ACTA ARITHMETICA
156.3 (2012)

Transcendence of the Artin–Mazur zeta function for polynomial maps of $\mathbb{A}^1(\overline{\mathbb{F}}_p)$

by

ANDREW BRIDY (Madison, WI)

1. Definitions and preliminaries. In the study of dynamical systems the Artin–Mazur zeta function is the generating function for counting periodic points. For any set X and map $f : X \to X$ it is a formal power series defined by

$$\zeta_f(X;t) = \exp\biggl(\sum_{n=1}^{\infty} \#(\mathrm{Fix}(f^n))\frac{t^n}{n}\biggr). \tag{1}$$

We use the convention that f^n means f composed with itself n times, and that $\mathrm{Fix}(f^n)$ denotes the set of fixed points of f^n. For $\zeta_f(X;t)$ to make sense as a formal power series we assume that $\#(\mathrm{Fix}(f^n)) < \infty$ for all n. The zeta function is also represented by the product formula

$$\zeta_f(X;t) = \prod_{x\in \mathrm{Per}(f,X)} (1 - t^{p(x)})^{-1}$$

where $\mathrm{Per}(f, X)$ is the set of periodic points of f in X and $p(x)$ is the least positive n such that $f^n(x) = x$. This function was introduced by Artin and Mazur in the case where X is a manifold and $f : X \to X$ is a diffeomorphism [AM]. In this context $\zeta_f(X;t)$ is proved to be a rational function for certain classes of diffeomorphisms (e.g. [G, M]). This shows that in these cases the growth of $\#(\mathrm{Fix}(f^n))$ is determined by the finitely many zeros and poles of ζ_f. From this point onward we make the definition

$$a_n = \#(\mathrm{Fix}(f^n))$$

for economy of notation.

We are interested in the rationality of the zeta function in an algebraic context, motivated by the following example.

2010 *Mathematics Subject Classification*: Primary 37P05; Secondary 11B85.
Key words and phrases: arithmetic dynamics, automatic sequences, finite fields.

DOI: 10.4064/aa156-3-6

Example. Let X be a variety over $\mathbb{F}_p$ and let $f : X \to X$ be the Frobenius map, i.e. the pth power map on coordinates. Then $\mathrm{Fix}(f^n)$ is exactly the set of $\mathbb{F}_{p^n}$-valued points of X. Therefore $\zeta_f(X;t)$ is the Hasse–Weil zeta function of X, and is rational by Dwork's theorem [D].

We study a simple, yet interesting case: fix a prime p and let $X = \mathbb{A}^1_{\overline{\mathbb{F}}_p}$, the affine line over $\mathbb{F}_p$. Let $f \in \overline{\mathbb{F}}_p[x]$, let $d = \deg f$, and assume that $d \geq 2$. Consider the dynamical system defined by f as a self-map of $\mathbb{A}^1(\overline{\mathbb{F}}_p)$. The points in $\mathrm{Fix}(f^n)$ are the roots in $\overline{\mathbb{F}}_p$ of the degree d^n polynomial $f^n(x) - x$ counted *without multiplicity*, so $a_n \leq d^n$. If we consider $\zeta_f(t)$ as a function of a complex variable t, it converges to a holomorphic function on $\mathbb{C}$ in a disc around the origin of radius d^{-1} (however, it is not clear that d^{-1} is the largest radius of convergence). Our motivating question is:

Question 1. *For which $f \in \overline{\mathbb{F}}_p[x]$ is $\zeta_f(\overline{\mathbb{F}}_p;t)$ a rational function?*

If we count periodic points with multiplicity, then $a_n = d^n$ for all n and Question 1 becomes completely trivial by the calculation

$$\zeta_f(\overline{\mathbb{F}}_p;t) = \exp\left(\sum_{n=1}^{\infty} \frac{d^n t^n}{n}\right) = \exp(-\log(1-dt)) = \frac{1}{1-dt}, \tag{2}$$

so we count each periodic point only once. A partial answer to our question is given by the following two theorems, which show that for some simple choices of f, ζ_f is not only irrational, but also not algebraic over $\mathbb{Q}(t)$.

