Acta Appl Math (2007) 99: 185–204
DOI 10.1007/s10440-007-9162-6

Rigid Analytic Uniformization of Curves and the Study of Isogenies

Samuel Kadziela

Received: 1 January 2007 / Accepted: 12 September 2007

Abstract Complex uniformization of curves is a popular tool in Number Theory. There are, however, some arithmetic and computational advantages in the use of p-adic uniformization. This paper compares the two theories and discusses how they can be used to study isogenies, with explicit examples of p-adic uniformization of hyperelliptic curves.

Keywords p-Adic uniformization · Rigid analytic spaces · Hyperelliptic curves · Jacobians · Isogenies

Mathematics Subject Classification (2000) 14G20 · 32P05 · 11G20 · 14H40 · 14Q05

1 Introduction

The theory of Rigid Analytic Spaces, developed by Tate in [9], has seen many applications in Number Theory and Arithmetic Geometry, including contributions to the resolution of Fermat's last theorem and Abhyankar's conjecture. Another interesting application of this theory lies in p-adic uniformization of curves and abelian varieties. The complex uniformization of an abelian variety A has been studied at length, because it provides a nice analytic model for $A(\mathbb{C})$, the complex points of A. In Number Theory, however, one is often interested in other points of A, and p-adic uniformization can give a model for $A(\mathbb{Q}_p)$. Moreover, as the actual computation of either one of the models requires approximation, often the p-adic model is easier to acquire. Despite of this, it seems that the rigid uniformization is less known, and is taken advantage of infrequently.

The main results of this paper are contained in Sect. 3.3, where we describe the possible isogenies of analytic tori, and Sect. 5.2, where explicit examples of rigid uniformizations are computed, in order to suggest the practical application of the theory. To provide the reader with the necessary background, we also give a self-contained review of rigid analytic

S. Kadziela (✉)
Department of Mathematics, University of California, Irvine, Irvine, CA 92697-3875, USA
e-mail: kadziela@math.uci.edu

uniformization of curves. As a motivation, the subject is presented alongside the theory of complex uniformization, and we often discuss the relevant differences and similarities.

We will use k to denote a field which is complete with respect to non-Archimedean valuation. Since $\overline{k}$ usually stands for the reduction, we will denote the algebraic closure by k_a. Also, $k\langle X\rangle$ will denote the subring of strictly convergent power series in $k[\![X]\!]$, which means that the sequence of the coefficients tends to zero. The paper is organized as follows: we first define rigid analytic spaces in Sect. 2, and define a rigid structure on analytic tori and Mumford curves in Sect. 3.2. Then we prove the structure theorem for isogenies of analytic tori (Sect. 3.3), and show how the Jacobians of Mumford curves are isomorphic to analytic tori. Equipped with this theory, we can discuss p-adic uniformization of curves, and apply it to the study of isogenies. Finally, we discuss some of the advantages of p-adic uniformization in Sect. 5.1, and give examples of genus 2 hyperelliptic curves over $\mathbb{Q}_5$ in Sect.5.2, calculating their isogenies.

2 Rigid Analytic Varieties

We would like to define a theory of analytic geometry over k. One could try to do so directly using the valuation of k, which induces a metric topology on k^n. However, k^n in this topology is totally disconnected, which affects the nature of analytic functions. For example, the global "analytic" (in the sense of having a power series expansion about every point) functions

$$f(x) = \begin{cases} 1, & |x| = 1, \\ 0, & |x| \neq 1, \end{cases} \qquad g(x) = 0$$

are not equal, even though $f = g$ on the open set $\{x \in k : |x| \neq 1\}$. The problem is that in this topology, the set $\{x \in k : |x| = 1\}$ is also open.

To fix this problem, we could consider a different approach. We could start with a notion of an analytic function, as an element of some power series ring, and to this ring associate a natural set of points on which all such functions converge. For example, the Tate algebra

$$T_n = \left\{ \sum a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n} \in k[\![X_1, \dots, X_n]\!] : \lim |a_{i_1 \dots i_n}| = 0 \right\}$$

serves as the function algebra on the unit ball

$$B^n = B^n(k_a, 1) = \{(x_1, \dots, x_n) \in k_a^n : |x_i| \leq 1\}.$$

In fact, T_n is the set of all continuous functions $B^n \to k_a$, which admit a power series expansion converging on all of B^n, and which map $B^n(k, 1)$ into k [1]. Moreover, T_n also serves as the ring of functions on the maximum spectrum $\operatorname{Max} T_n$ in the usual way: $f(x)$ is the image of f in the finite field extension T_n/x of k. As it turns out, T_n is a Jacobson, Noetherian domain, with closed ideals. For any ideal $I \in T_n$, the finitely generated k-algebra $A = T_n/I$ can be identified with the ring of analytic functions on $\operatorname{Max} A \hookrightarrow \operatorname{Max} T_n$. If we were to endow $\operatorname{Max} A$ with the Zariski topology, this construction would be very analogous to the theory of algebraic varieties. But in general, the Zariski topology is too coarse to be useful in analytic geometry, so the idea is to use a different topology.

Actually, the maximum spectrum of any Tate algebra carries a canonical topology, which is related to the metric topology on k^n. More generally, an affinoid algebra A is defined as a finitely generated k-algebra extension of some T_n. A can always be expressed as a quotient of the Tate algebra by an ideal. Since T_n is a Banach algebra with respect to the norm

$$\left\|\sum a_\nu X^\nu\right\| = \max|a_\nu|, \quad \forall \nu \in \mathbb{N}^n,$$

the affinoid algebra $A = T_n/I$ is a Banach algebra with respect to the quotient norm

$$\|f\| = \inf\{\|f+g\| : g \in I\}.$$

We would like to use affinoid algebras as the building blocks for analytic spaces. To define the canonical topology on Max A, we give $B^n(k_a)$ the subspace (metric) topology from k_a^n. Consider the surjection $\tau\colon\ B^n(k_a) \to \operatorname{Max} T_n\colon\ x \mapsto m_x$, where $m_x \subset T_n$ is the ideal of all functions vanishing on x. Then τ has finite fibers, and induces a bijection

$$B^n(k_a)/\operatorname{Gal}(k_a/k) \simeq \operatorname{Max}\ T_n.$$

Thus τ defines a quotient topology on Max T_n, which, in turn, gives the canonical topology on Max $A \hookrightarrow$ Max T_n for any affinoid k-algebra $T_n \twoheadrightarrow A$. This topology is canonical because it can be described independently of the presentation $A = T_n/I$. Namely, the sets

$$\{x \in \operatorname{Max}\ A : |f_i(x)| \le 1\} \quad \text{for some } \{f_i\}_{i=1}^r \subset A$$

form a basis.

One advantage of the canonical topology on Max A is that it still has a "flavor" of a metric topology. For example, all sets of the form $\{x \in \operatorname{Max}\ A : |f(x)| =, \neq, \le, \ge |\alpha|\}$ for any $f \in A$ and $\alpha \in k$ are open. But it is no longer immediately clear what an analytic function on a general open set in this topology should be. In fact, from the point of view of defining a sheaf, the most straightforward topology to use would only consist of the subsets $U = \operatorname{Max}\ B \subset \operatorname{Max}\ A$ corresponding to k-algebra homomorphisms $A \to B$, called affinoid subdomains. Then we could simply consider the presheaf $\mathcal{O}(U) = B$. Fortunately, all affinoid subdomains are open in the canonical topology, and even form a basis.

Actually, we can go one step further. For any $f_0, f_1, \ldots, f_n \in A$ generating the unit ideal, i.e. having no common zeros on Max A, call the set

$$R = \{x \in \operatorname{Max} A : |f_i(x)| \le |f_0(x)|\}$$

a rational domain. It is an open affinoid subdomain of Max A, corresponding to the affinoid algebra

$$A_R = A\langle X_1, \ldots, X_n\rangle/(\ldots, f_0X_i - f_i, \ldots).$$

Since any open affinoid subdomain of Max A is a finite union of rational domains, as far as sheaf theory is concerned, there is no loss in restricting ourselves to rational domains only. These domains satisfy some nice properties, which make them particularly useful as a basis for a (Grothendieck) topology. For example:

– If R_1 and R_2 are rational, then so is $R_1 \cap R_2$ with $A_{R_1 \cap R_2} \simeq A_{R_1} \widehat{\otimes}_A A_{R_2}$.
– If $R_1 \subset R_2$ is rational, and $R_2 \subset \operatorname{Max} A$ is rational, then R_1 is rational in Max A.

The final ingredient in the definition of rigid analytic spaces, sometimes called analytic varieties, is to make them determined by local data. Thus, an analytic variety should be obtained from gluing together "affinoid varieties," just as, for example, an algebraic variety is obtained from gluing together affine varieties. None of the topologies on Max A that we have considered so far are suitable for this purpose. Therefore, we give Max A a Grothendieck topology. Basically, a Grothendieck topology on a set Y consists of a system $\mathcal{F}$ of subsets of Y, called "admissible open" subsets, and for every $U \in \mathcal{F}$ a set $\mathrm{Cov}(U)$ of coverings by elements of $\mathcal{F}$, called "admissible coverings," all of which satisfy certain conditions. A sheaf on such a G-topological space is defined with respect to the admissible open subsets. In the usual way, one obtains a theory of G-ringed spaces, locally G-ringed spaces, and Čech cohomology for presheaves on G-topological spaces. A nice feature of Grothendieck topologies is that they come with a recipe for gluing, not only G-topological spaces, but also the maps between them.

