Critical Orbits in Arithmetic Dynamics

Rafe Jones

College of the Holy Cross

March 27, 2009
Let $K$ be a field and $f(x) \in K[x]$. Define $f^n$ to be the $n$th iterate of $f$:

$$f^n := f \circ f \circ \cdots \circ f.$$ 

Orbit of $\alpha \in K$ under $f$:

$$O_f(\alpha) := \{f^n(\alpha) : n = 1, 2, \ldots\}$$

Goal of dynamics: understand the orbits of $f$. 
Let $f \in \mathbb{C}[x]$. Typical goal is to understand topological properties of orbits of $f$.

**Definition**

We say that $f$ is *chaotic* at $x \in \mathbb{C}$ if it exhibits sensitive dependence on initial conditions near $x$: there exists $\epsilon > 0$ such that in all neighborhoods $U$ of $x$ there exists $y \in U$ with

$$|f^n(x) - f^n(y)| > \epsilon.$$ 

for some $n \geq 1$. 


The *Julia set* $J(f)$ is the set where $f$ behaves chaotically.

**Theorem**

Let $f \in \mathbb{C}[x]$ be quadratic, with critical point $\gamma$. Then $J(f)$ is a Cantor set if the critical orbit $O_f(\gamma)$ is unbounded, and $J(f)$ is connected if $O_f(\gamma)$ is bounded.

$f$ is conjugate to $f_c = z^2 + c$, and $\{c : O_{f_c} \text{ is bounded}\} \subset \mathbb{C}$ is called the Mandelbrot set.
The Mandelbrot set
Any quadratic $f \in \mathbb{R}[x]$ is conjugate (over $\mathbb{R}$) to $f_c := x^2 + c$, $c \in \mathbb{R}$.

If $-2 \leq c \leq 1/4$ (i.e. if $c$ belongs to the Mandelbrot set), then $f_c$ maps $[-\beta, \beta]$ to itself, where

$$
\beta = \frac{-1 - \sqrt{1 - 4c}}{2}.
$$
Theorem
Suppose that $f_c$ exhibits exponential expansion along the critical orbit: $|(f_c^n)'(f(0))|$ grows exponentially with $n$. Then $f_c$ is chaotic at almost every $x \in [-\beta, \beta]$.

Note: $|(f_c^n)'(f_c(0))| = |\prod_{i=1}^{n} f_c'(f_c^i(0))|$.

Theorem (Avila-Moreira 2005)
For $c$ belonging to a full-measure subset of $[-2, 1/4]$, the hypotheses of the previous theorem are satisfied.
Let $f(x) \in \mathbb{Z}[x]$ be quadratic.

For $\alpha \in \mathbb{Z}$, let

$$P(O_f(\alpha)) := \{ p \text{ prime} : p | f^n(\alpha) \text{ for at least one } n \geq 1 \}.$$ 

Example: $f = x^2 + 1$, $\alpha = 3$, $O_f(\alpha)) = \{10, 101, 10202, \ldots \}$. 
{2, 5, 101, 5101} $\subset P(O_f(\alpha))$.

For $S$ a set of primes, define its natural upper density $D^+(S)$ to be:

$$D^+(S) := \limsup_{x \to \infty} \frac{\#\{p \leq x : p \in S\}}{\#\{p \leq x\}}$$
Theorem (RJ)

Let $f$ have critical point $\gamma$, and let $v_p$ be the $p$-adic valuation. Suppose that $f^n$ is irreducible for all $n \geq 1$. Furthermore suppose that for infinitely many $n \geq 1$ the following holds:

$$\exists p \neq 2 \text{ with } v_p(f^n(\gamma)) \text{ odd and } v_p(f^m((\gamma))) = 0 \text{ for all } m < n.$$  

Then $D^+(P(O_f(\alpha))) = 0$ for all $\alpha \in \mathbb{Z}$.

Remarks: Loosely, this says that elements of orbits of $f$ do not have many small prime factors. The condition that $f^n$ be irreducible for all $n \geq 1$ holds for generic $f$ and is easy to verify for specific $f$. 
Example: \( f(x) = x^2 + 1 \). All \( f^n \) are irreducible. Critical orbit is 1, 2, 5, 26, 677, \ldots. Stoll (1991) showed for each \( n \geq 3 \) there is an odd \( p \) with \( v_p(f^n(0)) = 1 \) and \( v_p(f^m((0)) = 0 \) for all \( m < n \).

