Arithmetic of critical orbits and recurrence

Holly Krieger

November 10, 2013

Fix:

- E an elliptic curve over $\mathbb{Q}$,
- $\alpha \in E(K)$ a non-torsion point.

Question: For which natural numbers n does there exist a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that after reduction modulo $\mathfrak{p}$, α becomes a point of exact order n?

Fix:

- E an elliptic curve over $\mathbb{Q}$,
- $\alpha \in E(K)$ a non-torsion point.

Question: For which natural numbers n does there exist a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that after reduction modulo $\mathfrak{p}$, α becomes a point of exact order n?

Exact order: $[n]\alpha \equiv \mathcal{O} \mod \mathfrak{p}$, $[k]\alpha \not\equiv \mathcal{O} \mod \mathfrak{p}$ for all $k < n$.

In coordinates: if E is in Weierstrass form, $[n]\alpha$ coincides with $\mathcal{O}$ if and only if $\mathfrak{p}$ divides the denominator of $x([n]\alpha)$.

Alternative notation

Definition (Primitive prime divisor)

Let $\{a_n\}$ be a sequence of ideals in $\mathcal{O}_K$. We say a prime ideal p of $\mathcal{O}_K$ is a *primitive prime divisor* of a_n if

- $p \mid a_n$
- $\forall 1 \leq k < n, p \nmid a_k$

Alternative notation

Definition (Primitive prime divisor)

Let $\{a_n\}$ be a sequence of ideals in $\mathcal{O}_K$. We say a prime ideal p of $\mathcal{O}_K$ is a *primitive prime divisor* of a_n if

- $p \mid a_n$
- $\forall 1 \leq k < n, p \nmid a_k$

Definition (Zsigmondy set)

The *Zsigmondy set* of $\{a_n\}$ is

$$\mathcal{Z}_{\{a_n\}} := \{n \in \mathbb{N} : a_n \text{ has no primitive prime divisor}\}$$

Alternative notation

Definition (Primitive prime divisor)

Let $\{a_n\}$ be a sequence of ideals in $\mathcal{O}_K$. We say a prime ideal p of $\mathcal{O}_K$ is a *primitive prime divisor* of a_n if

- $p \mid a_n$
- $\forall 1 \leq k < n, p \nmid a_k$

Definition (Zsigmondy set)

The *Zsigmondy set* of $\{a_n\}$ is

$$\mathcal{Z}_{\{a_n\}} := \{n \in \mathbb{N} : a_n \text{ has no primitive prime divisor}\}$$

Theorem (Silverman)

The Zsigmondy set associated to the sequence of denominators of $x([n]\alpha)$ is finite.

Reduction mod p

Corollary

For all but finitely many n, there exists a prime p of $\mathcal{O}_K$ such that after reduction mod p, α has exact order n.

Reduction mod p

Corollary

For all but finitely many n, there exists a prime p of $\mathcal{O}_K$ such that after reduction mod p, α has exact order n.

More examples of sequences with finite Zsigmondy sets:

1. Bang-Zsigmondy sequences $a^n - b^n$, $a > b > 0$ coprime with $\frac{a}{b}$ not a root of unity. (Bang, Zsigmondy)
2. Fibonacci sequence (Carmichael) and its generalizations
3. CM elliptic divisibility sequences

Reduction mod p

Corollary

For all but finitely many n, there exists a prime p of $\mathcal{O}_K$ such that after reduction mod p, α has exact order n.

More examples of sequences with finite Zsigmondy sets:

1. Bang-Zsigmondy sequences $a^n - b^n$, $a > b > 0$ coprime with $\frac{a}{b}$ not a root of unity. (Bang, Zsigmondy)
2. Fibonacci sequence (Carmichael) and its generalizations
3. CM elliptic divisibility sequences

a_n	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}
$2^n - 1$	1	3	7	$3 \cdot 5$	31	$3^2 \cdot 7$	127	$3 \cdot 5 \cdot 17$	$7 \cdot 73$	$3 \cdot 11 \cdot 31$	$23 \cdot 89$	$3^2 \cdot 5 \cdot 7 \cdot 13$
F_n	1	1	2	3	5	2^3	13	$3 \cdot 7$	$2 \cdot 17$	$5 \cdot 11$	89	$2^4 \cdot 3^2$
w_n	1	1	1	-1	-2	-3	-1	7	11	$2^2 \cdot 5$	-19	$3 \cdot -29$

These are all examples of *strong divisibility sequences*:

$$\gcd(a_m, a_n) = a_{\gcd(m,n)}.$$

Reduction mod p

Corollary

For all but finitely many n, there exists a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that after reduction mod $\mathfrak{p}$, α has exact order n.

