NIKOLAY YESAYAN

THE PROOF OF FERMAT'S LAST THEOREM

1. THE FORMULATION OF THE THEOREM.

Fermat's Last Theorem is formulated in the following manner. Equation:

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

for the degrees n greater than 2, is impossible with integers a, b and c unequal to zero. If we prove the theorem for prime degrees n, this will suffice to prove the theorem in the general case, this became the purpose of our study.

2. SOME PROPERTIES OF NUMBERS.

Any odd number greater than 2, and any even number divisible by 8, can always be represented by the difference of squares of two other integers, or by the product of two conjugate variables:

$$a = c^2 - b^2; \qquad (2)$$

$$a = (c - b)(c + b). \qquad (2')$$

Let's consider this statement separately for the odd and even numbers a.

2.1. Any odd number a greater than 2, can always be represented by the difference of squares of two other integers, or by the product of two conjugate variables.

Really, any odd number a greater than 2, can always be represented by the product of two unequal mutually simple odd numbers a_1 and a_2 (if a is a prime number, then a is the product of the number one and the number a), converted into the product of two conjugate variables, or into the difference of squares of two other integers:

$$a = a_1 a_2; \qquad a_1 a_2 = (c - b)(c + b); \qquad a_1 a_2 = c^2 - b^2.$$

For the odd number a greater than 2, the following properties correspond to the conjugate variables $c - b$ and $c + b$:

- the variables $c - b$ and $c + b$ are formed by the mutually simple numbers c and b with different parity;
- the variables $c - b$ and $c + b$ are odd;
- the variables $c - b$ and $c + b$ are mutually simple;
- to the conjugate variables the following correlation corresponds: $c - b < c + b$.

If a is a prime number, then we have:

$$a = a_1 a_2; \qquad a_1 = 1; \qquad a_2 = a; \qquad a = 1 \cdot a;$$

$$1 \cdot a = (c - b)(c + b).$$

Composing the system of two linear equations with two unknowns, we will obtain:

$$\begin{cases} c - b = 1; \\ c + b = a. \end{cases} \qquad b = \frac{a - 1}{2}; \qquad c = \frac{a + 1}{2}.$$

If a is a composite number, then we have the following correlations:

$$a = a_1 a_2; \qquad 1 < a_1 < a_2; \qquad a_1 a_2 = (c - b)(c + b).$$

$$\begin{cases} c - b = a_1; \\ c + b = a_2. \end{cases} \qquad b = \frac{a_2 - a_1}{2}; \qquad c = \frac{a_2 + a_1}{2}.$$

The smallest odd number a converted into the difference of squares of two other integers, or into the product of two conjugate variables, is equal to 3:

$$a = a_1 a_2; \qquad a_1 = 1; \qquad a_2 = 3; \qquad a = 1 \cdot 3.$$

$$\begin{cases} c - b = 1; \\ c + b = 3. \end{cases} \qquad b = 1; \qquad c = 2.$$

© Copyright 2007

Composite number a can be converted as a prime number also, therefore to any odd number a greater than 2, the following expressions always correspond:

$$a = a_1 a_2; \qquad a_1 = 1; \qquad a_2 = a; \qquad a = 1 \cdot a.$$

$$\begin{cases} c - b = 1; \\ c + b = a. \end{cases} \qquad b = \frac{a - 1}{2}; \qquad c = \frac{a + 1}{2}.$$

This method of conversion of the odd number a greater than 2, into the difference of squares of two other integers, or into the product of two conjugate variables, has the form of the following sequence:

$$3 = 2^2 - 1^2 = (2 - 1)(2 + 1); \qquad 2 - 1 = 1; \qquad 2 + 1 = 3;$$
$$5 = 3^2 - 2^2 = (3 - 2)(3 + 2); \qquad 3 - 2 = 1; \qquad 3 + 2 = 5;$$
$$7 = 4^2 - 3^2 = (4 - 3)(4 + 3); \qquad 4 - 3 = 1; \qquad 4 + 3 = 7;$$

....

$$a = c^2 - b^2 = (c - b)(c + b); \qquad c - b = 1; \qquad c + b = a.$$

The numbers c and b are determined simply: these are the adjacent numbers on the number scale axis, and the sum of which is equal to the number a. If a is a prime number, then there is only one possible method of its conversion. If a is a composite number, then there are other possible methods of its conversion. In the general case (that is, for any odd number a greater than 2), the values of the numbers c and b are determined in the following manner: the number c exists in equidistance from the numbers a_1 and a_2, and the number b is this equidistance.

2.2. Any even number a divisible by 8, can always be represented by the difference of squares of two other integers, or by the product of two conjugate variables.

