University of Groningen

Albime triangles over quadratic fields

Chahal, Jasbir S.; Top, Jaap

Published in:
Rocky mountain journal of mathematics

DOI:
10.1216/RMJ-2017-47-7-2095

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2017

Link to publication in University of Groningen/UMCG research database

Citation for published version (APA):
Chahal, J. S., & Top, J. (2017). Albime triangles over quadratic fields. *Rocky mountain journal of mathematics*, *47*(7), 2095–2106. https://doi.org/10.1216/RMJ-2017-47-7-2095

Copyright
Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

Take-down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): http://www.rug.nl/research/portal. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Download date: 01-12-2020

ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 47, Number 7, 2017

ALBIME TRIANGLES OVER QUADRATIC FIELDS

JASBIR S. CHAHAL AND JAAP TOP

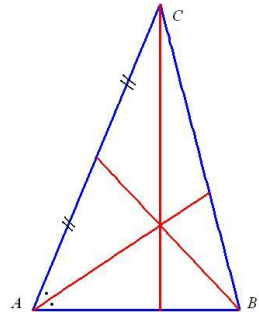
ABSTRACT. This note uses a diophantine problem arising in elementary geometry as a prerequisite to illustrate some theory of elliptic curves. As a typical example, Proposition 2.4 and Theorem 3.1 determine the exact set of rational numbers for which the specialization homomorphism from the torsion free rank 2 group of rational points on some elliptic curve over $\mathbb{Q}(t)$, is well defined and injective.

1. Introduction. The motivation for the present note is the following.

Definition 1.1. Let $K \subset \mathbb{R}$ be a field. A triangle ABC is called K-*albime* if the altitude from vertex C, the internal bisector of angle A and the median from vertex B are concurrent and, moreover, the lengths

$$a = |BC|, \qquad b = |AC|, \qquad c = |AB|$$

satisfy $a, b, c \in K$.



2010 AMS *Mathematics subject classification.* Primary 11D25, 11G05, 14G05, 97G40.

Keywords and phrases. Elliptic curve, quadratic twist, specialization map, Chabauty method, elementary geometry.

Received by the editors on May 26, 2016.

DOI:10.1216/RMJ-2017-47-7-2095 Copyright ©2017 Rocky Mountain Mathematics Consortium

In [**1**], some history and basic properties of albime triangles are given. As far as is known, the first one who mentioned triangles with the given property was New York Evander Childs High School teacher, David L. MacKay (1887–1961) [**10**] in 1937. The same MacKay [**11**] asked in 1939 for a classification of what we call here the $\mathbb{Q}$-albime triangles. The earliest nontrivial example of a $\mathbb{Q}$-albime triangle was given in 1991 by Hoyt [**9**]. More examples were found by Guy in 1995, whose paper [**7**] rephrases the problem in terms of rational points on a certain elliptic curve.

Let $\mathcal{S}$ be the set of equivalence classes of similar triangles. Clearly, 'albime' is a property of a class in $\mathcal{S}$. Suppose that $K \subset \mathbb{R}$ is a field. By $\mathcal{A}(K) \subset \mathcal{S}$, we denote the set of equivalence classes containing a K-albime triangle. We shall identify a given equivalence class with any of its members. Let E be "Guy's favourite elliptic curve" (see [**1, 7**]) over $\mathbb{Q}$ with equation $y^2 = x^3 - 4x + 4$. Write $I(K) \subset E(K)$ for the subset of K-rational points (x, y) such that $0 < x < 2$ and $y > 0$. A straightforward generalization of [**1,** Theorems 2.1, 3.2 (a)] is the following.

Theorem 1.2. *The map*

$$\Delta : I(K) \longrightarrow \mathcal{A}(K)$$

given by $\Delta(c, a)$ *is the triangle with side lengths* $a,\ b = 2 - c,$ *and* c *is bijective.*

Since every $\mathcal{A}(K)$ contains $\mathcal{A}(\mathbb{Q})$, and the latter set is infinite by [**1,** Theorem 3.2 (c)], every $\mathcal{A}(K)$ is infinite as well. In this text, we restrict to real quadratic fields K. As an example, it is not difficult to show that $I(\mathbb{Q}) = I(\mathbb{Q}(\sqrt{d}))$, for $d \in \{2, 3, 5, 6\}$. Therefore, up to similarity, for these values of d, no new albime triangles appear if lengths rather than only rational lengths are allowed in $\mathbb{Q}(\sqrt{d})$. On the other hand, starting from any rational r with $0 < r < 2$ such that $d := r^3 - 4r + 4$ is not a square in $\mathbb{Q}$, the 'new' $\mathbb{Q}(\sqrt{d})$-albime triangle is clearly obtained with sides $(\sqrt{d}, 2 - r, r)$.

