Canad. J. Math. Vol. 68 (6), 2016 pp. 1362–1381
http://dx.doi.org/10.4153/CJM-2016-009-9

Optimal Quotients of Jacobians With Toric Reduction and Component Groups

Mihran Papikian and Joseph Rabinoff

Abstract. Let J be a Jacobian variety with toric reduction over a local field K. Let $J \to E$ be an optimal quotient defined over K, where E is an elliptic curve. We give examples in which the functorially induced map $\Phi_J \to \Phi_E$ on component groups of the Néron models is not surjective. This answers a question of Ribet and Takahashi. We also give various criteria under which $\Phi_J \to \Phi_E$ is surjective and discuss when these criteria hold for the Jacobians of modular curves.

1 Introduction

Let J be the Jacobian variety of a smooth, projective, geometrically irreducible curve defined over a field K. An *optimal quotient* of J is an abelian variety E over K and a smooth surjective morphism $\pi: J \to E$ whose kernel is connected, *i.e.*, an abelian variety [7, Definition 3.1]. Henceforth we assume that E is an elliptic curve and K is a local field. The following question, originally posed by Ribet and Takahashi, appears in a letter from Matt Baker to Ken Ribet in 2009.

Question 1.1 Assume J has (purely) toric reduction; see §2.7 for the definition. Is the functorially induced map $\pi_*: \Phi_J(\overline{k}) \to \Phi_E(\overline{k})$ on component groups of the Néron models of J and E necessarily surjective, where $\overline{k}$ is the algebraic closure of the residue field of K?

In Section 5, we will construct examples which show that the answer is "no", contrary to the expectation expressed by Baker in the aforementioned letter. The interest in Question 1.1 comes from arithmetic geometry, where for certain modular Jacobians, such as $J_0(p)$ over $\mathbb{Q}_p$, the answer was known to be positive; see Section 4. It is natural then to ask whether the surjectivity of the map on component groups is a general geometric property of Jacobians with toric reduction, or whether it is a special arithmetic property of modular Jacobians with toric reduction. Our examples indicate that the latter is the case. Of course, Question 1.1 makes perfect sense without assuming that J has toric reduction, but the answer to that more general question was known to be negative even for the modular Jacobians $J_0(N)$ of small levels. The following example is due to William Stein.

Received by the editors March 2, 2015; revised February 17, 2016.
Published electronically August 19, 2016.
Author M. P. was supported in part by the Simons Foundation.
AMS subject classification: **11G18**, 14G22, 14G20.
Keywords: Jacobians with toric reduction, component groups, modular curves.

Example 1.2 There is a unique weight-2 newform of level 33 with integer Fourier coefficients, and the corresponding optimal quotient of $J_0(33)$ is the elliptic curve $E : y^2 + xy = x^3 + x^2 - 11x$. Consider the optimal quotient $\pi: J_0(33) \to E$ over $\mathbb{Q}_3$. The reduction of $J_0(33)$ over $\mathbb{Q}_3$ is semi-stable but not toric. By [18, p. 174], $\Phi_{J_0(33)}(\overline{\mathbb{F}}_3) \cong \mathbb{Z}/2\mathbb{Z}$. On the other hand, $\Phi_E(\overline{\mathbb{F}}_3) \cong \mathbb{Z}/6\mathbb{Z}$, so π_* is not surjective.

The idea of our construction giving a negative answer to Question 1.1 is to take two elliptic curves E_1 and E_2 over K with multiplicative reduction and non-trivial component groups. We show that one can choose a finite subgroup-scheme G of the abelian surface $E_1 \times E_2$ such that the quotient $J = (E_1 \times E_2)/G$ is a Jacobian variety and $\Phi_J = 1$. Moreover, E_1 and E_2 are optimal quotients of J. Due to §2.8 below, J automatically has toric reduction. Clearly the corresponding maps on component groups cannot be surjective. The study of Jacobians isogenous to a product of two elliptic curves has a long history dating back to Legendre and Jacobi. In more recent times such Jacobians have found applications in a variety of arithmetic problems, for example, the construction of curves with a maximal number of rational points over finite fields [26], or the construction of Jacobians over $\mathbb{Q}$ with large rational torsion subgroups [15].

From the work of Gerittzen, Mumford, and others it is known that abelian varieties with toric reduction have rigid-analytic uniformizations. (In fact any abelian variety has such a uniformization, but we will only be concerned with the totally degenerate case.) In Section 3, we investigate the map $\pi_*: \Phi_J \to \Phi_E$ using analytic techniques. Some of our arguments here are inspired by [10,23,31]. We show that the Tate period of E can be obtained from J via a natural evaluation map. In this construction, which is a generalization of the constructions due to Gekeler and Reversat [11], Bertolini and Darmon [2], and Takahashi [28], the uniformizing lattice of J maps to a subgroup in $K^\times$ isomorphic to $\mathbb{Z}/c\mathbb{Z} \oplus \mathbb{Z}$. We show that the cokernel of π_* is isomorphic to $\mathbb{Z}/c\mathbb{Z}$. We also show that c is closely related to the denominator of the idempotent in $\mathrm{End}(J) \otimes \mathbb{Q}$ corresponding to E. These results are of independent interest, and could be useful in the theory of Mumford curves. The main theorem of this section is Theorem 3.6, which gives equivalent conditions for π_* to be surjective. One of these conditions shows that Question 1.1 can be interpreted as an analogue for Mumford curves of the problem of the equality of the degree of modular parametrization of an elliptic curve over $\mathbb{Q}$ and the congruence number of the corresponding newform; see Remark 3.7. At the end of Section 3, we give two additional criteria for π_* being surjective, which are based on an assumption that $\mathrm{End}(J)$ contains a subring with certain properties; see Lemmas 3.8 and 3.9.

In Section 4, we discuss Question 1.1 in the context of Jacobians of modular curves. We show that this question has a positive answer for the following cases:

- $J_0(p)$ considered over $\mathbb{Q}_p$ (see Theorem 4.1),
- the Jacobian of Drinfeld modular curve $X_0(\mathfrak{n})$ of arbitrary level $\mathfrak{n} \in \mathbb{F}_q[T]$ considered over $\mathbb{F}_q((1/T))$ (see Theorem 4.4).

(Theorem 4.1 was known, but we give a different proof which relies on Lemma 3.9.) In this section we also point out a mistake in the published literature. Let $J_0^D(M)$ be the Jacobian of the Shimura curve over $\mathbb{Q}$ associated with an Eichler order of level M

in an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant D. For any prime p dividing D, the Jacobian $J_0^D(M)$ has toric reduction over $\mathbb{Q}_p$. Takahashi [27, Theorem 2.4] claimed that π_* is surjective in this case. The proof of this theorem crucially relies on a result of Bertolini and Darmon [2, Proposition 4.4]. Unfortunately, the proof of this latter proposition has a gap, *cf.* §4.2, so Question 1.1 in this case remains a very interesting open problem. Theorem 3.6 could be useful for a computational investigation of this problem; see Remark 4.3.

2 Néron Models

For the convenience of the reader and future reference we collect in this section some terminology and facts about abelian varieties and their Néron models. The standard reference for the theory of Néron models is [4].

2.1 Henceforth, we assume that K is a field equipped with a nontrivial discrete valuation $\mathrm{ord}_K\colon K \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$. Let $R = \{z \in K \mid \mathrm{ord}_K(z) \geq 0\}$ be its ring of integers. Let $\mathfrak{m} = \{z \in K \mid \mathrm{ord}_K(z) > 0\}$ be the maximal ideal of R, and $k = R/\mathfrak{m}$ be the residue field. Assume that k is a finite field of characteristic p, and define the non-archimedean absolute value on K by $|x| = (\#k)^{-\mathrm{ord}_K(x)}$. Finally, assume K is complete for the topology defined by this absolute value. Overall, our assumptions mean that K is a *local field*. It is known that every local field is isomorphic either to a finite extension of $\mathbb{Q}_p$ or to the field of formal Laurent series $k((x))$. We denote by $\mathbb{C}_K$ the completion of an algebraic closure $\overline{K}$ of K with respect to the extension of the absolute value (which is itself algebraically closed).

2.2 If X is a scheme over the base S and $T \to S$ is any base change, X_T will denote the pullback of X to T. If $T = \mathrm{Spec}(A)$, we may also denote this scheme by X_A. By $X(T)$ we mean the T-rational points of the S-scheme X, and again, if $T = \mathrm{Spec}(A)$, we may also denote this set by $X(A)$.

2.3 Let X be a scheme over K. A *model* of X over R is an R-scheme $\mathscr{X}$ such that its generic fiber $\mathscr{X}_K$ is isomorphic to X. Let A be an abelian variety over K. There is a model $\mathscr{A}$ of A which is smooth, separated, and of finite type over R, and which satisfies the following universal property. For each smooth R-scheme $\mathscr{X}$ and each K-morphism $\phi_K\colon \mathscr{X}_K \to A$ there is a unique R-morphism $\phi\colon \mathscr{X} \to \mathscr{A}$ extending ϕ_K. The model $\mathscr{A}$ is called the *Néron model* of A. It is obvious from the universal property that $\mathscr{A}$ is uniquely determined by A, up to unique isomorphism. Moreover, the group scheme structure of A uniquely extends to a commutative R-group scheme structure on $\mathscr{A}$, and $A(K) = \mathscr{A}(R)$.

2.4 The closed fibre $\mathscr{A}_k$ is usually not connected. Let $\mathscr{A}_k^0$ be the connected component of the identity section. There is an exact sequence

$$0 \to \mathscr{A}_k^0 \to \mathscr{A}_k \to \Phi_A \to 0,$$

where Φ_A is a finite étale group scheme over k. The group Φ_A is called the *group of connected components* of A.

2.5 Let $f_K: A \to B$ be a morphism of abelian varieties. By the Néron mapping property, the morphism f_K extends to a homomorphism $f: \mathscr{A} \to \mathscr{B}$. Restricting to the closed fibres, we get a homomorphism $f_k: \mathscr{A}_k \to \mathscr{B}_k$. This homomorphism maps $\mathscr{A}_k^0$ into $\mathscr{B}_k^0$. Hence there are induced homomorphisms $f_k^0: \mathscr{A}_k^0 \to \mathscr{B}_k^0$ and $f_*: \Phi_A \to \Phi_B$. We say that f_* is surjective, if the homomorphism of abelian groups $f_*: \Phi_A(\overline{k}) \to \Phi_B(\overline{k})$ is surjective.

2.6 Let K' be an unramified extension of K. Let R' be the ring of integers of K'. Let $f_{K'}: A_{K'} \to B_{K'}$ be the base change of f_K to K'. Then $f \otimes R': \mathscr{A} \otimes_R R' \to \mathscr{B} \otimes_R R'$ is the corresponding morphism of the Néron models [4, Corollary 7.2/2]. This implies that $f_*: \Phi_A(\overline{k}) \to \Phi_B(\overline{k})$ does not change under unramified field extensions of K.

