Werk

Titel: On the p-adic periods of X...(p).

Autor: Shalit, Ehud de

Jahr: 1995

PURL: https://resolver.sub.uni-goettingen.de/purl?235181684_0303|log44

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Math. Ann. 303, 457–472 (1995)

Mathematische Annalen
© Springer-Verlag 1995

On the p-adic periods of $X_0(p)$

Ehud de Shalit

Department of Mathematics, Hebrew University, Givat-Ram, Jerusalem 91904, Israel
(e-mail: deshalit@math.huji.ac.il)

Received: 10 May 1994 / Revised version: 27 October 1994

Introduction

In this paper we derive a formula, conjectured by J. Oesterlé, which relates the p-adic periods of the modular curve $X_0(p)$ to the j-invariants of supersingular elliptic curves in characteristic p.

0.1 P-adic uniformization of $X_0(p)$

Let $p \geqq 5$ be a prime, and let $X_0(p)/\mathbb{Q}$ be the modular curve parametrizing pairs (E, H) consisting of a (generalized) elliptic curve E, with a cyclic subgroup H of order p. Its genus g is given by the formula

$$g+1 = \begin{cases} (p-1)/12 & p \equiv 1 \bmod 12 \\ (p+7)/12 & p \equiv 5 \bmod 12 \\ (p+5)/12 & p \equiv 7 \bmod 12 \\ (p+13)/12 & p \equiv 11 \bmod 12\,. \end{cases} \tag{1}$$

Recall that $g+1$ is also the number of supersingular elliptic curves in characteristic p.

Over $\mathbb{C}$, let us map a point z in the upper half plane to the isomorphism class of the pair $(\mathbb{C}/(\mathbb{Z}z+\mathbb{Z}), \langle 1/p \bmod \mathbb{Z}z+\mathbb{Z}\rangle)$. This gives the well-known complex uniformization by the upper half plane (with the cusps) $X_0(p)(\mathbb{C}) \approx \Gamma_0(p)\backslash\mathfrak{h}^*$. Denote by ξ_∞ and ξ_0 the *cusps* of $X_0(p)$, corresponding under this uniformization to $i\infty$ and 0 respectively. Both cusps are points rational over $\mathbb{Q}$.

The curve $X_0(p)$ admits a p-adic uniformization by the theory of Mumford curves ([Mu], [Ge-vdP]). Consider the semi-stable model $\mathfrak{X}'/\mathbb{Z}_p$ of $X_0(p)/\mathbb{Q}_p$ which was constructed by Deligne and Rapoport [De-Ra]. Its special fiber has

two irreducible components, each isomorphic to $\mathbb{P}^1/\mathbb{F}_p$, which may be distinguished by the cusps. We call the component to which ξ_∞ specializes the ∞-component, and the one to which ξ_0 specializes the 0-component. (The ordinary points on the ∞-component parametrize elliptic curves in characteristic p, together with a subgroup scheme of order p of *multiplicative* type. The ordinary points on the 0-component parametrize elliptic curves, together with an *étale* subgroup of order p.) The two components intersect transversally at $g+1$ points, corresponding to the $g+1$ supersingular elliptic curves $e_0, e_1, \ldots, e_g$ in characteristic p. We denote by Δ' the dual graph of the special fiber of $\mathfrak{X}'$. It has two vertices, corresponding to the two components, and $g+1$ edges connecting them. Once and for all we *orient* the edges, so that they point from the ∞-vertex to the 0-vertex.

Now let $\delta_i = (1/2)\#\mathrm{Aut}(e_i)$. If $j(e_i) = 0$ (which happens if and only if $p \equiv 5, 11 \bmod 12$), $\delta_i = 3$. If $j(e_i) = 1728$ (which happens if and only if $p \equiv 7, 11 \bmod 12$), $\delta_i = 2$. Otherwise, $\delta_i = 1$. Let $\mathfrak{X}$ be the *regular* model obtained from $\mathfrak{X}'$ by blowing up those points e_i on the special fiber where $\delta_i > 1$, and replacing them by a chain of $\delta_i - 1$ $\mathbb{P}^1$'s. The dual graph Δ of its special fiber is obtained from Δ' by subdividing the edge corresponding to e_i into δ_i edges. In particular, $\tilde{\Gamma} = \pi_1(\Delta, 0\text{-vertex})$ is canonically identified with $\pi_1(\Delta', 0\text{-vertex})$. It is a free group of rank g. Let $S = \{e_0, \ldots e_g\}$ be the set of supersingular elliptic curves in characteristic p, and $\mathbb{Z}[S]_0$ the augmentation subgroup in the free abelian group $\mathbb{Z}[S]$. With our choice of orientation described above, we obtain a *canonical* identification

$$H_1(\Delta, \mathbb{Z}) = \tilde{\Gamma}^{ab} = \mathbb{Z}[S]_0 \,. \tag{2}$$

The group $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ acts on Δ. If we denote by e' the elliptic curve whose j-invariant is $j(e') = j(e)^p$, then the Galois action preserves the two vertices, but interchanges the edges corresponding to e_i and e_i'.

Let K be the quadratic unramified extension of $\mathbb{Q}_p$. According to a fundamental theorem of Mumford [Mu], there exists a discrete subgroup Γ in $PGL_2(K)$, unique up to conjugation, and a map of rigid analytic spaces defined over K

$$\tau : \mathfrak{H}_\Gamma \to \mathfrak{X}^{an} \tag{3}$$

inducing an isomorphism $\Gamma\backslash\mathfrak{H}_\Gamma \approx \mathfrak{X}^{an}$. Here $\mathfrak{H}_\Gamma$ is the complement, in $\mathbb{P}^1$, of the limit set of Γ, and $\mathfrak{X}^{an}$ is the rigid analytic space associated with the formal completion of $\mathfrak{X}$ along its special fiber. In particular, for any finite extension $L \supseteq K$, we obtain a Galois-equivariant map $\mathfrak{H}_\Gamma(L) \to X_0(p)(L)$, which we also denote by τ.

The dual graph of the special fiber of (the formal scheme underlying) $\mathfrak{H}_\Gamma$ is a tree $\mathcal{T}_\Gamma$. It is just the subtree of the Bruhat–Tits tree of $PGL_2(K)$ spanned by the axes of all the nontrivial elements in Γ. The group Γ acts on it, and (3) induces, upon reduction mod p, an isomorphism

$$\Gamma\backslash\mathcal{T}_\Gamma \approx \Delta \,. \tag{3}_\Gamma$$

Once we fix a base point in $\mathscr{T}_\Gamma$ above the 0-vertex, we obtain an isomorphism of fundamental groups $\Gamma \approx \tilde{\Gamma}$. A different base point changes this isomorphism by an inner automorphism, so the abelianizations of Γ and $\tilde{\Gamma}$ are *canonically* identified, and in view of (2) we identify Γ^{ab} too with $\mathbf{Z}[S]_0$.

We shall make use of the involution w_p, induced over $\mathbf{C}$ by the map $z \to -1/pz$. It is defined over $\mathbf{Q}$, and maps ξ_∞ to ξ_0. It extends to $\mathfrak{X}$, and its effect on the special fiber of $\mathfrak{X}$ is to interchange the two components, and also e_i with e_i'. As a result, w_p defines an orientation-reversing involution on Δ. From [Ge-vdP] ch. VII Sect. 1 it follows that there exists a unique class in $N(\Gamma)/\Gamma$ ($N(\Gamma)$ is the normalizer of Γ in $PGL_2(K)$) inducing w_p via the map τ (3).

