Natural Science, 2015, 7, 416-423
Published Online August 2015 in SciRes. http://www.scirp.org/journal/ns
http://dx.doi.org/10.4236/ns.2015.78044

Development of New Method for Generating Prime Numbers

Seidikassym Baibekov[1], Serik Altynbek[2]

[1]Research Institute of Coal Chemistry and Technology, Astana, Kazakhstan
[2]Eurasian National University, Astana, Kazakhstan
Email: baibekovsn@mail.ru, serik_aa@bk.ru

Received 30 June 2015; accepted 15 August 2015; published 18 August 2015

Abstract

The article is devoted to actual problems of prime numbers. A theorem that allows generating a sequence of prime numbers is proposed. An algorithm for generating prime numbers has been developed. A comparison of the proposed theorem, with Wilson's theorem is also provided.

Keywords

Prime Numbers, Theorem, Algorithm, Method, Prime Twins, Generation

1. Introduction

The reason for writing this article was a solution of the ancient problem. This problem in a simplified version is as follows: *Slandy a noble woman well-known in the Eastern world lived in ancient times. She had seven daughters. Slandy always wore amamazing beauty antique necklace of precious pearls, which according to tradition passed from mother-in-law to daughter-in-law. In old age, she told her daughters-in-law*: "*By inheritance it is time to pass the necklace to someone of you and if I will choose someone of you, the others will be offended. If I choose two of you and divide this necklace exactly into two parts, one pearl will be surplus. This is not a right way plus other fives will feel aggrieved what I don't want in my old ages. And also, when this necklace is divided into* 3, 4 *or* 5, *and* 6, *in each case one pearl is superfluous. And if I divide it by* 7, *the pearls split evenly, but this is also impossible, as this necklace according to the covenant of ancestors must be passed to only one daughter-in-law. Therefore I will pass the necklace to whom who will determine how many pearls are in this necklace. Others should not be offended.*"

"*It is known that the daughter-in-law, who decided this problem called Alkhan-Tumar, which means Necklace-Mascot.*

Legend also says that this necklace still exists."

Naturally today it is not difficult to solve the problem. Let's first recall Wilson's theorem which is formulated

How to cite this paper: Baibekov, S. and Altynbek, S. (2015) Development of New Method for Generating Prime Numbers. *Natural Science*, **7**, 416-423. http://dx.doi.org/10.4236/ns.2015.78044

as: *a natural number n* > 1 *is a prime number if and only if* $(n-1)!+1$ *is divided by n evenly* [1].

This formulation implies that $(n-1)!+1$ is divided by all natural numbers less than *n* (except 1) with a remainder of 1. Using given theorem, let's find a solution: 721. However, it is not a full solution and it is one of a set of solutions.

Using criterions for divisibility and properties of natural numbers factorial expansion, we can find a first solution as 301. Obviously, that the solutions of this problem set up an arithmetic progression, the first term of which is equal to 301 and the progression difference is 420. *i.e.* the sequence of solutions of this problem looks like: 301, 721, 1141, etc.

This example is interesting because, if in this problem we replace last number 7 by number 9, or by any composite number, then this problem has no solution, since a condition of a remainder of 1 will not be fulfilled. In short, this problem has a solution when and only when a final number is a prime number, such as 11, 13, $17,\cdots,101,\cdots,211,\cdots$

As you can see, this problem is devoted to the problems of prime numbers. We believe that such problems with some similar formulations can be found in folklores of many nations. This is not surprising, the problems of prime numbers appeared before the Common Era, have been affecting interests of the scientific community for more than 2300 years. Since Eratosthenes, scientists have been gradually progressing, and in recent decades computers appeared to help them. But the main problems of prime numbers are still unsolved.

The solution of the above mentioned problem shows a way for solving the following problem of prime numbers.

2. Prime Numbers Generation

Let we solve the following problem.

Suppose we are given an ordered sequence of prime numbers. It is necessary to find a next in order prime number. To solve the problem the following theorem is suggested.

