Contemporary Mathematics
Volume 210, 1998

Automata and Transcendence

DINESH S. THAKUR

Interesting quantities of number theory or geometry are often defined by analytic processes such as integration or infinite series or product expansions. A central question which transcendence theory addresses is whether they can also be described by simpler ('finite') algebraic methods; in particular, whether they turn out to be algebraic. For example, the most common analytic description of a number is by its infinite decimal or p-adic expansion and that of a function is by its power series expansion. It is well-known that any expansion that is eventually periodic represents a rational number (or a function). On the other hand, rational numbers and rational functions over a finite field give expansions that are eventually periodic.

More generally, we can ask for a similar, simple characterization of digit patterns for algebraic numbers or functions. We begin by describing an automata-theoretic criterion of discrete mathematics for this, and will prove three transcendence results in number theory as applications.

The first major advance in answering this general question was made by Furstenberg [F67]:

For $r = \sum r_{n_1,\cdots,n_k} x_1^{n_1} \cdots x_k^{n_k}$, define the 'diagonal' $Dr := \sum r_{n,\cdots,n} x^n$.

THEOREM 1. *For $k = \mathbb{C}$ or $\mathbb{F}_q$, the set of algebraic power series $f(x)$ over $k(x)$ is the same as the set of diagonals Dr of two-variable rational functions $r(x_1, x_2)$. The diagonal of a rational function of many variables over $\mathbb{F}_q$ (but not over $\mathbb{C}$) is algebraic.*

PROOF. : Over $\mathbb{C}$, for small ϵ and $|x|$, we have

$$Dr(x) = \frac{1}{2\pi i} \int_{|z|=\epsilon} r(z, \frac{x}{z}) \frac{dz}{z}.$$

1991 *Mathematics Subject Classification.* 11G07, 11R58; Secondary 11J89, 11B85, 11J91.
Key words and phrases. elliptic curve, gamma, function field.
This paper is in final form and no version of it will be submitted for publication elsewhere

Evaluating by residues gives an algebraic function. On the other hand, suppose f is algebraic, satisfying a polynomial equation $P(x, f(x)) = 0$. Also assume $f(0) = 0$ and that 0 is an isolated root of $P(0, w) = 0$, then expressing

$$f(x) = \int_\gamma w \frac{\partial P}{\partial w}(x, w)/P(x, w)dw$$

as an integral above, we see that f is a diagonal of a rational function. Also, if we have more than two variables, the resulting contour integration of an algebraic function of two variables is in general transcendental. Though this proof does not work over $\mathbb{F}_q$, the resulting formulae can be directly checked. □

Deligne [D84] generalized the last statement of the Theorem to algebraic functions of many variables.

From now on, we restrict to a coefficient field $\mathbb{F}_q$ of characteristic p.

COROLLARY 1. *(1) Algebraic power series are closed under Hadamard (term-by-term) product.*

(2) $\sum a_n x^n$ is algebraic if and only if $\sum_{a_n=a} x^n$ is algebraic for each $a \in \mathbb{F}_q$.

PROOF. : If $\sum a_n x^n = Dr_1(x_1, x_2)$, $\sum b_n x^n = Dr_2(x_1, x_2)$, then $\sum a_n b_n x^n = D(r_1(x_1, x_2)r_2(x_3, x_4))$. This implies (1). Then (2) follows from (1) by expanding out $\sum_{a_n=a} x^n = \sum(1 - (a_n - a)^{q-1})x^n$. □

By the Corollary, we can focus on characteristic sequences on subsets of natural numbers, i.e., on the series $\sum x^{n_i}$, if we wish. The main theorem giving the automata-theoretic criterion for algebraicity is the following theorem due to Christol [C79], [CKMR80]. In fact, the equivalence of the last two conditions (as well as another description in terms of substitutions) of the Theorem is due to Cobham [C072]. We sketch the proof later.

THEOREM 2. *(i) $\sum f_n x^n$ is algebraic over $\mathbb{F}_q(x)$ if and only if (ii) $f_n \in \mathbb{F}_q$ is produced by a q-automaton if and only if (iii) there are only finitely many subsequences of the form $f_{q^k n+r}$ with $0 \leq r < q^k$.*

Here, an m-automaton (we shall usually use $m = q$) consists of a finite set S of states, a table of how the digits base m operate on S, and a map τ from S to $\mathbb{F}_q$ (or some alphabet in general). For a given input n, fed in digit by digit from the left, each digit changing the state by the rule provided by the table, the output is $\tau(n\alpha)$ where α is some chosen initial state. For more details, see the expository article [A87].

Example: The following table, where $2 \leq i < p$, together with $\tau(\alpha) = \tau(\gamma) = 0$ and $\tau(\beta) = 1$ defines a p-automaton whose output f_n is the characteristic sequence of $\{p^m\}$, i.e., the numbers of the form $1000\cdots$ base p.