0.2 P-adic uniformization of $J_0(p)$

We shall review the results of Manin–Drinfel'd [M-D] in the context of the curve $X_0(p)$. Let $J = \mathrm{Pic}^0(X_0(p))$ be its Jacobian. For a, b in $\mathfrak{H}_\Gamma$, let

$$\Theta((a)-(b);z) = \Theta(a,b;z) = \prod_{\gamma\in\Gamma}\{(z-\gamma a)/(z-\gamma b)\}\,. \tag{4}$$

The product converges and describes a (rigid) meromorphic function in $\mathfrak{H}_\Gamma$. If Γ is replaced by $\alpha\Gamma\alpha^{-1}$ for some $\alpha \in PGL_2(K)$, then

$$\Theta_{\alpha\Gamma\alpha^{-1}}((\alpha a)-(\alpha b);\alpha z) = (\text{a constant})\cdot\Theta_\Gamma((a)-(b);z)$$

where the constant depends on Γ, a, b and α. Extend (4) by linearity to divisors $\mathbf{d}$ of degree 0 on $\mathfrak{H}_\Gamma$ (this being clearly possible), and denote the resulting function by $\Theta(\mathbf{d};z)$. It is entire (with entire inverse) precisely when $\tau_*(\mathbf{d}) = 0$.

Properties. (a) $\Theta(a,b;z) = c(a,b;\alpha)\cdot\Theta(a,b;\alpha z)$, and $c(a,b;\alpha\beta) = c(a,b;\alpha)c(a,b;\beta)(\alpha,\beta\in\Gamma)$ (Similarly, the factor of automorphy of $\Theta(\mathbf{d};z)$ will be written $c(\mathbf{d};-)$),

(b) $\Theta(a,b;z) = \Theta(\alpha a,\alpha b;z)\forall\alpha\in\Gamma$,

(c) $u_\alpha(z) = \Theta(a,\alpha a;z)$ is independent of a, and $u_{\alpha\beta} = u_\alpha u_\beta\forall\alpha,\beta\in\Gamma$,

(d) $c(a,b;\alpha) = u_\alpha(a)/u_\alpha(b)$,

(e) $\Theta(a,b;z)/\Theta(a,b;z') = \Theta(z,z';a)/\Theta(z,z';b)$.

Now let

$$Q(\alpha,\beta) = \Theta(a,\alpha a;z)/\Theta(a,\alpha a;\beta z)\,. \tag{5}$$

In view of the above, $Q(\alpha,\beta)$ is well defined, independent of a or z, and Q is a *bilinear symmetric* pairing from $\Gamma\times\Gamma$ to $K^\times$. It therefore factors through Γ^{ab}, so (2) (and the remark made above) allows us to view it as a pairing on $\mathbf{Z}[S]_0$. As such, it is also independent of the group Γ (unlike the functions u_α, which are multiplied by a constant if we conjugate Γ). Manin and Drinfel'd prove that $v_K\circ Q$ (where v_K is the valuation on K) is positive definite on $\mathbf{Z}[S]_0$. In particular Q is nondegenerate, and we obtain an embedding

$$q : \mathbf{Z}[S]_0 \subseteq \mathrm{Hom}(\mathbf{Z}[S]_0, K^\times),\quad q(\alpha) = Q(\alpha,-)\,. \tag{6}$$

Let J^{an} be the rigid analytic space whose points in any finite K-algebra L are $J^{an}(L) = \mathrm{Hom}(\mathbf{Z}[S]_0, L^\times)/q(\mathbf{Z}[S]_0)$. There exists a unique $\mathbf{Z}$-linear map $\phi : \mathrm{Div}^0(\mathfrak{H}_\Gamma) \to J^{an}$, which assigns to the divisor (a)–(b) the class of the homomorphism $\beta \mapsto c(a,b;\beta)$. If $b = \alpha a$, this is the homomorphism $q(\alpha)$, and its class is trivial. The map ϕ therefore factors through $\mathrm{Div}^0(\Gamma\backslash\mathfrak{H}_\Gamma)$. The main result of [M-D] is that ϕ is surjective, and its kernel consists precisely of the principal divisors. This way we obtain an isomorphism

$$\mathrm{Pic}^0(\Gamma\backslash\mathfrak{H}_\Gamma) \approx J^{an} . \tag{7}$$

0.3 A slightly different, but equivalent formulation, is that of Raynaud. Although we shall not use it, we give here the dictionary between the two. Let $\mathbf{d}$ be a divisor of degree 0 on $\mathfrak{H}_\Gamma$, defined over some finite extension L of K, and let $\mathscr{L}$ be a line bundle on $X_0(p)/L$ having a meromorphic section s whose divisor is $\tau_*(\mathbf{d})$. This $\mathscr{L}$ can be constructed as follows, using the analytic uniformization. Let Γ act on $\mathfrak{H}_\Gamma \times \mathbf{C}_p$ by $\gamma \cdot (z,u) = (\gamma(z), c(\mathbf{d};\gamma)^{-1}u)$. Then $\mathscr{L} = \Gamma\backslash(\mathfrak{H}_\Gamma \times \mathbf{C}_p)$, and the function $\Theta(\mathbf{d};z)$ defines the section s.

Let us write $\mathscr{L}_c$ for this $\mathscr{L}$, where $c = c(\mathbf{d};-)$. The kernel of the map $\mathrm{Hom}(\Gamma, L^\times) \to J(L)$, $c \mapsto \mathscr{L}_c$, is $q(\Gamma)$. Recall that the connected component of the special fiber of the Néron model of J, classifies line bundles which are of degree 0 on each component of the special fiber of $\mathfrak{X}$. If c belongs to $\mathrm{Hom}(\Gamma, U(L))$ (here $U(L)$ are the units of L), then $\mathscr{L}_c$ extends to the special fiber of $\mathfrak{X}$, and furthermore defines a point λ_c in the connected component of the special fiber of J. This connected component is a torus T. According to Raynaud we get in this way an isomorphism $\mathrm{Hom}(\Gamma, \ell^\times) \approx T(\ell)$, where ℓ is the residue field of L. Dualizing, we get an isomorphism of the character groups

$$X(T) \approx \Gamma^{ab} = \mathbf{Z}[S]_0 . \tag{8}$$

Now every line bundle λ on the special fiber of $\mathfrak{X}$, which is of degree 0 on each component, may be described in the following manner. Choose trivializations on the two components, and let s be a section of λ. Then on each component s becomes a *function*, and we write s_0 and s_∞ for these two functions. Put $\lambda(e_i) = s_\infty(e_i)/s_0(e_i)$. Then $(\lambda(e_0), \ldots \lambda(e_g))$ is determined up to a scalar multiple. Unwinding the definitions one gets that (8) associates with $e_i - e_0 \in \mathbf{Z}[S]_0$ the character $\lambda \mapsto \lambda(e_i)/\lambda(e_0)$.