Studying K-albime triangles is equivalent to studying the subset $I(K)$ of $E(K)$. Since, compare [**1,** Section 5], every point of infinite order in $E(K)$ generates a dense and equidistributed subgroup of $E(\mathbb{R})$, this essentially reduces a study of K-albime triangles to a study of the

group $E(K)$. Although much is known about the group of points over a quadratic extension on an elliptic curve over a given field, we take the opportunity to expose some of this theory by illustrating it in the special case related to K-albime triangles. Specifically, the main results of this paper are Theorem 3.1 and its corollary. These present an explicit family of real quadratic fields K such that K-albime triangles exist which are not $\mathbb{Q}$-albime.

2. Guy's elliptic curve over quadratic fields. In this section, $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$ denotes a quadratic field. Let E be the elliptic curve given by $y^2 = x^3 - 4x + 4$. Now, we present some results on the group $E(K)$.

Lemma 2.1. *For any quadratic field K, the group $E(K)$ is torsion free of finite rank.*

Proof. The fact that the group has finite rank is a special case of the Mordell-Weil theorem which states that this holds for any elliptic curve over any number field, see, e.g., [**14,** Chapter 13, Theorem 6.7] or [**18**]. In the present case, it can also be seen as follows. Write $K = \mathbb{Q}(\sqrt{d})$, and set

$$E^{(d)} : dy^2 = x^3 - 4x + 4.$$

This $E^{(d)}$ is an elliptic curve which is isomorphic to E; indeed, the map $\iota(x, y) := (x, y/\sqrt{d})$ defines an isomorphism

$$\iota : E \xrightarrow{\sim} E^{(d)}.$$

In the theory of elliptic curves, $E^{(d)}$ is the *quadratic twist* over $K/\mathbb{Q}$ of the curve E, compare, e.g., [**14,** Chapter 10, Section 5].

Let σ be the nontrivial automorphism of the field K; thus, $\sigma(\sqrt{d}) = -\sqrt{d}$. This defines an automorphism

$$P \longmapsto P^\sigma$$

of the group $E(K)$ where P^σ means that σ is applied to all coordinates of the point $P \in E(K)$. Define a homomorphism of groups

$$\mu : E(K) \longrightarrow E(\mathbb{Q}) \oplus E^{(d)}(\mathbb{Q})$$

by $\mu(P) := (P + P^\sigma, \iota(P - P^\sigma))$. Here, the fact that $P + P^\sigma$ and $\iota(P - P^\sigma)$ are defined over $\mathbb{Q}$ follows from the observation that they are invariant under the action of σ. In addition, the simple observation that the diagram of isomorphisms

$$\begin{array}{ccc} E(K) & \stackrel{\iota}{\longrightarrow} & E^{(d)}(K) \\ \sigma \downarrow & & \downarrow \sigma \\ E(K) & \underset{-\iota}{\longrightarrow} & E^{(d)}(K) \end{array}$$

commutes may be used. Next, μ is injective since, if P is in the kernel of μ, then $-P = P^\sigma = P$; hence, $P \in E(\mathbb{Q})$ is a point of order dividing 2. Since $E(\mathbb{Q})$ contains no points of order 2 (the polynomial $X^3 - 4X + 4$ is irreducible over $\mathbb{Q}$), injectivity of μ follows.

This argument shows that $E(K)$ can be regarded as a subgroup of $E(\mathbb{Q}) \oplus E^{(d)}(\mathbb{Q})$. The latter group is finitely generated (using Mordell's **[13]** result), hence, so is $E(K)$.

