DENSITY OF PERIODIC POINTS FOR LATTÈS MAPS OVER FINITE FIELDS

ZOË BELL, JASMINE CAMERO, KARINA CHO, TREVOR HYDE, CHIEH-MI LU, REBECCA MILLER, BIANCA THOMPSON, AND ERIC ZHU

Abstract. Let L_d be the Lattès map associated to the multiplication-by-d endomorphism of an elliptic curve E defined over a finite field $\mathbb{F}_q$. We determine the density $\delta(L_d, q)$ of periodic points for L_d in $\mathbb{P}^1(\mathbb{F}_q)$. We show that the periodic point densities $\delta(L_d, q^n)$ converge as $n \to \infty$ along certain arithmetic progressions, and compute simple explicit formulas for $\delta(L_\ell, q)$ when ℓ is a prime and E belongs to a special family of supersingular elliptic curves.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and suppose that $f(x) \in \mathbb{F}_q(x)$ is a rational function. The projective line $\mathbb{P}^1(\mathbb{F}_q)$ is a finite set closed under iteration of $a \mapsto f(a)$. We say that a point $a \in \mathbb{P}^1(\mathbb{F}_q)$ is *periodic* under f if $f^m(a) = a$ for some m, where f^m denotes the m-fold composition of f with itself.

Question 1.1. *What is the probability $\delta(f, q)$ that a randomly chosen element of $\mathbb{P}^1(\mathbb{F}_q)$ is periodic under iteration of f?*

In this paper we answer Question 1.1 for semiconjugates of elliptic curve endomorphisms, also known as Lattès maps. See Section 2 for background on elliptic curves and Lattès maps. Our first result determines the density of periodic points for Lattès maps over an arbitrary finite field $\mathbb{F}_q$. Some notation: Let $\mathrm{Per}(f, \mathbb{F}_q)$ denote the subset of points in $\mathbb{P}^1(\mathbb{F}_q)$ that are periodic under the rational function $f(x)$. If ℓ is a prime and k is an integer, then $v_\ell(k)$ denotes the multiplicity of ℓ as a factor of k.

Theorem 1.2. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and let τ be the integer defined by $\#E(\mathbb{F}_q) = q + 1 - \tau$. If d is an integer coprime to q and $L_d : \mathbb{P}^1 \to \mathbb{P}^1$ is the Lattès map associated to the multiplication-by-d map on E, then*

$$\delta(L_d, q) := \frac{\#\mathrm{Per}(L_d, \mathbb{F}_q)}{\#\mathbb{P}^1(\mathbb{F}_q)} = \frac{1}{2}\Big(\frac{1}{\pi_+} + \frac{1}{\pi_-}\Big) + \frac{\tau}{2(q+1)}\Big(\frac{1}{\pi_+} - \frac{1}{\pi_-}\Big),$$

where

$$\pi_\pm := \prod_{\ell | d} \ell^{v_\ell(q+1\pm\tau)},$$

and the product is taken over all primes ℓ dividing d. Furthermore,

$$\Big|\delta(L_d, q) - \frac{1}{2}\Big(\frac{1}{\pi_+} + \frac{1}{\pi_-}\Big)\Big| < \frac{1}{q^{1/2} + q^{-1/2}}.$$

Using Theorem 1.2 we study the behavior of the periodic point density $\delta(L_d, q^n)$ as n varies. Our second result shows that $\delta(L_d, q^n)$ converges as $n \to \infty$ along certain arithmetic progressions.

Theorem 1.3. *Let E be an elliptic curve defined over $\mathbb{F}_q$, let d be an integer coprime to q, and let τ_n be the sequence of integers such that $\#E(\mathbb{F}_{q^n}) = q^n + 1 - \tau_n$. Then for each $n \geq 1$ there exists some N depending on q, τ_1, d, n such that*

$$\lim_{\substack{m\to\infty \\ m\equiv n \bmod cd^N}} \delta(L_d, q^m) = \frac{1}{2}\Big(\frac{1}{\pi_{n,+}} + \frac{1}{\pi_{n,-}}\Big),$$

where

$$\pi_{n,\pm} := \prod_{\ell \mid d} \ell^{v_\ell(q^n+1\pm\tau_n)},$$

the product is taken over all primes ℓ dividing d, $c := \operatorname{lcm}(\ell^2 - 1 : \ell \mid d$ is prime$)$, and the limit is taken over all positive integers m such that $m \equiv n \bmod cd^N$.

Then N in Theorem 1.3 is, in principle, effectively computable as it comes from the modulus of continuity of several explicit exponential functions $n \mapsto \gamma^m$ with respect to the ℓ-adic metric for primes ℓ dividing d. Theorem 1.3 implies that any density that occurs for at least one n must occur infinitely often.

Our final result applies Theorem 1.2 to E in a special family of supersingular elliptic curves to get even more explicit formulas for the density $\delta(L_\ell, q^n)$ with ℓ prime.

Theorem 1.4. *Let E be an elliptic curve over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = q + 1$. If $\ell > 2$ is a prime not dividing q and e is the multiplicative order of q modulo ℓ, set*

$$w_n := v_\ell(q^e - 1) + v_\ell(n).$$

Then

$$\delta(L_\ell, q^n) = \begin{cases} \ell^{-w_n} & \text{if } n \text{ is odd, } e \mid 2n, \text{ and } e \nmid n, \\ \frac{1}{2}(1 + \ell^{-2w_n}) + \frac{\epsilon}{q^{n/2}+q^{-n/2}}(1 - \ell^{-2w_n}) & \text{if } n \text{ is even and } e \mid n, \\ 1 & \text{otherwise,} \end{cases}$$

where ϵ is a sign determined by

$$\epsilon = \begin{cases} +1 & \text{if } n \equiv 2 \bmod 4 \text{ and } e \nmid n/2, \text{ or } n \equiv 0 \bmod 4 \text{ and } e \mid n/2, \\ -1 & \text{if } n \equiv 2 \bmod 4 \text{ and } e \mid n/2, \text{ or } n \equiv 0 \bmod 4 \text{ and } e \nmid n/2. \end{cases}$$

Hence if e does not divide $2n$, then L_ℓ induces a permutation on $\mathbb{P}^1(\mathbb{F}_{q^n})$.

