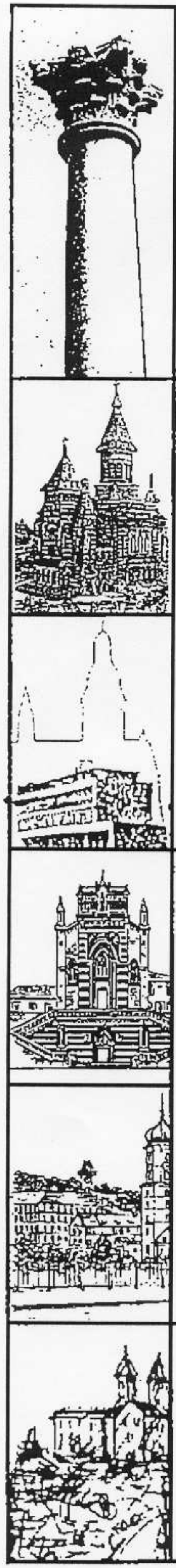

BULLETINS for APPLIED & COMPUTING MATHEMATICS

Pannonian Mathematical PAMM 1969 *Applied Meetings*

Interuniversity Network in Central Europe

BAM-1743/2000 XCII-A

BAICA'S GENERAL EUCLIDEAN ALGORITHM (BGEA) THE ONLY ALGORITHMIC EXPLICIT SOLUTION OF HILBERT'S TENTH PROBLEM

119 128

Written by

M.BAICA

University of Wisconsin-Whitewater

Caretaken by the **PAMM-Centre**

at the

Technical University of Budapest

1782

Balaton — **BUDAPEST 2000** — *Göd*

The PAMM's periodical

BULLETINS for APPLIED & COMPUTER MATHEMATICS

(BAM)

BAM 17.. – 17.. / 2000 – XCI

Lectured at the PC-129/ 2000 - Balatonalmádi
ISSN 0133-3526

-Manuscript-

Prepared for publication at the
PAMM – Centre
Budapest, June 2000.

(BULLFEDH)

BAICA'S GENERAL EUCLIDEAN ALGORITHM (BGEA) THE ONLY ALGORITHMIC EXPLICIT SOLUTION OF HILBERT'S TENTH PROBLEM

Malvina Baica
University of Wisconsin-Whitewater U.S.A.

Abstract In this paper the author will show that her General Euclidean Algorithm (BGEA) [1,10] is the only algorithmic explicit solution of Hilbert's tenth problem.

Key words and Phrases:	**Abbreviation:**
BAICA'S ALGORITHM IN A COMPLEX FIELD	(ACF)
JACOBI-PERRON ALGORITHM	(JPA)
(ACF) ALSO NAMED BAICA'S GENERAL EUCLIDEAN ALGORITHM	(BGEA)
HASSE-BERNSTEIN ALGORITHM	(HBA)

1. Introduction.

The subject of this paper is an algorithm and its development. To develop the algorithm one starts with an initial vector and a transformation function, T. A sequence is obtained by iterating T : $\{T^1, T^2, ..., T^l, T^{l+1}, ..., T^m, T^{m+1}, ...\}$. If for index values $l < m$, $T^l = T^m$, then the algorithm of the starting vector is called periodic. Then the length of the preperiod is l and the length of the period is m. An interpretation of the Euclidean algorithm (EA) which leads to a simple continued fraction is : Let the starting vector be $a^{(0)} = (a_1^{(0)})$, $a^{(0)} \in R$, and the transformation function be the greatest integer function $[a_1^{(0)}]$. A companion vector is denoted by $b^{(0)} = [a_1^{(0)}] = (b_1^{(0)})$; then the recursive transformation $a^{(v+1)} = (a_1^{(v)} - b_1^{(v)})^{-1} = \dfrac{1}{a_1^{(v)} - b_1^{(v)}}$ applied to these vectors becomes a sequence $\{a^{(v)}\}$, $v = 0,1,...$; which is called the continued fraction interpretation of the Euclidean Algorithm (EA).

For example, by using this algorithm it is easy to prove that every rational number $\frac{a}{b}$ can be represented as a finite simple continued fraction or by a finite sequence.

