<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Remark on the rank of elliptic curves</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Nikolaev, Igor</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Journal of Mathematics. 46(2) P.515-P.527</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>2009-06</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/7110">https://doi.org/10.18910/7110</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/7110</td>
</tr>
</tbody>
</table>

Osaka University Knowledge Archive: OUKA

http://ir.library.osaka-u.ac.jp/dspace/

Osaka University
REMARK ON THE RANK OF ELLIPTIC CURVES

IGOR NIKOLAEV

(Received August 17, 2007, revised February 15, 2008)

Abstract

A covariant functor on the elliptic curves with complex multiplication is constructed. The functor takes values in the noncommutative tori with real multiplication. A conjecture on the rank of an elliptic curve is formulated.

Introduction

A. Let \( \theta \) be an irrational number given by the regular continued fraction

\[
\theta = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}} = [a_0, a_1, a_2, \ldots].
\]

Consider an AF-algebra, \( A_\theta \), defined by the Bratteli diagram of Fig. 1, where \( a_i \) indicate the multiplicity of the edges of the graph. (For a definition of the AF-algebras and their Bratteli diagrams, we refer the reader to [2], or §1.2.) For the simplicity, we shall say that \( A_\theta \) is a noncommutative torus. Note that the classical definition of a noncommutative torus is slightly different but equivalent from the standpoint of the K-theory [3], [7], [13]. The \( A_\theta \) is said to have real multiplication, if \( \theta \) is a quadratic irrationality. Recall that the noncommutative tori \( A_\theta \), \( A_{\theta'} \) are stably isomorphic whenever \( A_\theta \otimes K \cong A_{\theta'} \otimes K \), where \( K \) is the \( C^* \)-algebra of the compact operators. It is known that \( A_\theta \), \( A_{\theta'} \) are stably isomorphic if and only if \( \theta' \equiv \theta \mod GL(2, \mathbb{Z}) \), i.e. \( \theta' = (a\theta + b)/(c\theta + d) \), where \( a, b, c, d \in \mathbb{Z} \) and \( ad - bc = \pm 1 \).

B. Let \( \Lambda = \omega_1 \mathbb{Z} + \omega_2 \mathbb{Z} \) be a lattice in the complex plane \( \mathbb{C} \). Recall that \( \Lambda \) defines an elliptic curve \( E(\mathbb{C}) \): \( y^2 = 4x^3 - g_2x - g_3 \) via the complex analytic map \( \mathbb{C}/\Lambda \to E(\mathbb{C}) \) given by the formula \( z \mapsto (\wp(z, \Lambda), \wp'(z, \Lambda)) \), where \( g_2 = 60 \sum_{\omega \in \Lambda^*} \omega^{-4} \), \( g_3 = 140 \sum_{\omega \in \Lambda^*} \omega \), \( \Lambda^\times = \Lambda - \{0\} \) and

\[
\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^\times} \left( \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).
\]
Fig. 1. The AF-algebra $A_0$.

is the Weierstrass $\wp$ function. We identify the elliptic curves $E(C)$ with the complex tori $C/\Lambda$. If $\tau = \omega_2/\omega_1$, then $E_\tau(C), E_{\tau'}(C)$ are isomorphic whenever $\tau' \equiv \tau \mod GL(2, \mathbb{Z})$. The endomorphism ring $End(C/\Lambda)$ is isomorphic either to $\mathbb{Z}$ or to an order in the imaginary quadratic number field $k$ [14]. In the second case, we say that the elliptic curve has a complex multiplication and denote such a curve by $E_{CM}$.

C. Consider the cubic $E_\lambda$: $y^2 = x(x-1)(x-\lambda), \lambda \in \mathbb{C} - \{0, 1\}$. The $j$-invariant of $E_\lambda$ is given by the formula $j(E_\lambda) = 2^6(\lambda^2-\lambda+1)^3\lambda^{-2}(\lambda-1)^{-2}$. To find $\lambda$ corresponding to an elliptic curve with the complex multiplication, one has to solve the polynomial equation $j(E_{CM}) = j(E_\lambda)$ with respect to $\lambda$. Since $j(E_{CM})$ is an algebraic integer, $\lambda_{CM} \in K$, where $K$ is an algebraic extension (of the degree at most six) of the field $\mathbb{Q}(j(E_{CM}))$. Thus, each $E_{CM}$ is isomorphic to the cubic $y^2 = x(x-1)(x-\lambda_{CM})$ defined over the field $K$. The Mordell-Weil theorem says that the set of the $K$-rational points of $E_{CM}$ is a finitely generated abelian group, whose rank we shall denote by $rk(E_{CM})$.

D. Let $E$ be a category whose objects are elliptic curves and the arrows are isomorphisms of the elliptic curves. Likewise, let $A$ be a category whose objects are noncommutative tori and the arrows are stable isomorphisms of the noncommutative tori. Our main goals can be expressed as follows.

