When is a complex elliptic curve the product of two real algebraic curves?

J. Bochnak and J. Huisman
Department of Mathematics
Vrije Universiteit
De Boelelaan 1081a
1081 HV Amsterdam
The Netherlands

1 Introduction and the main results

It is well known that a complex elliptic curve E, considered as a real Lie group, is isomorphic to the product $S^1 \times S^1$ of two circles (cf. [4]). However, such a statement is not fully satisfactory, because it says nothing about the underlying real algebraic structure $E_{\mathbb{R}}$ of E. Recall that a complex projective variety $V \subseteq \mathbb{P}^n(\mathbb{C})$ can be, in the obvious way, considered as a real algebraic variety and, as such, will be denoted by $V_{\mathbb{R}}$. Of course, $\dim V_{\mathbb{R}} = 2 \dim V$. Moreover, $V_{\mathbb{R}}$ is an affine real algebraic variety (cf. [1] Proposition 3.4.8). (For the background material on real algebraic geometry, the reader may refer to the book [1]. By an *affine real algebraic variety* we mean a locally ringed space, isomorphic to an algebraic subset of $\mathbb{R}^n$, for some n, equipped with the sheaf of $\mathbb{R}$-valued regular functions; cf. [1] Chapter 3).

The underlying real algebraic surface $E_{\mathbb{R}}$ of a complex elliptic curve E is definitely not biregularly isomorphic to $S^1 \times S^1$. (Clearly, every regular mapping from $S^1 \times S^1$ into $E_{\mathbb{R}}$ is constant. Indeed, the existence of a nonconstant real regular mapping $\mathbb{P}^1(\mathbb{R}) \cong S^1 \to E_{\mathbb{R}}$ would imply the existence of a nonconstant complex regular mapping from $\mathbb{P}^1(\mathbb{C})$ into E, which is impossible; see Section 2). The aim of this paper is to answer the question: When is $E_{\mathbb{R}}$ biregularly isomorphic to the product of two real algebraic curves?

Before stating our results we need some preparation. Recall that a complex elliptic curve E is said to have *complex multiplication* if its ring of endomorphisms $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$, that is, $\mathrm{End}(E) \cong \mathbb{Z} + f\mathcal{O}_d$, for some strictly positive integers f, d, with d square free, where $\mathcal{O}_d$ is the ring of integers in the field $\mathbb{Q}(\sqrt{-d})$. The number

$$\delta(E) = \begin{cases} -f^2 d & \text{for } d \equiv 3 \mod 4 \\ -4f^2 d & \text{for } d \equiv 1, 2 \mod 4 \end{cases}$$

is called the *discriminant* of $\mathrm{End}(E)$.

Let $\mathrm{H}_1^{alg}(E_{\mathbb{R}}, \mathbb{Z}/2)$ be the subgroup of the homology group $\mathrm{H}_1(E_{\mathbb{R}}, \mathbb{Z}/2)$ which consists of all homology classes represented by real algebraic curves contained in $E_{\mathbb{R}}$ (cf. [1] Chapter 11).

Our main results are contained in the following three theorems.

Theorem 1 *Given a complex elliptic curve E, the following conditions are equivalent:*

(i) *The underlying real algebraic surface $E_{\mathbb{R}}$ of E is biregularly isomorphic to the product of two real algebraic curves.*

(ii) *E has complex multiplication and the discriminant $\delta(E)$ of $\mathrm{End}(E)$ is odd.*

(iii) $\mathrm{H}_1^{alg}(E_{\mathbb{R}}, \mathbb{Z}/2) = \mathrm{H}_1(E_{\mathbb{R}}, \mathbb{Z}/2)$.

Clearly, (i) $\Rightarrow$ (iii) is trivial, while (iii) $\Rightarrow$ (ii) is shown in [2]. We shall prove (ii) $\Rightarrow$ (i) in Section 3.

The variety $E_{\mathbb{R}}$ has the natural structure of a 2-dimensional real algebraic group (with the group structure inherited from E).

Theorem 2 *If $E_{\mathbb{R}}$ is biregularly isomorphic to the product $C_1 \times C_2$ of two real algebraic curves, then necessarily C_1 and C_2 are projective nonsingular cubics in $\mathbb{P}^2(\mathbb{R})$ (and hence are 1-dimensional real algebraic groups). A biregular isomorphism $C_1 \times C_2 \to E_{\mathbb{R}}$ can be chosen, which is a group isomorphism.*

The next task is to identify all (unordered) pairs of cubics C_1, C_2, such that the product $C_1 \times C_2$ is biregularly isomorphic to a given $E_{\mathbb{R}}$. First we have to recall a few facts about real cubic curves in $\mathbb{P}^2(\mathbb{R})$.

Given $\alpha \in \mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$, let $\tau_\alpha = \frac{1}{2}(1 + \alpha\sqrt{-1})$ and define

$$D_\alpha = \{[x : y : z] \in \mathbb{P}^2(\mathbb{R}) \mid zy^2 = 4x^3 - g_2(\tau_\alpha)xz^2 - g_3(\tau_\alpha)z^3\},$$

where, as usual, the $g_i(\tau_\alpha)$ are the numbers (in this case real) defined by

$$g_2(\tau_\alpha) = 60 \sum_{\omega \in \Lambda'_\alpha} \omega^{-4},\ g_3(\tau_\alpha) = 140 \sum_{\omega \in \Lambda'_\alpha} \omega^{-6},$$

where $\Lambda_\alpha = \mathbb{Z} + \mathbb{Z}\tau_\alpha$ is a lattice in $\mathbb{C}$, $\Lambda'_\alpha = \Lambda_\alpha \backslash \{0\}$. Each D_α is a nonsingular connected real cubic curve in $\mathbb{P}^2(\mathbb{R})$. Moreover, D_α and D_β are not biregularly isomorphic, whenever $\alpha \neq \beta$, and every nonsingular connected real cubic curve in $\mathbb{P}^2(\mathbb{R})$ is isomorphic to some D_α. Observe that the complexification $D_{\mathbb{C}} \subseteq \mathbb{P}^2(\mathbb{C})$ of every nonsingular real cubic $D \subseteq \mathbb{P}^2(\mathbb{R})$ (that is, the complex cubic defined by the same equation as D) is itself nonsingular. Denote by E_α the complexification of D_α. For each $\alpha \in \mathbb{R}^+$, $\alpha \neq 1$, there exists precisely one $\beta \in \mathbb{R}^+$, $\beta \neq \alpha$, such that E_α and E_β are isomorphic complex curves (one takes $\beta = 1/\alpha$). The corresponding real cubics D_α and D_β are then called *associated real cubics*. They play a special role in our investigations.

Theorem 3 *Let E be a complex elliptic curve with complex multiplication. Assume that the discriminant $\delta(E)$ of* End(E) *is odd. Then, for a pair of real algebraic curves C_1, C_2, the following conditions are equivalent:*

(i) *The product $C_1 \times C_2$ is biregularly isomorphic to $E_{\mathbb{R}}$.*

(ii) *$\{C_1, C_2\}$ is, up to biregular isomorphism, a pair of associated real cubics $\{D_\alpha, D_{1/\alpha}\}$, for some $\alpha = \sqrt{m/n}$, where m, n are coprime positive integers with $mn = -\delta(E)$.*

The next statement follows immediately from Theorem 3.

Corollary 4 *Let E be a complex elliptic curve with complex multiplication. Assume that $-\delta(E)$ is the product of powers of $k+1$ distinct odd primes. Then, up to isomorphism, there are precisely 2^k unordered pairs $\{C_1, C_2\}$ of real algebraic curves, such that $E_{\mathbb{R}}$ is biregularly isomorphic to $C_1 \times C_2$.*

Example 5. There exist, up to isomorphism, exactly 8 complex elliptic curves defined over $\mathbb{Q}$, such that their underlying real algebraic structure is biregularly isomorphic to the product of two real algebraic curves. Indeed, let

$$\Omega = \{3, 7, 11, 19, 27, 43, 67, 163\}$$

and consider $E_{\sqrt{k}}$, for k in Ω. It is known (cf. [4] p.233 or [5] p.192) that the curves $E_{\sqrt{k}}$ are the only complex elliptic curves defined over $\mathbb{Q}$ with complex

multiplication, such that the discriminants of their rings of endomorphisms are odd (in fact, one has $\delta(E_{\sqrt{k}}) = -k$). It follows from Theorem 3 that $(E_{\sqrt{k}})_{\mathbb{R}}$ is isomorphic to $D_{\sqrt{k}} \times D_{1/\sqrt{k}}$ (even as real algebraic groups), and that this presentation as a product is unique. □ □

Theorems 1 and 2 are proved in Section 3. Theorem 3 is proved in Section 4.

