PROVE OF FERMAT'S LAST THEOREM WITH THE MATHEMATICAL KNOWLEDGE LEVEL OF THE FIRST HALF OF THE 17TH CENTURY

Vassil Manev

ABSTRACT

Pierre de Fermat noticed that in the diophantine equation $a^n + b^n = c^n$, when n increases, the difference between c^n and $a^n + b^n$ increases regardless of the choice of integers (a, b, c). He was struck by his discovery, so he has written **"I have discovered a truly wonderful proof".** Pierre de Fermat realized that the difference $c^n - (a^n + b^n)$ is dependent on the exponent n. So he has reached **term "function"** in 1637, before Leibniz (1670). It had been time to systematize and rationalize the **concept "function"** and to record $f(n) = c^n - (a^n + b^n)$, but human life is too short.

After Pierre de Fermat no man has realized the function $f(n) = c^n - (a^n + b^n)$ "hidden" in diophantine equation $a^n + b^n = c^n$, so no one until now has reached the Fermat's **"beautiful proof". The proof of Andrew Wiles and this proof will remain in the history of mathematics as an example of the following:**

- **Using a lot of knowledge and less thinking** the Fermat's Last Theorem can be proven indirectly, complicated, writing more than one hundred pages, so that few people understand the proof.

- **Using a lot of thinking and less knowledge** the Fermat's Last Theorem can be proved directly, simply, writing only a few pages, so it can be understood by almost everyone. When something can be shown directly, simple and understandable in a few pages it is folly to prove indirect, complicated and incomprehensible hundreds of pages.

INTRODUCTION

The achievement of *Andrew Wiles* in proving the *Fermat's Last Theorem* published in the work "**Modular elliptic curves and *Fermat's Last Theorem***" *[1]* provokes the question:

"Is that proof *Pierre de Fermat* had in mind, when in *1637* on the field of the book of *Diophantus [2]* he has written in Latin *[3]*:

"*It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.***"**

Obviously, the extremely complicated indirect method of building the proof of the theorem used by *Andrew Wiles*, does not express the level of mathematical knowledge in the first half of the *17th cen-*

tury. Therefore, the question "What proof had in mind *Pierre de Fermat*?" will continue to excite the mathematical community to the moment of appearance of a proof of *Fermat's Last Theorem*, that is to answer the question.

Is it possible that happen after over *358* years no other proof has been found, unless submitted by *Andrew Wiles*? Alternatively, likely *Pierre de Fermat* has not found proof of his theorem, as it is assumed in the work *[4], page 5*:

"He claimed that he had found a remarkable proof. There is some doubt as to various reasons. First, this note was published without his permission, in fact by his son after his death. Second, in his later correspondence Fermat discusses the case for $n = 3$ and 4, without mentioning *this alleged evidence*. *It seems as if this was an improvised comments that Fermat failed to erase".*

This comment is logically untenable because:

- *Pierre de Fermat* did not know about the interest in him and his notes that started after his death.
- He has been engaged in mathematics in his free time.
- After his death there was no way his son to seek permission from him to publish his notes.
- That in his correspondence, after having discovered his theorem, are discussed the cases for $n = 3$ and $n = 4$ does not mean that he has not found a **wonderful proof** of the theorem. In his correspondence everyone can discuss everything, depending on the situation.

Taking into account that *Pierre de Fermat* is a genius mathematician is entirely possible that he was not mistaken and found "***really wonderful proof***" of his theorem.

If the theorem proves with the knowledge of his time it will appear that everything written so far in connection with the proof of *Fermat's Last Theorem* is incorrect.

As Diophantine equation $a^n + b^n = c^n$ is unsolvable in general, it follows:

If *Pierre de Fermat* has discovered "*really wonderful proof*" of the theorem, then he noticed in equality $a^n + b^n = c^n$ not Diophantine equation everyone notice, but something else.

In the following content under integers we will mean ***1, 2, 3, 4, 5, . . .***

Pythagoras's theorem may be expressed in the following form:

For $n = 2$, there are integers (a, b, c), for which is satisfied the equation

$a^n + b^n = c^n$.

or in the form:

For $n = 2$, there are integers (a, b, c), for which is satisfied the equation

$c^n - (a^n + b^n) = 0$

Fermat's Last Theorem may be expressed in the following form:

For $n > 2$, there are no integers (a, b, c), for which is satisfied the equation

$c^n - (a^n + b^n) = 0$.

It follows from *Fermat's Last Theorem* that for $n > 2$ is satisfied

$c^n - (a^n + b^n) \neq 0$.

We may combine both equalities $c^n - (a^n + b^n) = 0$ and $c^n - (a^n + b^n) \neq 0$ can be united and we can write

$$c^n - (a^n + b^n) = m \qquad (1)$$

where for $n = 2$ is satisfied $m = 0$, and for $n > 2$ is satisfied $m \neq 0$.

It is noteworthy that in *(1)* where we have combined both equations (*Pythagoras*' and *Fermat's*) in one equation where the change of n from $n = 2$ to $n > 2$ changes also m from $m = 0$ to $m \neq 0$.

Then question raises:

Doesn't it mean that between n and $m = c^n - (a^n + b^n)$ there is a functional dependence

$f(n) = c^n - (a^n + b^n)$

wherein independently of the choice of integers (a, b, c) for each value of n corresponds a single value of $f(n)$, and vice versa — to each value of $f(n)$ corresponds a single value of n?

Example 1:

Let's assume that $(a, b, c) = (3, 4, 5)$.

It is satisfied:

$3^2 + 4^2 = 5^2$ and $5^2 - (3^2 + 4^2) = 0$

$3^3 + 4^3 < 5^3$ and $5^3 - (3^3 + 4^3) = 34$

$3^4 + 4^4 < 5^4$ and $5^4 - (3^4 + 4^4) = 288$

. . . .

From this example it is seen that for $(a, b, c) = (3, 4, 5)$ for the integers it results:

$f(2) = 0; f(3) = 34; f(4) = 288; \ldots ; f(n) = m; \ldots$

and is evident that the correlation between n and $f(n)$ is mutually uniquely.

Example 2:

Let's assume that $(a, b, c) = (3, 4, 5)$.

