International Journal of Discrete Mathematics
2016; 1(1): 30-32
http://www.sciencepublishinggroup.com/j/dmath
doi: 10.11648/j.dmath.20160101.15

Algorithm of Search of Large Prime Numbers

Kochkarev Bagram Sibgatullovich

Department of Mathematics and Mathematical Modeling, Institute of Mathematics and Mechanics Named After N. I. Lobachevsky, Kazan (Volga Region) Federal University, Kazan, Russia

Email address:
bkochkarev@rambler.ru

To cite this article:
Kochkarev Bagram Sibgatullovich. Algorithm of Search of Large Prime Numbers. *International Journal of Discrete Mathematics.* Vol. 1, No. 1, 2016, pp. 30-32. doi: 10.11648/j.dmath.20160101.15

Received: December 3, 2016; **Accepted**: December 22, 2016; **Published**: January 17, 2017

Abstract: The large number of problems in the theory of the numbers possessing one characteristic sign called by us binary mathematical statements from the natural parameter which in the time of Pythagoras and Euclid still aren't solved was prompted to us that the reason of such situation should be looked for in the mathematics bases. We have entered concept of the binary mathematical statement depending from natural parameter and have specified axiomatic of natural numbers of Peano, having added one axiom called by us the axiom of descent which is interpretation of a so-called method of descent of Fermat by means of which he has proved the Great Hypothesis for a special case of n=4. By means of a descent axiom we managed to receive a large number of the results published in Russian. Wishing to expand a readership, we have decided to give the review of our results which are already published in Russian without proofs and to add new results among which the algorithm of search of large prime numbers is dominating with proofs.

Keywords: Binary Mathematical Problem, Axiom of Descent, Algebraic Equation, Diophantine Equation

1. Introduction

The present article represents the review of the results received by the author in work [1-5], devoted to the subject touched by Pierre Fermat in his Great Hypothesis and remarks given on the fields of the book "Arithmetician" of Diophantus and published [6, 72] in 1670 by the son Fermat Clement-Samyuel in the book under the name "The Diophantine Arithmetics Contening Notes P. of De Fermat". Except the results published in [1-5] article contains also some not published results of the author yet.

2. Method

Definition 1. [4]. The mathematical statement A_n, depending from natural parameter n we will call binary if for any $n=\alpha$ A_α value has one or the other value: truth or lie.

In case of binary statements A_n Fermat has invent [7, 70] a so-called method of descent by means of which he has proved that a class of the Diophantine equations $u^n+v^n=w^n, uvw\neq 0$ for $n=4$ has no decision in a ring of integers. Method of Fermat's descent it is expedient to formulate in the form of an axiom of descent [4]: let A_n - the binary mathematical statement depending from natural parameter n it that 1) there is an algorithm which for any value n give the answer to the question " the statement of A_n is true or false?", 2) for some final series of values of the parameter $n_1<n_2<\ldots<n_k$ $A_{n_1}, A_{n_2}, \ldots, A_{n_k}$ are true and for any $n_{k+1}>n_k$ $A_{n_{k+1}}$ according to the assumption is false. Then the statement of A_n is true for an infinite set of values n.

(1). In [5] about infinity of a number of twins and Hardi and Littlewood [8,367] problem of the proof of existence of an infinite set of the three of prime numbers is easily proved: $p, p'=p+2, p''=p+6$.

(2). Definition 2. (Pythagoras) The natural number n is called perfect if $\sum_{d_i:n} d_i=n$, where $d_i\neq n$ is divider of number n.

Theorem 1 [4]. All odd natural numbers are not perfect.

Theorem 2[4]. A natural number $2^k(2^{k+1}-1), k\geq 1,$ is perfect if and only if $2^{k+1}-1$ is a prime number.

It is known [8, 37] that prime numbers of a type of 2^n-1 in literature are called Mersenn's numbers, the contemporary and correspondent of P. Fermat [7, 69].

In [4] by means of a descent axiom we have proved the theorem.

Theorem 3 [4]. The set of numbers of Mersenn is infinite.

Corollary 1 [4]. The set of perfect numbers is infinite.

Corollary 2 [4]. The sequence of numbers $2^n-1, n=1,2,...$ contains an infinite set of prime numbers.

By means of a descent axiom we have also easily proved (any prime $4n-1$ number never is the sum of two squares) statement for which proof required to Euler [6, 73] seven years of work.

(3). Theorem 4 [4]. (Binary problem of Goldbach-Euler). Each even number, since 4, can be presented in the form of the sum of two prime numbers

Corollary 3 [4]. (Euler) Each odd number, since 7, can be presented in the form of the sum of three prime numbers.