1.1. **Related work.** The most tractable cases of Question 1.1 are when the rational function f is a semiconjugate of an endomorphism of an algebraic group. In this case, one can translate questions about the dynamics of f into questions about the underlying group structure, which are easier to analyze. Such semiconjugates include power maps, Chebyshev polynomials, Dickson polynomials, and Lattès maps. Periodic densities for power maps (and monomial maps more generally) were studied in Hu, Sha [8], and for power maps and Chebyshev polynomials by Manes, Thompson [7]. In this paper we treat the Lattès case.

Juul, Kurlberg, Madhu, Tucker [2] studied the density of periodic points for the modulo $\mathfrak{p}$ reduction of a fixed rational function $f(x)$ defined over a global field K as $\mathfrak{p}$ varies through the primes in $\mathcal{O}_K$. They show that the limsup of the density of periodic points of f can be made arbitrarily small as the norm of $\mathfrak{p}$ tends to infinity by choosing f from a Zariski dense open set of degree d rational functions [2, Thm. 1.2]. In their Example 7.3 they fix an elliptic curve E defined over $\mathbb{Q}$ and a Lattès map L_ℓ with ℓ prime and show that in many cases the liminf of the periodic density of L_ℓ modulo $\mathfrak{p}$ converges to 0 as the norm of $\mathfrak{p}$ tends to infinity. Note that these limits are in a different direction from those we take in Theorem 1.3. See also the earlier work of Madhu [6] and the subsequent work of Juul [1].

Ugolini [11] studied the phase portraits of Lattès maps associated to ordinary elliptic curves over finite fields. The methods of [11] are substantively equivalent to those we use to prove Theorem 1.2, but there appears to be no direct overlap in results.

Küçüksakalli [4] analyzed the value sets of Lattès maps over finite fields, arriving at a characterization of when a given Lattès map L_d induces a permutation of $\mathbb{P}^1(\mathbb{F}_q)$, which is equivalent to our Corollary 2.6 (see Remark 2.7.)

1.2. **Acknowledgements.** This project began as part of the Summer@ICERM 2019 REU. We thank ICERM for hosting us and providing us access to their computational resources. We thank Joe Silverman for generously sharing insights that led us to the proof of Theorem 1.2. We also wish to thank Women in Sage: Sagedays 90, where this project was originally developed. Trevor Hyde is partially supported by the NSF MSPRF and the Jump Trading Mathlab Research Fund.

2. Density of periodic points for Lattès maps

The goal of this section is to prove the following theorem.

Theorem 2.1. *Let E be an elliptic curve defined over $\mathbb{F}_q$ with trace of Frobenius τ. If d is an integer coprime to q and $L_d : \mathbb{P}^1 \to \mathbb{P}^1$ is the Lattès map associated to the multiplication-by-d map on E, then*

$$\delta(L_d, q) := \frac{\#\mathrm{Per}(L_d, \mathbb{F}_q)}{\#\mathbb{P}^1(\mathbb{F}_q)} = \frac{1}{2}\Big(\frac{1}{\pi_+} + \frac{1}{\pi_-}\Big) + \frac{\tau}{2(q+1)}\Big(\frac{1}{\pi_+} - \frac{1}{\pi_-}\Big),$$

where

$$\pi_\pm := \prod_{\ell \mid d} \ell^{v_\ell(q+1\pm\tau)},$$

and the product is taken over all primes ℓ dividing d. Furthermore,

$$\Big|\delta(L_d, q) - \frac{1}{2}\Big(\frac{1}{\pi_+} + \frac{1}{\pi_-}\Big)\Big| < \frac{1}{q^{1/2} + q^{-1/2}}.$$

We begin by reviewing some of the basics of elliptic curves over finite fields and their Lattès maps. For a more complete treatment we refer the reader to Silverman [9], and Chapter V in particular.

2.1. **Elliptic curves.** An *elliptic curve* defined over a field K, denoted E/K, is a smooth, projective, algebraic curve E of genus 1 defined over K together with a prescribed *base point* $O \in E(K)$. There is a natural commutative algebraic group law on E defined over K with O as the identity element. In particular, if L/K is any field extension, the L-points of E form a group. If $P, Q \in E(\overline{K})$ are points on E, then we write $P + Q$ and $-P$ for the sum and inverse, respectively.

We say two elliptic curves E_1, E_2 defined over K are isomorphic if there is an invertible map $f : E_1 \to E_2$ of algebraic curves that respects base points $f(O_1) = O_2$. If f is an isomorphism, then $f : E_1(M) \xrightarrow{\sim} E_2(M)$ gives a group isomorphism between the M-points on the curves for any extension M/K [9, Thm. III.4.8].

Every elliptic curve E over a field K has a model as a plane curve given by a *Weierstrass equation* of the form

$$E : y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6, \tag{1}$$

where $A_i \in K$ [9, §III.1]. If the characteristic of K is at least 5, then there is a reduced Weierstrass equation of the form

$$E : y^2 = x^3 + Ax + B.$$

However, since we are primarily interested in elliptic curves over arbitrary finite fields, we use the Weierstrass equations of the form (1) for full generality.

Weierstrass curves intersect the line at infinity in $\mathbb{P}^2(K)$ at exactly one point expressed in homogeneous coordinates as $(0 : 1 : 0)$. By convention, we let the base point O of E be this unique point at infinity.

If $P = (a, b)$ is a point on E expressed in affine coordinates, then the additive inverse of P is

$$-P := (a, -b - A_1a - A_3). \tag{2}$$

Let $x : E \to \mathbb{P}^1$ be the x-coordinate projection $x(a, b) = a$. Since there are clearly at most 2 points on E with the same x-coordinate, it follows that $x(P) = x(Q)$ if and only if $P = \pm Q$ [9, §III.2].