In order to show that $E(K)$ is torsion free, the injective map μ is again used. First, it clearly suffices to show that $E(K)$ contains no point of prime order p. Now, let p be a prime number, and assume that $P \in E(K)$ has order p. Write $\mu(P) = (Q, R)$. Since μ is injective, (Q, R) has order p as well. This implies that $Q = O$ since $E(\mathbb{Q})$ contains no nontrivial torsion point. Hence, $P = -P^\sigma$ by the definition of μ. This means that the x-coordinate $x(P)$ of the point P is in $\mathbb{Q}$. Moreover, $Q = O$ implies that P and R have the same order, which is p. Thus, $R \in E^d(\mathbb{Q})$ is a point of order p. From a well-known result of Mazur **[12]** on torsion points of elliptic curves over $\mathbb{Q}$, this implies

$$p \in \{2, 3, 5, 7\}.$$

The possibilities are considered next.

Clearly, $p = 2$ is not possible since this would imply that $P = (x(P), 0)$ is in $E(\mathbb{Q})$. If $p = 3$, then $x(P)$ would be a rational zero of the 3-division polynomial of E (a polynomial having all x-coordinates of all points of order 3 as its zeros, see **[17,** subsection 3.2]**)**

$$\psi_3 = 3X^4 - 24X^2 + 48X - 16.$$

This polynomial is irreducible (its reciprocal is an Eisenstein polynomial for the prime 3); hence, $x(P) \in \mathbb{Q}$ cannot be a zero. A similar

argument eliminates the primes 5 and 7. Indeed,

$$\psi_5 = 5X^{12} - 248X^{10} + 1520X^9 - 1680X^8 - 3840X^7 + 15360X^6 - 44544X^5 + 90880X^4 - 81920X^3 - 10240X^2 + 61440X - 28672,$$

which is irreducible (modulo 3). The polynomial ψ_7 of degree 24 is irreducible since it is modulo 5. This completes the proof. □

The argument presented above suggests that, in order to find (real) quadratic fields $K = \mathbb{Q}(\sqrt{d})$ such that $E(K)$ properly contains $E(\mathbb{Q})$, quadratic twists $E^{(d)}$ should be searched for such that $E^{(d)}(\mathbb{Q})$ is nontrivial. Given any quadratic field $K = \mathbb{Q}(\sqrt{d})$, define

$$\lambda : E(\mathbb{Q}) \oplus E^{(d)}(\mathbb{Q}) \longrightarrow E(K)$$

by $\lambda(Q, R) := Q + \iota^{-1}(R)$. It can easily be verified that $\mu \circ \lambda$ is multiplication by 2 on $E(\mathbb{Q}) \oplus E^{(d)}(\mathbb{Q})$, which is an injective map. Hence, λ is injective as well. Lemma 2.1 implies that, for every $d \in \mathbb{Q}^\times$, which is not a square (and obviously also for square d), the group $E^{(d)}(\mathbb{Q})$ is torsion free.

We now briefly discuss two well-known methods for constructing many d such that $E^{(d)}(\mathbb{Q})$ is nontrivial. Both are based upon the simple idea of finding a suitable polynomial $d(t)$ and then considering

$$E^{(d(t))} : d(t)y^2 = x^3 - 4x + 4,$$

an elliptic curve over the function field $\mathbb{Q}(t)$. If $E^{(d(t))}(\mathbb{Q}(t))$ contains a point $P \neq O$, then specializing the variable t to a rational number t_0 will, in general, give a quadratic twist of E with a nontrivial rational point. By varying t_0, the existence of infinitely many such twists may be proved. This method is explained in **[15]**. Here, we specialize the above-mentioned to the present situation.

Proposition 2.2. *Let $d(t) \in \mathbb{Q}[t]$ be a polynomial not of the form a constant times a square. The group $E^{(d(t))}(\mathbb{Q}(t))$ is torsion free of finite rank equal to the rank of $\mathrm{Mor}_{\mathbb{Q}}(C, E)/E(\mathbb{Q})$, where C is the hyperelliptic curve over $\mathbb{Q}$, defined by the equation*

$$y^2 = d(x),$$

and $E(\mathbb{Q})$ is regarded as the subgroup of constant morphisms in the group $\mathrm{Mor}_{\mathbb{Q}}(C, E)$ of morphisms defined over $\mathbb{Q}$ from C to E.

