Reduction of Dynatomic Curves

Simon Rubinstein-Salzedo
simon@eulercircle.com
Euler Circle

Joint with John Doyle, Holly Krieger, Andrew Obus, Rachel Pries, and Lloyd West

December 19, 2016

Dynamical system

- X: a set
- $f : X \to X$.

Dynamical system

- X: a set
- $f : X \to X$.

Study orbits $x, f(x), f(f(x)), f(f(f(x))), \ldots$

Dynamical system

- X: a set
- $f : X \to X$.

Study orbits $x, f(x), f(f(x)), f(f(f(x))), \ldots$

When are these orbits finite? If so, x is said to be a preperiodic point. It is periodic if some $f^n(x) = x$.

Dynamical system

- X: a set
- $f : X \to X$.

Study orbits $x, f(x), f(f(x)), f(f(f(x))), \ldots$

When are these orbits finite? If so, x is said to be a preperiodic point. It is periodic if some $f^n(x) = x$.

Arithmetic dynamics: $X = \mathbb{P}^1(\mathbb{Q})$ (or similar), $f \in \mathbb{Q}(z)$.

Arithmetic dynamics and elliptic curves

Standard goal in arithmetic dynamics: convert standard theorems on elliptic curves to (very hard) conjectures about dynamical systems

Arithmetic dynamics and elliptic curves

Standard goal in arithmetic dynamics: convert standard theorems on elliptic curves to (very hard) conjectures about dynamical systems

Torsion point on elliptic curve $\rightsquigarrow$ (pre)periodic point of dynamical system

Arithmetic dynamics and elliptic curves

Standard goal in arithmetic dynamics: convert standard theorems on elliptic curves to (very hard) conjectures about dynamical systems

Torsion point on elliptic curve $\rightsquigarrow$ (pre)periodic point of dynamical system

Typical example: Compare

Theorem (Mazur)

$|E(\mathbb{Q})_{\text{tors}}| \leq 16.$

Arithmetic dynamics and elliptic curves

Standard goal in arithmetic dynamics: convert standard theorems on elliptic curves to (very hard) conjectures about dynamical systems

Torsion point on elliptic curve $\rightsquigarrow$ (pre)periodic point of dynamical system

Typical example: Compare

Theorem (Mazur)

$|E(\mathbb{Q})_{\text{tors}}| \leq 16.$

Conjecture (Uniform Boundedness Conjecture)

There is a constant $C(d)$ so that if f is any degree-d rational function, then $|\operatorname{PrePer}_f(\mathbb{Q})| \leq C(d)$.

Elliptic modular curves

$Y_1^{\mathrm{ell}}(n)$: parametrizes pairs (E, P): E an elliptic curve, $P \in E[n]$

$Y_0^{\mathrm{ell}}(n)$: parametrizes elliptic curves together with cyclic isogenies of degree n

Elliptic modular curves

$Y_1^{\text{ell}}(n)$: parametrizes pairs (E, P): E an elliptic curve, $P \in E[n]$

$Y_0^{\text{ell}}(n)$: parametrizes elliptic curves together with cyclic isogenies of degree n

What is a dynamical analogue?

Iteration of quadratic polynomials

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

$f_c^n(x) = f_c(f_c(\cdots(f_c(x))\cdots))$, n times

$x \in \mathbb{C}$ is *n-periodic* if $f_c^n(x) = x$, or $f_c^n(x) - x = 0$.

n-periodic points

If x is d-periodic and $d \mid n$, then x is also n-periodic.

n-periodic points

If x is d-periodic and $d \mid n$, then x is also n-periodic.

Consequence: $f_c^n(x) - x$ is reducible: $(f_c^d(x) - x) \mid (f_c^n(x) - x)$.

n-periodic points

If x is d-periodic and $d \mid n$, then x is also n-periodic.

Consequence: $f_c^n(x) - x$ is reducible: $(f_c^d(x) - x) \mid (f_c^n(x) - x)$.

Makes sense to filter out the points that are n-periodic but not d-periodic for d a proper divisor of n.

Dynatomic polynomials

$f_c^n(x) - x$: polynomial in x *and* polynomial in $c \rightsquigarrow$ polynomial in both variables.

Dynatomic polynomials

$f_c^n(x) - x$: polynomial in x *and* polynomial in $c \rightsquigarrow$ polynomial in both variables.

$\Phi_n(x, c) = f_c^n(x) - x$

Dynatomic polynomials

$f_c^n(x) - x$: polynomial in x *and* polynomial in $c \rightsquigarrow$ polynomial in both variables.

$\Phi_n(x,c) = f_c^n(x) - x$

Filter out points of exact period n: $\Phi_n(x,c) = \prod_{d|n} \Psi_n(x,c)$

Dynatomic polynomials

$f_c^n(x) - x$: polynomial in x *and* polynomial in $c \rightsquigarrow$ polynomial in both variables.

$\Phi_n(x,c) = f_c^n(x) - x$

Filter out points of exact period n: $\Phi_n(x,c) = \prod_{d|n} \Psi_n(x,c)$

Möbius inversion: $\Psi_n(x,c) = \prod_{d|n} \Phi_n(x,c)^{\mu(n/d)}$

Dynatomic polynomials

$f_c^n(x) - x$: polynomial in x *and* polynomial in c $\rightsquigarrow$ polynomial in both variables.

$\Phi_n(x, c) = f_c^n(x) - x$

Filter out points of exact period n: $\Phi_n(x, c) = \prod_{d|n} \Psi_n(x, c)$

Möbius inversion: $\Psi_n(x, c) = \prod_{d|n} \Phi_n(x, c)^{\mu(n/d)}$

Definition

$\Psi_n(x, c)$ is the n^{th} dynatomic polynomial

Dynatomic and cyclotomic polynomials

Dynatomic = dynamical + cyclotomic

Dynatomic polynomials are analogous to cyclotomic polynomials:

Dynatomic and cyclotomic polynomials

Dynatomic = dynamical + cyclotomic

Dynatomic polynomials are analogous to cyclotomic polynomials:

$c = 0$: $\Psi_n(x, 0)$ is a product of cyclotomic polynomials:

$$\Psi_n(x, 0) = \prod_{d|n} (x^{2^d} - x)^{\mu(n/d)}.$$

Compare with cyclotomic polynomials:

$$C_n(x) = \prod_{d|n} (x^d - x)^{\mu(n/d)}.$$

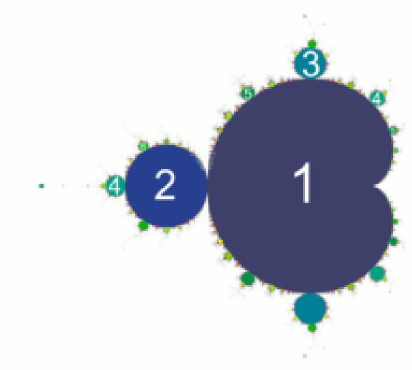
Multiple roots

Idea: solutions to $\Psi_n(x, c) = 0$ "should be" pairs (x, c) so that x has *exact* period n for $f_c(x)$.

Not quite true: there are points (x, c) where the period of x is a proper divisor of $f_c(x)$, when $f_c^n(x) - x$ has double (or higher) roots at x.

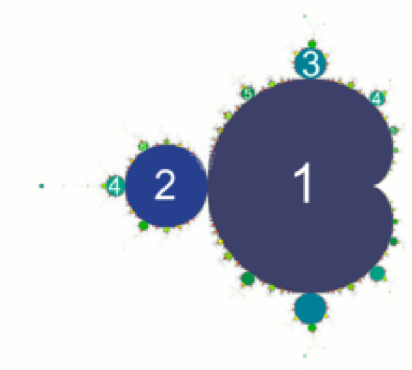
Formal period

This happens at the bifurcation points and cusps of the Mandelbrot set



Formal period

This happens at the bifurcation points and cusps of the Mandelbrot set



Definition

If $\Psi_n(x, c) = 0$, then we say that x has *formal period* n for $f_c(x)$.

Dynatomic curves

$Y_1(n) = \{(x, c) \in \mathbb{C}^2 : \Psi_n(x, c) = 0\}$: affine curve in $\mathbb{C}^2$

Dynatomic curves

$Y_1(n) = \{(x, c) \in \mathbb{C}^2 : \Psi_n(x, c) = 0\}$: affine curve in $\mathbb{C}^2$

Action of $(\mathbb{Z}/n\mathbb{Z})$ on $Y_1(n)$: $(1 \in \mathbb{Z}/n\mathbb{Z}) \cdot (x, c) = (f_c(x), c) \in Y_1(n)$

Dynatomic curves

$Y_1(n) = \{(x, c) \in \mathbb{C}^2 : \Psi_n(x, c) = 0\}$: affine curve in $\mathbb{C}^2$

Action of $(\mathbb{Z}/n\mathbb{Z})$ on $Y_1(n)$: $(1 \in \mathbb{Z}/n\mathbb{Z}) \cdot (x, c) = (f_c(x), c) \in Y_1(n)$

$Y_0(n) = Y_1(n)/(\mathbb{Z}/n\mathbb{Z})$, also an affine curve: $Y_1(n) \to Y_0(n)$ is a Galois cover with Galois group $\mathbb{Z}/n\mathbb{Z}$

Dynatomic curves

$Y_1(n) = \{(x,c) \in \mathbb{C}^2 : \Psi_n(x,c) = 0\}$: affine curve in $\mathbb{C}^2$

Action of $(\mathbb{Z}/n\mathbb{Z})$ on $Y_1(n)$: $(1 \in \mathbb{Z}/n\mathbb{Z}) \cdot (x,c) = (f_c(x), c) \in Y_1(n)$

$Y_0(n) = Y_1(n)/(\mathbb{Z}/n\mathbb{Z})$, also an affine curve: $Y_1(n) \to Y_0(n)$ is a Galois cover with Galois group $\mathbb{Z}/n\mathbb{Z}$

$X_1(n), X_0(n)$: (normalization of) projective closures of $Y_1(n)$, $Y_0(n)$: curves in projective space

Dynatomic curves

$Y_1(n) = \{(x, c) \in \mathbb{C}^2 : \Psi_n(x, c) = 0\}$: affine curve in $\mathbb{C}^2$

Action of $(\mathbb{Z}/n\mathbb{Z})$ on $Y_1(n)$: $(1 \in \mathbb{Z}/n\mathbb{Z}) \cdot (x, c) = (f_c(x), c) \in Y_1(n)$

$Y_0(n) = Y_1(n)/(\mathbb{Z}/n\mathbb{Z})$, also an affine curve: $Y_1(n) \to Y_0(n)$ is a Galois cover with Galois group $\mathbb{Z}/n\mathbb{Z}$

$X_1(n), X_0(n)$: (normalization of) projective closures of $Y_1(n)$, $Y_0(n)$: curves in projective space

Theorem (Buff, Lei)

All these dynatomic curves (X_0, X_1, Y_0, Y_1) are smooth and irreducible

Monodromy

- Branch points of $X_0(n) \to \mathbb{P}^1$ are some of the cusps of the Mandelbrot set.
- Branch points of $X_1(n) \to \mathbb{P}^1$ are some of the cusps and bifurcation points of the Mandelbrot set.

Monodromy

- Branch points of $X_0(n) \to \mathbb{P}^1$ are some of the cusps of the Mandelbrot set.
- Branch points of $X_1(n) \to \mathbb{P}^1$ are some of the cusps and bifurcation points of the Mandelbrot set.

Fact: for $X_0(n) \to \mathbb{P}^1$, monodromy around each branch point is a transposition.

Reduction

$\Psi_n(x, c) \in \mathbb{Z}[x, c]$. So is the defining polynomial for $X_0(n)$.

Reduction

$\Psi_n(x,c) \in \mathbb{Z}[x,c]$. So is the defining polynomial for $X_0(n)$.

Given $h(x,c) \in \mathbb{Z}[x,c]$: can reduce modulo p to obtain a curve over $\mathbb{F}_p$.

Reduction

$\Psi_n(x, c) \in \mathbb{Z}[x, c]$. So is the defining polynomial for $X_0(n)$.

Given $h(x, c) \in \mathbb{Z}[x, c]$: can reduce modulo p to obtain a curve over $\mathbb{F}_p$.

What can we say about its reduction? Good reduction: genus of curve in characteristic p = genus of curve in characteristic 0.

