$e^{i\pi}=-1$

OCTOGON MATHEMATICAL MAGAZINE
Vol. 19, No.1, April 2011, pp 46-58
Print: ISSN 1222-5657, Online: ISSN 2248-1893
http://www.uni-miskolc.hu/~matsefi/Octogon/

The Fermat's last theorem

Nicolae I. Bratu [5]

ABSTRACT. In article [1], published in the famous Mathematical Magazine Octogon, I have presented a new demonstration of Fermats Last Theorem for exponents 3 and 5. After 2 years from the article publication and after another 4 years from the monograph publication [3] with regard to the previous results, I have received many messages of acceptance, a few invitations at international conferences and no single note challenging my results.

In this article we will generalise and make some additions to the method used in this demonstration theorem for exponents 3 and 5 and we will present a complete algebraic demonstration of Fermats Last Theorem.

We will number the relationships and the paper chapters in continuation of the article [1]. The short demonstration can be found on the web page Nicolae Bratu [4], published in 2001 and updated in 2006.

1. THE PRIOR MAIN RESULTS

1.1 Rewrite. We will rewrite only sequence 3.3 from the previous article [1]:

3.3. The completion of the Legendre propositions

Through the above stated contributions, the Legendre propositions are completed as it follows:

The Legendre- Bratu propositions

In the rational number field, part k3 of the first Legendre proposition is modified as follows:
$k3$ / for any p exponent, there are at least three representations of the Y and Z functions, through the y and z variables;

[5] Received: 27.02.2008
2010 *Mathematics Subject Classification.*11A07,13A05.
Key words and phrases. The cyclotomic and the quadratic fields; the method "infinite descent"; the Legendre numerical functions; the Bratu method for generating rational solutions (g.r.s.).

Consequently, part $k1/$ of the Legendre proposition is also modified:
$k1/$ there is a representation of the numerical functions $Y(y, z)$ and $Z(-y, z)$, where they are symmetrical functions in relation to the two variables (y, z), respectively $(-y, z)$; the other representations are not, generally, symmetrical in relation to the y and z variables.

At first, we will keep part $k2/$ of the first and second Legendre propositions intact, but we will return to them in the following chapter:
$k2$ / if the y and z variables are integer and relative prime numbers, the Z and Y numbers are integer and relatively prime.
$k4/$ if we decompose:

$$v^p = \frac{1}{2}(Y + \sqrt{\varepsilon p}Z) \cdot \frac{1}{2}(Y - \sqrt{\varepsilon p}Z) \tag{11}$$

the two factors from the second member are relatively prime, each of the two factors being a p power, it results:

$$Z = 0(\text{mod } p) \tag{12}$$

In proving the relation (12), Legendre assumed that it is the unique prime factorization of the number in the form of

$$(Y + \sqrt{\varepsilon p}Z) \tag{11.1}$$

Observation 4. The denominator, that is appears in the expressions (17) of the B matrix, for generating the rational solutions is number $p \pm 1$, that is not null and is not divisible by $p : p \pm 1 \neq 0(modp)$.
In the proof proposed hereinafter, the modulo p congruence of the denominator in the following formulas will be essential:

$$\begin{bmatrix} Y_1 \\ Z_1 \end{bmatrix} = \begin{bmatrix} Y \\ Z \end{bmatrix} .B \tag{18}$$

and the denominator of numbers Y_1 and Z_1 cannot modify the congruence $Z‘1 = 0(\text{mod } p)$, respectively $Y‘1 = 0(modp)$, where $Y‘1$ and $Z‘1$ are the denominators, integer numbers from the rational expression of the numbers Y_1 and Z_1.

Thus, the possibility to further write directly the modulo p congruence on the rational numbers Yi and Zi, respectively their denominators, $Y‘i$ and $Z‘i$, integers, without mentioning that reference is made to the denominators of these rational numbers can be justified.

1.2. Observation. We notice that, for the exponents 3 and 5, the Legendre Y_1 and Z_1 numbers are integer numbers, as well as Y and Z.