2.7 By a theorem of Chevalley, $\mathscr{A}_k^0$ is uniquely an extension of an abelian variety B by a connected affine group $T \times U$ over k, where T is an algebraic torus and U is a unipotent algebraic group [4, §9.2]. We say that A has

- *good reduction* if U and T are trivial,
- *semi-stable reduction* if U is trivial,
- *toric reduction* if U and B are trivial,
- *split toric reduction* if U and B are trivial, and T is a split torus over k.

Some authors say that A has *purely* toric reduction over K when U and B are trivial. If A is an elliptic curve, then it is more common to say that A has *multiplicative* (resp. *split multiplicative*) reduction over K, instead of toric (resp. split toric) reduction.

2.8 If A has toric reduction and $f_K: A \to B$ is an isogeny, then f_k^0 is an isogeny [4, Corollary 7.3/7]. This implies that B also has toric reduction. If $f_K: B \to A$ is a closed immersion of abelian varieties and A has toric reduction, then f_k^0 is a closed immersion; see the proof of Theorem 8.2 in [7]. This implies that if A has (split) toric reduction, then any abelian subvariety of A also has (split) toric reduction. Denote by $A^\vee$ and $B^\vee$ the abelian varieties dual to A and B, respectively. Then f_K is an optimal quotient if and only if the dual morphism $f_K^\vee: B^\vee \to A^\vee$ is a closed immersion [7, Proposition 3.3].

3 Rigid-analytic Constructions

First, we briefly review some facts from the theory of rigid-analytic uniformization of abelian varieties. The abelian varieties in this section are assumed to have split toric reduction over K. Since an abelian variety with toric reduction acquires split toric reduction over an unramified extension of K, as far as the questions of surjectivity of the maps of component groups are concerned, the assumption that the reduction is split is not restrictive; *cf.* §2.6.

3.1 Let $\mathfrak{T} := (\mathbb{G}_{m,K}^g)^{\mathrm{an}}$ be the rigid-analytification of

$$\mathbb{G}_{m,K}^g = \operatorname{Spec} K[Z_1, Z_1^{-1}, \dots, Z_g, Z_g^{-1}].$$

https://doi.org/10.4153/CJM-2016-009-9 Published online by Cambridge University Press

A *character* of $\mathfrak{T}$ is a homomorphism of rigid-analytic groups $\chi\colon\mathfrak{T}\to\mathbb{G}_{m,K}^{\mathrm{an}}$. Denote the group of characters of $\mathfrak{T}$ by $\mathcal{X}(\mathfrak{T})$. It is known that analytic characters are all algebraic:

$$\mathcal{X}(\mathfrak{T})=\{Z_1^{n_1}\cdots Z_g^{n_g}\mid(n_1,\dots,n_g)\in\mathbb{Z}^g\}.$$

In fact, a stronger statement is true: any holomorphic, nowhere vanishing function on $\mathfrak{T}$ is a constant multiple of an algebraic character [9, §6.3]. Consider the group homomorphism

$$\begin{aligned}\mathrm{trop}\colon\mathfrak{T}(\mathbb{C}_K)&\to\mathrm{Hom}(\mathcal{X}(\mathfrak{T}),\mathbb{R})\approx\mathbb{R}^g\\ x&\mapsto(\chi\mapsto-\log|\chi(x)|).\end{aligned}$$

A (split) *lattice* Λ in $\mathfrak{T}$ is a free rank-g subgroup of $\mathfrak{T}(K)$ such that $\mathrm{trop}\colon\Lambda\to\mathbb{R}^g$ is injective and its image is a lattice in the classical sense. Such Λ is discrete in $\mathfrak{T}$, *i.e.*, the intersection of Λ with any affinoid subset of $\mathfrak{T}$ is finite. Hence we can form the quotient $\mathfrak{T}/\Lambda$ in the usual way by gluing the Λ-translates of a small enough affinoid. The Riemann form condition in this setting is the following.

Theorem 3.1 *$\mathfrak{T}/\Lambda$ is isomorphic to the rigid-analytification of an abelian variety over K if and only if there is a homomorphism $H\colon\Lambda\to\mathcal{X}(\mathfrak{T})$ such that $H(\lambda)(\mu)=H(\mu)(\lambda)$ for all $\lambda,\mu\in\Lambda$, and the symmetric bilinear form*

$$\begin{aligned}\langle\cdot,\cdot\rangle_H\colon\Lambda\times\Lambda&\to\mathbb{Z}\\ \lambda,\mu&\mapsto\mathrm{ord}_K H(\lambda)(\mu)\end{aligned}$$

is positive definite.

Proof See [9, Chapter 6] or [3, §2]. ∎

3.2 Let A be an abelian variety of dimension g defined over K. We say that A is *uniformizable by a torus* if $A^{\mathrm{an}}\cong\mathfrak{T}/\Lambda$ for some lattice Λ.

Theorem 3.2 *An abelian variety over K is uniformizable by a torus if and only if it has split toric reduction.*

Proof See [3, §1]. ∎

3.3 If A has split toric reduction, then $A^\vee$ also has split toric reduction; *cf.* §2.8. Let $\mathfrak{T}/\Lambda$ be the uniformization of A. Denote $\mathfrak{T}^\vee=\mathrm{Hom}(\Lambda,\mathbb{G}_{m,K}^{\mathrm{an}})$ and $\Lambda^\vee=\mathrm{Hom}(\mathfrak{T},\mathbb{G}_{m,K}^{\mathrm{an}})$. Note that $\Lambda^\vee$ is the group of characters $\mathcal{X}(\mathfrak{T})$. We have a natural bilinear pairing $\Lambda^\vee\times\mathfrak{T}(K)\to K^\times$ given by evaluation of characters on the points of $\mathfrak{T}$. For a fixed $\lambda'\in\Lambda^\vee$, this pairing induces, by restriction, a homomorphism $\Lambda\to K^\times$, $\lambda\mapsto\lambda'(\lambda)$, and hence a K-valued point in $\mathfrak{T}^\vee$. If we vary $\lambda'\in\Lambda^\vee$, we obtain a canonical homomorphism $\Lambda^\vee\to\mathfrak{T}^\vee$, which is easily seen to be the dual of $\Lambda\to\mathfrak{T}$. Hence $\Lambda^\vee$ is naturally a lattice in $\mathfrak{T}^\vee$, and we can form the quotient $\mathfrak{T}^\vee/\Lambda^\vee$ as a proper rigid-analytic group. As one might expect, $\mathfrak{T}^\vee/\Lambda^\vee$ is canonically isomorphic to $(A^\vee)^{\mathrm{an}}$; see [3, Theorem 2.1]. Let $H\colon\Lambda\to\Lambda^\vee$ be a Riemann form for A. Applying $\mathrm{Hom}(\cdot,\mathbb{G}_{m,K}^{\mathrm{an}})$ to H, we get a surjective homomorphism $H_{\mathfrak{T}}\colon\mathfrak{T}\to\mathfrak{T}^\vee$. From the definitions it is easy to see that the restriction of $H_{\mathfrak{T}}$ to $\Lambda\subset\mathfrak{T}$ is H. Hence we get a homomorphism

https://doi.org/10.4153/CJM-2016-009-9 Published online by Cambridge University Press

$H_{A^{\mathrm{an}}}: A^{\mathrm{an}} \to (A^\vee)^{\mathrm{an}}$. By GAGA, $H_{A^{\mathrm{an}}}$ canonically corresponds to a homomorphism $H_A: A \to A^\vee$. Since H is injective with finite cokernel, H_A is an isogeny. In fact, one can show that H_A is a polarization and every polarization arises in this manner; *cf.* [3, §2].

3.4 More symmetrically, let Λ and $\Lambda^\vee$ be two finitely generated free abelian groups of the same rank and let $[\,\cdot\,,\cdot\,]: \Lambda \times \Lambda^\vee \to K^\times$ be a bilinear pairing such that the pairing $\langle\,\cdot\,,\cdot\,\rangle = \mathrm{ord}_K \circ [\,\cdot\,,\cdot\,]: \Lambda \times \Lambda^\vee \to \mathbb{Z}$ becomes perfect after extending scalars from $\mathbb{Z}$ to $\mathbb{R}$. Let $\mathfrak{T} = \mathrm{Hom}(\Lambda^\vee, \mathbb{G}_{m,K}^{\mathrm{an}})$ and $\mathfrak{T}^\vee = \mathrm{Hom}(\Lambda, \mathbb{G}_{m,K}^{\mathrm{an}})$. Then $[\,\cdot\,,\cdot\,]$ defines injective homomorphisms $\Lambda \hookrightarrow \mathfrak{T}(K)$ and $\Lambda^\vee \hookrightarrow \mathfrak{T}^\vee(K)$, the images of which are lattices. With these notations, a Riemann form is a homomorphism $H: \Lambda \to \Lambda^\vee$ such that $[\,\cdot\,,\cdot\,]_H = [\,\cdot\,, H(\cdot)]$ is symmetric and $\langle\,\cdot\,,\cdot\,\rangle_H = \langle\,\cdot\,, H(\cdot)\rangle$ is positive-definite. If such a form exists, then $\mathfrak{T}/\Lambda$ and $\mathfrak{T}^\vee/\Lambda^\vee$ are dual abelian varieties.

3.5 Let $A_1^{\mathrm{an}} = \mathfrak{T}_1/\Lambda_1$ and $A_2^{\mathrm{an}} = \mathfrak{T}_2/\Lambda_2$ be uniformizable abelian varieties. Let $\mathrm{Hom}(\mathfrak{T}_1, \Lambda_1\,;\mathfrak{T}_2, \Lambda_2)$ denote the group of homomorphisms $\varphi: \mathfrak{T}_1 \to \mathfrak{T}_2$ of analytic tori such that $\varphi(\Lambda_1) \subset \Lambda_2$. By a result of Gerritzen [12], the natural map

$$\mathrm{Hom}(\mathfrak{T}_1, \Lambda_1\,; \mathfrak{T}_2, \Lambda_2) \to \mathrm{Hom}(A_1, A_2)$$

is a bijection (see also [14, §7]).