So let A be an affinoid algebra. We endow $Y = \mathrm{Max}\, A$ with a Grothendieck topology $\mathcal{G}$ where the admissible open sets are the rational domains, and the only admissible coverings are finite coverings by rational domains. The fact that the presheaf $\mathcal{O}_Y(Y) = A$, and $\mathcal{O}_Y(R) = A_R$ is a sheaf with respect to $\mathcal{G}$ is a consequence of Tate's Acyclicity Theorem, and we call $\mathcal{O}_Y$ the structure sheaf of Y. Thus, an affinoid variety is defined as the triple $\mathrm{Sp}(A) = (Y, \mathcal{G}, \mathcal{O}_Y)$, consisting of the topological space $Y = \mathrm{Max}\, A$, with its Grothendieck topology $\mathcal{G}$ and the structure sheaf $\mathcal{O}_Y$. A rigid analytic space over k is a triple $(X, \mathcal{G}, \mathcal{O})$, consisting of a topological space X, a Grothendieck topology $\mathcal{G}$ on X, and a sheaf $\mathcal{O}$, such that there exists an admissible covering $(X_i) \in \mathrm{Cov}(X)$ with $(X_i, \mathcal{G}|_{X_i}, \mathcal{O}|_{X_i})$ an affinoid variety. A good reference for this material is [1]. To give examples, in the next section we explicitly describe the rigid analytic structure on $(k^*)^n$, analytic tori and Mumford curves.

3 Analytic Tori

3.1 Rigid Structure on $(k^*)^n$ by Analytification of $\mathbf{G}^n_{m,k}$

First, note that the algebraic affine variety $(k^*)^n = \mathbf{G}^n_{m,k}$ is a product:

$$
\begin{aligned}
(k^*)^n &= \mathrm{Spec}\, k[z_1, z_1^{-1}, \ldots, z_n, z_n^{-1}] \\
&\simeq \mathrm{Spec}\,(k[z_1, z_1^{-1}] \otimes_k \cdots \otimes_k k[z_n, z_n^{-1}]) \simeq k^* \times_k \cdots \times_k k^*.
\end{aligned}
$$

In the category of k-affinoid varieties, fiber products also exist, but we use the completed tensor product:

$$\mathrm{Sp}\ A \times_k \mathrm{Sp}\ B = \mathrm{Sp}\ A \,\widehat{\otimes}_k\, B.$$

Thus, in the analytic case we also see products:

$$
\begin{aligned}
&\mathrm{Sp}\ k\langle z_1, z_1^{-1}, \ldots, z_n, z_n^{-1}\rangle \\
&\quad \simeq \mathrm{Sp}\,(\widehat{\otimes}_k k\langle z_i, w_i\rangle/(z_i w_i - 1)) \simeq \times_k \mathrm{Sp}\, k\langle z_i, z_i^{-1}\rangle,
\end{aligned}
$$

which follows from the isomorphism $T_n/\mathfrak{a} \,\widehat{\otimes}_k\, T_m/\mathfrak{b} \simeq T_{n+m}/(\mathfrak{a}, \mathfrak{b})$. However, unlike the algebraic case, it is not possible to describe all of $(k^*)^n$ as an affinoid variety in this way, since the space $\mathrm{Sp}\, k\langle x, x^{-1}\rangle$ only corresponds to the unit sphere centered at origin in $\mathrm{Spec}\, k[x, x^{-1}]$. But the spaces $\mathrm{Sp}\, k\langle z_1, z_1^{-1}, \ldots, z_n, z_n^{-1}\rangle$ can be extended to annuli, which provide an affinoid covering of the analytic space $(k^*)^n$ in a natural way.

More generally, there is an analytification functor $Y \rightsquigarrow Y^{\mathrm{an}}$ which assigns an analytic variety to any scheme Y of locally finite type over k. It is illuminating to see how it works in the case of affine schemes, and especially the affine n-space. For proofs and more details, the reader is referred to [1, Chap. 9].

To ease the notation, let $X = (x_1, \dots, x_n)$ be a system of indeterminates, and we'll write X^ν for $(x_1^{\nu_1}, \dots, x_n^{\nu_n})$ and $k\langle X\rangle \subset k[\![X]\!]$ for the Tate algebra T_n, serving as analytic functions on $B^n(k_a, 1)$. Fixing an element $\pi \in k$ with $|\pi| > 1$, we can also consider the subalgebras $A_i \subset k[\![X]\!]$

$$A_i = \left\{\sum a_\nu X^\nu \in k[\![X]\!] : \lim |a_\nu|(|\pi|^i, \dots, |\pi|^i)^\nu = 0\right\},$$

which we think of as function algebras on the ball $B^n(k_a, |\pi|^i)$ of radius $|\pi|^i$. Each A_i is affinoid, since it is the same as T_n with $\pi^{-i}x_i$ serving as indeterminates. Thus, we get a chain of affinoid algebras

$$k\langle X\rangle = A_0 \supset A_1 \supset \cdots \supset k[X]$$

which gives an increasing chain of affinoid subdomains

$$B^n = \operatorname{Sp} A_0 \hookrightarrow \operatorname{Sp} A_1 \hookrightarrow \cdots.$$

These affinoid subdomains are now glued together to give the analytic affine n-space $\mathbb{A}^n$, which has $\{\operatorname{Sp} A_i\}_{i\ge 0}$ as an admissible covering. Looking at the underlying topological spaces of $\operatorname{Sp} A_i$, we see an increasing chain

$$\operatorname{Max} A_0 \subset \operatorname{Max} A_1 \subset \cdots \subset \operatorname{Max} k[X]$$

of balls

$$\operatorname{Max} A_i = \{z \in \operatorname{Max} k[X] : |z_j| \le |\pi|^i \ \forall j\} \simeq B^n(k, |\pi|^i).$$

These balls are subsets of the affine algebraic space $\operatorname{Spec} k[X]$, but are not themselves affine subschemes. They are affinoid varieties, however, and paste together to give the analytic space $\mathbb{A}^n = (\operatorname{Spec} k[X])^{\mathrm{an}}$.

Now it is clear how to give a structure of an analytic space to any affine variety $V \hookrightarrow \operatorname{Spec} k[X]$. Namely, we paste together the affinoid covering obtained from the intersections

$$V \cap B^n(k, |\pi|^i) = \{z \in V : |z_j| \le |\pi|^i \ \forall j\}.$$

Explicitly, $V = \operatorname{Spec} B$ for some finitely generated k-algebra $B = k[X]/\mathfrak{a}$. So, there is a sequence of k-algebras

$$A_0/\mathfrak{a} A_0 \leftarrow A_1/\mathfrak{a} A_1 \leftarrow \cdots \leftarrow B$$

corresponding to a sequence of affinoid subdomains

$$\operatorname{Sp} A_0/\mathfrak{a} A_0 \hookrightarrow \operatorname{Sp} A_1/\mathfrak{a} A_1 \hookrightarrow \cdots.$$

We paste these together to obtain an analytic space V^{an} with $\{\operatorname{Sp} A_i/\mathfrak{a} A_i\}_{i\ge 0}$ as an admissible affinoid covering. Just as above, the underlying set of V^{an} can be identified with $\operatorname{Max} B$, and $\operatorname{Max} A_i/\mathfrak{a}A_i$ can be identified with $V \cap B^n(k, |\pi|^i)$.

Returning to $(k^*)^n$, we now have a recipe for giving it a structure of an analytic space, as the analytification of the algebraic variety $\mathbf{G}^n_{m,k}$. For example, we can take $B = k[X]/\mathfrak{a}$, with $\mathfrak{a} = (\dots, x_i x_{n+i} - 1, \dots)$ and $X = (x_1, \dots, x_n, x_{n+1}, \dots, x_{2n})$, and define $(k^*)^n := (\operatorname{Spec} B)^{\mathrm{an}}$. If we set $\zeta = (\zeta_1, \dots, \zeta_n)$, then the sequence

$$A_0/\mathfrak{a}A_0 \leftarrow A_1/\mathfrak{a}A_1 \leftarrow \cdots \leftarrow B$$

is isomorphic to

$$k\langle \zeta, \zeta^{-1}\rangle = B_0 \leftarrow B_1 \leftarrow \cdots \leftarrow k[\zeta, \zeta^{-1}] \simeq B,$$

where by B_i we denote the image of $A_i/\mathfrak{a}A_i$ in $k[\![\zeta, \zeta^{-1}]\!]$. Thus, B_i are the k-algebras

$$\begin{aligned} B_i &= \left\{ \sum_{\nu=-\infty}^{\infty} a_\nu \zeta^\nu : \lim_{\nu\to\infty} |\pi^i|^\nu |a_\nu| = 0,\ \lim_{\nu\to-\infty} |\pi^i|^\nu |a_\nu| = 0 \right\} \\ &= k\langle \pi^{-i}\zeta, (\pi^i\zeta)^{-1}\rangle \end{aligned}$$

of convergent Laurent series. As affinoid varieties, they are called Laurent domains.