Really, any even number a divisible by 8, can always be represented by the product of two unequal even numbers a_1 and a_2, converted into the product of two conjugate variables, or into the difference of squares of two other integers:

$$a = a_1 a_2; \qquad a_1 a_2 = (c - b)(c + b); \qquad a_1 a_2 = c^2 - b^2.$$

For the even number a divisible by 8, the following properties correspond to the conjugate variables $c - b$ and $c + b$:

- the variables $c - b$ and $c + b$ are formed by the mutually simple odd numbers c and b;
- the variables $c - b$ and $c + b$ are even;
- the variables $c - b$ and $c + b$ only have one common divisor - the number 2;
- one of the variables $c - b$ and $c + b$ is divisible by 2 , but is not divisible by 4, the second variable is divisible by 4; therefore their product is always divisible by 8;
- to the conjugate variables the following correlation corresponds: $c - b < c + b$.

Issued from this, we will obtain the following expressions:

$$a = a_1 a_2; \qquad a_1 < a_2; \qquad a_1 a_2 = (c - b)(c + b);$$

$$\begin{cases} c - b = a_1; \\ c + b = a_2. \end{cases} \qquad b = \frac{a_2 - a_1}{2}; \qquad c = \frac{a_2 + a_1}{2}.$$

If the number a does not contain the odd divisors, then we have:

$$a = a_1 a_2; \qquad a_1 = 2; \qquad a_2 = 2^{n-1}; \qquad a = 2^n.$$

$$\begin{cases} c - b = 2; \\ c + b = 2^{n-1}. \end{cases} \qquad b = 2^{n-2} - 1; \qquad c = 2^{n-2} + 1,$$

© Copyright 2007

where: n is any integer greater than 2.

The smallest even number a converted into the difference of squares of two other integers, or into the product of two conjugate variables, is equal to 8:

$$a = a_1\, a_2\ ; \qquad a_1 = 2\ ; \qquad a_2 = 4\ ; \qquad a = 2 \cdot 4\ .$$

$$\begin{cases} c - b = 2\ ; \\ c + b = 4\ . \end{cases} \qquad b = 1\ ; \qquad c = 3\ .$$

To any even number a divisible by 8, the following expressions always correspond:

$$a = a_1\, a_2\ ; \qquad a_1 = 2\ ; \qquad a_2 = 4d\ ; \qquad a = 2 \cdot 4d\ .$$

$$\begin{cases} c - b = 2\ ; \\ c + b = 4d\ . \end{cases} \qquad b = 2d - 1\ ; \qquad c = 2d + 1\ ,$$

where: d is any integer greater than zero.

This method of conversion of the even number a divisible by 8, into the difference of squares of two other integers, or into the product of two conjugate variables, has the form of the following sequence:

$$8 = 2 \cdot 4 \cdot 1 = 3^2 - 1^2 = (3 - 1)(3 + 1)\ ;\ \ 3 - 1 = 2\ ;\ \ 3 + 1 = 4\ ;$$
$$16 = 2 \cdot 4 \cdot 2 = 5^2 - 3^2 = (5 - 3)(5 + 3)\ ;\ \ 5 - 3 = 2\ ;\ \ 5 + 3 = 8\ ;$$
$$24 = 2 \cdot 4 \cdot 3 = 7^2 - 5^2 = (7 - 5)(7 + 5)\ ;\ \ 7 - 5 = 2\ ;\ \ 7 + 5 = 12\ ;$$

....

$$a = 2 \cdot 4d = c^2 - b^2 = (c - b)(c + b)\ ;\ \ c - b = 2\ ;\ \ c + b = 4d\ .$$

The values of the numbers c and b are determined simply: these are the nearest odd numbers on the number scale axis, and the sum of which is equal to half of the number a . If the number a does not contain the odd divisors, then there is only one possible method of its conversion. If the number a contains both even and odd divisors, then there are other possible methods of its conversion. In the general case (that is, for any even number a divisible by 8), the values of the numbers c and b are determined in the following manner: the number c exists in equidistance from the numbers a_1 and a_2 , and the number b is this equidistance.

2.3. For any odd numbers greater than 2, and for any even numbers divisible by 8, one or several systems of two linear equations with two unknowns can always be composed, that is, these numbers can always be represented by the difference of squares of two other integers or by the product of two conjugate variables, by one or several different methods.

Let's consider the odd numbers a greater than 2. Prime number a is the product of itself and the number one. An odd, composite number a is the product of two or several prime cofactors unequal to the number one. For prime number a only one system of two linear equations with two unknowns can be composed:

$$a = 1 \cdot a\ ; \qquad \begin{cases} c - b = 1\ ; \\ c + b = a\ . \end{cases}$$

That is, prime number a can be represented by the difference of squares of two other integers, or by the product of two conjugate variables in one manner only. If a is a composite number containing two prime divisors unequal to the number one:

$$a = a_1\, a_2\ ; \qquad 1 < a_1 < a_2\ ,$$

then we will obtain two systems of two linear equations with two unknowns:

$$\begin{cases} c - b = 1\ ; \\ c + b = a\ . \end{cases} \qquad \begin{cases} c - b = a_1\ ; \\ c + b = a_2\ . \end{cases}$$

