LOCAL TO GLOBAL TRACE QUESTIONS AND TWISTS OF GENUS ONE CURVES

by

Mirela Çiperiani and Ekin Ozman

Abstract. — Let E be an elliptic curve defined over a number field F and K/F a quadratic extension. For a point $P \in \mathrm{E}(\mathrm{F})$ that is a local trace for every completion of K/F, we find necessary and sufficient conditions for P to lie in the image of the global trace map. These conditions can then be used to determine whether a quadratic twist of E, as a genus one curve, has rational points. In the case of quadratic twists of genus one modular curves $X_0(N)$ with squarefree N, the existence of rational points corresponds to the existence of $\mathbb{Q}$-curves of degree N defined over K.

Contents

Introduction

Let F be a number field, E/F an elliptic curve of conductor $\mathcal{N}$, and K/F a quadratic extension. We want to find conditions which determine whether a point in E(F) lies in the image of the global trace map $\mathrm{tr}_{\mathrm{K/F}} : \mathrm{E}(\mathrm{K}) \to \mathrm{E}(\mathrm{F})$. An obvious necessary condition is that the point must be a local trace at every completion of F. Hence, for every prime v of F we consider the restriction map $\mathrm{res}_v : \mathrm{E}(\mathrm{F}) \to \mathrm{E}(\mathrm{F}_v)$ and we investigate the following question.

(0)2010 Mathematics Subject Classification: 11G05.
Keywords: Elliptic Curve, $\mathbb{Q}$-curves, twists of genus one curves.
The first author was partially supported by an NSA grant during the preparation of this paper.

Question. — *Let $P \in \mathrm{E}(\mathrm{F})$ such that $\mathrm{res}_v(P)$ lies in the image of the local trace maps $\mathrm{tr}_{\mathrm{K}_\nu/\mathrm{F}_v} : \mathrm{E}(\mathrm{K}_\nu) \to \mathrm{E}(\mathrm{F}_v)$ for every prime v of F, where ν is a prime of K lying over v. Is the point P in the image of the global trace map $\mathrm{tr}_{\mathrm{K/F}}$?*

Consider the map

$$\psi : \mathrm{E}(\mathrm{F})/\mathrm{tr}_{\mathrm{K/F}}\mathrm{E}(\mathrm{K}) \longrightarrow \prod_v \mathrm{E}(\mathrm{F}_v)/\mathrm{tr}_{\mathrm{K}_\nu/\mathrm{F}_v}\mathrm{E}(\mathrm{K}_\nu). \tag{1}$$

The kernel of ψ measures the failure of the local-global trace principle. For a subset $\mathcal{S}$ of $\mathrm{E}(\mathrm{F})$, we say that *the local-global trace principle holds for* $\mathcal{S}$ if every point $P \in \mathcal{S}$ is a global trace if and only if it is local trace for every prime v of F, i.e. if the kernel of ψ intersects trivially with $\mathcal{S}$.

In Proposition 1.1 we see that being a local trace for every prime is in fact a condition at only finitely many primes, specifically a subset of the primes that ramify in K/F and non-split prime divisors of $\mathcal{N}$. However, in Proposition 1.7 and Proposition 1.12 we find that a point $P \in \mathrm{E}(\mathrm{F})$ that is a local trace at every prime, is also a global trace only when either $\mathrm{E}(\mathrm{F})_2 \neq \mathrm{E}(\mathrm{K})_2$ or points in $\mathrm{E}(\mathrm{F}) \setminus \big(2\mathrm{E}(\mathrm{F}) + \mathrm{E}(\mathrm{F})_2\big)$ and in $\mathrm{E}^d(\mathrm{F}) \setminus 2\mathrm{E}^d(\mathrm{F})$ give rise to a point that is 2-divisible in $\mathrm{E}(\mathrm{K})$, here E^d denotes the quadratic twist of E with respect to K/F. Note that global 2-divisibility is equivalent to local 2-divisibility at almost all primes [**DZ**].

The motivation for considering these trace questions lies in the study of rational points on quadratic twists of the underlying genus one curve E. In Section 2, we consider the quadratic twist of E with respect to K/F and a point $P \in \mathrm{E}(\mathrm{F})$. We show that this twisted genus one curve has a F-rational (resp. F_v-rational) point if and only if P is a global trace (resp. local trace). Therefore, our analysis of local to global trace questions provides conditions under which a quadratic twist of the genus one curve E with local points for every completion of F is in fact an elliptic curve over F, see Theorem 2.4. Moreover, in the special case of genus one modular curves $X_0(N)$ with squarefree N, rational points of the twists of $X_0(N)$ correspond to quadratic $\mathbb{Q}$-curves of degree N, see [**El**]. Hence, by verifying finitely many 2-divisibility conditions we can determine whether $\mathbb{Q}$-curves of degree N exists over a quadratic extension K of $\mathbb{Q}$.

Notation. — We will use the following notation:

- E^d denotes the quadratic twist of the elliptic curve E with respect to $\mathrm{K} = \mathrm{F}(\sqrt{d})$.
- for an abelian group M, we denote by M_n the n-torsion subgroup of M.

– for a Galois extension L/F and a $\mathbb{Z}[\mathrm{Gal}(\mathrm{L}/\mathrm{F})]$-module M, we use $\mathrm{H}^1(\mathrm{L}/\mathrm{F}, M)$ to denote the Galois cohomology group $\mathrm{H}^1(\mathrm{Gal}(\mathrm{L}/\mathrm{F}), M)$; in addition, $\mathrm{H}^1(\overline{\mathrm{F}}/\mathrm{F}), M)$ is denoted by $\mathrm{H}^1(\mathrm{F}, M)$.

1. Local to global trace questions

We start by analyzing the condition of being a local trace.

Proposition 1.1. — *Let v be a prime of* F *and ν be a prime of* K *lying above v. Then the image of the map* $\mathrm{tr}_{\mathrm{K}_\nu/\mathrm{F}_v} : \mathrm{E}(\mathrm{K}_\nu) \to \mathrm{E}(\mathrm{F}_v)$ *equals*

i) $\mathrm{E}(\mathrm{F}_v)$ *if at least one of the following conditions holds:*
   (a) *v splits in* K/F*;*
   (b) *v is inert in* K/F *and* E *has good reduction at v;*
   (c) *v is inert in* K/F*,* E *has multiplicative reduction at v, and $ord_v(\Delta_E)$ is odd where Δ_E is the discriminant of some model of* E*;*
   (d) *$v \nmid 2\infty$ and* $\mathrm{E}(\mathrm{F}_v)[2] = 0$*;*
   (e) *v is real and $(\Delta_E)_v < 0$.*
ii) $2\mathrm{E}(\mathrm{F}_v)$ *if $v \nmid 2\mathcal{N}$ and v ramifies in* K/F*.*