In general, given an affinoid k-algebra A with $Z = \operatorname{Sp} A$, and a system of elements $f = (f_1, \dots, f_n)$, $g = (g_1, \dots, g_m)$ in A, the space

$$Z(f, g^{-1}) = \{x \in Z : |f_i(x)| \le 1, |g_j(x)| \ge 1\ \forall i, j\}$$

is called a Laurent Domain in Z. It is an affinoid subdomain of Z, corresponding to the ring

$$A\langle f, g^{-1}\rangle = A\langle X, Y\rangle/(X - f, gY - 1).$$

In our case, if we set $A_i = k\langle \pi^{-i}\zeta\rangle$, so $\operatorname{Sp} A_i \simeq B^n(k, |\pi|^i)$, we see that $B_i = A_i\langle 1, (\pi^i\zeta)^{-1}\rangle$. Hence,

$$\operatorname{Sp} B_i = \operatorname{Sp} A_i\langle 1, (\pi^i\zeta)^{-1}\rangle = B^n(k, |\pi|^i)(1, (\pi^i\zeta)^{-1})$$

is a Laurent domain in $B^n(k, |\pi|^i)$, whose underlying topological space is the annulus

$$\begin{aligned} \operatorname{Max} B_i &= \{x \in B^n(k, |\pi|^i) : |\pi^i x_j| \ge 1\ \forall j\} \\ &= \{x \in \operatorname{Max} k[\zeta, \zeta^{-1}] : |\pi|^{-i} \le |x_j| \le |\pi|^i\ \forall j\}. \end{aligned}$$

Thus, the analytic space $G = (k^*)^n$ is obtained by pasting together the affinoid annuli $\operatorname{Sp} B_i$. Moreover, the group operations are given by analytic maps, so G is actually an analytic group variety.

The fact that the analytic structure on G is obtained from an increasing chain of subdomains has consequences for the ring of global functions $\mathcal{O}_G(G)$. If $f \in \mathcal{O}_G(G)$, then the compatibility conditions on the intersections in the admissible covering $(\operatorname{Sp} B_i)$ determine f as an element of $k[\![\zeta, \zeta^{-1}]\!]$. Therefore, each global function has a unique Laurent series expansion converging on all of G. Moreover, since G has coordinate functions $\zeta_i(x) = x_i$, any morphism ϕ into G has components $\phi_i = \zeta_i \circ \phi$. When $\phi \in \operatorname{End}(G)$, the components ϕ_i are global nonvanishing functions.

3.2 Rigid Analytic Tori and Mumford Curves

If Y is a rigid analytic space, and Γ is a group of automorphisms of Y, then Γ acts discontinuously on Y if there is an admissible affinoid covering $(Y_i) \in \operatorname{Cov}(Y)$ such that the set $\{\gamma \in \Gamma : \gamma Y_i \cap Y_i \neq \emptyset\}$ is finite for each i. In this case, we can give the quotient $Z = Y/\Gamma$ a structure of a rigid analytic space as well. To do so, we need to specify for it a topology, a Grothendieck topology, and a structure sheaf. As a topological space, Z has the quotient topology via the canonical map $p\colon Y \to Z$. For the Grothendieck topology, we define a subset $U \subset Z$ to be an admissible affinoid if $p^{-1}U$ is admissible. Similarly, a covering of

U by admissible sets U_i is admissible if $(p^{-1}U_i)$ is an admissible covering of $p^{-1}U$. The structure sheaf is defined in the usual way: $\mathcal{O}_Z(Z) = k$ and $\mathcal{O}_Z(U) = \mathcal{O}_Y(p^{-1}U)^{\Gamma}$.

The examples of this quotient construction which we are interested in are analytic tori and Mumford curves. For the analytic torus, we start with the analytic group variety $G = (k^*)^n$. A subset $\Lambda \subset G$ is called discrete if its intersection with each affinoid in G is finite. If in addition Λ has full rank and no torsion elements, it is called a lattice. One can define a group homomorphism $\ell\colon (k^*)^n \longrightarrow \mathbb{R}^n$ given by

$$z = (z_1, \ldots, z_n) \mapsto \ell(z) = (-\log|z_1|, \ldots, -\log|z_n|),$$

and then Λ is a lattice in $(k^*)^n$ if and only if $\ell(\Lambda) \simeq \mathbb{Z}^n$ is a full rank lattice in $\mathbb{R}^n$. Since a lattice Λ viewed as a group of automorphisms acts discontinuously on G, we define an analytic torus as the quotient $T = (k^*)^n/\Lambda$.

The second construction we need is that of a Mumford curve. Consider the group $\mathrm{PGL}_2(k)$ acting as analytic automorphisms on $\mathbb{P}^1_k$, and let $\Gamma \subset \mathrm{PGL}_2(k)$ be a subgroup. A point $p \in \mathbb{P}^1_k$ is called a limit point of Γ if $\exists q \in \mathbb{P}^1_k$ and an infinite sequence $\{\gamma_n\}_{n\geq 1} \subset \Gamma$ of distinct elements with $\lim \gamma_n(q) = p$. The set of limit points of Γ is denoted $\mathcal{L}(\Gamma)$. Γ is called discontinuous if $\mathcal{L}(\Gamma) \neq \mathbb{P}^1_k$, and every orbit Γp has a compact closure. A finitely generated discontinuous group is called a Schottky group if it has no nontrivial elements of finite order. The set $\Omega = \mathbb{P}^1_k - \mathcal{L}(\Gamma)$ of "ordinary" points of a Schottky group has a structure of a rigid analytic space on which Γ acts discontinuously. The quotient $S = \Omega/\Gamma$, in the category of rigid analytic spaces, is called a Mumford curve. As the field of meromorphic functions on S is a finite algebraic extension of $k(t)$, S is actually a nonsingular curve. When the Schottky group Γ is generated by one element, which can be taken as

$$\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}, \quad \text{for some } q \in k \text{ with } |q| < 1,$$

then S is isomorphic to the Tate elliptic curve E_q. Otherwise, Γ is generated by g hyperbolic matrices, and S is the analytification of a projective, nonsingular and irreducible curve C/k of genus g. As we will see in Sect. 4, the Jacobians of Mumford curves are analytic tori whose period lattices can be described in terms of the Schottky group Γ. For more details on Mumford curves, as well as explicit constructions of the analytic spaces Ω and Ω/Γ, the reader is referred to [4, Sect. 5.4] and [7, Chaps. I–III].

3.3 The Isogeny Theorem for Analytic Tori

Complex uniformization of algebraic curves is useful in the study of isogenies because we understand well the isogenies of complex tori. In order to fully take advantage of p-adic uniformization of curves, we first need to study the structure of isogenies of rigid analytic tori. It turns out that these maps have a simple form, and are completely determined by the period lattices. Since the results are similar, it is interesting to consider the complex and non-Archimedean theories in parallel, so we first give a brief review of complex tori and their isogenies.

A lattice $\Lambda \subset \mathbb{C}^n$ is the $\mathbb{Z}$-span of some $\mathbb{R}$-basis of $\mathbb{C}^n$, and it defines a complex torus as the quotient $\mathbb{C}^n/\Lambda$. The torus is given the quotient topology, and the sheaf is defined by the principle that analytic functions on open subsets of the torus should be the Λ invariant analytic functions on the corresponding subsets of $\mathbb{C}^n$. In general, an isogeny of analytic tori should be an analytic mapping which is also a group homomorphism, and has finite kernel and cokernel. However, mostly due to Liouville's Theorem on $\mathbb{C}^n$, we find that there is very little choice of the form of an isogeny $\psi\colon \mathbb{C}^n/\Lambda_1 \longrightarrow \mathbb{C}^n/\Lambda_2$. As $\mathbb{C}^n$ is the universal cover of the tori, ψ lifts to an analytic map $\phi\colon \mathbb{C}^n \longrightarrow \mathbb{C}^n$ satisfying $\phi(\Lambda_1) \subset \Lambda_2$. Using basic theorems of complex analysis, one can show that ψ must be the map $z \mapsto Mz$ for some $M \in M_n(\mathbb{C})$. See for example [3, pp. 26 and 216]. The final result is that every isogeny of complex tori is given by an action of a complex matrix.

Let us apply this to the problem of determining if two curves C_1 and C_2 are isogenous. Uniformizing the curves, one obtains the period lattices Λ_1 and Λ_2, and isomorphisms $\rho_i\colon J_i \longrightarrow \mathbb{C}^n/\Lambda_i$ of the Jacobians J_i of C_i. Let $\{v_1, \ldots, v_{2n}\}$ and $\{w_1, \ldots, w_{2n}\}$ be the generators of Λ_1 and Λ_2, respectively. Determining if an isogeny $\phi\colon J_1 \longrightarrow J_2$ exists at the level of Jacobians can be difficult, but if it does, then it induces a matrix map M of the complex tori. This matrix must satisfy the condition $M(\Lambda_1) \subset \Lambda_2$, which gives a set of relations

$$Mv_i = \sum_{j=1}^{2n} a_{ij} w_j.$$

Hence, the problem of detecting isogenies of curves reduces to the following linear algebra problem: given two $n \times 2n$ matrices V and W whose columns are the lattice generators $\{v_i\}_{i=1}^{2n}$ and $\{w_i\}_{i=1}^{2n}$, respectively, can one find matrices $M \in M_n(\mathbb{C})$ and $A = (a_{ij}) \in M_{2n}(\mathbb{Z})$ such that $MV = WA^T$. If so, then the analytic map $z \mapsto Mz$ induces an algebraic map of the Jacobians, which is an isogeny of degree $\det A$ (and actually defined over the field of definition of M [10]).

