Transcendence of Elliptic Modular Functions in Characteristic $p$

**José Felipe Voloch**

*Department of Mathematics, University of Texas, Austin, Texas 78712*

Communicated by D. Goss

Received November 11, 1994; revised January 20, 1995

Classical transcendence theory began with the study of special values of the exponential function and later the study of special values of the logarithm and, more generally elliptic and abelian logarithms, was added (see [B]). Characteristic $p$ analogues have been considered, first with the analogues of the exponential function arising from the theory of Drinfeld modules (see [Y]) and also with $p$-adic exponentiation and its abelian analogue [MP, V]. Let us also note the general transcendence criterion obtained in [CKMR].

The purpose of this paper is to study the transcendence properties in positive characteristic of the power series introduced by Tate which give a non-archimedian analogue of elliptic functions. Let $p$ be a prime number, $k$ the algebraic closure of $F_p$, and $q$ be a transcendental over $k$, i.e., a variable. The following series determine elements of $k[[q]]$:

$$a_4 = -5 \sum_{n \geq 1} n^3 q^n/(1-q^n),$$

$$a_6 = (-1/12) \sum_{n \geq 1} (7n^5 + 5n^3) q^n/(1-q^n).$$

Swinnerton-Dyer has shown that $a_4$ and $a_6$ are algebraically dependent in positive characteristic, in contrast with characteristic zero [S-D]. In fact this is clear for $p < 11$, for example, $a_4 = a_6$ for $p = 2$ and $a_4 = 0$ for $p = 5$. Let $K = k((a_4, a_6))$ and $L = k((q))$. Note that $K$ is a subfield of $L$. Our first result is the following.

**Theorem A.** $q$ is transcendental over $K$.

* E-mail: voloch@math.utexas.edu.
We will prove this theorem below. First we will introduce some more notation and state our second result. Consider the following series:

\[ x = x(q, u) = \sum_{n \in \mathbb{Z}} q^n u/(1 - q^n u)^2 - 2 \sum_{n \geq 1} nq^n/(1 - q^n), \]

\[ y = y(q, u) = \sum_{n \in \mathbb{Z}} q^n u^2/(1 - q^n u)^3 + \sum_{n \geq 1} nq^n/(1 - q^n). \]

They converge for any \( u \) in \( L^* \), not a power of \( q \), and satisfy

\[ y^2 + xy = x^3 + a_4 x + a_6, \]

therefore giving an analytic parametrization over \( L \) of the elliptic curve \( E \) (the Tate curve), defined over \( K \) by this equation. For details on the Tate curve, the reader may consult [S, Chap. V].

**Theorem B.** If \( u \neq 0 \), \( q^n, n \in \mathbb{Z} \) is algebraic over \( L \) and such that \((x(q,u), y(q,u))\) is a point on \( E \) algebraic over \( K \) and of infinite order, then \( u \) is transcendental over \( K \).

Note that Theorem A is the analogue of transcendence of periods of an elliptic curve with algebraic coefficients and Theorem B is the analogue of the transcendence of the elliptic logarithm of algebraic points on such elliptic curves. See [B, Chap. 6].

After seeing this paper, Thakur [T] found another proof of Theorem A using the transcendence criterion of [CKMR].