OBJECTIVES. (i) to construct a functor (if any) $F: E \to A$, which maps isomorphic elliptic curves to the stably isomorphic noncommutative tori; (ii) to study the range of $F$ on the elliptic curves with complex multiplication and (iii) to interpret the invariants of the stable isomorphism classes of the noncommutative tori in terms of the arithmetic invariants of the elliptic curves.

In the course of this note, we were able to obtain an answer to (i) and (ii), while (iii) generates a conjecture. Namely, a covariant non-injective functor $F: E \to A$, which maps isomorphic elliptic curves to the stably isomorphic noncommutative tori, is constructed (Lemma 1). It is proved that $F$ sends the elliptic curves with complex multiplication to the noncommutative tori with real multiplication (Theorem 1). Finally, a conjecture on the rank of an elliptic curve with the complex multiplication is formulated (§3). The functor $F$ has been studied by Kontsevich [5] (e.g. §1.39), Manin [6], Polishchuk [8]–[11], Polishchuk-Schwarz [12], Soibelman [15] and [16], Soibelman-Vologodsky [17], Taylor [18] and [19] et al. Our terminology is freely and gratefully borrowed from the above works.
The existence and properties of $F$ are part of a Hodge theory for the measured foliations on a closed surface. Such a theory has been developed by Hubbard and Masur [4], who were inspired by the works of Thurston [20]. We shall give in §1 a brief account of the Hubbard-Masur-Thurston theory and the explicit formulas for the functor $F$. At the heart of the construction is a diagram:

$$F: \mathcal{E} \xrightarrow{h} \mathbb{R}^2 \xrightarrow{\pi} \mathbb{R}P^1 \cong \mathcal{A},$$

where $h$ is a bijection and $\pi$ is a projection map. For the sake of brevity, let $\text{Isom}(E) = \{E' \in \mathcal{E} \mid E' \cong E\}$ be the isomorphism class of an elliptic curve $E$, $h(\text{Isom}(E)) = \mu_E(\mathbb{Z} + \theta_E\mathbb{Z}) := m_E \subset \mathbb{R}$ be a $\mathbb{Z}$-module and $F(E) = \langle \theta_E \rangle$. A summary of our results can be formulated as follows.

**Lemma 1.** Let $\varphi: E \to E'$ be an isogeny of the elliptic curves. Then $\theta' \equiv \theta \mod M_2(\mathbb{Z})$, where $M_2(\mathbb{Z})$ is an integer matrix of the rank 2. In particular, $F$ maps the isomorphic elliptic curves to the stably isomorphic noncommutative tori.

**Theorem 1.** Let $E \in \text{Isom}(E_{CM})$. Then there exists an $h$, such that:

(i) $m_E$ is a full module in the real quadratic number field;

(ii) $m_E$ is an invariant of the class $\text{Isom}(E_{CM}).$

In particular, $\theta_E$ is a quadratic irrationality.

The structure of the note is as follows. In Section 1, we introduce the notation and some preliminary facts. Lemma 1 and Theorem 1 are proved in Section 2. In Section 3, a conjecture on the rank of an elliptic curve is formulated.

1. **Preliminaries**

This section contains a summary of measured foliations, $AF$-algebras and the functor $F$. The reader is encouraged to consult [2] (operator algebras) and [4] (measured foliations and Teichmüller space) for a systematic account.

1.1. **Measured foliations and $T(g)$**

A. A measured foliation, $\mathcal{F}$, on a surface $X$ is a partition of $X$ into the singular points $x_1, \ldots, x_n$ of order $k_1, \ldots, k_n$ and the regular leaves (1-dimensional submanifolds). On each open cover $U_i$ of $X - \{x_1, \ldots, x_n\}$ there exists a non-vanishing real-valued closed 1-form $\phi_i$ such that

(i) $\phi_i = \pm \phi_j$ on $U_i \cap U_j$;

(ii) at each $x_i$ there exists a local chart $(u, v): V \to \mathbb{R}^2$ such that for $z = u + iv$, it holds $\phi_i = \text{Im}(z^{k_i/2} dz)$ on $V \cap U_i$ for some branch of $z^{k_i/2}$. 


The pair \( (U_i, \phi_i) \) is called an atlas for the measured foliation \( \mathcal{F} \). Finally, a measure \( \mu \) is assigned to each segment \( (t_0, t) \in U_i \), which is transverse to the leaves of \( \mathcal{F} \), via the integral \( \mu(t_0, t) = \int_{t_0}^{t} \phi_i \). The measure is invariant along the leaves of the foliation \( \mathcal{F} \), hence the name.

B. Let \( S \) be a Riemann surface, and \( q \in H^0(S, \Omega^{\otimes 2}) \) a holomorphic quadratic differential on \( S \). The lines \( \text{Re} \, q = 0 \) and \( \text{Im} \, q = 0 \) define a pair of measured foliations on \( R \), which are transversal to each other outside the set of singular points. The set of singular points is common to the both foliations and coincides with the zeroes of \( q \). The above measured foliations are said to represent the vertical and horizontal trajectory structure of \( q \), respectively.

