U Positivo - UTFPR - PUCPr – 11/02/2019 - 12:33:56,9
Prof Dr P Kantek (pkantek@gmail.com)
Números Primos VIVO160a, V: 1,05 1 - 1

_____ / _____ / _____

Números Primos

Numa manhã de agosto de 1900, David Hilbert da Universidade de Göttingen foi fazer sua aguardada palestra no Congresso Internacional de Matemáticos na Sorbonne em Paris. Ele era um dos maiores matemáticos do mundo e havia preparado uma palestra ousada. Ao invés de falar do passado ou do presente, resolveu falar do futuro. Mostraria o desconhecido e não o que ja fora provado. Para anunciar o novo século desafiou a platéia com 23 problemas que segundo ele ditariam o rumo da *rainha das ciências* durante o século XX. Durante as décadas seguintes encontraram-se as respostas para muitos desses problemas. A propósito, a resposta ao décimo problema de Hilbert: *haverá um algoritmo capaz de decidir se uma equação diofantina tem ou não solução*, solucionado de forma independente por Alonso Church (cálculo λ) e por Alan Turing (Máquina Universal de Turing) ambos em 1936. Tangencialmente este último trabalho deu origem ao computador.

Voltando aos problemas de Hilbert, o oitavo, pedia a comprovação da Hipótese de Riemann, mas para poder trabalhar nela, precisa-se de alguma preparação.

Número Primo

Define-se um inteiro primo como aquele número que só tem 2 divisores inteiros: a unidade e o próprio número. Por exemplo, 5 é primo (divisores: 1 e 5) enquanto 6 não é primo, também chamado composto, (já que seus divisores são 1, 2, 3 e 6). Algumas curiosidades:

- O número 1 não é nem primo nem composto.
- 2 é o único par que também é primo. Todos os demais pares são divisíveis também por 2, logo compostos.
- O universo de divisores de n sempre existe em pares, cujo produto é igual ao número n.
- Se n é quadrado perfeito, sua raiz deve ser contada duas vezes para formar o par. Por exemplo, os divisores de 100 são: 1, 2, 4, 5, 10, 20, 25, 50 e 100. Neste caso, o 10 deve ser contado duas vezes.

Serão infinitos os primos ?

Eis uma demonstração do fato, devida a Euclides (há várias outras demonstrações). Quer-se provar o Teorema que diz que os primos são infinitos. A demonstração é por *redução ao absurdo*. Então, suponhamos que existem r números primos apenas, a saber: p_1, p_2,...,p_r. Façamos o conjunto $P = \{p_1, p_2, ..., p_r\}$. Imagine o número N, definido por $N = p_1 \times p_2 \times ... \times p_r$, obviamente composto. Agora, faça $M = N+1$. De cara, M não é divisível por nenhum $p \in P$ pois o resto desta divisão é sempre 1. Agora vamos especular sobre a natureza de M. Ele pode ser primo ou composto. Se for primo, achamos uma contradição (o "último" primo era r) e está demonstrado o teorema original. Se for composto, então existe um primo p que não pertence ao conjunto P, pois se pertencesse, ele dividiria N e também M e ao fazê-lo, deveria também dividir a diferença $M - N$ que como se sabe vale 1. Mas, não existe um primo que divida 1. Então, achou-se um novo primo p que não pertence a P, uma contradição o que demonstra o teorema original.

Distribuição dos números primos

Os primos são infinitos, embora eles venham se tornando mais raros à medida em que cresce o limite superior da contagem. Por exemplo, entre 1 e 10 há 4 primos (40%), entre 1 e 100, há 25 (25%), entre 1 e 1000, há 168 (16%), entre 1 e 10.000, há 1.229 (12%), entre 1 e 100.000 há 9.529 (9%) e assim por diante. A primeira descoberta na tentativa de entender a distribuição dos primos veio de Gauss, quando ele afirmou que o número de primos entre 1 e N é aproximadamente igual a

$$\frac{N}{\log_e(N)}$$

O número real é um pouco menor do que isso.

A próxima etapa é o surgimento da função zeta, originalmente proposta nos tempos de Euler, cuja definição é

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + ... \frac{1}{n^x} + ...$$

A origem do interesse dos matemáticos por esta soma infinita veio da música e tem origem numa descoberta dos gregos (Pitágoras) associando as oitavas da escala musical aos números 1, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$,...

Os matemáticos sabem há muito tempo que ao substituir $x = 1$ na função ζ, o resultado da soma, embora converja muito lentamente, tende a ∞. Números menores que 1, sempre convergem, eventualmente mais rapidamente, para infinito.

Euler, um dos maiores (senão o maior) torturadores de números da história resolveu estudar o que aconteceria se $x = 2$ na função ζ. A função fica

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + ...$$

e agora este número é menor, pois não inclui todas as parcelas de antes. A melhor estimativa era de $\frac{8}{5}$, mas Euler, *num dos cálculos mais intrigantes de toda a matemática (Satoy, 2004)* chegou a

