

## LOCAL TO GLOBAL TRACE QUESTIONS AND TWISTS OF GENUS ONE CURVES

MIRELA ÇIPERIANI AND EKIN OZMAN

(Communicated by Ken Ono)

**ABSTRACT.** Let  $E$  be an elliptic curve defined over a number field  $F$  and  $K/F$  a quadratic extension. For a point  $P \in E(F)$  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  $K$ .

### 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  $\text{tr}_{K/F} : E(K) \rightarrow E(F)$ . 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  $\text{res}_v : E(F) \rightarrow E(F_v)$  and we investigate the following question.

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

Consider the map

$$(1) \quad \psi : E(F)/\text{tr}_{K/F}E(K) \longrightarrow \prod_v E(F_v)/\text{tr}_{K_\nu/F_\nu}E(K_\nu).$$

The kernel of  $\psi$  measures the failure of the local-global trace principle. For a subset  $\mathcal{S}$  of  $E(F)$ , 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  $\psi$  intersects trivially with  $\mathcal{S}$ .

In Proposition 1.1 (almost entirely due to Mazur-Rubin [MR]) 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, through the following results (corresponding to Propositions 1.7 and 1.12 in the text) we find that being a global trace is equivalent to infinitely

---

Received by the editors October 28, 2013 and, in revised form, June 10, 2014.

2010 *Mathematics Subject Classification.* Primary 11G05.

*Key words and phrases.* 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.

many local conditions. Here  $E^d$  denotes the quadratic twist of  $E$  with respect to  $K/F$ , and  $\iota$  is the isomorphism from  $E$  to  $E^d$ .

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

- i) *if  $E(F)_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , then  $K/F$  is ramified at some infinite prime;*
- ii) *a non-trivial element of  $E(F)_2$  lies in the image of the local trace map for every prime of  $F$ .*

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

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

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

Observe that a point  $P \in E(F)$  that is a local trace at every prime is also a global trace only when  $P \in 2E(F)$  or  $E(F)_2 \neq E(K)_2$  or points in  $E(F) \setminus (2E(F) + E(F)_2)$  and in  $E^d(F) \setminus 2E^d(F)$  give rise to a point that is 2-divisible in  $E(K)$ . 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  $P \in E(F)$ . We show that this twisted genus one curve has an  $F$ -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  $N$  exist 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  $K = F(\sqrt{d})$ .
- For an abelian group  $M$ , we denote by  $M_n$  the  $n$ -torsion subgroup of  $M$ .
- For a Galois extension  $L/F$  and a  $\mathbb{Z}[\text{Gal}(L/F)]$ -module  $M$ , we use  $H^1(L/F, M)$  to denote the Galois cohomology group  $H^1(\text{Gal}(L/F), M)$ . In addition,  $H^1(F, M)$  denotes  $H^1(\text{Gal}(\bar{F}/F), M)$  where  $\bar{F}$  is an algebraic closure of  $F$ .

### 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  $\nu$  be a prime of  $K$  lying above  $v$ . Then the image of the map  $\text{tr}_{K_\nu/F_v} : E(K_\nu) \rightarrow E(F_v)$  equals*

- i)  $E(F_v)$  *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  $\text{ord}_v(\Delta_E)$  is odd where  $\Delta_E$  is the discriminant of some model of  $E$ ;
  - (d)  $v \nmid 2\infty$  and  $E(F_v)[2] = 0$ ;
  - (e)  $v$  is real and  $(\Delta_E)_v < 0$ .
- ii)  $2E(F_v)$  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,  $K_\nu = \mathbb{C}$  and  $F_\nu = \mathbb{R}$ . We know that there exist  $q \in \mathbb{R}^*$  such that

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

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

The following immediate implication of the above proposition transforms the 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*

