

A Medida de Mahler

Rui Soares Barbosa

2º ano - Ciências da Computação
Universidade do Minho

Setembro, 2008

- Contexto: o Problema de Lehmer
- Propriedades Básicas
- Resultados
- Aplicações

- Contexto: o Problema de Lehmer
- Propriedades Básicas
- Resultados
- Aplicações

Procura de primos grandes

1644 - Marin Mersenne (1588-1648)

$$M_n = 2^n - 1$$

p primo

$p =$	2	3	5	7	11	13
$M_p =$	3	7	31	127	2047	8191



Os maiores primos encontrados são primos de Mersenne.

1916/18 - Pierce estudou uma generalização de M_n :

A um polinómio $p \in \mathbb{Z}[x]$,

$$p(x) = \sum_{k=0}^d a_k x^k = a_d \prod_{i=1}^d (x - \alpha_i)$$

$a_k \in \mathbb{Z}$ (coeficientes) e $\alpha_i \in \mathbb{C}$ (raízes),

1916/18 - Pierce estudou uma generalização de M_n :

A um polinómio $p \in \mathbb{Z}[x]$,

$$p(x) = \sum_{k=0}^d a_k x^k = a_d \prod_{i=1}^d (x - \alpha_i)$$

$a_k \in \mathbb{Z}$ (coeficientes) e $\alpha_i \in \mathbb{C}$ (raízes),

associou a sequência de inteiros

$$\Delta_n(p) = |a_d|^n \prod_{i=1}^d (\alpha_i^n - 1)$$

$$\Delta_n(p) = |a_d|^n \prod_{i=1}^d (\alpha_i^n - 1)$$

- $m \mid n \Rightarrow \Delta_m \mid \Delta_n$
- outros divisores de Δ_n satisfazem condições estritas

pelo que $\frac{\Delta_p}{\Delta_1}$ (p primo) seriam bons candidatos a primos...

caso particular: Mersenne

$$p(x) = x - 2$$

- $p(x) = 0$ sse $x = 2$
- $\Delta_n = 2^n - 1$ (números de Mersenne)
- $\frac{\Delta_p}{\Delta_1} = \frac{2^p - 1}{2^1 - 1} = 2^p - 1$ (forma dos primos de Mersenne)

1933 - Lehmer estudou o crescimento da sucessão (Δ_n) :

$$|\alpha| > 1 \Rightarrow \lim_{n \rightarrow \infty} \frac{|\alpha^{n+1} - 1|}{|\alpha^n - 1|} = |\alpha|$$

$$|\alpha| < 1 \Rightarrow \lim_{n \rightarrow \infty} \frac{|\alpha^{n+1} - 1|}{|\alpha^n - 1|} = 1$$

Logo, se $|\alpha_i| \neq 1$,

$$\lim_{n \rightarrow \infty} \frac{|\Delta_{n+1}|}{|\Delta_n|} = \lim_{n \rightarrow \infty} \frac{|a_d|^{n+1} \prod |\alpha_i^{n+1} - 1|}{|a_d|^n \prod |\alpha_i^n - 1|} = \underbrace{|a_d| \prod_{i=1}^d \max\{1, |\alpha_i|\}}_{M(p)}$$

“Medida” (de Mahler):

$$M(p) := |a_d| \prod_{i=1}^d \max\{1, |\alpha_i|\}$$

$$\Delta_n \sim M(p)^n$$

.

- menor crescimento reduz factores extra ($\neq \Delta_m$).
- Logo, há potencialmente mais primos se $M(p)$ pequeno.

o problema de Lehmer

Lehmer -1933

“The following problem arises immediately. If ϵ is a positive quantity, to find a polynomial of the form



$$f(x) = x^r + a_{r-1}x^{r-1} + \dots + a_0$$

where the a 's are integers, such that the absolute value of the product of those roots of f which lie outside the unit circle, lies between 1 and $1 + \epsilon$.

This problem, in interest in itself, is especially important for our purposes. Whether or not the problem has a solution for $\epsilon < 0.176$ we do not know”

o problema de Lehmer

Problema

Dado $\epsilon > 0$ arbitrário, existe $p \in \mathbb{Z}[x]$ tal que $1 < M(p) < 1 + \epsilon$?