In 1737, Euler proved that every real quadratic irrational can be represented by an infinite periodic simple (the numerator is 1) continued fraction or by a periodic (EA) sequence development.

In 1770, Lagrange proved the converse. If a number is a real algebraic number of higher degree then its development by the Euclidean Algorithm can not be periodic. This is called Euler –Lagrange Theorem (ELT) for quadratics and it proves the periodicity of the (EA).

Periodicity is an important property. In the quadratic case it enables us to solve Euler-Pellian Equation $x^2 - my^2 = \pm 1$ or ± 4 where m is a square free natural number. We can find the fundamental unit in the quadratic field $Q(\sqrt{m})$. The problem of finding the multiplicative group of units in any algebraic field F over the field Q of rationals was a difficult open question and it is known as Dirichlet's problem. If this problem is solved it gives a complete solution to Galois' theory of polynomials, providing the factorization of higher degree polynomials. Once the factorization is known, then we can find the solution of higher degree polynomial equations. It is the always periodicity of the (EA) which solved Dirichlet's problem completely in the quadratic fields. The dimension of the (EA) is 2 and it is given by the degree of the irrational which makes (EA) periodic by (ELT). This justifies why we do not have a formula for the solutions for higher degree polynomial equations as we have for the quadratic equations. Hilbert related the existence of the integer solutions for the Diophantine equation $x^2 + y^2 = z^2$ with the always periodicity of the (EA) using the solvability by radicals. That is, since a quadratic equation is solvable by a quadratic irrational and every quadratic irrational makes (EA) always periodic it follows that the degree $n = 2$ in $x^2 + y^2 = z^2$ is related with the dimension $n = 2$ of the (EA).

Construction with the ruler and the compass of the quadratic irrationals on the real line is possible because the (EA) is always periodic, and because of its periodicity there is an (EA) algorithmic approximation for every quadratic irrational.

No such algorithmic approximation exists for higher degree irrationals. This is the reason why Hilbert introduced a new axiom of completeness in order to prove the one to one correspondence between the real numbers and the oriented straight line.

These problems solved in quadratics from the periodicity of the (EA) remained open problems in higher dimensions.

They are :

1. General simple continued fractions algorithm known as Hermite's problem.
2. An n-dimensional equivalent of (ELT) from quadratics.
3. Dirichlet's problem.
4. The solution of Galois' theory of polynomials problem.
5. An algorithmic approximation of irrationals.
6. Fermat's last theorem problem (FLT).

2. Statement of the problem

Hilbert's goal (Zahlbericht) was to determine an universal algorithm by means of which the open questions in algebraic number theory of n-dimensions could be solved, questions which had been solved in quadratics from the always periodicity of the Euclidean Algorithm.

That is Hilbert's tenth problem. Hilbert asked for the General Euclidean Algorithm (GEA) and its proof of always (unrestricted) periodicity, developing a n-dimensional Euler - Lagrange Theorem similar to the (ELT) from quadratics. By logic, without an explicit algorithmic proof, it was proved that such an always periodic algorithm does not exist. By asking for the invention of this always periodic universal algorithm Hilbert asked for the Euler System (ES) of the algebraic number theory of the n-dimensional Euclidean geometry (E^n).

The Euclidean Algorithm (EA) is the Euler System of the algebraic number theory in quadratics and that is the algebra or number theory of 2-dimensional Euclidean geometry (E^2). Hilbert asked for the invention of the General Euclidean Algorithm (GEA) and for the proof of its always periodicity. Some attempts were made to prove Hilbert's tenth problem by polynomial representation, but this approach failed to solve all of the n-dimensional open problems in the algebraic number theory.

We will show that Baica's General Euclidean Algorithm (BGEA) is the explicit algorithmic solution of Hilbert's tenth problem.

It is the evolutionary development from the Jacobi, Perron, Hasse-Bernstein and Baica algorithms.

I give a short historical survey of efforts to solve this problem.

3. Solution of the problem

Mathematicians had almost abandoned hope of obtaining further information about the arithmetic properties of higher degree algebraic irrationals by means of a simple continued fraction or (EA) after the proof of (ELT), when JACOBI [19] generalized the (EA) for the cubic case.