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

*Remark 1.3.* Let  $L$  be a field of characteristic distinct from 2, 3 and containing  $F$ ,  $F_\nu$  or the residue field of  $F_\nu$  for some good reduction prime  $\nu$ . If  $E$  is given by the equation  $y^2 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$  where  $\alpha_i \in \bar{L}$ , then a point  $P = (x_P, y_P) \in E^d(L)$  is divisible by 2 in  $E(L)$  if and only if  $x_P - \alpha_i \in L(\alpha_i)^2$  for  $i = 1, 2, 3$ . This follows from Theorem 4.2 of [Kn] and a simple analysis of the action of  $\text{Gal}(L(E_2)/L)$  on the set  $P/2 + E(\bar{L})_2$ ; here  $\text{Gal}(L(E_2)/L) := \ker(\text{Gal}(\bar{L}/L) \rightarrow \text{Aut}(E(\bar{L})_2))$ .

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

$$E(F_\nu)/2E(F_\nu) \simeq E(k_\nu)/2E(k_\nu)$$

where  $k_\nu$  denotes the residue field of  $F_\nu$ . Hence, under the conditions of the above corollary, verifying whether a point of  $E(F)$  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  $\iota : E(K) \rightarrow E^d(K)$ . 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  $\tau \in \text{Gal}(\bar{F}/F)$  be a generator of  $\text{Gal}(K/F)$  and observe that

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

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

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

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

*Proof.* We know that

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

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

By (2) we see that

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

Consequently, the map  $\iota$  induces the following isomorphism:

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

Hence, we have that

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

It follows that

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

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

As in Lemma 1.4, we also have that

$$(3) \quad \frac{E(F_v)}{\text{tr}_{K_\nu/F_v}E(K_\nu)} \simeq H^1(K_\nu/F_v, E^d(K_\nu)).$$

Then the map  $\psi$  in (1) can be identified with the natural map

$$\psi_c : H^1(K/F, E^d(K)) \rightarrow \prod_v H^1(K_\nu/F_v, E^d(K_\nu))$$

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

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \ker \psi & \longrightarrow & H^1(K/F, E^d(K)) & \longrightarrow & \prod_v H^1(K_\nu/F_v, E^d(K_\nu)) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{III}(E^d/F) & \longrightarrow & H^1(F, E^d) & \longrightarrow & \prod_v H^1(F_v, E^d) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{III}(E^d/K) & \longrightarrow & H^1(K, E^d) & \longrightarrow & \prod_v H^1(K_\nu, E^d) \end{array}$$

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

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

$$\text{III}(E^d/F)_2 \longrightarrow \text{III}(E^d/K)_2.$$

We now consider the following diagram:

$$\begin{array}{ccccccc}
 & & & & & & 0 \\
 & & & & & & \downarrow \\
 & & & & & & \ker \psi \\
 & & & & & & \downarrow \\
 0 & \longrightarrow & E^d(F)/2E^d(F) & \longrightarrow & H_{\text{Sel}}^1(F, E_2^d) & \longrightarrow & \text{III}(E^d/F)_2 \longrightarrow 0 \\
 & & \downarrow \pi_1 & & \downarrow \pi_2 & & \downarrow \\
 0 & \longrightarrow & (E^d(K)/2E^d(K))^{\text{Gal}(K/F)} & \longrightarrow & H_{\text{Sel}}^1(K, E_2^d)^{\text{Gal}(K/F)} & \longrightarrow & \text{III}(E^d/K)_2^{\text{Gal}(K/F)}
 \end{array}$$

Using the snake lemma we find the exact sequence

$$(4) \quad 0 \longrightarrow \ker \pi_1 \longrightarrow \ker \pi_2 \longrightarrow \ker \psi \xrightarrow{\delta} \text{coker } \pi_1.$$

Observe that

$$\ker \pi_2 = \ker \left( H^1(K/F, E^d(K)_2) \longrightarrow \prod_v H^1(K_\nu/F_\nu, E^d(K_\nu)) \right),$$

which has the following immediate implication:

$$(5) \quad \ker \pi_2 \simeq \ker \left( E(F)_2/\text{tr}_{K/F} E(K)_2 \longrightarrow \prod_v E(F_\nu)/\text{tr}_{K_\nu/F_\nu} E(K_\nu) \right).$$