Theorem. *If the numbers* $p_1, p_2, \cdots, p_i, \cdots, p_n$ *are terms of the original sequence of prime numbers, where <i> is an order of a prime number, i.e.* $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, *etc., then there is a whole number k for which* $p_1 \times p_2 \times \cdots \times p_{n-1} \times k + 1$ *is divided evenly by* p_n, *and by* p_i *with a remainder of* 1 *for all* $i = 1, 2, \cdots, n-1$.

It is easy to prove this theorem. For this purpose, it is only necessary to combine Wilson's theorem with a fundamental theorem of arithmetic ("*every natural number greater than* 1 *can be represented as a product of prime numbers, and this product is unique*"). The combination of these theorems makes required proof elementary and obvious. For this purpose, in a first approximation, it suffices to take $k$as a product of all composite numbers less than p_n, *i.e.* a product of those composite numbers that appear in Wilson's theorem. Therefore, we skip a proof of the theorem intentionally.

Now, using this theorem, we will show an algorithm for solving posed problem.

3. Algorithm for Generating Prime Numbers

Suppose we have a sequence of known prime numbers $p_1, p_2, \cdots, p_i, \cdots, p_n$, where *i* is an order number of prime numbers, *i.e.* $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, etc. and p_n desired prime number.

Let indicate P_{n-1} as a product of $p_1 \times p_2 \times \cdots \times p_{n-1}$. Therefore, according to the conditions of the suggested theorem, for some whole number $k > 0$ the following equality should be satisfied:

$$\frac{P_{n-1} \times k + 1}{p_n} = \frac{(p_1 \times p_2 \times \cdots \times p_{n-1}) \times k + 1}{p_n} = \text{a whole number}, \quad (1)$$

Lemma. *If equality* (1) *is true, then it is true for a infinite set of whole values of k. Plus a sequence of values of k forms an arithmetic progression, the first member of which is in interval from* 1 *to* p_n, *a common difference of this progression is equal to* p_n, *and one of the terms of the progression is a product of all composite numbers less* p_n, *i.e. a product of those composite numbers that appear in Wilson Theorem.*

4. Proof

For optimality of the proposed theorem implementation in practice, we need to determine a minimum, *i.e.* the initial value, of *k* or at least to identify an interval it belongs to.

For this we consider the ratio of $\frac{P_{n-1}\times k+1}{p_n}$.

First we will show, that, if the ratio at any *k* from 1 to p_n is not a whole number, then it will not be a whole number for any $k=1,2,3,\cdots,\infty$. Let prove this.

Suppose an expression $\frac{P_{n-1}\times k_1+1}{p_n}$ at $k_1=1,2,\cdots,p_n$ is not a whole number. Let try to determine, what this ratio will be for the next following values of *k* For this purpose we select a value of $k=k_1+p_n$. Then the ratio in question takes a form as:

$$\frac{P_{n-1}\times(k_1+p_n)+1}{p_n}=\frac{P_{n-1}\times p_n}{p_n}+\frac{P_{n-1}\times k_1+1}{p_n}$$

It is obvious, that this expression will not be a whole number, since an addend, as mentioned above, is not a whole number. After that, repeating this procedure similarly for any $k=k_1+i\times p_n$, where $i=0,1,2,\cdots,\infty$, we assure that this ratio will never be a whole number.

This means that, if the ratio in question of Equation (1) is a whole number, then the initial value of *k* must be in interval from 1 to p_{n-1}, *i.e.* if

$$\frac{P_{n-1}\times k_1+1}{p_n}=\text{a whole number, then } k_1>0 \text{ and } k_1<p_n.$$

We will also show here that when the equality (1) is satisfied, the parameter *k* takes a set of values that equal to $k=k_1+i\times p_n$, where $i=0,1,2,\cdots,\infty$. In fact, using this expression, we transform the original ratio in question into:

$$\frac{P_{n-1}\times k+1}{p_n}=\frac{P_{n-1}\times i\times p_n}{p_n}+\frac{P_{n-1}\times k_1+1}{p_n}$$

It is obvious, that the first term is a whole number and the second term, as was shown above, is also a whole number, therefore the ratio in question in the lump is also a whole number.

