JOURNAL OF NUMBER THEORY **58**, 60–63 (1996)
ARTICLE NO. 0061

Automata-Style Proof of Voloch's Result on Transcendence

DINESH S. THAKUR*

Department of Mathematics, University of Arizona, Tucson, Arizona 85721

Communicated by D. Goss

Received December 23, 1994; revised February 22, 1995

DEDICATED TO JOHN TATE ON HIS 70TH BIRTHDAY

We give another proof of Voloch's result on transcendence of the period of the Tate elliptic curve. The proof is based on the transcendence criterion of Christol involving notions of recognizable sequences and automata.

Let p be a prime number, k be an algebraic closure of $\mathbf{F}_p$. Let q be a variable and consider $a_4, a_6 \in \mathbb{Z}[\![q]\!]$ (sometimes we consider them in $k[\![q]\!]$) defined by

$$a_4 := a_4(q) := \sum_{n \geqslant 1} \frac{-5n^3 q^n}{1-q^n}, \qquad a_6 := a_6(q) := \sum_{n \geqslant 1} \frac{-(7n^5+5n^3)\, q^n}{12(1-q^n)}.$$

Let $K := k(a_4, a_6)$. In [V], Voloch proved the following function field analogue of the classical results of Siegel and Schneider proving the transcendence of periods of elliptic curves defined over algebraic number field.

THEOREM. *The period q of the Tate elliptic curve $y^2 + xy = x^3 + a_4 x + a_6$ over K is transcendental over K*

For more on the Tate curve (which we will not use directly) and for standard facts on modular forms (which we will use later), see [S, Chap. 5; M. Chap. 1], respectively. Voloch's nice proof involved approximating q by algebraic quantities and getting a contradiction by analyzing the Galois action using Igusa's theorem. We offer below a proof based on the criterion of algebraicity due to Christol. In [V] Voloch also proves transcendence of parameters of algebraic points by his method. It is unlikely that our method yields this easily.

* Supported in part by NSF grants DMS 9207706 and DMS 9314059. E-mail: thakur@math.arizona.edu.

0022-314X/96 $18.00

Proof of the Theorem. First, let $p=2$. Using straightforward divisibility arguments we see that

$$a_4 = a_6 = \sum_{n \text{ odd} \geqslant 1} q^n/(1-q^n) = \sum_{n \text{ odd} \geqslant 1} \sum_{k=0}^{\infty} q^{kn} = \sum_{m=1}^{\infty} d_{\mathrm{o}}(m)\, q^m,$$

where we have put $d_{\mathrm{o}}(m)$ to be the number of odd positive divisors of m. Writing $m = 2^k \prod p_i^{m_i}$, where p_i are distinct odd primes, we see that $d_{\mathrm{o}}(m) = \prod (m_i+1)$, so that $d_{\mathrm{o}}(m)$ is odd if and only if m is of the form n^2 or $2n^2$. Since we are in characteristic 2, this means

$$a_4 = \sum_{n=1}^{\infty} (q^{n^2} + q^{2n^2}) = f + f^2,$$

where we have put $f := \sum q^{n^2}$ (essentially the theta function).

By [E Chap. V, Example 5.2], the sequence of squares is not m-recognizable, for any integer $m > 1$. (For $m=2$, this is due to [Ri p. 530]). In particular, it is not p-recognizable, for any prime p. This implies by the Theorem 1 of [C] (or the Theorem 1 of [CKMR]) that f is transcendental over $k(q)$, for any p.

In particular, when $p=2$, $a_4 = a_6 = f + f^2$ is transcendental over $k(q)$; i.e., q is transcendental over $K = k(a_4)$.

Since f is transcendental over $k(q)$ for any p and since a_4 and a_6 are algebraically dependent over k (see Remark 1 below), the proof of the theorem will be complete for any p, if we can show that f is algebraic over $k(\bar{a}_4, \bar{a}_6)$, where $\bar{a}_4 := a_4(q^2)$, $\bar{a}_6 := a_6(q^2)$. (See Remarks 2 and 3 below). But $\bar{a}_4$, $\bar{a}_6$, and f are related to the well-known modular forms

$$e_4 := 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)\, q^{2n},$$

$$e_6 := 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)\, q^{2n},$$

$$\theta := 1 + 2 \sum_{n=1}^{\infty} q^{n^2}$$

(given by their q-expansion at the cusp at infinity) by the relations $e_4 = 1 - 48\bar{a}_4$, $e_6 = 1 - 72\bar{a}_4 + 864\bar{a}_6$, and $\theta = 1 + 2f$. Since any three modular forms, e.g., for $\Gamma_0(4)$ (our case) are algebraically dependent over $\mathbb{C}$ (in fact over $\mathbb{Q}$ in our case by the q-expansion principle), we get what we want by reduction modulo p, except possibly for finitely many p, where the reduction gives a trivial relation.

