Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
C. R. Acad. Sci. Paris, Ser. I 338 (2004) 47–50
COMPTES RENDUS MATHEMATIQUE

Algebraic Geometry/Group Theory

An analogue for elliptic curves of the Grunwald–Wang example

Roberto Dvornicich [a], Umberto Zannier [b]

[a] *Dipartimento di Matematica, Università di Pisa, via Buonarroti, 2, 56127 Pisa, Italy*
[b] *Istituto Universitario di Architettura D.C.A. S.Croce, 191 (Tolentini), 30135 Venezia, Italy*

Received 30 April 2003; accepted after revision 21 October 2003

Presented by Jean-Pierre Serre

Abstract

We give examples of elliptic curves $\mathcal{E}/\mathbb{Q}$ and rational points $P \in \mathcal{E}(\mathbb{Q})$ such that P is divisible by 4 in $\mathcal{E}(\mathbb{Q}_v)$ for each rational place v but P is not divisible by 4 in $\mathcal{E}(\mathbb{Q})$. This is an analogue of a well-known example, with $\mathbb{G}_m$ in place of $\mathcal{E}$: namely, $P = 16$ *is a rational* 8*-th power locally almost everywhere, but not globally in* $\mathbb{Q}^* = \mathbb{G}_m(\mathbb{Q})$. ***To cite this article: R. Dvornicich, U. Zannier, C. R. Acad. Sci. Paris, Ser. I 338 (2004).***

Résumé

Un analogue pour les courbes elliptiques de l'exemple de Grunwald–Wang. Nous donnons des exemples de courbes elliptiques $\mathcal{E}/\mathbb{Q}$ et de points rationnels $P \in \mathcal{E}(\mathbb{Q})$ tels que P soit divisible par 4 dans $\mathcal{E}(\mathbb{Q}_v)$ pour tout place rationnelle v, sans que P soit divisible par 4 dans $\mathcal{E}(\mathbb{Q})$. Il s'agit d'un analogue d'un exemple bien connu, avec $\mathbb{G}_m$ à la place de $\mathcal{E}$: on sait que, dans $\mathbb{Q}^* = \mathbb{G}_m(\mathbb{Q})$, $P = 16$ *est localement une puissance* 8*-ième presque partout, mais* P *n'est pas une puissance* 8*-ième globalement*. ***Pour citer cet article : R. Dvornicich, U. Zannier, C. R. Acad. Sci. Paris, Ser. I 338 (2004).***

1. Introduction

In the paper [2] we considered the following local-global question (see also [4]). Let $\mathcal{A}$ be a commutative algebraic group defined over a number field k, let q be a positive integer and let $P \in \mathcal{A}(k)$. Let M_k be the set of places on the field k and suppose that, for almost all places $v \in M_k$, one has $P \in q\mathcal{A}(k_v)$.

Question. Can one conclude that $P = qD$ for some $D \in \mathcal{A}(k)$?

After giving some general cohomological criteria, we concentrated on the cases when $\mathcal{A}$ is either a torus or an elliptic curve. In short, some results are as follows (note that it is sufficient to consider the case when q is a power p^m of a prime p).

(i) If $\mathcal{A} = \mathbb{G}_m$, then the answer is affirmative for all odd prime powers q and for $q|4$ (see [1, Chapter IX, Theorem 1]). On the other hand, it is negative for $q = 8$, $P = 16$ (and $k = \mathbb{Q}$). This celebrated counterexample, first

E-mail addresses: dvornic@dm.unipi.it (R. Dvornicich), zannier@iuav.it (U. Zannier).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2003.10.034

discovered by Trost [5], is related to the Grunwald–Wang Theorem (see [1, Chapter X, Theorem 1] and also [3]). (ii) For $q = p$, the answer is positive if $\mathcal{A}$ is a torus of dimension $\leqslant \max(3, 2(p-1))$, but it can be negative for general tori, no matter the prime p (see [2, §§4, 5]). (iii) The answer is positive if $\mathcal{A} = \mathcal{E}$ is an elliptic curve and $q = p$ (see also [6]).

