Rigidez em teoria ergódica e aplicações em teoria dos números

SEMEAR 2024

Bruno Santiago

Universidade Federal Fluminense

16 de outubro de 2024

Teoria dos Números

- Encontrar padrões nos números naturais $\mathbb{N} = \{1, 2, 3, 4, \dots\}$;
- Aproximações *diofantinas*: $\frac{p_n}{q_n} \to \alpha$;
- Subconjuntos densos de $\mathbb{R}$ obtidos por processos algébricos;
- Comportamento assintótico de sequências numéricas....

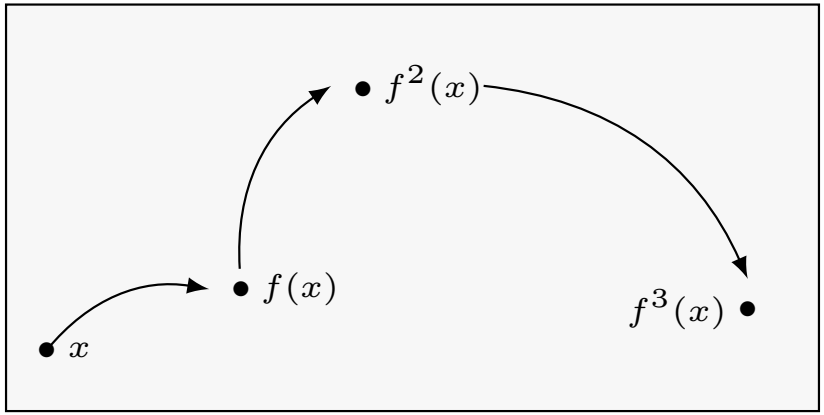
Teoria Ergódica

Estudo de ações de grupos $\phi : G \times X \to X$ que preservam espaços de probabilidade (X, μ)

Teoria Ergódica

Estudo de ações de grupos $\phi : G \times X \to X$ que preservam espaços de probabilidade (X, μ)

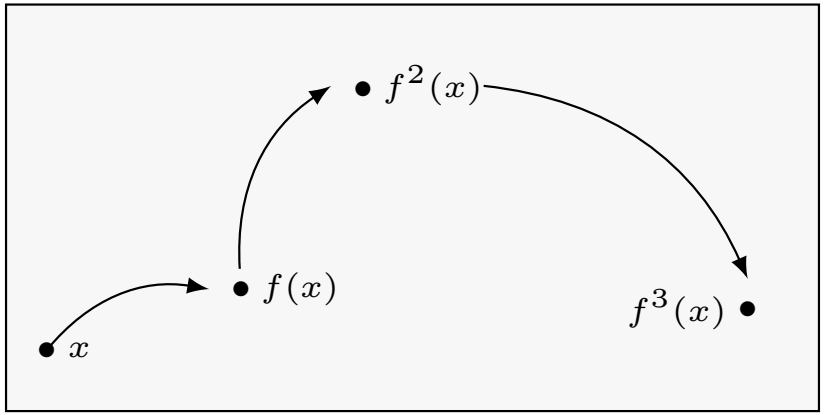
Exemplo $G = \mathbb{Z}$



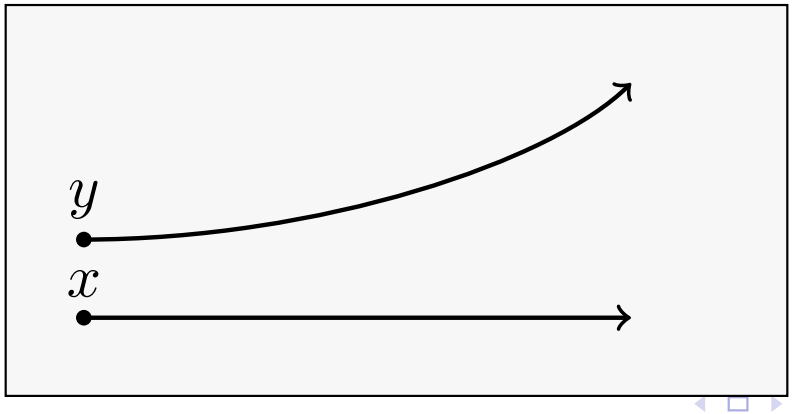
Teoria Ergódica

Estudo de ações de grupos $\phi : G \times X \to X$ que preservam espaços de probabilidade (X, μ)

