Damer Tufaile

Engenheiro Civil pela Escola de Engenharia da Universidade Mackenzie

Algoritmo Circular

Resumo

Baseado em três artigos anteriores de nossa autoria apresentamos os conceitos de terminações numéricas unitárias e decenárias e suas relações com as terminações diametrais que permitem um ganho substancial na diminuição da quantidade de cálculo relativa à decomposição de números inteiros. Na sequência apresentamos um estudo referente à invariância dos incrementos diametrais r, um exemplo numérico de decomposição pelo algoritmo circular e um estudo preliminar cujo objetivo é fornecer elementos para a criação de um algoritmo, híbrido dos algoritmos AHPEFP e circular, denominado hipercitcular.

Introdução

Para uma boa compreensão do texto, caso o leitor não conheça, recomendamos a leitura do artigo "***Goldbach – A conjectura que virou corolário***" (1) em particular, o item 7 "***Relações métricas no círculo***" onde apresentamos entre outras a equação 7.1 deduzida com base na figura 4.1 do Circulante, a qual é utilizada para a formulação do **algoritmo circular.**

Diferentemente do algoritmo **hiperbólico**, que utiliza a equação C=x*z nos cálculos de decomposição, onde C é uma constante correspondente ao produto de 2 números inteiros x e z, o algoritmo **circular** lança mão da variável D (diâmetro D do Circulante), que por sua vez corresponde à soma de dois inteiros x e z, para determinar, por meio de tentativas e erros, os inteiros x e z cujo produto corresponde à constante $C = y^2$. Inicialmente estabelecemos os conceitos de **terminações unitárias e decenárias numéricas e diametrais** e suas relações, úteis na formulação complementar do algoritmo circular**, r**elações estas que permitem substancial redução nas quantidades de cálculo a serem efetuadas. Na sequência apresentamos um exemplo de cálculo do algoritmo circular, um estudo sobre a **invariância** do **incremento diametral** r e por último um ensaio preparatório que servirá de base para formular um algoritmo híbrido denominado **hipercircula**r, misto do algoritmo AHPEFP e circular.

Transcrevemos a equação 7.1 acima citada:

$x \text{ ou } z = [D \pm (D^2 - 4y^2)^{1/2})] /2$ equação 7.1

Esta equação pode ser utilizada como fórmula de cálculo do algoritmo circular uma vez que x e z são calculados em função do diâmetro D que propicia , quando comparado com a determinação de z em função de x ao utilizamos o algoritmo hiperbólico, maiores incrementos na variação dos diâmetros.

De fato, as associações de x e z com D, permitem, até certo ponto, criar um artifício que diminui o número de tentativas de cálculo, de modo tal que a **terminação** do produto de dois números ímpares corresponda especificamente a determinados diâmetros.

Visando a clareza de exposição apresentamos estas terminações em duas etapas:

1 Terminações Unitárias

Diz respeito à **determinação** da forma ou modo como a **terminação numérica unitária** do número (último algarismo) a ser decomposto se relaciona com as **terminações diametrais unitárias** (2, 4, 6, 8 e 0) do Circulante.

Tem-se que:

. Produtos de dois números ímpares terminados em 1 resultam da combinação primária e básica dos seguintes produtos 1*1, 3*7 e 9*9 e têm os diâmetros do Circulante, respectivamente terminados em 2, 0 e 8.

. Produtos de dois números ímpares terminados em 3 resultam da combinação primária e básica dos seguintes produtos: 1*3 e 7*9 e tem os diâmetros do Circulante, respectivamente terminados em 4 e 6.

. Produtos de dois números ímpares terminados em 7 resultam da combinação primária e básica dos seguintes produtos: 1*7 e 3*9 e têm os diâmetros do Circulante, respectivamente terminados em 8 e 2.

. Produtos de dois números ímpares terminados em 9 resultam da combinação primária e básica dos seguintes produtos: 3*3, 1*9 e 7*7 e têm os diâmetros do Circulante, respectivamente terminados em 6, 0 e 4.

2 Terminações Decenárias

Diz respeito à **determinação** da forma ou modo como os dois últimos algarismos do número a ser decomposto (**terminação numérica decenária**) se relaciona com a dezena (**se par ou impar**) do diâmetro D do Circulante ou **terminação diametral decenária**.

As **terminações diametrais decenárias** podem ser obtidas a partir de uma matriz simétrica (ver tabela 1) na qual se ordenou horizontal e verticalmente a sequência numérica 1, 3, 7, 9, 11...97, 99 de onde se excluiu o primo 5 e seus múltiplos, uma vez que estes números são previamente eliminados antes de se aplicar tanto o algoritmo hiperbólico quanto o algoritmo circular. Nos cruzamentos das linhas e colunas desta matriz indicou-se os respectivos produtos dos números pertencentes à linha e à coluna igualmente ordenadas. Por exemplo, no cruzamento da coluna 11 com a linha 19 encontra-se 209 que corresponde ao produto desses dois números. O diâmetro resultante, por sua vez, corresponde à soma de 11 com 19, isto é, D=11+19=30. Para ilustrar a correspondência dos diâmetros com as terminações numéricas decenárias, apresentamos a tabela 2, a qual contém três quadros correspondentes **às terminações numéricas decenárias** 21, 23 e 27.

Exemplificando: no quadro com terminações decenárias em 21, ordenamos na 1ª coluna os números da tabela 1 em sua sequência natural. Na 2ª coluna colocamos a sequência complementar, que é pesquisada e obtida na tabela 1 (vide números terminados em 21) nesta tabela, assinalados em **negrito** com **bordas** das células mais **grossas**). Na 3ª coluna colocamos o diâmetro ou soma resultante. Nesta coluna os diâmetros substituídos por **asteriscos** significam que são **repetições** de combinações anteriores.

Uma vez ordenados os três tipos de diâmetros que este caso apresenta (diâmetros terminados em 8, 2 e 0) verifica-se que as séries de diâmetros obtidas podem ser representadas por progressões aritméticas. Vide nos rodapés das tabelas um resumo destas progressões. Para diâmetros com final 8 o 1º termo é 78 e o incremento ou razão r é igual a 100, para diâmetros com final 2 o 1º termo é 22 e o incremento ou razão r é igual a 100 e para diâmetros com final 0 o 1º termo é 10 e o incremento ou razão r é igual a 20.