It is satisfied:

$9^2 + 40^2 = 41^2$ and $41^2 - (9^2 + 40^2) = 0$

$9^3 + 40^3 < 41^3$ and $41^3 - (9^3 + 40^3) = 4192$

$9^4 + 40^4 < 41^4$ and $41^4 - (9^4 + 40^4) = 259200$

. . . .

From this example it is seen that for $(a, b, c) = (9, 40, 41)$ is satisfied:

$f(2) = 0; f(3) = 4192; f(4) = 259200; \ldots ; f(n) = m; \ldots$

and is evident that the correlation between n and $f(n)$ is mutually uniquely.

Of both examples (and all other examples that we can review) it may be seen:

- Between n and $f(n)$ exists uniquely each line, regardless of the choice of integers (a, b, c).
- When for $n = 2$ is satisfied $c^n - (a^n + b^n) = 0$ and n increases, then the difference $c^n - (a^2 + b^2)$ increases and there is no way to get equality $a^n + b^n = c^n$ for $n > 2$, regardless of the choice of integers (a, b, c).

Given the result the so far it follows:

Fermat's Last Theorem and the theorem of Pythagoras we can unite in the function in the following form:

$$f(n) = c^n - (a^n + b^n) \qquad (2)$$

where n is a positive integer, for which is satisfied $n \geq 2$.

Perhaps *Pierre de Fermat* had in mind the function *(2)*, and not Diophantine equation $a^n + b^n = c^n$, because (as it will be shown below) if used *(2)* it may be obtained simply and "***really wonderful proof***" of *Fermat's Last Theorem*.

If so, that means *Pierre de Fermat* has reached the term "***function***" in *1637*, before *Leibniz (1670)*.

This work offers proof of *Fermat's Last Theorem*, using the function *(2)* but expressed in such a way as to use the knowledge in mathematics from the time of *Pierre de Fermat*, in order to show two things:

- *Fermat's Last Theorem* can be proven with knowledge in mathematics from the time of *Pierre de Fermat*.
- *Pierre de Fermat* has not lied, had not deceived himself and has not fantasized, as he wrote that he found "**really wonderful proof"** of his theorem.

There are integers ***(a, b, c)***, for which is satisfied the relationship

$a^2 + b^2 = c^2$ *(3)*

Example:

$3^2 + 4^2 = 5^2$

If ***(a, b, c)*** are three random integers, for them is always carried one of the three relationships:

$a^2 + b^2 < c^2$ *(4)*

$a^2 + b^2 = c^2$ *(5)*

$a^2 + b^2 > c^2$ *(6)*

Relationships *(4), (5)* and *(6)* we may write as follows:

$c^2 – (a^2 + b^2) > 0$

$c^2 – (a^2 + b^2) = 0$

$c^2 – (a^2 + b^2) < 0$

and combine in one relationship

$c^2 – (a^2 + b^2) = m$ *(7)*

where for ***m*** may be satisfied: $m > 0$; $m = 0$; $m < 0$.

Dependence *(7)* is a particular case of the relationship *(1)* because *(7)* is obtained by *(1)*, for $n = 2$.

Plan of the proof:

Part 1: **If for the integers *(a, b, c)* is satisfied $a^2 + b^2 < c^2$,**

Part 2: **For the integers (a, b, c) is satisfied $a^2 + b^2 = c^2$,**

Part 3: **For the integers (a, b, c) is satisfied $a^2 + b^2 > c^2$,**

Part 4: **Proof of Fermat's Last Theorem, provided that for the integers *(a, b, c)* the function $f(n) = c^n - (a^n + b^n)$ is satisfied.**

Part 5: Conclusion:

If you use direct function (2), then the proof of *Fermat's Last Theorem* is expressed in a few lines, but can not fit in the margin of one page.

The direct use of the function ***f(n)*** to prove the *Fermat's Last Theorem* was made in ***Part 4***.

Now our goal is different:

To demonstrate that for all natural numbers ***(a, b, c)*** represented by the relations *(4)* ,*(5)* and *(6)* there is a function:

$f(n) = c^n – (a^n + b^n)$ *(8)*

wherein the correlation between ***n*** and ***f(n)*** is mutually uniquely, regardless of the choice of natural numbers ***(a, b, c)***.

PART 1

FOR INTEGERS (a, b, c) IS SATISFIED RELATIONSHIP $a^2 + b^2 < c^2$.

Theorem 1.1

If for the integers *(a, b, c)* is satisfied $a^2 + b^2 < c^2$, then for $n > 2$ is satisfied $a^n + b^n < c^n$ and might not be satisfied $a^n + b^n = c^n$.

Proof:

We multiply both sides of the inequality $a^2 + b^2 < c^2$ with c^{n-2} and we obtain

$a^2.c^{n-2} + b^2.c^{n-2} < c^2.c^{n-2}$ *(9)*

From the condition $a^2 + b^2 < c^2$ follows $a^2 < c^2$; $b^2 < c^2$, where we can write

$a^{n-2} < c^{n-2}$; $b^{n-2} < c^{n-2}$.

We multiply both sides of the inequality $a^{n-2} < c^{n-2}$ with a^2 and obtain

$a^2.a^{n-2} < a^2.c^{n-2}$

We multiply both sides of the inequality $b^{n-2} < c^{n-2}$ with b^2 and obtain

$b^2.b^{n-2} < b^2.c^{n-2}$

Since $a^2.a^{n-2} < a^2.c^{n-2}$ and $b^2.b^{n-2} < b^2.c^{n-2}$, when we replace in *(9)*, $a^2.c^{n-2}$ c $a^2.a^{n-2}$ and $b^2.c^{n-2}$ c $b^2.b^{n-2}$ we obtain the stronger inequality

$$a^2.a^{n-2} + b^2.b^{n-2} < c^2.c^{n-2} \qquad (10)$$

Of *(10)* it derives:

- For $n > 2$ is satisfied $a^n + b^n < c^n$.
- Where n grows, inequality $a^n + b^n < c^n$ strengthens as to each value of n corresponds one single value of $c^n - (a^n + b^n)$.
- For $n > 2$ is impossible to be satisfied the equality $a^n + b^n = c^n$.
- Mutually unambiguous correspondence between n and $c^n - (a^n + b^n)$ is expressed by the function $f(n) = c^n - (a^n + b^n)$.

Example:

Let's assume that $(a, b, c) = (3, 5, 7)$.