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

*Proof.* Let  $P \in E(F)$  be such that

$$\kappa(P) \in \text{im} \left( H^1(K/F, E^d(K)_2) \rightarrow H^1(K/F, E^d(K)) \right).$$

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

$$\kappa(P) = \kappa(R) \in \kappa(E(F)_2).$$

□

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

$$(6) \quad 0 \longrightarrow \ker \pi_1 \longrightarrow \ker \pi_2 \longrightarrow \ker \psi \cap \kappa(E(F)_2) \longrightarrow 0.$$

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

- i) *if  $E(F)_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , then  $K/F$  is ramified at some infinite prime;*
- ii) *a non-trivial element of  $E(F)_2$  lies in the image of the local trace map for every prime of  $F$ .*

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

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

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

$$\ker (E(F)_2 \rightarrow \prod_v E(F_v)/\text{tr}_{K_\nu/F_\nu} E(K_\nu)) \simeq \mathbb{Z}/2\mathbb{Z}.$$

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

If  $\ker \pi_2 \simeq \mathbb{Z}/2\mathbb{Z}$ , then  $\ker \psi \cap E(F)_2 = 0$  if and only if the map  $\pi_1$  is not injective, which is equivalent to

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

This concludes the proof of the proposition. □

We will now proceed by giving some examples. Note that throughout the examples in this paper:

- We check the 2-divisibility of points of  $E^d(F)$  in  $E^d(K)$  by making use of Remark 1.3.
- The equation we use for  $E^d$  is  $y^2 = x^3 + ad^2x + bd^3$ , where  $y^2 = x^3 + ax + b$  is the minimal Weierstrass model of  $E/\mathbb{Q}$ .

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

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

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

We will start by checking whether the non-trivial point  $T = (-121/4, 117/8) \in E(\mathbb{Q})_2$  is a local trace for every prime of  $\mathbb{Q}$ . The conductor of  $E/\mathbb{Q}$  equals 14 and the primes 2, 7 split in  $K/\mathbb{Q}$ . Consequently, by Corollary 1.2 and Remark 1.3 it is enough to determine whether  $T \in 2E(\mathbb{F}_\ell)$  for the primes  $\ell = 11, 43$  (the prime divisors of  $d = 473$ ). We find that  $T \in 2E(\mathbb{F}_{11})$  and  $T \in 2E(\mathbb{F}_{43})$ . This is easily verified, e.g., using MAGMA. It follows that  $T$  lies in the image of a local trace map for every prime of  $\mathbb{Q}$ .

In addition, we find

$$R = (-2305909614/4489, 4756157028/300763) \in E^d(\mathbb{Q}) \setminus (2E^d(\mathbb{Q}) + E^d(\mathbb{Q})_2)$$

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

**Example 1.9.** Consider the elliptic curve  $E : y^2 + xy + y = x^3 - 12x - 16$ <sup>2</sup> and  $K = \mathbb{Q}(\sqrt{73})$ . We have that

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

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

Using Corollary 1.2 and Remark 1.3 we verify that the point  $T = (-9/4, 5/8) \in E(\mathbb{Q})_2$  lies in the image of the local trace map for every prime of  $\mathbb{Q}$ . We choose

$$R = (26499, 4028724) \in E^d(\mathbb{Q}),$$

---

<sup>1</sup>The Cremona label for this elliptic curve is **14a5**.

<sup>2</sup>The Cremona label for this elliptic curve is **82a2**.

which together with  $\iota(T)$  generates  $E^d(\mathbb{Q})$ . Then we verify that  $R$  and  $R + \iota(T)$  are not in  $2E^d(\mathbb{K})$ . Since we also have that  $E(\mathbb{K})_2 = E(\mathbb{Q})_2$ , by Proposition 1.7 we deduce that  $T$  is not a global trace and consequently the local-global trace principle fails for  $E(\mathbb{Q})_2$ .