2 A convenient complexification of the underlying real algebraic structure

In this section we recall the construction of an intrinsic complexification of the underlying real algebraic structure of a complex algebraic variety, as described in [3] (essentially due to A. Weil).

A projective complex algebraic variety W together with an antiholomorphic involution σ will be said to be *defined over* $\mathbb{R}$. It is well known that if (W, σ) is defined over $\mathbb{R}$, then there exist a complex algebraic subvariety X of $\mathbb{P}^k(\mathbb{C})$, for some k, and a complex isomorphism $f: W \to X$ such that X is defined by polynomials with real coefficients, that is, $\sigma_k(X) = X$, where σ_k is the involution on $\mathbb{P}^k(\mathbb{C})$ given by complex conjugation, and $\sigma_k \circ f = f \circ \sigma$. Clearly, f maps the set $W_\sigma(\mathbb{R})$ of fixed points of σ, called the *real part* of (W, σ), onto $X \cap \mathbb{P}^k(\mathbb{R})$. Thus $W_\sigma(\mathbb{R})$ can be considered in the natural way as a real algebraic variety. In fact, $W_\sigma(\mathbb{R})$, or $W(\mathbb{R})$, when it is clear which involution σ is meant, is a real algebraic subvariety of $W_{\mathbb{R}}$. If $W_\sigma(\mathbb{R})$ is Zariski dense in W, then we say that W is a *complexification* of $W_\sigma(\mathbb{R})$.

Given a projective complex algebraic variety $V \subseteq \mathbb{P}^n(\mathbb{C})$, set $\overline{V} = \sigma_n(V)$. Observe that the mapping

$$\gamma_V: V \times \overline{V} \longrightarrow V \times \overline{V},$$

defined by $\gamma_V(x, y) = (\sigma_n(y), \sigma_n(x))$, is an antiholomorphic involution of $V \times \overline{V}$. Thus$(V \times \overline{V}, \gamma_V)$ is a projective complex algebraic variety defined over $\mathbb{R}$. Observe that its real part $(V \times \overline{V})(\mathbb{R})$ is biregularly isomorphic to $V_{\mathbb{R}}$. Indeed, the mapping

$$h_V: V_{\mathbb{R}} \longrightarrow (V \times \overline{V})(\mathbb{R}),$$

defined by $h_V(x) = (x, \sigma_n(x))$, is a biregular isomorphism of real algebraic varieties. Since $(V \times \overline{V})(\mathbb{R})$ is Zariski dense in $V \times \overline{V}$, it follows that, identifying $V_{\mathbb{R}}$ and $(V \times \overline{V})(\mathbb{R})$ through h_V, one can consider $V \times \overline{V}$ as a complexification of $V_{\mathbb{R}}$.

3 Proofs of Theorems 1 and 2

Lemma 6 *If Λ and Λ' are lattices in $\mathbb{R}^n$ and $L\colon \mathbb{R}^n \to \mathbb{R}^n$ is a linear mapping with $L(\Lambda) \subseteq \Lambda'$, then the induced mapping of the n-tori $\widetilde{L}\colon \mathbb{R}^n/\Lambda \to \mathbb{R}^n/\Lambda'$ has topological degree equal to*

$$(\det L)\frac{|\Lambda|}{|\Lambda'|},$$

where the orientation on $\mathbb{R}^n/\Lambda$ and $\mathbb{R}^n/\Lambda'$ is inherited from $\mathbb{R}^n$, and $|\Lambda|$ is the volume of a fundamental parallellogram of Λ.

Proof. Easy exercise. □

Lemma 7 *Let $\alpha = \sqrt{m/n}$, with m, n coprime odd positive integers such that*

$$m - n \equiv 2 \bmod 4.$$

Then there is a biregular isomorphism $f\colon (E_\alpha)_{\mathbb{R}} \to D_\alpha \times D_{1/\alpha}$ from the underlying real algebraic structure $(E_\alpha)_{\mathbb{R}}$ of E_α onto the product $D_\alpha \times D_{1/\alpha}$ of the associated real cubics $D_\alpha, D_{1/\alpha}$, which is also a group isomorphism.