0.4 Lemma. *The pairing Q takes values in $\mathbf{Q}_p^\times$.*

Proof. Since the curve $X_0(p)$ is defined over $\mathbf{Q}_p$, $\mathrm{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p) = \mathrm{Gal}(K/\mathbf{Q}_p)$ acts on $\mathbf{Z}[S]_0$ and the pairing Q is Galois-equivariant. However, the involution w_p also acts on $\mathbf{Z}[S]_0$, and (see [Ge-vdP], ch. VII, Sect. 3) Q is invariant under its action. Letting σ be the non-trivial element of the Galois group, and putting the two together we get

$$\begin{aligned}\sigma Q(e_i - e_0, e_j - e_0) &= Q(e_i' - e_0', e_j' - e_0') = Q(e_0' - e_i', e_0' - e_j') \\ &= Q(w_p(e_i - e_0), w_p(e_j - e_0)) = Q(e_i - e_0, e_j - e_0) .\end{aligned}$$

□

0.5 Let $U_1(L) = \{u \in L^\times \,|\, |u-1| < 1\}$ be the group of principal units. Let

$$\bar{Q} : \Gamma \times \Gamma \to \mathbb{Q}_p^\times / U_1(\mathbb{Q}_p) \tag{9}$$

be the map induced from Q in passing to the quotient. Observe that elements of $\mathbb{Q}_p^\times/U_1(\mathbb{Q}_p)$ have a well-defined valuation, which we denote by ord, normalized so that $\mathrm{ord}(p) = 1$, and that the subgroup of valuation 0 is identified with $\mathbb{F}_p^\times$. In 1985, J. Oesterlé made the following conjecture.

Conjecture. Let $\mathbb{Z}[S]^* = \sum \delta_i^{-1}\mathbb{Z}e_i \subseteq \mathbb{Q}[S]$. Define a $\mathbb{Q}_p^\times/U_1(\mathbb{Q}_p)$-valued pairing on $\mathbb{Z}[S] \times \mathbb{Z}[S]^*$ by the following formulae:

$$\langle e_i, \delta_j^{-1} e_j\rangle = (j(e_i) - j(e_j))^{(p+1)/\delta_j} \quad \text{if } i \neq j \tag{10}$$

$$\langle e_i, \delta_i^{-1} e_i\rangle = (-1)^{(p-1)/2} p \cdot \prod_{k \neq i} (j(e_i) - j(e_k))^{-(p+1)/\delta_k} . \tag{11}$$

Then this pairing coincides with $\bar{Q}$ on $\mathbb{Z}[S]_0 \times \mathbb{Z}[S]_0$.

In this paper we *prove* this conjecture when $p \equiv 1 \bmod 4$. When $p \equiv 3 \bmod 4$ we prove it up to a $\pm$ sign in (11) (see theorem 1.6 for the precise statement). It has been previously tested numerically in many cases (by J. Oesterlé and J.-P. Mestre). The evaluation of Q up to units is easy, and follows from the general theory.

Remarks. (i) δ_j (in fact $2\delta_j$) divides $p+1$, and one can show that $\langle \cdot, \cdot \rangle$, although a-priori $K^\times/U_1(K)$ valued, takes values in $\mathbb{Q}_p^\times/U_1(\mathbb{Q}_p)$.

(ii) if we denote by $\mathscr{J}_0(p)$ the special fiber of the Néron model of $J_0(p)$ over the ring of integers of K, We have a canonical isomorphism

$$\mathscr{J}_0(p)(\mathbb{F}_{p^2}) \approx \mathrm{Hom}(\Gamma, K^\times/U_1)/\Gamma^{ab} ,$$

and the group of connected components of $\mathscr{J}_0(p)$ is identified with $\mathrm{Hom}(\Gamma, K^\times/U)/\Gamma^{ab}$. Thus knowing $\bar{Q}$ amounts to knowing $\mathscr{J}_0(p)$, and knowing Q only up to units, amounts to knowing the group of connected components.

1 An extension of the pairing Q

1.1 Let us begin with some general remarks on the two pairings which we want to prove are equal. Let $\langle \cdot, \cdot \rangle$ be the pairing defined in Sect. 0 (10) and (11). The restriction of $\langle \cdot, \cdot \rangle$ to $\mathbb{Z}[S]_0 \times \mathbb{Z}[S]_0$ is expressed in terms of cross-ratios of j-invariants, and is therefore associated *intrinsically* to the geometry of $X_0(p)$, and does not depend on the choice of the function j, used to identify the moduli space of elliptic curves with $\mathbb{P}^1$. The restriction of $\langle \cdot, \cdot \rangle$ to $\mathbb{Z}[S]_0 \times \mathbb{Z}[S]^*$ already depends on the choice of j, but only up to the transformation $j \mapsto aj + b$. In other words, it depends on the choice of $j = \infty$ as a cusp. Indeed, we shall see below that it is related to the *generalized* jacobian of $X_0(p)$, with respect to the cuspidal modulus. Finally, on the full group $\mathbb{Z}[S] \times \mathbb{Z}[S]^*$, the pairing $\langle \cdot, \cdot \rangle$ depends on the choice of j up to $j \mapsto$

$j+b$. We may express this by saying that it depends on the choice of ∞ as a cusp and *also* on a choice of a tangent vector at ∞.

If we expect to extend Q (defined by Sect. 1(5)) from $\mathbb{Z}[S]_0 \times \mathbb{Z}[S]_0$ to $\mathbb{Z}[S] \times \mathbb{Z}[S]$ (at least), so that $\bar{Q}$ will be computed by $\langle \cdot, \cdot \rangle$, this extension ought to exhibit the same dependencies, and some of the symmetry in the original definition of Q must be sacrificed. To facilitate the computations, we impose a certain *normalization* condition on Γ, resulting in a particularly nice fundamental domain for its action on $\mathfrak{H}_\Gamma$.

Our reference for rigid analytic geometry in $\mathbb{P}^1$ is [Ge-vdP]. We call a disk in $\mathbb{P}^1$ *open* if it is defined by a strict inequality, and *closed* otherwise. We call it *K-rational* if its center can be chosen to be in K, and its radius is in $|K^\times|$. Similar terminology applies to annuli.

1.2 Since Γ is a free group, every nontrivial element in it is hyperbolic. If $\alpha \in \Gamma$, $\alpha \neq 1$, denote by z_α^+ (resp. z_α^-) the attractive (resp. repulsive) fixed point of α. A system $\{\alpha_1, \ldots, \alpha_g\}$ of free generators of Γ is called a *Schottky basis* if for each $1 \leqq i \leqq g$ there exists a (half-open, half-closed) annulus in $\mathbb{P}^1$, which is a fundamental domain for the cyclic group generated by α_i, and which contains all the $z_j^\pm$ for $j \neq i$ (here $z_j^\pm = z_{\alpha_j}^\pm$). A Schottky basis always exists.

Let v_0 and v_∞ be the two vertices of Δ', considered also as vertices of Δ. Recall that the tree $\mathscr{T}_\Gamma$ is the universal covering of Δ (via $(3)_r$) and denote by $r : \mathfrak{H}_\Gamma \to \mathscr{T}_\Gamma$ the reduction map. Thus if $\tilde{v}$ is a vertex of $\mathscr{T}_\Gamma$ which maps modulo Γ to v_0 or v_∞, $r^{-1}(\tilde{v})$ is an affinoid subdomain of $\mathfrak{H}_\Gamma$, isomorphic to the projective line with $g+1$ residue disks deleted. If $\tilde{v}$ is any other vertex of $\mathscr{T}_\Gamma$, it maps modulo Γ to a vertex of Δ which is not in Δ', and $r^{-1}(\tilde{v})$ is then an affinoid annulus. In any case, $r^{-1}(\tilde{v})$ is an affinoid with good reduction. For any edge $\tilde{e}$ of $\mathscr{T}_\Gamma$, $r^{-1}(\tilde{e})$ is an open annulus, conformal to $\{z \mid |p| < |z| < 1\}$.