Theorem 1. *If $f \in \overline{\mathbb{F}}_p[x^p]$, then $\zeta_f(\overline{\mathbb{F}}_p,t) \in \mathbb{Q}(t)$. In particular, if $p \mid m$, then $\zeta_{x^m}(\overline{\mathbb{F}}_p;t) \in \mathbb{Q}(t)$. If $p \nmid m$, then $\zeta_{x^m}(\overline{\mathbb{F}}_p;t)$ is transcendental over $\mathbb{Q}(t)$.*

Theorem 2. *If $a \in \mathbb{F}_{p^m}^\times$, with p odd and m any positive integer, then $\zeta_{x^{p^m}+ax}(\overline{\mathbb{F}}_p;t)$ is transcendental over $\mathbb{Q}(t)$.*

Our strategy of proof depends heavily on the following two theorems. Their proofs, as well as a good introduction to the theory of finite automata and automatic sequences, can be found in [AS].

Theorem 3 (Christol). *The formal power series $\sum_{n=0}^{\infty} b_n t^n$ in the ring $\mathbb{F}_p[[t]]$ is algebraic over $\mathbb{F}_p(t)$ iff its coefficient sequence $\{b_n\}$ is p-automatic.*

Theorem 4 (Cobham). *For p, q multiplicatively independent positive integers (i.e. $\log p/\log q \notin \mathbb{Q}$), the sequence $\{b_n\}$ is both p-automatic and q-automatic iff it is eventually periodic.*

The following is an easy corollary to Christol's theorem which we will use repeatedly [AS, Theorem 12.6.1].

Corollary 5. *If $\sum_{n=0}^{\infty} b_n t^n \in \mathbb{Z}[[t]]$ is algebraic over $\mathbb{Q}(t)$, then the reduction of $\{b_n\}$ modulo p is p-automatic for every prime p.*

We note that Corollary 5 will be applied to the logarithmic derivative $\zeta_f'/\zeta_f = \sum_{n=1}^{\infty} a_n t^{n-1}$, rather than to ζ_f.

Throughout this paper we use v_p to mean the usual p-adic valuation, that is, $v_p(a/b) = \mathrm{ord}_p(b) - \mathrm{ord}_p(a)$. We use $(n)_p$ as in [AS] to signify the base-p representation of the integer n, and we denote the multiplicative order of a modulo n by $o(a, n)$, assuming that a and n are coprime integers.

2. Proof of Theorem 1. Let $f(x) \in \overline{\mathbb{F}}_p[x^p]$, so that $f'(x) = 0$ identically. Then $f^n(x) - x$ has derivative $(f^n(x) - x)' = -1$, so it has distinct roots over $\overline{\mathbb{F}}_p$. Therefore $a_n = (\deg f)^n$ and $\zeta_f(\overline{\mathbb{F}}_p, t)$ is rational as in (2).

Now suppose $f(x) = x^m$ where $p \nmid m$. Assume by way of contradiction that ζ_f is algebraic over $\mathbb{Q}(t)$. The derivative $\zeta_f' = d\zeta_f/dt$ is algebraic, which can be shown by writing the polynomial equation that ζ_f satisfies and applying implicit differentiation. Hence ζ_f'/ζ_f is algebraic. We have

$$\zeta_f'/\zeta_f = (\log \zeta_f)' = \sum_{n=1}^{\infty} a_n t^{n-1},$$

so in particular $\zeta_f'/\zeta_f \in \mathbb{Z}[[t]]$. By Corollary 5, for every prime q the reduced sequence $\{a_n\}$ mod q is q-automatic.

First we count the roots of $f^n(x) - x = x^{m^n} - x = x(x^{m^n - 1} - 1)$ in $\overline{\mathbb{F}}_p$. There is one root at zero, and we write $m^n - 1 = p^a b$, where $p \nmid b$, so

$$x^{m^n-1} - 1 = x^{p^a b} - 1 = (x^b - 1)^{p^a}.$$

The polynomial $x^b - 1$ has derivative bx^{b-1}, and $(x^b - 1, bx^{b-1}) = 1$, so $x^b - 1$ has exactly b roots in $\overline{\mathbb{F}}_p$, as does $x^{m^n} - 1$. Therefore

$$a_n = 1 + \frac{m^n - 1}{p^{v_p(m^n-1)}}. \tag{3}$$

Now we need to reduce modulo some carefully chosen prime q. There are two cases to consider, depending on whether $p = 2$.