From the above said it follows that under the equality (1), the parameter *k* takes is a set of values which, as stated above, form an arithmetic progression. The first term of the progression should be in interval from 1 to p_{n-1}, *i.e.* $0<k<p_n$. The common difference of this progression is equal p_n. One of the terms of the arithmetic progression is a product of all composite numbers less than p_n, *i.e.* it is equal to the product of those composite numbers that appear in Wilson's theorem.

5. The Proof of the Lemma Is Completed

From this moment and further, it is sufficient to know an initial value of parameter *k*, which is in interval of $0<k<p_n$. For convenience, we introduce parameter $P(n,k)$, such that
$P(n,k)=P_{n-1}\times k+1=(p_1\times p_2\times\cdots\times p_{n-1})\times k+1$.

Note that expression of Equation (1) includes two conditions:

a) A number $P_{n-1}\times k+1$ *should be separately divided by all* $p_1,p_2,\cdots,p_{n-1}$ *with a remainder* 1, *i.e. for all* $i=1,2,\cdots,n-1$:

$$P(n,k)=1(\text{mod } p_i) \tag{1a}$$

b) A number $P_{n-1}\times k+1$ *should be divided by* p_n *evenly, i.e.*

$$P(n,k)=0(\text{mod } p_n) \tag{1b}$$

Thus, let we have an initial ordered sequence of prime numbers $p_1,p_2,\cdots,p_i,\cdots,p_{n-1}$ To find the next in order prime number p_n we will build the following algorithm. For this, first for p_n we take the next odd number to p_{n-1}. After that, taking *k* from 1 to p_{n-1}, we execute arithmetic operation given in Equation (1). If in this case and at some value of *k* the conditions of Equations (1a) and (1b) will be observed, *i.e.* a result of division according the Equation (1) will be a whole number and then considered number p_n is the next prime number. After that, in the same way we start to search next prime number p_{n+1}.

And, if the conditions of Equations (1a) and (1b) are not met, then we deal with a composite number, *i.e.* in this case, considered number of p_n is not a prime number. It should be noted here that if the number p_n will be a composite number, then during the calculation of $\frac{P_{n-1}\times k+1}{p_n}$, a sequence of digits of the fractional part of this division result is periodically repeated while sorting parameter *k*. It can be easily seen after a few steps of cycle by *k* parameter, and it becomes clear that considered number p_n is not a prime number. Then we can immediately stop the cycle. This greatly increases the efficiency and speed of the proposed algorithm.

Then we proceed to the next odd number. The procedure is repeated again for different values of *k*.

If even in this case, the selected number is again a composite number, then proceed again to the next odd number. The operation is repeated until the conditions of Equations (1a) and (1b) will not be fulfilled. For clarity, we will show this based on a simple example.

Suppose we have an original sequence of prime numbers $p_1=2, p_2=3$, $p_3=5$ and $p_4=7$. It is required to find the next fifth prime number $p_5=?$ In this case, $n=5$. For this, first for p_n we take 9 as an odd number next to 7. Then we calculate the values of $P(n,k)=P(5,k)$ for different values of *k* from 1 to p_{n-1}: $P(5,1)=211$, $P(5,2)=421$, $P(5,3)=631$, $P(5,4)=841$, $P(5,5)=1051$, $P(5,6)=1261$, etc. As can be seen, the values of $P(n,k)$ constitutes an arithmetic progression with a difference of $=2\times3\times5\times7=210$. Note that among these values 841 and 1261 are composite numbers, and the rest of them are prime numbers. But we are looking for a prime number following 7.

Conducting the series of calculations, we see that a result of division of $\frac{P(5,k)}{9}$ at any value of $k<9$ will not be a whole number. This means that 9 is a composite number. After that for p_n we take the next odd number 11. Repeating the operation we obtain that at *k* = 10 value of $P(n,k)=P(5,10)=2101$ is divided by 11 evenly. Actually, 2101:11 = 191. This means that a prime number next to 7 is 11, *i.e.* $p_n=p_5=11$.

