INVARIANTS OF STATIONARY AF-ALGEBRAS AND TORSION SUBGROUPS OF ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

IGOR NIKOLAEV

Abstract. Let $G_A$ be an AF-algebra given by a periodic Bratteli diagram with the incidence matrix $A \in GL(n, \mathbb{Z})$. For a given polynomial $p(x) \in \mathbb{Z}[x]$ we assign to $G_A$ a finite abelian group $\text{Ab}_{p(x)}(G_A) = \mathbb{Z}^n / p(A)\mathbb{Z}^n$. It is shown that if $p(0) = \pm 1$ and $\mathbb{Z}[x]/\langle p(x) \rangle$ is a principal ideal domain, then $\text{Ab}_{p(x)}(G_A)$ is an invariant of the strong stable isomorphism class of $G_A$. For $n = 2$ and $p(x) = x - 1$ we conjecture a formula linking values of the invariant and torsion subgroup of elliptic curves with complex multiplication.

1. Introduction

Let $A \in GL(n, \mathbb{Z})$ be a strictly positive integer matrix and consider the following two objects, naturally attached to $A$. The first one, which we denote by $(G_A, \sigma_A)$, is a pair consisting of an AF-algebra, $G_A$, given by an infinite periodic Bratteli diagram with the incidence matrix $A$ and a shift automorphism, $\sigma_A$, canonically attached to $G_A$. (The definitions of an AF-algebra, a Bratteli diagram, and a shift automorphism are given in Section 2.) The second object is an abelian group, which can be introduced as follows. Let $p(x) \in \mathbb{Z}[x]$ be a polynomial over $\mathbb{Z}$, such that $p(0) = \pm 1$ and $\mathbb{Z}[x]/\langle p(x) \rangle$ is a principal ideal domain; here $\langle p(x) \rangle$ means the ideal generated by $p(x)$. Notice that $\mathbb{Z}[x]/\langle p(x) \rangle$ is a principal ideal domain whenever $p(x)$ is an irreducible polynomial and roots of $p(x)$ generate an algebraic number field whose ring of integers is a principal ideal domain.

Consider the following abelian group:

$$\mathbb{Z}^n / p(A)\mathbb{Z}^n := \text{Ab}_{p(x)}(G_A),$$

which we shall call an abelianized $G_A$ at the polynomial $p(x)$. Recall that the AF-algebras $G_A$ and $G_A'$ are said to be stably isomorphic, whenever $G_A \otimes \mathcal{K} \cong G_A' \otimes \mathcal{K}$, where $\mathcal{K}$ is the $C^*$-algebra of compact operators on a Hilbert space $\mathcal{H}$.

---

Partially supported by NSERC.
Definition 1. The AF-algebras $G_A$ and $G_A'$ are said to be strongly stably isomorphic if they are stably isomorphic and $\sigma_A, \sigma_A'$ are the conjugate shift automorphisms.

Roughly speaking, the stable isomorphism is a property of AF-algebra $G_A$, while the strong stable isomorphism is a property of the AF-algebra $G_A$ along with its incidence matrix $A$. The main result of the present note is the following theorem.

Theorem 1. For each polynomial $p(x) \in \mathbb{Z}[x]$, such that $p(0) = \pm 1$ and $\mathbb{Z}[x]/\langle p(x) \rangle$ is a principal ideal domain, the abelian group $\text{Ab}_{p(x)}(G_A)$ is an invariant of the strong stable isomorphism class of the AF-algebra $G_A$.

Remark 1. The reader can find many more numerical invariants of stationary AF-algebras in the remarkable monograph by Bratteli, Jorgensen & Ostrovsky [2]; notice that the authors consider the case when $A$ is not necessarily a unimodular matrix.

Let $E_{CM}$ be an elliptic curve with complex multiplication by an order of conductor $f \geq 1$ in the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$, where $d \neq 1$ [12, p. 96]. Consider a periodic continued fraction $f\omega = [a_0, a_1, \ldots, a_n]$, where $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod{4}$ and $\omega = \sqrt{d}$ if $d \equiv 2, 3 \pmod{4}$. We shall introduce an integer matrix $A = \prod_{i=1}^{n} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$, see Section 4.1 for a motivation.

Conjecture 1. (“Weil’s Conjecture for torsion points”) For each $E_{CM}$ there exists a number field $K$ such that $E_{CM} \cong E(K)$ and a twist of $E(K)$ such that $E_{tors}(K) \cong \text{Ab}_{x-1}(G_A)$, where $E_{tors}(K)$ is the torsion subgroup of $E(K)$.

