1 Primos em uma PA?

O famoso *teorema de Dirichlet*, também conhecido como PCP (=princípio das casas dos primos), diz:

Teorema 1.1 (Dirichlet) *Sejam a e n dois inteiros com $(a, n) = 1$. Então existem infinitos primos na progressão aritmética de termo inicial a e razão n, i.e., existem infinitos primos p com $p \equiv a \pmod n$.*

A prova deste teorema consiste em mostrar a divergência da série

$$\sum_{\substack{p \text{ primo} \\ p \equiv a \pmod n}} \frac{1}{p} \to \infty$$

o que certamente implica a existência de infinitos primos p com $p \equiv a \pmod n$. A idéia geral já pode ser vista no caso pequeno $n = 4$, então é por ele que começamos.

2 Pequeno teorema de Dirichlet

A fim de obter a soma dos recíprocos dos primos $p \equiv 1 \pmod 4$ e $p \equiv 3 \pmod 4$, consideramos para $s > 1$ as funções

$$L_0(s) \overset{\text{df}}{=} \sum_{n \geq 0} \frac{1}{(2n+1)^s} \underset{\text{extenso}}{\overset{\text{por}}{=}} 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \cdots$$

$$L_1(s) \overset{\text{df}}{=} \sum_{n \geq 0} \frac{(-1)^n}{(2n+1)^s} \underset{\text{extenso}}{\overset{\text{por}}{=}} 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - \cdots$$

As duas séries convergem absolutamente para $s > 1$. Quando $s \to 1^+$, temos que $L_0(s) \to \infty$ enquanto que $L_1(s)$ permanece limitado. De agora em diante, deixarei de lado algumas destas questões rotineiras de convergência, que vocês podem checar na sua intimidade, quando ninguém estiver olhando, e que por hora podem ser ignoradas (especialmente se não houver analistas na platéia).

A razão para considerarmos estas duas funções é a seguinte **fatoração euleriana**:

$$L_0(s) = \prod_{\substack{p \neq 2 \\ p \text{ primo}}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right) \underset{\text{da PG}}{\overset{\text{soma}}{=}} \prod_{\substack{p \neq 2 \\ p \text{ primo}}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

De fato, expandindo o produto do termo central, obtemos cada parcela $1/(2n+1)^s$ da soma em $L_0(s)$ exatamente uma vez, já que pela fatoração única cada inteiro ímpar é escrito de maneira única como produto de primos ímpares. Analogamente, como um número ímpar é congruente a 1 módulo 4 se e somente se em sua fatoração a soma de todos os expoentes dos primos $p \equiv 3 \pmod 4$ é par, obtemos a fatoração euleriana:

$$L_1(s) = \prod_{\substack{p \equiv 1 \pmod 4 \\ p \text{ primo}}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right) \cdot \prod_{\substack{p \equiv 3 \pmod 4 \\ p \text{ primo}}} \left(1 - \frac{1}{p^s} + \frac{1}{p^{2s}} - \frac{1}{p^{3s}} + \cdots\right)$$

$$\underset{\text{da PG}}{\overset{\text{soma}}{=}} \prod_{\substack{p \equiv 1 \pmod 4 \\ p \text{ primo}}} \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_{\substack{p \equiv 3 \pmod 4 \\ p \text{ primo}}} \left(1 + \frac{1}{p^s}\right)^{-1}$$

Agora, para "linearizar" as expressões acima, utilizaremos uma ferramenta muito avançada, especialmente desenvolvida para transformar produtos em somas: o logaritmo. Temos

$$\log(1-x)^{-1} = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots \qquad \text{para} \quad |x| < 1$$

e assim

$$\log L_0(s) = \sum_{\substack{p \neq 2 \\ p \text{ primo}}} \sum_{k \geq 1} \frac{1}{k \cdot p^{ks}} = \sum_{\substack{p \neq 2 \\ p \text{ primo}}} \frac{1}{p^s} + \sum_{\substack{p \neq 2 \\ p \text{ primo}}} \sum_{k \geq 2} \frac{1}{k \cdot p^{ks}}$$