Proof. — The assertion (i) is Lemma 2.10 of [**MR**] and assertion (ii) for finite primes is Lemma 2.11 of [**MR**]. We now consider real infinite primes v of F which are ramified in K. In this case, $\mathrm{K}_\nu = \mathbb{C}$ and $\mathrm{F}_v = \mathbb{R}$. We know that there exist $q \in \mathbb{R}^*$ such that

$$\mathrm{E}(\mathbb{C}) \simeq \mathbb{C}^*/q^{\mathbb{Z}} \quad \text{and} \quad \mathrm{E}(\mathbb{R}) \simeq \mathbb{R}^*/q^{\mathbb{Z}}.$$

Since under the above identifications the trace map $\mathrm{tr}_{\mathrm{K}_\nu/\mathrm{F}_v}$ is induced by the norm map, we find that $P \in \mathrm{E}(\mathbb{R})$ is a local trace if and only if it is 2-divisible in $\mathrm{E}(\mathbb{R})$. Note that $q < 0$ corresponds to $(\Delta_E)_v < 0$ and in that case $\mathrm{E}(\mathbb{R}) = 2\mathrm{E}(\mathbb{R})$. This concludes the proof of the proposition. □

The following immediate implication of the above proposition transforms question of whether a point is a local trace at all primes into a question about local divisibility by 2 at a finite set of primes for a subset of quadratic extensions K/F.

Corollary 1.2. — *Let $\mathcal{Q}$ be the set of primes that are ramified in* K/F*. If all primes dividing $2\mathcal{N}$ split in* K/F*, then the subgroup of elements of* E(F) *that are local traces at all*

primes equals the kernel of the map

$$\mathrm{E}(\mathrm{F}) \longrightarrow \prod_{v\in\mathcal{Q}} \mathrm{E}(\mathrm{F}_v)/2\mathrm{E}(\mathrm{F}_v).$$

Remark 1.3. — Let L be a field of characteristic distinct from $2, 3$ and containing F, F_v, or the residue field of F_v for some good reduction prime v. If E is given by the equation $y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ where $\alpha_i \in \overline{\mathrm{L}}$, then a point $P = (x_P, y_P) \in \mathrm{E}^d(\mathrm{L})$ is divisible by 2 in $\mathrm{E}(\mathrm{L})$ if and only if $x_P - \alpha_i \in \mathrm{L}(\alpha_i)^2$ for $i = 1, 2, 3$. This follows from Theorem 4.2 of [**Kn**] and a simple analysis of the action of $\mathrm{Gal}\big(\mathrm{L}(\mathrm{E}_2)/\mathrm{L}\big)$ on the set $P/2 + \mathrm{E}(\overline{\mathrm{L}})_2$, here $\mathrm{Gal}\big(\mathrm{L}(\mathrm{E}_2)/\mathrm{L}\big) := \ker\big(\mathrm{Gal}(\overline{\mathrm{L}}/\mathrm{L}) \to \mathrm{Aut}(\mathrm{E}(\overline{\mathrm{L}})_2)\big)$.

Moreover, for finite primes v of F coprime to $2\mathcal{N}$ we have that

$$\mathrm{E}(\mathrm{F}_v)/2\mathrm{E}(\mathrm{F}_v) \simeq \mathrm{E}(k_v)/2\mathrm{E}(k_v)$$

where k_v denotes the residue field of F_v. Hence, under the conditions of the above corollary verifying whether a point of $\mathrm{E}(\mathrm{F})$ is a local trace at all primes involves only a finite number of simple computations over finite fields and potentially $\mathbb{R}$.

Consider the isomorphism $\iota : \mathrm{E}(\mathrm{K}) \to \mathrm{E}^d(\mathrm{K})$. Using the short Weierstrass models $y^2 = x^3 + ax + b$ for both E and E^d we have $\iota(x, y) = (xd, yd\sqrt{d})$. Let $\tau \in \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F})$ be a generator of $\mathrm{Gal}(\mathrm{K}/\mathrm{F})$ and observe that

$$\iota(\tau P) = -\tau\iota(P) \quad \text{for all } P \in \mathrm{E}(\mathrm{K}). \tag{2}$$

Lemma 1.4. — *The group* $\mathrm{E}(\mathrm{F})/\mathrm{tr}_{\mathrm{K}/\mathrm{F}}\mathrm{E}(\mathrm{K})$ *is isomorphic to* $\mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K}))$ *under the map* $\bar{\kappa}$ *induced by*

$$\kappa : \mathrm{E}(\mathrm{F}) \longrightarrow \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})),$$

where $\kappa(P) \in \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K}))$ *such that* $\kappa(P)(\tau) = \iota(P)$.

Proof. — We know that

$$\mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})) \simeq \frac{\ker(\mathrm{tr}_{\mathrm{K}/\mathrm{F}} : \mathrm{E}^d(\mathrm{K}) \to \mathrm{E}^d(\mathrm{K}))}{\mathrm{im}\,(\tau - 1 : \mathrm{E}^d(\mathrm{K}) \to \mathrm{E}^d(\mathrm{K}))}$$

under the map that sends a cocycle $c \in \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K}))$ to $c(\tau)$.

By (2) we see that

$$\iota(\mathrm{tr}_{\mathrm{K}/\mathrm{F}}P) = (1-\tau)\iota(P) \quad \text{and} \quad \iota((\tau-1)P) = -\mathrm{tr}_{\mathrm{K}/\mathrm{F}}\iota(P).$$

Consequently, the map ι induces the following isomorphism

$$\frac{\ker(\tau - 1 : \mathrm{E}(\mathrm{K}) \to \mathrm{E}(\mathrm{K}))}{\mathrm{im}\,(\mathrm{tr}_{\mathrm{K}/\mathrm{F}} : \mathrm{E}(\mathrm{K}) \to \mathrm{E}(\mathrm{K}))} \simeq \frac{\ker(\mathrm{tr}_{\mathrm{K}/\mathrm{F}} : \mathrm{E}^d(\mathrm{K}) \to \mathrm{E}^d(\mathrm{K}))}{\mathrm{im}\,(\tau - 1 : \mathrm{E}^d(\mathrm{K}) \to \mathrm{E}^d(\mathrm{K}))}.$$

Hence, we have that

$$\mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})) \simeq \frac{\ker(\tau - 1 : \mathrm{E}(\mathrm{K}) \to \mathrm{E}(\mathrm{K}))}{\mathrm{im}\,(\mathrm{tr}_{\mathrm{K}/\mathrm{F}} : \mathrm{E}(\mathrm{K}) \to \mathrm{E}(\mathrm{K}))}$$

It follows that

$$\mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})) \simeq \frac{\mathrm{E}(\mathrm{F})}{\mathrm{tr}_{\mathrm{K}/\mathrm{F}}\mathrm{E}(\mathrm{K})}$$

under the map $\bar{\kappa}^{-1}$ which sends $c \in \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K}))$ to $\iota^{-1}\big(c(\tau)\big)$. □

