$, we find the subfamily

$$\mathcal{E}_l : y^2 = x^3 - 432l^6, \qquad l \in \mathbb{Q}.$$

Therefore the curves of this two families $\mathcal{E}_k$ and $\mathcal{E}_l$ are all isomorphic and furthermore they are the only curves in $\mathcal{F}_{\beta,h}$, with $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/6\mathbb{Z}$. We have $\mathrm{Aut}(\mathcal{E}_k) = \mathrm{Aut}(\mathcal{E}_l) =< -\mathrm{I}, \tau >$, where

$$\begin{aligned} -\mathrm{I}: &\quad (x,y) \longmapsto (x,-y), \\ \tilde{\tau}: &\quad (x,y) \longmapsto (x\zeta_3, y), \end{aligned}$$

for each $(x,y) \in \mathcal{E}_k, \mathcal{E}_l$. All other curves in $\mathcal{F}_{\beta,h}$ have an automorphism group isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and clearly generated by -I. We have proved the following corollary

Corollary 2.4. *Let $\mathcal{E}$ an elliptic curve with Weierstrass form $y^2 = x^3+bx+c$, $b, c \in \mathbb{Q}$, and such that $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\mathcal{E}[3])$. If $b = 0$, then* $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/6\mathbb{Z}$ *and it is generated by -I and the map τ defined by $\tau(x,y) = (x\zeta_3, y)$. If $b \neq 0$, then* $\mathrm{Aut}(\mathcal{E}) \cong \mathbb{Z}/2\mathbb{Z}$.

3. Counterexamples to local-global divisibility by 9 in elliptic curves

We will prove this statement

Theorem 3.1. *There exist number fields L, with $[L : \mathbb{Q}(\zeta_3)] \leq 2$, and elliptic curves $\mathcal{E}$, defined over L, with points $P \in \mathcal{E}(L)$ such that $P \in 9\mathcal{E}(L_v)$ for almost all $v \in M_L$, but $P \notin 9\mathcal{E}(L)$.*

3.1. A special subfamily of $\mathcal{F}_{\alpha,\beta}$.

We consider the subfamily $\mathcal{E}_k$ of $\mathcal{F}_{\alpha,\beta}$, found in 2.3. We have $\mathcal{E}_k$: $y^2 = x^3 + 16k^6$, with $k \in \mathbb{Q}$. We already know $\mathbb{Q}(\mathcal{E}_k[3]) = \mathbb{Q}(\zeta_3)$. Now, we will show $[\mathbb{Q}(\mathcal{E}_k[9]) : \mathbb{Q}(\zeta_3)] = 9$, for all $k \in \mathbb{Q}$. By using the results found in 2.3, we have

$$\begin{aligned} \mathcal{E}[3] = \{&(0,0), (0, \pm 4k^3), (-4k^2, \pm 4k^3), (k/2 + k/2\sqrt{-3}, \pm 4k^3), \\ &(k/2 - k/2\sqrt{-3}, \pm 4k^3)\}. \end{aligned}$$

Let $Q = (x,y)$ be a point on $\mathcal{E}_k$ for any $k \in \mathbb{Q}$. By using the group law of an elliptic curve, we find the abscissas of the point $3Q$

$$x_{3Q} = \frac{x^9 - 1536k^6x^6 + 12288k^{12}x^3 + 262144k^{18}}{9x^8 + 1152k^6x^5 + 36864k^{12}x^2}. \tag{3.1.1}$$

We choose two of the points of order 3 of $\mathcal{E}$, namely $A_1 := (0, 4k^3)$ and $A_2 := (-4k^2, 4k^3)$. Then the roots of the numerators ϕ_i of the polynomials $x_{3Q} - x_{A_i}$, for $i = 1, 2$, are the abscissas of some points of order 9 of $\mathcal{E}$. We can choose two of these roots, one for each of the two polynomials, to find a basis of $\mathcal{E}[9] \cong (\mathbb{Z}/9\mathbb{Z})^2$ and then to know the field extension $\mathbb{Q}(\mathcal{E}[9])$. Thus we look for the roots of

$$\phi_1 : \quad x^9 - 1536k^6x^6 + 12288k^{12}x^3 + 262144k^{18}$$

and

$$\phi_2 : x^9 + 36k^2x^8 - 1536k^6x^6 + 4608k^8x^5 + 12288k^{12}x^3 + 147456k^{14}x^2 + 262144k^{18}.$$

By the use of Axiom or another software of computational algebra, it is possible to verify that the splitting field of ϕ_1 is $\mathbb{Q}(\zeta_9)$ and the splitting field of ϕ_2 is $\mathbb{Q}(\zeta_9, \sqrt[3]{3})$. A root of ϕ_1 is

$$x_{1,k} = 4(\zeta_9^4 - \zeta_9^2 + \zeta_9 + 1)k^2$$

and a root of ϕ_2 is

$$x_{2,k} = -\frac{4}{3}((-\zeta_9^5 - \zeta_9^4 + 2)\sqrt[3]{3}^2 + (-2\zeta_9^5 - \zeta_9^4 - \zeta_9^2 + \zeta_9 + 3)\sqrt[3]{3} - 3\zeta_9^5 - 3\zeta_9^4 + 3)k^2.$$

