The underlying real algebraic structure of complex elliptic curves

J. Huisman
Department of Mathematics
Vrije Universiteit
De Boelelaan 1081a
1081 HV Amsterdam
The Netherlands
telefax: +31 20 6427705
e-mail: huisman@cs.vu.nl

1 Introduction and the main results

In this paper we study the underlying real algebraic structure of complex elliptic curves. Before going into the details let us recall a few basic definitions of real algebraic geometry (for the background material the reader may refer to the book [1]).

Let $V \subseteq \mathbb{R}^n$ be an algebraic set endowed with the Zariski topology. If U is a Zariski-open subset of V, then a regular function $f: U \to \mathbb{R}$ is a function of the form $f = p/q$, where $p, q \in \mathbb{R}[X_1, ..., X_n]$ and q does not vanish on U. Denote by $\mathcal{R}_V$ the sheaf of regular functions on V. It is a sheaf of local $\mathbb{R}$-algebras.

A locally ringed space $(X, \mathcal{O}_X)$, where the sheaf $\mathcal{O}_X$ is a sheaf of local $\mathbb{R}$-algebras, is called an *affine real algebraic variety* if $(X, \mathcal{O}_X)$ is isomorphic to $(V, \mathcal{R}_V)$, for some algebraic set $V \subseteq \mathbb{R}^n$. More general, $(X, \mathcal{O}_X)$ is called

a *real algebraic variety* if there exists a finite open covering $\{U_i\}$ of X such that each locally ringed space $(U_i, \mathcal{O}_X \restriction_{U_i})$ is an affine real algebraic variety (one furthermore requires the diagonal in $X \times X$ to be closed). Morphisms between real algebraic varieties are just morphisms of locally ringed spaces preserving the $\mathbb{R}$-algebra structure.

A typical feature of real algebraic geometry is that every projective real algebraic variety $X \subseteq \mathbb{P}^n(\mathbb{R})$ is affine (cf. [1] Théorème 3.4.4).

Now let us explain what is meant by the *underlying real algebraic structure* of a complex algebraic variety. If $X \subseteq \mathbb{C}^n$ is an affine complex algebraic variety then, identifying $\mathbb{C}$ with $\mathbb{R}^2$ in the usual way, X is an algebraic subset of $\mathbb{R}^{2n}$. This defines the structure of a real algebraic variety on X, called the underlying real algebraic structure of X, and denoted by $X_{\mathbb{R}}$. Since an arbitrary complex algebraic variety X can be covered by finitely many open affine subsets, we see that the underlying real algebraic structure of each of these affine complex varieties determines uniquely the structure of a real algebraic variety $X_{\mathbb{R}}$ on X, the underlying real algebraic structure of X.

Since the underlying real algebraic structure $\mathbb{P}^n(\mathbb{C})_{\mathbb{R}}$ of complex projective space $\mathbb{P}^n(\mathbb{C})$ is affine (Proposition 3.4.8 of [1]), the underlying real algebraic structure of every projective complex algebraic variety is affine.

Obviously, $\dim_{\mathbb{R}} X_{\mathbb{R}} = 2 \dim_{\mathbb{C}} X$, for any complex algebraic variety X.

The natural question arises when, given two complex algebraic varieties X and Y, their underlying real algebraic structures $X_{\mathbb{R}}$ and $Y_{\mathbb{R}}$ are isomorphic. Another, closely related, problem can be formulated as follows. Given a real algebraic variety M, one can try to classify all complex algebraic varieties X with $X_{\mathbb{R}}$ isomorphic to M. An interesting part of this classification problem is the question whether the cardinality $\rho(M)$ of the set of (isomorphism classes of) complex algebraic varieties X such that $X_{\mathbb{R}}$ is isomorphic to M is finite or infinite.

To the best of our knowledge none of these questions has ever been seriously investigated. In this paper we shall give the full solution in the case of complex elliptic curves, being the only nontrivial case for complex algebraic curves (see [5]). We shall show that if M is a real algebraic torus, i.e. an affine nonsingular real algebraic surface homeomorphic to a torus, then $\rho(M)$ is finite (of course, possibly 0) and can take arbitrarily large values.

In fact our results are much more precise and allow us to compute the number $\rho(M)$ explicitly in each case $M = E_{\mathbb{R}}$ for a complex elliptic curve E (if M is a real algebraic torus not of this type then, of course, $\rho(M) = 0$).

This computation and other questions about the structure of $E_{\mathbb{R}}$ are related to the theory of quadratic number fields, both imaginary and real (the former intervene when E has complex multiplication, the latter when E is without complex multiplication). Before stating our main results let us recall briefly a few definitions and facts of this theory [3, 4].

Let $K = \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$ be a quadratic extension of $\mathbb{Q}$, where d is a square free integer, different from 0 and 1. Denote the ring of integers in K by $\mathcal{O}(d)$. Recall that every order $\mathcal{O}$ in $\mathcal{O}(d)$, that is, a subring of finite index, is uniquely determined by a positive integer c, called the conductor of $\mathcal{O}$, such that

$$\mathcal{O} = \mathbb{Z} + c\,\mathcal{O}(d).$$

Let us denote this ring by $\mathcal{O}_c(d)$. The discriminant $\delta = \delta(\mathcal{O}_c(d))$ of $\mathcal{O}_c(d)$ is an integer defined by

$$\delta = \begin{cases} c^2 d, & \text{for } d \equiv 1 \pmod 4, \\ 4c^2 d, & \text{for } d \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

One easily sees that an order in a quadratic extension of $\mathbb{Q}$ is completely determined by its discriminant. The classical theorem of Gauss says that the class number $h(\mathcal{O})$ of an order in a quadratic extension of $\mathbb{Q}$, i.e. the cardinality of the class group $Cl(\mathcal{O})$, is finite.

If X is a complex abelian variety, then $X_{\mathbb{R}}$ is a real algebraic group, with the group structure inherited from X. The following theorem will be proved in section 2.

Theorem 1 *Let X and Y be complex abelian varieties. Then the following conditions are equivalent:*

(i) *$X_{\mathbb{R}}$ and $Y_{\mathbb{R}}$ are birationally isomorphic as real algebraic varieties,*

(ii) *$X_{\mathbb{R}}$ and $Y_{\mathbb{R}}$ are isomorphic as real algebraic varieties,*

(iii) *$X_{\mathbb{R}}$ and $Y_{\mathbb{R}}$ are isomorphic as real algebraic groups.*

We shall briefly say that $X_{\mathbb{R}}$ and $Y_{\mathbb{R}}$ are *isomorphic* whenever one of these conditions is satisfied, and we shall denote this by $X_{\mathbb{R}} \cong Y_{\mathbb{R}}$.

Given a complex elliptic curve E, let $\operatorname{End} E$ denote its ring of endomorphisms. Consider first the case when E has complex multiplication, that is, $\operatorname{End} E \neq \mathbb{Z}$. In such a case $\operatorname{End} E$ is (isomorphic to) an order in an imaginary quadratic number field (and conversely) [10, 11]. Let us denote the

discriminant and the class number of $\mathrm{End}\, E$ by $\delta(E)$ and $h(E)$, respectively. If E is given as $\mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{C}$, then one can easily compute $\delta(E)$ and $h(E)$.

Theorem 2 *Let E and E' be complex elliptic curves. Assume that E has complex multiplication. Then the following conditions are equivalent:*

(i) *$E_{\mathbb{R}}$ and $E'_{\mathbb{R}}$ are isomorphic,*

(ii) $\mathrm{End}\, E$ *and* $\mathrm{End}\, E'$ *are isomorphic,*

(iii) *E' has complex multiplication and $\delta(E) = \delta(E')$.*

For $\tau \in \mathbb{C}\backslash\mathbb{R}$, let E_τ be the complex elliptic curve which is isomorphic, as a complex Lie group, to $\mathbb{C}/\Lambda_\tau$, where $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$.