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

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

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

Using Corollary 1.2 and Remark 1.3 we verify that the non-trivial point  $T = (1, 0) \in E(\mathbb{Q})_2$  is a local trace for every prime of  $\mathbb{Q}$ . We choose

$$R = (-19388, 306656) \in E^d(\mathbb{Q})$$

such that it generates  $E^d(\mathbb{Q})/E^d(\mathbb{Q})_2$ , and verify that  $(R + E^d(\mathbb{Q})_2) \cap 2E^d(\mathbb{K}) = \emptyset$ . Hence, Proposition 1.7 implies that  $T$  is not a global trace and the local-global trace principle fails for  $E(\mathbb{Q})_2$ .

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

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

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

$$\tilde{\iota} : E^d(\mathbb{F}) \oplus E(\mathbb{F})/E(\mathbb{F})_2 \longrightarrow \left( E^d(\mathbb{K})/2E^d(\mathbb{K}) \right)^{\text{Gal}(\mathbb{K}/\mathbb{F})},$$

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

$$\text{coker } \pi_1 \simeq \tilde{\iota}(E(\mathbb{F}))/\tilde{\iota}(E^d(\mathbb{F}))$$

and in particular the map  $\iota$  induces a surjection of  $E(\mathbb{F})/(2E(\mathbb{F}) + E(\mathbb{F})_2)$  onto  $\text{coker } \pi_1$ .

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

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

Observe that  $c_S$  maps to  $b_S$  under the restriction map

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

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

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

$$H^1(\mathbb{K}/\mathbb{F}, E^d(\mathbb{K}))/\text{im} \left( H^1(\mathbb{K}/\mathbb{F}, E^d(\mathbb{K})_2) \rightarrow H^1(\mathbb{K}/\mathbb{F}, E^d(\mathbb{K})) \right),$$

---

<sup>3</sup>The Cremona label for this elliptic curve is 96a1.

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

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

$$d_{\iota(P)} \in \text{III}(\text{E}^d/\text{F}) + \text{im}(\text{H}^1(\text{K}/\text{F}, \text{E}^d(\text{K})_2) \rightarrow \text{H}^1(\text{F}, \text{E}^d))$$

*if and only if the kernel of the map*

$$\text{E}(\text{F}) \rightarrow \prod_v \text{E}(\text{F}_v) / \text{tr}_{\text{K}_v/\text{F}_v} \text{E}(\text{K}_v)$$

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

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

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

*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  $\text{E}(\text{F})_2$  implies that the map  $\delta : \ker \psi \rightarrow \text{coker } \pi_1$  is injective. Consequently,  $P$  is a global trace if and only if  $\delta(P) = 0$ . Since  $\delta(P) = \tilde{\iota}(P) \in \text{coker } \pi_1$  it follows that  $P$  is a global trace if and only if  $\iota(P) \in 2\text{E}^d(\text{K}) + \text{E}^d(\text{F})$ . □

**Example 1.13.** Consider the elliptic curve  $\text{E} : y^2 + xy = x^3 + 4x + 1$ <sup>4</sup> and  $\text{K} = \mathbb{Q}(\sqrt{-311})$ . Then

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

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

Let  $T = (-1/4, 1/8) \in \text{E}(\mathbb{Q})_2$  and  $S = (1, 2) \in \text{E}(\mathbb{Q})$  such that  $\text{E}(\mathbb{Q}) = \langle T, S \rangle$ . Since  $T, S \in 2\text{E}(\mathbb{R})$  and  $T, S \in 2\text{E}(\mathbb{F}_{311})$ , 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  $\text{E}^d(\mathbb{Q})/2\text{E}^d(\mathbb{Q})$ , we find

$$P_1 = (98587, -31724488) \in \text{E}^d(\mathbb{Q}) \setminus (2\text{E}^d(\mathbb{Q}) + \text{E}^d(\mathbb{Q})_2)$$