	α	β	γ
0	α	β	γ
1	β	γ	γ
i	γ	γ	γ

It is easy to see directly that $f := f(x) := \sum x^{p^n}$ satisfies $f^p - f + x = 0$, in accordance with Theorem 2. In fact, this f is Mahler's famous counterexample to the analogue of Roth's theorem in characteristic p. The partial sums to f approximate f with Liouville bounds.

From the proof of the first theorem, we find that $f = D(x_1/(1-(x_1^{p-1}+x_2)))$. We leave to the reader the interesting exercise of verifying this equation directly from the definition by expanding the right hand side via a geometric series, and proving the necessary divisibility properties of the binomial coefficients thus arising.

As a warm-up to the proof in the second application, we now prove that f is transcendental in finite characteristic $\ell \neq p$. Clearly, there are infinitely many k's such that $0 < p^m - \ell^k\mu < \ell^k$, for some m and some $0 < \mu < \ell$. So the subsequence $f_{\ell^k n+(p^m-\ell^k\mu)}$ assumes the value 1, for $n = \mu < \ell$. The next n for which it is 1 corresponds to $\ell^k n + (p^m - \ell^k\mu) = p^{m+w}$, with $w > 0$ the least such. So ℓ^k divides $p^w - 1$ and hence $n = \mu + p^m(p^w-1)/\ell^k > p^m \to \infty$ as k tends to ∞. Hence there are infinitely many such subsequences, and (iii) of Theorem 2 finishes the proof.

In fact, this is a special case of a very general result of Cobham [Co69]:

THEOREM 3. *Non-periodic sequences produced by m-automata cannot be produced by n-automata, if m and n are multiplicatively independent.*

We do not sketch the proof. To quote Eilenberg [E74], "The proof is correct, long and hard. It is a challenge to find a more reasonable proof of this fine theorem". See [BHMV94] for survey of other proofs based on logic.

Together with Theorem 2, this implies

COROLLARY 2. *If $\sum x^{n_i}$ is irrational and algebraic in one finite characteristic, then it is transcendental in all other finite characteristics.*

The natural question is whether corresponding real numbers, e.g. the decimal $\sum 10^{-n_i}$, are transcendental. For our example $f(x)$ above, instead of using the algebraicity equation $f(x)^p - f(x) + x = 0$, which is special to characteristic p, Mahler [M29] used the characteristic-free functional equation $f(x^p) - f(x) + x = 0$ and established (for $p = 2$) the transcendence of various values of $f(x)$. It implies the transcendence of real numbers $f(1/k) = \sum k^{-2^n}$, for any integral base $k > 1$. See [LP77] for a nice exposition of the proof of a more general result.

Loxton and van der Poorten generalized Mahler's method, but it should be noted here that the proof of the often quoted result of Loxton and van der Poorten that under the hypothesis of the Corollary, the real number $\sum 10^{-n_i}$

is transcendental, has a gap, as van der Poorten has mentioned to the author. Thus, this statement and similar p-adic statement remain as challenging open questions.

We now present an example due to Richie [Ri63], which we shall use, and which does not look as special as the first example.

THEOREM 4. *The characteristic sequence of the set of squares is not produced by any 2-automaton.*

PROOF. : Consider the 2-automaton given by the following table and $\tau(f) = 1$, $\tau(\text{rest}) = 0$.

	α	s_1	s_2	s_3	s_4	f	n
0	n	s_3	s_4	s_4	s_3	n	n
1	s_1	s_2	s_1	n	f	n	n

A straight entry chase in the table shows that this produces the characteristic function χ_A of the set $A = \{1^n 0^m 1 : n, m > 0, n+m \text{ odd}\}$. It is easy to see that the intersection of A with the set of squares is $B = \{1^n 0^{n+1} 1 : n > 0\}$ and also that in general, the intersection corresponds to the direct product of automata or the Hadamard product of series.

But χ_B can not be produced by a 2-automaton: As there are only a finite number of states, $1^\ell \alpha = 1^{\ell+m}\alpha$, for some ℓ, m. But $1^{\ell+m}0^{\ell+1}1$ is not in B whereas $1^\ell 0^{\ell+1} 1 \in B$. □

We finish this introduction by giving a very brief sketch of the ideas involved in the proof of Theorem 2. For more details, see [CKMR80] or [A87].

(ii) implies (iii): There are only finitely many possible maps $\beta : S \to S$ and any $f_{q^k n+r}$ is of the form $\tau(\beta(n\alpha))$.

(iii) implies (i): Let V be the vector space over $\mathbb{F}_q(x)$ generated by monomials in $\sum f_{q^k n+r} x^n$. Then V is finite dimensional with $fV \subset V$, so f satisfies its characteristic polynomial.