2.2. **Elliptic curves over $\mathbb{F}_q$.** Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. The *Frobenius automorphism* $F : \mathbb{P}^2(\overline{\mathbb{F}}_q) \to \mathbb{P}^2(\overline{\mathbb{F}}_q)$ is the map defined on projective coordinates by

$$F(a : b : c) = (a^q : b^q : c^q).$$

If $E \subseteq \mathbb{P}^2$ is an elliptic curve defined over $\mathbb{F}_q$, then F restricts to an automorphism of E. Furthermore, Galois theory implies that $P \in E(\overline{\mathbb{F}}_q)$ belongs to $E(\mathbb{F}_{q^n})$ if and only if $F^n(P) = P$.

If E is an elliptic curve over $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ is a finite abelian group. Let τ be the unique integer such that

$$\#E(\mathbb{F}_q) = q + 1 - \tau.$$

The integer τ is called the *trace of Frobenius* for E over $\mathbb{F}_q$. This name comes from the fact that τ may be realized as the trace of the action of F as a linear endomorphism of the ℓ-adic Tate module associated to E [9, Rmk. V.2.6].

2.3. **Lattès maps.** For each $d \in \mathbb{Z}$, the *multiplication-by-d* map $[d] : P \mapsto dP$ is a group endomorphism of $E(\mathbb{F}_q)$. Since $E(\mathbb{F}_q)$ is abelian, $[d]$ commutes with the inverse map $[-1]$. Galois theory implies that there exists a rational function $L_d(x) \in \mathbb{F}_q(x)$ such that the following diagram commutes,

$$\begin{array}{ccc} E & \xrightarrow{[d]} & E \\ {\scriptstyle x}\downarrow & & \downarrow{\scriptstyle x} \\ \mathbb{P}^1 & \xrightarrow{L_d} & \mathbb{P}^1. \end{array}$$

That is, for all points $P \in E(\overline{\mathbb{F}}_q)$,

$$L_d(x(P)) = x(dP).$$

Since every $a \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ is the x-coordinate of some point $P \in E(\overline{\mathbb{F}}_q)$, this identity completely determines $L_d(x)$. If $d, e \in \mathbb{Z}$, then $[de] = [d] \circ [e]$, hence the above diagram implies that $L_{de} = L_d \circ L_e$.

The rational function L_d is called the *dth Lattès map* associated to E. We are interested in the dynamics of Lattès maps. The conjugacy class of L_d is determined by the isomorphism class of E. Hence the dynamical properties of L_d are independent of our choice of model for E over $\mathbb{F}_q$. For simplicity, when we talk about Lattès maps for an elliptic curve E, we will always mean with respect to a Weierstrass model for E as in (1). For more background on Lattès maps and their dynamics, see Silverman [10, Chp. 6].

The following lemma characterizes the periodic points of L_d in terms of the group structure on E.

Lemma 2.2. *Let $E/\mathbb{F}_q$ be an elliptic curve and let $L_d : \mathbb{P}^1 \to \mathbb{P}^1$ be the dth Lattès map associated to E. Then $a \in \mathbb{P}^1(\mathbb{F}_q)$ is periodic under L_d if and only if there is some point $P \in E(\mathbb{F}_{q^2})$ such that $a = x(P)$ and P has order coprime to d.*

Proof. Since $\infty \in \mathbb{P}^1(\mathbb{F}_q)$ is the x-coordinate of the identity O on $E(\mathbb{F}_q)$ (which has order 1), it follows from the definition of Lattès maps that

$$L(\infty) = L(x(O)) = x(dO) = x(O) = \infty.$$

Hence ∞ is always periodic under L.

Suppose that E has a Weierstrass equation as in (1). Then for each $a \in \mathbb{F}_q$, the quadratic equation

$$y^2 + A_1ay + A_3y = a^3 + A_2a^2 + A_4a + A_6,$$

splits completely in $\mathbb{F}_{q^2}$. Hence every $a \in \mathbb{F}_q$ is the x-coordinate of some point on $E(\mathbb{F}_{q^2})$. Note that since $\mathbb{F}_{q^2}$ is a finite field, $E(\mathbb{F}_{q^2})$ is a finite abelian group. Suppose that $a = x(P)$ where $P \in E(\mathbb{F}_{q^2})$ has order n. Then a is periodic under L if and only if there is some k such that $L^k(a) = a$, which is equivalent to

$$a = L^k(a) = L^k(x(P)) = x(d^kP).$$

Thus $d^kP = \pm P$, hence $d^{2k}P = P$, which is equivalent to $d^{2k} \equiv 1 \bmod n$. Such an integer k exists if and only if d is a unit modulo n, which is to say that P is a point with order coprime to d. ∎

2.4. **Quadratic twists.** Let E be an elliptic curve over $\mathbb{F}_q$. The *quadratic twist* of E is an elliptic curve E' over $\mathbb{F}_q$ characterized up to isomorphism defined over $\mathbb{F}_q$ by the following property: There exists an isomorphism $\iota : E \to E'$ defined over $\mathbb{F}_{q^2}$, and for all such isomorphisms ι and points $P \in E(\mathbb{F}_{q^2})$ we have

$$F(\iota(P)) = -\iota(F(P)). \tag{3}$$

If the characteristic of $\mathbb{F}_q$ is at least 5 and

$$E : y^2 = x^3 + Ax + B$$

is a reduced Weierstrass equation for E, then

$$E' : \alpha^2y^2 = x^3 + Ax + B$$

is an explicit formula for the quadratic twist E', where α is a primitive element of $\mathbb{F}_{q^2}$ such that $\alpha^2 \in \mathbb{F}_q$. An isomorphism $\iota : E \to E'$ is given in affine coordinates by

$$\iota(a, b) = (a, b/\alpha).$$

Note that by construction, $\alpha^q = -\alpha$. Hence if $P = (a, b) \in E(\mathbb{F}_{q^2})$, then

$$F(\iota(P)) = F(a, b/\alpha) = (a^q, b^q/\alpha^q) = (a^q, -b^q/\alpha) = -\iota(F(P)).$$

There are similar explicit formulas for E' in characteristics 2 and 3, but for our purposes the simplest way to work with quadratic twists in arbitrary characteristic is via the characterization (3). For the general theory of twists see Silverman [9, §X.2], and for quadratic twists of elliptic curves in particular, see [9, Ex. X.2.4].