Proof (sketch): Let \( K_n \) be splitting field of \( f^n \) over \( \mathbb{Q} \), and \( G_n = \text{Gal}(K_n/\mathbb{Q}) \).

Using probability theory, can show there exists \( \tau_n \to 0 \) such that for each \( n \), \( D^+(P(O_f(\alpha))) \leq \tau_n \) provided that

\[
G_n \cong G_{n-1} \wr \mathbb{Z}/2\mathbb{Z},
\]

where \( \wr \) denotes the wreath product.
(1) holds provided that there exists \( p \) ramifying in \( K_n \) that does not ramify in \( K_{n-1} \).

Up to squares,

\[ \text{Disc}(f^n) = 2^k f^n(\gamma). \]

Also up to squares,

\[ \text{Disc}(K_n) = \text{Disc}(f^n), \]

so \( v_p(f^n(\gamma)) \) odd implies \( p \mid \text{Disc}(K_n) \), and the theorem follows.
The family $x^2 + c$

Conjugation does not preserve irreducibility and Galois-theoretic properties of polynomials. Example: $x^2$ and $(x + 3)^2 - 3$.

For $f(x) = x^2 + c$, $c \in \mathbb{Z} \setminus \{0, -1, -2\}$, the critical orbit has a property called rigid divisibility:

Let $\beta_n = f^n(0)$. Then for all $m \geq 1$,

1. $\beta_n | \beta_{nm}$ and
2. $v_p(\beta_n) = e > 0 \Rightarrow v_p(\beta_{nm}) = e$.

This property arises because of the lack of a linear term in $f$. 
The family $x^2 + c$, continued

Example: $f = x^2 + 3$.

$\beta_1 = 3$
$\beta_2 = 2^2 \cdot 3$
$\beta_3 = 3 \cdot 7^2$
$\beta_4 = 2^2 \cdot 3 \cdot 1801$
$\beta_5 = 3 \cdot 13 \cdot 3019 \cdot 3967$
$\beta_6 = 2^2 \cdot 3 \cdot 7^2 \cdot 40867 \cdot 9078827347$
$\beta_7 = 3 \cdot 79 \cdot 200822022266672286333740239816831$

Note: when $\ell$ is prime, $\beta_\ell$ is divisible by $\beta_1$, and $\beta_\ell/\beta_1$ is relatively prime to all $\beta_m$ for $m < \ell$. 
The family $x^2 + c$, continued

**Theorem**

Let $f = x^2 + c$, where $c \in \mathbb{Z} \setminus \{0, -1, -2\}$ and $-c$ not a square. Then for any $\alpha \in \mathbb{Z}$,

$$D^+(P(O_f(\alpha))) = 0.$$

Remark: The theorem can be extended to cover all $x^2 + c$ except for $c = -1$. 
Density Results (cont.)

Proof (sketch): Since $-c$ is a square, one can show that $f^n$ is irreducible for all $n$.

If $\beta_\ell/\beta_1 = y_0^2$ for $\ell \geq 3$, the curve $C : \beta_1 y^2 = f^3(x)$ has the integral point $(\beta_{\ell-3}, y_0)$. Since $f^3$ has degree 8 and no repeated roots, $C$ has genus 3, and thus by Siegel’s Theorem only finitely many rational points.
Conjecture

Suppose that $f = x^2 + ax + b \in \mathbb{Z}[x]$ with critical point $\gamma$, and suppose that $O_f(\gamma)$ is infinite and $f^n$ is irreducible for all $n$. Then for any $\alpha \in \mathbb{Z}$,

$$D + (P(O_f(\alpha))) = 0.$$ 

Bad example: $f(x) = (x + 945)^2 - 945 + 3$.

$\beta_1 = 2 \cdot 3 \cdot 157$
$\beta_2 = 3 \cdot 311$
$\beta_3 = 2 \cdot 3 \cdot 7 \cdot 19$
$\beta_4 = 3 \cdot 83^2$
$\beta_5 = 2 \cdot 3 \cdot 103 \cdot 755789$