World Applied Sciences Journal 29 (5): 655-659, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.05.13896

The New Theorem on Prime Number Criterion with Few Operations for the Identification of Prime Number

[1]Mukhidin Tashbulatovish Mamaraimov and [2]Esenbek Riskulovich Ushtenov

[1]Kazakhstan Engineering and Pedagogical University of Friendship of the People, City of Shymkent, Kazakhstan
[2]Limited Lability Company "Talapker-Yuk", City of Saryagash, Kazakhstan

Abstract: In this article, the authors give the description of contemporary problems that used to face throughout many centuries and attracted the attention of the most outstanding mathematicians, such as Pierre de Fermat, Leonhard Euler, Carl Gauss and Bernhard Riemann. Many of these problems are still not solved. They continue to be an object for the interest of thousands of amateurs and professionals of the world. The authors give the examples showing the impracticality of the method based on Eratosthenes sieve, Leibniz theorem, Sierpinsky theorem and Wilson theorem.

Key words: Millennia · Congress · Mathematics · Hypothesis · The Clay Mathematics Institute (CMI) · Riemann hypothesis · Navier-Stokes equation · Poincaré hypothesis · Hodge conjecture · Yang-Mills theory · Birch and Swinnerton-Dyer conjecture · Cook problem · Distribution of primes · "prime pair" · Cryptography · Prize · "Eratosthenes sieve" · Remainder in division · Proving · Character · Features · Algorithm · Theorem · Fermat · Wilson · Euler · Leibniz · Criterion · Number divisibility · Multidigit numbers · Natural number · Certificate of authorship

INTRODUCTION

Seven problems of the millennium attract the attention of world scientific community. This interest is not accidental.

In 1900, during the II congress of mathematicians in Paris, well-known German mathematician David Gilbert presented a list of 23 urgent problems of mathematics [1, 2]. In the previous century, 15 of these problems were solved. One of the 8 residuary problems was removed from the agenda due to the lack of conditions.

In 2000, American Clay Institute announced a $1,000,000 prize for each of the 7 remaining problems and called them the Millennium Problems. Only one of these problems – the Poincaré hypothesis – is solved by now by outstanding Russian mathematician Gregory Perelman.

Here is the summarizing list of millennium problems:

- Riemann hypothesis, 1859. (Number theory). It is considered that prime numbers spread among natural numbers without any regularity. However, German mathematician Riemann made an assumption concerning features of the sequence of prime numbers. If Riemann hypothesis is proved, this will cause revolutionary changes in our knowledge about number theory, in the correctness of many theorems about prime numbers and in the sphere of encryption. This may lead to an unprecedented breakthrough in Internet security.
- Navier-Stokes equation about turbulent flows, 1822 (aerohydrodynamics). There are no solutions for these equations (empirical power polynomial functions?) and nobody knows how to solve them.

Corresponding Author: Mukhidin Tashbulatovish Mamaraimov, Kazakhstan Engineering and Pedagogical University of Friendship of the People, Kazakhstan, 160019, Southern Kazakhstan Area, City of Shymkent, Zhangeldin Street, 13.

It is necessary to show that the solution does exist being a sufficiently smooth function. This will make it possible to perform great changes in the methods of hydrodynamic and aerodynamic calculations. (The integration of curvilinear tensors as the matrix of curls and divergences?).