Proof. As usual, we identify the quotient torus $\mathbb{C}/\Lambda_\alpha$ with the elliptic curve $E_\alpha \subseteq \mathbb{P}^2(\mathbb{C})$. If $\pi_\alpha\colon \mathbb{C} \to \mathbb{C}/\Lambda_\alpha$ is the canonical projection, then, under the above identification,

$$\pi_\alpha(\mathbb{R}) = D_\alpha.$$

Let $\beta = \frac{1}{2}(m + \alpha\sqrt{-1})$. The assumption about α implies that $\beta\Lambda_{1/\alpha} \subseteq \Lambda_\alpha$. Hence $\overline{\beta}\Lambda_{1/\alpha} \subseteq \overline{\Lambda_\alpha}$. The $\mathbb{C}$-linear mapping $\psi\colon \mathbb{C}^2 \to \mathbb{C}^2$, defined by $\psi(x, y) = (x + \beta y, x + \overline{\beta} y)$, maps the lattice $\Lambda_\alpha \times \Lambda_{1/\alpha}$ into $\Lambda_\alpha \times \overline{\Lambda_\alpha}$. Hence it induces a complex morphism

$$\widetilde{\psi}\colon E_\alpha \times E_{1/\alpha} \longrightarrow E_\alpha \times \overline{E_\alpha},$$

with $\widetilde{\psi}(D_\alpha \times D_{1/\alpha}) \subseteq (E_\alpha \times \overline{E_\alpha})(\mathbb{R})$. Therefore, the restriction

$$\varphi\colon D_\alpha \times D_{1/\alpha} \longrightarrow (E_\alpha \times \overline{E_\alpha})(\mathbb{R})$$

of $\widetilde{\psi}$ to $D_\alpha \times D_{1/\alpha}$ is a regular morphism of real algebraic varieties. We claim that φ is an isomorphism. To show the claim it suffices to prove that $\widetilde{\psi}$ is an isomorphism of complex abelian surfaces, or equivalently, that $\deg \widetilde{\psi} = 1$. Applying Lemma 6 one has

$$\deg \widetilde{\psi} = \left| \det \begin{pmatrix} 1 & \beta \\ 1 & \overline{\beta} \end{pmatrix} \right|^2 \frac{|\Lambda_\alpha| \cdot |\Lambda_{1/\alpha}|}{|\Lambda_\alpha|^2} = 1.$$

Since $(E_\alpha)_\mathbb{R}$ is biregularly isomorphic to $(E_\alpha \times \overline{E_\alpha})(\mathbb{R})$ (cf. Section 2), the proof of Lemma 7 is complete. □

We shall also need the following result, proved in [3].

Theorem 8 *Let E and F be complex elliptic curves. Assume that E has complex multiplication. Then the following conditions are equivalent:*

(i) *$E_\mathbb{R}$ and $F_\mathbb{R}$ are biregularly isomorphic (as real algebraic surfaces).*

(ii) *F has complex multiplication and $\delta(E) = \delta(F)$.* □

Proof of Theorem 1. The implication (i) ⇒ (iii) is trivial, and (iii) ⇒ (ii) is proved in [2].

(ii) ⇒ (i). Assume that E has complex multiplication and $\delta(E)$ is odd. Set $\alpha = \sqrt{-\delta(E)}$. Since $\delta(E) = \delta(E_\alpha)$, it follows from Theorem 8 that $E_\mathbb{R}$ and $(E_\alpha)_\mathbb{R}$ are biregularly isomorphic. By Lemma 7, $(E_\alpha)_\mathbb{R}$ is biregularly isomorphic to $D_\alpha \times D_{1/\alpha}$. This completes the proof of Theorem 1. □

Proof of Theorem 2. Assume that $E_\mathbb{R}$ is biregularly isomorphic to the product $C_1 \times C_2$ of two real algebraic curves C_1, C_2. Without loss of generality we may assume that C_j, $j = 1, 2$, is the real part of a nonsingular complex projective curve $C_{j\mathbb{C}}$. Since $C_1 \times C_2$, $E_\mathbb{R}$ and $(E \times \overline{E})(\mathbb{R})$ are biregularly isomorphic real algebraic surfaces (cf. Section 2), it follows that the complex varieties $C_{1\mathbb{C}} \times C_{2\mathbb{C}}$ and $E \times \overline{E}$ are birationally isomorphic. This immediately implies that the curves $C_{1\mathbb{C}}$ and $C_{2\mathbb{C}}$ have genus 1, which concludes the first part of Theorem 2. The second part of the theorem follows from well known properties of rational mappings between complex abelian varieties. □