(i) implies (iii): For $0 \le r < q$, define C_r (twisted Cartier operators) by $C_r(\sum f_n x^n) = \sum f_{qn+r} x^n$. Considering the vector space over $\mathbb{F}_q$ generated by the roots of the polynomial satisfied by f, we can assume that $\sum_{i=0}^k a_i f^{q^i} = 0$, with $a_0 \neq 0$. Using $g = \sum_{r=0}^{q-1} x^r (C_r(g))^q$ and $C_r(g^q h) = gC_r(h)$, we see that

$$\{h \in \mathbb{F}_q((x)) : h = \sum_{i=0}^k h_i (f/a_0)^{q^i}, h_i \in \mathbb{F}_q[x], \deg h_i \le \max(\deg a_0, \deg a_i a_0^{q^{i-2}})\}$$

is a finite set containing f and stable under C_r's.

(iii) implies (ii): If there are m subsequences $f_n^{(i)}$ with $f_n^{(1)} = f_n$ say, put $S := \{\alpha := \alpha_1, \cdots, \alpha_m\}$. Define a digit action by, $r\alpha_i := \alpha_k$ if $f_{qn+r}^{(i)} = f_n^{(k)}$. Define $\tau(\alpha_i) := f_n$, if $n^- \alpha_1 = \alpha_i$ with n^- being the base q expansion of n written in the reverse order. □

Now we shall present three applications of Theorem 2 to Number Theory, where the quantities are not naturally presented as power series, but are convertible to manageable power series.

1. Application I

Let k be an algebraic closure of $\mathbb{F}_p$, q be a variable and let

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

THEOREM 5. *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 Theorem was proved by Voloch [V96] using Igusa theory and we provided another proof [T96a]. The Theorem can be considered as an analogue of the result of Siegel and Schneider on the transcendence of the period of elliptic curve (over a number field) over its field of definition. If, more appropriately, we consider q as the multiplicative version of the period, then it can be considered as an analogue of a conjecture of Mahler (in p-adic setting) and a conjecture of Manin (in the complex setting), as pointed out to us by Waldschmidt. These conjectures themselves were settled since then by Barre-Sirieix, Diaz, Gramain, Philibert [BDGP96]. In particular, they show that the '$\log_p q$' appearing in the p-adic Birch-Swinnerton-Dyer conjectures of Mazur, Tate and Teitelbaum (Theorem of Stevens/Greenberg) does not vanish, so that the order of vanishing is exactly as predicted in the conjectures.

PROOF. : First, let $p=2$. Then

$$a_4 = a_6 = \sum_{n\ odd\geq 1} q^n/(1-q^n) = \sum_{n\ odd\geq 1}\sum_{k=0}^{\infty} q^{kn} = \sum_{m=1}^{\infty} d_o(m)q^m,$$

where $d_o(m)$ = number of odd positive divisors of m. Hence, if $m = 2^k\prod p_i^{m_i}$, then $d_o(m) = \prod(m_i+1)$. So $d_o(m)$ is odd if and only if $m=n^2$ or $2n^2$. Hence, with $f := \sum q^{n^2}$ (essentially theta), we have

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

Now Theorems 2 and 4 imply that f and so $a_4 = a_6 = f+f^2$ is transcendental over $k(q)$, i.e., q is transcendental over $K = k(a_4)$, finishing the proof when $p=2$.

Now consider the case of general p. We will show:

(1) f is transcendental over $k(q)$: This follows from the generalization [E74] of the Theorem 4 to any base.

(2) a_4 and a_6 are algebraically dependent over k.

(3) f is algebraic over $k(\overline{a}_4, \overline{a}_6)$, where $\overline{a}_4 := a_4(q^2)$, $\overline{a}_6 := a_6(q^2)$.

It is easy to see that (1), (2) and (3) imply the Theorem.

Proof of (2): Elementary congruences show that $a_4 = a_6$ if $p = 2$, $a_4 = 0$ if $p = 5$ and $a_4 = 5a_6$ if $p = 7$.

Swinnerton-Dyer [S-D73] noticed that expressing the fact that the Hasse invariant of the Tate elliptic curve is one in terms of a_4 and a_6 gives (2) for $p > 3$.

For $p = 3$, the Hasse invariant is identically one and we do not get a relation this way. Nonetheless, we claim that $a_6 + a_4 + 2a_4^2 = 0$. In fact, $a_4 + a_6$ is

$$\sum_{n\equiv 2,4(9)} \frac{q^n}{1-q^n} + 2\sum_{n\equiv 5,7(9)} \frac{q^n}{1-q^n} = \sum_{n\not\equiv 0(3)} \frac{n+(-1)^{n-3\lfloor n/3\rfloor}}{3} \frac{q^n}{1-q^n} = a_4^2$$

The first two equalities follow by analyzing n modulo 9 and the last equality is a rearrangement of Ramanujan's identity (19) of [R16].