To prove these theorems we will need to develop some results on the arithmetic of \( E/K \), specially regarding higher \( p \)-descents. Let us recall some well-known facts first. The Tate curve \( E : y^2 + xy = x^3 + a_4 x + a_6 \) is indeed an elliptic curve with discriminant \( D = q \prod_{n=1}^{\infty} (1 - q^n)^{24} \) and \( j \)-invariant \( j = q^{-1} + 744 + \cdots \). Moreover, \( E \) is ordinary with Hasse invariant 1. Indeed, this fact gives the algebraic relation between \( a_4 \) and \( a_6 \) when the Hasse invariant is expressed as polynomial in \( a_4 \) and \( a_6 \). Let \( E^{(p)} \) be the image of \( E \) under the \( n \)th power of the Frobenius map \( F_n \) and \( V_n : E^{(p^n)} \to E \) the dual isogeny, the \( n \)th-order Verschiebung, which is separable since \( E \) is ordinary. Let \( K_n \) be the field of definition of the points of \( \ker V_n \). These fields were studied by Igusa [I] (see also [KM, Theorem 12.6.1]), who showed that their degree over \( K \) grows with \( n \). He actually showed much more, but that is all we will need. Note that \((x(q^n, u), y(q^n, u))\) parametrize \( E^{(p^n)} \) and that the image of \( u = q \) gives a generator \( P_n \) of \( \ker V_n \). Let \( E[p^n] \) denote, as usual, the group scheme which is the kernel of multiplication by \( p^n \) on \( E \). We have the following exact sequence \( 0 \to \ker F^n \to E[p^n] \to \ker V_n \to 0 \). Over \( K_n \), \( \ker V_n \) is isomorphic to \( \mathbb{Z}/p^n \mathbb{Z} \) and one can choose the isomorphism so that \( 1 \) corresponds to the image of \( q \) as above. By Cartier duality, we get an isomorphism between
ker $F^n$ and $\mu_{\rho}$. Thus, the above exact sequence gives a class $q_n$, the Serre–Tate parameter, in $\text{Ext}^1_{L^n}(\mathbb{Z}[p^n]^{*}, \mu_{\rho}) = H^1(K_n, \mu_{\rho}) = K_n^{*}(K_n^{*})^{\rho}$, where here and elsewhere the cohomology of group schemes. The absolute Galois group $G$ acts on this group; and we wish to describe its action on $q_n$. First, $G$ acts on $V_n$ by a $p$-adic character $\gamma : G \rightarrow \mathbb{Z}_p^*$, which is independent of $n$ and is of infinite order by Igusa’s theorem. Let $K_s$ be the separable closure of $K$. Taking cohomology of the exact sequence $0 \rightarrow \ker F^n \rightarrow E[p^n] \rightarrow V_n \rightarrow 0$, we get $q_n$ as the image of $1 \in \ker V_n$ in $H^1(K_n, \mu_{\rho})$. We will, more generally, consider the map $\beta_n : E[p^n](K_s)/F^n(E(K_s)) \rightarrow H^1(K_s, \mu_{\rho}) = K_s^{*}(K_s^{*})^{\rho}$ obtained from the exact sequence $0 \rightarrow \ker F^n \rightarrow E \rightarrow E[p^n] \rightarrow 0$ and the identification of ker $F^n$ and $\mu_{\rho}$ given above.

**Lemma 1.** If $p \in E[p^n](K_s)$ and $\sigma \in G$ then $\sigma(\beta_n(P)) = (\beta_n(\sigma(P)))^{\epsilon(\sigma)}$.

**Proof.** The map $E[p^n](K_s) \rightarrow H^1(K_s, \ker F^n)$ commutes with the action of $G$, and $G$ acts on Hom(ker $F^n, \mu_{\rho}) = \ker V_n$, by $\chi$, hence the lemma.

**Lemma 2.** The class of $u$ in $L^*(L^*)^{\rho}$ is equal to $\beta_n(x(q^{\rho}), y(q^{\rho}, u))$.

**Proof.** The Tate parametrization gives that $E(L)$ is isomorphic to $L^*/q^n$ and that $E[p^n](L)$ is isomorphic to $L^*/q^{n\rho}$ and that $F^n$ is induced by $u \mapsto u^{\rho}$ in $L^*$. The lemma follows.

**Proof of Theorem A.** If $P_n \in E[p^n](K_s)$ corresponds to $u = q$ then $\beta_n(P_n) = q_n$. Also, $G$ acts on ker $V_n$ via $\chi$. Therefore, applying Lemma 1 to $P_n$ yields $\sigma(q_n) = q_n^{\epsilon(\sigma)}$. From Lemma 2, $q = q_n$ in $L^*/(L^*)^{\rho}$. If $q$ is algebraic, then it follows that $q = q_n$ in $K_s^{*}(K_s^{*})^{\rho}$ also. This is impossible since, on one hand, $G$ would act on $q$ by a finite quotient and, on the other hand, $G$ acts on $q_n$ by cyclic groups that grow with $n$, since $\chi$ is of infinite order.

