Dynamics of units and packing constants of ideals

Curtis T McMullen
Harvard University

Perspectives

- Continued Fractions in $\mathbb{Q}(\sqrt{D})$
- The Diophantine semigroup
- Geodesics in $SL_2(\mathbb{R})/SL_2(\mathbb{Z})$
- (Classical) Arithmetic Chaos
- Well-packed ideals
- Dynamics of units on $P^1(\mathbb{Z}/f)$
- Link Littlewood & Zaremba conjectures

Continued Fractions

Q. How to test if a real number x is in $\mathbb{Q}$?

Q. How to test if a real number x is in $\mathbb{Q}(\sqrt{D})$?

$$x = [a_0, a_1, a_2, a_3, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}}$$

A. x is in $\mathbb{Q}(\sqrt{D})$ iff a_i's repeat.

Diophantine numbers

$$x = [a_0, a_1, a_2, a_3, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots}}}$$

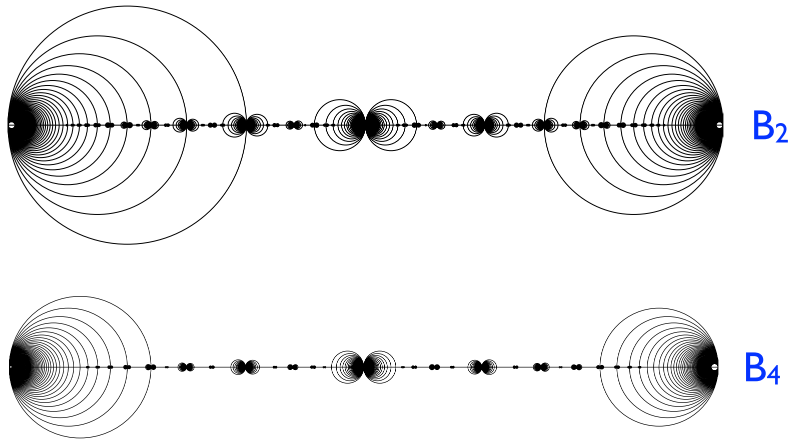
$$B_N = \{x \text{ real} : a_i \leq N\}$$

$B_N - \mathbb{Q}$ is a Cantor set of dim $\to 1$ as $N \to \infty$.

Conjecture: x algebraic and Diophantine iff x is rational or quadratic

Diophantine sets in [0,1]

$B_N = \{x : a_i \leq N\}$



Examples

γ = golden ratio = $(1+\sqrt{5})/2$ = [1,1,1,1....] = [1]

σ = silver ratio = $1+\sqrt{2}$ = [2]

[1,2]	$\mathbb{Q}(\sqrt{3})$	[1,2,2,2]	$\mathbb{Q}(\sqrt{30})$
[1,2,2]	$\mathbb{Q}(\sqrt{85})$	[1,1,1,2]	$\mathbb{Q}(\sqrt{6})$
[1,1,2]	$\mathbb{Q}(\sqrt{10})$	[1,1,2,2]	$\mathbb{Q}(\sqrt{221})$

Question: Does $Q(\sqrt{5})$ contain infinitely many periodic continued fractions with $a_i \leq M$?

Theorem

Every real quadratic field contains infinitely many uniformly bounded, periodic continued fractions.

Wilson, Woods (1978)

Example: [1,4,2,3], [1,1,4,2,1,3], [1,1,1,4,2,1,1,3]... all lie in $Q(\sqrt{5})$.

Thin group perspective

G_N = Diophantine semigroup in $SL_2(\mathbb{Z})$ generated by

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \ldots \begin{pmatrix} 0 & 1 \\ 1 & N \end{pmatrix}.$$

Theorem

Infinitely many primitive A in G_N have eigenvalues in $\mathbb{Q}(\sqrt{D})$, provided $N \gg 0$.