1.3. The number of relationships. We will number the relationships and the paper chapters in continuation of the article [1].

Chapter 4. THE PROOF FOR THE LAST THEOEM

Remark. *If the method for generating the rational solutions - g.r.s.- enabled the passage from the cyclotomic to the quadratic field, through the Euler-Legendre- Bratu Lemma- proved hereinafter - the entire issue can be transferred to the rational number divisional ring where the fundamental arithmetic theorem has validity.*

4.3- The proof of the Last Fermat Theorem for the exponents $p = 4k + 1$

4.3.1. The case of the exponents $p = 4k + 1$ can be solved in the real quadratic divisional ring $R(\sqrt{p})$.
If Legendre‘s argumentation was accepted, regarding the prime factorization in the real quadratic divisional rings $R(\sqrt{p})$, the L-B proposition, used in proving the theorem for the exponent $p = 5$ is applicable in the "real case" proof.

For the exponent $p = 5$- discussed above in chapter 4.2- the algebraic integers

$$U_5 = (Y + \sqrt{5}Z)$$

are real numbers.
By the completion of Euler and Legendres ideas, the method applied to the exponent 5 may be fit for any $p = 4k + 1$.

4.3.2. It may analogously be proved to Legendre that the numbers

$$Up = (Y + \sqrt{\varepsilon p}Z) \tag{25}$$

for any p prime number $4k + 1$ and $\varepsilon = 1$ are algebraic numbers.

4.3.3. If the numbers Y and Z are relatively prime, through the Legendre-Bratu proposition, it is obtained that:

$$Z = (\text{mod } p) \tag{21}$$

4.3.4. We apply the k3 part of the L-B proposition, respectively the relation (17-1), and, from the integer and symmetrical functions of Legendre, Y and Z, we obtain expressions for the rational functions of Legendre, Y_1 and Z_1:

$$\begin{bmatrix} Y_1 \\ Z_1 \end{bmatrix} = \begin{bmatrix} Y \\ Z \end{bmatrix} .B_p \tag{18 − p}$$

where B_p is the B matrix in the real case, from the relation (17-1):

$$B = \frac{1}{p-1}\begin{bmatrix} p+1 & 2p \\ 2 & p+1 \end{bmatrix}$$

It results:

$$Y_1 = \frac{1}{p-1}[(p+1)Y + 2pZ] \text{ and } Z_1 = \frac{1}{p-1}[2Y + (p+1)Z] \tag{26}$$

4.3.5. From the congruence

$$Z_1 = 0\,(\text{mod } p) \tag{27}$$

applied to the denominator Z‘1,
It results that $Y = 0(\text{mod } p)$, so $z = y = 0(\text{mod } p)$, i.e. an infinite descent and the conclusion of the Fermat theorem.
We notice that for exponents $p > 5$, the Legendre Y_1 and Z_1 numbers are generally no longer integer numbers like Y and Z.

4.4-The proof of the last Fermat theorem for what ever p exponents

For the exponents $p = 4k + 3$, named "imaginary case", the uniqueness of the prime factorization in the imaginary quadratic divisional ring $R(\sqrt{-p})$, assumed by Euler and Legendre, is no longer valid.
This dilemma has also come up during the proof of the proposition k4, that belongs to Legendre and that we reproduce:
k4/ If we factorize:

$$v^p = \frac{1}{2}(Y + \sqrt{\varepsilon p}Z) \cdot \frac{1}{2}(Y - \sqrt{\varepsilon p}Z) \tag{11}$$

The two factors from the second member are relatively prime and each of the two factors being p power, it results:

$$Z = 0(\text{mod } p) \tag{12}$$

In proving the relation (12), Legendre assumed that it is the unique prime factorization of the numbers in the form of

$$(Y + \sqrt{\varepsilon p} Z) \tag{11 - 1}$$

But, we wonder: Is the way of proving the Legendre relation (12) really unique?
If we could avoid the factorization in quadratic imaginary fields $R(\sqrt{-p})$, the Euler- Legendre proof, completed as above, could be generalized. Therefore, we resume the proof, *ab* initio, by inserting a new idea.

