*Hokkaido Mathematical Journal Vol. 45 (2016) p. 43–51*

# On a symmetry of complex and real multiplication

Igor V. Nikolaev

(Received July 26, 2013; Revised November 13, 2013)

**Abstract.** It is proved that each lattice with complex multiplication by $f\sqrt{-D}$ corresponds to a pseudo-lattice with real multiplication by $f'\sqrt{D}$, where $f'$ is an integer defined by $f$.

*Key words*: complex and real multiplication.

## 1. Introduction

The paper continues a study of the duality between elliptic curves with complex multiplication and noncommutative tori with real multiplication initiated in [5]; let us introduce some notation and basic facts. Fix an irrational number $0 < \theta < 1$; a *noncommutative torus* is the universal $C^*$-algebra $A_\theta$ generated by the unitaries $u$ and $v$ satisfying the commutation relation $vu = e^{2\pi i\theta}uv$ (Rieffel, 1981 [6]). Two such tori are stably isomorphic (Morita equivalent) whenever $A_\theta \otimes \mathcal{K} \cong A_{\theta'} \otimes \mathcal{K}$, where $\mathcal{K}$ is the $C^*$-algebra of compact operators; the isomorphism occurs if and only if $\theta' = (a\theta + b)/(c\theta + d)$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. The K-theory of $A_\theta$ is Bott periodic with $K_0(A_\theta) = K_1(A_\theta) \cong \mathbb{Z}^2$. The range of the trace on projections of $A_\theta \otimes \mathcal{K}$ is a subset $\Lambda = \mathbb{Z} + \mathbb{Z}\theta$ of the real line (Rieffel, 1981 [6]); $\Lambda$ is called a pseudo-lattice (Manin, 2004 [4]). The torus $A_\theta$ is said to have *real multiplication* if $\theta$ is a quadratic irrationality; we shall denote the set of such algebras by $\mathcal{A}_{RM}$. The real multiplication entails existence of the non-trivial endomorphisms of $\Lambda$ coming from multiplication by the real numbers – hence the name. If $D > 1$ is a square-free integer, we shall write $A_{RM}^{(D,f)}$ to denote real multiplication by an order $R_f$ of conductor $f \geq 1$ in the field $\mathbb{Q}(\sqrt{D})$; each torus in $\mathcal{A}_{RM}$ can be written in this form (Manin, 2004 [4]).

Let $\mathbb{H} = \{x + iy \in \mathbb{C} \mid y > 0\}$ be the upper half-plane and for $\tau \in \mathbb{H}$ let $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ be a complex torus; we routinely identify the latter with a

*2000 Mathematics Subject Classification* : 11G15 (complex multiplication); 46L85 (noncommutative topology).

Partially supported by NSERC.

non-singular elliptic curve via the Weierstrass $\wp$ function (Silverman, 1994 [7, pp. 6–7]). Recall that two complex tori are isomorphic, whenever $\tau' = (a\tau+b)/(c\tau+d)$, where $a,b,c,d \in \mathbb{Z}$ and $ad-bc=1$. If $\tau$ is an imaginary quadratic number, the elliptic curve is said to have *complex multiplication*; in this case the lattice $L=\mathbb{Z}+\mathbb{Z}\tau$ admits non-trivial endomorphisms given as multiplication of $L$ by certain complex (quadratic) numbers. Elliptic curves with complex multiplication are fundamental and have long history in number theory; we shall denote the set of such curves by $\mathcal{E}_{CM}$. We write $E_{CM}^{(-D,f)}$ to denote the elliptic curve with complex multiplication by an order $\mathfrak{R}_f$ of conductor $f \geq 1$ in the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$; each curve in $\mathcal{E}_{CM}$ is isomorphic to $E_{CM}^{(-D,f)}$ for some integers $D$ and $f$ (Silverman, 1994 [7, pp. 95–96]).

