Damer Tufaile

Engenheiro Civil pela Escola de Engenharia da Universidade Mackenzie

Algoritmo Hiperbólico Parcialmente Eliminado de Falsos Primos

Resumo

Baseado em dois artigos anteriores de nossa autoria "**Goldbach** – ***A conjectura que virou corolário***" (1) e "***A ciência de eliminar falsos primos***" (2), apresentamos um exemplo de decomposição numérica feita através do algoritmo hiperbólico parcialmente eliminado de falsos primos e elaborado com auxílio de planilhas Excell. Na sequência introduzimos a noção de **sinalizadores** e **balizadores** e mostramos, através de um exemplo, a possibilidade de **multiuso** das séries numéricas parcialmente eliminadas de falsos primos nos cálculos de decomposição de números inteiros.

1 Introdução

Vimos em artigos anteriores (1) e (2) que a função, dita hiperbólica, C=x*z pode ser utilizada para testar a primalidade ou executar a decomposição de um número inteiro qualquer. Nesta equação C é uma constante igual ao produto de dois números inteiros x e z, primos ou não, onde x é menor ou igual a z. No caso do número ter terminação par ou 5 deve-se dividi-lo previamente pelos fatores primos 2 e 5, quantas vezes forem necessárias, até que resulte num novo número C constante terminado em 1, 3, 7 ou 9. Os fatores primos 2 e 5, porventura existentes, devem ser arquivados e posteriormente resgatados para compor os fatores primos do número a ser decomposto. A partir daí, o teste de primalidade ou a execução da decomposição do número passa a ser feita com o auxílio do algoritmo hiperbólico. Explicita-se z=C/x e utiliza-se para valores da variável x a série numérica 1, 3,7, 9, 11.... $C^{1/2}$ (onde $C^{1/2}$ corresponde ao valor máximo que a variável z pode assumir) até se obter um valor inteiro de z ou não, caso C seja um número primo. Por sua vez, os valores de x e z assim obtidos devem ser testados quanto à primalidade até se obter ao fim da sequência de cálculos um conjunto formado somente por números primos.

O algoritmo hiperbólico parcialmente eliminado de falsos primos funciona de forma similar ao algoritmo hiperbólico, porem, ao invés de utilizar a série numérica 1, 3, 7, 9, 11..... $C^{1/2}$, lança mão de séries numéricas das quais se eliminaram parcialmente os falsos primos de primos menores ou igual a um primo limite previamente escolhido.

Adotamos como **sigla** deste algoritmo as iniciais das palavras que o descreve, isto é, AHPEFP - **A**lgoritmo **H**iperbólico **P**arcialmente **E**liminado de **F**alsos **P**rimos.

2 Exemplo numérico de decomposição de um número inteiro pelo algoritmo AHPEFP

7	
11	
13	2
17	4
19	2
23	4
29	6
31	2
37	6
41	4
43	2
47	4
53	6
59	6
61	2
67	6
71	4
73	2
79	6
83	4
89	6
97	8
101	4
103	2
107	4
109	2
113	4
121	8
127	6
131	4
137	6
139	2
143	4
149	6
151	2
157	6
163	6
167	4
169	2
173	4
179	6
181	2
187	6
191	4
193	2
197	4
199	2
209	10
211	2
221	10

Tabela 1

1 - Primo limite = p_{llm}	6 - Somatória dos termos contidos num ciclo igual a $S_{tc} = n_{plim}!$
3	6
5	30
7	210
11	2.310
13	30.030
17	510.510
19	**9.699.690**
23	**223.092.870**
29	**6.469.693.230**
31	**200.560.490.130**
37	**7.420.738.134.810**

Tabela 2

O exemplo dado a seguir tem a finalidade de familiarizar o leitor com as rotinas de cálculo utilizadas no algoritmo AHPEFP. Para tanto lançamos mão de planilhas Excell que permitem uma clara visualização e melhor compreensão das operações. Seja decompor o número 4667930.

São dados: P_{lim}=7; $SNPEFP_7$ (ver tabela 1).

Stc = Somatório dos termos contidos num ciclo =210 (ver tabela 2)

Lista de primos (exceto 2 e 5) até p_{lim}.... 3 e 7

Elemento inicial da $SPFP_{lim7}$=Ei= 11

1º passo: Verificar se o número a ser decomposto tem terminação par ou 5.