For completeness of the visualization, we consider one more sequence of prime numbers, with its last term as 23. In this case, first for p_n we take 25 as an odd number, next to number 23. And we see that it is a composite number. Then we select a number 27. At this time, the condition of Equation (1) will not be fulfilled, that is, we see that 27 is a composite number. When we select number 29, then at *k* = 17 condition of Equation (1) is satisfied, *i.e.* a value of $\frac{P(n,k)}{29}=\frac{P(10,17)}{29}=(223,092,870\times17+1)/29=130,778,579$ is a whole number. This means that a prime number after 23 will be 29, *i.e.* $p_n=p_{10}=29$.

Sometimes it happens, that even at *k* = 1, we obtain desired results. For example, a value of $\frac{P(n,k)}{19}=\frac{P(8,1)}{19}=\frac{(51010\times1+1)}{19}=26869$ is a whole number, *i.e.* 19 is a prime number after 17. In addition, the numbers 17 and 19 are twins.

Some answers to the posed problem for a small set of primary prime numbers are given as **Table 1**. In this table, *n* is a counting number of a prime number.

In short, if there is a set of primary prime numbers, then while using expression of Equation (1) it is always possible to find the next prime number.

To show diversity to the proposed method, we offer one more elegant algorithm, the essence of which is primarily to find a value of *k* through existing prime numbers.

For this, we use Chinese remainder theorem, which states: "*If natural numbers* $p_1, p_2, \cdots, p_n$ *are coprimes in pairs, then for any whole numbers* $r_1, r_2, \cdots, r_n$ *such that* $0\le r_i<p_i$ *for all* $i\in(1,2,3,\cdots,n)$ *there is a number N, which when divided by* p_i *gives a reminder* r_i *for all* $i\in(1,2,3,\cdots,n)$." [2].

It is known that constructive method for proving this theorem allows to solve the following system of linear equations modulo [3] [4]:

$$x=r_1\left(\operatorname{mod} p_1\right)$$
$$x=r_2\left(\operatorname{mod} p_2\right) \tag{2}$$

Table 1. Using with proposed theorem found primes number.

n	p_n	k	$P_{n-1} \times k + 1$
1	3	1	3
2	5	4	25
3	7	3	91
4	11	10	2101
5	13	10	23101
6	17	2	60061
7	19	1	510511

$$x = r_{n-1} \left(\text{mod } p_{n-1} \right)$$

$$x = r_n \left(\text{mod } p_n \right)$$

If sets ($p_1, p_2, \cdots, p_n$) и ($r_1, r_2, \cdots, r_n$) fulfill conditions of Chinese theorem, then solution for system of Equations (2) exists and is unique within the accuracy of an operation by modulo $P_n = \prod_{i=1}^{n} p_i = p_1 \times p_2 \times \cdots \times p_n$, and this solution looks like [2]-[4]:

$$x = \sum_{i=1}^{n} r_i M_i M_i^{-1} \tag{3}$$

$$\text{where} \quad M_i = p_n / p_i \tag{4}$$

$$M_i M_i^{-1} = 1 \left(\text{mod } p_i \right) \tag{5}$$

i.e. M_i^{-1} is inverse for M_i by module p_i.

Now, knowing the solution of Equation (3) we can easily find the values of factor *k*. It is obvious, that Chinese theorem is true for any sequence of prime numbers since prime numbers are always coprimes in pairs. Then, considering for $p_1, p_2, \cdots, p_n$ in the system of Equation (2) a sequence of prime numbers, for our case we obtain that

$$r_1 = r_2 = \cdots = r_{n-1} = 1 \text{ and } r_n = 0 . \tag{6}$$

Now, by combining the proposed theorem with Chinese theorem, we have from Equations (1)-(6):

$$k = p_n \left(\sum_{i=1}^{n-1} \frac{M_i^{-1}}{p_i} - \frac{1}{P_n} \right) \tag{7}$$

Expression of Equation (7) shows that if a sequence of prime numbers is known, we are always able to calculate a value of *k* in advance. Then, by substituting of calculated value of *k* in Equation (1), we verify the fulfillment of the conditions of Equations (1a) and (1b). If these conditions are not fulfilled, then a number considered as p_n is not a prime number. This number is the next composite number that stands for the prime number p_{n-1}. And, if the conditions of Equations (1a) and (1b) are met, then p_n is a desired prime number. After that, we proceed with finding next prime p_{n+1} and the cycle repeats.