Case 1. If $p = 2$, let q be a prime dividing m, $q \neq 2$. There is such a prime because $m > 1$ and $2 \nmid m$. Let $r = 2^{-1}$ in $\mathbb{F}_q$. Reducing modulo q,

$$a_n = 1 + \frac{m^n - 1}{2^{v_2(m^n-1)}} \equiv 1 - r^{v_2(m^n-1)} \pmod{q}. \tag{4}$$

The subsequence $\{a_{2n}\}$ reduced modulo q is q-automatic because subsequences of automatic sequences indexed by arithmetic progressions are automatic [AS, Theorem 6.8.1]. We define the sequence $\{b_n\}$ as

$$b_n = -(a_{2n} - 1).$$

Then $\{b_n\}$ is q-automatic, because subtracting 1 and multiplying by -1 simply permute the elements of $\mathbb{F}_q$. We have $b_n = r^{v_2(m^{2n}-1)}$ by (4). To proceed, we need the following proposition.

Proposition 6.

(i) *For any $n, m \in \mathbb{N}$, m odd,*

$$v_2(m^{2n} - 1) = v_2(n) + v_2(m^2 - 1).$$

(ii) *If p is an odd prime and $n, m \in \mathbb{N}$, $p \nmid m$, then*

$$v_p(m^{(p-1)n} - 1) = v_p(n) + v_p(m^{p-1} - 1).$$

Proof. The proof is an elementary consequence of the structure of the unit group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ (see for example [L]), and is omitted. ∎

By Proposition 6,

$$b_n = r^{v_2(n) + v_2(m^2-1)}. \tag{5}$$

Let $d = o(r, q)$, the multiplicative order of r in $\mathbb{F}_q$, and note that $d > 1$ because $r \neq 1$. We see that b_n is a function of $v_2(n)$ reduced modulo d, and $v_2(n)$ is simply the number of leading zeros of $(n)_2$ (if we read the least significant digit first).

Lemma 7. *If β_n is a function of the equivalence class mod d of $v_p(n)$, then the sequence $\{\beta_n\}$ is p-automatic.*

Proof. We can build a finite automaton (with output) whose output depends on the equivalence class modulo d of the number of initial zeros of a string, as in Figure 1 for $d = 4$. There are d states arranged in a circle

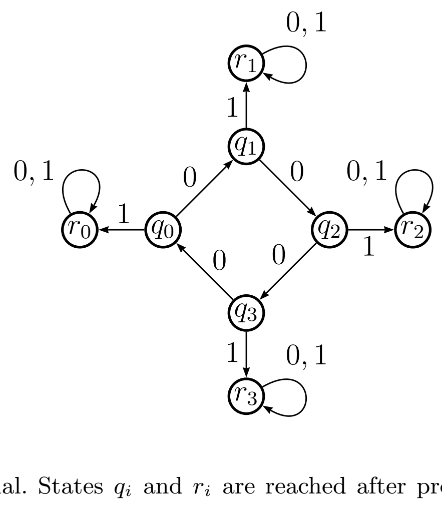

Fig. 1. State q_0 is initial. States q_i and r_i are reached after processing $i \bmod 4$ leading zeros.

(the q_i in the figure), reading a zero moves from one of these states to the next, and reading any other symbol moves to a final state (the r_i) marked with the corresponding output. Therefore $\{\beta_n\}$ is p-automatic. ∎

By Lemma 7, $\{b_n\}$ is 2-automatic. It is also q-automatic, so by Cobham's theorem, $\{b_n\}$ is eventually periodic of period k. For some large n, we have $b_{nk} = b_{nk+k} = b_{nk+2k} = \cdots = b_{(n+a)k}$ for any positive integer a. This means that $b_{Nk} = b_{nk}$ for all $N > n$. By (5),

$$r^{v_2(Nk)+v_2(m^2-1)} = r^{v_2(nk)+v_2(m^2-1)}$$

which means $v_2(Nk) \equiv v_2(nk) \pmod{d}$ and so $v_2(N) \equiv v_2(n) \pmod{d}$ for all $N > n$. This is a contradiction, as $d > 1$.

