CHAPTER I - ALGORITHMS FOR REAL NUMBERS

Section 0. Introduction.

In mathematics we can construct as many geometrical models as we please. All that we need is to have the elements declared, to state the axioms and the definitions, and to have consistency in our mathematical logic. All of those geometries are not related to each other, but they all report to the topology.

Because of this, if we prove something in one geometry it may not be the same as in another geometry. Only one geometry is the Euclidean Geometry (EG), the other geometries are non-Euclidean Geometries. For example if we consider instead the V-th postulate in (EG) where two parallel lines do not intersect, the condition that they intersect at two ideal points Ω and Ω', we enter the Hyperbolic Geometry (HYG).

Since we cannot compute in a geometry, it is known that to every geometry we can associate a corresponding algebra but the converse is not true, and we call this algebra the Number Theory corresponding to that geometry. In the 1940, E. Schmidt was the first to say that since we can not compute in a geometry, to every geometry is corresponding an algebra. He is the father of the General Algebraic Geometry as F. Gauss is the father of the Algebraic Number Theory, which is the algebra of the n-dimensional Euclidean Geometry.

In every number theory there is a very strong theorem where if we implement rightly the conditions of other new theorems in the conditions of this main strong theorem, then those new theorems become immediate consequences of that initial strong theorem. This is known in the modern mathematics as the Euler System (ES) of that number theory. In other words, the (ES) in that corresponding number theory is a very powerful tool to prove many theorems in that number theory.

The basis of all results of this book is an algorithm and we shall therefore give a short historical survey of its development.

In order to develop an algorithm all we need is a starting vector and a transformation function, T. Iterating T we obtain a sequence $\{T^1,T^2,...,T^l,T^{l+1},...,T^{l+m}, T^{l+m+1},...\}$. If $T^l = T^{l+m}$, then the algorithm of the starting vector is called periodic with the length of the preperiod, or tail l, and the length of the period m

Section 1. The Euclidean Algorithm (EA).

We start with the well known and powerful Euclidean Algorithm (EA), known to Euclid more than 2000 years ago. Another interpretation of the (EA) which leads to the simple continued fractions is as follows:

Let the starting vector be $a^{(0)} = (a_1^{(0)})$, $a^{(0)} \in R$, and the transformation function which is the greatest integer function $[a_1^{(0)}]$ as a companion vector $b^{(0)} = [a_1^{(0)}] = (b_1^{(0)}) \in R$; then the recursive transformation $a^{(v+1)} = (a_1^{(v)} - b_1^{(v)})^{-1} = \frac{1}{a_1^{(v)} - b_1^{(v)}}$ applied to these vectors becomes a sequence $\{a^{(v)}\}$, $v = 0,1,...$; which is called the continued fraction interpretation of (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.

EXAMPLE 1

$$\frac{293}{41} = 7 + \frac{6}{41} = 7 + \frac{1}{\frac{41}{6}} = 7 + \frac{1}{6 + \frac{5}{6}} = 7 + \frac{1}{6 + \frac{1}{1 + \frac{1}{5}}}$$

therefore :

$$\frac{293}{41} = 7 + \frac{1}{6 + \frac{1}{1 + \frac{1}{5}}} \quad , \quad \frac{293}{41} = \{7,6,1,5\}$$

In 1737, Euler proved that every real quadratic irrational can be represented by an infinite periodic continued fraction or by a periodic (EA) sequence development. The converse was proved by Lagrange in 1770. Of course, if the number is not a quadratic irrational, but is a real algebraic number of higher degree or a transcendental real number, then its development by the (EA) cannot be periodic.

EXAMPLE 2

For $a^{(0)} = \sqrt{3}$, $b^{(0)} = 1$

$$a^{(1)} = \frac{1}{\sqrt{3}-1}\cdot\frac{\sqrt{3}+1}{\sqrt{3}+1} = \frac{\sqrt{3}+1}{2} = ; \quad b^{(1)}=1$$

$$a^{(2)} = \frac{1}{\frac{\sqrt{3}+1}{2}-1} = \frac{2}{\sqrt{3}-1}\cdot\frac{\sqrt{3}+1}{\sqrt{3}+1} = \sqrt{3}+1 \ ; \quad b^{(2)}=2$$

$$a^{(3)} = \frac{1}{\sqrt{3}+1-2} = \frac{1}{\sqrt{3}-1} = \frac{1}{\sqrt{3}-1}\cdot\frac{\sqrt{3}+1}{\sqrt{3}+1} = \frac{\sqrt{3}+1}{2} = a^{(1)}$$

$$\sqrt{3} = \left[b^{(0)}, \overline{b^{(1)}\, b^{(2)}}\right] = \left[1, \overline{1, 2}\right].$$

