An arithmetic dynamical Mordell-Lang theorem

Trevor Hyde
University of Michigan

Joint work with Mike Zieve

Squares in orbits

- Let $f(x) \in \mathbb{Q}(x)$ be a rational function, $a \in \mathbb{Q}$.
- Which $f^n(a)$ are squares?

Squares in orbits

- $f(x) = x^2$ and $a =$ anything
  - $f^n(a)$ is a square for all $n \geq 1$.
- $f(x) = x + 1$ and $a = 0$
  - $f^n(0) = n$ is a square when n is a square.
- These are boring examples...too easy.

Squares in orbits

- $f(x) = -x^3 + 4x^2 - 4x$ and $a = 1$

n	$f^n(1)$		
0	1	$=$	1^2
1	-1		
2	9	$=$	3^2
3	-441		
4	86545809	$=$	9303^2
5	$-648243402857703503235441$		

- Every other iterate is a square!

Squares in orbits

- $f(x) = -x^3 + 4x^2 - 4x$ and $a = 3$

n	$f^n(3)$
0	3
1	-3
2	75
3	-399675
4	63844765677693075

- No square iterates!

Squares in orbits

- All orbits of $f(x) = -x^3 + 4x^2 - 4x$ have one of these two forms (with the exception of the fixed point $a = 0$.)
- Hint: $f(x) = -x^3 + 4x^2 - 4x = -x(x-2)^2$.
- **Main observation:** When there are infinitely many squares in an orbit, they appear periodically.

General question

- Suppose we have
  - a field K,
  - rational function $f(x) \in K(x)$,
  - $a \in K$,
  - a curve $\mathcal{C}/K$ together with a map $u : \mathcal{C} \to \mathbb{P}^1$.
- Which iterates $f^n(a)$ are in $u(\mathcal{C}(K))$?
- Original question: $\mathcal{C} = \mathbb{P}^1$ and $u(x) = x^2$.

General question

- Which iterates $f^n(a)$ are in $u(\mathcal{C}(K))$?
- Question posed by Cahn, Jones, Spear (2016) who give a complete answer when $\mathcal{C} = \mathbb{P}^1$ and $u(x) = x^m$.
- They conjecture the answer in general.

Main result

Theorem (H, Zieve)

Let K be a finitely generated field of characteristic 0. Suppose

- *$\mathcal{C}/K$ is a curve together with $u : \mathcal{C} \to \mathbb{P}^1$,*
- *$f(x) \in K(x)$ is a rational function with $\deg(f) \geq 2$.*

If $a \in K$, then $\{n : f^n(a) \in u(\mathcal{C}(K))\}$ is a finite union of arithmetic progressions.

- Arithmetic progression $= \{m + k\ell : k \in \mathbb{N}\}$ for some m, ℓ. Note: $\ell = 0$ is allowed.

- $\deg(f) \geq 2$ excludes counterexamples like $f(x) = x + 1$.

Main result

Theorem (H, Zieve)

Let K be a finitely generated field of characteristic 0. Suppose

- *$\mathcal{C}/K$ is a curve together with $u : \mathcal{C} \to \mathbb{P}^1$,*
- *$f(x) \in K(x)$ is a rational function with $\deg(f) \geq 2$.*

If $a \in K$, then $\{n : f^n(a) \in u(\mathcal{C}(K))\}$ is a finite union of arithmetic progressions.

- This result may be seen as an "arithmetic dynamical Mordell-Lang theorem for curves."
- Roughly: if an orbit of f enters the image of u infinitely often, then it does so periodically with only finitely many exceptions.

Step 1: Translation

1. Translate into the “dynamics of fiber products.”

Fiber products

- A, B, C curves defined over a field K.

$$\begin{array}{ccc} A & \xleftarrow{v'} & A \times_C B \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u'} \\ C & \xleftarrow[v]{} & B \end{array}$$

- $A \times_C B$ is a union of curves defined over K ($K(A) \otimes_{K(C)} K(B)$ not necessarily a field.)

- **Concretely:** If u, v are rational functions, then $A \times_C B$ is defined by $u(x) = v(y)$, and u', v' are projections onto y, x coordinates.

Fiber products

- A, B, C curves defined over a field K.

$$\begin{array}{ccc} A & \xleftarrow{v'} & A \times_C B \\ {\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u'} \\ C & \xleftarrow[v]{} & B \end{array}$$

- **Key property:** Points on $A \times_C B$ are the same as pairs of points on A and B mapping to the same point in C.