Corollary 4 [5]. Whatever even number $2n, n \geq 2$, was, there will be a prime number p such that $n \leq p < 2n$ and if n is compound, then $n < p < 2n$ and $2n = p + p'$, where $p' < n$ is a prime number.

Theorem 5 [4]. Slightly excess numbers [6,29] don't exist.

3. New Results

Corollary 5 to theorem 2. Mersenn's numbers are never representable in the form of the sum of two squares.

Proof. Let 2^n-1 be Mersenn' number, i.e. it is a prime number. Obviously, $2^n-1 = 4\cdot 2^{n-2}-1 = 4n'-1$.

In Fermat's notes there is a statement [9, 11], that all numbers of a type $2^{2^n}+1$ are primes but Fermat is the statement has accompanied with a mark that he has no him the satisfactory proof. With some specification of this statement easily by means of an axiom of descent the theorem is proved.

Theorem 6. The sequence of numbers $2^{2^n}+1, n=1,2,3,4,...$ contains infinitely many prime numbers.

Proof. It is easy to be convinced that $2^{2^n}+1$ gives prime numbers for natural $n=1,2,3,4$ and for $n=5$ Euler has shown [9, 11], that $2^{2^5}+1$ is a composite number. We will assume the theorem for $n_1=1, n_2=2, n_3=3, n_4=4, n_5$ is fair, and for any $n_6 > n_5$ $2^{2^{n_6}}+1$ is a composite number. Then on an axiom of descent $2^{2^{n_5}}+1$ is also a composite number that contradict the inductive assumption. The received contradiction proves the theorem. We will notice that according to [8, 38] $n_5 \geq 17$.

Definition 3. We will call prime numbers of a type $2^{2^n}+1$, $n=1,2,3,4,n_5,...$ Fermat's numbers.

We will consider the sequence of numbers $2^n+1, n=2,3,4,...$. Obviously, this sequence of numbers includes the sequence of numbers of a type $2^{2^n}+1, n=1,2,3,...$, and consequently Fermat's numbers in the structure. It is easy to show [8, 35] that the prime numbers entering these sequences coincide and as $2^n+1 = 4\cdot 2^{n-2}+1 = 4n'+1, n \geq 2$ they according to the theorem 2 [5] are representable in the form of the sum of two squares. If n has an odd divider $a>1$, then from [8, 35] follows that 2^n+1 is a composite number. From here also follows.

Theorem 7. If n is a prime number, $n \geq 3$, then 2^n+1 is the work $3\cdot p$, where p is a prime number.

Proof. We will assume $p_1 > 2$ there is the first prime number in a natural number sequence. In this case we have $2^{p_1}+1 = 9 = 3\cdot 3$. If $p_2 = 5$, then $2^{p_2}+1 = 33 = 3\cdot 11$. We will assume for p_k takes place $2^{p_k}+1 = 3p'$, where p' is a prime number, and for p_{k+1} $2^{p_{k+1}}+1 = 3t$, where t is a composite number. Then on an axiom of descent $2^{p_k}+1 = 3t'$, where t' is also a composite number, and it contradicts the inductive assumption. The received contradiction proves the theorem.

The proved theorem to us delivers an algorithm of search of large prime numbers. If p is a prime number, $p>3$, then $2^p+1 = 3\cdot p'$, where $p' > p, p' = \frac{2^p+1}{3} = \frac{2^p+1}{2^{\log_2 3}} > 2^{p-\log_2 3}$.

4. Class of Diophantine Equations of Fermat

It is known [7, 70] that the Diophantine equation $u^2+v^2=w^2$ which solution Fermat has studied from the book "Arithmetician" of Diophantus has formed for him a basis for the formulation of the well-known hypothesis. In [3] we have offered a method of the solution of the equation $u^2+v^2=w^2$ of Pythagoras by the reduction him to a class of the algebraic equations $(x-i)^2+(x-j)^2=x^2$ from two natural parameters.

Fermat has generalized the specified equation and on fields of the book "Arithmetician" of Diophantus [7, 70] against of equation $u^2+v^2=w^2$ he has written: "it is impossible to spread out neither a cube to two cubes, nor a biquadrate on two biquadrates, and in general any degree, big a square on two degrees with the same indicator. I have opened to it really wonderful proof, but this field for it is very narrow".

In [1],[10] we have proved stronger statement, than the statement formulated by P. Fermat.

Theorem 8 [10]. The Diophantine equation $u^n+v^n=w^n, n \geq 3, uvw \neq 0$ has no decision not only in a ring of integers, but also in the field of rational numbers.

We will notice that the proof of the theorem 8 at the same time give an algorithm of the proof of this statement for any concrete $n \geq 3$ whereas others, starting with Euler proved this statement only for some n.