There exists a covariant functor between elliptic curves and noncommutative tori; the functor maps isomorphic curves to the stably isomorphic tori. To give an idea, let $\phi$ be a closed form on a topological torus; the trajectories of $\phi$ define a measured foliation on the torus. By the Hubbard-Masur theorem, such a foliation corresponds to a point $\tau \in \mathbb{H}$. The map $F: \mathbb{H} \to \partial\mathbb{H}$ is defined by the formula $\tau \mapsto \theta = \int_{\gamma_2}\phi / \int_{\gamma_1}\phi$, where $\gamma_1$ and $\gamma_2$ are generators of the first homology of the torus. The following is true: (i) $\mathbb{H} = \partial\mathbb{H} \times (0,\infty)$ is a trivial fiber bundle, whose projection map coincides with $F$; (ii) $F$ is a functor, which maps isomorphic complex tori to the stably isomorphic noncommutative tori. We shall refer to $F$ as the *Teichmüller functor*. It was proved in [5] that $F(\mathcal{E}_{CM}) \subseteq \mathcal{A}_{RM}$, i.e. $F$ sends elliptic curves with complex multiplication to the noncommutative tori with real multiplication. Namely, $F(E_{CM}^{(-D,f)}) = A_{RM}^{(D,f')}$, where $f'$ is the least integer satisfying equation $|Cl\ (R_{f'})| = |Cl\ (\mathfrak{R}_f)|$ for the class numbers of orders $R_{f'}$ and $\mathfrak{R}_f$, respectively; the latter constraint is a necessary and sufficient condition for $A_{RM}^{(D,f')}$ to discern non-isomorphic curves $E_{CM}^{(-D,f)}$ having the same endomorphism ring $R_f$.

Denote by $\Lambda_{RM}^{(D,f)}$ a pseudo-lattice corresponding to the torus $A_{RM}^{(D,f)}$; the $\Lambda_{RM}^{(D,f)}$ can be identified with points of the boundary $\partial\mathbb{H}$ of the half-plane $\mathbb{H}$. Let $x,\bar{x} \in \Lambda_{RM}^{(D,f)}$ be a pair of the conjugate quadratic irrationalities and consider a geodesic half-circle through $x$ and $\bar{x}$:

$$\widetilde{\gamma}(x,\bar{x}) = \frac{xe^{t/2}+i\bar{x}e^{-t/2}}{e^{t/2}+ie^{-t/2}}, \qquad -\infty \leq t \leq \infty. \tag{1}$$

A Riemann surface $X$ is said to be *associated to* $A_{RM}^{(D,f)}$, if the covering of the geodesic spectrum of $X$ contains the set $\{\widetilde{\gamma}(x,\bar{x}) : \forall x \in \Lambda_{RM}^{(D,f)}\}$, see Definition 1; such a surface will be denoted by $X(A_{RM}^{(D,f)})$. Our main result can be expressed as follows.

**Theorem 1** *For every square-free integer $D > 1$ and integer $f \geq 1$ there exists a holomorphic map $F^{-1} : X(A_{RM}^{(D,f')}) \to E_{CM}^{(-D,f)}$, where $F(E_{CM}^{(-D,f)}) = A_{RM}^{(D,f')}$.*

The note is organized as follows. Section 2 is reserved for notation and preliminary facts. Theorem 1 is proved in Section 3.

## 2. Riemann surface $X(A_{RM}^{(D,f)})$

Let $X$ be a Riemann surface; consider the geodesic spectrum of $X$, i.e. the set $\mathrm{Spec}\,X$ consisting of all closed geodesics of $X$. Recall that for the covering map $\mathbb{H} \to X$ each geodesic $\gamma \in \mathrm{Spec}\,X$ is the image of a geodesic half-circle $\widetilde{\gamma}(x,x') \in \mathbb{H}$ with the endpoints $x \neq x'$. Denote by $\widetilde{\mathrm{Spec}}X \subset \mathbb{H}$ the set of geodesic half-circles covering the geodesic spectrum of $X$.

