Prova da Hipótese de Riemann para Funções Zeta de Curvas sobre Corpos Finitos

Marcos Antônio Sobral Filho, Fabio Enrique Brochero Martinez (orientador)

Universidade Federal de Minas Gerais - UFMG

Av. Pres. Antônio Carlos, 6627 - Pampulha, Belo Horizonte - MG, 31270-901

sobralmarquinhos@gmail.com, fbrochero@ufmg.br

Resumo

Em Novembro de 1859, Bernhard Riemann publicou o artigo Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*, onde ele conjecturou que todos os zeros "não-óbvios" da sua função zeta tinham parte real $\frac{1}{2}$. Apesar de não sabermos ainda se a conjectura é verdadeira, sabemos que ela vale quando se trata de uma função zeta de uma curva algébrica definida sobre um corpo finito.*

A primeira prova para esse resultado instigante foi dada por André Weil na década de 1940. Em 1969, Stepanof forneceu um novo método de prova, o qual foi generalizado por Bombieri em 1973. Neste trabalho, vamos prová-lo a partir do Lema de Bombieri, cuja demonstração será omitida para fins didáticos.

1. Função Zeta de uma Curva sobre um Corpo Finito

Sejam $\mathbb{F}_q$ um corpo finito com q elementos e C uma curva projetiva não-singular, geometricamente conexa, definida sobre $\mathbb{F}_q$, com corpo de funções $\mathbb{K}$ e $\mathbb{F}_q$ exatamente o seu corpo de constantes.

Definição 1. *Dado um ponto fechado P em C, definimos o **grau de P** por*

$$d(P) \doteq \left[\frac{R_P}{\mathfrak{m}_P} : \mathbb{F}_q\right]$$

*onde $(R_P, \mathfrak{m}_P)$ é o anel de valuação discreta correspondente à P. Definimos a **norma de P** por $N(P) \doteq q^{d(P)}$.*
Seja $Div(C)$ o grupo dos divisores da curva C. Para cada $D \in Div(C)$, o número

$$d(D) \doteq \sum_{P \in C} ord_P(D) \cdot d(P)$$

*é o **grau de D** e o número $N(D) \doteq q^{d(D)}$ é a **norma de D**.*
*A **função zeta de C** sobre $\mathbb{F}_q$ é a série formal*

$$Z(t) \doteq \sum_{D \geq 0} t^{d(D)}.$$

A *priori* deveríamos mostrar que a função zeta acima está bem-definida, i.e, que a série formal que a define, tem raio de convergência positivo. No entanto, esse e outros fatos básicos (mas bem importantes) sobre ela serão assumidos, em detrimento dos lemas que envolvem a demonstração da Hipótese de Riemann, no nosso caso.

A função zeta de C sobre $\mathbb{F}_q$ carrega propriedades bastante úteis, que estão resumidas no seguinte teorema.

Teorema 1. *1.* $Z(t) = \prod_{P \in C} (1 - t^{d(P)})^{-1}$*;*

2. $Z(t) = \dfrac{L(t)}{(1-qt)(1-t)}$ *onde* $L(t) \in \mathbb{Z}[t]$ *com grau* $2g$*, satisfazendo* $L(0) = 1$ *e* $L(t) = q^g t^{2g} L\left(\dfrac{1}{qt}\right)$*;*

3. $Z(t) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{t_m}{m}\right)$ *onde N_m é o número de pontos fechados de C, que são racionais sobre $\mathbb{F}_{q^m}$, i.e.,*

$$N_m \doteq \#\{P \in C \mid d(P) | m\}$$

4. Se C_n é a curva obtida de C, extendendo o corpo de constantes $\mathbb{F}_q$ a $\mathbb{F}_{q^n}$, então

$$Z(t^n, C_n) = \prod_{\zeta^n = 1} Z(\zeta t, C).$$

Observação 1. *Note que a segunda propriedade mostra que se $\alpha_1, \ldots, \alpha_{2g}$ são os recíprocos das raízes de $L(t)$, então $\alpha_i \alpha_{g+i} = q$, para todo $i = 1, \ldots, g$.*

2. A Hipótese de Riemann sobre $Z(t)$

Sejam C uma curva completa, não-singular, definida sobre $\mathbb{F}_q$ e $\zeta(s, C) \doteq Z(q^{-s}, C)$. A **Hipótese de Riemann** afirma que todos os zeros de $\zeta(s, C)$ estão na linha crítica $Re(s) = \frac{1}{2}$. Isso é claramente equivalente ao seguinte resultado.