We know ([M, p. 36]) all conjugates of θ^8 under $\Gamma := SL_2(\mathbb{Z})$. Now e_4, e_6 generate modular forms for Γ. Hence, a calculation shows

$$4e_6^2 - 4e_4^3 + 27e_4^2\theta^8 - 54e_4\theta^{16} + 27\theta^{24} = 0.$$

A straight translation to the original variables gives the following identity of power series:

$$2^8(\bar{a}_6 - \bar{a}_4^2) - 2^{11}3^2\bar{a}_4\bar{a}_6 + 2^{12}3^3\bar{a}_6^2 + 2^{14}\bar{a}_4^3 + \theta^8(1 - 2^5 3\bar{a}_4 + 2^8 3^2\bar{a}_4^2) + \theta^{16}(-2 + 2^5 3\bar{a}_4) + \theta^{24} = 0.$$

This reduces to a non-trivial relation modulo p. (For $p = 2$ we get our relation back by transforming to f variable, since $\theta = 1$). Hence the proof of the theorem is complete. ∎

Remark. (1) Elementary congruences show that $a_4 = a_6$ if $p = 2$, $a_4 = 0$ if $p = 5$ and $a_4 = 5a_6$ if $p = 7$. In fact, e_4 and e_6 are algebraically dependent for all p by [S-D], which implies that a_4 and a_6 are algebraically dependent for all $p > 3$. In the remaining case $p = 3$, we claim that $a_6 + a_4 + 2a_4^2 = 0$. This is seen by

$$a_6 + a_4 = \sum_{n \equiv 2, 4(9)} \frac{q^n}{1 - q^n} + 2 \sum_{n \equiv 5, 7(9)} \frac{q^n}{1 - q^n} = \sum_{3 \nmid n} \frac{n + (-1)^{n - 3\lfloor n/3 \rfloor}}{3} \frac{q^n}{1 - q^n} = a_4^2,$$

where the first two equalities follow by considering the possibilities of n modulo 9 and the last equality is rearrangement of Ramanujan's identity (19) in [R] (which is also Theorem 383 of [HW] for $\theta = 2\pi/3$ in the notation there).

(2) The differences between q's and q^2's in some formulae here and in standard textbooks are due to the different classical normalizations $q = e^{\pi i \tau}$ or $q = e^{2\pi i \tau}$.

(3) In view of the immense literature on representations as sums of squares, both from elementary and modular points of view, it is possible that such an algebraicity relation between theta and Eisenstein series already exists in the literature.

Acknowledgments

I am grateful to Felipe Voloch for explaining his result and suggesting the algebraic dependency calculation using modular forms; to Jeremy Teitelbaum for calculating the relation between θ and e_i's on Maple; and to Noam Elkies for a suggestion simplifying the calculation.

References

[C] G. Christol, Ensembles presque périodiques k-reconnaissables, *Theoret. Comput. Sci.* **9** (1979), 141–145.

[CKMR] G. Christol, T. Kamae, M. Mendès-France, and G. Rauzy, Suites algébriques, automates et substitutions, *Bull. Soc. Math. France* **108** (1980), 401–419.

[E] S. Eilenberg, "Automata, Languages and Machines," Vol. A, Academic Press, New York, 1974.

[HW] G. Hardy and E. Wright, "An Introduction to the Theory of Numbers," 4th ed., Oxford Univ. Press, Oxford, 1971.

[M] D. Mumford, Tata lectures on Theta I, Birkhäuser, Boston, 1983.

[R] S. Ramanujan, On certain arithmetical functions, *Trans. Cambridge Philos. Soc.* **22**, No. 9 (1916), 159–184; Paper 18, *in* "Collected papers of Srinivasa Ramanujan" (G. H. Hardy *et al.*, Eds.), Chelsea, New York, 1962.

[Ri] R. Ritchie, Finite automata and the set of squares, *J. Assoc. Comput. Mach.* **10** (1963), 528–531.

[S] J. Silverman, "Advanced Topics in the Arithmic of Elliptic Curves," Springer-Verlag, New York, 1994.

[S-D] H. P. F. Swinnerton-Dyer, On l-adic representations and congruences of modular forms, *in* "Lect. Notes in Math.," Vol. 350, pp. 1–55, Springer-Verlag, New York, 1973.

[V] J. Voloch, Transcendence of elliptic modular functions in characteristic p, *J. Number Theory* **57**, No. 2 (1996).