Corollary 3 *Let E be a complex elliptic curve with complex multiplication. Then $E_{\mathbb{R}}$ is isomorphic to $(E_\tau)_{\mathbb{R}}$, where*

$$\tau = \frac{\delta(E) + \sqrt{\delta(E)}}{2}$$

In particular, $E_{\mathbb{R}}$ is isomorphic to $E'_{\mathbb{R}}$, for some complex elliptic curve E' defined over $\mathbb{R}$.

Proof. It is trivial to check that E_τ has complex multiplication and that $\delta(E_\tau) = \delta(E)$, so condition *(iii)* of Theorem 2 is satisfied. Furthermore, E_τ can be defined over $\mathbb{R}$. Indeed, since $\Lambda_\tau = \overline{\Lambda_\tau}$, the image of the Weierstrass embedding of $\mathbb{C}/\Lambda_\tau$ into $\mathbb{P}^2(\mathbb{C})$ is defined over $\mathbb{R}$. □

Corollary 4 *Let E be a complex elliptic curve with complex multiplication. Then the number of (isomorphism classes of) complex elliptic curves E' with $E'_{\mathbb{R}}$ isomorphic to $E_{\mathbb{R}}$ is finite and equal to the class number of* $\mathrm{End}\, E$*, that is,*

$$\rho(E_{\mathbb{R}}) = h(E).$$

Proof. It is well known that the number of (isomorphism classes of) complex elliptic curves E' having $\mathrm{End}\, E'$ isomorphic to $\mathrm{End}\, E$ is precisely $h(E)$ (cf. [10]). The corollary follows therefore from Theorem 2. □

Corollary 5 *Let E be a complex elliptic curve defined over $\mathbb{Q}$. Then $E_{\mathbb{R}}$ admits precisely one complex structure (E itself), that is $\rho(E_{\mathbb{R}}) = 1$.*

Proof. If E, as above, has complex multiplication then $h(E) = 1$. (There are exactly 13 curves having this property; they are listed in [6] p. 233.) So in this case, the conclusion follows from Corollary 4. If E is without complex multiplication, then $\rho(E_{\mathbb{R}}) = 1$ by Corollary 11 below. □

Remark 6. If E has complex multiplication, then $\rho(E_{\mathbb{R}}) = 1$ if and only if E can be defined over $\mathbb{Q}$ (see [10]). □ □

Consider now the case of complex elliptic curves without complex multiplication. Given E, let $\overline{E}$ be the complex elliptic curve with j-invariant $j(\overline{E}) = \overline{j(E)}$. If $E \subseteq \mathbb{P}^2(\mathbb{C})$ then one can take $\overline{E} = \sigma(E)$, where $\sigma\colon \mathbb{P}^2(\mathbb{C}) \to \mathbb{P}^2(\mathbb{C})$ is the standard conjugation. It is convenient to distinguish two types of complex elliptic curves without complex multiplication.
Type I : E is not isogenous to $\overline{E}$.
Type II : E is isogenous to $\overline{E}$.

Theorem 7 *Let E be a complex elliptic curve without complex multiplication and of type I. If E' is a complex elliptic curve with $E'_{\mathbb{R}}$ isomorphic to $E_{\mathbb{R}}$ then either E' is isomorphic to E, or E' is isomorphic to $\overline{E}$. In particular $\rho(E_{\mathbb{R}}) = 2$.*

The computation of $\rho(E_{\mathbb{R}})$ for E of type II is more complicated. Let $\alpha_E\colon E \to \overline{E}$ be an isogeny of minimal degree, say

$$\nu_E = \deg \alpha_E.$$

We shall show in section 5 that ν_E is an invariant of the underlying real algebraic structure of E.

Before formulating our result describing the values of $\rho(E_{\mathbb{R}})$ for E of type II, define an arithmetic function $r\colon \mathbb{N} \to \mathbb{N}$ by $r(\nu) = \#\Gamma_\nu$, for $\nu \in \mathbb{N}$, where

$$\Gamma_\nu = \{d \in \mathbb{N} \mid d \text{ divides } \nu \text{ and the binary quadratic form } dx^2 - \frac{\nu}{d}y^2 \text{ represents 1 or } -1 \text{ over } \mathbb{Z}\}.$$

The following Proposition will be proved in Section 6. It also follows from a result of K. Petr [9], as A. Schinzel pointed out to us.

Proposition 8 *Let ν be a positive integer. Then*

(i) $r(1) = 1$,
(ii) *if* $\nu > 1$, *then* $r(\nu) = 2$ *or* 4.

Example 9. (i) $r(n(n+1)) = 4$, for $n \geq 2$,
(ii) $r(n^2) = 2$, for $n \geq 2$.

□

Finally, we prove in section 5 the following result.

Theorem 10 *Let E be a complex elliptic curve without complex multiplication, of type II, and let ν_E be the invariant introduced above. Then*

$$\rho(E_{\mathbb{R}}) = r(\nu_E).$$

Corollary 11 *Let E be a complex elliptic curve without complex multiplication. Then*

(i) $\rho(E_{\mathbb{R}}) = 1$, *that is, $E_{\mathbb{R}}$ admits precisely one complex structure, if and only if $j(E) \in \mathbb{R}$.*
(ii) *if $j(E) \in \mathbb{C}\backslash\mathbb{R}$ then $E_{\mathbb{R}}$ admits precisely two or precisely four nonisomorphic complex structures, that is, $\rho(E_{\mathbb{R}}) = 2$ or 4.*

Proof. (i) If $\rho(E_{\mathbb{R}}) = 1$, then necessarily E is isomorphic to $\overline{E}$. Hence $j(E) \in \mathbb{R}$. Conversely, if $j(E) \in \mathbb{R}$ then E is of type II and $\nu_E = 1$, so, by Proposition 8 and Theorem 10, $\rho(E_{\mathbb{R}}) = 1$.

(ii) Follows from Theorem 7, Proposition 8 and Theorem 10. □

We shall now examine the problem of determining, for a given integer n, the size of the family $\mathcal{F}_n$ of real algebraic tori which admit precisely n, mutually nonisomorphic, complex structures. A theorem of Heilbronn, conjectured already by Gauss, says that the number of orders $\mathcal{O}$ of negative discriminant with $h(\mathcal{O}) = n$ is finite. Let us denote this number by $\vartheta(n)$ (see [8] for a method of computing $\vartheta(n)$).

Theorem 12 *If $n = 0, 1, 2$ or 4 then $\mathcal{F}_n$ is uncountable. Otherwise, $\mathcal{F}_n$ is finite and has precisely $\vartheta(n)$ elements.*

Proof. Let us first deal with the case $n = 0$. Let $\{C_\alpha\}_\alpha$ be an uncountable family of mutually nonisomorphic compact connected nonsingular real algebraic curves, and let S^1 be the unit circle. By Theorem 1.2 of [2] $\mathcal{F}_0$ contains the uncountable family $\{S^1 \times C_\alpha\}_\alpha$.

To show that $\mathcal{F}_n$ is uncountable for $n = 1, 2$ and 4, we shall use the following fact, proved in section 5 (Corollary 29): for every positive integer ν, the set of (isomorphism classes of) complex elliptic curves E of type II, with $\nu_E = \nu$, is uncountable. This, together with Example 9 and Theorem 10, implies that $\mathcal{F}_1$,$\mathcal{F}_2$ and $\mathcal{F}_4$ are uncountable.

