Acta Mathematica Nitriensia
Vol. 8, No. 1, p. 1 – 10
ISSN 2453-6083

Fundamental Contributions in the History of Number Theory

Viliam Ďuriš[1] – Veronika Bojdová[1] – Timotej Šumný[2]

[1*]*Department of Mathematics Faculty of Natural Sciences and Informatics Constantine the Philosopher University in Nitra, Tr. A. Hlinku 1, 949 74 Nitra, Slovakia*
[2]*Štefan Moyses Primary School, Školská 608, Tesárske Mlyňany, Slovakia*
Received March 28, 2022; received in revised form March 29, 2022; accepted April 1, 2022

Abstract

The present contribution is devoted to the history of Number theory and mentions the most important mathematicians who contributed to the field of Number theory through several significant open problems. The article also shows one of the possible approaches to prove the Fermat's Last Theorem as a Millennium Prize Problem for $n = 4$ using a division relation and some properties of Diophantine equations.

Keywords: Fermat's Last Theorem, Number theory history, proof

Classification: 01A99, 11D25, 03B35

1 A brief historical overview

Throughout human history, great importance has been attached to the number as such. One of the most important philosophical principles of Pythagoras' was his assertion: "*the number is the essence of things*". Natural numbers, positive fractions and their various properties were first explored by the Pythagoreans [1] sometime around the mid-6th century BC. The Pythagoreans paid close attention to issues of divisibility. In particular, they looked at even and odd numbers and developed a whole theory of "even and odd", which Euclid later included in his "Elements" [2 - 5] as a separate book. The Pythagoreans used the relation of a number to the sum of all its divisors to divide all natural numbers into so-called **abundant numbers**, where the sum of all divisors was greater than the given number, **perfect numbers**, where the sum of all divisors was equal to the given number, and **deficient numbers**, where the sum of all divisors of the given number was smaller than the given number [6]. The Pythagoreans also introduced **amicable numbers**: the pairs of numbers, where the sum of all divisors of one number was equal to the other number and vice versa.

At the beginning of the Alexandrian period (in the last third of the 4th century BC), a book titled "Elements" appeared. Its glory had not yet been overshadowed by any other work in the history of mathematics. A book written by Euclid, one of the greatest mathematicians in all of history. Even though Elements undoubtedly served as the main tool for teaching geometry, it also dealt with Number theory and arithmetic structures. Some sections in Euclid's Elements relate to divisibility and the Euclidean algorithm.

*Corresponding author; email: vduris@ukf.sk
DOI: 10.17846/AMN.2022.8.1.1-10

Greek mathematician Diophantus of Alexandria, who was active around 250 AD, also contributed significantly to Number theory. During this period, he compiled a work titled "Arithmetica" ("science of numbers") [7-10] in which he focused on the algebraic Number theory and Theory of equations. Diophantus (so-called "father of algebra") significantly influenced mathematics for many next centuries with this work. The original Diophantus' work consisted of 13 volumes, but only six were preserved. Arithmetica contained 130 equations – they were named as "Diophantine" later. Solutions to many Diophantine equations (e.g. exponential) remained unknown for many centuries.

During the Middle Ages, Arabian mathematicians also looked at many problems nowadays included in Number theory - mainly problems of indeterminate equations, congruences and divisibility. One of the first works dealing with them was Abū Kāmil's book "Kitāb al-ṭarā'if fi'l-ḥisāb" [11-12], whose Arabian transcript from somewhere around 1211 – 1218 had been preserved. The content of the book focused on solving systems of linear indeterminate equations whose roots are to be ordered groups of natural numbers.

Persian mathematician and engineer Abū Bakr Muḥammad ibn al Ḥasan al-Karajī provided examples of non-linear indeterminate equations in his work "Al-Fakhri". He took some of the problems and solutions directly from Diophantus' "Arithmetica" (3rd century AD). An attempt by Abū Maḥmūd Ḥāmid ibn al-Khiḍr al-Khujandī in the last century of the first millennium AD to prove the non-existence of an integer solution for equation $x^3 + y^3 = z^3$ may also be considered as an original contribution to Number theory, even if the proof was not sufficient.