- Poincaré hypothesis, 1904 (the topology and geometry of multidimensional space): any simply connected closed tree-manifold is homeomorphic to three-dimensional sphere (that is there cannot be a four-dimensional toroid and our Universe is a three-dimensional sphere).
- Hodge conjecture, 1941 (algebra, topology). In 21 century, mathematicians discovered a powerful method for researching the shape of complex objects by using simple "blocks" instead of the object itself. These "blocks" stick together and form its likeness (aren't they "cubic integrals"?). The Hodge conjecture is connected with some assumptions concerning features of such "blocks" and objects.
- Yang-Mills theory, 1954 (connection between geometry and quantum physics). The equation of quantum physics describes the world of elementary particles. Physicists Yang and Mills wrote their equations when they found a connection between geometry and physics of elementary particles. Thus they discovered a way to uniting theories of electromagnetic, weak and strong interaction. It followed from Yang-Mills equations that there are particles which were really observed in laboratories. That is why the majority of physicists accepted the Yang-Mills theory, though they still do not manage to predict the masses of elementary particles.
- Birch and Swinnerton-Dyer conjecture, 1960 (algebra and number theory). This conjecture is connected with the description of many solutions for algebraic equations in several variables integer coefficients. Expression $x^2 + y^2 = z^2$ can be an example of such equation. (Fermat conjecture is a special case for the Birch and Swinnerton-Dyer. Isn't it possible to prove it with the help of modular functions?).
- Cook problem, 1971 (mathematics of logic and cybernetics): is it possible that the check of problem solution is longer than the solution itself regardless of check algorithm? This problem is one of unsolved problems of logics and information science. Its solution would introduce revolutionary changes into the basics of cryptography (as the proof of the Riemann hypothesis).

The Riemann hypothesis about the noughts of Zeta function and the problem of prime numbers is the object of discussion in this article [3].

The Riemann hypothesis is closely connected with the problem of distributing prime numbers in natural series.

The simple regularity of prime numbers' distribution is still not found. There is no any effective method for detecting the primality of a number. There is no satisfactory formula for the quantity of prime numbers. In general, the extent of knowledge about features, characteristics and behaviour of prime numbers is very scant. That is why we don't have the complete picture of this phenomenon [4]. This is caused, first of all, by their exceptional complexity.

Professor of mathematics Louis de Branges de Bourcia, the Edward Elliot prize winner, from the Purdue University asserts that he had found the proof for the Riemann hypothesis that scientists of the world have been trying to solve for a century and a half. Riemann hypothesis was formulated in 1859. It deals with the distribution of prime numbers. Let us remind you that prime numbers are such numbers which can be divided without remainder only by one or themselves. Besides, there are so called "prime pairs" among prime numbers. The difference between them is 2. For example, 5 and 7 or 17 and 19. The more digits in numerical sequence, the rarer "prime pairs" are. According to Riemann hypothesis, a row of "prime pairs" is eternal, but there are no proofs for this assumption so far.

However, Louis de Branges de Bourcia announced recently that he had managed to solve the problem set by German mathematician Bernhard Riemann (1826-1866) about 150 years ago. The 23-page research of this French scientist is available in the Internet and everybody can get acquainted with it. If the scientific community conclude that the calculations made by Louis de Branges de Bourcia are correct, he will be rewarded with one million dollars by the Clay Mathematic Institute (Cambridge, MA).

The proof for Riemann hypothesis will have practical application first of all in cryptography. By the way, it should be noted that the members of the Great Internet Mersenne Prime Search (GIMPS) had recently announced that they found the biggest prime number of all known.

Professor Marcus du Sautoy from Oxford University states that the solution of Riemann problem will make it possible to understand better the "behaviour" of prime

numbers and to predict it. As Vnunet reports, this can cause the impossibility to ensure the security of electronic transactions by encryption.

Eratosthenes was a contemporary and friend of Archimed and a witty person, too. His inventions include so called "Eratosthenes sieve" that "screens" numbers searching for the prime ones. In fact, this was the first algorithm in the world that looks like a set of rules. If following these rules one will certainly get correct results: it is necessary to arrange a sequence of numbers in their natural succession beginning with one and crossing out all numbers after two – the next but one numeral; after tree – the next but two numerals; after four – the next but three numerals etc.

So, only prime numbers, which can be divided only by one or themselves, will remain. Since earliest times until Chebyshev and even to this day, researchers of prime numbers used Eratosthenes sieve. In modern literature on number theory, or "higher arithmetic" as professionals call it sometimes, the algorithm for searching prime numbers by Eratosthenes sieve is given at the beginning.

The main thing that helps to understand Riemann hypothesis is a multilateral examination of features, characteristics, criteria and interconnections of prime numbers.