Now let k be a field complete with respect to a non-Archimedean valuation. We could try to study isogenies of rigid analytic tori by mimicking the complex theory, but this approach quickly runs into problems, as there are some significant differences. First of all, $(k^*)^n$ is not simply connected. Thus, it is not the universal cover of $(k^*)^n/\Lambda$, at least not in the usual topological sense. So one can not automatically assume that analytic maps of tori lift to analytic maps of $(k^*)^n$.

Another significant difference is that $(k^*)^n$ is not a k vector space. For an isogeny ϕ of complex tori, the fact that $\phi(\Lambda_1) \subset \Lambda_2$ induces a mapping

$$\gamma\colon \{v_i\} \longrightarrow \left\{\sum a_{ij} w_j\right\}$$

between the basis elements. But any such mapping extends to a global linear map

$$\mathbb{C}^n \longrightarrow \mathbb{C}^n\colon z = \sum \alpha_i v_i \mapsto \sum \alpha_i \gamma(v_i),$$

given by some matrix M. Then one can argue that ϕ must have been the map $z \mapsto Mz$.

In the rigid analytic case, the condition $\phi(\Lambda_1) \subset \Lambda_2$ still defines a mapping on the lattice generators

$$\gamma\colon \{v_i\} \longrightarrow \left\{\prod w_j^{a_{ij}}\right\},$$

but as the lattice generators are no longer a basis of $(k^*)^n$, it is not clear how to extend the mapping γ to a global map on all of $(k^*)^n$. Hence, the condition $\phi(\Lambda_1) \subset \Lambda_2$ does not automatically present us with a candidate for the map ϕ, as is the case over the complex numbers.

Furthermore, the multiplicative analogy of the map $z \mapsto Mz$ is the map $z \mapsto z^M$, where for a vector $z = (z_1, \ldots, z_n) \in (k^*)^n$ and a matrix $M = (m_{ij}) \in M_n(k)$, by z^M we mean the vector

$$z^M = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}^{(m_{ij})} = \begin{pmatrix} z_1^{m_{11}} z_2^{m_{12}} \dots z_n^{m_{1n}} \\ \vdots \\ z_1^{m_{n1}} z_2^{m_{n2}} \dots z_n^{m_{nn}} \end{pmatrix}.$$

Clearly, this map is an analytic group homomorphism, whenever defined. The problem is, of course, that in general this map is not well defined, as there is no canonical action $x \mapsto x^a$ of k on k^*. For example, note that while $\frac{1}{n}x$ is uniquely determined by x, there are n choices for $x^{\frac{1}{n}}$.

In light of these differences, it may be a little surprising that the form of isogenies of rigid analytic tori is still very similar to the complex analytic case. The key ingredient in the p-adic theory is the nontrivial fact that the group of invertible global functions $\mathcal{O}((k^*)^n)^*$ is the group of monomials $\{\lambda z^\alpha \mid \lambda \in k^*, \alpha \in \mathbb{Z}^n\}$, proved in [4, Chap. 6]. Since the component functions of any $\phi \in \mathrm{End}((k^*)^n)$ are group homomorphisms, they lie in $\mathcal{O}((k^*)^n)^*$, with constant term $\lambda = 1$. This gives a canonical identification $\mathrm{End}((k^*)^n) \simeq M_n(\mathbb{Z})$. (Note, for comparison, that $\mathrm{End}(\mathbb{C}^n) \simeq M_n(\mathbb{C})$.) The second necessary fact is that analytic maps of tori ϕ: $(k^*)^n/\Lambda_1 \longrightarrow (k^*)^n/\Lambda_2$ do lift to $\hat{\phi} \in \mathrm{End}((k^*)^n)$ satisfying $\hat{\phi}(\Lambda_1) \subset \Lambda_2$. The proof of this is a consequence of the sheaf definition on the torus, and can be found in [5, 6]. Together, these facts could be used to prove Theorem 1 below for a general field k (complete with respect to a non-Archimedean valuation). However, for subfields of $\mathbb{C}_p$, we prove the theorem using basic methods, which do not require any of the machinery of [4]. Moreover, this proof is constructive, and we use it later for the computation of the isogenies.

To fix the notation, we will consider two lattices Λ_1 and Λ_2 generated by vectors $v_1, \dots, v_n$ and $w_1, \dots, w_n$, respectively. Using the group homomorphism ℓ: $(k^*)^n \longrightarrow \mathbb{R}^n$: $z \mapsto (-\log|z_1|, \dots, -\log|z_n|)$, set $x_i = \ell(v_i)$ and $y_i = \ell(w_i)$, and let $X, Y \in M_n(\mathbb{R})$ be the matrices with column vectors x_i and y_i. Also, X' and Y' will denote the lattices in $\mathbb{R}^n$ generated by the columns of X and Y, respectively.

Theorem 1 ($k \subset \mathbb{C}_p$) *Let ψ: $(k^*)^n/\Lambda_1 \longrightarrow (k^*)^n/\Lambda_2$ be an isogeny of analytic tori. Then it induces an isogeny of real analytic tori $\tilde{\phi}$: $\mathbb{R}^n/X' \longrightarrow \mathbb{R}^n/Y'$, given by matrix multiplication map $z \mapsto Mz$, where $M = YA^TX^{-1} \in M_n(\mathbb{Z})$. Moreover, ψ is the map $z \mapsto z^M$.*

Proof ψ lifts to an analytic homomorphism ϕ: $(k^*)^n \longrightarrow (k^*)^n$ such that $\phi(\Lambda_1) \subset \Lambda_2$. Restricting to the respective lattices, we have the following commutative diagram, in which the vertical maps are isomorphisms:

$$\begin{array}{ccc} \Lambda_1 & \xrightarrow{\ \phi\ } & \Lambda_2 \\ \Big\downarrow{\scriptstyle l} & & \Big\downarrow{\scriptstyle l} \\ X' & \xrightarrow{\ \tilde{\phi}\ } & Y' \end{array}$$

The condition $\phi(\Lambda_1) \subset \Lambda_2$ specifies a set of relations $\phi(v_t) = \prod_{j=1}^n w_j^{a_{tj}}$, which give a matrix $A = (a_{ij}) \in M_n(\mathbb{Z})$. Since

$$\ell(\phi(v_t)) = \begin{pmatrix} -\log|\phi(v_t)_1| \\ \vdots \\ -\log|\phi(v_t)_n| \end{pmatrix} = \begin{pmatrix} \sum_{j=i}^n a_{tj}(y_j)_1 \\ \vdots \\ \sum_{j=1}^n a_{tj}(y_j)_n \end{pmatrix} = \sum_{j=1}^n a_{tj} y_j,$$

and $\ell^{-1}(x_t) = v_t$, we see that the group homomorphism $\tilde{\phi} = \ell \circ \phi \circ \ell^{-1}$ is given on the generators of X' by the relations $\tilde{\phi}(x_t) = \sum_{j=1}^{n} a_{tj} y_j$. In matrix notation, we have the single equation

$$\begin{pmatrix} | & \dots & | \\ \tilde{\phi}(x_1) & \dots & \tilde{\phi}(x_n) \\ | & \dots & | \end{pmatrix} = YA^T.$$

Since X is nonsingular, we can consider the matrix $M = YA^T X^{-1}$. We see that $Mx_i = YA^T X^{-1} x_i = i$th column of YA^T, which is by construction $\tilde{\phi}(x_i)$. It follows that as a map on lattices, $\tilde{\phi}$ is the map $z \mapsto Mz$. But the matrix M extends to a linear map on all of $\mathbb{R}^n$, satisfying $M(X') \subset Y'$, and so it descends to an isogeny

$$\mathbb{R}^n/X' \longrightarrow \mathbb{R}^n/Y' \colon z + X' \mapsto Mz + Y',$$

which we will also call $\tilde{\phi}$.

Now suppose that M actually has integral coefficients. Then the map $z \mapsto Mz$ lifts to the homomorphism $z \mapsto z^M$ such that the following diagram commutes

$$\begin{array}{ccc} (k^*)^n & \xrightarrow{z \mapsto z^M} & (k^*)^n \\ l \downarrow & & \downarrow l \\ \mathbb{R}^n & \xrightarrow{z \mapsto Mz} & \mathbb{R}^n \end{array}$$

since for $M \in M_n(\mathbb{Z})$ we have $\ell(z^M) = M\ell(z)$. Clearly, $(z \mapsto z^M)|_{\Lambda_1} = \phi|_{\Lambda_1}$, so by the following lemma, ϕ is the map $z \mapsto z^M$, and the same for ψ.

