ON THE FERMAT'S LAST THEOREM
A NEW PROOF FOR THE CASES n-3 AND n-5

NICOLAE I. BRATU
Email: mathnib@yahoo.com

ABSTRACT

In the work "Disquisitiones Diophanticae", published in 2006 in Romanian, I had gathered succinctly and schematized the content of the "Memorandum to the Romanian Academy" in 1983, concerning the Fermat's Last Theorem. This paper demonstrates a lemma representing a completion of the algebraic method proposed by us to prove the Fermat's Theorem.

Keywords: The cyclotomic and the quadratic fields; the method "infinite descent"; the method "g.r.s"(method for generating rational solutions); the algebraic integers.

1. History

In the 17th century, Pierre Fermat conjectured that the equation $x^n + y^n = z^n$ (1) had no solution in nonzero integers with n greater than 2. Known as Fermat's Last Theorem, the problem has little direct impact on broader fields of mathematics, but has precipitated considerable research of significant impact on number theory and algebraic geometry.

Fermat himself provided a proof for the case n=4; indeed he proved by induction (popularly: by "infinite descent") the slightly stronger result that no two fourth powers can ever sum to a perfect square. Euler proved the result for n=3, and Dirichlet and Legendre proved it for n=5.

By the 1980s attention had shifted from algebraic number theory to algebraic geometry as the appropriate tool for the problem. Gerd Faltings' work on the Mordell conjecture implied in particular that for any n there were at most a finite number of solutions to the Fermat equation

What Ribet proved is that given a nontrivial solution to the Fermat equation, the elliptic curve described by the equation $y^2 = x (x - a^n) (x + b^n)$ would be fairly well-behaved, but would also be a counterexample to the Taniyama-Shimura conjecture. The T-S conjecture is of great interest in elliptic curves and was not completely proved by 1994.

However, Wiles has given a proof valid for most elliptic curves; in particular, his proof is sufficient to prove that counterexamples of the Frey/Ribet sort cannot exist. This proves there are no nontrivial solutions to the Fermat equation.

I considered that, after the success of its proof by Andrew Wiles, a return to some considerations, presented many years ago in the Memo to the Academy, would not have the skepticism impact and the impossible appearance it had back then.

2. The current elementary and algebraic theory of the Last Theorem

2.1- The cyclotomic field

It is obvious that the theorem must be proved in the case of all odd prime numbers. It was also agreed that in the study of the Fermat equation (1), two cases be distinguished: *when the rational integers* x,y,z *are not divided by* n *was named the "first case" of the theorem, and when one and only one of the numbers* x,y,z *in divided by* n *was considered to be the "second case" of the theorem.*

The algebraic proof of the Fermat Theorem is related to the prime factorization issue of the algebraic numbers. The sole general method of proof comes up with Kummer, where the fundamental role is played by a *Km divisional ring*, named the *m-cyclotomic field.*

Definition1- Let *m* be a natural number and ζ a mth primitive root of the unit. As all the mth roots of 1 are represented in the complex number plan by points dividing the circle with the unit radius in *m* equal parts, the R (ζ) field was named *field for the division of the circle in* m *parts*, or *m- cyclotomic field.*

Any *a* number from the *Km* divisional ring is uniquely represented in the form of:

$$a = a_0 + a_1 \zeta + \ldots\ldots\ldots + a_{(m-2)} \zeta^{m-2} \qquad (2)$$

For the proof of the Great Theorem, Kummer studies through profound methods the *Dm* ring unit group structure, created the theory of ideals and introduced the regular numbers. We will not try to detail these methods here, exceptional for the development of mathematics, used by Kummer and other remarkable researchers.

In summary, we presented such theories in the work [7].

2.2 The Euler proof, for the exponent p=3

The Euler Method remains essential for the Fermat theorem approach.