Remark 2. Conjecture 1 is an analog of (one of) classical Weil’s Conjectures for projective varieties over finite fields [4, pp. 449–451]; indeed, it identifies $E_{tors}(K)$ with the fixed points of an automorphism $A$ of the cohomology group $H^1(E(K); \mathbb{Z})$, see also the last paragraph of Section 3.

The note is organized as follows. The preliminary facts are brought together in Section 2. Theorem 1 is proved in Section 3. In Section 4 conjecture 1 is explained and some examples are given.

2. Preliminaries

An AF-algebra (approximately finite-dimensional 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
Invariants of Stationary AF-Algebras

The 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 $A = \lim M_i$ 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 $V_i, V_{i'}$ and $V_{i'_1}, \ldots, V_{i'_{k'}}$ joined by the $a_{rs}$ edges, whenever the summand $M_{i_r}$ contains $a_{rs}$ 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 $[1]$. The Bratteli diagram defines a unique AF-algebra.

If the homomorphisms $\varphi_1 = 1 = \varphi_2 = \cdots = Const$ in the definition of the AF-algebra $A$, the Bratteli diagram of the AF-algebra $A$ is called stationary. By an abuse of notation, we shall refer to the corresponding AF-algebra as stationary as well. The stationary Bratteli diagram looks like a periodic graph with the incidence matrix $A = (a_{rs})$ repeated over and over again. Since matrix $A$ is a non-negative integer matrix, one can take a power of $A$ to obtain a strictly positive integer matrix which we always assume to be the case. We shall denote the above AF-algebra by $G_A$. Recall that in the case of AF-algebras, the abelian monoid $V_0(A)$ of finitely-generated projective modules over $A$ (and a scale) defines the AF-algebra up to an isomorphism and is known as a dimension group of $A$. We shall use a standard dictionary existing between the AF-algebras and their dimension groups [10, Section 7.3]. Instead of dealing with the AF-algebra $G_A$, we shall work with its dimension group $(K_0(G_A), K_0^+(G_A))$, where $K_0(G_A)$ is the lattice and $K_0^+(G_A)$ is a positive cone inside the lattice given by a sequence of the simplicial dimension groups:

$$\mathbb{Z}^n \overset{\lambda}{\rightarrow} \mathbb{Z}^n \overset{\lambda}{\rightarrow} \mathbb{Z}^n \overset{\lambda}{\rightarrow} \cdots.$$  \hspace{1cm} (2)

(The above notation comes from the $K_0$-group of $G_A$ [10, p. 122].) There exists a natural automorphism, $\sigma_A$, of the dimension group $(K_0(G_A), K_0^+(G_A))$ [3, p. 37]. It can be defined as follows. Let $\lambda_A > 1$ be the Perron-Frobenius eigenvalue and $v_A = (v_A^{(1)}, \ldots, v_A^{(n)}) \in \mathbb{R}_+^n$ the corresponding eigenvector of the matrix $A$. It is known that $K_0^+(G_A)$ is defined by the inequality $\mathbb{Z} v_A^{(1)} + \cdots + \mathbb{Z} v_A^{(n)} \geq 0$ and one can multiply $\mathbb{Z}$-module $\mathbb{Z} v_A^{(1)} + \cdots + \mathbb{Z} v_A^{(n)}$ by $\lambda_A$. It is easy to see that such a multiplication defines an automorphism of the dimension group $(K_0(G_A), K_0^+(G_A))$. The automorphism is called a shift automorphism and denoted by $\sigma_A$. The shift automorphisms $\sigma_A, \sigma_{A'}$. 

Missouri J. of Math. Sci., Spring 2014 25
are said to be conjugate, if \( \sigma_A \circ \theta = \theta \circ \sigma_{A'} \) for some order-isomorphism \( \theta \) between the dimension groups \((K_0(G_A), K_0^+(G_A))\) and \((K_0(G_{A'}), K_0^+(G_{A'}))\).

We shall write this fact as \((G_A, \sigma_A) \cong (G_{A'}, \sigma_{A'})\) (an isomorphism).

**Lemma 1.** The pairs \((G_A, \sigma_A)\) and \((G_{A'}, \sigma_{A'})\) are isomorphic if and only if the matrices \(A\) and \(A'\) are similar.