4 Proof of Theorem 3

Given a system $\{a_1, a_2, a_3, a_4\}$ of 4 vectors in $\mathbb{C}^2$, linearly independent over $\mathbb{R}$, let us denote the lattice $\mathbb{Z}a_1 + \mathbb{Z}a_2 + \mathbb{Z}a_3 + \mathbb{Z}a_4$ by

$$\mathbb{Z}\langle a_1, \ldots, a_4 \rangle .$$

Proof of Theorem 3. (ii) $\Rightarrow$ (i). Let α be as in condition (ii). Then, by Lemma 7, $(E_\alpha)_{\mathbb{R}}$ is biregularly isomorphic to $D_\alpha \times D_{1/\alpha}$. Since $\delta(E_\alpha) = -mn = \delta(E)$, it follows from Theorem 8 that $(E_\alpha)_{\mathbb{R}}$ and $E_{\mathbb{R}}$ are isomorphic too. This implies (i).

(i) $\Rightarrow$ (ii). Let E be a complex elliptic curve such that $E_{\mathbb{R}}$ is biregularly isomorphic to $C_1 \times C_2$, and let $\beta = \sqrt{-\delta(E)}$. Theorem 2 implies that C_1 and C_2 are real cubic curves in $\mathbb{P}^2(\mathbb{R})$. Therefore, there exist positive real numbers α_1 and α_2, such that $C_j = D_{\alpha_j}$, $j = 1, 2$. Since E has complex multiplication, α_1^2 and α_2^2 are necessarily in $\mathbb{Q}$. As real varieties, $E_{\mathbb{R}}$ and $(E_\beta)_{\mathbb{R}}$ are biregularly isomorphic (because $\delta(E) = \delta(E_\beta)$, cf. Theorem 8) Hence we may assume that $E = E_\beta$. In particular, $E = \overline{E}$.

Set

$$\Lambda = \mathbb{Z}\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} \frac{1}{2}(1+\alpha_1 i) \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1}{2}(1+\alpha_2 i) \end{pmatrix} \right\rangle ,$$

where $i = \sqrt{-1}$. Clearly, $\overline{\Lambda} = \Lambda$. Observe now that $C_1 \times C_2$ is biregularly isomorphic to the real part $(\mathbb{C}^2/\Lambda)(\mathbb{R})$ of $\mathbb{C}^2/\Lambda$, with respect to the antiholomorphic involution on $\mathbb{C}^2/\Lambda$ induced by the standard conjugation on $\mathbb{C}^2$.

Set

$$\Lambda' = \mathbb{Z}\left\langle \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2i} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ \frac{-1}{2i} \end{pmatrix}, \begin{pmatrix} \frac{\tau}{2} \\ \frac{\tau}{2i} \end{pmatrix}, \begin{pmatrix} \frac{\overline{\tau}}{2} \\ \frac{-\overline{\tau}}{2i} \end{pmatrix} \right\rangle ,$$

where $\tau = \frac{1}{2}(1 + \beta i)$. Note that $\Lambda' = L_1(\Lambda_\beta \times \overline{\Lambda_\beta})$, where $L_1 \colon \mathbb{C}^2 \to \mathbb{C}^2$ is defined by $L_1(z, w) = (\frac{1}{2}(z + w), \frac{1}{2i}(z - w))$. Again $\overline{\Lambda'} = \Lambda'$.

Consider, $E \times \overline{E} = E \times E$ endowed with the involution γ_E defined in Section 2. Let $\mathbb{C}^2/\Lambda'$ be endowed with the involution induced by the standard conjugation on $\mathbb{C}^2$. Then L_1 induces an equivariant isomorphism of abelian varieties

$$E \times \overline{E} \longrightarrow \mathbb{C}^2/\Lambda'.$$

Since $C_1 \times C_2$, $E_{\mathbb{R}}$, and $(E \times \overline{E})(\mathbb{R})$ are isomorphic as real algebraic groups (cf. Theorem 2 and Section 2), it follows from the above constructions that there is an isomorphism

$$\mathbb{C}^2/\Lambda \longrightarrow \mathbb{C}^2/\Lambda',$$

induced by a $\mathbb{C}$-linear automorphism L_2 of $\mathbb{C}^2$, defined over $\mathbb{R}$. In particular, $L_2(\Lambda) = \Lambda'$.

