Prime Numbers Theorem and related sequence calculation algorithm

by: Dott. Ing. Alessandro Ratti,
Ctr.S.Giovannello Coop.Amicizia 82, Messina (Italy)
Tel.090 710 166 – Cell.347 82 79 576
e-mail: rattialessandro@gmail.com

Abstract

In this paper we illustrate a new mathematical theorem with proof regarding prime numbers that give a simple interpretation of the nature of prime numbers sequence, and, according to that theorem, we propose a simple algorithm to make a fast calculation of prime numbers sequence. As regards to other algorithm, this requires a lower amount of calculation power. Only five numbers at a time have to be used to obtain the sequent prime and only four simple operations (sum, product and compare) are required.

Keywords

Prime number, Theorem, Sequence.

1. Introduction

For some millenniums, as long ago as in ancient Greek, the comprehension of the basic laws of prime numbers has represented an enigma for the scientists, Pythagoras, Euclid were been the first to study it.
Everything make suppose that some law regarding prime numbers sequence exist but till now it have been not identified. In the contemporary age the prime numbers are very important in information technology, particularly for data cryptography. To discover more big prime numbers to improve internet security are used very sophisticated and expansive informatic systems, to discover a new prime number some years are needed.
In this paper we illustrate a new mathematical theorem with proof regarding prime numbers that give a simple interpretation of the nature of prime numbers sequence, and, according to that theorem, we propose a simple algorithm to make a fast calculation of prime numbers sequence. As regards to other algorithm, this requires a lower amount of calculation power. Only five numbers at a time have to be used to obtain the sequent prime and only four simple operations (sum, product and compare) are required.

2. Theorem

All the odd numbers in the form:

$P=2n+1$

are prime if:

$n \hat{I} N$

and $n?2md+m+d \ " \ m,d \hat{I} N$ with N natural numbers (positive integer)

Literally:
"Are prime all the odd numbers in the form $P=2n+1$ with n positive integer for which n is not member of the infinite subset of positive integer numbers obtained with the relation $n=2md+m+d$ with also m and d positive integer."

3. Demonstration

We know that:

- The even numbers are not prime
- The product of two odd numbers give an other odd number

According to last rule we simply obtain that if an odd number is not prime it is obtained by the product of other two odd numbers, that two numbers are themselves prime or odd numbers and so on.
Finally we can assert that an odd number *A=(2n+1)* is not a prime number if there are other two odd numbers *B=(2m+1)* e *C=(2d+1)* for which:

(2n+1)=(2m+1)(2d+1) with *m, d*, *n* Î *N*

so:

2n+1=4md+2d+2m+1

and also:

n=2md+d+m

so, if *2n+1* is not a prime number we have that *n=2md+d+m* with *m* and *d* Î *N*, how we would like to demonstrate.

Corollary:
Particularly *dm= md* so we can reduce the range for m or d in: *m=d* or *d=m*.

4. Verify

Give attention to the follow table:

1	3		1	26	53	53	
2	5	5		27	55		27
3	7	7		28	57		28
4	9		4	29	59	59	
5	11	11		30	61	61	
6	13	13		31	63		31
7	15		7	32	65		32
8	17	17		33	67	67	
9	19	19		34	69		34
10	21		10	35	71	71	
11	23	23		36	73	73	
12	25		12	37	75		37
13	27		13	38	77		38
14	29	29		39	79	79	
15	31	31		40	81		40
16	33		16	41	83	83	
17	35		17	42	85		42
18	37	37		43	87		43
19	39		19	44	89	89	
20	41	41		45	91		45
21	43	43		46	93		46
22	45		22	47	95		47
23	47	47		48	97	97	
24	49		24	49	99		49
25	51		25	50	101	101	

In that table are enumerated: in the first column the *n* value of the odd numbers *2n+1* reported in the second column; in the third column there are prime numbers until 101; in the last column are copied the *n* value for which the odd number is not a prime number.
In the following table we enumerate the odd numbers obtained by means of the relation n=2dm+d+m:

d\m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58	61
2	7	12	17	22	27	32	37	42	47	52	57	62	67	72	77	82	87	92	97	102
3	10	17	24	31	38	45	52	59	66	73	80	87	94	101	108	115	122	129	136	143
4	13	22	31	40	49	58	67	76	85	94	103	112	121	130	139	148	157	166	175	184
5	16	27	38	49	60	71	82	93	104	115	126	137	148	159	170	181	192	203	214	225
6	19	32	45	58	71	84	97	110	123	136	149	162	175	188	201	214	227	240	253	266
7	22	37	52	67	82	97	112	127	142	157	172	187	202	217	232	247	262	277	292	307
8	25	42	59	76	93	110	127	144	161	178	195	212	229	246	263	280	297	314	331	348
9	28	47	66	85	104	123	142	161	180	199	218	237	256	275	294	313	332	351	370	389
10	31	52	73	94	115	136	157	178	199	220	241	262	283	304	325	346	367	388	409	430
11	34	57	80	103	126	149	172	195	218	241	264	287	310	333	356	379	402	425	448	471
12	37	62	87	112	137	162	187	212	237	262	287	312	337	362	387	412	437	462	487	512
13	40	67	94	121	148	175	202	229	256	283	310	337	364	391	418	445	472	499	526	553
14	43	72	101	130	159	188	217	246	275	304	333	362	391	420	449	478	507	536	565	594
15	46	77	108	139	170	201	232	263	294	325	356	387	418	449	480	511	542	573	604	635
16	49	82	115	148	181	214	247	280	313	346	379	412	445	478	511	544	577	610	643	676
17	52	87	122	157	192	227	262	297	332	367	402	437	472	507	542	577	612	647	682	717
18	55	92	129	166	203	240	277	314	351	388	425	462	499	536	573	610	647	684	721	758
19	58	97	136	175	214	253	292	331	370	409	448	487	526	565	604	643	682	721	760	799
20	61	102	143	184	225	266	307	348	389	430	471	512	553	594	635	676	717	758	799	840

In the firs row and column are indicated the m and d numbers from which are obtained the n value in the table.
Simply deleting the numbers in the last column of the first table from the second table you can see how progressively the tables became empty (the grey cells indicate that the value is repeated in table according to the corollary).
You can verify that disquisition by means of an electronic sheet.

5. Algorithm for computation

Prime numbers are very important in IT application for data cryptography in secure communication. For largest security are used the more big prime number in humane knowledge. Looking for big prime number determination are used more complex and expansive elaborators, particularly are used distributed computer technology. What let the problem to be serious concerns the amount of operation and memory necessary to hold in temporary memory and to manage so big numbers (many million of decimal units). With actual known prime sequence calculation algorithm it is necessary to execute millions of operation with number composed by millions of decimal units. Each new prime numbers is discovered with some years of delay each other.
According to the proposed theorem we know the relation to obtain the sequence of the not prime odd numbers (following indicate with the NPO acronym):

$n=2md+d+m$

All the odd numbers from one NPO and the sequent are primes.
In the last relation we use for *m* and *d* the values that give the NPO in increasing sequence. To do this we have to compare the NPO obtained in increasing singularly *m* and *d* and then we choose the minor.
For each iteration we obtain a new NPO, all the odd numbers in the range from the precedent and the new DNP are prime numbers.

In a elaborator, the calculation of n for each *m* and *d* can be made only a time, the found value can be kept in memory and compared with the following one until it will be the minor. Each time we keep in memory only the *n* that is not the minor and use the other to obtain the next prime number.
To evidence the calculation economy of this method, we observe that compared to other algorithm in which it is necessary to compare an enormous quantity of numbers, paying a lot of time and requiring a lot of memory to keep comparing numbers, in this method we have to keep only five numbers at a time and only few simple operations.
The numbers to keep are: last actual prime number, the *n* value kept in last compare, actual *m* and *d* value and the subsequent DNP.

After the primes selection (odd numbers in the range from precedent to actual DNP) the precedent DNP could be deleted.
The required operations are:

- calculation of n value according to: $n=2md+m+d$
- compare the n values obtained with separate increment of m and d
- calculation of $2n+1$ to obtain the next DNP
- search of odd numbers between the last two DNP.

6. Conclusion

In this paper we enunciate a theorem concerning prime numbers and its proof. This theorem explains the nature of the prime numbers sequence.
According to that theorem we propose also an algorithm for prime numbers determination.
The proposed algorithm is much more efficient respect to other similar algorithms.
For example the "Sieve of Eratostene" and "Sieve of Atkin" (in which it is required the building of a table containing a lot of numbers from which you have to delete all the numbers multiple of more small numbers) require a lot of memory for the storage of tables with numerous numbers, that for big numbers (with million of unity) could be more and more expansive and require also a lot of elaborations.
The proposed algorithm has a direct approach, knowing exactly the DNP sequence we obtain immediately prime numbers with only few calculations.