4.4.1. We write the Fermat equation symmetrically:

$$x^p + y^p + z^p = 0 \tag{28}$$

4.4.2. Legendre used the decomposition of the sum $y^p + z^p$, with p odd prime number:

$$y^p + z^p = (y + z)\,\frac{y^p + z^p}{y + z}$$

For the second factor from the right member, Legendre proved the general relation where Z and Y are integer numerical functions of z and y, and $\varepsilon = (-1)^{\frac{p-1}{2}}$.

4.4.3. We keep and use the Legendre formula and propositions:

The First Legendre Proposition. The numerical functions $Y(y, z)$ and $Z(-y, z)$ have the following properties:
k1/ they are symmetrical functions in relation to the two variables (y, z), respectively $(-y, z)$;
k2 / if the variables y and z are integer and relatively prime numbers, the numbers Z and Y are integer and relatively prime.

4.4.4. Legendre succeeded to prove that if:

$$w^p = (Y^2 + pZ^2) \tag{29}$$

where Y and Z are relatively prime, it is obtained:

$$Z = 0\,(\text{mod } p) \tag{31}$$

Euler, Legendre and all the researchers that studied the general equation (29) searched correctly [we proved it in the first part - 1.4.] solutions such as:

$$w = \left(r^2 + ps^2\right) \tag{30}$$

where r and s are arbitrary integers

4.4.5. Then, by the method initiated by Euler- Legendre, the factorization of the numbers w^p and w in the imaginary quadratic field is performed, considering that:

$$Y + \sqrt{-p}Z = \left(r + \sqrt{-p}s\right)^p; \qquad Y - \sqrt{-p}Z = \left(r - \sqrt{-p}s\right)^p$$

Y and Z result as polynomial expressions in r and s.
The uniqueness of the prime factorization in the $R(\sqrt{-p})$ fields must be proved.
The resolution is particular for various fields, being necessary to study the algebraic integer Dp ring units, according to the methods initiated by Kummer, regarding the regulated prime numbers.
Through this method, but omitting the requirement to prove the uniqueness of the prime factorization, Euler proved the Fermat theorem, for $p = 3$.
Euler obtained the relations (4) in chapter 2.2:

$$Y = s(s^2 - 9t^2) \text{ and } Z = 3t(s^2 - t^2)$$

4.4.5-1. We replace fragment 4.4.5 from the proof above with the following:

The Euler- Legendre-Bratu Lemma- that we will prove in chapter 4.5
B1- If number w is represented as

$$w = \left(r^2 + ps^2\right) \tag{32}$$

where r and s are arbitrary integers, then

$$w^p = \left(Y^2 + pZ^2\right) \tag{33}$$

where $p \geq 3$ is an odd prime number, Y and Z are numerical functions of r and s, and for number Z we have the congruence:

$$Z = 0 \,(\text{mod } p) \tag{34}$$

B2- For number $w^p = (Y^2 + pZ^2)$, in the rational numbers field, there is a representation by the integer and symmetrical functions Y and Z of Legendre and there are at least another two representations by rational functions Y_i and Z_i.
B3- The lemma is also valid for the representation of the number w by the quadratic form $(r^2 - ps^2)$, referred to above as the "real case".

4.4.6- Fragment 4.3.5 in the proof is kept.
We proved (chapter 1) that the property $Z = 0(\text{mod } p)$ is kept for all the linear transformations proper to the quadratic representation form of the w number.
From the congruence

$$Z_1 = 0 \,(\text{mod } p) \tag{37}$$

applied to the denominator Z'1 in the relation (36) , results $Y = 0$, therefore r, respectively z, i.e. the infinite descent, discovered by Fermat.

4.4.7-We reached to the conclusion:

Between the non-zero integer numbers, there is no fermatian 3-tuple;
that is the formulation of the Last Fermat Theorem.