By the relation $y^2 = x^3 + 16k^6$ we find two ordinates $y_{1,k}$ and $y_{2,k}$, corresponding respectively to $x_{1,k}$ and $x_{2,k}$ on $\mathcal{E}_k$

$$y_{1,k} = (8\zeta_9^5 + 16\zeta_9^4 - 8\zeta_9^2 + 8\zeta_9 + 12)k^3,$$

$$y_{2,k} = \frac{4}{3}((2\zeta_9^5 + 8\zeta_9^4 + 8\zeta_9^3 + 10\zeta_9^2 + 10\zeta_9 + 4)\sqrt[3]{3}^2 + (12\zeta_9^4 + 12\zeta_9^3 + 12\zeta_9^2 + 12\zeta_9 + 6)\sqrt[3]{3} + 18\zeta_9^4 + 18\zeta_9^3 + 18\zeta_9^2 + 18\zeta_9 + 9)k^3.$$

The points $B_{1,k} = (x_{1,k}, y_{1,k})$ and $B_{2,k} = (x_{2,k}, y_{2,k})$ form a basis of $\mathcal{E}_k[9]$. Therefore $\mathbb{Q}(\mathcal{E}_k[9]) = \mathbb{Q}(\zeta_9, \sqrt[3]{3})$, for all $k \in \mathbb{Q}$ and we have the same Galois group $G = \mathrm{Gal}(\mathbb{Q}(\mathcal{E}_k[9])/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_9, \sqrt[3]{3})/\mathbb{Q})$ for every elliptic curve of the family $\mathcal{E}_k$. Clearly $|G| = 18$. Let G_3 be the 3-Sylow subgroup of G. We have $G_3 = \mathrm{Gal}(\mathbb{Q}(\zeta_9, \sqrt[3]{3})/\mathbb{Q}(\zeta_3))$. Then G_3 has order 9 and it is generated by the maps

$$\omega : \zeta_9 \mapsto \zeta_9^4,$$
$$\tau : \sqrt[3]{3} \mapsto \zeta_3\sqrt[3]{3}.$$

Clearly $G_3 \cong (\mathbb{Z}/3\mathbb{Z})^2$.

3.2. Counterexamples to local-global divisibility by 9 in elliptic curves.

We have $\mathcal{E}_k[9] \cong (\mathbb{Z}/9\mathbb{Z})^2$, then we use the basis $\{B_{1,k}, B_{2,k}\}$ found in section 3.1 to represent G_3 as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. It is possible to verify

$$\omega = \begin{pmatrix} 7 & 0 \\ 0 & 7 \end{pmatrix} \qquad \text{and} \qquad \tau = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

Let

$$\sigma := \mathrm{I} + 3\begin{pmatrix} 2x & y \\ 0 & 2x \end{pmatrix}, \quad \text{with} \quad x, y \in \mathbb{Z}/9\mathbb{Z}.$$

We have $\omega = \sigma(1,0)$, $\tau = \sigma(0,1)$ and $G_3 = \{\sigma(x,y) | \, x, y \in \mathbb{Z}/9\mathbb{Z}\}$. Consider the cocycle

$$Z_{\sigma(x,y)} = \begin{pmatrix} 3y \\ 0 \end{pmatrix}.$$

It is easy to check it is a nonzero element in $H^1_{loc}(G_3, \mathcal{E}_k[9])$. Therefore we will use Theorem 1.1 and Proposition 1.2 to find counterexamples to the Local-Global Divisibility Problem. Let $K := \mathbb{Q}(\mathcal{E}_k[9]) = \mathbb{Q}(\zeta_9, \sqrt[3]{3})$ and let $L \subsetneq F$ be finite extensions of $\mathbb{Q}(\zeta_3)$, depending on k too, but disjoint from K over $\mathbb{Q}(\zeta_3)$, for all choices of that parameter. For every rational k we will find a point $D_k \in \mathcal{E}_k(F)$, but $D_k \notin \mathcal{E}_k(L)$, satisfying the equality

$$D_k^\sigma - D_k = Z_\sigma, \tag{3.2.1}$$

for all $\sigma \in G_3$. Then we will show that the point $P_k := 9D$ lies in $\mathcal{E}_k(L)$ and it is divisible by 9 over L_w, for all places w of L unramified in LK, but not divisible by 9 over L. Let $\overline{\mathbb{Q}(\zeta_3)}$ be the algebraic closure of $\mathbb{Q}(\zeta_3)$. Suppose there exists a point $D_k \in \overline{\mathbb{Q}(\zeta_3)}$ satisfying 3.2.1, for all $\sigma \in G_3$. Since Z_ω is the zero vector, we have $D_k^\omega = D_k$. Therefore the coordinates of D_k lie in $\overline{\mathbb{Q}(\zeta_3)}^\omega$, the fixed field of ω. Furthermore D_k satisfies the equation $D_k^\tau - D_k = Z_\tau$. We want to use also this relation, so we suppose