Lemma 2.3. *Let E be an elliptic curve defined over $\mathbb{F}_q$ with quadratic twist E'. Let $A, A' \subseteq E(\mathbb{F}_{q^2})$ be the subgroups*

$$A := \{P \in E(\mathbb{F}_{q^2}) : F(P) = P\} = E(\mathbb{F}_q)$$
$$A' := \{P \in E(\mathbb{F}_{q^2}) : F(P) = -P\},$$

where F is the Frobenius automorphism.

(1) If $\iota : E \to E'$ is an isomorphism defined over $\mathbb{F}_{q^2}$, then the restriction of ι to A' gives a group isomorphism $\iota : A' \to E'(\mathbb{F}_q)$.
(2) $\#E(\mathbb{F}_q) + \#E'(\mathbb{F}_q) = 2(q + 1)$.
(3) If τ is the trace of Frobenius of $E/\mathbb{F}_q$, then the trace of Frobenius for $E'/\mathbb{F}_q$ is $-\tau$.

Proof. (1) It suffices to show that $\iota(A') \subseteq E'(\mathbb{F}_q)$ and $\iota^{-1}(E'(\mathbb{F}_q)) \subseteq A'$.cIf $P \in A'$, then (3) implies

$$F(\iota(P)) = -\iota(F(P)) = -\iota(-P) = \iota(P),$$

hence $\iota(P) \in E'(\mathbb{F}_q)$ by Galois theory. If $Q \in E'(\mathbb{F}_q)$, then

$$F(\iota^{-1}(Q)) = -\iota^{-1}(F(Q)) = -\iota^{-1}(Q),$$

where the first equality is equivalent to (3) and the second equality follows from $F(Q) = Q$. Hence $\iota^{-1}(Q) \in A'$.

(2) Consider the map $\widetilde{x} : A \sqcup A' \to \mathbb{P}^1(\mathbb{F}_q)$ from the disjoint union of A and A' to $\mathbb{P}^1(\mathbb{F}_q)$ induced by the x-coordinate projection map. We claim that $\widetilde{x}$ is exactly 2-to-1. Since $A = E(\mathbb{F}_q)$ and $A' \cong E'(\mathbb{F}_q)$ by (1), this will imply that

$$\#E(\mathbb{F}_q) + \#E'(\mathbb{F}_q) = 2\#\mathbb{P}^1(\mathbb{F}_q) = 2(q + 1).$$

If $a \in \mathbb{P}^1(\mathbb{F}_q)$, then as we argued in the proof of Lemma 2.2, there exists some $P \in E(\mathbb{F}_{q^2})$ such that $x(P) = a$. Since $F(P)$ is another point in $E(\mathbb{F}_{q^2})$ with $x(F(P)) = a^q = a$, it follows that $F(P) = \pm P$. Thus $P \in A$ or A', hence $\widetilde{x}$ is surjective. If $P \neq -P$, then $\pm P$ both belong to exactly one of A or A', and these are precisely the two points in $A \sqcup A'$ mapping to a under $\widetilde{x}$. If $P = -P$, then P is the only point on $E(\mathbb{F}_{q^2})$ with x-coordinate a. Since $P \in A \cap A'$, there are two copies of P in $A \sqcup A'$ and these are precisely the two points mapping to a under $\widetilde{x}$. Hence $\widetilde{x}$ is exactly 2-to-1.

(3) Since $\#E(\mathbb{F}_q) = q + 1 - \tau$, it follows from (2) that

$$\#E'(\mathbb{F}_q) = 2(q + 1) - (q + 1 - \tau) = q + 1 + \tau.$$

Therefore the trace of Frobenius for $E'/\mathbb{F}_q$ is $-\tau$. □

We now turn to the proof of Theorem 2.1.

Proof of Theorem 2.1. Lemma 2.2 implies that $a \in \mathbb{P}^1(\mathbb{F}_q)$ is periodic under L_d if and only if there exists some point $P \in E(\mathbb{F}_{q^2})$ with order coprime to d such that $a = x(P)$. Let $A, A' \subseteq E(\mathbb{F}_{q^2})$ be the subgroups defined in Lemma 2.3. Then any point $P \in E(\mathbb{F}_{q^2})$ with $x(P) \in \mathbb{P}^1(\mathbb{F}_q)$ must belong to $A \cup A'$.

Let A_d and A'_d denote the subsets of A and A', respectively, of elements with order coprime to d. Lemma 2.3 implies that $\#A = \#E(\mathbb{F}_q) = q+1-\tau$ and $\#A' = \#E'(\mathbb{F}_q) = q+1+\tau$. If G is a finite abelian group, then the number of elements of G with order coprime to d is the largest factor of $\#G$ coprime to d. Hence

$$\#A'_d = \frac{q+1+\tau}{\pi_+}, \qquad \#A_d = \frac{q+1-\tau}{\pi_-},$$

where

$$\pi_\pm := \prod_{\ell \mid d} \ell^{v_\ell(q+1\pm\tau)}.$$

Suppose that $A'_d \cap A_d$ consists of r points. The involution $P \mapsto -P$ acts freely on $A'_d \cup A_d \setminus (A'_d \cap A_d)$ and fixes each point of $A'_d \cap A_d$. Thus,

$$\begin{aligned}
\#\operatorname{Per}(L_d, \mathbb{F}_q) &= \#x(A'_d \cup A_d) \\
&= \#x(A'_d \setminus (A'_d \cap A_d)) + \#x(A_d \setminus (A'_d \cap A_d)) + \#x(A'_d \cap A'_d) \\
&= \frac{(q+1+\tau)/\pi_+ - r}{2} + \frac{(q+1-\tau)/\pi_- - r}{2} + r \\
&= \frac{q+1}{2}\Big(\frac{1}{\pi_+} + \frac{1}{\pi_-}\Big) + \frac{\tau}{2}\Big(\frac{1}{\pi_+} - \frac{1}{\pi_-}\Big).
\end{aligned}$$

