Uniform Bounds for Rational Iterated Pre-Images

Xander Faber
University of Georgia

AMS Spring Eastern Sectional Meeting
Special Session on Number Theory, Arithmetic Topology, and Arithmetic Dynamics
April 9, 2011
Motivation

**Theorem.** (Manin, ’69) Given a number field $k$ and a rational prime $p$, there exists $C(k, p) \geq 1$ so that: For an elliptic curve $E/k$, the order of the $p$-power torsion subgroup of $E(k)$ does not exceed $C(k, p)$. 
**Motivation**

**Theorem.** (Manin, ’69) Given a number field $k$ and a rational prime $p$, there exists $C(k, p) \geq 1$ so that: For an elliptic curve $E/k$, the order of the $p$-power torsion subgroup of $E(k)$ does not exceed $C(k, p)$.

\[
\text{“} p^n \text{-torsion on } E \text{”} := \{Q \in E(\overline{k}) : p^n Q = O\} = \phi_{E,p}^{-n}(O) \\
= \text{“} n \text{th pre-images of } O \text{ under } \phi_{E,p} \text{”},
\]

where $\phi_{E,p} : E \to E$ is the multiplication-by-$p$ morphism.
**Motivation**

**Theorem.** (Manin, ’69) Given a number field $k$ and a rational prime $p$, there exists $C(k, p) \geq 1$ so that: For an elliptic curve $E/k$, the order of the $p$-power torsion subgroup of $E(k)$ does not exceed $C(k, p)$.

\[ \text{“}p^n\text{-torsion on } E\text{”} := \{ Q \in E(\overline{k}) : p^n Q = \mathcal{O} \} = \phi_{E,p}^{-n}(\mathcal{O}) \]

\[ = \text{“}n^{th}\text{ pre-images of } \mathcal{O} \text{ under } \phi_{E,p}\text{”,} \]

where $\phi_{E,p} : E \to E$ is the multiplication-by-$p$ morphism.

**Rephrase:**  $C(k, p) := \sup_{E/k \text{ elliptic curve}} \# \bigcup_{n \geq 1} \phi_{E,p}^{-n}(\mathcal{O})(k) < \infty$. 
A Dynamical Analogue

**Theorem.** (Manin) For any elliptic curve $E/k$, \[ \# \bigcup_{n \geq 1} \phi_{E,p}^{-n}(\mathcal{O})(k) \leq C(k,p). \]
A Dynamical Analogue

**Theorem.** (Manin) For any elliptic curve $E/k$, \( \# \bigcup_{n \geq 1} \phi_{E,p}^{-n}(\mathcal{O})(k) \leq C(k, p) \).

1-parameter family of dynamical systems $f_c : \mathbb{P}^1 \to \mathbb{P}^1$ defined by

$$f_c(z) = z^2 + c$$
A Dynamical Analogue

**Theorem.** (Manin) For any elliptic curve $E/k$, $\# \bigcup_{n \geq 1} \phi_{E,p}^{-n}(\mathcal{O})(k) \leq C(k,p)$.

1-parameter family of dynamical systems $f_c : \mathbb{P}^1 \to \mathbb{P}^1$ defined by

$$f_c(z) = z^2 + c$$

**Theorem.** (FHIJMTZ, '09) Let $k$ be a number field. For all but finitely many basepoints $b \in \mathbb{A}^1(k)$,

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty.$$
A Dynamical Analogue

**Theorem.** (Manin) For any elliptic curve $E/k$, $\# \bigcup_{n \geq 1} \phi_{E,p}^{-n}(\mathcal{O})(k) \leq C(k, p)$.

1-parameter family of dynamical systems $f_c : \mathbb{P}^1 \to \mathbb{P}^1$ defined by

$$f_c(z) = z^2 + c$$

**Theorem.** (FHIJMTZ, '09) Let $k$ be a number field. For all but finitely many basepoints $b \in \mathbb{A}^1(k)$,

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty.$$ 

**Remarks.**
1. Number of exceptional basepoints is $\leq 16[k : \mathbb{Q}]$. (Expect zero.)
2. If $k = \mathbb{Q}$, then no exceptional basepoints.
3. For fixed $c$, $\# \bigcup_{N \geq 1} f_c^{-N}(b)(k)$ is finite by a descent argument.
Proof Ideas

**Theorem.** (FHIJMTZ) Let \( k \) be a number field. For all but finitely many \( b \in \mathbb{A}^1(k) \), we have

\[
\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty.
\]
Proof Ideas

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

\[
\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty.
\]

