JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Andrew BRIDY

The Artin-Mazur Zeta Function of a Dynamically Affine Rational Map in Positive Characteristic

Tome 28, n° 2 (2016), p. 301-324.

<http://jtnb.cedram.org/item?id=JTNB_2016__28_2_301_0>

© Société Arithmétique de Bordeaux, 2016, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/), implique l'accord avec les conditions générales d'utilisation (http://jtnb.cedram.org/legal/). Toute reproduction en tout ou partie de cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Journal de Théorie des Nombres
de Bordeaux **28** (2016), 301–324

The Artin-Mazur Zeta Function of a Dynamically Affine Rational Map in Positive Characteristic

par Andrew BRIDY

Résumé. Soit k un corps algébriquement clos de caractéristique positive. Nous déterminons la rationalité ou la transcendance de la fonction zêta d'Artin-Mazur d'une fonction dynamiquement affine $\mathbb{P}^1(k) \to \mathbb{P}^1(k)$.

Abstract. We determine the rationality or the transcendence of the Artin-Mazur zeta function of a dynamically affine self-map of $\mathbb{P}^1(k)$ for k an algebraically closed field of positive characteristic.

1. The Artin-Mazur Zeta Function

Let X be a set and let $f : X \to X$ define a dynamical system. Let $\mathrm{Per}_n(f) = \{x \in X : f^n(x) = x\}$, where f^n denotes the composition of f with itself n times. The Artin-Mazur zeta function of this dynamical system is the formal power series given by

$$\zeta(f, X; t) = \exp\left(\sum_{n=1}^{\infty} \#\,\mathrm{Per}_n(f)\frac{t^n}{n}\right).$$

Assume that $\#\,\mathrm{Per}_n(f) < \infty$ for all n, as otherwise ζ is not defined. The power series $\zeta(f, X; t)$ has rational coefficients, and it is not hard to show that $\zeta(f, X; t) \in \mathbb{Z}[[t]]$ by means of the product formula

$$\zeta(f, X; t) = \prod_{\text{cycles } C} \left(1 - t^{|C|}\right)^{-1}.$$

This zeta function was introduced by Artin and Mazur in [2], where it is studied for X a manifold and f a diffeomorphism. In this setting, only the *isolated* periodic points are counted. This will not be an important distinction for our purposes.

This paper continues the study of the following question, introduced in [4] for polynomials, but just as easily phrased for rational functions.

Question 1.1. *For which $f \in \overline{\mathbb{F}}_p(x)$ is $\zeta(f, \mathbb{P}^1(\overline{\mathbb{F}}_p); t)$ rational?*

Manuscrit reçu le 24 février 2014, accepté le 28 juin 2014.
Mathematics Subject Classification. 37P05, 11G20, 11B85.
Mots-clefs. Arithmetic dynamics, algebraic groups, automatic sequences, finite fields.

The purpose of this paper is to answer this question for rational maps that are dynamically affine. These are maps that, loosely speaking, come from endomorphisms of algebraic groups; a precise definition will be given in Section 2. There are five families of dynamically affine maps in one dimension: power maps, Chebyshev polynomials, Lattès maps, additive polynomials, and subadditive polynomials. We will prove this classification in Sections 3, 4, and 5. (To be precise, this classification only holds up to conjugacy by $\mathrm{Aut}(\mathbb{P}^1)$, but ζ is a conjugacy invariant.) We determine the rationality of the zeta function for each of these families, and we show that when it fails to be rational, it is transcendental.

Let k be an arbitrary algebraically closed field of characteristic p, and assume that $f \in k(x)$ is separable. Our main results are the following.

Theorem 1.2. *Let f be a power map, Chebyshev polynomial, or Lattès map. Then $\zeta(f, \mathbb{P}^1(k); t)$ is transcendental over $\mathbb{Q}(t)$.*

Theorem 1.3. *Let f be an additive or subadditive polynomial. If $f'(0)$ is algebraic over $\mathbb{F}_p$, then $\zeta(f, \mathbb{P}^1(k); t)$ is transcendental over $\mathbb{Q}(t)$. If $f'(0)$ is transcendental over $\mathbb{F}_p$, then $\zeta(f, \mathbb{P}^1(k); t)$ is rational.*

These theorems can be seen as the broadest possible generalization of the work in [4], as the maps considered there are very specific cases of one-dimensional dynamically affine maps. In order to handle the new cases, we need to study the arithmetic of the endomorphism rings of one-dimensional algebraic groups, which can be somewhat complicated in the case of an elliptic curve.

Inseparable maps are excluded from the above theorems because their zeta functions are trivially rational. Let $f \in k(x)$ be inseparable and of degree d. The derivative of f is identically zero, so $f^n(x) - x$ has distinct roots for every n and $\#\operatorname{Per}_n(f) = d^n + 1$. Therefore

$$\zeta(f, \mathbb{P}^1(k); t) \;=\; \exp\left(\sum_{n=1}^{\infty} \frac{(d^n+1)t^n}{n}\right) \;=\; \frac{1}{(1-t)(1-dt)}.$$

For a general $f \in k(x)$, it is not always the case that $\#\operatorname{Per}_n(f) = d^n+1$, but it is certainly true that $\#\operatorname{Per}_n(f) \leq d^n + 1$. So if we consider $\zeta(f, \mathbb{P}^1(k); t)$ as a function of a complex variable, it converges to a holomorphic function in a positive radius around the origin.

Remark. In higher dimensions, the formula $\deg(f^n) = (\deg f)^n$ is not necessarily true. This complicates the above calculation of rationality. See, for example, [3], [8], and [16] for a discussion of this phenomenon.

Remark. In characteristic zero, the situation is very different. Hinkkanen shows that every $f \in \mathbb{C}(x)$ has a rational zeta function [9]. The proof relies on the fact that there are only finitely many $x \in \mathbb{P}^1(\mathbb{C})$ such that

$(f^n)'(x)$ is a root of unity. This argument fails catastrophically in positive characteristic because every element of $\overline{\mathbb{F}}_p$ is a root of unity. Nevertheless, it is somewhat peculiar that the conclusion of Hinkkanen's theorem holds in positive characteristic almost exclusively when f is inseparable, which is a phenomenon that cannot occur in characteristic 0.

The rest of the paper will prove Theorems 1.2 and 1.3. In Section 2 we define dynamically affine maps, and in Sections 3, 4, and 5 we classify all dynamically affine maps of $\mathbb{P}^1$ and establish some facts about their periodic points. A crucial and interesting feature of these maps is that we can count their periodic points by studying the arithmetic of certain endomorphism rings. Section 6 provides some algebraic lemmas that are useful in this direction. Our proof also employs the theory of sequences generated by finite automata. Section 7 sketches the necessary background in this area. Sections 8 and 9 finish the proof of Theorems 1.2 and 1.3.

The results of this paper suggest the following conjecture.

Conjecture 1.4. *If $f \in \overline{\mathbb{F}}_p(x)$ is separable, $\zeta(f, \mathbb{P}^1(\overline{\mathbb{F}}_p); t)$ is transcendental over $\mathbb{Q}(t)$.*

If f is not dynamically affine, the size of $\mathrm{Per}_n(f)$ can vary wildly as n increases, making it difficult to determine the algebraic structure of the zeta function. Even the low degree map $f(x) = x^2 + 1$ behaves very irregularly in its periodic point counts (for $p \notin \{2, 3\}$), so the nature of ζ is unclear. However, note that by Theorem 1.3 the above conjecture is false if we replace $\overline{\mathbb{F}}_p$ by an algebraically closed field k that is transcendental over $\mathbb{F}_p$.

2. Overview of Dynamically Affine Maps

The following definitions are taken from [13, Ch 6.8].

Definition. Let G be a commutative algebraic group. An *affine morphism* of G is a map $\psi : G \to G$ that can be written as a composition of a finite endomorphism of degree at least 2 and a translation.

Definition. Let V be a variety. A morphism $f : V \to V$ is *dynamically affine* if there exist a connected commutative algebraic group G, an affine morphism $\psi : G \to G$, a finite subgroup $\Gamma \subseteq \mathrm{Aut}(G)$ and a quotient map $\pi : G \to G/\Gamma$, and a morphism that identifies G/Γ with a Zariski dense

open subset of V such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\psi} & G \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ G/\Gamma & \longrightarrow & G/\Gamma \\ \downarrow & & \downarrow \\ V & \xrightarrow{f} & V \end{array} \tag{2.1}$$

It is well known that the only dynamically affine maps of $\mathbb{P}^1(\mathbb{C})$ are power maps, Chebyshev polynomials, and Lattès maps (up to conjugacy by fractional linear transformations) [13, p. 378]. These arise when G is either the multiplicative group $\mathbb{G}_m$ or an elliptic curve.

In characteristic p, there are two additional families of dynamically affine maps, both of which arise from the additive group $\mathbb{G}_a$. These are additive polynomials, which are maps such as $f(x) = x^p - x$ that distribute over addition, and subadditive polynomials such as $f(x) = x(x-1)^{p-1}$, which arise as the maps induced by additive polynomials on the quotient of $\mathbb{G}_a$ by a group of roots of unity.

We elaborate on these families in the sections that follow. The only connected one-dimensional algebraic groups are $\mathbb{G}_m$, $\mathbb{G}_a$, and elliptic curves. By considering all of the possibilities for the group Γ, we show that the maps listed above are all of the dynamically affine maps of $\mathbb{P}^1$. First, however, we establish a lemma that counts $\mathrm{Per}_n(f)$ in terms of the kernels of endomorphisms of G.

Lemma 2.1. *Let $f : V \to V$ be dynamically affine. Assume that the affine morphism $\psi : G \to G$ is surjective. Write ψ as $\psi(g) = \sigma(g) + h$, where $\sigma \in \mathrm{End}(G)$, $h \in G$ and the group law of G is written additively. Then*

$$\#\,\mathrm{Per}_n(f) = \#(\mathrm{Per}_n(f) \setminus (G/\Gamma)) + \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma} \#\ker(\sigma^n - \gamma).$$

Proof. Recall that G/Γ is identified with a Zariski open subset of V. The equation above claims that the n-periodic points that lie in this set are counted by the formula $\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma} \#\ker(\sigma^n - \gamma)$.

