# Arithmetic Dynamics and Finite Fields

Michelle Manes (mmanes@math.hawaii.edu)

University of Hawaiʻi at Mānoa

July 16, 2012

# Definitions

## Definition

A *discrete dynamical system* is a set $S$ with a self-map

$$\phi : S \to S.$$

$$\phi^n(x) = \underbrace{\phi \circ \phi \circ \cdots \circ \phi}_{n \text{ times}}(x) \quad \text{and} \quad \phi^0(x) = x.$$

The *orbit* of $x$ is the set of iterates:

$$\mathcal{O}_\phi(x) = \left\{x, \phi(x), \phi^2(x), \ldots\right\}.$$

# Definitions

## Definition

A point $x \in S$ is

- *periodic* if $\phi^n(x) = x$ for some $n > 0$,
- *preperiodic* if $\phi^n(x) = \phi^m(x)$ for some $n > m \geq 0$ (equivalently, $\mathcal{O}_\phi(x)$ is finite), and
- *wandering* if $\mathcal{O}_\phi(x)$ is infinite.

$$\mathrm{Per}(\phi, S) = \{x \in S\colon\ x \text{ is periodic}\}.$$
$$\mathrm{PrePer}(\phi, S) = \{x \in S\colon\ x \text{ is preperiodic}\}.$$

# A suggestive diagram

## Lattès Maps

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

## Key parallels

| **Arithmetic Geometry** | | **Dynamical Systems** |
|---|---|---|
| rational points on varieties | $\longleftrightarrow$ | rational points in orbits |
| torsion points | $\longleftrightarrow$ | preperiodic points |
| finitely generated groups | $\longleftrightarrow$ | orbits of wandering points |

# Dynamical Versions of Classical Results

## Theorem (Mordell-Weil)

*If $A$ is an abelian variety defined over a number field $K$, then the group of $K$-rational points is a finitely generated abelian group. In particular,*

$$A(K)_{\text{tors}} \text{ is finite.}$$

## Theorem (Northcott)

*If $\phi : \mathbb{P}^n \to \mathbb{P}^n$ is a morphism defined over a number field $K$, then* $\mathrm{PrePer}\left(\phi, \mathbb{P}^n_{\overline{K}}\right)$ *is a set of bounded height. In particular,*

$$\mathrm{PrePer}\left(\phi, \mathbb{P}^n(K)\right) \text{ is finite.}$$

# Dynamical Versions of Classical Results

### Conjecture

*For each pair $(d, g)$ of positive integers, there exists a positive integer $B(d, g)$ such that if $[K : \mathbb{Q}] = d$ and $A$ is any $g$-dimensional abelian variety defined over $K$, then*

$$\#A(K)_{\text{tors}} \leq B(d, g).$$

### Conjecture

*For each triple of positive integers $m \geq 2$, $d \geq 1$, and $n \geq 1$, there exists a positive integer $C = C(m, d, n)$ such that if $[K : \mathbb{Q}] = d$ and $\phi : \mathbb{P}^n \to \mathbb{P}^n$ is a morphism of degree $m$ defined over $K$, then*

$$\#PrePer(\phi, \mathbb{P}^n(K)) \leq C(m, d, n).$$

# Dynamical Versions of Classical Results

## Theorem (Raynaud)

*Let $A/\mathbb{C}$ be an abelian variety and let $X \subset A$ be an algebraic subvariety. Then the Zariski closure of $A_{\mathrm{tors}} \cap X$ in $A$ is a union of a finite number of translates of abelian subvarieties of $A$ by torsion points of $A$.*

## Conjecture (Dynamical Manin-Mumford Conjecture)

*Let $\phi : \mathbb{P}^n_{\mathbb{C}} \to \mathbb{P}^n_{\mathbb{C}}$ be a morphism of degree at least 2 and let $X \subset \mathbb{P}^n$ be an algebraic subvariety. Then the Zariski closure of*

$$PrePer(\phi, \mathbb{P}^n_{\mathbb{C}}) \cap X$$

*in $\mathbb{P}^n$ is a union of a finite number of $\phi$-preperiodic subvarieties of $\mathbb{P}^n$.*