Conjectura

Não

polinómio mínimo

encontrado por Lehmer:

$$\ell(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

$$M(\ell) = 1.176280818$$

Ainda não ultrapassado.

- Contexto: o Problema de Lehmer
- **Propriedades Básicas**
- Resultados
- Aplicações

$M(p)$ como medida de polinómios

- $M(pq) = M(p)M(q)$
- $M(p) = M(-p)$

propriedades da medida de Mahler

M(p) como medida de polinómios

- $M(pq) = M(p)M(q)$
- $M(p) = M(-p)$
- $M(p) = M(p^*)$

Definição (polinómio recíproco)

$$p^*(x) = x^d p(1/x)$$

exemplo

$$\begin{aligned} p(x) &= x^4 + 3x^3 - 5x^2 + 0x + 7 \\ p^*(x) &= x^4 \left(\frac{1}{x^4} + 3\frac{1}{x^3} - 5\frac{1}{x^2} + 0\frac{1}{x^1} + 7 \right) \\ &= 1 + 3x - 5x^2 + 0x^3 + 7x^4 \end{aligned}$$

propriedades da medida de Mahler

M(p) como medida de polinómios

- $M(pq) = M(p)M(q)$
- $M(p) = M(-p)$
- $M(p) = M(p^*)$

Demonstração.

$$p(x) = \sum_{k=0}^d a_k x^k = \prod_{i=1}^d (x - \alpha_i)$$

$$|p(0)| = |a_0| = |a_d| \prod_{i=1}^d |\alpha_i|$$

Logo

$$\prod_{i=1}^d |\alpha_i| = \frac{|a_0|}{|a_d|}$$



propriedades da medida de Mahler

M(p) como medida de polinómios

- $M(pq) = M(p)M(q)$
- $M(p) = M(-p)$
- $M(p) = M(p^*)$

Demonstração.

$$\prod_{i=1}^d |\alpha_i| = \frac{|a_0|}{|a_d|}$$

Logo

$$\frac{M(p^*)}{M(p)} = \frac{|a_0| \prod_{|\alpha_i^{-1}| > 1} |\alpha_i^{-1}|}{|a_d| \prod_{|\alpha_i| > 1} |\alpha_i|} = \frac{\prod_i |\alpha_i| \prod_{|\alpha_i| \leq 1} |\alpha_i^{-1}|}{\prod_{|\alpha_i| > 1} |\alpha_i|} = 1$$

$M(p)$ como medida de polinómios

- $M(pq) = M(p)M(q)$
- $M(p) = M(-p)$
- $M(p) = M(p^*)$
- $|a_j| \leq \binom{d}{j} M(p)$

consequência

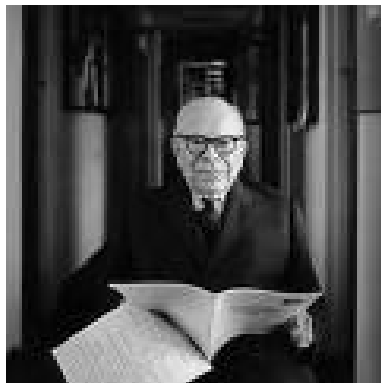
$\forall D \in \mathbb{N}, M \in \mathbb{R}, \{p \in \mathbb{Z}[x] \mid \deg(p) \leq D, M(p) < M\}$ é finito.

propriedades da medida de Mahler

$M(p)$ como medida de polinómios

- $M(pq) = M(p)M(q)$
- $M(p) = M(-p)$
- $M(p) = M(p^*)$
- $|a_j| \leq \binom{d}{j} M(p)$
- $M(p) = \exp(\int_0^1 \log |p(e^{2\pi i t})| dt)$

permite definir $M(p)$ para $p \in \mathbb{Z}[x_1, \dots, x_n]$

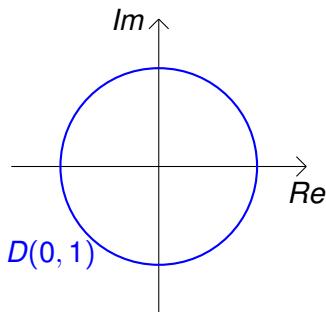


propriedades da medida de Mahler

$$M(p) := |a_d| \prod_{i=1}^d \max\{1, |\alpha_i|\} \geq 1$$

observação

$M(p)$ é o produto dos zeros fora do disco unitário.