Now let F be a *connected* fundamental domain for the action of Γ on $\mathscr{T}_\Gamma$. We choose F to have the following shape: F consists of two vertices $\tilde{v}_0$ and $\tilde{v}_\infty$, mapping modulo Γ to v_0 and v_∞ respectively; of a segment $\tilde{e}_0$ consisting of δ_0 edges and $\delta_0 - 1$ vertices, connecting $\tilde{v}_\infty$ to $\tilde{v}_0$, which reduces in Δ' to the edge labelled by e_0 (subdivided into δ_0 edges in Δ); and of g "open" segments $\tilde{e}_i$ emanating from $\tilde{v}_\infty$, the i-th of which reduces in Δ' to the edge labelled by e_i, and consists of δ_i edges and $\delta_i - 1$ vertices ($1 \leqq i \leqq g$).

Clearly $D := r^{-1}(F)$ is a fundamental domain for Γ in $\mathfrak{H}_\Gamma$. Let $A = r^{-1}(\tilde{v}_0)$ and $A' = r^{-1}(\tilde{v}_\infty)$. It follows that

$$\mathbb{P}^1 - A = \bigcup_{0 \leqq i \leqq g} B_i \quad \text{and} \quad \mathbb{P}^1 - A' = \bigcup_{0 \leqq i \leqq g} C_i'$$

where the B_i and C_i' are open disks. Each of the B_i (resp. C_i') determines an edge in $\mathscr{T}_\Gamma$ attached to $\tilde{v}_0$ (resp. $\tilde{v}_\infty$). We index them in such a way that the edge determined by B_i (resp. C_i') is mapped modulo Γ to e_i. Then $A' \subseteq B_0$ and $A \subseteq C_0'$. Furthermore, letting

$$W = r^{-1}\left(\bigcup_{0 \leqq i \leqq g} \tilde{e}_i \cup \{\tilde{v}_\infty\}\right)$$

we see that $\mathbb{P}^1 - W = \bigcup_{0 \leqq i \leqq g} C_i$ where C_i are closed disks, $C_0 = \mathbb{P}^1 - B_0$, and $C_i \subseteq C_i'$. It follows that $W \subseteq B_0$ and

$$D = A \cup W = \mathbb{P}^1 - \bigcup_{1 \leqq i \leqq g} (B_i \cup C_i) .$$

Now put $c_i = C_i' - C_i$ $(1 \leqq i \leqq g)$ and $a = c_0 = C_0' - C_0$. These are open annuli. In the regular model $\mathfrak{X}$ discussed in the introduction, A reduces to the 0-component, A' to the ∞-component, $a = c_0$ to e_0, and c_i to e_i (see Fig. 1).

Lemma (normalization of Γ and its fundamental domain). *There exists a choice of Γ, a choice of a Schottky basis $\alpha_1, \ldots \alpha_g$ for Γ, and a choice of a fundamental domain as above, such that the following conditions hold (no attempt is made to give a minimal set of conditions from which the rest follow, and one should also note that a small perturbation of Γ, or of the α_i, once Γ is fixed, will not affect any of the conclusions below).*

(i) *B_i is the (open) residue disk in the unit disk of $\mathbb{P}^1$ which reduces to $j(e_i), \forall\, 0 \leqq i \leqq g$.*

(ii) *For $1 \leqq i \leqq g$, α_i corresponds, under the identification $\Gamma^{ab} = \mathbb{Z}[S]_0$, to $e_i - e_0$.*

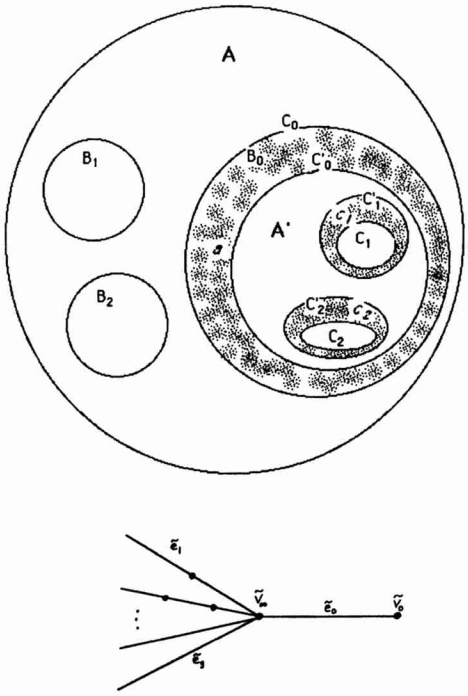

Fig. 1

(iii) α_i *maps* $\mathbb{P}^1 - B_i$ *isomorphically onto* C_i. *The fixed points* z_i^+ *and* z_i^- *lie in* C_i *and* B_i *respectively.*
(iv) *The annuli* c_i *are isomorphic, as rigid analytic spaces, to* $A(p^{\delta_i}, 1) = \{z \,|\, |p^{\delta_i}| < |z| < 1\}$.

Proof (sketch). For a given choice of Γ we choose fundamental domains F (in the tree) and D (in $\mathfrak{H}_\Gamma$) as above. Conjugating Γ in $PGL_2(K)$ we can satisfy condition (i), because the reduction of the affinoid A is *isomorphic* to $\mathbb{P}^1 -$ {the supersingular points}.

Finally, choose α_i in Γ satisfying (ii). Then (iii) holds too. The proof that the α_i generate Γ follows the proof of the existence of a Schottky basis. One only has to note that Γ and its subgroup generated by the α_i have the same fundamental domain. □

From now on fix Γ and the notation as in the lemma, and let

$$\tau : \mathfrak{H}_\Gamma \to X_0(p) \tag{1}$$

be the uniformization map. Let j and j' be the two functions on $X_0(p)/\mathbb{Q}$ given on the pair (E, H) by $j(E, H) = j(E)$, and $j'(E, H) = j(E/H)$. They generate the function field of $X_0(p)/\mathbb{Q}$, and are related via Kronecker's modular equation. The involution w_p interchanges them: $j \circ w_p = j'$.

1.3 Extension of Q *to* $\mathbb{Z}[S]_0 \times \mathbb{Z}[S]$

Choose ($\forall 0 \leqq i \leqq g$) points $z_0^{(i)}$ and $z_\infty^{(i)}$ in $\tau^{-1}(\xi_0)$ and $\tau^{-1}(\xi_\infty)$ respectively, belonging to two affinoids with good reduction, which are separated (in the rigid analytic topology) only by an open annulus reducing to e_i. Thus $\tau^{-1}(\xi_0)$ and $\tau^{-1}(\xi_\infty)$ are contained in $r^{-1}(\tilde{v})$ and $r^{-1}(\tilde{w})$ respectively, where $\tilde{v}$ and $\tilde{w}$ are vertices of $\mathcal{T}_\Gamma$ mapping in Δ to v_0 and v_∞, and which are connected by a segment consisting of δ_i edges, which maps, modulo Γ, to $e_i \subseteq \Delta$. Explicitly, we may choose $z_0^{(i)} = z_0 \in A$ (for all i), $z_\infty^{(0)} \in A'$, and $z_\infty^{(i)} = \alpha_i^{-1}(z_\infty^{(0)}) \in B_i$ for $1 \leqq i \leqq g$. Any other choice of $(z_0^{(i)}, z_\infty^{(i)})$ is obtained by applying some $\beta \in \Gamma$ to the pair described here. Note also that perturbing Γ a little if necessary, we may assume that in this specific choice $z_0 \neq \infty$ (all the other points are obviously finite), without affecting the validity of lemma 1.2. Define

$$Q(\alpha, e_i) = \Theta(a, \alpha a; z_\infty^{(i)})/\Theta(a, \alpha a; z_0^{(i)}) \in K^\times . \tag{2}$$

