On the Brahmagupta-Fermat-Pell Equation: The Chakravāla or Cyclic algorithm revisited

Pronob Mitter

-

On the Brahmagupta- Fermat-Pell Equation:

The Chakravāla or Cyclic algorithm revisited

Laboratoire Charles Coulomb
CNRS-Université Montpellier- UMR5221
Place E. Bataillon, Case 070, 34095 Montpellier Cedex 05 France

e-mail: Pronob.Mitter@umontpellier.fr

Abstract

In the following pages we take a fresh look at the ancient Indian *Chakravāla* or *Cyclic* algorithm for solving the Brahmagupta-Fermat-Pell quadratic Diophantine equation in integers taking account of recent developments. This is the oldest general algorithm (1150 CE) for solving this equation. The algorithm can be proved directly in its own terms, following a recent work by A. Bauval, to always lead to a periodic solution in a finite number of steps. We review a slightly modified version of this work. It forms the basis of a re-interpretation of this algorithm in the framework of a reduction theory of binary indefinite integer valued quadratic forms on which the modular group $SL(2,\mathbb{Z})$ acts. The reduction condition of this algorithm are restated in terms of the roots of the quadratic form. The $SL(2,\mathbb{Z})$ action on (reduced) roots of this form furnish semi-regular continued fractions which are periodic and which furnish $SL(2,\mathbb{Z})$ automorphisms of the quadratic form. Very much as in the classical theory of Gauss, this gives solutions of the Brahmagupta-Fermat-Pell equation. We give a proof that the solution at the end of the first cycle is fundamental (positive and least). We also give the conversion to regular continued fractions which involve larger periods. A number of worked out examples are given to illustrate the main points and this for the benefit of the uninitiated reader.

1. Introduction

The present work is concerned with integer solutions of the Brahmagupta-Fermat-Pell equation. This is the well known quadratic Diophantine equation:

$$y^2 - Dx^2 = 1 \tag{1.1}$$

where $D > 0$ is a positive non-square integer. By a non-square integer we always mean an integer which is not a perfect square.

As an associated problem we have

$$y^2 - Dx^2 = m \tag{1.2}$$

where m is any integer, positive or negative. We are interested in solving (1.1) in integers. But other cases (1.2) arise in intermediate steps of the *Chakravāla* or Cyclic algorithm for solving (1.1) which is the subject of this work. We are interested in positive integer solutions.

This equation has a long history, (Weil [W] Chapter 1). It has come to be known as the "Pell equation" due to an erroneous attribution of Euler (see e.g. the MacTutor article [MT] which gives an account of the history). This error has however propagated through history. *Integer solutions* of this equation were in fact studied systematically in some particular cases (see later) by the Indian mathematician Brahmagupta (circa 628 CE). *Bhāskarachārya* (commonly referred to as *Bhāskara* II) (1150 CE) gave an algorithm (the so-called *Chakravāla* or Cyclic algorithm) in 1150 CE to solve this equation in the general case. However this algorithm is said to be older and has been attributed to Jayadeva (mid 11th century CE) in [KS]. In any event it is the version of *Bhāskara* II which is known explicitly (Datta and Singh, [DS Part 2]) and to which we will refer. As recounted by Weil in [W], five hundred years later Fermat (1657 CE), who was unaware of the earlier work of Brahmagupta and *Bhāskara* II, proposed the study of integer solutions of this equation. It is thus proper to call this the Brahmagupta-Fermat-Pell equation.

We give further details of some of the historical work, which might not be known to all. Brahmagupta obtained integer solutions of (1.1) for some particular cases, e.g. $D = 83, 92$, exploiting a composition law known as Brahmagupta's identity. The Diophantus identity (see [W]) is the particular case $D = -1$ of Brahmagupta's identity which is algebraic and thus true for arbitrary D. The composition law generates new solutions (in fact an infinite number) given a particular one. Furthermore, exploiting his composition law, he showed that integer solutions of (1.2) for $m = -1, \pm 2, \pm 4$ implied the solution of (1.1), $m = 1$. This is reviewed in [DS], Part 2. The algebraic identity of Brahmagupta was rediscovered later by Euler. *Bhāskaracharya* (*Bhāskara II*) (c.1150 CE) exploited Brahmagupta's composition law to devise the Cyclic or *Chakravāla* algorithm, for solving this equation in the general case. *Bhāskara II* solved many difficult cases (D=61, 67 etc) using the Cyclic algorithm. *Nārāyana* (circa 1340- 1400 CE) solved the cases $D = 97, 103$ using the same algorithm. These solutions are reviewed in [DS], Part 2. This algorithm is the subject of this work.