# Dynamical Versions of Classical Results

**Theorem (Faltings)**

*Let $A/\mathbb{C}$ be an abelian variety, let $\Gamma \subset A(\mathbb{C})$ be a finitely generated subgroup, and let $X \subset A$ be an algebraic subvariety that contains no nontrivial abelian subvarieties of $A$. Then*

$$X \cap \Gamma \text{ is a finite set.}$$

**Conjecture (Dynamical Mordell-Lang Conjecture)**

*Let $\phi : \mathbb{P}^n_{\mathbb{C}} \to \mathbb{P}^n_{\mathbb{C}}$ be a morphism of degree at least 2, let $P \in \mathbb{P}^n(\mathbb{C})$ be a wandering point for $\phi$, and let $X \subset \mathbb{P}^n$ be an irreducible algebraic subvariety that contains no $\phi$-periodic subvarieties of dimension at least one. Then*

$$X \cap \mathcal{O}_\phi(P) \text{ is a finite set.}$$

# Good reduction

A rational map $\phi(z) \in \mathbb{Q}(z)$ is in *normalized form* if

$$\phi(z) = \frac{F(z)}{G(z)} = \frac{a_d z^d + a_{d-1} z^{d-1} + \cdots + a_0}{b_d z^d + b_{d-1} z^{d-1} + \cdots + b_0},$$

with $F, G \in \mathbb{Z}[z]$ having no common factor and having coefficients that satisfy

$$\gcd(a_0, \ldots, a_d, b_0, \ldots, b_d) = 1.$$

Reduce modulo a prime $p$ to get

$$\tilde{\phi}(z) = \frac{\tilde{F}(z)}{\tilde{G}(z)} = \frac{\tilde{a}_d z^d + \tilde{a}_{d-1} z^{d-1} + \cdots + \tilde{a}_0}{\tilde{b}_d z^d + \tilde{b}_{d-1} z^{d-1} + \cdots + \tilde{b}_0} \in \mathbb{F}_p[z].$$

# Good reduction

**Definition**

$\phi$ has *good reduction* at $p$ if $\deg(\phi) = \deg(\tilde{\phi})$ (equivalently if $\tilde{F}$ and $\tilde{G}$ have no common factors in $\mathbb{F}_p[z]$).

$\mathrm{Res}(F, G) = 0$ precisely when $F$ and $G$ have a common factor.

**Definition**

$\phi$ has *good reduction* at $p$ if and only if $p \nmid \mathrm{Res}(F, G)$.

# Periodic points mod $p$

**Theorem (Morton-Silverman)**

*Let $\phi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \geq 2$ and let $p$ be a prime of good reduction for $\phi$. Let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a periodic point for $\phi$ and set*

$$n = \text{the exact period of } \alpha \text{ for the map } \phi.$$
$$m = \text{the exact period of } \tilde{\alpha} \text{ for the map } \tilde{\phi}.$$
$$r = \text{the smallest integer such that } \left(\left(\tilde{\phi}^m\right)'(\tilde{\alpha})\right)^r = 1.$$

*Then*

$$n = m \quad \text{or} \quad n = mr \quad \text{or} \quad n = mrp.$$

*(If $p \geq 5$ then only the first two are possible.)*

# Periodic points mod $p$

## Sketch of Proof.

If $m \neq n$: Write $n = m\gamma + \rho$ with $0 \leq \rho < m$.
WLOG take $\alpha = 0$. We have $\tilde{\phi}^n(0) = 0$, but also $\tilde{\phi}^m(0) = 0$.
So $\phi^\rho(0) = 0$, and $m$ minimal $\Rightarrow r = 0$. Hence $m \mid n$.

Replace $\phi$ by $\phi^m$, $m$ by 1, $n$ by $n/m$. Write $\lambda = \tilde{\phi}'(0)$.
Iterate the Taylor expansion for $\phi$ around $z = 0$ and see that

$$1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1} \equiv 0 \pmod{p}. \qquad (*)$$

If $\lambda \not\equiv 1 \pmod{p}$, then $\lambda^n \equiv 1 \pmod{p}$ so $r \mid n$.

If $n \neq r$: Replace $\phi$ by $\phi^r$ and $n$ by $n/r$.
This replaces $\lambda$ with $\lambda^r \equiv 1 \pmod{p}$, so by $(*)$ $p \mid n$.
Repeat argument to get $n = mrp^e$.
Take one more term in Taylor expansion to get $e = 1$. □

# Periodic points mod $p$

**Sketch of Proof.**

If $m \neq n$: Write $n = m\gamma + \rho$ with $0 \leq \rho < m$.
WLOG take $\alpha = 0$. We have $\tilde{\phi}^n(0) = 0$, but also $\tilde{\phi}^m(0) = 0$.
So $\phi^\rho(0) = 0$, and $m$ minimal $\Rightarrow r = 0$. Hence $m \mid n$.

