International Journal of Discrete Mathematics
2018; 3(2): 32-35
http://www.sciencepublishinggroup.com/j/dmath
doi: 10.11648/j.dmath.20180302.11

An Binary Problem of Goldbach Euler and Its Generalization

Bagram Sibgatullovich Kochkarev

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

Email address:
bkochkarev@rambler.ru

To cite this article:
Bagram Sibgatullovich Kochkarev. An Binary Problem of Goldbach Euler and Its Generalization. *International Journal of Discrete Mathematics.* Vol. 3, No. 2, 2018, pp. 32-35. doi: 10.11648/j.dmath.20180302.11

Received: March 30, 2018; **Accepted**: May 3, 2018; **Published**: May 24, 2018

Abstract: We prove that for any even positive integer 2k greater than 6 one can find a pair of primes one of which is less than k and the other is greater than k and their sum is 2k. The article shows that such property of even numbers allows to build effective cryptographic systems.

Keywords: Prime Numbers, Binary Problem, Axiom of Descent

1. Introduction

The Goldbach binary problem is a statement that any even number starting with 4 can be represented as a sum of two primes. This problem is a well-known open mathematical problem together with the Riemann hypothesis included under number 8 in the Hilbert problem list (1900) and is one of several Hilbert problems still unresolved for 2018.

Still Euler in correspondence with Goldbach in 1742 it was observed that from the validity of the binary Goldbach problem it follows that any odd number starting with 7 can be represented as an sum of three primes. This statement, unlike the binary Goldbach problem, is called the ternary Goldbach problem.

In 1923, Hardy and Littlewood's mathematicians shoved that in the case of some generalization of Riemann's conjecture, the ternary Goldbach problem is true for all sufficiently large odd numbers.

In 1937 Vinogradov [1] presented a proof independent of the validity of the Riemann hypothesis, i.e. proved that any sufficiently large odd number can be represented as a sum of three primes.

Finally, in 2013, Harald Helfgott [2] proved the ternary Goldbach problem.

We published (in Russian) the solution of some problems [3-4] discovered in number theory, but apparently the American reader is not able to get acquainted with it. In order not to repeat the publication of these papers, we have decided in this paper to generalize this binary Goldbach-Euler problem from which the binary Goldbach-Euler problem follows immediately and to give an overview of the results from [3-4] without proof. In addition, the theorem proved in the paper is useful for creating effective cryptographic system by constructing appropriate algorithms for finding pairs of Prime number $p, p', p \neq p'$ satisfying the condition $p + p' = n$.

2. The Proof of the Main Theorem

First of all, let us recall [3] the mathematical definition of a binary statement from the natural parameter n .

Definition. An mathematical statement A_n , depending on natural parameter n we will call binary if for any value $n = \alpha$ the statement A_α has one or the other values: truth or lie.

In case of binary statements A_n Fermat has invent 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 decent it is expedient to formulate in the form of an axiom of descent [3].

Axiom of descent [3]: let A_n will be the binary statement from natural parameter n such that:

1. There is an algorithm which for any value n gives the answer to the question "statement A_n truth or lie";

2. For values of parameter $n_1 < n_2 < ... < n_k$ the statements

$A_{n_1}, A_{n_2},,,,, A_{n_k}$ are true, and for any $n_{k+1} > n_k$ the statement $A_{n_{k+1}}$ is fals.

Then the statement A_n is true for infinitely many values n.

Example [4]: prime numbers twins – couple of odd prime numbers with perhaps small difference 2. Obviously, problem: the number of twins of course or not, is the binary problem meeting descent axiom conditions. The theorem 4 [4] about infinity of a number of twins is easily proved. Note that we in our work [4], published in Russian also solved the problem of Hardy and Littlewood [5, 367] proof of the existence of infinitely many such triples of primes: $p, p' = p+2, p'' = p+6$ and four primes: $p, p' = p+2, p'' = p+6, p''' = p+8$ and so on …. Among the most significant for Pythagoreans of natural numbers there were so-called "perfect" numbers. The natural nember n is called perfect if $\sum_{d_i \vdots n} d_i = n$, where $d_i \neq n$ is divider of number n. All degrees of number 2 slightly "don't get" before perfect as the sum of their dividers is always one unit less than the number. In other words, all degrees of the two are slightly defective. Two centuries later [6, 28]Euclid has opened, that perfect numbers are always multiple to two numbers, one of which is equal to number 2 degree, and another is one unit less than the following degree of number 2, i.e. the perfect number is representable in the form $2^k(2^{k+1}-1)$. In 18 century Euler has proved [5, 318] that Euclid's formula exhausts all set of even perfect numbers.