© Copyright 2007

If the odd number a contains three prime divisors unequal to the number one:

$$a = a_1\ a_2\ a_3\ ; \qquad 1 < a_1 < a_2 < a_3\ ,$$

then first we will obtain three systems of two linear equations with two unknowns :

$$\begin{cases} c - b = 1\ ; \\ c + b = a\ . \end{cases} \qquad \begin{cases} c - b = a_1\ ; \\ c + b = a_2\ a_3\ . \end{cases} \qquad \begin{cases} c - b = a_2\ ; \\ c + b = a_1\ a_3\ . \end{cases}$$

Besides the three previous systems, one more system can be composed. For the correlation:

$$a_1\ a_2 < a_3$$

we will obtain the following system:

$$\begin{cases} c - b = a_1\ a_2\ ; \\ c + b = a_3\ . \end{cases}$$

But if the other correlation is correct:

$$a_1\ a_2 > a_3\ ,$$

then this system will take on the form:

$$\begin{cases} c - b = a_3\ ; \\ c + b = a_1\ a_2\ . \end{cases}$$

That is, if the odd number a contains three prime divisors unequal to the number one, then we have four systems of two linear equations with two unknowns c and b. For the odd number a containing k prime divisors unequal to the number one:

$$a = a_1\ a_2\ a_3 \ldots\ldots\ldots\ldots\ldots\ldots\ a_k\ ; \qquad 1 < a_1 < a_2 < a_3 < \ldots\ldots\ldots\ldots\ldots < a_k\ ,$$

we will obtain 2^{k-1} systems of two linear equations with two unknowns c and b. This means, that the odd number a can be represented by the difference of squares of two other integers, or by the product of two conjugate variables by 2^{k-1} different methods.

Let's consider the even numbers a divisible by 8. If these numbers do not contain the odd divisors:

$$a = 2^n\ ,$$

where: n is any integer greater than 2,

then only one method of conversion is possible:

$$a = 2 \cdot 2^n . \qquad \begin{cases} c - b = 2\ ; \\ c + b = 2^{n-1}\ . \end{cases}$$

That is, the even number a divisible by 8 and not containing the odd divisors, can be represented by the difference of squares of two other integers, or by the product of two conjugate variables in one manner only. If the even number a contains an even divisor and a prime divisor:

$$a = 2^n\ d\ ,$$

where: d is a prime number greater than 2,

then we have two methods of conversion. First we will obtain the following system**:**

$$\begin{cases} c - b = 2\ ; \\ c + b = 2^{n-1}\ d\ . \end{cases}$$

If the correlation is justified:

$$2^{n-2} < d\ ,$$

then we have one more system of two linear equations with two unknowns c and b **:**

$$\begin{cases} c - b = 2^{n-1}\ ; \\ c + b = 2\ d\ . \end{cases}$$

But if the other correlation is correct:

© Copyright 2007

$$2^{n-2} > d ,$$

then the second system will take on the form:

$$\begin{cases} c - b = 2d ; \\ c + b = 2^{n-1} . \end{cases}$$

If the even number a contains three divisors - the even number 2^n and two prime numbers d_1 and d_2 unequal to the number one, then we will obtain four methods of conversion. If the even number a contains k divisors - the even number 2^n and $k-1$ prime numbers $d_1 , d_2 , d_3 \ldots\ldots d_{k-1}$ unequal to the number one, then we have 2^{k-1} systems of two linear equations with two unknowns c and b . This means, that the even number a can be represented by the difference of squares of two other integers, or by the product of two conjugate variables by 2^{k-1} different methods.

For the odd numbers a greater than 2, we will always obtain the expressions:

$$a = a_1 a_2 ; \qquad a_1 = 1 ; \qquad a_2 = a ; \qquad a = 1 \cdot a .$$

$$\begin{cases} c - b = 1 ; \\ c + b = a . \end{cases}$$

For the even numbers a divisible by 8, we will always get:

$$a = a_1 a_2 ; \qquad a_1 = 2 ; \qquad a_2 = 2^{n-1} d ; \qquad a = 2^n d .$$

$$\begin{cases} c - b = 2 ; \\ c + b = 2^{n-1} d . \end{cases}$$

Thus, for the odd numbers a greater than 2, we will always obtain the system of two linear equations with two unknowns c and b , where the difference $c - b$ is equal to the number one. For the even numbers a divisible by 8, we will always get the system of two linear equations with two unknowns c and b , where the difference $c - b$ is equal to the number 2.

3. THE STUDY OF CONJUGATION SIGNS .

The signs of conjugation form the conditions of conversion of the integer a into the product of two cofactors, which are the difference and the sum of two mutually simple integers. The odd number a greater than 2, can always be converted into the product of two conjugate variables, which is the product of the difference and the sum of two mutually simple numbers with different parity. The even number a divisible by 8, can always be converted into the product of two conjugate variables, which is the product of the difference and the sum of two mutually simple odd numbers. Since we agreed, that the number a is odd, then on this basis we build our following study. The odd number a greater than 2, can be converted into the product of two conjugate variables, if, as originally given, we also have both of its unequal and mutually simple divisors a_1 and a_2 . Having the numbers a_1 and a_2 , we have, as a result, the conjugate variables $c - b$ and $c + b$, and, through the composition of the system of two linear equations with two unknowns, we can determine these unknowns - the numbers c and b . That is, the numbers a_1 and a_2 are originally given, and the numbers c and b are their derivatives. The number a can also be an integer that is raised to any degree.