For the case p=3:

$$\mathbf{x^3 + y^3 = z^3} \qquad (3),$$

Euler was based on the following lemma:

The Euler Lemma- *If the integer and relative prime numbers* a *and* b *have the property that* $(a^2 + 3b^2)$ *is the cub of an integer number, then the* **s** *and* t integers exist, *so that:*

$$a = s(s^2 - 9t^2) \quad \text{si} \quad b = 3t(s^2 - t^2) \qquad (4)$$

The Euler proof can be schematized in the following steps:

2.2.1- It is assumed that, in the 3-tuple (x,y,z), x is an even number and that we choose the minimal 3-tuple, where $|\mathbf{x}|$ has the smallest value

2.2.2- We build the integer numbers a and b, that are relatively prime and of different parities, through the relations:

$$z = b + a; \quad y = b - a \qquad (5)$$

2.2.3- Putting x=2u, it is obtained:

$$u^3 = \frac{1}{4} a(a^2 + 3b^2) \qquad (6),$$

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

The relation (6) is essential in proving the Theorem and, in the general form, it was used by Legendre and overtaken in our research.

2.2.4- Because the factor $(a^2 + 3b^2)$ is a cube, the lemma is proved, by assuming that the factors $(a+ b\sqrt{-3})$ and $(a - b\sqrt{-3})$ are relatively prime and also, cubes:

$$(a + b\sqrt{-3}) = (s + t\sqrt{-3})^3 \qquad (7)$$

The relations (4) are obtained, where

$$a = s(s^2 - 9t^2) \quad \text{si} \quad b = 3t(s^2 - t^2)$$

2.2.5- According to the lemma, it is concluded that the number is a cube:

$$2s(s^2-9t^2) = 2s(s-3t)(s+3t) \qquad (8)$$

2.2.6- The factors from the right side are again relatively prime and by writing the algebraic sum of the three cubes, with $x_1^3 = 2s$: $y_1^3 = -(s+3t)$: $z_1^3 = (s-3t)$,

it is obtained: $$\mathbf{x_1^3 + y_1^3 = z_1^3} \qquad (9)$$

where $|\mathbf{x}_1| > |\mathbf{x}|$, i.e. a contradiction compared to the hypothesis.

This relation is a brilliant identity found by Euler that, yet, singularizes the proof for the exponent 3.

2.2.7- The same contradiction is reached descending the 3-tuple **(x, y, z)** and if the number **a** would be assumed as divisible by 3**,** i.e. for a=3r.
2.2.8- Euler proved the Lema, by assuming that the complex numbers *$(a + b\sqrt{-3}\ )$* are uniquely prime factorized.
It had to be proven and the following corollary was subsequently proved:
In the quadratic integer D3 ring, the fundamental arithmetic theorem is applied.
2.2.9- Subsequently, Legendre, through the congruent theory, proved that one and only one of the numbers x,y,z , of an equation solution, is divided by 3, i.e., we face the "second case" of the Fermat Theorem. Thus, the proof simplified.

2.3 A formula and two propositions of Legendre

In the work "Mem de la Acad. des Sciences, Institut de France" (1823), A. M. Legendre, among other special results, presented a formula we used in order to make the passage from the cyclotomic field to the quadratic field possible.
By writing the Fermat equation symmetrically:

$$\mathbf{x^p + y^p + z^p = 0} \qquad (1\text{-}p),$$

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

$$\frac{y^p + z^p}{y+z} = \frac{1}{4}\ (Y^2 - \varepsilon\, pZ^2) \qquad (10),$$

where ***Z*** and ***Y*** are integer numerical functions of *z* and *y*, and $\varepsilon = (-1)^{\frac{p-1}{2}}$

"The Legendre Formulas – for the numerical functions Z and Y- are very complicated" {[1], [2], [3]} but integers will always be obtained and the **Y** function will be symmetrical in relation to (z, y), while the **Z** function will be symmetrical in relation to (z, -y).
We reproduce the formulas found by Legendre, for several exponents:
For p=3: $\mathbf{Y= z+y}$; $\mathbf{Z= z- y}$ (10-3)
For p=5: $\mathbf{Y=(z+y)^2}$; $\mathbf{Z= z^2+ y^2}$ (10-5)
For p=7: $\mathbf{Y= 2(y^3+z^3)- yz\ (y+z)}$; $\mathbf{Z= yz\ (z- y)}$ (10-7)
Definition 1- We named the expressions **Y** and **Z**, obtained by Legendre, the "*Legendre integer and symmetrical functions",* in order to separate them from other expressions, that we will name the "*rational Legendre functions",* obtained by using our method for solving the Pell equations [9], generally, non-integer and non-symmetrical in relation to the variables.
The authors {[1], [2],[3]} believed, to date, the reproduction of the Legendre formulas to be useless, because *"they are very complicated and useless".*
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 y and z variables are integer and relatively prime numbers, the numbers **Z** and **Y** are integer and relatively prime.*
Legendre also stated that:
k3/ Y and Z have a unique expression, depending on the variables y and z;
In our works, we showed that the last statement is not true in the integer number ring, for certain exponents, and, if we extend the problem to the rational number divisional ring, the statement is not true for any **p** exponent.
The Second Legendre Proposition - Legendre also showed:
k4/ if we decompose:

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

the two factors in the second member are relatively prime and, each one of the two factors being a **p** *power, it results:*

$$Z = 0\ (\mathrm{mod}\ p) \qquad (12)$$

Legendre assumed that it is the unique prime factorization of the numbers in the form of $(Y + \sqrt{\varepsilon p}\,Z)$ *(11-1)*

For the numbers **p= 4k+1**, respectively for the real quadratic divisional ring, his proof was accepted, and his statement can be considered to be a theorem.

As regards the imaginary quadratic field, respectively for the exponents **p= 4k+3**, the statement was not proved subsequently either, although Kummer, through his theory of ideals, and through the non-elementary methods, remarkable progress was made.

That is why, for **p= 4k+3**, *the second Legendre proposition* remained at the conjecture level.

2.4 The representation of numbers through quadratic forms

We resume the theory {[9] and [10]}, through the following observations and completions:

Observation 1- For the particular case of an integer number ***w*** that can be represented by binary quadratic forms:

$$w = Y^2 - \varepsilon\, pZ^2 \qquad (13),$$

the theory especially according to Gauss and Lagrange, solved all three subjects (S), defined above [7]

The quadratic forms (13) result from the formulas (10), introduced by Legendre.

Observation 2- For w=4 and for number **p** not a perfect square, the equation (13) is identical to the reputed Pell equation.

3. Contributions to the current theory

3.1- The reduction of the second case of the Fermat theorem in the first case

Until 1983 it had already been proven that, if there are solutions for the Fermat theorem, in a counter-example, it had to be operated with number larger than 10^6

In the work [5] we proved that, the statement above can be greatly consolidated, i.e., in a counter-example, one must operate with numbers x,y,z larger than 10^{30}, in the first case of the theorem and larger than 10^{18}, in the second case of the theorem.

We reproved a proposition that we reproduce from [5], by changing a few notations:

Proposition B1- *In the rational integer ring, if we decompose the sum* $\mathbf{y^p + z^p}$, *where* p - *odd prime, in two factors, that is*:

$$y^p + z^p = (y+z)\ \frac{y^p + z^p}{y+z} \qquad (14),$$

where y and z *are relatively prime to each other and relatively prime also to the exponent* p – *then the first factor is divided by* p, *if and only if the second factor is divided by* p *and is not divided by* p^2

In the first case of the Fermat Theorem, the left member of the relation (11) being a pth power, and the factors being relatively prime, we write the relation:

$$v^p = \frac{1}{4}\,(Y^2 - \varepsilon\, pZ^2) \qquad (15\text{-}1)$$

Consequence 1 - From *Proposition B1, the second case of the Great Theorem is reduced to the first case.*

If we denote: **Y=pZ'** si **Z=Y'**, we will get:

$$(-\varepsilon v)^{p} = \frac{1}{4}(Y'^{2} - \varepsilon pZ'^{2}) \qquad (15\text{-}2),$$

i.e. an identical relation.

3.2- The method for generating rational solutions - g.r.s.

The method for generating rational solutions of the homogenous equations (g.r.s. method), presented in [[9],[10],[11]], proves its utility in this particular case as well.