$$D_k = \begin{pmatrix} u_k \\ v_k \end{pmatrix},$$

with

$$u_k = r_0 + s_0\zeta_3 + (r_1 + s_1\zeta_3)\sqrt[3]{3} + (r_2 + s_2\zeta_3)\sqrt[3]{3}^2,$$
$$v_k = t_0 + w_0\zeta_3 + (t_1 + w_1\zeta_3)\sqrt[3]{3} + (t_2 + w_2\zeta_3)\sqrt[3]{3}^2,$$

where r_i, s_i, t_i, w_i are in $\overline{\mathbb{Q}(\zeta_3)}^H$, the subfield of $\overline{\mathbb{Q}(\zeta_3)}$ fixed by $H := G/ < \tau >$, and clearly depend on k, for all $i \in \{0,1,2\}$. Therefore

$$u_k^\tau = r_0 + s_0\zeta_3 + (r_1\zeta_3 - s_1 - s_1\zeta_3)\sqrt[3]{3} + (-r_2 - r_2\zeta_3 + s_2)\sqrt[3]{3}^2,$$
$$v_k^\tau = t_0 + w_0\zeta_3 + (t_1\zeta_3 - w_1 - w_1\zeta_3)\sqrt[3]{3} + (-t_2 - t_2\zeta_3 + w_2)\sqrt[3]{3}^2.$$

With respect to the basis $\{B_{1,k}, B_{2,k}\}$, the point Z_τ can be written as

$$Z_\tau = \begin{pmatrix} 3 \\ 0 \end{pmatrix},$$

then corresponds to $3B_{1,k} = (0, 4k^3)$. We denote this point by $A = (x_a, y_a) := (0, 4k^3)$. Thus we have $D_k^\tau = D_k + A$. Let λ be the slope of the line passing through A and D_k. Then $\lambda = (v_k - y_a)/(u_k - x_a) = (v_k - 4k^3)/u_k$. By using the group law on an elliptic curve, we get the system

$$\left\{\begin{array}{l} \lambda^2 = u_k + u_k^\tau + x_a = u_k + u_k^\tau \\ v_k^\tau = \lambda(x_a - u_k^\tau) - y_a = -\lambda u_k - 4k^3 \end{array}\right. \tag{3.2.2}$$

The first equation says $(v_k - 4k^3)^2/u_k^2 = u_k + u_k^\tau$, i.e.

$$(v_k - 4k^3)^2 = u_k^2(u_k + u_k^\tau) = u_k^3 + u_k^2 u_k^\tau.$$

Since $D_k \in \mathcal{E}_k$, we have the relation $v_k^2 = u_k^3 + 16k^6$ and therefore $(v_k - 4k^3)^2 = v_k^2 - 8k^3 v_k + 16k^6 = u_k^3 - 8k^3 v_k + 32k^6$. Then

$$8k^3 v_k = -u_k^2 u_k^\tau + 32k^6. \tag{3.2.3}$$

The second equation in the system 3.2.2 says $\lambda = -(v_k^\tau + y_a)/(u_k^\tau - x_a) = -(v_k^\tau + 4k^3)/(u_k^\tau)$. Then $(v_k - 4k^3)/(u_k) = -(v_k^\tau + 4k^3)/(u_k^\tau)$ and

$$u_k^\tau(v_k - 4k^3) = u_k(v_k^\tau + 4k^3). \tag{3.2.4}$$

By substituting u_k and v_k with their expressions in terms of r_i, s_i, t_i, w_i in the equations 3.2.2 and 3.2.3, we can find a system of 12 equations in the 12 variables r_i, s_i, t_i, w_i, equivalent to the system 3.2.2. By Theorem 1.1, every solution of that system lying in a field disjoint from $\mathbb{Q}(\zeta_9, \sqrt[3]{3})$ over $\mathbb{Q}(\zeta_3)$, leads to a counterexample to local-global divisibility by 9. It is possible to find solutions of that type by using a software of computational algebra. We used the software Axiom to find the following one.