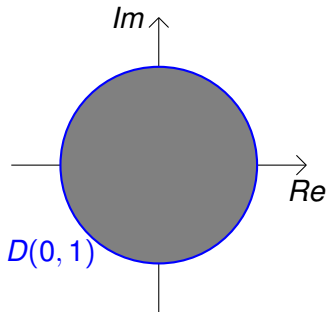
propriedades da medida de Mahler

$$M(p) := |a_d| \prod_{i=1}^d \max\{1, |\alpha_i|\} \geq 1$$

observação

$M(p)$ é o produto dos zeros fora do disco unitário.

$M(p) = 1$ quando $\forall i, |\alpha_i| < 1$



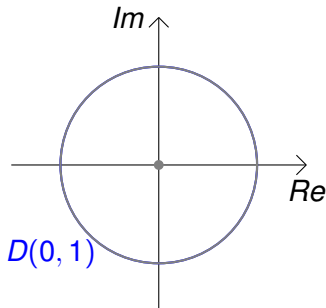
propriedades da medida de Mahler

$$M(p) := |a_d| \prod_{i=1}^d \max\{1, |\alpha_i|\} \geq 1$$

observação

$M(p)$ é o produto dos zeros fora do disco unitário.

$M(p) = 1$ quando $\forall i, |\alpha_i| = 0 \vee |\alpha_i| = 1$ $M(p) = M(p^*)$



os polinómios mais “simples” ...

Uma raíz n -ésima ζ da unidade satisfaz

$$\zeta^n = 1$$

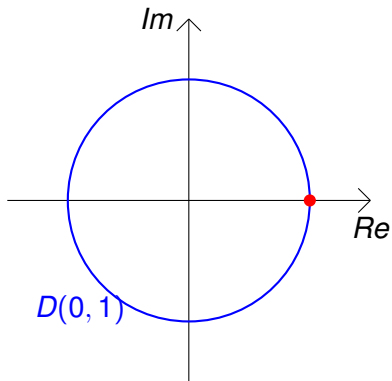
$$\zeta_k = e^{k \frac{2\pi}{n} i} \quad k = 1, \dots, n$$

os polinómios mais “simples” ...

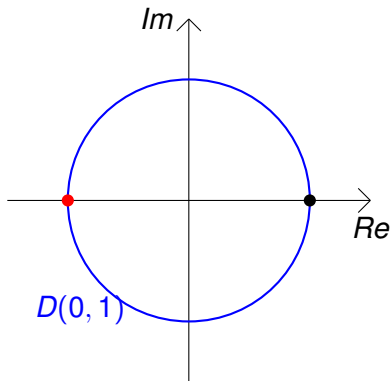
Uma raiz n -ésima ζ **primitiva** da unidade satisfaz

$$\begin{cases} \zeta^n = 1 \\ \zeta^m \neq 1 \quad \forall m, 0 < m < n \end{cases}$$

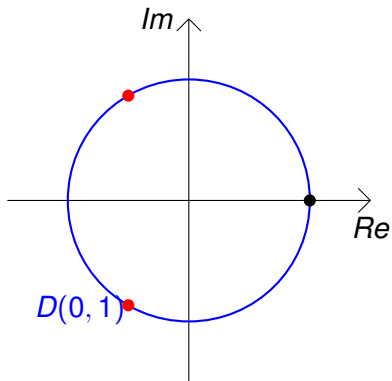
$$\zeta_k = e^{k \frac{2\pi}{n} i} \quad k = 1, \dots, n, \text{gcd}(k, n) = 1$$



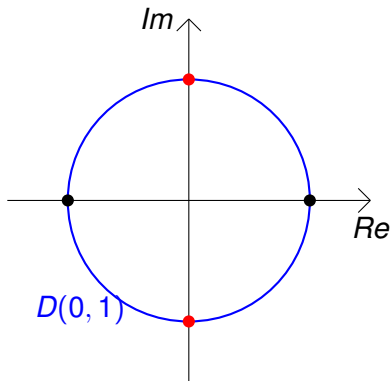
$$\begin{cases} \zeta^1 = 1 \\ \zeta^m \neq 1 \quad (0 < m < 1) \end{cases}$$