Replace $\phi$ by $\phi^m$, $m$ by 1, $n$ by $n/m$. Write $\lambda = \tilde{\phi}'(0)$.
Iterate the Taylor expansion for $\phi$ around $z = 0$ and see that

$$1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1} \equiv 0 \pmod{p}. \qquad (*)$$

If $\lambda \not\equiv 1 \pmod{p}$, then $\lambda^n \equiv 1 \pmod{p}$ so $r \mid n$.

If $n \neq r$: Replace $\phi$ by $\phi^r$ and $n$ by $n/r$.
This replaces $\lambda$ with $\lambda^r \equiv 1 \pmod{p}$, so by $(*)$ $p \mid n$.
Repeat argument to get $n = mrp^e$.
Take one more term in Taylor expansion to get $e = 1$. □

# Periodic points mod $p$

**Sketch of Proof.**

If $m \neq n$: Write $n = m\gamma + \rho$ with $0 \leq \rho < m$.
WLOG take $\alpha = 0$. We have $\tilde{\phi}^n(0) = 0$, but also $\tilde{\phi}^m(0) = 0$.
So $\phi^\rho(0) = 0$, and $m$ minimal $\Rightarrow r = 0$. Hence $m \mid n$.

Replace $\phi$ by $\phi^m$, $m$ by 1, $n$ by $n/m$. Write $\lambda = \tilde{\phi}'(0)$.
Iterate the Taylor expansion for $\phi$ around $z = 0$ and see that

$$1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1} \equiv 0 \pmod{p}. \qquad (*)$$

If $\lambda \not\equiv 1 \pmod{p}$, then $\lambda^n \equiv 1 \pmod{p}$ so $r \mid n$.

If $n \neq r$: Replace $\phi$ by $\phi^r$ and $n$ by $n/r$.
This replaces $\lambda$ with $\lambda^r \equiv 1 \pmod{p}$, so by $(*)$ $p \mid n$.
Repeat argument to get $n = mrp^e$.
Take one more term in Taylor expansion to get $e = 1$. □

# An application

## Corollary

*Let $\phi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \geq 2$ and let $p$ be the smallest prime for which $\phi(z)$ has good reduction. Suppose that $\alpha \in \mathbb{P}^1(\mathbb{Q})$ is a periodic point for $\phi$ of exact period $n$. Then*

$$n \leq p^3 - p.$$

*(If $p \geq 5$, then $n \leq p^2 - 1$.)*

## Proof.

$$n \leq mrp \leq (p+1)(p-1)p = p^3 - p.$$

□

# An application

**Corollary**

*Let $\phi(z) \in \mathbb{Q}[z]$ have good reduction at 2. Then all rational periodic points in $\mathbb{P}^1(\mathbb{Q})$ have period 1, 2, or 4.*

**Proof.**

$n = m$ or $n = mr$ or $n = 2mr$.

$\#\mathbb{F}_2^* = 1$, so $r$ can only be 1.

$\#\mathbb{P}^1(\mathbb{F}_2) = 3$, so possible values of $m$ are 1, 2, and 3.

But $\infty$ is fixed, so $m$ can just be 1 or 2. □

# Open questions

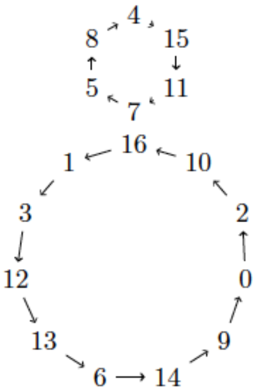
**Idea:** look at $\tilde{\phi}_p$ for varying primes $p$ of good reduction, and see what we can conclude about $\phi$ itself.

**Vague question:** If Per $\left(\tilde{\phi}_p, \mathbb{P}^1(\mathbb{F}_p)\right)$ is "large," does that imply that Per$(\phi, \mathbb{P}^1(\mathbb{Q}))$ is non-empty?

**Specific question:** If $\tilde{\phi}_p$ has a point of exact period $n$ for all but finitely many primes $p$ (all primes of good reduction?), does that imply that $\phi$ has a rational point of exact period $n$? Does it imply anything?

# Polynomial maps on $\mathbb{F}_q$

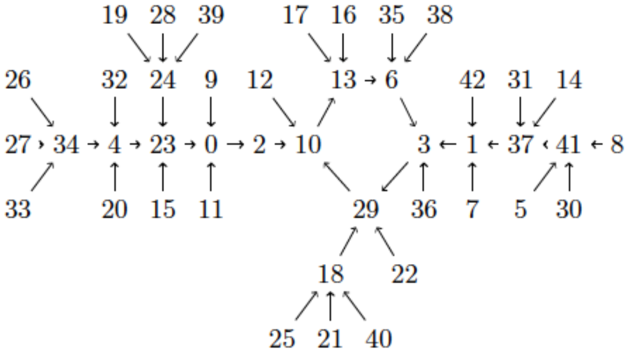
Do we expect a lot of periodic points?