Suppose that $z \in \mathrm{Per}_n(f) \cap G/\Gamma$. By diagram 2.1, there exists $g \in \pi^{-1}(z)$ and $\gamma \in \Gamma$ such that $\psi^n(g) = \gamma(g)$, and every such choice of g and γ gives some $z \in \mathrm{Per}_n(f) \cap G/\Gamma$. Therefore

$$\mathrm{Per}_n(f) \cap G/\Gamma = \pi(\{g \in G : \psi^n(g) = \gamma(g) \text{ for some } \gamma \in \Gamma\}).$$

By slight abuse of notation, let $\ker(\psi^n - \gamma) = (\psi^n - \gamma)^{-1}(0)$. Define

$$S = \bigcup_{\gamma\in\Gamma} \ker(\psi^n - \gamma),$$

so that $\mathrm{Per}_n(f) \cap G/\Gamma = \pi(S)$. We claim that Γ acts on S.

Let $g \in S$, so that $\psi^n(g) = \delta(g)$ for some $\delta \in \Gamma$. Let $\gamma \in \Gamma$. Observe that

$$\pi(\psi^n(\gamma(g))) = f^n(\pi(\gamma(g))) = f^n(\pi(g)) = \pi(\psi^n(g)).$$

As $\psi^n(\gamma(g))$ and $\psi^n(g)$ have the same image under π, there exists some $\delta' \in \Gamma$ such that $\psi^n(\gamma(g)) = \delta'(g)$, and therefore $\gamma(g) \in S$. (Somewhat surprisingly, δ' depends only on γ and not on g, but we do not need this for our purposes. See [13, Prop 6.77].)

If $z \in \mathrm{Per}_n(f) \cap G/\Gamma$, the set $\pi^{-1}(z)$ is a Γ-orbit in S, so there is a bijection between $\mathrm{Per}_n(f) \cap G/\Gamma$ and the set of orbits S/Γ. Let Γ_g be the subgroup of Γ that fixes $g \in S$, and let δ be such that $\psi^n(g) = \delta(g)$. Then

$$\#\{\gamma \in \Gamma : g \in \ker(\psi^n - \gamma)\} = \#\{\gamma \in \Gamma : g = \gamma^{-1}\delta(g)\} = |\Gamma_g|$$

By the orbit-stabilizer theorem [10, Cor 4.10],

$$\begin{aligned}
\#S/\Gamma &= \sum_{g \in S} \frac{|\Gamma_g|}{|\Gamma|} \\
&= \frac{1}{|\Gamma|} \sum_{g \in S} \#\{\gamma \in \Gamma : g \in \ker(\psi^n - \gamma)\} \\
&= \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \#\{g \in S : g \in \ker(\psi^n - \gamma)\} \\
&= \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \#\ker(\psi^n - \gamma).
\end{aligned}$$

Recall that $\psi(g) = \sigma(g) + h$. So $\psi^n(g) = \sigma^n(g) + h_n$ for some $h_n \in G$, and

$$\ker(\psi^n - \gamma) = (\psi^n - \gamma)^{-1}(0) = (\sigma^n - \gamma)^{-1}(-h_n).$$

We assumed ψ is surjective, so $\ker(\psi^n - \gamma)$ is nonempty. Therefore

$$\#(\sigma^n - \gamma)^{-1}(-h_n) = \#\ker(\sigma^n - \gamma),$$

completing the proof. □

3. Maps from $\mathbb{G}_m$: Power Maps and Chebyshev Polynomials

Let $\mathbb{G}_m$ be the multiplicative group. The endomorphism ring $\mathrm{End}(\mathbb{G}_m)$ is isomorphic to $\mathbb{Z}$, where the integer d corresponds to the power map $x \mapsto x^d$. So every affine morphism $\psi : \mathbb{G}_m \to \mathbb{G}_m$ has the form $\psi(x) = ax^d$. The automorphism group is $\mathrm{Aut}(\mathbb{G}_m) \cong \mathbb{Z}^\times = \{\pm 1\}$. There are only two subgroups $\Gamma \subseteq \mathrm{Aut}(\mathbb{G}_m)$: either Γ is trivial or $\Gamma = \{x, x^{-1}\}$.

The underlying scheme of $\mathbb{G}_m$ is $\mathrm{Spec}\, k[x, x^{-1}] \cong \mathbb{A}^1 \setminus \{0\}$, which is Zariski open in $\mathbb{P}^1$. If Γ is trivial, then a power map arises from the following

commutative diagram:

$$\begin{array}{ccc}
\mathbb{G}_m & \xrightarrow{x\mapsto ax^d} & \mathbb{G}_m \\
\downarrow\wr & & \downarrow\wr \\
\mathbb{A}^1\setminus\{0\} & \longrightarrow & \mathbb{A}^1\setminus\{0\} \\
\downarrow & & \downarrow \\
\mathbb{P}^1 & \xrightarrow{f} & \mathbb{P}^1
\end{array}$$

There are many choices for the inclusion map $\mathbb{A}^1 \setminus \{0\} \hookrightarrow \mathbb{P}^1$. The most obvious is the map that extends to the identity map on $\mathbb{P}^1$, in which case f is the "affine power map" $f(x) = ax^d$. Other inclusions have the effect of conjugating f by a fractional linear transformation. Over an algebraically closed field, we can always conjugate by a linear polynomial $x \mapsto cx$ in order to make f monic, so we may assume $f(x) = x^d$. (Recall that ζ is a conjugacy invariant.)

There are only two points in $\mathbb{P}^1$ that lie outside $\mathbb{A}^1 \setminus \{0\}$, namely, 0 and ∞. If $d > 0$, then f fixes these two points, and if $d < 0$, then f swaps them. The group law of $\mathbb{G}_m$ is written multiplicatively, so if $d > 0$, Lemma 2.1 gives

$$\#\operatorname{Per}_n(f) = 2 + \#\ker(x^{d^n-1}), \tag{3.1}$$

and if $d < 0$, then

$$\#\operatorname{Per}_n(f) = \begin{cases} 2 + \#\ker(x^{d^n-1}) & : d \text{ even} \\ \#\ker(x^{d^n-1}) & : d \text{ odd} \end{cases} \tag{3.2}$$

If we let $\Gamma = \{x, x^{-1}\}$, then $\mathbb{G}_m/\Gamma \cong \mathbb{A}^1$, and the quotient can be realized by the map $\pi(x) = x + x^{-1}$. There exists a polynomial f such that the following diagram commutes [13, Prop 6.6].

$$\begin{array}{ccc}
\mathbb{G}_m & \xrightarrow{x\mapsto ax^d} & \mathbb{G}_m \\
\downarrow\pi & & \downarrow\pi \\
\mathbb{A}^1 & \longrightarrow & \mathbb{A}^1 \\
\downarrow & & \downarrow \\
\mathbb{P}^1 & \xrightarrow{f} & \mathbb{P}^1
\end{array}$$

If the inclusion $\mathbb{A}^1 \hookrightarrow \mathbb{P}^1$ extends to the identity map and $a = 1$, then f is the dth Chebyshev polynomial $T_d(x)$ and satisfies

$$f(x + x^{-1}) = x^d + x^{-d}.$$

As with power maps, choosing other inclusions or $a \neq 1$ simply results in fractional linear conjugates of Chebyshev polynomials. Because of the symmetry in the definition, positive and negative d give rise to the same f. Here the count of Lemma 2.1 is

$$\#\operatorname{Per}_n(f) = 1 + \frac{1}{2}\left(\#\ker(x^{d^n-1}) + \#\ker(x^{d^n+1})\right). \tag{3.3}$$

The kernel of the endomorphism $x \mapsto x^m$ is the set of $|m|$th roots of unity in k. If $(p, |m|) = 1$, there are $|m|$ of these, and in general

$$\#\ker(x^m) = \frac{|m|}{p^{v_p(|m|)}}$$

because there are no nontrivial pth roots of unity.

Therefore, for a power map $f \in k(x)$ associated to the endomorphism $\sigma(x) = x^d$, if $d > 0$ we have the formula

$$\#\operatorname{Per}_n(f) = 2 + \frac{d^n - 1}{p^{v_p(d^n-1)}}, \tag{3.4}$$

and if $d < 0$,

$$\#\operatorname{Per}_n(f) = \begin{cases} 2 + \frac{|d|^n-1}{p^{v_p(|d|^n-1)}} & : d \text{ even} \\ \frac{|d|^n+1}{p^{v_p(|d|^n+1)}} & : d \text{ odd} \end{cases} \tag{3.5}$$

For a Chebyshev polynomial f, the formula reads

$$\#\operatorname{Per}_n(f) = 1 + \frac{1}{2}\left(\frac{|d|^n - 1}{p^{v_p(|d|^n-1)}} + \frac{|d|^n + 1}{p^{v_p(|d|^n+1)}}\right). \tag{3.6}$$

4. Maps from $\mathbb{G}_a$: Additive and Subadditive Polynomials

Let $\mathbb{G}_a$ be the additive group. In characteristic zero, all endomorphisms of $\mathbb{G}_a$ are of the form $x \mapsto cx$, so $\operatorname{End}(\mathbb{G}_a) \cong k$. In positive characteristic, the Frobenius map $\phi(x) = x^p$ and its iterates are also endomorphisms, and $\operatorname{End}(\mathbb{G}_a)$ is the noncommutative polynomial ring $k\langle\phi\rangle$ with multiplication rule $\phi c = c^p\phi$ for $c \in k$.