Teorema 2. *(Hipótese de Riemann)*
Os recíprocos das raízes de $L(t)$ satisfazem $|\alpha_i| = q^{\frac{1}{2}}$, para todo $i = 1, \ldots, 2g$.

Observação 2. *A validade do teorema 2 implica imediatamente que*

$$|N_m - (q^m + 1)| \leq 2g q^{\frac{n}{2}}$$

pois $N_m = q^n + 1 - \sum_{i=1}^{2g} \alpha^i$, para todo $m \geq 1$.

A partir dessa observação será simples mostrar que vale a seguinte equivalência.

Proposição 1. *A Hipótese de Riemann vale para $Z(t, C)$ se, e somente se, existem A, B constantes e $N > 0$ inteiro tais que*

$$|N_d - (q^d + 1)| \leq A + B q^{\frac{d}{2}}$$

para todo $d >> 0$ múltiplo de N.

Demonstração. Suponha que vale a H. R. para $Z(t, C)$. Pela observação 2, obtemos $N = 1, A = 0$ e $B = 2g$.
Reciprocamente, suponha que existem A, B constantes e $N > 0$ inteiro tais que

$$|N_d - (q^d + 1)| \leq A + B q^{\frac{d}{2}}$$

para todo $d >> 0$ múltiplo de N. O item 4 do teorema 1, implica que a H. R. segue para $Z(t, C)$ se, e somente se, segue para $Z(t, C_n)$. Então basta mostrarmos que a H. R. vale em $Z(t, C_n)$. Temos

$$\left|\sum_{j=1}^{2g} \alpha_j^d\right| \leq A + B q^{\frac{d}{2}}$$

para todo $d \geq 1$. Como $\prod_{j=1}^{2g} \alpha_j^d = q^g$, pela observação 1, basta mostrarmos que $|\alpha_j| \leq q^{\frac{1}{2}}$, para todo $j = 1, \ldots, 2g$.
Seja $L(t) = \prod_{j=1}^{2g} (1 - \alpha_j t)$ e considere a série de potências

$$\log\left(\frac{1}{L(t)}\right) = \sum_{d=1}^{\infty} (\alpha_1^d + \cdots + \alpha_{2g}^d) \frac{t^d}{d}.$$

A partir da desigualdade acima, temos

$$\left|\log\left(\frac{1}{L(t)}\right)\right| \leq \sum_{d=1}^{\infty} (A + B q^{\frac{d}{2}}) \frac{|t|^d}{d} \leq$$

$$\leq A \log\left(\frac{1}{1-|t|}\right) + B \log\left(\frac{1}{1-|q^{\frac{1}{2}}t|}\right).$$

Isso garante que $\log\left(\frac{1}{L(t)}\right)$ converge absolutamente, para todo $t \in \mathbb{C}; |t| < q^{\frac{-1}{2}}$. Assim, todas as singularidades de $\log\left(\frac{1}{L(t)}\right)$ encontram-se na região $|t| \geq q^{\frac{-1}{2}}$ do plano complexo, donde os zeros de $L(t)$ satisfazem $\left|\frac{1}{\alpha_j}\right| \geq q^{\frac{-1}{2}}$. □