O número tem terminação par, portanto, dividimo-lo primeiramente por 2:

4667930 / 2 = 2333965. O número remanescente tem terminação 5, da mesma forma dividimo-lo por 5, donde obtemos 2333965 / 5 = 466793. Antes de prosseguir, arquivamos estes dois primeiros fatores primos obtidos (2 e 5) e verificamos ainda se o número remanescente obtido (novo valor constante de C) é divisível pelos números que constituem a lista dos primos menores ou igual ao primo limite (no caso, primos 3 e 7). Então, fazendo a divisão de 466793 por 3 e 7, obtemos respectivamente 15559,67 e 65684,71, valores que não são inteiros. Como o número remanescente obtido tem terminação impar diferente de 5 o teste de decomposição ou de primalidade passa a ser **regido** pelo AHPEFP que neste exemplo utiliza a $SNPEFP_{7.}$

2º passo: Calculo do valor máximo da variável x.

O cálculo de x_{max} é feito para delimitar o intervalo de variação da variável x. Fazendo C=466793 calculamos $x_{max} = C^{1/2} = 683,225$.

Os cálculos são feitos a partir da divisão de C por Ei = 11, sendo que os demais divisores da variável x são obtidos pela soma sucessiva e acumulada dos termos da $SNPEFP_7$ a Ei=11(ver Tabela 1 onde na 1ª coluna se localizam os elementos da $SPFP_7$ e na 2ª coluna os termos da $SNPEFP_7$). A sequência de cálculo prossegue num looping contínuo até que uma das duas condições pré-estabelecidas no roteiro de cálculo sejam satisfeitas. A **primeira condição** para interrupção implica em se obter um valor de x inteiro e a **segunda** em atingir-se um valor da variável x, não inteiro, maior que x_{max}. Caso ocorra a 2ª condição a conclusão é a de que C é um número primo. A tabela 3 apresenta na 1ª coluna a ordem da sequência de cálculos onde se observa a existência de 130 operações até se obter o valor inteiro de x = 577. Em consequência o outro inteiro vale z =488793 / 577 = 809. A 2ª coluna contem os valores da variável x que são obtidos a partir do 1º elemento Ei =11 ao qual se soma sucessiva e cumulativamente os termos da $SNPEFP_7$. A 3ª coluna contem os termos da $SNPEFP_7$. A 4ª coluna contem os valores calculados de z.

		C=	466793
Ordem dos cálculos	x	$SNPEFP_7$	z=C/x
	11		42435,73
1	13	2	35907,15
2	17	4	27458,41
3	19	2	24568,05
4	23	4	20295,35
5	29	6	16096,31
6	**31**	2	15057,84
7	37	6	12616,03
8	41	4	11385,2
9	43	2	10855,65
10	47	4	9931,766
.	.	.	.
.	.	.	.
40	181	2	2578,967
41	187	6	2496,219
42	191	4	2443,942
43	193	2	2418,617
44	197	4	2369,508
45	199	2	2345,693
46	209	10	2233,459
47	211	2	2212,289
48	221	10	2112,186
49	223	2	2093,242
50	227	4	2056,357
51	229	2	2038,397
52	233	4	2003,403
53	239	6	1953,109
54	241	2	1936,9
55	247	6	1889,85
56	251	4	1859,733
57	253	2	1845,032
58	257	4	1816,315
59	263	6	1774,878
60	269	6	1735,29
.	.	.	.
.	.	.	.
90	401	4	1164,072
91	403	2	1158,295
92	407	4	1146,912
93	409	2	1141,303
94	419	10	1114,064
95	421	2	1108,772
96	431	10	1083,046
97	433	2	1078,044
98	437	4	1068,176
99	439	2	1063,31
100	443	4	1053,709
101	449	6	1039,628
102	451	2	1035,018
103	457	6	1021,429
104	461	4	1012,566
105	463	2	1008,192
.	.	.	.
.	.	.	.
125	557	6	838,0485
126	559	2	835,0501
127	563	4	829,1172
128	569	6	820,3743
129	571	2	817,5009
130	577	6	809