A great interest in Number theory emerged in the 17th century in France and later also in other Western European countries after the French translation of Diophantus' "Arithmetica" by Claude-Gaspard Bachet de Méziriac (1581 – 1638) was published. The group of enthusiasts and people interested in the translation of "Arithmetica" included also lawyer and advisor to the Parliament of Toulouse Pierre de Fermat, advisor to the Mint Office Bernard Frenicle de Bessy, mathematics teacher Jacques de Billy, monk Marin Mersenne [13], philosopher René Descartes and philosopher, mathematician and physicist Blaise Pascal. Later on, the English (e.g. Wallis or Brouncker) and the Dutch (e.g. Huygens or Schooten) also became involved in Number theory. Pierre de Fermat brought key knowledge to Number theory during this period and he is also the author of one of the key methods for proving theorems in Number theory – "the method of infinite descent". Fermat formulated several problems related to prime numbers known as **Fermat numbers, Fermat primes** or **Fermat's Little Theorem**.

Fermat was also interested in representability of primes by various quadratic forms (e.g. $x^2 + y^2$). Some of the knowledge he gained had already been known to Diophantus, such as e.g. the fact that those primes in the form of $4n + 1$, where n is a natural number, are representable by the form $x^2 + y^2$. In his commentary to Diophantus' "Arithmetica" in 1621, Bachet de Méziriac formulated his conjecture that every natural number can be represented as the sum of at most four natural numbers´ squares. Fermat expanded this conjecture into an assertion that every natural number is either n-gonal or it is the sum of several n-gonal numbers. Later, the most prominent mathematicians of the 18th and 19th [11-12] century, such as Euler, Lagrange, Gauss or Cauchy devoted their time to solve this problem.

The 17th century also brought an advancement in understanding the solution to indeterminate equations. Bachet de Méziriac, using examples with specific coefficients, demonstrated in detail the solution to linear indeterminate equation $ax - by = 1$ with unknowns x, y and positive integer coefficients a, b, where the values of the root (x, y) had to be natural numbers. The collection of these problems was published under the title "Problèmes plaisants et délectables qui se font par les nombres" in Lyon in 1612 and afterward it was repeatedly published until the second half of the 20th century. In 1657, Fermat formulated a problem of finding the root (x, y) of equation $ax^2 + 1 = y^2$ within the range of natural numbers, where coefficient a is a non-square natural number. It´s called the "Pell's equation" nowadays, since in the 18th century Leonhard Euler mistakenly attributed its ownership to English mathematician John Pell. The significance of this equation as a means of finding the general method for solving indeterminate equations was not understood in the 17th century. An effective solution to the equation was presented only later by Euler and Lagrange and its generalization was presented in 1846 by Peter Gustav Lejeune-Dirichlet (1805 – 1859). During this period, Fermat also looked at many other more generally formulated problems that were not solved by his contemporaries. Among the best known was also the unsolvable equation $x^n + y^n = y^n$ for $n \geq 3$, which is nowadays known as Fermat's Last Theorem [14] (Section 2). The validity of this theorem was proven by English mathematician Andrew Wiles in 1994 and published in 1995 by his article "Modular Elliptic Curves and Fermat's Last Theorem". The whole Number theory up to Gauss was based on the direction set by Fermat in the middle of the 17th century through his problems, methods and results. Fermat's work had a significant impact on the development of other branches of mathematics in the 19th and 20th century, such as algebra, arithmetic or geometry.

In the 18th century [11-12], Number theory dealt mostly with problems formulated earlier in the 17th century. The only mathematician who, after 1730, dealt with Number theory problems in a greater extent was Euler. In 1736 he proved the so called Fermat's Little Theorem, which states that $a^{p-1} \equiv 1 (\operatorname{mod} p)$ holds for any natural number a and prime p. Later on, in 1760, after the introduction of the so called Euler function $\varphi(n)$, he showed the validity of congruence $a^{\varphi(m)} \equiv 1 (\operatorname{mod} m)$, which is a generalization of Fermat's Little Theorem. Euler was also interested in the problem of integer roots of Pell's equation, on which he published several articles and introduced his own method of problem solving, which, however, lacked the proof that the method always lead to the root and that it allowed to obtain all the roots. Proof of the existence and form of the roots was brought only by Lagrange. The validity of Fermat's Last Theorem was proved by Euler for $n = 3, 4$.

