PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 5, Pages 1309–1312
S 0002-9939(99)04650-X
Article electronically published on January 27, 1999

AUTOMATA AND TRANSCENDENCE OF THE TATE PERIOD IN FINITE CHARACTERISTIC

JEAN-PAUL ALLOUCHE AND DINESH S. THAKUR

(Communicated by David E. Rohrlich)

ABSTRACT. Using the techniques of automata theory, we give another proof of the function field analogue of the Mahler-Manin conjecture and prove transcendence results for the power series associated to higher divisor functions $\sigma_k(n) = \sum_{d|n} d^k$.

Let p be a prime number, and let k be an algebraic closure of $\mathbf{F}_p$. Let q be a variable and consider $a_4, a_6 \in k[[q]]$ defined by

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

Theorem. *The period q of the Tate elliptic curve $y^2 + xy = x^3 + a_4x + a_6$ over $K := k(a_4, a_6)$ is transcendental over K.*

This function field analogue of the Mahler-Manin conjecture was proved by Voloch [V96] (soon afterwards the original conjecture was proved in [BDGP96]; see also [W96]), by 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 automata criterion of algebraicity due to Christol [C79, CKMR80].

Proof. It suffices to prove that a_4 (resp. a_6) is transcendental over $k(q)$, if $p \neq 5$ (resp. $p = 5$). Namely, the Hasse invariant of the Tate elliptic curve, i.e., the coefficient of x^{p-1} in $(x^3 + x^2/4 + a_4x + a_6)^{(p-1)/2}$ for $p > 3$, is equal to one, which shows (essentially first noticed in [S-D73]) that a_4 and a_6 are algebraically dependent, for $p > 3$. (See the first part of the remarks below for the case $p \leq 3$.) In fact, we prove

Proposition. *If $h := (p-1)/\gcd(u, p-1)$ is even (e.g., if $p > 2$ and u is odd), then $\sum_{n\geq 1} n^u q^n/(1-q^n)$ is transcendental over $\mathbf{F}_p(q)$.*

Proof. With $\sigma_u(\ell) := \sum_{d|\ell} d^u$, we have

$$\sum_{n\geq 1} \frac{n^u q^n}{1-q^n} = \sum_{n\geq 1} n^u \sum_{k\geq 1} q^{kn} = \sum_{\ell\geq 1} \sigma_u(\ell) q^\ell.$$

Received by the editors August 27, 1997.
1991 *Mathematics Subject Classification.* Primary 11J89, 11G07, 68Q68, 11B85.
Key words and phrases. Transcendence, periods, elliptic curves, automata, recognizability.
The second author was supported in part by NSF grant DMS 9623187.

Now, from Christol's theorem [C79], [CKMR80], the series $\sum b_n q^n \in \mathbf{F}_p[[q]]$ is transcendental over $\mathbf{F}_p(q)$ if and only if the sequence b_n is not p-automatic. Furthermore, from a theorem of Cobham [Co72], for any p-automatic sequence b_n, and for any value α taken by this sequence, if $\sharp\{n \le x,\ b_n = \alpha\}$ is $o(x)$, then

– either there exist an integer $d \ge 1$ and a real number s with $0 < s < 1$, such that

$$0 < \liminf \frac{\sharp\{n \le x,\ b_n = \alpha\}}{x^s \log^{d-1} x} < \limsup \frac{\sharp\{n \le x,\ b_n = \alpha\}}{x^s \log^{d-1} x} < \infty,$$

– or there exist integers $d \ge 1$, $m \ge 2$, and a rational number $c > 0$, such that

$$\sharp\{n \le x,\ b_n = \alpha\} \sim c \left(\frac{\log x}{\log m}\right)^{d-1}.$$

On the other hand, since h is even, for some $A > 0$, we have

$$\sharp\{n \le x,\ \sigma_u(n) \neq 0 \bmod p\} \sim \frac{Ax}{(\log x)^{1/h}}.$$

(We learned this result in [R77], but it had been first proved in [Ran61].) Now define $b_n = 0$ if $\sigma_u(n) = 0 \bmod p$, and $b_n = 1$ otherwise. If $\sum_{n\ge1} \sigma_u(n) q^n$ were algebraic over $k(q)$, then the sequence $(\sigma_u(n) \bmod p)_n$ would be p-automatic, as would be the sequence b_n, and the two statements above give us the desired contradiction.

Remarks. (1) In [T96], another proof of the theorem above was given by reducing the question to the transcendence of the theta function and using the theory of modular forms to show algebraic dependence between the theta function and a_4, a_6, which are related to Eisenstein series. The present proof avoids this modular technology form by directly establishing the transcendence of a_4 or a_6. For $p \le 7$, the proof is simpler in that we do not then need the fact on the Hasse invariant either: it is easy to see that $a_4 = a_6$ if $p = 2$; $a_4 = 0$ if $p = 5$; $a_4 = 5a_6$ if $p = 7$; and (see [T96]) $a_6 + a_4 = a_4^2$ if $p = 3$. A more conceptual proof of the last equality has been recently given (private communication) by Antonios Broumas, based on his generalization of the Hasse invariant (taking values in Witt vectors). Another proof follows from the results of Katz mentioned in (2). It would be nice to have a direct elementary proof of the algebraic relation between a_4 and a_6, in general.