Tabela 3

Ordem dos		C_1=	809
Cálculos	x	$SNPEFP_7$	z=C/x
1	11		73,54545
2	13	2	62,23077
3	17	4	47,58824
4	19	2	42,57895
5	23	4	35,17391
6	29	6	27,89655

Tabela 4

Ordem dos		C_2=	577
Cálculos	x	$SNPEFP_7$	z=C/x
1	11		73,54545
2	13	2	62,23077
3	17	4	47,58824
4	19	2	42,57895
5	23	4	35,17391
6	29	6	27,89655

Tabela 5

Observe que foi executado dois loopings completos (x variando de 13 a 221 e 223 a 431). O 3º looping (x variando de 433 a 577) foi interrompido quando resultaram valores inteiros para x=577 e z=809.

3º passo: Verificação da primalidade dos dois números obtidos

Fazendo $C_1 = 809$ calculamos $x_{max}=(C_1)^{1/2} =(809)^{1/2} = 28,44$. .

De forma similar aos cálculos feitos na tabela 3 montamos a tabela 4 onde após 6 verificações nas quais nenhum dos valores calculados para z resultou em inteiro e onde obtemos z = 27,896 para x = 29 valor que é maior que $x_{max}= 28,44$, donde se conclui que 809 é um número primo.

Finalmente, testamos $C_2 = 577$, calculamos $x_{max}=(C_2)^{1/2} = (577)^{1/2} = 24,021$. Montamos a tabela 5 onde após 6 verificações nas quais nenhum dos valores calculados para z resultou em inteiro tem-se para x=29 z=19,89655. Como $x_{max}=24,021$ é menor que x=29 conclui-se que $C_2=577$ também é um número primo.

Concluindo, o número 4667930 tem os seguintes fatores primos: 2, 5, 577 e 809.

3 Multiuso do algoritmo AHPEFP

Não bastasse a possibilidade de adequar o uso do algoritmo AHPEFP à magnitude do número a ser decomposto ele também permite, devido à periodicidade das SNPEFPs, o **fracionamento** das verificações utilizando uma única série numérica conveniente escolhida. Basta que tenhamos para a série escolhida, além dos dados usuais, o que denominamos de **sinalizadores** e **balizadores** de uma $SPFP_{plim}$, isto é, os conjuntos parciais, respectivamente, dos **elementos** de uma dada $SPFP_{lim}$ que **antecedem** e **sucedem** o início de cada ciclo da série numérica escolhida. Devido ao caráter aleatório da busca, este fracionamento teria a eventual probabilidade de diminuir o tempo gasto para resolver o problema utilizando dois ou mais processadores que trabalhariam simultaneamente (em paralelo).

Para fixar ideia vejamos através de um exemplo numérico como seria possível fazer este fracionamento. Suponhamos, utilizando a $SNPEFP_{13}$, que quiséssemos fracionar os cálculos para decompor o número C = 90999979969, já devidamente expurgado dos múltiplos de 2, 3, 5, 7, ...p_{lim13}.

São dados: $SNPEFP_{13}$; elemento inicial da $SPFP_{13}$ Ei=17; Somatório dos termos de um ciclo=30030; sinalizadores e balizadores que podem ser obtidos conforme tabela 6 da seguinte maneira:

Sinalizadores: somando cumulativa e sucessivamente a Ei=17 o somatório dos termos contidos num ciclo, igual a 30030.

Balizadores: somando a cada um dos sinalizadores o 1º termo da $SNPEFP_{13}$=4.

Somatório dos termos da $SNPEFP_{13}$	Sinalizadores	Balizadores
.	17	.
30030	30047	30051
30030	60077	60081
30030	90107	90111
30030	120137	120141
30030	150167	150171
30030	180197	180201
30030	210227	210231
30030	240257	240261
30030	270287	270291
30030	300317	300321
C^1/2	301662,0294	.

Tabela 6

Calculamos o valor máximo que a variável x pode atingir, isto é,

$C^{1/2}$ = (90999979969)½ =301662,0294 e o número de ciclos ou a quantidade de vezes que $C^{1/2}$ contém a somatória dos termos: 301662,0294/30030 = 10,04536. A partir daí, obtemos os sinalizadores e balizadores dos 11 ciclos em que é possível fracionar os cálculos conforme se indica na tabela 6.