**Proof of Theorem B.** Replacing $u$ by $u^{\rho}$ for suitable $m$, we may assume $u$ is separable over $L$. Let $L_s$ denote the separable closure of $L$. The point in $E[p^n]$ with parameter $u$ is a point $Q_n$ satisfying $V_n(Q_n) = Q_n$, so it is an algebraic point. By Lemma 2, $\beta_n(Q_n) = u$ in $L_s^{*}(L_s^{*})^{\rho}$. If $\sigma \in G$ acts trivially on $Q_n$, then $\sigma(Q_n) = Q_n \in \ker V_n$. Therefore there exists an additive $p$-adic character $\psi$ such that $\beta_n(\sigma(Q_n)) = \beta_n(Q_n)^{\psi(\epsilon)}$. Assume now that $u$ is algebraic over $K$ and assume also that $\sigma$ fixes $u$. Then, on $K_s^{*}(K_s^{*})^{\rho}$, $u = \sigma(u) = \sigma(\beta_n(Q_n)) = \beta_n(\sigma(Q_n))^{\psi(\epsilon)}$, by Lemma 1. Hence $u = u^{\psi(\epsilon)}q_n^{\psi(\epsilon)}$ in $K_s^{*}(K_s^{*})^{\rho}$. Finally choose $\sigma$ satisfying the above conditions and such that $\psi(\epsilon) \neq 1$, which exists by Igusa’s theorem. The above equation then gives that there are $p$-adic integers $r \neq 0$, $m$ such that $u = q_m^{\psi(\epsilon)}$ in $L_s^{*}(L_s^{*})^{\rho}$, for all $n$. Furthermore, we can assume without loss of generality that $m$ is
an ordinary integer. If \( v \) is the valuation on \( L_s \), extending the natural one on \( L \), this gives \( r v(u) \equiv m \mod p^n \), for all \( n \) sufficiently large, so \( r v(u) = m \).

If \( v(u) \neq 0 \), this shows that \( r \) in a rational number and raising everything to a suitable power, we can assume that \( r \) is an integer. Since the only elements of \( L_s \) which are \( p^n \)-th powers for all \( n \) are the elements of \( k \), we obtain an equation \( u' = x q^n \) in \( L \) where \( x \in k^* \), which gives that \( Q_0 \) is torsion, proving the theorem in this case. If \( v(u) = 0 \) then \( Q_0 \) is in the formal group of \( E \) which is a \( \mathbb{Z}_p \)-module (see [V]). The equation \( u' = q^n \) in \( L_s^n / (L_s^n)^r \) for all \( n \) lead to \( r Q_0 = 0 \) and the same holds for any multiple of \( r \) in \( \mathbb{Z}_p \) instead of \( r \). In particular it holds for some non-zero integer, which completes the proof of the theorem.

If \( u \) gives a torsion point on \( E \) then \( u = x q' \), where \( x \) is in \( k \) and \( r \) is a rational number. Therefore, \( u \) is transcendental over \( K \) if and only if \( r \neq 0 \).

Finally, one could ask for analogues of the classical statements dealing with linear forms in logarithms. However, the only sense that apparently can be made of that is through \( p \)-adic exponentiation, which makes sense for elements of \( 1 + qk[[q]] \). It then follows from the results of [V] that if \( u_1, ..., u_r \in 1 + qk[[q]] \) give \( \mathbb{Z} \)-linearly independent points on \( E \), algebraic over \( K \) then \( u_1, ..., u_r \) are \( \mathbb{Z}_p \)-multiplicatively independent.

ACKNOWLEDGMENTS

The author thanks D. Thakur and J. Tate for helpful discussions and the NSF (Grant DMS-9301157) and the Alfred P. Sloan Foundation for financial support.


REFERENCES


TRANSCENDENCE OF ELLIPTIC FUNCTIONS