For $n = 5$ this theorem was proved only by Legendre in 1823. Further interest in Number theory was brought on by Fermat numbers in the form $2^{2^n} + 1$, which were primes for $n \in \{0,1,2,3,4\}$. In 1732 Euler showed that for $n = 5$ the Fermat number was not a prime. At the end of the century, Gauss explained the importance of these numbers for the construction of regular polygons. Euler examined most of Fermat's assertions. In 1754 –1755 he proved Fermat's assertion that each prime in the form of $4n + 1$, where n is a natural number, is the sum of two squares of natural numbers. He also achieved some results in proving Fermat's assertion that each natural number is the sum of at most four natural number squares. The theorem was finally proved by Lagrange by using Euler's results. Euler also published several results on decomposition of certain expressions with exponents of natural numbers and on perfect and amicable numbers. In 1770, Edward Waring (1734 – 1798) showed that every natural number is either the 3rd power of a natural number or it is the sum of at most nine 3rd powers of natural numbers. He also showed that every natural number is either the 4th power of a natural number or the sum of at most nineteen 4th powers of natural numbers. One of the best known and still unproved problems of Number theory is from 1742, the so called Goldbach conjecture. It states that every even natural number is the sum of two prime numbers. Another conjecture based on this hypothesis. It states that every odd natural number is either a prime number or the sum of three prime numbers. Another significant result of the 18th century is the so called Wilson's theorem formulated by mathematician John Wilson (1741 – 1793), which states that number $(p-1)!+1$ is divisible by number p if and only if p is a prime number. This theorem was proved by Lagrange in 1773.

Euler introduced several terms in Number theory such as quadratic residue and quadratic nonresidue in the law of quadratic reciprocity, which was probably the most important Number theory discovery of the 18th century, and his work and results despite the lack of strict proofs in several areas were generally accepted by the great mathematicians of the 18th and 19th century (e.g. by Gauss or Legendre). It was Legendre who included the problems that Euler studied in his work "Théorie des nombres" which was published in 1798 and summarized the Number theory results of the 18th century.

The development in Number theory in the 19th century [8 - 9] was guided by Gauss' work from 1801, "Disquisitiones arithmeticae", in which he summarized and systematized results of previous centuries and developed solutions in three important areas – in congruence theory, algebraic number theory and theory of forms. Gauss followed up on the research of Euler and Legendre from the 18th century. The proof of the law of quadratic reciprocity by Euler was an excellent result. In the second and third decades of the 19th century, Gauss examined the topic of cubic and biquadratic congruences. He introduced the concept of a complex integer in the form of $a+b\mathrm{i}$, where a, b are integers, the concept of complex prime number as a complex integer non-divisible by other complex integer apart from itself and numbers one ± 1 and $\pm \mathrm{i}$, and the concept of an odd complex integer which is non-divisible in the domain of complex integers by number $1+\mathrm{i}$. Gauss also formulated the law of reciprocity for biquadratic residues which was later proved by Jacobi and Eisenstein. The first attempts to introduce the new concept of algebraic numbers into Number theory were related to the effort to generalize Gauss' concept of complex integers and to the attempt of Ernst Eduard Kummer (1810 – 1893) to prove Fermat's Last Theorem. In 1843, Kummer attempted a comprehensive theory of algebraic integers, which, however, contained an error in its assumption on the validity of theorem of the unique factorization of algebraic numbers to algebraic primes. Despite that, Kummer's approach was successful in proving Fermat's Last Theorem for many prime exponents. Kummer's student Leopold Kronecker (1823 – 1891) approached the building of algebraic Number theory in a more general way. Kronecker introduced new terminology and showed the validity of several relationships (e.g. he defined the so called modular systems). Algebraic Number theory in its current form comes from Dedekind who published it in 1871. Dedekind also introduced terms number field, number ring or ideal within algebraic number theory. Algebraic number theory was successfully concluded in the 19th century by Hilbert who first engaged in this topic in 1892 and in 1897 he published many new results. Another number theory problem – the theory of forms was studied by Gauss (e.g. quadratic forms $ax^2 + 2bxy + cy^2$ with integer coefficients and allowed integer values of variables x, y, that are nowadays referred to as quadratic Diophantine equations). The main motive of interest in the topic of forms was the intention to develop Number theory and produce new results. The theory of forms offers a unifying methodology of proofs for earlier results by Euler and Lagrange on expressing certain types of natural numbers in the form of finite sums of certain kinds of natural numbers. In 1830, Gauss laid the foundations of geometric interpretation of methods and results of theory of forms, which then successfully developed throughout the 19th century and in 1896 it culminated in the publication of "Geometrie der Zahlen" by Hermann Minkowski. In the 19th century, to solve problems of Number theory and to prove certain properties of integers, methods and results of mathematical analysis were also successfully used. The first attempts to use analysis to study integers were made by Euler and Jacobi, however, it was Peter Gustav Lejeune-Dirichlet who made the first systematic effort. His lectures on Number theory "Vorlesungen über Zahlentheorie" published in 1863 were a continuation and expansion on Gauss' work Disquisitiones arithmeticae. Dirichlet brought several important results on sequences of prime numbers in real and complex areas. One of the main motives for using analysis methods was to study function $\pi(x)$ expressing the number of primes not exceeding number x. Euler, Legendre, Gauss and others expressed a conjecture that $\lim\limits_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$. In 1854, a professor at St. Petersburg University, Pafnuty Lvovich Chebyshev (1821 – 1894), found approximation $0{,}92129 < \frac{\pi(x)}{x/\ln x} < 1{,}10555$ for function $\pi(x)$ which was later improved by several other mathematicians.