More examples of sequences with finite Zsigmondy sets:

1. Bang-Zsigmondy sequences $a^n - b^n$, $a > b > 0$ coprime with $\frac{a}{b}$ not a root of unity. (Bang, Zsigmondy)
2. Fibonacci sequence (Carmichael) and its generalizations
3. CM elliptic divisibility sequences

a_n	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}
$2^n - 1$	1	3	7	$3 \cdot 5$	31	$3^2 \cdot 7$	127	$3 \cdot 5 \cdot 17$	$7 \cdot 73$	$3 \cdot 11 \cdot 31$	$23 \cdot 89$	$3^2 \cdot 5 \cdot 7 \cdot 13$
F_n	1	1	2	3	5	2^3	13	$3 \cdot 7$	$2 \cdot 17$	$5 \cdot 11$	89	$2^4 \cdot 3^2$
w_n	1	1	1	-1	-2	-3	-1	7	11	$2^2 \cdot 5$	-19	$3 \cdot -29$

These are all examples of *strong divisibility sequences*:

$$\gcd(a_m, a_n) = a_{\gcd(m,n)}.$$

Key idea: Strong divisibility + rapid growth $\Rightarrow$ finite Zsigmondy set.

Coinciding with periodic points

Dynamical analogue of this elliptic curve example? The identity is fixed point.

Let $f(z) = z^d, d \geq 2$, K a number field. Let $\alpha \in K$ be a point with infinite forward f-orbit, and $\zeta \in \bar{\mathbb{Q}}$ a non-zero f-periodic point.

Coinciding with periodic points

Dynamical analogue of this elliptic curve example? The identity is fixed point.

Let $f(z) = z^d, d \geq 2$, K a number field. Let $\alpha \in K$ be a point with infinite forward f-orbit, and $\zeta \in \bar{\mathbb{Q}}$ a non-zero f-periodic point.

Theorem (Bang, Zsigmondy, Schinzel 1974)

The sequence $\{(\alpha)^n - \zeta\}$ has finite, effectively computable Zsigmondy set.

Coinciding with periodic points

Dynamical analogue of this elliptic curve example? The identity is fixed point.

Let $f(z) = z^d, d \geq 2$, K a number field. Let $\alpha \in K$ be a point with infinite forward f-orbit, and $\zeta \in \bar{\mathbb{Q}}$ a non-zero f-periodic point.

Theorem (Bang, Zsigmondy, Schinzel 1974)

The sequence $\{(\alpha)^n - \zeta\}$ has finite, effectively computable Zsigmondy set.

This generalizes broadly:

Theorem (Ingram-Silverman 2007)

Let $\phi(z) \in \mathbb{Q}(z)$ with degree $d \geq 2$, $\alpha \in \mathbb{Q}$ a point with infinite forward orbit, and $\gamma \in \mathbb{Q}$ periodic for ϕ. Assume that γ is not totally ramified. Then the numerator sequence associated to $\{\phi^n(\alpha) - \gamma\}$ has finite Zsigmondy set.

Reducing to period n

Broad idea in arithmetic dynamics: torsion points on elliptic curves and preperiodic points of dynamical systems have similar properties.

So given $f(z) \in K(z)$ and $\alpha \in K$ with infinite forward orbit, we ask: for which $n \in \mathbb{N}$ does there exist a prime p of $\mathcal{O}_K$ such that α has exact *period* n after reduction mod p?

Reducing to period n

Broad idea in arithmetic dynamics: torsion points on elliptic curves and preperiodic points of dynamical systems have similar properties.

So given $f(z) \in K(z)$ and $\alpha \in K$ with infinite forward orbit, we ask: for which $n \in \mathbb{N}$ does there exist a prime p of $\mathcal{O}_K$ such that α has exact *period* n after reduction mod p?

New question: Let $f(z) \in K(z)$ and $\alpha \in K$ with infinite forward orbit. Is the Zsigmondy set of (the numerator sequence of) $\{f^n(\alpha) - \alpha\}$ finite?

Reducing to period n

Broad idea in arithmetic dynamics: torsion points on elliptic curves and preperiodic points of dynamical systems have similar properties.

So given $f(z) \in K(z)$ and $\alpha \in K$ with infinite forward orbit, we ask: for which $n \in \mathbb{N}$ does there exist a prime p of $\mathcal{O}_K$ such that α has exact *period n* after reduction mod p?