Thin group questions

G_N = semigroup generated by

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}, \ldots \begin{pmatrix} 0 & 1 \\ 1 & N \end{pmatrix}.$$

Open Question

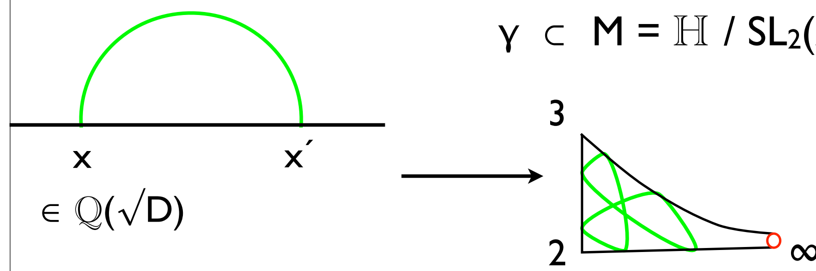
Does {tr(A) :A in G_N} have density one in {1,2,3,4,...} for $N \gg 0$?

Yes for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to d$ instead of $(a+d)$.

Bourgain-Kontorovich

Geometric perspective

$\gamma \subset M = \mathbb{H} / SL_2(\mathbb{Z})$



Theorem

Given one loop of length L, there is a bounded set $B \subset M$ containing ∞ many loops with lengths in {L, 2L, 3L, 4L, ...}.

Even though most loops of with these lengths are uniformly distributed (Duke).

Hyperbolic 3-manifolds

$\gamma \subset M = \mathbb{H}^3 / SL_2([\mathbb{Z}\sqrt{-D}])$

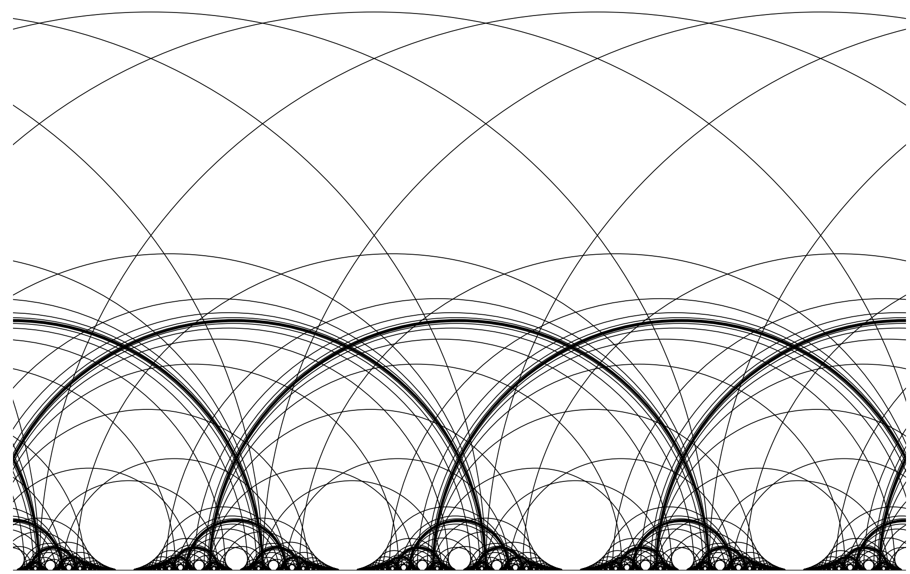
e.g. $M = S^3 - K$

beyond continued fractions

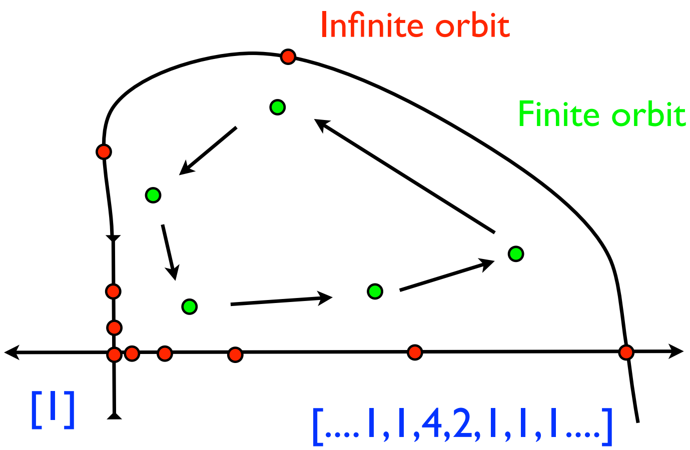
Theorem

Again, there is a bounded set $B \subset M$ made up of ∞ many loops with lengths in {L, 2L, 3L, 4L, ...}.