Lemma 2 *Let Λ be a lattice in $(k^*)^n$, and suppose that $\alpha, \beta\colon (k^*)^n \longrightarrow (k^*)^n$ are analytic group homomorphisms such that $\alpha|_\Lambda = \beta|_\Lambda$. Then $\alpha = \beta$.*

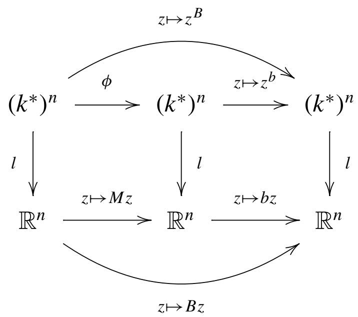
Proof It is enough to prove that the component functions $g_i(z) = \zeta_i \circ \alpha(z)$ and $h_i(z) = \zeta_i \circ \beta(z)$ are equal for all i. Since $h_i \in \mathcal{O}((k^*)^n)^*$, the function $F(z) = g_i(z)/h_i(z)$ is analytic. Then $\alpha|_\Lambda = \beta|_\Lambda$ implies that

$$F(\lambda z) = \frac{g_i(\lambda z)}{h_i(\lambda z)} = \frac{g_i(\lambda) g_i(z)}{h_i(\lambda) h_i(z)} = \frac{g_i(z)}{h_i(z)} = F(z), \quad \forall \lambda \in \Lambda.$$

Let G be the torus $(k^*)^n/\Lambda$. Since F is analytic on $(k^*)^n$ and Λ-invariant, it descends to an element $\rho \in \mathcal{O}_G(G) = k$. Thus, $g_i(z) = \rho h_i(z)$, and since these functions are group homomorphisms, it follows that $\rho = 1$. Repeating this argument for each i shows that $\alpha = \beta$. □

In general, $k \subset \mathbb{C}_p$ implies that $|k^*| \subset |\mathbb{C}_p^*| = p^{\mathbb{Q}} = \{p^\nu : \nu \in \mathbb{Q}\}$. So $\ell(z_1, \dots, z_n) = \log p(\nu_1, \dots, \nu_n)$ for $\nu_i \in \mathbb{Q}$. In particular, we can write $X = (\log p)\bar{X}$ and $Y = (\log p)\bar{Y}$ where $\bar{X}, \bar{Y} \in M_n(\mathbb{Q})$. Thus, $M = YA^T X^{-1} = \bar{Y} A^T \bar{X}^{-1} \in M_n(\mathbb{Q})$. So we can find an integer

b such that $bM = B \in M_n(\mathbb{Z})$. Consider the following diagram:



The top diagram commutes by Lemma 2, since $(z \mapsto z^B)|_{\Lambda_1} = (\phi^b)|_{\Lambda_1}$. This proves the theorem. □

Nota bene Strictly speaking, we have only shown that $\psi^b \in M_n(\mathbb{Z})$. But since ψ is an isogeny $\Longrightarrow \psi^b$ is an isogeny, we can assume that $\psi = \psi^b$, at least from the point of view of detecting when two tori are isogenous. In practice, one would always find that $b = 1$, as $M \in M_n(\mathbb{Z})$ by [4].

We finally come to the main theorem of this section, about isogenies of rigid analytic tori. It is modeled after the one-dimensional case, which says that two Tate elliptic curves E_{q_1} and E_{q_2} are isogenous iff there are integers a and b such that $q_1^a = q_2^b$ [8]. To state the theorem in a concise form, we will write the matrix equation $V^B = {}^A W$ as the multiplicative version of $BV = WA$. In other words, if the columns of W are the vectors $w_1, \ldots, w_n$, then ${}^A W$ is the matrix whose ith column is the vector $\prod_{j=1}^n w_j^{a_{ji}}$, whereas the ith column of V^B is the vector v_i^B. In our case, the columns of V and W are the generators of the lattices Λ_1 and Λ_2, respectively. Also, considering the remarks made prior to Theorem 1, we can dispense with the condition $k \subset \mathbb{C}_p$.

Theorem 3 *ψ: $(k^*)^n/\Lambda_1 \longrightarrow (k^*)^n/\Lambda_2$ is an isogeny $\Longleftrightarrow \exists A, B \in M_n(\mathbb{Z})$ such that $V^B = {}^A W$. Moreover, $\psi = (z \mapsto z^B)$ is completely determined by A, $\ell(\Lambda_1)$ and $\ell(\Lambda_2)$.*

Proof ($\Longleftarrow$) Given such matrices A and B, the map $\psi(z) = z^B$ is an analytic group homomorphism $(k^*)^n \longrightarrow (k^*)^n$. Since $\psi(v_i) = \prod_{j=1}^n w_j^{a_{ji}}$, where $A = (a_{ij})$, it follows that $\psi(\Lambda_1) \subset \Lambda_2$, so it descends to an isogeny of the tori.

($\Longrightarrow$) Given an isogeny ψ of the tori, we lift it to a map $\phi \in \mathrm{End}((k^*)^n)$, which must have the form $z \mapsto z^B$ for some $B \in M_n(Z)$, by the previous theorem. Then $\phi(\Lambda_1) \subset \Lambda_2$, which specifies the second matrix $A = (a_{ij}) \in M_n(\mathbb{Z})$ such that $V^B = {}^A W$.

Moreover, by passing to the induced map on the real tori, we see that in both directions, the matrix B must equal $\ell(\Lambda_2) A^T \ell(\Lambda_1)^{-1}$. □

This theorem turns out to have important computational consequences, which stem from the fact that the homomorphism ℓ only depends on the valuation of its argument. We will discuss this along with other advantages of p-adic uniformization in Sect 5.2.

4 Jacobians of Mumford Curves

In this section we give an overview of Jacobians of Mumford curves. For comparison, the theory is presented in parallel with the complex theory of Jacobians. As it turns out, Mumford curves over any non-Archimedean field k admit the type of explicit description of their Jacobians as is available only for curves over $\mathbb{C}$ in the Archimedean case. Our goal here is to give a general idea of the concepts involved. For proofs of the statements and more details, the reader is referred to [7, Chap. VI].

In general, given a nonsingular projective curve C over a field k, its Jacobian J_C should be an abelian variety whose group of closed points is isomorphic to $\mathrm{Pic}^0(C)$, the group of degree zero divisor classes on the curve. At least when $C(k) \neq \emptyset$, the Jacobian of C is defined by a universal property as a variety over k, so it is unique. In fact, J_C is the unique abelian variety which is birational to $C^{(g)}$, where g is the genus of the curve. However, since the Jacobian is defined by a universal property, it is usually not given in terms of any explicit equations which could be used for computations, except possibly in the case of elliptic curves. The situation, though, is much better when $k = \mathbb{C}$, as now the curve has a structure of a compact Riemann surface, also denoted by C. Topologically, C is a g-holed torus with a canonical basis $\{\gamma_1, \dots, \gamma_{2g}\}$ for $H_1(C, \mathbb{Z})$. It also comes with a g-dimensional complex vector space $\Omega^1(C)$ of holomorphic differentials. The map $\gamma \mapsto \int_\gamma$ identifies $H_1(C, \mathbb{Z})$ with a subgroup of $\Omega^1(C)^\vee$, and one could consider the quotient

$$J = \Omega^1(C)^\vee / H_1(C, \mathbb{Z}).$$

Given any choice of a basis $\{\omega_1, \dots, \omega_g\}$ of $\Omega^1(C)$ over $\mathbb{C}$, the $2g$ period vectors

$$v_j = \begin{pmatrix} \int_{\gamma_j} \omega_1 \\ \vdots \\ \int_{\gamma_j} \omega_g \end{pmatrix} \in \mathbb{C}^g$$

are $\mathbb{R}$-linearly independent, and their $\mathbb{Z}$-span defines the period lattice Λ of C. Moreover, the evaluation map

$$\int_\gamma \mapsto \left(\int_\gamma \omega_1, \dots, \int_\gamma \omega_g \right)$$

identifies J with the complex torus $\mathbb{C}^g/\Lambda$. J also has a Riemann form, so in fact it is an abelian variety.

To see which abelian variety it is, pick a basepoint $P_0 \in C$ and consider the map

$$C \longrightarrow J\colon\ P \mapsto \int_{P_0}^{P}.$$

Moding $\Omega^1(C)^\vee$ by $H_1(C, \mathbb{Z})$ guarantees that the integral on the right is path independent, so the map is well defined. It extends to the map

$$\psi\colon \mathrm{Pic}^0(C) \longrightarrow J\colon \left[\sum n_i P_i \right] \mapsto \sum n_i \int_{P_0}^{P_i},$$

and the Abel–Jacobi Theorem says that ψ is a group isomorphism. Thus, J is an abelian variety which is isomorphic as a group to $\mathrm{Pic}^0(C)$, and so by uniqueness of Jacobians,

$J = J_C$. Therefore, when $k = \mathbb{C}$, we obtain a nice representation of the Jacobian of a curve, which is very useful for computations.

Now let us consider the non-Archimedean case, where $S = \Omega/\Gamma$ is a genus g Mumford curve. Even though we can no longer rely on Riemann surface theory, we can find analogues of J, the Abel–Jacobi map ψ, and the identification of J with an analytic torus. These analogues allow us to write down a description of the Jacobian of S which is as explicit as it was over $\mathbb{C}$.