Proof of (3): Note that $\overline{a_4}$, $\overline{a_6}$, f are connected to the well-known Eisenstein series and theta function: $\theta = 1 + 2f$, $e_4 = 1 - 48\overline{a}_4$ and $e_6 = 1 - 72\overline{a}_4 + 864\overline{a}_6$.

We have the following explicit algebraic dependency relation between the three modular forms:

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

A straight translation to the original variables implies (3). □

2. Application II

Here we give an application to the transcendence of the gamma monomials (in the function field case) evaluated at fractions.

The most well-known classical result is : $\Gamma(1/2) = (-1/2)! = \sqrt{\pi}$. Chudnovsky [Chu84] showed that Γ values at proper fractions with denominator 4 or 6 are transcendental. This is basically all that is known about the transcendence of the individual gamma values at proper fractions.

We shall consider $A = \mathbb{F}_q[T]$, $K = \mathbb{F}_q(T)$, $K_\infty = \mathbb{F}_q((t))$ (with $t = 1/T$) and $\Omega =$ the completion of an algebraic closure of K_∞. These are analogues of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ respectively, in the theory of function fields.

The Carlitz factorial $\Pi(n) \in A$ for $n \in \mathbb{Z}_{\geq 0}$ is defined by

$$[n] := T^{q^n} - T, \; D_n := \prod_{k=1}^{n} [k]^{q^{n-k}}$$

$$\Pi(n) := \prod D_i^{n_i}, \text{ for } n = \sum n_i q^i, \; 0 \leq n_i < q.$$

David Goss noticed that

$$\overline{D_i} := \frac{D_i}{T^{\deg D_i}} = 1 - t^{q^i - q^{i-1}} + \text{higher degree terms} \to 1 \text{ as } i \to \infty$$

gives an interpolation: $\overline{\Pi}(n) \in K_\infty$ for $n \in \mathbb{Z}_p$ by

$$n! := \overline{\Pi}(n) := \prod \overline{D_i}^{n_i} \text{ for } n = \sum n_i q^i, \; 0 \leq n_i < q.$$

Why is this gamma function good? We mention some reasons as catch-phrases: analogous prime factorization, divisibility properties, analogous occurrence in the Taylor coefficients in the relevant exponential (of Carlitz-Drinfeld module), right functional equations, interpolations at finite primes and connection with Gauss sums (Gross-Koblitz type formula), and connection with periods (Chowla-Selberg type formula). See [T92] for details and references.

For our factorial $(-1/2)! = \sqrt{\tilde{\pi}}$, when $p \neq 2$, where $\tilde{\pi} \in \Omega$ is the period of the Carlitz-Drinfeld exponential (the analogue of $2\pi i \in \mathbb{C}$). This is known [W41] to be transcendental. See also [A90] for an automata-theoretic proof.

In fact, the correct analogue for classical $(-1/2)!$ is $(1/(1-q))!$, because 2 and $q-1$ are the number of roots of unity in $\mathbb{Z}$ and $\mathbb{F}_q[T]$, respectively. And the analogue of Chudnovsky's 4, 6 (which are numbers of roots of unity in quadratic imaginary fields) is q^2-1 (the number of roots of unity in $\mathbb{F}_{q^2}[T]$).

We have an analogue of the Chowla-Selberg formula for constant field extensions, expressing periods of Drinfeld modules with complex multiplication in terms of gamma values at particular fractions. Combining with their results on transcendence of periods, Jing Yu [Y92] and Thiery [Thi92] (by different techniques) proved that $(1/(1-q^2))!$ is transcendental. So far, the results are parallel in the classical and the function field case.

Using Christol's criterion, we proved [T96b] the transcendence of gamma values at rationals with any denominator, but with some restrictions on numerators. Using logarithmic derivatives on the product formula, which makes exponents relevant only modulo p, instead (a trick also used by L. Denis), Allouche [A96] then proved the transcendence for all values at fractions. Finally, we have shown how Allouche's technique, in fact, settles completely the question of which monomials in gamma values at fractions are algebraic and which are transcendental. Let us describe the result in detail and sketch the simplest case. For the full details and the history, we refer to [A96].

For a proper fraction f, let $\langle f \rangle$ denote its fractional part. For a finite formal sum $\underline{f} = \sum m_i[f_i]$, with $m_i \in \mathbb{Z}$ and $f_i \in \mathbb{Q}$, put $m(f) = \sum m_i \langle -f_i \rangle$ and $\Gamma(\underline{f}) = \prod \Gamma(f_i)^{m_i}$. Also, for $\sigma \in \mathbb{Z}$, put $\underline{f}^{(\sigma)} = \sum m_i [f_i \sigma]$

Let $\underline{f}$ be given, with all f_i's having a common denominator, say N.

THEOREM 6. *(Usual Gamma) If $m(\underline{f}^{(\sigma)}) = 0$ for all σ relatively prime to N, then $\Gamma(\underline{f})$ is algebraic.*

The way we have presented it, this was conjectured (together with Galois action) by Deligne [D79] (proved in [D82]). But using the ideas of Lang and Kubert on distributions, it was shown in the appendix by Koblitz and Ogus to [D79] that the algebraicity also follows by taking the correct combinations of multiplication and reflection formulae. The converse is not known, but is conjectured, because it follows from the general belief that functional equations force all the relations and also from conjectures [D82] in algebraic geometry.

THEOREM 7. *(Our case)* $m(\underline{f}^{(\sigma)}) = 0$ *for all* $\sigma = q^j$ *if and only if* $\Gamma(\underline{f})$ *is algebraic.*

The conditions of the two theorems are analogous, since the Galois group in the relevant cyclotomic theory is $(\mathbb{Z}/N\mathbb{Z})^* = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ in the classical case and $\mathrm{Gal}(\mathbb{F}_q(T)(\zeta_k)/\mathbb{F}_q(T))$ (generated by q-power Frobenius) in our case. In our case, the monomials are not obtained by combinations of naive analogues of multiplication and reflection formulae, but the 'only if' part was proved directly [T91] by showing that in the multiplicative basis of factorials of $1/(1-q^i)$ our monomial turns out to be a trivial monomial. Automata theory takes care of the converse, as mentioned above. We explain the simplest case below:

Claim: $(1/(1-q^\mu))!$ is transcendental.

PROOF. : After some simple manipulations, we get

$$P := (\frac{1}{1-q^\mu})!^{1-q^\mu} = \prod_{i=1}^{\infty}\prod_{j=0}^{\mu-1}(1-t^{q^{\mu i}-q^j})$$

Write $P = \sum a_n t^n$ and use Christol's criterion (Theorem 2).

Consider the representations

$$n = \sum (q^{\mu i} - q^j), \quad \text{all terms distinct, } 0 \le j < \mu.$$

If such a representation is impossible, then $a_n = 0$, whereas if such a representation is unique (not always the case), then $a_n = \pm 1$. (In a special case, when the representations are always unique, a different type of proof for the next claim is given in [A90]).

Claim: There are infinitely many subsequences of the form $b_n := a_{q^k n+(q^k-k)} = a_{q^k(n+1)-k}$. (Hence P is transcendental).

An imbalance between what $q^{\mu i}$'s can add up to and what q^j's can subtract makes it impossible to have representations of $q^k(n+1)-k$ of the required form, for at least the first $k/q^{\mu-1}-1$ values of n, if k is sufficiently large. This implies that for sufficiently large k, b_n is 0 for at least the first $k/q^{\mu-1}-1$ values of n. Since $k/q^{\mu-1}-1 \to \infty$ as $k \to \infty$, to show that there are infinitely many distinct subsequences (b_n), it is enough to show that infinitely many of these subsequences are not identically zero.

Let $m := k/q^{\mu-1}-1$ and $n := q^\mu + q^{2\mu} + \cdots + q^{m\mu}$. Then

$$q^k(n+1) - k = (q^k - q^{\mu-1}) + (q^{k+\mu} - q^{\mu-1}) + \cdots + (q^{k+m\mu} - q^{\mu-1})$$

is the unique representation of the form required, and so $b_n = \pm 1 \neq 0$. □

Since then another proof of this case has been given by Hellegouarch [H95], using de Mathan's criterion [Ma95] instead. Note also that Koskas [K95] has given an automata-theoretic proof of de Mathan's criterion.

In fact, there is another gamma function in function field theory, and a breakthrough in establishing the transcendence of its values at proper fractions has been recently achieved by S. Sinha [S95], using Anderson's theory of t- motives and solitons, in particular. The proof expresses the gamma values as periods on analogues of Fermat Jacobians in the setting of t- motives and uses Jing Yu's transcendence results for this. In a sense the reason why we can do better than the classical case by similar (philosophically!) methods is that in the setting of Drinfeld modules and t- motives, we can have arbitrary fractions (and not just half integers) as 'weights'.

3. Application III

Recently, using the automata-theoretic techniques, as well as the logarithmic differentiation trick used in Allouche's proof, Mendès France and Yao gave a very nice proof [MY] proving that $n! = \overline{\Pi}(n)$ is transcendental for all $n \in \mathbb{Z}_p - \mathbb{Z}_{\geq 0}$. This settles the question of the transcendence of the values of $\overline{\Pi}(n)$ completely, as it is easy to see that $\overline{\Pi}(n) \in K$ if $n \in \mathbb{Z}_{\geq 0}$.

We cannot expect to have analogous result for the classical gamma function, because its domain and range are archimedean, and continuity is a quite strong condition in the classical case. In other words, a non-constant continuous real valued function on an interval cannot fail to take on algebraic values. Since, as we have seen above, the values at proper fractions are expected to be transcendental, many values at irrationals should be algebraic.