Exemplo $G = \mathbb{Z}$



Exemplo $G = \mathbb{R}$



Um exemplo onde G é um grupo de Lie

O espaço de reticulados

Um reticulado em $\mathbb{R}^d$ é o conjunto de todas as combinações lineares **com coeficientes em** $\mathbb{Z}$ de uma base de $\mathbb{R}^d$

Um exemplo onde G é um grupo de Lie

O espaço de reticulados

Um reticulado em $\mathbb{R}^d$ é o conjunto de todas as combinações lineares **com coeficientes em** $\mathbb{Z}$ de uma base de $\mathbb{R}^d$,i.e.

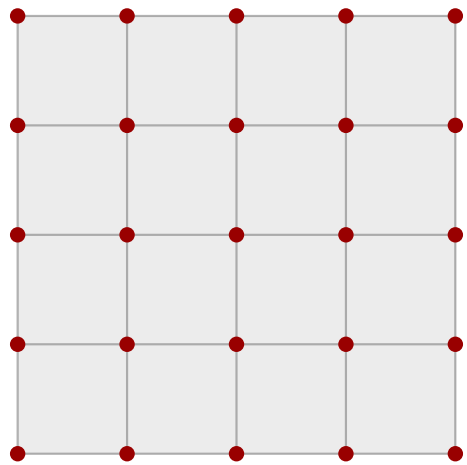
Se $\{v_1, \ldots, v_d\}$ é uma base, o conjunto
$\{v = \alpha_1 v_1 + \cdots + \alpha_d v_d; \alpha_1, \ldots, \alpha_d \in \mathbb{Z}\}$ é um reticulado.

Um exemplo onde G é um grupo de Lie

O espaço de reticulados

Um reticulado em $\mathbb{R}^d$ é o conjunto de todas as combinações lineares **com coeficientes em** $\mathbb{Z}$ de uma base de $\mathbb{R}^d$,i.e.

Se $\{v_1, \ldots, v_d\}$ é uma base, o conjunto
$\{v = \alpha_1 v_1 + \cdots + \alpha_d v_d; \alpha_1, \ldots, \alpha_d \in \mathbb{Z}\}$ é um reticulado.

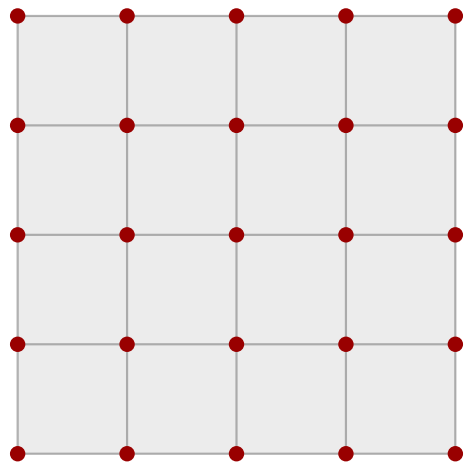


Um exemplo onde G é um grupo de Lie

O espaço de reticulados

Um reticulado em $\mathbb{R}^d$ é o conjunto de todas as combinações lineares **com coeficientes em** $\mathbb{Z}$ de uma base de $\mathbb{R}^d$,i.e.

Se $\{v_1, \ldots, v_d\}$ é uma base, o conjunto
$\{v = \alpha_1 v_1 + \cdots + \alpha_d v_d; \alpha_1, \ldots, \alpha_d \in \mathbb{Z}\}$ é um reticulado.