This is independent of a, and of the pair $(z_\infty^{(i)}, z_0^{(i)})$ (by the properties listed in Sect. 0.2). It is linear in α, and we extend it linearly in the second variable, to a pairing on $\mathbb{Z}[S]_0 \times \mathbb{Z}[S]$. As in Sect. 0.4, one can show that (2) is $\mathbb{Q}_p$-valued, but we shall not need it. To check that (2) indeed extends the definition given in Sect. 0.2 (5), compute, using the special choices of $z_\infty^{(i)}$ and $z_0^{(i)}$ given above, and Properties 0.2

$$\begin{aligned} Q(\alpha, e_i)/Q(\alpha, e_0) &= u_\alpha(z_\infty^{(i)})/u_\alpha(z_\infty^{(0)}) = u_\alpha(z_\infty^{(i)})/u_\alpha(\alpha_i(z_\infty^{(i)})) \\ &= Q(\alpha, \alpha_i) = Q(\alpha, e_i - e_0) . \end{aligned}$$

1.4 Relation with generalized Jacobians

Let $m = (\xi_0) + (\xi_\infty)$ be the "cuspidal modulus" on $X_0(p)$, and $J_m = J_0(p)_m$ the generalized Jacobian with that modulus, an extension of $J = J_0(p)$ by $\mathbb{G}_m$. Its $\mathbb{C}_p$-valued points are classes of divisors of degree 0 on $X_0(p)(\mathbb{C}_p)$ which are prime to m (denoted by $\mathrm{Div}^0(X_0(p)(\mathbb{C}_p))(m)$) modulo principal divisors of functions f for which $f(\xi_0) = f(\xi_\infty) \neq 0, \infty$ (denoted by P_m):

$$J_m(\mathbb{C}_p) = \mathrm{Div}^0(X_0(p)(\mathbb{C}_p))(m)/P_m \,. \tag{3}$$

On the analytic side, let $q : \mathbb{Z}[S]_0 \to \mathrm{Hom}(\mathbb{Z}[S], K^\times)$ be defined via $q(\alpha) = Q(\alpha, -)$. Let

$$J_m^{an} = \mathrm{Hom}(\mathbb{Z}[S], \mathbb{C}_p^\times)/q(\mathbb{Z}[S]_0)\,, \tag{4}$$

an extension of J^{an} by $\mathbb{C}_p^\times$. Define a map $\phi : \mathrm{Div}^0(\mathfrak{H}_\Gamma)(m) \to J_m^{an}$ by assigning to the divisor (a)–(b) the class of the homomorphism defined by $e_i \mapsto \Theta(a, b; z_\infty^{(i)})/\Theta(a, b; z_0^{(i)})$. If $b = \alpha a$, this homomorphism is $q(\alpha)$, and its class is trivial. The map ϕ therefore factors through $\mathrm{Div}^0(X_0(p))(m)$. As in [M-D], we have the following

Proposition. *ϕ induces an isomorphism $J_m \approx J_m^{an}$.*

Proof. If f is a meromorphic function on $X_0(p)$ and $(f) = \sum n_i(\tau(a_i))$ we may choose the a_i (and change f by a constant) so that

$$f = \prod \Theta(a_i, a; z)^{n_i} \quad (a \text{ arbitrary})\,.$$

With our previous terminology, letting $\mathbf{d} = \sum n_i(a_i)$, $f = \Theta(\mathbf{d}; z)$. But if $f \in P_m$,

$$1 = f(\xi_\infty)/f(\xi_0) = \Theta(\mathbf{d}; z_\infty^{(i)})/\Theta(\mathbf{d}; z_0^{(i)})$$

is the image of e_i under the homomorphism to which ϕ sends $\mathbf{d}$. Thus (f) is in the kernel of ϕ, and ϕ induces a map from J_m to J_m^{an} as contended. The proof that this map is an isomorphism is similar to the proof in the case of the ordinary Jacobian [M-D]. □

1.5 Extension of Q to $\mathbb{Z}[S] \times \mathbb{Z}[S]$

Let z and z' be two variables near $z_0^{(i)}$ and $z_\infty^{(i)}$ respectively, related by

$$j' \circ \tau(z) = j \circ \tau(z') \tag{5}$$

(equivalently, $\tau(z) = w_p(\tau(z'))$). Define

$$Q(e_i, e_j) = \lim[j' \circ \tau(z)]^2 \cdot \Theta(z', z; z_\infty^{(j)})/\Theta(z', z; z_0^{(j)})\,, \tag{6}$$

the limit taken as $z \to z_0^{(i)}$ and $z' \to z_\infty^{(i)}$, with (5) holding.

Observe that at $z = z_0^{(i)}$ $j' \circ \tau(z)$ has a simple pole, while the Θ function in the numerator has a simple zero, and the one in the denominator a simple

pole, so the expression is finite. Q takes its values in K, because we may restrict z and z' to K-rational points in computing the limit, and K is complete. Having defined it on a basis, extend Q linearly to $\mathbb{Z}[S] \times \mathbb{Z}[S]$. To check that it generalizes (2), one computes $Q(e_i, e_j)/Q(e_0, e_j)$ with the specific choices described in Sect. 1.3 above, and one gets $Q(\alpha_i, e_j)$.

This concludes the definition of Q on $\mathbb{Z}[S] \times \mathbb{Z}[S]$. It does not seem to extend naturally to $\mathbb{Z}[S] \times \mathbb{Z}[S]^*$ (at least we could not find any such natural extension). One can probably prove that the extended Q is symmetric and $\mathbb{Q}_p$-valued, but we will not need these facts. Instead, we will obtain the analogous statements for $\bar{Q}$ in the course of the proof of our main theorem.

1.6 Denote by

$$\hat{e} = \sum \delta_i^{-1} e_i \in \mathbb{Z}[S]^* \,. \tag{7}$$

Let $d = (12, p-1)$, and observe that $(12/d)\hat{e} \in \mathbb{Z}[S]$. We will find the following table handy:

$p \bmod 12$	$j(e_i)$ with $\delta_i > 1$	δ_i	$d = (12, p-1)$	$12/d$
1	–	1	12	1
5	0	1, 3	4	3
7	1728	1, 2	6	2
11	0, 1728	1, 2, 3	2	6

In Sect. 3, we shall prove the following formulae for the reduction $\bar{Q}$ of our extended pairing Q modulo principal units:

$$\bar{Q}(e_i, e_j) = (j(e_i) - j(e_j))^{p+1} \quad (i \neq j) \tag{8}$$

$$\bar{Q}(e_i, (12/d)\hat{e}) = p^{12/d} \,. \tag{9}$$

Main Theorem. (a) *If* $p \equiv 1 \bmod 4$, *the (extended) pairing* $\bar{Q}$ *and* $\langle \cdot, \cdot \rangle$ *agree on* $\mathbb{Z}[S] \times \mathbb{Z}[S]$ (*in particular, conjecture* 0.5 *is true*).

(b) *If* $p \equiv 3 \bmod 4$, *there exist signs* $\varepsilon_i \in \{\pm 1\}$, *such that*

$$\bar{Q}(e_i, e_j) = \langle e_i, e_j \rangle \quad \forall i \neq j$$
$$\bar{Q}(e_i, e_i) = \varepsilon_i \langle e_i, e_i \rangle \,.$$

Furthermore, if $j(e_i) \in \mathbb{F}_p$ (*except possibly in the case* $p \equiv 11 \bmod 12$, $j(e_i) = 0$), $\varepsilon_i = 1$.