The most important ingredient in the theory of Jacobians of Mumford curves is the theta function. Essentially every object which we will consider is related somehow to this remarkable function, so its definition is a good place to start. For any $a, b \in \Omega$, we define

$$\Theta(a, b; z) = \prod_{\gamma \in \Gamma} \frac{z - \gamma(a)}{z - \gamma(b)}.$$

The product converges to give a meromorphic function on all of Ω. If a and b are in the same Γ orbit, then $\Theta(a, b; z)$ has no zeros or poles; otherwise, it has simple zeros at Γa and simple poles at Γb, and no others. As a special case, for any $\alpha \in \Gamma$, we define on Ω the analytic, nonvanishing function

$$u_\alpha(z) = \Theta(a, \alpha(a); z).$$

These functions are independent of the choice of $a \in \Omega$, and satisfy the relations

$$u_{\alpha\beta}(z) = u_\alpha(z) \cdot u_\beta(z) \quad \forall \alpha, \beta \in \Gamma.$$

Also, $u_\alpha(z)$ is constant if and only if $\alpha \in [\Gamma, \Gamma]$. As $\alpha \equiv \gamma_1^{n_1} \cdots \gamma_g^{n_g} \bmod [\Gamma, \Gamma]$ for some $n_i \in \mathbb{Z}$, where $\{\gamma_i\}$ are the generators of Γ, if we set $u_i(z) := u_{\gamma_i}(z)$, we have

$$u_\alpha(z) = a_0 u_1(z)^{n_1} \cdots u_g(z)^{n_g} \quad \text{for some } a_0 \in k^*.$$

An automorphic form is defined as a meromorphic function f on Ω such that for any $\alpha \in \Gamma$, there exists a constant $c(\alpha) \in k^*$ for which $f(z) = c(\alpha) f(\alpha z)$. $c = c_f$ is called the automorphy factor of f. Quite remarkably, the automorphy factors are group homomorphisms $\Gamma \to k^*$, since for any $\alpha, \beta \in \Gamma$,

$$f(z) = c(\beta) f(\beta z) = c(\beta) c(\alpha) f(\alpha\beta z), \quad \text{and}$$
$$f(z) = c(\alpha\beta) f(\alpha\beta z),$$

so $c(\alpha\beta) = c(\alpha) \cdot c(\beta)$.

Returning to the theta function $\Theta(a, b; z)$, its automorphy factors depend analytically on the parameters a and b, and are given by the equation

$$c_{\Theta(a,b'z)}(\alpha) = \frac{u_\alpha(a)}{u_\alpha(b)}.$$

Next, we state the two most important theorems of this section. The first one says that every automorphic form is a product of theta functions, and the second says that every group homomorphism $\Gamma \to k^*$ is an automorphy factor of some automorphic form. Together, they define the Abel–Jacobi isomorphism.

Theorem 4 [7] *Let $f(z)$ be an automorphic form on Ω. Then*

$$f(z) = a_0 \cdot \Theta(a_1, b_1; z) \cdots \Theta(a_r, b_r; z)$$

for $a_0 \in k$, $a_i, b_i \in \Omega$.

In particular,

$$c_f(\alpha) = \prod_{i=1}^{r} c_{\Theta(a_i,b_i;z)}(\alpha) = \prod_{i=1}^{r} \frac{u_\alpha(a_i)}{u_\alpha(b_i)}.$$

Theorem 5 [7] *Let $\Gamma^\vee = \mathrm{Hom}(\Gamma, k^*)$, and let $c \in \Gamma^\vee$. Then there exists an automorphic form $f(z)$ on Ω such that $c = c_f$.*

To define the Abel–Jacobi map, we first need to describe the Picard group on S. Let f be an automorphic form on Ω, and $a \in \Omega$. Because of the relation $f(z) = c(\alpha) f(\alpha z)$, we see that if a is a pole or a zero of f of order r, then so is αa for every $\alpha \in \Gamma$. Hence the usual function $\mathrm{ord}_s f(z)$ is well defined for all automorphic forms on Ω and all points $s \in S$. We define

$$\mathrm{div}\, f = \sum_{s \in S : \mathrm{ord}_s f(z) > 0} \mathrm{ord}_s f \cdot s - \sum_{s \in S : \mathrm{ord}_s f(z) < 0} (-\mathrm{ord}_s f(z)) \cdot s.$$

Given a divisor $\mathfrak{a} = \sum_{i=1}^{r} \bar{a}_i - \bar{b}_i \in \mathrm{Div}^0(S)$, $\mathfrak{a} = \mathrm{div} \prod_{i=1}^{r} \Theta(a_i, b_i; z)$. Conversely, let $f(z)$ be an automorphic form on Ω. If $f(z)$ has no zeros or poles, then $f(z) = a_0 \cdot u_\alpha(z)$ for some $\alpha \in \Gamma$, and $\mathrm{div}\, f = 0$. Otherwise, f has a representation

$$f(z) = a_0 \prod_{i=1}^{r} \Theta(a_i, b_i; z) \quad \text{such that } a_i\Gamma \neq b_j\Gamma \ \ \forall i, j,$$

and $\mathrm{div}\, f = \sum_{i=1}^{r} \bar{a}_i - \bar{b}_i$. This gives an easy and explicit correspondence between degree zero divisors $\mathfrak{a}$ and automorphic forms f with $\mathrm{div}\, f = \mathfrak{a}$.

The degree zero principal divisors are the divisors of the form $\mathrm{div}\, h$, where h is a Γ-invariant meromorphic function on Ω, that is, an actual meromorphic function on S. Then as usual, we define an equivalence on $\mathrm{Div}^0(S)$ by

$$\mathfrak{a} \sim \mathfrak{b} \iff \mathfrak{a} - \mathfrak{b} \text{ is principal},$$

and denote by $\mathrm{Pic}^0(S)$ the group of equivalence classes.

Considering what guided our choice of the model J for the Jacobian in the complex case, we can isolate two important factors. First, there was an evaluation map, given by path integration, which identified J with a complex torus, and through this map J acquired the structure of an abelian variety. Second, there was a connection between degree zero divisors and elements of J, through which we proved that the abelian variety J is the Jacobian. In the case at hand, we have just described a connection between degree zero divisors and automorphic forms. Also, the automorphy factors of these forms are maps into k^*, which could be used to define an evaluation map. This suggests that the right analogue of the group $\Omega^1(C)^\vee$ in the complex case is the group $\Gamma^\vee$ in the non-Archimedean case. Theorem 5 tells us that every element of $\Gamma^\vee$ is the automorphy factor of some automorphic form. So the connection with divisors could simply be $c = c_f \mapsto \mathrm{div}\, f$. Moreover, in the complex case, a genus g curve gave a choice of g basis elements $\{\omega_1, \dots, \omega_g\}$ of $\Omega^1(C)$ over $\mathbb{C}$, which then defined an identification

$$e\colon \Omega^1(C)^\vee \longrightarrow \mathbb{C}^g\colon \int_\gamma \mapsto \left(\int_\gamma \omega_1, \dots, \int_\gamma \omega_g\right).$$

In the present case, a genus g Mumford curve is defined by a matrix group Γ on g generators, and a choice of a basis $\{\gamma_1, \dots, \gamma_g\}$ of this group defines an identification

$$e\colon \Gamma^\vee \longrightarrow (k^*)^g\colon c \mapsto (c(\gamma_1), \dots, c(\gamma_g)).$$

Next, we develop these ideas into a construction of J_S.

Consider the map

$$\lambda\colon \Gamma^\vee \longrightarrow \mathrm{Pic}^0(S)\colon c \mapsto [\mathrm{div}\, f_c(z)],$$

where the brackets denote an equivalence class, and f_c is an automorphic form on Ω with the factor c. λ^{-1} is the more usual form of the Abel–Jacobi map, and can be defined as follows: since every $\mathfrak{a} = \sum_{i=1}^r \bar{a}_i - \bar{b}_i$ can be written as $\mathrm{div} \prod_{i=1}^r \Theta(a_i, b_i; z)$, λ^{-1} sends $\mathfrak{a} = \mathrm{div}\, f$ to c_f. Returning to the map λ, one can show that it is a well defined, surjective homomorphism whose kernel is a subgroup L of $\Gamma^\vee$ of rank g. L is exactly the subgroup of automorphy factors of the forms $u_\alpha(z)$ for different $\alpha \in \Gamma$, and its image under the evaluation map is a lattice Λ in $(k^*)^g$. Thus, we define

$$J = \Gamma^\vee / L = \mathrm{Hom}(\Gamma, k^*)/L,$$

and obtain the following isomorphisms:

$$\mathrm{Pic}^0(S) \underset{\simeq}{\overset{\lambda}{\longleftarrow}} J \underset{\simeq}{\overset{e}{\longrightarrow}} (k^*)^g/\Lambda.$$

The identification e endows J with the structure of a rigid analytic group variety. There is a p-adic analogue of the Riemann period relations, which determines when an analytic torus is a projective algebraic space. The requirement is that the period matrix defining the torus be symmetric and definite. As we will see below, this is true of $e(L)$. Thus, by the rigid analytic version of GAGA, the analytic group structure on J is an algebraic group structure, which makes J into an abelian variety. Now the group isomorphism λ and uniqueness of Jacobians imply that the abelian variety J is the Jacobian of the Mumford curve S. For more details, see [7].

We can also give an explicit description of the analytic, birational map ϕ_g between $S^{(g)}$ and the analytic torus $(k^*)^g/\Lambda = e(J)$. We start with the analytic mappings

$$\phi\colon \Omega \longrightarrow (k^*)^g\colon z \mapsto (u_1(z), \dots, u_g(z)),$$

and

$$\phi_g\colon \Omega^g \longrightarrow (k^*)^g\colon (z_1, \dots, z_g) \mapsto \phi(z_1) \cdot \phi(z_2) \cdots \phi(z_g).$$

Recall that $\Lambda = e(L)$, where L was the subgroup of the automorphy factors of the forms $u_\alpha(z)$. The value in k^* of c_{u_α} on $\beta \in \Gamma$ is given by the quotient

$$Q(\alpha, \beta) = \frac{u_\alpha(z)}{u_\alpha(\beta z)}.$$

Q is a symmetric, bimultiplicative form

$$\bar{\Gamma} \times \bar{\Gamma} \longrightarrow k^*,$$

where $\bar{\Gamma} = \Gamma/[\Gamma, \Gamma]$. With respect to the basis $\{\gamma_i\}$ of Γ, if $\alpha \equiv \prod_i \gamma_i^{n_i}$ and $\beta \equiv \prod_j \gamma_j^{m_j}$ mod $[\Gamma, \Gamma]$, then

$$\begin{aligned} Q(\alpha, \beta) &= \prod_i \left(\frac{u_i(z)}{u_i(\beta z)} \right)^{n_i} = \prod_i c_{u_i}(\beta)^{n_i} \\ &= \prod_i \left(\prod_j c_{u_i}(\gamma_j)^{m_j} \right)^{n_i} = \prod_{i,j} Q(\gamma_i, \gamma_j)^{m_j n_i}, \end{aligned}$$

so $\Lambda = e(L)$ is generated by the columns of the $n \times n$ period matrix $(q_{ij}) = (Q(\gamma_i, \gamma_j))$. The form Q is also positive definite, in the sense that

$$|Q(\alpha, \alpha)| < 1 \quad \text{for any } \alpha \not\equiv \text{id mod } [\Gamma, \Gamma].$$

Since the form Q is definite and symmetric, so is the period matrix (q_{ij}) of the Mumford curve S, which ensures that the Jacobian J_S is an abelian variety.