Cabe observar que em alguns casos a combinação que resultaria num determinado diâmetro pode **estar fora** dos **limites** fixados na tabela 1. Isto, porém, não invalida a conclusão de que a série de diâmetros obtida pode ser representada por progressões aritméticas de razões r iguais a 20 ou 100.

Ressalte-se ainda que o 1º termo de uma dada progressão só é **significativo** na medida em que ele indica se o **1º algarismo** da dezena é **par ou impar**. Quem na verdade, teoricamente, irá determinar **o diâmetro mínimo ou de partida** para as tentativas de cálculo é a expressão literal oriunda do teorema da soma de dois número pares ou impares:

$$D_{min} \geq 2\ (y^{2)1/2}$$

Que uma vez calculado é **arredondado** para cima, para valores de $D_{inicial}$. O valor de $D_{inicial}$, por sua vez, é obtido através da **correspondência** entre **as terminações numéricas decenárias** do número a ser decomposto e as **terminações diametrais unitárias e decenárias** dos diâmetros. No caso da razão r ser igual a 20 o tipo de dezena da decenária do diâmetro (o 1º algarismo da dezena) pode ser par ou impar.

Para além das terminações decenárias (centenárias, milenárias, etc.) devido às **repetições** que passam a se suceder; não é mais **possível** aplicar este **artifício**. De forma simplificada esta repetição pode ser visualizada na tabela 3 onde apresentamos os diâmetros obtidos para as terminações 53, 153 e 253 em que a variação numérica das linhas da tabela foi limitada ao número 99 e as colunas estendidas até o número 999. Apesar de não ser **completa** os resultados assim obtidos são **suficientes** para a verificação destas repetições. Examinando o resumo no **rodapé** das tabelas observa-se que os primeiros termos das progressões que representam os diâmetros podem ser diferentes, porem as **razões r** permanecem **iguais** e, o que é importante **enfatizar**, os primeiros algarismos das dezenas dos primeiros termos da progressão permanecem como **impar** no caso de terminação numérica unitária igual a 4 ou **par** no caso de terminação numérica unitária igual a 0.

"Na tabela 4 apresentamos um quadro resumo das terminações diametrais unitárias e decenárias e suas **correspondências** com as terminações numéricas decenárias dos números a serem decompostos. Os termos **impa**r e **par** das terminações diametrais decenárias significam que os **primeiros** algarismos das **dezenas** são respectivamente impar e par. Exemplos de terminações diametrais decenárias: Impar: **3**8 e Par: **6**2.

Na última coluna indicamos as razões r ou taxas de incremento dos diâmetros.

	1	**3**	**7**	**9**	**11**	**13**	**17**	**19**	**21**	**23**	**27**	**29**	**31**	**33**
1	1	3	7	9	11	13	17	19	**21**	23	27	29	31	33
3	3	9	**21**	27	33	39	51	57	63	69	81	87	93	99
7	7	**21**	49	63	77	91	119	133	147	161	189	203	217	231
9	9	27	63	81	99	117	153	171	189	207	243	261	279	297
11	11	33	77	99	**121**	143	187	209	231	253	297	319	341	363
13	13	39	91	117	143	169	**221**	247	273	299	351	377	403	429
17	17	51	119	153	187	**221**	289	323	357	391	459	493	527	561
19	19	57	133	171	209	247	323	361	399	437	513	551	589	627
21	21	63	147	189	231	273	357	399	441	483	567	609	651	693
23	23	69	161	207	253	299	391	437	483	529	**621**	667	713	759
27	27	81	189	243	297	351	459	513	567	**621**	729	783	837	891
29	29	87	203	261	319	377	493	551	609	667	783	841	899	957
31	31	93	217	279	341	403	527	589	651	713	837	899	961	1023
33	33	99	231	297	363	429	561	627	693	759	891	957	1023	1089
37	37	111	259	333	407	481	629	703	777	851	999	1073	1147	**1221**
39	39	117	273	351	429	507	663	741	819	897	1053	1131	1209	1287
41	41	123	287	369	451	533	697	779	861	943	1107	1189	1271	1353
43	43	129	301	387	473	559	731	817	903	989	1161	1247	1333	1419
47	47	141	329	423	517	611	799	893	987	1081	1269	1363	1457	1551
49	49	147	343	441	539	637	833	931	1029	1127	1323	**1421**	1519	1617
51	51	153	357	459	561	663	867	969	1071	1173	1377	1479	1581	1683
53	53	159	371	477	583	689	901	1007	1113	1219	1431	1537	1643	1749
57	57	171	399	513	627	741	969	1083	1197	1311	1539	1653	1767	1881
59	59	177	413	531	649	767	1003	**1121**	1239	1357	1593	1711	1829	1947
61	61	183	427	549	671	793	1037	1159	1281	1403	1647	1769	1891	2013
63	63	189	441	567	693	819	1071	1197	1323	1449	1701	1827	1953	2079
67	67	201	469	603	737	871	1139	1273	1407	1541	1809	1943	2077	2211
69	69	207	483	**621**	759	897	1173	1311	1449	1587	1863	2001	2139	2277
71	71	213	497	639	781	923	1207	1349	1491	1633	1917	2059	2201	2343
73	73	219	511	657	803	949	1241	1387	1533	1679	1971	2117	2263	2409
77	77	231	539	693	847	1001	1309	1463	1617	1771	2079	2233	2387	2541
79	79	237	553	711	869	1027	1343	1501	1659	1817	2133	2291	2449	2607
81	81	243	567	729	891	1053	1377	1539	1701	1863	2187	2349	2511	2673
83	83	249	581	747	913	1079	1411	1577	1743	1909	2241	2407	2573	2739
87	87	261	609	783	957	1131	1479	1653	1827	2001	2349	2523	2697	2871
89	89	267	623	801	979	1157	1513	1691	1869	2047	2403	2581	2759	2937
91	91	273	637	819	1001	1183	1547	1729	1911	2093	2457	2639	**2821**	3003
93	93	279	651	837	1023	1209	1581	1767	1953	2139	2511	2697	2883	3069
97	97	291	679	873	1067	1261	1649	1843	2037	2231	2619	2813	3007	3201
99	99	297	693	891	1089	1287	1683	1881	2079	2277	2673	2871	3069	3267

