

Local-global divisibility by 4 in elliptic curves defined over $\mathbb{Q}$

Laura Paladino

Abstract

In 2004 R. Dvornicich and U. Zannier produced an elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}$ and a rational point $P \in \mathcal{E}(\mathbb{Q})$ with this characteristics: $\mathcal{E}$ has a Galois group $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, where $\mathcal{E}[4]$ is the 4-torsion subgroup of $\mathcal{E}$, and P is divisible by 4 in $\mathcal{E}(\mathbb{Q}_v)$, for almost all rational places v , but not divisible by 4 in $\mathcal{E}(\mathbb{Q})$. This is an analogue of the Grunwald-Wang example over $\mathbb{G}_m$. There were no other known counterexamples to the local-global divisibility in the case of elliptic curves so far. In this paper we will complete the case when $q = 2^2$ for such algebraic groups, giving answer for all possible Galois groups $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$. In particular, we produce a counterexample for an elliptic curve with $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^3$.

1 Introduction

Let k be a number field and $\mathcal{A}$ 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:

PROBLEM: *Assume that 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 is sufficient 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 [AT], 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 [Tro]) 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 [Gru], [Wan], [Wan2] and [Wha]).

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 strictly connected to the behavior of two cohomological groups. The first of them is the cohomological group $H^1(\text{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p])$, where $\mathcal{A}[p]$ is the p -torsion subgroup of $\mathcal{A}$. The second is one of its subgroups, named $H_{loc}^1(\text{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[p])$, that

interprets the hypothesis of the problem in the cohomological context. This last group was defined in 2001 by R. Dvornicich and U. Zannier (see [DZ])

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 $H_{loc}^1(\Sigma, M)$ 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 and they proved that if p is a prime, an affirmative answer to the problem holds when $q = p$ (see [DZ], Thm 3.1, and [Won]) 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 [DZ3], Thm 1). They used a result found by Mazur to count out the primes in S (see [Maz]). 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 also proved the following theorem, that relates the existence of a nonzero element in $H_{loc}^1(\text{Gal}(k(\mathcal{A}[p])/k), \mathcal{A}[q])$ to the existence of a counterexample to the Local-Global Divisibility Problem over a finite extension of $\mathbb{Q}$ (see [DZ3])

Proposition 1. (Dvornicich, Zannier, 2007)

Let $K := k(\mathcal{A}[q])$ and let $G := \text{Gal}(k(\mathcal{A}[p])/k)$. Let $\{Z_\sigma\}_{\sigma \in G}$ be a cocycle of G representing a nontrivial element in $H_{loc}^1(G, \mathcal{A}[q])$. 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 is not divisible by q in $\mathcal{A}(L)$.

It is possible to find a suitable field L using the following proposition (see [DZ3], Prop. 1)

Proposition 2. (Dvornicich, Zannier, 2007)

Let $\{Z_\sigma\}_{\sigma \in G}$ be a cocycle whose image in $H_{loc}^1(G, \mathcal{A}[q])$ 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 $\text{Gal}(LK/L)$. 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 [Ser]), 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 it is possible to verify that has the desired properties. Every L -rational point over $\mathcal{B}$ leads to a point $P \in \mathcal{A}(L)$ that is locally divisible for all unramified primes of L , but not globally divisible.

In 2004 they found a counterexample, by applying this method, in the case when $q = 2^2$. They produced an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ with a Galois group $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$, then in particular of order 4, and a point $P \in$

$\mathcal{E}(\mathbb{Q})$ locally divisible by 4 almost everywhere over the p -adic numbers, but not divisible by 4 over $\mathbb{Q}$ (see [DZ2]). There were no other known counterexamples so far. Now, we will complete the case when $q = 2^2$ for elliptic curves defined over $\mathbb{Q}$, giving answer for all possible Galois groups $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$. In particular, we produce a counterexample for an elliptic curve with $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^3$.