Obtemos assim uma expressão com a soma dos recíprocos dos primos ímpares. O outro termo, por outro lado, é limitado pois

$$\sum_{\substack{p \neq 2 \\ p \text{ primo}}} \sum_{k \geq 2} \frac{1}{k \cdot p^{ks}} \leq \sum_{n \geq 2} \sum_{k \geq 2} \frac{1}{n^k} \underset{\text{da PG}}{\overset{\text{soma}}{=}} \sum_{n \geq 2} \frac{1/n^2}{1 - 1/n} = \sum_{n \geq 2} \left(\frac{1}{n-1} - \frac{1}{n}\right) \overset{\text{telescópica}}{=} 1$$

A mesma análise funciona para $L_1(s)$. Resumindo, obtemos

$$\boxed{\begin{aligned} \log L_0(s) &= \sum_{\substack{p\neq 2\\ p \text{ primo}}} \frac{1}{p^s} + (\text{termo limitado}) \\ \log L_1(s) &= \sum_{\substack{p\equiv 1 \pmod 4\\ p \text{ primo}}} \frac{1}{p^s} - \sum_{\substack{p\equiv 3 \pmod 4\\ p \text{ primo}}} \frac{1}{p^s} + (\text{termo limitado}) \end{aligned}}$$

e assim

$$\log L_0(s) + \log L_1(s) = 2 \sum_{\substack{p\equiv 1 \pmod 4\\ p \text{ primo}}} \frac{1}{p^s} + (\text{termo limitado})$$

$$\log L_0(s) - \log L_1(s) = 2 \sum_{\substack{p\equiv 3 \pmod 4\\ p \text{ primo}}} \frac{1}{p^s} + (\text{termo limitado})$$

Mas quando $s \to 1^+$, temos que $L_0(s) \to \infty$ enquanto que $L_1(s) \to 1 - 1/3 + 1/5 - \cdots \neq 0$. Assim, cada uma das somas acima diverge, o que mostra que existem tanto infinitos primos congruentes a 1 como a 3 módulo 4.

3 Marcadores (também conhecidos como caracteres)

Um dos "segredos" da demonstração acima foi a utilização do 1 e do -1 como "marcadores" dos números respectivamente congruentes a 1 e 3 módulo 4. Uma característica marcante destes marcadores é a sua "compatibilidade" com a multiplicação: por exemplo, o produto de dois números congruentes a 3 módulo 4 é um número congruente a 1 módulo 4, o que se traduz na identidade $(-1)(-1) = 1$ de marcadores. Generalizando, temos

Definição 3.1 Seja n um inteiro positivo. Um **caracter** χ módulo n é um morfismo de grupos $\chi\colon (\mathbb{Z}/n)^\times \to \mathbb{C}^\times$. Mais explicitamente: χ pode ser vista como uma função de $\mathbb{Z}$ assumindo valores complexos tal que, para todos $x, y \in \mathbb{Z}$,

1. $\chi(x+n) = \chi(x)$ (χ é periódica módulo n)
2. $\chi(x \cdot y) = \chi(x) \cdot \chi(y)$ (χ é multiplicativa)
3. $\chi(x) = 0 \iff (x, n) \neq 1$ (χ só é interessante para inteiros inversíveis módulo n)

Exemplo 3.2 Para qualquer valor de n temos sempre o **caracter trivial** χ_0 dado por

$$\chi_0(x) = \begin{cases} 1 & \text{se } (x,n) = 1 \\ 0 & \text{caso contrário} \end{cases}$$

Para $n = 4$ temos o caracter da seção anterior

$$\chi(x) = \begin{cases} 0 & \text{se } x \text{ é par} \\ 1 & \text{se } x \equiv 1 \pmod 4 \\ -1 & \text{se } x \equiv 3 \pmod 4 \end{cases}$$

Para $n = 5$, como 2 é uma raiz primitiva módulo 5 (i.e., as potências de 2 geram todos os inteiros módulo 5 não nulos), basta determinar o valor de $\chi(2)$ a fim de determinar o caracter. Podemos tomar, por exemplo, qualquer valor $\chi(2) \in \{\pm 1, \pm i\}$.