The case of an elliptic curve and $q = p^m$ with $m \geqslant 2$ remained open. We checked that a certain underlying cohomological condition (recalled in Section 2 below), sufficient for a positive answer, is not always verified. Conversely, however, it was not clear whether a counterexample to that condition would necessarily lead to a negative answer to our question.

Actually, we have now found that, similarly to the 'Grunwald–Wang case' of $\mathbb{G}_m$, for certain elliptic curves the *question* has a negative answer, already when $q = 4$ and $k = \mathbb{Q}$. The purpose of this note is just to describe explicitly some relevant examples and to discuss how they were found. In particular, we shall prove the following

Theorem 1.1. *There exist elliptic curves $\mathcal{E}$ defined over $\mathbb{Q}$ 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 $P \notin 4\mathcal{E}_{\mathbb{Q}}$.*

It is worth noticing that, in the Grunwald–Wang example, 'almost all' cannot be replaced by 'all', in view of the exceptional case $v = 2$ (there exists a completely similar example without exceptions, but with $k = \mathbb{Q}(i)$). On the contrary, for elliptic curves we are able to produce an example in which $P \in 4\mathcal{E}(\mathbb{Q}_v)$ for *all* $v \in M_{\mathbb{Q}}$ but $P \notin 4\mathcal{E}_{\mathbb{Q}}$ (see Section 4).

As to possible generalizations, for a given elliptic curve and a field k, results by Serre [4] on the Galois action on torsion points show that the alluded cohomological (sufficient) condition is verified for large q (see also [6]), hence our *question* has a positive answer for given k, $\mathcal{E}$ and $q > q_0(k, \mathcal{E})$. On the other hand, we do not know whether, in general, examples similar to the present ones, with curves defined over $\mathbb{Q}$ and $P \in \mathcal{E}(\mathbb{Q})$, actually exist for any given prime p and $q = p^m$ with $m \geqslant 2$. We intend to give more detail on these points in a future paper.

2. A cohomological condition

We briefly recall a few things from [2]. Let $\mathcal{A}$, k, P, q be as above and denote by $\bar{k}$ an algebraic closure of k. Suppose that $P \in q\mathcal{A}(k_v)$ for almost all $v \in M_k$. We write $P = qD$ for some $D \in \mathcal{A}(\bar{k})$; letting σ run over $G_k := \mathrm{Gal}(\bar{k}/k)$, we consider the cocycle $Z_\sigma := D^\sigma - D$, with values in $\mathcal{A}[q]$. It turns out [2, Corollary 2.3] that $D \in \mathcal{A}(K)$, where $K = k(\mathcal{A}[q])$ is the field generated over k by the q-torsion points of $\mathcal{A}(\bar{k})$, and that what really matters is $G := \mathrm{Gal}(K/k)$ rather than G_k. We then view Z as a cocycle on G and denote by the same symbol its class in $H^1(G, \mathcal{A}[q])$. In view of the Tchebotarev theorem, the local conditions amount to the vanishing of the restriction of $\{Z_\sigma\}$ in $H^1(C, \mathcal{A}[q])$ for any cyclic $C \subset G$. These cocycle classes make up a subgroup denoted $H^1_{\mathrm{loc}}(G, \mathcal{A}[q])$. A simple argument shows that, if the cocycle vanishes in $H^1(G, \mathcal{A}[q])$, then the point P is globally divisible by q, i.e., the *question* has a positive answer. In particular, this holds when $H^1_{\mathrm{loc}}(G, \mathcal{A}[q]) = 0$.

In [2, §3] we have listed some cases when $q = p$ or $q = p^2$. For $q = p^2$, several counterexamples to the vanishing of H^1_{loc} were found. However, it is not true *a priori* that the counterexamples come from cocycles obtained as above, by division of a point; namely, we do not know whether $H^1_{\mathrm{loc}}(G, \mathcal{A}[q]) \neq 0$ implies a negative answer to our *question*; to verify this, further checking is needed. In order to perform calculations 'by hand' on elliptic curves, we have chosen the counterexamples with $q = 4$ and G of smallest possible size, i.e., of order 4. The group of order 4 we shall work with (not explicitly given in the list of examples in [2]) is as follows.