In 1839, HERMITE [18] in one of his letters to Jacobi, challenged Jacobi to find an algorithm to develop irrationals of any degree into periodic sequences. Hermite was asking for the general simple periodic continued fractions algorithm. But it was only after thirty years of frustration that Jacobi in 1869 extended (EA) methods to successfully represent some cubic irrationals by means of simple continued fractions.

An application of the (JA) starts with the initial vector $a^{(0)} = (a_1^{(0)}, a_2^{(0)}) \in R^{3-1=2}$, $n = 3$, the components of which are algebraic numbers, by use of the greatest integer function a "companion vector" $b^{(0)} = (b_1^{(0)}, b_2^{(0)}) \in R^2$ with $b_i^{(0)} = [a_i^{(0)}]$, $i = 1,2$ is defined. A recursive transformation $a^{(v+1)} = (a_1^{(v)} - b_1^{(v)})^{-1} (a_2^{(v)} - b_2^{(v)}, 1)$ is constructed and applied to these vectors. Then the sequence $\{a^{(v)}\}$, $v = 0,1,2...$; is called Jacobi algorithm (JA) of $a^{(0)}$.

For good choices of the starting vector $a^{(0)}$ and for the transformation, the iteration of the transformation becomes periodic, that is the transformation cycles around a finite set of vectors . In this instance (JA) is said to be periodic, and the results lead to the (JA) periodic representation of third degree irrationals. The difficulties associated with this work are many. Jacobi's results were confined to a few numerical examples in a cubic field , where Jacobi, exhibited period developments for $\sqrt[3]{2}$, $\sqrt[3]{4}$, $\sqrt[3]{3}$, $\sqrt[3]{9}$, $\sqrt[3]{5}$, $\sqrt[3]{25}$. With all Jacobi's efforts, Euler direction in proving periodicity for the cubic case remained open .

In 1907, PERRON [20] generalized the work of Jacobi. This generalization is known as the Jacobi- Perron algorithm (JPA).

In its general form, as defined by Jacobi for $n = 3$, and by Perron $n \geq 2$, an application of the (JPA) starts with the definition of an initial vector $a^{(0)} = (a_1^{(0)}, a_2^{(0)}, \ldots, a_{n-1}^{(0)}) \in R^{n-1}$, $n \geq 2$, the components of which are algebraic numbers. By use of the greatest integer function a "companion vector" $b^{(0)} = (b_1^{(0)}, b_2^{(0)}, \ldots, b_{n-1}^{(0)}) \in R^{n-1}$, with $b_i^{(0)} = [a_i^{(0)}]$, $(i = 1,2,\ldots,n-1)$ is defined, a recursive transformation $a^{(v+1)} = (a_1^{(v)} - b_1^{(v)})^{-1} (a_2^{(v)} - b_2^{(v)}, \ldots, a_{n-1}^{(v)} - b_{n-1}^{(v)}, 1)$ is constructed and applied to these vectors. Then the sequence $\{a^{(v)}\}$, $v = 0,1,2\ldots$; is called (JPA).

Perron generalized Jacobi's methods to apply to irrationals of any degree but since the choices of starting vector and transformation are difficult to make, he was also limited to a few periodic developments of higher degree irrationals. Those results were to prove an Euler direction for higher degree irrationals.

With all Perron's efforts Euler's direction remains open, also. Perron was more successful in showing that if a development is periodic then the components of the initial vector are algebraic numbers. This latter result was general, with this proving completely Lagrange direction for higher degree irrationals.

Advances were slow and difficult and no further progress occurred until BERNSTEIN and HASSE [21] turned their attention to them.

In 1965, HASSE and BERNSTEIN [21] made a broader approach to the periodicity problem (Euler direction) associated with the (JPA). They started with an algebraic extension of the rational numbers Q(w), where w takes the form $w = \sqrt[n]{D^n + d}$ with

$P(x) = (\prod_{i=1}^{n}(x^n - D_i^n) - d)$, $d \in Z$, $D_i \in N$ and $d \mid D$.

$a^{(0)} = ((w-D_1) \cdot (w-D_2) \cdot \ldots \cdot (w-D_{n-1}), \ldots, (w-D_1) \cdot (w-D_2), (w-D_1))$ with $b^{(0)} = a^{(0)}(D_1)$.

