Transcendence of elliptic modular functions in characteristic p

José Felipe Voloch

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, firstly 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 be the algebraic closure of $\mathbf{F}_p$ and q a transcendental over k, i.e., a variable. The following series determine elements of $k[[q]]$:

$$a_4 = -5\sum_{n\geq 1} n^3q^n/(1-q^n),$$
$$a_6 = (-1/12)\sum_{n\geq 1}(7n^5+5n^3)q^n/(1-q^n).$$

Swinnerton-Dyer has shown that a_4 and a_6 are algebraically dependent in positive characteristic in contrast with characteristic zero [S-D]. Let $K = k(a_4, a_6)$ and $L = k((q))$. Note that K is a subfield of L. Our first result is:

Theorem A. *q is transcendental over K.*

We will prove this theorem below. First we will introduce some more notation and state our second result. Consider the following series:

$$x = x(q,u) = \sum_{n\in\mathbf{Z}} q^nu/(1-q^nu)^2 - 2\sum_{n\geq 1} nq^n/(1-q^n),$$
$$y = y(q,u) = \sum_{n\in\mathbf{Z}} q^{2n}u^2/(1-q^nu)^3 + \sum_{n\geq 1} nq^n/(1-q^n).$$

They converge for any u in L^*, not a power of q and satisfy $y^2+xy = x^3+a_4x+a_6$, therefore giving an analytic parametrization of the elliptic curve E (the Tate curve), defined over K by this equation.

Theorem B. *If $u \in L$ is such that $x(q,u), y(q,u)$ are algebraic over K and define a point of infinite order in E 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 the analogue of the transcendence of the elliptic logarithm of algebraic points on such elliptic curves.

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 $E : y^2 + xy = x^3 + a_4x + a_6$ is indeed an elliptic curve with discriminant $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ 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 $E^{(p^n)}$ 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 $x(q^{p^n},u), y(q^{p^n},u)$ 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 $\mathbf{Z}/p^n\mathbf{Z}$ 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 μ_{p^n}. Thus, the above exact sequence gives a class q_n, the Serre-Tate parameter, in $\mathrm{Ext}^1_{K_n}(\mathbf{Z}/p^n\mathbf{Z}, \mu_{p^n}) = H^1(K_n, \mu_{p^n}) = K_n^*/(K_n^*)^{p^n}$ where here and elsewhere the cohomology groups are in the flat cohomology of group schemes. The absolute Galois group G of K acts on this group, and we wish to describe its action on q_n. Firstly, G acts on $\ker V_n$ by a p-adic character $\sigma \mapsto \chi(\sigma)$, which is of infinite order by Igusa's theorem. The action of G on $\ker F^n$ is by χ also. Let K_s be the separable closure of K. Taking cohomology of the exact sequence $0 \to \ker F^n \to E[p^n] \to \ker V_n \to 0$, we get q_n as the image of $1 \in \ker V_n$ in $H^1(K_n, \mu_{p^n})$. We will, more generally, consider the

map $\beta_n : E^{(p^n)}(K_s)/F^n(E(K_s)) \to H^1(K_s, \mu_{p^n}) = K_s^*/(K_s^*)^{p^n}$ obtained from the exact sequence $0 \to \ker F^n \to E \to E^{(p^n)} \to 0$ and the identification of $\ker F^n$ and μ_{p^n} given above.

Lemma 1. *If $P \in E^{(p^n)}(K_s)$ and $\sigma \in G$ then $\sigma(b_n(P)) = (b_n(\sigma(P))^{\chi(\sigma)}$.*

Proof: The map $E^{(p^n)}(K_s) \to H^1(K_s, \ker F^n)$ commutes with the action of G, but upon the identification of $\ker F^n$ with μ_{p^n}, there is the further action of G via χ, hence the lemma.

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

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

Proof of Theorem A: If $P_n \in E^{(p^n)}(K_n)$ corresponds to $u = q$ then $b_n(P_n) = q_n$. Also, G acts on $\ker V_n$ via χ. Therefore, applying lemma 1 to P_n yields $\sigma(q_n) = q_n^{\chi(\sigma)^2}$. From lemma 2, $q = q_n$ in $L^*/(L^*)^{p^n}$. If q is algebraic, then it follows that $q = q_n$ in $K_s^*/(K_s^*)^{p^n}$ 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 χ is of infinite order.

Proof of Theorem B: The point with parameter u in $E^{(p^n)}$ is a point Q_n satisfying $V_n(Q_n) = Q_0$, so is an algebraic point. By lemma 2 we get that $\beta_n(Q_n) = u$ in $L^*/(L^*)^{p^n}$. If $\sigma \in G$ acts trivially on Q_0, then $\sigma(Q_n) - Q_n \in \ker V_n$, therefore there exists an additive p-adic character ψ such that $b_n(\sigma(Q_n)) = b_n(Q_n)q_n^{\psi(\sigma)}$. Assume now that u is algebraic over K and assume also that σ fixes u. We get the following relation in $K_s^*/(K_s^*)^{p^n}$, $u = \sigma(u) = \sigma(b_n(Q_n)) = b_n(\sigma(Q_n))^{\chi(\sigma)}$, by lemma 1. Hence $u = u^{\chi(\sigma)}q_n^{\chi(\sigma)\psi(\sigma)}$ in $K_s^*/(K_s^*)^{p^n}$. Finally choose σ satisfying the above conditions and such that $\chi(\sigma) \neq 1$, which exists by Igusa's theorem. Since the above equation is valid for all n and the only elements of L which are p^n-th powers for all n are the elements of k, we obtain from this equation an equation $u^r = \alpha q^m$, where r, m are p-adic integers, $r \neq 0$ and $\alpha \in k^*$. By raising both sides of the equation to a suitable power, we can assume that $\alpha = 1$ and

without loss of generality we can further assume that $m \in \mathbf{Z}$. It follows from corollary 2 of [V] that u must represent a torsion point on E, which completes the proof of the theorem.

If u gives a torsion point in $L^*/q^{\mathbf{Z}}$ then $u = \alpha q^r$, where α 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 $u_1, \ldots, u_r \in 1 + qk[[q]]$ give $\mathbf{Z}$-linearly independent points on E, algebraic over K, then $u_1, \ldots, u_r$ are $\mathbf{Z}_p$-multiplicatively independent.

Acknowledgements: The author would like to thank J. Tate for helpful discussions and the NSF (grant DMS-9301157) and the Alfred P. Sloan Foundation for financial support.

References.

[B] A. Baker, *Transcendental number theory*, Cambridge Univ. Press, 1975.

[CKMR] G. Christol et al., *Suites algèbriques, automates et substituitions*, Bull. Soc. Math. France, **108** (1980) 401-419.

[I] J.-I. Igusa, *On the algebraic theory of elliptic modular functions*, J. Math. Soc. Japan, **20** (1968) 96-106.

[K] N. M. Katz, *Serre-Tate local moduli*, Springer LNM 868 (1981) 138-202.

[KM] N. M. Katz, B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton Univ. Press, 1985.

[MP] M. Mendès France, A. J. van der Poorten, *Automata and the arithmetic of formal power series*, Acta Arithmetica, **XLVI** (1986) 211-214.

[S-D] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences of modular forms*, Springer LMN 350 (1973), 1-55.

[V] J. F. Voloch, *Diophantine Approximation on Abelian varieties in in characteristic p*, Amer. J. Math., to appear.

[Y] J. Yu, *Transcendence in finite characteristic*, in *The arithmetic of function fields*, D. Goss et al.,eds., de Gruyter, Berlin 1992, pp.253-264.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu