BULLETINS for APPLIED & COMPUTER MATHEMATICS

Pannonian Mathematical PAMM 1969 Applied Meetings

Interuniversity Network in Central Europe

BAM-1841 / 2001 (XCVI-A)

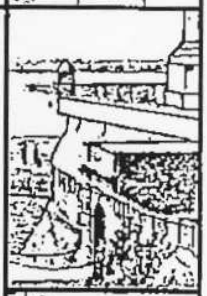
ALGORITHMIC SOLUTION OF THE ORIGINAL EUCLIDEAN FERMAT'S LAST THEOREM (EFLT)

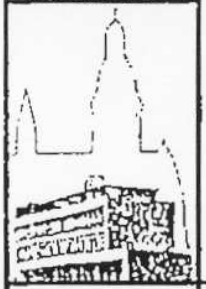
027 036

Written by

Malvina BAICA

University of Wisconsin – Whitewater





Caretaken by the **PAMM-Centre**

at the

Technical University of Budapest

BME

1782

BUDAPEST

Balaton — *Göd*

2001

The PAMM's periodical
BULLETINS for APPLIED & COMPUTER MATHEMATICS
(BAM)

BAM 1839-1865 / 2001 – XCVI-A

Lectred at the PC-133 / 2001 - Balatonalmádi and PC-134 / 2001 - Maribor–Trieste
ISSN 0133-3526

- Manuscript -

Prepared for publication at the
PAMM–Centre
Budapest, September 2001.

ALGORITHMIC SOLUTION OF THE ORIGINAL EUCLIDEAN FERMAT'S LAST THEOREM (EFLT).

MALVINA BAICA

Department of Mathematical and Comp. Sciences
The University of Wisconsin
Whitewater, WI 53190
U.S.A.

Abstract

In this paper the author will show that the Elliptical Fermat's Last Theorem (ELFLT) proved by Faltings in the geometry of the elliptic curves is equivalent to (not the same as) the original Fermat's Last Theorem stated by Fermat in Euclidean Geometry and proved by the author.

Key word and phrases:	Abbreviation:
Euclidean Algorithm	(EA)
Baica's General Euclidean Algorithm	(BGEA)
Euclidean Fermat's Last Theorem	(EFLT)
Elliptic Fermat's last Theorem	(ELFLT)

AMS (1991) subject classification : 11Y40, 11A05.

1. Introduction

In [12] the author expressed her genuine concern about the proof of Fermat's Last Theorem in the geometry of the elliptic curves (ELFLT) which may not be equivalent (let alone the same as) the result in the Euclidean Geometry where Fermat's Last Theorem originated (EFLT) about three hundred fifty years ago.

Problems are solved in mathematical models. We can generate as many mathematical models as we please. The elements are declared in order to determine the axioms and the definitions of the model. Using the mathematical logic consistent with the axioms and definitions, we can build any mathematical model required to solve mathematical problems in that corresponding model.

Likewise, we construct numerous geometrical models or geometries, but only one is the Euclidean Geometry. All of the others are called non-Euclidean geometries. The classical Euclidean Geometry is (E^n) in which $n = 2$ or (E^2), known as the Euclidean Geometry in quadratics.

We can not compute in a geometry and therefore to every geometry there is a corresponding specific algebra (although the converse is not true).

The algebra corresponding to a specific geometry is called the number theory (or arithmetic) of that geometry.

The tool that proves almost everything in any such number theory corresponding to a geometry is called the Euler System of that number theory.

If we want to prove a theorem in that number theory which satisfies the conditions of the Euler System (and the implementation is done right) then this theorem becomes a direct consequence of the Euler System [18] which itself is a theorem.

The geometries do not relate to each other, but they all relate to the topology. Because of this, if you prove something in one geometry it may not be the same as in another geometry.