In this case algorithm for searching prime numbers in odd numbers series looks as follows.

Step 1. Input values of existing prime numbers $p_1, p_2, \cdots, p_{n-1}$, where $p_1 = 2,\ p_2 = 3,\ p_3 = 5$, etc.

Step 2. For p_n, we input an odd number, which in a line of odd numbers follows a prime number p_{n-1}. Here $p_n = p_{n-1} + 2m$, where $m = 1, 2, 3, \cdots$ In this case for 1st step $m = 1$.

Step 3. Calculate $P_{n-1} = \prod_{i=1}^{n-1} p_i$ and $P_n = P_{n-1} \times p_n$.

Step 4. Calculate $M_i = p_n / p_i$ for all $i \in \left(1, 2, 3, \cdots, n\right)$.

Step 5. Using extended Euclid's algorithm, we find M_i^{-1} for all $i \in \left(1, 2, 3, \cdots, n\right)$ from the condition $M_i^{-1} M_i = 1 \left(\text{mod } p_i \right)$

Table 2. Comparison results between Wilson's theorem and proposed theorem.

Results obtained based on Wilson's theorem			Results obtained based on proposed theorem			
n	$\left(P_{n-1}\times k+1\right)\text{mod } p_n$	$\left((n-1)!+1\right)$ **mod *n***	p_i	$P_{n-1}=p_1,\ p_2,\cdots,\ p_{n-1}$	***k***	$\left(P_{n-1}\times k+1\right)\text{mod } p_n$
1	**2**	**3**	**1**	**2**	**3**	**4**
2	1	**0**	**2**	1	1	**0**
3	2	**0**	**3**	2	1	**0**
4	6	3				
5	24	**0**	**5**	6	4	**0**
6	120	1				
7	720	**0**	**7**	30	3	**0**
8	5,040	1				
9	40,320	1				
10	362,880	1				
11	3,628,800	**0**	**11**	210	10	**0**
12	39,916,800	1				
13	479,001,600	**0**	**13**	2310	10	**0**
14	6,227,020,800	1				
15	87,178,291,200	1				
16	1,307,674,368,000	1				
17	20,922,789,888,000	**0**	**17**	30,030	2	**0**
18	355,687,428,096,000	1				
19	6,402,373,705,728,000	**0**	**19**	510,510	1	**0**
20	121,645,100,408,832,000	1				
21	2,432,902,008,176,640,000	1				
22	51,090,942,171,709,400,000	1				
23	1,124,000,727,777,610,000,000	**0**	**23**	9,699,690	3	**0**
24	25,852,016,738,885,000,000,000	1				
25	620,448,401,733,239,000,000,000	1				
26	15,511,210,043,331,000,000,000,000	1				
27	403,291,461,126,606,000,000,000,000	1				
28	10,888,869,450,418,400,000,000,000,000	1				
29	304,888,344,611,714,000,000,000,000,000	**0**	**29**	223,092,870	17	**0**
30	8,841,761,993,739,700,000,000,000,000,000	1				
31	265,252,859,812,191,000,000,000,000,000,000	**0**	**31**	6,469,693,230	13	**0**
32	8,222,838,654,177,920,000,000,000,000,000,000	1				
33	263,130,836,933,694,000,000,000,000,000,000,000	1				
34	8,683,317,618,811,890,000,000,000,000,000,000,000	1				
35	295,232,799,039,604,000,000,000,000,000,000,000,000	1				
36	10,333,147,966,386,100,000,000,000,000,000,000,000,000	1				
37	371,993,326,789,901,000,000,000,000,000,000,000,000,000	**0**	**37**	200,560,490,130	10	**0**
38	13,763,753,091,226,300,000,000,000,000,000,000,000,000,000	1				
39	523,022,617,466,601,000,000,000,000,000,000,000,000,000,000	1				
40	20,397,882,081,197,400,000,000,000,000,000,000,000,000,000,000	1				
41	815,915,283,247,898,000,000,000,000,000,000,000,000,000,000,000	**0**	**41**	7,420,738,134,810	34	**0**

Step 6. Calculate the desired value of k by the formula:

$$k = p_n\left(\sum_{i=1}^{n-1}\frac{M_i^{-1}}{p_i}-\frac{1}{P_n}\right)\text{mod}\, P_n$$

Step 7. Check fulfillment of equality (1).