- Todo reticulado pode ser identificado com o conjunto $g\mathbb{Z}^d$, com $g \in \mathrm{GL_d}(\mathbb{R})$

Um exemplo onde G é um grupo de Lie

O espaço de reticulados

O covolume de um reticulado é o volume do paralelepípedo gerado pela base $\{v_1, \ldots, v_d\}$.

Um exemplo onde G é um grupo de Lie

O espaço de reticulados

O covolume de um reticulado é o volume do paralelepípedo gerado pela base $\{v_1, \ldots, v_d\}$. Seja

$\mathcal{L}_d \stackrel{\text{def.}}{=} \{L; L \text{ é um reticulado de covolume : } 1\}$.

Um exemplo onde G é um grupo de Lie

O espaço de reticulados

O covolume de um reticulado é o volume do paralelepípedo gerado pela base $\{v_1, \ldots, v_d\}$. Seja

$\mathcal{L}_d \stackrel{\text{def.}}{=} \{L; L \text{ é um reticulado de covolume : } 1\}$.

Lema

$\mathcal{L}_d = \{g\mathbb{Z}^d; g \in \mathrm{SL_d}(\mathbb{R})\} \simeq \mathrm{SL}_d(\mathbb{R})/\,\mathrm{SL_d}(\mathbb{Z})$

Um exemplo onde G é um grupo de Lie

O espaço de reticulados

O covolume de um reticulado é o volume do paralelepípedo gerado pela base $\{v_1, \ldots, v_d\}$. Seja

$$\mathcal{L}_d \stackrel{\text{def.}}{=} \{L; L \text{ é um reticulado de covolume : } 1\}.$$

Lema

$\mathcal{L}_d = \{g\mathbb{Z}^d; g \in \mathrm{SL_d}(\mathbb{R})\} \simeq \mathrm{SL}_d(\mathbb{R})/\,\mathrm{SL_d}(\mathbb{Z})$

- Dado $H < \mathrm{SL_d}(\mathbb{R})$ temos uma ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$:

$$\phi_h(g\mathbb{Z}^d) = hg\mathbb{Z}^d$$

Teoria dos Números via Teoria Ergódica

- Frequentemente sequências numéricas escondem por trás sistemas dinâmicos

Teoria dos Números via Teoria Ergódica

- Frequentemente sequências numéricas escondem por trás sistemas dinâmicos
- E estes sistemas quase sempre possuem algum tipo de estrutura algébrica

Teoria dos Números via Teoria Ergódica

- Frequentemente sequências numéricas escondem por trás sistemas dinâmicos
- E estes sistemas quase sempre possuem algum tipo de estrutura algébrica
- Essa estrutura força o fenômeno de *rigidez*: propriedades que em princípio deveriam ser verdade para μ-**quase todo ponto** na verdade são verdade para **todo** ponto do espaço!

Exemplo 1: primeiros dígitos de potências de 2

```
2
4
8
16
32
64
128
256
512
1024
2048
4096
8192
16384
32768
65536
131072
262144
524288
1048576
2097152
4194304
8388608
16777216
33554432
67108864
134217728
268435456
536870912
1073741824
2147483648
4294967296
8589934592
17179869184
34359738368
68719476736
137438953472
274877906944
549755813888
1099511627776
```

Exemplo 1: primeiros dígitos de potências de 2

Um dígito $D \in \{1, \ldots, 9\}$ é o primeiro dígito de 2^n se, e somente se

$$D \times 10^k < 2^n < (D+1) \times 10^k$$
$$\iff \log_{10} D + k < n \log_{10} 2 < \log_{10}(D+1) + k$$