They showed that certain significant restrictions on D and d led to a purely periodic (JPA) (that is that the length of the preperiod is zero).

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

B) For $d < 0$ the sequence is also purely periodic when $D \geq 2 \cdot (n-1) \cdot d$, $d \mid D$ and $n \geq 3$. With these conditions, the length of the period is $n \cdot (n-1)$.

From this work, periodicity remained an open question since there are bounds on D and the restriction $d \mid D$ must hold. For example no periodicity for $w = \sqrt[5]{12^5 + 6}$ can be proved under (HBA) restrictions since $12 \not\geq (5-2) \cdot 6 = 18$. The Hasse and Bernstein results were limited by their choices of w as real numbers. The closest (GEA) for real numbers is (HBA). Thus (HBA) is more than the general continued fractions algorithm. There are more n-degree irrationals which have a periodic (HBA) development than have a general periodic continued fraction development or a periodic (JPA) algorithmic development. The shortcomings of these very important results are the restriction on d and the bounds on D.

Consequently, the Euler direction in proving the periodicity of their algorithm is an open question too.

In 1980, BAICA [1] defined a modification of the (JPA) that used the Hasse and Bernstein initial vector $a^{(0)}$, but was not restricted to the real numbers. For the first time the complex (not only the real) numbers were considered. The only differences in the definitions stated alone are that the Di's are now complex numbers. An immediate consequence of these extensions is that the bounds on D in the (HBA) are now eliminated and only the divisibility condition, $d \mid D$, remains. Returning to the example cited before it can now be seen that $w = \sqrt[5]{12^5 + 6}$ has a periodic Baica Algorithmic (BA) development, since only $6 \mid 12$ is required. At that time BAICA [1] proved, that $d \mid D$ is a necessary condition to make her algorithm to be periodic and named her algorithm, the algorithm for complex numbers (ACF).

In order to have a complete proof for the periodicity of this (ACF) algorithm the sufficient condition should be proved, also.

Then (ACF) is the General Euclidean Algorithm. BAICA [10] proved that $d \mid D$ is also the sufficient condition in proving the Euler direction for the periodicity of (ACF). In doing that, then her (ACF) algorithm becomes the General Euclidean Algorithm, which is not always periodic. In 1995, BAICA [10] used the result proved by the logicians (not an explicit proof) of Hilbert's 10-th problem to prove that $d \mid D$ is also a sufficient condition in proving (ACF) restricted periodicity. By logic it was proved that Hilbert's dreamed periodic algorithm does not exist to be always periodic and to prove all the problems in the number theory from its always periodicity.

If $d \mid D$ in the periodicity of (ACF) could be eliminated then it is in contradiction with Hilbert's 10-th problem proved by the logicians, and therefore the restriction $d \mid D$ can not be eliminated in proving (ACF) periodic and as such (ACF) now is proved to be restrictiv periodic. It is true that if $d \nmid D$, then (ACF) is not periodic since otherwise it will contradict Hilbert's 10-th problem.

This completed the proof for the restricted periodicity of (ACF). Since (ACF) is of the same cut or prototype as (EA), then (ACF) is the only general Euclidean and we call it Baica's General Euclidean Algorithm (BGEA).

In (BGEA) $n = 2$ becomes (EA), $n = 3$ becomes (JA), for any $n \geq 3$ of real numbers is Perron (PA), (JPA) modification for reals is (HBA) and (HBA) extension over the complex numbers is (BGEA).

(BGEA) is a very powerful algorithm when it is periodic. In [1] – [17] the author used (BGEA) to prove up to its restricted periodicity $(d \mid D)$ all of these problems in higher dimensions which were proved in quadratics from the always periodicity of the (EA). All of these problems in higher dimensions do not have solutions when (BGEA) fails to be periodic, and (FLT) is true because (BGEA) is not always periodic for $n \geq 3$, and this proves that (BGEA) is the explicit form of Hilbert's demanded algorithm. In Hilbert's 10-th problem he asked for the General Euclidean Algorithm (GEA) which will prove from its always periodicity all the open questions in n-dimensions which were proved in quadratics from the always periodicity of the (EA). (BGEA) does this when $d \mid D$.