Following the notations in §3.4, for $i = 1, 2$ let $\Lambda_i^\vee = \mathfrak{X}(\mathfrak{T}_i)$, let $\mathfrak{T}_i^\vee$ be the torus with character lattice Λ_i, let $[\,\cdot\,,\cdot\,]_i: \Lambda_i \times \Lambda_i^\vee \to K^\times$ denote the pairing induced by the inclusion $\Lambda_i \hookrightarrow \mathfrak{T}_i(K)$, and let $\langle\,\cdot\,,\cdot\,\rangle_i = \mathrm{ord} \circ [\,\cdot\,,\cdot\,]_i$. Let $\varphi \in \mathrm{Hom}(\mathfrak{T}_1, \Lambda_1; \mathfrak{T}_2, \Lambda_2)$. Then φ is determined by the induced homomorphism $\varphi^\vee: \Lambda_2^\vee \to \Lambda_1^\vee$ of character groups, and since $\varphi(\Lambda_1) \subset \Lambda_2$, we have

$$[\varphi(\lambda_1), \lambda_2^\vee]_2 = [\lambda_1, \varphi^\vee(\lambda_2^\vee)]_1 \tag{3.1}$$

for all $\lambda_1 \in \Lambda_1$ and $\lambda_2^\vee \in \Lambda_2^\vee$. We can therefore define $\mathrm{Hom}(\mathfrak{T}_1, \Lambda_1\,;\,\mathfrak{T}_2, \Lambda_2)$ more symmetrically as the group of pairs $(\varphi, \varphi^\vee)$ of homomorphisms $\varphi: \Lambda_1 \to \Lambda_2$ and $\varphi^\vee: \Lambda_2^\vee \to \Lambda_1^\vee$ satisfying (3.1). Since $\langle\,\cdot\,,\cdot\,\rangle_i$ is nondegenerate for $i = 1, 2$, it is clear that φ and $\varphi^\vee$ determine each other. If $(\varphi, \varphi^\vee) \in \mathrm{Hom}(\mathfrak{T}_1, \Lambda_1\,;\mathfrak{T}_2, \Lambda_2)$ corresponds to the homomorphism $f: A_1 \to A_2$, then $(\varphi^\vee, \varphi) \in \mathrm{Hom}(\mathfrak{T}_2^\vee, \Lambda_2^\vee\,;\,\mathfrak{T}_1^\vee, \Lambda_1^\vee)$ corresponds to the dual homomorphism $f^\vee: A_2^\vee \to A_1^\vee$.

Now let $H_i: \Lambda_i \xrightarrow{\sim} \Lambda_i^\vee$ be Riemann forms determining principal polarizations $A_i \xrightarrow{\sim} A_i^\vee$ for $i = 1, 2$. Using H_i to identify Λ_i with $\Lambda_i^\vee$, we can describe an element of $\mathrm{Hom}(\mathfrak{T}_1, \Lambda_1\,;\mathfrak{T}_2, \Lambda_2)$ as a pair $(\varphi, \varphi^\vee)$, where $\varphi: \Lambda_1 \to \Lambda_2$ and $\varphi^\vee: \Lambda_2 \to \Lambda_1$ are homomorphisms satisfying $[\varphi(\lambda_1), \lambda_2]_{H_2} = [\lambda_1, \varphi^\vee(\lambda_2)]_{H_1}$ for all $\lambda_1 \in \Lambda_1$ and $\lambda_2 \in \Lambda_2$. As above, if $(\varphi, \varphi^\vee)$ corresponds to the homomorphism $f: A_1 \to A_2$, then $(\varphi^\vee, \varphi)$ corresponds to the dual homomorphism $f^\vee: A_2 \cong A_2^\vee \to A_1^\vee \cong A_1$.

Proposition 3.3 *Assume $A^{\mathrm{an}} \cong \mathfrak{T}/\Lambda$ is a principally polarizable abelian variety. Fix a principal polarization $H: \Lambda \xrightarrow{\sim} \mathfrak{X}(\mathfrak{T})$. An endomorphism $T \in \mathrm{End}(A)$ induces an endomorphism of Λ, which we denote by the same letter. Let $T^\dagger \in \mathrm{End}(A)$ be the image of T under the Rosati involution with respect to the principal polarization H. Then for any $\lambda, \mu \in \Lambda$, $H(T\lambda)(\mu) = H(\lambda)(T^\dagger\mu)$.*

Proof Let $\Lambda^\vee = \mathfrak{X}(\mathfrak{T})$ and let $[\,\cdot\,,\cdot\,]\colon \Lambda\times\Lambda^\vee \to K^\times$ be the pairing induced by the inclusion $\Lambda \hookrightarrow \mathfrak{T}(K)$, as in §3.4. By §3.5, we can describe T as a pair of endomorphisms $\varphi, \varphi^\vee\colon \Lambda \to \Lambda$ satisfying

$$H(\varphi(\lambda))(\lambda') = [\varphi(\lambda),\, \lambda']_H = [\lambda,\, \varphi^\vee(\lambda')]_H = H(\lambda)(\varphi^\vee(\lambda'))$$

for all $\lambda, \lambda' \in \Lambda$. The endomorphism $T^\dagger$ then corresponds to the pair $(\varphi^\vee, \varphi)$. Under these identifications, the endomorphism of Λ induced by T (resp. $T^\dagger$) is exactly φ (resp. $\varphi^\vee$). ∎

3.6 Let $J := \mathrm{Pic}^0_{X/K}$ be the Jacobian variety of a smooth, projective, geometrically irreducible curve X over K. Assume J has split toric reduction; this is equivalent to X being a Mumford curve. Let H be the canonical principal polarization on J. The uniformization of J is given by $0 \to \Lambda \xrightarrow{H} \mathrm{Hom}(\Lambda, \mathbb{C}_K^\times) \to J(\mathbb{C}_K) \to 0$.

Remark More generally, throughout this section we could take J to be any abelian variety with split toric reduction and a fixed K-rational principal polarization. We only assume that J is a Jacobian for consistency with the sequel.

Let E be an elliptic curve which is an optimal quotient $\pi\colon J \to E$. Using the canonical principal polarizations on E and J, we can consider E as an abelian subvariety of J via the dual morphism $\pi^\vee\colon E \hookrightarrow J$; *cf.* §2.8. Sometimes to emphasize that we consider E as the image of π (resp. the domain of $\pi^\vee$) we will write E_* (resp. E^*).

To simplify the notation, we will denote the pairing $\langle\,\cdot\,,\cdot\,\rangle_H$ of Theorem 3.1 for the canonical principal polarization on J by $\langle\,\cdot\,,\cdot\,\rangle$. Likewise we denote the pairing $[\,\cdot\,,\cdot\,]_H\colon \Lambda\times\Lambda \to K^\times$ of §3.4 by $[\,\cdot\,,\cdot\,]$.

3.7 Since E is a subvariety of J, it has split toric reduction; *cf.* §2.8. Therefore E is uniformizable by a torus $0 \to \Gamma \to \mathbb{C}_K^\times \to E(\mathbb{C}_K) \to 0$, where Γ, as a subgroup of $\mathbb{C}_K^\times$, is $q_E^{\mathbb{Z}}$ for some $q_E \in \mathbb{C}_K^\times$ with $\mathrm{ord}_K(q_E) > 0$. More precisely, since E carries a canonical principal polarization, it is uniformized by the torus $\mathrm{Hom}(\Gamma, \mathbb{C}_K^\times)$; fixing a generator ρ of Γ, we identify $\mathrm{Hom}(\Gamma, \mathbb{C}_K^\times)$ with $\mathbb{C}_K^\times$ via the isomorphism $f \mapsto f(\rho)$. By §3.5, the closed immersion $\pi^\vee\colon E \to J$ induces a homomorphism $\pi^\vee\colon \Gamma \to \Lambda$ and a homomorphism of tori $\mathbb{C}_K^\times \to \mathrm{Hom}(\Lambda, \mathbb{C}_K^\times)$ making the following diagram commute:

(3.2)
$$\begin{tikzcd}
0 \arrow[r] & \Gamma \arrow[r] \arrow[d, "\pi^\vee"'] & \mathbb{C}_K^\times \arrow[r] \arrow[d] & E(\mathbb{C}_K) \arrow[r] \arrow[d, "\pi^\vee"] & 0 \\
0 \arrow[r] & \Lambda \arrow[r] & \mathrm{Hom}(\Lambda, \mathbb{C}_K^\times) \arrow[r] & J(\mathbb{C}_K) \arrow[r] & 0
\end{tikzcd}$$

It is easy to see that the vertical arrows in (3.2) are injective. In general, $\pi^\vee(\Gamma)$ need not be saturated in Λ, *i.e.*, the abelian group $\Lambda/\pi^\vee(\Gamma)$ might have non-trivial torsion. Let Γ' be the saturation of $\pi^\vee(\Gamma)$ in Λ. We can write $\pi^\vee(\rho) = c\cdot\lambda_E$, where c is a uniquely determined positive integer, λ_E is a generator of Γ', and ρ is our fixed generator of Γ.

3.8 Let $\pi\colon \Lambda \to \Gamma$ be the homomorphism of character groups associated with the middle vertical arrow of (3.2). The homomorphism $\pi^\vee\colon \Gamma \to \Lambda$ induces the homomorphism of tori $\mathrm{ev}_\rho\colon \mathrm{Hom}(\Lambda, \mathbb{C}_K^\times) \to \mathrm{Hom}(\Gamma, \mathbb{C}_K^\times) = \mathbb{C}_K^\times$ given by $\mathrm{ev}_\rho(f) = f(\pi^\vee(\rho))$. By the discussion in §3.5, the following diagram commutes:

$$\begin{tikzcd} 0 \arrow[r] & \Lambda \arrow[r] \arrow[d, "\pi"'] & \mathrm{Hom}(\Lambda, \mathbb{C}_K^\times) \arrow[r] \arrow[d, "\mathrm{ev}_\rho"'] & J(\mathbb{C}_K) \arrow[r] \arrow[d, "\pi"] & 0 \\ 0 \arrow[r] & \Gamma \arrow[r] & \mathbb{C}_K^\times \arrow[r] & E(\mathbb{C}_K) \arrow[r] & 0 \end{tikzcd} \tag{3.3}$$

It is easy to see that the vertical arrows in (3.3) are surjective.

3.9 Let $c^{-1}\Gamma = \{x \in \mathbb{C}_K^\times \mid x^c \in \Gamma\}$. Since $\Gamma = q_E^{\mathbb{Z}}$, we have $c^{-1}\Gamma = \mu_c \times w^{\mathbb{Z}}$, where $\mu_c \subset \mathbb{C}_K^\times$ is the group of c-th roots of unity and w is any c-th root of q_E. In particular, $\mathrm{ord}_K(q_E) = c \cdot \mathrm{ord}_K(w)$. Define $\mathrm{ev}_E : \mathrm{Hom}(\Lambda, \mathbb{C}_K^\times) \to \mathbb{C}_K^\times$ by $\mathrm{ev}_E(f) = f(\lambda_E)$. Then $\mathrm{ev}_E^c = \mathrm{ev}_\rho$, so we have a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \Lambda \arrow[r] \arrow[d] & \mathrm{Hom}(\Lambda, \mathbb{C}_K^\times) \arrow[r] \arrow[d, "\mathrm{ev}_E"'] & J(\mathbb{C}_K) \arrow[r] \arrow[d, "\pi"] & 0 \\ 0 \arrow[r] & c^{-1}\Gamma \arrow[r] & \mathbb{C}_K^\times \arrow[r] & E(\mathbb{C}_K) \arrow[r] & 0 \end{tikzcd} \tag{3.4}$$

where the map $\mathbb{C}_K^\times \to E(\mathbb{C}_K)$ in (3.4) is the c-th power of the one in (3.3). We claim that the vertical arrows in (3.4) are again surjective. Since ev_E is surjective, by the snake lemma it suffices to prove that $\ker(\mathrm{ev}_E) \to \ker(\pi)$ is surjective. Let $x \in \ker(\pi)$. Since $\ker(\pi)$ is an abelian subvariety of J, it is divisible; choose $y \in \ker(\pi)$ such that $cy = x$. Since $\ker(\mathrm{ev}_\rho)$ surjects onto $\ker(\pi)$, there exists $z \in \ker(\rho)$ such that $z \mapsto y$. Then $z^c \mapsto x$ and $\mathrm{ev}_E(z^c) = \mathrm{ev}_\rho(z) = 1$, which proves the claim. This implies

$$c^{-1}\Gamma = \{[\lambda, \lambda_E] \mid \lambda \in \Lambda\} \subset K^\times. \tag{3.5}$$

In particular, c divides the order of the group of roots of unity in K.