New question: Let $f(z) \in K(z)$ and $\alpha \in K$ with infinite forward orbit. Is the Zsigmondy set of (the numerator sequence of) $\{f^n(\alpha) - \alpha\}$ finite?

Big problem: These are not necessarily divisibility sequences!

Reducing to period n

Broad idea in arithmetic dynamics: torsion points on elliptic curves and preperiodic points of dynamical systems have similar properties.

So given $f(z) \in K(z)$ and $\alpha \in K$ with infinite forward orbit, we ask: for which $n \in \mathbb{N}$ does there exist a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that α has exact *period n* after reduction mod $\mathfrak{p}$?

New question: Let $f(z) \in K(z)$ and $\alpha \in K$ with infinite forward orbit. Is the Zsigmondy set of (the numerator sequence of) $\{f^n(\alpha) - \alpha\}$ finite?

Big problem: These are not necessarily divisibility sequences!

unless... we consider the *critical* orbits of polynomials.

Theorem (K.)

Let $f(z) \in K[z]$ and α a critical point with infinite forward orbit. Then the Zsigmondy set of $\{f^n(\alpha) - \alpha\}$ is finite.

Theorem (K.)

Let $f(z) \in K[z]$ and α a critical point with infinite forward orbit. Then the Zsigmondy set of $\{f^n(\alpha) - \alpha\}$ is finite.

Bad news: ineffective (uses a version of Roth's theorem).

Theorem (K.)

Let $f(z) \in K[z]$ and α a critical point with infinite forward orbit. Then the Zsigmondy set of $\{f^n(\alpha) - \alpha\}$ is finite.

Bad news: ineffective (uses a version of Roth's theorem).

Theorem (K.)

Let $f(z) = z^d + c, c \in \mathbb{Q}$. Then the Zsigmondy set of $\{f^n(0)\}$ has at most 8 elements, and there is an effectively computable bound depending on c on the maximal element.

A computational question

Fix d, n. Does there exist $c \in \mathbb{Q}$ such that $f(z) = z^d + c$ has n in the Zsigmondy set of the critical orbit?

A computational question

Fix d, n. Does there exist $c \in \mathbb{Q}$ such that $f(z) = z^d + c$ has n in the Zsigmondy set of the critical orbit?

Reduces to existence of integer points on a finite number of Thue curves:
$(d, n) = (d, 2) : x + y = \pm 1$ (not really Thue)
$(d, n) = (2, 3) : x^3 + 2x^2y + xy^2 + y^3 = \pm 1$
$(d, n) = (4, 3) : x^3(x^3 + y^3)^4 + y^{15} = \pm 1$
etc.

A computational question

Fix d, n. Does there exist $c \in \mathbb{Q}$ such that $f(z) = z^d + c$ has n in the Zsigmondy set of the critical orbit?

Reduces to existence of integer points on a finite number of Thue curves:
$(d, n) = (d, 2) : x + y = \pm 1$ (not really Thue)
$(d, n) = (2, 3) : x^3 + 2x^2y + xy^2 + y^3 = \pm 1$
$(d, n) = (4, 3) : x^3(x^3 + y^3)^4 + y^{15} = \pm 1$
etc.

For $d \leq 10$, $n \leq 4$: Sage can solve this in reasonable time, calling thue.init from PARI/GP. This is pretty weak.

A computational question

Fix d, n. Does there exist $c \in \mathbb{Q}$ such that $f(z) = z^d + c$ has n in the Zsigmondy set of the critical orbit?

Reduces to existence of integer points on a finite number of Thue curves:
$(d, n) = (d, 2) : x + y = \pm 1$ (not really Thue)
$(d, n) = (2, 3) : x^3 + 2x^2 y + xy^2 + y^3 = \pm 1$
$(d, n) = (4, 3) : x^3(x^3 + y^3)^4 + y^{15} = \pm 1$
etc.

For $d \leq 10$, $n \leq 4$: Sage can solve this in reasonable time, calling thue.init from PARI/GP. This is pretty weak.

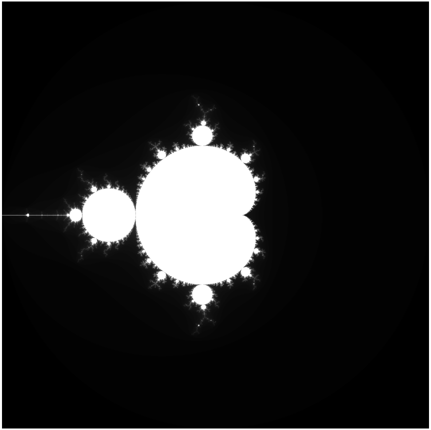
Remark: $f(z) = z^2 - \frac{7}{4}$

Critical recurrence

What's the deal with $c = -\frac{7}{4}$?