Matriz Simétrica - Tabela 1

	37	39	41	43	47	49	51	53	57	59	61	63	67
1	37	39	41	43	47	49	51	53	57	59	61	63	67
3	111	117	123	129	141	147	153	159	171	177	183	189	201
7	259	273	287	301	329	343	357	371	399	413	427	441	469
9	333	351	369	387	423	441	459	477	513	531	549	567	603
11	407	429	451	473	517	539	561	583	627	649	671	693	737
13	481	507	533	559	611	637	663	689	741	767	793	819	871
17	629	663	697	731	799	833	867	901	969	1003	1037	1071	1139
19	703	741	779	817	893	931	969	1007	1083	**1121**	1159	1197	1273
21	777	819	861	903	987	1029	1071	1113	1197	1239	1281	1323	1407
23	851	897	943	989	1081	1127	1173	1219	1311	1357	1403	1449	1541
27	999	1053	1107	1161	1269	1323	1377	1431	1539	1593	1647	1701	1809
29	1073	1131	1189	1247	1363	**1421**	1479	1537	1653	1711	1769	1827	1943
31	1147	1209	1271	1333	1457	1519	1581	1643	1767	1829	1891	1953	2077
33	**1221**	1287	1353	1419	1551	1617	1683	1749	1881	1947	2013	2079	2211
37	1369	1443	1517	1591	1739	1813	1887	1961	2109	2183	2257	2331	2479
39	1443	**1521**	1599	1677	1833	1911	1989	2067	2223	2301	2379	2457	2613
41	1517	1599	1681	1763	1927	2009	2091	2173	2337	2419	2501	2583	2747
43	1591	1677	1763	1849	**2021**	2107	2193	2279	2451	2537	2623	2709	2881
47	1739	1833	1927	**2021**	2209	2303	2397	2491	2679	2773	2867	2961	3149
49	1813	1911	2009	2107	2303	2401	2499	2597	2793	2891	2989	3087	3283
51	1887	1989	2091	2193	2397	2499	2601	2703	2907	3009	3111	3213	3417
53	1961	2067	2173	2279	2491	2597	2703	2809	**3021**	3127	3233	3339	3551
57	2109	2223	2337	2451	2679	2793	2907	**3021**	3249	3363	3477	3591	3819
59	2183	2301	2419	2537	2773	2891	3009	3127	3363	3481	3599	3717	3953
61	2257	2379	2501	2623	2867	2989	3111	3233	3477	3599	**3721**	3843	4087
63	2331	2457	2583	2709	2961	3087	3213	3339	3591	3717	3843	3969	***4221***
67	2479	2613	2747	2881	3149	3283	3417	3551	3819	3953	4087	***4221***	4489
69	2553	2691	2829	2967	3243	3381	3519	3657	3933	4071	4209	4347	4623
71	2627	2769	2911	3053	3337	3479	**3621**	3763	4047	4189	4331	4473	4757
73	2701	2847	2993	3139	3431	3577	3723	3869	4161	4307	4453	4599	4891
77	2849	3003	3157	3311	3619	3773	3927	4081	4389	4543	4697	4851	5159
79	2923	3081	3239	3397	3713	3871	4029	4187	4503	4661	4819	4977	5293
81	2997	3159	**3321**	3483	3807	3969	4131	4293	4617	4779	4941	5103	5427
83	3071	3237	3403	3569	3901	4067	4233	4399	4731	4897	5063	5229	5561
87	3219	3393	3567	3741	4089	4263	4437	4611	4959	5133	5307	5481	5829
89	3293	3471	3649	3827	4183	4361	4539	4717	5073	5251	5429	5607	5963
91	3367	3549	3731	3913	4277	4459	4641	4823	5187	5369	5551	5733	6097
93	3441	3627	3813	3999	4371	4557	4743	4929	5301	5487	5673	5859	6231
97	3589	3783	3977	4171	4559	4753	4947	5141	5529	5723	5917	6111	6499
99	3663	3861	4059	4257	4653	4851	5049	5247	5643	5841	6039	6237	6633

Matriz Simétrica - Tabela 1 - continuação

	69	**71**	**73**	**77**	**79**	**81**	**83**	**87**	**89**	**91**	**93**	**97**	**99**
1	69	71	73	77	79	81	83	87	89	91	93	97	99
3	207	213	219	231	237	243	249	261	267	273	279	291	297
7	483	497	511	539	553	567	581	609	623	637	651	679	693
9	**621**	639	657	693	711	729	747	783	801	819	837	873	891
11	759	781	803	847	869	891	913	957	979	1001	1023	1067	1089
13	897	923	949	1001	1027	1053	1079	1131	1157	1183	1209	1261	1287
17	1173	1207	1241	1309	1343	1377	1411	1479	1513	1547	1581	1649	1683
19	1311	1349	1387	1463	1501	1539	1577	1653	1691	1729	1767	1843	1881
21	1449	1491	1533	1617	1659	1701	1743	1827	1869	1911	1953	2037	2079
23	1587	1633	1679	1771	1817	1863	1909	2001	2047	2093	2139	2231	2277
27	1863	1917	1971	2079	2133	2187	2241	2349	2403	2457	2511	2619	2673
29	2001	2059	2117	2233	2291	2349	2407	2523	2581	2639	2697	2813	2871
31	2139	2201	2263	2387	2449	2511	2573	2697	2759	2821	2883	3007	3069
33	2277	2343	2409	2541	2607	2673	2739	2871	2937	3003	3069	3201	3267
37	2553	2627	2701	2849	2923	2997	3071	3219	3293	3367	3441	3589	3663
39	2691	2769	2847	3003	3081	3159	3237	3393	3471	3549	3627	3783	3861
41	2829	2911	2993	3157	3239	***3321***	3403	3567	3649	3731	3813	3977	4059
43	2967	3053	3139	3311	3397	3483	3569	3741	3827	3913	3999	4171	4257
47	3243	3337	3431	3619	3713	3807	3901	4089	4183	4277	4371	4559	4653
49	3381	3479	3577	3773	3871	3969	4067	4263	4361	4459	4557	4753	4851
51	3519	***3621***	3723	3927	4029	4131	4233	4437	4539	4641	4743	4947	5049
53	3657	3763	3869	4081	4187	4293	4399	4611	4717	4823	4929	5141	5247
57	3933	4047	4161	4389	4503	4617	4731	4959	5073	5187	5301	5529	5643
59	4071	4189	4307	4543	4661	4779	4897	5133	5251	5369	5487	5723	5841
61	4209	4331	4453	4697	4819	4941	5063	5307	5429	5551	5673	5917	6039
63	4347	4473	4599	4851	4977	5103	5229	5481	5607	5733	5859	6111	6237
67	4623	4757	4891	5159	5293	5427	5561	5829	5963	6097	6231	6499	6633
69	4761	4899	5037	5313	5451	5589	5727	6003	6141	6279	6417	6693	6831
71	4899	5041	5183	5467	5609	5751	5893	6177	6319	6461	6603	6887	7029
73	5037	5183	5329	***5621***	5767	5913	6059	6351	6497	6643	6789	7081	7227
77	5313	5467	***5621***	5929	6083	6237	6391	6699	6853	7007	7161	7469	7623
79	5451	5609	5767	6083	6241	6399	6557	6873	7031	7189	7347	7663	***7821***
81	5589	5751	5913	6237	6399	6561	6723	7047	7209	7371	7533	7857	8019
83	5727	5893	6059	6391	6557	6723	6889	***7221***	7387	7553	7719	8051	8217
87	6003	6177	6351	6699	6873	7047	***7221***	7569	7743	7917	8091	8439	8613
89	6141	6319	6497	6853	7031	7209	7387	7743	***7921***	8099	8277	8633	8811
91	6279	6461	6643	7007	7189	7371	7553	7917	8099	8281	8463	8827	9009
93	6417	6603	6789	7161	7347	7533	7719	8091	8277	8463	8649	***9021***	9207
97	6693	6887	7081	7469	7663	7857	8051	8439	8633	8827	***9021***	9409	9603
99	6831	7029	7227	7623	***7821***	8019	8217	8613	8811	9009	9207	9603	9801