Proof that (8) *and* (9) *imply the main theorem.* If $p \equiv 1 \bmod 12$, there is nothing more to prove. All the arguments below are needed to deal with the complications that $j = 0$ and 1728 cause when they happen to be supersingular.

1.7 Lemma. $\bar{Q}$ *is* $\mathbb{Q}_p^\times / U_1(\mathbb{Q}_p)$*-valued.*

Proof. We know this to be the case on $Z[S]_0 \times \mathbb{Z}[S]_0$, by lemma 0.4. We also know that $\bar{Q}(e_i, e_j) \in \mathbb{Q}_p^\times / U_1(\mathbb{Q}_p)$ for $i \neq j$ by (8), and that $\bar{Q}(e_i, e_i)^{12/d\delta_i} \in \mathbb{Q}_p^\times / U_1(\mathbb{Q}_p)$ by (8) and (9). If $p \equiv 1 \bmod 12$ there is nothing to prove. If $p \equiv 5, 7 \bmod 12$, suppose $\delta_0 > 1$. Then $12 = d\delta_0$ and $\bar{Q}(e_0, e_0) \in \mathbb{Q}_p^\times / U_1(\mathbb{Q}_p)$. Since $\bar{Q}(e_i, e_i) = \bar{Q}(e_i - e_0, e_i - e_0) \cdot \bar{Q}(e_i, e_0)^2 \cdot \bar{Q}(e_0, e_0)^{-1}$ this proves the

lemma. If $p \equiv 11 \bmod 12$, and $\delta_0 = 3$, $\delta_1 = 2$, then $\bar{Q}(e_0, e_0)^2$ and $\bar{Q}(e_1, e_1)^3 \in \mathbb{Q}_p^\times / U_1(\mathbb{Q}_p)$. As before, this implies that $\bar{Q}^2$ and $\bar{Q}^3$ take their values in $\mathbb{Q}_p^\times / U_1(\mathbb{Q}_p)$, hence so does $\bar{Q}$. □

1.8 Now let $p \equiv 5 \bmod 12$. Then (8) and (9) imply that $\bar{Q}(e_i, e_j)^3 = \langle e_i, e_j \rangle^3$. However, $\mathbb{Q}_p^\times / U_1(\mathbb{Q}_p)$ has no 3-torsion in this case, so part (a) of the theorem follows.

If $p \equiv 7 \bmod 12$, $\bar{Q}^2 = \langle \cdot, \cdot \rangle^2$, and therefore $\bar{Q}(e_i, e_i)$ and $\langle e_i, e_i \rangle$ agree up to a sign. If $p \equiv 11 \bmod 12$, $\bar{Q}^6 = \langle \cdot, \cdot \rangle^6$. Again $\mathbb{Q}_p^\times / U_1(\mathbb{Q}_p)$ has no 3 torsion, so we can extract cubic roots and deduce that $\bar{Q}(e_i, e_i)$ and $\langle e_i, e_i \rangle$ agree up to a sign.

To finish the proof of part (b) let us first deal with the exceptional values 0 and 1728. If $p \equiv 7 \bmod 12$, and $j(e_0) = 1728$, then (8) and (9) give directly $\bar{Q}(e_0, e_0) = \langle e_0, e_0 \rangle$. If $p \equiv 11 \bmod 12$ and $j(e_0) = 1728$, then (8) and (9) give $\bar{Q}(e_0, 3e_0) = \langle e_0, 3e_0 \rangle$, and since $\mathbb{Q}_p^\times / U_1(\mathbb{Q}_p)$ has no 3-torsion, $\bar{Q}(e_0, e_0) = \langle e_0, e_0 \rangle$.

For any other e_i with $\delta_i = 1$, $j(e_i) \in \mathbb{F}_p$, we prove elsewhere (see [dS], Theorem 2(iii)) that $\bar{Q}(e_i, e_i)/(-p)$ is a square in $\mathbb{F}_p^\times$. This results from a different characterization of the pairing $\bar{Q}$, by means of Kronecker's modular equation. However, $\prod_{k \neq i} (j(e_i) - j(e_k))^{-(p+1)/\delta_k}$ is also a square in $\mathbb{F}_p^\times$, so $\langle e_i, e_i \rangle / (-p)$ is a square there. Since -1 is not a square, we must have $\varepsilon_i = 1$. □

2 Lemmas on rigid analytic functions

2.1 In this section we gather several lemmas on rigid analytic functions in $\mathbb{P}^1$, that will be used in the next section in the proof of Sect. 1 (8) and (9).

Lemma. *Let $U = \{z \mid |z| \leqq 1\}$ be the unit disk, $D_1, D_2, \ldots D_m$ mutually disjoint (open) residue disks in U, $U' = U - \bigcup D_i$, and $A = \mathbb{P}^1 - \bigcup D_i$. Let f be a rigid analytic homeomorphism of A onto itself, which maps U' isomorphically onto itself, and which satisfies $|f(z) - z| < 1$ for $z \in U'$. For $x, y \in \mathbb{A}^1$ write $x \sim y$ for the equivalence relation $|x/y - 1| < 1$. Let $f(z_0) = \infty$, and assume that $z_0 \neq \infty$. Then for $z \in \mathbb{A}^1$ near z_0,*

$$f(z) \sim -z_0^2/(z - z_0)\,.$$

Proof. f has a simple pole at z_0, hence from the Mittag–Leffler decomposition ([G-vdP], p. 41) we know that

$$f = (az + b)/(z - z_0) + \sum_{1 \leqq i \leqq m} f_i\,, \tag{1}$$

where each $f_i = \sum_{1 \leqq j < \infty} c_{i,j} (z - z_i)^{-j}$, and $z_i \in D_i$. Furthermore, for the sup-norm we have

$$\|f\|_{U'} = \operatorname{Max} \{\|f_i\|_{U'}, |a/z_0|, |b/z_0|\} = 1\,.$$

Clearly on $\alpha(t) = \{z \mid 1 < |z| < t\}$, $|f_i| < 1$. On the other hand, if t is small enough $z \sim f(z)$ in $\alpha(t)$, because this is an "open" relation that extends beyond the "closed" affinoid $\subseteq U$ where it holds by assumption. Thus in $\alpha(t)$, for t small

$$z \sim f(z) \sim (az + b)/(z - z_0) \sim (az + b)/(-z_0),$$

so

$$|1 + a/z_0 + b/zz_0| < 1 \quad \forall z \in \alpha(t), t \text{ small}.$$

Now this can only hold if $a \sim -z_0$, and $|b| < |z_0|$. It follows that when $z \sim z_0$, $f \sim (az + b)/(z - z_0) \sim -z_0^2/(z - z_0)$. □

2.2 Next we want to introduce the notion of the "winding number" or degree of a rigid analytic function on an open annulus.