3.10 The endomorphism $e_0 = \pi^\vee \circ \pi : J \to J$ corresponds to an idempotent $e \in \mathrm{End}^0(J) := \mathrm{End}(J) \otimes_{\mathbb{Z}} \mathbb{Q}$. Up to isogeny, we can decompose $J \sim_K A_1 \times A_2 \times \cdots \times A_s$, where A_i's are K-simple abelian varieties. This decomposition produces idempotents $e_1, \ldots, e_s \in \mathrm{End}^0(J)$ which are mutually orthogonal: $e_i e_j = 0$ if $i \neq j$. The idempotent e is one of those. The $\mathbb{Q}$-bilinear form $B(x, y) = \mathrm{Tr}(xy^\dagger)$ on $\mathrm{End}^0(A)$ is symmetric and positive definite (here the Rosati involution is with respect to the canonical principal polarization H). This implies that the Rosati involution must fix each idempotent e_i. Therefore $e^\dagger = e$, and also $e_0^\dagger = e_0$. This observation will simplify some calculations and is useful in the following paragraph.

We denote by n the denominator of e in $\mathrm{End}(J)$, *i.e.*, the least natural number such that $ne \in \mathrm{End}(J)$. Note that §3.5 implies that $\mathrm{End}(J)$ is naturally a subring of $\mathrm{End}(\Lambda)$ when we regard Λ as the lattice uniformizing J, and $\mathrm{End}(J)$ is a subring of $\mathrm{End}(\Lambda)^{\mathrm{opp}}$ when we regard Λ as the character group of the torus uniformizing J. By Proposition 3.3 and the above discussion, the image of e_0 in $\mathrm{End}(\Lambda)$ is the same under either identification. We define the denominator r of e in $\mathrm{End}(\Lambda)$ as the least natural number such that $re \in \mathrm{End}(\Lambda)$. Obviously, r divides n.

Lemma 3.4 *The morphism $\pi \circ \pi^\vee : E^* \to E_*$ is the multiplication-by-n map on E.*

Proof See the proof of Theorem 3 in [31]. ∎

3.11 Recall that the closed immersion $E \hookrightarrow J$ gives rise to the inclusion $\pi^\vee\colon \Gamma \hookrightarrow \Lambda$ sending $\rho \mapsto c\lambda_E$, and that the projection $\pi\colon J \to E$ induces a surjective homomorphism $\pi\colon \Lambda \twoheadrightarrow \Gamma$. The endomorphism $\pi \circ \pi^\vee\colon E^* \to E_*$ corresponds to the endomorphism $\pi \circ \pi^\vee\colon \Gamma \hookrightarrow \Lambda \twoheadrightarrow \Gamma$, so by Lemma 3.4, $\pi(c\lambda_E) = \pi \circ \pi^\vee(\rho) = n\rho$, and therefore

$$\pi(\lambda_E) = \frac{n}{c}\rho. \tag{3.6}$$

The idempotent e_0 corresponds to the composition $\pi^\vee \circ \pi\colon \Lambda \twoheadrightarrow \Gamma \hookrightarrow \Lambda$. We have $\pi^\vee \circ \pi(\lambda_E) = \pi^\vee(\frac{n}{c}\rho) = n\lambda_E$, so $e_0 = ne$ because $e(\lambda_E) = \lambda_E$. Since $\frac{1}{c}\pi^\vee(\Gamma) \subset \Lambda$, but $\frac{1}{c'}\pi^\vee(\Gamma) \not\subset \Lambda$ for $c' > c$, we have $\frac{1}{c}e_0 \in \operatorname{End}(\Lambda)$, but $\frac{1}{c'}e_0 \notin \operatorname{End}(\Lambda)$ for $c' > c$. Thus $re = \frac{1}{c}e_0 = \frac{n}{c}e$, *i.e.*,

$$c = \frac{n}{r} \tag{3.7}$$

3.12 The pairing $\langle \cdot\,, \cdot \rangle$ coincides with (the H-polarized version of) Grothendieck's monodromy pairing; see [14, (14.2.5)] and [6, Theorem 2.1]. By [14, (11.5)], the cokernel of the map $\Lambda \to \operatorname{Hom}(\Lambda, \mathbb{Z})$ induced by the monodromy pairing $\langle \cdot\,, \cdot \rangle$ is naturally isomorphic to the component group Φ_J. The analogous statement holds for E, and we have a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \Lambda \arrow[r, "\langle \cdot\,,\cdot \rangle"] \arrow[d, "\pi"'] & \operatorname{Hom}(\Lambda, \mathbb{Z}) \arrow[r] \arrow[d, "\mathrm{ev}_\rho"'] & \Phi_J \arrow[r] \arrow[d, "\pi_*"] & 0 \\ 0 \arrow[r] & \Gamma \arrow[r] & \mathbb{Z} \arrow[r] & \Phi_E \arrow[r] & 0 \end{tikzcd} \tag{3.8}$$

where $\mathrm{ev}_\rho(f) = f(\pi^\vee(\rho))$ as in (3.3). Since $\pi^\vee(\rho) = c\lambda_E$ and $\mathbb{Z}\lambda_E$ is a direct summand of Λ, the cokernel of ev_ρ is isomorphic to $\mathbb{Z}/c\mathbb{Z}$. As $\pi\colon \Lambda \to \Gamma$ is surjective, this implies that

$$\operatorname{coker}(\pi_*\colon \Phi_J \to \Phi_E) \cong \mathbb{Z}/c\mathbb{Z}. \tag{3.9}$$

This is a generalization of Formula 1 in [23]. The following corollary is also observed in [29, Theorem 2] in the context of Jacobians of Shimura curves.

Corollary 3.5 $\#\operatorname{coker}(\pi_*)$ *divides the order of the group of roots of unity in* $K^\times$.

Proof Follows from §3.9 and (3.9). ∎

3.13 The map $\Gamma \to \mathbb{Z}$ is the composition of $\Gamma \to K^\times$ with $\operatorname{ord}_K\colon K^\times \to \mathbb{Z}$; hence ρ maps to $\operatorname{ord}_K(q_E)$. (This recovers the well-known fact that $\#\Phi_E = \operatorname{ord}_K(q_E)$.) We have $\rho = \frac{c}{n}\pi(\lambda_E)$ by (3.6), so since the left square commutes,

$$c\langle \lambda_E, \lambda_E \rangle = \langle \lambda_E, \pi^\vee(\rho) \rangle = \frac{n}{c}\operatorname{ord}_K(q_E),$$

and therefore,

$$c^2 \langle \lambda_E, \lambda_E \rangle = n \operatorname{ord}_K(q_E). \tag{3.10}$$

https://doi.org/10.4153/CJM-2016-009-9 Published online by Cambridge University Press

This is essentially Formula 3 in [23].

3.14 Let

$$m := \min\{\langle\lambda,\lambda_E\rangle > 0 \mid \lambda\in\Lambda\},\quad \lambda_E^{\perp} := \{\lambda\in\Lambda \mid \langle\lambda,\lambda_E\rangle = 0\}.$$

The image of $\mathrm{ev}_\rho\circ\langle\cdot\,,\cdot\rangle$ in (3.8) is generated by $\min\{\langle\lambda,c\lambda_E\rangle > 0 \mid \lambda\in\Lambda\} = c\cdot m$; as $\pi\colon\Lambda\to\Gamma$ is surjective and the image of Γ in $\mathbb{Z}$ is generated by $\mathrm{ord}_K(q_E)$, this implies

$$c\cdot m = \mathrm{ord}_K(q_E). \tag{3.11}$$

Theorem 3.6 *The following are equivalent.*

(i) *The functorially induced map on component groups $\Phi_J\to\Phi_E$ is surjective.*
(ii) *e_0 is primitive in* $\mathrm{End}(\Lambda)$.
(iii) $c = 1$.
(iv) $n = r$.
(v) $\langle\lambda_E,\lambda_E\rangle = n\,\mathrm{ord}_K(q_E)$.
(vi) $m = \mathrm{ord}_K(q_E)$.
(vii) $n = [\Lambda : \lambda_E^{\perp}\oplus\mathbb{Z}\lambda_E]$.

Proof We have (i) ⇔ (iii) by (3.9), (iii) ⇔ (iv) by (3.7), and (iv) ⇔ (ii) since $e_0 = ne$. Conditions (v) and (vi) are equivalent to (iii) by (3.10) and (3.11), respectively. It is easy to see that $r = [\Lambda:\lambda_E^{\perp}\oplus\mathbb{Z}\lambda_E]$; hence (iv) ⇔ (vii). ∎

Remark 3.7 Assume X has a K-rational point. Fix such a point P_0, and let $\theta\colon X\hookrightarrow J$ be the Abel–Jacobi map which sends P_0 to the origin of J. Since $\theta(X)$ generates J, the composition $\pi\circ\theta$ gives a non-constant morphism $w\colon X\to E$. It is easy to show that the degree $\deg(w)$ of w is n. The index $[\Lambda:\lambda_E^{\perp}\oplus\mathbb{Z}\lambda_E]$ is the "congruence number" of λ_E with respect to the monodromy pairing, *i.e.*, it is the largest integer R_E such that there is an element in $\lambda_E^{\perp}$ congruent to λ_E modulo R_E. Hence Theorem 3.6 (or more precisely, (3.7)) implies that R_E divides $\deg(w)$ and the ratio is c. As we will show in Section 5, $n/R_E = c$ can be strictly larger than 1. It is interesting to compare this fact with the relation between the degree of modular parametrization of an elliptic curve over $\mathbb{Q}$ and the congruence number of the corresponding newform.