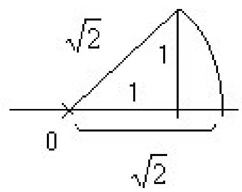
This theorem is called Euler –Lagrange Theorem (ELT) for quadratics and it proves the always periodicity of the (EA). Periodicity is a very important property. For instance, in the quadratic case it enables us to solve the incorrectly named Pellian Equation (it is an Euler Ecuation) $x^2 - my^2 = \pm 1$ or ± 4 where m is a square free natural number, and to find the fundamental unit in the quadratic field $Q(\sqrt{m})$. As it is known, the problem of finding the multiplicative group of units in any algebraic field F over the field Q of rationals (or relative to an algebraic field A over Q) was a difficult open question and it is known as Dirichlet's problem. This is to find the Galois' multiplicative group of fundamental units in any algebraic number field. If Dirichlet's 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 solutions 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.

EXAMPLE 3



1.4141 …

$\sqrt{2}$

1

100   2 [4]. 4

96

400   2 8 [1]. 1

281

11900   2 8 2 [4]. 4

11296

60400   5 6 4 8 [1]. 1

56481

391900   M

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

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

Section 2. Jacobi Algorithm (JA).

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), when Jacobi [VI] generalized the Euclidean Algorithm for the cubic case.

In 1839, Hermite [V], 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 $a^{(0)} = (a_1^{(0)}, a_2^{(0)}) \in R^2$, $n = 3$, 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 $\{a^{(v)}\}$, $v = 0,1,2\ldots;$ is called Jacobi algorithm (JA) of $a^{(0)}$.

EXAMPLE 1

$$a^{(0)} = (a_1^{(0)}, a_2^{(0)}) = (\sqrt[3]{2}, \sqrt[3]{4}) \qquad b^{(0)} = (b_1^{(0)}, b_2^{(0)}) = (1,1)$$

$$a^{(1)} = (\sqrt[3]{2} - 1)^{-1} (\sqrt[3]{4} - 1, 1)$$

$$a^{(1)} = \left(\frac{\sqrt[3]{4} - 1}{\sqrt[3]{2} - 1}, \frac{1}{\sqrt[3]{2} - 1} \right) = (a_1^{(1)}, a_2^{(1)})$$

$$a_1^{(1)} = \frac{(\sqrt[3]{4} - 1) \cdot (\sqrt[3]{4} + \sqrt[3]{2} + 1)}{(\sqrt[3]{2} - 1) \cdot (\sqrt[3]{4} + \sqrt[3]{2} + 1)} = \frac{2\sqrt[3]{2} - \sqrt[3]{4} + 2 - \sqrt[3]{2} + \sqrt[3]{4} - 1}{2 - 1} = \sqrt[3]{2} + 1$$

$$a_2^{(1)} = \frac{1 \cdot (\sqrt[3]{4} + \sqrt[3]{2} + 1)}{(\sqrt[3]{2} - 1) \cdot (\sqrt[3]{4} + \sqrt[3]{2} + 1)} = \frac{\sqrt[3]{4} + \sqrt[3]{2} + 1}{2 - 1} = \sqrt[3]{4} + \sqrt[3]{2} + 1$$

$$a^{(1)} = (\sqrt[3]{2} + 1, \sqrt[3]{4} + \sqrt[3]{2} + 1) \qquad b^{(1)} = (2,3)$$

$$a^{(2)} = \left(\frac{\sqrt[3]{4} + \sqrt[3]{2} + 1 - 3}{\sqrt[3]{2} - 1}, \frac{1}{\sqrt[3]{2} - 1} \right) = (a_1^{(2)}, a_2^{(2)})$$

$$a_1^{(2)} = \frac{(\sqrt[3]{4} + \sqrt[3]{2} - 2) \cdot (\sqrt[3]{4} + \sqrt[3]{2} + 1)}{(\sqrt[3]{2} - 1) \cdot (\sqrt[3]{4} + \sqrt[3]{2} + 1)} = \sqrt[3]{2} + 2$$

$$a_2^{(2)} = \frac{1 \cdot (\sqrt[3]{4} + \sqrt[3]{2} + 1)}{(\sqrt[3]{2} - 1) \cdot (\sqrt[3]{4} + \sqrt[3]{2} + 1)} = \frac{\sqrt[3]{4} + \sqrt[3]{2} + 1}{2 - 1}$$

$$a^{(2)} = (\sqrt[3]{2} + 2, \sqrt[3]{4} + \sqrt[3]{2} + 1) \qquad b^{(2)} = (3,3)$$