**Proof.** By Theorem 6.4 of [3], \((G_A, \sigma_A) \cong (G_{A'}, \sigma_{A'})\) if and only if the matrices \(A\) and \(A'\) are shift equivalent, see [14] for a definition of the shift equivalence. On the other hand, since the matrices \(A\) and \(A'\) are unimodular, the shift equivalence between \(A\) and \(A'\) coincides with a similarity of the matrices in the group \(GL(n, \mathbb{Z})\) [14, Corollary 2.13]. \(\square\)

**Corollary 1.** The AF-algebras \(G_A\) and \(G_{A'}\) are strongly stably isomorphic if and only if the matrices \(A\) and \(A'\) are similar.

**Proof.** By a dictionary between the dimension groups and AF-algebras, the order-isomorphic dimension groups correspond to the stably isomorphic AF-algebra [3, Theorem 2.3]. Since \(\sigma_A\) and \(\sigma_{A'}\) are conjugate, one gets a strong stable isomorphism. \(\square\)

**Example 1.** Let us show that Theorem 1 is non-trivial and the condition strong stable isomorphism cannot be relaxed to just stable isomorphism. Consider the unimodular matrices

\[
A = \begin{pmatrix} a & a - 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad A_h = \begin{pmatrix} a - h & (a - h)(h + 1) - 1 \\ 1 & h + 1 \end{pmatrix}, \quad (3)
\]

where \(a, h \in \mathbb{Z}\) and \(a > h \geq 1\). Because eigenvalues of \(A\) and \(A_h\) coincide, one concludes that \((K_0(G_A), K_0^+(G_A)) \cong (K_0(G_{A_h}), K_0^+(G_{A_h}))\), i.e. \(G_A\) and \(G_{A_h}\) are stably isomorphic AF-algebras (see Section 2 for notation). It is verified directly, that \(\theta \circ \sigma_{A_h} = \sigma_A \circ \theta\) for \(\theta = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}\); therefore \(G_A\) and \(G_{A_h}\) are also strongly stably isomorphic. Notice that the strong stable class of \(G_A\) contains more than one representative. Using the Smith normal form of a matrix (see below), one can find that e.g. \(Ab_{x-1}(G_A) \cong Ab_{x-1}(G_{A_h}) \cong \mathbb{Z}_{x-1}\), which is in accord with Theorem 1 for \(p(x) = x - 1\). However, because the eigenvalues \(\lambda_A\) and \(\lambda_{A^2} = \lambda_A^2\) generate the same number field, we have an isomorphism of dimension groups \((K_0(G_A), K_0^+(G_A)) \cong (K_0(G_{A^2}), K_0^+(G_{A^2}))\); on the other hand, because \(tr(A) \neq tr(A^2)\) matrices \(A\) and \(A^2\) (and, therefore, the shift automorphisms \(\sigma_A\) and \(\sigma_{A^2}\)) cannot be conjugate. In this case, the proof of Theorem 1 breaks, see Lemma 1 and Section 3; therefore the condition strong stable isomorphism cannot be replaced by the stable isomorphism alone.
3. Proof of Theorem 1

Our proof is based on the following criterion [3, Theorem 6.4]: the dimension groups

\[ \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^n \rightarrow \cdots \]  

and

\[ \mathbb{Z}^n \xrightarrow{A'} \mathbb{Z}^n \xrightarrow{A'} \mathbb{Z}^n \rightarrow \cdots \]  

are order-isomorphic and \( \sigma_A, \sigma_{A'} \) are conjugate if and only if the matrices \( A \) and \( A' \) are similar in the group \( GL(n, \mathbb{Z}) \), i.e. \( A' = BAB^{-1} \) for a \( B \in GL(n, \mathbb{Z}) \). The rest of the proof follows from the structure theorem for the finitely generated modules given by the matrix \( A \) over a principal ideal domain [11, p. 43]. The result says the normal form of the module (in our case – over the principal ideal domain \( \mathbb{Z}[x]/(p(x)) \)) is independent of the particular choice of a matrix in the similarity class of \( A \).

Before proceeding to a formal proof, let us give an intuitive idea why \( Ab_{p(x)}(G_A) \) is invariant of the similarity class of matrix \( A \). Recall that \( \mathbb{Z}[x]/(p(x)) \) is isomorphic to the ring of integers \( \mathcal{O}_K \) of an algebraic number field \( K = \mathbb{Q}(\alpha) \), where \( \alpha \) is a root of polynomial \( p(x) \). Since \( p(0) = \pm 1 \) one can exclude all rational integer entries of matrix \( A \in GL(n, \mathbb{Z}) \) using equation \( p(\alpha) = 0 \); thus one gets \( A \in GL(n, \mathcal{O}_K) \). But \( \mathcal{O}_K \) is a principal ideal domain (by hypothesis) and, therefore, one can use the Euclidean algorithm to bring \( A \) to a diagonal form (the Smith normal form); the factor of \( \mathcal{O}_K \)-module \( GL(n, \mathcal{O}_K) \) by a submodule defined by matrix \( A \) is a cyclic abelian group – denoted by \( Ab_{p(x)}(G_A) \) – which is independent of the similarity class of matrix \( A \). Let us pass to a step by step argument based on the theory of modules.