In 1995 article has been published in Annals of Mathematics (USA) [11] which has caused a lot of noise in the press and some publications, for example, in the form of the monograph [6] and on the Internet [12].

From theorem 8 follows that this article, unfortunately, wrong as the elliptic curve of Frey according to the theorem 8 in the nature doesn't exist.

In the history of mathematics such cases happened: so, for example, the 21 st problem of D. Gilbert "has been positively solved" at the beginning of the 20 th century by the mathematician E. Plemel, but in 70 years the mathematician A. A. Bolibrukh has noticed an error in E. Plemel's proof and has solved D. Gilbert's problem has the negative decision [13].

We weren't satisfied with the proof of the specified statement (the theorem 8) and have closed a question of solution of the Diophantine equation of Fermat.

Theorem 9 [10]. The Diophantine equation of Fermat for $n = 3, 4$ has decisions in radicals.

Theorem 10 [10]. The Diophantine equation of Fermat for $n \geq 5$ algorithmically unsoluble.

Obviously, justice of the Great Hypothesis of Fermat as the result follows from the results received above.

At last, in [2] we have formulated a problem: to find natural numbers pressing between $n-1$ and n degrees.

This problem has the infinite number of decisions for $n = 2$, the unique decision 26 for $n = 3$ (Fermat) and there are no decisions for $n \geq 4$ [14]. Though this problem has been published by us in 2014 [2] and we have thrown a call to fans and to mathematical community to prove it, we still haven't received a response to our call.

5. Conclusion

From the history of mathematics is well known [15] that many mathematical problems, seemingly insurmountable, with proper revision foundations of mathematics are solvable. Analisis of this type of problems in the theory of numbers helped us by introducing the concept of binary mathematical statements and corresponding adjustements of axioms of natural numbers Peano, solve the problems, which the age of some of them reaches more than 2500 years.

References

[1] Kochkarev B. S. Ob odnom klasse algebraicheskikh uravnenii, ne imejutchikh ratsionalnykh reshenii. Problems of modern science and education. 2014. 4 (22), s. 9-11 (in Russian).

[2] Kochkarev B. S. Ob odnom svoistve naturalnykh chisel. Problems of modern science and education. 2014. 7 (25), s. 6-7 (in Russian).

[3] Kochkarev B. S. Svedenie odnogo Diophantova uravnenija k klassu algebraicheskikh uravnenii ot dvukh naturalnykh parametrov. Problems of modern science and education. 2015. 7 (37), s. 6-7 (in Russian).

[4] Kochkarev B. S. K metodu spuska Ferma. Problems of modern science and education. 2015. 11 (41), s. 7-10 (in Russian).

[5] Kochkarev B. S. Problema bliznetsov i drugie binarnye problem. Problems of modern science and education 2015. 11 (41), s. 10-12 (in Russian).

[6] Singkh S. Velikaya teorema Ferma. MTSNMO. 2000. s. 288.

[7] Samin D. K. Sto velikikh uchenykh. Moskow, "Veche". 2001. S. 592 (in Russian).

[8] Bukhshtab A. A. Teoriya chisel. Moskow. Izd. "Prosvetchenie". 1966, s. 384 (in Russian).

[9] Postnikov M. M. Vvedenie v teoriju algebraicheskikh chisel. Moskow, "Nauka" Glavnaya redaktsiya fiziko-matematicheskoy literatury, 1982. s. 240 (in Russian).

[10] Kochkarev B. S. About one binary problem in a class of algebraic equations and her communication with the Great Hypothesis of Fermat. International Journal of Current Multidisciplinary Studies. Vol. 2, Issue, 10, pp. 457-459, October, 2016.

[11] Wiles A. Modular elliptic curves and Fermat's Last Theorem. Annals of Mathematics, v. 141 Second series 3 May 1995 pp. 445-551.

[12] Abrarov D. Teorema Ferma: fenomen dokazatelstva Uailsa. http: //polit.ru/article/2006/12/28/abrarov/.

[13] Kudryavtsev L. D. O matematike//Tezisy dokladov Mejdunarodnoi nauchno-obrazovatelnoi konferentsii 23-27 marta 2009 goda. Nauka v Vuzakh: matematika, fizika, informatika. Moskow, RUDN, 2008 (in Russian).

[14] Kochkarev B. S. Otlichitelnoe svoistvo naturalnykh chisel v razlichnykh geometriyakh. Problems of modern science and education 2015. 5 (35), s. 6-9 (in Russian).

[15] Laptev B. L. Nikolai Ivanovich Lobachevsky. Izd. Kazanskogo universiteta. 1976. s. 136 (in Russian).