At first, we will list the most important features and characteristics of prime numbers:

- Each prime number, which is more than 3, can be represented as 6k+1 or 6k-1; the converse is not correct.
- If p is a prime number then p^2-1 is multiple of 24; the converse is not correct.
- If p is a prime number then congruence $a^{\varphi(m)}$ (mod p), (a,m)=1 is correct. This means that the reminder in division $a^{\varphi(m)}$ by p is 1 (Euler theorem). The converse is not correct.
- If p is a prime number then congruence $a^{p-1}\equiv 1 \pmod p$, (a,p)=1 and $a^p \equiv a \pmod p$. (a,p)=1 is correct. This means that the reminder in division a^{p-1} by p is 1 and, thereafter, the reminder in division a^p by p is a. (Fermat's little theorem [5]). The converse is not correct.

There are other criteria (indications) of number's primality. They are essential conditions but not sufficient.

Two criteria can be an essential and sufficient condition for number's primality: Wilson theorem [6, 7, 8] and method based on the Eratosthenes sieve.

- Wilson theorem: If p is a prime number then there is a congruence:

$$(P-1)!+1 \equiv 0 \pmod p. \quad (1)$$

The converse theorem is also correct: If there is relation (1) for whole positive number p then p is a prime number. That is if sum (p-1)!+1 can be divided by p without reminder then p is a prime number.

But the point is that, even for small numbers n, number (n-1)!+1 is very large!.

If we want to know, for instance, whether number 997 is a prime number using the above mentioned criterion, we should check the divisibility of number 996!+1 (number containing 2556 decimal digits) by 997. But it is impossible to check the primality of a number even with the help of modern computers.

- Another good method of checking number's primality is the division of a number a by all prime numbers $p_1; p_2; p_3 \ldots p_n \le \sqrt{x}$. If after these operations we do not get a single number without reminder, then x is a prime number. This method is also accurate but it doesn't have practical application. Indeed, if number x is 32-ten-digit, it is necessary to divide it by all prime numbers that are less than $\sqrt{x}$. This amount of operations will be approximately equal to $\frac{\sqrt{x}}{\ln\sqrt{x}}$.

  This means that there are many divisors with numbers having up to 16 decimal digits.

In view of the foregoing, we think that our theorem on prime number criterion is in-demand.

Theorem on Prime Number Criterion: The authors are: Mukhidin Tashbulatovich Mamaraimov and Yesenbek Riskulovich Ushtenov. The certificate of authorship is registered by the Committee on Intellectual Property Rights of the Ministry of Justice of Kazakhstan under No. 067 of 19.01.2012.

Theorem: Suppose n is an odd natural number. The essential and sufficient condition for the primality of number n is the fulfillment of the following congruence:

$$(-1)^{\frac{n-1}{2}}\left(\left(\frac{n-1}{2}\right)!\right)^2+1 \equiv 0 \pmod n,$$

Proof: On the basis of Wilson theorem: if there is congruence:

(n-1)!+1=0 (mod n) (1)

then n is a prime number.

Now we transform term (n-1)! Into the following form: (n-1)!= =1•2•3•4…•(n-1)=

$$\left(\frac{n-1}{2}\right)\cdot\left(n-\frac{n-1}{2}\right)\cdot\ldots\cdot(n\text{-}4)\cdot(n\text{-}3)\cdot(n\text{-}2)\cdot(n-1)=$$

=1•2•3•4•…•

$$=1(n-1)\cdot 2(n-2)\cdot 3(n-3)\cdot 4(n-4)\cdot\ldots\cdot\left(\frac{n-1}{2}\right)\cdot\left(n-\frac{n-1}{2}\right)=$$

$$=(n-1)\cdot\left(2n-2^2\right)\cdot\left(3n-3^2\right)\cdot\left(4n-4^2\right)\cdot\ldots\cdot\left(\frac{n-1}{2}\cdot n-\left(\frac{n-1}{2}\right)^2\right); \quad (2)$$

Since terms containing n are equal to zero by module n then expression (1) can be written as follows:

$$(-1)\cdot\left(-2^2\right)\cdot\left(-3^2\right)\cdot\left(-4^2\right)\cdot\ldots\cdot\left(-\frac{n-1}{2}\right)^2+1\equiv 0 \pmod{n}; \quad (3)$$