Since for an elliptic curve $\mathcal{E}$ the group $\mathcal{E}[4](\bar{k})$ is isomorphic to $(\mathbb{Z}/(4))^2$, we identify G with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/(4))$. We define

$$G = \left\{ I + 2\begin{pmatrix} x & y \\ x+y & x+y \end{pmatrix},\ x, y \in \mathbb{Z}/(4) \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix} \right\}.$$

As is straightforward to verify, a nonzero element in $H^1_{\mathrm{loc}}(G, (\mathbb{Z}/(4))^2)$ is given by the cocycle

$$Z_\sigma = \begin{pmatrix} 2y \\ 0 \end{pmatrix}, \quad \text{for } \sigma = \sigma(x, y) = I + 2\begin{pmatrix} x & y \\ x+y & x+y \end{pmatrix}. \tag{1}$$

Starting from these data, and working in the simplest case of the rationals, we seek an elliptic curve $\mathcal{E}/\mathbb{Q}$ and a point $P \in \mathcal{E}(\mathbb{Q})$ with the following properties. Let $K = \mathbb{Q}(\mathcal{E}[4])$; we first require that the representation of $\mathrm{Gal}(K/\mathbb{Q})$ on $(\mathbb{Z}/(4))^2$ corresponds to G with respect to some basis for $\mathcal{E}[4]$ over $\mathbb{Z}/(4)$, so that in particular $[K:\mathbb{Q}] = 4$. Then we require that, for some point $D \in \mathcal{E}(K)$ with $4D = P$, the cocycle $D^\sigma - D \in \mathcal{E}[4]$ corresponds to Z_σ (with respect to the same basis for $\mathcal{E}[4]$), namely

$$Z_\sigma = D^\sigma - D. \tag{2}$$

We shall give numerical examples in Section 4, proving Theorem 1.1. In the next Section 3 we shall present a general family and describe the motivations which led to the sought construction.

3. The construction

We first note that the above conditions and (1) yield $D^{\sigma(1,0)} = D$. Thus we seek $D \in \mathcal{E}(k)$, for the fixed field $k \subset K$ of $\sigma(1,0)$. We have $[k:\mathbb{Q}] = 2$.

For simplicity we work with curves $\mathcal{E}$ having a Weierstrass equation of the form

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma), \tag{3}$$

where $\alpha, \beta, \gamma \in \mathbb{Q}$ are distinct rationals which satisfy $\alpha+\beta+\gamma = 0$. They correspond of course to the three points of order 2, denoted A, B, C respectively.

Since $2Z_\sigma = 0$, the conjugate point D' over $\mathbb{Q}$ differs from D by a 2-torsion point; thus we write

$$D' = D + A. \tag{4}$$

Also, write $D = (u, v) = (u_0 + \sqrt{\delta}u_1, v_0 + \sqrt{\delta}v_1)$, where $u_0, u_1, v_0, v_1, \delta \in \mathbb{Q}$ and where $k = \mathbb{Q}(\sqrt{\delta})$ and δ is not a rational square.

Setting $D' := (u', v')$, by a standard calculation we find from (4) that

$$\begin{cases} \lambda^2 = u' + u + \alpha = 2u_0 + \alpha \in \mathbb{Q}, \\ -v' = \lambda(u' - \alpha), \end{cases}$$

where $\lambda = v/(u-\alpha)$ is the slope of the line AD (D cannot be a 2-torsion point, so λ is well defined). Note that the second equation yields $\lambda' = -\lambda$. Therefore $\lambda = t\sqrt{\delta}$ for some $t \in \mathbb{Q}$.