**Definition 1** We shall say that the Riemann surface $X$ is associated to the noncommutative torus $A_{RM}^{(D,f)}$, if $\{\widetilde{\gamma}(x,\bar{x}) : \forall x \in \Lambda_{RM}^{(D,f)}\} \subset \widetilde{\mathrm{Spec}}X$; the associated Riemann surface will be denoted by $X(A_{RM}^{(D,f)})$.

Let $N \geq 1$ be an integer; by $\Gamma_1(N)$ we understand a subgroup of the modular group $SL_2(\mathbb{Z})$ consisting of matrices of the form

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; a, d \equiv 1 \bmod N,\; c \equiv 0 \bmod N \right\}; \tag{2}$$

the corresponding Riemann surface $\mathbb{H}/\Gamma_1(N)$ will be denoted by $X_1(N)$. The following lemma links $X(A_{RM}^{(D,f)})$ to $X_1(N)$.

**Lemma 1** $X(A_{RM}^{(D,f)}) \cong X_1(fD)$.

*Proof.* Let $\Lambda_{RM}^{(D,f)}$ be a pseudo-lattice with real multiplication by an order $R$ in the real quadratic number field $\mathbb{Q}(\sqrt{D})$; it is known, that $\Lambda_{RM}^{(D,f)} \subseteq R$ and $R = \mathbb{Z} + (f\omega)\mathbb{Z}$, where $f \geq 1$ is the conductor of $R$ and

$$\omega = \begin{cases} \dfrac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \bmod 4, \\ \sqrt{D} & \text{if } D \equiv 2,3 \bmod 4, \end{cases} \tag{3}$$

see e.g. (Borevich & Shafarevich, 1988 [1, pp. 130–131]) Recall that matrix $(a,b,c,d) \in SL_2(\mathbb{Z})$ has a pair of real fixed points $x$ and $\bar{x}$ if and only if $|a+d| > 2$ (the hyperbolic matrix); the fixed points can be found from the equation $x = (ax+b)(cx+d)^{-1}$ by the formulas:

$$x = \frac{a-d}{2c} + \sqrt{\frac{(a+d)^2-4}{4c^2}}, \qquad \bar{x} = \frac{a-d}{2c} - \sqrt{\frac{(a+d)^2-4}{4c^2}}. \tag{4}$$

Case I. If $D \equiv 1 \bmod 4$, then formula (3) implies that $R = (1+f/2)\mathbb{Z} + (\sqrt{f^2D}/2)\mathbb{Z}$. If $x \in \Lambda_{RM}^{(D,f)}$ is fixed point of a transformation $(a,b,c,d) \in SL_2(\mathbb{Z})$, then formula (4) implies:

$$\begin{cases} \dfrac{a-d}{2c} = \left(1+\dfrac{f}{2}\right) z_1 \\ \dfrac{(a+d)^2-4}{4c^2} = \dfrac{f^2D}{4} z_2^2 \end{cases} \tag{5}$$

for some integer numbers $z_1$ and $z_2$. The second equation can be written in the form $(a+d)^2 - 4 = c^2 f^2 D z_2^2$; we have therefore $(a+d)^2 \equiv 4 \bmod (fD)$ and $a+d \equiv \pm 2 \bmod (fD)$. Without loss of generality we assume $a+d \equiv 2 \bmod (fD)$ since matrix $(a,b,c,d) \in SL_2(\mathbb{Z})$ can be multiplied by $-1$. Notice that the last equation admits a solution $a = d \equiv 1 \bmod (fD)$.

The first equation yields us $(a-d)/c = (2+f)z_1$, where $c \neq 0$ since the matrix $(a,b,c,d)$ is hyperbolic. Notice that $a - d \equiv 0 \bmod (fD)$; since the ratio $(a-d)/c$ must be integer, we conclude that $c \equiv 0 \bmod (fD)$. All together, we get:

$$a \equiv 1 \bmod (fD), \quad d \equiv 1 \bmod (fD), \quad c \equiv 0 \bmod (fD). \tag{6}$$