Let E be an elliptic curve over $\mathbb{Q}$. One may view E as an abelian variety quotient over $\mathbb{Q}$ of the modular Jacobian $J_0(N)$, where N is the conductor of E. Assume E is an optimal quotient of $J_0(N)$. The modular degree n_E is the degree of the composite map $X_0(N)\to J_0(N)\to E$, where the second map is an optimal quotient, and the first map is the Abel–Jacobi map $X_0(N)\to J_0(N)$ sending the cusp $[\infty]$ to the origin. Let $S_2(N,\mathbb{Z})$ be the space of weight-2 cusp forms on $\Gamma_0(N)$ with integer Fourier coefficients. Let $f_E\in S_2(N,\mathbb{Z})$ be the newform attached to E. Let $R'_E := [S_2(N,\mathbb{Z}):f_E^{\perp}\oplus\mathbb{Z}f_E]$, where $f_E^{\perp}$ is the orthogonal complement of f_E in $S_2(N,\mathbb{Z})$ with respect to the Petersson inner product. In [1], the authors showed that n_E divides R'_E, but the ratio R'_E/n_E can be strictly larger than 1. See also Remark 4.2.

We use Theorem 3.6 to give two conditions under which $\Phi_J\to\Phi_E$ is surjective.

Lemma 3.8 *Let $\mathbb{T}$ be a commutative subring of* $\mathrm{End}(J)$ *with the same identity element and such that $e \in \mathbb{T} \otimes \mathbb{Q}$. Suppose there is a bilinear $\mathbb{T}$-equivariant pairing*

$$(\cdot\,,\cdot) : \mathbb{T} \times \Lambda \to \mathbb{Z},$$

which is perfect if we consider $\mathbb{T}$ and Λ as free $\mathbb{Z}$-modules. Then the equivalent conditions of Theorem 3.6 are satisfied.

Proof Let s be the denominator of e in $\mathbb{T}$, *i.e.*, the smallest positive integer such that $se \in \mathbb{T}$. Note that r divides n and n divides s, since $\mathbb{T} \subseteq \mathrm{End}(J) \subseteq \mathrm{End}(\Lambda)$. Let $\lambda \in \Lambda$ be arbitrary, and denote $\lambda' = (re)\lambda \in \Lambda$. Because $se \in \mathbb{T}$ is primitive, we can take it as part of a $\mathbb{Z}$-basis of $\mathbb{T}$. Now

$$(se, \lambda) = (1, (se)\lambda) = \Big(1, \frac{s}{r}\lambda'\Big) = \frac{s}{r}(1, \lambda') \in \frac{s}{r}\mathbb{Z}.$$

Hence s/r divides the determinant of $(\cdot\,,\cdot)$ with respect to some $\mathbb{Z}$-bases of $\mathbb{T}$ and Λ. The perfectness of the pairing is equivalent to this determinant being ±1. Therefore $s = r$, which implies $r = n$. ∎

3.15 We keep the notation of Lemma 3.8. As it is easy to check, the assumption $e \in \mathbb{T} \otimes \mathbb{Q}$ implies that Γ' is $\mathbb{T}$-invariant, that is, for any $T \in \mathbb{T}$ we have $T\lambda_E = a(T) \cdot \lambda_E$ for some $a(T) \in \mathbb{Z}$. It is clear that the map $T \mapsto a(T)$ gives a homomorphism $\mathbb{T} \to \mathbb{Z}$. Denote the kernel of this homomorphism by I_E. Define

$$I_E\Lambda = \{T\lambda \mid T \in I_E, \lambda \in \Lambda\} = \{T\lambda - a(T)\lambda \mid T \in \mathbb{T}, \lambda \in \Lambda\}.$$

Assume $a(T^\dagger) = a(T)$ for all $T \in \mathbb{T}$. Since

$$\langle T\lambda - a(T)\lambda, \lambda_E\rangle = \langle \lambda, T^\dagger\lambda_E\rangle - a(T)\langle\lambda, \lambda_E\rangle = 0,$$

we have an inclusion $I_E\Lambda \subseteq \lambda_E^\perp$. Note that the index $[\lambda_E^\perp : I_E\Lambda]$ is finite since $1 - e$ is the projection onto $\lambda_E^\perp \otimes \mathbb{Q}$.

Lemma 3.9 *The index $[\lambda_E^\perp : I_E\Lambda]$ is divisible by c. In particular, if $I_E\Lambda = \lambda_E^\perp$, then the equivalent conditions of Theorem 3.6 are satisfied.*

Proof For $T \in \mathbb{T}$ and $\lambda \in \Lambda$ we have

$$\begin{aligned}[T\lambda - a(T)\lambda,\ \lambda_E] &= [T\lambda,\ \lambda_E]\,[\lambda,\ \lambda_E]^{-a(T)} \\ &= [\lambda,\ T^\dagger\lambda_E]\,[\lambda,\ \lambda_E]^{-a(T)} = [\lambda,\ a(T^\dagger)\lambda_E]\,[\lambda,\ \lambda_E]^{-a(T)} = 1.\end{aligned}$$

Hence by (3.5) we have a surjection $[\,\cdot\,, \lambda_E] : \Lambda/I_E\Lambda \twoheadrightarrow c^{-1}\Gamma \cong \mu_c \times w^{\mathbb{Z}}$. Consider the short exact sequence

$$0 \longrightarrow \lambda_E^\perp/I_E\Lambda \longrightarrow \Lambda/I_E\Lambda \longrightarrow \Lambda/\lambda_E^\perp \longrightarrow 0. \tag{3.12}$$

Since $\Lambda/\lambda_E^\perp \cong \mathbb{Z}$, this identifies $\lambda_E^\perp/I_E\Lambda$ with the torsion part of $\Lambda/I_E\Lambda$. Since $\Lambda/I_E\Lambda$ surjects onto $\mu_c \times w^{\mathbb{Z}}$, no non-torsion element of $\Lambda/I_E\Lambda$ maps into μ_c, so we must have $\lambda_E^\perp/I_E\Lambda \twoheadrightarrow \mu_c$. ∎

https://doi.org/10.4153/CJM-2016-009-9 Published online by Cambridge University Press

4 Modular Jacobians

In this section we discuss Question 1.1 in the context of Jacobians of certain modular curves.

4.1 Consider the modular curve $X_0(p)$ defined over $\mathbb{Q}$ classifying elliptic curves with cyclic subgroups of order p where p is prime. Assume the genus of $X_0(p)$ is not 0, or equivalently, $p \neq 2, 3, 5, 7, 13$. By a well-known result of Deligne and Rapoport, the Jacobian $J_0(p)$ of $X_0(p)$ has good reduction over $\mathbb{Q}_\ell$ for any prime $\ell \neq p$, and has toric reduction over $\mathbb{Q}_p$; *cf.* [4, p. 288].

Theorem 4.1 *Let $\pi: J_0(p) \to E$ be an optimal quotient defined over $\mathbb{Q}_p$ where E is an elliptic curve. The induced map on component groups $\pi_*: \Phi_{J_0(p)} \to \Phi_E$ of the Néron models over $\mathbb{Z}_p$ is surjective.*

Proof This was proved by Mestre and Oesterlé [19, Corollary 3]. A more general result was proved by Emerton [8]. Both proofs rely on Ribet's level-lowering theorem [24], and the deepest results in [18]. We give a different proof, which uses Lemma 3.9.

Since $J_0(p)$ is defined over $\mathbb{Q}$ and has semi-stable reduction, all its endomorphisms are defined over $\mathbb{Q}$; see [21, Theorem 1.1]. This implies that π and E can be defined over $\mathbb{Q}$. Let $\mathbb{T}$ be the subring of $\operatorname{End}(J_0(p))$ generated by the Hecke operators T_n, $n \geq 1$ (see [24, §3] for the definition). If $f_E(z) = \sum_{n\geq 1} a_n e^{2\pi i z n}$ is the newform attached to E, then one checks that $T_n \lambda_E = a_n \lambda_E$, which implies $e \in \mathbb{T} \otimes \mathbb{Q}$. By [24, p. 444], $T^\dagger = w_p T w_p$ for $T \in \mathbb{T}$, where w_p is the Atkin–Lehner involution of J. Since $w_p \lambda_E = \pm\lambda_E$, the condition $a(T) = a(T^\dagger)$ of §3.15 is satisfied. Let I_E be the kernel of the map $\mathbb{T} \to \mathbb{Z}$, $T_n \mapsto a_n$.

The Jacobian $J_0(p)$ acquires split toric reduction over the unramified quadratic extension of $\mathbb{Q}_p$; let Λ be the lattice uniformizing the analytification of $J_0(p)$ over this quadratic extension. Since p is odd, Corollary 3.5 and §2.6 imply that p does not divide $c = \#\operatorname{coker}(\Phi_{J_0(p)} \to \Phi_E)$. By Lemma 3.9, it is enough to show that for all $\ell \neq p$ such that $\Phi_E[\ell] \neq 0$, we have $(\lambda_E^\perp / I_E \Lambda) \otimes \mathbb{F}_\ell = 0$. From the sequence (3.12) we see that $\Lambda / I_E \Lambda \cong \mathbb{Z} \times (\lambda_E^\perp / I_E \Lambda)$ as abelian groups; so it is enough to prove that $(\Lambda / I_E \Lambda) \otimes \mathbb{F}_\ell \cong \mathbb{F}_\ell$. If $\mathfrak{m}_\ell = (I_E, \ell) \lhd \mathbb{T}$, then $(\Lambda / I_E \Lambda) \otimes \mathbb{F}_\ell = \Lambda / \mathfrak{m}_\ell \Lambda$. When $\ell \neq 2$ or $\mathfrak{m}_\ell$ is Eisenstein, it is a consequence of [25, Theorem 2.3] that $\Lambda / \mathfrak{m}_\ell \Lambda \cong \mathbb{F}_\ell$. We claim that $\mathfrak{m}_\ell$ is Eisenstein when $\Phi_E[\ell] \neq 0$. Considering the ℓ-torsion subgroup $E[\ell]$ of E as a $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, we obtain a representation $\rho: \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$. This representation is isomorphic to the residual representation $\rho_{\mathfrak{m}_\ell}$ attached to $\mathfrak{m}_\ell$; see [24, §5] for the construction and properties of $\rho_{\mathfrak{m}_\ell}$. If $\mathscr{E}$ is the Néron model of E, then, since $\Phi_E[\ell] \neq 0$, we have that $\mathscr{E}[\ell]$ is a finite étale group-scheme over $\mathbb{Z}_p$ which extends $E[\ell]$. Therefore the Galois representation $\rho \cong \rho_{\mathfrak{m}_\ell}$ is finite; so $\mathfrak{m}_\ell$ is Eisenstein by [25, Proposition 2.2]. ∎

Remark 4.2 Let $N \geq 1$ be an integer. As in Remark 3.7, let $S_2(N, \mathbb{Z})$ be the space of weight-2 cusp forms on $\Gamma_0(N)$ with integer Fourier expansions. Let $\mathbb{T}(N)$ be the

https://doi.org/10.4153/CJM-2016-009-9 Published online by Cambridge University Press

subring of $\mathrm{End}(J_0(N))$ generated by the Hecke operators T_n, $n \geq 1$. The pairing

$$\mathbb{T}(N) \times S_2(N, \mathbb{Z}) \to \mathbb{Z} \qquad (4.1)$$
$$T, f \mapsto a_1(Tf),$$

where $a_1(f)$ denotes the first Fourier coefficient of f, is bilinear, and $\mathbb{T}(N)$-equivariant. Moreover, it is perfect by [22, Theorem 2.2].