4.5- The Euler- Legendre- Bratu Lemma -
Using the Lemma stated and proved herein, the issue can be transferred from the quadratic field to the rational numbers field, where the fundamental arithmetic theorem has validity.

Lemma ELB:
B1- If the number w is represented

$$w = \left(r^2 + ps^2\right) \tag{31}$$

where r and s are arbitrary integers and p is an odd prime number, then

$$w^p = \left(Y^2 + pZ^2\right) \tag{33}$$

where p is an odd prime number, Y and Z are numerical functions of r and s, and for number Z we have the congruence:

$$Z = 0 \, (\text{mod } p) \tag{34}$$

B2- For the number $w^p = (Y^2 + pZ^2)$, in the rational number divisional ring, there is a representation through the integer and symmetrical functions Y si Z of Legendre and there are at least other two representations by the rational functions Y_i and Z_i.

B3- The lemma is also valid for the representation of the number w by the quadratic form $(r^2 - ps^2)$, respectively, for exponents $p = 4k + 1$, named the real case.

The proof of the part B1 of lemma is made by starting from the identity:

$$\left(a^2 + pb^2\right)\left(c^2 + pd^2\right) = (ac - pbd)^2 + p\,(ad + bc)^2 \tag{35}$$

If we raise $\left(a^2 + pb^2\right)$ to power p, by repeated multiplications, and by using the identity (35), and if we denote the two terms from the second member of the relation (35) through Cj and Dj, accordingly to the power j of the number w, we obtain:

$w^2 = \left(a^2 + pb^2\right)^2 = \left(a^2 - pb^2\right)^2 + p\,(2ab)^2 = C_2 + pD_2$;

$w^3 = \left(a^2 + pb^2\right)^3 = \left(a^3 - 3pab^2\right) + p\left(3a^2b - pb^3\right) = C_3 + pD_3$; etc.

For the simplicity of the explanation, we will only refer to the term D_j that we will write according to the modulo p congruence.

Thus, for the j power, we will have:

$Dj = [ja^{j-1}b + pf(a,b)]$, and at the p power we obtain:

$D_p = [pa^{p-1}b + pf(a,b)]$, which involves:

$D_p - = Z = 0(modp)$ - q. e. d.

Part B2 of the lemma was proved above, in chapter 4.3.

We apply part k3 of the L-B proposition, respectively the relation (17-2) and, from the Legendre integer and symmetrical functions Y and Z, we obtain expressions for the rational functions Legendre, Y_1 and Z_1:

$$\begin{bmatrix} Y_1 \\ Z_1 \end{bmatrix} = \begin{bmatrix} Y \\ Z \end{bmatrix} .B_p \tag{18 - p}$$

where B_p is B matrix in the imaginary case, from the relation (17-2), for $p = 4k + 3$:

$$B = \frac{1}{p+1}\begin{bmatrix} p-1 & 2p \\ -2 & p-1 \end{bmatrix} \qquad (17-2)$$

The first rational solution that may be solution in integer numbers, as in the cases $p = 3$ and $p = 5$ - from the relation (18-p) it results:

$$Y_1 = \frac{1}{p+1}\left[(p-1)\,Y + 2pZ\right] \text{ and } Z_1 = \frac{1}{p+1}\left[-2Y + (p-1)\,Z\right] \qquad (36)$$

Part B3 of the lemma refers to the real case and in the above relations, p will be replaced by (p). The lemma has, therefore, general validity, for any exponent $p \geq 3$, odd prime number.

4.6- The exemplification of the method by proving the cases p=3 and p=5.

In the conclusion of our contribution to proving the last Fermat theorem, we provide examples for the proof in the simplest cases of exponents.

