O Mistério dos Números Primos

Aspirante Anderson Silva Prata

Os números primos, 2,3,5,7,11,13,17,19,23,29,..., consistem em um mistério secular, porque se apresentam aparentemente sem critério algum. Os mais brilhantes da história da matemática estudaram os primos e, por isso, grandes avanços ocorreram. Riemann, por exemplo, ao conjecturar sobre os zeros da função zeta, provocou uma série de estudos que engrandeceu a Teoria Analítica dos Números e que atualmente se aplica no avanço da ciência da computação.

A encriptação de dados, que garante a segurança da internet, por mais estranho que possa parecer, depende dos números primos. No entanto, mais do que mera abstração matemática, os primos regem os mais eficientes sistemas de segurança. Resumidamente, isso ocorre porque, com os algoritmos disponíveis para fatorar um número, o tempo que se levaria para decodificar chaves seria impraticável devido ao crescimento exponencial de processamento que constitui tais algoritmos.

Podemos dizer que três pesquisadores indianos do Instituto Indiano de Tecnologia de Kanpur, liderados por Manindra, tiveram função relevante nesta corrida. Eles conseguiram um método simples de dizer se um número é ou não primo. Mas o trabalho deles consiste de um método probabilístico(com 99,99% de chance de acerto); além disso, não há implicação na segurança dos computadores, porque não verifica os divisores de um número e um método probabilístico de dizer se um número é ou não primo já existia.

Encontrar um algoritmo que forneça os divisores de um número em tempo hábil e definir uma lógica para a seqüência dos primos é uma tarefa hercúlea e, se conquistado pode ter conseqüências que vão da segurança de computadores até as teorias sobre a origem do Universo.

Vamos aqui fazer uma pequena abordagem de uma solução para o mistério dos números primos.

Idéia principal Idéia principal

A idéia principal consiste em analisar a relação entre a soma, S, e a diferença, D, de dois fatores, f1, f2, com o número não primo N=f1xf2. Isto é, estudaremos os números não primos, porque, se soubermos a seqüência dos números compostos, estaremos obtendo a seqüência dos primos e, além disso, estaremos produzindo uma lógica para fatorar números.

Podemos obter, através de determinados S e D, os possíveis valores de N.

Sendo 1<f1<f2 (se N=1xf2, obviamente, f2=N e não obtemos necessariamente um número não primo).

Através de um desenrolar de equações podemos chegar ao seguinte resultado:

Corolário: **Dado o valor de S = 2k, a diferença máxima entre os divisores de N é 2k - 4 , D = 0, 2, 4, 6 , ..., 2k - 4 , resolvendo os diversos sistemas que satisfazem à condição de D e S, encontramos os seguintes valores de N correspondentes:**

S = 6
D = 0,2 Þ N = 9,8
S= 8
D = 0, 2, 4,6 Þ N = 16,15,12
S= 10
D = 0,2,4,6 Þ N = 25,24,21,16
(...)

Note então que há uma lógica de progressão para todos os valores de S e D, assim todos os compostos ímpares estarão no conjunto solução dos valores de N.

Após um algebrismo não muito difícil, conseguimos eliminar os valores pares de N que fornece a seguinte tabela:

9				
15				
25	21			
35	27			
49	45	33		
63	55	39		
81	77	65	45	
99	91	75	51	
121	117	105	85	57
143	135	119	95	63
(...)				

Donde estão mergulhados todos os números compostos ímpares e não há nenhum número primo. Obviamente que existe uma lógica para a construção da tabela.

A tabela que consiste de todos os ímpares compostos e alguns pares (que são da forma 0mod4) é a seguinte

MATRIZ DE PRATA

8							
15	12						
24	21	16					
35	32	27	20				
48	45	40	33	24			
63	60	55	48	39	28		
80	77	72	65	56	45	32	
99	96	91	84	75	64	51	36
120	117	112	105	96	85	72	57
143	140	135	128	119	108	95	80
168	165	160	153	144	133	120	105
195	192	187	180	171	160	147	132
224	221	216	209	200	189	176	161
255	252	247	240	231	220	207	192
288	285	280	273	264	253	240	225
323	320	315	308	299	288	275	260
360	357	352	345	336	325	312	297
399	396	391	384	375	364	351	336
440	437	432	425	416	405	392	377
483	480	475	468	459	448	435	420
528	525	520	513	504	493	480	465
575	572	567	560	551	540	527	512

Propriedades

1) Quando N é composto de apenas dois fatores primos em potência de 1, então N só tem uma soma, aparece apenas uma vez na matriz; caso contrário, teremos diferentes somas para f1 e f2, N se repete na matriz. Esta propriedade pode ser aplicada à conjectura de Goldbach.

2) Um número primo nunca aparece na matriz.

Teorema da composição

Teorema : Dada a matriz de prata donde os valores de N = f2 f1 , disposta em ordem crescente, de cima para baixo, em relação a f1 + f2 ; e chamando de l e c , a linha e coluna, respectivamente desta tabela, então l + c + 2 e l - c + 2 correspondem aos valores de f1 e f2.

O mais interessante é que para fatorar N a partir deste teorema, não precisamos escrever toda a matriz, até porque seria impraticável. Existe, porém, um método que acha N muito rapidamente.

A seqüência dos primos

Ordenando os números da matriz em que só aparecem os ímpares, obtemos os compostos ímpares e, consequentemente, a série dos primos é obtida. Nós conseguimos um jeito muito rápido de determinar isso.

Para se ter mais ou menos uma idéia da aparente mágica, tome os seguintes valores:

11
11001000
1100100001000000
110010000100000010000000
11001000010000001000000001000000000000
(...)

Agora, some os elementos da n-ésima linha à(n+1)-ésima linha, a partir do primeiro elemento mais à direita desta linha, na seguinte forma: 1+0 =1,1+1=1 e 0+0=0. Assim:

A primeira linha, 11, somada á segunda, 11001000, será igual á 11001011.

A segunda linha, agora, igual a 1100101, somada à terceira,1100100001000000, será 1100100011001011.

Na próxima etapa, analogamente, obtemos a quarta linha igual a 11001000011100101011001011.

Sucessivamente, quando obtivemos a n-ésima linha L, através da soma anterior feita, teremos que nos 3(L-1) primeiros elementos, da direita para esquerda, estão determinados todos os primos da forma 1mod4 e que são maiores que 17.

Você os consegue fazendo 17 + 4k , donde k é o n-ésimo 0, da direita para esquerda, da linha obtida, k< 3(L-1).

Assim, por exemplo:

Para L=2, 1001001011, k< 3, k Î {1,2}, não há zero neste intervalo, note que 17+4x1, 21, e 17+4x2, 25, são compostos.

Para L=3, 1100111001011, k<6, k Î {1, 2, 3, 4, 5}, o terceiro e quinto elementos são zeros, portanto, 17+4x3, 29, e 17+4x5, 37, são primos da forma 1mod4. Note que o quarto elemento que é 1, é o composto 17+4x4, 33.

Para L=4,11001000011100101011001011, analogamente, obtemos os primos 17+4x3, 29; 17+4x5,37;17+4x6,41;17+4x9,53.

(...)

E os primos da forma 3mod4? Pode-se obtê-los com a mesma simplicidade dos obtidos anteriormente e fica como exercício para o leitor.

Ressaltamos que aqui temos uma abordagem simples da solução. Existe um método, por simetria, em que as linhas são obtidas através de uma única soma, além de podermos escolher o intervalo dos números naturais