Now we prove finiteness of $\mathcal{F}_n$ for $n \neq 0, 1, 2$ and 4. If $M \in \mathcal{F}_n$, then by Corollary 11, M is isomorphic to $X_{\mathbb{R}}$, for some complex elliptic curve X with complex multiplication. But then, by Theorem 2, the number of elements of $\mathcal{F}_n$ is equal to the number $\vartheta(n)$ of orders $\mathcal{O}$ of negative discriminant having class number $h(\mathcal{O})$ equal to n. □

Example 13. There exist precisely 25 nonisomorphic real algebraic tori, each admitting exactly 3 complex structures. Indeed, there exist precisely 16 fundamental negative discriminants [8] and 9 nonfundamental ones, each having class number 3, i.e. $\vartheta(3) = 25$. □

The paper is organized as follows. In section 2 we shall construct a convenient complexification of the underlying real algebraic structure of a complex algebraic variety. In section 3 we study the structure of morphisms of the underlying real algebraic structure of complex abelian varieties. Theorems 17 and 19, proved in this section, will be frequently used later on. In section 4 we prove Theorem 2. The proof is based on a result about primitive binary quadratic forms (proofs of which have been independently communicated to us by J.W.S. Cassels, A. Pfister and A. Schinzel; cf Proposition 24). Section 5 contains the proofs of Theorems 7 and 10.

This paper is a part of author's Ph. D. thesis written under supervision of Professor J. Bochnak (Vrije Universiteit Amsterdam).

2 Complexification of the underlying real algebraic structure

In this section we shall give the construction of an intrinsic complexification of the underlying real algebraic structure of a complex algebraic variety

(essentially due to A. Weil [12] p. 4).

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 an irreducible 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 $V_{\mathbb{R}}$. More precisely, one has the following result.

Theorem 14 *Let V be an irreducible projective complex algebraic variety. Identifying $V_{\mathbb{R}}$ and $(V \times \overline{V})(\mathbb{R})$ through h_V, the variety $V \times \overline{V}$ is a complexification of $V_{\mathbb{R}}$. That is, for every complex algebraic variety Y defined over $\mathbb{R}$ and every rational map $f: V_{\mathbb{R}} \to Y(\mathbb{R})$ of real algebraic varieties, there exists a unique rational map $f_{\mathbb{C}}: V \times \overline{V} \to Y$ defined over $\mathbb{R}$ extending f.*

Now we shall formulate a few consequences of Theorem 14. A real algebraic group G is said to be of *abelian type* if G admits a complexification $G_{\mathbb{C}}$ which is a complex abelian variety defined over $\mathbb{R}$, such that G is a real

algebraic subgroup of $(G_{\mathbb{C}})_{\mathbb{R}}$. Of course, every real algebraic group of abelian type is abelian as a group, but not conversely (for example, the unit circle is not of abelian type).

Examples 15. (i) Each nonsingular real cubic curve C in $\mathbb{P}^2(\mathbb{R})$ is a real algebraic group of abelian type.

(ii) The underlying real algebraic group $A_{\mathbb{R}}$ of a complex abelian variety A is of abelian type. Indeed, by Theorem 14 one can take as a complexification $A \times \overline{A}$, which is an abelian variety over $\mathbb{R}$.

(iii) The product $G_1 \times G_2$ of two real algebraic groups of abelian type is of abelian type. □

Proposition 16 *Let G_1 and G_2 be two real algebraic groups of abelian type, and let $\varphi: G_1 \to G_2$ be a rational map. Then φ is regular and $\varphi - \varphi(0)$ is a morphism of real algebraic groups.*

Proof. The rational map φ extends to a complex rational map $\varphi_{\mathbb{C}}: G_{1\mathbb{C}} \to G_{2\mathbb{C}}$ of complex abelian varieties. It is well known (cf. [7]) that $\varphi_{\mathbb{C}}$ is then, up to a translation, a morphism of abelian varieties. The proposition follows. □

As a consequence of Proposition 16 we can prove Theorem 1.

Proof of Theorem 1. Let X and Y be complex abelian varieties. By Example 15 (ii), $X_{\mathbb{R}}$ and $Y_{\mathbb{R}}$ are real algebraic groups of abelian type. The conclusion follows from Proposition 16. □

3 Morphisms of the underlying real algebraic structure of complex abelian varieties

In this section we shall study real algebraic morphisms from $X_{\mathbb{R}}$ into $Y_{\mathbb{R}}$, where X and Y are complex abelian varieties.

For any complex algebraic variety $X \subseteq \mathbb{P}^n(\mathbb{C})$ one has a canonical isomorphism of real algebraic varieties

$$\sigma_X = \sigma_n \restriction_X : X_{\mathbb{R}} \longrightarrow \overline{X}_{\mathbb{R}}.$$

Furthermore, if $f: X \to Y$ is a morphism of complex algebraic varieties, then $f^\sigma = \sigma_Y \circ f \circ \sigma_X^{-1}: \overline{X} \to \overline{Y}$ is again a morphism of complex algebraic varieties.

The structure of real algebraic morphisms $X_{\mathbb{R}} \to Y_{\mathbb{R}}$, for complex abelian varieties X and Y, is fully described by the following theorem.

Theorem 17 *Let X and Y be complex abelian varieties. Each morphism of real algebraic varieties $f: X_{\mathbb{R}} \to Y_{\mathbb{R}}$, with $f(0) = 0$, is a morphism of real algebraic groups, and*

$$f = f_1 + \sigma_Y^{-1} \circ f_2,$$

where $f_1: X \to Y$ and $f_2: X \to \overline{Y}$ are uniquely determined morphisms of complex abelian varieties.

Proof. Given f as above, there exists, as in the proof of Proposition 16, a unique morphism of complex abelian varieties

$$f_{\mathbb{C}}: X \times \overline{X} \longrightarrow Y \times \overline{Y},$$

such that

$$f_{\mathbb{C}} \circ h_X = h_Y \circ f.$$

The map $f_{\mathbb{C}}$ determines uniquely the morphisms $f_1: X \to Y$, $f_2: X \to \overline{Y}$, $f_3: \overline{X} \to Y$, $f_4: \overline{X} \to \overline{Y}$, such that

$$f_{\mathbb{C}}(x, y) = (f_1(x) + f_3(y), f_2(x) + f_4(y)).$$

Since $f_{\mathbb{C}} \circ \gamma_X = \gamma_Y \circ f_{\mathbb{C}}$, it follows that $f_4 = f_1^{\sigma}$ and $f_3 = f_2^{\sigma}$. This implies $f = f_1 + \sigma_Y^{-1} \circ f_2$, which completes the proof. □

The following lemma will be frequently used.

Lemma 18 *If Λ and Λ' are lattices in $\mathbb{R}^n$ and $L: \mathbb{R}^n \to \mathbb{R}^n$ is a linear map with $L(\Lambda) \subseteq \Lambda'$, then the induced mapping of n-tori $\widetilde{L}: \mathbb{R}^n/\Lambda \to \mathbb{R}^n/\Lambda'$ has degree*

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

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. We may assume that $\det L \neq 0$. Then, the degree of the canonical map $\pi\colon \mathbb{R}^n/L(\Lambda) \to \mathbb{R}^n/\Lambda'$ is the index $[\Lambda'\colon L(\Lambda)]$, which is equal to

$$\frac{|L(\Lambda)|}{|\Lambda'|}.$$

Let $\epsilon = \operatorname{sign}(\det L)$. Since $\deg \widetilde{L} = \epsilon \deg \pi$ and $\epsilon|L(\Lambda)| = (\det L)|\Lambda|$, the lemma follows. □

Let us consider now the case of complex elliptic curves. The orientation on the underlying real surface is induced by the complex structure.