The signs of conjugation also determine the conditions for finding the value of the number a_2 , which is the conjugate to the originally given odd number a_1 . Let's have an odd number a_1 (including the number one), for whom it is necessary to find the conjugate number a_2 . In this case the task has an infinite solution. Really, it is possible to find the endless sets of the numbers c and b , the difference of which is equal to the

© Copyright 2007

number a_1 . Therefore the sum of the numbers c and b , and together with it - the product of two conjugate variables, assume the same endless sets. That is, to the given number a_1 corresponds the infinite set of the number a_2 , which could compose with the number a_1 a pair of conjugate variables. But if the originally given number a_1 is the difference of specific values of the numbers c and b , which are also given originally:

$$a_1 = c - b ,$$

then we will obtain the only number a_2 , which is equal to the sum of the numbers c and b , and is conjugate to the number a_1 :

$$a_2 = c + b .$$

That is, in this case we have, as originally given, the odd number a_1 and two unequal mutually simple numbers c and b with different parity, the difference of which is equal to the number a_1 . By this, the task is: to find the number a_2 , which is conjugate to the number a_1 . Since the sum of the numbers c and b is conjugate to their difference, and the number a_1 is equal to this difference, then, obviously, as conjugate to the number a_1 can only be the number a_2 , which is equal to the sum of the numbers c and b . Consequently, the only solution of this task is possible, if together with originally given number a_1 we also have as originally given the numbers c and b , the difference of which is equal to the number a_1 . In this case we will obtain the only value of the number a_2 , which forms with the number a_1 a pair of conjugate variables. Therefore, we will get the only product of the numbers a_1 and a_2 .

Any given integer by itself does not determine the value of another integer, which is conjugate to it. With any odd number a_1 greater than 2, any odd number a_2 , which is simple in relation to a_1 (if the number a_1 is equal to the number one, then any odd number a), can compose a pair of conjugate variables. That is, any two unequal, mutually simple odd numbers a_1 and a_2 (the number one and any odd number a) can always compose such a pair. But by specific conditions, to any odd number a_1 can correspond only one, simple in relation to a_1 , the odd number a_2 (if the number a_1 is equal to the number one, then a certain odd number a), which appears as conjugate to a_1 . These conditions consist on the fact, that the value of the odd number a_1 is not assigned by itself, but as the difference of two other mutually simple numbers with different parity. As the conjugate to this difference can only be the sum of these numbers. Having the values of the numbers c and b , the difference of which is equal to the number a_1 , we will obtain the only number a_2 , which is equal to the sum of the numbers c and b , and is conjugate to the number a_1 . Having any odd number (including the number one) selected arbitrarily, we can always compose on its basis the endless sets of pairs of conjugate variables. Having any odd number (including the number one) as a difference of the specific values of the minuend and the subtrahend, we can always compose on its basis only one pair of conjugate variables.

The mechanism of the formation of the value of the derivatives c and b of originally given number a and both of its divisors a_1 and a_2 , is simple. Let's have, as originally given, the odd number a greater than 2. Composite number a is the product of two odd mutually simple numbers a_1 and a_2 , unequal to the number one:

$$a = a_1 a_2 ; \qquad 1 < a_1 < a_2 .$$

In this case, the number c is equal to the arithmetic mean of the numbers a_1 and a_2 , and the number b is equal to the difference of the number c and any of the numbers a_1 and a_2:

© Copyright 2007

$$\begin{cases} c - b = a_1 ; \\ c + b = a_2 . \end{cases} \qquad c = \frac{a_1 + a_2}{2} ; \quad b = c - a_1 = a_2 - c .$$

If the odd number a is a product of several, unequal to the number one, mutually simple cofactors, then we, correspondingly, have several methods of its conversions (the dependence of the quantity of methods of conversions of the odd number a from a quantity of its prime divisors is presented above). In each of the methods the number a has the form of the product of only two odd mutually simple cofactors, and on this basis can the systems of two linear equations with two unknowns, c and b , be composed. If a is a prime number, then we will obtain the following expressions:

$$a = a_1 a_2 ; \qquad a_1 = 1 ; \qquad a_2 = a ; \qquad a = 1 \cdot a .$$

$$\begin{cases} c - b = 1 ; \\ c + b = a . \end{cases} \qquad c = \frac{1 + a}{2} ; \quad b = c - 1 = a - c .$$

That is, if a is a prime number, then the number c is equal to half the value of a number which is greater than a by one, and the number b is less than c by one.