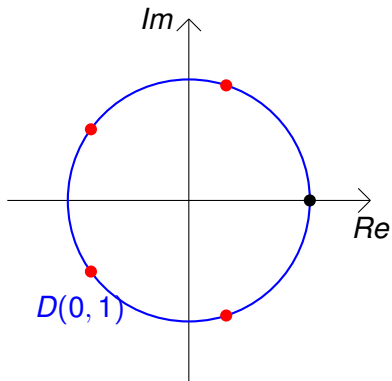
$$\begin{cases} \zeta^2 = 1 \\ \zeta^m \neq 1 \quad (m = 1) \end{cases}$$



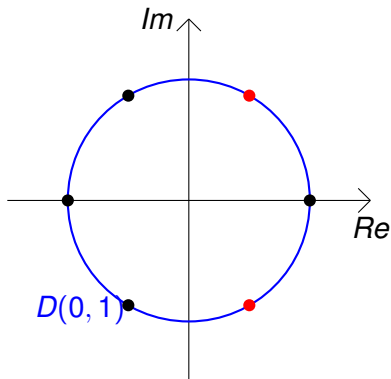
$$\begin{cases} \zeta^3 = 1 \\ \zeta^m \neq 1 \quad (m = 1, 2) \end{cases}$$



$$\begin{cases} \zeta^4 = 1 \\ \zeta^m \neq 1 \quad (m = 1, 2, 3) \end{cases}$$



$$\begin{cases} \zeta^5 = 1 \\ \zeta^m \neq 1 \quad (m = 1, 2, 3, 4) \end{cases}$$



$$\begin{cases} \zeta^6 = 1 \\ \zeta^m \neq 1 \quad (m = 1, 2, 3, 4, 5) \end{cases}$$

As raízes primitivas têm o mesmo polinómio mínimo

$$\Phi_n(x) = \prod_{\zeta_k \text{ primitiva}} (x - \zeta_k) = \begin{cases} x - 1 & \text{se } n = 1 \\ \frac{x^n - 1}{\prod_{m|n} \Phi_m(x)} & \text{se } n > 1 \end{cases}$$

observação

$$M(\Phi_n) = \prod |\zeta_k| = 1$$

Esta medida é mínima.

polinómios ciclotómicos

observação

$$M(\Phi_n) = \prod |\zeta_k| = 1$$

Esta medida é mínima.

Questão

Que outros polinómios têm medida 1?

exemplos

- x , pois a sua única raiz é 0.
- produtos de polinómios já conhecidos de medida 1.

polinómios ciclotómicos

observação

$$M(\Phi_n) = \prod |\zeta_k| = 1$$

Esta medida é mínima.

Questão

Que outros polinómios têm medida 1?

exemplos

- x , pois a sua única raiz é 0.
- produtos de polinómios já conhecidos de medida 1.

Em geral, $p = x^a \Phi_{b_1} \dots \Phi_{b_r}$, com $a, r, b_i \in \mathbb{N}_0$

...

teorema de Kronecker

...

Haverá outros?

Teorema (Kronecker)

Não!

$M(p) = 1$ sse p é produto de ciclotômicos e potências de x .

ou seja,

$M(p) = 1$ sse as raízes de p são raízes da unidade ou zero.

teorema de Kronecker

Demonstração.

Seja $p \in \mathbb{Z}[x]_d$ com raízes α_i tal que $M(p) = 1$.
Consideremos $p_k = a_d^k \prod (x - \alpha_i^k)$.

$$M(p_k) = 1$$

$$\Rightarrow |a_{j(k)}| \leq \binom{d}{j} \quad (\text{desigualdade da norma})$$

$$\Rightarrow \{f_k | k \in \mathbb{N}\} \text{ é finito}$$

$$\Rightarrow \{\beta | \exists k, f_k(\beta) = 0\} \text{ é finito}$$

$$\Rightarrow \forall i, \exists r > s, \alpha_i^r = \alpha_i^s$$

$$\Rightarrow \forall i, \alpha_i = 0 \vee \alpha_i^{r-s} = 1$$



- Contexto: o Problema de Lehmer
- Propriedades Básicas
- Resultados
 - Limites Globais
 - Limites Restritos
 - Explorações Computacionais
- Aplicações