O número de processadores seria no mínimo 2 e no máximo11 a depender da escolha dos intervalos de variação de x. Vejamos como seria o fracionamento caso optássemos por 11 processadores. O 1º processador testaria os valores de x variando entre o 1º e o 2º sinalizadores, isto é, entre 17 e 30047. O 2º processador testaria os valores de x variando entre o 1º balizador e o 3º sinalizador, isto é, entre 30051 e 60077 e assim por diante até o 11º processador com os valores de x variando entre o 11º balizador e $C^{1/2}$, isto é, entre 330351 e 301662,0294. Um destes processadores seria programado para coordenar os demais. Os cálculos prosseguiriam até que se encontrasse x inteiro. Caso nenhum dos processadores encontre x inteiro isto significaria que o número testado é primo. No caso de se encontrar x e z inteiros estes devem ser testados quanto à primalidade e assim por diante.

4 Comentários relacionados com o desempenho do algoritmo AHPEFP

Teoricamente não existe limite para utilização do AHPEFP. Praticamente este limite depende do estado da arte da criação de dispositivos não só capazes de armazenar enormes quantidades de termos de SNPEFPs, mas também de processadores de alto desempenho.

Temos para nós que este tipo de questão deve ser analisado e debatido, em momento oportuno, por profissionais especializados em Ciência da Computação.

Entretanto, isto não impede que façamos breves comentários relacionados com a experiência de elaborar o software DNI (Decomposição de Números Inteiros).

O software DNI roda on line num servidor (ambiente compartilhado), atualmente na Locaweb, e usa linguagem de programação Asp. Net 4.0. Nos testes foram utilizadas SNPEFPs com p_{lim} variando entre 3 e 17. A que melhor se adaptou ao software DNI foi a do primo 11 que possui 480 termos, os quais puderam ser incorporados na estrutura do programa fonte. As SNPEFPs 13 e 17, por não caberem na estrutura do programa fonte, foram armazenadas nos arquivos do servidor o que implicou, ao se utilizá-las no 1º cálculo, num delay da ordem de um décimo de segundo o que corresponde ao tempo gasto para trazer a SNPEFP armazenada para ser processada pelo software.

O desempenho do AHPEFP, quando utilizado de forma isolada com a $SNPEFP_{11}$, nas condições mais desfavoráveis (números primos da ordem de 15 dígitos) apresentou valores de tempo cerca de 3 vezes superiores aos obtidos quando se realiza os mesmos cálculos pelo software DECO.

Explica-se a razão desta diferença: o software DECO utiliza dois algoritmos: o Hiperbólico (usa parcialmente a série 1, 3, 7, 9, 11... $C_{1/2}$) e o Circular (usa parcialmente diâmetros pares variando de 20 em 20 ou de 100 em 100) onde trabalham de forma colaborativa em termos de rapidez dentro de intervalos numéricos complementares. Também devemos ter presente que, dependendo do p_{lim} e da SNPEFP escolhidas, quando se usa exclusivamente o algoritmo AHPEFP, a lentidão nos cálculos, em menor escala, pode se manifestar.

Vale lembrar: ainda que se tenha uma boa margem de ganho na quantidade de cálculo, o número de primos e falsos primos ainda podem ser relativamente elevados. O software DNI decompõe qualquer número de até 15 dígitos num intervalo de tempo variando entre aproximadamente zero e um segundo o que julgamos satisfatório. Se tentarmos efetuar a mesma decomposição seguidas vezes, de um mesmo número pelo software DNI, dependendo das tarefas que o servidor estará realizando simultaneamente, a tela de dados de **output** fornecerá, em geral, diferentes valores de tempo de processamento enquanto que a quantidade de cálculos efetuados permanece invariável.

Ao final do próximo artigo versando sobre **Algoritmo Circular** apresentaremos um estudo preliminar que permitirá entrever a possibilidade de elaborar um algoritmo **híbrido** composto dos algoritmos AHPEFP e Circular.

5 Bibliografia

(1) **Tufaile**, Damer " A conjectura que virou corolário" Acesse o artigo pelo blog DNI

(2) **Tufaile**, Damer "Como eliminar falsos primos" Acesse o artigo pelo blog DNI