The only automorphisms of $\mathbb{G}_a$ are the nonzero maps $x \mapsto cx$, as the Frobenius morphism ϕ is a bijection on k-valued points (k is algebraically closed) but is not an isomorphism on the underlying scheme, which is $\mathbb{A}^1$. Therefore $\operatorname{Aut}(\mathbb{G}_a) \cong k^\times$. The finite subgroups $\Gamma \subseteq \operatorname{Aut}(\mathbb{G}_a)$ are all cyclic by a basic fact of field theory [10, Lem 17.12], so there is some d such that $\Gamma \cong \mu_d$, the group of dth roots of unity.

Let $\psi : \mathbb{G}_a \to \mathbb{G}_a$ be an affine morphism, that is, an element of $k\langle\phi\rangle$ composed with a translation. If $\Gamma = \{1\}$, then $\pi : \mathbb{G}_a \to G/\Gamma \cong \mathbb{A}^1$ is the

identity morphism on the underlying scheme. There always exists an f that fits into the following diagram:

$$\begin{array}{ccc} \mathbb{G}_a & \xrightarrow{\psi} & \mathbb{G}_a \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{A}^1 & \longrightarrow & \mathbb{A}^1 \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & \xrightarrow{f} & \mathbb{P}^1 \end{array}$$

There are many possible inclusions $\mathbb{A}^1 \hookrightarrow \mathbb{P}^1$, but as with power maps, f is determined up to conjugacy. Therefore we may assume that the inclusion extends to the identity, in which case f fixes ∞ and is a polynomial. We call f an additive polynomial, as $f(x+y) = f(x) + f(y)$ for all $x, y \in k$.

If $\Gamma \cong \mu_d$ for $d > 1$ and $(p, d) = 1$, then the map $\pi : \mathbb{G}_a \to \mathbb{G}_a/\mu_d \cong \mathbb{A}^1$ can be taken to be $\pi(x) = x^d$. In this case there exists an f to make the diagram commute if and only if ψ satisfies $\psi(\omega_d x) = \omega_d \psi(x)$ for a primitive dth root of unity ω_d. (This happens if and only if $\psi(x)$, written as a polynomial, has terms whose degrees are all 1 mod d.) If there is such an f, we call it a subadditive polynomial.

Let $\sigma \in k\langle\phi\rangle$ be an endomorphism of $\mathbb{G}_a$. The size of $\ker \sigma$ depends on the divisibility of σ by ϕ, that is,

$$\#\ker \sigma = \frac{\deg \sigma}{p^{v_\phi(\sigma)}}.$$

Here $v_\phi(\sigma)$ is the largest power of the two-sided maximal ideal $(\phi) = \phi k\langle\phi\rangle$ that contains σ.

Let $\psi(x) = \sigma(x) + c$ for some $c \in \mathbb{G}_a$. For an additive or subadditive polynomial f, Lemma 2.1 and the above observation yield

$$\#\operatorname{Per}_n(f) \;=\; 1 + \frac{1}{d}\sum_{\omega \in \mu_d} \#\ker(\sigma^n - \omega) \;=\; 1 + \frac{1}{d}\sum_{\omega \in \mu_d} \frac{(\deg \sigma)^n}{p^{v_\phi(\sigma^n - \omega)}}. \tag{4.1}$$

Note that $\deg(\sigma^n - \omega) = \deg(\sigma^n)$ because $\omega : \mathbb{G}_a \to \mathbb{G}_a$ is the linear polynomial $\omega(x) = \omega x$, and $\deg \sigma = \deg \psi \geq 2$ by assumption.

5. Maps from Elliptic Curves: Lattès Maps

Let E be an elliptic curve and let $\psi : E \to E$ be an affine morphism. The endomorphism ring $\operatorname{End}(E)$ can be identified with either $\mathbb{Z}$, an order in an imaginary quadratic field, or a maximal order in a quaternion algebra [14, Thm V.3.1]. There are only six possibilities for $\operatorname{Aut}(E)$: it may be a cyclic group of order 2,3,4, or 6, or a certain nonabelian group of order 12 or

24 [14, Thm III.10.1]. Let Γ be a nontrivial subgroup of $\mathrm{Aut}(E)$. We say that f is a Lattès map if the diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{\psi} & E \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ E/\Gamma & \longrightarrow & E/\Gamma \\ \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \wr} \\ \mathbb{P}^1 & \xrightarrow{f} & \mathbb{P}^1 \end{array}$$

As E is projective, the curve E/Γ is isomorphic to $\mathbb{P}^1$, unlike in the cases coming from $\mathbb{G}_m$ and $\mathbb{G}_a$. For a given choice of ψ and Γ, there is not necessarily an f that makes the diagram commute.

Remark. A Lattès map is often defined to be $f \in k(x)$ such that there exists a morphism $\psi : E \to E$ with $\deg \psi \geq 2$ and a finite separable cover $\pi : E \to \mathbb{P}^1$ such that the following diagram commutes.

$$\begin{array}{ccc} E & \xrightarrow{\psi} & E \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1 & \xrightarrow{f} & \mathbb{P}^1 \end{array}$$

This is equivalent to our definition. Any self-morphism of an elliptic curve can be written as the composition of an isogeny and a translation [14, p 75], so any morphism $\psi : E \to E$ with $\deg \psi \geq 2$ is affine. Also, if there exists a diagram as above, then there exists such a diagram with the same f and a possibly different triple (E', ψ', π') where the map π' is the quotient of E' by a subgroup of automorphisms. This result is due to Milnor over $\mathbb{C}$ [12], and Ghioca and Zieve in arbitrary characteristic [7]. For a sketch of the Ghioca-Zieve proof, see [15, pp. 54-56].

By a general fact about morphisms of elliptic curves [14, Thm III.4.10(a)],

$$\#\ker\sigma \;=\; \deg_s \sigma \;=\; \frac{\deg\sigma}{\deg_i \sigma}.$$

Here $\deg_s$ and $\deg_i$ denote separable and inseparable degrees. In the rest of this section we develop a formula for $\deg_i(\sigma)$ in terms of the arithmetic of $\mathrm{End}(E)$.

First we set some notation. Let $N, \mathrm{tr} : \mathrm{End}(E)\otimes\mathbb{Q} \to \mathbb{Q}$ denote the norm and trace maps, or the reduced norm and trace in the case that $\mathrm{End}(E)\otimes\mathbb{Q}$ is a quaternion algebra. Let $\phi_m : E \to E^{(p^m)}$ be the p^mth power Frobenius morphism. For an isogeny $\sigma : E_1 \to E_2$, write $\hat{\sigma} : E_2 \to E_1$ for the dual isogeny. The j-invariant of E is denoted by $j(E)$. For our purposes, E is defined over an algebraically closed field k of characteristic p, so $j(E) \in k$.

Proposition 5.1. *Suppose that $j(E)$ is transcendental over $\mathbb{F}_p$ and let $\sigma \in \mathrm{End}(E)$. Then $\sigma \in \mathbb{Z}$ and*

$$\deg_i(\sigma) = p^{v_p(\sigma)}.$$

Proof. If $j(E) \notin \overline{\mathbb{F}}_p$, then $\mathrm{End}(E) \cong \mathbb{Z}$ [14, p 145]. The multiplication by p map $[p] : E \to E$ has inseparable degree p, because $[p] = \hat{\phi}_1 \circ \phi_1$ and the dual isogeny $\hat{\phi}_1$ is separable [14, Thm V.3.1]. The multiplication by m map is separable if $(p, m) = 1$. Therefore the isogeny $[m] : E \to E$ has inseparable degree equal to $p^{v_p(m)}$. □

For the rest of this section suppose that $j(E)$ is algebraic over $\mathbb{F}_p$, so that up to isomorphism, E is defined over a finite field. In this situation the endomorphism ring $\mathrm{End}(E)$ can be identified with an order in an imaginary quadratic field if E is ordinary or a maximal order in a quaternion algebra if E is supersingular [14, Thm V.3.1].

Proposition 5.2. *Let E be ordinary and let $K = \mathrm{End}(E) \otimes \mathbb{Q}$. Let $\mathfrak{p}$ be the extension to $\mathcal{O}_K$ of the ideal in $\mathrm{End}(E)$ consisting of all inseparable isogenies. Then $\mathfrak{p}$ is prime, and for any $\sigma \in \mathrm{End}(E)$,*

$$\deg_i(\sigma) = p^{v_{\mathfrak{p}}(\sigma)}.$$

Proof. By [14, Cor II.2.12] we can write $\sigma = \lambda \circ \phi_m$ where $p^m = \deg_i(\sigma)$ and $\lambda : E^{(p^m)} \to E$ is separable. It follows that $\deg_i(\sigma) \geq p^m$ if and only if σ factors through $\phi_m : E \to E^{(p^m)}$. (If $\sigma = 0$, we set $\deg_i(\sigma) = \infty$.)

We know that $\mathrm{End}(E)$ is an order in $\mathcal{O}_K$ for some imaginary quadratic field K, and the conductor of $\mathrm{End}(E)$ is prime to p [6]. Let I_m be the mth *inseparable ideal* of $\mathrm{End}(E)$, defined as follows:

$$I_m = \{\sigma \in \mathrm{End}(E) : \deg_i(\sigma) \geq p^m\}.$$

It is routine to show that I_m is an ideal. If $\sigma\tau \in I_m$, then

$$\deg_i(\sigma\tau) = \deg_i(\sigma)\deg_i(\tau) \geq p^m.$$

If $\sigma \notin I_m$ then necessarily $\deg_i(\tau) \geq p$, so $\deg_i(\tau^m) \geq p^m$ and $\tau^m \in I_m$. For $m = 1$ this shows that I_1 is prime, and for $m > 1$ that I_m is I_1-primary.