Let's look for example at the V-th postulate in (EG) where two parallel lines do not intersect. In the Hyperbolic Geometry (HG) they intersect in two ideal points Ω and Ω' . Something nice can happen when the results are equivalent. The necessary transformation from Elliptic to Euclidean is required to show that those results in two distinct geometries are equivalent. But this is not enough. Once they are proved equivalent, in order to show that the results are actually the same, there is a need to provide the Galois' connection from category theory which requires the transformation to be an analytic continuous function. In other words, the functor has to be provided.

2. Statement of the problem

A. Wiles [30] announced his proof of the (ELFLT) in the summer of 1993. At that time the author was concerned that this was not the original (EFLT) and also that the implementation in their Euler System was not correct. Better saying the higher levels of the Euler System could not be constructed.

The number theory of the Geometry of the Elliptic Curves (GEC) is Hecke Algebra and the number theory of the Euclidean Geometry (E^n) is the Algebraic Number Theory, and therefore the original (EFLT) has to be proved in the Algebraic Number Theory.

In May 1994, the author presented her algorithmic euclidean proof of (EFLT) [10] at the International Conference on Analytic Number Theory in Allerton Park, at the University of Illinois in Urbana-Champaign.

Before its publication it was sent for revision to the Annals of Mathematics and on January 23, 1995 the answer was "There is no justification given for the claim that the (BGEA) algorithm has anything to do with Fermat's Last Theorem".

Hasse, who was the author's Ph.D. dissertation advisor, once stated : "The end of the 20-th century will bring the solution for Fermat's Last Theorem (FLT), and the solution will come from the use of the Euclidean Number Theory tools, as Fermat had intended".

Because of Hasse's beliefs, I was very surprised when the above mentioned answer was that Baica's General Euclidean Algorithm (BGEA), or that any generalized euclidean algorithm, does not have anything to do with the proof of the original Fermat's Last Theorem, which was stated in euclidean terms, and has a strong euclidean character.

Again, before its publication at the Conference on Number Theory and Fermat's Last Theorem held at Boston University on August 9-18, 1995, the author presented the paper with her (BGEA) algorithmic solution of the original euclidean Fermat's Last Theorem (EFLT). It generated many unprofessional responses at the conference from the opposing group. The author was deeply insulted by the organizing people because she expressed her concern about the proof of (EFLT) in the (GEC).

After the one hour talk titled "The geometry of elliptic curves", the author asked the invited speaker : "Sir, do you recognize that the geometry of the elliptic curves which you were describing just now is not euclidean ?". In response the author was told that : "You do not know any geometry, of course it is euclidean. Do you not know that the conic sections are euclidean, etc. ?". At this reaction to my very legitimate question, I was surprised that these very fine algebraic geometers do not make the distinction that the elliptic curves are elements in the (GEC), while they are definitions in the (EG).

In 1995 an in-house publication in the Annals of Mathematics at Princeton [30] accepted a proof of Fermat's Last Theorem in the Geometry of Elliptic Curves and its corresponding number theory which is Hecke Algebra, which was overwhelmingly embraced by the American Mathematical Society. The July 1995 Notices of the AMS published a translation from German of G. Faltings' March 1995 article [22] in which the author said at the beginning of the paper : "The proof of the conjecture mentioned in the title was finally completed in September of 1994. A. wiles announced this result in the summer of 1993. However, there was a gap in his work. The paper of Taylor and Wiles does not close this gap but circumvents it."

With this statement one of my concerns was justified. A. Wiles did not prove (ELFLT). It is G. Faltings who did it.

Now we will show that Faltings' (ELFLT) is equivalent to the original (EFLT) proved by Baica using her generalized Euclidean Algorithm known as Baica's General Euclidean Algorithm (BGEA). With this we show to the Annals of Mathematics that Baica's General Euclidean Algorithm (BGEA) has everything to do with the euclidean solution of (EFLT).

3. Solution of the problem

Hilbert related the existence of integer solutions for $x^2 + y^2 = z^2$ and the unrestricted periodicity of the (EA).