Case 2. If $p > 2$, we pick some prime $q > m^{p-1}$ such that $q \not\equiv 1 \pmod{p}$ (for example we can choose $q \equiv 2 \pmod{p}$ by Dirichlet's theorem on primes in arithmetic progressions). Clearly $q \nmid m$, so $m^{q-1} \equiv 1 \pmod{q}$. Let $r = p^{-1}$ in $\mathbb{F}_q$. The sequence $\{a_n\}$ is as in (3). We take the subsequence $a_{(p-1)((q-1)n+1)}$ and reduce it modulo q. The reduced subsequence is q-automatic. We compute

$$\begin{aligned} a_{(p-1)((q-1)n+1)} &= 1 + \frac{m^{(p-1)((q-1)n+1)} - 1}{p^{v_p(m^{(p-1)((q-1)n+1)}-1)}} = 1 + \frac{(m^{q-1})^{(p-1)n} m^{p-1} - 1}{p^{v_p(m^{(p-1)((q-1)n+1)}-1)}} \\ &\equiv 1 + (m^{p-1} - 1) r^{v_p(m^{(p-1)((q-1)n+1)}-1)} \pmod{q}. \end{aligned}$$

As $m^{p-1} - 1 < q$ we can invert $m^{p-1} - 1$ modulo q. If we subtract 1 and multiply by $(m^{p-1} - 1)^{-1}$ as in Case 1, we get

$$b_n = r^{v_p(m^{(p-1)((q-1)n+1)}-1)},$$

which is q-automatic.

By Proposition 6, $b_n = r^{v_p((q-1)n+1)+v_p(m^{p-1}-1)}$. Let $d = o(r, q)$, noting that $d > 1$. Let

$$Y = \{n \in \mathbb{N} : v_p((q-1)n + 1) \equiv 0 \pmod{d}\}.$$

Then Y is the fiber of $\{b_n\}$ over $r^{v_p(m^{p-1}-1)}$ and is therefore a q-automatic set (i.e. its characteristic sequence is q-automatic). We argue that Y is p-automatic.

Consider a finite-state transducer T on strings over $\{0, \ldots, p-1\}$ such that $T((n)_p) = ((q-1)n + 1)_p$. On strings with no leading zeros, T is one-to-one. Let L be the set of base-p strings $(n)_p$ such that $n \in Y$. Then

$$T(L) = \{(n)_p : n \equiv 1 \pmod{q-1} \text{ and } v_p(n) \equiv 0 \pmod{d}\}.$$

We observe that $T(L)$ is a regular language, as both of its defining conditions can be recognized by a finite automaton (for the second condition, this follows from Lemma 7). Therefore $T^{-1}(T(L)) = L$ is regular, that is, the characteristic sequence of Y is p-automatic. We use Cobham's theorem again to conclude that the characteristic sequence of Y is eventually periodic.

Let $\{y_n\}$ be the characteristic sequence of Y:

$$y_n = \begin{cases} 1, & n \in Y, \\ 0, & n \notin Y, \end{cases}$$

and let k be its (eventual) period. Write k as $k = Mp^N$, where $p \nmid M$ (it is possible that $N = 0$). As $q \not\equiv 1 \pmod p$, $q-1$ is invertible modulo p-powers, so we can solve the following equation for n:

$$(q-1)n \equiv -1 + p^{dN} \pmod{p^{dN+2}}. \tag{6}$$

Any n that solves this equation satisfies $v_p((q-1)n+1) = dN$ and so $y_n = 1$. Choose a large enough solution n so that $\{y_n\}$ is periodic at n. We can solve the following equation for a, and choose such an a to be positive:

$$(q-1)aM \equiv p^{(d-1)N}(p-1) \pmod{p^{dN+2}} \tag{7}$$

Multiplying (7) by p^N gives

$$(q-1)ak \equiv p^{dN+1} - p^{dN} \pmod{p^{dN+2}}. \tag{8}$$

Adding (6) and (8) gives

$$(q-1)(n+ak) \equiv -1 + p^{dN+1} \pmod{p^{dN+2}},$$

from which we conclude $v_p((q-1)(n+ak)+1) = dN+1$. So $y_{n+ak} = 0$. But $y_n = y_{n+ak}$ by periodicity, which is a contradiction.