Morita's p-adic gamma function has domain and range $\mathbb{Z}_p$, which being non-archimedean is closer to our situation. In fact, let us also look at interpolation of $\Pi(n)$ at a finite prime v of $A = \mathbb{F}_q[T]$:

Carlitz showed that D_i is the product of all monic polynomials in A of degree i. Following Morita's idea of throwing out terms divisible by p, David Goss defined $D_{i,v}$ to be the product of all monic polynomials of degree i, which are not divisible by v. He showed (an analogue of Wilson-type theorem) that $-D_{i,v}$ approaches 1 as i tends to infinity and defined $\Pi_v(n) \in A_v$ for $n \in \mathbb{Z}_p$ by

$$\Pi_v(n) = \prod(-D_{i,v})^{n_i}, \text{ for } n = \sum n_i q^i, \ 0 \leq n_i < q.$$

We refer to [T92] and references there for several properties of this interpolation, as well as a discussion of the transcendence question at fractions.

In particular, we have proved that if d is the degree of v, then $\Pi_v(1/(1-q^d))$ is algebraic (connected to function field Gauss sums).

As our third application of the automaton method, we will prove

THEOREM 8. *If v is a prime of degree* 1, *then $\alpha_k := \Pi_v(1/(1-q^k)) \in A_v$ is transcendental for all $k > 1$.*

Before we begin the proof, let us give direct proofs of some results quoted above, in the case where v is of degree one. Using the automorphism sending T to $T + \theta$, $\theta \in \mathbb{F}_q$, we can assume without loss of generality that $v = T$. Now, for a general monic prime v of degree d, we have $D_{i,v} = D_i/v^w D_{i-d}$, where w is such that $D_{i,v}$ is a unit at v. So in our case,

$$-D_{n,T} = \left(\prod_{i=0}^{n-1}(1 - T^{q^n - q^i})\right)/\left(\prod_{i=0}^{n-2}(1 - T^{q^{n-1}-q^i})\right) \to 1, \text{ as } n \to \infty$$

and

$$\Pi_T\left(\frac{1}{1-q}\right) = \lim \prod_{i=0}^{N} -D_{i,T} = -\lim \prod_{j=0}^{N-1}(1 - T^{q^N - q^j}) = -1$$

because the product telescopes after the first term $-D_{0,T} = -1$.

Proof of the theorem . We have

$$-\alpha_k = \lim \prod_{i=1}^{N} -D_{ki,T} = \prod_{i=1}^{N} \prod_{0 \le j < ki} (1 - T^{q^{ki} - q^j}) / \prod_{0 \le j < ki-1} (1 - T^{q^{ki-1} - q^j})$$

Notice that the logarithmic derivative with respect to T of $1 - T^{q^i - q^j}$, when $i > j \ge 0$, is $-(q^i - q^j)T^{q^i - q^j - 1}/(1 - T^{q^i - q^j}) = \delta_{j0} T^{q^i - 2}/(1 - T^{q^i - 1})$. Hence we have

$$T\frac{\alpha_k'}{\alpha_k} = \sum \frac{T^{q^{ki}-1}}{1 - T^{q^{ki}-1}} - \sum \frac{T^{q^{ki-1}-1}}{1 - T^{q^{ki-1}-1}} = \sum c(n) T^n$$

where $c(n)$ is the number of divisors of n of the form $q^{ki} - 1$ minus the number of divisors of the form $q^{ki-1} - 1$, as we can see by expanding the sums above in geometric series. We shall show using Theorem 2 that $T\alpha_k'/\alpha_k$ is transcendental, which is enough to prove the Theorem.

Let us first do the simplest case: $p = k = 2$. Then $c(n)$ is just the number of divisors of n of the form $q^i - 1$. Note that $q^i - 1$ divides $q^j - 1$ if and only if i divides j. Let $\mathcal{P}$ be the set of primes. Since this is an infinite set, by the Theorem 2, it is enough to show that if $p_1, p_2 \in \mathcal{P}$, $p_1 > p_2$, then the subsequences c_{p_1} and c_{p_2} are distinct, where we define $c_a(n) := c(q^a n + q^a - 1)$. Let n be so large that $n^2 - (p_1 - p_2)$ is not a square and put $u = n^2 - p_1$. Then we claim that $c_{p_1}(q^u - 1) \neq c_{p_2}(q^u - 1)$. The left hand side is $c(q^{n^2} - 1)$, which is the number of divisors of n^2 and hence odd (equals one, since $p = 2$), whereas the right hand side is $c(q^{n^2 - (p_1 - p_2)} - 1)$, which is the number of divisors of the non-square $n^2 - (p_1 - p_2)$ and hence even. This finishes the proof of the simplest case.