It is satisfied:

$3^2 + 5^2 < 7^2$ and $7^2 - (3^2 + 5^2) = 15$

$3^3 + 5^3 > 7^3$ and $7^3 - (3^3 + 5^3) = 191$

$3^4 + 5^4 > 7^4$ and $7^4 - (3^4 + 5^4) = 1695$

. . . .

From this example it is seen that for $(a, b, c) = (3, 5, 7)$ for the integers it results:

$f(2) = 15; f(3) = 191; f(4) = 1695; . . . ; f(n) = m; . . .$

and is apparent that in the case for $a^2 + b^2 < c^2$ correspondence between n and $f(n)$ is mutually unambiguous.

PART 2

FOR INTEGERS (a, b, c) IS SATISFIED RELATIONSHIP $a^2 + b^2 = c^2$.

Theorem 2.1

If for the integers (a, b, c) is satisfied $a^2 + b^2 = c^2$,

$n > 2$ is satisfied $a^n + b^n < c^n$ and might not be satisfied $a^n + b^n = c^n$.

Proof:

From equality $a^2 + b^2 = c^2$ follows $a^2 < c^2$; $b^2 < c^2$ and $a < c$; $b < c$ and for $n > 2$ is satisfied:

$$a^{n-2} < c^{n-2} \qquad (11)$$

$$b^{n-2} < c^{n-2} \qquad (12)$$

Multiplying both sides of *(11)* with a^2, and both sides of *(12)* with b^2, it is obtained

$$a^2.a^{n-2} < a^2.c^{n-2} \qquad (13)$$

$$b^2.b^{n-2} < b^2.c^{n-2} \qquad (14)$$

When we sum left and right sides of both inequalities *(13)* and *(14)*, it results

$$a^2.a^{n-2} + b^2.b^{n-2} < a^2.c^{n-2} + b^2.c^{n-2} \qquad (15)$$

When we multiply both sides of the equality $a^2 + b^2 = c^2$ with c^{n-2} we receive

$$a^2.c^{n-2} + b^2.c^{n-2} = c^2.c^{n-2} \qquad (16)$$

When replacing right side of *(15)* with its equal of *(16)*, it results

$$a^2.a^{n-2} + b^2.b^{n-2} < c^2.c^{n-2} \qquad (17)$$

Of *(17)* it derives:

- For $n > 2$ is satisfied $a^n + b^n < c^n$.

- Where n grows, inequality $a^n + b^n < c^n$ strengthens as to each value of n corresponds one single value of $c^n - (a^n + b^n)$.
- For $n > 2$ is impossible to be satisfied the equality $a^n + b^n = c^n$.
- Mutually unambiguous correspondence between n and $c^n - (a^n + b^n)$ is expressed by the function $f(n) = c^n - (a^n + b^n)$.

Example:

Let's assume that $(a, b, c) = (3, 4, 5)$.

It is satisfied:

$3^2 + 4^2 = 5^2$ and $5^2 – (3^2 + 4^2) = 0$

$3^3 + 4^3 < 5^3$ and $5^3 – (3^3 + 4^3) = 34$

$3^4 + 4^4 < 5^4$ and $5^4 – (3^4 + 4^4) = 288$

. . . .

From this example it is seen that for $(a, b, c) = (3, 4, 5)$ for the integers it results:

$f(2) = 0; f(3) = 34; f(4) = 288; . . . ; f(n) = m; . . .$

and is apparent that in the case for $a^2 + b^2 = c^2$ correspondence between n and $f(n)$ is mutually unambiguous.

Lemma 2.1

If for the integers s and q is satisfied $s > q$, when n increases, then difference $s^n – q^n$ is growing.

Proof:

As $s > q$, we mark:

$s^1 – q^1 = p_1$

$s^2 – q^2 = p_2$

$s^3 – q^3 = p_3$

$s^4 – q^4 = p_4$

. . . .

$s^n – q^n = p_n$

. . . .

For entered indications it may be written

$s^1 – q^1 = s – q = p_1$

$s^2 – q^2 = (s – q).(s + q) = p_2$

$s^3 – q^3 = (s – q).(s^2+ s.q + q^2) = p_3$

$s^4 – q^4 = (s – q).(s^3+ s^2.q + s.q^2+ q^3) = p_4$

. . . .

$s^n – q^n = (s – q).(s^{n-1} + s^{n-2}.q + s^{n-3}.q^2 + . . . + s.q^{n-2}+ q^{n-1}) = p_n$ (18)

. . . .

Given that s and q are integers and $s – q = p_1 > 0$, it follows:

$0 < p_1 < p_2 < p_3 < p_4 < . . . < p_n . . .$

Theorem 2.2

If for integers (a, b, c) for $n = 2$ is satisfied $c^n – (a^n + b^n) = 0$, where n grows from 2 and tends to infinity, then difference $c^n – (a^n + b^n)$ grows from 0 and tends to infinity.

Proof:

If in *(18)* we lay down $s = c$ and $q = a$, for degree $n – 2$ we obtain:

$c^{n-2} – a^{n-2} = (c – a).(c^{n-3} + c^{n-4}.a + c^{n-5}.a^2 + . . . + c.a^{n-4} + a^{n-3}) = p_{an}$ (19)

If in *(18)* we lay down $s = c$ and $q = b$ for degree $n – 2$ we obtain:

$c^{n-2} – b^{n-2} = (c – b).(c^{n-3} + c^{n-4}.b + c^{n-5}.b^2 + . . . + c.b^{n-4} + b^{n-3}) = p_{bn}$ (20)

Multiplying both sides of*(19)* with a^2, and both sides of *(20)* with b^2, we receive

$a^2.c^{n-2} - a^2.a^{n-2} = a^2.p_{an}$ *(21)*

$b^2.c^{n-2} - b^2.b^{n-2} = b^2.p_{bn}$ *(22)*

When we sum both sides of both inequalities *(21)* and *(22)*, is obtained

$a^2.c^{n-2} + b^2.c^{n-2} - (a^2.a^{n-2} + b^2.b^{n-2}) = a^2.p_{an} + b^2.p_{bn}$

$c^{n-2}.(a^2 + b^2) - (a^n + b^n) = a^2.p_{an} + b^2.p_{bn}$

Given that it is satisfied, as provided that $a^2 + b^2 = c^2$, it follows

$c^{n-2}.c^2 - (a^n + b^n) = a^2.p_{an} + b^2.p_{bn}$

$c^n - (a^n + b^n) = a^2.p_{an} + b^2.p_{bn}$

Since according to the *Lemma 2.1*, p_{an} and p_{bn} grow, where n grows, it follows that where n grows of primary value $n = 2$ and tends to infinity, then difference $c^n - (a^n + b^n)$ increases from primary value 0 and tends to infinity.