- Contexto: o Problema de Lehmer
- Propriedades Básicas
- Resultados
 - Limites Globais
 - Limites Restritos
 - Explorações Computacionais
- Aplicações

$$M(p) > 1 + R(d)$$

- 1971 - Blanksby e Montgomery: $R(d) = \frac{1}{52d \log 6d}$
- 1978 - Stewart: $R(d) = \frac{1}{10^4 d \log d}$

$$M(p) > 1 + R(d)$$

- 1971 - Blanksby e Montgomery: $R(d) = \frac{1}{52d \log 6d}$
- 1978 - Stewart: $R(d) = \frac{1}{10^4 d \log d}$
- 1979 - Dobrowolski: $R(d) = \frac{1}{1200} \left(\frac{\log \log d}{\log d} \right)^3$ (com $d \geq 2$).
- idem (assimptótico) $R(d) = (1 - \epsilon) \left(\frac{\log \log d}{\log d} \right)^3$
- 1982 - Cantor e Strauss: $R(d) = (2 - \epsilon) \left(\frac{\log \log d}{\log d} \right)^3$
- 1983 - Louboutin: $R(d) = \left(\frac{9}{4} - \epsilon \right) \left(\frac{\log \log d}{\log d} \right)^3$
- 1996 - Voutier: $R(d) = \frac{1}{4} \left(\frac{\log \log d}{\log d} \right)^3$ (com $d \geq 2$)

$$M(p) > 1 + R(d)$$

Mas...

Em qualquer caso,

$$\lim_{d \rightarrow \infty} R(d) = 0$$

Problema de Lehmer ainda em aberto...

- Contexto: o Problema de Lehmer
- Propriedades Básicas
- Resultados
 - Limites Globais
 - Limites Restritos
 - Explorações Computacionais
- Aplicações

polinómios recíproco

Recordemos que...

$$p^*(x) = x^d p(1/x)$$

Definição (polinómio recíproco)

p diz-se recíproco quando $p = p^*$.

observação

Se p recíproco,

- $a_j = a_{d-j}$ (coeficientes simétricos)
- Se $p(\alpha) = 0 \Rightarrow p(1/\alpha) = 0$ (raízes estáveis sob $z \rightarrow 1/z$)

mínimos para certas classes de polinómios

- Smyth(1971) - recíprocos

Teorema

Se $p \in \mathbb{Z}[x]$ é não recíproco e $p(0)p(1) \neq 0$, então

$$M(p) \geq M(x^3 - x - 1) = 1.3247 = \theta$$

onde θ é a solução real do polinómio acima.

mínimos para certas classes de polinómios

- Smyth(1971) - recíprocos
- O teorema de Smyth aplica-se a qualquer polinómio irreduzível de grau ímpar

- Se p recíproco, $p = p^* = x^d p(1/x)$.
- $p(-1) = p^*(-1) = (-1)^d p(1/(-1)) = -p(-1)$
- $p(-1) = 0$
- $p = (x + 1)q$ $M(x + 1) = 1$.

mínimos para certas classes de polinómios

- Smyth(1971) - recíprocos
- O teorema de Smyth aplica-se a qualquer polinómio irreduzível de grau ímpar
- Borwein, Dobrowolski, Mossinghoff (2007) - coef. ímpares

Teorema

Se p é um polinómio com coeficiente ímpares, irreduzível, não ciclotómico e $p(0) \neq 0$, então

$$M(p) \geq 5^{1/4} = 1.495 \dots$$

- Contexto: o Problema de Lehmer
- Propriedades Básicas
- Resultados
 - Limites Globais
 - Limites Restritos
 - Explorações Computacionais
- Aplicações

pesquisa de polinómios de medida pequena

Para $M(p) < 2$, temos $|a_j| \leq 2\binom{d}{j}$.

Assim, a_j tem $4\binom{d}{j} + 1$ possibilidades.

exemplo (grau=4)

número de polinómios a procurar (exaustivamente):

$$\underbrace{4\binom{4}{4}}_{a_4} \underbrace{(4\binom{4}{3} + 1)}_{a_3} \underbrace{(4\binom{4}{2} + 1)}_{a_2} \underbrace{(4\binom{4}{1} + 1)}_{a_1} \underbrace{(4\binom{4}{0} + 1)}_{a_0} = 144500$$

medidas mínimas para cada $\mathbb{Z}_d[x]$

d	nº polys	polinómio	M(p)
1	20	$x - 2$	2
2	180	$x^2 - x - 1$	1.618...
3	3380	$x^3 + 0x^2 - x + 1$	1.324...
4	144500	$x^4 - x^3 + 0x^2 + 0x - 1$	1.380...
5	14826420	$x^5 - x^4 + x^3 + 0x^2 - x + 1$	1.349...
10	1.8×10^{23}	$\ell(x)$	1.176...