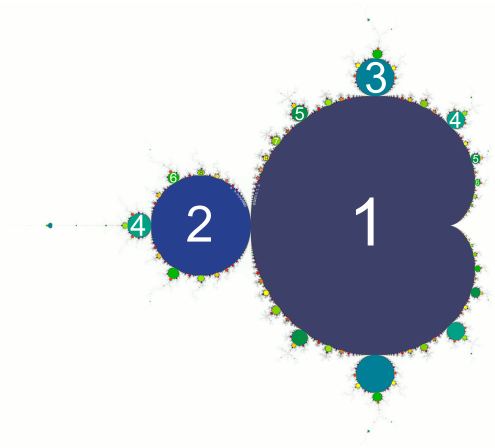
Critical recurrence

What's the deal with $c = -\frac{7}{4}$?



Better results through complex dynamics

Consider the case of $d = 2$. The *hyperbolic components* of the Mandelbrot set are the loci where the critical orbit is in the basin of attraction of some attracting periodic cycle of fixed period n.



On the boundary of the Mandelbrot set

Let $\rho_n := \min\left\{\frac{1}{4}, \frac{1}{2^{2^{n-2}}}\right\}$. Define $D(n)$ to be the set of complex parameters c such that 0 lies in the basin of attraction of a point of period n with multiplier less than ρ_n.

On the boundary of the Mandelbrot set

Let $\rho_n := \min\left\{\frac{1}{4}, \frac{1}{2^{2^{n-2}}}\right\}$. Define $D(n)$ to be the set of complex parameters c such that 0 lies in the basin of attraction of a point of period n with multiplier less than ρ_n.

Theorem

Let $f(z) = z^2 + c$, and suppose $\forall n \in \mathbb{N}, c \notin D(n)$. Then $\mathcal{Z}_f \subset \{1, 2, 3\}$.

On the boundary of the Mandelbrot set

Let $\rho_n := \min\{\frac{1}{4}, \frac{1}{2^{2^{n-2}}}\}$. Define $D(n)$ to be the set of complex parameters c such that 0 lies in the basin of attraction of a point of period n with multiplier less than ρ_n.

Theorem

Let $f(z) = z^2 + c$, and suppose $\forall n \in \mathbb{N}, c \notin D(n)$. Then $\mathcal{Z}_f \subset \{1, 2, 3\}$.

Note:

- This is the best possible bound, as expected!
- This tells us where to look for possible higher values of n in Zsigmondy sets: when c is a good rational approximation of a center of a hyperbolic component.

On the boundary of the Mandelbrot set

Let $\rho_n := \min\{\frac{1}{4}, \frac{1}{2^{2^{n-2}}}\}$. Define $D(n)$ to be the set of complex parameters c such that 0 lies in the basin of attraction of a point of period n with multiplier less than ρ_n.

Theorem

Let $f(z) = z^2 + c$, and suppose $\forall n \in \mathbb{N}, c \notin D(n)$. Then $\mathcal{Z}_f \subset \{1, 2, 3\}$.

Note:

- This is the best possible bound, as expected!
- This tells us where to look for possible higher values of n in Zsigmondy sets: when c is a good rational approximation of a center of a hyperbolic component.

Break: explain this! White board time.

$\mathcal{Z}_f \subset \{1, 2, 3\}$ for all $c \in \mathbb{Q}$?

Checking rational approximations of centers of hyperbolic components?

$\mathcal{Z}_f \subset \{1, 2, 3\}$ for all $c \in \mathbb{Q}$?

Checking rational approximations of centers of hyperbolic components?

For $n \leq 8$, the first 22 convergents of the real centers of hyperbolic components with attracting cycles of period n all have $\mathcal{Z}_f \subset \{1, 2\}$, except for $c = -\frac{7}{4}$, with $3 \in \mathcal{Z}_f$.

$\mathcal{Z}_f \subset \{1, 2, 3\}$ for all $c \in \mathbb{Q}$?

Checking rational approximations of centers of hyperbolic components?

For $n \leq 8$, the first 22 convergents of the real centers of hyperbolic components with attracting cycles of period n all have $\mathcal{Z}_f \subset \{1, 2\}$, except for $c = -\frac{7}{4}$, with $3 \in \mathcal{Z}_f$.