Proof. By hypothesis, \( \mathbb{Z}[x]/(p(x)) \) is a principal ideal domain; we shall consider the following \( \mathbb{Z}[x]/(p(x)) \)-module. If \( A \in M_n(\mathbb{Z}) \) is an \( n \times n \) integer matrix, one endows the abelian group \( \mathbb{Z}^n \) with a \( \mathbb{Z}[x]/(p(x)) \)-module structure by defining:

\[ p_n(A)v = (p_n(A))v, \quad p_n(x) \in \mathbb{Z}[x]/(p(x)), \quad v \in \mathbb{Z}^n. \]  

Notice that the obtained module depends on matrix \( A \); we shall write \( (\mathbb{Z}^n)^A \) for this module.

Fix a set of generators \( \{\varepsilon_1, \ldots, \varepsilon_n\} \) of \( (\mathbb{Z}^n)^A \). We shall talk about quotient modules in terms of generators and relations, see e.g. lecture notes by Morandi [6]. The relation submodule can be identified with the kernel of a module homomorphism \( \phi_{p(x)}: (\mathbb{Z}^n)^A \rightarrow \mathbb{Z}^n \) defined by the formula

\[ \{p(x)\varepsilon_1, \ldots, p(x)\varepsilon_n\} \mapsto \sum_{i=1}^n p(x)\varepsilon_i. \]  

The relation matrix is a mapping from the module generators to the relation submodule generators; in our case the relation matrix is \( p(A) \). Since the relation submodule depends on
I. NIKOLAEV

the polynomial \( p(x) \), the factor-module of \( \mathbb{Z}[x]/(p(x)) \) modulo \( \ker \phi_{p(x)} \) will be denoted by \((\mathbb{Z}^n)^A_{p(x)}\).

Let \( G = (g_{ij}) \) be a matrix over the principal ideal domain [11, p. 43]. It is well-known that by the elementary transformations (the Euclidean algorithm) consisting of (i) an interchange of two rows, (ii) a multiplication of a row by \(-1\), (iii) an addition of a multiple of one row to another and similar operations on columns, brings the matrix \((g_{ij})\) to a diagonal form:

\[
D = \begin{pmatrix}
g_1 & & \\
& \ddots & \\
& & g_r \\
& & \\
& & \\
0 & \cdots & 0 \\
\end{pmatrix},
\]

(6)

where \( g_i \) are positive integers, such that \( g_i \mid g_{i+1} \); the latter is known as the Smith normal form of a matrix over the principal ideal domain [11, p. 44]. The elementary transformations are equivalent to a matrix equation \( D = PGQ \), where \( P, Q \in GL(n, \mathbb{Z}) \).

We claim that matrices \( p(A) \) and \( p(A') \) have the same Smith normal form. First, notice that \( p(A) \) and \( p(A') \) are similar matrices. Indeed, we know that \( A' \) is a matrix similar to \( A \), i.e. \( A' = BAB^{-1} \) for a matrix \( B \in GL(n, \mathbb{Z}) \); then it is verified directly that \( p(A') = Bp(A)B^{-1} \), i.e. \( p(A) \) and \( p(A') \) are similar matrices. Now let \( D \) be the Smith normal form of \( p(A) \), then \( D = Pp(A)Q \) for some \( P, Q \in GL(n, \mathbb{Z}) \). If \( B \in GL(n, \mathbb{Z}) \) is such that \( p(A') = Bp(A)B^{-1} \), then \( PB^{-1} \) and \( BQ \) are also in \( GL(n, \mathbb{Z}) \). One gets the following identities:

\[
PB^{-1}(p(A'))BQ = PB^{-1}(Bp(A)B^{-1})BQ = Pp(A)Q = D.
\]

(7)