Exemplo 1: primeiros dígitos de potências de 2

O sistema dinâmico subjacente

Considere o número *irracional* $\alpha = \log_{10} 2$. Considere o espaço $\mathbb{S}^1 = \mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z}; x \in \mathbb{R}\}$ e o sistema dinâmico $f : \mathbb{S}^1 \to \mathbb{S}^1$ (=ação do grupo $\mathbb{Z}$ em $\mathbb{S}^1$) dado por

$$f(x) = x + \alpha.$$

Exemplo 1: primeiros dígitos de potências de 2

O sistema dinâmico subjacente

Considere o número *irracional* $\alpha = \log_{10} 2$. Considere o espaço $\mathbb{S}^1 = \mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z}; x \in \mathbb{R}\}$ e o sistema dinâmico $f : \mathbb{S}^1 \to \mathbb{S}^1$ (=ação do grupo $\mathbb{Z}$ em $\mathbb{S}^1$) dado por

$$f(x) = x + \alpha.$$

Então $f^n(0) = n \log_{10} 2$.

Exemplo 1: primeiros dígitos de potências de 2

O sistema dinâmico subjacente

Considere o número *irracional* $\alpha = \log_{10} 2$. Considere o espaço $\mathbb{S}^1 = \mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z}; x \in \mathbb{R}\}$ e o sistema dinâmico $f : \mathbb{S}^1 \to \mathbb{S}^1$ (=ação do grupo $\mathbb{Z}$ em $\mathbb{S}^1$) dado por

$$f(x) = x + \alpha.$$

Então $f^n(0) = n \log_{10} 2$.Portanto,

Proposição

D é o primeiro dígito de $2^n \iff$
$f^n(0) \in J(D) \stackrel{\text{def.}}{=} [\log_{10}(D+1), \log_{10} D]$.

Exemplo 1: primeiros dígitos de potências de 2

O poder da teoria ergódica

f é uma transformação **unicamente ergódica**, um caso particular do fenômeno de rigidez e que implica:

$$\lim_{n\to\infty} \frac{\#\{j=0,...,n-1; f^j(0)\in J(D)\}}{n} = \log_{10}\left(\frac{D+1}{D}\right)$$

```
In [13]: for i=1:9
             println(log10((i+1)/i))
         end
```

```
0.3010299956639812
0.1760912590556812
0.12493873660829993
0.09691001300805642
0.07918124604762482
0.06694678963061322
0.05799194697768673
0.05115252244738129
0.04575749056067514
```

Exemplo 2: pequenos valores de formas quadráticas

A Conjectura de Oppenheim

- **Equações diofantinas**: Existe solução $(x, y, z) \in \mathbb{Z}^d$ para $x^d + y^d = z^d$? Existe solução em $(x, y, z) \in \mathbb{Z}^d$ para $x^2 + y^2 - \sqrt{2}z^2 = 0$?

Exemplo 2: pequenos valores de formas quadráticas

A Conjectura de Oppenheim

- **Equações diofantinas**: Existe solução $(x, y, z) \in \mathbb{Z}^d$ para $x^d + y^d = z^d$? Existe solução em $(x, y, z) \in \mathbb{Z}^d$ para $x^2 + y^2 - \sqrt{2}z^2 = 0$?
- **Inequações diofantinas**: Existe solução $(x, y, z) \in \mathbb{Z}^d$ para $|x^d + y^d - z^d| < 10^{-10!}$? Existe solução $(x, y, z) \in \mathbb{Z}^d$ para $|x^2 + y^2 - \sqrt{2}z^2| < 10^{-10!}$?

Exemplo 2: pequenos valores de formas quadráticas

A Conjectura de Oppenheim

A função $f(x, y, z) = x^2 + y^2 - \sqrt{2}z^2$ é uma forma quadrática, e a pergunta

Existe solução $(x, y, z) \in \mathbb{Z}^d$ para $|x^2 + y^2 - \sqrt{2}z^2| < 10^{-10!}$?

Foi feita em 1929 pelo matemático britânico *Alexander Oppenheim*, considerando mais geralmente formas quadráticas $Q(x_1, \ldots, x_d) = \sum a_{ij} x_i x_j$ que tomam valores positivos e negativos (são indefinidas) e que não são múltiplas de formas com coeficientes em $\mathbb{Q}$.