Theorem 2.3

If for $n = 2$ is satisfied $a^n + b^n = c^n$, then

- **For $n > 2$ is satisfied $a^n + b^n < c^n$.**
- **For $n < 2$ is satisfied $a^n + b^n > c^n$.**
- **For $n > 2$ and n < 2 is impossible to be satisfied the equality $a^n + b^n = c^n$.**

Proof:

According to Theorem 2.1, if for $n = 2$ is satisfied $a^n + b^n = c^n$, where n increases (for $n > 2$) is satisfied $a^n + b^n < c^n$ and might not be satisfied $a^n + b^n = c^n$. In that case between n and $c^n - (a^n + b^n)$ there is mutually unambiguous correspondence that is expressed by the function $f(n) = c^n - (a^n + b^n)$.

For $n < 2$ only one single value for n ($n = 1$) is possible, corresponding with one single value of the function $f(1) = c^1 - (a^1 + b^1)$.

For $n = 2$ only one single value of the function $f(2) = c^2 - (a^2 + b^2)$ is possible.

Example:

$3^1 + 4^1 > 5^1$ and $5^1 - (3^1 + 4^1) = -2$

$3^2 + 4^2 = 5^2$ and $5^2 - (3^2 + 4^2) = 0$

$3^3 + 4^3 < 5^3$ and $5^3 - (3^3 + 4^3) = 34$

$3^4 + 4^4 < 5^4$ and $5^4 - (3^4 + 4^4) = 288$

. . . .

Insofar we explored the integers (a, b, c), where for their second degrees are satisfied relationships $a^2 + b^2 < c^2$, $a^2 + b^2 = c^2$ and we proved that in both cases:

- For $n > 2$, equality $a^n + b^n = c^n$ might not be satisfied in integers (a, b, c).
- Between n and $c^n - (a^n + b^n)$ there is mutually unambiguous correspondence that is expressed by the function $f(n) = c^n - (a^n + b^n)$.

PART 3

FOR INTEGERS (a, b, c) IS SATISFIED RELATIONSHIP $a^2 + b^2 > c^2$.

From the relationship $a^2 + b^2 > c^2$, 9 cases are following:

$a^2 > c^2; b^2 > c^2$

$a^2 > c^2; b^2 < c^2$

$a^2 < c^2; b^2 > c^2$

$a^2 > c^2; b^2 = c^2$

$a^2 = c^2; b^2 > c^2$

$a^2 = c^2; b^2 < c^2$

$a^2 < c^2; b^2 = c^2$
$a^2 = c^2; b^2 = c^2$
$a^2 < c^2; b^2 < c^2$

of which:

- First case is limited to the second.
- Fifth case is limited to the fourth.
- Seventh case is limited to the sixth.

and only ***6*** cases remain for review:

$a^2 > c^2; b^2 > c^2$
$a^2 > c^2; b^2 < c^2$
$a^2 > c^2; b^2 = c^2$
$a^2 = c^2; b^2 < c^2$
$a^2 = c^2; b^2 = c^2$
$a^2 < c^2; b^2 < c^2$

Case 1:
$a^2 + b^2 > c^2$ and $a^2 > c^2; b^2 > c^2$.
Theorem 3.1
If a, b and c are integers for which is satisfied $a^2 + b^2 > c^2$ and $a^2 > c^2; b^2 > c^2$, where n increases, for $n > 2$ is satisfied $a^n + b^n > c^n$ and might not be satisfied $a^n + b^n = c^n$.
Proof:
Of $a^2 > c^2; b^2 > c^2$ it follows: $a^{n-2} > c^{n-2}$, $b^{n-2} > c^{n-2}$, for $n > 2$.
When we multiply both sides of the inequality $a^2 + b^2 > c^2$ with c^{n-2} we receive

$$a^2.c^{n-2} + b^2.\ c^{n-2} > c^2.c^{n-2} \qquad (23)$$

When we multiply both sides of the inequality $a^{n-2} > c^{n-2}$ with a^2 and obtain

$$a^2.a^{n-2} > a^2.c^{n-2}$$

When we multiply both sides of the inequality $b^{n-2} > c^{n-2}$ with b^2 and obtain

$$b^2.b^{n-2} > b^2.c^{n-2}$$

Since $a^2.a^{n-2} > a^2.c^{n-2}$ and $b^2.b^{n-2} > b^2.c^{n-2}$, when we replace in *(23)*, $a^2.c^{n-2}$ with $a^2.a^{n-2}$ and $b^2.c^{n-2}$ with $b^2.b^{n-2}$ we obtain the stronger inequality

$$a^2.a^{n-2} + b^2.b^{n-2} > c^2.c^{n-2} \qquad (24)$$

Of *(24)* it derives:

- For $n > 2$ is satisfied $a + b^n > c^n$.
- Where n grows, inequality $a^n + b^n > c^n$ strengthens as to each value of n corresponds one single value of $c^n - (a^n + b^n)$.
- For $n > 2$ is impossible to be satisfied the equality $a^n + b^n = c^n$.
- Mutually unambiguous correspondence between n and $c^n - (a^n + b^n)$ is expressed by the function $f(n) = c^n - (a^n + b^n)$.

Example:
$4^2 + 5^2 > 3^2$ and $3^2 - (4^2 + 5^2) = - 32$
$4^3 + 5^3 > 3^3$ and $3^3 - (4^3 + 5^3) = - 164$
$4^4 + 5^4 > 3^4$ and $3^4 - (4^4 + 5^4) = - 800$
. . . .

Case 2:
$a^2 + b^2 > c^2; a^2 > c^2 ; b^2 < c^2$
Theorem 3.2

If *(a, b, c)* are integers for which is satisfied $a^2 + b^2 > c^2; a^2 > c^2; b^2 < c^2$, where *n* grows for $n > 2$ is satisfied $a^n + b^n > c^n$ and might not be satisfied $a^n + b^n = c^n$.