such that  $P_1 \in 2\text{E}^d(\text{K})$ , which by Proposition 1.7 implies that  $T$  is a global trace. Therefore, the local-global trace condition holds for  $\text{E}(\mathbb{Q})_2$ . Moreover, we also find

$$P_2 = (2271, -455220) \in \text{E}^d(\mathbb{Q}) \setminus (2\text{E}^d(\mathbb{Q}) + \text{E}^d(\mathbb{Q})_2)$$

such that  $\iota(S) + P_2$  is 2-divisible in  $\text{E}^d(\text{K})$ . Then by Proposition 1.12 we deduce that  $S$  is also a global trace. Hence, the local-global trace principle holds for  $\text{E}(\mathbb{Q})$ .

---

<sup>4</sup>The Cremona label for this elliptic curve is 65a2.

2. TWISTS OF GENUS ONE CURVES

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

$$\text{Aut}(E) \simeq \text{Aut}(E, O) \times E(\overline{F})$$

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

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

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

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

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

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

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

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

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

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

Hence, the map  $\theta$  gives the following isomorphism:

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

□

We would like to be able to determine whether  $E_{K,S}$  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,  $S \in E(F)$ , and  $E_{K,S}/F$  the corresponding twist of  $E$ . Then*

- a)  $E_{K,S}$  has an  $F$ -rational point if and only if  $S$  is a global trace.
- b)  $E_{K,S}$  has a point defined over  $F_v$  if and only if  $S$  lies in the image of the trace map  $\text{tr}_{K_\nu/F_\nu} : E(K_\nu) \rightarrow E(F_\nu)$ , where  $\nu$  denotes a prime of  $K$  above a prime  $v$  of  $F$ .

Moreover, if  $E_{K,S}$  has a point defined over  $F$  (resp. over  $F_v$ ), then  $E_{K,S}$  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  $E_{K,S}(F)$  is non-empty if and only if  $\zeta_{K,S}$  is cohomologous to  $\zeta_{K,O}$  in which case  $E_{K,S}$  is isomorphic over  $F$  to the quadratic twist  $E^d$ .

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

$$\begin{aligned} \varphi^\tau \zeta_{K,S}(\tau) &= (-1, \tau P)(-1, S) = (1, \tau P - S), \\ \zeta_{K,O}(\tau)\varphi &= (-1, O)(-1, P) = (1, -P). \end{aligned}$$

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

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

$$\begin{aligned} \varphi^\sigma \zeta_{K,S}(\sigma) &= (\pm 1, \sigma P)(1, O) = (\pm 1, \sigma P), \\ \zeta_{K,O}(\sigma)\varphi &= (1, O)(\pm 1, P) = (\pm 1, P). \end{aligned}$$

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

Part (b) is trivially true if  $v$  splits in  $K/F$  since  $E_{K,S}(K)$  is non-empty, 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 gives the following result.

**Theorem 2.4.** *Let  $K/F$  be a quadratic extension and  $S \in E(F)$ . Assume that the corresponding genus one curve  $E_{K,S}/F$  has a local point over  $F_v$  for all primes  $v$ . Then  $E_{K,S}(F)$  is non-empty if either of the following is true:*

- i)  $S \in (2E(F) + E(F)_2) \setminus 2E(F)$  and
  - a) if  $E(F)_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , then  $K/F$  is ramified at some infinite prime;
  - b)  $E(K)_2 \neq E(F)_2$  or  $2E^d(F) \neq E^d(F) \cap 2E^d(K)$ .
- ii)  $S \in E(F) \setminus (2E(F) + E(F)_2)$  and
  - a) the local-global trace principle holds for  $E(F)_2$ ,
  - b)  $\iota(S) \in 2E^d(K) + E^d(F)$ .