Proof. The function field $\mathbb{Q}(C)$ of C is the quadratic extension $\mathbb{Q}(t,s)$ of $\mathbb{Q}(t)$ defined by $s^2 = d(t)$. Any point $R = (\alpha, \beta) \in E(\mathbb{Q}(C))$ can be identified with a morphism

$$\varphi_R : C \longrightarrow E,$$

given by $\varphi_R(x,y) = (\alpha(x,y), \beta(x,y))$. Furthermore, analogous to the reasoning in the proof of Lemma 2.1, $E^{(d(t))}(\mathbb{Q}(t))$ can be regarded as a subgroup of $E(\mathbb{Q}(C))$. As a consequence, $E^{(d(t))}(\mathbb{Q}(t))$ can be identified with a subgroup of the group $\mathrm{Mor}_{\mathbb{Q}}(C,E)$ of all morphisms defined over $\mathbb{Q}$ from C to E. In fact, the identified subgroup consists of all morphisms π which satisfy $\pi \circ h = [-1] \circ \pi$, where h is the hyperelliptic involution

$$(x,y) \longmapsto (x,-y) \quad \text{on } C.$$

Any nonconstant morphism between curves is known to be surjective (over an algebraic closure). If a nontrivial point in $E^{(d(t))}(\mathbb{Q}(t))$ has finite order n, then the corresponding morphism $C \to E$ would have its image in the n-torsion subgroup of E. As a result, this map is constant, and, since the morphism is defined over $\mathbb{Q}$, it maps all of C to a point of order n in $E(\mathbb{Q})$. However, $E(\mathbb{Q})$ is torsion free, which also shows that $E^{(d(t))}(\mathbb{Q}(t))$ is torsion free.

The statement concerning rank is verified as follows. Let σ be the nontrivial automorphism of $\mathbb{Q}(C)$ over $\mathbb{Q}(t)$ and

$$\iota : E \longrightarrow E^{d(t)}$$

the isomorphism analogous to that used earlier. The homomorphism

$$\mathrm{Mor}_{\mathbb{Q}}(C,E) = E(\mathbb{Q}(C)) \longrightarrow E^{d(t)}(\mathbb{Q}(t)),$$

given as

$$P \longmapsto \iota(P - \sigma(P)),$$

has kernel $E(\mathbb{Q}(t)) = \mathrm{Mor}_{\mathbb{Q}}(\mathbb{P}^1, E) = E(\mathbb{Q})$. The homomorphism maps $\iota^{-1}(E^{(d(t))}(\mathbb{Q}(t)))$ onto $2E^{(d(t))}(\mathbb{Q}(t))$, which has finite index in $E^{(d(t))}(\mathbb{Q}(t))$. Hence, indeed, $E^{(d(t))}(\mathbb{Q}(t))$ and $\mathrm{Mor}_{\mathbb{Q}}(C,E)/E(\mathbb{Q})$ have equal rank. □

The first and simplest example illustrating Proposition 2.2 in the case of Guy's elliptic curve is to take

$$d(t) := t^3 - 4t + 4,$$

in which case the point $(t, 1)$ is in $E^{(d(t))}(\mathbb{Q}(t))$.

Proposition 2.3. *For $d(t) := t^3 - 4t + 4$, the group $E^{(d(t))}(\mathbb{Q}(t))$ is infinite cyclic with $(t, 1)$ as a generator.*

Proof. In the case under consideration, $C = E$; thus, we consider morphisms $\varphi : E \to E$ defined over $\mathbb{Q}$ with $-\varphi = \varphi \circ [-1]$. Set $R := \varphi(O) \in E(\mathbb{Q})$. Applying the condition on φ to O gives $-R = R$. Since $E(\mathbb{Q})$ is torsion free, $R = O$. Therefore, φ is an endomorphism of E defined over $\mathbb{Q}$. It is well known that any endomorphism π of an elliptic curve E, with π and E both defined over $\mathbb{Q}$, is multiplication by an integer n. This group of endomorphisms is generated by the identity map, which, in this case, equals φ_P for $P = (t, 1)$. This proves Proposition 2.3. □

A second example follows.

Proposition 2.4. *Let*

$$d(t) := (t^2 + t + 1)(t^6 + 7t^5 + 16t^4 + 7t^3 - 4t^2 - t + 1).$$

The group $E^{(d(t))}(\mathbb{Q}(t))$ is torsion free of rank 2, with

$$P := \left(\frac{-4t - 2}{t^2 + t + 1}, \frac{2}{(t^2 + t + 1)^2} \right)$$

and

$$Q := \left(\frac{-2t^2 + 2}{t^2 + t + 1}, \frac{2}{(t^2 + t + 1)^2} \right)$$

as generators.