Observe que, como um caracter χ é multiplicativo, temos $\chi(1) = 1$. Além disso, pelo teorema de Euler-Fermat,

$$\chi(x)^{\phi(n)} = \chi(x^{\phi(n)}) = \chi(1) = 1$$

para $(x, n) = 1$, ou seja, $\chi(x)$ é uma $\phi(n)$-ésima raiz da unidade. Note ainda que o produto de dois caracteres é também um caracter.

Quando $n = p^\alpha$ é uma potência de um primo, a existência de uma raiz primitiva $g \bmod p^\alpha$ mostra que um caracter χ é determinado por seu valor $\chi(g)$, que pode ser qualquer raiz $\phi(p^\alpha)$-ésima da unidade. Logo existem exatamente $\phi(p^\alpha)$ caracteres distintos módulo p^α.

Exercício 3.1 Mostre que se $x \not\equiv 1 \pmod n$ então existe um caracter ψ tal que $\psi(x) \neq 1$.

Exercício 3.2 Mostre que para qualquer n existem exatamente $\phi(n)$ caracteres distintos módulo n.

Exercício 3.3 Prove que o conjunto de todos os caracteres módulo n é um grupo. Mostre que este grupo é (não canonicamente) isomorfo a $(\mathbb{Z}/n)^\times$, o grupo de unidades de $\mathbb{Z}/n$.

A grande utilidade dos caracteres é a sua incrível capacidade de "filtragem".

Lema 3.3 (Filtrando inteiros módulo n) *Sejam a e n dois inteiros primos entre si. Seja χ_0 o caracter trivial módulo n. Então*

1.
$$\sum_{\chi} \chi(a)^{-1}\chi(x) = \begin{cases} \phi(n) & \text{se } x \equiv a \pmod n \\ 0 & \text{caso contrário} \end{cases}$$

onde a soma percorre todos os caracteres módulo n.

2.
$$\sum_{0 \le x < n} \chi(x) = \begin{cases} \phi(n) & \text{se } \chi = \chi_0 \\ 0 & \text{caso contrário} \end{cases}$$

Prova Como $\chi(a)^{-1}\chi(x) = \chi(xa^{-1})$ e $x \equiv a \iff xa^{-1} \equiv 1$ basta provar o item 1 para $a = 1$. Se $x \equiv 1$ o resultado é trivial, caso contrário pelo exercício 3.1, existe um caracter ψ tal que $\psi(x) \neq 1$. Assim, como a multiplicação por ψ permuta os caracteres, temos

$$\sum_{\chi} \psi(x) \cdot \chi(x) \overset{\text{gira}}{\underset{\text{gira}}{=}} \sum_{\chi} \chi(x) \Rightarrow \big(\psi(x) - 1\big) \cdot \sum_{\chi} \chi(x) = 0 \Rightarrow \sum_{\chi} \chi(x) = 0$$

como queríamos demonstrar. O item 2 fica como exercício. $\square$

Exercício 3.4 Seja $g(x)$ a ordem de x mod n. Mostre que

$$\prod_{\chi} \big(1 - \chi(x) \cdot T\big) = \big(1 - T^{g(x)}\big)^{\phi(n)/g(x)}$$

Agora, após esta digressão característica, voltamos ao teorema de Dirichlet. Para um caracter χ e $s > 1$ definimos

$$L(\chi, s) \overset{\text{df}}{=} \sum_{k \ge 1} \frac{\chi(k)}{k^s} \overset{\text{fatoração}}{\underset{\text{euleriana}}{=}} \prod_{p \text{ primo}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

(a convergência desta série será demonstrada na próxima seção). Novamente temos

$$\log L(\chi, s) \overset{\text{após várias}}{\underset{\text{contas}}{=}} \sum_{p \text{ primo}} \frac{\chi(p)}{p^s} + (\text{termo limitado})$$

Agora basta tomar uma combinação linear destas funções que "filtra" os termos congruentes a a módulo n:

$$\boxed{\sum_{\chi} \chi(a)^{-1} \log L(\chi, s) \overset{\text{lema}}{\underset{3.3}{=}} \phi(n) \cdot \sum_{\substack{p \text{ primo} \\ p \equiv a \pmod n}} \frac{1}{p^s} + (\text{termo limitado})}$$

Finalmente, o teorema segue do seguinte fato: quando $s \to 1^+$, $L(\chi_0, s) \to \infty$, ao passo que $L(\chi, s)$ converge para um número não nulo quando $\chi \neq \chi_0$. A demonstração deste fato é o tópico da próxima seção.