Proof:

Of $a^2 > c^2; b^2 < c^2$ it follows: $a^{n-2} > c^{n-2}$, $b^{n-2} < c^{n-2}$, for $n > 2$.

When we multiply both sides of the inequality $a^2 + b^2 > c^2$ with c^{n-2} we receive

$$a^2.c^{n-2} + b^2.c^{n-2} > c^2.c^{n-2} \quad (25)$$

When we multiply both sides of the inequality $a^{n-2} > c^{n-2}$ with a^2 and obtain

$$a^2.a^{n-2} > a^2.c^{n-2}$$

When we multiply both sides of the inequality $b^{n-2} < c^{n-2}$ with b^2 and obtain

$$b^2.b^{n-2} < b^2.c^{n-2}$$

Since $a^2.a^{n-2} > a^2.c^{n-2}$ (regardless the value of $^2.b^{n-2}$), when we replace in *(25)*, $a^2.c^{n-2}$ with $a^2.a^{n-2}$ and $b^2.c^{n-2}$ with $b^2.b^{n-2}$ we obtain

$$a^2.a^{n-2} + b^2.b^{n-2} > c^2.c^{n-2} \quad (26)$$

Of *(26)* it derives:

- For $n > 2$ is satisfied $a^n + b^n > c^n$.
- Where *n* grows, inequality $a^n + b^n > c^n$ strengthens as to each value of *n* corresponds one single value of $c^n - (a^n + b^n)$.
- For $n > 2$ is impossible to be satisfied the equality $a^n + b^n = c^n$.
- Mutually unambiguous correspondence between *n* and $c^n - (a^n + b^n)$ is expressed by the function $f(n) = c^n - (a^n + b^n)$.

Example:

$7^2 + 3^2 > 5^2$ and $5^2 - (7^2 + 3^2) = - 34$

$7^3 + 3^3 > 5^3$ and $5^3 - (7^3 + 3^3) = - 245$

$7^4 + 3^4 < 5^4$ and $5^4 – (7^4 + 3^4) = - 1857$

. . . .

Case 3:

$a^2 + b^2 > c^2; a^2 > c^2; b^2 = c^2$

Theorem 3.3

If *(a, b, c)* are integers for which is satisfied $a^2 + b^2 > c^2; a^2 > c^2; b^2 = c^2$, where *n* grows for $n > 2$ is satisfied $a^n + b^n > c^n$ and might not be satisfied $a^n + b^n = c^n$.

Proof:

Of $a^2 > c^2; b^2 = c^2$ it follows: $a^{n-2} > c^{n-2}$, $b^{n-2} = c^{n-2}$, for $n > 2$.

When we multiply both sides of the inequality $a^2 + b^2 > c^2$ with c^{n-2} we receive

$$a^2.c^{n-2} + b^2.c^{n-2} > c^2.c^{n-2} \quad (27)$$

When we multiply both sides of the inequality $a^{n-2} > c^{n-2}$ with a^2 and obtain

$$a^2.a^{n-2} > a^2.c^{n-2}$$

When we multiply both sides of the equality $b^{n-2} = c^{n-2}$ with b^2 and obtain

$$b^2.b^{n-2} = b^2.c^{n-2}$$

Since $a^2.a^{n-2} > a^2.c^{n-2}$ and $b^2.b^{n-2} > b^2.c^{n-2}$, when we replace in *(27)*, $a^2.c^{n-2}$ with $a^2.a^{n-2}$ and $b^2.c^{n-2}$ with $b^2.b^{n-2}$ we obtain

$$a^2.a^{n-2} + b^2.b^{n-2} > c^2.c^{n-2} \quad (28)$$

Of *(28)* it derives:

- For $n > 2$ is satisfied $a^n + b^n > c^n$.
- Where *n* grows, inequality $a^n + b^n > c^n$ strengthens as to each value of *n* corresponds one single value of $c^n - (a^n + b^n)$.
- For $n > 2$ is impossible to be satisfied the equality $a^n + b^n = c^n$.

- Mutually unambiguous correspondence between n and $c^n - (a^n + b^n)$ is expressed by the function $f(n) = c^n - (a^n + b^n)$.

Example:

$7^2 + 5^2 > 5^2$ and $5^2 - (7^2 + 5^2) = -49$

$7^3 + 5^3 > 5^3$ and $5^3 - (7^3 + 5^3) = -343$

$7^4 + 5^4 > 5^4$ and $5^4 - (7^4 + 5^4) = -2401$

. . . .

Case 4:

$a^2 + b^2 > c^2; a^2 = c^2 ; b^2 < c^2$

Theorem 3.4

If (a, b, c) are integers for which is satisfied $a^2 + b^2 > c^2; a^2 = c^2; b^2 < c^2$, where n grows for $n > 2$ is satisfied $a^n + b^n > c^n$ and might not be satisfied $a^n + b^n = c^n$.

Proof:

Of $a^2 = c^2; b^2 < c^2$ it follows: $a^{n-2} = c^{n-2}$, $b^{n-2} < c^{n-2}$, for $n > 2$.

When we multiply both sides of the inequality $a^2 + b^2 > c^2$ with c^{n-2} it results

$$a^2.c^{n-2} + b^2.c^{n-2} > c^2.c^{n-2} \qquad (29)$$

When we multiply both sides of the equality $a^{n-2} = c^{n-2}$ with a^2 we obtain

$$a^2.a^{n-2} = a^2.c^{n-2}$$

When we multiply both sides of the inequality $b^{n-2} < c^{n-2}$ with b^2 and obtain

$$b^2.b^{n-2} < b^2.c^{n-2}$$

Since $a^2.a^{n-2} = a^2.c^{n-2}$ and $b^2.b^{n-2} < b^2.c^{n-2}$, when we replace in *(29)*, $a^2.c^{n-2}$ with $a^2.a^{n-2}$ and $b^2.c^{n-2}$ with $b^2.b^{n-2}$ we obtain

$$a^2.a^{n-2} + b^2.b^{n-2} > c^2.c^{n-2} \qquad (30)$$

Of *(30)* it derives:

- For $n > 2$ is satisfied $a^n + b^n > c^n$.
- Where n grows, inequality $a^n + b^n > c^n$ strengthens as to each value of n corresponds one single value of $c^n - (a^n + b^n)$.
- For $n > 2$ is impossible to be satisfied the equality $a^n + b^n = c^n$.
- Mutually unambiguous correspondence between n and $c^n - (a^n + b^n)$ is expressed by the function $f(n) = c^n - (a^n + b^n)$.