Theorem 19 *If X and Y are complex elliptic curves and $f\colon X_{\mathbb{R}} \to Y_{\mathbb{R}}$ is a morphism, $f = f_1 + \sigma_Y^{-1} \circ f_2$, where $f_1\colon X \to Y$ and $f_2\colon X \to \overline{Y}$ are complex morphisms, then*

$$\deg f = \deg f_1 - \deg f_2.$$

Furthermore, $f\colon X_{\mathbb{R}} \to Y_{\mathbb{R}}$ is an isomorphism if and only if $\deg f = \pm 1$.

Proof. If the complex elliptic curve X is isomorphic to the complex torus $\mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{C}$, then the conjugate complex elliptic curve $\overline{X}$ can be identified with $\mathbb{C}/\overline{\Lambda}$, where $\overline{\ }$ is complex conjugation. Moreover, under this identification, $\sigma_X\colon X \to \overline{X}$ corresponds to the map $\mathbb{C}/\Lambda \to \mathbb{C}/\overline{\Lambda}$ induced by complex conjugation on $\mathbb{C}$.

Let $X = \mathbb{C}/\Lambda_1$ and $Y = \mathbb{C}/\Lambda_2$. There exist $\alpha_1, \alpha_2 \in \mathbb{C}$ with $\alpha_1\Lambda_1 \subseteq \Lambda_2$ and $\alpha_2\Lambda_1 \subseteq \overline{\Lambda_2}$, such that the induced map $\widetilde{\alpha_j} = f_j$, $j = 1, 2$. Then $f = f_1 + \sigma_Y^{-1} \circ f_2$ is equal to the map $\widetilde{L}\colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ induced by the $\mathbb{R}$-linear map $L\colon \mathbb{C} \to \mathbb{C}$, given by $L(z) = \alpha_1 z + \overline{\alpha_2 z}$. Applying Lemma 18, one gets

$$\deg f = (\det L)\frac{|\Lambda_1|}{|\Lambda_2|} = (|\alpha_1|^2 - |\alpha_2|^2)\frac{|\Lambda_1|}{|\Lambda_2|} = \deg f_1 - \deg f_2,$$

as claimed.

To prove that f is an isomorphism if and only if $\deg f = \pm 1$, observe that f is an isomorphism if and only if $\deg f_{\mathbb{C}} = 1$. Since $f_{\mathbb{C}}$ is induced by the $\mathbb{C}$-linear map $L_{\mathbb{C}}\colon \mathbb{C}^2 \to \mathbb{C}^2$ given by the matrix

$$\begin{pmatrix} \alpha_1 & \overline{\alpha_2} \\ \alpha_2 & \overline{\alpha_1} \end{pmatrix},$$

we have, by Lemma 18,

$$\deg f_{\mathbb{C}} = |\det L_{\mathbb{C}}|^2 \frac{|\Lambda_1 \oplus \overline{\Lambda_1}|}{|\Lambda_2 \oplus \overline{\Lambda_2}|} = (\deg f)^2.$$

The claim follows. □

Remark 20. The last statement of Theorem 19 is false if we replace $X_{\mathbb{R}}$ by an arbitrary real algebraic group of abelian type. Indeed, let us consider the complex elliptic curve $E = E_\xi = \mathbb{C}/\Lambda_\xi$, where $\xi \in \mathbb{C}$, $\xi^3 = 1$ and $\xi \neq 1$. Let $\widetilde{\alpha}$ be the automorphism of E induced by $\alpha\colon \mathbb{C} \to \mathbb{C}$, $\alpha(z) = \xi z$. Let $\pi\colon \mathbb{C} \to E$ be the canonical projection. Then the image $D = \pi(\mathbb{R})$ of $\mathbb{R}$ is a real algebraic subgroup of $E_{\mathbb{R}}$, and has E as a complexification.

The map

$$\begin{array}{rcl} f\colon D \times D & \longrightarrow & E_{\mathbb{R}} \\ (x, y) & \longmapsto & x + \widetilde{\alpha}(y) \end{array}$$

is a morphism of real algebraic groups of abelian type. Since $\{1, \xi\}$ is a $\mathbb{Z}$-basis for the lattice Λ_ξ, $\ker f = 0$. Hence, the degree of f is 1. We claim that f is not an isomorphism. To show this, it suffices to check that the degree of the complexification

$$f_{\mathbb{C}}\colon E \times E \longrightarrow E \times \overline{E} = E \times E$$

of f is different from 1. Now, $f_{\mathbb{C}}$ is induced by the $\mathbb{C}$-linear map given by the matrix

$$\begin{pmatrix} 1 & \xi \\ 1 & \overline{\xi} \end{pmatrix}.$$

By Lemma 18, the degree of $f_{\mathbb{C}}$ is then

$$\left|\det \begin{pmatrix} 1 & \xi \\ 1 & \overline{\xi} \end{pmatrix}\right|^2 \frac{|\Lambda_\xi \oplus \Lambda_\xi|}{|\Lambda_\xi \oplus \overline{\Lambda_\xi}|} = |\overline{\xi} - \xi|^2 = 3.$$

It follows that f is not an isomorphism, in spite of the fact that $\deg f = 1$. □

We conclude this section with the following observation.

Proposition 21 *If X and Y are complex elliptic curves with isomorphic underlying real algebraic structures $X_{\mathbb{R}}$ and $Y_{\mathbb{R}}$ then, either X and Y are isogenous, or X and $\overline{Y}$ are isogenous. In particular,*

$$\mathbb{Q} \otimes_{\mathbb{Z}} \operatorname{End} X \cong \mathbb{Q} \otimes_{\mathbb{Z}} \operatorname{End} Y.$$

Proof. Follows directly from Theorem 19. □

4 Classification of the underlying real algebraic structure of complex elliptic curves with complex multiplication

In this section we shall give a proof of Theorem 2. The main point is to show that if X and Y are complex elliptic curves with complex multiplication, then

$$X_{\mathbb{R}} \cong Y_{\mathbb{R}} \Longleftrightarrow \operatorname{End} X \cong \operatorname{End} Y.$$

As usual we shall consider the ring of endomorphisms $\operatorname{End} X$ as an order in some imaginary quadratic field $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

Lemma 22 *If $f\colon X \to Y$ is a morphism of complex elliptic curves with complex multiplication, then c_X divides $c_Y \deg f$, where c_X is the conductor of the order* $\operatorname{End} X$.

Proof. Of course, we may assume $\deg f \neq 0$. Since X and Y are isogenous, $\operatorname{End} X$ and $\operatorname{End} Y$ are orders in the same ring of integers $\mathcal{O}$ of some quadratic extension of $\mathbb{Q}$. If $\{1, \omega\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$ then $\{1, c_X\omega\}$ and $\{1, c_Y\omega\}$ are $\mathbb{Z}$-basis for $\operatorname{End} X$ and $\operatorname{End} Y$, respectively. Define a $\mathbb{Z}$-linear mapping

$$f^\star\colon \operatorname{End} Y \longrightarrow \operatorname{End} X,$$

by $f^\star(\varphi) = \widehat{f} \circ \varphi \circ f$, for $\varphi \in \operatorname{End} Y$, where $\widehat{f}\colon Y \to X$ is the dual isogeny of f. Then $f^\star(\varphi) = (\deg f)\varphi$ (which makes sense, considering $\operatorname{End} X$ and $\operatorname{End} Y$ as subrings of $\mathcal{O}$). Hence

$$f^\star(c_Y\omega) = (\deg f)c_Y\omega = kc_X\omega,$$

for some $k \in \mathbb{Z}$. The lemma follows. □

Corollary 23 *If X and Y are complex elliptic curves with complex multiplication and $X_{\mathbb{R}} \cong Y_{\mathbb{R}}$, then the rings of endomorphisms* $\operatorname{End} X$ *and* $\operatorname{End} Y$ *are isomorphic.*