Exemplo 2: pequenos valores de formas quadráticas

A Conjectura de Oppenheim

Teorema(Grigori Margulis)

Seja Q uma forma quadrática indefinida em $d \geq 3$ variáveis que não é múltipla de uma forma com coeficientes racionais. Então, para todo $\varepsilon > 0$ a inequação

$$|Q(x)| < \varepsilon$$

admite solução $x \in \mathbb{Z}^d$.

Exemplo 2: pequenos valores de formas quadráticas

Um olhar dinâmico para o problema

Considere $H \stackrel{\text{def.}}{=} \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ o grupo das transformações $h : \mathbb{R}^d \to \mathbb{R}^d$ que preservam Q, i.e.

$$Q(hx) = Q(x).$$

Exemplo 2: pequenos valores de formas quadráticas

Um olhar dinâmico para o problema

Considere $H \overset{\text{def.}}{=} \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ o grupo das transformações $h : \mathbb{R}^d \to \mathbb{R}^d$ que preservam Q, i.e.

$$Q(hx) = Q(x).$$

Então $|Q(x)| < \varepsilon$ tem solução $\iff$ $Q(H\mathbb{Z}^d)$ acumula na origem

Exemplo 2: pequenos valores de formas quadráticas

Um olhar dinâmico para o problema

Considere $H \overset{\text{def.}}{=} \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ o grupo das transformações $h : \mathbb{R}^d \to \mathbb{R}^d$ que preservam Q, i.e.

$$Q(hx) = Q(x).$$

Então $|Q(x)| < \varepsilon$ tem solução $\iff$ $Q(H\mathbb{Z}^d)$ acumula na origem $\iff$ $H\mathbb{Z}^d$ acumula na origem

Exemplo 2: pequenos valores de formas quadráticas

Um olhar dinâmico para o problema

Considere $H \stackrel{\text{def.}}{=} \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ o grupo das transformações $h : \mathbb{R}^d \to \mathbb{R}^d$ que preservam Q, i.e.

$$Q(hx) = Q(x).$$

Então $|Q(x)| < \varepsilon$ tem solução $\iff$ $Q(H\mathbb{Z}^d)$ acumula na origem $\iff$ $H\mathbb{Z}^d$ acumula na origem $\iff$ a órbita de $\mathbb{Z}^d \in \mathcal{L}_d$ pela ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$ contém vetores arbitrariamente pequenos

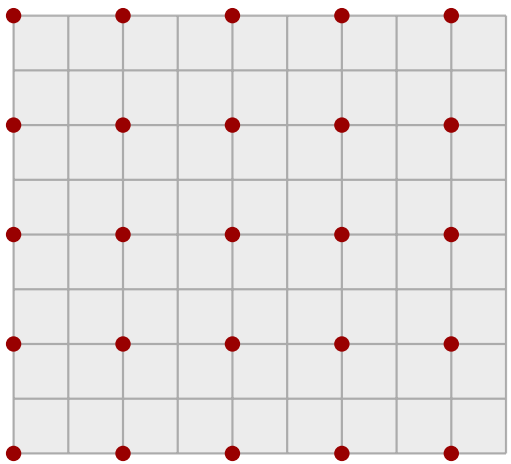
Exemplo 2: pequenos valores de formas quadráticas

Um olhar dinâmico para o problema

Considere $H \stackrel{\text{def.}}{=} \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ o grupo das transformações $h : \mathbb{R}^d \to \mathbb{R}^d$ que preservam Q, i.e.

$$Q(hx) = Q(x).$$

Então $|Q(x)| < \varepsilon$ tem solução $\iff$ $Q(H\mathbb{Z}^d)$ acumula na origem $\iff$ $H\mathbb{Z}^d$ acumula na origem $\iff$ a órbita de $\mathbb{Z}^d \in \mathcal{L}_d$ pela ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$ contém vetores arbitrariamente pequenos