Example: Geodesic for [1,1,1,...,4,2,1,1,1...3] $\in \mathbb{Q}(\sqrt{5})$



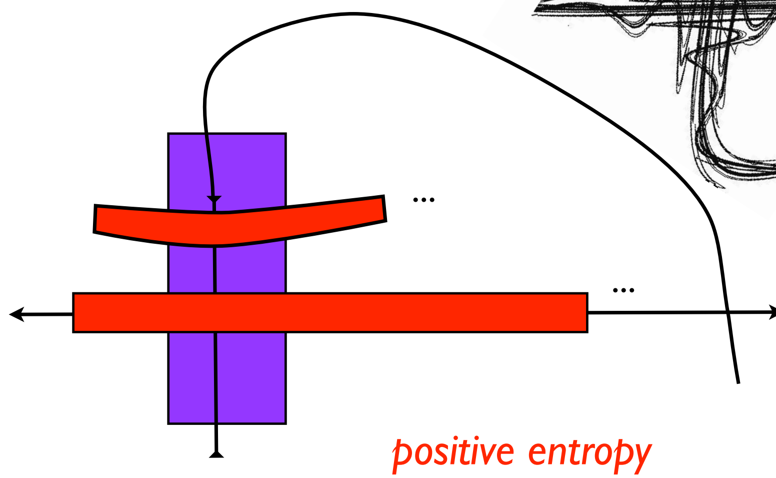
Dynamical perspective



Cross-section to geodesic flow

Same scenario

$\Longrightarrow$ chaotic dynamics



Arithmetic chaos?

Does the number of $[a_1,\ldots,a_p]$ in $\in \mathbb{Q}(\sqrt{D})$ with $a_i \leq 2$ grow exponentially as the period $p \to \infty$?

Example:

[1], [1, 1, 1, 1, 1, 1, 2, 1, 1, 2, 2, 1, 1, 1, 1, 2, 2], ...?...
lie in $Q(\sqrt{5})$.

Packing Perspective

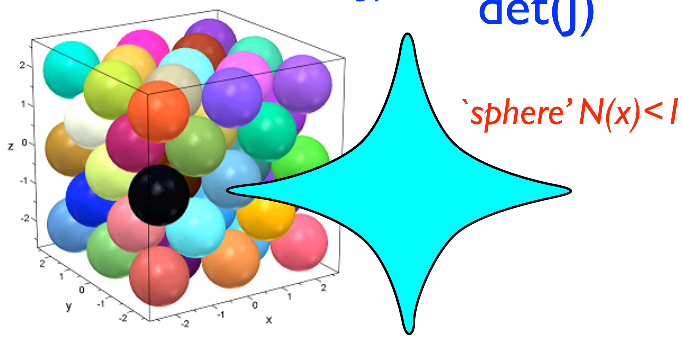
$K/\mathbb{Q}$ = number field of degree d

$J \subset K$: an "ideal" in K ($J \simeq \mathbb{Z}^d$)

{ideals J} / K^* = class ``group" (infinite)

Every J is an ideal for an order O(J) in K.

Packing constant $\delta(J) = \dfrac{N(J)}{\det(J)}$



$N(x)$ = Norm from K to $\mathbb{Q}$ = $x_1 \ldots x_d$

$N(J) = \inf \{|N(x)| : x \text{ in } J,\ N(x) \neq 0\}$

$\det(J) = \sqrt{|\mathrm{disc}(J)|} = \sqrt{|\det \mathrm{Tr}(a_i a_j)|}$

Well-packed ideals

Theorem

In any real quadratic field $K=\mathbb{Q}(\sqrt{D})$, *there are infinitely many ideal classes with* $\delta(J) > \delta_K > 0$.

Dictionary

x in K $\Leftrightarrow$ $J = \mathbb{Z} + \mathbb{Z}x$

A in $SL_2(\mathbb{Z})$ $\Leftrightarrow$ $J = \mathbb{Z}^2$ as a $\mathbb{Z}[A]$-module

Unit group rank 1

Conjecture

If K is a number field whose unit group has rank one, then there are infinitely many ideal classes with $\delta(J) > \delta_K > 0$.