Proof. As mentioned in the proof of Lemma 22, one has

$$\operatorname{End} X = \mathbb{Z} + c_X\mathcal{O}$$

and

$$\operatorname{End} Y = \mathbb{Z} + c_Y \mathcal{O},$$

where $\mathcal{O}$ is the ring of integers in a quadratic extension of $\mathbb{Q}$. We shall show that $c_X = c_Y$. Let $f\colon X_{\mathbb{R}} \to Y_{\mathbb{R}}$ be an isomorphism. By Theorem 17, there exist complex morphisms $f_1\colon X \to Y$ and $f_2\colon X \to \overline{Y}$ such that $f = f_1 + \sigma_Y^{-1} \circ f_2$ and $\deg f = \deg f_1 - \deg f_2 = \pm 1$. By Lemma 22, c_X divides $c_Y \deg f_1$ and c_X divides $c_{\overline{Y}} \deg f_2$. Since $\operatorname{End} \overline{Y}$ and $\operatorname{End} Y$ are isomorphic, one has $c_{\overline{Y}} = c_Y$, and c_X divides $(\deg f_1 - \deg f_2)c_Y = \pm c_Y$. Changing the role of X and Y one has also that c_Y divides c_X. Hence both conductors are equal and $\operatorname{End} X = \operatorname{End} Y$. □

To prove the converse of Corollary 23 we need the following result, of which proofs have been independently communicated to us by J.W.S. Cassels, A. Pfister and A. Schinzel. The proof reproduced below is due to Cassels.

Proposition 24 *Let $q(x,y) = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$, be a primitive quadratic form and let s be an odd integer. Then the quaternary quadratic form $q \perp (-q)$ represents s over $\mathbb{Z}$.*

Proof. By making, if necessary, an appropriate unimodular substitution, one can assume that a is odd. Then (by writing $4y$ for y, if necessary) we may assume $b = 4\beta$, $\beta \in \mathbb{Z}$. Now we shall show that there are integers u, v, x, y such that $q(u,v) - q(x,y) = s$. Put $u = sl + x$ and $v = sm + y$. Then

$$\begin{aligned} q(u,v) - q(x,y) &= sl(a(sl+2x) + 2\beta(sm+2y)) + \\ &\quad + sm(2\beta(sl+2x) + c(sm+2y)) \\ &= s(lL + mM), \end{aligned}$$

where

$$\begin{aligned} L &= aX + 2\beta Y, \\ M &= 2\beta X + cY \end{aligned}$$

and

$$\begin{aligned} X &= sl + 2x, \\ Y &= sm + 2y. \end{aligned}$$

Now we go in the reverse direction. Since a is odd, we can find integers X and Y, X odd and Y even, such that L and M defined above are coprime. Clearly L is odd, so one can choose integers l, m, l odd and m even, such that

$$lL + mM = 1.$$

Now $x = \frac{1}{2}(X - sl)$ and $y = \frac{1}{2}(Y - sm)$ are integers. Taking $u = sl + x$ and $v = sm + y$ we have $q(u, v) - q(x, y) = s$ as desired. □

In the proof of the next proposition we shall apply Proposition 24 with $s = 1$.

Proposition 25 *If X and Y are complex elliptic curves with complex multiplication, having isomorphic rings of endomorphisms, then $X_{\mathbb{R}} \cong Y_{\mathbb{R}}$.*

Proof. First observe that $\operatorname{End} X$, considered as a subring of $\mathbb{C}$, is itself a lattice. The complex elliptic curve $\widehat{X} = \mathbb{C}/\operatorname{End} X$ has the ring $\operatorname{End} X$ as its ring of endomorphisms. Therefore, to prove the proposition it suffices to show that $X_{\mathbb{R}} \cong \widehat{X}_{\mathbb{R}}$.

Let $X = \mathbb{C}/\Lambda$, with $\Lambda = \Lambda_\tau$ for some τ in $\mathbb{C}$ contained in a quadratic extension of $\mathbb{Q}$, and let a, b and c be rational integers satisfying

$$a > 0,\ \gcd(a, b, c) = 1 a\tau^2 + b\tau + c = 0.$$

Since the lattice $\operatorname{End} X$ is equal to its conjugate lattice $\overline{\operatorname{End} X}$, the curve $\widehat{X}$ coincides with its conjugate. To show that $X_{\mathbb{R}}$ is isomorphic to $\widehat{X}_{\mathbb{R}}$ we shall apply Theorem 19, i.e. , we shall show the existence of two complex morphisms $f_j \colon X \to \widehat{X}$, $j = 1, 2$ such that $\deg f_1 - \deg f_2 = 1$. Then $f = f_1 + \sigma_{\widehat{X}}^{-1} \circ f_2$ will be an isomorphism between $X_{\mathbb{R}}$ and $\widehat{X}_{\mathbb{R}}$.

Let

$$\Lambda^\star = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \operatorname{End} X\}.$$

If $\alpha \in \Lambda^\star$, then the morphism

$$\widetilde{\alpha} \colon X \longrightarrow \widehat{X},$$

induced by α is of degree $|\alpha|^2|\Lambda|/|\operatorname{End} X|$. To find the f_j as above we must find two elements α_1 and α_2 in $\Lambda^\star$ satisfying

$$\deg \widetilde{\alpha_1} - \deg \widetilde{\alpha_2} = 1.$$

Now, since $a\tau^2+b\tau+c=0$, End $X=\mathbb{Z}+\mathbb{Z}a\tau$. From this, one deduces easily that

$$\Lambda^\star=\mathbb{Z}a+\mathbb{Z}(a\tau+b).$$

For $\alpha\in\Lambda^\star$, written in the form $\alpha=ma+n(a\tau+b)$, with $m,n\in\mathbb{Z}$, one has $|\alpha|^2=a(am^2+bmn+cn^2)$. Since $|\mathrm{End}\,X|=a|\Lambda|$, it follows that

$$\deg\widetilde{\alpha}=am^2+bmn+cn^2.$$

Let q be the binary quadratic form $ax^2+bxy+cy^2$. By Proposition 24, we can find $m_j,n_j\in\mathbb{Z}$, $j=1,2$, such that $q(m_1,n_1)-q(m_2,n_2)=1$. Taking

$$\alpha_j=m_ja+n_j(a\tau+b),$$

we have $\deg\widetilde{\alpha_1}-\deg\widetilde{\alpha_2}=1$. □

Proof of Theorem 2. Follows directly from Corollary 23 and Proposition 25. □

5 Classification of the underlying real algebraic structure of complex elliptic curves without complex multiplication

In this section we will prove, among other things, Theorem 7 and 10 of the introduction.

Proof of Theorem 7. Let E be a complex elliptic curve of type I, i.e. E does not have complex multiplication and E is not isogenous to $\overline{E}$. Given a complex elliptic curve E' such that $E'_{\mathbb{R}}$ is isomorphic to $E_{\mathbb{R}}$, we have, by Theorem 19, morphisms $f_1\colon E'\to E$ and $f_2\colon E'\to\overline{E}$ such that $\deg f_1-\deg f_2=\pm1$. Now, if both f_1 and f_2 are nonzero, then $f_2\circ\widehat{f_1}$ would be an isogeny between E and $\overline{E}$. Hence, either f_1 or f_2 must be zero, and therefore, either f_1 or f_2 is an isomorphism. □

Before giving the proof of Theorem 10, we prove the following result.