4.6.1- The proof of the Last Fermat theorem for the exponent p=3

/3.1/ We write the Fermat equation in the form of:

$$x^3 + y^3 + z^3 = 0 \qquad (38)$$

/3.2/ From all the third forms (x, y, z) of integer relatively prime numbers, with x even number, that satisfy the equation (38), we choose the minimal 3-tuple;

/3.3/ We create the integer numbers Z and Y, that are relatively prime numbers and of different parities through the relations:

$$Z = z - y; \qquad Y = z + y \qquad (39)$$

/3.4/ Putting $x = 2u$, it is obtained:

$$u^3 = \frac{1}{4}Y\left(Y^2 + 3Z^2\right) \qquad (40)$$

where the integer factors from the right member are relatively prime.

/3.5/ Because the factor (Y2 + 3Z2) is a cube, and Y and Z are relatively prime, the Lemma E-L-B applies for the cube:

$$w^3 = \left(Y^2 + 3Z^2\right) \qquad (41)$$

and we obtain:

$$Z = z - y = 0\,(\text{mod } 3) \tag{42}$$

If we assumed we were in the second case of the Theorem, i.e. $y = 0(\text{mod } 3)$, the infinite descent follows immediately; otherwise, we can continue as follows;
/3.6/ We linearly transform the quadratic form (41) by matrix relation:

$$\begin{bmatrix} Y_1 \\ Z_1 \end{bmatrix} = \begin{bmatrix} Y \\ Z \end{bmatrix} .B, \text{ where } B = \frac{1}{p+1} \begin{bmatrix} p-1 & 2p \\ -2 & p-1 \end{bmatrix}, \text{ for } p = 3 \tag{43}$$

and we will obtain other expressions for the Legendre functions, Y and Z:

$$Y_1 = 2z - y \text{ and } Z_1 = y \tag{44}$$

/3.7/ From the congruence

$$Z_1 = y = 0\,(\text{mod } 3) \tag{45}$$

associated by the congruence (42), it results

$$z = y = 0(\text{mod } 3) \tag{46}$$

/3.8/ Therefore, we reached the contradiction to the hypothesis and the infinite descendant, a procedure found by Fermat and used by Euler and Legendre in proving the Last theorem for the exponents 3 and 5.

4.6.2- The proof of the Last Fermat theorem for the exponent p=5
We follow a sequence similar to the one in the case of exponent 3.
/5.1/ We write the Fermat equation in the form of:

$$x^5 + y^5 + z^5 = 0 \tag{47}$$

/5.2/ From all the third forms (x, y, z) of integer relatively prime numbers, with x as even number, that satisfy the equation (38), we choose the minimal 3-tuple;
/5.3/ We build the integer numbers Z and Y, that are relatively prime numbers of different parities through the relations:

$$Y = (z + y)^2; \qquad Z = z^2 + y^2 \tag{48}$$

/5.4/ The Fermat equation turns into:

$$u^5 = \frac{1}{4} Y \left(Y^2 + 3Z^2\right) \tag{49}$$

where the integer factors in the right member are relatively prime.
/5.5/ Because the factor $(Y^2 + 3Z^2)$ is a 5^{th} power, and Y and Z are relatively prime, the E-L-B Lemma is applicable for

$$w^5 = \left(Y^2 + 3Z^2\right) \tag{50}$$

and we obtain:

$$Z = z^2 - y^2 = 0 \,(\mathrm{mod}\ 5) \tag{51}$$

/5.6/ We linearly transform the quadratic form (50) through the matrix relation

$$\begin{bmatrix} Y_1 \\ Z_1 \end{bmatrix} = \begin{bmatrix} Y \\ Z \end{bmatrix} .B, \text{ where } B = \frac{1}{p-1} \begin{bmatrix} p+1 & 2p \\ -2 & p+1 \end{bmatrix}, \text{ for } p = 5 \tag{52}$$

and we will obtain other expressions for the Legendre Y_1 and Z_1 functions:

$$Y_1 = 4z^2 + 3zy + 4y^2 \text{ and } Z_1 = 2z^2 + zy + 2y^2 \tag{53}$$

/5.7/ From the congruence

$$Z_1 = 2z^2 + zy + 2y^2 = 0(\mathrm{mod}\ 5), \tag{54}$$

associated to the congruence (51), it results

$$z = y = 0(\mathrm{mod}\ 5) \tag{55}$$

/5.8/ Therefore, we reached a contradiction to the hypothesis and by it, to the infinite descent and to proving the Last Theorem. Q. E. D.
At this point we conclude the presentation of our contribution for the proof of the Last Theorem