$x^3 + 2$ over $\mathbb{F}_{17}$

# Polynomial maps on $\mathbb{F}_q$

Or do we expect a lot of strictly preperiodic points?




$x^3 + 2$ over $\mathbb{F}_{43}$

# Heuristic answer

Suppose $\phi : \mathbb{F}_q \to \mathbb{F}_q$ is $m$-to-1 over most points.

Iterating $\alpha \to \phi(\alpha) \to \phi^2(\alpha) \to \ldots$ is like picking with replacement from a set of $q$ elements.

Expect match after picking $\sqrt{q}$ elements. (Birthday problem.)
That is, we expect orbits have length about $\sqrt{q}$.

Each point in the orbit is equally likely to be the match.
So we don't expect to come back to the initial point.
That is, we expect to find strictly preperiodic points.

Since $\phi$ is $m$-to-1, we find branching in backwards orbits.
So we expect lots of strictly preperiodic points.

# One result

**Theorem (Madhu)**

*Let $\phi(z) = z^m + c$, with $m, c \in \mathbb{Z}$ and $m \geq 2$. Suppose that m, c are such that 0 is not a preperiodic point of $\phi$ over $\mathbb{Z}$. Let $E_m := \{\text{primes } p \colon p \equiv 1 \pmod{m}\}$. Then*

$$\lim_{\substack{p \to \infty \\ p \in E_m}} \frac{\mathrm{Per}(\phi, \mathbb{F}_p)}{p} = 0.$$

# Proof sketch

Notice: $\alpha$ periodic for $\phi$ iff $\alpha \in \mathrm{Im}(\phi^n)$ for all $n$.

## Step 1: Prime ideals of function field $\mathbb{F}_p(t)$

- Define polynomials $\phi_n(t) = \phi^n(z) - t \in \mathbb{F}_p(t)[z]$ and a principal prime ideal $\mathfrak{p}_\alpha := (t - \alpha)$
- $\phi_n$ has a root modulo $\mathfrak{p}_\alpha$ for every $n$ iff $\alpha$ is periodic.
- $K_n =$ splitting field of $\phi_n$ over $\mathbb{F}_p(t)$,
  $G_n = \mathrm{Gal}(K_n/\mathbb{F}_p(t))$, and
  $\mathrm{Frob}(\mathfrak{p}_\alpha) =$ conjugacy class of Frobenius in $G_n$.
- Factor $\phi_n \mod \mathfrak{p}_\alpha = \prod_{i=1}^{s} g_i(z)$ with $\deg(g_i) = m_i$.
- Each element of $\mathrm{Frob}(\mathfrak{p}_\alpha) = s$ disjoint cycles of length $m_i$.

# Proof sketch

**Step 1: Summary**

$\alpha$ is periodic for $\phi$ iff the elements of $\mathrm{Frob}(\mathfrak{p}_\alpha)$ in $G_n$ have a fixed point for every $n$.

# Proof sketch

## Step 2: Effective Chebotarev

- $g_n =$ genus of the curve $X_n$ given by $\phi_n$ (equivalently genus of the field $K_n$).
- $C_i \subset G_N$ conj classes whose elements have fixed points, $N = \#C_i$, and $C = \bigcup_{i=1}^{N} C_i$.
- $\psi = \{$points in $\mathbb{P}^1(\mathbb{F}_p)$ that are unramified in $X_n\}$, $\psi_C = \{\beta \in \psi \colon \text{Frob}(\beta) \subset C\}$, and $D = \#\left(\mathbb{P}^1(\mathbb{F}_p) \setminus \psi\right)$ (number of ramified points).

## Theorem

$$\left| \frac{\#\psi_C}{\#\psi} - \frac{\#C}{\#G_n} \right| < \frac{1}{\#\psi} \left( 2g_n \frac{\#C}{\#G_n} \sqrt{p} + ND \right).$$

# Proof sketch

**Theorem**

$$\left| \frac{\#\psi_C}{\#\psi} - \frac{\#C}{\#G_n} \right| < \frac{1}{\#\psi} \left( 2g_n \frac{\#C}{\#G_n} \sqrt{p} + ND \right).$$

**Step 2: Effective Chebotarev**

- For $p$ sufficiently large, $N$, $D$ and $g_n$ depend only on $\phi_n$. So RHS goes to 0 as $p$ goes to $\infty$.
- Proportion of periodic points for $\phi$ in $\mathbb{F}_p$ approximated by proportion of elements in $G_n$ that fix at least one root of $\phi_n$.
- Structure of $G_n$ with result of Odoni $\Longrightarrow \lim_{n\to\infty} \frac{\#C}{\#G_n} \to 0$.