If $\mathrm{End}(E)$ were a Dedekind domain, it would follow that $I_m = (I_1)^m$ for each $m > 1$, but orders of Dedekind domains are not in general Dedekind domains. Instead, consider the integral extension $\mathcal{O}_K / \mathrm{End}(E)$ and the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over I_1. The multiplication by p map $[p] : E \to E$ is inseparable, so $p \in I_1$, and therefore $p\mathcal{O}_K \subseteq I_1\mathcal{O}_K \subseteq \mathfrak{p}$. So $I_1\mathcal{O}_K$ is either $\mathfrak{p}$ or $p\mathcal{O}_K = \mathfrak{p}\hat{\mathfrak{p}}$ (as p splits in $\mathcal{O}_K$ [6]).

This shows that the ideal $I_1\mathcal{O}_K$ is prime to the conductor of $\mathrm{End}(E)$. For ideals in an order that are prime to the conductor, extension to $\mathcal{O}_K$ and contraction are inverses, and unique factorization holds [5, Prop 7.20]. Therefore $I_1\mathcal{O}_K = \mathfrak{p}$ and the I_1-primary ideal I_m equals $(I_1)^m$ for each

$m > 1$. It follows easily that $(I_1)^m \mathcal{O}_K = (I_1 \mathcal{O}_k)^m = \mathfrak{p}^m$. We conclude that $\deg_i(\sigma) = p^{v_{\mathfrak{p}}(\sigma)}$. □

Remark. If E is defined over $\mathbb{F}_p$, the pth power Frobenius morphism ϕ_1 is an element of $\mathrm{End}(E)$. In this case, the ideal $\mathfrak{p}$ in Proposition 5.2 is the principal ideal $\phi_1 \mathcal{O}_K$, and $v_{\mathfrak{p}}(\sigma)$ is simply the highest power of ϕ_1 that divides σ in $\mathcal{O}_K$. In general, the ideal $\mathfrak{p}$ need not be principal.

Proposition 5.3. *Let E be supersingular, so that* $\mathrm{End}(E)$ *can be identified with a maximal order $\mathcal{O}$ of the quaternion algebra B. There exists a two-sided maximal ideal I of $\mathcal{O}$ such that*

$$\deg_i(\sigma) = p^{v_I(\sigma)}.$$

Proof. If we write $\sigma = \lambda \circ \phi_m$ where λ is separable, then $\deg(\lambda)$ is not divisible by p. If it were, the map $\lambda \circ \hat{\lambda} = [N(\lambda)] = [\deg(\lambda)] : E \to E$ would factor through $[p] : E \to E$ and would be inseparable, so one of λ or $\hat{\lambda}$ would be inseparable. If $\hat{\lambda}$ were inseparable it would factor through ϕ_1, so λ would factor through $\hat{\phi_1}$, which is inseparable [14, Thm V.3.1], contradicting the fact that λ is separable. Moreover, $\deg \phi_m$ is a p-power, and is therefore the largest power of p that divides $\deg \sigma$. This shows that

$$\deg_i \sigma = \deg \phi_m = p^{v_p(\deg \sigma)} = p^{v_p(N(\sigma))}.$$

We have $\mathrm{End}(E) \cong \mathcal{O}$, where $\mathcal{O}$ is a maximal order of B, which is the unique quaternion algebra over $\mathbb{Q}$ ramified exactly at p and ∞ [6]. Consider the localization $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$, which is the unique maximal order of $B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p$, and the inclusion $\mathcal{O} \hookrightarrow \mathcal{O}_p$.

In $\mathcal{O}_p$ there is a uniformizing element π such that $\pi \mathcal{O}_p$ is the unique two-sided maximal ideal of $\mathcal{O}_p$, and moreover every ideal of $\mathcal{O}_p$ is a power of $\pi \mathcal{O}_p$ [17, Ch 2, Thm 1.3]. In particular, $p\mathcal{O}_p = \pi^2 \mathcal{O}_p$, so $v_{\pi \mathcal{O}_p}(p) = 2$. Let $I = \pi \mathcal{O}_p \cap \mathcal{O}$. The ideal I is maximal in $\mathcal{O}$ because locally it is either maximal or the unit ideal: $I_p = \pi \mathcal{O}_p$, and $I_\ell = \mathcal{O}_\ell$ for $\ell \neq p$ (this is because p, which lies in I, is invertible in $\mathcal{O}_\ell$). The ideal I is also two-sided because it is two-sided locally [17, p. 84]. Therefore v_I is a valuation on $\mathcal{O}$.

Any supersingular elliptic curve E is defined over $\mathbb{F}_{p^2}$, and there exists an automorphism $i : E \to E$ such that $\phi_2 = i \circ [p]$. As $v_I(p) = 2$, it follows that $v_I(\sigma) = v_p(N(\sigma))$ for all $\sigma \in \mathcal{O}$ such that $v_p(N(\sigma))$ is even, i.e. such that $\sigma = \lambda \circ [p^n]$ for some separable λ. If $v_p(N(\sigma))$ is odd then $v_p(N(\sigma^2))$ is even, so $v_I(\sigma^2) = v_p(N(\sigma^2))$, and therefore $v_I(\sigma) = v_p(N(\sigma))$. □

Write $\psi : E \to E$ as $\psi(x) = \sigma(x) + P$ for $\sigma \in \mathrm{End}(E)$ and $P \in E$. The above propositions together with Lemma 2.1 prove the following formulas. If $j(E)$ is transcendental, then necessarily $\Gamma = \{\pm 1\}$, and

$$\#\,\mathrm{Per}_n(f) = \frac{1}{2}\left(\frac{|\sigma^n - 1|}{p^{v_p(\sigma^n - 1)}} + \frac{|\sigma^n + 1|}{p^{v_p(\sigma^n + 1)}}\right). \tag{5.1}$$

If $j(E)$ is algebraic and E is ordinary, then there exists $\mathfrak{p}$ such that

$$\#\operatorname{Per}_n(f) = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\frac{N(\sigma^n-\gamma)}{p^{v_{\mathfrak{p}}(\sigma^n-\gamma)}}. \tag{5.2}$$

If $j(E)$ is algebraic and E is supersingular, then there exists I such that

$$\#\operatorname{Per}_n(f) = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\frac{N(\sigma^n-\gamma)}{p^{v_I(\sigma^n-\gamma)}}. \tag{5.3}$$

The sequence $n \mapsto N(\sigma^n-\gamma)$ that appears in the above equations satisfies a linear recurrence relation and is therefore periodic when reduced mod any prime ℓ. We record for future reference the next proposition, which determines its possible periods.

Proposition 5.4. *Let $j(E) \in \overline{\mathbb{F}}_p$ and let $a_n = N(\sigma^n-\gamma)$, where $\sigma,\gamma \in \operatorname{End}(E)$. For any prime ℓ, the sequence $(a_n \pmod{\ell})$ is periodic of period dividing $(\ell-1)(\ell^2-1)\ell^A$ for some integer A.*

Proof. Let $T = \operatorname{tr}(\sigma)$ and $N = N(\sigma)$. We compute

$$\begin{aligned} a_n &= \widehat{(\sigma^n-\gamma)}(\sigma^n-\gamma) \\ &= \hat{\sigma}^n\sigma^n - \sigma^n\hat{\gamma} - \hat{\sigma}^n\gamma + \hat{\gamma}\gamma \\ &= N^n - \operatorname{tr}(\sigma^n\hat{\gamma}) + N(\gamma). \end{aligned}$$

Let $b_n = N^n$, $c_n = \operatorname{tr}(\sigma^n\hat{\gamma})$, and $d_n = N(\gamma)$. Certainly $b_n = Nb_{n-1}$ and $d_n = d_{n-1}$; this shows that the linearly recurrent sequences (b_n) and (d_n) have characteristic polynomials $x-N$ and $x-1$ in the sense of [11, Ch 6].

Whether $\operatorname{End}(E)$ is an order in an imaginary quadratic field or an order in a quaternion algebra, any $\sigma \in \operatorname{End}(E)$ satisfies the Cayley-Hamilton identity $\sigma^2 - T\sigma + N = 0$. For $n \geq 2$,

$$\begin{aligned} c_n - Tc_{n-1} + Nc_{n-2} &= \operatorname{tr}(\sigma^n\hat{\gamma}) - T\operatorname{tr}(\sigma^{n-1}\hat{\gamma}) + N\operatorname{tr}(\sigma^{n-2}\hat{\gamma}) \\ &= \operatorname{tr}((\sigma^2 - T\sigma + N)\sigma^{n-2}\hat{\gamma}) \\ &= \operatorname{tr}(0) \\ &= 0. \end{aligned}$$

Therefore (c_n) is a linearly recurrent sequence. Its characteristic polynomial is $x^2 - Tx + N$. It follows from [11, Thm 6.55] that (a_n) is linearly recurrent with characteristic polynomial equal to

$$g(x) = (x-1)(x-N)(x^2-Tx+N) \in \mathbb{F}_\ell[x].$$

Recall that if $g(0) \neq 0$, $\operatorname{ord} g(x)$ is defined to be the least n such that $g(x)$ divides $x^n - 1$. By [11, Thm 6.27], the least period of $(a_n \pmod{\ell})$ divides $\operatorname{ord} g(x)$, and by [11, Thm 3.11], there is some $A \geq 0$ such that

$$\operatorname{ord} g(x) = LCM[\operatorname{ord}(x-1), \operatorname{ord}(x-N), \operatorname{ord}(x^2-Tx+N)]\ell^A.$$

The integer A reflects the possible presence of repeated factors of $g(x)$. If $x-1$, $x-N$, and x^2-Tx+N are coprime in $\mathbb{F}_\ell[x]$, then $A=0$. □

6. Lifting the Exponent

The periodic point counts established in the previous sections all contain an expression of the form $v_P(x^n-\gamma)$, where P is a prime ideal of an endomorphism ring R. In this section we develop formulas for writing these expressions in terms of $v_p(n)$. These resemble a result in elementary number theory popularly known as "lifting the exponent", which is related to (but does not follow from) Hensel's Lemma.