- Define the “pre-image curve” $X^\text{pre}(N, b)$: nonsingular complete model of $\{(c, x) : f_c^N(x) = b\} \subset \mathbb{A}^2$. They fit into a tower:

\[
\cdots \longrightarrow X^\text{pre}(N, b) \longrightarrow X^\text{pre}(N - 1, b) \longrightarrow \cdots \longrightarrow X^\text{pre}(1, b)
\]

\[
(c, x) \mapsto (c, f_c(x))
\]
Proof Ideas

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty.$$  

- Define the “pre-image curve” $X^{\text{pre}}(N, b)$: nonsingular complete model of $\{(c, x) : f_c^N(x) = b\} \subset \mathbb{A}^2$. They fit into a tower:

  \[
  \cdots \longrightarrow X^{\text{pre}}(N, b) \longrightarrow X^{\text{pre}}(N - 1, b) \longrightarrow \cdots \longrightarrow X^{\text{pre}}(1, b)
  \]

  \[
  (c, x) \mapsto (c, f_c(x))
  \]

- If $X^{\text{pre}}(N, b)$ is smooth and irreducible,
  \[
  \Rightarrow \quad \text{genus}(X^{\text{pre}}(N, b)) = 2^{N-2}(N - 3) + 1
  \]

- $X^{\text{pre}}(N, b)$ is smooth and irreducible for fixed $N$ and almost all $b$. 
Proof Ideas

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$
\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty.
$$

- Define the “pre-image curve” $X^{\text{pre}}(N, b)$: nonsingular complete model of $\{(c, x): f_c^N(x) = b\} \subset \mathbb{A}^2$. They fit into a tower:

$$
\cdots \rightarrow X^{\text{pre}}(N, b) \rightarrow X^{\text{pre}}(N - 1, b) \rightarrow \cdots \rightarrow X^{\text{pre}}(1, b)
$$

$$(c, x) \mapsto (c, f_c(x))$$

- If $X^{\text{pre}}(N, b)$ is smooth and irreducible,

$$
\quad \implies \quad \text{genus}(X^{\text{pre}}(N, b)) = 2^{N-2}(N-3) + 1
$$

- $X^{\text{pre}}(N, b)$ is smooth and irreducible for fixed $N$ and almost all $b$.

- $N = 4 \implies X^{\text{pre}}(4, b)(k)$ is a finite set by Faltings’ theorem.

- Treat finitely many remaining $c$-values with a descent argument.
What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} \mathcal{S}_{c^N}(b)(k) < \infty.$$
What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_{c}^{-N}(b)(k) < \infty.$$ 

**Answer 1 (Easy):** It depends on $b$.

*e.g.*, $b := f_0^N(2) = 2^{2^N} \implies \beta(k, b) \geq N$
What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty.$$ 

**Answer 1 (Easy):** It depends on $b$.

*e.g.*, $b := f_0^N(2) = 2^{2^N} \implies \beta(k, b) \geq N$

**Answer 2 (Harder):** Conjecturally, for fixed $k$ it depends at most on the height of $b$.

**Theorem.** (F, ’10) Let $k$ be a number field. If an effective Mordell conjecture for families is true, then there exists a constant $\gamma = \gamma(k) > 0$ such that

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) \ll_k H(b)^{\gamma}.$$
What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty.$$
What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_{c^{-N}}(b)(k) < \infty.$$  

**Answer 3 (Easy):** It depends on $k$.

e.g., Fix $N$ and $b$. Choose $k$ so that $X_{\text{pre}}(N, b)$ has “interesting” $k$-rational points. Then $\beta(k, b) \geq N$. 

What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) : = \sup_{c \in k} \# \bigcup_{N \geq 1} f^{-N}_c(b)(k) < \infty.$$ 

**Answer 3 (Easy):** It depends on $k$.

* e.g., Fix $N$ and $b$. Choose $k$ so that $X^{\text{pre}}(N, b)$ has “interesting” $k$-rational points. Then $\beta(k, b) \geq N$.

**Answer 4 (Harder):** It depends at most on $D = [k : \mathbb{Q}]$.

**Theorem.** (FHIJMTZ, ’09) Fix $D \geq 1$. For all but finitely many $b \in \overline{\mathbb{Q}}$,

$$\beta'(D, b) : = \sup_{k \in S_{D, b}} \sup_{c \in k} \# \bigcup_{N \geq 1} f^{-N}_c(b)(k) < \infty,$$

where $S_{D, b}$ is the set of number fields $k$ such that $[k : \mathbb{Q}] \leq D$ and $b \in k$. 
What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty.$$ 

**Answer 3 (Easy):** It depends on $k$.

* e.g., Fix $N$ and $b$. Choose $k$ so that $X^{\text{pre}}(N, b)$ has “interesting” $k$-rational points. Then $\beta(k, b) \geq N$.