Now let $N = p$ be prime. Let Λ be the lattice from the proof of Theorem 4.1. Then Λ and $S_2(p, \mathbb{Z})$ are $\mathbb{T}(p)$-modules, which are free $\mathbb{Z}$-modules of the same rank. If $\Lambda \cong S_2(p, \mathbb{Z})$ as $\mathbb{T}(p)$-modules, then the perfectness of the pairing (4.1) and Lemma 3.8 imply that $\pi_*: \Phi_{J_0(p)} \to \Phi_E$ is surjective. One can use Eichler's trace formula to show that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ and $S_2(p, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}$ are isomorphic $\mathbb{T}(p)$-modules [13]. On the other hand, it is most likely that Λ and $S_2(p, \mathbb{Z})$ are generally not isomorphic as $\mathbb{T}(p)$-modules. Although, at the moment, we do not have an explicit example of this for prime levels, the following closely related example came up in the work of the first author with Fu-Tsun Wei on Jacquet–Langlands isogenies. Let $N = 65 = 5 \cdot 13$. The Jacobian $J_0(65)$ has toric reduction at 5 and 13. Let Λ_5 and Λ_{13} be the uniformizing lattices at 5 and 13, respectively. Then neither Λ_5 nor Λ_{13} is isomorphic to $S_2(65, \mathbb{Z})$ as $\mathbb{T}(65)$-modules, although all three $\mathbb{T}(65)$-modules become isomorphic after tensoring with $\mathbb{Q}$.

4.2 Let $D > 1$ be a square-free integer divisible by an even number of primes, and let $M \geq 1$ be a square-free integer coprime to D. Let $\Gamma_0^D(M)$ be the group of norm-1 units in an Eichler order of level M in the indefinite quaternion algebra B over $\mathbb{Q}$ of discriminant D. Since B is indefinite, by fixing an isomorphism $B \otimes \mathbb{R} \cong \mathbb{M}_2(\mathbb{R})$, we can regard $\Gamma_0^D(M)$ as a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$. Let $X_0^D(M) = \Gamma_0^D(M) \backslash \mathcal{H}$ be the associated Shimura curve, where $\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$. This is a smooth projective curve, which has a canonical model over $\mathbb{Q}$. It is a moduli space of abelian surfaces equipped with an action of B and $\Gamma_0(M)$-level structure.

The Jacobian $J_0^D(M)$ of $X_0^D(M)$ has toric reduction over $\mathbb{Q}_p$ if p divides D; this follows from the work of Cherednik and Drinfeld [5]. Assume $\pi: J_0^D(M) \to E$ is an optimal quotient defined over $\mathbb{Q}$, where E is an elliptic curve. Fix a prime p dividing D, and let π_* be the induced map on component groups of the corresponding Néron models over $\mathbb{Z}_p$. In the proofs of Proposition 4.4 and Corollary 4.5 in [2], Bertolini and Darmon implicitly assume that c in the diagram (3.4) with $J = J_0^D(M)$ is 1. By Theorem 3.6 this assumption is equivalent to π_* being surjective. On the other hand, Question 1.1 in general has a negative answer, so it is not clear whether the answer is always positive for the Jacobians of Shimura curves. In the positive direction, Takahashi proved that if the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $E[\ell]$ is irreducible, then ℓ does not divide the order of the cokernel of π_*; see [29, Theorem 1]. The proof relies on the comparison of the degrees of different modular parametrizations of E by both modular and Shimura curves.

Remark 4.3 Theorem 3.6 suggests a computational approach to finding an example of an optimal quotient E of $J_0^D(M)$ such that the homomorphism π_* of component groups is not surjective. The computer algebra package Magma has an implementation of Brandt modules which allows one to do calculations with the lattice Λ uniformizing the analytification of $J_0^D(M)$. In particular, one can efficiently calculate the idempotent e. The surjectivity question then reduces to whether or not re, as an endomorphism of $\mathrm{Hom}(\Lambda, K^\times)$, takes Λ to itself. This calculation can in theory be carried out using p-adic Θ-functions.

4.3 Let $A = \mathbb{F}[T]$ be the ring of polynomials with coefficients in a finite field $\mathbb{F}$, and $F = \mathbb{F}(T)$ be the field of fractions of A. Let $K = \mathbb{F}((1/T))$ be the completion of F at the place $1/T$, and R the ring of integers of K. Let $\mathfrak{n} \triangleleft A$ be an ideal and

$$\Gamma_0(\mathfrak{n}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \mathrm{GL}_2(A) \mid c \in \mathfrak{n} \right\}.$$

The group $\Gamma_0(\mathfrak{n})$ acts discontinuously on the Drinfeld half plane $\Omega := \mathbb{C}_K - K$, and the quotient $\Gamma_0(\mathfrak{n}) \setminus \Omega$ is the analytification of the Drinfeld modular curve $Y_0(\mathfrak{n})$, which is a smooth affine algebraic curve defined over K. The $\mathbb{C}_K$-valued points of $Y_0(\mathfrak{n})$ are in bijection with rank-2 Drinfeld A-modules over $\mathbb{C}_K$ with certain level structures. Let $J_0(\mathfrak{n})$ be the Jacobian of the smooth projective curve containing $Y_0(\mathfrak{n})$ as a Zariski dense subset. The Jacobian $J_0(\mathfrak{n})$ has split toric reduction over K; *cf.* [10, Theorem 2.10].

Theorem 4.4 *Assume $\pi: J_0(\mathfrak{n}) \to E$ is an optimal quotient defined over K, where E is an elliptic curve. The induced map on component groups $\pi_*: \Phi_{J_0(\mathfrak{n})} \to \Phi_E$ of the Néron models over R is surjective.*

Proof The proof essentially consists of showing that the condition in Lemma 3.8 is satisfied. This heavily relies on the arithmetic theory of Drinfeld modular curves.

There are Hecke operators defined in terms of correspondences on $Y_0(\mathfrak{n})$ which generate a commutative $\mathbb{Z}$-subalgebra $\mathbb{T}$ of $\mathrm{End}(J_0(\mathfrak{n}))$; see [10, §1] for the definitions and basic properties. The Hecke algebra $\mathbb{T}$ also naturally acts on the space of $\mathbb{Z}$-valued $\Gamma_0(\mathfrak{n})$-invariant harmonic cochains $H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{n})}$ on the Bruhat–Tits tree $\mathcal{T}$ of $\mathrm{PGL}_2(K)$; again we refer to [10, §1] for the definitions. (The $\mathbb{Z}$-module $H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{n})}$ is the analogue in this context of $S_2(N, \mathbb{Z})$.) Let Λ be the uniformizing lattice of $J_0(\mathfrak{n})$. The algebra $\mathbb{T}$ naturally acts on Λ; *cf.* §3.5. A crucial fact is that there is a canonical $\mathbb{T}$-equivariant isomorphism between Λ and $H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{n})}$; see [10, Theorem 1.9] and [11, Lemma 9.3.2]. Gekeler [10, Theorem 3.17] defined a bilinear $\mathbb{T}$-equivariant pairing $\mathbb{T} \times H_!(\mathcal{T}, \mathbb{Z})^{\Gamma_0(\mathfrak{n})} \to \mathbb{Z}$, and proved that it is perfect after tensoring with $\mathbb{Z}[p^{-1}]$ where p is the characteristic of $\mathbb{F}$. (This pairing is the function field analogue of (4.1).) Using the facts listed above, the argument in the proof of Lemma 3.8 shows that c is a p-power. On the other hand, according to Corollary 3.5, c divides $\#\mathbb{F} - 1$, so c is coprime to p. This implies that $c = 1$. ∎

5 Jacobians Isogenous to a Product of Two Elliptic Curves

We start by giving a very explicit, equation-based, example. We will explain later in this section how this example can be obtained as a special case of a general construction.

https://doi.org/10.4153/CJM-2016-009-9 Published online by Cambridge University Press

Example 5.1 Let $K = \mathbb{Q}_p$ where p is odd. Let X be the hyperelliptic curve of genus 2 with two affine charts $y^2 = f(x)$ and $Y^2 = g(t)$ glued in the obvious way, where

$$f(x) = (px^2 + (p-1))((p+1)x^2 + p)(x^2 + 1),$$

$Y = y/x^3$, $t = 1/x$, and $g(t) = f(x)/x^6$. These equations define the minimal regular model of X over K. Indeed, modulo p, the equation $y^2 = f(x)$ becomes

$$y^2 = -x^2(x^2 + 1),$$

which is a curve with singular point $(0,0)$. It is clear from the equation $y^2 = f(x)$ that the maximal ideal (x, y, p) is a regular point on this model. Similarly, on the other chart, we have the reduction $Y^2 = -t^2(1+t^2)$, and the maximal ideal (t, Y, p) is again regular. Hence, the model is regular, and has a special fibre consisting of an irreducible rational curve with two nodes. It follows from [4, Example 9.2/8] that the Jacobian J of X has toric reduction over K, and [4, Remark 9.6/12] implies that $\Phi_J(\overline{\mathbb{F}}_p) = 1$.

Next, let E be the elliptic curve given by the equation $y^2 = x(x-1)(x+p)$. The j-invariant of E has valuation $\mathrm{ord}_K(j) = -2$, so by the Tate algorithm E has multiplicative reduction over K and $\Phi_E(\overline{\mathbb{F}}_p) \cong \mathbb{Z}/2\mathbb{Z}$.

There is a morphism $f\colon X \to E$ of degree 2 given by

$$(x, y) \mapsto (p(p+1)x^2 + p^2, p(p+1)y).$$

Let $\pi\colon J \to E$ be the homomorphism of the Jacobians induced by f by the Albanese functoriality. Note that the induced map on component groups $\pi_*\colon \Phi_J(\overline{\mathbb{F}}_p) \to \Phi_E(\overline{\mathbb{F}}_p)$ is not surjective. We claim that π is an optimal quotient. If π is not optimal, then it factors as $J \to E' := J/\ker(\pi)^\circ \xrightarrow{\varphi} E$, where φ is an isogeny of degree greater than 1. Let $X \to J^{(1)}$ be the canonical morphism to the degree-1 part of the Picard scheme (as $X(K)$ may be empty, there may be no Abel–Jacobi map $X \to J$ defined over K). Then the composition $X \to J^{(1)} \to E'^{(1)} = E' \xrightarrow{\varphi} E$ factors f, which is impossible since the degree of f is 2.