3. Proof of Theorem 2. Let $f(x) = x^{p^m} + ax$ for $a \in \mathbb{F}_{p^m}^{\times}$, p odd. First we compute $f^n(x)$.

Proposition 8. $f^n(x) = \sum_{k=0}^{n} \binom{n}{k} x^{p^{km}} a^{n-k}$

Proof. Let $\phi(x) = x^{p^m}$ and $a(x) = ax$, so $f = \phi + a$. Both ϕ and a are additive polynomials (they distribute over addition) and they commute, so the proof is simply the binomial theorem applied to $(\phi + a)^n$. ∎

Assume that ζ_f is algebraic. By Corollary 5, the sequence $\{a_n\}$ reduced modulo q is q-automatic for every prime q, as is the subsequence $\{a_{(p^m-1)n}\}$ by previous remarks. Now we need to compute a_n when $p^m - 1$ divides n.

Proposition 9. *If $p^m - 1$ divides n, then $a_n = p^{(n-p^{v_p(n)})m}$.*

Proof. The coefficient of x in $f^n(x)$ is a power of $a^{p^m-1} = 1$. Let l be the smallest positive integer such that $\binom{n}{l} \not\equiv 0 \pmod p$. Then

$$f^n(x) - x = \sum_{k=l}^{n} \binom{n}{k} x^{p^{km}} a^{n-k} = \left(\sum_{k=l}^{n} \binom{n}{k} x^{p^{(k-l)m}} (a^{n-k})^{p^{-l}} \right)^{p^l},$$

where raising to the p^{-l} power means applying the inverse of the Frobenius automorphism l times. Let $g(x) = \sum_{k=l}^{n} \binom{n}{k} x^{p^{(k-l)m}} (a^{n-k})^{p^{-l}}$. The derivative

$g'(x) = (a^{n-l})^{p^{-l}}$ is nonzero, so $g(x)$ has $p^{(n-l)m}$ distinct roots over $\overline{\mathbb{F}}_p$, as does $f^n(x) - x$. So $a_n = p^{(n-l)m}$.

Kummer's classical theorem [K] on binomial coefficients modulo p says that $v_p(\binom{n}{l})$ equals the number of borrows involved in subtracting l from n in base p [K]. It is clear that the smallest integer l that results in no borrows in this subtraction is $l = p^{v_p(n)}$, and we are done. ∎

Let $q > p$ be a prime to be determined and let $r = p^{-1}$ in $\mathbb{F}_q$. The sequence given by $b_n = r^{(p^m-1)nm}$ is eventually periodic and hence q-automatic. Let $c_n = a_{(p^m-1)n} b_n$. By [AS, Corollary 5.4.5] the product of q-automatic sequences over $\mathbb{F}_q$ is q-automatic, so c_n is q-automatic. Therefore

$$\begin{aligned} c_n = a_{(p^m-1)n} b_n &= p^{((p^m-1)n - p^{v_p((p^m-1)n)})m} r^{(p^m-1)nm} \\ &= (p^{-1})^{p^{(v_p(p^m-1)+v_p(n))m}} = (r^m)^{p^{v_p(n)}}. \end{aligned}$$

Choose $q > p^{mp}$ such that $q \equiv 2 \pmod{p^m}$. Note that $o(r^m, q)$ divides $q-1$, so $o(r^m, q) \not\equiv 0 \pmod p$ and p is invertible modulo $o(r^m, q)$. The value of c_n depends only on $p^{v_p(n)}$ reduced modulo $o(r^m, q)$, which in turn is a function of $v_p(n) \bmod o(p, o(r^m, q))$, so c_n is p-automatic by Lemma 7.