Matriz Simétrica - Tabela 1 - continuação

Números terminados	em 2	1	Números terminados	em 2	3	Números terminados	em 2	7
Seqüência Natural	Seqüência Complementar	D	Seqüência Natural	Seqüência Complementar	D	Seqüência Natural	Seqüência Complementar	D
1	21	22	1	23	24	1	27	28
3	7	10	3	41	44	3	9	12
7	3	*	7	89	96	7	61	68
9	69	78	9	47	56	9	3	*
11	11	22	11	93	104	11	57	68
13	17	30	13	71	84	13	79	92
17	13	*	17	19	36	17	31	48
19	69	88	19	17	*	19	33	52
21	1	*	21	63	84	21	87	108
23	27	50	23	1	*	23	49	72
27	23	*	27	49	76	27	1	*
29	49	78	29	87	116	29	63	92
31	91	122	31	33	64	31	17	*
33	37	70	33	31	*	33	19	52
37	33	*	37	79	116	37	71	108
39	39	78	39	57	96	39	93	132
41	81	122	41	3	*	41	47	88
43	47	90	43	61	104	43	89	132
47	43	*	47	9	*	47	41	*
49	29	*	49	27	*	49	23	*
51	71	122	51	73	124	51	77	128
53	57	110	53	91	144	53	59	112
57	53	*	57	89	*	57	11	*
59	19	*	59	97	156	59	53	*
61	61	122	61	43	*	61	7	*
63	67	130	63	21	*	63	29	*
67	63	*	67	69	*	67	81	148
69	9	*	69	67	136	69	83	152
71	51	*	71	13	**	71	37	*
73	77	150	73	51	*	73	99	172
77	73	150	77	99	176	77	51	*
79	99	178	79	37	*	79	13	*
81	41	*	81	83	164	81	67	*
83	87	170	83	81	*	83	69	*
87	83	*	87	29	*	87	21	*
89	89	178	89	7	*	89	43	*
91	31	*	91	53	*	91	97	188
93	97	190	93	11	*	93	39	132
97	93	190	97	59	*	97	91	*
99	79	*	99		*	99	73	*
Nºs terminados	1º Termo	Razão	Nºs terminados	1º Termo	Razão	Nºs terminados	1º Termo	Razão
	78	100		24	20		28	20
em 21	22	100	**em 23**			**em 27**		
	10	20		36	20		12	20

Tabela 2

Números terminados em	53		Números terminados em	153		Números terminados em	253	
Seqüência Natural	Seqüência Complementar	D	Seqüência Natural	Seqüência Complementar	D	Seqüência Natural	Seqüência Complementar	D
1	53	54	1	153	154	1	253	254
3	51	54	3	51	54	3	751	754
7	79	86	7	879	886	7	179	186
9	17	26	9	17	26	9	417	426
11	23	34	11	923	934	11	23	34
13	81	94	13	781	794	13	481	494
17	9	*	17	9	*	17	309	326
19	87	106	19	587	606	19	487	506
21	93	114	21	293	314	21	393	414
23	11	*	23	311	334	23	11	*
27	39	66	27	339	366	27	639	666
29	57	86	29	557	586	29	457	486
31	63	94	31	263	294	31	263	294
33	41	74	33	641	674	33	341	374
37	69	106	37	869	906	37	169	206
39	27	*	39	927	966	39	827	866
41	33	*	41	833	874	41	933	974
43	71	114	43	771	814	43	471	514
47	79	126	47	599	646	47	899	946
49	97	146	49	697	746	49	597	646
51	3	*	51	3	*	51	103	154
53	1	*	53	701	754	53	401	454
57	29	*	57	529	586	57	829	886
59	67	126	59	867	926	59	767	826
61	73	134	61	773	834	61	873	934
63	31	*	63	431	494	63	131	194
67	59	*	67	659	726	67	959	1026
69	37	*	69	437	506	69	337	406
71	43	114	71	143	214	71	243	314
73	61	*	73	961	1034	73	661	734
77	89	166	77	989	1066	77	289	366
79	7	*	79	407	486	79	307	386
81	13	*	81	113	194	81	213	294
83	91	174	83	291	374	83	991	1074
87	19	106	87	519	606	87	819	906
89	77	*	89	777	866	89	677	766
91	83	*	91	683	774	91	783	874
93	21	*	93	421	514	93	121	214
97	49	*	97	249	346	97	549	646
99	47	*	99	547	646	99	447	546
Nºs terminados em	1º Termo	Razão r	Nºs terminados em	1º Termo	Razão r	Nºs terminados em	1º Termo	Razão r
	34	20		54	20		34	20
53			**153**			**253**		
	26	20		26	20		186	20