C. Let \( T(g) \) be the Teichmüller space of the topological surface \( X \) of genus \( g \), i.e. the space of complex structures on \( X \). Consider the vector bundle \( p: Q \to T(g) \) over \( T(g) \) whose fiber above a point \( S \in T(g) \) is the vector space \( H^0(S, \Omega^{\otimes 2}) \). Given non-zero \( q \in Q \) above \( S \), one can consider the horizontal measured foliation \( \mathcal{F}_q \in \Phi_X \) of the quadratic differential \( q \), where \( \Phi_X \) is the space of (equivalence classes of) measured foliations on \( X \). If \( [0] \) is the zero section of \( Q \), the above construction defines a map \( Q - [0] \to \Phi_X \). For any \( \mathcal{F} \in \Phi_X \), let \( E_\mathcal{F} \subset Q - [0] \) be the fiber above \( \mathcal{F} \). In other words, \( E_\mathcal{F} \) is a subspace of the holomorphic quadratic differentials, whose horizontal trajectory structure coincides with the measured foliation \( \mathcal{F} \).

**Theorem** ([4]). The restriction \( E_\mathcal{F} \to T(g) \) of \( p \) to \( E_\mathcal{F} \) is a homeomorphism.

D. Let \( \Phi_X \) be the space of measured foliations on the topological surface \( X \). Following Douady and Hubbard [1], we shall consider a coordinate system on \( \Phi_X \), suitable for the construction of the functor \( F \). For clarity, let us make a generic assumption that \( q \in H^0(S, \Omega^{\otimes 2}) \) is a holomorphic quadratic differential with the simple zeroes only. We wish to construct a Riemann surface of \( \sqrt{q} \), which is a double cover of \( S \) with the ramification over the zeroes of \( q \). Such a surface, denoted by \( \tilde{S} \), is unique and has an advantage of carrying a holomorphic differential \( \omega \), such that \( \omega^2 = q \). Denote by \( \pi: \tilde{S} \to S \) a covering projection. The vector space \( H^0(\tilde{S}, \Omega) \) splits into the direct sum \( H^0_{\text{even}}(\tilde{S}, \Omega) \oplus H^0_{\text{odd}}(\tilde{S}, \Omega) \) in view of the involution \( \pi^{-1} \) of \( \tilde{S} \), and the vector space \( H^0(S, \Omega^{\otimes 2}) \cong H^0_{\text{odd}}(\tilde{S}, \Omega) \). Let \( H^1_{\text{odd}}(\tilde{S}) \) be an odd part of the homology of \( \tilde{S} \) relatively the zeroes of \( q \). Consider a pairing \( H^1_{\text{odd}}(\tilde{S}) \times H^0(S, \Omega^{\otimes 2}) \to \mathbb{C} \), defined by the integration \( \gamma, q \mapsto \int_{\gamma} \omega \). Take the associated map \( \psi_q: H^0(S, \Omega^{\otimes 2}) \to \text{Hom}(H^1_{\text{odd}}(\tilde{S}); \mathbb{C}) \) and let \( h_q = \text{Re} \, \psi_q \).

**Theorem** ([1]). The map \( h_q: H^0(S, \Omega^{\otimes 2}) \to \text{Hom}(H^1_{\text{odd}}(\tilde{S}); \mathbb{R}) \) is an \( \mathbb{R} \)-isomorphism.
ON THE RANK OF ELLIPTIC CURVES
519

Since each \( F \in \Phi_X \) is the vertical foliation \( \text{Req} = 0 \) for a \( q \in H^0(S, \Omega^{\otimes 2}) \), the theorem implies that \( \Phi_X \cong \text{Hom}(H_1^{\text{odd}}(\tilde{S}); \mathbb{R}) \). By the formulas for the relative homology:

\[
H_1^{\text{odd}}(\tilde{S}) \cong \mathbb{Z}^n, \quad \text{where} \quad n = \begin{cases} 6g - 6, & \text{if } g \geq 2, \\ 2, & \text{if } g = 1. \end{cases}
\]

Thus, if \( \{\gamma_1, \ldots, \gamma_n\} \) is a basis in \( H_1^{\text{odd}}(\tilde{S}) \), the reals \( \lambda_i = \int_{\gamma_i} \text{Re} \omega \) are natural coordinates in the space \( \Phi_X \) [1].

1.2. \( \mathcal{A}F \)-algebras.

**A.** The \( C^* \)-algebra is an algebra \( A \) over \( \mathbb{C} \) with a norm \( a \mapsto \|a\| \) and an involution \( a \mapsto a^* \) such that it is complete with respect to the norm and \( \|ab\| \leq \|a\| \|b\| \) and \( \|a^*a\| = \|a^2\| \) for all \( a, b \in A \). If \( A \) is commutative, then the Gelfand theorem says that \( A \) is isomorphic to the \( C^* \)-algebra \( C_0(X) \) of continuous complex-valued functions on a locally compact Hausdorff space \( X \). For otherwise, \( A \) represents a noncommutative topological space \( X \).