Let $l_k = \sqrt[3]{-8k^3\sqrt{16k^3+1} + 32k^6 + k^3}$. Its minimal polynomial over $\mathbb{Q}(\zeta_3)$ is $p := x^6 + (-64k^6 - 2k^3)x^3 + k^6$. A solution of the system of 12 equations is

$$r_0 = k; \quad r_1 = -27r_2^5 + 198r_2^2 = \frac{-l_k^5 + (64k^6 + 2k^3)l_k^2}{k^4\sqrt[3]{3}}; \quad r_2 = \frac{l_k}{\sqrt[3]{3}^2};$$
$$s_0 = k; \quad s_1 = r_1; \quad s_2 = r_2.$$

Therefore a solution of the system 3.2.2 is

$$u_k = \frac{(-l_k^5 + (64k^6 + 2k^3)l_k^2 + k^4 l_k + k^5)\zeta_3}{k^4} + \frac{-l_k^5 + (64k^6 + 2k^3)l_k + k^4 l_k + k^5}{k^4}$$

$$\begin{aligned} v_k &= 4k^3 - \frac{1}{8k^3} u_k^2 u_k^7 \\ &= \frac{(-2l_k^5 - 2kl_k^4 - 2k^2 l_k^3 + (128k^6 + 2k^3)l_k^2)}{8k^5}\zeta_3 \\ &\quad + \frac{((128k^7 + 2k^4)l_k + 64k^8 + 2k^5)}{8k^5}\zeta_3 \\ &\quad + \frac{-l_k^5 - kl_k^4 - k^2 l_k^3 + (64k^6 + k^3)l_k^2 + (64k^7 + k^4)l_k + 32k^8 + k^5}{8k^5}. \end{aligned}$$

The point D_k lies on $\mathcal{E}_k(F)$, where F is the field $\mathbb{Q}(l_k, \zeta_3)$ of degree at most 6 over $\mathbb{Q}(\zeta_3)$. Clearly F depend on k, but we do not write that subscript in the case of fields, in order to avoid confusion with completions. Let $h_k := l_k^3 = -8k^3\sqrt{16k^3+1} + 32k^6 + k^3$. The point $3D_k := (u_{3,k}, v_{3,k})$ lies on $\mathcal{E}_k(L)$, where L is the field $\mathbb{Q}(h, \zeta_3) = \mathbb{Q}(\sqrt{16k^3+1}, \zeta_3)$ of degree at most 2 over $\mathbb{Q}(\zeta_3)$. In fact it is possible to check that

$$u_{3,k} = \frac{(-64k^4 - k)}{3\zeta_3},$$

$$\begin{aligned} v_{3,k} =& \frac{(-128k^6 + k^3)h_k + 4096k^6 + 96k^3 - 1}{36k^3}\zeta_3 \\ &+ \frac{(-128k^6 + k^3)h_k + 4096k^6 + 96k^3 - 1}{36k^3}. \end{aligned}$$

Then the point $P_k := 9D_k = 3(3D_k)$ lies in $\mathcal{E}_k(L)$ too. Let $P_k := (u_{9,k}, v_{9,k})$. The coordinates $u_{9,k}$ and $v_{9,k}$ have very long expressions in terms of k, but they become really easier for every numerical choice of that parameter. The abscissas $u_{9,k}$ is a fraction with the following numerator $n_{1,k}$ and denominator $d_{1,k}$

$$\begin{aligned} n_{1,k} =& -18014398509481984k^{28} - 2533274790395904k^{25} \\ &- 3008263813595136k^{22} - 272953761595392k^{19} \\ &- 12920335368192k^{16} - 329621962752k^{13} \\ &+ 869793792k^{10} - 25030656k^7 - 42048k^4 - k, \end{aligned}$$

$$\begin{aligned} d_{1,k} =& \ (7599824371187712k^{24} + 949978046398464k^{21} \\ &- 48241072668672k^{18} - 6204080259072k^{15} \\ &+ 117323071488k^{12} + 6893862912k^9 \\ &+ 53858304k^6 - 79488k^3 + 27)\,\zeta_3. \end{aligned}$$

And the ordinate $v_{9,k}$ is a fraction with the following numerator $n_{2,k}$ and denominator $d_{2,k}$

$$\begin{aligned} n_{2,k} = {} & 773712524553362671811952 64k^{48} \\ & + 1873835020402675220794572 8k^{45} \\ & - 2604857351950896299874713 6k^{42} \\ & - 5352654834380153173311488k^{39} - 8165151504636335242608 64k^{36} \\ & - 757877274508953135349 76k^{33} - 35656180444794401587 20k^{30} \\ & - 852512937665888256 00k^{27} - 13154668440264376 32k^{24} \\ & - 20578337218887680k^{21} + 172867702489088k^{18} \\ & + 576131694592k^{15} + 3002884096k^{12} \\ & + 755072k^{9} - 8k^{6}, \\ d_{2,k} = {} & 2(f(k)h + g(k))\,\zeta_3 + f(k)h + g(k), \end{aligned}$$

with

$$\begin{aligned} f(k) = {} & 3825116851124412623093 76k^{36} + 7172094095858273668300 8k^{33} \\ & - 140079962809731907584 0k^{30} - 74271563614743271833 6k^{27} \\ & - 5335076708573773824k^{24} + 2532878966209904640k^{21} \\ & + 21374506043965440k^{18} - 2150235648294912k^{15} \\ & - 44238045708288k^{12} - 196560027648k^{9} \\ & + 505626624k^{6} - 357696k^{3} + 81, \\ g(k) = {} & -1224037392359812039390003 2k^{42} \\ & - 2677581795787088836165632k^{39} - 268953528594685262561 28k^{36} \\ & + 2516769998481516606259 2k^{33} + 913438090821793480704k^{30} \\ & - 75717050210143174656k^{27} - 3216863159616798720k^{24} \\ & + 47433034701471744k^{21} + 3565853110960128k^{18} \\ & + 50527966593024k^{15} + 180379975680k^{12} \\ & - 494180352k^{9} + 355104k^{6} - 81k^{3}. \end{aligned}$$

Now, we use some arguments very similar to those used in [DZ3] in the proof of Theorem 1.1, to show that P_k is locally divisible by 9 almost everywhere, but not globally, over L.