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

- In Example 1.8,  $E_{K,T}(\mathbb{Q}) \neq \emptyset$  for  $K = \mathbb{Q}(\sqrt{473})$  and every  $T \in E(\mathbb{Q})_2$ .
- In Example 1.9, for  $K = \mathbb{Q}(\sqrt{73})$  and  $T \in E(\mathbb{Q})_2 \setminus \{O\}$  we find that  $E_{K,T}(\mathbb{Q}_v) \neq \emptyset$  for every prime  $v$ , but  $E_{K,T}$  has no rational points.
- In Example 1.10,  $E(\mathbb{Q})_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  and for  $K = \mathbb{Q}(\sqrt{-407})$  there is a unique non-trivial  $T \in E(\mathbb{Q})_2$  such that  $E_{K,T}(\mathbb{Q}_v) \neq \emptyset$  for every prime  $v$ ; however  $E_{K,T}(\mathbb{Q}) = \emptyset$  for every  $T \in E(\mathbb{Q})_2 \setminus \{O\}$ .
- In Example 1.13,  $E_{K,T}(\mathbb{Q}) \neq \emptyset$  for  $K = \mathbb{Q}(\sqrt{-311})$  and every  $T \in E(\mathbb{Q})$ .

One interesting application of the above theorem is in the study of rational points on twists of genus one modular curves. For  $K = \mathbb{Q}(\sqrt{d})$ , the twist  $X^d(N)$  of the modular curve  $X_0(N)$  is constructed by Galois descent from  $X_0(N)/K$ . It is a

smooth proper curve over  $\mathbb{Q}$ , isomorphic to  $X_0(N)$  over  $K$  but not over  $\mathbb{Q}$ . The action of  $\tau \in \text{Gal}(K/\mathbb{Q})$  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  $K = \mathbb{Q}(\sqrt{d})$ . A  $\mathbb{Q}$ -curve of degree  $N$  over  $K = \mathbb{Q}(\sqrt{d})$  is an elliptic curve defined over  $K$  which is isogenous to its Galois conjugate over  $K$  via an isogeny  $\phi$  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  $w_N = (-1, S) \in \text{Aut}(X_0(N))$  for some  $S \in X_0(N)(\mathbb{Q})$ . Therefore, given a quadratic field  $K = \mathbb{Q}(\sqrt{d})$ , the corresponding twist  $X^d(N)$  equals  $X_0(N)^{\zeta_{K,S}}$ . 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  $X_0(14) : y^2 + xy + y = x^3 + 4x - 6$ . We have that  $E(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$  and  $w_{14} = (-1, S) \in \text{Aut}(X_0(14))$  for  $S = (9, 23) \in E(\mathbb{Q})$  which is a point of order 6.

Consider the quadratic field  $K = \mathbb{Q}(\sqrt{17})$ . 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  $E^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ , where  $d = 17$ . We find that there exists a point

$$P = (10897/16, -473671/64) \in E^d(\mathbb{Q}) \setminus (2E^d(\mathbb{Q}) + E^d(\mathbb{Q})_2)$$

such that  $P \in 2E^d(K)$ . Then by Theorem 2.4(i) we deduce that  $E_{K,S}(\mathbb{Q}) = X^{17}(14)(\mathbb{Q}) \neq \emptyset$ , 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  $X_0(15) : y^2 + xy + y = x^3 + x^2 - 10x - 10$ . Then  $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ , and  $w_{15} = (-1, S) \in \text{Aut}(X_0(15))$  for  $S = (8, 18) \in E(\mathbb{Q})$  which is a point of order 4.

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

Since  $K/\mathbb{Q}$  is imaginary, at most one of the non-trivial 2-torsion points of  $E(\mathbb{Q})$  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  $E(\mathbb{Q})_2$ . Then we also find

$$R = (56247, 13204620) \in E^d(\mathbb{Q}) \setminus (2E^d(\mathbb{Q}) + E^d(\mathbb{Q})_2)$$

such that  $\iota(S) + R \in 2E^d(K)$ . Hence, by Theorem 2.4(ii) we deduce that  $E_{K,S}(\mathbb{Q}) = X^{-71}(15)(\mathbb{Q}) \neq \emptyset$ , 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  $X_0(17) : y^2 + xy + y = x^3 - x^2 - x - 14$ . We have that  $E(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$  and  $w_{17} = (-1, S) \in \text{Aut}(X_0(17))$  for  $S = (7, 13) \in E(\mathbb{Q})$  which is a point of order 4.