Substituting $v = \lambda(u-\alpha)$ into $v^2 = (u-\alpha)(u-\beta)(u-\gamma)$ we find $(u-\beta)(u-\gamma) = \lambda^2(u-\alpha) = t^2\delta(u-\alpha)$ or, equivalently,

$$\begin{cases} u_0^2 + \delta u_1^2 + \alpha u_0 + \beta\gamma = t^2\delta(u_0 - \alpha), \\ 2u_0u_1 + \alpha u_1 = t^2\delta u_1. \end{cases}$$

Note that the last equation is actually implicit in the previous ones $2u_0 + \alpha = \lambda^2 = t^2\delta$. Using $2u_0 = t^2\delta - \alpha$ to substitute for u_0 in the first equation of the last displayed pair, and putting $s = 2u_1$, we get

$$\delta s^2 = \delta^2 t^4 - 6\alpha\delta t^2 + (\beta-\gamma)^2. \tag{5}$$

Conversely, given a rational solution of this equation, we may proceed backwards and get a point D as above, satisfying (4).

We may verify that $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha-\beta}, \sqrt{\beta-\gamma}, \sqrt{\gamma-\alpha})$. To represent $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/(4))$, we use a basis $A', B' \in \mathcal{E}[4]$ with $A = 2A'$, $B = 2B'$; specifically, for some given determination of the square roots, $A' = (\alpha + \sqrt{(\alpha-\beta)(\alpha-\gamma)}, (\alpha-\beta)\sqrt{\alpha-\gamma} + (\alpha-\gamma)\sqrt{\alpha-\beta})$, $B' = (\beta + \sqrt{(\beta-\alpha)(\beta-\gamma)}, (\beta-\gamma)\sqrt{\beta-\alpha} + (\beta-\alpha)\sqrt{\beta-\gamma})$.

We require that $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[4])/\mathbb{Q})$ corresponds to the group G defined above; by direct computation, this amounts to the conditions that $\gamma - \alpha$ and $(\alpha-\beta)(\beta-\gamma)$ are (nonzero) rational squares and that $\mathbb{Q}(\mathcal{E}[4]) = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha-\beta})$ has degree 4 over $\mathbb{Q}$.

Also, recall that we want to satisfy (2), namely $Z_\sigma = D^\sigma - D$. This means that D is fixed by $\sigma(1,0)$ and that is sent to $D + A$ by $\sigma(0,1)$ and by $\sigma(1,1)$ or, equivalently, that $\sqrt{\delta}$ lies in the fixed field of $\sigma(1,0)$. By computation, using the above basis A', B', it may be verified that this fixed field is $\mathbb{Q}(\sqrt{-1})$; hence we must impose that δ equals -1 (up to nonzero squares).

Now, the arithmetical conditions on α, β, γ mentioned above correspond to rational points on a certain rational curve. It is easy to parametrize it: setting $\gamma - \alpha = \xi^2$, $\alpha - \beta = (\beta - \gamma)\eta^2$ and combining these equations with $\alpha + \beta + \gamma = 0$, we obtain

$$\alpha = -\frac{\xi^2(1+2\eta^2)}{3(1+\eta^2)}, \qquad \beta = -\frac{\xi^2(1-\eta^2)}{3(1+\eta^2)}, \qquad \gamma = \frac{\xi^2(2+\eta^2)}{3(1+\eta^2)}. \tag{6}$$

From this parametrization, however, we have to discard the points corresponding to $\xi\eta = 0$ (for which α, β, γ are not distinct) and to $1 + \eta^2$ a rational square (for which $[K : \mathbb{Q}] = 2$).

Finally, given α, β, γ, Eq. (5) (with $\delta = -1$) parametrizes a point D suitable for us. Namely, the suitable choices for D correspond to the rational points on the (s, t)-plane curve defined by

$$-s^2 = t^4 + 6\alpha t^2 + (\beta - \gamma)^2. \tag{7}$$

Note that the right side has distinct roots in t, since $36\alpha^2 - 4(\beta - \gamma)^2 = 16(\alpha - \gamma)(\alpha - \beta) \neq 0$. Therefore (7) represents a curve of genus 1.[1]

We may reformulate these conclusions by saying that the relevant curves $\mathcal{E}$ are parametrized rationally by (6), while for a given curve $\mathcal{E}$ the relevant points D and $P = 4D$ are parametrized by the rational points on the curve (7) of genus 1.