Bad reduction

Elliptic curve case: $X_0^{\text{ell}}(n)$ has bad reduction at a prime $p \iff p \mid n$.

Bad reduction

Elliptic curve case: $X_0^{\mathrm{ell}}(n)$ has bad reduction at a prime $p \iff p \mid n$.

Dynatomic case: more complicated!

Bad reduction

Elliptic curve case: $X_0^{\text{ell}}(n)$ has bad reduction at a prime $p \iff p \mid n$.

Dynatomic case: more complicated!

Example

$X_0(5)$ has bad reduction at p iff $p = 2$ or 3701.

X_0 versus X_1

How does reduction of $X_0(n)$ compare to reduction of $X_1(n)$?

X_0 versus X_1

How does reduction of $X_0(n)$ compare to reduction of $X_1(n)$?

X_0 has bad reduction at $p \Rightarrow X_1$ has bad reduction at p.

X_0 versus X_1

How does reduction of $X_0(n)$ compare to reduction of $X_1(n)$?

X_0 has bad reduction at $p \Rightarrow X_1$ has bad reduction at p.

Theorem

If n and p are distinct odd primes, then $X_0(n)$ has bad reduction at $p \iff X_1(n)$ has bad reduction at p.

X_0 versus X_1

How does reduction of $X_0(n)$ compare to reduction of $X_1(n)$?

X_0 has bad reduction at $p \Rightarrow X_1$ has bad reduction at p.

Theorem

If n and p are distinct odd primes, then $X_0(n)$ has bad reduction at $p \iff X_1(n)$ has bad reduction at p.

False if n is composite: $X_0(6)$ has good reduction at 67, whereas $X_1(6)$ has bad reduction at 67.

Discriminants and related objects

Want to construct discriminant-like object that measures (potential) bad reduction for $X_0(n)$.

Discriminants and related objects

Want to construct discriminant-like object that measures (potential) bad reduction for $X_0(n)$.

Definition

(Up to a factor of a unit)

$$\Delta_{n,n}^{n} = \prod_{\alpha,\beta} (\alpha - \beta),$$

where α and β have formal period n for $f_c(x)$ that lie in different orbits.

Discriminants and related objects

Want to construct discriminant-like object that measures (potential) bad reduction for $X_0(n)$.

Definition

(Up to a factor of a unit)

$$\Delta_{n,n}^{n} = \prod_{\alpha,\beta}(\alpha - \beta),$$

where α and β have formal period n for $f_c(x)$ that lie in different orbits.

$\Delta_{n,n} \in \mathbb{Z}[c]$. Roots of $\Delta_{n,n}$: two orbits of formal period n collide, i.e. certain cusps of the Mandelbrot set, which are also branch points of $X_0(n) \to \mathbb{P}^1$.

Discriminant of $\Delta_{n,n}$

$\mathrm{Disc}(\Delta_{n,n})$ tells us about bad reduction of $X_0(n)$.

Discriminant of $\Delta_{n,n}$

$\mathrm{Disc}(\Delta_{n,n})$ tells us about bad reduction of $X_0(n)$.

Theorem

If $X_0(n)$ has bad reduction at p, then $p \mid \mathrm{Disc}(\Delta_{n,n})$.

Discriminant of $\Delta_{n,n}$

$\mathrm{Disc}(\Delta_{n,n})$ tells us about bad reduction of $X_0(n)$.

Theorem

If $X_0(n)$ has bad reduction at p, then $p \mid \mathrm{Disc}(\Delta_{n,n})$.

However, many primes dividing $\mathrm{Disc}(\Delta_{n,n})$ still have good reduction.