Dividing by $\#\mathbb{P}^1(\mathbb{F}_q) = q+1$ we conclude that

$$\delta(L_d, q) := \frac{\#\operatorname{Per}(L, \mathbb{F}_q)}{\#\mathbb{P}^1(\mathbb{F}_q)} = \frac{1}{2}\Big(\frac{1}{\pi_+} + \frac{1}{\pi_-}\Big) + \frac{\tau}{2(q+1)}\Big(\frac{1}{\pi_+} - \frac{1}{\pi_-}\Big).$$

Hasse proved the following bound on the trace of Frobenius,

$$|\tau| \le 2\sqrt{q}. \tag{4}$$

See, for example, [9, Thm. V.1.1]. Since $|\pi_+^{-1} - \pi_-^{-1}| < 1$ it follows that

$$\Big|\delta(L_d, q) - \frac{1}{2}\Big(\frac{1}{\pi_+} + \frac{1}{\pi_-}\Big)\Big| = \frac{|\tau|}{2}\Big|\frac{1}{\pi_+} - \frac{1}{\pi_-}\Big| < \frac{2q^{1/2}}{2(q+1)} = \frac{1}{q^{1/2} + q^{-1/2}}. \qquad \square$$

Example 2.4. Let $E/\mathbb{F}_5$ be the elliptic curve with Weierstrass equation $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$. We quickly count the number of points in $E(\mathbb{F}_5)$ by an exhaustive search and find

$$9 = \#E(\mathbb{F}_5) = q + 1 - \tau = 5 + 1 + 3,$$

hence the trace of Frobenius is $\tau = -3$. Thus $q + 1 + \tau = 5 + 1 - 3 = 3$. Therefore Theorem 2.1 implies that the density of periodic points for L_d with d coprime to 5 depends only on whether or not d is divisible by 3. In particular,

$$\delta(L_d, 5) = \begin{cases} 1 & \text{if } 3 \nmid d \\ \frac{1}{6} & \text{if } 3 \mid d. \end{cases}$$

Example 2.5. Let $E/\mathbb{F}_7$ be the elliptic curve with Weierstrass equation $y^2 = x^3 + x - 1$ over $\mathbb{F}_7$. We compute

$$11 = \#E(\mathbb{F}_7) = q + 1 - \tau = 7 + 1 + 3.$$

Hence $\tau = -3$ and $q + 1 + \tau = 5$. Thus Theorem 2.1 implies that the there are 4 cases for the density of periodic points of L_d on $\mathbb{P}^1(\mathbb{F}_7)$ with $7 \nmid d$ depending on the greatest common divisor $(d, 55)$ of d and 55.

$$\delta(L_d, 7) = \begin{cases} 1 & \text{if } (d, 55) = 1, \\ \frac{3}{4} & \text{if } (d, 55) = 5, \\ \frac{3}{8} & \text{if } (d, 55) = 11, \\ \frac{1}{8} & \text{if } (d, 55) = 55. \end{cases}$$

Corollary 2.6. *Let $E/\mathbb{F}_q$ be an elliptic curve with trace of Frobenius τ. Then the dth Lattès map associated to E induces a permutation of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $(q + 1)^2 - \tau^2$ is coprime to d.*

Proof. Note that L_d induces a permutation of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if every point in $\mathbb{P}^1(\mathbb{F}_q)$ is periodic. Theorem 2.1 implies that

$$\delta(L_d, q) = \frac{1}{2}\Big(\frac{1}{\pi_+} + \frac{1}{\pi_-}\Big) + \frac{\tau}{2(q + 1)}\Big(\frac{1}{\pi_+} - \frac{1}{\pi_-}\Big) \leq 1,$$

with equality achieved if and only if

$$1 = \pi_\pm = \prod_{\ell \mid d} \ell^{v_\ell(q+1\pm\tau)},$$

which is equivalent to $(q + 1)^2 - \tau^2 = (q + 1 - \tau)(q + 1 + \tau)$ being coprime to d. □

Remark 2.7. Küçüksakalli [4] studied the value sets of Lattès maps associated to elliptic curves over $\mathbb{F}_q$ which arise by starting with an elliptic curve with complex multiplication (CM) by the ring of integers in an imaginary quadratic field and reducing modulo a prime ideal π of good reduction with norm $N(\pi) = q$. Their Corollary 2.8 gives a necessary and sufficient condition for such Lattès maps to induce permutations on $\mathbb{P}^1(\mathbb{F}_q)$ which is essentially equivalent to our Corollary 2.6: Any elliptic curve $E/\mathbb{F}_q$ which is not supersingular has endomorphism ring isomorphic to an order in an imaginary quadratic field [9, Thm. V.3.1] and thus may be realized as the reduction of a CM elliptic curve defined over a number field at a prime of good reduction. While their result is stated for elliptic curves with CM by the full ring of integers in an imaginary quadratic field, the arguments appear to hold in greater generality.

3. Lattès periodic density in towers

In this section we use Theorem 2.1 to prove the following result on the density of periodic points for a fixed Lattès map in $\mathbb{P}^1(\mathbb{F}_{q^n})$ as n varies.

Theorem 3.1. *Let $E/\mathbb{F}_q$ be an elliptic curve, let τ_n be the trace of Frobenius of E as an elliptic curve over $\mathbb{F}_{q^n}$, and let d be an integer coprime to q. For each positive integer n, there exists some N depending on q, τ_1, d, n such that*

$$\lim_{\substack{m\to\infty \\ m \equiv n \bmod cd^N}} \delta(L_d, q^m) = \frac{1}{2}\Big(\frac{1}{\pi_{n,+}} + \frac{1}{\pi_{n,-}}\Big),$$

where

$$\pi_{n,\pm} := \prod_{\ell \mid d} \ell^{v_\ell(q^n+1\pm\tau_n)},$$

the product is taken over all primes ℓ *dividing* d, $c := \operatorname{lcm}(\ell^2-1 : \ell \mid d$ *is prime), and the limit is taken over all positive integers* m *such that* $m \equiv n \bmod cd^N$.