Lemma 6.1. *Let K be a number field. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ lying over the rational prime p, and let e be the ramification index of $\mathfrak{p}$ over p. Let $x,y\in\mathcal{O}_K$ be such that $x,y\notin\mathfrak{p}$ and $x-y\in\mathfrak{p}$. If $e+1\geq p-1$, further assume that $v_\mathfrak{p}(x-y)\geq\frac{e+1}{p-1}$. Then*

$$v_\mathfrak{p}(x^n-y^n)=v_\mathfrak{p}(x-y)+ev_p(n).$$

Proof. The proof is by induction on $v_p(n)$. Assume that $x\neq y$; otherwise the proposition holds trivially.

First suppose that $v_p(n)=0$, which guarantees $v_\mathfrak{p}(n)=0$. We compute

$$v_\mathfrak{p}(x^n-y^n)=v_\mathfrak{p}(x-y)+v_\mathfrak{p}(x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1}).$$

As $x-y\in\mathfrak{p}$, we have $x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1}\equiv nx^n \pmod{\mathfrak{p}}$, and $nx^n\notin\mathfrak{p}$. Therefore $v_\mathfrak{p}(x^n-y^n)=v_\mathfrak{p}(x-y)$, proving the proposition in this case.

If we show that the proposition holds for $n=p$, it follows for all n by induction. Let $v=v_\mathfrak{p}(x-y)$, so that $x=y+z$ for some $z\in\mathfrak{p}^v\setminus\mathfrak{p}^{v+1}$. By the binomial theorem,

$$x^p=\sum_{i=0}^{p}\binom{p}{i}z^iy^{p-i}\equiv y^n+pzy^{n-1}\pmod{\mathfrak{p}^{v+e+1}}.$$

For $i\geq 2$, the ith term of the expansion is in $\mathfrak{p}^{v+e+1}$. If $i\neq p$ this is because p divides $\binom{p}{i}$, so $\binom{p}{i}\in\mathfrak{p}^e$ and $\binom{p}{i}z^iy^{n-i}$ lies in $\mathfrak{p}^{e+iv}\subseteq\mathfrak{p}^{v+e+1}$, as $v\geq 1$. If $i=p$, this is because we assumed that $v=v_\mathfrak{p}(z)\geq\frac{e+1}{p-1}$, so $v_\mathfrak{p}(z^p)=pv\geq v+e+1$ and $z^p\in\mathfrak{p}^{v+e+1}$. The $i=1$ term is not in $\mathfrak{p}^{v+e+1}$, as $v_\mathfrak{p}(pz)=e+1$. Therefore $x^p-y^p\in\mathfrak{p}^{v+e}\setminus\mathfrak{p}^{v+e+1}$, so $v_\mathfrak{p}(x^p-y^p)=v+e$ and we are done. □

Lemma 6.2. *Let p be a prime. Let B be the unique quaternion algebra over $\mathbb{Q}$ ramified precisely at p and ∞, and let $\mathcal{O}$ be a maximal order of B. Let π be a uniformizer for $\mathcal{O}_p$, and let $I=\pi\mathcal{O}_p\cap\mathcal{O}$. Let $x,y\in\mathcal{O}$ be such*

that $x, y \notin I$ and $x - y \in I$. If $p = 3$, assume further that $v_I(x-y) \geq 2$, and if $p = 2$, assume further that $v_I(x-y) \geq 3$. Then

$$v_I(x^n - y^n) = v_I(x-y) + 2v_p(n).$$

Proof. The proof is essentially the same as the proof of Lemma 6.1, and is omitted. □

Lemma 6.3. *Let k be an algebraically closed field of characteristic p, and let $k\langle\phi\rangle$ be the noncommutative polynomial ring with the multiplication rule $\phi c = c^p \phi$ for $c \in k$. Let $x \in k\langle\phi\rangle$ be such that $x - 1 \in \phi k\langle\phi\rangle$. Then*

$$v_\phi(x^n - 1) = v_\phi(x-1)p^{v_p(n)}.$$

Proof. First assume that $v_p(n) = 0$. Then

$$x^n - 1 = (1 + (x-1))^n - 1 \equiv n(x-1) \pmod{\phi^{2v_\phi(x-1)} k\langle\phi\rangle},$$

and $v_\phi(x^n - 1) = v_\phi(x-1)$.

Next let $n = p$. As $x^p - 1 = (x-1)^p$, we have $v_\phi(x^p - 1) = pv_\phi(x-1)$. The proposition follows by induction on $v_p(n)$. □

7. Background from Automatic Sequences

This section contains several results from the theory of finite automata and automatic sequences. A sequence (a_n) is k-automatic if it can be produced as the output of a deterministic finite automaton that takes as input the base-k expansion of the integer n. The theorems in this section are stated so that they can be used later without any specific knowledge of finite automata or automatic sequences. A good introduction to the theory can be found in [1].

The next two theorems underlie our proof of transcendence. Christol's theorem gives a correspondence between automatic sequences and algebraic power series, and Cobham's theorem shows that the only sequences that are automatic with respect to two multiplicatively independent bases are eventually periodic sequences.

Theorem 7.1 (Christol)**.** *The formal power series $\sum_{n=0}^{\infty} a_n t^n \in \mathbb{F}_p[[t]]$ is algebraic over $\mathbb{F}_p(t)$ if and only if the sequence (a_n) is p-automatic.*

Proof. [1, Thm 12.2.5]. □

Theorem 7.2 (Cobham)**.** *Suppose p and q are positive integers that are multiplicatively independent (i.e. $\log p / \log q \notin \mathbb{Q}$). If the sequence (a_n) is both p-automatic and q-automatic, then it is eventually periodic.*

Proof. [1, Thm 11.2.2]. □

The converse to Cobham's theorem is also true.

Theorem 7.3. *Let (a_n) be eventually periodic. Then (a_n) is k-automatic for every positive integer k.*

Proof. [1, Thm 5.4.2]. □

The following is a corollary to Christol's theorem that will be used to derive the contradiction that shows that ζ_f is transcendental.

Corollary 7.4. *If $\sum_{n=0}^{\infty} a_n t^n \in \mathbb{Z}[[t]]$ is algebraic over $\mathbb{Q}(t)$, then for every prime p, the reduced sequence $((a_n) \bmod p)$ is p-automatic.*

Proof. [1, Thm 12.6.1]. □

The next two propositions shows that the set of p-automatic sequences over a ring is closed under both the pointwise application of arithmetic operations and the operation of extracting subsequences that are indexed by arithmetic progressions.

Proposition 7.5. *Let (a_n) and (b_n) be p-automatic sequences with entries in the ring R, and let $c \in R$. The sequences $(a_n + b_n)$, $(a_n b_n)$, and (ca_n) are p-automatic, as is the sequence (a_n^{-1}) if each a_n is invertible. Also, the subsequence (a_{mn+b}) is p-automatic for any $m, b \in \mathbb{Z}_+$.*

Proof. The closure properties under arithmetic operations are special cases of the general theorem that the set of p-automatic sequences with entries in the set Δ is closed under the pointwise application of any binary operation $(\cdot,\cdot) : \Delta \times \Delta \to \Delta$ [1, Cor 5.4.5] and the completely trivial theorem that it is closed under the pointwise application of any unary operation $(\cdot) : \Delta \to \Delta$ (this follows directly from the definition of an automatic sequence). For the claim about the subsequences (a_{mn+b}), see [1, Thm 6.8.1]. □

Propositions 7.6 and 7.7 are the major technical results of this section. They will be needed to produce a contradiction at key moments in the proof of Theorems 1.2 and 1.3.

Proposition 7.6. *Let p and ℓ be distinct primes. Suppose $a \in \mathbb{Z}_+$, $a \not\equiv 1 \pmod{\ell}$, and $(a, \ell) = 1$. Also suppose $\alpha, \beta \in \mathbb{Z}$, $\alpha \neq 0$, and $v_p(\alpha) \leq v_p(\beta)$. Let the sequence (a_n) with entries in $\mathbb{Z}/\ell\mathbb{Z}$ be defined by*

$$a_n = a^{v_p(\alpha n + \beta)} \pmod{\ell}.$$

The sequence (a_n) is not ℓ-automatic.

Proof. Let d be the multiplicative order of $a \bmod \ell$. It follows from the assumptions that d exists and $d > 1$. The sequence $n \mapsto a^{v_p(n)}$ is a function of the equivalence class of $v_p(n) \bmod d$, so it is p-automatic by [4, Lem 6]. Therefore the sequence (a_n) is p-automatic by Proposition 7.5.

Assume by way of contradiction that (a_n) is ℓ-automatic. Any distinct primes are multiplicatively independent, so by Cobham's theorem, (a_n) is

eventually periodic. Let c be its eventual period, so that $a_{n+xc} = a_n$ for sufficiently large n and every positive x. This means that

$$a^{v_p(\alpha n+\beta)} \equiv a^{v_p(\alpha(n+xc)+\beta)} \pmod{\ell}, \tag{7.1}$$

which implies that

$$v_p(\alpha n + \beta) \equiv v_p(\alpha(n + xc) + \beta) \pmod{d}. \tag{7.2}$$

Let $\alpha' = \alpha/p^{v_p(\alpha)}$ and $\beta' = \beta/p^{v_p(\alpha)}$. It is clear that $(p, \alpha') = 1$, and it follows from our assumption that $v_p(\alpha) \leq v_p(\beta)$ that β' is an integer. So

$$v_p(\alpha' n + \beta') \equiv v_p(\alpha'(n + xc) + \beta') \pmod{d}. \tag{7.3}$$

Let $m = v_p(c)$ so that $c' = c/p^m$ and $(p, c') = 1$. We can solve

$$\alpha' n \equiv -\beta' + p^m \pmod{p^{m+2}} \tag{7.4}$$

for n, and choose such an n to be large enough so that the sequence (a_n) is periodic at n. Therefore $v_p(\alpha' n + \beta') = m$. We can also solve

$$\alpha' c' x \equiv p - 1 \pmod{p^{m+2}} \tag{7.5}$$

for x, and choose such an x to be positive. Adding Equation 7.4 and p^m times Equation 7.5 gives

$$\alpha'(n + xc) \equiv -\beta' + p^{m+1} \pmod{p^{m+2}} \tag{7.6}$$

and therefore $v_p(\alpha'(n + xc) + \beta') = m + 1$. So by Equation 7.3,

$$m \equiv m + 1 \pmod{d}. \tag{7.7}$$

As $d > 1$, this is a contradiction. □

Proposition 7.7. *Let $a \in \mathbb{Z}_+$ and let p and ℓ be primes so that $\ell > p^{ap^a}$. If p is odd, also assume that $(p, \ell - 1) = 1$. If $p = 2$, instead assume that $\ell \equiv 7 \pmod 8$. Let the sequence (a_n) with entries in $\mathbb{Z}/\ell\mathbb{Z}$ be defined by*

$$a_n = p^{ap^{v_p(n)}} \pmod{\ell}.$$

The sequence (a_n) is not ℓ-automatic.