Fermat in 1657 CE issued a challenge to English mathematicians to obtain integer solution of this equation for the case D=61, not knowing the earlier solution given by *Bhāskara II*. In response, the English mathematician Viscount Brouncker solved the case $D = 61$ as well as other cases. See Weil [W] for Brouncker's method. Euler, starting

1730 CE, solved particular cases of this equation using the continued fraction for $\sqrt{D}$ and noticed the periodicity of the continued fraction. Later Lagrange took up Euler's continued fraction method and proved the existence of periodic solutions after a finite number of steps. All of this is recounted by Weil in [W]. For the Indian work see [W, pages 14-24] and [DS, Part 2]. The Indian algorithm was known to work for all the cases that had been tried. But a proof, in its own terms, that the algorithm would always work in a finite number of steps was missing. This would come later.

So matters stood until in 1929-30 Ayyangar, [A1], in a pioneering work, took up the analysis of the *Chakravāla* algorithm in terms of the evolution of particular indefinite (integer valued) binary quadratic forms (which he called *Bhāskara* reduced forms). However, Ayyangar's proof of the finiteness and periodicity of the *Chakravāla* algorithm is marred by some lacunae, as was noted by Bauval [B][1]. This has since then been corrected, and, as an improvement of Ayyangar's earlier work, a new proof of the finiteness and periodicity of this algorithm has been produced by Bauval in [B]. A version of the results in [B] is given later.

Ayyangar [A2], in 1940-42, developed a type of semi-regular continued fractions (Nearest Square Continued Fractions), noted NSCF. According to Ayyangar the NSCF was the natural sequel to Bhāskara's cyclic method. However the connection of his NSCF with the *Chakravāla* algorithm is unclear as was pointed out by Selenius ([Se] and [Se1, Se2]). The semi-regular continued fractions of [A2] and those *derived* directly from the Chakravāla algorithm (see Section 5) are not always the same. As mentionned earlier, in the Chakravāla algorithm a successor step is not always unique (see later). This produces sequences which split and join up locally with, however, the same common fundamental solution of the Brahmagupta-Fermat-Pell equation. This will be seen in Sections 3 and then in Section 5, where the semi-regular continued fractions (SRCF) are derived. The case $D = 29$ was pointed out in [B]. The cases $D = 97,\ 58$ are further examples of this phenomenon. One now has only to compare this with Ayyangar's NSCF sequences for the same cases as they appear in [A2] and where this non-uniqueness does not appear to occur. Thus it appears that the NSCF continued fractions do not always coincide with the SRCF *derived* from

[1] In particular a successor step in the algorithm is not always unique. This and some other technical gaps are pointed out in the various footnotes of [B].

the Chakravāla algorithm. They do so only when the successor step is unique. [2]

These notes are organized as follows:

In section 2, we recall briefly Brahmagupta's composition law (identities) and some of his solutions. Moreover we prove by iteration that if there is one positive integer solution, then there is an infinite number of them. This was stated by Brahmagupta himself. We show in a now standard way that they provide units of a quadratic ring and that, if all the units have been obtained, there is a fundamental unit (the smallest solution).