Now we transform the last expression (3):

$$(-1)\cdot(-1)2^2\cdot(-1)3^3\cdot(-1)4^2\cdot\ldots\cdot(-1)\cdot\left(\frac{n-1}{2}\right)^2+1\equiv 0 \pmod{n}; \quad (4)$$

Finally, the congruence looks like this:

$$(-1)^{\frac{n-1}{2}}\cdot\left(\left(\frac{n-1}{2}\right)!\right)2+1\equiv 0 \pmod{n}; \quad (5)$$

The last expression (5) can be represented as follows:

$$\left(\left(\frac{n-1}{2}\right)!\right)^2\equiv(-1)^{\frac{n+1}{2}} \pmod{n}; \quad (6)$$

The theorem is proved.

The corollaries:

We can obtain two results from our theorem:

1. $\left[\left(\frac{p-1}{2}\right)!\right]^2+1\equiv 0(\bmod p),$ if $p=4k+1,$

This result is known as Sierpinsky theorem [9, 10].

2. $\left[\left(\frac{p-1}{2}\right)!\right]^2-1\equiv 0(\bmod p),$ if $p=4k+3,$

The second result has not been found in technical literature before.

The last congruence means that $(y-1)\cdot(y+1)=0(\bmod p)$, where $y=\left(\frac{p-1}{2}\right)!$. Hence it follows that:

3. $\left[\left(\frac{p-1}{2}\right)!\right]\equiv\varepsilon_p(\bmod p);\quad \varepsilon_p=\pm 1,$ for prime numbers like $p=4k+3,$

where there is no positive and negative ε_p simultaneously with one and the same prime number. Examples show that $\varepsilon_p=+1$ is fulfilled for some prime numbers and $\varepsilon_p=-1$ is fulfilled for others. We haven't found the criterion by which $\varepsilon_p=+1$ and $\varepsilon_p=-1$ are fulfilled for different prime numbers. We think that both cases will take place for countless times.

CONCLUSIONS

The method based on Eratosthenes sieve presupposes the division of given number x by all prime numbers $\le\sqrt{x}$. That is why this method is not practical.

Leibniz theorem: if n is a prime number then the following statement is correct:

$(n-2)!-1\equiv 0 \pmod{n}$,

This theorem is actually based on Wilson theorem and repeats it.

The shortcoming of Sierpinsky theorem is that it is true only for numbers like 4k+1, while it cannot be used for numbers like 4k+3.

As opposed to all previous theorems, our theorem on prime number criterion is more progressive. It differs from Wilson theorem by the fact that it has a half number of factors and consequently a half number of operations for the identification of prime number.

REFERENCES

1. Is there no more cryptography? Date view 08.09.2004 http://www.xakep.ru/post/23781/default.asp?print=true.

2. Mathematicians stand on a threshold of the abolishment of cryptography. Date view 08.10.2011 http://live.cnews.ru/forum/index.php?s=7c0313adf167b1036262e16ea951d1c6&showtopic=75841&st=0.
3. Roman, S., 2007. Advanced Linear Algebra, Publishing house: Third Edition.
4. Buhler, J., 1998. Algorithmic Number Theory: Proc. ANTS-III, Portland, OR, volume 1423 of Lecture Notes in Computer Science. Springer–Verlag.
5. Crandall, R. and C. Pomerance, 2005. The prime numbers: A computational perspertive. Second edition. Springer Publ. Berlin.
6. Vinogradov, I.M., 2009. The Basics of Number Theory. “Lan” Publishing House.
7. Trost, E., 1959. The Prime Numbers. Moscow.
8. Shoup, V., 2005. A Computational Introduction to Number Theory and Algebra. Cambridge University Press.
9. Sierpinsky, V., 1963. What We Know and What We Do Not Know About Prime Numbers. State Publishing House of Literature on Physics and Mathematics. Moscow, Leningrad.
10. Morrison, M.A. and J. Brillhart, 1975. A Method of Factoring and the Factorization of F7. Mathematics of Computation, AMS, 29(129).