Hence, for the lattices in $\mathbb{C}^2 = \mathbb{R}^2 + i\mathbb{R}^2$

$$\widehat{\Lambda} = \Lambda \cap \mathbb{R}^2 + \Lambda \cap i\mathbb{R}^2 = \mathbb{Z}\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, i\begin{pmatrix} \alpha_1 \\ 0 \end{pmatrix}, i\begin{pmatrix} 0 \\ \alpha_2 \end{pmatrix} \right\rangle$$

and

$$\widehat{\Lambda}' = \Lambda' \cap \mathbb{R}^2 + \Lambda' \cap i\mathbb{R}^2 = \mathbb{Z}\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \operatorname{Re}\tau \\ \operatorname{Im}\tau \end{pmatrix}, \begin{pmatrix} 0 \\ i \end{pmatrix}, i\begin{pmatrix} \operatorname{Im}\tau \\ -\operatorname{Re}\tau \end{pmatrix} \right\rangle,$$

one has $L_2(\widehat{\Lambda}) = \widehat{\Lambda}'$. Denote

$$L = \begin{pmatrix} 1 & \operatorname{Re}\tau \\ 0 & \operatorname{Im}\tau \end{pmatrix}^{-1}$$

and set $A = L \circ L_2$. Then

$$A(\widehat{\Lambda}) = L(\widehat{\Lambda}') = \mathbb{Z}\left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \frac{i}{\operatorname{Im}\tau}\begin{pmatrix} -\operatorname{Re}\tau \\ 1 \end{pmatrix}, \frac{i}{\operatorname{Im}\tau}\begin{pmatrix} |\tau|^2 \\ -\operatorname{Re}\tau \end{pmatrix} \right\rangle.$$

Since

$$A(\mathbb{Z}^2) = A(\widehat{\Lambda} \cap \mathbb{R}^2) = L(\widehat{\Lambda}') \cap \mathbb{R}^2 = \mathbb{Z}^2,$$

one has necessarily $A \in \mathrm{GL}_2(\mathbb{Z})$, $\det A = \pm 1$ and

$$A(\widehat{\Lambda} \cap i\mathbb{R}^2) = L(\widehat{\Lambda}') \cap i\mathbb{R}^2 \tag{1}$$

Denoting the volume of the fundamental parallellogram of a lattice Ω by $|\Omega|$, one has from (1)

$$\alpha_1\alpha_2 = |\det A| \cdot |\widehat{\Lambda} \cap i\mathbb{R}^2| = |L(\widehat{\Lambda}') \cap i\mathbb{R}^2| = \left|\frac{(\operatorname{Re}\tau)^2 - |\tau|^2}{(\operatorname{Im}\tau)^2}\right| = 1.$$

Hence $\alpha_1 = 1/\alpha_2$, that is C_1 and C_2 are associated real cubics.

By construction, $\alpha_1 = \sqrt{m/n}$, for some coprime positive integers m, n. We claim that $\delta(E) = -mn$. Indeed, since $E_{\mathbb{R}}$ is biregularly isomorphic to $D_{\alpha_1} \times D_{1/\alpha_1}$, it follows that $E \times E$ is isomorphic to $E_{\alpha_1} \times E_{1/\alpha_1}$, and hence to $E_{\alpha_1} \times E_{\alpha_1}$. This implies that the rings of endomorphisms $\mathrm{End}(()E \times E)$ and $\mathrm{End}(()E_{\alpha_1} \times E_{\alpha_1})$ are isomorphic. In particular, their centers, isomorphic to $\mathrm{End}(E)$ and $\mathrm{End}(E)_{\alpha_1}$, respectively, are isomorphic. Therefore $\delta(E) = \delta(E_{\alpha_1}) = -mn$, which shows the claim.

This completes the proof of Theorem 3. □

References

[1] J. Bochnak, M. Coste, and M.-F. Roy. *Géométrie algébrique réelle.* Ergebnisse der Math. Springer-Verlag, Berlin Heidelberg New-York, 1987.

[2] J. Bochnak and W. Kucharz. Real algebraic hypersurfaces in complex projective varieties (to appear).

[3] J. Huisman. The underlying real algebraic structure of complex elliptic curves (to appear).

[4] D. Husemöller. *Elliptic Curves.* Springer-Verlag, Berlin Heidelberg New-York, 1987.

[5] J.-P. Serre. *Lectures on the Mordell-Weil Theorem.* Vieweg, 1989.