The most simple method of conversion of the odd number a greater than 2, into a difference of squares of two other integers, or into the product of two conjugate variables, which was, in essence, indicated above, consists in the following. The sum of two adjacent numbers on the number scale axis is always equal to the difference of their squares:

$$c^2 - b^2 = (c - b)(c + b) ; \ c - b = 1 ; \ c^2 - b^2 = c + b .$$

Consequently, any odd number a greater than 2, can always be converted into a difference of squares of two adjacent numbers on the number scale axis, the sum of which is equal to the number a :

$$a = c + b ; \quad c - b = 1 ; \quad c + b = c^2 - b^2 ; \quad a = c^2 - b^2 .$$

In this manner, any odd number a greater than 2, can always be represented by a difference of squares of two other integers, or by the product of two conjugate variables.

4. THE PROOF OF THE THEOREM .

In equation (1) with mutually simple numbers a , b and c , one of these is even, and two others are odd. Therefore, one of the numbers a and b is always odd. We will let the number a be odd, and on this basis we build the following study. Equation (1) for the second degree can be represented in the form of two other equations:

$$a^2 = c^2 - b^2 ;$$
$$b^2 = c^2 - a^2 .$$

Converting the right side of the previous equations, we will obtain:

$$a^2 = (c - b)(c + b) ; \qquad (1')$$
$$b^2 = (c - a)(c + a) . \qquad (1'')$$

Equation (1) for the odd degree n greater than 2, can also be represented in the form of two other equations:

$$a^n = c^n - b^n ;$$
$$b^n = c^n - a^n .$$

After conversion of the right side of these equations we will obtain:

$$a^n = (c - b)(c^{n-1} + c^{n-2} b + \dots\dots + b^{n-1}) ; \qquad (1''')$$
$$b^n = (c - a)(c^{n-1} + c^{n-2} a + \dots\dots + a^{n-1}) . \qquad (1'''')$$

© Copyright 2007

Issued from the above, the proof of the theorem is based on the following prerequisites:
- the properties of the numbers, which consist on the fact that any odd number greater than 2, and any even number divisible by 8, can always be represented by the difference of squares of two other integers, or by the product of two conjugate variables formed by those integers;
- the special feature of equation (1), which consists on the fact that all three numbers entered into the structure of this equation, are raised to the same degree;
- the special feature of the difference, of two numbers that are raised to the same degree, which consists on the fact that this difference can always be represented by the product of two cofactors, one of which is organically entered into the structure of two conjugate variables;
- the property of equation (1), which consists on the fact that the divisor, of the number $\boldsymbol{a}$ that is raised to any degree, is the difference formed by the minuend $\boldsymbol{c}$ and the subtrahend $\boldsymbol{b}$, and the divisor, of the number $\boldsymbol{b}$ that is raised to any degree, is the difference formed by the minuend $\boldsymbol{c}$ and the subtrahend $\boldsymbol{a}$.

These prerequisites determine the matter of our continued study. If we have an equation, one side of which contains either the odd number greater than 2, or the even number divisible by 8, and the other side is conversion of one of those numbers into the difference of squares of two other integers, or into the product of two conjugate variables, then this equation is correct. In this equation, an originally given integer converts directly into the difference of squares of two other integers, or into the product of two conjugate variables. This kind of conversion is presented in equation (1) for the second degree and in equation (2). If an originally given number corresponds to the demands of conjugation and is not a degree of an integer, then we have equation (2), where only two of three numbers entered into its structure are the square of an integer. In equation (2), only number $\boldsymbol{a}$ can be represented by the difference of squares of two other integers entered into the structure of triplet $\boldsymbol{a}$, $\boldsymbol{b}$ and $\boldsymbol{c}$, or by the product of two conjugate variables formed by the integers entered into the structure of the same triplet of numbers. If an originally given number corresponds to the demands of conjugation and is the square of an integer, then we have equation (1), where all three numbers entered into its structure are the square of an integer. In equation (1), both numbers $\boldsymbol{a}^2$ and $\boldsymbol{b}^2$ can always be represented by the difference of squares of two other integers of triplet $\boldsymbol{a}$, $\boldsymbol{b}$ and $\boldsymbol{c}$, or by the product of two conjugate variables formed by the integers entered into the structure of the same triplet of numbers. If in equations (1) and (2), the number $\boldsymbol{a}$ is originally given, then the numbers $\boldsymbol{c}$ and $\boldsymbol{b}$ are its derivatives. In equation (2), as originally given, can also be the numbers $\boldsymbol{c}$ and $\boldsymbol{b}$, and the number $\boldsymbol{a}$ is their derivative. In equation (1), only by certain values of originally given numbers $\boldsymbol{c}$ and $\boldsymbol{b}$ will we obtain, as their derivative, the square of an integer.