5.1 Let $c \geq 2$ be an integer dividing the order of the group of roots of unity in $K^\times$. Assume c is coprime to the characteristic of the residue field k. Let E_1 and E_2 be two elliptic curves over K with multiplicative reduction, which are not isogenous over the algebraic closure $\overline{K}$ of K. Assume $\Phi_{E_1}(\overline{k}) \cong \Phi_{E_2}(\overline{k}) \cong \mathbb{Z}/c\mathbb{Z}$; equivalently, the j-invariants of E_1 and E_2 have valuation $-c$. Assume

$$E_i[c](K) = E_i[c](\overline{K}) \approx \mathbb{Z}/c\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}, \quad (i = 1, 2);$$

this condition is automatic if E_i has split multiplicative reduction and satisfies the previous assumption.

5.2 Let $e_c\colon E_i[c] \times E_i[c] \to \mu_c$ be the Weil pairing. Recall that the Weil pairing is alternating, *i.e.*, $e_c(P, P) = 1$ for any $P \in E_i[c]$; *cf.* [17, (2.8.7)]. There is a canonical subgroup of $E_i[c]$ corresponding to $(\mathscr{E}_i^0)_k[c] \cong \mathbb{Z}/c\mathbb{Z}$. Fix a generator g_i of this subgroup and a generator ζ of μ_c. Since e_c is non-degenerate, we can find $h_i \in E_i[c]$ such that $E_i[c] \approx \langle g_i \rangle \times \langle h_i \rangle$, and $e_c(g_1, h_1) = e_c(g_2, h_2) = \zeta$. Let $\psi\colon E_1[c] \xrightarrow{\sim} E_2[c]$ be the unique isomorphism such that $\psi(g_1) = h_2$ and $\psi(h_1) = g_2$. This is an anti-isometry with respect to the e_c pairings on $E_1[c]$ and $E_2[c]$ because

$$e_c(\psi(g_1), \psi(h_1)) = e_c(h_2, g_2) = e_c(g_2, h_2)^{-1} = e_c(g_1, h_1)^{-1}.$$

Let $A = E_1 \times E_2$ and let $G \subset A[c]$ be the graph of ψ:

$$G = \{ (P, \psi(P)) \mid P \in E_1[c] \}.$$

The product of the canonical principal polarizations on E_1 and E_2 is a principal polarization θ on the product variety $A = E_1 \times E_2$.

Proposition 5.2 *There is a principal polarization on the quotient abelian variety $J := A/G$ defined by G and θ. With this principal polarization, J is isomorphic to the canonically principally polarized Jacobian variety of a smooth projective curve X defined over K. The Jacobian J has toric reduction.*

Proof The existence of X follows from [16, Theorem 3]. It is important here that ψ is an anti-isometry, and E_1 and E_2 are not isogenous. The curve X can be defined over K because ψ, by construction, is an isomorphism of Galois modules [15, Proposition 3]. The claim that J has toric reduction follows from §2.8. ■

Lemma 5.3 $\Phi_J = 1$.

Proof Clearly $G \subset A(K)$ is a subgroup isomorphic to $\mathbb{Z}/c\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$. By §2.3, G extends to a constant étale subgroup-scheme of $\mathscr{A}$. The restriction to the closed fibre gives an injection $G \hookrightarrow \mathscr{A}_k(k)$, which composed with $\mathscr{A}_k \to \Phi_A$ gives a canonical homomorphism $\phi: G \to \Phi_A$. It is clear that $\Phi_A \cong \Phi_{E_1} \times \Phi_{E_2}$. Since

$$\mathscr{A}_k^0[c] \cong \{(P_1, P_2) \mid P_i \in \langle g_i \rangle\},$$

$G \cap \mathscr{A}_k^0 = 0$. Therefore, ϕ is an isomorphism. Now Theorem 4.3 in [20] implies that $\Phi_J \cong \Phi_A/G = 1$. ■

Lemma 5.4 *E_1 and E_2 are optimal quotients of J.*

Proof Note that E_i embeds into J as a closed subvariety since $E_i \cap G = 0$. The claim then follows from §2.8. Alternatively, note that the quotient J/E_1 is isomorphic to $E_2/E_2[c] \cong E_2$, so, by definition, E_2 is an optimal quotient of J. ■

5.3 In the special case when $c = 2$, Proposition 4 in [15] allows us to compute an explicit equation for X starting with equations for E_1 and E_2. Moreover, in this case the assumption that E_1 and E_2 are not isogenous can be relaxed to the assumption that E_1 and E_2 are not isomorphic over $\overline{K}$, *i.e.*, have distinct j-invariants [16, Theorem 3]. With this in mind, consider the Legendre curves

$$E_1 : y^2 = x(x-1)(x-p) \quad \text{and} \quad E_2 : y^2 = x(x-1)(x+p)$$

over $\mathbb{Q}_p$, where p is odd. These curves have distinct j-invariants, multiplicative reduction, $\Phi_{E_i} \cong \mathbb{Z}/2\mathbb{Z}$, and $E_i[2]$ is $\mathbb{Q}_p$-rational. (Note that E_i has split multiplicative reduction if and only if -1 is a square modulo p.)

Let $P_1 = (1,0)$, $P_2 = (0,0)$, and $P_3 = (p,0)$ be the non-trivial elements of $E_1[2]$. Similarly, let $Q_1 = (1,0)$, $Q_2 = (0,0)$, and $Q_3 = (-p,0)$ be the non-trivial elements of $E_2[2]$. Modulo p the point P_1 lies in the smooth locus of the reduction of E_1, hence its specialization lies in the connected component $\mathscr{E}_1^0$ of the identity. Define ψ by $\psi(O) = O$, $\psi(P_1) = Q_2$, $\psi(P_2) = Q_1$, $\psi(P_3) = Q_3$. Using the formulas in [15, Proposition 4], one obtains the equation in Example 5.1.

Remark 5.5 When $c \geq 3$, it seems rather difficult to write down an explicit equation for X. Below we will compute the p-adic periods of J from the Tate periods of E_1 and E_2. Teitelbaum [30] developed a method for computing an equation for a genus 2 curve X with split degenerate reduction from the periods of its Jacobian. Teitelbaum's formulae are p-adic, *i.e.*, the coefficients of the equation of X are given by infinite series.

In order to illustrate the machinery of Section 3, we give an analytic interpretation of our previous algebraic construction, with some generalizations. For simplicity, we only treat the case of *split* toric reduction.

5.4 Let $\mathfrak{T} = (\mathbb{G}_{m,K}^2)^{\mathrm{an}}$ be a two-dimensional split analytic torus over K. Fix $q_1, q_2 \in K^\times$ such that $\mathrm{ord}_K(q_1), \mathrm{ord}_K(q_2) > 0$ and $q_1^u \neq q_2^w$ for any non-zero $u, w \in \mathbb{Z}$. Let $c > 1$ be an integer and let $\zeta \in K^\times$ be a primitive c-th root of unity. Let $\Lambda \subset \mathfrak{T}(K) = (K^\times)^2$ be the free abelian group generated by (q_1, ζ) and (ζ, q_2). We have $\mathrm{trop}(q_1,\zeta) = (-\log|q_1|, 0)$ and $\mathrm{trop}(\zeta, q_2) = (0, -\log|q_2|)$ which are linearly independent in $\mathbb{R}^2$, so Λ is a lattice in $\mathfrak{T}$. Let J^{an} be the analytic quotient $\mathfrak{T}/\Lambda$.

5.5 We identify $(n_1, n_2) \in \mathbb{Z}^2$ with the character of $\mathfrak{T}$ defined by $(Z_1, Z_2) \mapsto Z_1^{n_1} Z_2^{n_2}$. Define $H\colon \Lambda \xrightarrow{\sim} \mathbb{Z}^2$ by $H(q_1,\zeta) = (1,0)$ and $H(\zeta, q_2) = (0,1)$. We have

$$H(q_1,\zeta)(q_1,\zeta) = q_1, \quad H(q_1,\zeta)(\zeta,q_2) = \zeta = H(\zeta,q_2)(q_1,\zeta), \\ H(\zeta,q_2)(\zeta,q_2) = q_2,$$

so $H(\lambda)(\mu) = H(\mu)(\lambda)$ for all $\lambda, \mu \in \Lambda$. Moreover, the symmetric bilinear form $\langle\cdot,\cdot\rangle_H$ has the matrix form $\begin{bmatrix} \mathrm{ord}_K(q_1) & 0 \\ 0 & \mathrm{ord}_K(q_2) \end{bmatrix}$ with respect to the above choice of basis, so $\langle\cdot,\cdot\rangle_H$ is positive definite. Therefore by Theorem 3.1, J^{an} is the analytification of an abelian variety J, and the Riemann form H gives rise to a principal polarization of J by §3.3.

5.6 By an *elliptic subvariety* of J we will mean an abelian subvariety E of J of dimension one. By §2.8, any elliptic subvariety of J has split multiplicative reduction; moreover, if $0 \to \Gamma \to \mathbb{C}_K^\times \to E(\mathbb{C}_K) \to 0$ is the Tate uniformization of E, then we have a homomorphism of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Gamma & \longrightarrow & \mathbb{C}_K^\times & \longrightarrow & E(\mathbb{C}_K) & \longrightarrow & 0 \\ & & \big\downarrow & & \big\downarrow{\scriptstyle\varphi} & & \big\downarrow & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & (\mathbb{C}_K^\times)^2 & \longrightarrow & J(\mathbb{C}_K) & \longrightarrow & 0 \end{array} \tag{5.1}$$

with injective vertical arrows. In particular, $\varphi(\mathbb{C}_K^\times) \cap \Lambda = \varphi(\Gamma)$. Conversely, let $\mathbb{G}_{m,K}^{\mathrm{an}} \cong \mathfrak{T}' \subset \mathfrak{T}$ be a subtorus of dimension one such that $\Gamma = \mathfrak{T}'(K) \cap \Lambda \cong \mathbb{Z}$ (equivalently, such that $\mathfrak{T}'(\mathbb{C}_K) \cap \Lambda \neq \{1\}$), and let $E^{\mathrm{an}} = \mathfrak{T}'/\Gamma$. Then E^{an} is the analytification of an elliptic curve E over K and the induced map $E \to J$ is a closed immersion, so E is an elliptic subvariety of J and the diagram (5.1) commutes.