Cubic fields, 1 complex place

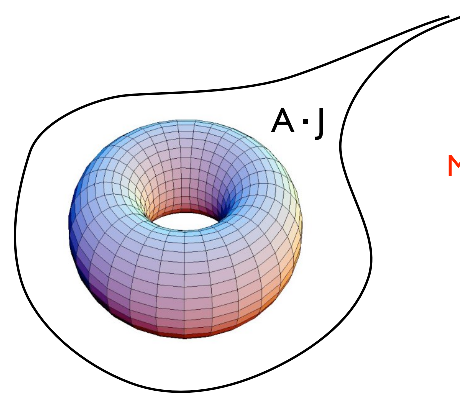
Quartic fields, 2 complex places

No cubic case is known
(e.g. $x^3 = x+1$ is open)

Higher rank

Conjecture [Cassel-Swinnerton-Dyer 1955]

In a total real cubic field K, only finitely many ideal classes satisfy $\delta(J) > \delta > 0$.



$SL_3(\mathbb{R})/SL_3(\mathbb{Z})$

Margulis Conjecture 2000 ⇒

Littlewood's Conjecture &
Conjecture above

Einsiedler, Katok, Lindenstrauss, Michel, Venkatesh;
CTM-, Minkowski's Conjecture

Fibonacci orders

$\mathcal{O}_D$ = the real quadratic order of discriminant D

$\cong \mathbb{Z}[x]/(x^2+bx+c)$, $D = b^2-4c$

$K = \mathbb{Q}(\sqrt{D})$ = real quadratic field

ε = unit in K

D = discriminant of $\mathbb{Z}[\varepsilon]$

$D f_m^2$ = discriminant of $\mathbb{Z}[\varepsilon^m]$

$\mathbb{Z}[\varepsilon^m]$ = m^{th} Fibonacci order $\cong \mathcal{O}_{f_m^2 D}$

Fibonacci orders for golden mean

$K = \mathbb{Q}(\sqrt{5})$ = real quadratic field

ε = unit in K = $(1+\sqrt{5})/2$

$\mathbb{Z}[\varepsilon] \cong \mathcal{O}_D$ D = 5

$D f_m^2$ = discriminant of $\mathbb{Z}[\varepsilon^m]$

$(f_1, f_2, \ldots) = (1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots)$

$f_m \sim \varepsilon^m$, $\varepsilon > 1$

grows exponentially fast

Class numbers

Pic $\mathbb{Z}[\varepsilon^m]$ has order about $f_m \sim \sqrt{(D f_m^2)}$

(as large as possible)

Fibonacci Conjecture

Given α>0, there is a δ>0 such that

$|\{J \text{ in Pic } \mathbb{Z}[\varepsilon^m] : \delta(J) > \delta\}| > f_m^{1-\alpha}$

for all $m \gg 0$.

Lots of ideals ⇒ many well packed

(But not most)

Dynamics of units

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Acts on $\mathbb{Z}^2$

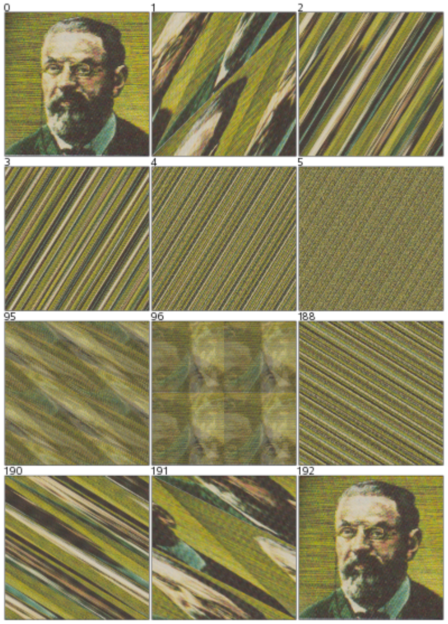
Just as ε acts on $\mathbb{Z}[\varepsilon]$

Acts on $E = \mathbb{R}^2/\mathbb{Z}^2$ and on $E[f] \cong (\mathbb{Z}/f)^2$

KEY FACT: $U^{2m} = \mathrm{Id}$ on $E[f_m]$

Proof. $$U^m = \begin{pmatrix} f_{m-1} & f_m \\ f_m & f_{m+1} \end{pmatrix} \equiv f_{m+1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod f_m.$$

"Poincaré Recurrence"



$U^{2m} = I$
mod f_m

$f_{192} =$
59723042738777441355693383976920205335 04

= 256 x ....