As in Lemma 1.4, we also have that

$$\frac{\mathrm{E}(\mathrm{F}_v)}{\mathrm{tr}_{\mathrm{K}_\nu/\mathrm{F}_v}\mathrm{E}(\mathrm{K}_\nu)} \simeq \mathrm{H}^1(\mathrm{K}_\nu/\mathrm{F}_v, \mathrm{E}^d(\mathrm{K}_\nu)). \tag{3}$$

Then the map ψ in (1) can be identified with the following natural map

$$\psi_c : \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})) \to \prod_v \mathrm{H}^1(\mathrm{K}_\nu/\mathrm{F}_v, \mathrm{E}^d(\mathrm{K}_\nu))$$

and $\ker\psi \simeq \ker\psi_c$ under $\bar{\kappa}$. Consequently we see that the kernel of ψ fits into the following diagram where each row and column is exact:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \ker\psi & \to & \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})) & \to & \prod_v \mathrm{H}^1(\mathrm{K}_\nu/\mathrm{F}_v, \mathrm{E}^d(\mathrm{K}_\nu)) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & Ш(\mathrm{E}^d/\mathrm{F}) & \to & \mathrm{H}^1(\mathrm{F}, \mathrm{E}^d) & \to & \prod_v \mathrm{H}^1(\mathrm{F}_v, \mathrm{E}^d) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & Ш(\mathrm{E}^d/\mathrm{K}) & \to & \mathrm{H}^1(\mathrm{K}, \mathrm{E}^d) & \to & \prod_\nu \mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E}^d)
\end{array}$$

Then since $[\mathrm{K} : \mathrm{F}] = 2$ we see that $\ker\psi$ is a subgroup of $Ш(\mathrm{E}^d/\mathrm{F})_2$ and we have the following result.

Proposition 1.5. — *The group* $\ker\psi$ *is isomorphic to the kernel of the restriction map*

$$Ш(\mathrm{E}^d/\mathrm{F})_2 \longrightarrow Ш(\mathrm{E}^d/\mathrm{K})_2.$$

We now consider the following diagram:

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & \ker\psi & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & \mathrm{E}^d(\mathrm{F})/2\mathrm{E}^d(\mathrm{F}) & \longrightarrow & \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{F},\mathrm{E}^d_2) & \longrightarrow & Ш(\mathrm{E}^d/\mathrm{F})_2 & \longrightarrow & 0 \\
 & & \pi_1\downarrow & & \pi_2\downarrow & & \downarrow & & \\
0 & \longrightarrow & \Big(\mathrm{E}^d(\mathrm{K})/2\mathrm{E}^d(\mathrm{K})\Big)^{\mathrm{Gal}(\mathrm{K}/\mathrm{F})} & \longrightarrow & \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K},\mathrm{E}^d_2)^{\mathrm{Gal}(\mathrm{K}/\mathrm{F})} & \longrightarrow & Ш(\mathrm{E}^d/\mathrm{K})_2^{\mathrm{Gal}(\mathrm{K}/\mathrm{F})} & &
\end{array}$$

Using the snake lemma we find the exact sequence

$$0 \longrightarrow \ker\pi_1 \longrightarrow \ker\pi_2 \longrightarrow \ker\psi \xrightarrow{\delta} \mathrm{coker}\,\pi_1. \tag{4}$$

Observe that

$$\ker\pi_2 = \ker\Big(\mathrm{H}^1(\mathrm{K}/\mathrm{F},\mathrm{E}^d(\mathrm{K})_2) \longrightarrow \prod_v \mathrm{H}^1(\mathrm{K}_\nu/\mathrm{F}_v,\mathrm{E}^d(\mathrm{K}_\nu))\Big)$$

which has the following immediate implication:

$$\ker\pi_2 \simeq \ker\left(\mathrm{E}(\mathrm{F})_2/\mathrm{tr}_{\mathrm{K}/\mathrm{F}}\mathrm{E}(\mathrm{K})_2 \longrightarrow \prod_v \mathrm{E}(\mathrm{F}_v)/\mathrm{tr}_{\mathrm{K}_\nu/\mathrm{F}_v}\mathrm{E}(\mathrm{K}_\nu)\right). \tag{5}$$

Lemma 1.6. — *The intersection of* $\kappa\big(\mathrm{E}(\mathrm{F})\big)$ *with the image of* $\mathrm{H}^1(\mathrm{K}/\mathrm{F},\mathrm{E}^d(\mathrm{K})_2)$ *equals* $\kappa\big(\mathrm{E}(\mathrm{F})_2\big)$.

Proof. — Let $P \in \mathrm{E}(\mathrm{F})$ such that

$$\kappa(P) \in \mathrm{im}\,\big(\mathrm{H}^1(\mathrm{K}/\mathrm{F},\mathrm{E}^d(\mathrm{K})_2) \to \mathrm{H}^1(\mathrm{K}/\mathrm{F},\mathrm{E}^d(\mathrm{K}))\big).$$

It follows that $P = (\tau+1)Q + R$ where $R \in \mathrm{E}(\mathrm{K})_2$ and $Q \in \mathrm{E}(\mathrm{K})$. Consequently, we have that $R \in \mathrm{E}(\mathrm{F})_2$ and

$$\kappa(P) = \kappa(R) \in \kappa\big(\mathrm{E}(\mathrm{F})_2\big).$$

□

Observe that the exactness of (4) and Lemma 1.6 implies that the kernel of the map δ lies in $\ker\psi \cap \kappa(\mathrm{E}(\mathrm{F})_2)$. Then by (5) we have that the following exact sequence:

$$0 \longrightarrow \ker\pi_1 \longrightarrow \ker\pi_2 \longrightarrow \ker\psi \cap \kappa(\mathrm{E}(\mathrm{F})_2) \longrightarrow 0. \tag{6}$$

Proposition 1.7. — *Let* E/F *be an elliptic curve with non-trivial* F*-rational* 2*-torsion. Assume that*

i) *if* $\mathrm{E}(\mathrm{F})_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *then* K/F *is ramified at some infinite prime;*

ii) *a non-trivial element of* $\mathrm{E}(\mathrm{F})_2$ *lies in the image of the local trace map for every prime of* F.

Then the local-global trace principle holds for $\mathrm{E}(\mathrm{F})_2$ *if and only if*

$$\mathrm{E}(\mathrm{K})_2 \neq \mathrm{E}(\mathrm{F})_2 \quad \text{or} \quad 2\mathrm{E}^d(\mathrm{F}) \neq \mathrm{E}^d(\mathrm{F}) \cap 2\mathrm{E}^d(\mathrm{K}).$$

Proof. — We will show that $\mathrm{E}(\mathrm{F})_2$ intersects the kernel of ψ trivially if and only if at least one of the above two conditions holds. Our assumptions and Proposition 1.1(ii) imply that

$$\ker\left(\mathrm{E}(\mathrm{F})_2 \to \prod_v \mathrm{E}(\mathrm{F}_v)/\mathrm{tr}_{\mathrm{K}_\nu/\mathrm{F}_v}\mathrm{E}(\mathrm{K}_\nu)\right) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Then by (5) we have that $\ker \pi_2$ is either trivial or isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

If $\ker \pi_2$ is trivial then $\ker \psi \cap \mathrm{E}(\mathrm{F})_2 = 0$. By (5) and assumption (ii) we know that $\ker \pi_2 = 0$ if and only if $\mathrm{tr}(\mathrm{E}(\mathrm{K})_2) \neq 0$ which is equivalent to $\mathrm{E}(\mathrm{K})_2 \neq \mathrm{E}(\mathrm{F})_2$.