Equations (2) and (2’) contain the conversion of the integer $\boldsymbol{a}$ into the difference of squares of two other integers**,** or into the product of two conjugate variables. Having, as originally given, the odd number $\boldsymbol{a}$ greater than 2, and both its divisors, $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$, we compose the system of two linear equations with two unknowns, $\boldsymbol{c}$ and $\boldsymbol{b}$, from here, can these unknowns be obtained. To the given number $\boldsymbol{a}$ and both its divisors, $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$, correspond their only derivatives - the numbers $\boldsymbol{c}$ and $\boldsymbol{b}$. From here, we obtain the only triplet of numbers, which form equation (2). This means, that

© Copyright 2007

by the specific divisors a_1 and a_2, the number a can be converted into the product of two conjugate variables by one method only. If the number a is prime, then only one pair of divisors a_1 and a_2 correspond to it, therefore the number a can be converted into the product of two conjugate variables by one method only. If the number a is composite, then several pairs of divisors a_1 and a_2 correspond to it, therefore, the number a can be converted into the product of two conjugate variables by several methods. But for the specific pair of divisors a_1 and a_2, only one method of conversion of the number a is possible. Thus, for given odd number a greater than 2, we will obtain only one pair (if a is a prime number), or multitude of pairs (if a is a composite number) of the numbers c and b, forming the product of two conjugate variables, by which, the number a can be represented. But in any case, the pairs of the numbers c and b, forming the product of two conjugate variables, always stay within the limit of conditions, which provide the existence of equation (2) with integers a, b and c. Outside of the indicated multitude, the numbers c and b do not exist. This means, that by any divisors, a_1 and a_2, the number a converts into the product of two conjugate variables only by the numbers entered into the structure of a, b and c, and cannot be converted into this product by the numbers not entered into the structure of a, b and c.

As the derivative of equation (2), besides (2'), is the following equation:

$$b^2 = c^2 - a .$$

The right side of this equation is not a difference of squares of two other numbers entered into the structure of a, b and c, therefore, this side cannot be converted into the product of two conjugate variables by the numbers a, b and c. But if the number b^2 corresponds to the demands of conjugation, then the number b^2 can be represented by the product of two conjugate variables, however, it can only be formed by the numbers not entered into the structure of a, b and c. Therefore, to equation (2) corresponds equation (2''):

$$b^2 = (c_1 - a_1)(c_1 + a_1) . \qquad (2'')$$

As a result, the numbers a and b^2 can be converted into the product of two conjugate variables independently of each other only and only by the numbers not entered into the structure of the same triplet of numbers. If the number b^2 can be converted into the product of two conjugate variables by several methods, then any of these methods will correspond to equations (2) and (2').

The difference, of two numbers that are raised to the same degree, converts into the product of two cofactors, one of which is always the difference of those two numbers. The difference, of two numbers that are raised to the second degree, converts into the product of two cofactors, which is always the product of two conjugate variables. Differing from equation (2), both derivatives of equation (1) for the second degree [equations (1') and (1'')] contain the conversion of an integer (the numbers a^2 and b^2) into the product of two conjugate variables formed by the triplet of numbers a, b and c. Having, as originally given, the squares of the odd number a greater than 2, and both its divisors, a_1 and a_2, we can compose the system of two linear equations with two unknowns, c and b, from where we will obtain these unknowns. To the given number a and both its divisors, a_1 and a_2, correspond their only derivatives - the numbers c and b, therefore, we have the only triplet of numbers a, b and c, forming equation (1). To the other divisors, a_1 and a_2, of the number a (if the number a is composite), obviously, their other derivatives, c and b, will correspond. But for any

© Copyright 2007

pair of the divisors, a_1 and a_2, of the number a, we will obtain as their derivatives the only integers, c and b. That is, to the multitude of divisors, a_1 and a_2, of the number a, corresponds such a multitude of derivatives, c and b, by which, equation (1) exists with integers a, b and c. Outside of the indicated multitude of the divisors a_1 and a_2, the numbers c and b do not exist.

To equation (1) for the second degree, the following properties correspond:
- equation (1) is formed by the triplet of numbers a, b and c;
- in the derivatives of equation (1), the numbers a^2 and b^2 convert into the product of two cofactors by one and one method only;
- in the derivatives of equation (1), the numbers a^2 and b^2 convert into the product of two cofactors, which is simultaneously the product of two conjugate variables;
- in the derivatives of equation (1), the numbers a^2 and b^2 convert into the product of two conjugate variables only by the numbers entered into the structure of the same triplet of numbers, that is, by the numbers a, b and c;
- in equations (1') and (1''), the numbers a^2 and b^2 convert into the product of two conjugate variables only by the numbers entered into the structure of the same triplet of numbers, therefore, these conversions of the numbers a^2 and b^2 are intercommunicated and interdependent of each other and cannot occur separately and independently of each other;
- in equation (1'), the divisor of the number a^2 is the difference $c - b$, and simultaneously in equation (1''), the divisor of the number b^2 is the difference $c - a$.