**B.** Let \( A \) be a \( C^* \)-algebra deemed as a noncommutative topological space. One can ask when two such topological spaces \( A, A' \) are homeomorphic? To answer the question, let us recall the topological \( K \)-theory. If \( X \) is a (commutative) topological space, denote by \( V_C(X) \) an abelian monoid consisting of the isomorphism classes of the complex vector bundles over \( X \) endowed with the Whitney sum. The abelian monoid \( V_C(X) \) can be made to an abelian group, \( K(X) \), using the Grothendieck completion. The covariant functor \( F : X \to K(X) \) is known to map the homeomorphic topological spaces \( X, X' \) to the isomorphic abelian groups \( K(X), K(X') \). Let now \( A, A' \) be the \( C^* \)-algebras. If one wishes to define a homeomorphism between the noncommutative topological spaces \( A, A' \), it will suffice to define an isomorphism between the abelian monoids \( V_C(A) \) and \( V_C(A') \) as suggested by the topological \( K \)-theory. The rôle of the complex vector bundle of degree \( n \) over the \( C^* \)-algebra \( A \) is played by a \( C^* \)-algebra \( M_n(A) = A \otimes M_n \), i.e. the matrix algebra with the entries in \( A \). The abelian monoid \( V_C(A) = \bigcup_{n=1}^{\infty} M_n(A) \) replaces the monoid \( V_C(X) \) of the topological \( K \)-theory. Therefore, the noncommutative topological spaces \( A, A' \) are homeomorphic, if \( V_C(A) \cong V_C(A') \) are isomorphic abelian monoids. The latter equivalence is called a stable isomorphism of the \( C^* \)-algebras \( A \) and \( A' \) and is formally written as \( A \otimes \mathcal{K} \cong A' \otimes \mathcal{K} \), where \( \mathcal{K} = \bigcup_{n=1}^{\infty} M_n \) is the \( C^* \)-algebra of compact operators. Roughly speaking, the stable isomorphism between the \( C^* \)-algebras \( A \) and \( A' \) means that \( A \) and \( A' \) are homeomorphic as the noncommutative topological spaces.

**C.** Let \( A \) be a unital \( C^* \)-algebra and \( V(A) \) be the union (over \( n \)) of projections in the \( n \times n \) matrix \( C^* \)-algebra with entries in \( A \). Projections \( p, q \in V(A) \) are equivalent if there exists a partial isometry \( u \) such that \( p = u^*u \) and \( q = uu^* \). The equivalence class
of projection \( p \) is denoted by \([p]\). The equivalence classes of orthogonal projections can be made to a semigroup by putting \([p]+[q]=[p+q]\). The Grothendieck completion of this semigroup to an abelian group is called a \( K_0 \)-group of algebra \( A \). Functor \( A \to K_0(A) \) maps a category of unital \( C^* \)-algebras into the category of abelian groups so that projections in algebra \( A \) correspond to a positive cone \( K_0^+ \subset K_0(A) \) and the unit element \( 1 \in A \) corresponds to an order unit \( u \in K_0(A) \). The ordered abelian group \((K_0, K_0^+, u)\) with an order unit is called a dimension group.

**D.** An \( AF \)-algebra (approximately finite \( C^* \)-algebra) is defined to be the norm closure of an ascending sequence of the finite dimensional \( C^* \)-algebras \( M_n \)'s, where \( M_n \) is the \( C^* \)-algebra of the \( n \times n \) matrices with the entries in \( \mathbb{C} \). Here the index \( n = (n_1, \ldots, n_k) \) represents a semi-simple matrix algebra \( M_n = M_{n_1} \oplus \cdots \oplus M_{n_k} \). The ascending sequence mentioned above can be written as

\[
M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \cdots,
\]

where \( M_i \) are the finite dimensional \( C^* \)-algebras and \( \varphi_i \) the homomorphisms between such algebras. The set-theoretic limit \( \Lambda = \lim M_n \) has a natural algebraic structure given by the formula \( a_m + b_k \to a + b \); here \( a_m \to a \), \( b_k \to b \) for the sequences \( a_m \in M_m \), \( b_k \in M_k \). The homomorphisms \( \varphi_i \) can be arranged into a graph as follows. Let \( M_i = M_{i_1} \oplus \cdots \oplus M_{i_k} \) and \( M_i' = M_{i_1}' \oplus \cdots \oplus M_{i_k}' \) be the semi-simple \( C^* \)-algebras and \( \varphi_i : M_i \to M_i' \) the homomorphism. One has the two sets of vertices \( V_{i_1}, \ldots, V_{i_k} \) and \( V_{i_1}', \ldots, V_{i_k}' \) joined by the \( a_{i_s} \) edges, whenever the summand \( M_{i_s} \) contains \( a_{i_s} \) copies of the summand \( M_{i_s}' \) under the embedding \( \varphi_i \). As \( i \) varies, one obtains an infinite graph called a Bratteli diagram of the \( AF \)-algebra.