Proof. Let d be the multiplicative order of p^a mod ℓ. Since $\ell > p^{ap^a}$, we have $d > p^a$. The sequence a_n is a function of the equivalence class of $p^{v_p(n)}$ mod d.

First assume that p is odd. Then $(p^a, \ell - 1) = 1$, and as d divides $\ell - 1$, also $(p^a, d) = 1$. Let e be the multiplicative order of p^a mod d, and note that $e \geq 2$. So $a_n = a_m$ iff $p^{v_p(n)} \equiv p^{v_p(m)} \pmod d$ iff $v_p(n) \equiv v_p(m) \pmod e$. In particular, a_n is a function of the equivalence class of $v_p(n)$ mod e. By [4, Lem 6], (a_n) is p-automatic.

If instead $p = 2$, then $\ell \equiv 7 \pmod 8$, so 2 is a quadratic residue mod ℓ. It follows that d divides $\frac{\ell-1}{2}$, so d is odd and $(p, d) = 1$. Let e be the

multiplicative order of p mod d, and again note that $e \geq 2$, so again $a_n = a_m$ if and only if $v_p(n) \equiv v_p(m) \pmod{e}$. In particular, (a_n) is p-automatic.

Assume that (a_n) is also ℓ-automatic. It follows from Cobham's theorem that (a_n) is eventually periodic. Let c be its eventual period. For n large and $x > 0$,

$$v_p(n + xc) \equiv v_p(n) \pmod{e}. \tag{7.8}$$

But this is impossible by the argument in the proof of Proposition 7.6; simply set $\alpha = 1$ and $\beta = 0$. □

8. Proof of Theorem 1.2

Let k be an algebraically closed field of characteristic p, and let $f \in k(x)$ be a separable power map, Chebyshev polynomial, or Lattès map. Let $\zeta = \zeta(f, \mathbb{P}^1(k); t)$. Assume by way of contradiction that ζ is algebraic over $\mathbb{Q}(t)$. Its derivative ζ' is algebraic, so its logarithmic derivative ζ'/ζ is algebraic. We compute

$$\zeta'/\zeta = (\log \zeta)' = \sum_{n \geq 1} \#\operatorname{Per}_n(f) t^{n-1}.$$

By Corollary 7.4, for any prime ℓ, the reduction mod ℓ of the sequence $(\#\operatorname{Per}_n(f))$ is ℓ-automatic. By carefully choosing ℓ, we will produce a contradiction, showing that ζ is transcendental.

8.1. Power Maps and Chebyshev Polynomials. Let f be the power map $f(x) = x^d$, and note that $(p, d) = 1$ because f is separable. Let m be even and such that $d^m \equiv 1 \pmod{p}$. Let $\ell > p$ be a prime to be determined, and consider the sequence (a_n) with entries in $\mathbb{F}_\ell$ given by

$$a_n = \#\operatorname{Per}_{mn}(f) \pmod{\ell}.$$

By Proposition 7.5, (a_n) is ℓ-automatic. As mn is even, Equation 3.4 and Proposition 6.1 give

$$a_n = 2 + \frac{d^{mn} - 1}{p^{v_p(d^{mn}-1)}} = 2 + (d^{mn} - 1)(p^{-1})^{v_p(d^m-1)+v_p(n)}.$$

First suppose p is odd. Note that $(d^{mn} - 1) = d^m - 1$ when $n \equiv 1 \pmod{\ell - 1}$, and that $d^m - 1 \not\equiv 0 \pmod{\ell}$. Consider the subsequence

$$b_n = (d^m - 1)(p^{v_p(d^m-1)})^{-1}(a_{(\ell-1)n+1} - 2)^{-1},$$

which is ℓ-automatic by proposition 7.5. Then

$$b_n = p^{v_p((\ell-1)n+1)}.$$

Choose ℓ such that $\ell \equiv 2 \pmod{p}$. Then $v_p(\ell - 1) = 0 = v_p(1)$, and by Proposition 7.6, (b_n) is not automatic, which is a contradiction.

Now suppose $p = 2$. Let $m = 2$, so that $d^m \equiv 1 \pmod 4$ (the separability of f forces d to be odd). Let b_n be given by

$$b_n = (d^2 - 1)(p^{v_p(d^2-1)})^{-1}(a_{(\ell-1)n+2} - 2)^{-1},$$

so that

$$b_n = p^{v_p((\ell-1)n+2)}.$$

Choose ℓ such that $\ell \equiv 3 \pmod 4$ and $(\ell, d^2 - 1) = 1$. Then we have $v_p(\ell - 1) = 1 = v_p(2)$, and again Proposition 7.6 gives a contradiction.

Now let f be the dth Chebyshev polynomial. Again it must be true that $(p, d) = 1$, because otherwise the $\psi(x)$ that fits into Diagram 2.1 factors through the pth power map and is inseparable, so f is also inseparable. Let m be such that $d^m \equiv 1 \pmod p$, and let $a_n = \#\operatorname{Per}_{mn}(f) \pmod \ell$ for some ℓ to be determined. By equation 3.6 and Proposition 6.1,

$$\begin{aligned} a_n &= 1 + \frac{1}{2}\left(\frac{d^{mn} - 1}{p^{v_p(d^{mn}-1)}} + \frac{d^{mn} + 1}{p^{v_p(d^{mn}+1)}}\right) \\ &= 1 + \frac{1}{2}\left((d^{mn} - 1)(p^{-1})^{v_p(d^m-1)+v_p(n)} + (d^{mn} + 1)(p^{-1})^{v_p(d^{mn}+1)}\right). \end{aligned}$$

First suppose p is odd. Then $v_p(d^{mn} + 1) = 0$ because $v_p(d^{mn} - 1) > 0$ by Proposition 6.1. The sequence

$$n \mapsto (d^{mn} + 1)$$

is periodic, and so is ℓ-automatic. Let b_n be defined by

$$b_n = (2(a_{(\ell-1)n+1} - 1) - (d^{m(\ell-1)n+1}))(d^m - 1)^{-1}(p^{v_p(d^m-1)}).$$

As before, b_n is ℓ-automatic, but

$$b_n^{-1} = p^{v_p((\ell-1)n+1)}.$$

Choosing $\ell \equiv 2 \pmod p$ gives a contradiction by Proposition 7.6.

If $p = 2$, then let $m = 2$. In this case, $d^{2n} \equiv 1 \pmod 4$ for all n, so $v_p(d^{2n} + 1) = 1$. The sequence

$$n \mapsto (d^{2n} + 1)$$

is still eventually periodic, so using the same manipulations as above, the sequence

$$b_n^{-1} = p^{v_p((\ell-1)n+2)}$$

is ℓ-automatic. If we pick ℓ such that $\ell \equiv 3 \pmod 4$ and $(\ell, d^2 - 1) = 1$, then $v_p(\ell - 1) = 1$ and again this is a contradiction by Proposition 7.6.

8.2. Lattès Maps. Let f be a Lattès map associated to the elliptic curve E. If $j(E)$ is transcendental over $\overline{\mathbb{F}}_p$, then $\sigma \in \mathbb{Z}$, and as f is separable we have $(p, \sigma) = 1$ (otherwise σ would be inseparable). By equation 5.1,

$$\#\operatorname{Per}_n(f) = \frac{1}{2}\left(\frac{|\sigma^n - 1|}{p^{v_p(\sigma^n - 1)}} + \frac{|\sigma^n + 1|}{p^{v_p(\sigma^n + 1)}}\right).$$

If $\sigma > 0$, then this is the same as the periodic point count for the degree $|\sigma|$ Chebyshev polynomial $T_{|\sigma|}$, and we have already shown that there exists an ℓ such that $\#\operatorname{Per}_n(f) \pmod{\ell}$ is not ℓ-automatic. In fact, the argument also goes through if $\sigma < 0$, as we simply choose an even m and use the subsequence $\#\operatorname{Per}_{mn}(f) \pmod{\ell}$, in which case σ^{mn} is always positive.

Now suppose $j(E) \in \overline{\mathbb{F}}_p$ and E is ordinary. The ring $\operatorname{End}(E)$ is an order in an imaginary quadratic field K, and $\operatorname{Aut}(E)$ is cyclic of order 2,4, or 6. Therefore Γ is isomorphic to one of μ_2, μ_3, μ_4, or μ_6. By Proposition 5.2, there is a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that

$$\#\operatorname{Per}_n(f) = \frac{1}{|\Gamma|}\sum_{\gamma \in \Gamma} \frac{N(\sigma^n - \gamma)}{p^{v_{\mathfrak{p}}(\sigma^n - \gamma)}},$$

and $\mathfrak{p}$ is the extension to $\mathcal{O}_K$ of the ideal in $\operatorname{End}(E)$ that consists of all inseparable isogenies, so $\sigma \notin \mathfrak{p}$.