If $\ker \pi_2 \simeq \mathbb{Z}/2\mathbb{Z}$ then $\ker \psi \cap \mathrm{E}(\mathrm{F})_2 = 0$ if and only if the map π_1 is not injective which is equivalent to

$$2\mathrm{E}^d(\mathrm{F}) \neq \mathrm{E}^d(\mathrm{F}) \cap 2\mathrm{E}^d(\mathrm{K}).$$

This concludes the proof of the proposition. □

Note that when applying the above result we check the 2-divisibility of points of $\mathrm{E}^d(\mathrm{F})$ in $\mathrm{E}^d(\mathrm{K})$ by making use of Remark 1.3.

Example 1.8. — Consider the elliptic curve $\mathrm{E} : y^2 + xy + y = x^3 - 2731x - 55146$ [(1)] and $\mathrm{K} = \mathbb{Q}(\sqrt{473})$. We know that

$$\mathrm{E}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad \mathrm{E}^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$$

where $d = 473$. We now show that the local-global trace principle holds for $\mathrm{E}(\mathbb{Q})_2$.

We will start by checking whether the non-trivial point $T \in \mathrm{E}(\mathbb{Q})_2$ is a local trace for every prime of $\mathbb{Q}$. The conductor of $\mathrm{E}/\mathbb{Q}$ equals 14 and the primes $2, 7$ split in $\mathrm{K}/\mathbb{Q}$. Consequently, by Corollary 1.2 and Remark 1.3 it is enough to determine whether $T \in 2\mathrm{E}(\mathbb{F}_\ell)$ for the primes $\ell = 11, 43$ (the prime divisors of $d = 473$). Using MAGMA we find that $T \in 2\mathrm{E}(\mathbb{F}_{11})$ and $T \in 2\mathrm{E}(\mathbb{F}_{43})$. It follows that T lies in the image of local trace map for every prime of $\mathbb{Q}$.

In addition, we find $R \in \mathrm{E}^d(\mathbb{Q}) \setminus \left(2\mathrm{E}^d(\mathbb{Q}) + \mathrm{E}^d(\mathbb{Q})_2\right)$ such that $R + \iota(T) \in 2\mathrm{E}^d(\mathrm{K})$. Hence, Proposition 1.7 implies that T is a global trace and the local-global trace principle holds for $\mathrm{E}(\mathbb{Q})_2$.

(1) The Cremona label for this elliptic curve is `14a5`.

Example 1.9. — Consider the elliptic curve $\mathrm{E} : y^2 + xy + y = x^3 - 12x - 16$ [(2)] and $\mathrm{K} = \mathbb{Q}(\sqrt{73})$. We have that

$$\mathrm{E}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \quad \text{and} \quad \mathrm{E}^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$$

where $d = 73$. The conductor of $\mathrm{E}/\mathbb{Q}$ equals $82 = 2 \cdot 41$ and $2, 41$ split in $\mathrm{K}/\mathbb{Q}$.

Using Corollary 1.2 and Remark 1.3 we verify that the non-trivial point $T \in \mathrm{E}(\mathbb{Q})_2$ lies in the image of local trace map for every prime of $\mathbb{Q}$. Now we choose $R \in \mathrm{E}^d(\mathbb{Q})$ which together with $\iota(T)$ generates $\mathrm{E}^d(\mathbb{Q})$. We verify that R and $R + \iota(T)$ are not in $2\mathrm{E}^d(\mathrm{K})$. Since we also have that $\mathrm{E}(\mathrm{K})_2 = \mathrm{E}(\mathbb{Q})_2$, by Proposition 1.7 we deduce that T is not a global trace and consequently the local-global trace principle fails for $\mathrm{E}(\mathbb{Q})_2$.

Example 1.10. — Consider the elliptic curve $\mathrm{E} : y^2 = x^3 + x^2 - 2x$ [(3)] and $\mathrm{K} = \mathbb{Q}(\sqrt{-407})$. We know that

$$\mathrm{E}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad \mathrm{E}^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$$

where $d = -407$. Observe that the conductor of $\mathrm{E}/\mathbb{Q}$ equals 96, and the primes $2, 3$ split in $\mathrm{K}/\mathbb{Q}$.

Using Corollary 1.2 and Remark 1.3 we verify that the non-trivial point $T = (1, 0) \in \mathrm{E}(\mathbb{Q})_2$ is a local trace for every prime of $\mathbb{Q}$. Now we choose $R \in \mathrm{E}^d(\mathbb{Q})$ such that it generates $\mathrm{E}^d(\mathbb{Q})/\mathrm{E}^d(\mathbb{Q})_2$ and verify that $\big(R + \mathrm{E}^d(\mathbb{Q})_2\big) \cap 2\mathrm{E}^d(\mathrm{K}) = \emptyset$. Hence, Proposition 1.7 implies that T is not a global trace and the local-global trace principle fails for $\mathrm{E}(\mathbb{Q})_2$.

In order to address local to global trace questions about $\mathrm{E}(\mathrm{F}) \setminus \big(2\mathrm{E}(\mathrm{F}) + \mathrm{E}(\mathrm{F})_2\big)$, we need to understand the map $\delta : \ker \psi \to \operatorname{coker} \pi_1$ in (4). We start by analyzing $\operatorname{coker} \pi_1$. Consider the map

$$\mathrm{E}^d(\mathrm{K})/2\mathrm{E}^d(\mathrm{K}) \xrightarrow{\widetilde{\tau+1}} \mathrm{E}^d(\mathrm{F})/2\mathrm{E}^d(\mathrm{F})$$

induced by $P \mapsto (\tau+1)P$. The kernel of $\widetilde{\tau + 1}$ consists of $P \in \mathrm{E}^d(\mathrm{K})$ such that $P = R + \iota(Q)$, where $R \in \mathrm{E}^d(\mathrm{F})$ and $Q \in \mathrm{E}(\mathrm{F})$ are uniquely determined modulo $\mathrm{E}(\mathrm{F})_2$. Consequently, the map

$$\tilde{\iota} : \mathrm{E}^d(\mathrm{F}) \oplus \mathrm{E}(\mathrm{F})/\mathrm{E}(\mathrm{F})_2 \longrightarrow \Big(\mathrm{E}^d(\mathrm{K})/2\mathrm{E}^d(\mathrm{K})\Big)^{\mathrm{Gal}(\mathrm{K}/\mathrm{F})},$$

where $\tilde{\iota}(R, Q) := R + \iota(Q) + 2\mathrm{E}^d(\mathrm{K})$ for $R \in \mathrm{E}^d(\mathrm{F})$ and $Q \in \mathrm{E}(\mathrm{F})$, is surjective. It follows that

$$\operatorname{coker} \pi_1 \simeq \tilde{\iota}\big(\mathrm{E}(\mathrm{F})\big)/\tilde{\iota}\big(\mathrm{E}^d(\mathrm{F})\big)$$

(2) The Cremona label for this elliptic curve is `82a2`.
(3) The Cremona label for this elliptic curve is `96a1`.

and in particular the map ι induces a surjection of $\mathrm{E}(\mathrm{F})/\big(2\mathrm{E}(\mathrm{F})+\mathrm{E}(\mathrm{F})_2\big)$ onto $\operatorname{coker}\pi_1$.