Let K be a finite extension of $\mathbb{Q}_p$, and $r \in K^\times, |r| < 1$. Let $A = \{z \in \bar{K} \mid |r| < |z| < 1\}$ be an open annulus. Let f be a K-rational rigid analytic function without zeroes in A, which extends to some affinoid containing A. Let $f = \sum_{n \in \mathbb{Z}} a_n z^n$ be its Laurent expansion in A, $a_n \in K$. The assumption that f extends to some affinoid implies that it is bounded on A, and $\|f\|_A = \max\{|a_n|, |r^n a_n|\}$. The assumption that f has no zeroes in A implies that an equality of the type $\max\{|a_i|t^i\} = |a_n|t^n = |a_m|t^m$, with $n \neq m$ and $|r| < t < 1$, does not occur. It follows easily that there exists an $e \in \mathbb{Z}$ such that for all $z \in A$

$$|f(z)| = |a_e z^e| > |a_n z^n| \quad (n \neq e). \tag{2}$$

Equivalently, $e = \mathrm{Res}_A(df/f)$, where the residue is defined as usual (see [G-vdP], p. 94). We refer to this e as the *degree* of f on A (or its winding number), and write it $\deg(f|_A)$. If $z' = a_1 z +$ (higher terms) is another parameter on A, inducing the same orientation, the degree of f computed with respect to z' is the same as that computed with respect to z. If we reverse the orientation (e.g. choose r/z as a local parameter), the degree changes sign.

Now let $D_i = \{z \mid |z - z_i| < |r_i|\}$ be mutually disjoint open disks in $\mathbb{P}^1$, and $F = \mathbb{P}^1 - \bigcup D_i$. Let $A_i = \{z \mid |r_i'| < |z - z_i| < |r_i|\}$, so that $D_i' = D_i - A_i$ is an affinoid disk, and $F \cup \bigcup A_i = \mathbb{P}^1 - \bigcup D_i'$. Let f be a rigid meromorphic function in $F \cup \bigcup A_i$. Assume that f has no poles or zeroes in the A_i (this can always be achieved by shrinking the size of the A_i if necessary). Orient A_i so that $z - z_i$ is a local parameter on it (we say it points *into* F).

Lemma. *Under the above hypotheses,*

$$\sum_i \deg(f|_{A_i}) = \#(\text{poles of } f \text{ in } F) - \#(\text{zeroes of } f \text{ in } F) \tag{3}$$

(zeroes and poles counted with multiplicities).

Proof. This analogue of Cauchy's residue theorem clearly holds for rational functions. By uniform approximation, it also holds for rigid meromorphic ones. See [G-vdP], p. 52. □

2.3 Lemma. *Assume that* $\deg(f|A_i) = 0$ *for all* i, *and that* f *is analytic in* F. *Then* $|f|$ *is constant.*

Proof. [G-vdP], p. 54. □

2.4 Corollary. *Let* f *be a rigid analytic funciton in* $\mathfrak{H}_\Gamma$, *without any zeroes. Assume that for any edge* ε *of the tree of* Γ, $\deg(f|_{r^{-1}(\varepsilon)}) = 0$, *where* $r^{-1}(\varepsilon)$ *is the open annulus which is the preimage of* ε *under the reduction map. Then* f *is constant.*

Proof. By the previous lemma, $|f|$ is constant and so f is bounded on $\mathfrak{H}_\Gamma$. By the p-adic analogue of Liouville's theorem ([G-vdP], p. 57), f must be constant. The assumption that f has no zeroes is only needed to guarantee that the degrees are defined. □

3 Conclusion of the proof of the main theorem

3.1 We begin by proving formula (8) of Sect. 1. Fix the choice of $z_\infty^{(i)}$ and $z_0^{(i)} = z_0 \in A$ $(0 \leqq i \leqq g)$ as suggested in Sect. 1.3 (in particular they are all finite). Let $x \sim y$ denote the equivalence relation $|x/y - 1| < 1$ as before, and denote by $\rho(a,b;c,d)$ the cross ratio $\{(a-c)(b-d)\}/\{(a-d)(b-c)\}$. Fix $i \neq 0$. Let z and z' be variables as in Sect. 1.5, and proceed to compute $Q(e_i, e_0)$ using Sect. 1.5(6).

In computing $\Theta(z_\infty^{(0)}, z_0; z')/\Theta(z_\infty^{(0)}, z_0; z)$ all the terms of the product 0.2(4) corresponding to $\gamma \neq 1, \alpha_i^{-1}$ are principal units, and therefore may be ignored up to $\sim$. The term with $\gamma = 1$ is

$$\begin{aligned}\rho(z', z; z_\infty^{(0)}, z_0) &= \{(z' - z_\infty^{(0)})(z - z_0)\}/\{(z' - z_0)(z - z_\infty^{(0)})\} \\ &\sim (j(e_i) - j(e_0)) \cdot (z_0 - z)/z_0^2 . \end{aligned} \tag{1}$$

The one with $\gamma = \alpha_i^{-1}$ is

$$\rho(z', z; \alpha_i^{-1} z_\infty^{(0)}, \alpha_i^{-1} z_0) = \rho(\alpha_i z', \alpha_i z; z_\infty^{(0)}, z_0) . \tag{2}$$

Now consider the involution w_p, and *assume first* that $j(e_0) \in \mathbb{F}_p$. Since w_p fixes e_0, there exists a unique $w \in N(\Gamma)$ inducing it, which maps the annulus a to itself. Then necessarily $w(A) = A'$, w reverses orientation on a, and $w(B_{i'}) = C_i'$, where i' is the index for which $j(e_{i'}) = j(e_i)^p$. Since $w^2 \in \Gamma$, but Γ contains no elliptic elements, $w^2 = 1$. In this case $w z_\infty^{(0)} = z_0$, $w\alpha_i z' = z$ (because both are variables near z_0, and $j' \circ \tau(w\alpha_i z') = j \circ \tau(\alpha_i z') = j \circ \tau(z') = j' \circ \tau(z)$), and $w\alpha_i z \in B_{i'}$. Using the invariance of the cross ratio under w, we obtain for (2)

$$\rho(z, w\alpha_i z; z_0, z_\infty^{(0)}) \sim (j(e_{i'}) - j(e_0)) \cdot (z_0 - z)/z_0^2 . \tag{3}$$

Multiplying (1) and (3), we get (remember $j(e_0) \in \mathbb{F}_p$)

$$\Theta(z_\infty^{(0)}, z_0; z')/\Theta(z_\infty^{(0)}, z_0; z) \sim (j(e_i) - j(e_0))^{p+1} \cdot (z_0 - z)^2/z_0^4 . \tag{4}$$

Lemma 2.1 tells us that $j' \circ \tau(z) \sim z_0^2/(z_0 - z)$. To see this recall the normalization of Γ and our fundamental domain (lemma 1.2), according to which $j' \circ \tau$ maps A just onto itself. It is a rigid analytic *homeomorphism*, because an ordinary elliptic curve has a unique subgroup of order p which reduces to a multiplicative subgroup-scheme, namely the unique subgroup contained in the formal group (in "the kernel of reduction"). Finally $j' \circ \tau$ maps $U' = A \cap$ (the closed unit disk U) onto itself, and by condition (ii) of lemma 1.2, its reduction mod p is the identity map. Thus lemma 2.1 is applicable. We finally get from the definition in Sect. 1.5 that

$$\tilde{Q}(e_i, e_0) = (j(e_i) - j(e_0))^{p+1} , \tag{5}$$

as desired.