**E.** By \( \mathbb{A}_0 \) we denote an \( AF \)-algebra given by the Bratteli diagram of Fig. 1. It is known that \( K_0(\mathbb{A}_0) \cong \mathbb{Z}^2 \) and \( K_0^+(\mathbb{A}_0) = \{(p, q) \in \mathbb{Z}^2 \mid p + \theta q \geq 0\} \). The \( AF \)-algebras \( \mathbb{A}_0, \mathbb{A}_0' \) are stably isomorphic, i.e. \( \mathbb{A}_0 \otimes K \cong \mathbb{A}_0' \otimes K \), if and only if \( \mathbb{Z} + \theta \mathbb{Z} = \mathbb{Z} + \theta' \mathbb{Z} \) as the subsets of \( \mathbb{R} \).

**1.3. The functor \( F \).**

**A.** The Hubbard-Masur theory (§1.1) has been treated in a general setting so far. From now on, we switch to the case \( g = 1 \) (complex torus). Notice that \( S = \tilde{S} \cong T^2 \), since every holomorphic quadratic differential \( q \) on the complex torus is the square of a holomorphic differential \( \omega \).
ON THE RANK OF ELLIPTIC CURVES

Fig. 2. The measured foliation $\mathcal{F}$ on $T^2 = \mathbb{R}^2/\mathbb{Z}^2$.

B. Let $\phi = R\omega$ be a 1-form defined by $\omega$. Since $\omega$ is holomorphic, $\phi$ is a closed 1-form on $T^2$. The $\mathbb{R}$-isomorphism $h_q : H^0(S, \Omega) \to \text{Hom}(H_1(T^2); \mathbb{R})$, as explained, is given by the formulas:

$$
\begin{align*}
\lambda_1 &= \int_{\gamma_1} \phi, \\
\lambda_2 &= \int_{\gamma_2} \phi,
\end{align*}
$$

where $\{\gamma_1, \gamma_2\}$ is a basis in the first homology group of $T^2$. We further assume that, after a proper choice of the basis, $\lambda_1, \lambda_2$ are positive real numbers.

C. Denote by $\Phi_{T^2}$ the space of measured foliations on $T^2$. Each $\mathcal{F} \in \Phi_{T^2}$ is (measure) equivalent to a foliation by a family of the parallel lines of a slope $\theta$ and the invariant (transverse) measure $\mu$ (Fig. 2).

We use the notation $\mathcal{F}_{\theta}^\mu$ for such a foliation. There exists a simple relationship between the reals $(\lambda_1, \lambda_2)$ and $(\theta, \mu)$. Indeed, the closed 1-form $\phi = \text{Const}$ defines a measured foliation, $\mathcal{F}_{\theta}^\mu$, so that

$$
\begin{align*}
\lambda_1 &= \int_{\gamma_1} \phi = \int_0^1 \mu \, dx, \\
\lambda_2 &= \int_{\gamma_2} \phi = \int_0^1 \mu \, dy,
\end{align*}
$$

where $\frac{dy}{dx} = \theta$.

By the integration:

$$
\begin{align*}
\lambda_1 &= \int_0^1 \mu \, dx = \mu, \\
\lambda_2 &= \int_0^1 \mu \theta \, dx = \mu \theta.
\end{align*}
$$

Thus, one gets $\mu = \lambda_1$ and $\theta = \lambda_2/\lambda_1$.

D. Recall that the Hubbard-Masur theory (§1.1.C) establishes a homeomorphism $h : T_S(1) \to \Phi_{T^2}$, where $T_S(1) \cong \mathbb{H} = \{\tau : \text{Im} \tau > 0\}$ is the Teichmüller space of the torus. Denote by $\omega_N$ an invariant (Néron) differential of the complex torus $\mathbb{C}/(\omega_1 \mathbb{Z} + \omega_2 \mathbb{Z})$. 

It is well known that \( \omega_1 = \int_{\gamma_1} \omega_N \) and \( \omega_2 = \int_{\gamma_2} \omega_N \), where \( \gamma_1 \) and \( \gamma_2 \) are the meridians of the torus. Let \( \pi \) be a projection acting by the formula \( (\theta, \mu) \mapsto \theta \). An explicit formula for the functor \( F : \mathcal{E} \to \mathcal{A} \) is given by the composition: \( F = \pi \circ h \), where \( h \) is the Hubbard-Masur homeomorphism. In other words, one gets the following (explicit) correspondence between the complex and noncommutative tori:

\[
E_\tau = E\left(\frac{\omega_2}{\omega_N}\right) \mapsto (\mathcal{L}) \mapsto \mathcal{F}(\mathcal{L}) \mapsto (\mathcal{L}) \mapsto h_{\mathcal{L}} \equiv h_{\mathcal{L}}(\mathcal{L}) = \mathcal{L} = \theta,
\]

where \( E_\tau = \mathbb{C}/(\mathbb{Z} + \tau \mathbb{Z}) \).