To do the general case, we use lemma 1 of [MY], which states that for positive integers a, b, c; $q^c - 1$ divides $q^a(q^b - 2) + 1$ if and only if c divides (a, b), the greatest common divisor of a and b. We do not repeat the proof, which is an elementary exercise in divisibility.

First we assume that $k > 2$. Let S be the set of primes which are not congruent to -1 modulo k and which are greater than k. By Dirichlet's theorem, S is infinite, so it is enough to show that if $p_1 > p_2$ are members of S, then the subsequences C_{kp_1} and C_{kp_2} are distinct, where we define $C_a(n) := c(q^a n + 1)$. In fact, we claim that $C_{kp_1}(q^{kp_2} - 2) \neq C_{kp_2}(q^{kp_2} - 2)$. The left hand side is

$c(q^{kp_1}(q^{kp_2}-2)+1)$, which equals, by the lemma quoted above, the number of divisors of k of the form ki minus the number of divisors of k that are congruent to -1 modulo k, and so is $1-0=1$. On the other hand, the right hand side is $c(q^{kp_2}(q^{kp_2}-2)+1)$, which equals, again by the lemma quoted above, the number of divisors of kp_2 of the form ki minus the number of divisors of kp_2 that are congruent to -1 modulo k, and so is $2-0=2$. This establishes the claim and finishes the case, when $k>2$.

Finally, we settle the remaining case $k=2$. As before, it is enough to show that if $p_1, p_2 \in \mathcal{P}$ and $p_1 > p_2 > 2$, then $C_{p_1}(q^{p_1}-2) \neq C_{p_2}(q^{p_1}-2)$. The left hand side is the number of even divisors of p_1 minus the number of odd divisors of p_1 and so is $0-2=-2$, whereas the right hand side is the number of even divisors of 1 minus the number of odd divisors of 1 and so is $0-1=-1$. □

The referee has pointed out that the proof could have been made shorter (but less self-contained) by appealing to Theorem 3 of [MY], which says that for a sequence $n_j \in \mathbb{F}_q$ which is not ultimately zero, $\sum_{j=1}^{\infty} n_j/(x^{q^j}-x) \in \mathbb{F}_q((1/x))$ is transcendental over $\mathbb{F}_q(x)$. With $T=1/x$ and with n_j being 1, -1 or 0 depending on whether j is congruent to 0, 1 modulo k or otherwise, we immediately get the transcendence of $T\alpha_k'/\alpha_k$.

In fact, by a similar argument, Yao has recently proved (private communication) that with $0 \le n_j < q$, and for v of degree one, $\Pi_v(\sum n_j q^j)$ is transcendental if (and only if, by the results quoted above) n_j is not ultimately constant.

The author would be grateful to learn about any progress by the reader on these questions or related questions of transcendence of gamma or zeta values for rational function fields or higher genus function fields, by automata-theoretic or other methods. For the results on the zeta values, the reader should look at [Y92], [B94], [B95] and the references there.

What should be the implications for the Morita's p-adic gamma function? As explained in [T92], the close connection to cyclotomy leads us to think that the situation for values at proper fractions should be parallel. But then this implies that the algebraic values in the image not taken at fractions (conjecturally (see [T92]) the only algebraic values at fractions arise at fractions with denominators dividing $p-1$, and we know these values by the Gross-Koblitz theorem and functional equations) should be taken at irrational p-adic integers. Thus we do not expect a Mendès France-Yao type result for Morita's p-adic gamma function, but it may be possible to have such a result for Π_v's. This breakdown of analogies seems to be due to an important difference: in the function field situation, the range is a 'huge' finite characteristic field of Laurent series over a finite field, and the resulting big difference in the function theory prevents analogies being as strong for non-fractions.

Acknowledgements: The portion of the paper before the third application is based on the talk given at the International Conference on Discrete Mathematics and Number Theory, January 96. I thank the organizers from the Ramanujan

Mathematical Society, as well as the Number Theory session organizers Kumar Murty and Michel Waldschmidt. I am obliged to Jean-Paul Allouche for pointing out several related references, and to the referee and Robert Maier for correcting several mistakes related to grammar and style. I am also grateful to the Vaughn Foundation and the University of Arizona for the travel support.

References

[A87] Allouche J. -P. - Automates finis en théorie des nombres, Expo. Math. 5 (1987), 239-266.

[A90] Allouche J. -P. - Sur la transcendance de la série formelle Π, Séminaire de Théorie des Nombres, Bordeaux 2 (1990), 103-117.

[A96] Allouche J. -P. - Transcendence of the Carlitz-Goss gamma function at rational arguments, J. Number Theory 60 (1996), 318-328.

[BDGP96] Barre-Sirieix, Diaz, Gramain, Philibert - Une Preuve de la conjecture de Mahler-Manin, Invent. Math. 124 (1996), 1-9.