Tabela 3

TABELA DE TERMINAÇÕES DIAMETRAIS UNITÁRIAS E DECENÁRIAS

Dezenas terminadas em	têm Terminações Unitárias dos Diâmetros em	e Terminações Decenárias dos Diâmetros em	Com Taxa de Incremento de	Dezenas terminadas em	têm Terminações Unitárias dos Diâmetros em	e Terminações Decenárias dos Diâmetros em	Com Taxa de Incremento de
	8	98	100		8	88	100
1	2	2	100	11	2	12	100
	0	Impar	20		0	Par	20
	8	78	100		8	68	100
21	2	22	100	31	2	32	100
	0	Impar	20		0	Par	20
	8	58	100		8	48	100
41	2	42	100	51	2	52	100
	0	Impar	20		0	Par	20
	8	38	100		8	28	100
61	2	62	100	71	2	72	100
	0	Impar	20		0	Par	20
	8	18	100		8	108	100
81	2	82	100	91	2	92	100
	0	Impar	20		0	Par	20
, 23, 43, 63, 8	4	Par	20	13, 33, 53, 73,	4	Impar	20
	6	Impar	20		6	Par	20
, 27, 47, 67, 8	8	Par	20	17, 37, 57, 77,	8	Impar	20
	2	Impar	20		2	Par	20
	6	6	100		6	76	100
9	4	94	100	19	4	24	100
	0	Impar	20		0	Par	20
	6	46	100		6	16	100
29	4	54	100	39	4	84	100
	0	Impar	20		0	Par	20
	6	86	100		6	56	100
49	4	14	100	59	4	44	100
	0	Impar	20		0	Par	20
	6	26	100		6	96	100
69	4	74	100	79	4	104	100
	0	Impar	20		0	Par	20
	6	66	100		6	36	100
89	4	34	100	99	4	64	100
	0	Impar	20		0	Par	20

Tabela 4

3 Invariância dos incrementos diametrais r

Vimos no item 2 que as razões ou incrementos r diametrais, dependendo do caso, variam de 20 em 20 ou de 100 em 100. Como a tabela 1 foi montada baseando-se na série 3, 7, 9, 11, 13..., surge naturalmente a seguinte dúvida: será que se eliminarmos desta série os múltiplos de primos até um primo limite inclusive, estas razões ou incrementos se alterarão?

Para esclarecer esta dúvida adotamos a terminação numérica decenária 21 e nas tabelas 5, 6 e 7 indicamos nas duas primeiras colunas os valores de x e z oriundos de uma SNB cujos produtos têm terminação numérica decenária igual a 21 entre os quais foram eliminados os primos 3 e 7 e seus respectivos múltiplos. Nas terceiras e quartas colunas indicamos respectivamente os produtos x*z e a soma D=x+z. Observe que todos os produtos tem terminação numérica decenária em 21e que os diâmetros resultantes na tabela 5 apresentam incrementos r=20. Por sua vez os diâmetros resultantes nas tabelas 6 e 7 apresentam incrementos r=100.

As linhas assinaladas com asteriscos na tabela 5 indicam exceções onde a combinação

x	z	x*z	D
13	17	221	30
*	*	*	*
*	*	*	*
43	47	2021	90
*	*		*
17	113	1921	130
23	127	2921	150
*	*	*	*
47	143	6721	190
53	157	8321	210
67	163	10921	230
23	227	5221	250
37	233	8621	270
97	193	18721	290
53	257	13621	310
163	167	27221	330
73	277	20221	350
137	233	31921	370
97	293	28421	390
157	253	39721	410
113	317	35821	430
173	277	47921	450
187	283	52921	470
47	443	20821	490
107	403	43121	510
13	517	6721	530
23	527	12121	550
233	337	78521	570
43	347	14921	390
67	563	37721	630
73	577	42121	650
83	587	48721	670

Tabela 5

x	z	x*z	D
47	643	30221	690
103	607	62521	710
113	617	69721	730
73	677	49421	750
37	733	27121	770
47	743	34921	790
53	757	40121	810
163	667	108721	830
23	827	19021	850
83	787	65321	870
97	793	76921	890
53	857	45421	910
113	817	92321	930
73	877	64021	950
83	887	73621	970
47	943	44321	990
103	907	93421	1010
17	1013	17221	1030
23	1027	23621	1050
87	983	85521	1070
143	947	135421	1090
103	1007	103721	1110
67	1063	71221	1130
173	977	169021	1150
137	1033	141521	1170
97	1093	106021	1190
53	1157	61321	1210
113	1117	126221	1230
127	1123	142621	1250
137	1133	155221	1270
97	1193	115721	1290
103	1207	124321	1310

Tabela 5 - Continuação

x	z	x*z	D
11	11	121	22
61	61	3721	122
31	191	5921	222
71	251	17821	322
31	191	5921	222
101	221	22321	322
181	241	43621	422
191	331	63221	522
101	521	52621	622
61	661	40321	722
61	761	46421	822
101	821	82921	922
61	961	58621	1022
131	991	129821	1122
71	1151	81721	1222
61	1261	76921	1322

Tabela 6

x	z	x*z	D
19	59	1121	78
29	149	4321	178
79	199	15721	278
179	199	35621	378
89	389	34621	478
139	439	61021	578
109	569	62021	678
89	689	61321	778
139	739	102721	878
109	769	83821	878
139	839	116621	978
59	1019	60121	1078
139	1039	144421	1178
79	1199	94721	1278

Tabela 7

só existe com primos menores ou igual a 7 ou com seus múltiplos. No caso de D=50 existe uma única combinação 23*27=621 cuja soma D é igual a 50, porém o diâmetro D=50 não foi considerado porque 27 é um falso primo múltiplo de 3. Já no caso de D=110 há 3 combinações possíveis: 3*107=321, 7*103=721 e 53*57=3021 que foram desconsiderados porque os valores de x no 1º caso é o primo 3 e no 2º e 3º casos são múltiplos de 3.

Conclui-se daí que os incrementos r=20 e r=100 são **invariantes**, isto é, mesmo introduzindo **a eliminação parcial** de falsos primos, não é possível dar saltos superiores a estes incrementos a menos que se queira correr o risco dos cálculos falharem.

Observe ainda que o descrito neste item corrobora o exposto na tabela 3 onde se mostrou que para além das terminações decenárias os cálculos passam a ser recorrentes e repetitivos com incrementos r invariantes.

4 Exemplo numérico de decomposição pelo algoritmo circular

Seja decompor o número 10623890 utilizando o algoritmo circular.