By Cobham's theorem, c_n is eventually periodic, so the set

$$\begin{aligned} Y &= \{n \in \mathbb{N} : c_n = r^m\} = \{n \in \mathbb{N} : p^{v_p(n)} \equiv 1 \pmod{o(r^m, q)}\} \\ &= \{n \in \mathbb{N} : v_p(n) \equiv 0 \pmod{o(p, o(r^m, q))}\} \end{aligned}$$

has an eventually periodic characteristic sequence $\{y_n\}$. Essentially the same argument as in Case 2 of Theorem 1 shows this is a contradiction when $o(p, o(r^m, q)) > 1$. We sketch the argument for completeness.

As we chose $q > p^{mp}$, we have $o(r^m, q) = o(p^m, q) > p$, and $o(p, o(r^m, q)) > 1$. Let $d = o(p, o(r^m, q))$, and let $k = Mp^N$ be the eventual period of Y, where $p \nmid M$. We can solve

$$n \equiv p^{dN} \pmod{p^{dN+2}}, \tag{9}$$

$$aM \equiv p^{(d-1)N}(p-1) \pmod{p^{dN+2}} \tag{10}$$

for large n and positive a, so $y_n = 1$. Adding (9) and p^N times (10) gives

$$n + ak \equiv p^{dN+1} \pmod{p^{dN+2}},$$

from which we conclude $v_p(n + ak) = dN + 1$, so $y_{n+ak} = 0$, contradicting periodicity of $\{y_n\}$. This contradiction shows that ζ_f is transcendental.

4. Concluding remarks. The polynomial maps in Theorems 1 and 2 are homomorphisms of the multiplicative and additive groups of $\overline{\mathbb{F}}_p$, respectively. It should be possible to prove similar theorems for other maps associated to homomorphisms, e.g. Chebyshev polynomials, general additive polynomials, and Lattès maps on $\mathbb{P}^1(\overline{\mathbb{F}}_p)$. See [S1] for a discussion of special properties of these maps.

It is more difficult to study the rationality or transcendence of ζ_f when the map f has no obvious structure. For example, there is a standard heuristic that the map $f(x) = x^2 + 1$ behaves like a random mapping on a finite field of odd order (see [B], [P], [S2] and many others). We conclude with the following tantalizing question without hazarding a guess as to the answer.

QUESTION 2. *For p odd and $f = x^2 + 1$, is $\zeta_f(\overline{\mathbb{F}}_p, t)$ in $\mathbb{Q}(t)$?*

Acknowledgements. This research was partly supported by NSF grant no. CCF-0635355. The author wishes to thank Eric Bach for many helpful suggestions and comments, Jeff Shallit for useful clarifications, and an anonymous referee for helpful remarks on style and presentation.

References

[AS] J.-P. Allouche and J. Shallit, *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge Univ. Press, Cambridge, 2003.

[AM] M. Artin and B. Mazur, *On periodic points*, Ann. of Math. (2) 81 (1965), 82–99.

[B] E. Bach, *Toward a theory of Pollard's rho method*, Inform. and Comput. 90 (1991), 139–155.

[D] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. 82 (1960), 631–648.

[G] J. Guckenheimer, *Axiom* A + *No Cycles* $\Rightarrow \zeta_f(t)$ *rational*, Bull. Amer. Math. Soc. 76 (1970), 592–594.

[K] E. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. 44 (1852), 93–146.

[L] W. J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley, Reading, MA, 1977.

[M] A. Manning, *Axiom* A *diffeomorphisms have rational zeta functions*, Bull. London Math. Soc. 3 (1971), 215–220.

[P] J. M. Pollard, *A Monte Carlo method for factorization*, BIT 15 (1975), 331–334.

[S1] J. Silverman, *The Arithmetic of Dynamical Systems*, Grad. Texts in Math. 241, Springer, 2007.

[S2] J. Silverman, *Variation of periods modulo p in arithmetic dynamics*, New York J. Math. 14 (2008), 601–616.

Andrew Bridy
Department of Mathematics
University of Wisconsin-Madison
Madison, WI 53706, U.S.A.
E-mail: bridy@math.wisc.edu

Received on 2.2.2012
and in revised form on 25.8.2012 (6956)