[B94] Berthé V. - Automates et valeurs de transcendance du logarithme de Carlitz, Acta Arith. 66 (1994), 369-390.

[B95] Berthé V. - Combinaisons linéaires de $\zeta(s)/\Pi^s$ sur $\mathbb{F}_q(x)$, pour $1 \leq s \leq q-2$, J. Number Theory 53 (1995), 272-299.

[BHMV94] Bruyère V., Hansel G., Michaux C., Villemaire R. - Logic and p-recognizable sets of integers, Bull. Belg. Math. Soc. 1 (1994), 191-238. (Corrigendum pp. 577)

[C79] Christol G. - Ensembles presque periodiques k-reconnaissables, Theoretical Computer Science, t. 9 (1979), 141-145.

[CKMR80] Christol G., Kamae T., Mendes-France M., Rauzy G. - Suites algebriques, automates et substitutions, Bull. Soc. Math. France. 108 (1980) 401-419.

[Chu84] Chudnovsky G. - Contributions to the Theory of transcendental Numbers, Mathematical surveys and monographs, no. 19, (1984), American Math. Soc. , Providence.

[Co69] Cobham A. - On the base-dependence of sets of numbers recognizable by finite automata, Math. Systems theory, 3 (1969), 186-192.

[Co72] Cobham A. - Uniform tag sequences, Math. Systems theory, 6 (1972), 164-192.

[D79] Deligne P. - Valeurs de fonctions L, in Proc. Symp. Pure Math. 33 (1979), 313-346.

[D82] Deligne P. - Hodge cycles on Abelian varieties, in Lecture Notes in Math. 900 (1982).

[D84] Deligne P. - Intégration sur un cycle évanescent, Invent. Math., 76 (1984), 129-143.

[E74] Eilenberg S. - Automata, Languages and machines, vol. A, Academic Press, New York, 1974.

[F67] Furstenberg H. - Algebraic functions over finite fields, J. of Algebra 7 (1967), 271-277.

[GHR92] Goss D., Hayes D., Rosen M. (Ed.) - The Arithmetic of Function Fields, Walter de Gruyter, Berlin, NY 1992.

[H95] Hellegouarch Y. - Une généralisation d'un critére de DeMathan, C. R. Acad. Sci. Paris, t. 321, I (1995), 677-680.

[K95] Koskas M. - Une démonstration par automates d'un critère de transcendance, Thèse, Université de Bordeaux, Chapter III (1995).

[LP77] Loxton J.H. and van der Poorten - Transcendence and algebraic independence by a method of Mahler, pp. 211-226 in Transcendence theory: Advances and applications, Edited by Baker A. and Masser D. W. , Academic Press (1977), London.

[M29] Mahler K. - Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen, Math. Ann. 101 (1929), 342-366.

[Ma95] de Mathan B. - Irrationality measures and transcendence in positive characteristic, J. Number Theory 54 (1995), 93-112.

[MY] Mendès France M. and Yao J. - Transcendence of the Carlitz-Goss Gamma function, To appear in J. Number Theory.

[R16] Ramanujan S. - On certain arithmetical functions, Trans. Cambridge Phil. Soc.

XXII no. 9, 1916, 159-184. Also, paper 18 in Collected Papers of Srinivasa Ramanujan, Ed. by Hardy G. H. et al, Chelsea Pub. Co. , NY 1962.

[Ri63] Ritchie R. - Finite automata and the set of squares, J. Assoc. Comput. Mach. 10 (1963), 528-531.

[S95] Sinha S. - Periods of t- motives and special functions in characteristic p, Ph.D. thesis, U. of Minnesota, (1995).

[S-D73] Swinnerton-Dyer H. P. F. - On l-adic representations and congruences of modular forms, Springer LNM 350 (1973), 1-55.

[T91] Thakur D. - Gamma function for function fields and Drinfeld modules, Ann. Math. 134 (1991), 25-64.

[T92] Thakur D. - On Gamma functions for function fields, in [GHR] (1992), 75-86.

[T96a] Thakur D. - Automata-style proof of Voloch's result on Transcendence, J. Number Theory, 58 (1996), 60-63.

[T96b] Thakur D. - Transcendence of Gamma values for $\mathbb{F}_q[T]$, Ann. Math. 144 (1996), 181-188.

[Thi92] Thiery A. - Indépendance algébrique des périodes et quasi-périodes d'un module de Drinfeld, in [GHR] (1992), 265-284.

[V96] Voloch J. F. - Transcendence of elliptic modular functions in characteristic p, J. Number Theory, 58 (1996), 55-59.

[W41] Wade L. - Certain quantities transcendental over $GF(p^n, x)$, Duke Math. J. 8 (1941), 701-720.

[Y92] Yu J. - Transcendence in finite characteristic, in [GHR] (1992), 253-264.

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