Proposition 26 *Let E and E' be isogenous complex elliptic curves without complex multiplication. Then*

(i) $\mathrm{Hom}_(E,,)E')$ *is a free abelian group of rank 1.*

(ii) If $\alpha\colon E \to E'$ *is an isogeny, then* $\ker\alpha$ *is a cyclic group if and only if* $\deg\alpha$ *is minimal.*

Proof. (i) Let $\beta\colon E' \to E$ be an isogeny. Then the mapping

$$\begin{array}{rcl} \mathrm{Hom}_(E,,)E') & \longrightarrow & \mathrm{End}\, E' \cong \mathbb{Z} \\ \gamma & \longmapsto & \gamma \circ \beta \end{array}$$

is a monomorphism. Since $\mathrm{Hom}_(E,,)E') \neq 0$, this implies that $\mathrm{Hom}_(E,,)E')$ is a free abelian group of rank 1.

(ii) Let $\alpha \in \mathrm{Hom}_(E,,)E')$ be an isogeny of minimal degree. It follows from (i) that any other isogeny $\alpha' \in \mathrm{Hom}_(E,,)E')$ is of the form $\alpha' = k\alpha$, for some integer k. If $\deg\alpha' > \deg\alpha$, then $k \neq \pm 1$ and $\ker\alpha'$ contains a subgroup isomorphic to $(\mathbb{Z}/k)^2$. Hence, clearly, $\ker\alpha'$ is not cyclic. On the other hand, $\ker\alpha$ is cyclic, since otherwise it would contain a subgroup isomorphic to $(\mathbb{Z}/k)^2$, for some $k > 1$, and hence α would factor into $\alpha = k\beta$, for some isogeny β, with $\deg\beta < \deg\alpha$. □

Given a complex elliptic curve E of type II (that is, E is without complex multiplication and is isogenous to $\overline{E}$), let

$$\alpha_E\colon E \to \overline{E}$$

be an isogeny of minimal degree. Define

$$\nu_E = \deg\alpha_E.$$

Proof of Theorem 10. Let E be a complex elliptic curve of type II. Let G be the kernel of α_E. By Proposition 26, G is a cyclic group of order $\nu = \nu_E$. Recall that Γ_ν was defined to be the set of $d \in \mathbb{N}$ such that d divides ν and there exist integers m and n satisfying

$$dm^2 - \frac{\nu}{d}n^2 \;=\; \pm 1. \tag{1}$$

Given $d \in \Gamma_\nu$, let H_d be the unique subgroup of G of order d, let $E_d = E/H_d$ be the quotient complex elliptic curve and let $\pi_d\colon E \to E_d$ be the canonical mapping. Observe that $E_\nu = E/G = \overline{E}$.

To prove Theorem 10 it suffices to show the following three facts.

(i) For each $d \in \Gamma_\nu$, one has $(E_d)_{\mathbb{R}} \cong E_{\mathbb{R}}$.

(ii) For $d, e \in \Gamma_\nu$, if E_d is isomorphic to E_e, then $d = e$.

(iii) If E' is a complex elliptic curve with $E'_{\mathbb{R}} \cong E_{\mathbb{R}}$, then E' is isomorphic to E_d, for some $d \in \Gamma_\nu$.

To prove (i), let $d \in \Gamma_\nu$, and choose integers m and n satisfying equation (1). Since $\ker \pi_d \subseteq \ker \pi_\nu = G$, there exists an isogeny $g\colon E_d \to E_\nu = \overline{E}$ such that $\pi_\nu = g \circ \pi_d$. Then the morphism

$$h = m\widehat{\pi}_d + \sigma_E^{-1} \circ ng\colon (E_d)_{\mathbb{R}} \longrightarrow E_{\mathbb{R}}$$

has degree

$$\deg h = \deg(m\widehat{\pi}_d) - \deg(ng) = dm^2 - \frac{\nu}{d}n^2 = \pm 1.$$

By Theorem 19, $(E_d)_{\mathbb{R}}$ and $E_{\mathbb{R}}$ are isomorphic.

(ii) By Proposition 26, d (resp. e) is the smallest degree an isogeny from E into E_d (resp. E_e) can have. If E_d is isomorphic to E_e, these degrees are, of course, equal.

(iii) Let E' be a complex elliptic curve with $E'_{\mathbb{R}}$ isomorphic to $E_{\mathbb{R}}$. By Theorem 19, there exist morphisms $g_1\colon E \to E'$ and $g_2\colon E' \to \overline{E}$ such that $\deg g_1 - \deg g_2 = \pm 1$. Let $\alpha_1\colon E \to E'$ and $\alpha_2\colon E' \to \overline{E}$ be isogenies of minimal degree. By Proposition 26, there exist integers k_1, k_2 such that $g_j = k_j\alpha_j$, $j = 1, 2$. Now

$$k_1^2 \deg \alpha_1 - k_2^2 \deg \alpha_2 = \deg g_1 - \deg g_2 = \pm 1.$$

Hence $\ker \alpha_1$ and $\ker \alpha_2$ are cyclic groups of coprime order, which implies that $\ker(\alpha_2 \circ \alpha_1)$ is cyclic. By Proposition 26, $\alpha_2 \circ \alpha_1\colon E \to \overline{E}$ is an isogeny of minimal degree, that is $\alpha_2 \circ \alpha_1 = \pm\alpha_E$, $\deg(\alpha_2 \circ \alpha_1) = \nu$ and $H = \ker \alpha_1$ is a subgroup of $G = \ker \alpha_E$. Furthermore, if $d = \deg \alpha_1$ is the order of H, then

$$dk_1^2 - \frac{\nu}{d}k_2^2 = k_1^2 \deg \alpha_1 - k_2^2 \deg \alpha_2 = \pm 1.$$

It follows that $d \in \Gamma_\nu$ and $H = H_d$. Hence E' is isomorphic to $E/\ker \alpha_1 = E_d$, as claimed.

This completes the proof that $\rho(E_{\mathbb{R}}) = r(\nu_E)$. □

We shall now record a few results concerning the distribution of complex elliptic curves of type I and type II. Recall that, given $\tau \in \mathbb{C}\backslash\mathbb{R}$, E_τ denotes the complex elliptic curve isomorphic to $\mathbb{C}/\Lambda_\tau$, where $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. Let $\mathcal{E}_I$ (resp. $\mathcal{E}_{II}$) be the set of $\tau \in \mathbb{C}\backslash\mathbb{R}$ such that E_τ is of type I (resp. II). Define

$$\begin{aligned} A &= \{\tau \in \mathbb{C}\backslash\mathbb{R} \mid \operatorname{Re}\tau \in \mathbb{Q}\} \\ B &= \{\tau \in \mathbb{C}\backslash\mathbb{R} \mid |\tau - p|^2 \in \mathbb{Q} \text{ for some } p \in \mathbb{Q}\}. \end{aligned}$$

Lemma 27 *Given $\tau \in \mathbb{C}\backslash\mathbb{R}$ and $\alpha \in \mathbb{C}$, the following conditions are equivalent.*

(i) *α induces an isogeny $E_\tau \to \overline{E_\tau}$.*

(ii) *There exist integers m, n such that $\alpha = m + n\overline{\tau}$, $m^2 + n^2 \neq 0$ and $2m\operatorname{Re}\tau + n|\tau|^2 \in \mathbb{Z}$.*

Proof. Easy exercise. □

Proposition 28 (i) *$A \cap B = \{\tau \in \mathbb{C}\backslash\mathbb{R} \mid E_\tau$ has complex multiplication$\}$.*

(ii) *$\mathcal{E}_I = (\mathbb{C}\backslash\mathbb{R})\backslash(A \cup B)$.*

(iii) *$\mathcal{E}_{II} = (A \cup B)\backslash(A \cap B)$.*

Proof. (i) One sees immediately that $A \cap B$ is the union of all sets of the form $\mathbb{Q}(\sqrt{-d})\backslash\mathbb{Q}$, $d \in \mathbb{N}$, which implies (i).