4. Numerical examples

It is not hard to recognize that the curve (7) has rational points for infinitely many values of (ξ, η), with $\xi\eta \neq 0$ and $1 + \eta^2$ not a rational square, giving rise to non-isomorphic curves. The simplest numerical choice is $\xi = 5$, $\eta = 2$, which, in view of the above formulas, gives $\alpha = -15$, $\beta = 5$, $\gamma = 10$. The curve (7) becomes $-s^2 = t^4 - 90t^2 + 25$, which admits the rational point $t = 1$, $s = 8$. In turn, this gives the points $D = (7 + 4\sqrt{-1}, -4 + 22\sqrt{-1})$, $P = (1561/12^2, 19459/12^3)$ on the elliptic curve $y^2 = (x + 15)(x - 5)(x - 10)$. We may indeed verify directly that P is divisible by 4 locally with a single exception, but not globally. In fact, one finds that the set of 16 points D^* such that $4D^* = P$ may be partitioned as follows: four of them verify $\mathbb{Q}(D^*) = \mathbb{Q}(\sqrt{-1})$, eight of them verify $\mathbb{Q}(D^*) = \mathbb{Q}(\sqrt{5})$ and four of them $\mathbb{Q}(D^*) = \mathbb{Q}(\sqrt{-5})$, hence none is rational. As to the local divisibility, it follows from the fact that for each place $v \in M_{\mathbb{Q}}$, $v \neq 2$, at least one among $\sqrt{-1}$, $\sqrt{5}$, $\sqrt{-5}$ lies in $\mathbb{Q}_v$. Note that this feature is again similar to the situation of the Grunwald–Wang example, where four of the division points of 16 by 8 are defined over $\mathbb{Q}(\sqrt{-1})$, two over $\mathbb{Q}(\sqrt{2})$ and two over $\mathbb{Q}(\sqrt{-2})$.

To get rid of exceptions regarding the local divisibility, we can choose $\xi = 65$, $\eta = 8$, which gives $\alpha = -2795$, $\beta = 1365$, $\gamma = 1430$; the curve (7) has the rational point $(s, t) = (112, 1)$, which corresponds to $D = (1397 + 56\sqrt{-1}, -56 + 4192\sqrt{-1})$, $P = (5086347841/1848^2, -35496193060511/1848^3)$. Here we have that $\mathbb{Q}(D^*) = \mathbb{Q}(\sqrt{-1})$ (four times), $\mathbb{Q}(D^*) = \mathbb{Q}(\sqrt{65})$ (eight times) and $\mathbb{Q}(D^*) = \mathbb{Q}(\sqrt{-65})$ (four times), and *for all* v at least one among $\sqrt{-1}$, $\sqrt{65}$, $\sqrt{-65}$ lies in $\mathbb{Q}_v$.

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] H. Flanders, Generalization of a theorem of Ankeny and Rogers, Ann. Math. 57 (2) (1953) 392–400.
[4] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972) 259–331.
[5] E. Trost, Zur Theorie der Potenzreste, Nieuw Archief voor Wiskunde 18 (2) (1934) 58–61.
[6] S. Wong, Power residues on Abelian varieties, Manuscripta Math. 102 (2000) 129–137.

[1] Actually, it is easily seen that this curve is birational with $\mathcal{E}$ over $\mathbb{Q}(\sqrt{-1})$; however, it has not always a rational point, even if α, β, γ are subject to (6); in fact, it may be verified that for $\xi = \eta = 1$ the curve (7) has no points over $\mathbb{Q}_2$, and *a fortiori* over $\mathbb{Q}$.