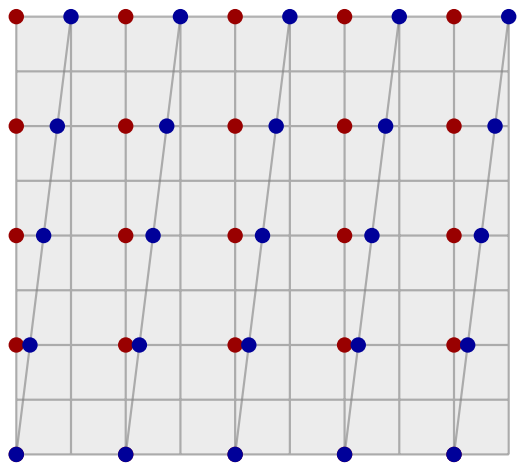
Exemplo 2: pequenos valores de formas quadráticas

Um olhar dinâmico para o problema

Considere $H \stackrel{\text{def.}}{=} \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ o grupo das transformações $h : \mathbb{R}^d \to \mathbb{R}^d$ que preservam Q, i.e.

$$Q(hx) = Q(x).$$

Então $|Q(x)| < \varepsilon$ tem solução $\iff$ $Q(H\mathbb{Z}^d)$ acumula na origem $\iff$ $H\mathbb{Z}^d$ acumula na origem $\iff$ a órbita de $\mathbb{Z}^d \in \mathcal{L}_d$ pela ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$ contém vetores arbitrariamente pequenos



Exemplo 2: pequenos valores de formas quadráticas

Um olhar dinâmico para o problema

Considere $H \stackrel{\text{def.}}{=} \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ o grupo das transformações $h : \mathbb{R}^d \to \mathbb{R}^d$ que preservam Q, i.e.

$$Q(hx) = Q(x).$$

Então $|Q(x)| < \varepsilon$ tem solução $\iff$ $Q(H\mathbb{Z}^d)$ acumula na origem $\iff$ $H\mathbb{Z}^d$ acumula na origem $\iff$ a órbita de $\mathbb{Z}^d \in \mathcal{L}_d$ pela ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$ contém vetores arbitrariamente pequenos

Critério de Compacidade de Mahler

Um subconjunto $K \subset \mathcal{L}_d$ é compacto se, e somente se, não contém vetores arbitrariamente pequenos.

Exemplo 2: pequenos valores de formas quadráticas

Um olhar dinâmico para o problema

Considere $H \overset{\text{def.}}{=} \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ o grupo das transformações $h : \mathbb{R}^d \to \mathbb{R}^d$ que preservam Q, i.e.

$$Q(hx) = Q(x).$$

Então $|Q(x)| < \varepsilon$ tem solução $\iff$ $Q(H\mathbb{Z}^d)$ acumula na origem $\iff$ $H\mathbb{Z}^d$ acumula na origem
$\iff$ a órbita de $\mathbb{Z}^d \in \mathcal{L}_d$ pela ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$ contém vetores arbitrariamente pequenos

Critério de Compacidade de Mahler

Um subconjunto $K \subset \mathcal{L}_d$ é compacto se, e somente se, não contém vetores arbitrariamente pequenos.

- Portanto, $|Q(x)| < \varepsilon$ tem solução $\iff$ a órbita de $\mathbb{Z}^d$ pela ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$ **não** é compacta.

Exemplo 2: pequenos valores de formas quadráticas

Um olhar dinâmico para o problema

Considere $H \stackrel{\text{def.}}{=} \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ o grupo das transformações $h : \mathbb{R}^d \to \mathbb{R}^d$ que preservam Q, i.e.

$$Q(hx) = Q(x).$$

Então $|Q(x)| < \varepsilon$ tem solução $\iff$ $Q(H\mathbb{Z}^d)$ acumula na origem $\iff$ $H\mathbb{Z}^d$ acumula na origem
$\iff$ a órbita de $\mathbb{Z}^d \in \mathcal{L}_d$ pela ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$ contém vetores arbitrariamente pequenos

Critério de Compacidade de Mahler

Um subconjunto $K \subset \mathcal{L}_d$ é compacto se, e somente se, não contém vetores arbitrariamente pequenos.