(iii) Suppose that $\tau \in (A \cup B)\backslash(A \cap B)$. If $\operatorname{Re}\tau \in \mathbb{Q}$ then $2m\operatorname{Re}\tau \in \mathbb{Z}$, for some $m \in \mathbb{Z}\backslash\{0\}$ and, by Lemma 27, $\alpha = m$ induces an isogeny from E_τ into $\overline{E_\tau}$. If $\operatorname{Re}\tau \notin \mathbb{Q}$ then $|\tau - p|^2 = q$, for some $p, q \in \mathbb{Q}$. Choose $n \in \mathbb{Z}\backslash\{0\}$ such that np and $n(q - p^2)$ are integers. Define $m = -np$ and $\alpha = m + n\overline{\tau}$. Then

$$2m\operatorname{Re}\tau + n|\tau|^2 = n(q - p^2) \in \mathbb{Z},$$

and, again by Lemma 27, α induces an isogeny from E_τ into $\overline{E_\tau}$.

Conversely, suppose that $\tau \in \mathcal{E}_{II}$, and assume that $\tau \notin A$. Let $\alpha \in \mathbb{C}$ induce an isogeny $\widetilde{\alpha}\colon E_\tau \to \overline{E_\tau}$. Then, by Lemma 27, $\alpha = m + n\overline{\tau}$, for some $m \in \mathbb{Z}$, $n \in \mathbb{Z}\backslash\{0\}$. But then $|m + n\tau|^2 = \deg\widetilde{\alpha} \in \mathbb{Z}$, and hence

$$\left|\tau - \frac{-m}{n}\right|^2 = \frac{\deg\widetilde{\alpha}}{n^2} \in \mathbb{Q},$$

i.e. , $\tau \in B$.

(ii) Follows from (i) and (iii). □

Corollary 29 *For each positive integer ν, there exists an uncountable family of mutually nonisomorphic complex elliptic curves E of type II with $\nu_E = \nu$.*

Proof. It follows from Proposition 28 (iii) that there exist uncountably many $\tau \in \mathbb{C}$ with $|\tau|^2 = \nu$, $0 < \operatorname{Re}\tau < \frac{1}{2}$ and $\operatorname{Im}\tau > 0$, such that E_τ is of type II. Clearly, E_τ is not isomorphic to $E_{\tau'}$, for $\tau \neq \tau'$ as described. Since $\overline{\tau}\Lambda_\tau \subseteq \Lambda_{\overline{\tau}}$, it follows that $\overline{\tau}$ induces an isogeny $f\colon E_\tau \to \overline{E_\tau}$. One sees easily that $\ker f$ is cyclic. By Proposition 26, $\deg f = |\tau|^2 = \nu$ is minimal,i.e. $\nu_{E_\tau} = \nu$. □

We end this section with the following observation concerning the structure of the ring of endomorphisms $\operatorname{End} E_{\mathbb{R}}$ of the real algebraic group $E_{\mathbb{R}}$.

Proposition 30 *Let E be a complex elliptic curve without complex multiplication. Then*

(i) $\operatorname{End} E_{\mathbb{R}} \cong \mathbb{Z}$, *if E is of type I.*

(ii) $\operatorname{End} E_{\mathbb{R}} \cong \mathbb{Z}[T]/(T^2 - \nu_E)$, *if E is of type II. In particular, ν_E is an invariant of the underlying real algebraic structure $E_{\mathbb{R}}$ of E.*

Proof. (i) Let $f \in \operatorname{End} E_{\mathbb{R}}$. Then, by Theorem 19, $f = f_1 + \sigma_E^{-1} \circ f_2$, for some $f_1 \in \operatorname{Hom}_{(}(E,,)E)$, $f_2 \in \operatorname{Hom}_{(}(E,,)\overline{E})$. Since, by assumption, $\operatorname{Hom}_{(}(E,,)\overline{E}) = 0$, one has $f = f_1$, which implies (i).

(ii) By Theorem 19 and Proposition 26, $\operatorname{End} E_{\mathbb{R}}$ is freely generated by the identity and $\sigma_E^{-1} \circ \alpha_E$. Since $(\sigma_E^{-1} \circ \alpha_E)^2 = \alpha_E^\sigma \circ \alpha_E = [\nu_E]$, where $[\nu_E]$ denotes the multiplication-by-ν_E morphism, (ii) follows. □

6 Proof of Proposition 8

Before giving a proof of Proposition 8 we need some preparation.

Let $\mathcal{O}$ be an order of discriminant δ in a real quadratic extension K of $\mathbb{Q}$, let $\operatorname{Id}(\mathcal{O})$ be the group of invertible fractional ideals of $\mathcal{O}$, and let $Cl_+(\mathcal{O})$ be the quotient group of $\operatorname{Id}(\mathcal{O})$ consisting of strict equivalence classes of elements of $\operatorname{Id}(\mathcal{O})$, that is, $Cl_+(\mathcal{O}) = \operatorname{Id}(\mathcal{O})/\equiv$, where

$$I \equiv J \iff \exists \alpha \in K : N(\alpha) > 0 \text{ and } \alpha I = J.$$

It is well known that there is a one-to-one correspondence between the elements of $Cl_+(\mathcal{O})$ and the orbits of the action of $\mathrm{SL}_2(\mathbb{Z})$ on the set of primitive

binary quadratic forms of discriminant δ. If $I \in \mathrm{Id}(\mathcal{O})$ then

$$\Phi(I)(x,y) = \frac{N(x\alpha + y\beta)}{N(I)}$$

is a primitive binary quadratic form, where $N(I)$ is the norm of I, $N(v)$ is the norm of an element $v \in K$, and $\{\alpha, \beta\}$ is an oriented $\mathbb{Z}$-basis of I, that is,

$$\alpha\sigma(\beta) - \sigma(\alpha)\beta < 0,$$

where σ is the nontrivial element of the Galois group G of $K/\mathbb{Q}$. The mapping Φ induces the correspondence mentioned above (cf. [3] p. 159 or [4] Theorem 14.19).

Given $\alpha \in K^\star$, let (α) be the principal fractional ideal $\mathcal{O}\alpha$.

Lemma 31 *If $\mathcal{O}$ is an order of discriminant δ in a real quadratic field, and $I \in \mathrm{Id}(\mathcal{O})$, then*

(i) *the ideal I is strictly equivalent to the ideal (1) if and only if $\Phi(I)$ represents 1 over $\mathbb{Z}$,*

(ii) *the ideal I is strictly equivalent to the ideal $(\sqrt{\delta})$ if and only if $\Phi(I)$ represents -1 over $\mathbb{Z}$.*

Proof. Since $\mathcal{O} = \mathbb{Z}[\frac{1}{2}(\delta + \sqrt{\delta})]$, one has

$$\Phi((1)) = N\left(x + \frac{\delta + \sqrt{\delta}}{2}y\right) = x^2 + \delta xy + \frac{\delta^2 - \delta}{4}y^2$$

which clearly represents 1 over $\mathbb{Z}$. Taking $\{\frac{1}{2}(\delta + \delta\sqrt{\delta}), \sqrt{\delta}\}$ as an oriented basis for $(\sqrt{\delta})$, one has

$$\Phi((\sqrt{\delta})) = \frac{\delta - \delta^2}{4}x^2 - \delta xy - y^2$$

which clearly represents -1 over $\mathbb{Z}$. Hence for each I strictly equivalent to (1) (resp. $(\sqrt{\delta})$), the form $\Phi(I)$ represents 1 (resp. -1) over $\mathbb{Z}$.