Proof. Part of this follows from [**15,** Theorem 4]. Indeed, with notation as in loc. cit., taking $a = -2$ and $c = 0$ gives the polynomial $d(t)$ and the points P, Q.[1] The cited result shows that P and Q are independent. The group $E^{(d(t))}(\mathbb{Q}(t))$ is torsion free by Proposition 2.2.

It remains to show that $E^{(d(t))}(\mathbb{Q}(t))$ has rank 2 with P, Q as its generators. Using `Magma`, it can be verified that C and E have good reduction at 5, and the characteristic polynomial of Frobenius at 5 acting on the Tate module of the Jacobian of C equals $(T^2+3T+5)^2 \times (T^2+5)$. The same calculation for the elliptic curve E yields the polynomial T^2+3T+5. As a consequence (compare **[16]**), the rank of $E^{(d(t))}(\mathbb{Q}(t))$ is at most 2. Therefore, it equals 2.

Finally, consider the maps φ_P, φ_Q from C to E associated with the points P, Q. It may be verified that both maps have degree 2. Moreover,

$$R \longmapsto \deg(\varphi_R)$$

defines the canonical height on the group $E^{(d(t))}(\mathbb{Q}(t))$. A calculation shows that the x-coordinate of $P+Q$ is $(2t(2+t))/(1+t+t^2)$; hence, φ_{P+Q} has degree 2. Therefore, the height pairing satisfies $\langle P, P\rangle = \langle Q, Q\rangle = 2$ and $\langle P, Q\rangle = -1$. This means that $E^{(d(t))}(\mathbb{Q}(t))$, equipped with the height pairing, is an integral lattice of rank 2. It has a sublattice equal to the root lattice A_2, defined as the lattice of all points in $\mathbb{Z}^3$ having coordinate sum 0, equipped with the standard Euclidean inner product. The observation that A_2 is not properly contained in any rank 2 integral lattice completes the proof. □

3. Examples of albime triangles over quadratic fields. Proposition 2.4 is particularly suitable for constructing K-albime triangles: the given polynomial $d(t)$ satisfies $d(\xi) > 0$ for all $\xi \in \mathbb{R}$. Bruin explained, using his `Magma` implementation of the Chabauty method for hyperelliptic curves, that $d(t_0)$ is a rational square only if

$$t_0 \in \{-1, 0, 1, -2, -1/2\}.$$

For any rational t_0 not in this finite set, $\mathbb{Q}(\sqrt{d(t_0)})$ is a real quadratic field and $E' := E^{(d(t_0))}$ is a nontrivial twist of E. As was shown in Lemma 2.1, $E'(\mathbb{Q})$ is torsion free. Specializing P and Q to points P', Q' yields two nontrivial points; thus, $E'(\mathbb{Q})$ is free of positive rank. Independence of P', Q' for any particular value of $t = t_0$ is tested as follows.

Let θ denote a zero of $x^3 - 4x + 4$, and set $L := \mathbb{Q}(\theta)$, which is a degree 3 field extension of $\mathbb{Q}$. Define $\alpha(t),\ \beta(t) \in L(t)^\times$ as

$$\alpha(t) := \left(\frac{-4t-2}{t^2+t+1} - \theta\right) d(t) \quad \text{and} \quad \beta(t) := \left(\frac{-2t^2+2}{t^2+t+1} - \theta\right) d(t).$$

This yields a commutative diagram:

$$\begin{array}{ccc} E^{(d(t))}(\mathbb{Q}(t)) & \longrightarrow & L(t)^\times/L(t)^{\times 2} \\ \downarrow & & \downarrow \\ \mathbb{Z}\cdot P' + \mathbb{Z}\cdot Q' & \longrightarrow & L^\times/L^{\times 2}. \end{array}$$

Here, the vertical maps are obtained by specializing t to t_0; the upper horizontal map is defined by

$$mP + nQ \longmapsto \alpha(t)^m\beta(t)^n L(t)^{\times 2}.$$

The lower horizontal map is the restriction to the subgroup generated by P', Q' of the homomorphism

$$E'(\mathbb{Q}) \longrightarrow L^\times/L^{\times 2} : (a,b) \longmapsto d(t_0)(a-\theta)L^{\times 2}.$$

It is a classical result that this defines a homomorphism. Indeed, the basic tools for this are already present in Mordell's paper [**13,** Sections 5, 6]; for a precise statement and proof, see [**5,** Section 2].