Bad reduction and Disc($\Delta_{n,n}$)

$\mathrm{Disc}(\Delta_{5,5}) = 2^{274} \cdot 3^{12} \cdot 31^{27} \cdot 3701^{1} \cdot 4217^{3}$

Bad reduction and Disc($\Delta_{n,n}$)

$\mathrm{Disc}(\Delta_{5,5}) = 2^{274} \cdot 3^{12} \cdot 31^{27} \cdot 3701^{1} \cdot 4217^{3}$

$\mathrm{Disc}(\Delta_{6,6}) =$
$2^{956} \cdot 3^{91} \cdot 5^{25} \cdot 7^{66} \cdot 13^{8} \cdot 29^{3} \cdot 61^{2} \cdot 8029187^{1} \cdot 55218797^{2} \cdot 4754857884301186 7^{2}$

Bad reduction and Disc($\Delta_{n,n}$)

$\mathrm{Disc}(\Delta_{5,5}) = 2^{274} \cdot 3^{12} \cdot 31^{27} \cdot 3701^{1} \cdot 4217^{3}$

$\mathrm{Disc}(\Delta_{6,6}) =$
$2^{956} \cdot 3^{91} \cdot 5^{25} \cdot 7^{66} \cdot 13^{8} \cdot 29^{3} \cdot 61^{2} \cdot 8029187^{1} \cdot 55218797^{2} \cdot 4754857884301186 7^{2}$

Theorem

If $v_p(\mathrm{Disc}(\Delta_{n,n})) = 1$, then $X_0(n)$ has bad reduction at p.

Bad reduction and $\mathrm{Disc}(\Delta_{n,n})$

$\mathrm{Disc}(\Delta_{5,5}) = 2^{274} \cdot 3^{12} \cdot 31^{27} \cdot 3701^{1} \cdot 4217^{3}$

$\mathrm{Disc}(\Delta_{6,6}) =$
$2^{956} \cdot 3^{91} \cdot 5^{25} \cdot 7^{66} \cdot 13^{8} \cdot 29^{3} \cdot 61^{2} \cdot 8029187^{1} \cdot 55218797^{2} \cdot 475485788430118 67^{2}$

Theorem

If $v_p(\mathrm{Disc}(\Delta_{n,n})) = 1$, then $X_0(n)$ has bad reduction at p.

But:

Theorem

If n is odd and $v_p(\mathrm{Disc}(\Delta_{n,n})) = 1$, then $X_0(n)$ has irreducible reduction at p.

Some of the primes dividing $\mathrm{Disc}(\Delta_{n,n})$

$c = 0$: roots of $\Phi_n(x, 0)$ are $(2^n - 1)^{\text{st}}$ roots of unity (and 0)

Some of the primes dividing $\mathrm{Disc}(\Delta_{n,n})$

$c = 0$: roots of $\Phi_n(x, 0)$ are $(2^n - 1)^{\text{st}}$ roots of unity (and 0)

Roots of $\Psi_n(x, 0)$ are $(2^n - 1)^{\text{st}}$ roots of unity that are not $(2^d - 1)^{\text{st}}$ roots of unity for $d \mid n$, $d \neq n$.

Some of the primes dividing Disc($\Delta_{n,n}$)

$c = 0$: roots of $\Phi_n(x, 0)$ are $(2^n - 1)^{\text{st}}$ roots of unity (and 0)

Roots of $\Psi_n(x, 0)$ are $(2^n - 1)^{\text{st}}$ roots of unity that are not $(2^d - 1)^{\text{st}}$ roots of unity for $d \mid n$, $d \neq n$.

Recall that there is only one $(p^k)^{\text{th}}$ root of unity in $\overline{\mathbb{F}}_p$, but otherwise roots of unity remain distinct modulo (primes above) p.

Some of the primes dividing $\mathrm{Disc}(\Delta_{n,n})$

$c = 0$: roots of $\Phi_n(x, 0)$ are $(2^n - 1)^{\text{st}}$ roots of unity (and 0)

Roots of $\Psi_n(x, 0)$ are $(2^n - 1)^{\text{st}}$ roots of unity that are not $(2^d - 1)^{\text{st}}$ roots of unity for $d \mid n$, $d \neq n$.

Recall that there is only one $(p^k)^{\text{th}}$ root of unity in $\overline{\mathbb{F}}_p$, but otherwise roots of unity remain distinct modulo (primes above) p.

Thus: if $p \mid 2^n - 1$, then many points above $c = 0$ in $X_0(n)$ or $X_1(n)$ collide modulo p.