The unrestricted periodicity of the (EA) is a very important property and in the quadratic case it enables us to solve the Euler-Pell's equations $x^2 - m y^2 = \pm 1$ or ± 4 where m is a square free natural number, and to find the fundamental units in the quadratic field $Q(\sqrt{m})$. For quadratic extensions of Q, the group of units was completely determined when the above equations could be completely solved by simple continued fractions or from the (EA)'s unrestricted periodicity proved by the Euler-Lagrange Theorem.

In [20] Hasse and Bernstein investigated fields of the form $Q(\sqrt[n]{D^n + d})$ and proved the periodicity of their algorithm (HBA) which is a modification of the Jacobi-Perron Algorithm (JPA).

1) For $d > 0$ they proved that (HBA) of $a^{(0)}$ is purely periodic when $D \geq d\,(n - 2)$, $d \mid D$ and $n \geq 3$, and

2) For $d < 0$ the sequence is also purely periodic when $D \geq 2\,d\,(n - 1)$, $d \mid D$ and $n \geq 3$.

In the same paper they proved that the group of units can be found by multiplying the last components of the companion vectors in the period. In this way they proved that in both cases (1) and (2)

$$(1.1) \qquad l_k = \frac{w^k - D^k}{(w - D)^k}, \quad k \mid n, \quad k > 1$$

are the $\Im(n) - 1$ units in the corresponding real fields $Q(\sqrt{w})$, $w = \sqrt[n]{D^n + d}$, $d \mid D$, $D \in N$, $d \in Z$, $n \geq 3$.

(BGEA) is the extension of (HBA) to the complex numbers. It eliminates the bound on D and only the restriction $d \mid D$ remains in proving (BGEA) restrictive periodic.

The Hasse-Bernstein Theorem to find the group of units in $Q(\sqrt[n]{D^n + d})$ remains valid and we have the same units in both real and complex fields. We call the group of units the 'Galois group of units' referring to a Lemma on pg. 244 of [25] where it is proved that

Lemma 1. The Galois group of the cyclotomic field of order n over F of characteristic 0 is abelian.

Proof: Since $(x^n - 1)' = n x^{n-1}$ and $x^n - 1$ are relatively prime, $x^n - 1$ has n distinct roots $z_1, z_2, \ldots, z_n$. These constitute a subgroup U of the multiplicative group of the cyclotomic field. We know that U is cyclic. The map $\Phi \to \Phi \mid U$ of the Galois group G is a monomorphism of G into Aut U, the group of automorphism of the cyclic group U of order n. Thus G is isomorphic to a subgroup of Aut U and we know that the latter is isomorphic to the abelian group of units of the ring $Z/(n)$. Hence G is abelian.

Using this result we named the group of units in the ring of integers of an algebraic number field to be the Galois multiplicative group of units in the algebraic number field. Many mathematicians seem to object to this nomenclature and therefore we drop Galois and we stay with the old name of the multiplicative group of units in the algebraic number fields.

The author used (BGEA) to find solutions to infinitely many complicated n-dimensional Diophantine equations using units in the algebraic number fields.

In [17] the author gives the totality of solutions to this quadratic Diophantine equation of the form

(1.2) $$a^2 \pm a\,b + b^2 = c^2$$

Hasse gave the totality of solutions to (1.2) in parameter form and they are known as Hasse equations.

No explicit solutions of $a^2 + a\,b + b^2 = c^2$, $a + b > c > b > a$; $a, b, c \in N \setminus \{0\}$ and $a^2 - a\,b + b^2 = c^2$, $b > c > a > 0$; $a, b, c \in N \setminus \{0\}$ were known until the author observed that these are homogeneous Diophantine equations and with a proper linear transformation, they can be reduced to a simple Diophantine equation which can be solved explicitly.

This new method of solving $a^2 + a\,b + b^2 = c^2$ explicitly is to set $a = y - 1$, $b = y + 1$, $y \in N \setminus \{0\}$ and get Euler-Pell's equation $c^2 - 3\,y^2 = 1$ which can be solved by continued fractions or by the always-periodic (EA).