2. Proof

2.1. Proof of Lemma 1. Let \( \varphi : E_\tau \to E_{\tau'} \) be an isogeny of the elliptic curves. The action of \( \varphi \) on the homology basis \{\( \gamma_1, \gamma_2 \)\} of \( T^2 \) is given by the formulas:

\[
\begin{align*}
\gamma'_1 &= a\gamma_1 + b\gamma_2, \\
\gamma'_2 &= c\gamma_1 + d\gamma_2,
\end{align*}
\]

(1)

where \( \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in M_2(\mathbb{Z}) \).

Recall that the functor \( F : \mathcal{E} \to \mathcal{A} \) is given by the formula:

\[
\tau = \frac{\int_{\gamma_2} \omega_N}{\int_{\gamma_1} \omega_N} \mapsto \theta = \frac{\int_{\gamma_2} \phi}{\int_{\gamma_1} \phi}.
\]

(2)

where \( \omega_N \) is an invariant differential on \( E_\tau \) and \( \phi = \text{Re} \omega \) is a closed 1-form on \( T^2 \).

(i) From the left-hand side of (2), one obtains

\[
\begin{align*}
\omega'_1 &= \int_{\gamma'_1} \omega_N = \int_{a\gamma_1 + b\gamma_2} \omega_N = a \int_{\gamma_1} \omega_N + b \int_{\gamma_2} \omega_N = a\omega_1 + b\omega_2, \\
\omega'_2 &= \int_{\gamma'_2} \omega_N = \int_{c\gamma_1 + d\gamma_2} \omega_N = c \int_{\gamma_1} \omega_N + d \int_{\gamma_2} \omega_N = c\omega_1 + d\omega_2,
\end{align*}
\]

(3)

and therefore \( \tau' = \frac{\int_{\gamma'_2} \omega_N}{\int_{\gamma'_1} \omega_N} = (c + d\tau) / (a + b\tau) \).

(ii) From the right-hand side of (2), one obtains

\[
\begin{align*}
\lambda'_1 &= \int_{\gamma'_1} \phi = \int_{a\gamma_1 + b\gamma_2} \phi = a \int_{\gamma_1} \phi + b \int_{\gamma_2} \phi = a\lambda_1 + b\lambda_2, \\
\lambda'_2 &= \int_{\gamma'_2} \phi = \int_{c\gamma_1 + d\gamma_2} \phi = c \int_{\gamma_1} \phi + d \int_{\gamma_2} \phi = c\lambda_1 + d\lambda_2,
\end{align*}
\]

(4)

and therefore \( \theta' = \frac{\int_{\gamma'_2} \phi}{\int_{\gamma'_1} \phi} = (c + d\theta) / (a + b\theta) \).

Comparing (i) and (ii), one gets the conclusion of the first part of Lemma 1. To prove the second part, recall that...
the invertible isogeny is an isomorphism of the elliptic curves. In this case \((a\ b\ c\ d)\in GL_2(\mathbb{Z})\) and \(\theta' = \theta \mod GL_2(\mathbb{Z})\). Therefore \(F\) sends the isomorphic elliptic curves to the stably isomorphic noncommutative tori. The second part of Lemma 1 is proved.

It follows from the proof that \(F: \mathcal{E} \to \mathcal{A}\) is a covariant functor. Indeed, \(F\) preserves the morphisms and does not reverse the arrows: \(F(\varphi_1\varphi_2) = \varphi_1\varphi_2 = F(\varphi_1)F(\varphi_2)\) for any pair of the isogenies \(\varphi_1, \varphi_2 \in \text{Mor}(\mathcal{E})\).

2.2. Proof of Theorem 1. The following lemma will be helpful.

Lemma 2. Let \(m \in \mathbb{R}\) be a module of the rank 2, i.e. \(m = \mathbb{Z}\lambda_1 + \mathbb{Z}\lambda_2\), where \(\theta = \lambda_2/\lambda_1 \notin \mathbb{Q}\). If \(m' \subseteq m\) is a submodule of the rank 2, then \(m' = km\), where either:

(i) \(k \in \mathbb{Z} - \{0\}\) and \(\theta \in \mathbb{R} - \mathbb{Q}\), or

(ii) \(k\) and \(\theta\) are the irrational numbers of a quadratic number field.

Proof. Any rank 2 submodule of \(m\) can be written as \(m' = \lambda'_1\mathbb{Z} + \lambda'_2\mathbb{Z}\), where

\[
\begin{align*}
\lambda'_1 &= a\lambda_1 + b\lambda_2 \\
\lambda'_2 &= c\lambda_1 + d\lambda_2
\end{align*}
\]

and \(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})\).

(i) Let us assume that \(b \neq 0\). Let \(\Delta = (a + d)^2 - 4(ad - bc)\) and \(\Delta' = (a + d)^2 - 4bc\). We shall consider the following cases.