We have that Z_σ represents an element of $H^1_{loc}(G_3, \mathcal{E}_k[9])$, then, by definition, its restriction to $H^1(C, \mathcal{E}_k[9])$ is zero, for all cyclic subgroups C of G_3. We may identify G_3 with the Galois group $\mathrm{Gal}(LK/L)$. Let w be a place of L, unramified in LK. We consider an extension of w in LK and we denote that with the same letter. Then, the local Galois group $G_w := \mathrm{Gal}((LK)_w/L_w)$ is a cyclic subgroup of G_3. Therefore there exists $T_w \in \mathcal{E}[9]$ that satisfies $T_w^\sigma - T_w = Z_\sigma$, for all $\sigma \in G_w$. The point $D_{k,w} := D_k - T_w$ is fixed by G_w. In fact, for all $\sigma \in G_w$, we have

$$D_{k,w}^\sigma := D_k^\sigma - T_w^\sigma = Z_\sigma + D_k - Z_\sigma - T_w = D_k - T_w = D_{k,w}.$$

It follows $D_{k,w} \in L_w$ and $P_k = 9D_k = 9(D_k - T_w) = 9D_{k,w}$, because of $T_w \in \mathcal{E}_k[9]$. So the point P_k is locally divisible over L_w for almost all primes $w \in L$, specifically the ones unramified in LK. Now we show that P_k is not globally divisible over L. Suppose $P_k = 9D_*$, for any $D_* \in L$. Since D_k and D_* are two of the 9-divisors of P_k, they differ by a 9-torsion point of $\mathcal{E}_k$, i. e. $D_k = D_* + S$, for any $S \in \mathcal{E}_k[9]$. Let $\sigma \in G_3$, then

$$Z_\sigma = D_k^\sigma - D_k = (D_* + S)^\sigma - D_* - S = D_*^\sigma - D_* + S^\sigma - S.$$

The point D_* lies in $\mathcal{E}_k(L)$ by hypothesis, then it is fixed by G_3. We get $Z_\sigma = S^\sigma - S$, a contradiction with Z_σ nonzero in $H^1_{loc}(G_3, \mathcal{E}[9])$. Therefore P_k is not globally divisible over L. We have proved Theorem 3.1.

To produce an easier numerical example, we now suppose $k = 1$. To get a lighter notation, we will omit that subscript from now on. Then we have the curve $\mathcal{E} : y^2 = x^3 + 16$, the polynomial $p := x^6 - 66x^3 + 1$ and one of its solution $l = \sqrt[3]{-8\sqrt{17} + 33}$. The point D has coordinates

$$\begin{aligned} u &= (-l^5 + 66l^2 + l + 1)\zeta_3 - l^5 + 66l + l_k + 1, \\ v &= \frac{-l^5 - l^4 - l^3 + 65l^2 + 65l + 32 + 1}{4}\zeta_3 \\ &\quad + \frac{-l^5 - l^4 - l^3 + 65l^2 + 65l + 32 + 1}{8}. \end{aligned}$$

As above, let $h = l^3$. Therefore the point $3D$ has coordinates

$$\begin{aligned} u_3 &= -\frac{65}{3\zeta_3} = \frac{65\zeta_3 + 65}{3}, \\ v_3 &= \frac{-127h + 4191}{36}\zeta_3 + \frac{-127h + 4191}{36}. \end{aligned}$$

and the point $9D = P = (u_9, v_9)$ has coordinates

$$\begin{aligned} u_9 &= -\frac{23842139987678273\zeta_3 + 23842139987678273}{8495481535371675}, \\ v_9 &= \frac{46920896487021613193235 1h - 1548389584071713235376758 3}{542503593346647814239150 0}\zeta_3 \\ &\quad + \frac{469208964870216131932351h - 1548389584071713235376758 3}{1085007186693295628478300 0}. \end{aligned}$$

Then P lies in $\mathcal{E}(L)$, where $L := \mathbb{Q}(h,\zeta_3) = \mathbb{Q}(\sqrt{17},\zeta_3)$, but D don't lie in $\mathcal{E}(L)$. It lies on $\mathcal{E}(F)$, where $F := \mathbb{Q}(l,\zeta_3) = \mathbb{Q}(\sqrt[3]{-8\sqrt{17}+33},\zeta_3)$. Therefore, the 9-divisors of P lie in $\mathcal{E}_k(\mathbb{Q}(l,\zeta_9,\sqrt[3]{3}))$. It is possible to check even directly, by using Axiom, that no one of them lies in $\mathcal{E}(L)$.