Case II. If $D \equiv 2$ or $3 \bmod 4$, then $R = \mathbb{Z} + (\sqrt{f^2D})\mathbb{Z}$. If $x \in \Lambda_{RM}^{(D,f)}$ is fixed point of a transformation $(a,b,c,d) \in SL_2(\mathbb{Z})$, then formula (4) implies:

$$\begin{cases} \dfrac{a-d}{2c} = z_1 \\ \dfrac{(a+d)^2-4}{4c^2} = f^2 D z_2^2 \end{cases} \tag{7}$$

for some integer numbers $z_1$ and $z_2$. The second equation gives $(a+d)^2 - 4 = 4c^2 f^2 D z_2^2$; therefore $(a+d)^2 \equiv 4 \bmod (fD)$ and $a+d \equiv \pm 2 \bmod (fD)$. Again without loss of generality we assume $a+d \equiv 2 \bmod (fD)$ since matrix $(a,b,c,d) \in SL_2(\mathbb{Z})$ can be multiplied by $-1$. The last equation admits a solution $a = d \equiv 1 \bmod (fD)$.

The first equation is $(a-d)/c = 2z_1$, where $c \neq 0$. Since $a - d \equiv 0 \bmod (fD)$ and the ratio $(a-d)/c$ must be integer, one concludes that $c \equiv 0 \bmod (fD)$. All together, we get equations (6). Since all possible cases are exhausted, Lemma 1 follows. □

**Remark 1** There exist other finite index subgroups of $SL_2(\mathbb{Z})$ whose geodesic spectrum contains the set $\{\widetilde{\gamma}(x,\bar{x}) : \forall x \in \Lambda_{RM}^{(D,f)}\}$; however $\Gamma_1(fD)$ is a unique group with such a property among subgroups of the principal congruence group.

**Remark 2** Not all geodesics of $X_1(fD)$ have form (1); thus the set $\{\widetilde{\gamma}(x,\bar{x}) : \forall x \in \Lambda_{RM}^{(D,f)}\}$ is strictly included in the geodesic spectrum of modular curve $X_1(fD)$.

## 3. Proof of Theorem 1

Recall, that $\Gamma(N) := \{(a,b,c,d) \in SL_2(\mathbb{Z}) \mid a,d \equiv 1 \bmod N,\ b,c \equiv 0 \bmod N\}$ is called a *principal congruence group* of level $N$; the corresponding (compact) Riemann surface will be denoted by $X(N) = \mathbb{H}/\Gamma(N)$.

**Lemma 2** (Hecke) *There exists a holomorphic map* $X(fD) \to E_{CM}^{(-D,f)}$.

*Proof.* A detailed proof of this beautiful fact is given in (Hecke, 1928 [3]).

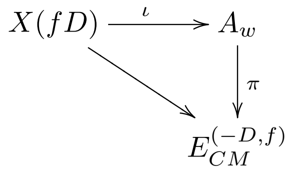
To give an idea of the proof, let $\mathfrak{R}$ be an order of conductor $f \geq 1$ in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-D})$; consider an $L$-function attached to $\mathfrak{R}$:

$$L(s,\psi) = \prod_{\mathfrak{P} \subset \mathfrak{R}} \frac{1}{1 - \psi(\mathfrak{P})/N(\mathfrak{P})^s}, \quad s \in \mathbb{C}, \tag{8}$$

where $\mathfrak{P}$ is a prime ideal in $\mathfrak{R}$, $N(\mathfrak{P})$ its norm and $\psi$ a Grössencharacter. A crucial observation (Section 1) says that the series $L(s,\psi)$ converges to a cusp form $w(s)$ of the principal congruence group $\Gamma(fD)$.

By the Deuring Theorem, $L(E_{CM}^{(-D,f)}, s) = L(s,\psi)L(s,\bar{\psi})$, where $L(E_{CM}^{(-D,f)}, s)$ is the Hasse-Weil $L$-function of the elliptic curve and $\bar{\psi}$ a conjugate of the Grössencharacter, see (Silverman, 1994 [7, p. 175]); moreover $L(E_{CM}^{(-D,f)}, s) = L(w,s)$, where $L(w,s) := \sum_{n=1}^{\infty} \frac{c_n}{n^s}$ and $c_n$ the Fourier coefficients of the cusp form $w(s)$. In other words, $E_{CM}^{(-D,f)}$ is a modular elliptic curve.