Example:

$5^2 + 7^2 > 5^2$ and $5^2 - (5^2 + 7^2) = -49$

$5^3 + 7^3 > 5^3$ and $5^3 - (5^3 + 7^3) = -343$

$5^4 + 7^4 > 5^4$ and $5^4 - (5^4 + 7^4) = -2401$

. . . .

Case 5:

$a^2 + b^2 > c^2; a^2 = c^2 ; b^2 = c^2$

Theorem 3.5

If (a, b, c) are integers for which is satisfied $a^2 + b^2 > c^2; a^2 = c^2; b^2 = c^2$, where n grows for $n > 2$ is satisfied $a^n + b^n > c^n$ and might not be satisfied $a^n + b^n = c^n$.

Proof:

Of $a^2 = c^2; b^2 = c^2$ it follows: $a^{n-2} = b^{n-2} = c^{n-2}$, for $n > 2$.

When we multiply both sides of the inequality $a^2 + b^2 > c^2$ with c^{n-2}we receive

$$a^2.c^{n-2} + b^2.c^{n-2} > c^2.c^{n-2} \qquad (31)$$

When we multiply both sides of the equality $a^{n-2} = c^{n-2}$ with a^2 we obtain

$$a^2.a^{n-2} = a^2.c^{n-2}$$

When we multiply both sides of the equality $b^{n-2} = c^{n-2}$ with b^2 and obtain
$b^2.b^{n-2} = b^2.c^{n-2}$
When replacing in *(31)*, $a^2.c^{n-2}$ with $c^2.c^{n-2}$ and $b^2.c^{n-2}$ with $c^2.c^{n-2}$ we obtain strengthened inequality
$$c^2.c^{n-2} + c^2.c^{n-2} > c^2.c^{n-2} \quad (32)$$
Of *(32)* it derives:

- For $n > 2$ is satisfied $a^n + b^n > c^n$.
- Where n grows, inequality $a^n + b^n > c^n$ strengthens as to each value of n corresponds one single value of $c^n - (a^n + b^n)$.
- For $n > 2$ is impossible to be satisfied the equality $a^n + b^n = c^n$.
- Mutually unambiguous correspondence between n and $c^n - (a^n + b^n)$ is expressed by the function $f(n) = c^n - (a^n + b^n)$.

Example:
$5^2 + 5^2 > 5^2$ and $5^2 - (5^2 + 5^2) = - 25$
$5^3 + 5^3 > 5^3$ and $5^3 - (5^3 + 5^3) = - 125$
$5^4 + 5^4 > 5^4$ and $5^4 - (5^4 + 5^4) = - 625$
. . . .

Of the five cases reviewed
$a^2 > c^2; b^2 > c^2$
$a^2 > c^2; b^2 < c^2$
$a^2 > c^2; b^2 = c^2$
$a^2 = c^2; b^2 < c^2$
$a^2 = c^2; b^2 = c^2$
given that $a^2 + b^2 > c^2$, it follows:

- For $n < 2$ is satisfied the inequality $a^n + b^n > c^n$.
- For $n > 2$ might not be satisfied the equality $a^n + b^n = c^n$.
- Where n grows (for $n > 2$), difference between c^n and $a^n + b^n$ increases.
- Between n and $c^n – (a^n + b^n)$ there is mutually unambiguous correspondence that is expressed by the function $f(n) = c^n - (a^n + b^n)$.

The sixth (last) case remained for consideration that is more special than others thus deserving more attention.

Case 6:
$a^2 + b^2 > c^2$ and $a^2 < c^2; b^2 < c^2$

Theorem 3.6
If (a, b, c) are integers for which is satisfied $a^2 + b^2 > c^2; a^2 < c^2; b^2 < c^2$, where n grows, for $n > 2$ there is a value of n ($n = k$) so:

- **For $n \leq k$ is satisfied $a^n + b^n > c^n$.**
- **For $n > k$ is satisfied $a^n + b^n > c^n$.**
- **For $n = 2$ might not be satisfied $a^n + b^n = c^n$.**
- **The value of n ($n = k$) after which the inequality $a^n + b^n > c^n$ reverses its direction and is dependent of the integers (a, b, c).**

Proof:
According to *Lemma 2.1*

- Where n increases, for $n > 2$ difference between c^n and a^n is increasing (c^n grows faster than a^n).
- Where n increases, for $n > 2$ difference between c^n and b^n is increasing (c^n grows faster than b^n).

That means:

Where n grows (provided that $a^2 + b^2 > c^2$ and $a^2 < c^2; b^2 < c^2$), there is a value of n ($n = k + 1$), where inequality $a^n + b^n > c^n$ reverses direction, and acquires type $a^n + b^n < c^n$.

Example 1:

$7^2 + 8^2 > 9^2$ and $9^2 – (7^2 + 8^2) = -32$
$7^3 + 8^3 > 9^3$ and $9^3 – (7^3 + 8^3) = -126$
$7^4 + 8^4 < 9^4$ and $9^4 – (7^4 + 8^4) = 64$
$7^5 + 8^5 < 9^5$ and $9^5 – (7^5 + 8^5) = 9474$
$7^6 + 8^6 < 9^6$ and $9^6 – (7^6 + 8^6) = 151648$

. . . .

From this example it follows:

- $9^3 – (7^3 + 8^3) < 9^2 – (7^2 + 8^2)$.
- $9^4 – (7^4 + 8^4) < 9^5 – (7^5 + 8^5) < 9^6 – (7^6 + 8^6) < . . .$
- Value of n, after which the inequality $7^n + 8^n > 9^n$ reverses its direction, is $k = 3$.
- For $n < 3$ is satisfied $7^n + 8^n < 9^n$.
- For $n > 3$, where n grows, inequality $7^n + 8^n < 9^n$ strengthens as to each value of n corresponds one single value of $9^n – (7^n + 8^n)$.
- For $n > 3$ might not be satisfied the equality $7^n + 8^n = 9^n$.
- Mutually unambiguous correspondence between n and $9^n - (7^n + 8^n)$ is expressed by the function $f(n) = 9^n - (7^n + 8^n)$.