To solve $a^2 - a\,b + b^2 = c^2$, we set $a = (y + 1)/2$, $b = y - 1$, $y \geq 2$, $y \in N \setminus \{0\}$ and get a corresponding Euler-Pell's equation of the same type $c^2 - 3\,y^2 = 1$.

The infinite number of solutions to Euler-Pell's equation gives rise to an infinity of solutions to the Hasse's quadratic Diophantine equations. In quadratics it is always possible to find some transformations to reduce almost any quadratic equation to an Euler-Pell's equation and then to solve it explicitly from the periodicity of the (EA) which is related to units in the quadratic fields.

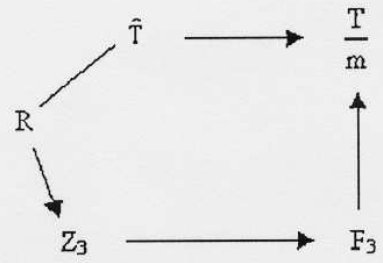
For higher degree Diophantine equations this is not possible since (BGEA) is not always periodic for any $\sqrt[n]{k}$.

In [2,5] Baica obtained the solutions of all higher degree Diophantine equations from units in the higher degree fields where (BGEA) became periodic, and those equations are not of the type $x^2 + y^2 = z^2$ for $n \geq 3$. Therefore since (BGEA) is the higher dimension Euler-System [18] as (EA) is the Euler-System for quadratics in the algebraic number theory (which is the number theory or algebra of the (EG)), $x^2 + y^2 = z^2$, $n \geq 3$ is not of the type [2,5] which were solved from the restricted periodicity of (BGEA), and therefore it does not have integer solutions for $n \geq 3$.

As we see the solution of (EFLT) has everything to do with the restricted periodicity of (BGEA) for $n \geq 3$.

4. Faltings' solution of (ELFLT)

In [22], the constructed l – adic representation for $l = 3$, starting with the representation on the 3 – division points, leads to the following commutative diagram :



The problem was to show that in this diagram $R = \hat{T}$.

Modularity is essential and this can be considered the Euler-System for their number theory (Hecke Algebra).

At the beginning A. Wiles attempted to establish equality by using Euler Systems (invented by Kolyvagin). The higher levels of the Euler System could not be constructed.

In Faltings' proof, he shows the minimal case and then reduces to it.

In the limit R_l and $\hat{T}_l$ become rings of power series and they become equal. R is obtained from R_l and $\hat{T}$ from $\hat{T}_l$. To reduce to the minimal case, from level M to a higher level N, an upper bound and a lower bound were found, and they coincided. At the end both deal with the solvability by radicals in the algebraic numbers.

This completes the proof that the (ELFLT) is equivalent to the original (EFLT) in Euclidean Geometry. The (ELFLT) is not the same as (EFLT). The original (EFLT) is stated and proved by the author in euclidean Geometry and the other (ELFLT) is proved finally by Faltings in Elliptic Geometry. They are equivalent, but not the same.

REFERENCES :

[1] M. BAICA, An algorithm in a complex field and its applications to the calculation of units (ACF). Pacific J.Math.Vol.110, No.1, (1984), 21-40.

[2] M. BAICA, n-Dimensional Fibonacci numbers and their applications. The Fibonacci quarterly.Vol.21, No.4(1983), 285-301.

[3] M. BAICA, Some new combinatorial identities derived from units in algebraic number fields. Discrete Mathematics 54(1985), 133-141.

[4] M. BAICA, Approximation of irrationals. Internat.J.Math. Sci.Vol.8. No.2, (1985) 303-320.

[5] M. BAICA, Diophantine Equations and Identities. Internat. J.Math. Math. Sci. Vol.8. No.4(1985), 755-777

[6] M.BAICA, More units from the periodicity of an algorithm. Bul.NumbTheory, Vol.XII (1988), p.81-89.

[7] M. BAICA, Halter-Koch units from the periodicity of (ACF) Algorithm. Bul.Numb.Theory, Vol.XIII (1989), p.73-80.