Theorem 1 [3]. Natural number $2^k(2^{k+1}-1), k \geq 1$, is perfect only in case when if $2^{k+1}-1$ is a prime number.

It is known [5, 37] that prime numbers of a type of $2^n - 1$ in literature are called Mersenn's numbers. It is easy to be convinced that number $2^n - 1$ can be both prime, and compound. In [3] by means of a descent axiom we have proved that the set of numbers of Mersenn is infinite. In [3] we also have proved, that set of perfect numbers is infinite and sequence of numbers $2^n - 1, n = 1, 2, \ldots$ contains an infinite set of prime numbers. We will notice that this sequence of numbers unlike an arithmetic progression of the theorem 337 Dirichlet [5, 356], has that property that distances between the next numbers increase and strive for infinity. 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. We also have proved [7], that Mersenn's numbers are never representable in the form of the sum of two squares.

In Fermat's notes there is a statement [8, 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 is proved, that the sequence of numbers $2^{2^n}+1, n = 1, 2, 3, 4, \ldots$ contains infinitely many prime numbers [9]. we also have proved [9], that if n is a prime number, $n \geq 3$, then $2^n + 1$ is the work $3p$, where p is a prime number.

Theorem. For any even number $n > 6$ there is a pair of primes p, p' such that $p < \frac{n}{2}, p' > \frac{n}{2}$ and $p + p' = n$.

Proof. Denote the statement of the theorem though A_n Obviously, it is a binary statement that satisfies the condition of the axiom of descent. For $n = 8$ we have $8 = 3 + 5$, for $n = 10$ we have $10 = 3 + 7$,…, for $n = 2k$ suppose $2k = p + p'$, where $p < k, p' > k$ are two prime numbers, and for $n = 2k + 2$ there is no pair of Prime numbers $p < k+1, p' > k+1$ such that $p + p' = 2k + 2$. Then, according to the descent axiom, for $n = 2k$ there is also no pair of primes $p < k, p' > k$ such that $p + p' = 2k$ but this contradict the inductive assumption. Hence the fairness of our theorem follows.

Corollary. The proven theorem implies a binary Goldbach problem.

Proof. Indeed, since 4=2+2 and 6=3+3, according to the proven theorem, all even numbers starting with 4 are represented as the sum of two primes.

We published (in Russian) the solution of some problems [3-4] discovered in number theory, but apparently the American reader is not able to get acquainted with it. In order not to repeat the publication of these papers, we have decided in this paper to generalize this binary Goldbach-Euler problem from which the binary Goldbach-Euler problem follows immediately. In addition, the theorem proved in the paper is useful for creating effective cryptographic system by constructing appropriate algorithms for finding pairs of Prime number $p, p', p \neq p'$ satisfying the condition $p + p' = n$.

Using the main theorem, we can offer the following cryptographic system when encrypting information: if the alphabet of the langage in which the information is written contain n characters, then to encrypt the information, you must select n distinct even numbers greater than 6 and find for each of these even numbers $2k$, according to the main theorem, a pair of primes p, p' such that $p + p' = 2k$. In encryption, one of the two possibilities p or p' is selected for each character. Therefore, if the word contains t distinct characters, then the number of distinct possibilities will be 2^t, that is exponent, and to decode the information would be difficult.

In [9-10] we showed that every finite Hardy and Littlewood sequence of primes $p_1, p_2, \ldots, p_k$ with possibly small difference satisfies $p_k - p_{k-1} = 2(k-1)$. This statement, which is obviously binary, is proved according to the General scheme of the proof using the descent axiom. It follows from this that for any even natural $2k, k = 1, 2, \ldots$ there are infinitely many pairs of prime p, p' such that $p' - p = 2k$. Hence, as a special case, the infinity of the set of prime numbers of twins follows. It we take into account the idea of information encryption, described using the proven generalized Goldbach-Euler binary problem, it is clear how to apply the same idea of information encryption, using, for example, prime twins numbers.