Now as $u_i(\alpha z) = u_i(z) \cdot c_{u_i}(\alpha) \equiv u_i(z)$ mod Λ, the maps ϕ and ϕ_g induce analytic mappings

$$S \longrightarrow (k^*)^g/\Lambda \quad \text{and} \quad S^g \longrightarrow (k^*)^g/\Lambda,$$

respectively. Moreover, the map ϕ_g is clearly invariant under the permutation group Σ on $\{1, \ldots, g\}$, so it induces an analytic mapping

$$\phi_g\colon\ S^{(g)} \longrightarrow (k^*)^n/\Lambda,$$

which is actually bianalytic outside a hypersurface, and birational. Thus, we obtain explicitly the embedding ϕ of the curve S into its Jacobian $e(J)$, the birational map ϕ_g between $e(J)$ and $S^{(g)}$, and the Abel–Jacobi group isomorphism $\lambda^{-1}\colon \mathrm{Pic}^0(S) \longrightarrow J$.

To complete the picture, we could define another map

$$\tilde{\phi_g}\colon\ S^{(g)} \longrightarrow J\colon\ (a_1, \ldots, a_g) \mapsto c_f,$$

where $f(z) = \prod_{i=1}^g \Theta(a_i, \infty; z)$. Here we assume that $\infty \in \Omega$, but if not, we can choose any other basepoint. div $f = \sum_{i=1}^g \bar{a}_i - g \cdot \bar{\infty}$, so $\lambda \circ \tilde{\phi_g}$ is the usual map

$$S^{(g)} \longrightarrow \mathrm{Pic}^0(S)\colon\ [a_1 + \cdots + a_g] \mapsto [(a_1) + \cdots + (a_g) - g(\infty)].$$

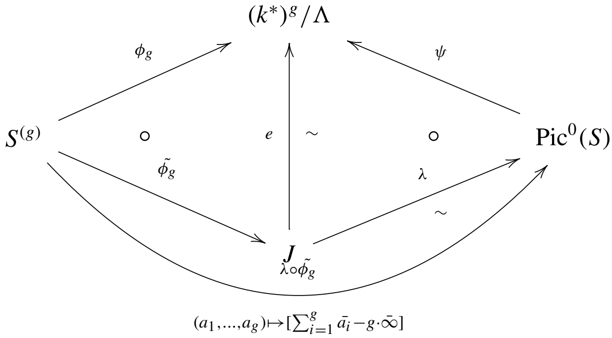
Moreover, we have $e \circ \tilde{\phi_g} = \phi_g$. To see this, note that $\forall i$, $u_i(\infty) = 1$. Since $c_{\Theta(a,b;z)}(\alpha) = \frac{u_\alpha(a)}{u_\alpha(b)}$, we see that $c_{\Theta(a,\infty;z)}(\alpha) = u_\alpha(a)$, and so for $f(z) = \prod_{i=1}^g \Theta(a_i, \infty; z)$, $c_f(\gamma_j) = \prod_{i=1}^g u_j(a_i)$. Thus, for $(a_1, \ldots, a_g) \in S^{(g)}$,

$$\begin{aligned} e(\tilde{\phi_g}(a_1, \ldots, a_g)) &= (c_f(\gamma_1), \ldots, c_f(\gamma_g)) = \left(\prod_{i=1}^g u_1(a_i), \ldots, \prod_{i=1}^g u_g(a_i) \right) \\ &= \phi(a_1) \cdot \phi(a_2) \cdots \phi(a_g) = \phi_g(a_1, \ldots, a_g). \end{aligned}$$

If, in addition, we define the map

$$\psi = e \circ \lambda^{-1}\colon \operatorname{Pic}^0(S) \longrightarrow (k^*)^g/\Lambda : \mathfrak{a} = \operatorname{div} f \mapsto (c_f(\gamma_1), \ldots, c_f(\gamma_g)),$$

then we obtain the following commutative diagram which summarizes this section:



5 Non-Archimedean Uniformization

5.1 Comparison with Complex Uniformization

The main difference between complex and p-adic uniformization of a curve C, from a practical point of view, is the step at which one must do the bulk of the work. In the complex case, the main difficulty lies in trying to explicitly represent the basis of $H_1(C, \mathbb{Z})$ in a way that computer can use to approximate line integrals. The resulting integrals, computed to a reasonably high precision, form the period lattice of the Jacobian of C. In the p-adic case, once a description of the Mumford curve Ω/Γ is obtained, the period lattice and all of the desired maps are explicitly given in terms of Θ, and one only needs to approximate this infinite product. Therefore, most of the work is centered around obtaining the generators for Γ so that Ω/Γ is isomorphic to C. (Note: this procedure is what we refer to as p-adic uniformization of a curve. In some special cases, it is possible to obtain the Jacobian using p-adic line integrals—see for example [2]. We do not analyze those methods here.)

This type of p-adic uniformization has a nice benefit. Since the analytic object we need to approximate is a curve, the complexity of the problem does not increase rapidly with the genus of C. As the genus grows, more generators of Γ need to be computed, but these are always 2×2 matrices acting on $\mathbb{P}^1$. In the complex case, the analytic object we are approximating is the Jacobian, which is defined by a $g \times 2g$ period matrix, generating a lattice in $\mathbb{C}^g$. Ignoring the obvious computational advantages of working in PGL_2, one must in general solve for $2g^2$ unknowns over $\mathbb{C}$, but p-adically only $3g$ unknowns (g matrices, projectively 3 coefficients each).

Moreover, let's consider the problem of detecting isogenies. In the complex case, uniformization produces the period matrices V and W, and the following system must be solved for $M \in M_g(\mathbb{C})$ and $A \in M_{2g}(\mathbb{Z})$:

$$MV = WA^T, \quad V, W \in M_{g,2g}(\mathbb{C}).$$

Using the real and imaginary parts separately, this system involves $4g^2$ equations in $5g^2$ unknowns. The complexity of the linear algebra involved grows significantly with the genus, since solving the system requires finding linear integral relations among a collection of complex numbers. On the p-adic side, after uniformization we are presented with the equation

$$V^B = {}^A W, \quad A, B \in M_g(\mathbb{Z}),\ V, W \in M_g(k).$$

As explained in Sect. 3.3, we can apply the ℓ homomorphism and invert $\ell(V)$, to obtain the equation $B = \ell(W)A^T\ell(V)^{-1}$ over $\mathbb{R}$, which determines B in terms of the coefficients of A. Thus, $V^B = {}^A W$ is a system of g^2 equations in g^2 unknowns, and can be solved rather quickly (for example, by considering the induced mod p^n equations).

Another, and perhaps the most important advantage of p-adic uniformization, is that the homomorphism $\ell(x) = -\log|x|$, which is used to solve for B, only depends on the valuation of x. For example, if $k = \mathbb{Q}_p$ and we are approximating the period lattice (q_{ij}) using p-expansions of the coefficients, then even a very poor approximation of q_{ij} (i.e. just getting the first term right) will produce the correct value of $\ell(q_{ij})$. This does not completely solve the problem, as we still have to determine the matrix A. However, it is clear that in a generic case, only few terms of q_{ij} are needed to solve for A, if it exists. Thus, in general, finding an isogeny or determining if it exists does not require a good approximation of the period lattices. This phenomenon does not have an analogy in the complex case, where poor approximations of the lattices simply result in incorrect answers.

To see a concrete example, let's consider the case of two Tate elliptic curves E_{q_1} and E_{q_2} over $\mathbb{Q}_p$. As the only maps $\mathbb{Q}_p^*/(q_1^{\mathbb{Z}}) \longrightarrow \mathbb{Q}_p^*/(q_2^{\mathbb{Z}})$ of the rigid tori are of the form $x \mapsto x^a$, $a \in \mathbb{Z}$, we see that E_{q_i} are isogenous (in fact over $\mathbb{Q}$) iff there exist $a, b \in \mathbb{Z}$ such that $q_1^a = q_2^b$. Let $a = na'$, $b = nb'$, where $n = \gcd(a, b)$, and let $v_i = \text{Valuation}(q_i)$, and $v_i' = v_i/(\gcd(v_1, v_2))$. Applying ℓ to the equation $q_1^a = q_2^b$ gives us $(a', b') = (v_2', v_1')$. So if an isogeny ϕ: $E_{q_1} \to E_{q_2}$ exists, then $q_1^{v_2'}/q_2^{v_1'}$ must be an nth root of unity, where $n|\deg\phi$. It is clear that in a generic case, only few terms of q_i are needed to determine n, if it exists, especially if deg ϕ is known. What is even better is that much information can be deduced without ever actually computing the uniformizations. Since

$$j(E_q) = \frac{1}{q} + 744 + 196884q + \cdots,$$

we see that $|j(E_q)|_p = 1/|q|_p$, so we can obtain v_i from the j invariants of the curves, without knowing the actual periods q_i. This allows us, for example, to make the following statement:

If a rational isogeny ϕ: $E_{q_1} \to E_{q_2}$ exists, then $v_1'|\deg\phi$,

which is a consequence of p-adic uniformization, but doesn't require any computations.