**Case 1.** \(\Delta > 0\) and \(\Delta \neq m^2\), \(m \in \mathbb{Z} - \{0\}\). The real number \(k\) can be determined from the equations:

\[
\begin{align*}
\lambda'_1 &= k\lambda_1 = a\lambda_1 + b\lambda_2, \\
\lambda'_2 &= k\lambda_2 = c\lambda_1 + d\lambda_2.
\end{align*}
\]

Since \(\theta = \lambda_2/\lambda_1\), one gets the equation \(\theta = (c\theta + d)/(a\theta + b)\) by taking a ratio of the two equations above. A quadratic equation for \(\theta\) writes as \(b\theta^2 + (a - d)\theta - c = 0\). The discriminant of the equation coincides with \(\Delta\) and therefore there exist the real roots \(\theta_{1,2} = (a - d \pm \sqrt{\Delta})/(2c)\). Moreover, \(k = a + b\theta = a + (b/(2c))(a - d \pm \sqrt{\Delta})\). Since \(\Delta\) is not the square of an integer, \(k\) and \(\theta\) are the irrationalities of the quadratic number field \(\mathbb{Q}(\sqrt{\Delta})\). 

**Case 2.** \(\Delta > 0\) and \(\Delta = m^2\), \(m \in \mathbb{Z} - \{0\}\). Note that \(\theta = (a - d \pm |m|)/(2c)\) is a rational number. Since \(\theta\) does not satisfy the rank assumption of the lemma, the case should be omitted.

**Case 3.** \(\Delta = 0\). The quadratic equation has a double root \(\theta = (a - d)/(2c) \in \mathbb{Q}\). This case leads to a module of the rank 1, which is contrary to an assumption of the lemma.
**Case 4.** $\Delta < 0$ and $\Delta' \neq m^2, m \in \mathbb{Z} - \{0\}$. Let us define a new basis $[\lambda_1', \lambda_2']$ in $m'$ so that

$$
\begin{align*}
\lambda_1' &= \lambda_1, \\
\lambda_2' &= -\lambda_2.
\end{align*}
$$

Then:

$$
\begin{align*}
\lambda_1'' &= a\lambda_1 + b\lambda_2, \\
\lambda_2'' &= -c\lambda_1 - d\lambda_2,
\end{align*}
$$

and $\theta = \lambda_2''/\lambda_1'' = (-c - d\theta)/(a + b\theta)$. The quadratic equation for $\theta$ has the form $b\theta^2 + (a + d\theta + c = 0$, whose discriminant is $\Delta' = (a + d)^2 - 4bc$. Let us show that $\Delta' > 0$. Indeed, $\Delta = (a + d)^2 - 4(ad - bc) < 0$ and the evident inequality $-(a - d)^2 \leq 0$ have the same sign, and we shall add them up. After an obvious elimination, one gets $bc < 0$.

Therefore $\Delta'$ is a sum of the two positive integers, which is always a positive integer. Thus, there exist the real roots $\theta_{1,2} = (-a - d \pm \sqrt{\Delta})/(2b)$. Moreover, $k = a + b\theta = (1/2)(a - d \pm \sqrt{\Delta'})$. Since $\Delta'$ is not the square of an integer, $k$ and $\theta$ are the irrational numbers in the quadratic field $\mathbb{Q}(\sqrt{\Delta'})$.

**Case 5.** $\Delta < 0$ and $\Delta' = m^2, m \in \mathbb{Z} - \{0\}$. Note that $\theta = (-a - d \pm |m|)/(2b)$ is a rational number. Since $\theta$ does not satisfy the rank assumption of the lemma, the case should be omitted.

(ii) Assume that $b = 0$.

**Case 1.** $a - d \neq 0$. The quadratic equation for $\theta$ degenerates to a linear equation $(a - d)\theta + c = 0$. The root $\theta = c/(d - a) \in \mathbb{Q}$ does not satisfy the rank assumption again, and we omit the case.

**Case 2.** $a = d$ and $c \neq 0$. It is easy to see, that the set of the solutions for $\theta$ is an empty set.

**Case 3.** $a = d$ and $c = 0$. Finally, in this case all coefficients of the quadratic equation vanish, so that any $\theta \in \mathbb{R} - \mathbb{Q}$ is a solution. Note that in the view of (6), $k = a = d \in \mathbb{Z}$. Thus, one gets case (i) of the lemma. Since there are no other possibilities left, Lemma 2 is proved.

**Lemma 3.** Let $E$ be an elliptic curve with a complex multiplication and $h$ the Hubbard-Masur map, which acts by the formulas of §1.3.D. Consider a module $h(\text{Isom}(E)) = \mu_E(\mathbb{Z} + \theta E \mathbb{Z}) := m_E$. Then:

(i) $\theta_E$ is a quadratic irrationality,

(ii) $a\mu_E \in \mathbb{Q}$ (up to a choice of $h$).