Let $P \in \mathrm{E}(\mathrm{F}) \setminus \mathrm{E}(\mathrm{F})_2$. Consider $S = \iota(P) \in \mathrm{E}^d(\mathrm{K})$ and its corresponding cocycle $b_S \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}^d_2)^{\mathrm{Gal}(\mathrm{K}/\mathrm{F})}$. By fixing $\frac{S-\tau S}{2} = S \in \mathrm{E}^d(\mathrm{K})$ we define the cocycle $c_S \in \mathrm{H}^1(\mathrm{F}, \mathrm{E}^d_2)$ as follows

$$c_S(\sigma) = \sigma(S/2) - S/2 - \frac{S-\sigma S}{2} \quad \text{for all } \sigma \in \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F}).$$

Observe that c_S maps to b_S under the restriction map

$$\mathrm{H}^1(\mathrm{F}, \mathrm{E}^d_2) \longrightarrow \mathrm{H}^1(\mathrm{K}, \mathrm{E}^d_2)^{\mathrm{Gal}(\mathrm{K}/\mathrm{F})}$$

and that the other choices of $\frac{S-\tau S}{2} \in \mathrm{E}^d(\mathrm{K})$ correspond to the other elements of the coset $c_S + \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})_2)$.

The image of c_S in $\mathrm{H}^1(\mathrm{F}, \mathrm{E}^d)$ equals $d_S \in \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K}))$ where $d_S(\tau) = S$. Note that d_S is uniquely determined only as an element of

$$\mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K}))/\mathrm{im}\left(\mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})_2) \to \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K}))\right),$$

and $d_S \in \mathrm{im}\left(\mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})_2) \to \mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K}))\right)$ if and only if $S \in 2\mathrm{E}^d(\mathrm{K}) + \mathrm{E}^d(\mathrm{F})$. By (3) the following lemma is immediate.

Lemma 1.11. — *Let $P \in \mathrm{E}(\mathrm{F}) \setminus \mathrm{E}(\mathrm{F})_2$. Then*

$$d_{\iota(P)} \in \ Ш(\mathrm{E}^d/\mathrm{F}) + \mathrm{im}\left(\mathrm{H}^1(\mathrm{K}/\mathrm{F}, \mathrm{E}^d(\mathrm{K})_2) \to \mathrm{H}^1(\mathrm{F}, \mathrm{E}^d)\right).$$

if and only if the kernel of the map

$$\mathrm{E}(\mathrm{F}) \to \prod_v \mathrm{E}(\mathrm{F}_v)/\mathrm{tr}_{\mathrm{K}_\nu/\mathrm{F}_v}\mathrm{E}(\mathrm{K}_\nu)$$

intersects non-trivially with the coset $P + \mathrm{E}(\mathrm{F})_2$.

As a consequence we now see that $\delta : \ker\psi \to \operatorname{coker}\pi_1$ maps $P \mapsto \tilde{\iota}(P)$ and we have the following result.

Proposition 1.12. — *Let* E/F *be an elliptic curve such that the local-global trace principle holds for* $\mathrm{E}(\mathrm{F})_2$*, and* $P \in \mathrm{E}(\mathrm{F})$ *be a local trace for all primes of* F*. Then P is a global trace if and only if $\iota(P) \in 2\mathrm{E}^d(\mathrm{K}) + \mathrm{E}^d(\mathrm{F})$.*

Proof. — Since P is a local trace at all primes we know that $P \in \ker\psi$. By (4) and (6) we see that the assumption that the local-global trace principle holds for $\mathrm{E}(\mathrm{F})_2$ implies that the map $\delta : \ker\psi \to \operatorname{coker}\pi_1$ is injective. Consequently, P is a global trace if and only if $\delta(P) = 0$. Since $\delta(P) = \tilde{\iota}(P) \in \operatorname{coker}\pi_1$ it follows that P is a global trace if and only if $\iota(P) \in 2\mathrm{E}^d(\mathrm{K}) + \mathrm{E}^d(\mathrm{F})$. □

Example 1.13. — Consider the elliptic curve $\mathrm{E} : y^2 + xy = x^3 + 4x + 1$ [(4)] and $\mathrm{K} = \mathbb{Q}(\sqrt{-311})$. Then

$$\mathrm{E}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \quad \textit{and} \quad \mathrm{E}^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$$

where $d = -311$. Observe that the conductor of $\mathrm{E}/\mathbb{Q}$ equals 65 and the primes $2, 5, 13$ split in $\mathrm{K}/\mathbb{Q}$. We now verify that the local-global trace principle holds for $\mathrm{E}(\mathbb{Q})$.

Let $T \in \mathrm{E}(\mathbb{Q})_2$ and $S \in \mathrm{E}(\mathbb{Q})$ such that $\mathrm{E}(\mathbb{Q}) = \langle T, S \rangle$. Since $T, S \in 2\mathrm{E}(\mathbb{R})$ and $T, S \in 2\mathrm{E}(\mathbb{F}_{311})$, by Corollary 1.2 and Remark 1.3 we know that T and S are local traces for all primes of $\mathbb{Q}$.

Then, after identifying generators of $\mathrm{E}^d(\mathbb{Q})/2\mathrm{E}^d(\mathbb{Q})$, we find $P_1 \in \mathrm{E}^d(\mathbb{Q}) \setminus \big(2\mathrm{E}^d(\mathbb{Q}) + \mathrm{E}^d(\mathbb{Q})_2\big)$ such that $P_1 \in 2\mathrm{E}^d(\mathrm{K})$, which by Proposition 1.7 implies that T is a global trace. Therefore, the local-global trace condition holds for $\mathrm{E}(\mathbb{Q})_2$. Moreover, we also find $P_2 \in \mathrm{E}^d(\mathbb{Q}) \setminus \big(2\mathrm{E}^d(\mathbb{Q}) + \mathrm{E}^d(\mathbb{Q})_2\big)$ such that $\iota(S) + P_2$ is 2-divisible in $\mathrm{E}^d(\mathrm{K})$. Then by Proposition 1.12 we deduce that S is a also global trace. Hence, the local-global trace principle holds for $\mathrm{E}(\mathbb{Q})$.