Proof. Recall that the *Hasse-Weil zeta function* of E over $\mathbb{F}_q$ is the formal power series

$$Z(E/\mathbb{F}_q, x) := \exp\Big(\sum_{m\geq 1} \frac{\#E(\mathbb{F}_{q^m})}{m} x^m\Big).$$

The zeta function of E may be expressed as a rational function [9, Thm. V.2.4] given explicitly by

$$Z(E/\mathbb{F}_q, x) = \frac{1-\tau x + qx^2}{(1-x)(1-qx)}.$$

Let α, β be the algebraic integers such that

$$1-\tau x + qx^2 = (1-\alpha x)(1-\beta x).$$

Then by taking a logarithm of $Z(E/\mathbb{F}_q, x)$ and comparing coefficients we see that

$$\#E(\mathbb{F}_{q^m}) = q^m + 1 - \alpha^m - \beta^m.$$

Thus the trace of Frobenius of E viewed as an elliptic curve over $\mathbb{F}_{q^m}$ is $\tau_m = \alpha^m + \beta^m$.

Suppose ℓ is a prime dividing d. Let $|\cdot|_\ell$ be the ℓ-adic absolute value on $\mathbb{Q}$, let $\mathbb{Q}_\ell$ be the ℓ-adic completion of $\mathbb{Q}$, and let $K/\mathbb{Q}_\ell$ be a finite extension. Every unit $\gamma \in K$ may be expressed as $\gamma = \zeta(1+\delta\lambda)$ for some root of unity ζ, some δ with $|\delta|_\ell \leq 1$, and some uniformizer λ. Furthermore the order of ζ divides $\ell^f - 1$ where f is the residue degree of $K/\mathbb{Q}_\ell$ (see Koblitz[3, §III.3].) The binomial theorem implies that $m \mapsto (1+\delta\lambda)^m$ is an ℓ-adically continuous function of m [3, §II.2]. Hence $m \mapsto \gamma^m = \zeta^m(1+\delta\lambda)^m$ is ℓ-adically continuous when restricted to m in a residue class modulo $\ell^f - 1$.

Now let $K := \mathbb{Q}_\ell(\alpha, \beta)$ be the splitting field of $1-\tau x + qx^2$ over $\mathbb{Q}_\ell$. Since α, β are algebraic integers such that $\alpha\beta = q$ and q is coprime to ℓ by assumption, it follows that $|q|_\ell = |\alpha|_\ell = |\beta|_\ell = 1$. The residue degree of $K/\mathbb{Q}_\ell$ is at most 2. Therefore, with n fixed, the functions

$$\varepsilon_+(m) := q^m + 1 + \alpha^m + \beta^m, \qquad \varepsilon_-(m) := q^m + 1 - \alpha^m - \beta^m$$

are ℓ-adically continuous on the set of all integers m such that $m \equiv n \bmod \ell^2 - 1$. Thus there exists some N_ℓ depending on q, τ, ℓ such that $m \equiv n \bmod (\ell^2-1)\ell^{N_\ell}$ implies

$$|\varepsilon_\pm(m) - \varepsilon_\pm(n)|_\ell < |\varepsilon_\pm(n)|_\ell.$$

The ultrametric property of $|\cdot|_\ell$ implies that $|\varepsilon_\pm(m)|_\ell = |\varepsilon_\pm(n)|_\ell$ for all such m. This is equivalent to

$$v_\ell(q^m + 1 \pm \tau_m) = v_\ell(q^n + 1 \pm \tau_n).$$

Let $N := \max_{\ell \mid d} N_\ell$ and let $c : \operatorname{lcm}(\ell^2 - 1 : \ell \mid d$ is prime). Hence if $m \equiv n \bmod cd^N$, then $m \equiv n \bmod (\ell^2-1)\ell^{N_\ell}$ for each prime $\ell \mid d$. Therefore, Theorem 2.1 implies that for any such m,

$$\Big|\delta(L_d, q^m) - \frac{1}{2}\Big(\frac{1}{\pi_{n,+}} + \frac{1}{\pi_{n,-}}\Big)\Big| < \frac{1}{q^{m/2} + q^{-m/2}}.$$

We conclude that

$$\lim_{\substack{m\to\infty \\ m\equiv n \bmod cd^N}} \delta(L_d, q^m) = \frac{1}{2}\Big(\frac{1}{\pi_{n,+}} + \frac{1}{\pi_{n,-}}\Big). \qquad \square$$

4. Lattès periodic densities when $\tau = 0$

In this section we consider a special family of elliptic curves where the periodic density in $\mathbb{P}^1(\mathbb{F}_{q^n})$ of L_ℓ, with ℓ prime, may be computed in terms of the ℓ-adic valuation of n and $q^e - 1$, where e is the multiplicative order of q modulo ℓ.

Theorem 4.1. *Let $E/\mathbb{F}_q$ be an elliptic curve with trace of Frobenius $\tau = 0$. If $\ell > 2$ is a prime not dividing q and e is the multiplicative order of q modulo ℓ, then set $w_n := v_\ell(q^e - 1) + v_\ell(n)$. Then*

$$\delta(L_\ell, q^n) = \begin{cases} \ell^{-w_n} & \text{if } n \text{ is odd, } e \mid 2n, \text{ and } e \nmid n, \\ \frac{1}{2}(1+\ell^{-2w_n}) + \frac{\epsilon}{q^{n/2}+q^{-n/2}}(1-\ell^{-2w_n}) & \text{if } n \text{ is even and } e \mid n, \\ 1 & \text{otherwise,} \end{cases}$$

where ϵ is a sign determined by

$$\epsilon = \begin{cases} +1 & \text{if } n \equiv 2 \bmod 4 \text{ and } e \nmid n/2, \text{ or } n \equiv 0 \bmod 4 \text{ and } e \mid n/2, \\ -1 & \text{if } n \equiv 2 \bmod 4 \text{ and } e \mid n/2, \text{ or } n \equiv 0 \bmod 4 \text{ and } e \nmid n/2. \end{cases}$$

Hence if e does not divide $2n$, then L_ℓ induces a permutation on $\mathbb{P}^1(\mathbb{F}_{q^n})$.