Lehmer-1933

“We have not made an examination of all 10th degree symmetric polynomials, but a rather intensive search has failed to reveal a better polynomial than

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1, \Omega = 1.176280818$$

All efforts to find a better equation of degree 12 and 14 have been unsuccessful.”

teste de $M(p)$

- candidatos: mónicos, recíprocos, irredutíveis, de grau par

pesquisa de polinómios de medida pequena

teste de $M(p)$

- candidatos: mónicos, recíprocos, irredutíveis, de grau par
- filtro de quadrados das raízes (método de Graeffe)

$$\begin{aligned} p(x) = g(x^2) + xh(x^2) &\rightsquigarrow (G(p))(x) = g(x)^2 - xh(x)^2 \\ \{\alpha_j\} &\rightsquigarrow \{\alpha_j^2\} \end{aligned}$$

$$p_m := G^m(p)$$

- Se $M(p) < M$, $|a_{m,j}| \leq \binom{d}{j} + \binom{d-2}{j-2}(M^{2^m} + M^{-2^m} - 2)$
- Se p é produto de ciclotómicos, $\forall m > \log_2 dp_m = p_{m+1}$

teste de $M(p)$

- candidatos: mónicos, recíprocos, irredutíveis, de grau par
- filtro de quadrados das raízes (método de Graeffe)
- remover factores ciclotómicos
- calcular $M(P)$

pesquisa de polinómios de medida pequena

estratégias de pesquisa

- exaustiva ($\mathcal{O}(C^{d^2})$)

realizada até $d \leq 24$, $M = 1.3$

pesquisa de polinómios de medida pequena

estratégias de pesquisa

- exaustiva ($\mathcal{O}(C^{d^2})$)
- 1989 - Boyd: Altura 1 ($\mathcal{O}(C^d)$)

$p \in \mathbb{Z}[x]$ com $M(p) < 2 \Rightarrow \exists g \in \mathbb{Z}[x], H(g) = 1$

- pesquisa até $d \leq 40$ (encontrou anteriores)

pesquisa de polinómios de medida pequena

estratégias de pesquisa

- exaustiva ($\mathcal{O}(C^{d^2})$)
- 1989 - Boyd: Altura 1 ($\mathcal{O}(C^d)$)
- 1998 - Mossinghoff, Pinner, Vaaler: Perturbações ($\mathcal{O}(C^{\sqrt{d}})$)

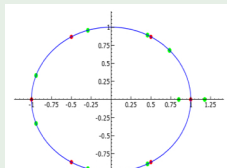
Produtos de ciclotómicos perturbados

encontrar produto de Φ s e perturbar o coeficiente do meio (± 1)

- pesquisa até $d \leq 64$ (encontrou $> 80\%$ dos anteriores)

polinómio de Lehmer

$$\ell(x) = \Phi_1^2 \Phi_2^2 \Phi_3^2 \Phi_6 - x^5$$



estratégias de pesquisa

- exaustiva ($\mathcal{O}(C^{d^2})$)
- 1989 - Boyd: Altura 1 ($\mathcal{O}(C^d)$)
- 1998 - Mossinghoff, Pinner, Vaaler: Perturbações ($\mathcal{O}(C^{\sqrt{d}})$)
- Sparse Polynomials

número fixo de coeficientes não nulos

pesquisa de polinómios de medida pequena

estratégias de pesquisa

- exaustiva ($\mathcal{O}(C^{d^2})$)
- 1989 - Boyd: Altura 1 ($\mathcal{O}(C^d)$)
- 1998 - Mossinghoff, Pinner, Vaaler: Perturbações ($\mathcal{O}(C^{\sqrt{d}})$)
- Sparse Polynomials
- 2000 - Rhin, Sac-Épée: Estatístico

gerar coeficientes segundo uma dist. multinormal de média $x^n + 1$

estratégias de pesquisa

- exaustiva ($\mathcal{O}(C^{d^2})$)
- 1989 - Boyd: Altura 1 ($\mathcal{O}(C^d)$)
- 1998 - Mossinghoff, Pinner, Vaaler: Perturbações ($\mathcal{O}(C^{\sqrt{d}})$)
- Sparse Polynomials
- 2000 - Rhin, Sac-Épée: Estatístico
- 2000 - Rhin, Sac-Épée: Minimização

começar com uma semente e procurar mínimo local
(perturbações pequenas)