3. Conclusions

From the history of mathematics it is known [11] that many mathematical problems seem unsolvable, with careful analysis of the foundations of mathematics are solvable. Thus, in 1826 Lobachevsky discovered the non-Euclidean (hyperbolic) geometry.

The analysis of such problems in number theory allowed us to introduce the notion of binary mathematical statement and refinement of Peano axiomatics, to solve the problems [3-4, 7, 9-10] some of which are older than even 2000 years.

In this regard, it should be noted, that in 1995, more than 20 years ago, an erroneous work [12] was published, for which the author received more than a dozen prestigious prizes, including the Abel prize, and which is still on the internet considered as correct. Error of work [12] is proved in articles [13-14].

In 2017, we published [15], which gives a definitive solution to Hilbert's Tenth problem.

It is known that in 1970 the mathematical community accepted the proof of Hilbert's tenth problem presented by Matiyasevich Yu. V. In 2014, we published a paper [16], which disprove the theses Turing, Church and Markov. Therefore, the unsolvability of tenth problem of Hilbert's published in [17] cannot be considered as correct. Note, that 10-th Hilbert problem really unsoluble, as Diofantine equations Fermat for $n>4$ is generally insoluble [13], not only in integers.

In [13] it was shown that equations of Fermat $u^n+v^n=w^n$ for $n>4$ in general algorithmically unsolvable. Hence, as a consequence implies the unsolvabilitiy of the tenth problem of D. Hilbert [15]. Therefore the proof of the unsolvability of Hilbert's tenth problem by Matiyasevich is incorrect, since uses Church's thesis which for the reason [16] is incorrect.

In General any mathematical statement, in the proof of which one of the theses of formal, algorithms is used, cannot be considered as proved, since in [16] an algorithm is constructed that fits into the intuitional concept of the algorithm, but not is equivalent to the formal concept of algorithm.

In the 30s and 40s of the last century, mathematicians in England, the USA and the USSR attempted to formalize the intuitive notion of algorithm. In England Turing in 1937, introduced the concept of machines later named after him, in the United States in the 30's 40-ies of the Church and Post introduced the notion of recursive functions and effective computability, and finally in the late 40's and early 50-ies of the last century in the USSR Markov introduced the notion of normal algorithm. These objects served as a means to process information, which is any algorithm in an intuitive sense. The form of setting the initial information to be processed for these objects is different, but these forms can be reduced to one another by means of appropriate transcoding and the main question was in comparison of their capabilities. As a result of researches of these objects their mutual equivalence [18] has been proved and this circumstance has prompted authors of these objects to declare the corresponding theses which essence consists, for example, on an example of the Turing machine, in the following: if there is some algorithm intuitively, is possible to construct the Turing machine equivalent to this algorithm.

In this paper, we refute Turing's thesis, and together with it Church and Markov's theses, due to the equivalence of the corresponding formal concepts of algorithms [18].

The most exceptional phenomenon in the mathematical world of the last century was the work of D. Hilbert, who determined the prospects for the development of mathematics for the twentieth century by its problems formulated at the Congress of mathematicians in Paris in 1900.

Perhaps the most prolific issue was the last issue of the Farm associated with the well-known Diophantine equations. Fermat's problem has been dealt with since the date of its formulation (1637) by almost all known mathematicians, beginning with Euler, but the proof that Fermat's Diophantine equations have no solutions in integers has been obtained only for individual values of n. In the 19th century Kummer shoved [5, 117] that the full proof of Fermat's great theorem lay beyond the possibilities of existing mathematical approaches (at that time Peano axiomatics was not and Fermat's descent method was not fully understood). As noted above, one erroneous work was published in 1995 [12], unfortunately, until now the mathematical community has not recognized it, although more than 20 years have passed and both works with a full solution of this problem appeared in the press [13], and works [14], indicating the inaccuracy of the work [12].