Dynamics of units (con't)

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Acts on $\mathbb{P}^1(\mathbb{Z}/f)$
$\{x = [a:b]\}$

$J(x) = \mathbb{Z}\,(a+b\,\varepsilon) + f\,\mathbb{Z}[\varepsilon]$ an ideal for $\mathcal{O}_{Df^2}$

Pic $\mathcal{O}_{Df^2} \approx$ {orbits of U acting on $\mathbb{P}^1(\mathbb{Z}/f)$}

$U^m = Id \Rightarrow$ Pic $\mathbb{Z}[\varepsilon^m]$ has order $\approx f_m / m$

large class numbers

Height and packing

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Acts on $\mathbb{P}^1(\mathbb{Z}/f)$

Height $H(x) = \inf a^2+b^2 : x = [a:b]$

$H(x) = O(f)$

$\delta(J(x)) \approx \min_i H(U^i x)/f$

Events $E_i = H(U^i x)/f > \delta$ Each have probability $p \approx 1$

Assume more or less independent! [Arithmetic chaos]

$\Rightarrow |x : \delta(J(x)) > \delta| \approx p^m f_m \geq f_m^{1-\alpha}$

⇒ Fibonacci Conjecture

The quadratic \`field' K = $\mathbb{Q} \oplus \mathbb{Q}$

$\mathbb{Z} \oplus \mathbb{Z}$ = quadratic ring $\mathcal{O}_1$ of discriminant 1

$\mathcal{O}_{f^2}$ = {(a,b) : a = b mod f} $\subset \mathbb{Z} \oplus \mathbb{Z}$

Conjecture

Given $\alpha>0$, there is a $\delta>0$ s.t.

$|\{ J \text{ in Pic}\,\mathcal{O}_{f^2} : \delta(J) > \delta\}| > f^{1-\alpha}$

for all $f \gg 0$.

[All class numbers large.]

This conjecture implies Zaremba's conjecture.

Zaremba's Conjecture

$\exists N$: *For any* $q>0$, $\exists$ $p/q = [a_1,\dots,a_n]$

with $a_i \le N$.

How it follows: Pic $\mathcal{O}_{f^2} \simeq (\mathbb{Z}/f)^*$

$J(x) = \{(a,b) : a = xb \bmod f\} \subset \mathbb{Z} \oplus \mathbb{Z}$ det $J(x) = f$

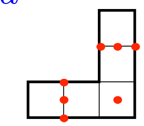
$$\delta(J(x)) > \delta \quad \Leftrightarrow$$

$$N(J(x)) = \min_{p,q} \{|q|\ |xq-pf|\} > \delta f \quad \Leftrightarrow$$

$$|x/f - p/q| > \delta/q^2 \quad \Leftrightarrow$$

continued fraction of x/f is bounded by $N(\delta)$.

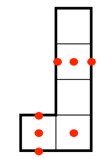
Coda: Expanders from $\mathcal{O}_{d^2}$

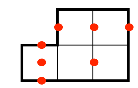


$V(X_d)$ = {genus 2 covering spaces

$S \to E = \mathbb{R}^2/\mathbb{Z}^2$,

branched over one point}





$SL_2(\mathbb{Z})$ acts transitively $\Rightarrow$

Graphs X_d

Conjecture: *These X_d are expanders.*

$X_d = SL_2(\mathbb{Z})/\Gamma_d$, Γ_d not congruence!

$Z*Z \to S_d$ Jac(S) real multiplication by $\mathcal{O}_{d^2}$

Restrospective

- CF's; Geodesics/A-orbits; Packing constants
- Arithmetic chaos in rank 1
- Margulis-Littlewood-CSD rigidity in higher rank

Uniformly Diophantine numbers in a fixed real quadratic field.
Compos. Math. 145(2009)

slides online

Theorem 2.2 *Given $A \in \mathrm{GL}_2(\mathbb{Z})$ such that $A^2 = I$, $\mathrm{tr}(A) = 0$ and $\mathrm{tr}(A^\dagger U) = \pm 1$, let*

$$L_m = U^m + U^{-m} A.$$

Then for all $m \geq 0$:

1. $|\det(L_m)| = f_{2m}$ *is a generalized Fibonacci number;*
2. *The lattice $[L_m]$ is fixed by U^{2m};*
3. *We have $L_{-m} = L_m A$;*
4. *For $0 \leq i \leq m$ we have:*

$$\|U^i L_m U^{-i}\|, \|U^{-i} L_{-m} U^i\| \ \leq C\sqrt{|\det L_m|}, \tag{2.7}$$

where C depends only on A and U.