- Contexto: o Problema de Lehmer
- Propriedades Básicas
- Resultados
- Aplicações

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- normas L_p

Para cada $r \in \mathbb{R}^+$, definimos a norma L_r como

$$\|p\|_r = \left(\int_0^1 |p(e^{2\pi i t})|^r dt \right)^{1/r}$$

Então

$$\lim_{r \rightarrow 0} \|p\|_r = \exp\left(\int_0^1 \log |p(e^{2\pi i t})| dt\right) = M(p)$$

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- normas L_p
- teoria de números transcendententes

desigualdades úteis no estudo de números transcendententes
(área onde Mahler a aplicou)

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- normas L_p
- teoria de números transcendentess
- factorização de polinómios

se a conjectura de Lehmer for verdadeira, existe um limite ao número de factores não ciclotómicos de um polinómio dependente dos seus coeficientes.

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

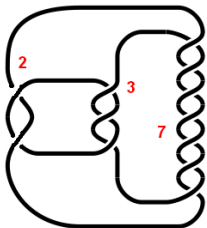
- normas L_p
- teoria de números transcendententes
- factorização de polinómios
- funções-L e curvas elípticas

Existem relações entre a medida de Mahler para polinómios de várias variáveis e o valor de séries-L.

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- normas L_p
- teoria de números transcendententes
- factorização de polinómios
- funções-L e curvas elípticas
- teoria de nós



os polinómios de Alexander são um invariante de nó.

A medida mínima de polinómios de enlacs de “pretzel” é

$$M(\ell(x)) = 1.176 \dots - \text{“pretzel”}-(2,3,7).$$

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- normas L_p
- teoria de números transcendententes
- factorização de polinómios
- funções-L e curvas elípticas
- teoria de nós
- sequências de inteiros
- sistemas dinâmicos algébricos

- Contexto: o Problema de Lehmer
- Propriedades Básicas
- Resultados
- Aplicações
 - Sequências de Lehmer-Pierce
 - Sistemas Dinâmicos “Algébricos”

Sequências de Lehmer-Pierce

$$\Delta_n(p) = |a_d|^n \prod_{i=1}^d |\alpha_i^n - 1|$$

generalizam a sequência de Mersenne

- Lehmer - procura de primos “grandes”

$$p(x) = x^3 - x - 1$$

$$\Delta_{133} = 63088004325217$$

$$\Delta_{127} = 3233514251032733$$

Sequências de Lehmer-Pierce

$$\Delta_n(p) = |a_d|^n \prod_{i=1}^d |\alpha_i^n - 1|$$

generalizam a sequência de Mersenne

- Lehmer - procura de primos “grandes”
- pequeno $M(p) \rightsquigarrow$ mais primos...

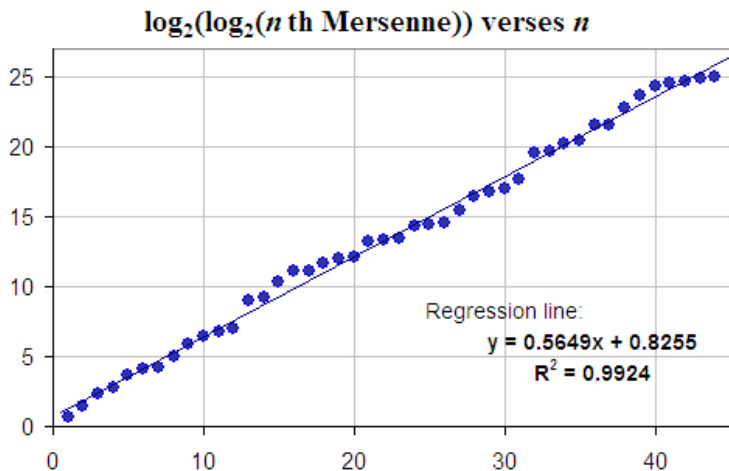
Sequências de Lehmer-Pierce

$$\Delta_n(p) = |a_d|^n \prod_{i=1}^d |\alpha_i^n - 1|$$

generalizam a sequência de Mersenne

- Lehmer - procura de primos “grandes”
- pequeno $M(p) \rightsquigarrow$ mais primos...
- mas são demasiado pequenos!
- no entanto...permitem conhecer melhor sequências como a de Mersenne