The (BGEA) will dominate algebraic number theory for higher dimensions (E^n) over the years to come, exactly as the Euclidean Algorithm (EA) dominated mathematics for quadratics (E^2) for so many years in the past.

It put together the work of great mathematicians during the entire history of mathematics beginning with Euclid and finishing with Baica and so much in between.

REFERENCES

[1] M. BAICA , An Algorithm in a complex field (ACF) and its applications to the calculation of units , Pacific J. Math. (1) 110 (1984) p. 21-40.

[2] M. BAICA , n – Dimensional Fibonacci Numbers and their Applications , The Fibonacci Quarterly , v. 21 , No. 4 , (1983) , p. 285-301.

[3] M. BAICA'S , Euclidean Solution of Fermat's Last Theorem - accepted for publication and will appear on July, 2000.

[4] M. BAICA , Hermite's Problem from the periodicity of (ACF) Algorithm, Bull. Numb. Theory, vol.XIV (1990) p.56-67.

[5] M. BAICA , Hilbert's demand for the disclosure of units in Algebraic Number Fields, Bull. Numb. Theory, vol.XVI (1992) p.149-163.

[6] M. BAICA , More units from the periodicity of an Algorithm , Bull. Numb. Theory, vol.XII (1988) p.81-89.

[7] M. BAICA , Halter-Koch units from the periodicity of (ACF) Algorithm, Bull. Numb. Theory, vol.XIII (1989) p.81-89.

[8] M. BAICA , Approximations of irrationals, Internat. J. Math. And Math. Sci. (2) 8 (1985) p.303-320.

[9] M. BAICA, Diophantine equations and identities, Internat. J. Math. And Math. Sci. vol.8 no.4 (1990) p.755-777.

[10] M. BAICA, Baica's General Euclidean Algorithm (BGEA) and the solutions of Fermat's Last Theorem, NNTDM 1, (1995) 3, p.120-134.

[11] M. BAICA, More explanations about Baica's proof of Fermat's Last Theorem, NNTDM 2, (1996) 1, p.15-19.

[12] M. BAICA, The Euclidean Character of the Fermat's Last Theorem, NNTDM 2, (1996) 1, p.20-23.

[13] M. BAICA, Some new combinatorial identities derived from units in Algebraic Number Fields, Discrete Mathematics 54 (1985) 133-141.

[14] M. BAICA, Pythagorean Triangles of Equal Areas, Internat. J. Math. And Math. Sci. (11) 4 (1988) p.769-780.

[15] M. BAICA, Baica's General Euclidean Algorithm Restricted Periodicity an n-Dimensional Equivalent of Euler-LaGrange Theorem from Quadratics. Scientific Bulletin of the Polytechnic University Timişoara (Math. & Physics), Romania TOM 42 (56), 2, (1997), p. 18-23 (AMS-SU.CL. 11Y40, 11A05).

[16] M. BAICA, General Euclidean Algorithm (BGEA) and Sums of Some Infinite Series. Scientific Bulletin of the Polytechnic University Timişoara (Math. & Physics), Romania TOM 43(57), 1, (1998), p.54-61

[17] M. BAICA, Some Infinite Series and Sums From (BGEA) Scientific Bulletin of the Polytechnic University Timişoara (Math. & Physics), Romania TOM 43 (57), 2, (1999), p. 8-15.

[18] C. H. HERMITE, Letter to C.G.Jacobi, J.f.d. Reine. Angew. Math 40 (1939) p.286.

[19] C.G.J. JACOBI, Allgemeine Theorie der kettenbruchaehnlichen Algorithmen, in velchen jede zahl aus drei vorhergehenden gebildet, J.f.d. Reine. Angew. Math 69 (1969) p.29-64.

[20] O. PERRON, Grundlagen fur eine Theorie des Jacobischen Kettenbruchalgorithmus, Math. Ann. 64 (1907), p.1-76.

[21] L. BERNSTEIN and H. HASSE, Einheitenberechnung mittels des Jacobi Perronschen Algorithmus, J.f.d. Reine. Angew. Math 218 (1965) p.51-69.

[22] G. FALTINGS, The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles, Notices of the AMS, V.42, No.7, (July 1995), p.743-746.