2. Twists of genus one curves

Let (E, O) be an elliptic curve over F where O denotes the distinguished element of $\mathrm{E}(\mathrm{F})$. In this section we study quadratic twists of the genus one curve E. Consider $\mathrm{Aut}(\mathrm{E})$ the automorphism group of E viewed as a genus one curve. We know that

$$\mathrm{Aut}(\mathrm{E}) \simeq \mathrm{Aut}(\mathrm{E}, O) \ltimes \mathrm{E}(\overline{\mathrm{F}})$$

where $\mathrm{Aut}(\mathrm{E}, O)$ is the automorphism group of E viewed as an elliptic curve. Therefore, if E does not have complex multiplication, a generic element of $\mathrm{Aut}(\mathrm{E})$ is of the form $(\pm 1, S)$ and sends a point $X \in \mathrm{E}(\overline{\mathrm{F}})$ to $\pm X + S \in \mathrm{E}(\overline{\mathrm{F}})$.

For any quadratic extension $\mathrm{K} = \mathrm{F}(\sqrt{d})$ and any point $S \in \mathrm{E}(\mathrm{F})$, we consider $\zeta_{\mathrm{K},S} \in \mathrm{H}^1\big(\mathrm{Gal}(\bar{\mathrm{F}}/\mathrm{F}), \mathrm{Aut}(\mathrm{E})\big)$ defined by the following cocycle:

$$\zeta_{\mathrm{K},S}(\sigma) = \begin{cases} (-1, S) & \text{if } \sigma(\sqrt{d}) = -\sqrt{d} \\ (1, O) & \text{otherwise.} \end{cases}$$

Let $\mathrm{E}_{\mathrm{K},S}$ denote the twist of E corresponding to $\zeta_{\mathrm{K},S}$ [**Si**, §X.2]. The twisted curve, $\mathrm{E}_{\mathrm{K},S}$ is a genus one curve defined over F and it is isomorphic to E over K. We refer to $\mathrm{E}_{\mathrm{K},S}$ as the twist of E with respect to K/F and $S \in \mathrm{E}(\mathrm{F})$.

(4) The Cremona label for this elliptic curve is `65a2`.

Lemma 2.1. — *The group* $\mathrm{E}_{\mathrm{K},S}(\mathrm{F})$ *of* F*-rational points of* $\mathrm{E}_{\mathrm{K},S}$ *is isomorphic to the following subgroup of* $\mathrm{E}(\overline{\mathrm{F}})$*:*

$$\{P \in \mathrm{E}(\overline{\mathrm{F}}) \mid \zeta_{\mathrm{K},S}(\sigma)\big(\sigma(P)\big) = P \text{ for all } \sigma \in \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F})\}.$$

Proof. — By Theorem 2.2 [**Si**, §X.2] we know that there is an isomorphism $\theta : \mathrm{E}_{\mathrm{K},S} \to \mathrm{E}$ such that $\theta^\sigma = \zeta_{\mathrm{K},S}(\sigma)\theta$, here $\theta^\sigma := \sigma\theta\sigma^{-1}$. It follows that

$$\theta\sigma = \begin{cases} (-1, S)\sigma\theta & \text{if } \sigma(\sqrt{d}) = -\sqrt{d} \\ \sigma\theta & \text{otherwise.} \end{cases} \tag{7}$$

Let $R \in \mathrm{E}_{\mathrm{K},S}(\overline{\mathrm{F}})$ and $P \in \mathrm{E}(\overline{\mathrm{F}})$ such that $P = \theta(R)$. Note that since θ is an isomorphism $R \in \mathrm{E}_{\mathrm{K},S}(\mathrm{F})$ if and only if $\theta(\sigma R) = P$ for every $\sigma \in \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F})$. By (7) we see that

$$\theta(\sigma R) = \zeta_{\mathrm{K},S}(\sigma)(\sigma P).$$

Hence, the map θ gives the following isomorphism:

$$\mathrm{E}_{\mathrm{K},S}(\mathrm{F}) \simeq \{P \in \mathrm{E}(\overline{\mathrm{F}}) \mid \zeta_{\mathrm{K},S}(\sigma)\big(\sigma(P)\big) = P \text{ for all } \sigma \in \mathrm{Gal}(\overline{\mathrm{F}}/\mathrm{F})\}.$$

□

We would like to be able to determine whether $\mathrm{E}_{\mathrm{K},S}$ is an elliptic curve over F or over F_v for some prime v of F.

Lemma 2.2. — *Let* K/F *be a quadratic extension,* $S \in \mathrm{E}(\mathrm{F})$*, and* $\mathrm{E}_{\mathrm{K},S}/\mathrm{F}$ *the corresponding twist of* E*. Then*

a) $\mathrm{E}_{\mathrm{K},S}$ *has an* F*-rational point if and only if* S *is a global trace.*
b) $\mathrm{E}_{\mathrm{K},S}$ *has a point defined over* F_v *if and only if* S *lies in the image of the trace map* $\mathrm{tr}_{\mathrm{K}_\nu/\mathrm{F}_v} : \mathrm{E}(\mathrm{K}_\nu) \to \mathrm{E}(\mathrm{F}_v)$*, here* ν *denotes a prime of* K *above a prime* v *of* F*.*

Moreover, if $\mathrm{E}_{\mathrm{K},S}$ *has a point defined over* F *(resp. over* F_v*) then* $\mathrm{E}_{\mathrm{K},S}$ *is isomorphic over* F *(resp. over* F_v*) to the quadratic twist* E^d*.*

Remark 2.3. — Note that part (a) of the above lemma follows immediately from Lemma 2.1 but we will proceed to give a different argument that addresses all three statements simultaneously.

Proof. — We will show that $\mathrm{E}_{\mathrm{K},S}(\mathrm{F})$ is nonempty if and only if $\zeta_{\mathrm{K},S}$ is cohomologous to $\zeta_{\mathrm{K},O}$ in which case $\mathrm{E}_{\mathrm{K},S}$ is isomorphic over F to the quadratic twist E^d.

Assume that $\mathrm{E}_{\mathrm{K},S}(\mathrm{F})$ is not empty. By Lemma 2.1 it follows that there exists $P \in \mathrm{E}(\mathrm{K})$ such that $(\tau+1)P = S$. Let $\varphi = (-1, P)$ and observe that

$$\varphi^{\tau}\zeta_{\mathrm{K},S}(\tau) = (-1, \tau P)(-1, S) = (1, \tau P - S),$$
$$\zeta_{\mathrm{K},O}(\tau)\varphi = (-1, O)(-1, P) = (1, -P).$$

Since $-P = \tau P - S$, it follows that $\zeta_{\mathrm{K},S}$ and ζ_O are cohomologous.