Acknowledgments. I would like to thank R. Dvornicich for his precious suggestions during the developing of this work. I'm also grateful to A. Bandini for his remarks about the preliminarily version of this paper.

2 The case when $q = 2^2$ for elliptic curves

We will prove the following statement

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

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

where $\alpha, \beta, \gamma \in \mathbb{Q}$, $\alpha \neq \beta \neq \gamma$ and $\alpha + \beta + \gamma = 0$. Let G be the Galois group $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$. Then $G \cong (\mathbb{Z}/2\mathbb{Z})^n$, with $n \in \{1, 2, 3, 4\}$. We have:

- i) for every elliptic curve $\mathcal{E}$ such that $G \cong (\mathbb{Z}/2\mathbb{Z})^n$, with $n \in \{1, 4\}$, the Local-Global Divisibility Problem when $q = 2^2$ has an affirmative answer for all $P \in \mathcal{E}(\mathbb{Q})$,
- ii) for every $n \in \{2, 3\}$ there exist elliptic curves $\mathcal{E}$ with $G \cong (\mathbb{Z}/2\mathbb{Z})^n$ and points $P \in \mathcal{E}(\mathbb{Q})$, such that $P \in 4\mathcal{E}(\mathbb{Q}_v)$ for almost all $v \in M_{\mathbb{Q}}$, but $P \notin 4\mathcal{E}(\mathbb{Q})$.

2.1 Proof of the Main Theorem

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

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

where $\alpha, \beta, \gamma \in \mathbb{Q}$, $\alpha \neq \beta \neq \gamma$ and $\alpha + \beta + \gamma = 0$.

It is possible to verify that

$$\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha - \beta}, \sqrt{\beta - \gamma}, \sqrt{\gamma - \alpha})$$

(see [DZ2]).

Therefore $G \cong (\mathbb{Z}/2\mathbb{Z})^n$, with $n = 1, 2, 3, 4$.

i) Since $H_{loc}^1(G, \mathcal{E}[4]) = 0$ when G is cyclic, the Local-Global Divisibility Problem has an affirmative answer for $n = 1$ (see [DZ], Prop 2.1). Let $n = 4$. In this case we have $G \cong (\mathbb{Z}/2\mathbb{Z})^4$. Since $\mathcal{E}[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$, we may identify G with a subgroup of $\text{GL}_2(\mathbb{Z}/4\mathbb{Z})$. We have supposed that the parameters α, β and γ are

rational numbers, then the points of order two of $\mathcal{E}$ are fixed by all automorphism of G . Therefore, every automorphism of G has to be the identity modulo 2. Let G_0 be the kernel of the restriction map

$$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}),$$

and let $H := G \cap G_0$. Clearly we have $H = G$. Then the dimension of H as $\mathbb{F}_2$ -vector space is 4. By Proposition 3.2 (iii) of [DZ3], the local-global divisibility by 4 holds for all points $P \in \mathcal{E}$.

ii) Now, we suppose $n \in \{2, 3\}$. Because of the cited Dvornicich-Zannier example, we have to find counterexamples only when $n = 3$.

A counterexample when $|G| = 8$

We suppose $G \cong (\mathbb{Z}/2\mathbb{Z})^3$. Since $\mathcal{E}[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$, we identify G with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. Consider the group

$$G = \langle \sigma_1, \sigma_2, \sigma_3 \rangle \quad \text{with} \quad \sigma_1 = \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix}.$$

$$\text{Let} \quad \sigma(x, y, z) := I + 2 \begin{pmatrix} x+y+z & y+z \\ x+z & x+z \end{pmatrix}, \quad \text{with} \quad x, y, z \in \mathbb{Z}/4\mathbb{Z}.$$

Then $\sigma_1 = \sigma(1, 0, 0)$, $\sigma_2 = \sigma(0, 1, 0)$, $\sigma_3 = \sigma(0, 0, 1)$ and $G_3 = \{\sigma(x, y, z) | x, y, z \in \mathbb{Z}/4\mathbb{Z}\}$. Let $\{Z_\sigma\}_{\sigma \in G}$ be the cocycle defined by