Proof. (i) Since $E$ has a complex multiplication, $\text{End}(E) > \mathbb{Z}$. In particular, there exists a nontrivial endomorphism $\varphi$, i.e. an endomorphism which is not the multiplication by $k \in \mathbb{Z}$. By Lemma 1, $\varphi$ defines a submodule $m'_E$ of the rank 2 of the
ON THE RANK OF ELLIPTIC CURVES

module \( m_E \). By Lemma 2, \( m'_E = km_E \) for a \( k \in \mathbb{R} \). Since \( \varphi \) is a nontrivial endomorphism, \( k \notin \mathbb{Z} \). Thus, the option (i) of Lemma 2 is excluded. Therefore, by the item (ii) of Lemma 2, \( \theta_E \) is a quadratic irrationality.

(ii) Recall that \( E_F \subset Q - \{0\} \) is the space of holomorphic differentials on the complex torus, whose horizontal trajectory structure is equivalent to given measured foliation \( F = \mathcal{F}_\mu \). We shall vary \( \mathcal{F}_\mu \), thus varying the Hubbard-Masur homeomorphism \( h = h(\mathcal{F}_\mu): E_F \to T(1) \). Namely, consider a 1-parameter continuous family of such maps \( h = h_\mu \), where \( \theta = \text{Const} \) and \( \mu \in \mathbb{R} \). Recall that \( \mu_E = \lambda_1 \int_{\gamma_1} \phi \), where \( \phi = \text{Re} \omega \) and \( \omega \in E_F \). The family \( h_\mu \) generates a family \( \omega_\mu = h_\mu^{-1}(C) \), where \( C \) is a fixed point in \( T(1) \). Denote by \( \phi_\mu \) and \( \lambda_1^{\mu} \) the corresponding families of the closed 1-forms and their periods, respectively. By the continuity, \( \lambda_1^{\mu} \) takes on a rational value for a \( \mu = \mu' \). (Actually, every neighborhood of \( \mu_0 \) contains such a \( \mu' \).) Thus, \( \mu_E \in \mathbb{Q} \) for the Hubbard-Masur homeomorphism \( h = h_\mu' \).

Lemma 3 implies (i) of Theorem 1. To prove (ii), notice that when \( E_1, E_2 \in \text{Isom}(E_{CM}) \), the respective modules \( m_1 = m_2 \). It follows from the fact that an isomorphism between the elliptic curves corresponds to a change of basis in the module \( m \) (Lemma 1). Theorem 1 is proved.

3. Arithmetic complexity of the noncommutative tori

Let \( \mathbb{A}_0 \) be the noncommutative torus with a real multiplication. Since \( \theta \) is a quadratic irrationality, the regular continued fraction of \( \theta \) is eventually periodic:

\[
\theta = [a_0, a_1, \ldots, \overline{a_{k+1}, \ldots, a_{k+p}}],
\]

where \( \overline{a_{k+1}, \ldots, a_{k+p}} \) is the minimal period of the continued fraction.

**Definition 1.** Let us call the number \( c(\mathbb{A}_0) = p \) an arithmetic complexity of the noncommutative torus with real multiplication.

**Lemma 4.** The number \( c(\mathbb{A}_0) \) is an invariant of the stable isomorphism class of the noncommutative torus \( \mathbb{A}_0 \).

Proof. It follows from Lemma 1 that \( \mathbb{A}_0, \mathbb{A}_0' \) are stably isomorphic if and only if \( \theta' = \theta \mod GL(2, \mathbb{Z}) \). By the main property of the regular continued fractions, the expansion of \( \theta \) and \( \theta' \) must coincide, except possibly a finite number of the entries. Since the continued fraction of \( \theta \) is eventually periodic, so must be the continued fraction of \( \theta' \). Moreover, the minimal periods of \( \theta, \theta' \) must coincide as well as their lengths. Thus \( c(\mathbb{A}_0') = c(\mathbb{A}_0) \).
Example 1. Let us find an arithmetic complexity of the noncommutative torus $\mathbb{A}_{3,\sqrt{6}}$. The continued fraction expansion of $3/\sqrt{6} = 54$ is $[7; 2, 1, 6, 1, 2, 14]$. Since the continued fraction is six-periodic, we have $c(\mathbb{A}_{3,\sqrt{6}}) = 6$.

It is very useful to think of the normalized period $(1/a_{k+2}/a_{k+1}, \ldots, a_{k+p}/a_{k+1})$ of $\mathbb{A}_{\theta}$ as coordinates of the ‘rational points’ of the noncommutative torus, taken up to a cyclic permutation. In the sense, such points are the generators of an abelian group of all rational points of $\mathbb{A}_{\theta}$ modulo the points of a finite order.

Conjecture 1. $c(\mathbb{A}_{\theta_{ECM}}) = rk(E_{CM}) + 1$.

Acknowledgments. I am grateful to Lawrence D. Taylor for the helpful remarks regarding the manuscript. The referee’s suggestions are kindly acknowledged and incorporated in the text.

References

ON THE RANK OF ELLIPTIC CURVES


The Fields Institute for Mathematical Sciences
Toronto, ON
Canada

e-mail: igor.v.nikolaev@gmail.com