A sufficient criterion for independence of P' and Q' is that their images in $L^\times/L^{\times 2}$ generate a noncyclic group. This is equivalent to the condition that none of $\alpha(t_0), \beta(t_0)$ or $\alpha(t_0)\beta(t_0)$ is a square in $L^\times$. Since $\mathbb{Z}[\theta]$ becomes a unique factorization domain, this condition is easy to test.

The set of rational numbers failing this test is found as follows. Define

$$\begin{array}{ll} C : y^2 = d(x), & C_\alpha : y^2 = \alpha(x), \\ C_\beta : y^2 = \beta(x), & C_{\alpha\beta} : y^2 = \alpha(x)\beta(x). \end{array}$$

The first is a curve over $\mathbb{Q}$, the others are defined over L. Set

$$\begin{aligned} S :&= \{\xi \in \mathbb{Q} : \text{there exists an } \eta \in \mathbb{Q} \text{ with } (\xi,\eta) \in C(\mathbb{Q})\} \\ &= \{-1, 0, 1, -2, -1/2\} \end{aligned}$$

(as computed by Bruin), and

$$T := \{\xi \in \mathbb{Q} : \text{there exists an } \eta \in L \text{ with } (\xi,\eta) \in C_\alpha(L) \cup C_\beta(L) \cup C_{\alpha\beta}(L)\}.$$

Using the `Magma` package, it can easily be verified that the curves C_α, C_β and $C_{\alpha\beta}$ have genus 1 and contain a point with coordinates in L. Hence, they define elliptic curves over L. The elliptic Chabauty

method implemented in `Magma`, introduced by Bruin and described, e.g., in [**4,** Section 7], is perfectly suited for computing the L-rational points on these curves with $\mathbb{Q}$-rational x-coordinate. The three elliptic curves over L are isomorphic and have torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The rank over L equals 1. Magma's elliptic Chabauty reveals that the only $\mathbb{Q}$-rational x-coordinate of a point in $C_\alpha(L)$ is $-1/2$, corresponding to $(-1/2, \pm 9(\theta^2+2\theta-4)/32)$. The same technique applied to $C_\beta(L)$ yields as x-coordinates $\{\pm 1\}$, coming from the points $(-1, \pm(\theta^2+2\theta-4)/2)$ and $(1, \pm 9(\theta^2+2\theta-4)/2)$. Finally, the only $\mathbb{Q}$-rational x-coordinates of points in $C_{\alpha\beta}(L)$ are $\{-2, 0\}$. These are derived from the points $(-2, \pm 81(\theta^2+\theta-2))$ and $(0, \pm(\theta^2+\theta-2))$.

As a consequence, we have determined *all* $t_0 \in \mathbb{Q}$ such that specialization at t_0 is injective:

Theorem 3.1. *Let*

$$d(t) := (t^2+t+1)(t^6+7t^5+16t^4+7t^3-4t^2-t+1)$$

and

$$E : y^2 = x^3 - 4x + 4.$$

For $t_0 \in \mathbb{Q}$, the specialization homomorphism

$$E^{(d(t))}(\mathbb{Q}(t)) \longrightarrow E^{(d(t_0))}(\mathbb{Q})$$

is injective precisely when $t_0 \notin \{-1, 0, 1, -2, -1/2\}$.

Note that the argument presented here allows determination of injectivity of the specialization homomorphism for all values $t_0 \in \mathbb{Q}$. Similar but simpler examples in this spirit were obtained by Hazama [**8**]. A recent discussion of this specialization may be found in a paper by Gusić and Tadić [**6**]. The present example illustrates that their work can be extended, resulting in more examples where it is possible to explicitly determine the set for which specialization is injective.