When studying function $\pi(x)$, Chebyshev used a real function which in the complex domain in its form $\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$ is known under the name Riemann function (zeta function). This function had already been known to Euler in the 18th century but it was only Bernhard Riemann who fully discover its potential. Riemann tried to find nontrivial zero values of function $\zeta(z)$ during his attempt to use function ζ to prove formula $\lim\limits_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$. In 1859 he formulated a conjecture that in a plane of complex numbers $z = x + \mathrm{i}y$ in a planar strip defined by inequality $0 \le x \le 1$, all these zero points lie on line $x = \frac{1}{2}$. Riemann hypothesis on distribution of roots of Riemann zeta function is one of the greatest unsolved problems of today's mathematics. A decision on the validity of Riemann hypothesis would solve a large number of problems from various areas of mathematics, especially from the number theory domain, such as the question of prime number distribution. The theorem $\lim\limits_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$ of analytical number theory is called Prime Number Theorem [15] and it is one of the most remarkable results of modern mathematics.

2 Fermat's Last Theorem

Pierre de Fermat (1607 - 1665) was a versatile man and an excellent judge. He spoke many languages and was an expert in publishing Greek classics. He was so busy all his life that he never got to Paris and spent his whole life in Toulouse. In 1629 he wrote the work „Introduction to the Study of Planar and Spatial Curves", in which he built the analytic geometry in the plane before Descartes. The fact that Descartes overshadowed Fermat probably lies in the fact that Fermat did not publish his work, he communicated it only by letters to his friends and familiars. The reason may also be the new, more appropriate symbolism introduced by Descartes and also the fact that Descartes presented his method as a general method for solving all mathematical problems. We also thank the fact that Fermat wrote the letters for one of the most famous problems of Number theory, namely the Fermat's Last Theorem „*The equation* $x^n + y^n = z^n;\ n > 2;\ x, y, z \neq 0$*; has no integer solution.*" [16].

He marked this theorem on the margin of the Diophantus' "Arithmetica" at Pythagoras' Theorem in the form: „*It is not possible to divide a cube into two cubes, or a fourth power into two fourth powers, or generally any power higher than two into two equal powers. I have really discovered such a strange proof that this edge of the book is too small to fit it in.*". Although Fermat claimed that he know the proof, he probably did not, because no one could solve this problem for centuries after him [17]. Fermat's theorem was only discovered after Fermat's death in 1665 by his son Samuel de Fermat who cataloged his articles for publication [18]. However, he could not find any general proof of the "Last Theorem" in any of his father's notes.