**Answer 4 (Harder):** It depends at most on $D = [k : \mathbb{Q}]$.

**Theorem.** (FHIJMTZ, ’09) Fix $D \geq 1$. For all but finitely many $b \in \overline{\mathbb{Q}}$,

$$\beta'(D, b) := \sup_{k \in S_{D,b}} \sup_{c \in k} \# \bigcup_{N \geq 1} f_c^{-N}(b)(k) < \infty,$$

where $S_{D,b}$ is the set of number fields $k$ such that $[k : \mathbb{Q}] \leq D$ and $b \in k$.

**Idea:** Determine gonality of $X^{\text{pre}}(N, b)$ and apply Vojta’s refinement of Faltings’ theorem.
What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_{c^{-N}}(b)(k) < \infty.$$
What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

$$\beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f^{-N}_c(b)(k) < \infty.$$  

**Answer 5 (Harder):** It depends on the arithmetic of the curves $X^{\text{pre}}(N, b)$ for small $N$.

**Theorem.** (F / Hutz / Stoll, ’11) Assuming standard conjectures*, $\beta(\mathbb{Q}, 0) = 6$.  

Unconditionally, we have

$$\overline{\beta}(\mathbb{Q}, 0) := \limsup_{c \in \mathbb{Q}} \# \bigcup_{N \geq 1} f^{-N}_c(0)(\mathbb{Q}) = 6.$$  

---

* BSD plus analytic continuation and existence of the functional equation for the $L$-series of a particular abelian variety of dimension 5.
What does $\beta(k, b)$ depend on?

**Theorem.** (FHIJMTZ) Let $k$ be a number field. For all but finitely many $b \in \mathbb{A}^1(k)$, we have

\[ \beta(k, b) := \sup_{c \in k} \# \bigcup_{N \geq 1} f_{c}^{-N}(b)(k) < \infty. \]

**Answer 5 (Harder):** It depends on the arithmetic of the curves $X^{\text{pre}}(N, b)$ for small $N$.

**Theorem.** (F / Hutz / Stoll, '11) Assuming standard conjectures*, $\beta(\mathbb{Q}, 0) = 6$.

Unconditionally, we have

\[ \overline{\beta}(\mathbb{Q}, 0) := \limsup_{c \in \mathbb{Q}} \# \bigcup_{N \geq 1} f_{c}^{-N}(0)(\mathbb{Q}) = 6. \]

**Ideas:**

1. Find all rational points on the genus 5 curve $X^{\text{pre}}(4, 0)$. [Hard, but feasible subject to standard conjectures]

2. Define algebraic curves parameterizing different pre-image configurations and find all rational points on them. [Hard, but feasible.]

* BSD plus analytic continuation and existence of the functional equation for the $L$-series of a particular abelian variety of dimension 5.
Levin’s Conjecture

\[ \text{Hom}_d := \{ \phi : \mathbb{P}^1 \to \mathbb{P}^1 \text{ of degree } d \} \]
Levin’s Conjecture

\[ \text{Hom}_d := \{ \phi : \mathbb{P}^1 \to \mathbb{P}^1 \text{ of degree } d \} \hookrightarrow \mathbb{P}^{2d+1} \]

\[ \phi(z) = \frac{a_d z^d + \cdots + a_0}{b_d z^d + \cdots + b_0} \mapsto (a_d : \cdots : a_0 : b_d : \cdots : b_0) \]
Levin’s Conjecture

\[ \text{Hom}_d := \{ \phi : \mathbb{P}^1 \rightarrow \mathbb{P}^1 \text{ of degree } d \} \hookrightarrow \mathbb{P}^{2d+1} \]

\[ \phi(z) = \frac{a_d z^d + \cdots + a_0}{b_d z^d + \cdots + b_0} \mapsto (a_d : \cdots : a_0 : b_d : \cdots : b_0) \]

\( \text{PGL}_2 \) acts on \( \text{Hom}_d \) via conjugation: \( \phi^\sigma = \sigma^{-1} \circ \phi \circ \sigma \)

\( M_d := \text{Hom}_d / \text{PGL}_2 \)
Levin’s Conjecture

\[ \text{Hom}_d := \{ \phi : \mathbb{P}^1 \to \mathbb{P}^1 \text{ of degree } d \} \hookrightarrow \mathbb{P}^{2d+1} \]

\[ \phi(z) = \frac{a_d z^d + \cdots + a_0}{b_d z^d + \cdots + b_0} \mapsto (a_d : \cdots : a_0 : b_d : \cdots : b_0) \]

\[ \text{PGL}_2 \text{ acts on } \text{Hom}_d \text{ via conjugation: } \phi^\sigma = \sigma^{-1} \circ \phi \circ \sigma \]

\[ M_d := \text{Hom}_d / \text{PGL}_2 \]

**Definition.** An algebraic family of dynamical systems \( V \subset \text{Hom}_d \)

is **simple** if it is quasi-finite over its image in \( M_d \).