Conjectura de Wagstaff (Mersenne)



Conjectura de Wagstaff (Mersenne)

Conjectura

Seja n_j o j -ésimo primo para o qual M_{n_j} é primo. Então

$$\frac{j}{\log \log M_{n_j}} \rightarrow \frac{e^\gamma}{\log 2}$$

i.e., o número de primos de Mersenne $\leq x$ tende para

$$\frac{e^\gamma}{\log 2} \log \log x$$

onde γ é a constante de Euler-Mascheroni:

$$\gamma = \lim_{n \rightarrow \infty} \left(\sum_{k=1}^n 1/k - \log n \right)$$

Conjectura de Wagstaff (Mersenne)

Argumentação Heurística

Questão

Qual a probabilidade de M_k ser primo para k aleatório?

Conjectura de Wagstaff (Mersenne)

- Pelo teorema dos números primos, $\mathbb{P}(k \text{ primo}) = 1 / \log k$
- Assumindo k primo, qual a probabilidade de M_k tb ser?

Primeira aproximação

$$P_0 := \frac{1}{\log 2^k - 1}$$

Observação

$$M_k \text{ primo} \Rightarrow \forall q < 2k + 1 \text{ primo}, q \nmid M_k$$

Conjectura de Wagstaff (Mersenne)

$$N_0 = \mathbb{N} = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20,$$

$$P_0 \sim \frac{|V|}{|N_0|}$$

$2^k - 1$ não é divisível por 2 se for primo. Logo

$$P_1 : \sim \frac{|V|}{\frac{1}{2}|N_0|} = 2P_0$$

Conjectura de Wagstaff (Mersenne)

$$N_1 = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, \dots$$

$$P_1 \sim \frac{|V|}{|N_1|}$$

$2^k - 1$ não é divisível por 3 se for primo. Logo

$$P_2 : \sim \frac{|V|}{\frac{2}{3}|\mathbb{N}|} = \frac{3}{2}P_1 = \frac{3}{2}2P_0$$

Conjectura de Wagstaff (Mersenne)

$$N_2 = 1, , , 5, , 7, , , 11, , 13, , , 17, , 19, , \dots$$

$$P_2 \sim \frac{|V|}{|N_2|}$$

$2^k - 1$ não é divisível por 5 se for primo. Logo

$$P_3 := \frac{|V|}{\frac{4}{5}|\mathbb{N}|} = \frac{5}{4}P_2 = \frac{5}{4} \frac{3}{2}P_0$$

Conjectura de Wagstaff (Mersenne)

...

$$\mathbb{P}(2^k - 1 \text{ primo} | k \text{ primo}) = \frac{1}{k \log 2} \frac{2}{1} \frac{3}{2} \frac{5}{4} \frac{7}{6} \cdots \frac{q}{q-1}$$

para q primo $< 2k + 1$.

⋮

Conjectura de Wagstaff (Lehmer-Pierce)

procurando generalizar o raciocínio

Conjectura

Seja n_j o j -ésimo primo para o qual M_{n_j} é primo. Então

$$\frac{j}{\log \log \Delta_{n_j}(p)} \rightarrow \frac{e^\gamma}{\log M(p)}$$

- Contexto: o Problema de Lehmer
- Propriedades Básicas
- Resultados
- Aplicações
 - Sequências de Lehmer-Pierce
 - Sistemas Dinâmicos “Algébricos”

- X - grupo compacto abeliano
- δ - métrica em X
- μ - medida em X
- $T : \alpha \mapsto T^\alpha$ ($\alpha \in \mathbb{Z}^r$)
- $T^\alpha : X \rightarrow X$ automorfismo
- $T^n \Delta T^m = T^{n+m}$ (acção de \mathbb{Z}^r em X)

consideramos $X = \mathbb{T}^d$

Dado $p(x)$, considerar $T(x) = Ax$, onde A é a matriz companheira de p .

$$|Per_n| = \Delta_n$$