4 O L da questão

Primeiro vamos analisar $L(\chi_0, s)$. Esta função é essencialmente a conhecida função ζ de Riemann:

$$\zeta(s) \overset{\text{df}}{=} \sum_{k \ge 1} \frac{1}{k^s} \overset{\text{fatoração}}{\underset{\text{euleriana}}{=}} \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

De fato, temos

$$L(\chi_0, s) = \prod_{p \text{ prime}} \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \prod_{\substack{p \text{ prime} \\ p \nmid n}} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s) \cdot \prod_{\substack{p \text{ prime} \\ p \mid n}} \left(1 - \frac{1}{p^s}\right)$$

Isto já mostra que $L(\chi_0, s) \to \infty$ quando $s \to 1^+$. Mais precisamente, temos

Lemma 4.1

1. *A função $\zeta(s)$, e portanto a função $L(\chi_0, s)$, pode ser estendida para uma função meromorfa definida em todo o semi-plano $\Re(s) > 0$ com um único pólo em $s = 1$.*
2. *Se $\chi \neq \chi_0$, a série*
$$\sum_{k\geq 1} \frac{\chi(k)}{k^s}$$
converge para $\Re(s) > 0$.

Prova Para estender a função ζ, a idéia é tentar aproximá-la por uma integral:

$$\sum_{k\geq 1} \frac{1}{k^s} = \int_1^\infty \frac{dx}{x^s} + \sum_{k\geq 1}\left(\frac{1}{k^s} - \int_k^{k+1} \frac{dx}{x^s}\right) = \frac{1}{s-1} + \sum_{k\geq 1} \int_k^{k+1} \left(\frac{1}{k^s} - \frac{1}{x^s}\right) dx$$

Cada função $\phi_k(s) \stackrel{\text{df}}{=} \int_k^{k+1} \left(\frac{1}{k^s} - \frac{1}{x^s}\right) dx$ é analítica, e $|\phi_k(s)| \leq \sup_{x\in[k,k+1]} \left|\frac{1}{k^s} - \frac{1}{x^s}\right| \leq |s|/k^{\Re(s)+1}$ (mais um exercício, veja a desigualdade abaixo para uma dica...) e portanto a soma dos $\phi_k(s)$ converge para uma função analítica em $\Re(s) > 0$.

Para mostrar que a soma do item 2 converge, utilizamos o critério de Cauchy e aplicamos o truque da "integração por partes", versão discreta (também conhecida pelos mais hábeis por critério da soma de Abel). Defina $S(k) = \sum_{1\leq j\leq k} \chi(j)$. Observe que pelo lema 3.3 existe uma constante M tal que $|S(k)| \leq M$ para todo k. Assim temos

$$\left|\sum_{k_0\leq k\leq k_1} \frac{\chi(k)}{k^s}\right| = \left|\sum_{k_0\leq k\leq k_1} \frac{S(k) - S(k-1)}{k^s}\right| = \left|\frac{S(k_1)}{(k_1+1)^s} - \frac{S(k_0-1)}{k_0^s} + \sum_{k_0\leq k\leq k_1} S(k)\cdot\left(\frac{1}{k^s} - \frac{1}{(k+1)^s}\right)\right|$$
$$\leq \frac{2M}{k_0^{\Re(s)}} + M\cdot \sum_{k_0\leq k\leq k_1} \int_k^{k+1} |sx^{-s-1}|\, dx \leq \frac{2M}{k_0^{\Re(s)}} + M|s|\cdot \int_{k_0}^{k_1+1} x^{-\Re(s)-1}\, dx \leq \frac{2M}{k_0^{\Re(s)}} + \frac{M|s|}{\Re(s)\cdot k_0^{\Re(s)}}$$

que converge para 0 quando $k_0 \to \infty$. □

Pelo lema acima temos que $L(\chi, 1)$ é finito quando $\chi \neq \chi_0$. Para que $\log L(\chi, 1)$ seja também finito devemos mostrar que $L(\chi, 1) \neq 0$. Para isto, precisaremos do seguinte lema técnico.