We know for sure that Fermat proved the theorem for $n = 4$, because in his correspondence, Fermat mentioned the cases $n = 3,4$, and he even proved the theorem for $n = 4$. But for others n probably did not. In the period from 1630 to the end of the 20th century, thousands of mathematicians – from amateurs to professional mathematicians – were trying to find a proof for Fermat's Theorem, and these experiments made a significant contribution to the Number theory and other related disciplines with new pieces of knowledge and methods. The mathematician Leonhard Euler proved the validity of the theorem for $n = 3$ using complex numbers. Based on his work, validity of the theorem was extended for n equal to all multiples of the numbers 3 and 4 (3, 6, 9, ...; 4, 8, 12, ...). In 1825, Peter Gustav Lejeune-Dirichlet and Adrien-Marie Legendre extended the validity of the theorem for $n = 5$, and in 1839 Gabriel Lame proved the validity of the theorem for $n = 7$. The problem was ultimately solved in the 20th century by a number of mathematicians such as Yutaka Taniyama, Goro Shimura, Gerhard Frey, Kenneth Alan Ribet, Andrew John Wiles and Richard Lawrance Taylor. The author of the full proof covering Fermat's theorem in general is the British mathematician Andrew Wiles. Andrew Wiles verified the validity of Fermat's Last Theorem already in 1993, however, the correctness of his proof was not approved by several experts due to a small deficiency in the proof, the removal of which took another year till 1994, before presenting the generally approved proof in 1995 in a paper titled „Modular Elliptic Curves and Fermat's Last Theorem", which was accepted as conclusive proof. It took Andrew Wiles eight years to verify Fermat's Last Theorem and it is one of the most complex mathematical proofs in the history of mathematics [14].

Now we prove the Fermat's Last Theorem for $n = 4$.

Theorem 1.

$$x^4 + y^4 = z^4$$

does not have an integer solution, if $xyz \neq 0$*.*

Proof. We will prove the proposition that the equation

$$x^4 + y^4 = z^2$$

does not have an integer solution if $xyz \neq 0$, from which already immediately follows the validity of main theorem, because if the triplet of integers $[x, y, z]$, $xyz \neq 0$, be a solution of the equation $x^4 + y^4 = z^2$, then the triplet of numbers $[x, y, z^2]$ would satisfy the equation $x^4 + y^4 = z^4$.

If the equation $x^4 + y^4 = z^2$ has a solution $[x, y, z], x, y, z \in \mathbb{Z}, xyz \neq 0$, so we can assume that the numbers x, y, z are pairwise coprime. Because if $\mathrm{GCD}(x, y) = d > 1$ holds, then $x = dx_1$, $y = dy_1$, where $\mathrm{GCD}(x_1, y_1) = 1$. If we multiply the equation $x^4 + y^4 = z^2$ by the number $\frac{1}{d^4}$ we get

$$x_1^4 + y_1^4 = \left(\frac{z}{d^2}\right)^2 = z_1^2.$$

Since $x_1, y_1 \in \mathbb{Z}$, also $z_1 = \frac{z}{d^2} \in \mathbb{Z}$. If $\mathrm{GCD}(y_1, z_1) = k > 1$ holds true, then x_1 would have to be divisible by the number k, on the basis of relation $x_1^4 + y_1^4 = z_1^2$. Hence numbers x_1 and k, and therefore also numbers x_1, y_1 could not be coprime. Hereby, we have proved, if there is an integer solution of the equation $x^4 + y^4 = z^2$, for which $xyz \neq 0$ holds, then this equation has also an integer solution $[x_1, y_1, z_1]$, for which $x_1 y_1 z_1 \neq 0$ holds and these numbers are pairwise coprime. Therefore, it is enough to prove that the equation $x^4 + y^4 = z^2$ does not have integer solution $[x, y, z], xyz \neq 0$, where x, y, z are pairwise coprime.