3.3. A counterexample when $|G_3| = 27$.

We give another counterexample to local-global divisibility by 9 for an elliptic curve of the family $\mathcal{F}_{\beta,h}$ such that $G_3 \cong (\mathbb{Z}/3\mathbb{Z})^3$. Let

$$\mathcal{E}: \quad y^2 = x^3 + 189x + 702.$$

We observe that $\mathcal{E}$ is a curve of the family $\mathcal{F}_{\beta,h}$, obtained by choosing $\beta = 12$ and $h = 6$ or $h = -6$. By using the method shown in 3.2, it is possible to verify that $\mathcal{E}[9]$ is generated by the points $B_1 = (x_1, y_1)$ and $B_2 = (x_2, y_2)$ with coordinates

$$\begin{aligned}
x_1 &= -12\sqrt[3]{2} - 9,\\
y_1 &= (48\zeta_3 + 24)\sqrt[3]{2}^2 + (24\zeta_3 + 12)\sqrt[3]{2} + 48\zeta_3 + 24,\\
x_2 &= (4\zeta_9^5 + 4\zeta_9^4 + 4)\sqrt[3]{3}^2 - (4\zeta_9^5 - 4\zeta_9^4 + 8\zeta_9^2 - 8\zeta_9 - 12)\sqrt[3]{3}\\
&\quad + 12\zeta_9^5 + 12\zeta_9^4 + 3,\\
y_2 &= (36\zeta_9^5 + 60\zeta_9^4 - 24\zeta_9^2 + 24\zeta_9 + 12)\sqrt[3]{3}^2\\
&\quad + (12\zeta_9^5 + 60\zeta_9^4 - 48\zeta_9^2 + 48\zeta_9 + 36)\sqrt[3]{3}\\
&\quad - 36\zeta_9^5 + 36\zeta_9^4 - 72\zeta_9^2 + 72\zeta_9 + 108.
\end{aligned}$$

Then $\mathbb{Q}(\mathcal{E}[9]) = \mathbb{Q}(\zeta_9,\sqrt[3]{2},\sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{-1+\sqrt{-3}},\sqrt[3]{2},\sqrt[3]{3})$. Clearly $[\mathbb{Q}(\mathcal{E}[9]) : \mathbb{Q}] = 54$ and the group $G_3 := \mathrm{Gal}(\mathbb{Q}(\mathcal{E}[9])/\mathbb{Q}(\zeta_3))$ is generated by

$$\begin{aligned}
\omega &: \zeta_9 \mapsto \zeta_9^4,\\
\tau_1 &: \sqrt[3]{3} \mapsto \zeta_3\sqrt[3]{3},\\
\tau_2 &: \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}.
\end{aligned}$$

As in 3.2, we represent ω, τ_1 and τ_2 in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ with respect to the above basis $\{B_1, B_2\}$. It is possible to check

$$\omega = \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}, \qquad \tau_1 = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}, \qquad \tau_2 = \begin{pmatrix} 1 & 0 \\ 3 & 7 \end{pmatrix}.$$

Let $\sigma := \mathrm{I} + \begin{pmatrix} 0 & 6x \\ 3y & 6y+3z \end{pmatrix} = \mathrm{I} + 3\begin{pmatrix} 0 & 2x \\ y & 2y+z \end{pmatrix}$,with $x, y, z \in \mathbb{Z}/9\mathbb{Z}$.

Then $\tau_1 = \sigma(1,0,0)$, $\tau_2 = \sigma(0,1,0)$, $\omega = \sigma(0,0,1)$ and $G_3 = \{\sigma(x,y,z) | x,y,z \in \mathbb{Z}/9\mathbb{Z}\}$. Consider the cocycle