Proposition 5.6 *Let J be as in §5.4. There are exactly two elliptic subvarieties of J, given by $E_1(\mathbb{C}_K) = \mathbb{C}_K^\times \times \{1\}/(q_1^c, 1)^{\mathbb{Z}}$ and $E_2(\mathbb{C}_K) = \{1\} \times \mathbb{C}_K^\times/(1, q_2^c)^{\mathbb{Z}}$.*

Proof It is clear that E_1 and E_2 are elliptic subvarieties of J. Any dimension-one subtorus $\mathfrak{T}'$ of $\mathfrak{T}$ is of the form $\mathfrak{T}'(\mathbb{C}_K) = \{(z, w) \mid z^\alpha w^\beta = 1\}$ for some coprime integers $\alpha, \beta \in \mathbb{Z}$. Let $\mathfrak{T}'$ be such a subtorus, and suppose that $\mathfrak{T}'(K) \cap \Lambda \neq \{1\}$. Let $\lambda \in \Lambda \setminus \{1\}$ be an element of $\mathfrak{T}'(K) \cap \Lambda$. Then $\lambda = (q_1, \zeta)^\gamma (\zeta, q_2)^\delta = (q_1^\gamma \zeta^\delta, q_2^\delta \zeta^\gamma)$ for some integers γ, δ, not both equal to zero, and we have $q_1^{\alpha\gamma} q_2^{\beta\delta} \zeta^{\alpha\delta + \beta\gamma} = 1$. Raising both sides to the c-th power gives $q_1^{\alpha\gamma c} q_2^{\beta\delta c} = 1$, so we must have $\alpha\gamma = \beta\delta = 0$ by the way we chose q_1, q_2. If $\alpha \neq 0$ and $\beta \neq 0$, then $\gamma = \delta = 0$, which contradicts our choice of λ. Hence either $\alpha = 0$ and $\beta = \pm 1$, in which case $\mathfrak{T}'(\mathbb{C}_K) = \mathbb{C}_K^\times \times \{1\}$, or $\beta = 0$ and $\alpha = \pm 1$, in which case $\mathfrak{T}'(\mathbb{C}_K) = \{1\} \times \mathbb{C}_K^\times$. ■

5.7 Let Λ' be the sublattice of Λ generated by $(q_1^c, 1)$ and $(1, q_2^c)$. Identify E_1 (resp. E_2) with $\mathbb{C}_K^\times / q_1^{c\mathbb{Z}}$ (resp. $\mathbb{C}_K^\times / q_2^{c\mathbb{Z}}$) in the obvious way. Let $A = E_1 \times E_2$, so $A(\mathbb{C}_K) = (\mathbb{C}_K^\times)^2/\Lambda'$, and the kernel of the multiplication map $A \to J$ is $\Lambda/\Lambda' \cong (\mathbb{Z}/c\mathbb{Z})^2$. Since E_1 and E_2 are the only elliptic subvarieties of J, it follows that J is not isomorphic to a product of elliptic curves. Therefore the theta divisor of J is a smooth curve X of genus 2, and J is isomorphic to the Jacobian of X as principally polarized abelian varieties.

5.8 Since E_1 and E_2 are subvarieties of J, for $i = 1, 2$ the dual homomorphism $J \to E_i$ is an optimal quotient by §2.8. Let $\Gamma_1 = (q_1^c, 1)^{\mathbb{Z}}$ and $\Gamma_2 = (1, q_2^c)^{\mathbb{Z}}$, and for $i = 1, 2$ let Γ_i' be the saturation of Γ_i in Λ. Then $\Gamma_1' = (q_1, \zeta)^{\mathbb{Z}}$ and $\Gamma_2' = (\zeta, q_2)^{\mathbb{Z}}$. It follows from (3.9) that the cokernel of the map on component groups $\Phi_J \to \Phi_{E_i}$ is isomorphic to $\mathbb{Z}/c\mathbb{Z}$. In particular, $\Phi_J \to \Phi_{E_i}$ is not surjective. Note that the image of Λ in $\mathbb{C}_K^\times$ under the evaluation map ev_{E_i} is generated by ζ and q_i — this is immediate from the definition of H in §5.5. This illustrates the surjectivity of the map $\Lambda \to c^{-1}\Gamma_i$ of (3.4).

5.9 A calculation involving p-adic Θ-functions shows that the Weil pairing on the c-torsion of the Tate curve E_i is given by the rule $e_c(\zeta, q_i) = \zeta$. Note that $\zeta \in E_i$ generates the subgroup of $E_i[c]$ which reduces to the identity component of the Néron model of E_i. Let $\psi: E_1[c] \to E_2[c]$ be the unique isomorphism such that $\psi(\zeta) = q_2$ and $\psi(q_1) = \zeta$. Then the graph $G = \{(P, \psi(P)) \mid P \in E_1[c]\}$ is exactly the kernel of the map $A = E_1 \times E_2 \to J$, so this analytic construction coincides with our algebraic construction, at least when $1 = \mathrm{ord}_K(q_1) = \mathrm{ord}_K(q_2)$, $\mathrm{char}(k) \nmid c$, and J has split toric reduction.

5.10 Let $E = E_1$. In the notation of Section 3, we have $q_E = q_1^c$, so $\mathrm{ord}_K(q_E) = c \cdot \mathrm{ord}_K(q_1)$. We can take $\lambda_E = (q_1, \zeta) \in \Lambda$, so $\langle \lambda_E, \lambda_E \rangle = \mathrm{ord}_K H(q_1, \zeta)(q_1, \zeta) = \mathrm{ord}_K(q_1)$. It is clear that $m = \min\{\langle\lambda,\lambda_E\rangle > 0 \mid \lambda \in \Lambda\}$ is equal to $\langle\lambda_E,\lambda_E\rangle = \mathrm{ord}_K(q_1) = \mathrm{ord}_K(q_E)/c$. Hence $c\langle\lambda_E,\lambda_E\rangle = \mathrm{ord}_K(q_E)$, so $c = n$ by (3.10), and hence $r = 1$ by (3.7). The fact that $r = 1$ is easy to see directly, as the idempotent e corresponds to the endomorphism $(a,b) \mapsto (a,0)$ of the character group $\mathbb{Z}^2 \cong \Lambda$ of $\mathfrak{T}$, so $e \in \mathrm{End}(\Lambda)$. The equality $n = c$ is then clear as well since the smallest power of the endomorphism $(x,y) \mapsto (x,1)$ of $\mathbb{G}_{m,K}^2$ sending Λ to itself is c.

Acknowledgements The authors would like to thank M. Baker, M. Bertolini, and H. Darmon for interesting discussions, and the referee for corrections and several helpful observations.

References

[1] A. Agashe, K. Ribet, and W. Stein, *The modular degree, congruence primes, and multiplicity one*. In: Number theory, analysis and geometry, Springer, New York, 2012, pp. 19–49.

[2] M. Bertolini and H. Darmon, *p-adic periods, p-adic L-functions, and the p-adic uniformization of Shimura curves*. Duke Math. J. **98**(1999), no. 2, 305–334. http://dx.doi.org/10.1215/S0012-7094-99-09809-5

[3] S. Bosch and W. Lütkebohmert, *Degenerating abelian varieties*. Topology **30**(1991), 653–698. http://dx.doi.org/10.1016/0040-9383(91)90045-6

[4] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 21, Springer-Verlag, Berlin, 1990.

[5] J.-F. Boutot and H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld*. Astérisque (1991), no. 196-197, 45–158 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[6] R. Coleman, *The monodromy pairing*. Asian J. Math. **4**(2000), 315–330. http://dx.doi.org/10.4310/AJM.2000.v4.n2.a2

[7] B. Conrad and W. Stein, *Component groups of purely toric quotients*. Math. Res. Let. **8**(2001), 745–766. http://dx.doi.org/10.4310/MRL.2001.v8.n6.a5

[8] M. Emerton, *Optimal quotients of modular Jacobians*. Math. Ann. **327**(2003), no. 3, 429–458. http://dx.doi.org/10.1007/s00208-003-0449-2

[9] J. Fresnel and M. van der Put, *Rigid analytic geometry and its applications*, Progress in Mathematics, 218, Birkhäuser Boston, Boston, MA, 2004.

[10] E.-U. Gekeler, *Analytical construction of Weil curves over function fields*. J. Théor. Nombres Bordeaux **7**(1995), 27–49. http://dx.doi.org/10.5802/jtnb.129

[11] E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*. J. Reine Angew. Math. **476**(1996), 27–93.

[12] L. Gerritzen, *Über Endomorphismen nichtarchimedischer holomorpher Tori*. Invent. Math. **11**(1970), 27–36. http://dx.doi.org/10.1007/BF01389803

[13] B. Gross, *Heights and the special values of L-series*. In: Number theory. CMS Conf. Proc. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115–187.

[14] A. Grothendieck, *Modèles de Néron et monodromie*, SGA 7, Exposé IX, 1972.

[15] E. Howe, F. Leprévost, and B. Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*. Forum Math. **12**(2000), no. 3, 315–364.

[16] E. Kani, *The number of curves of genus two with elliptic differentials*. J. Reine Angew. Math. **485**(1997), 93–121.

[17] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*. Annals of Mathematics Studies 108, Princeton University Press, 1985.

[18] B. Mazur, *Modular curves and the Eisenstein ideal*. Inst. Hautes Études Sci. Publ. Math. **47**(1977), 33–186.

[19] J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*. J. Reine Angew. Math. **400**(1989), 173–184.

[20] M. Papikian, *On Jacquet–Langlands isogeny over function fields*. J. Number Theory **131**(2011), no. 7, 1149–1175. http://dx.doi.org/10.1016/j.jnt.2011.01.002

[21] K. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*. Ann. Math. (2) **101**(1975), 555–562. http://dx.doi.org/10.2307/1970941

[22] ———, *Mod p Hecke operators and congruences between modular forms*. Invent. Math. **71**(1983), no. 1, 193–205. http://dx.doi.org/10.1007/BF01393341

[23] ———, *Letter to J.-F. Mestre*. 1987. arxiv:math.AG/0105124

[24] ———, *On the modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*. Invent. Math. **100**(1990), 431–476. http://dx.doi.org/10.1007/BF01231195

[25] ———, *Torsion points on* $J_0(N)$ *and Galois representations*. In: Arithmetic theory of elliptic curves. Lecture Notes in Math. 1716, Springer, Berlin, 1999, pp. 145–166.

[26] J.-P. Serre, *Rational points on curves over finite fields*, Lectures given at Harvard University, Notes by F. Gouvêa, 1985.

[27] S. Takahashi, *Degrees of parametrizations of elliptic curves by Shimura curves*. J. Number Theory **90**(2001), no. 1, 74–88. http://dx.doi.org/10.1006/jnth.2000.2614

[28] ———, *p-adic periods of modular elliptic curves and the level-lowering theorem*. Int. J. Number Theory **4**(2008), no. 1, 15–23. http://dx.doi.org/10.1142/S1793042108001183

[29] ———, *Maps on groups of connected components induced from parametrizations of elliptic curves by Shimura curves*. JP J. Algebra Number Theory Appl. **13**(2009), no. 1, 57–63.

[30] J. Teitelbaum, *p-adic periods of genus two Mumford–Schottky curves*, J. Reine Angew. Math. **385**(1988), 117–151.

[31] D. Zagier, *Modular parametrizations of elliptic curves*. Canad. Math. Bull. **28**(1985), no. 3, 372–384. http://dx.doi.org/10.4153/CMB-1985-044-8

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
e-mail: papikian@psu.edu

School of Mathematics, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA 30332
e-mail: rabinoff@post.harvard.edu