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + ... = \frac{1}{6}\pi^2$$

Depois disso, Euler lembrou da descoberta grega de que qualquer número pode ser expresso como um produto de primos, e reescreveu ζ de outra maneira. Antes, veja-se a base do raciocínio $60 = 2 \times 2 \times 3 \times 5$ e daqui $\frac{1}{60} = \frac{1}{2} \times \frac{1}{2} \times \frac{1}{3} \times \frac{1}{5} \times = (\frac{1}{2})^2 \times \frac{1}{3} \times \frac{1}{5}$ e agora

$$\zeta(x) = (1 + \frac{1}{2^x} + \frac{1}{4^x} + ...) \times (1 + \frac{1}{3^x} + \frac{1}{9^x} + ...) \times$$

$$... \times (1 + \frac{1}{p^x} + \frac{1}{(p^2)^x} + ...) \times ...$$

Os gregos já haviam provado há 2000 anos que os números primos eram infinitos, mas a expressão acima apresentava nova prova do mesmo fato. Estamos por volta de 1850 em Göttingen, quando Dirichlet foi trabalhar lá, entusiasmado com a função ζ. Lá já estava um aluno de Gauss, Riemann por sua vez entusiasmado com os números complexos de Cauchy. O pulo do gato agora foi dado por Riemann que foi introduzir números imaginários na função ζ. Recém eleito para a Academia de Berlim, Riemann aproveitou o costume (novos associados deveriam apresentar um relato de suas pesquisas recentes) e em novembro de 1859 ele apresentou um artigo de 10 páginas sobre os números primos. Aqui Riemann herdou de seu professor Gauss (*pauca sed madura*) o costume de ao apresentar um bela construção retirar antes todos os andaimes e ferramentas usadas na construção. Quase perdido no texto está declarado o problema cuja solução hoje possui uma etiqueta de 1.000.000 de dólares: a hipótese de Riemann. Junto uma observação: *É claro que gostaríamos de ter uma prova rigorosa, mas deixei de lado essa busca após breves tentativas fracassadas, pois ela não é necessária para o objetivo imediato de minha investigação*. O principal objetivo do artigo em Berlim era confirmar que a função de Gauss fornecia uma aproximação cada vez melhor do número de primos à medida em que se atinge contagens cada vez mais elevadas. A recompensa por este artigo foi a cadeira universitária que Gauss havia ocupado e que a morte de Dirichlet deixara vaga.

Baseado no trabalho de Cauchy (funções podem ser representadas por equações) e estas desenhadas em um gráfico ele estudou o gráfico da função ζ. O problema aqui é que os reais usam um eixo e a função o outro. Ao passar para complexos (que exigem 2 eixos para o número) são necessários 4 eixos: 2 para o número e mais dois para a função. A chave para pensar neste mundo é pensar na sombra: ela é a imagem bidimensional de algo que tem 3 dimensões. Em alguns ângulos ela fornece informação pobre, mas em outros isso muda: ao olhar o perfil de alguém eventualmente pode-se reconhecê-lo.

Hipótese de Riemann

No artigo de 1859, Riemann obteve a fórmula (exata) para $\pi(x)$, na qual aparecem 2 parcelas: primeiro uma excelente estimativa para $\pi(x)$ e depois uma subtração do erro cometido através de uma parcela de correção. Esta correção exige saber onde estão os zeros da equação ζ. Há dois tipos de zeros: os triviais e os não triviais. Se $\Re(s) > 1$ então $\zeta(x) \neq 0$, isto é não há raizes nessa porção do plano complexo. Se $\Re(s) < 0$, a própria equação dá os zeros triviais. A afirmação de Riemann, feita em 1859 e que hoje vale 1 milhão de dólares diz que todos os zeros da função ζ se encontram sobre a reta $\Re(s) = \frac{1}{2}$. A validade deste resultado implica que não há surpresas no comportamento da sequência de primos, isto é que os primos têm padrão de regularidade e que não há surpresas lá adiante, onde a vista não alcança. Uma consequência prática importante deste estudo é a garantia de integridade do método RSA de criptografia na Internet.

Função Möebius É uma função cuja imagem comporta apenas 3 valores: 0, -1 e 1, a depender da seguinte regra. $\mu(n) = 0$ se n tem como divisor outro natural ao quadrado. Senão, $\mu(n) = 1$ se n é decomposto em uma quantidade par de primos e $\mu(n) = -1$ se n é decomposto em quantidade impar de primos.

Função Totiente de Euler É uma função, denotada $\phi(n)$ que conta a quantidade de números x, tais que $x \leq n$ e que são co-primos em relação a n (Ou seja, o $mdc(x, n) = 1$). Conhecida também como função tociente.

Exemplo

Seja o seguinte enunciado
1. Ache o maior fator primo de 1.894.383 (R=210.487).
2. Ache o k-ésimo número primo. k=137.255 (R=1.831.187).
3. Ache o primo anterior a 1.618.439 (R=1.618.433).
4. Teste de primalidade. Informe 0=não e 1=sim se 1.431.559 for primo (R=0).
5. Quantos primos p há, tal que $p \leq 947.085$? (R=74.702).
6. Ache a função contador de divisores de 18.387 (R=10).
7. Ache a função soma de divisores de 14.396 (R=26.040).
8. Ache a função de Möebius de 10.616 (R=0).
9. Ache a função totiente de Euler de 14.971 (R=13.600).

☞ Para você fazer

1. Ache o maior fator primo de 1.731.654	
2. Ache o k-ésimo número primo. k= 139.577	
3. Ache o primo anterior a 1.915.091	
4. Teste de primalidade: Informe 0=não e 1=sim se 1.914.593 for primo	
5. Quantos primos p há, tal que $p \leq 1.435.561$?	
6. Ache a função contador de divisores de 12.888	
7. Ache a função soma de divisores de 12.604	
8. Ache a função de Möebius de 10.420	
9. Ache a função totiente de Euler de 13.692	