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

With a quick calculation it is possible to verify that $\{Z_\sigma\}_{\sigma \in G}$ is a nonzero element in $H_{loc}^1(G, \mathcal{E}[4])$. By Proposition 1, there exists a counterexample over a finite extension of $\mathbb{Q}$. We will produce a counterexample over $\mathbb{Q}$. We want to find a point $D \in \mathcal{E}$, satisfying $Z_\sigma = D^\sigma - D$, for all $\sigma \in G$. Since

$$Z_{\sigma_1} = Z_{\sigma_3} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

we obtain $D = D^{\sigma_1}$ and $D = D^{\sigma_3}$. Then the coordinates of D lie in the subfield of $\mathbb{Q}(\mathcal{E}[4])$ fixed by σ_1 and σ_3 . We denote this field by K_0 . Clearly $[K_0 : \mathbb{Q}] = 2$ and $\mathrm{Gal}(K_0/\mathbb{Q}) \cong G / \langle \sigma_1, \sigma_3 \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Let $K_0 = \mathbb{Q}(\sqrt{\delta})$ and let $D = (u, v) = (u_0 + u_1\sqrt{\delta}, v_0 + v_1\sqrt{\delta})$. Furthermore we have

$$Z_{\sigma_2} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Thus $2Z_{\sigma_2} = 0$ and D^{σ_2} differs from D by a 2-torsion point. Let $A := (\alpha, 0)$, and suppose $D^{\sigma_2} = D + A$. By using a calculation showed in [DZ2], based on the group law of an elliptic curve, from the last equality we get the curve

$$\delta s^2 = \delta^2 t^4 - 6\alpha\delta t^2 + (\beta - \gamma)^2, \quad (*)$$

with $s = 2u_1$ and $t\sqrt{\delta} = \frac{v}{u-\alpha}$.

Now we have to require that $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ corresponds to the group G defined above. By using a basis $A', B' \in \mathcal{E}[4]$, we may represent $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ as a subgroup of $\text{GL}_2(\mathbb{Z}/4\mathbb{Z})$. We choose A', B' such that $A' = 2A$ and $B' = 2B$, where $B = (\beta, 0)$. Specifically, for some given determinations of the square roots, it is possible to verify

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

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

(see [DZ2]).

By calculating the images of this basis under the generators σ_1, σ_2 and σ_3 of G , it is possible to check that $\text{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q}) \cong G$ if and only if $\gamma - \alpha$ is a (nonzero) rational square and $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha - \beta}, \sqrt{\beta - \gamma})$ has degree 8 over $\mathbb{Q}$. Furthermore, by using the same calculation of the images of A' and B' under σ_1, σ_2 and σ_3 , it is possible to verify that $K_0 = \mathbb{Q}(\sqrt{-1})$. So we have $\delta = -1$ and the curve $(*)$, in our case become the (s, t) -plane curve

$$-s^2 = t^4 + 6\alpha t^2 + (\beta - \gamma)^2. \quad (**)$$

By Theorem 1 and Proposition 2, every rational point of that curve leads to a counterexample to the local-global divisibility by 4 over $\mathbb{Q}$.

A numerical example

Let $\alpha = -7, \beta = 13$ and $\gamma = -6$. We observe that $\gamma - \alpha = 1$ is a rational square and the field $\mathbb{Q}(\sqrt{-1}, \sqrt{\alpha - \beta}, \sqrt{\beta - \gamma}) = \mathbb{Q}(\sqrt{-1}, \sqrt{5}, \sqrt{19})$ has degree 8 over $\mathbb{Q}$, as required. For this choice of α, β, γ we have the elliptic curve

$$\mathcal{E} : y^2 = (x + 7)(x - 13)(x + 6) = x^3 - 127x - 546$$

and the (s, t) -plane curve $(**)$ is

$$-s^2 = t^4 - 42t^2 + 361.$$

The point $(s, t) = (8, 5)$ is a rational point of this curve and we find the corresponding points on $\mathcal{E}$

$$D = (-9 + 4\sqrt{-1}, -20 - 10\sqrt{-1})$$

and

$$P := 4D = \left(\frac{6320521}{435600}, \frac{7420105819}{287496000} \right).$$