Corollary 3.2. *For Guy's elliptic curve*

$$E : y^2 = x^3 - 4x + 4$$

and

$$d(t) := (t^2+t+1)(t^6+7t^5+16t^4+7t^3-4t^2-t+1)$$

and every $t_0 \in \mathbb{Q} \setminus \{-1, 0, 1, -2, -1/2\}$*, the field* $K = \mathbb{Q}(\sqrt{d(t_0)})$ *is real quadratic and* $E(\mathbb{Q}(\sqrt{d(t_0)}))$ *is free of rank* ≥ 3*. In these cases, many* K*-albime triangles exist which are not* $\mathbb{Q}$*-albime.*

Indeed, the group $E(\mathbb{Q})$ is free of rank 1 with generator $(2, 2)$. The fact that the rank is 1 was already established during calculations in the early 1960s by Birch and Swinnerton-Dyer, leading to their famous conjecture. More precisely, it is the entry for $A = 4$, $B = -4$ in [**3,** Table 1]. According to the comments on the tables published in [**2,** pages 75–77], Nelson Stephens and James Davenport computed the generator while Nelson Stephens and Jacques Vélu determined the torsion subgroups of all curves in the tables, including the case at hand.

The method of the present paper shows that $(2, 2)$, together with

$$\left(\frac{-4t_0 - 2}{t_0^2 + t_0 + 1}, \frac{2\sqrt{d(t_0)}}{(t_0^2 + t_0 + 1)^2}\right) \quad \text{and} \quad \left(\frac{-2t_0^2 + 2}{t_0^2 + t_0 + 1}, \frac{2\sqrt{d(t_0)}}{(t_0^2 + t_0 + 1)^2}\right),$$

is a set of three independent points in $E(\mathbb{Q}(\sqrt{d(t_0)}))$.

Acknowledgments. We thank Nils Bruin for taking the time to compute and explain to us the fact that the only rational solutions (s, t) for the equation

$$s^2 = (t^2 + t + 1)(t^6 + 7t^5 + 16t^4 + 7t^3 - 4t^2 - t + 1)$$

are those with $t \in \{-1, 0, 1, -2, -1/2\}$. We also thank Andrew Bremner for pointing out an error in an earlier version of this manuscript, and the unknown referee of that same version for suggestions leading to stronger versions of our initial results.

ENDNOTES

1. Note the misprint in the proof of [**15,** Theorem 4]: the numerator of the y-coordinate of the given points should be 2, not 1.

REFERENCES

1. Erika Bakker, Jasbir S. Chahal and Jaap Top, *Albime triangles and Guy's favourite elliptic curve*, Expos. Math. **34** (2016), 82–94.

2. B.J. Birch and W. Kuyk, eds., *Modular functions of one variable*, IV, Lect. Notes Math. **476**, Springer, Berlin, 1975.

3. B.J. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves*, I, J. reine angew. Math. **212** (1963), 7–251.

4. Nils Bruin, *Some ternary Diophantine equations of signature* $(n, n, 2)$, in *Discovering mathematics with Magma*: *Reducing the abstract to the concrete*, Wieb Bosma and John Cannon, eds., Springer, Berlin, 2006.

5. Armand Brumer and Kenneth Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–743.

6. Ivica Gusić and Petra Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, J. Num. Th. **148** (2015), 137–152.

7. Richard K. Guy, *My favorite elliptic curve*: *A tale of two types of triangles*, The Amer. Math. Month. **102** (1995), 771–781.

8. Fumio Hazama, *The Mordell Weil group of certain abelian varieties defined over the rational function field*, Tôhoku Math. J. **44** (1992), 335–344.

9. John P. Hoyt, *Problem* E 3434, The Amer. Math. Month. **98** (1991), 365.

10. David L. MacKay, *Problem* E 263, The Amer. Math. Month. **44** (1937), 104.

11. _____, *Problem* E 374, The Amer. Math. Month. **46** (1939), 168.

12. Barry Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. **47** (1977), 33–186.

13. L.J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambr. Philos. Soc. **21** (1922), 179–192.

14. J.H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts Math. **106**, Springer, New York, 1986.

15. C.L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

16. J.T. Tate and I.R. Shafarevich, *The rank of elliptic curves*, Soviet Math. Dokl. **8** (1967), 917–920.

17. Lawrence C. Washington, *Elliptic curves*: *Number theory and cryptography*, Chapman & Hall/CRC, Boca Raton, 2003.

18. A. Weil, *Sur un théorème de Mordell*, Bull. Sci. Math. **54** (1930), 182–191.

Brigham Young University, Department of Mathematics, Provo, Utah 84602
Email address: **jasbir@math.byu.edu**

University of Groningen, Johann Bernoulli Institute, P.O. Box 407, 9700 AK Groningen, The Netherlands
Email address: **j.top@rug.nl**