FINAL NOTE

A few words about the Romanian scientific research: They say Research is the golden foot used by science to move one step ahead -and I would add-, conditional on the whole nation encouraging it". This is the way in which all developed countries have worked and they still do. Leaving aside the dark age of the 60 years of immoral ideology of the fight between social classes, when the scientific research was not supported, but controlled, what has happened in Romania in the past 20 years is an impiety. Frustration, mistrust and many times incompetence and professional rivalry have created and maintained malign elite.

With regret I must say that all the ideas from my work, and they were not a few, which were scientific novelties 20 years ago, have now randomly appeared and have lost their Romanian inception.

It is relevant the story of what I have called in 1994 the Pythagorean Ternary Tree", which is a special case of the theory Generalisation of Gauss Theorem for the Homogenous Quadratic Forms. In 1997 I sent to the Mathematical Gazette the work that I had already published in [4]. After 2 years, the article was still not being published. I have recovered with difficulty only a part of the work, and on the page where the Pythagorean Tree was drawn, it is calligraphically written: This would be too good!. Back then I wrote to the Romanian Academy and to the Institute of Mathematics which gave me a very brief reply: try publishing abroad".

But, after 7 years, in the year 2006, the graph on the page together with the irony This would be too good (to be true)! was completely taken over, including the praising of the unusual beauty of the tree, by the American professor R.A. [13] under the title Pythagorus Modular Tree. I have written before about this sad episode in [2]. The American Scientific Community, their colleagues, the magazine and the university defended R.A., considering that after 2500 years of Pythagoras enunciation, after 11 years, it is possible for two researchers to find an absolutely identical solution. In exchange, the Romanian community has remained deaf and mute, despite all explicit pleas sent by a few [academies and] international mathematical personalities. And it is not only about the systems inefficient and defective organisation, also not only about incompetence and not even about stupidity, but about something which is by far more serious: we do not feel in the Romanian style any longer and thus we put in jeopardy the very historical existence of our nation.

REFERENCES

[1] Bratu I.N. On the Fermats Last Theorem; a new proof for the cases n=3 and n=5 - Octogon Math. Mag., Vol. 16-no 2A- October 2008

[2] Bratu I.N. Graphs in the Theory of the Quadratic Forms- Octogon Math. Mag., Vol 16-no 1A- April 2008

[3] Bratu I.N. Disquisitiones Diophanticae, Craiova-2006, Ed .Reprograph

[4] http://bratu.oltenia.ro/ - The web page, published in 2001 and updated in 2006

[5] Bratu I.N. - O afirmatie mai tare pentru criteriul lui Grunnert din Ultima Teorema a lui Fermat, Bucuresti- 1991, Gaz. Mat. nr. 3- 4
[6] Bratu I.N. - Eseu asupra ecuatiilor diofantice, Craiova-1994, Ed. Adel
[7] Bratu I.N. - Note de analiza diofantica, Craiova-1996, Ed .M. Dutescu
[8] Bratu I.N. - Diophantine equations, The First Intern.. Conf. in Numb.Th., Craiova- 1997
[9] Bratu I.N - Memoriu catre Academia Romana- 1983 (nepublicat)
[10] Wiles Andrew - Fermats Last Theorem, Conf. of the proof, Boston University-1995
[11] Dickson, L. E. - History of the Theory of Numbers, Washington - 1920, Add. Washington Press
[12] Bachmann P.- Das Fermatproblem in seiner bisherigen Entwicklung- Springer Verlag- Berlin- 1976
[13] Alperin R. Pythagorus Modular Tree, American Math. Monthly- 2006

Email: mathnib@yahoo.com