Conversely, we now assume that $\zeta_{\mathrm{K},S}$ and $\zeta_{\mathrm{K},O}$ are cohomologous. Hence, there exists $\varphi = (\pm 1, P) \in \mathrm{Aut}(\mathrm{E})$ such that $\varphi^{\tau}\zeta_{\mathrm{K},S}(\tau) = \zeta_{\mathrm{K},O}(\tau)\varphi$. This implies that $(\mp 1, \pm S + \tau P) = (\mp 1, -P)$ and hence $S = \tau(\mp P) + (\mp P)$ for some $P \in \mathrm{E}(\overline{\mathrm{F}})$. For $\sigma \in \mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$ we have that

$$\varphi^{\sigma}\zeta_{\mathrm{K},S}(\sigma) = (\pm 1, \sigma P)(1, O) = (\pm 1, \sigma P),$$
$$\zeta_{\mathrm{K},O}(\sigma)\varphi = (1, O)(\pm 1, P) = (\pm 1, P).$$

Since $\varphi^{\sigma} * \zeta_{\mathrm{K},S}(\sigma) = \zeta_{\mathrm{K},O}(\sigma) * \varphi$, it follows that $\sigma P = P$ for all $\sigma \in \mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$. Hence, $S = \tau P' + P'$ for some $P' \in \mathrm{E}(\mathrm{K})$. This concludes the proof of part (a).

Part (b) is trivially true if v splits in K/F since $\mathrm{E}_{\mathrm{K},S}(\mathrm{K})$ is nonempty, and otherwise it follows by a local argument that is identical to the one used in the global case. □

The above lemma together with Proposition 1.7 and Proposition 1.12 give the following result.

Theorem 2.4. — *Let* K/F *be a quadratic extension and* $S \in \mathrm{E}(\mathrm{F})$. *Assume that the corresponding genus one curve* $\mathrm{E}_{\mathrm{K},S}/\mathrm{F}$ *has a local point over* F_v *for all primes* v. *Then* $\mathrm{E}_{\mathrm{K},S}(\mathrm{F})$ *is nonempty if the following holds:*

i) *if* $S \in \big(2\mathrm{E}(\mathrm{F}) + \mathrm{E}(\mathrm{F})_2\big) \setminus 2\mathrm{E}(\mathrm{F})$, *then*
   a) *if* $\mathrm{E}(\mathrm{F})_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *then* K/F *is ramified at some infinite prime, and*
   b) $\mathrm{E}(\mathrm{K})_2 \neq \mathrm{E}(\mathrm{F})_2$ *or* $2\mathrm{E}^d(\mathrm{F}) \neq \mathrm{E}^d(\mathrm{F}) \cap 2\mathrm{E}^d(\mathrm{K})$.

ii) *if* $S \in \mathrm{E}(\mathrm{F}) \setminus \big(2\mathrm{E}(\mathrm{F}) + \mathrm{E}(\mathrm{F})_2\big)$, *then*
   a) *the local-global trace principle holds for* $\mathrm{E}(\mathrm{F})_2$, *and*
   b) $\iota(P) \in 2\mathrm{E}^d(\mathrm{K}) + \mathrm{E}^d(\mathrm{F})$.

The conclusions in the examples described in §1 can now be rephrased as follows:

- in Example 1.8, $\mathrm{E}_{\mathrm{K},T}(\mathbb{Q}) \neq \emptyset$ for $\mathrm{K} = \mathbb{Q}(\sqrt{473})$ and every $T \in \mathrm{E}(\mathbb{Q})_2$.
- in Example 1.9, for $\mathrm{K} = \mathbb{Q}(\sqrt{73})$ and $T \in \mathrm{E}(\mathbb{Q})_2 \setminus \{O\}$ we find that $\mathrm{E}_{\mathrm{K},T}(\mathbb{Q}_v) \neq \emptyset$ for every prime v but $\mathrm{E}_{\mathrm{K},T}$ has no rational points.

- in Example 1.10, $\mathrm{E}(\mathbb{Q})_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and for $\mathrm{K} = \mathbb{Q}(\sqrt{-407})$ there is a unique non-trivial $T \in \mathrm{E}(\mathbb{Q})_2$ such that $\mathrm{E}_{\mathrm{K},T}(\mathbb{Q}_v) \neq \emptyset$ for every prime v; however $\mathrm{E}_{\mathrm{K},T}(\mathbb{Q}) = \emptyset$ for every $T \in \mathrm{E}(\mathbb{Q})_2 \setminus \{O\}$.
- in Example 1.13, $\mathrm{E}_{\mathrm{K},T}(\mathbb{Q}) \neq \emptyset$ for $\mathrm{K} = \mathbb{Q}(\sqrt{-311})$ and every $T \in \mathrm{E}(\mathbb{Q})$.

One interesting application of the above theorem is in the study of rational points on twists of genus one modular curves. For $\mathrm{K} = \mathbb{Q}(\sqrt{d})$, the twist $X^d(N)$ of the modular curve $X_0(N)$ is constructed by Galois descent from $X_0(N)/\mathrm{K}$. It is a smooth proper curve over $\mathbb{Q}$, isomorphic to $X_0(N)$ over K but not over $\mathbb{Q}$. The action of $\tau \in \mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ on $X^d(N)$ is 'twisted', in particular $\mathbb{Q}$-rational points of $X^d(N)$ are naturally identified with the K-rational points of $X_0(N)$ that are fixed by $\tau \circ w_N$, where w_N denotes the Atkin-Lehner involution. Like $X_0(N)$, if N is squarefree the twisted curve $X^d(N)$ is a parameter space and its $\mathbb{Q}$-rational points correspond to $\mathbb{Q}$-curves of degree N defined over $\mathrm{K} = \mathbb{Q}(\sqrt{d})$. A $\mathbb{Q}$-curve of degree N over $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ is an elliptic curve defined over K which is isogenous to its Galois conjugate over K via an isogeny ϕ with $\ker(\phi) \cong \mathbb{Z}/N\mathbb{Z}$, see Ellenberg's survey article [**El**] for more on $\mathbb{Q}$-curves.

If $X_0(N)$ has genus one then $w_N = (-1, S) \in \mathrm{Aut}(X_0(N))$ for some $S \in X_0(N)(\mathbb{Q})$. Therefore, given a quadratic field $\mathrm{K} = \mathbb{Q}(\sqrt{d})$, the corresponding twist $X^d(N)$ equals $X_0(N)^{\zeta_{\mathrm{K},S}}$. Hence, for modular curves of genus one, the study of rational points on the twist $X^d(N)$ is related to trace questions (see Lemma 2.2). The values of squarefree N such that $X_0(N)$ has genus one are: $11, 14, 15, 17, 19, 21$. Among these, for $N = 11, 19$ the group $X_0(N)(\mathbb{Q})$ is cyclic of odd order and hence $X^d(N)(\mathbb{Q}) \neq \emptyset$ for every $d \in \mathbb{Q}$. We will now give one example of the study of the rational points for a twist of each of the remaining genus one modular curves.

Example 2.5. — Let E be the modular curve $X_0(14)$. We have that $\mathrm{E}(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ and $w_{14} = (-1, S) \in \mathrm{Aut}(X_0(14))$ for a point $S \in \mathrm{E}(\mathbb{Q})$ of order 6.