We will proceed further indirectly. Suppose that the equation $x^4 + y^4 = z^2$ has an integer solution $[x, y, z]$, where $x, y, z \in \mathbb{N}$ are pairwise coprime. We can express all solutions of the Pythagorean equation $x^2 + y^2 = z^2$, where $x, y, z \in \mathbb{N}$ are pairwise coprime, in the form of:

$$x = uv, y = \frac{u^2 - v^2}{2}, z = \frac{u^2 + v^2}{2},$$

where $u, v \in \mathbb{N}$ are any odd coprime numbers, $u > v$. Let us simplify this statement so that we put

$$\frac{u+v}{2} = a, \frac{u-v}{2} = b,$$

where $a, b \in \mathbb{N}$ are numbers of different parity. Then

$$u = a + b, v = a - b.$$

Therefore, to any pair of odd coprime numbers $u, v \in \mathbb{N}, u > v$, there is a pair of coprime numbers $a, b \in \mathbb{N}$, $a > b$, of different parities, and vice versa. Therefore, if we substitute u, v from relations $u = a + b, v = a - b$ into the relations $x = uv, y = \frac{u^2 + v^2}{2}, z = \frac{u^2 + v^2}{2}$, we get that all solutions $[x, y, z]$ of the equation $x^2 + y^2 = z^2$, where $x, y, z \in \mathbb{N}$ are pairwise coprime, x is an odd (y is even), can be expressed it in the form

$$x = a^2 - b^2, y = 2ab, z = a^2 + b^2,$$

where $a, b \in \mathbb{N}$ are coprime numbers of different parity such that $a > b$.

If the equation $x^4 + y^4 = z^2$ has a solution $[x_0, y_0, z_0]$, then $(x_0^2)^2 + (y_0^2)^2 = z_0^2$ holds, which means that the triplet of numbers $[x_0^2, y_0^2, z_0]$ is the solution of the equation $x^2 + y^2 = z^2$. However, this means that there exist coprime numbers of different parity: $a, b \in \mathbb{N}, a > b$, such that

$$x_0^2 = a^2 - b^2, y_0^2 = 2ab, z_0 = a^2 + b^2.$$

At the same time, we assume that x_0 is odd and y_0 is even. For the other case, we just need to mutually exchange the numbers x_0, y_0. If $c \in \mathbb{N}$ is any odd number, then $c = 2k + 1, k \in \mathbb{N}$ and $c^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, thus the square of an odd number always has a remainder of 1 when divided by 4. Therefore, from the equality $x_0^2 = a^2 - b^2$ it follows, that a is an odd number and b is an even number. Since a is an odd number and $\mathrm{GCD}(a, b) = 1$, then also $\mathrm{GCD}(a, 2b) = 1$ holds. However, then from the equality $\mathrm{y}_0^2 = 2ab$ follows that

$$a = t^2, 2b = s^2,$$

where $t, s \in \mathbb{N}$. We will simplify the equality $x_0^2 = a^2 - b^2$ to $x_0^2 + b^2 = a^2$. Then the triplet of numbers $[x_0, b, a]$ is the solution for $x^2 + y^2 = z^2$ and we have

$$x_0 = m^2 - n^2, b = 2mn, a = m^2 + n^2,$$

where $m, n \in \mathbb{N}$ are some coprime numbers of different parity. From the relation $b = 2mn$, we get $mn = \frac{b}{2} = \left(\frac{s}{2}\right)^2$, from which (because of the coprimality of the numbers m, n) it follows

$$m = p^2, n = q^2,$$

where $p, q \in \mathbb{Z}, pq \neq 0$. As $a = t^2$ and $a = m^2 + n^2$, we have

$$q^4 + p^4 = t^2.$$

Since $z_0 = a^2 + b^2, 0 < t = \sqrt{a} < z_0, z_0 > 1$. If we put $q = x_1, p = y_1$ and $t = z_1$, we get, if there is a solution $[x_0, y_0, z_0]$ of the equation $x^4 + y^4 = z^2$, then it must exist an additional solution $[x_1, y_1, z_1]$ of this equation, while $0 < z_1 < z_0$. This consideration can be repeated many times and we get a sequence of solutions:

$$[x_0, y_0, z_0], [x_1, y_1, z_1], \dots, [x_n, y_n, z_n], \dots,$$

while

$$z_0 > z_1 > \cdots > z_n > \cdots.$$

Natural numbers that are at most equal $z_0 \in \mathbb{N}$ cannot form an infinite decreasing sequence, and thus the presumption that the equation $x^4 + y^4 = z^2$ has at least one solution brought us to a contradiction. Thus, the equation $x^4 + y^4 = z^2$ has not a non-zero integer solution. Then, neither the equation $x^4 + y^4 = z^4$ has a non-zero integer solution.