To prove the implications in the opposite direction, suppose that $\Phi(I)$ represents 1 or -1. Then there exists $\alpha \in I$ with $N(\alpha) = \pm N(I)$. But then $I = (\alpha)$. It follows that $I \equiv (1)$ if $N(\alpha) > 0$, and $I \equiv (\sqrt{\delta})$ if $N(\alpha) < 0$. $\square$

Let ν be an integer such that $\nu \geq 2$ and ν is not a square. From now on, $\mathcal{O}$ will be the order $\mathbb{Z}[\sqrt{\nu}]$. If m is a positive integer such that m divides ν and $\gcd(m, \nu/m) = 1$, then

$$I_m = \mathbb{Z}m + \mathbb{Z}\sqrt{\nu}$$

is an invertible fractional ideal of $\mathcal{O}$ and

$$\Phi(I_m) = \frac{N(xm + y\sqrt{\nu})}{N(I_m)} = mx^2 - \frac{\nu}{m}y^2.$$

It follows from Lemma 31 that

$$mx^2 - \frac{\nu}{m}y^2 \text{ represents } 1 \text{ (resp. } -1) \iff I_m \equiv (1) \text{ (resp. } I_m \equiv (\sqrt{\nu})).$$

We shall use this property of I_m in the proof of Proposition 8, after further preparations.

The Galois group $G = \{1, \sigma\}$ of $K/\mathbb{Q}$ acts on $\mathrm{Id}(\mathcal{O})$ in the obvious way, and this action induces an action of G on $Cl_+(\mathcal{O})$. Given an action of G on a set A, let us denote

$$A^G = \{a \in A \mid \sigma(a) = a\}.$$

The multiplicative group $\mathbb{Q}^+ = \{q \in \mathbb{Q} \mid q > 0\}$ will be identified with its image under the monomorphism

$$\begin{array}{rcl} \mathbb{Q}^+ & \longrightarrow & \mathrm{Id}(\mathcal{O})^G \\ q & \longmapsto & (q). \end{array}$$

Let $\mathcal{O}^\star$ be the group of units of $\mathcal{O}$ and let U be the subgroup

$$\{\varepsilon \in \mathcal{O}^\star \mid \varepsilon = \frac{\alpha}{\sigma(\alpha)} \text{ for some } \alpha \in K,\ N(\alpha) > 0\}$$

of $\mathcal{O}^\star$. It follows easily from Hilbert's Theorem 90 [4] that, given a unit η in $\mathcal{O}$ with $N(\eta) = 1$, exactly one of the elements $\eta, -\eta$ is in U. In particular, using Dirichlet's Unit Theorem (cf. [3] p. 129), the group U is isomorphic to $\mathbb{Z}$.

Define now a homomorphism

$$\varphi: U/U^2 \longrightarrow (\mathrm{Id}\mathcal{O})^G/\mathbb{Q}^+$$

by sending the class of $\varepsilon \in U$ to the class of (α) in $(\mathrm{Id}\mathcal{O})^G/\mathbb{Q}^+$, where $\varepsilon = \alpha/\sigma(\alpha)$. Then define a homomorphism

$$\psi\colon (\mathrm{Id}\mathcal{O})^G/\mathbb{Q}^+ \longrightarrow Cl_+(\mathcal{O})^G$$

by sending the class of an ideal $I \in (\mathrm{Id}\mathcal{O})^G$ to its class in $Cl_+(\mathcal{O})^G$.

Lemma 32 *The sequence of group homomorphisms*

$$0 \longrightarrow U/U^2 \xrightarrow{\varphi} (\mathrm{Id}\mathcal{O})^G/\mathbb{Q}^+ \xrightarrow{\psi} Cl_+(\mathcal{O})^G \longrightarrow 0$$

is exact.

Proof. To prove injectivity of φ, assume $\varphi(\varepsilon \bmod U^2) = 0$ for some $\varepsilon \in U$. Choose $\alpha \in K$ with $N(\alpha) > 0$ and $\varepsilon = \alpha/\sigma(\alpha)$. Then $(\alpha) = (q)$, for some $q \in \mathbb{Q}^+$. Hence, there exists a unit η in $\mathcal{O}$ such that $\alpha = \eta q$. It follows that η has norm 1 and $\varepsilon = \eta^2 = (-\eta)^2$. Since either η or $-\eta$ is in U, $\varepsilon \in U^2$. This implies the injectivity of φ.

Clearly, ψ is surjective and, since φ sends the class of $\varepsilon \in U$ to the class of (α) with $N(\alpha) > 0$, one has $\psi \circ \varphi = 0$.

Let us show that $\ker\psi \subseteq \mathrm{im}\,\varphi$. If ψ sends the class of an ideal $I \in (\mathrm{Id}\mathcal{O})^G$ to the class of (1) in $Cl_+(\mathcal{O})^G$, then $I = (\alpha)$, for some $\alpha \in K$, $N(\alpha) > 0$. Since $\sigma(I) = I$, there is an $\varepsilon \in \mathcal{O}^\star$ such that $\varepsilon\sigma(\alpha) = \alpha$. Then ε is in U and φ sends the class of ε to the class of $(\alpha) = I$. □

Proof of Proposition 8. It is trivial to see that $r(1) = 1$. We shall show now that for each integer $\nu > 1$ the number $r(\nu) = \#\Gamma_\nu$, defined in the introduction, is either 2 or 4. In the proof we shall use the notation introduced above in this section without further explanation.

If ν is a square, then obviously $r(\nu)$ is 2, so without loss of generality we may assume that ν is not a square.

Let $m \in \Gamma_\nu$. Then necessarily $\gcd(m, \nu/m) = 1$ and $\sigma(I_m) = I_m$, that is $I_m \in (\mathrm{Id}\mathcal{O})^G$. The mapping

$$\Gamma_\nu \longrightarrow (\mathrm{Id}\mathcal{O})^G/\mathbb{Q}^+,$$

which sends m to the class of I_m is injective, for if $I_m = qI_n$, for some $q \in \mathbb{Q}^+$, then $\sqrt{\nu} = q\sqrt{\nu}$, so $q = 1$ and $m = n$.

Since U/U^2 is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, ψ is a two-to-one mapping. It follows from Lemma 31 that $mx^2 - (\nu/m)y^2$ represents ± 1 if and only if $\psi(I_m) = (1)$ or $(\sqrt{\nu})$ in $Cl_+(\mathcal{O})$. Since $r(\nu)$ is obviously even, it must be 2 or 4 as claimed. □

References

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

[2] Bochnak, J., Huisman, J.: When is a complex elliptic curve the product of two real algebraic curves? (to appear in Math. Ann.)

[3] Borewicz, S.I., Šafarevič, I.R.: *Zahlentheorie.* Boston-Basel-Stuttgart: Birkhäuser 1966

[4] Cohn, H.: *A classical invitation to algebraic numbers and class fields.* Berlin Heidelberg New-York: Springer 1978

[5] Huisman, J.: A note on the underlying real algebraic structure of complex algebraic curves of genus different from 1. (to appear)

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

[7] Lang, S.: *Abelian Varieties.* Berlin Heidelberg New-York: Springer 1983

[8] Oesterle, J.: Le problème de Gauss sur le nombre de classes. *Enseign. Math.*, 34, 43–67, (1988)

[9] Petr, K.: O rovnici Pelloě (Sur l'équation de Pell). *Časopis pro pěstování matematiky a fysiky*, 56, 57–66, (1927)

[10] Serre, J.-P.: Complex multiplication. In Cassels, J.W., Fröhlich, A. (eds.) *Algebraic Number Theory*, (pp. 292–296) Academic Press 1967

[11] Silverman, J.H.: *The Arithmetic of Elliptic Curves.* Berlin Heidelberg New-York: Springer 1986

[12] Weil, A.: *Adeles and Algebraic Groups.* Progress in Mathematics, Vol. 23, Boston-Basel-Stuttgart: Springer 1982