One can now apply the modularity principle: if $A_w$ is an abelian variety given by the periods of holomorphic differential $w(s)ds$ (and its conjugates) on $X(fD)$, then the following diagram commutes




The holomorphic map $X(fD) \to E_{CM}^{(-D,f)}$ is obtained as a composition of the canonical embedding $\iota : X(fD) \to A_w$ with the subsequent holomorphic projection $\pi : A_w \to E_{CM}^{(-D,f)}$. $\square$

**Lemma 3** *The functor $F$ acts by the formula $E_{CM}^{(-D,f)} \mapsto A_{RM}^{(D,f')}$.*

*Proof.* Let $L_{CM}$ be a lattice with complex multiplication by an order $\mathfrak{R} = \mathbb{Z} + (f\omega)\mathbb{Z}$ in the imaginary quadatic field $\mathbb{Q}(\sqrt{-D})$; the multiplication by $\alpha \in \mathfrak{R}$ generates an endomorphism $(a,b,c,d) \in M_2(\mathbb{Z})$ of the lattice $L_{CM}$. It is known, that the endomorphisms of lattice $L_{CM}$ and endomorphisms of the pseudo-lattice $\Lambda_{RM} = F(L_{CM})$ are related by the following explicit map [4, p. 524]:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{End}(L_{CM}) \longmapsto \begin{pmatrix} a & b \\ -c & -d \end{pmatrix} \in \mathrm{End}(\Lambda_{RM}). \tag{9}$$

Moreover, one can always assume $d = 0$ in a proper basis of $L_{CM}$. We shall consider the following two cases.

Case I. If $D \equiv 1 \bmod 4$ then by (3) $\mathfrak{R} = \mathbb{Z} + ((f + \sqrt{-f^2D})/2)\mathbb{Z}$; thus the multiplier $\alpha = (2m + fn)/2 + \sqrt{(-f^2Dn^2)/4}$ for some $m, n \in \mathbb{Z}$. Therefore multiplication by $\alpha$ corresponds to an endomorphism $(a, b, c, 0) \in M_2(\mathbb{Z})$, where

$$\begin{cases} a = Tr(\alpha) = \alpha + \bar{\alpha} = 2m + fn \\ b = -1 \\ c = N(\alpha) = \alpha\bar{\alpha} = \left(\dfrac{2m + fn}{2}\right)^2 + \dfrac{f^2Dn^2}{4}. \end{cases} \tag{10}$$

To calculate a primitive generator of endomorphisms of the lattice $L_{CM}$ one should find a multiplier $\alpha_0 \neq 0$ such that

$$|\alpha_0| = \min_{m.n \in \mathbb{Z}} |\alpha| = \min_{m.n \in \mathbb{Z}} \sqrt{N(\alpha)}. \tag{11}$$

From the last equation of (10) the minimum is attained for $m = -f/2$ and $n = 1$ if $f$ is even or $m = -f$ and $n = 2$ if $f$ is odd. Thus

$$\alpha_0 = \begin{cases} \pm\dfrac{f}{2}\sqrt{-D}, & \text{if } f \text{ is even} \\ \pm f\sqrt{-D}, & \text{if } f \text{ is odd.} \end{cases} \tag{12}$$

To find the matrix form of the endomorphism $\alpha_0$, we shall substitute in (9) $a = d = 0$, $b = -1$ and $c = f^2D/4$ if $f$ is even or $c = f^2D$ if $f$ is odd. Thus the Teichmüller functor maps the multiplier $\alpha_0$ into

$$F(\alpha_0) = \begin{cases} \pm\dfrac{f'}{2}\sqrt{D}, & \text{if } f' \text{ is even} \\ \pm f'\sqrt{D}, & \text{if } f' \text{ is odd.} \end{cases} \tag{13}$$

Comparing equations (12) and (13) one verifies that formula $F(E_{CM}^{(-D,f)}) = A_{RM}^{(D,f')}$ is true in this case.