Lemma 4.2 *Sejam reais $a_k \geq 0$ tais que*
$$f(s) \stackrel{\text{df}}{=} \sum_{k\geq 1} \frac{a_k}{k^s}$$
convirja para $Re(s) > s_0$. Se $f(s)$ pode ser estendida analiticamente para $Re(s) > s_0 - \epsilon$ para algum $\epsilon > 0$ então a série converge para $Re(s) > s_0 - \epsilon$.

Prova Séries desta forma são chamadas de **séries de Dirichlet**. Séries de Dirichlet possuem **semi-planos** de convergência, assim como séries de potências possuem **raio** de convergência. Este lema é uma versão "invertida" do fato correspondente de que uma série de potências só pára de convergir quando encontra uma singularidade.

Transladando, podemos supor que $s_0 = 0$. Temos que para todo $0 < \eta < \epsilon$, $f(s)$ tem expansão em série de potências convergente para $|s - 1| \leq 1 + \eta$ dada por

$$f(s) = \sum_{j\geq 0} \frac{(s-1)^j}{j!} \cdot f^{(j)}(1)$$

Assim, para $s = -\eta$ temos portanto uma série convergente

$$f(-\eta) = \sum_{j\geq 0} \frac{(-\eta-1)^j}{j!} \cdot \sum_{k\geq 1} \frac{a_k(-\log k)^j}{k} = \sum_{j\geq 0} \frac{(\eta+1)^j}{j!} \cdot \sum_{k\geq 1} \frac{a_k(\log k)^j}{k}$$

Como todos os termos são positivos, sem perda de convergência podemos rearranjá-los obtendo

$$f(-\eta) = \sum_{k\geq 0} \frac{a_k}{k} \sum_{j\geq 0} \frac{\big((\eta+1)\cdot\log k\big)^j}{j!} = \sum_{k\geq 1} \frac{a_k}{k} \exp\big((\eta+1)\cdot\log k\big) = \sum_{k\geq 1} \frac{a_k}{k^{-\eta}}$$

□

Agora definimos a função

$$\boxed{P(s) \stackrel{\text{df}}{=} \prod_{\chi} L(\chi, s) = \prod_{p \text{ primo}} \prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \underset{3.4}{\overset{\text{exercício}}{=}} \prod_{p \text{ primo}} \left(1 - \frac{1}{p^{g(p)s}}\right)^{-\phi(n)/g(p)}}$$

onde, como no exercício, $g(p)$ denota a ordem de $p \bmod n$. Se algum $L(\chi, s)$ tivesse um zero em $s = 1$, como $L(\chi_0, s)$ tem um pólo simples teríamos que $P(s)$ seria analítica em $\Re(s) > 0$. Observe que na série

$$\sum_{n \geq 1} \frac{a_k}{k^s} \stackrel{\text{df}}{=} \prod_{p \text{ primo}} \left(1 + \frac{1}{p^{g(p)s}} + \frac{1}{p^{2g(p)s}} + \cdots\right)^{\phi(n)/g(p)} = P(s)$$

temos $a_k \geq 0$ e portanto pelo lema técnico a série acima converge para $\Re(s) > 0$. Porém este último produto é maior ou igual a

$$\prod_{p \text{ primo}} \left(1 + \frac{1}{p^{\phi(n)s}} + \frac{1}{p^{2\phi(n)s}} + \cdots\right) = \sum_{k \geq 1} \frac{1}{k^{\phi(n) \cdot s}}$$

que diverge para $s = 1/\phi(n)$, contradição. Isto mostra que $L(\chi, 1) \neq 0$ para $\chi \neq \chi_0$ e completa a demonstração do teorema de Dirichlet.

5 Referências

Para aprender mais sobre o teorema de Dirichlet e suas aplicações e generalizações (como o teorema de Chebotarev), eis uma lista com referências úteis.

1. H. Iwaniec, E. Kowalski, *Analytic Number Theory*, AMS.
2. S. Lang, *Algebraic Number Theory*, Addison-Wesley.
3. J. Neukirch, *Algebraic Number Theory*, Springer-Verlag.
4. J.-P. Serre, *A Course in Arithmetic*, GTM 7, Springer-Verlag.