In other words, \( p(A') \) has the same Smith normal form as \( p(A) \). Recall that the module \((\mathbb{Z}^n)^A_{p(x)}\) can be written as:

\[
(\mathbb{Z}^n)^A_{p(x)} \cong \mathbb{Z}/g_1 \oplus \cdots \oplus \mathbb{Z}/g_r \oplus \mathbb{Z}^{n-r},
\]

(8)

where \( \mathbb{Z}/g_i = \mathbb{Z}/g_i \mathbb{Z} \). Since the same set of integers \( g_i \) will appear in the diagonal form of the matrix \( p(A') \), one gets \( Ab_{p(x)}(G_A) \cong Ab_{p(x)}(G_{A'}) \) for every choice of the polynomial \( p(x) \), such that \( p(0) = \pm 1 \) and \( \mathbb{Z}[x]/(p(x)) \) is a principal ideal domain. (In the practical considerations, we often have \( r = n \) so that our invariant is a finite abelian group.) Theorem 1 follows now from Corollary 1.
The most important special case of the above invariant is when \( p(x) = x - 1 \) (the Bowen-Franks invariant). The invariant takes the form:

\[
Ab_{x-1}(G_A) = \mathbb{Z}^n/(A-I)\mathbb{Z}^n.
\]  

(9)

The Bowen-Franks invariant is covered extensively in the literature [14]; such an invariant has a geometric meaning of tracking an algebraic structure of the periodic points of an automorphism of the lattice \( \mathbb{Z}^n \) defined by the matrix \( A \). In particular, the cardinality of the group \( Ab_{x-1}(G_A) \) is equal to the total number of the isolated fixed points of the automorphism \( A \). It is easy to see that such a number coincides with \( |\det(A-I)| \).

\[\square\]

4. Torsion Conjecture

The basic facts on elliptic curves, complex multiplication, etc., can be found in [12]; an excellent introduction to the subject is [13]. The torsion of rational elliptic curves with complex multiplication was studied in [8]. A link between complex multiplication and \( G_A \) was the subject of [7].

4.1. Teichmüller functor.

Let \( \theta \in [0,1) \) be an irrational number. The universal \( C^* \)-algebra \( A_\theta \) generated by the unitaries \( u \) and \( v \) satisfying the commutation relation \( vu = e^{2\pi i \theta} uv \) is called a noncommutative torus [9], [3, Chapter 5 (p. 34)], and [10, Exercise 5.8, pp. 86–88]. The torus \( A_\theta \) is not an AF-algebra, but can be embedded into an AF-algebra given by the following Bratteli diagram:

\[
\begin{array}{ccc}
& a_0 & a_1 \\
\cdots & \cdots & \cdots \\
\end{array}
\]

Figure 1. The AF-algebra corresponding to \( A_\theta \).

where \( \theta = [a_0, a_1, \ldots] \) is the continued fraction of \( \theta \) [3, p. 65]. A pair of noncommutative tori is said to be stably isomorphic (Morita equivalent) whenever \( A_\theta \otimes K \cong A_{\theta'} \otimes K \), where \( K \) is the \( C^* \)-algebra of compact operators. The \( A_\theta \) is stably isomorphic to \( A_{\theta'} \) 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 trace on projections of \( A_\theta \otimes K \) is a subset \( \Lambda = \mathbb{Z} + \mathbb{Z}\theta \) of the real line; the set \( \Lambda \cong K_0(A_\theta) \) is known as a pseudo-lattice [5]. The noncommutative torus \( A_\theta \) is said to have real multiplication, if \( \theta \) is a quadratic irrationality; we denote such an algebra by \( A_{RM} \). Real multiplication implies non-trivial endomorphisms of the
pseudo-lattice \( \Lambda_{RM} \) given as a multiplication by real numbers – hence the name. Such endomorphisms make a ring under addition and composition of the endomorphisms; the latter is isomorphic to an order of conductor \( f \geq 1 \) in the ring of integers of quadratic field \( \mathbb{Q}(\theta) \). Recall that each order of \( \mathbb{Q}(\sqrt{d}) \) has the form \( \mathbb{Z} + (f\omega)\mathbb{Z} \), where \( \omega = \frac{1 + \sqrt{d}}{2} \) if \( d \equiv 1 \pmod{4} \) and \( \omega = \sqrt{d} \) if \( d \equiv 2, 3 \pmod{4} \). It is known that continued fraction of \( \theta = f\omega \) is periodic and has the form \([a_0, a_1, \ldots, a_n]\); we shall consider a matrix \( A = \prod_{i=1}^{n} \begin{pmatrix} a_i & 1 \\ 0 & 1 \end{pmatrix} \).