- Portanto, $|Q(x)| < \varepsilon$ tem solução $\iff$ a órbita de $\mathbb{Z}^d$ pela ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$ **não** é compacta.

Exemplo 2: pequenos valores de formas quadráticas

O Teorema de Ratner

Teorema (Marina Ratner)

Se $H < \mathrm{SL_d}(\mathbb{R})$ é um subgrupo gerado por subgrupos a um parâmetro unipotentes então o fecho de toda órbita pela ação $\phi : H \times \mathcal{L}_d \to \mathcal{L}_d$ é da forma $\hat{H}\mathbb{Z}^d$, onde $H < \hat{H} < \mathrm{SL_d}(\mathbb{R})$

Exemplo 2: pequenos valores de formas quadráticas

Solução da conjectura de Oppenheim usando o Teorema de Ratner

- O grupo $H = \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ é maximal

Exemplo 2: pequenos valores de formas quadráticas

Solução da conjectura de Oppenheim usando o Teorema de Ratner

- O grupo $H = \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ é maximal
- Logo, para o grupo $\hat{H}$ do Teorema de Ratner só temos duas opções: $H = \hat{H}$ ou $H = \mathrm{SL_d}(\mathbb{R})$.

Exemplo 2: pequenos valores de formas quadráticas

Solução da conjectura de Oppenheim usando o Teorema de Ratner

- O grupo $H = \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ é maximal
- Logo, para o grupo $\hat{H}$ do Teorema de Ratner só temos duas opções: $H = \hat{H}$ ou $H = \mathrm{SL_d}(\mathbb{R})$.
- Se primeiro caso acontece então Q é múltipla de uma forma com coeficientes racionais.

Exemplo 2: pequenos valores de formas quadráticas

Solução da conjectura de Oppenheim usando o Teorema de Ratner

- O grupo $H = \mathrm{SO}(Q) < \mathrm{SL_d}(\mathbb{R})$ é maximal
- Logo, para o grupo $\hat{H}$ do Teorema de Ratner só temos duas opções: $H = \hat{H}$ ou $H = \mathrm{SL_d}(\mathbb{R})$.
- Se primeiro caso acontece então Q é múltipla de uma forma com coeficientes racionais.
- Logo, a órbita $H\mathbb{Z}^d$ é densa em $\mathcal{L}_d$ e portanto não é compacta!

Outros exemplos

- Conjectura de Littlewood: a inequação $|m(n\alpha - m)(n\beta - \ell)| < \varepsilon$ admite solução $(m, n, \ell) \in \mathbb{Z}^3$?
- Teorema de Elkies-McMullen: as lacunas deixadas pela sequência $\sqrt{n} \mod 1$ em $\mathbb{S}^1$ se distribuem de acordo com uma função F analítica por partes e com duas transições de fase.

Outros exemplos

- Conjectura de Littlewood: a inequação $|m(n\alpha - m)(n\beta - \ell)| < \varepsilon$ admite solução $(m, n, \ell) \in \mathbb{Z}^3$?
- Teorema de Elkies-McMullen: as lacunas deixadas pela sequência $\sqrt{n} \mod 1$ em $\mathbb{S}^1$ se distribuem de acordo com uma função F analítica por partes e com duas transições de fase.

"Grosso modo, a ideia de Elkies e McMullen consiste em traduzir o problema do calculo da distribuição $F(t)$ das lacunas de $\sqrt{n} \mod 1$ para a questão de computar a probabilidade de um reticulado"aleatorio" de $\mathbb{R}^2$ intersectar um certo triângulo fixado. A vantagem desse procedimento aparentemente artificial consiste no fato de que a teoria ergódica de reticulados aleatórios esta bem desenvolvida gracas a poderosos resultados do calibre dos teoremas de Ratner, o que nos permite saber precisamente a probabilidade desejada (de um reticulado encontrar um triângulo fixo)". Texto do Blog do Carlos Matheus.

Obrigado!