Some of the primes dividing $\mathrm{Disc}(\Delta_{n,n})$

$c = 0$: roots of $\Phi_n(x, 0)$ are $(2^n - 1)^{\text{st}}$ roots of unity (and 0)

Roots of $\Psi_n(x, 0)$ are $(2^n - 1)^{\text{st}}$ roots of unity that are not $(2^d - 1)^{\text{st}}$ roots of unity for $d \mid n$, $d \neq n$.

Recall that there is only one $(p^k)^{\text{th}}$ root of unity in $\overline{\mathbb{F}}_p$, but otherwise roots of unity remain distinct modulo (primes above) p.

Thus: if $p \mid 2^n - 1$, then many points above $c = 0$ in $X_0(n)$ or $X_1(n)$ collide modulo p.

By monodromy considerations, there must be points of $X_0(n)$ or $X_1(n)$ in characteristic 0 which reduce to $\bar{c} = 0$ upon reduction modulo $\mathfrak{p}$ that collide $\rightsquigarrow p \mid \mathrm{Disc}(\Delta_{n,n})$.

Reduction and $p \mid (2^n - 1)$

Example

$n = 5$. Roots of $\Psi_n(x, 0)$ are ζ^i, $\zeta = e^{2\pi i/31}$, $1 \leq i \leq 30$.
6 orbits (in terms of i):

- 1, 2, 4, 8, 16
- 3, 6, 12, 24, 17
- 5, 10, 20, 9, 18
- 7, 14, 28, 25, 19
- 11, 22, 13, 26, 21
- 15, 30, 29, 27, 23

All collide modulo 31, remain distinct modulo all other primes

Reduction and $p \mid (2^n - 1)$

Example

$n = 6$. Roots of $\Psi_n(x, 0)$ are ζ^i, $\zeta = e^{2\pi i/63}$, $1 \leq i \leq 62$, $i \not\equiv 0 \pmod{21}$, $i \not\equiv 0 \pmod 9$. 9 orbits:

- 1, 2, 4, 8, 16, 32
- 3, 6, 12, 24, 48, 33
- 5, 10, 20, 40, 17, 34
- 7, 14, 28, 56, 49, 35
- 11, 22, 44, 25, 50, 37
- 13, 26, 52, 41, 19, 38
- 15, 30, 60, 57, 51, 39
- 23, 46, 29, 58, 53, 43
- 31, 62, 61, 59, 55, 47

Modulo 7: Seven orbits collide (the ones that aren't multiples of 3), and two other orbits collide (the ones that are) $\rightsquigarrow$ wild ramification!

$c = 0$ and $c = -2$

Similarly, roots of $\Phi_n(x, -2)$ are of the form $\zeta + \zeta^{-1}$, $\zeta \in \mu_{2^n-1} \cup \mu_{2^n+1}$.

Thus, except for certain small values of n: if $p \mid (2^n \pm 1)$, then $p \mid \mathrm{Disc}(\Delta_{n,n})$.

$c = 0$ and $c = -2$

Similarly, roots of $\Phi_n(x, -2)$ are of the form $\zeta + \zeta^{-1}$, $\zeta \in \mu_{2^n-1} \cup \mu_{2^n+1}$.

Thus, except for certain small values of n: if $p \mid (2^n \pm 1)$, then $p \mid \mathrm{Disc}(\Delta_{n,n})$.

Necessary criterion for good reduction: contribution to ramification divisors at $\bar{c} = 0$ and $\bar{c} = -2$ must be the same in characteristic 0 and characteristic p.

In many cases e.g. $(n, p) =$ $(6, 5), (6, 7), (6, 13), (7, 3), (7, 43), (7, 127), (8, 3), (8, 5), (8, 17), (8, 257)$, the only contribution to the ramification divisor comes from $\bar{c} = 0$ and $\bar{c} = -2$.

$c = 0$ and reduction

So, to prove good reduction: suffices to check that contributions match up at those two points.

$c = 0$ and reduction

So, to prove good reduction: suffices to check that contributions match up at those two points.

Example

$\Delta_{5,5} \equiv c^5(c+2)^2 h(c) \pmod{31}$, where h is squarefree and not divisible by c or $c+2$ modulo 31. In the reduced curve, we have one six-cycle, so contribution is $6-1=5$ (tame ramification). This matches the exponent of c in $\Delta_{5,5}$, which is what we need.

Thank you

Thank you for your attention!