Caso o número a ser decomposto termine num número par ou em cinco, da mesma forma que fizemos para o exemplo numérico do algoritmo hiperbólico, ele deve ser previamente dividido sucessivamente por 2 ou 5 até que o número remanescente resulte num número C com terminação numérica unitária impar diferente de 5, isto é em 1, 3, 7 ou 9.

O número dado é par, portanto, dividindo-o por 2 obtemos :5311945. O número resultante também é divisível por 5. Dividindo-o por este valor obtemos: 1062389. O número finalmente obtido tem terminação impar diferente de 5 e se enquadra entre os números passíveis de serem decompostos tanto pelo algoritmo hiperbólico como pelo algoritmo circular. Arquivamos os fatores primos 2 e 5 para recuperá-los após o término da decomposição.

Efetuamos primeiramente os **cálculos preliminares** que serão utilizados na decomposição de $C=y^2 = 1062389$. Obtemos x_{max} extraindo a raiz quadrada de C, isto é: $X_{max} = C^{1/2} = 1030,72$. O diâmetro mínimo (ou de partida para testes) vale $2*x_{max}$, portanto $D_{min} = 2*1030,72 = 2061,44$.

São duas as **condições** para a interrupção dos cálculos quando utilizamos o algoritmo circular:

1ª - Quando por tentativas de acerto ou erro obter-se valores inteiros para x e z.

2ª – Quando por tentativas de acerto ou erro obter-se x menor que 3.

Caso **ocorra** a 2ª condição seu **significado** é o de que o número C testado é **primo**.

$C=y^2$ tem terminação numérica decenária em 89. Consultando a tabela 4 obtemos para terminações diametrais 6 (unitária), 66 (decenária) a cada 100; 4 (unitária), 34 (decenária) a cada 100 e 0, impar a cada 20. Arredondamos para cima o D_{min} encontrado para cada um dos diâmetros a serem utilizados nos três tipos de cálculo: 2066; 2134 e 2070 respectivamente a cada 100, 100 e 20. A partir desses valores ordenamos os diâmetros de forma crescente, isto é, adotamos a seguinte sequência: 2066; 2070; 2090; 2110; 2130, 2134, 2150, 2166, 2170; 2190; 2210; 2230, 2234, 2250...

Os valores de x em função de D são calculados através da equação 7.1 mostrada na introdução deste artigo e que foi extraída do artigo “Goldbach; a conjectura que virou corolário” (1). O primeiro diâmetro a ser testado é D=2066.

Tem-se que: $x \text{ ou } z = [D \pm (D^2 - 4y^2)^{1/2})] /2$ equação 7.1

$x \text{ ou } z=[(2066 \pm (2066^2-4*1062389)^{1/2}]/2$ onde x, por hipótese, é o inteiro menor, isto é x=964.44. Como x não resultou num inteiro e é menor que x_{max}=1030,62 (x calculado é sempre menor que x_{max}) então devemos partir para o segundo teste fazendo D=2070

Obtemos: x ou z=[(2070 ± (2070^2-4*1062389)$^{1/2}$]/2 donde resulta x=941 (inteiro menor) e z=1129 (inteiro maior). Encontramos uma primeira solução do problema em que ainda é necessário comprovar ou não a primalidade dos números inteiros determinados.

Fazendo agora $C=y^2$= 1129 temos $x_{max} = C^{1/2}$ = 33,6 e $D_{min} = 2*x_{max}$ = 67,2. C tem terminação numérica decenária em 29. Consultando a tabela 4 obtemos para terminações diametrais unitárias e decenárias respectivamente, 6, 4, 0 e 66, 34, impar com incrementos respectivos de 100, 100 e 20. Arredondamos para cima o D_{min} encontrado para os três tipos de cálculos a serem efetuados a partir dos diâmetros: 166; 134 e 70 respetivamente com incrementos r iguais a 100, 100 e 20. A partir desses diâmetros iniciais ordenamos os diâmetros crescentemente, isto é adotando a seguinte sequência para os diâmetros:

70, 90, 110, 130, 134, 150, 166, 170, 190, 210, 230, 234, 250, 266, 270...

D	x	z
70	25,20204	44,79796
90	15,06674	74,93326
110	11,45692	98,54308
130	9,358289	120,6417
134	9,034493	124,9655
150	7,947782	142,0522
166	7,105336	158,8947
170	6,923115	163,0769
190	6,14056	183,8594
210	5,521359	204,4786
230	5,018183	224,9818
234	4,928594	229,0714
250	4,600664	245,3993
266	4,314336	261,6857
270	4,248327	265,7517
290	3,946819	286,0532
310	3,685757	306,3142
330	3,457436	326,5426
334	3,41516	330,5848
350	3,256004	346,744
366	3,111145	362,8889
370	3,076939	366,9231
390	2,916685	387,0833
	TABELA 8	

Numa planilha Excell (tabela8) indicamos na 1ª coluna os diâmetros D e nas 2ª e 3ª colunas os valores obtidos para x e z. Como fizemos anteriormente, utilizamos a equação 7.1 e após 23 tentativas obtemos x=2,91185 valor este menor que 3 indicando com isto que o número 1129 é primo.

Fazendo procedimento análogo ao exemplo anterior para o número 941 se chega à conclusão que ele também é primo.

Então a decomposição do número 10623890 resulta nos seguintes fatores primos:

2, 5, 941 e 1129.

5 Estudo preparatório visando à criação de um algoritmo híbrido que utilize, de forma parcial, porém, eficiente, os algoritmos AHPEFP e circular.

No próximo artigo intitulado "***Algoritmo hipercicular***" (híbrido dos algoritmos AHPEFP e circular) apresentaremos uma pesquisa mais aprofundada relacionada com a determinação da proporção ideal de participação destes dois algoritmos na criação do algoritmo hipercircular. Antes, porém, vamos dar ao leitor uma ideia mais clara da dificuldade de resolver o problema da decomposição do produto de dois números primos e daí tirarmos algumas conclusões úteis para a formulação do algoritmo hipercircular.

Andrea Sgarro em seu livro "**Códigos Secretos**"(2) no capítulo que trata da criptografia do futuro, para mostrar a dificuldade de resolver este tipo de problema, propõe ao leitor uma tarefa relativamente simples: decompor o número 66167.

Vamos utilizar este problema para realizar a exposição.

Uma resolução expedita do problema pode ser obtida usando o algoritmo hiperbólico e a série numérica 3, 7, 9, 11, 13, 17...113, 117, 119, 121, 123, 127, 129, 131. Dividindo sucessivamente 66167 por esta série numérica obtêm-se após 50 operações z=521 e x=127. Se utilizássemos, por exemplo, a SNPEFP$_7$ o número de operações diminuiria para 27.