Observation 3- Lemma 1a {[9] and[10]} that we reproduce is important: *Given a non-zero solution* $(x_1, x_2 \ldots\ldots x_n)$ *of a quadratic equation with n>1, , at least two other solutions in positive rational numbers can be deduced through a recurrence relation; except for the common solution, from where only one other solution can be deduced.*

We showed before (ibidem) that, by applying the method for generating the rational solutions (g.r.s.), always possible in the case of equations of the type (13), we can determine concretely the representations of an integer number ***w***, respectively, we can deduce other rational solutions, if an ordinary solution is known, including the common one, of the Pell type quadratic equation (13).

Through the *method g.r.s.* finding the positive minimal solution is avoided, used in Lagrange's method, where finding the solution is not always easy.

In the real case of the Pell equation:

$$\mathbf{x^2 - py^2 = 1} \qquad (16\text{-}1).$$

for **p>1**, the **B** matrix is written:

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

In the general method for finding the rational solutions for the Pell type equation, we proved that **Lemma 1a** also applies in the imaginary case, i.e. for the equation:

$$\mathbf{x^2 + py^2 = 1} \qquad (16\text{-}2).$$

The **B** Matrix in the imaginary case and for **p ≠ -1**, is written:

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

By using the notation $\varepsilon = (-1)^{\frac{p-1}{2}}$, we can write a general form equation:

$$\mathbf{Y^2 - \varepsilon\, pZ^2 = 1} \qquad (16)$$

For **p= 4k+1**, we will have the real case, **B** Matrix, that generates the set of rational solutions, having the form (17-1), and for **p= 4k+3**, we will be placed in the imaginary case, **B** Matrix being denoted as (17-2).

4.3- The completion of the Legendre propositions

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

The Legendre- Bratu proposition – 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;

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.*

For the starters, 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:

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

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

$$\boldsymbol{Z= 0\ (mod\ p)} \qquad (12)$$

In proving the relation (12), Legendre assumed that it is the unique prime factorization of the number in the form of $\boldsymbol{(Y + \sqrt{\varepsilon p}\,Z\,)}$ *(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±1,** that is not null and is not divisible by *p:* p±1 ≠ 0 (mod p).

In the proof proposed hereinafter, the modulo p congruence of the denominator in the following formulas will be essential:

$$\begin{pmatrix} Y_1 \\ Z_1 \end{pmatrix} = \begin{pmatrix} Y \\ Z \end{pmatrix} . \mathbf{B} \qquad (18),$$

and the denominator of numbers *Y1* and *Z1* cannot modify the congruence *Z'1= 0 (mod p)*, respectively *Y'1=0 (mod p)*, where *Y'1* and *Z'1* are the denominators, integer numbers from the rational expression of the numbers *Y1* and *Z1*. 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.

Observation 5-From this summarized presentation, it results that, in the rational number field, there are other expressions for the Y and Z numerical functions in the relation (10). The new expressions, *Yi* and *Zi*, generated by the method g.r.s., are generally no longer symmetrical in relation to the variables (y, z), respectively (-y,z), and we named them *the Legendre rational functions.*

4.1- Another path in the Euler proof, for the exponent p=3

It is obvious that in an attempt to generalize Euler's ideas, in the contents of his proof for the exponent 3, another path must be found to avoid the use of the particular identity found by Euler, in step 2.2.6, above, where we obtained the relation (9): $\mathbf{x1^3 + y1^3 = z1^3}$

First of all, we notice that it is valid and the statement *k4/* of the Legendre propositions can be easily verified. If we write:

$\mathbf{Y = a = s(s^2 - 9t^2\,)}$ and $\mathbf{Z= b = 3t(s^2 - t^2}$) (19),

it is verified **Z= 0 (mod3)** (12-3)

We will apply the **Legendre- Bratu proposition** for the case **p=3** and **ε= -1:**

We write the equation (3) in the form of:

$$\mathbf{x^3 + y^3 + z^3 = 0} \qquad (1\text{-}3)$$

The proof for this new method, for the exponent **p=3**, was schematized [6] in the following steps:

4.1.1- It is assumed that, in the third form **(x,y,z)**, **x** is an even number and that we choose the "minimal" third form, where ı**x** ı has the smallest value.

4.1.2- Legendre proved that for the exponent **p=3,** we find ourselves in the second case of the Theorem. We assume that y= 0 (mod 3).