Example 2:

$19^2 + 20^2 > 21^2$ и $21^2 - (19^2 + 20^2) = -320$
$19^3 + 20^3 > 21^3$ и $21^3 - (19^3 + 20^3) = -5598$
$19^4 + 20^4 > 21^4$ и $21^4 - (19^4 + 20^4) = -95840$
$19^5 + 20^5 > 21^5$ и $21^5 - (19^5 + 20^5) = -1591998$
$19^6 + 20^6 > 21^6$ и $21^6 - (19^6 + 20^6) = -25279760$
$19^7 + 20^7 > 21^7$ и $21^7 - (19^7 + 20^7) = -372783198$
$19^8 + 20^8 > 21^8$ и $21^8 - (19^8 + 20^8) = -4760703680$
$19^9 + 20^9 > 21^9$ и $21^9 - (19^9 + 20^9) = -40407651198$
$19^{10} + 20^{10} < 21^{10}$ и $21^{10} - (19^{10} + 20^{10}) = 308814720400$
$19^{11} + 20^{11} < 21^{11}$ и $21^{11} - (19^{11} + 20^{11}) = 28987241644002$
$19^{12} + 20^{12} < 21^{12}$ и $21^{12} - (19^{12} + 20^{12}) = 1046512592320480$
$19^{13} + 20^{13} < 21^{13}$ и $21^{13} - (19^{13} + 20^{13}) = 30499394276862402$

. . . .

From this example it follows:

- $21^9 - (19^9 + 20^9) < 21^8 - (19^8 + 20^8) < 21^7 - (19^7 + 20^7) < 21^6 - (19^6 + 20^6) < 21^5 - (19^5 + 20^5) <$ $< 21^4 - (19^4 + 20^4) < 21^3 - (19^3 + 20^3) < 21^2 - (19^2 + 20^2)$
- $21^{10} - (19^{10} + 20^{10}) < 21^{11} - (19^{11} + 20^{11}) < (19^{12} + 20^{12}) < 21^{13} - (19^{13} + 20^{13}) < . . .$
- Value of n, after which the inequality $19^n + 20^n > 21^n$ reverses its direction, is $k = 9$.
- For $n < 9$ is satisfied $19^n + 20^n < 21^n$.
- For $n > 9$, where n grows, inequality $19^n + 20^n < 21^n$ strengthens as to each value of n corresponds one single value of $21^n – (19^n + 20^n)$.
- For $n > 9$ might not be satisfied the equality $19^n + 20^n = 21^n$.

- Mutually unambiguous correspondence between n and $21^n - (19^n + 20^n)$ is expressed by the function $f(n) = 21^n - (19^n + 20\ )$.

From both examples (and all other examples that we may review) it is seen that where n increases, given that $a^2 + b^2 > c^2$ and $a^2 < c^2; b^2 < c^2$:

- The inequality $a^n + b^n > c^n$ (for $n < k$) leads to the inequality $a^n + b^n < c^n$ (for $n > k$), without passing through inequality $a^n + b^n = c^n$ (for $n = k$).
- For $n > k$ is satisfied $a^n + b^n < c^n$.
- For $n \leq k$ is satisfied $a^n + b^n > c^n$.
- The value of n, ($n = k$) after which the inequality $a^n + b^n > c^n$ reverses its direction and is dependent of the selection of integers (a, b, c).
- Between n and $c^n - (a^n + b^n)$ there is mutually unambiguous correspondence that is expressed by the function $f(n) = c^n - (a^n + b^n)$.

We explored the inequality $a^n + b^n < c^n$ in ***Part 1*** .

From *Theorem 1.1* and obtained above it follows:

- For $n > k$ is satisfied $a^n + b^n < c^n$.
- For $n > k$, where n grows, inequality $a^n + b^n < c^n$ strengthens as to each value of n corresponds one single value of $c^n - (a^n + b^n)$.
- For $n > k$ might not be satisfied the equality $a^n + b^n = c^n$.
- Mutually unambiguous correspondence between n and $c^n - (a^n + b^n)$ is expressed by the function $f(n) = c^n - (a^n + b^n)$.

Only the inequality $a^n + b^n > c^n$, for $n \leq k$ remained to be explored.

Of $a^2 + b^2 > c^2$, it follows:

$$c^2 - (a^2 + b^2) < 0 \tag{33}$$

We multiply both sides of *(33)* with c and we obtain

$$c^2.c - (a^2.c + b^2.c) < 0 \tag{34}$$

It is satisfied:

$$c^2.c - (a^2.c + b^2.c) < c^2 - (a^2 + b^2) < 0.$$

Of $a^2 < c^2; b^2 < c^2$ we obtain $a < c; b < c$.

Because $a < c; b < c$ it follows $a^2.a < a^2.c; b^2.b < b^2.c$.

Replacing in *(34)* $a^2.c$ with $a^2.a$; $b^2.c$ with $b^2.b$, we obtain

$$c^2.c - (a^2.a + b^2.b) < 0 \tag{35}$$

since $a^2.a + b^2.b < a^2.c + b^2.c$ it follows

$$c^2.c - (a^2.a + b^2.b) < c^2.c - (a^2.c + b^2.c) < c^2 - (a^2 + b^2) < 0$$

$$c^3 - (a^3 + b^3) < c^2 - (a^2 + b^2)$$

In the same way we obtain

$$c^k - (a^k + b^k) < . . . < c^4 - (a^4 + b^4) < c^3 - (a^3 + b^3) < c^2 - (a^2 + b^2) < 0 \tag{36}$$

Where n increases in the closed interval $[2, k]$, then the difference between c^n and $a^n + b^n$ is increasing and an equality might not be obtained. For $n > k$ the inequality reverses its direction. We have studied this case in ***Part 1*** and there when n increases by the value of $n = k + 1$ to infinity, the difference between c^n and $a^n + b^n$ increases and an equality might not be obtained.

As of each value of n for $n \in [2, k]$ and $n > k$ corresponds only one value of $c^n - (a^n + b^n)$, it follows that between n and $c^n - (a^n + b^n)$ there is mutual uniquely line, which is expressed by the function $f(n) = c^n - (a^n + b^n)$.