3 Conclusion

Number theory as a scientific discipline is not only about some historical or theoretical knowledge or theoretical applications. It is an area of mathematics with a real connection to everyday problems of the modern world. The knowledge, theorems and principles that are valid in Number theory together form an area with many open problems with an impact on all areas of mathematics. Number theory is also widely used in today's modern era of information technologies. Our article therefore presented the most important contributions from the history of mathematics concerning the Number theory. The paper also focused on the most famous problem of all times, the Fermat's Last Theorem, and showed the proof of the theorem for $n = 4$, which was historically the first one.

References

[1] Clifford A. P. (2011). *The Math Book: From Pythagoras to the 57th Dimension, 250 Milestones in the History of Mathematics*. New York, NY: Sterling Publishing, ISBN: 9781402757969.

[2] Heath T. (2012). *The Thirteen Books of the Elements*, Vol. I. 464p., 2nd ed., US: Dover Publications, ISBN: 9780486600888.

[3] Heath T. (2012). *The Thirteen Books of the Elements*, Vol. II. 464p., 2nd ed., US: Dover Publications, ISBN: 9780486600895.

[4] Heath T. (2012). *The Thirteen Books of the Elements*, Vol. III. 874p., 2nd ed., US: Dover Publications, ISBN: 9780486600901.

[5] Mueller I. (2006). *Philosophy of Mathematics and Deductive Structure in Euclid's Elements*. 400p, US: Dover Publications, ISBN: 9780486453002.

[6] Ďuriš V. (2020). *Solving Some Special Task for Arithmetic Functions and Perfect Numbers*. In. 19th Conference on Applied Mathematics: proceeding, Bratislava: STU, 4th -6th of February, 2020, pp. 374-383, ISBN 978-80-227-4983-1.

[7] Bunt L. N. H. et al. (2012). *The Historical Roots of Elementary Mathematics*. US: Dover Publications, 525p, 1st ed., ISBN: 9780486255637.

[8] Heath T. (1981). *A History of Greek Mathematics*, Vol. I. 464p., 1st ed., US: Dover Publications, ISBN: 9780486240732.

[9] Heath T. (1981). *A History of Greek Mathematics*, Vol. II. 608p., 2nd ed., US: Dover Publications, ISBN: 9780486240749.

[10] Heath T. (2003). *A Manual of Greek Mathematics*. 576p., US: Dover Publications, ISBN: 9780486432311.

[11] Smith D. E. (1958). *History of Mathematics*, Vol. I. 618p., 1st ed., US: Dover Publications.

[12] Smith D. E. (1958). *History of Mathematics*, Vol. II. 736p., 1st ed., US: Dover Publications.

[13] Crilly T. (2007). *50 Mathematical Ideas You Really Need to Know*. London: Quercus Publishing Plc, ISBN: 9781847240088.

[14] Singh S. (1997). *Fermat's Last Theorem*. London: Fourth Estate Limited. ISBN: 9781857025217.

[15] Ribenboim P. (2004). *The Little Book of Bigger Primes. USA, NY:* Springer-Verlag, 368 p., ISBN 978-0-387-21820-5.

[16] Guy, R. K. (2004). *Unsolved problems in number theory*, 3rd ed., 456 p., New York: Springer-Velag, ISBN 978-0-387-26677-0.

[17] Křížek, M., Luca, F., Somer, L. (2001). *17 Lectures on Fermat Numbers: From Number Theory to Geometry*. 1st ed., 280 p., New York: Springer-Verlag, ISBN 978-0-387-21850-2.

[18] Jackson T. (2017). *Mathematics: An Illustrated History of Numbers* (Ponderables: 100 Breakthroughs that Changed History) Revised and Updated Edition. New York, NY: Shelter Harbor Press, ISBN: 9781627950954.