Issued from this, in the derivatives of equation (1) [in equations (1') and (1'')], the divisors of the numbers a^2 and b^2 can only be the differences formed by the numbers a, b and c, and cannot be the differences formed by the numbers other than a, b and c. In this connection the following conclusion can be made: if the divisor of the number a^2 is the difference $c - b$, then the divisor of the number b^2 can only be the difference $c - a$; and, correspondingly, if the divisor of the number b^2 is the difference $c - a$, then the divisor of the number a^2 can only be the difference $c - b$. That is, in the derivatives of equation (1), the differences $c - b$ and $c - a$ determine the existence of each other, and only by the conditions stated in the previous sentence, the existence of both derivatives of equation (1) and the existence of equation (1) are possible. This means, that in the derivatives of equation (1), the divisors of the numbers a^2 and b^2 are not only the values of the differences $c - b$ and $c - a$, but only these specific differences, that is, the differences formed only by the minuend and the subtrahend entered into the structure of the triplet of numbers a, b and c. Consequently, in equation (1'), the divisor of the number a^2 can only be the difference $c - b$, that is, the difference formed only by the minuend c and the subtrahend b; and in equation (1''), the divisor of the number b^2 can only be the difference $c - a$, that is, the difference formed only by the minuend c and the subtrahend a.

In equations (1'), (1'') and (2'), the integer converts directly into the product of two conjugate variables formed by the numbers a, b and c. In equations (1''') and (1''''), the integer converts into the product of two cofactors, which, by the numbers a, b and c, cannot be represented by the product of two conjugate variables. Really, in the product of two cofactors on the right side of equations (1''') and (1''''), only one of those cofactors is organically entered into the structure of the pair of conjugate variables (

© Copyright 2007

the differences $c - b$ and $c - a$); and the second cofactor is a simple number in regard to the second variable of this pair (the sums $c + b$ and $c + a$). However, the right side of equations (1''') and (1'''') corresponds to the demands of conjugation, therefore, this side can always be converted into the product of two conjugate variables, but only by the numbers other than a , b and c . The left side of equations (1''') and (1'''') also corresponds to the demands of conjugation [except the case where $a = 1$, by which, equation (1) with integers a , b and c does not exist], therefore, this side can also always be converted into the product of two conjugate variables, and only by the numbers other than a , b and c . If both sides of each of equations (1''') and (1'''') can be represented by the equal products of two conjugate variables, then these equations exist with integers a , b and c . In this case, equation (1) also exists with integers a , b and c . But if both sides of each of equations (1''') and (1'''') cannot be represented by the equal products of two conjugate variables, then these equations do not exist with integers a , b and c . In this case, equation (1) also does not exist with integers a , b and c . Since equations (1''') and (1'''') are interdependent of each other through equation (1), then for the revelation of the possibility of the existence of equations (1''') and (1'''') with integers, it is sufficient to examine only one of these equations. If, for example, both sides of equation (1''') can be represented by the equal products of two conjugate variables, then this equation exists with integers a , b and c , and together with it, equation (1'''') also exists with integers a , b and c . But if both sides of equation (1''') cannot be represented by the equal products of two conjugate variables, then this equation does not exist with integers a , b and c , and together with it, equation (1'''') also does not exist with integers a , b and c .

Let's now consider equation (1) for the odd degree n greater than 2. As indicated above, the difference of two numbers with equal degrees converts into the product of two cofactors, one of which is always the difference of those two numbers. Therefore, in the derivatives of equation (1), the numbers a and b that are raised to the odd degree n , are represented by the product of two cofactors, one of which is the difference formed by the other two numbers of the triplet a , b and c , that is, one of the differences $c - b$ or $c - a$. The integer greater than the number one that is raised to the odd degree n , can always be represented by the product of two conjugate variables. The difference, of two mutually prime numbers greater than zero that are raised to the same odd degree n, can also always be represented by the product of two conjugate variables. But if the integer greater than the number one that is raised to the odd degree n, and the difference of two mutually prime numbers greater than the number one that are raised to the same odd degree n , are united in the same equation, then this equation acquires the properties which influence the possibility of the existence of this equation with integers. In particular, if the number a that is raised to the odd degree n , and the difference of the numbers c and b that are raised to the same odd degree n , are united in the same equation, then this equation can be converted into another equation, where the number b that is raised to the odd degree n , and the difference of the numbers c and a that are raised to the same odd degree n , are united. Therefore, the divisor of the number a that is raised to the odd degree n , is the difference $c - b$, which is obtained as a result of conversion of the difference of the numbers c and b that are raised to the same odd degree n , into the product of two cofactors. Correspondingly, the

© Copyright 2007

divisor of the number b that is raised to the odd degree n, is the difference $c - a$, which is obtained as a result of conversion of the difference of the numbers c and a that are raised to the same odd degree n, into the product of two cofactors.