(2) For a non-negative integer u, let $S_u := \sum_{n\ge1} \sigma_u(n) q^n \in \mathbf{F}_p[[q]]$. One might ask in general whether S_u is transcendental over $k(q)$ and when S_u and S_v are algebraically dependent over $\mathbf{F}_p$, or more generally what the transcendence degree of the field generated by all S_u's over $\mathbf{F}_p$ is. It is easy to see that $S_u = S_{u+k(p-1)}$, if $u, k > 0$ and $S_{p-1} = S_0 - S_0^p$, so that the answers depend only on u, v modulo $p-1$ and the case $p = 2$ has been completely settled. The situation of algebraic dependence, in general, is unclear when u or v is even. Poonen checked that there is no non-trivial algebraic relation of total degree < 21 between S_1 and S_2, when $p = 3$. Even when u and v are odd, the question of the possible algebraic dependences is non-trivial because the well-known relations between Eisenstein series when expressed in terms of S_u's and reduced modulo p can sometimes become trivial. For example, the fact that the Hasse invariant is one, gives a non-trivial relation between S_3 and S_5 for

$p > 7$, and we have $S_3 = S_5$ for $p = 2, 3$ as explained above. Even though the relation obtained is trivial for $p = 5, 7$, Bjorn Poonen found by computer calculation that with $x = S_3$ and $y = S_5$, we have $x^5 - x = 3y^4 + 2y^3 - y^2 - y$, for $p = 5$ and $y^7 - y = 4x^{12} + 3x^{11} + 3x^{10} + x^9 - x^8 + x^6 + 5x^5 - x^3 + 4x^2 - x$ for $p = 7$. He proved these relations using some results of Katz and pointed out that Theorem 2.1 of [K75] on higher congruences between modular forms implies that for odd u and v, S_u and S_v are algebraically dependent over $\mathbf{F}_p$, because of their relation with the q-expansion of Eisenstein series.

As for the transcendence question, we have (for example) the following result: *If $c_p := \zeta(p)/\zeta(p-1)$ is an irrational real number (here ζ is the Riemann zeta function), and if $p - 1$ divides u, then S_u is transcendental over $k(q)$.* The proof uses again Rankin's result [Ran61] for the case where the number h defined above is odd. Here $h = 1$, and Rankin's result implies that, for some positive rational r,

$$\sharp\{n \le x,\ \sigma_u(n) \neq 0 \bmod p\} \sim (c_p r)x.$$

But from Cobham's theorem [Co72], if the sequence b_n is p-automatic and if the set $\{n,\ b_n = \alpha\}$ has a natural density, then this density must be a rational number.

(3) Watson proved in [Wat35] a conjecture of Ramanujan, stating that the Ramanujan τ function satisfies $\tau(n) = 0 \bmod 691$ for almost all n. Watson used the congruence $\tau(n) = \sigma_{11}(n) \bmod 691$. We can add a modest contribution to the study of the sequence $\tau(n)$ by proving, as above, that it is not 691-automatic.

Acknowledgements

This work was done when the first author visited the University of Arizona. The first author warmly thanks his colleagues for the very nice and fruitful time he spent there. We also thank Antonios Broumas and Bjorn Poonen for their comments.

References

[BDGP96] K. Barre-Sirieix, G. Diaz, F. Gramain, G. Philibert, *Une preuve de la conjecture de Mahler-Manin*, Invent. Math. **124** (1996), 1–9. MR **96j:**11103

[C79] G. Christol, *Ensembles presque-périodiques k-reconnaissables*, Theoret. Comput. Sci. **9** (1979), 141–145. MR **80e:**68141

[CKMR80] G. Christol, T. Kamae, M. Mendès France, G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France **108** (1980), 401–419. MR **82e:**10092

[Co72] A. Cobham, *Uniform tag sequences*, Math. Systems Theory **6** (1972), 164–192. MR **56:**15230

[K75] N. Katz, *Higher congruences between modular forms*, Ann. Math. **101** (1975), 332-367. MR **54:**5120

[R77] C. Radoux, *Divisibilité de $\sigma_k(n)$ par un nombre premier*, Séminaire Delange-Pisot-Poitou, Théorie des Nombres, 19e année, 1977/78, Exposé n° 3, (1978), 3-01–3-05. MR **80b:**10064

[Ran61] R. A. Rankin, *The divisibility of divisor functions*, Proc. Glasgow Math. Assoc. **5** (1961), 35–40. MR **26:**2407

[S-D73] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences of modular forms*, in: Modular functions of one variable III, Proc. Internat. Summer School, Univ. Antwerp 1972, Springer Lecture Notes in Math. **350** (1973), 1–55.

[T96] D. Thakur, *Automata-style proof of Voloch's result on transcendence*, J. Number Theory **58** (1996), 60–63. MR **98a:**11100

[V96] J. F. Voloch, *Transcendence of elliptic modular functions in characteristic p*, J. Number Theory **58** (1996), 55–59. MR **98a:**11099

[W96] M. Waldschmidt, *Sur la nature arithmétique des valeurs de fonctions modulaires*, Séminaire Bourbaki, 49^{e} année, vol. 1996–1997, exposé 824, Nov. 96, Paris, pp. 824-1–824-36.

[Wat35] G. N. Watson, *Über Ramanujansche Kongruenzeigenschaften der Zerfällungsanzahlen (I)*, Math. Z. **39** (1935), 712–731.

CNRS, LRI, Bâtiment 490, Université d'Orsay F-91405 Orsay Cedex, France
E-mail address: allouche@lri.fr

Department of Mathematics, University of Arizona, Tucson, Arizona 85721
E-mail address: thakur@math.arizona.edu