**Levin’s Conjecture.** Let \( V \subset \text{Hom}_d \) be a simple family defined over a number field \( k \), and let \( b \in k \) be a basepoint. Then

\[ \sup_{v \in V(k)} \# \bigcup_{N \geq 1} \phi_{v}^{-N}(b)(k) < \infty. \]
Levin’s Conjecture

$$\text{Hom}_d := \{ \phi : \mathbb{P}^1 \to \mathbb{P}^1 \text{ of degree } d \} \hookrightarrow \mathbb{P}^{2d+1}$$

$$\phi(z) = \frac{a_d z^d + \cdots + a_0}{b_d z^d + \cdots + b_0} \mapsto (a_d : \cdots : a_0 : b_d : \cdots : b_0)$$

PGL$_2$ acts on Hom$_d$ via conjugation: $$\phi^\sigma = \sigma^{-1} \circ \phi \circ \sigma$$

$$M_d := \text{Hom}_d / \text{PGL}_2$$

**Definition.** An algebraic family of dynamical systems $V \subset \text{Hom}_d$ is simple if it is quasi-finite over its image in $M_d$.

**Levin’s Conjecture.** Let $V \subset \text{Hom}_d$ be a simple family defined over a number field $k$, and let $b \in k$ be a basepoint. Then

$$\sup_{v \in V(k)} \# \bigcup_{N \geq 1} \phi_v^{-N}(b)(k) < \infty.$$ 

**Theorem.** (Levin, ’11) $\text{Morton/Silverman Conjecture} + \text{Dynamical Lang Conjecture} \implies \text{Levin’s Conjecture.}$
A Geometric Conjecture

Fix a 1-parameter family of rational functions $\phi_t \in \mathbb{C}(t)(z)$ of generic degree $d \geq 2$. Define a rational map of surfaces:

$$\Phi : \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$$

$$(t, x) \mapsto (t, \phi_t(x))$$

Here $\phi_t$ defines a simple family in $\text{Hom}_d$ if and only if $\Phi$ does not factor as a product $\text{id} \times \psi$ for some rational function $\psi$ defined over $\mathbb{C}$, even after a suitable change of coordinates.
A Geometric Conjecture

Fix a 1-parameter family of rational functions $\phi_t \in \mathbb{C}(t)(z)$ of generic degree $d \geq 2$. Define a rational map of surfaces:

$$\Phi : \mathbb{P}^1 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^1 \times \mathbb{P}^1$$

$$(t, x) \mapsto (t, \phi_t(x))$$

Here $\phi_t$ defines a simple family in $\text{Hom}_d$ if and only if $\Phi$ does not factor as a product $\text{id} \times \psi$ for some rational function $\psi$ defined over $\mathbb{C}$, even after a suitable change of coordinates.

**Conjecture.** (F / Ingram) Let $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ be an irreducible horizontal curve. If $\phi_t$ is a simply family, then for $N$ sufficiently large, the number of irreducible components of $\Phi^{-N}(C)$ is stable and each component has geometric genus at least 2.
A Geometric Conjecture

Fix a 1-parameter family of rational functions \( \phi_t \in \mathbb{C}(t)(z) \) of generic degree \( d \geq 2 \). Define a rational map of surfaces:

\[
\Phi : \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^1 \times \mathbb{P}^1
\]

\[
(t, x) \mapsto (t, \phi_t(x))
\]

Here \( \phi_t \) defines a simple family in \( \text{Hom}_d \) if and only if \( \Phi \) does not factor as a product \( \text{id} \times \psi \) for some rational function \( \psi \) defined over \( \mathbb{C} \), even after a suitable change of coordinates.

**Conjecture.** (F / Ingram) Let \( C \subset \mathbb{P}^1 \times \mathbb{P}^1 \) be an irreducible horizontal curve. If \( \phi_t \) is a simply family, then for \( N \) sufficiently large, the number of irreducible components of \( \Phi^{-N}(C) \) is stable and each component has geometric genus at least 2.

**Theorem.** (F / Ingram, '10) Assume the above conjecture. If \( k \) is a number field, \( \phi_t / k \) is a simple family, and \( b_t \in k(t) \) is a 1-parameter family of basepoints, then

\[
\sup_{t \in k} \# \bigcup_{N \geq 1} \phi_t^{-N}(b_t)(k) < \infty.
\]
The End

All of these papers are available at my web page:
http://www.math.uga.edu/~xander/research.html
All of these papers are available at my web page:
http://www.math.uga.edu/~xander/research.html

Thanks for your attention!