[8] M. BAICA, Hermite's problem from the periodicity of (ACF) algorithm. Bul.Numb.Theory, Vol.XIV (1990), p.57-67.

[9] M. BAICA, Hilbert's demand for the disclosure of units in algebraic number fields. Bul.numb.Theory, vol.XVI (1992), p.149-163.

[10] M. BAICA, Baica's General Euclidian Algorithm (BGEA) and the solution of Fermat's last Theorem (FLT).Notes on number theory and discrete mathematics (NNTDM) 1. (1995)3, (120-134).

[11] M. BAICA, More explanations about Baica's proof of Fermat's last theorem. NNTOM 2, (1996)1, 15-19.

[12] M. BAICA, The Euclidian character of the Fermat's last theorem.NNTDM 2 (1996) 1, 20-23

[13] M. BAICA, Baica's solution of Fermat's last theorem in euclidian, models and algorithms, the transition from abstract to applied mathematics, Analele Universității "Eftimie Murgu", Reşiţa, Fascicole III. Anul III, (1996) 267-278.

[14] M. BAICA, Baica's general euclidian algorithm (BGEA) restricted periodicity an N-dimensional equivalent of Euler-Lagrange theorem from quadratics. Buletinul Stiințific al Universității "Politehnica" din Timişoara, Tom 42(56). 2 Mat.&Fizică, (1997), 18-23.

[15] M. BAICA, General Euclidian algorithm (BGEA) and sums of some infinite series. Buletinul Stiințific al Universității "Politehnica" din Timişoara Tom.43(57).1 Mat.&Fizică (1998) 54-61.

[16] M. BAICA, Some infinite series and sums from (BGEA). Buletinul Stiințific al Universității "Politehnica" din Timişoara Tom 43 (57),2 Mat.&Fizică. (1998) 8-15.

[17] M. BAICA, Pythagorean triangles of equal areas, Internat. J. Math. Sci. Vol II No. 4 (1988), 269-280.

[18] M. BAICA, The Euler System for the Algebraic Number Theory and mathematical models in pollution, MB – 15 / PAMM (Book – 144 pages).

[19] L. BERNSTEIN : The Jacobi - Perron algorithm, its theory and application, Springer, Berlin-Heidelberg-New York. Lect. notes, Math, 207 (1971).

[20] L. BERNSTEIN and H. HASSE : Einheitenberechnung mittles des Jacobi - Perronschen algorithmus, J.Reine. Angew, Math, 218 (1965), 51-69.

[21] P. ERDOS : Arithmetical properties of polynomials. J. London. Math. Soc. 28 (1953), 416-425.

[22] G. FALTINGS : The proof of Fermat,s last theorem by R. Taylor and A.Wiels. Notices of the AMS, V.42, No.1, (July 1995), p.743.-746.

[23] C. HERMITE : Letter to C.G.J.Jacobi, J.f.d.Reine Angew. Math.40 (1839), 286.

[24] C.G.J. JACOBI : Allgemeine theorie der kettenbruchaehnlichen algortihmen, in velchen jede zahl aus drei vorhergehenben gebildet wird, J.f.d. keine angew. Math, 69 (1869), 29-67.

[25] N. JACOBSON : Basic Algebra I, W.H. Freeman and Company.

[26] H. LONDON and R. FINENSTEIN, On Mordell's equation, Bowling Green State University Press, Bowling Green 1973.

[27] O. PERRON : Grundlagen füer eine theorie des Jacobischen kettenbruchalgoritmus, math. ANN, 64 (1907), 1-76.

[28] O. PERRON : Ein Neues komvergenzkriterium für Jacobi-Ketten 2, ordung, Arch.Math.Phys (Reine 3) 17 (1911) 204 -211.

[29] A.J. VAN DER PORTEN : Remarks on Fermat's Last Theorem, Macquario Number Theory Reports from : Austral. Math. Soc. Gazette 21 (1994), p. 150-159.

[30] A. WILES : Modular elliptic curves and Fermat's Last Theorem, Annals of Mathematics, Vol. 142, No. 3 (1995), 443-551.