Step 8. Conditional operator works here.

-If conditions of Equations (1a) and (1b) are not met, then considered number p_n is not a prime number, then assign $m = m + 1$ and proceed to step 2. The cycle repeats until conditions of Equations (1a) and (1b) will not be met.

-If conditions of Equations (1a) and (1b) are fulfilled, then p_n is a desired prime number, followed a prime number p_{n-1}.

Step 9. Generation of the next prime number p_{n+1} is carried out similarly.

The cycle repeats.

We assume that the process of generating prime numbers based on the proposed theorem is faster than a generation based on Wilson's theorem.

In case of Wilson's theorem it is quite difficult to calculate the factorial of $(n - 1)!$. In fact, if generation is carried out in the area of the large numbers, then calculation of given factorial creates significant difficulties. This is explained by the fact that there are intervals in the sequence of natural numbers which include thousands, millions, billions and even some arbitrarily large number of natural numbers standing in a row, among which there is no prime number. For example, if you set an arbitrary large natural number *m*, let build a series of numbers $m!+2,\ m!+3,\ m!+4,\cdots,\ m!+m$ then it is obvious that each of these numbers is a composite number. You can easily check, particularly $m! + 2$ is evenly divided by 2, $m! + 3$ is divided by 3, and$m!+m$is evenly divided by *m*, *i.e.* there is no a prime number in the large interval of $\left[(m!+2)/(m!+m)\right]$. If, for example, $m = 10^{10}$, then in case of Wilson's theorem, calculation of the factorial will inevitably lead to a large number of calculations involving a huge amount of large composite numbers. And in case of the proposed theorem calculations are mainly made with prime numbers.

This is clearly illustrated from **Table 2**, which shows results of searching prime numbers using methods following from Wilson's theorem (left part of the table) and proposed theorem (right part of the table).

The left part of the table provides calculations made for values of n from 2 to 41. In the 1st column of left part of the table (case of Wilson's theorem) all natural numbers*n*are given. In this column cells containing prime numbers which are green highlighted for illustrative purposes. In the 2nd column the calculated values of $(n-1)!$ factorial are shown. And 3rd column provides remainders which take zero values in case of prime numbers.

Similar results, obtained using proposed theorem, are shown in the right part of the table. First column of the right part shows prime numbers. Second column of this part presents calculated values of $P_{n-1}=\prod_{i=1}^{n-1}p_i$. And the last column shows values of remainders which also take zero values for prime numbers.

Table 2 shows that, in case of Wilson's theorem, in order to carry out generation of prime numbers at least up to 13th prime number, *i.e.* up to $p_{13}=41$ it is necessary to perform a lot of laborious calculations with large numbers.

A right part of the table shows only those numbers with which the calculations have been made using the proposed method. Comparing the left and right parts of the table, we can see that efficiency, speed, and convenience of the proposed method are beyond question, this is obvious. Plus, for a set of large integers, this obviousness becomes even more than self-evident.

Note again that in case of Wilson's theorem the complexity lies in calculation of $(n-1)!$ factorial. It is easier to calculate a^{n-1}; therefore elementary tests, determining whether a number is prime number, are based on Fermat's theorem, rather than on Wilson's theorem. However, note that in contrast to Fermat's small theorem, Wilson's theorem simultaneously is a necessary and sufficient condition for determining primality of any number.

References

[1] Vinogradov, I.M. (1952) Fundamental of the Theory of Number. 5th Edition, Publishing House of Technology & Scientific Literature, 262.

[2] Ishmuchametov, Sh.T. (2011) Methods of Factoring Natural Numbers. Kazan Federal University Press, Kazan, 202.

[3] Nesterenko, A. (2011) Introduction to Modern Cryptography, Theoretical Numbers Algorithms. 190. http://img0.liveinternet.ru/images/attach/c/4/3908/3908902_ntheory.pdf

[4] Gabidulin, E.M., Kshevetshkii, A.S. and Kolybelnikov, A.I. (2011) Information Security. MFTI, 262.