Consider  $K = \mathbb{Q}(\sqrt{19})$  and observe that  $E^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ , where  $d = 19$ . 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

$$R = (6993/4 : 145503/8) \in E^d(\mathbb{Q}) \setminus (2E^d(\mathbb{Q}) + E^d(\mathbb{Q})_2)$$

such that  $\iota(S) + R \in 2E^d(K)$ . Since in this case the local-global trace principle holds trivially for  $E(\mathbb{Q})_2$ , Theorem 2.4(ii) implies that  $E_{K,S}(\mathbb{Q}) = X^{19}(17)(\mathbb{Q}) \neq \emptyset$ . 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  $X_0(21) : y^2 + xy = x^3 - 4x - 1$ . Then  $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$  and  $w_{21} = (-1, S) \in \text{Aut}(X_0(21))$  for  $S = (5, 8) \in E(\mathbb{Q})$  which is a point of order 4.

Consider  $K = \mathbb{Q}(\sqrt{-47})$  and observe that  $E^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ , where  $d = -47$ . The primes 2, 3, 7 split in  $K/\mathbb{Q}$ , and we verify that  $S \in 2E(\mathbb{R})$  and  $S \in 2E(\mathbb{F}_{47})$ . Then Corollary 1.2 and Remark 1.3 imply that  $S$  is a local trace for all primes of  $\mathbb{Q}$ . Hence,  $E_{K,S}(\mathbb{Q}_v) = X^{-47}(21)(\mathbb{Q}_v) \neq \emptyset$  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  $E(\mathbb{Q})_2$ . Then we proceed to find

$$R = (-187953/121, 175350420/1331) \in E^d(\mathbb{Q}) \setminus (2E^d(\mathbb{Q}) + E^d(\mathbb{Q})_2)$$

such that  $\iota(S) + R \in 2E^d(K)$ . Hence, by Theorem 2.4(ii) we deduce that  $E_{K,S}(\mathbb{Q}) = X^{-47}(21)(\mathbb{Q}) \neq \emptyset$ , which implies the existence of a  $\mathbb{Q}$ -curve of degree 21 defined over  $\mathbb{Q}(\sqrt{-47})$ .

## REFERENCES

- [DZ] Roberto Dvornicich and Umberto Zannier, *Local-global divisibility of rational points in some commutative algebraic groups* (English, with English and French summaries), Bull. Soc. Math. France **129** (2001), no. 3, 317–338. MR1881198 (2002k:14031)
- [El] Jordan S. Ellenberg,  *$\mathbb{Q}$ -curves and Galois representations*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 93–103. MR2058645 (2005g:11088)
- [Kn] Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR1193029 (93j:11032)
- [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, DOI 10.1007/s00222-010-0252-0. MR2660452 (2012a:11069)
- [Oz] Ekin Ozman, *Points on quadratic twists of  $X_0(N)$* , Acta Arith. **152** (2012), no. 4, 323–348, DOI 10.4064/aa152-4-1. MR2890545
- [Si] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005)

DEPARTMENT OF MATHEMATICS, RLM 8.100, UNIVERSITY OF TEXAS AT AUSTIN, 2515 SPEEDWAY STOP C1200, AUSTIN, TEXAS 78712-1202

*E-mail address:* mirela@math.utexas.edu

DEPARTMENT OF MATHEMATICS, RLM 8.100, UNIVERSITY OF TEXAS AT AUSTIN, 2515 SPEEDWAY STOP C1200, AUSTIN, TEXAS 78712-1202

*E-mail address:* ozman@math.utexas.edu