Dynamics of fiber products

- If $f : \mathbb{P}^1 \to \mathbb{P}^1$ is a rational function, we can take fiber products of u with f^n.

$$\begin{array}{ccccccccc}
\mathcal{C} & \longleftarrow & \mathcal{C}_1 & \longleftarrow & \mathcal{C}_2 & \longleftarrow & \mathcal{C}_3 & \longleftarrow & \mathcal{C}_4 \\
{\scriptstyle u}\big\downarrow & & \big\downarrow{\scriptstyle u_1} & & \big\downarrow{\scriptstyle u_2} & & \big\downarrow{\scriptstyle u_3} & & \big\downarrow{\scriptstyle u_4} \\
\mathbb{P}^1 & \xleftarrow[f]{} & \mathbb{P}^1 & \xleftarrow[f]{} & \mathbb{P}^1 & \xleftarrow[f]{} & \mathbb{P}^1 & \xleftarrow[f]{} & \mathbb{P}^1
\end{array}$$

- View this as a dynamical system: u_n is the "nth iterate of u" under iterated fiber products with f.

Translation

$$
\begin{array}{ccccccccc}
\mathcal{C} & \longleftarrow & \mathcal{C}_1 & \longleftarrow & \cdots & \longleftarrow & \mathcal{C}_m & \longleftarrow & \cdots & \longleftarrow & \mathcal{C}_{m+\ell} \\
{\scriptstyle u}\downarrow & & \downarrow{\scriptstyle u_1} & & & & \downarrow{\scriptstyle u_m} & & & & \downarrow{\scriptstyle u_{m+\ell}} \\
\mathbb{P}^1 & \underset{f}{\longleftarrow} & \mathbb{P}^1 & \underset{f}{\longleftarrow} & \cdots & \underset{f}{\longleftarrow} & \mathbb{P}^1 & \underset{f}{\longleftarrow} & \cdots & \underset{f}{\longleftarrow} & \mathbb{P}^1
\end{array}
$$

- **Correspondence:** $f^m(a) \in u(\mathcal{C}(K)) \iff a \in u_m(\mathcal{C}_m(K))$.

- Suppose u has a finite orbit under f, say $u_{m+\ell} = u_m$.

$$a \in u_m(\mathcal{C}_m(K)) \Longrightarrow f^{m+k\ell}(a) \in u(\mathcal{C}(K))$$

- u **has finite orbit** $\Longrightarrow \{n : f^n(a) \in u(\mathcal{C}(K))\}$ **is a finite union of arithmetic progressions.**

Step 2: Reduction

- If we can show u has a finite orbit under iterated fiber products with f, then we are done!
- ...but that's not true.
- **Generic case:** $\{n : f^n(a) \in u(\mathcal{C}(K))\}$ is finite.
- We show u has finite orbit when $\{n : f^n(a) \in u(\mathcal{C}(K))\}$ is infinite.

Step 2: Reduction

- **Reduction:** suppose all $\mathcal{C}_m$ are geometrically irreducible and that there are infinitely many distinct $f^n(a)$ in $u(\mathcal{C}(K))$.
  - $\implies \mathcal{C}_m(K)$ is infinite for all $m \geq 0$.

Theorem (Faltings)

Let K be a finitely generated field of characteristic 0 and let $\mathcal{C}$ be a smooth projective curve defined over K.
If $\mathcal{C}(K)$ is infinite, then $\mathcal{C}$ has genus at most 1.

- Therefore $\mathcal{C}_m$ has genus at most 1 for all m.

Bounded genus

- All $\mathcal{C}_m$ having genus at most 1 is a very strong constraint!

Theorem (H, Zieve)

Let $V \subset \mathbb{P}^1(\overline{K})$ be the set of critical values of u_m for all m. The following are equivalent:

1. *All $\mathcal{C}_m$ have genus at most 1,*
2. *V is finite,*
3. *V has at most 4 elements.*

In this case, $f(V) \subseteq V$.

- Given our reduction, all u_m have critical values contained in a set V with at most 4 elements.

Step 3: Topology

- **Topology:** up to isomorphism there are finitely many branched covers of $\mathbb{P}^1(\overline{K})$ with degree d and critical values contained in a finite set V.
- For all m, $\deg(u_m) = \deg(u)$ and $\mathrm{crit}(u_m) \subseteq V$.
- Therefore u has a finite orbit!

Strategy overview

1. Translate into the "dynamics of fiber products."
   - $\{n : f^n(a) \in u(\mathcal{C}(K))\}$ = a finite union of arithmetic progressions $\approx$ u has finite orbit under iterated fiber products with f.
2. Reduce to a tractable problem with Faltings's Theorem.
   - All $\mathcal{C}_m$ have genus at most 1.
   - This is where we need K to be finitely generated.
3. Topology of branched covers $\implies$ u has finite orbit.
   - This is where we need $\mathrm{char}(K) = 0$.

Further questions

- Given f, can we determine all preperiodic maps u?
- Can we give sharp bounds on the tail length and period length of a map u?

Thank you!