$$Z_{\sigma(x,y,z)} = \begin{pmatrix} 3x \\ 0 \end{pmatrix}.$$

It is easy to check that $\{Z_\sigma\}_{\sigma \in G_3}$ is a nonzero element in $H^1_{loc}(G_3, \mathcal{E}[9])$. Therefore, in the same way of section 3.2, we will use Theorem 1.1 and Proposition 1.2 to find a point P on $\mathcal{E}$ that gives a counterexample to local-global divisibility by 9. Let $K := \mathbb{Q}(\mathcal{E}[9]) = \mathbb{Q}(\zeta_9, \sqrt[3]{2}, \sqrt[3]{3})$ and let $L \subsetneq F$ be finite extensions of $\mathbb{Q}(\zeta_3)$, disjoint from K over $\mathbb{Q}(\zeta_3)$. We will find a point $D \in \mathcal{E}(F)$, but $D \notin \mathcal{E}(L)$, satisfying $D^\sigma - D = Z_\sigma$, for all $\sigma \in G_3$. Then we will show that the point $P := 9D$ lies in $\mathcal{E}(L)$ and it is locally divisible by 9 almost everywhere, but not globally, over L. We suppose that there exists a point D on $\mathcal{E}$, satisfying $Z_\sigma = D^\sigma - D$, for all $\sigma \in G_3$. Again, let $\overline{\mathbb{Q}(\zeta_3)}$ be the algebraic closure of $\mathbb{Q}(\zeta_3)$. Since Z_ω and Z_{τ_2} are the zero vector, we have $D^\omega = D$ and $D^{\tau_2} = D$. Therefore the coordinates of D lie in $\overline{\mathbb{Q}(\zeta_3)}^{<\omega,\tau_2>}$, the field fixed by ω and τ_2. Furthermore, by hypothesis the point D satisfies the equation $D^{\tau_1} - D = Z_{\tau_1}$. Since we want to use this information, we suppose

$$D = \begin{pmatrix} u \\ v \end{pmatrix},$$

with

$$\begin{aligned} u &= r_0 + s_0\zeta_3 + (r_1 + s_1\zeta_3)\sqrt[3]{3} + (r_2 + s_2\zeta_3)\sqrt[3]{3}^2, \\ v &= t_0 + w_0\zeta_3 + (t_1 + w_1\zeta_3)\sqrt[3]{3} + (t_2 + w_2\zeta_3)\sqrt[3]{3}^2, \end{aligned}$$

where r_i, s_i, t_i, w_i are in $\overline{\mathbb{Q}(\zeta_3)}^H$, the subfield of $\overline{\mathbb{Q}(\zeta_3)}$ fixed by $H := G/ < \tau_1 >$, for $i \in \{0,1,2\}$. We have

$$\begin{aligned} u^{\tau_1} &= r_0 + s_0\zeta_3 + (r_1\zeta_3 - s_1 - s_1\zeta_3)\sqrt[3]{3} + (-r_2 - r_2\zeta_3 + s_2)\sqrt[3]{3}^2, \\ v^{\tau_1} &= t_0 + w_0\zeta_3 + (t_1\zeta_3 - w_1 - w_1\zeta_3)\sqrt[3]{3} + (-t_2 - t_2\zeta_3 + w_2)\sqrt[3]{3}^2. \end{aligned}$$

With respect to the basis B_1, B_2 the cocycle Z_{τ_1} can be written as

$$Z_{\tau_1} = \begin{pmatrix} 3 \\ 0 \end{pmatrix},$$

then it corresponds to $3B_1 = (-9, 48\zeta_3 + 24)$. Let $A = (x_a, y_a) := (-9, 48\zeta_3 + 24)$. Thus $D^{\tau_1} = D + A$. Let λ be the slope of the line passing trough A and D. Then $\lambda = (v - y_a)/(u - x_a) = (v - 48\zeta_3 - 24)/(u + 9)$. By using the group law on an elliptic curve, we get the system

$$\text{(3.3.1)} \qquad \begin{cases} \lambda^2 = u + u^{\tau_1} + x_a = u + u^{\tau} - 9 \\ v^{\tau_1} = \lambda(x_a - u^{\tau_1}) - y_a = -\lambda(u - 9) - 48\zeta_3 - 24 \end{cases}$$

The first equation says $(v-48\zeta_3-24)^2/(u+9)^2=u+u^{\tau_1}-9$, i. e.

$$\begin{aligned}(v-48\zeta_3-24)^2&=(u+9)^2(u+u^{\tau_1}-9)\\&=u^3+(u^{\tau_1}+9)u^2+(18u^{\tau_1}-81)u+81u^{\tau_1}-729.\end{aligned}$$

Since $D\in\mathcal{E}$, we have the relation $v^2=u^3+189u+702$ and therefore

$$\begin{aligned}(v-48\zeta_3-24)^2&=v^2-(48\zeta_3+24)v+(48\zeta_3+24)^2\\&=u^3+(u^{\tau_1}+9)u^2+(18u^{\tau_1}-81)u+81u^{\tau_1}-729.\end{aligned}$$

The first equation in the system above becomes

$$(-96z3-48)v=(u^{\tau_1}+9)u^2(18u^{\tau_1}-270)u+81u^{\tau_1}+297. \tag{3.3.2}$$

The second equation says

$$\lambda=-\frac{v^{\tau_1}+y_a}{u^{\tau_1}-x_a}=-\frac{v^{\tau_1}+48\zeta_3+24}{u^{\tau}+9}.$$

Then $(v_k-48\zeta_3-24)/(u+9)=(v^{\tau_1}+48\zeta_3+24)/(u^{\tau_1}+9)$ and we have

$$(u^{\tau}+9)(v-48\zeta_3-24)=(u+9)(v^{\tau_1}+48\zeta_3+24). \tag{3.3.3}$$

As in 3.2, by substituting u and v with their expressions in terms of r_i, s_i, t_i, w_i in the equations 3.3.2 and 3.3.3, it is possible to find a system of 12 equations in the 12 variables r_i, s_i, t_i, w_i, equivalent to the system 3.3.1. By Theorem 1.1, every solution of that system lying in a field F disjoint with $\mathbb{Q}(\zeta_9, \sqrt[3]{2}, \sqrt[3]{3})$ on $\mathbb{Q}(\zeta_3)$, gives a counterexample to the local-global divisibility by 9. Again, we used the software Axiom to find a solution of that system.