Lemma 2. \( K_0(G_A) \cong K_0(A_{RM}) \).

Proof. It follows easily from the definition of \( A \), that \( K_0(G_A) \cong \mathbb{Z} + \mathbb{Z}\theta' \), where \( \theta' = \theta - a_0 \). In other words, \( K_0(G_A) \cong K_0(A_{RM}) \). \( \square \)

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 non-singular elliptic curve via the Weierstrass \( \wp \) function [12, 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, elliptic curve is said to have complex multiplication; we shall denote such curves by \( E_{CM} \). Complex multiplication means that lattice \( L = \mathbb{Z} + \mathbb{Z}\tau \) admits non-trivial endomorphisms given as multiplication of \( L \) by certain complex (quadratic) numbers. Again, such endomorphisms make a ring under addition and composition of the endomorphisms; the latter is isomorphic to an order of conductor \( f \geq 1 \) in the ring of integers of imaginary quadratic field \( \mathbb{Q}(\tau) \).

Our calculations of torsion are based on a covariant functor between elliptic curves and noncommutative tori. Roughly speaking, the functor maps isomorphic curves to the stably isomorphic tori; we refer the reader to [7] for the details and terminology. To give an idea, let \( \phi \) be a closed 1-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 \( F: \mathbb{H} \rightarrow \partial\mathbb{H} \) 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. Remarkably, functor \( F \) maps \( E_{CM} \) to \( A_{RM} \); more specifically, complex multiplication by order of conductor \( f \) in imaginary field \( \mathbb{Q}(\sqrt{-d}) \) goes to real multiplication by an order of conductor \( f \) in the real field \( \mathbb{Q}(\sqrt{d}) \), see an explicit formula for \( F \) [7, p. 524].
4.2. Numerical examples. We conclude by examples supporting Conjecture 1; they cover all rational $E_{CM}$ [8], except $d = -1$ and $d = -163$.

Remark 3. Note that $E_{tors}(\mathbb{Q}) \subseteq E_{tors}(K)$ since $K$ is a non-trivial extension of $\mathbb{Q}$. The reader can see, that $K = \mathbb{Q}$ only for the first two rows; we do not have specific results for $K$ in other cases, but the table admits existence of such a field. The third column lists all twists of $E(\mathbb{Q})$ satisfying conjecture 1.

5. Acknowledgments

I thank G. A. Elliott for the helpful discussions. I am grateful to the referee for extended comments which brought the article to its current shape.

REFERENCES

[1] O. Bratteli, Inductive limits of finite dimensional $C^*$-algebras, Trans. Amer. Math. Soc., 171 (1972), 195–234.
[2] O. Bratteli, P. E. T. Jorgensen, and V. Ostrovsky, Representation Theory and Numerical AF-Invariants, Memoirs Amer. Math. Soc., Vol. 168 (2004).
[3] E. G. Effros, Dimensions and $C^*$-Algebras, Conf. Board of the Math. Sciences, Regional conference series in Math., Vol. 46, AMS, 1981.
[4] R. Hartshorne, Algebraic Geometry, GTM 52, Springer, New York, 1977.
I. NIKOLAEV

[5] Yu. I. Manin, *Real multiplication and noncommutative geometry*, in “Legacy of Niels Hendrik Abel”, 685–727, Springer, New York, 2004.

[6] P. J. Morandi, *The Smith normal form of a matrix*, 2005, available at http://sierra.nmsu.edu/morandi/notes/SmithNormalForm.pdf

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

[8] L. D. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Math., 14 (1974), 195–205.

[9] M. A. Rieffel, *Non-commutative tori – a case study of non-commutative differentiable manifolds*, Contemp. Math., 105 (1990), 191–211. http://math.berkeley.edu/~rieffel/

[10] M. Rørdam, F. Larsen, and N. Laustsen, *An introduction to K-theory for C*-algebras*, London Mathematical Society Student Texts, 49, Cambridge University Press, Cambridge, 2000.

[11] I. R. Shafarevich, *Basic Notions of Algebra*, in Algebra I, E.M.S, Vol. 11, Springer, New York, 1990.

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

[13] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, New York, 1992.

[14] J. B. Wagoner, *Strong shift equivalence theory and the shift equivalence problem*, Bull. Amer. Math. Soc., 36 (1999), 271–296.

MSC2010: 11G15, 46L85

Key words and phrases: AF-algebras, elliptic curves

1505-657 Worcester St., Southbridge, MA 01550

E-mail address: igor.v.nikolaev@gmail.com