Case II. If $D \equiv 2$ or $3 \bmod 4$ then by (3) $\mathfrak{R} = \mathbb{Z} + (\sqrt{-f^2D})\mathbb{Z}$; thus the multiplier $\alpha = m + \sqrt{-f^2Dn^2}$ for some $m, n \in \mathbb{Z}$. A multiplication by $\alpha$ corresponds to an endomorphism $(a, b, c, 0) \in M_2(\mathbb{Z})$, where

$$\begin{cases} a &= Tr(\alpha) = \alpha + \bar{\alpha} = 2m \\ b &= -1 \\ c &= N(\alpha) = \alpha\bar{\alpha} = m^2 + f^2Dn^2. \end{cases} \quad (14)$$

We shall repeat the argument of Case I; then from the last equation of (14) the minimum of $|\alpha|$ is attained for $m = 0$ and $n = \pm 1$. Thus $\alpha_0 = \pm f\sqrt{-D}$.

To find the matrix form of the endomorphism $\alpha_0$ we substitute in (9) $a = d = 0$, $b = -1$ and $c = f^2D$. Thus the Teichmüller functor maps the multiplier $\alpha_0 = \pm f\sqrt{-D}$ into $F(\alpha_0) = \pm f'\sqrt{D}$. In other words, formula $F(E_{CM}^{(-D,f)}) = A_{RM}^{(D,f')}$ is true in this case as well.

Since all possible cases are exhausted, Lemma 3 is proved. □

**Lemma 4** *For every $N \geq 1$ there exists a holomorphic map $X_1(N) \to X(N)$.*

*Proof.* Indeed, $\Gamma(N)$ is a normal subgroup of index $N$ of the group $\Gamma_1(N)$; therefore there exists a degree $N$ holomorphic map $X_1(N) \to X(N)$. □

Theorem 1 follows from Lemmas 1–3 and Lemma 4 for $N = fD$. □

**Remark 3** While this note was in print, the author came across a preprint (D'Andrea, Fiore & Franco, 2013 [2]). Using the idea of quantum deformation of the line bundles over elliptic curves, the authors establish a remarkable formula

$$\tau - \frac{p\theta}{2} i \in \mathbb{Z} + \mathbb{Z}i, \quad (15)$$

where $p \in \mathbb{Z}$ is the first Chern class of the line bundle. The reader is encouraged to verify, that Theorem 1 satisfies equation (15) for a line bundle of the Chern class $p = 2f'$ with $\tau = f\sqrt{-D}$ and $\theta = \sqrt{D}$.

**Acknowledgment** I thank the referee for helpful comments.

## References

[1] Borevich Z. I. and Shafarevich I. R., Number Theory, Acad. Press, 1966.

[2] D'Andrea F., Fiore G. and Franco D., *Modules over the noncommutative torus and elliptic curves.* Lett. Math. Phys. **104** (2014), 1425–1443.

[ 3 ] Hecke E., *Bestimmung der Perioden gewisser Integrale durch die Theorie der Klassenkörper*. Math. Z. **28** (1928), 708–727.

[ 4 ] Manin Yu. I., *Real multiplication and noncommutative geometry*, in "Legacy of Niels Hendrik Abel", 685–727, Springer, 2004.

[ 5 ] Nikolaev I., *Remark on the rank of elliptic curves.* Osaka J. Math. **46** (2009), 515–527.

[ 6 ] Rieffel M. A., *$C^*$-algebras associated with irrational rotations.* Pacific J. of Math. **93** (1981), 415–429.

[ 7 ] Silverman J. H., *Advanced Topics in the Arithmetic of Elliptic Curves.* GTM 151, Springer 1994.

The Fields Institute for Research in Mathematical Sciences
Toronto, ON, Canada
E-mail: igor.v.nikolaev@gmail.com

Current address:
1505-657 Worcester St., Southbridge, MA 01550, U.S.A.