Consider the quadratic field $\mathrm{K} = \mathbb{Q}(\sqrt{17})$. We know that $X^{17}(14)(\mathbb{Q}_v) \neq \emptyset$ for every prime v of $\mathbb{Q}$, see [**Oz**, Theorem 1.1]. Consequently, Lemma 2.2 implies that S is a local trace at all primes of $\mathbb{Q}$.

Observe that $\mathrm{E}^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, here $d = 17$. We find that there exists a point $P \in \mathrm{E}^d(\mathbb{Q}) \setminus \left(2\mathrm{E}^d(\mathbb{Q}) + \mathrm{E}^d(\mathbb{Q})_2\right)$ such that $P \in 2\mathrm{E}^d(\mathrm{K})$. Then by Theorem 2.4(i) we deduce that $\mathrm{E}_{\mathrm{K},S}(\mathbb{Q}) = X^{17}(14)(\mathbb{Q}) \neq \emptyset$ and this implies the existence of a $\mathbb{Q}$-curve of degree 14 defined over $\mathbb{Q}(\sqrt{17})$.

Example 2.6. — Let E be the modular curve $X_0(15)$. Then $\mathrm{E}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $w_{15} = (-1, S) \in \mathrm{Aut}(X_0(15))$ for a point $S \in \mathrm{E}(\mathbb{Q})$ of order 4.

Consider $\mathrm{K} = \mathbb{Q}(\sqrt{-71})$ and observe that $\mathrm{E}^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, here $d = -71$. The primes $2, 3, 5$ split in $\mathrm{K}/\mathbb{Q}$, and we verify that $S \in 2\mathrm{E}(\mathbb{R})$, and $S \in 2\mathrm{E}(\mathbb{F}_{71})$. Then Corollary 1.2 and Remark 1.3 imply that S is a local trace for all primes of $\mathbb{Q}$. Hence, $\mathrm{E}_{\mathrm{K},S}(\mathbb{Q}_v) = X^{-71}(15)(\mathbb{Q}_v) \neq \emptyset$ for every prime v of $\mathbb{Q}$.

Since $\mathrm{K}/\mathbb{Q}$ is imaginary, at most one of the non-trivial 2-torsion points of $\mathrm{E}(\mathbb{Q})$ can be a local trace at all primes of $\mathbb{Q}$, see Proposition 1.1. It follows that $2S$ is that point and that the local-global trace principle holds for $\mathrm{E}(\mathbb{Q})_2$. Then we also find $R \in \mathrm{E}^d(\mathbb{Q}) \setminus \big(2\mathrm{E}^d(\mathbb{Q}) + \mathrm{E}^d(\mathbb{Q})_2\big)$ such that $\iota(S) - R \in 2\mathrm{E}^d(\mathrm{K})$. Hence, by Theorem 2.4(ii) we deduce $\mathrm{E}_{\mathrm{K},S}(\mathbb{Q}) = X^{-71}(15)(\mathbb{Q}) \neq \emptyset$ and this implies the existence of a $\mathbb{Q}$-curve of degree 15 defined over $\mathbb{Q}(\sqrt{-71})$.

Example 2.7. — Let E be the modular curve $X_0(17)$. We have that $\mathrm{E}(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ and $w_{17} = (-1, S) \in \mathrm{Aut}(X_0(17))$ for a point $S \in \mathrm{E}(\mathbb{Q})$ of order 4.

Consider $\mathrm{K} = \mathbb{Q}(\sqrt{19})$ and observe that $\mathrm{E}^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, here $d = 19$. We know that $X^{19}(17)(\mathbb{Q}_v) \neq \emptyset$ for every prime v of $\mathbb{Q}$, see [**Oz**, Theorem 1.1]. Hence, Lemma 2.2 implies that S is a local trace at all primes of $\mathbb{Q}$.

We then find $R \in \mathrm{E}^d(\mathbb{Q}) \setminus \big(2\mathrm{E}^d(\mathbb{Q}) + \mathrm{E}^d(\mathbb{Q})_2\big)$ such that $\iota(S) - R \in 2\mathrm{E}^d(\mathrm{K})$. Since in this case the local-global trace principle holds trivially for $\mathrm{E}(\mathbb{Q})_2$, Theorem 2.4(ii) implies that $\mathrm{E}_{\mathrm{K},S}(\mathbb{Q}) = X^{19}(17)(\mathbb{Q}) \neq \emptyset$. Hence, there exists a $\mathbb{Q}$-curve of degree 17 defined over $\mathbb{Q}(\sqrt{19})$.

Example 2.8. — Let E be the modular curve $X_0(21)$. Then $\mathrm{E}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $w_{21} = (-1, S) \in \mathrm{Aut}(X_0(21))$ for a point $S \in \mathrm{E}(\mathbb{Q})$ of order 4.

Consider $\mathrm{K} = \mathbb{Q}(\sqrt{-47})$ and observe that $\mathrm{E}^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, here $d = -47$. The primes $2, 3, 7$ split in $\mathrm{K}/\mathbb{Q}$, and we verify that $S \in 2\mathrm{E}(\mathbb{R})$ and $S \in 2\mathrm{E}(\mathbb{F}_{47})$. Then Corollary 1.2 and Remark 1.3 imply that S is a local trace for all primes of $\mathbb{Q}$. Hence, $\mathrm{E}_{\mathrm{K},S}(\mathbb{Q}_v) = X^{-47}(21)(\mathbb{Q}_v) \neq \emptyset$ for every prime v of $\mathbb{Q}$.

Since K is imaginary, at most one of the non-trivial 2-torsion points can be a local trace (see Proposition 1.1). It follows that $2S$ is that point and that the local-global trace principle holds for $\mathrm{E}(\mathbb{Q})_2$. Then we proceed to find $R \in \mathrm{E}^d(\mathbb{Q}) \setminus \big(2\mathrm{E}^d(\mathbb{Q}) + \mathrm{E}^d(\mathbb{Q})_2\big)$ such that $\iota(S) - R \in 2\mathrm{E}^d(\mathrm{K})$. Hence, by Theorem 2.4(ii) we deduce that $\mathrm{E}_{\mathrm{K},S}(\mathbb{Q}) = X^{-47}(21)(\mathbb{Q}) \neq \emptyset$ which implies the existence of a $\mathbb{Q}$-curve of degree 21 defined over $\mathbb{Q}(\sqrt{-47})$.

References

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

[El] J.S. Ellenberg, $\mathbb{Q}$-*curves and Galois representations*, Modular curves and abelian varieties, 93103, Progr. Math., 224, Birkhuser, Basel, 2004.

[Kn] A.W. Knapp, *Elliptic curves*, Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992.

[MR] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. 181 (2010), no. 3, 541–575.

[Oz] E. Ozman, *Points on Quadratic Twists of* $X_0(N)$, Acta Arith. 152 (2012), no. 4, 323–348.

[Si] J. H. Silverman, *The arithmetic of elliptic curves*, Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp.

October 28, 2013

Mirela Çiperiani and Ekin Ozman