To solve this problem with almost 400 years of experience managed by reducing the class of Fermat Diophantine equations to the equivalent class of algebraic equation:

$$(x-2)^n+(x-1)^n=x^n, n>2.$$

It turned out that for $n=3,4$ Fermat's equations have solution in radicals, and for $n>4$ they are algorithmically unsolvable.

And Hilbert touched upon this problem in his report by formulating his Tenth problem on the definition of solvability of an arbitrary Diophantine equation in integers. The studies related to the mentioned problems have received their final results. That is the final solution of Farm and gave the final solution of Hilbert's Tenth problem. Because for n>4 Fermat's equations in general intractable [13], whener it follows the unsolvability of Hilbert's Tenth problem in General, not only in integers [15], and for n=3, 4, Fermat's Diophantine equations have solutions in radicals, and in rational numbers there are no solutions. In this regard, note that the work [12] no useful information for mathematics does not carry.

Finally, note also that [6], [13-14] show that modular forms and elliptic curves have nothing to do with Fermat's Diophantine equations.

References

[1] Vinogradov I. M. Represantation of an odd number as a sum of three primes. Dokl. Akad. Nauk. SSR 15 (1937). 291-294.

[2] Helfgott. La conjectura debil de Goldbach. Gac. R. Soc. Mat. Esp. 16 (2013) no 4.

[3] Kochkarev B. S. K metody spuska Ferma. Problems of modern science and education. No 11 (41) (2015). 7-10. (in Russian).

[4] Kochkarev B. S. Problema bliznetsov I drugie binarnye problemy. Problems of modern science and education. No 11 (41) (2015). 10-12. (in Russian)

[5] Bukhshtab A. A. Teoriya Chisel. Izd. "Prosvetchenie", Moskva. 1966. 384s.

[6] Singh S. Velikaya teorema Ferma.-M.: Izd. Moskovskogo Tsentra nepreryvnogo obrazovaniya, 2000. 288 s. (in Russian).

[7] Kochkarev B. S. Algorithm of Search of Large Prime Numbers, International Journal of Discrete Mathematics, Jan. 17, 2017, 30-32.

[8] Postnikov M. M. Vvedenie v teoriyu algebraicheskikh chisel. Moskva, "nauka" Glavnaya redktsiya fiziko-matematicheskoy literatury, 1982, s. 240 (in Russian).

[9] Kochkarev B. S. Axiom of Descent and Binary Mathematical Problems, American of Engineering Research (AJER) Volume-7, Issue-2 pp. 117-118.

[10] Kochkarev B. S. Infinite Sequences Primes of Form 4n-1 and 4n+1, International Journal of Humanities and Social Science Invention, Vol. 5, Issue, 12. December, 2016, pp. 102-108.

[11] Laptev B. L. Nikolai Ivanovich Lobachevsky izd. Kazanskogo Universiteta. 1976. 136 s.

[12] Wiles A. Modular elliptic curves and Fermat's last theorem. Annals of Mathematics. V. 141 Second series 3 May 1995 pp. 445-551. International Journal of Disctete Mathematics, Jan. 17, 2017, 30-32.

[13] 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.

[14] Kochkarev B. S. About One Binary Problem in a Certain Class of Algebraic Equations and its Connection with the Great Hypothesis Farm, https://dspace.kpfu.ru/xmlui/bi9tstream/handle/net/...

[15] Kochkarev B. S. About Tenth Problem of D. Hilbert, American Journal of Engineering Research (AJER), 2017, Vol. 6, Issue, 12, pp. 241-242 www.ajer. Org Open Access.

[16] Kochkarev B. S. Ob odnom algoritme, ne soglasuyutchemsya s tezisami Turinga, Chercha I Markova, Problems of modern Science and Education, 2014, 3 (21)23-25 (in Russian).

[17] Matiyasevich Yu. V. Diophantine sets, Uspekhi Matematicheskikh Nauk, 27:5 (167) (1972), 185-222 (NN Russian)

[18] Igoshin V. I. Matematicheskaya logika I teoriya algoritmov. Moskva, Academia, 2004, s. 448.