$$a^{(3)} = \left(\frac{\sqrt[3]{4}+\sqrt[3]{2}+1-3}{\sqrt[3]{2}+2-3}, \frac{1}{\sqrt[3]{2}-1} \right) = (a_1^{(3)}, a_2^{(3)})$$

$$a_1^{(3)} = \frac{\left(\sqrt[3]{4}+\sqrt[3]{2}-2\right)\cdot\left(\sqrt[3]{4}+\sqrt[3]{2}+1\right)}{\left(\sqrt[3]{2}-1\right)\cdot\left(\sqrt[3]{4}+\sqrt[3]{2}+1\right)} = \sqrt[3]{2}+2 = a_1^{(2)}$$

$$a_2^{(3)} = \frac{1\cdot\left(\sqrt[3]{4}+\sqrt[3]{2}+1\right)}{\left(\sqrt[3]{2}-1\right)\cdot\left(\sqrt[3]{4}+\sqrt[3]{2}+1\right)} = \frac{\sqrt[3]{4}+\sqrt[3]{2}+1}{2-1} = a_2^{(2)}$$

$$a^{(3)} = \left(\sqrt[3]{2}+2, \sqrt[3]{4}+\sqrt[3]{2}+1\right) = a^{(2)}, \quad b^{(3)} = (3,3) = b^{(2)}$$

(JA) of $\sqrt[3]{2}$ and $\sqrt[3]{4}$ is periodic and (JA) of $\{\sqrt[3]{2}, \sqrt[3]{4}\} = \{(1,1), (2,3), \overline{(3,3)}\}$ or $\sqrt[3]{2} = \{1, 2, \overline{3}\}$ and $\sqrt[3]{4} = \{1, \overline{3}\}$.

For good choices of the starting vector $a^{(0)}$ and transformation $b^{(0)}$, 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 periodic developments for $\sqrt[3]{2}$, $\sqrt[3]{4}$, $\sqrt[3]{3}$, $\sqrt[3]{9}$, $\sqrt[3]{5}$, $\sqrt[3]{25}$. Those results were to prove Euler direction for cubic irrationals. This problem is known as Hermite's problem for higher degree irrationals. In spite of all Jacobi's efforts Herm ite's problem remains unsolved

Section 3. Perron Algorithm (PA).

In 1907, Perron [VII] 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 for n ≥ 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 ≥ 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,…,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 $\{a^{(v)}\}$, $v = 0,1,2..$; 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, also. With all Perron's efforts Euler's direction in proving Hermite's problem remains o pen.

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, but in 1873 Bachman [I] proved results for other cubic irrationals using the (JPA); results that were accompanied by many restrictions.

With this work on Hermite's problem progress come to a halt, because of the failure of the (JPA) to produce new numerical results, that is, additional cases in which the transformation becomes periodic were not achieved. Perron and all others recognised that the usual choices for starting vector were too limited. No further progress occurred on these problems until Hasse and Bernstein [II] turned their attention to them.

Section 4. Hasse and Bernstein Algorithm (HBA).

In 1965, Hasse and Bernstein made a broader approach to the periodicity problem associated with the (JPA). Hasse and Bernstein 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 $d \mid D$.

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

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

1) For $d > 0$ they proved that that (JPA) of $a^{(0)}$ is purely periodic when

$$D \geq (n-2) \cdot d,\ d \mid D \text{ and } n \geq 3, \text{ and}$$

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

With these conditions, the length of the period is $n\ (n-1)$. For this approach the periodicity remains an open problem 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 $12 \geq (5\text{-}2) \cdot 6 = 18$.

The Hasse and Bernstein results were limited by their choices of w as real numbers. It should be known that Hasse and Bernstein were not interested in Hermite's problem in spite of the fact that their results had a strong relation to that problem. Specially, they did not realize that the periodicity of their algorithm leads to a solution of Hermite's problem for some real algebraic number w, when (HBA) becomes the general continued fractions algorithm. There are more n-degree irrationals which have periodic (HBA) algorithmic development than they have a general periodic continued fraction development or a periodic (JPA) algorithmic development. Hasse and Bernstein were interested in solving Dirichlet's problem to find units in algebraic number fields or Galois' group of units from the periodicity of their algorithm. From these results they proved that in both cases (1) and (2)

$$e_k = \frac{w^k - D^k}{(w - D)^k}, \quad k \mid n, \quad k > 1$$ are the $\hat{\alpha}(n) - 1$ units in the corresponding fields $Q(w)$, $w = \sqrt[n]{D^n + d}$, $d \mid D$, $D \in N$, $d \in Z$, $n \geq 3$.

The shortcomings of these very important results are the restriction on d and the bounds on D. As of this result the Euler direction in proving the periodicity of their algorithm is an open question too.