Assume for the moment that $p \notin \{2, 3\}$. Let m be the multiplicative order of the image of σ in the residue field $\mathcal{O}_K/\mathfrak{p}$, so that $\sigma^m - 1 \in \mathfrak{p}$. By Proposition 6.1,

$$v_{\mathfrak{p}}(\sigma^{mn} - 1) = v_{\mathfrak{p}}(\sigma^m - 1) + v_p(n).$$

In particular, $\sigma^{mn} - 1 \in \mathfrak{p}$ for $n \geq 1$. We argue that $\sigma^{mn} - \gamma \notin \mathfrak{p}$ for $\gamma \in \Gamma \setminus \{1\}$.

If $\sigma^{mn} - \gamma$ were in $\mathfrak{p}$, then $1 - \gamma$ would be in $\mathfrak{p}$, and $p = N(\mathfrak{p})$ would divide $N(1 - \gamma)$. We compute

$$N(1 - \gamma) \;=\; (1 - \gamma)(1 - \hat{\gamma}) \;=\; 1 - \operatorname{tr}(\gamma) + N(\gamma) \;=\; 2 - \operatorname{tr}(\gamma).$$

As γ is a root of the kth cyclotomic polynomial for some $k \in \{2, 3, 4, 6\}$, it follows that $\operatorname{tr}(\gamma) \in \{-2, -1, 0, 1\}$. Therefore $N(1 - \gamma) \in \{1, 2, 3, 4\}$, so $v_p(N(1 - \gamma)) = 0$ and $1 - \gamma \notin \mathfrak{p}$, so $\sigma^{mn} - \gamma \notin \mathfrak{p}$. Therefore

$$\#\operatorname{Per}_{mn}(f) = \frac{1}{|\Gamma|}\frac{N(\sigma^{mn} - 1)}{p^{v_{\mathfrak{p}}(\sigma^m - 1) + v_p(n)}} + \frac{1}{|\Gamma|}\sum_{\gamma \in \Gamma \setminus \{1\}} N(\sigma^{mn} - \gamma).$$

Let $\ell > p$ be a rational prime to be determined. For now, assume that $(\ell, N(\sigma)) = (\ell, |\Gamma|) = 1$. Each sequence $n \mapsto N(\sigma^{mn} - \gamma) \pmod{\ell}$ is periodic and therefore ℓ-automatic. It follows that the sequence given by

$$a_n = \frac{1}{|\Gamma|}\frac{N(\sigma^{mn} - 1)}{p^{v_{\mathfrak{p}}(\sigma^m - 1) + v_p(n)}} \pmod{\ell}$$

is ℓ-automatic. By Proposition 5.4, the sequence $n \mapsto N(\sigma^{mn} - 1) \pmod{\ell}$ is periodic of period dividing $(\ell - 1)(\ell^2 - 1)\ell^A$ for some A. Let c be this period. Choose $\ell \equiv 2 \pmod{p}$ subject to the previous restrictions on ℓ and such that $(\ell, N(\sigma^m - 1)) = 1$. Therefore

$$N(\sigma^{m(cn+1)} - 1) \equiv N(\sigma^m - 1) \not\equiv 0 \pmod{\ell}.$$

By the closure properties of Proposition 7.5, the sequence given by

$$n \mapsto p^{v_p(cn+1)} \pmod{\ell}$$

is ℓ-automatic. We know $(p, \ell) = (p, \ell - 1) = (p, \ell^2 - 1) = 1$, so $v_p(c) = 0$. So $v_p(c) \leq v_p(1) = 1$, and this is a contradiction by Proposition 7.6.

If $p \in \{2, 3\}$, then $\mathrm{Aut}(E) \cong \mu_2$, as the only possible larger automorphism groups in characteristic 2 or 3 are nonabelian and cannot be realized as subgroups of $\mathcal{O}_K^\times$ [14, Appendix A]. Therefore $\Gamma = \mathrm{Aut}(E) = \{\pm 1\}$.

First assume that $p = 3$. Everything in the above argument holds, except possibly that c, the period of $n \mapsto N(\sigma^{mn} - 1) \pmod{\ell}$, might be divisible by 3. Choose ℓ such that $\ell \equiv 2 \pmod{9}$ and $(\ell, N(\sigma^{3m} - 1)) = 1$. By Proposition 5.4, $v_3(c) \leq v_3((\ell - 1)(\ell^2 - 1)\ell^A) = 1$. The contradiction by Proposition 7.6 now comes from manipulating (a_{cn+3}) to produce the sequence

$$n \mapsto 3^{v_3(cn+3)} \pmod{\ell}.$$

Now assume that $p = 2$. As $\sigma \notin \mathfrak{p}$, the image of σ in the finite ring $\mathcal{O}_K/\mathfrak{p}^2$ is invertible. Let m be the multiplicative order of the image of σ, so that $\sigma^m - 1 \in \mathfrak{p}^2$. Using Lemma 6.1 and following the above argument, we arrive at

$$\#\operatorname{Per}_{mn}(f) = \frac{1}{2}\left(\frac{N(\sigma^{mn} - 1)}{2^{v_\mathfrak{p}(\sigma^{mn}-1)}} + \frac{N(\sigma^{mn} + 1)}{2^{v_\mathfrak{p}(\sigma^{mn}+1)}}\right)$$

As $v_\mathfrak{p}(\sigma^m - 1) \geq 2$, we have $v_\mathfrak{p}(\sigma^{mn} - 1) \geq 2$ for all n. By properties of valuations,

$$v_\mathfrak{p}(\sigma^{mn} + 1) = \min(v_\mathfrak{p}(\sigma^{mn} - 1), v_\mathfrak{p}(2)) = 1,$$

where $v_\mathfrak{p}(2) = 1$ because 2 splits in K. Therefore

$$\#\operatorname{Per}_{mn}(f) = \frac{1}{2}\left(\frac{N(\sigma^{mn} - 1)}{2^{v_\mathfrak{p}(\sigma^{mn}-1)}} + \frac{N(\sigma^{mn} + 1)}{2}\right).$$

Again the only difficulty is that c, the period of $n \mapsto N(\sigma^{mn} - 1) \pmod{\ell}$, might be even. Choose $\ell \equiv 3 \pmod{8}$ such that $(\ell, N(\sigma^{16m} - 1)) = 1$. Now $v_2(c) \leq v_2((\ell - 1)(\ell^2 - 1)\ell^A) = 4$, and the same contradiction comes from the sequence

$$n \mapsto 2^{v_2(cn+16)} \pmod{\ell}.$$

Now suppose that E is supersingular. In this case $\mathrm{End}(E)$ can be identified with a maximal order $\mathcal{O}$ of a rational quaternion algebra B that is ramified only at p and ∞. Let I be the two-sided maximal ideal of $\mathcal{O}$

from Proposition 5.3. As $\sigma : E \to E$ is separable, $\sigma \notin I$. Let m be the multiplicative order of σ in the residue field $\mathcal{O}/I$, so that $v_I(\sigma^m - 1) \geq 1$.

Assume first that $p \notin \{2, 3\}$ so that $\Gamma \cong \mu_2$, μ_3, μ_4, or μ_6. By Proposition 5.3 and Lemma 6.2,

$$v_I(\sigma^{mn} - 1) = v_I(\sigma^m - 1) + 2v_p(n).$$

As in the case of E ordinary, for $\xi \in \Gamma \backslash \{1\}$, ξ is a root of the kth cyclotomic polynomial some for $k \in \{2, 3, 4, 6\}$, so $N(1-\xi) \in \{1, 2, 3, 4\}$. Norm considerations show that $\sigma^{mn} - \xi \notin I$ for $n \geq 1$, so $\#\ker(\sigma^{mn} - \xi) = N(\sigma^{mn} - \xi)$. Therefore

$$\#\operatorname{Per}_{mn}(f) = \frac{1}{|\Gamma|} \frac{N(\sigma^{mn} - 1)}{p^{v_I(\sigma^m - 1) + 2v_p(n)}} + \frac{1}{|\Gamma|} \sum_{\xi \in \Gamma \backslash \{1\}} N(\sigma^{mn} - \xi).$$

The same reasoning as in the ordinary case shows that there is a prime ℓ such that $\#\operatorname{Per}_{mn}(f) \pmod{\ell}$ is not ℓ-automatic.

Now assume that $p \in \{2, 3\}$. If $j(E) \neq 0$, then $\operatorname{Aut}(E) = \{\pm 1\}$, and the argument proceeds exactly as when E is ordinary. Therefore assume that $j(E) = 0$. For both the cases $p = 2$ and $p = 3$, the maximal order $\mathcal{O}$ has trivial class group and is therefore the unique maximal order of B up to conjugacy [17, Ch 1, Cor 4.11]. Therefore, for the purposes of identifying $\operatorname{End}(E)$ with $\mathcal{O}$, we may take $\mathcal{O}$ to be any maximal order of B.

First let $p = 2$. In this case, B is the Hamilton quaternions given by $\left(\frac{-1,-1}{\mathbb{Q}}\right) = \mathbb{Q}(i, j)$ where $i^2 = j^2 = -1$ and $k = ij$. A maximal order of B is given by the Hurwitz quaternions

$$\mathcal{O} = \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k + \mathbb{Z}(1 + i + j + k)/2.$$

Here $\operatorname{Aut}(E) \cong \mathrm{SL}_2(\mathbb{F}_3)$ can be described explicitly as

$$\operatorname{Aut}(E) \cong \mathcal{O}^\times = \{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}.$$

For $\gamma \in \operatorname{Aut}(E)$, explicit calculation of norms shows that $v_I(1 - \gamma) = 0$ unless $\gamma \in \{\pm 1, \pm i, \pm j, \pm k\} \cong Q_8$, which is the unique Sylow 2-subgroup of $\operatorname{Aut}(E)$. As $\sigma \notin I$, the image of σ is invertible in $\mathcal{O}/I^3$. Pick m such that $\sigma^m - 1 \in I^3$, i.e. $v_I(\sigma^m - 1) \geq 3$. Then for $\gamma \neq 1$,

$$v_I(\sigma^{mn} - \gamma) = \min\{v_I(\sigma^{mn} - 1), v_I(1 - \gamma)\} = \begin{cases} 2 & : \gamma = -1 \\ 1 & : \gamma = \pm i, \pm j, \pm k \\ 0 & : \text{otherwise} \end{cases}$$

So for each $\gamma \in \Gamma$, there exists a constant $C(\gamma)$ such that

$$\#\operatorname{Per}_{mn}(f) = \frac{1}{|\Gamma|} \left(\frac{N(\sigma^{mn} - 1)}{2^{v_I(\sigma^m - 1) + 2v_2(n)}} + \sum_{\gamma \in \Gamma \backslash \{1\}} \frac{N(\sigma^{nm} - \gamma)}{C(\gamma)} \right)$$

Choosing ℓ appropriately, we can reduce this to the sequence

$$n \mapsto 4^{v_2(cn+16)}$$

and get a contradiction as before.