Remark 4.2. Recall that if $\mathbb{F}_q$ has characteristic p, then an elliptic curve E over $\mathbb{F}_q$ is said to be *supersingular* if τ is divisible by p. Supersingular elliptic curves have many exceptional properties, see Silverman [9, §V.3]. In particular, if $\tau = 0$, then E must be supersingular. On the other hand, if E is supersingular and $q = p \geq 5$, then the Hasse bound $|\tau| \leq 2\sqrt{p}$ implies that $\tau = 0$. Thus Theorem 4.1 applies to all Lattès maps L_ℓ associated to supersingular elliptic curves over $\mathbb{F}_p$ when $p \geq 5$.

Lemma 4.3. *Suppose that $q \in \overline{\mathbb{Q}}_\ell$ is an element such that $v_\ell(q-1) > \frac{1}{\ell-1}$. Then*

$$v_\ell(q^n - 1) = v_\ell(q-1) + v_\ell(n).$$

In particular, this holds when q is an integer such that $q \equiv 1 \bmod \ell$.

Proof. Let ζ_n denote a primitive nth root of unity. Recall that

$$|N(1-\zeta_n)| = \begin{cases} p & \text{if } n = p^k \text{ for some prime } p \text{ and } k \geq 1, \\ 1 & \text{if } n \text{ is not a prime power,} \end{cases}$$

where $N : \mathbb{Q}(\zeta_n) \to \mathbb{Q}$ is the norm function (see, for example, Lang [5, Chp. IV, §1].) Recall that the degree of the field extension $\mathbb{Q}(\zeta_{\ell^m})/\mathbb{Q}$ is $\varphi(\ell^m) := \ell^m - \ell^{m-1}$. Thus if n is coprime to ℓ, then $v_\ell(1-\zeta_n^k) = 0$ for all $k \not\equiv 0 \bmod n$, and

$$v_\ell(1-\zeta_{\ell^m}^k) = \frac{1}{[\mathbb{Q}(\zeta_{\ell^m}) : \mathbb{Q}]} v_\ell(N(1-\zeta_{\ell^m}^k)) = \frac{1}{\varphi(\ell^m)} v_\ell(N(1-\zeta_{\ell^m})) = \frac{1}{\varphi(\ell^m)},$$

for any $k \not\equiv 0 \bmod \ell$. Thus, $v_\ell(1-\zeta_n^k) \leq \frac{1}{\ell-1}$ for all $k \not\equiv 0 \bmod n$ and for all $m \geq 1$,

$$\sum_{k\in(\mathbb{Z}/(\ell^m))^\times} v_\ell(1-\zeta_{\ell^m}^k) = 1.$$

If $n \geq 1$, the factorization $q^n - 1 = \prod_{k=0}^{n-1}(q - \zeta_n^k)$ implies that

$$v_\ell(q^n-1) - v_\ell(q-1) = \sum_{k=1}^{n-1} v_\ell(q-\zeta_n^k) = \sum_{k=1}^{n-1} \min(v_\ell(q-1), v_\ell(1-\zeta_n^k)) = \sum_{k=1}^{n-1} v_\ell(1-\zeta_n^k),$$

where the second and third equalities follow from our assumption that $v_\ell(q-1) > \frac{1}{\ell-1} \geq v_\ell(1-\zeta_n^k)$. Observe that each ζ_n^k has a unique expression as ζ_d^j where $d \mid n$ and j is a unit modulo d. Thus, if $v_\ell(n) = m$, then

$$v_\ell(q^n-1) - v_\ell(q-1) = \sum_{d \mid n} \sum_{j \in (\mathbb{Z}/(d))^\times} v_\ell(1-\zeta_d^j) = \sum_{i=1}^{m} \sum_{j \in (\mathbb{Z}/(\ell^i))^\times} v_\ell(1-\zeta_{\ell^i}^j) = m. \qquad \square$$

Proof of Theorem 4.1. Let E be an elliptic curve over $\mathbb{F}_q$ with $\tau = 0$. Let τ_n be the trace of Frobenius of E over $\mathbb{F}_{q^n}$. Then as discussed in the proof of Theorem 3.1, we have $\tau_n = \alpha^n + \beta^n$ where

$$(1-\alpha x)(1-\beta x) = 1 - \tau x + q x^2 = 1 - q x^2.$$

Hence $\alpha, \beta = \pm i\sqrt{q}$ and

$$\tau_n = (i^n + (-i)^n) q^{n/2} = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ 2(-1)^{n/2} q^{n/2} & \text{if } n \text{ is even.} \end{cases}$$

Therefore,

$$q^n + 1 \pm \tau_n = \begin{cases} q^n + 1 & \text{if } n \text{ is odd,} \\ (q^{n/2} \pm (-1)^{n/2})^2 & \text{if } n \text{ is even.} \end{cases}$$

If n is odd, then Theorem 2.1 implies that

$$\begin{aligned} \delta(L_\ell, \mathbb{F}_{q^n}) &= \frac{1}{2}\left(\ell^{-v_\ell(q^n+1+\tau_n)} + \ell^{-v_\ell(q^n+1-\tau_n)}\right) + \frac{\tau_n}{q^n+1}\left(\ell^{-v_\ell(q^n+1+\tau_n)} - \ell^{-v_\ell(q^n+1-\tau_n)}\right) \\ &= \ell^{-v_\ell(q^n+1)}. \end{aligned}$$