From insofar obtained for $n > 2$ and $n < k + 1$, where n grows, in $a^2 + b^2 > c^2$ and $a^2 < c^2; b^2 < c^2$, it follows:

- The inequality $a^n + b^n > c^n$ (for $n < k$) leads to the inequality $a^n + b^n < c^n$ (for $n > k$), without passing through inequality $a^n + b^n = c^n$ (for $n = k$).
- For $n > k$ is satisfied $a^n + b^n < c^n$.
- For $n \leq k$ is satisfied $a^n + b^n > c^n$.
- The value of n, ($n = k$) where the inequality $a^n + b^n > c^n$ reverses its direction is dependent of the selection of integers ***(a, b, c)***. (there is nothing else in the expression $c^n - (a^n + b^n)$, from which k may be dependent).
- Between n and $c^n - (a^n + b^n)$ there is mutually unambiguous correspondence that is expressed by the function $f(n) = c^n - (a^n + b^n)$.

We explored the integers ***(a, b, c)***, where for their second degrees are satisfied relationships $a^2 + b^2 < c^2$, $a^2 + b^2 = c^2$, $a^2 + b^2 > c^2$ and we proved that in all cases:

- For $n > 2$, equality $a^n + b^n = c^n$ might not be satisfied in integers ***(a, b, c)***.
- Between n and $c^n - (a^n + b^n)$ there is mutually unambiguous correspondence that is expressed by the function $f(n) = c^n - (a^n + b^n)$.

That means:

- **Equality $a^n + b^n = c^n$ *is possible in integers (a, b, c) for n = 2.***
- **Equality $a^n + b^n = c^n$ *is not possible in integers (a, b, c) for n > 2.***

By that, ***the most complete, most accurate, most consistent and most general proof of Fermat's Last Theorem***, with the mathematical knowledge from the first half of the *17th century*, has been completed.

PART 4

PROOF OF FERMAT'S LAST THEOREM, PROVIDED THAT FOR INTEGERS *(a, b, c)* is Satisfied The Function $f(n) = c^n - (a^n + b^n)$.

Existence of the function $f(n) = c^n - (a^n + b^n)$ and of the mutually unambiguous correspondence between n and $f(n)$ is evident and does not need any proof.

To prove the existence of function $f(n) = c^n - (a^n + b^n)$ is tantamount to prove the existence of function $f(x) = a.x^2 + b.x + c$.

Nevertheless, the proofs we have made in ***Part 1***, ***Part 2*** and ***Part 3*** were necessary to recognize the existence of the function $f(n) = c^n - (a^n + b^n)$ and its amazing properties.

Here the variable is n, and not the integers ***(a, b, c)***.

Integers ***(a, b, c)*** are randomly selected. Where n changes, function $f(n)$ changes, and not integers ***(a, b, c)*** (the argument is n). In the modification of n the function changes, but so that to each of the argument n corresponds to a single value of the function $f(n)$ and to each value of the function $f(n)$ corresponds one single value of the argument n.

It is impossible and improper the function $f(n) = c^n - (a^n + b^n)$ to be regarded as an argument and the argument n to be regarded as a feature.

Given the result the so far it follows

- For $n = 2$ there are integers ***(a, b, c)***, for which is satisfied $f(n) = 0$.
- For $n > 2$ there are no integers ***(a, b, c)***, for which is satisfied $f(n) = 0$.

Fermat's Last Theorem

Equality $a^n + b^n = c^n$ *is not possible in integers (a, b, c) for n > 2.*

Proof:

From the fact that for positive integers ***(a, b, c)*** when ***n = 2*** is satisfied ***f(2) = 0*** it follows that for ***n > 2*** can not be satisfied ***f(n) = 0***, since the disturbing the mutually uniquely correlation between ***n*** and ***f(n)***.

In the selected positive integers ***(a, b, c)*** cannot, at two different values of ***n*** (***n = 2*** and ***n = k > 2***) to correlate one the same value of ***f(n)*** (***f(2) = 0*** and ***f(k) = 0***).

A value of ***n*** may be compared with different values of ***f(n)***, only when changing the integers ***(a, b, c)***.

With this the proof of *Fermat's Last Theorem* is complete.

Obviously, ***Pierre de Fermat* was right, recording that the proof of his theorem might not fit in the box on the page, but using function it might be.**

PART 5

CONCLUSION:

It appeared that the simple evidence mentioned by *Pierre de Fermat* exists.

That means:

***Pierre de Fermat* has not lied, had not deceived himself and has not fantasized, as he recorded that he found "really wonderful proof" of his theorem.**

Even more:

***Pierre de Fermat* was the first person on *Earth* reaching the term "function".**

Presented in this work, proof of *Fermat's Last Theorem* allows us to note the following:

● Proof of *Fermat's Last Theorem* may be accomplished using mathematical knowledge from the first half of the *17th century* as in the above discussion the term "function" may be avoided.

● *Pierre de Fermat* was aware that Diophantine equation $a^n + b^n = c^n$ may be represented as a function that makes the proof of the theorem his ***"really wonderful"***.

Perhaps *Pierre de Fermat* did not publish his proof, because he wanted to link it with the term *"function"*, but since has failed to properly define for the rest of his life, the proof remained not published.

We hope that in this way we have succeeded to protect the authority of *Pierre de Fermat* and remove doubts in his genius that emerged after the evidence of Andrew Wiles and the claim that only mediocre, with ***"unsuccessful career"*** people can look for simple proof of *Fermat's last theorem [5].*

In this way Pierre de Fermat was placed at the level of mediocre people because he is a lawyer by education and He was not only looking for simple proof of the theorem, but he even wrote "*I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.***"**

We, ordinary people, must learn to respect genius.

The author expresses his gratitude to:

Nenko Ivanov, Alexander Ivanov, Todor Penchev, Stefko Banev that during the initial discussions on the manuscript provided their useful comments and helped this work to be finished.

References

[1]. Wiles Andrew, Modular Elliptic Curves and Fermat’s Last Theorem, Annals of Mathematics, 1995, 142 (3), 443 – 551.

[2]. Diophanti Alexandrini, Arithmeticum, 1621.

[3]. T. Heath, Diophantus of Alexandria, Cambridge University Press, 1910, reprinted by Dover, NY, 1964, 144-145.

[4]. Nigel Boston, The Proof of Fermat’s Last Theorem, University of Wisconsin-Madison, 2003.

[5]. Singh S (October 1998). Fermat's Enigma. New York: Anchor Books. ISBN 978-0-385-49362-8*, 295 - 296.*