Vamos aprofundar um pouco mais na análise deste problema examinando o que acontece com a decomposição de números próximos de 66167. Para tanto devemos ter presente que o **objetivo primordial** é estudar o **problema básico** que é a decomposição do produto de dois números primos ou testar a primalidade de um número inteiro. Já vimos anteriormente que a decomposição do produto de 3 ou mais números, sejam eles primos ou múltiplos de primos sempre recai no **problema básico**. Portanto a análise que se segue restringir-se-á ao produto de dois números primos.

Para este fim, elaboramos a tabela 9 na qual indicamos em seu topo o incremento diametral r=20 válido para produtos, que por uma questão de **coerência**, têm terminações numéricas unitárias somente em 3 ou 7. Na 2ª linha titulamos as quantidades de cálculo efetuadas para os algoritmos hiperbólico e circular e o somatório das quantidades calculadas para ambos os algoritmos. Finalmente na 3ª linha indicamos as variáveis do problema.

Em relação às colunas temos:

1ª - os valores das relações x/z.

2ª - os valores de x (primos menores) 1, 3, 7, 17, 23, 31, 37, 41, 47, 53, 59, 61, 67, 89, 101, 107, 109, 127, 131, 137, 149, 157, 163, 179, 181, 191, 211, 229, 239, 241, 251 onde, como exceção, incluímos o número 1 (para formar produto com o número 66169 que é primo) e se excluiu os primos 2 e 5 (por não terem terminações numéricas unitárias em 3 ou 7) onde todos os números são menores que $x_{max}= (66167)^{1/2} =$ 257,258.

3ª - z' corresponde á divisão de C=66167 pelos valores x da 2ª coluna.

4ª - Os valores dos primos z (primos maiores), superiores ou inferiores, mais próximos de z.

5ª - os valores dos produtos C.

6ª- Os diâmetros D=x+z dos Circulantes correspondentes.

6ª - Os produtos C = x*z mais próximos possíveis de C=66167

7ª – As quantidades de cálculo efetuadas para o algoritmo hiperbólico.

8ª– As quantidades de cálculo efetuadas para o algoritmo circular.

9ª– O somatório das quantidades de cálculo dos dois algoritmos.

Observe que na 2ª e 4ªcolunas (vide última linha assinalada em negrito na tabela 9) só há um único par de números x e z que multiplicados resultam no número 66167 = 127*521 que corresponde à solução do problema. Os demais números, exceto 66169, formam um conjunto de produtos C de primos terminados em 3 ou 7cujos valores são os mais próximos possíveis de C=66167. O conjunto de elementos C constante da 6ª coluna, exceto 66169 que tem terminação numérica unitária em 9, corresponde a uma nuvem de produtos de pares de primos do mesmo tipo (têm a mesma terminação numérica unitária em 3 ou7) que se aglomeram em torno do produto C=66167.

Suponhamos que ao invés de decompor 66167 fosse pedida a decomposição de C= 66169 (vide a 1ª linha da tabela 9). Neste caso as quantidades de cálculo obtidas, para os algoritmos hiperbólico e circular, são respectivamente 103 e 2157, isto em virtude de 66169 ser primo o que exige quantidades máximas de cálculo para ambos os algoritmos. Observando os elementos das demais linhas constata-se que a quantidade de cálculo é função da relação x/z cuja variação se situa entre aproximadamente zero e um. No caso do algoritmo hiperbólico há uma mudança brusca na quantidade de cálculo de um máximo de 103 para um mínimo de 1 e a partir daí passa a ter variação aproximadamente proporcional à quantidade de testes que se efetua. Já a quantidade de cálculo para o algoritmo circular decresce de um máximo de 2157 para um mínimo de 1 cuja variação é aproximadamente quadrática. Portanto, para o algoritmo hiperbólico quanto maior for a quantidade de testes tanto maior será a quantidade de cálculo (direta e aproximadamente proporcional). Já para o algoritmo circular a variação é quadrática, pois, o cálculo de x ou z depende do discriminante existente na fórmula do algoritmo e neste caso quanto maior for D tanto maior será a quantidade de cálculo exigida.

Para a nuvem de produtos C que se aglomeram em torno do produto 66167, dependendo da relação x/z, o problema pode ser mais facilmente resolvido por um ou por outro algoritmo, isto é, se x tiver um valor relativamente baixo em geral seria mais

interessante utilizar o algoritmo hiperbólico e se for relativamente alto (valores mais próximos da raiz quadrada de C) seria mais interessante utilizar o algoritmo circular. Observe ainda que as quantidades de cálculo para os dois algoritmos perfazem caminhos opostos, porem, complementares. Eis que no algoritmo hiperbólico, exceto

quando o número é primo, a quantidade de cálculo cresce com o crescimento de x e no circular decresce de um máximo correspondente a aproximadamente à raiz quadrada de C até o primo 3.

Assinalamos ainda na tabela 9 as duas primeiras linhas em negrito onde aproximadamente deixa de ser vantajosa a aplicação de um ou de outro algoritmo, isto é, neste exemplo para relações x/z menores ou iguais a 0,1786 seria interessante aplicar o algoritmo hiperbólico e para relações maiores o algoritmo circular. Ocorre que no

caso geral de decomposição de números inteiros a relação x/z é desconhecida e o único dado que se conhece é o produto C =x*z e a informação adicional de que os valores de x e z são inteiros. Tendo em vista que estes dois algoritmos funcionam bem em intervalos de cálculo complementares (intervalos de cálculo onde, em termos de desempenho, um algoritmo funciona bem e o outro mal e vice-versa) no caso de se pretender criar um algoritmo híbrido surge a seguinte importante questão: qual seria a

proporção ótima a ser adotada para que os cálculos por um algoritmo possa prevalecer em relação ao outro?

Visualizamos duas formas de abordar a questão:

1ª Uma mais simples, que iremos adotar, baseada no estudo preparatório apresentado neste item, porém, com um grau de aprofundamento maior Neste caso o critério a ser utilizado é o de pesquisar a proporção ótima usando um procedimento que permita, ainda que de forma aproximada, obter v**alores mínimos** para a **totalidade** da quantidade de cálculo processada pelos dois algoritmos.

Em que nos baseamos para adotar tal critério?