Better convergents seem to do worse:

Example: convergents of the center of the $n = 4$ hyperbolic component closest to -2.

c	$\frac{-31}{16}$	$\frac{-33}{17}$	$\frac{-295}{152}$	$\frac{1213}{625}$	$\frac{14851}{7652}$	$\frac{16064}{8277}$	$\frac{1428483}{736028}$	$\frac{5729996}{2952389}$
D	19	19	33	43	27	58	...?	...?

Here D is the number of digits of the largest primitive prime factor!

Existence of powers in orbits

Question: Fix $f(z) \in K(z)$ and $\alpha \in K$ a point of infinite forward orbit. What can we say about the set of indices n which have $f^n(z) - z = y^m$ for some $y \in K$, $m > 1$?

Existence of powers in orbits

Question: Fix $f(z) \in K(z)$ and $\alpha \in K$ a point of infinite forward orbit. What can we say about the set of indices n which have $f^n(z) - z = y^m$ for some $y \in K$, $m > 1$?

Not always finite, obviously (e.g. $f(z) = g(z)^2, \alpha = 0$).

Conjecture The set $\{n \in \mathbb{N} : f^n(z) - z = y^m, y \in K, m \geq 2\}$ consists of a finite union of singletons and arithmetic progressions.

Existence of powers in orbits

Question: Fix $f(z) \in K(z)$ and $\alpha \in K$ a point of infinite forward orbit. What can we say about the set of indices n which have $f^n(z) - z = y^m$ for some $y \in K$, $m > 1$?

Not always finite, obviously (e.g. $f(z) = g(z)^2, \alpha = 0$).

Conjecture The set $\{n \in \mathbb{N} : f^n(z) - z = y^m, y \in K, m \geq 2\}$ consists of a finite union of singletons and arithmetic progressions.

Faltings' theorem says it suffices to bound m.

Diophantine results for polynomials

Theorem (Schinzel, Tijdeman)

Let $f(z) \in \mathbb{Q}[z]$. There exists an effectively computable bound M such that for $m \geq M$,

$$f(x) = y^m$$

has no solutions for $x, y \in \mathbb{Z}$ with $y \neq 0, \pm 1$.

Diophantine results for polynomials

Theorem (Schinzel, Tijdeman)

Let $f(z) \in \mathbb{Q}[z]$. There exists an effectively computable bound M such that for $m \geq M$,

$$f(x) = y^m$$

has no solutions for $x, y \in \mathbb{Z}$ with $y \neq 0, \pm 1$.

This can be easily extended to S-integers in a number field, so long as y is not a root of unity. S-units in orbits are finite, so this is ok, and with some work we get:

Corollary

The conjecture holds for polynomials.

Connection to recurrence

Again, if we restrict to critical orbits (of polynomials), there is a dynamical interpretation:

Connection to recurrence

Again, if we restrict to critical orbits (of polynomials), there is a dynamical interpretation:

Away from primes of bad reduction or primes less than the degree, if p is a prime divisor of $f^n(0) = y^m$, then there exists a point of small norm in $\mathbb{C}_p$ which is p-adically attracting of small multiplier norm.

Why? Break: white board time!

Connection to recurrence

Again, if we restrict to critical orbits (of polynomials), there is a dynamical interpretation:

Away from primes of bad reduction or primes less than the degree, if p is a prime divisor of $f^n(0) = y^m$, then there exists a point of small norm in $\mathbb{C}_p$ which is p-adically attracting of small multiplier norm.

Why? Break: white board time!
So we can ask the stronger question: is the set of exponents m such that $p^m | f^n(z) - z$ for some n a bounded set?

Connection to recurrence

Again, if we restrict to critical orbits (of polynomials), there is a dynamical interpretation:

Away from primes of bad reduction or primes less than the degree, if p is a prime divisor of $f^n(0) = y^m$, then there exists a point of small norm in $\mathbb{C}_p$ which is p-adically attracting of small multiplier norm.

Why? Break: white board time!
So we can ask the stronger question: is the set of exponents m such that $p^m | f^n(z) - z$ for some n a bounded set?

Theorem (Benedetto-Ingram-Jones-Levy)

If f is a rational PCF map, the answer is yes, away from a finite set of primes.

The moral of the conjecture

BIJL doesn't help us with the question of powers in critical orbits; why do we expect the stronger question to be true generally?

To finish: the moral, with $f(z) = z^2 + c$. White board time!

The moral of the conjecture

BIJL doesn't help us with the question of powers in critical orbits; why do we expect the stronger question to be true generally?

To finish: the moral, with $f(z) = z^2 + c$. White board time!

Thanks!