Having discussed some of the advantages of rigid uniformization, it is important to point out one significant drawback: the methods only apply to curves with totally split reduction. This technical condition means that the curve has a stable model whose special fiber is a union of projective lines, intersecting only at ordinary double points (see [4] or [7]). In contrast, all smooth curves can be studied through complex uniformization. This is an important difference, which limits the application of rigid uniformization to the problem of detecting isogenies. For example, in the case of elliptic curves, totally split reduction simply means "bad reduction" (i.e. $|j(E)|_p > 1$ if $E/\mathbb{Q}_p$). Given a curve $E/\mathbb{Q}$, one can always find a prime p of bad reduction, and find the uniformization for $E(\mathbb{Q}_p)$. However, to determine if there is an isogeny between a given pair of curves, one would need a common prime of bad reduction, and that is quite restrictive.

5.2 Examples Drawn from Genus 2 Hyperelliptic Curves

To obtain concrete examples, we chose the field $\mathbb{Q}_5$ and generated six "random" (with totally split reduction) genus 2 hyperelliptic curves X_i. Each curve is defined by three ramification points, with the choice of $0, 1, \infty$ for the remaining three. All computations were done in Magma, which conveniently outputs $x \in \mathbb{Q}_5$ in the form $x = (\ldots) \cdot 5^v$, where v is the valuation of x.

For each hyperelliptic curve X_i, we compute the Mumford curve S_i with affine model X_i. The Mumford curves are described by the pair of matrices generating their Schottky group Γ. Finally, for each Mumford curve we compute its period matrix P_i, and its image under the $\ell/\log 5$ homomorphism. Since we are primarily interested in the isogeny problem, only few digits of precision are required, and to avoid unnecessary clutter, we give only the first six.

The hyperelliptic curves:

$$\mathbf{X}_1\colon\ y^2 = x^5 - 326x^4 + 1052 \cdot 5^2x^3 - 5914 \cdot 5^2x^2 + 39 \cdot 5^5x,$$

$$\mathbf{X}_2\colon\ y^2 = x^5 - 1126x^4 + 14519 \cdot 5^2x^3 - 1395074 \cdot 5^2x^2 + 55224 \cdot 5^4x,$$

$$\mathbf{X}_3\colon\ y^2 = x^5 - 34876x^4 + 69609 \cdot 5^3x^3 - 567866 \cdot 5^4x^2 + 4432 \cdot 5^7x,$$

$$\mathbf{X}_4\colon\ y^2 = x^5 - 11250626x^4 - 163599 \cdot 5^4x^3 + 9966639 \cdot 5^6x^2 + 8342073 \cdot 5^{16}x,$$

$$\mathbf{X}_5\colon\ y^2 = x^5 + 1624999x^4 + 4424271 \cdot 5^6x^3 + 18836006 \cdot 5^{10}x^2 - 13455749 \cdot 5^{22}x,$$

$$\mathbf{X}_6\colon\ y^2 = x^5 - 209060401x^4 + 18131925775313 \cdot 5^4x^3 \\ -7291674407447953921259 \cdot 5^2x^2 + 291666958165992716034 \cdot 5^4x.$$

The Mumford curves:

$$S_1\colon\ g_1 = \begin{pmatrix} -375001 * 5 & 938432 * 5 \\ 2 & 78116 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 928593 * 5^3 & 95939 * 5^3 \\ 2 & 839746 \end{pmatrix},$$

$$S_2\colon\ g_1 = \begin{pmatrix} -481331 * 5 & -322158 * 5 \\ 2 & -453534 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} -480457 * 5^2 & 960914 * 5^2 \\ 2 & -292679 \end{pmatrix},$$

$$S_3\colon\ g_1 = \begin{pmatrix} 548603 * 5^2 & 338894 * 5^2 \\ 2 & 43196 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 232706 * 5^3 & -465412 * 5^3 \\ 2 & -208629 \end{pmatrix},$$

$$S_4\colon\ g_1 = \begin{pmatrix} 968583 * 5^3 & -652916 * 5^3 \\ 2 & -20879 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} -84456 * 5^{10} & 168912 * 5^{10} \\ 2 & -4 \end{pmatrix},$$

$$S_5\colon\ g_1 = \begin{pmatrix} -543576 * 5^5 & -378473 * 5^5 \\ 2 & 543746 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} -599148 * 5^{12} & -754829 * 5^{12} \\ 2 & -4 \end{pmatrix},$$

$$S_6\colon\ g_1 = \begin{pmatrix} 704404 * 5 & -754828 * 5 \\ 2 & -384234 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 423453 * 5^2 & -846906 * 5^2 \\ 2 & 820696 \end{pmatrix}.$$

The period matrices:

$$P_1 : \begin{pmatrix} -661001 * 5^2 & -486614 * 5^2 \\ -486614 * 5^2 & 46676 * 5^6 \end{pmatrix}, \qquad P_2 : \begin{pmatrix} 13734 * 5^2 & 23926 * 5^2 \\ 23926 * 5^2 & 69326 * 5^4 \end{pmatrix},$$

$$P_3 : \begin{pmatrix} 193531 * 5^4 & 913819 * 5^4 \\ 913819 * 5^4 & -895176 * 5^6 \end{pmatrix}, \qquad P_4 : \begin{pmatrix} -294049 * 5^6 & -132671 * 5^6 \\ -132671 * 5^6 & -238496 * 5^{20} \end{pmatrix},$$

$$P_5 : \begin{pmatrix} 809529 * 5^{10} & 85486 * 5^{10} \\ 85486 * 5^{10} & -119224 * 5^{24} \end{pmatrix}, \qquad P_6 : \begin{pmatrix} 41994 * 5^2 & 56706 * 5^2 \\ 56706 * 5^2 & 29006 * 5^4 \end{pmatrix}.$$

The homomorphism $\ell/\log 5$ simply produces the matrix of valuations, so for example

$$\frac{\ell}{\log 5}(P_1) = \begin{pmatrix} 2 & 2 \\ 2 & 6 \end{pmatrix} \quad \text{and} \quad \frac{\ell}{\log 5}(P_5) = \begin{pmatrix} 10 & 10 \\ 10 & 24 \end{pmatrix}.$$

To check for possible isogenies, we first took each period matrix, and considered only the leading term in the p-expansion of each coefficient. This was enough to conclude that none of the curves could be isogenous, except possibly for X_2 and X_6, where we obtained two pairs of matrices

$$(B, A) \in \left\{ \left(\begin{pmatrix} 3 & 1 \\ 8 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 3 & 1 \end{pmatrix} \right), \left(\begin{pmatrix} 5 & 0 \\ 10 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix} \right) \right\},$$

satisfying $P_2^B = {}^A P_6$. This equation continues to hold as we allow more terms in the p-expansion of the coefficients in P_2 and P_6, suggesting that the pairs (B, A) define actual isogenies (which is true, since we chose $X_6/\mathbb{Q}_5$ to be isogenous to X_2). Technically speaking, one could never obtain a definite, positive answer using this method, since the results only hold up to the precision under consideration. However, if A and B satisfy the equation $P_2^B = {}^A P_6$ to a reasonably good precision, there is a high probability that the curves are isogenous. If one wanted to know for sure, one could try to use the matrices A and B to construct the actual map. This was successfully done in the complex case in [10].

Acknowledgements The author is grateful to Iwan Duursma for invaluable comments and suggestions.

References

1. Bosch, S., Güntzer, U., Remmert, R.: Non-Archimedean Analysis. Springer, Berlin (1984)
2. Darmon, H.: Rational Points on Modular Elliptic Curves. CBMS, vol. 101. Published for the Conference Board of the Mathematical Sciences, Washington (2004)
3. Diamond, F., Shurman, J.: A First Course in Modular Forms. Springer, New York (2005)
4. Fresnel, J., van der Put, M.: Analytic Geometry and Its Applications. Birkhäuser, Boston (2004)
5. Gerritzen, L.: Über Endomorphismen nichtarchimedischer holomorpher Tori. Invent. Math. **11**, 27–36 (1970)
6. Gerritzen, L.: On non-Archimedean representations of abelian varieties. Math. Ann. **169**, 323–346 (1972)
7. Gerritzen, L., van der Put, M.: Schottky Groups and Mumford Curves. Springer, Berlin (1980)
8. Serre, J.-P.: Abelian l-Adic Representations and Elliptic Curves. AK Peters, Wellesley (1998)
9. Tate, J.: Rigid analytic spaces. Invent. Math. **12**, 257–289 (1971)
10. van Wamelen, P.: Poonen's question concerning isogenies between smart's genus 2 curves. Math. Comput. **69**(232), 1685–1697 (2000)