A explicação está na observação dos números apresentados na tabela 9. Observe que as quantidades de cálculo dos dois algoritmos se cruzam na região das duas primeiras linhas assinaladas em negrito na tabela 9, onde o somatório das quantidades de cálculo dos dois algoritmos sugere a existência de um mínimo o que, caso efetivamente confirmado, propiciaria a criação de um algoritmo misto que poderia minimizar as quantidades de cálculo a serem processadas.

A razão do uso do somatório das quantidades de cálculo dos dois algoritmos se deve ao fato de desconhecermos a relação entre x e z. Ao assim procedermos, estaríamos garantindo que pelo menos o somatório das quantidades de calculo de ambos os algoritmos seria mínimo para um dado conjunto de produtos de dois números primos, conjunto este estabelecido de tal modo que a relação x/z seja variável e tenha um incremento i constante variando entre 0 e1 de forma a representar, ainda que de forma aproximada, qualquer relação x/z que por sua vez deverá coincidir com uma relação x/z adotada ou estar entre dois valores próximos das relações x/z adotadas.

Variação diametral r=20 (2 vezes) para terminação numérica unitária em 3 e7								
						Quantidade de cálculos		Somatório das
Variáveis						Algoritmo hiperbólico	Algoritmo Circular	quantidades
x/z	x	z'	z	D	C			de cálculo
0,00002	1	66169	66169	66170	66169	103	2157	2260
0,00014	3	22055,667	22051	22054	66153	1	2156	2157
0,00074	7	9452,4286	9461	9468	66227	2	900	902
0,00437	17	3892,1765	3889	3906	66113	6	340	346
0,00799	23	2876,8261	2879	2902	66217	9	240	249
0,01451	31	2134,4194	2137	2168	66247	12	166	178
0,02068	37	1788,2973	1789	1826	66193	14	132	146
0,02542	41	1613,8293	1613	1654	66133	16	114	130
0,03336	47	1407,8085	1409	1456	66223	18	96	114
0,04243	53	1248,434	1249	1302	66197	21	80	101
0,05254	59	1121,4746	1123	1182	66257	23	68	91
0,05612	61	1084,7049	1087	1148	66307	24	64	88
0,06761	67	987,56716	991	1058	66397	26	56	82
0,11978	89	743,44944	743	832	66127	35	32	67
0,15467	101	655,11881	653	754	65953	40	26	66
0,17286	**107**	**618,38318**	**619**	**726**	**66233**	**42**	**22**	**64**
0,17957	**109**	**607,0367**	**607**	**716**	**66163**	**43**	**22**	**65**
0,24376	**127**	**521**	**521**	**648**	**66167**	**50**	**14**	**64**
0,26044	131	505,0916	503	634	65893	52	14	66
0,28601	137	482,9708	479	616	65623	54	12	66
0,33634	149	444,07383	443	592	66007	59	8	67
0,372922	157	421,44586	421	578	66097	62	8	70
0,39853	163	405,93252	409	572	66667	65	6	71
0,48774	179	369,64804	367	546	65693	71	4	75
0,49319	181	365,56354	367	548	66427	72	4	76
0,55043	191	346,42408	347	538	66277	76	4	80
0,67412	211	313,58768	313	524	66043	84	2	86
0,78157	229	288,93886	293	522	67097	91	2	93
0,86282	239	276,84937	277	516	66203	95	2	97
0,87004	241	274,55187	277	518	66757	96	2	98
0,95437	251	263,61355	263	514	66013	100	2	102

Tabela 9

Se o processador for **único** então, ao executar os cálculos, temos que priorizar ou privilegiar um ou outro algoritmo. Como se desconhece a relação x/z e em que ponto dos cálculos se dará a solução do problema, então, em termos de probabilidade, tanto faz começar os cálculos por um ou por outro algoritmo. O ideal neste caso seria trabalhar com dois processadores (um máster e o outro slave) atuando simultaneamente cada qual com um algoritmo.

2ª) Outra mais **complexa**, feita através da **alternância** de uso dos dois algoritmos. Por exemplo, os cálculos poderiam começar pelo algoritmo parabólico com x crescente, menor ou igual a $x_{max} = C^{1/2}$, variando de forma parcial de um mínimo até determinado ponto previamente estabelecido a partir do qual se usaria também de forma parcial, até

outro ponto, previamente definido, o algoritmo circular com x decrescente em função de D variando aproximadamente de um mínimo ($D_{min}= 2C^{1/2}$) a um máximo $D_{max}=C+1$. Esta alternância prosseguiria até que se obtivesse x e z inteiros, ou no caso em que o número a ser decomposto for primo, o valor de x, calculado pelo algoritmo hiperbólico, ultrapassar $C^{1/2}$, ou ainda quando x crescente calculado pelo algoritmo hiperbólico superar x decrescente calculado pelo algoritmo circular. Apesar de possível, o assunto necessita ser ainda melhor explorado. Esta forma de abordar o problema aparentemente esbarra na relativa dificuldade de se estabelecer proporções harmoniosas que garantiriam certo equilíbrio nas quantidades parciais de cálculo a serem executadas.

Finalmente, raciocinando em termos de **algoritmo hiperbólico**, quando o número é primo o limite para variação de x nos testes corresponde a $x_{max}=C^{1/2}$ e a quantidade de cálculo é máxima. Para relações x/z próximas de zero a quantidade de cálculo é pequena e cresce gradualmente á medida que x cresce até o ponto (como vimos no exemplo numérico acima no problema proposto por **Sgarro** (2)) onde passa a ser vantajoso o uso do algoritmo circular. Sendo assim, haverá um momento onde isto ocorre em que a variação de x passa por um valor x' menor que x_{max} .

Seja k a relação entre x_{max} e x'. O valor de x' deve ser tal que $x' = C^{1/2}/k$ com $k > 1$.

No próximo artigo intitulado "**Algoritmo hipercircular"** detalharemos os passos para a obtenção dos valores da **relação k** que **minimize** a **totalidade** da quantidade de cálculo executada pelos dois algoritmos.

5 Bibliografia

(1) Tufaile, Damer - "Goldbach : A conjectura que virou corolário" – Vide artigo no blog DNI –www.damer.tufaile.nom.br

(2) Sgarro, Andrea – Códigos Secretos – Companhia Melhoramentos 1994. Vide capítulo 14 – Criptografia do futuro – itens: "Divagações sore números primos" e "Criptografia por chave publica: o cifrário RSA"