# Open questions

**Other polynomials?** The only critical point of $z^m + c$ is $z = 0$, so all ramification is over 0.

**Non-polynomials?** These are "almost polynomial":

$$\phi_a(x) = \frac{1 + ax + (3+a)x^2}{1 - (4+a)x - (a+1)x^2}, \qquad a \in \mathbb{Q} \setminus \{-2\}.$$

Critical points are 1 and $-1/3$
$\phi_a$ has the two-cycle $0 \mapsto 1 \mapsto -1 \mapsto 1$.

**Towers of finite fields?** For any map $\phi$, investigate

$$\lim_{n \to \infty} \frac{\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{p^n}))}{p^n + 1}.$$

# Remark

Let $\phi(z) = z^p + c$. In characteristic $p$, $\phi^n(z) = z^{p^n} + nc$.

$\phi^n(z)$ is a permutation polynomial on $\mathbb{F}_{p^n}$, so all points are periodic under $\phi$.

# Data: $\phi(z) = z^3$ over $\mathbb{F}_{2^n}$

For odd $n$, all points are periodic. For even $n$ we have:

| $n$ | proportion of periodic points |
|---|---|
| 2 | 0.500000000000000 |
| 4 | 0.375000000000000 |
| 6 | 0.125000000000000 |
| 8 | 0.335937500000000 |
| 10 | 0.333984375000000 |
| 12 | 0.111328125000000 |
| 14 | 0.333374023437500 |

# Data: $\phi(z) = z^2$ over $\mathbb{F}_{3^n}$

| $n$ | proportion of periodic points |
|---|---|
| 1 | 0.666666666666667 |
| 2 | 0.222222222222222 |
| 3 | 0.518518518518518 |
| 4 | 0.0740740740740741 |
| 5 | 0.502057613168724 |
| 6 | 0.126200274348422 |
| 7 | 0.500228623685414 |
| 8 | 0.0313976527968298 |
| 9 | 0.500025402631713 |
| 10 | 0.125014818201832 |

# Data: $\phi(z) = z^2 + 1$ over $\mathbb{F}_{3^n}$

| | |
|---|---|
| 1 | 0.333333333333333 |
| 2 | 0.333333333333333 |
| 3 | 0.370370370370370 |
| 4 | 0.283950617283951 |
| 5 | 0.374485596707819 |
| 6 | 0.312757201646091 |
| 7 | 0.374942844078647 |
| 8 | 0.265660722450846 |
| 9 | 0.374993649342072 |
| 10 | 0.312503175328964 |

# Data: $\phi(z) = z^2 + 2$ over $\mathbb{F}_{3^n}$

| | |
|---|---|
| 1 | 0.666666666666667 |
| 2 | 0.444444444444444 |
| 3 | 0.185185185185185 |
| 4 | 0.0493827160493827 |
| 5 | 0.296296296296296 |
| 6 | 0.0589849108367627 |
| 7 | 0.0841335162322817 |
| 8 | 0.0164609053497942 |
| 9 | 0.0313468475334045 |
| 10 | 0.0105674947924605 |

# More results

## Flynn and Garton

Consider a finite field $\mathbb{F}_q$ and rational maps $\phi : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ of degree $m$. When $m \geq \sqrt{q}$:

- The average number of connected components of the graphs of all such $\phi$ is bounded below by

$$\frac{1}{2} \log q - 4.$$

- The average number of periodic points bounded below by

$$\frac{5}{6}\sqrt{q} - 4.$$

# Sketch of proof

Count the number of rational functions of a fixed degree that give an arbitrary cycle, then sum over possible cycles to obtain the results. More precisely, we compute the following quantities:

$$\sum_{\substack{\phi \in \mathbb{F}_q(z) \\ \deg \phi = m}} |\{\text{cycles in } \Gamma_\phi\}|, \text{ and}$$

$$\sum_{\substack{\phi \in \mathbb{F}_q(z) \\ \deg \phi = m}} |\{k\text{-cycles in } \Gamma_\phi\}|.$$

# Open questions

**Small degree?** The techniques used don't work for small degree because you can get "long cycles" (length greater than $m + 2$), and Flynn & Garton don't count those.