Equation (1) for the odd degree n greater than 2, corresponds to the previous type of equations. Therefore, to equation (1) the following properties correspond:
- equation (1) is formed by the triplet of numbers a, b and c;
- in the derivatives of equation (1), the numbers a^n and b^n convert into the product of two cofactors by one and one method only;
- in the derivatives of equation (1), the numbers a^n and b^n convert into the product of two cofactors, which, by the numbers a, b and c, cannot be represented by the product of two conjugate variables;
- in the derivatives of equation (1), the numbers a^n and b^n convert into the product of two cofactors only by the numbers entered into the structure of the same triplet of numbers, that is, by the numbers a, b and c;
- in equations (1''') and (1''''), the numbers a^n and b^n convert into the product of two cofactors only by the numbers entered into the structure of the same triplet of numbers, therefore, these conversions of the numbers a^n and b^n are intercommunicated and interdependent of each other and cannot occur separately and independently of each other;
- in equation (1'''), the divisor of the number a^n is the difference $c - b$, and simultaneously in equation (1''''), the divisor of the number b^n is the difference $c - a$.

Issued from this, in the derivatives of equation (1) [in equations (1''') and (1'''')], the divisors of the numbers a^n and b^n can only be the differences formed by the numbers a, b and c, and cannot be the differences formed by the numbers other than a, b and c. In this connection, the following conclusion can be made: if the divisor of the number a^n is the difference $c - b$, then the divisor of the number b^n can only be the difference $c - a$; and, correspondingly, if the divisor of the number b^n is the difference $c - a$, then the divisor of the number a^n can only be the difference $c - b$. That is, in the derivatives of equation (1), the differences $c - b$ and $c - a$ determine the existence of each other, and only by these conditions, the existence of both derivatives of equation (1) and the existence of equation (1) are possible. This means, that in the derivatives of equation (1), the divisors of the numbers a^n and b^n are not only the values of the differences $c - b$ and $c - a$, but only these specific differences, that is, the differences formed only by the minuend and the subtrahend entered into the structure of the triplet of numbers a, b and c. Consequently, in equation (1'''), the divisor of the number a^n can only be the difference $c - b$, that is, the difference formed only by the minuend c and the subtrahend b; and in equation (1''''), the divisor of the number b^n can only be the difference $c - a$, that is, the difference formed only by the minuend c and the subtrahend a.

Therefore, in the derivatives of equation (1), the numbers a^n and b^n can be represented by the product of two cofactors only by the differences $c - b$ and $c - a$. On the other hand, the numbers a^n and b^n correspond to the demands of conjugation, therefore, these numbers can always be represented by the product of two conjugate values. In this connection, the conversion of the numbers a^n and b^n into the product of two conjugate values is possible only by the differences $c - b$ and $c - a$, that

© Copyright 2007

this, by the differences formed by the triplet of numbers a , b and c , and not by the differences formed by the numbers other than a , b and c . However, the numbers a^n and b^n cannot be represented by the product of two conjugate variables by this method, because the second cofactor on the right side of equations (1''') and (1'''') is simple in relation to the sums $c + b$ and $c + a$, which form with the differences $c - b$ and $c - a$ the pairs of two conjugate variables. But the numbers a^n and b^n cannot be represented by the product of two conjugate variables by numbers other than a , b and c also. Since, in equation (1) the other methods of conversion of the numbers a^n and b^n into the product of two conjugate variables do not exist, then in this equation the numbers a^n and b^n in general cannot be represented by the product of two conjugate variables. But this is a contradiction of the properties of numbers, because any odd number greater than 2, and any even number divisible by 8, can always be represented by the product of two conjugate variables. We obtained a contradiction, which means, that an integer that is raised to the odd degree n cannot be represented by the difference of two other integers that are raised to the same odd degree n . Consequently, equation (1) for the odd degrees n greater than 2, does not exist with integers a , b and c .

Thus, in equation (1), the numbers a and b that are raised to the odd degree n , convert into the product of two cofactors only by the differences $c - b$ and $c - a$, which are organically entered into the structure of the product of two conjugate variables. On the other hand, the numbers a and b that are raised to the odd degree n , correspond to the demands of conjugation [except the case where $a = 1$, by which, equation (1) does not exist], therefore, the numbers a and b that are raised to the odd degree n , can always be represented by the product of two conjugate variables. However, only in equation (1) for the second degree, the numbers a^2 and b^2 convert into the product of two cofactors, which is simultaneously the product of two conjugate variables. Therefore, equation (1) for the second degree exists with integers a , b and c . In equation (1) for the odd degree n greater than 2, the numbers a^n and b^n convert into the product of two cofactors, which, by the numbers a , b and c cannot be represented by the product of two conjugate variables. But in equation (1) for the odd degree n greater than 2, the other methods of conversion of the numbers a^n and b^n into the product of two conjugate variables do not exist. Consequently, the numbers a^n and b^n , which correspond to the demands of conjugation, cannot be represented by the product of two conjugate variables. This is a contradiction to the properties of numbers. Fermat's Last Theorem is proved.

Nikolay Yesayan

NIKOLAY YESAYAN
December 05, 2008
Address: 7408 Kilcullen Drive, Charlotte, North Carolina 28270 – 2210, USA
E-mail address: umnikim@aol.com

© Copyright 2007