4.1.3- We take the integer numbers **Z** and **Y**, that are relatively prime and of different parities through the relations:

Z= z-y ;   Y= z+y   (20)

4.1.4- Putting **x=2u**, it is obtained:

$$u^3= \frac{1}{4}\, Y\,(Y^2 + 3Z^2) \qquad (21),$$

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

4.1.5- Because the factor is a cube, and Y and Z are relatively prime, the L-B proposition applies for the cube:

$$w^3= (Y^2 + 3Z^2) \qquad (22)$$

and because we assumed that we are in the second case with y= 0 (mod 3), having:

Z= z -y and Z=0 (mod 3),   it follows

z=0 (mod 3) and the infinite descent result, i.e. the Fermat theory is true.

4.1.6- The proof was completed for the same gaps as in case of the Euler theorem, mainly the corollary had to be proved: *In the ring of the quadratic integers D3, it applies the fundamental theorem of arithmetic's.*

4.2- Another path in the Legendre proof, for the exponent p=5

4.2.1 - Legendre proved the Fermat theorem for p=5, by applying the congruent theorem and by starting from the study of algebraic integers in the form of

$V_5 = \frac{1}{2}\,(Y + \sqrt{5}\,Z\,)$,   where Y and Z are relatively prime and we have:

Z=0 (mod 5)   (12-5).

The algebraic integers V_5 are real numbers, and the prime factorization did not face the difficulties in case **p=3**, where the numbers were complex.

4.2.2 For **p=5**, accordingly (10-5), we have:

Y=(z+y)^2 si   **Z= z^2+ y^2**   (10-5).

4.2.3- Instead of going deeply into the study of the congruent theory, following the Legendre proof, we apply the k3 part of the **L-B proposition**, respectively the relation (17-2) and we obtain other expressions for the Legendre Y and Z functions:

$$\begin{pmatrix} Y_1 \\ Z_1 \end{pmatrix} = \begin{pmatrix} Y \\ Z \end{pmatrix} \cdot \mathbf{B}5 \qquad (18\text{-}5)$$

where **B**5 is the **B** Matrix in the real case, in the relation (17-1), for **p=5**. It results:

Y1 = 4z^2 +3zy+4y^2 si   **Z1= 2z^2 + zy +2y^2**   (23),

and from the congruence   **Z1= 0 (mod 5**   (24),

it follows **Y= 0 (mod 5)**, therefore **z=y=0 (mod 5)**, i.e. the infinite descent.

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.

5. Final note

We repeat the solicitation from the head note: Among our hypotheses and conclusions there may be some gaps that any reader can comment via our e-mail address. And if, by solving the gaps, a generalization of the demonstration may be possible, we shall be the first to yield due praise to the solver. We have sent the present demonstration so several Academies: the Romanian Academy has responded without involvement: “Publish it in magazines of worldwide circulation, in order to be acknowledged”. The Austral Academy, through the brilliant mathematician Mike Hirschhorn, gave us a polite response: “We have found a new demonstration of the Fermat's Last Theorem for exponents 3 and 5, but we do not believe that it can be generalized. The Romanian Academy must be the first to admit and decide if they will make it public to the international community". The same answer was given by other mathematicians in the world as well.

REFERENCES

1. DICKSON L. E. - *History of the Theory of Numbers*, Washington- 1920, Add. Washington Press.
2. BACHMANN P.- *Das Fermat problem in seiner bisherigen Entwicklung*- Springer Verlag- Berlin- 1976.
3. HARDY G.H., WRIGHT E.M. – *An introduction to theory numbers* –Oxford 1960.
4. WILES ANDREW- *Fermat's Last Theorem,* Conf. of the proof, Boston University- 1995.
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- *Memoriu catre Academia Romana*- 1983 (nepublicat).
9. BRATU I.N. – *Disquisitiones Diophanticae*, Craiova-2006, Ed .Reprograph.
10. BRATU I.N. –*Graphs in the Theory of the Quadratic Forms*- Octogon Math. Mag., vol. 16, no 1A, 2008.
11. BRATU I .N. and CRETAN N. A. – *A Generalization of Gauss Theorem on quadratic Forms,* New Delhi 2002, Bulletin of Pure and Applied Sciences, vol. 21E/1.