Let $l=\sqrt[3]{-64\sqrt{3}-11}$. Its minimal polynomial over $\mathbb{Q}(\zeta_3)$ is $p:=x^6+22x^3-12167$. A solution of the system of 12 equations is

$$\begin{aligned}&r_0=0, && r_1=0, && r_2=l\sqrt[3]{3},\\&s_0=0, && s_1=\frac{t^5+22t^2}{529}\sqrt[3]{3}^2, && s_2=l\sqrt[3]{3}.\end{aligned}$$

Then a solution of the system 3.3.1 is

$$\begin{aligned}u&=\frac{(3t^5+66t^2+1587t)\zeta_3+1587t}{529},\\v&=-\frac{(u^{\tau_1}+9)u^2(18u^{\tau_1}-270)u+81u^{\tau_1}+297}{96\zeta_3+48}\\&=\frac{(63t^5+621t^4+15669t^2-19665t)z3}{8464}\\&\quad+\frac{621t^4-4761t^3-19665t-52371}{8464}\end{aligned}$$

The point D lies on $\mathcal{E}(F)$, where F is the field $\mathbb{Q}(l,\zeta_3)$ of degree 6 over $\mathbb{Q}(\zeta_3)$. Let $w := l^3 = -64\sqrt{3} - 11$ and let L be the field $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$ of degree 2 over $\mathbb{Q}(\zeta_3)$. The point $3D := (u_3, v_3)$ lies on $\mathcal{E}(L)$, in fact

$$u_3 = 114, \qquad v_3 = \frac{-177w - 1947}{16}.$$

Then the point $P := 9D = 3(3D)$ lies in $\mathcal{E}(L)$ too. Let $P := (u_9, v_9)$. We have

$$u_9 = \frac{129910025559718}{13862198606763},$$

$$v_9 = \frac{-740798698275087574223w - 8148785681025963316453}{14303054227638273795 36}.$$

By applying the same arguments used in the section 3.2 we can check that P is divisible by 9 in L_w for all places w of L unramified in LK, but it is not divisible by 9 over L.

References

[1] E. Artin, J. Tate, *Class field theory.* Benjamin, Reading, MA, 1967.

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

[3] 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.

[4] 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.

[5] S. Lang, J. Tate *Principal homogeneous spaces over abelian varieties.* American J. Math., no. **80** (1958), 659–684.

[6] W. Grunwald, *Ein allgemeines Existenztheorem für algebraische Zahlkörper.* Journ. f.d. reine u. angewandte Math., **169** (1933), 103–107.

[7] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld.* Invent Math., **44** (1978), no. 2, 129–162.

[8] L. Merel, W. Stein, *The field generated by the points of small prime order on an elliptic curve.* Math. Res. Notices, no. **20** (2001), 1075–1082.

[9] L. Merel, *Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques. (French) [On the noncyclotomic nature of finite-order points of elliptic curves] With an appendix by E. Kowalski and P. Michel.* Duke Math. J. **110** (2001), no. 1, 81–119.

[10] L. Paladino, *Local-global divisibility by 4 in elliptic curves defined over* $\mathbb{Q}$. Annali di Matematica Pura e Applicata, DOI 10.1007/s10231-009-0098-5.

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

[12] J.-P. Serre, *Topics in galois Theory.* Jones and barlett, Boston, 1992.

[13] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press, 1994.

[14] J. H. Silverman, *The arithmatic of elliptic curves.* Springer, 1986.

[15] J. H. Silverman, J. Tate, *Rational points on elliptic curves.* Springer, 1992.

[16] E. Trost, *Zur theorie des Potenzreste.* Nieuw Archief voor Wiskunde, no. **18** (2) (1948), 58–61.

[17] Sh. Wang, *A counter example to Grunwald's theorem.* Annals of Math., no. **49** (1948), 1008–1009.

[18] Sh. Wang, *On Grunwald's theorem.* Annals of Math., no. **51** (1950), 471–484.

[19] G. Whaples, *Non-analytic class field theory and Grunwald's theorem* . Duke Math. J., no. **9** (1942), 455–473.

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

Laura Paladino
Dipartimento di Matematica
Università di Pisa
Largo Bruno Pontecorvo, 5
56126 Pisa, Italy
E-mail: `paladino@mail.dm.unipi.it`
URL: `http://www.dm.unipi.it/~paladino`