3. Coberturas de Galois

Agora, seja C_0 uma curva completa, conexa, não-singular, definida e racional sobre $\mathbb{F}_0 \doteq \mathbb{F}_q$, com corpo de funções $\mathbb{K}_0$. Considere $\mathbb{F} \doteq \overline{\mathbb{F}_0}$, $\mathbb{K} \doteq \mathbb{K}_0 \cdot \mathbb{F}$, $\varphi : \mathbb{K} \longrightarrow \mathbb{K}$ dado por $\varphi(f) = f^q$, o mapa de Frobenius e C o modelo não-singular tal que $\mathbb{K}$ é o corpo algébrico de funções associado. Sabemos que existe um elemento $t \in \mathbb{K}$ transcendente sobre $\mathbb{F}$ tal que a extensão $\mathbb{K}|\mathbb{F}(t)$ é separável. Logo, existe uma extensão $\mathbb{K}'$ de $\mathbb{F}(t)$ que é normal com relação à $\mathbb{F}(t)$ e a $\mathbb{K}$, simultaneamente. Isso significa que existe uma curva suave C' com corpo de funções $\mathbb{K}'$ tal que $C' \longrightarrow C \longrightarrow \mathbb{P}^1$ são coberturas de Galois, i.e., $\mathbb{K}'|\mathbb{K}$ e $\mathbb{K}'|\mathbb{F}(t)$ são extensões de Galois. Além disso, tais coberturas são não-ramificadas fora de um conjunto finito de pontos de $\mathbb{P}^1$.
Sejam $G \doteq Aut(C'|\mathbb{P}^1)$ e $H \leq G$ que age trivialmente em C. Como G age sobre qualquer extensão finita de $\mathbb{F}_q$, pelo item 4 do Teorema 1, a Hipótese de Riemann segue para $Z(t, C_0)$ se, e somente se, segue para $Z(t, (C_0)_n)$. Assim, para nossos fins, podemos assumir, sem perda de generalidade, que G age sobre $\mathbb{F}_q$.
Dado $P \in \mathbb{P}^1$ racional sobre $\mathbb{F}$ e não-ramificado em $C' \longrightarrow \mathbb{P}^1$, tome $Q \in C'$ que está sobre P. Então $\varphi(Q) = g \cdot Q$, para algum $g \in G$. Essa substituição é conhecida como **substituição de Frobenius** de G no ponto Q. Considere o número

$$N_1(C', g) \doteq \#\{Q \in C'(\mathbb{F}) | \varphi(Q) = g \cdot Q\}.$$

Os seguintes resultados (cujas demonstrações omitiremos por razões didáticas) são a chave da demonstração da H. R. para um cobertura de Galois sobre um corpo finito (isso é o bastante para provar a H. R. para um curva qualquer sobre um corpo finito, pois o caso geral pode ser reduzido facilmente usando uma cobertura de Galois).

Lema 1. *1.*

$$\sum_{g \in G} N_1(C', g) = |G| N_1(\mathbb{P}^1) + \mathcal{O}(1)$$

onde $\mathcal{O}(1)$ é uma constante que independe de q e

$$N_1(\mathbb{P}^1) \doteq \#\{P \in \mathbb{P}^1 | \varphi(P) = P\}$$

2. (Bombieri) Se $q = p^\alpha > (\mathbf{g} + 1)^4$ e $C \longrightarrow \mathbb{P}^1$ é cobertura de Galois sobre $\mathbb{F}_q$, então

$$N_1(C, g) \leq 1 + q + (2\mathbf{g} + 1) q^{\frac{1}{2}}.$$

4. Prova da H. R. para uma Cobertura de Galois

Finalmente podemos mostrar a H. R. para uma cobertura de Galois. Suponha que $C \longrightarrow \mathbb{P}^1$ é uma cobertura de Galois. Pelo lema de Bombieri, temos a desigualdade

$$N_1(C, g) \leq 1 + q + A + B q^{\frac{1}{2}}$$

e pelo item 1 do lema 1, temos

$$N_1(C, 1) = -\sum_{g \in G \setminus \{1\}} N_1(C, g) + |G| N_1(C) + \mathcal{O}(1) \geq$$

$$\geq -(|G| - 1)(1 + q + A + B q^{\frac{1}{2}}) + |G|(1 + q) + \mathcal{O}(1)$$

e isso ocorre se, e somente se,

$$N_1(C, 1) \geq q + 1 + A' + B' q^{\frac{1}{2}}.$$

Por outro lado, pondo $g = 1$ na desigualdade acima gerada por Bombieri, obtemos

$$N_1(C, 1) \leq A + B q^{\frac{1}{2}}$$

donde

$$|N_1(C, 1) - (q + 1)| \leq A'' + B'' q^{\frac{1}{2}}.$$

Portanto, pela equivalência da proposição 1, a H. R. está provada para uma cobertura de Galois.

5. Referências

[1] MORENO, C. J. - *Algebraic Curves over Finite Fields*, Cambrigde Tracts in Mathematics, 1991;
[2] MACK-CRANE, S. - *The Riemann Hypothesis for Varieties over Finite Fields*, Berkeley, 2015.