Since $\ell > 2$ and $(q^n+1) + (q^n-1) = 2q^n$, at most one of $v_\ell(q^n+1)$ and $v_\ell(q^n-1)$ is positive. Note that

$$v_\ell(q^n+1) + v_\ell(q^n-1) = v_\ell(q^{2n}-1),$$

and $v_\ell(q^{2n}-1) > 0$ if and only if $e \mid 2n$. Similarly, $v_\ell(q^n-1) > 0$ if and only if $e \mid n$. Hence $v_\ell(q^n+1) > 0$ is equivalent to $e \mid 2n$ and $e \nmid n$. In that case Lemma 4.3 implies that

$$\begin{aligned} v_\ell(q^n+1) &= v_\ell(q^{2n}-1) - v_\ell(q^n-1) \\ &= v_\ell(q^{2n}-1) \\ &= v_\ell(q^e-1) + v_\ell(2n/e) \\ &= v_\ell(q^e-1) + v_\ell(n) \\ &= w_n. \end{aligned}$$

The fourth equality follows from the fact that e is a divisor of $\varphi(\ell) = \ell - 1$, hence $v_\ell(e) = 0$. Therefore, if n is odd,

$$\delta(L_\ell, q^n) = \begin{cases} \ell^{-w_n} & \text{if } e \mid 2n \text{ and } e \nmid n, \\ 1 & \text{otherwise.} \end{cases}$$

Next suppose that n is even. Then by Theorem 2.1,

$$\delta(L_\ell, q^n) = \frac{1}{2}\Big(\ell^{-2a_n^+} + \ell^{-2a_n^-}\Big) + \frac{(-1)^{n/2}}{q^{n/2}+q^{-n/2}}\Big(\ell^{-2a_n^+} - \ell^{-2a_n^-}\Big),$$

where $a_n^\pm = v_\ell(q^{n/2} \pm (-1)^{n/2})$. Since

$$(q^{n/2} - (-1)^{n/2}) + (q^{n/2} + (-1)^{n/2}) = 2q^{n/2},$$

and $\ell > 2$ by assumption, it follows that at most one of $a_n^\pm$ is positive. Then

$$a_n^+ + a_n^- = v_\ell(q^n - 1)$$

is positive if and only if $e \mid n$. Suppose that $e \mid n$. Lemma 4.3 implies that

$$v_\ell(q^n - 1) = v_\ell(q^e - 1) + v_\ell(n/e) = w_n.$$

Furthermore, we have $v_\ell(q^{n/2} - 1) > 0$ if and only if $e \mid n/2$, hence $v_\ell(q^{n/2} + 1) > 0$ if and only if $e \nmid n/2$. Putting it all together, for n even and $e \mid n$ we have

$$\delta(L_\ell, q^n) = \frac{1}{2}\Big(1 + \ell^{-2w_n}\Big) + \frac{\epsilon}{q^{n/2}+q^{-n/2}}\Big(1 - \ell^{-2w_n}\Big),$$

where

$$\epsilon = \begin{cases} +1 & \text{if } n \equiv 2 \bmod 4 \text{ and } e \nmid n/2, \text{ or } n \equiv 0 \bmod 4 \text{ and } e \mid n/2, \\ -1 & \text{if } n \equiv 2 \bmod 4 \text{ and } e \mid n/2, \text{ or } n \equiv 0 \bmod 4 \text{ and } e \nmid n/2. \end{cases}$$

In all other cases, $\delta(L_\ell, q^n) = 1$. For example, this holds when e does not divide $2n$. ☐

References

[1] Jamie Juul. Fixed point proportions for Galois groups of non-geometric iterated extensions. *Acta Arith.*, 183(4):301–315, 2018.

[2] Jamie Juul, Pär Kurberg, Kalyani Madhu, and Tom J. Tucker. Wreath products and proportions of periodic points. *Int. Math. Res. Not.*, 13:3944–3969, 2016.

[3] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 2nd edition, 1984.

[4] Ömer Küçüksakalli. Value sets of Lattès maps over finite fields. *J. Number Theory*, 143:262–278, 2014.

[5] Serge Lang. *Algebraic Number Theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.

[6] Kalyani Madhu. *Galois Theory and Polynomial Orbits*. PhD thesis, University of Rochester, 2011.

[7] Michelle Manes and Bianca Thompson. Periodic points in towers of finite fields for polynomials associated to algebraic groups. *Rocky Mountain J. Math.*, 49(1):171–197, 2019.

[8] Min Sha and Su Hu. Monomial dynamical systems of dimension one over finite fields. *Acta Arith.*, 148(4):309–331, 2011.

[9] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1992.

[10] Joseph H. Silverman. *The Arithmetic of Dynamical Systems*, volume 241 of *Graduate Texts in Mathematics*. Springer-Verlag, 2007.

[11] Simone Ugolini. Functional graphs of rational maps induced by endomorphisms of ordinary elliptic curves over finite fields. *Period. Math. Hungar.*, 77(2):237–260, 2018.

(Z. Bell) Harvey Mudd College, Claremont, CA 91711
Email address: zbell@g.hmc.edu

(J. Camero) Dept. of Mathematics, Emory University, Atlanta, GA 30322
Email address: jasmine.camero@emory.edu

(K. Cho) Dept. of Mathematics, Stony Brook University, Stony Brook, NY, 11794-3651
Email address: karina.cho@stonybrook.edu

(T. Hyde) Dept. of Mathematics, University of Chicago, Chicago, IL 60637
Email address: tghyde@uchicago.edu

(F. Lu) California Sate University San Marcos, 333 S Twin Oaks Valley Rd, San Marcos, CA 92096
Email address: clu@csusm.edu

(R. Miller) Dept. of Mathematics and Statistics, Saint Louis University, MO, 63103
Email address: r.lauren.miller@slu.edu

(B. Thompson) Dept. of Mathematics, Westminster College, 1840 S 1300 E, Salt Lake City, UT 84105, USA
Email address: bthompson@westminstercollege.edu

(E. Zhu) Dept. of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332
Email address: ezhu31@gatech.edu