Now let $p = 3$, so that $B = \left(\frac{-1,-3}{\mathbb{Q}}\right) = \mathbb{Q}(i,j)$ where $i^2 = -1$, $j^2 = -3$, and $k = ij$. A maximal order $\mathcal{O}$ is given by

$$\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}(1+j)/2 + \mathbb{Z}(i+k)/2$$

and again $\mathrm{Aut}(E) \cong C_3 \rtimes C_4$ has an explicit description as

$$\mathrm{Aut}(E) \cong \mathcal{O}^\times = \{\pm 1, \pm i, (\pm 1 \pm j)/2, (\pm i \pm k)/2\}.$$

For $\gamma \in \mathrm{Aut}(E)$, another norm calculation shows that $v_I(1-\gamma) = 0$ unless $\gamma \in \{1, \frac{-1\pm j}{2}\} \cong C_3$, the unique Sylow 3-subgroup of $\mathrm{Aut}(E)$. Pick m such that $v_I(\sigma^m - 1) \geq 2$. If $\gamma \neq 1$,

$$v_I(\sigma^{mn} - \gamma) = \min\{v_I(\sigma^{mn}-1), v_I(1-\gamma)\} = \begin{cases} 1 & : \gamma = (-1 \pm j)/2 \\ 0 & : \text{otherwise} \end{cases}$$

As above, there are $C(\gamma)$ so that

$$\#\operatorname{Per}_{mn}(f) = \frac{1}{|\Gamma|}\left(\frac{N(\sigma^{mn}-1)}{3^{v_I(\sigma^m-1)+2v_3(n)}} + \sum_{\gamma \in \Gamma \setminus \{1\}} \frac{N(\sigma^{mn}-\gamma)}{C(\gamma)})\right).$$

We can reduce this to the sequence

$$n \mapsto 9^{v_3(c_n+3)}$$

and the same argument gives a contradiction.

9. Proof of Theorem 1.3

Let k be an algebraically closed field of characteristic p, and let $f \in k[x]$ be an additive or subadditive polynomial. The map f fits into Diagram 2.1 with $G = \mathbb{G}_a$, $\Gamma \cong \mu_d$, and $\pi(x) = x^d$, where possibly $d = 1$. Therefore $\psi(x)^d = f(x^d)$. As usual, let ψ be the endomorphism σ composed with a translation.

Let a be the constant term of $\sigma \in k\langle\phi\rangle$, so that $\sigma = a + (\phi)$ (that is, $\sigma(x) = ax + g(x)$ for some $g \in (\phi)$). If $d = 1$, then $f(x)$ is $\sigma(x)$ composed with a translation, so $f'(0) = a$. If $d \geq 2$, then $\psi(\omega_d x) = \omega_d \psi(x)$, so $\psi(0) = 0$ and $\psi = \sigma$. So $\sigma^d = a^d + (\phi)$, and $f'(0) = a^d$. Therefore $f'(0)$ is algebraic if and only if a is algebraic.

By equation (4.1),

$$\#\operatorname{Per}_n(f) = 1 + \frac{1}{d}\sum_{\omega \in \mu_d} \frac{(\deg \sigma)^n}{p^{v_\phi(\sigma^n - \omega)}}.$$

As σ is separable, $v_\phi(\sigma) = 0$, so $a \neq 0$.

If $f'(0)$ is transcendental, then so is a. The constant term of $\sigma^n - \omega$ is $a^n - \omega$, which is never zero (if it were, a would be algebraic). Therefore

$$\#\operatorname{Per}_n(f) = 1 + \frac{1}{d}\sum_{\omega\in\mu_d}(\deg\sigma)^n = 1 + (\deg\sigma)^n.$$

It follows easily that $\zeta(f, \mathbb{P}^1(k); t)$ is rational.

Suppose $f'(0)$ is algebraic over $\mathbb{F}_p$, so a is algebraic and therefore is a root of unity. Aiming for a contradiction, assume that $\zeta(f, \mathbb{P}^1(k); t)$ is algebraic. There exists m such that the image of σ^m in $k\langle\phi\rangle/(\phi)$ is 1, and so $\sigma^m - 1 \in (\phi)$. By Lemma 6.3, for $n \geq 1$,

$$v_\phi(\sigma^{mn} - 1) = v_\phi(\sigma^m - 1)p^{v_p(n)}.$$

In particular, $\sigma^{mn} - 1 \in (\phi)$. Therefore, for $\omega \in \mu_d \setminus \{1\}$, we must have $\sigma^{mn} - \omega \notin (\phi)$, because otherwise $1 - \omega$ would be in (ϕ). But the element $1 - \omega \in k\langle\phi\rangle$ represents the linear polynomial $x \mapsto (1 - \omega)x$, which does not factor through $\phi : x \mapsto x^p$. Therefore

$$\#\operatorname{Per}_{mn}(f) = 1 + \frac{1}{d}\left(\frac{(\deg\sigma)^n}{p^{v_\phi(\sigma^m-1)p^{v_p(n)}}} + \sum_{\omega\in\mu_d\setminus\{1\}}(\deg\sigma)^n\right).$$

Let ℓ be a prime. If p is odd, choose ℓ such that $\ell \equiv 2 \pmod p$, and if $p = 2$, choose $\ell \equiv 7 \pmod 8$. Let $a_n = \#\operatorname{Per}_{mn} \pmod \ell$. Note that $n \mapsto (\deg\sigma)^n$ is periodic and therefore ℓ-automatic. By Proposition 7.5, we can manipulate a_n to arrive at the sequence

$$b_n = (\deg\sigma)^n p^{-p^{\left(v_\phi(\sigma^m-1)p^{v_p(n)}\right)}},$$

which is ℓ-automatic. The subsequence $b_{(\ell-1)n}$ is ℓ-automatic, as is its reciprocal

$$(b_{(\ell-1)n})^{-1} = p^{p^{\left(v_\phi(\sigma^m-1)p^{v_p(n)}\right)}}.$$

For a large enough prime ℓ, the above sequence satisfies the assumptions of Proposition 7.7, so it is not ℓ-automatic, which is a contradiction.

Acknowledgements. We would like to thank Michael Zieve for drawing our attention to the results in [7], Tonghai Yang for helpful advice regarding quaternion algebras, and Bjorn Poonen for pointing out the counterexample to Conjecture 1.4 in the case where k contains transcendentals over $\mathbb{F}_p$. This research was partly supported by NSF Grant no. EMSW21-RTG and by the Wisconsin Alumni Research Foundation.

References

[1] J.-P. Allouche & J. Shallit, *Automatic sequences*, Cambridge University Press, Cambridge, 2003, Theory, applications, generalizations, xvi+571 pages.

[2] M. Artin & B. Mazur, "On periodic points", *Ann. of Math. (2)* **81** (1965), p. 82-99.

[3] M. P. Bellon & C.-M. Viallet, "Algebraic entropy", *Comm. Math. Phys.* **204** (1999), no. 2, p. 425-437.

[4] A. Bridy, "Transcendence of the Artin-Mazur zeta function for polynomial maps of $\mathbb{A}^1(\overline{\mathbb{F}}_p)$", *Acta Arith.* **156** (2012), no. 3, p. 293-300.

[5] D. A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication, xviii+356 pages.

[6] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper", *Abh. Math. Sem. Hansischen Univ.* **14** (1941), p. 197-272.

[7] D. Ghioca & M. Zieve, "Lattes maps in arbitrary characteristic", in preparation.

[8] B. Hasselblatt & J. Propp, "Degree-growth of monomial maps", *Ergodic Theory Dynam. Systems* **27** (2007), no. 5, p. 1375-1397.

[9] A. Hinkkanen, "Zeta functions of rational functions are rational", *Ann. Acad. Sci. Fenn. Ser. A I Math.* **19** (1994), no. 1, p. 3-10.

[10] I. M. Isaacs, *Algebra*, Brooks/Cole Publishing Co., Pacific Grove, CA, 1994, A graduate course, xii+516 pages.

[11] R. Lidl & H. Niederreiter, *Introduction to finite fields and their applications*, first ed., Cambridge University Press, Cambridge, 1994, xii+416 pages.

[12] J. Milnor, "On Lattès maps", in *Dynamics on the Riemann sphere*, Eur. Math. Soc., Zürich, 2006, p. 9-43.

[13] J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007, x+511 pages.

[14] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009, xx+513 pages.

[15] ———, *Moduli spaces and arithmetic dynamics*, CRM Monograph Series, vol. 30, American Mathematical Society, Providence, RI, 2012, viii+140 pages.

[16] ———, "Dynamical degree, arithmetic entropy, and canonical heights for dominant rational self-maps of projective space", *Ergodic Theory Dynam. Systems* **34** (2014), no. 2, p. 647-678.

[17] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980, vii+169 pages.

Andrew Bridy
University of Rochester
RC Box 270138
Rochester, NY, 14627
USA
E-mail: abridy@ur.rochester.edu
URL: http://www.math.rochester.edu/people/faculty/abridy/