3.2 If, on the other hand, $j(e_0) \in \mathbb{F}_{p^2} \backslash \mathbb{F}_p$ let $e_g = e_0'$, i.e. $j(e_g) = j(e_0)^p$. Then w_p interchanges e_0 with e_g, and there exists a unique $w \in N(\Gamma)$ inducing w_p, such that $w(a) = c_g$. Since $w^2 \in \Gamma$, we must have $w^2 = \alpha_g$. Clearly $w(A) = A'$, $w(B_g) = \mathbb{P}^1 - C_0$, $w(B_0) = C_g'$, and $w(B_{i'}) = C_i'$. In this case apply w^{-1} to the entries of (2). Then $w^{-1} z_\infty^{(0)} = z_0$, $w^{-1} z_0 \in B_g$, $w^{-1} \alpha_i z' = z$ (for the same reason as before), and $w^{-1} \alpha_i z \in B_{i'}$. Using the invariance of the cross ratio under w^{-1} we get for (2)

$$\rho(z', z; \alpha_i^{-1} z_\infty^{(0)}, \alpha_i^{-1} z_0) \sim (j(e_{i'}) - j(e_g)) \cdot (z_0 - z)/z_0^2 . \tag{6}$$

Multiplying (1) and (6) we get (4) again, and the rest of the proof is identical to the case $j(e_0) \in \mathbb{F}_p$. This concludes the proof of Sect. 1(8). □

3.3 Let us now turn to the proof of Sect. 1(9). Consider the *modular unit* μ in the function field of $X_0(p)/\mathbb{Q}$, whose logarithmic derivative $d\mu/\mu$ is the unique Eisenstein series of weight 2 on $X_0(p)$. Over $\mathbb{C}$

$$\mu(z) = (\Delta(pz)/\Delta(z))^{1/d} = q^{(p-1)/d} \prod_{(i,p)=1} (1 - q^i)^{-24/d} \quad (q = e^{2\pi i z}) \tag{7}$$

where $d = (p-1, 12)$ as before. We shall regard μ as a meromorphic function on $X_0(p)(\mathbb{C}_p)$, and therefore via τ also as a function on $\mathfrak{H}_\Gamma$. Let

$$\nu(z) = \prod_{0 \leqq \ell \leqq g} \Theta(z_\infty^{(\ell)}, z_0; z)^{12/d\delta_\ell} \quad z \in \mathfrak{H}_\Gamma . \tag{8}$$

Proposition. *The function $\nu(z)$ is a constant multiple of $\mu(z)$.*

Proof. Since $\sum 12/\delta_\ell = p - 1$, both functions have the same divisor on $\mathfrak{H}_\Gamma$, namely $((p-1)/d) \cdot \{\Gamma z_\infty - \Gamma z_0\}$. Thus ν/μ is an entire nowhere vanishing function on $\mathfrak{H}_\Gamma$. We shall use the criterion of corollary 2.4 to deduce that it is constant.

It is easy to see (from the infinite product defining the theta functions) that if ε is an annulus in $\mathfrak{H}_\Gamma$ reducing to an edge of the tree, which modulo Γ corresponds to e_ℓ, then

$$\deg(v|_\varepsilon) = 12/d\delta_\ell \,. \tag{9}$$

Here the orientation of the annuli is chosen to be compatible with the orientation of the edges of the graph fixed in Sect. 0.1: they always point *from* an affinoid containing an ∞-cusp (where v and μ have a zero) *into* an affinoid containing a 0-cusp (where they have a pole). (To fix ideas, we say that the annulus $\{z \mid |p| < |z| < 1\}$ with the orientation given by the parameter z, points from the disk $\{|z| \leqq |p|\}$ into $\{|z| \geqq 1\}$.) We shall show that (9) holds for μ in place of v.

Let F (resp. F') be the subaffinoid of $X_0(p)$ parametrizing pairs (E,H) where E has good ordinary reduction, and H is not contained (resp. contained) in the kernel of reduction. Thus $F = \tau(A)$ and $F' = \tau(A')$. We claim that $|\mu(z)| = |p|^{-12/d}$ for all $z \in F$, and $|\mu(z)| = 1$ on F'. Since $\mu \circ w_p = p^{-12/d}\mu^{-1}$ (this is most easily proved over $\mathbb{C}$), and since w_p maps F onto F', it is enough to prove that $|\mu| = p^{-12/d}$ on F. Pick (E,H) representing a point z in F, and let ω be a Néron differential on E. Let ω' be the unique differential on E/H whose pull-back to E is ω. Since H extends to an *étale* group-scheme in a model of E over some ring of integers, ω' is also a Néron differential. But

$$\mu(z) = \{\Delta(E/H, \omega'/p)/\Delta(E,\omega)\}^{1/d}$$

(this again is most easily checked over $\mathbb{C}$), and $\Delta(E,\omega)$ as well as $\Delta(E/H,\omega')$ are p-adic units. Our claim follows.

Now if f is a rigid analytic function without zeroes on the annulus $\varepsilon = \{z \mid |p^\delta| < |z| < 1\}$ we have

$$-\delta \cdot \deg(f|_\varepsilon) = \lim_{|z|\to 1} \operatorname{ord} f(z) - \lim_{|z|\to|p|^\delta} \operatorname{ord} f(z)$$

(ord is the valuation normalized by $\operatorname{ord}(p) = 1$). Since we have just seen that for μ the right hand side is $12/d$, for all the supersingular annuli, we get that if ε is a supersingular annulus which reduces to an edge corresponding to e_ℓ,

$$\deg(\mu|_\varepsilon) = 12/d\delta_\ell \,. \tag{10}$$

Comparing (9) with (10), the proposition follows from corollary 2.4. □

3.4 All that remains is to compute Sect. 1(9). By definition, this is

$$\lim [j' \circ \tau(z)]^{2(p-1)/d} \cdot v(z')/v(z) \,, \tag{11}$$

where z and z' are as in Sect. 1.5. By the proposition, we may substitute μ for v in this computation. Furthermore, the function $\mu(z')/\mu(z)$ is an *algebraic* function of the point $\tau(z) \in X_0(p)(\mathbb{C}_p)$, since μ is algebraic and z' and z are related by $\tau(z') = w_p(\tau(z))$. So is $j' \circ \tau(z) = j(w_p(\tau(z))$, of course. It follows that the limit in (11) is computed from the formal Laurent expansion at the cusp ξ_0, so we may revert to the *complex* q-expansion (7), and to the well-known complex q-expansion of j to compute it. Noting that μ satisfies the

functional equation $\mu \circ w_p = p^{-12/d}\mu^{-1}$, we find that (11) is equal to $p^{12/d}$. This concludes the proof of Sect. 1(9), and of the main theorem. □

Acknowledgement. I learned about the subject of this paper during a visit to Paris in October 1989. I would like to thank Université Paris VI for the hospitality and the support during that visit. I would like to thank J. Oesterlé for suggesting the problem and sharing his ideas with me. Further discussions with him in 1991 helped to improve our results considerably. I would also like to thank Ron Livné for illuminating discussions related to this work.

References

[D-R] Deligne, P., Rapoport, M.: Schémas de modules de courbes elliptiques. LNM **349**, Springer-Verlag (1973), 143–316

[dS] de Shalit, E.: Kronecker's polynomial, supersingular elliptic curves, and p-adic periods of modular curves. In: Proceedings of the workshop on p-adic monodromy and the Birch–Swinnerton–Dyer conjecture (Boston 1991). Contemporary Mathematics **165**, AMS (1994), 135–148

[Ge-vdP] Gerritzen, L.: van-der-Put, M. Schottky groups and Mumford curves. LNM **817**, Springer-Verlag (1980)

[M-D] Manin, J., Drinfel'd, V.G.: Periods of p-adic Schottky groups. J. reine angew. Math. **262/3** (1973), 239–247

[Mu] Mumford, D.: An analytic construction of degenerating curves over complete local rings. Comp. Math. **24** (1972), 129–174