The cocycle $\{Z_\sigma\}_{\sigma \in G}$, where $Z_\sigma = D^\sigma - D$, is in $H_{loc}^1(G, \mathcal{E}[4])$, then, by definition, vanishes in $H^1(C, \mathcal{E}[4])$, for all cyclic subgroups $C \leq G$. Let v be a place of $\mathbb{Q}$ unramified in K . We consider an extension of v in K and we denote that with the same letter. By the Tchebotarev Density Theorem the group $G_v := \text{Gal}(K_v/\mathbb{Q}_v)$ varies over all cyclic subgroups of G . Then there exists a point $T_v \in \mathcal{E}[4]$ such that $Z_\sigma = T_v^\sigma - T_v$, for all $\sigma \in G_v$. Let $D_v := D - T_v$. Clearly it is fixed by G_v , then lies in $\mathbb{Q}_v$. We have $P = 4D = 4D - 4T_v = 4D_v$. Therefore P is locally divisible over $\mathbb{Q}_v$ for all primes $v \in \mathbb{Q}$ unramified in K . On the other hand, the abscissas of the 16 points D^* such that $4D^* = P$ are the roots of the polynomials:

$$f_1 = 25x^4 + 636x^3 + 6350x^2 + 28428x - 55969$$

$$f_2 = 121x^4 + 3208x^3 + 30734x^2 + 121112x + 200041$$

$$f_3 = 9x^4 - 1684x^3 + 2286x^2 + 253180x + 1064625$$

$$f_4 = x^4 - 97x^3 + 254x^2 + 16687x + 69091.$$

It is possible to check that the roots of f_1 lie in $\mathbb{Q}(\sqrt{-1})$, the roots of f_2 lie in $\mathbb{Q}(\sqrt{5}, \sqrt{-19})$, the roots of f_3 lie in $\mathbb{Q}(\sqrt{-19})$ and the roots of f_4 lie in $\mathbb{Q}(\sqrt{5})$. Therefore P is not globally divisible over $\mathbb{Q}$.

References

- [AT] Artin E., Tate J., *Class field theory*, Benjamin, Reading, MA, 1967.
- [DZ] Dvornicich R., Zannier U., *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France, **129** (2001), 317-338.
- [DZ2] Dvornicich R., Zannier U., *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Acad. Sci. Paris, Ser. I **338** (2004), 47-50.
- [DZ3] Dvornicich R., Zannier U., *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lon. Math. Soc., no. **39** (2007), 27-34.
- [Gru] Grunwald W., *Ein allgemeines Existenztheorem für algebraische Zahlkörper*, Journ. f.d. reine u. angewandte Math., **169** (1933), 103-107.
- [Maz] Mazur B., *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent Math., **44** (1978), no. 2, 129-162.
- [Ser] Serre J.-P. *Topics in galois Theory*, Jones and barlett, Boston 1992.

-
- [Tro] Trost E., *Zur theorie des Potenzreste*, Nieuw Archief voor Wiskunde, no. **18** (2) (1948), 58-61.
- [Wan] Wang Sh., *A counter example to Grunwald's theorem*, Annals of Math., no. **49** (1948), 1008-1009.
- [Wan2] Wang Sh., *On Grunwald's theorem*, Annals of Math., no. **51** (1950), 471-484.
- [Wha] Whaples G., *Non-analytic class field theory and Grunwald's theorem*, Duke Math. J., no. **9** (1942), 455-473.
- [Won] Wong S., *Power residues on abelian variety*, Manuscripta Math., no. **102** (2000), 129-137.