In section 3, we give a version of the *Chakravāla* or Cyclic algorithm. In particular the algorithm is designed to solve (1.1) whereas (1.2) plays an auxiliary role in intermediate stages of the algorithm. *The integer m in (1.2) is thus allowed to be positive or negative.* This therefore differs from the version in [B] where the equation to be solved has an absolute value taken. This does not distinguish between $m = +1$ and $m = -1$, and m called k in [B] is always positive. It is useful for various reasons to separate the two cases which are very different. The positive equation ($m = 1$) is always solvable when D is a positive non-square integer, and the solutions are periodic with even period and infinite in number. The solvability of the negative equation ($m = -1$) is a harder problem. If we have a solution for $m = -1$, then a second iteration (see later) using the Brahmagupta composition produces a solution for $m = 1$. However to obtain solutions for the case $m = -1$ additional conditions have to be imposed on D.[3]

[2] Selenius in [Se1, Se2]] develops what he calls the ideal half-regular continued fraction (ideal SRCF) as a counterpart of the $Chakravāla$ algorithm. The following issue arises: For $D = 58$ on page 31 of [S2], Selenius transforms a regular (RCF) to a semi-regular continued fraction for $\sqrt{58}$ (by a singularization process which is opposite to that of Perron's transformation of a SRCF to an RCF). However he obtains only one of the two possible SRCF. We can compare this with those derived from the $Chakravāla$ algorithm in Section 5 of this paper. See example 5 in section 5 for the case $D = 58$ where the the semi-regular (SRCF) and regular continued fractions (RCF) are given. The two split SRCF sequences (ν_+ and ν_- cycles) give the same RCF by the Perron tranformation. This RCF coincides with that of Selenius. It appears that the possibility of non-uniqueness in the $Chakravāla$ algorithm and the SRCFs engendered therefrom is absent in the considerations of Selenius. For further work on the NSCF of Ayyangar see [MRW], [MR].

[3] There is a well known result, see e.g ([S1],theorem 5.1), that the equation for $m = -1$ has no solution if D is divisible by a prime $p \equiv 3 \pmod 4$. Moreover, it is well known (see e.g. Stark ([S1], theorem 7.26)) that the equation for $m = -1$ is solvable if the continued fraction expansion of $\sqrt{D}$ has a period length that is odd. It was shown by Legendre in [Le] and Dirichlet in [D, §83, page 141, footnote 71] that $D \equiv 1 \pmod 4$ is a necessary condition for solvability of the $m = -1$. More recently it has been shown by Mollin and Srinivasan ([MS]) that a necessary and sufficient condition for the solvability of the negative equation is that $D \equiv 1 (\mathrm{mod}\ 4)$ together with $y_0 \equiv -1 (\mathrm{mod}\ 2D)$ where y_0, x_0 is the fundamental solution of the $m = 1$ equation (1.1), $y^2 - Dx^2 = 1$, with D as above. Illustrative examples for this result are the cases $D = 61, 29, 97, 13, 41$, see e.g. examples $2, 3, 4, 6, 7$ of Section 5 where the fundamental solutions of the

Another reason is that for the derivation of continued fractions from the algorithm we have to distinguish the two cases.[4] Hereafter we consider only the $m = 1$ case ((1.1) to be solved, and, as mentioned earlier, (1.2) where positive and negative values of m occur plays an auxiliary role in the algorithm in intermediate stages. However the principal results of Bauval, namely her Proposition 1 and Theorem 2 (Main Theorem) in [B], remain valid after some trivial changes.

It will be useful to summarise briefly some features of the algorithm as it figures in Sections 3, 4 and 5. In Weil's notation, [W], a solution of equation (1.2) at a given stage n of the algorithm

$$Da_n^2 + m_n = b_n^2$$

can be represented as $(a_n, b_n; m_n)$. The integers in this triple are relatively prime. The algorithm (Section 3) introduces another positive integer ν_n chosen to fullfil two conditions: (1) $\nu_n \equiv -\nu_{n-1} \pmod{m_n}$ and amongst such ν_n, (2) ν_n is then chosen so as to make $|\nu_n^2 - D|$ least in the congruence class (mod m_n). To start the algorithm, we take $\nu_0 = 0, a_0 = 0, b_0 = 1, m_0 = 1$. The algorithm then gives $(a_{n+1}, b_{n+1}; m_{n+1})$ as well as the integer ν_{n+1}. In particular m_{n+1} is given by $m_{n+1}m_n = \nu_n^2 - D$. In fact it is enough to to record the evolution of the triple (m_n, ν_n, m_{n+1}) (as noted in [A1]) to prove the finiteness and periodicity of the algorithm.

The condition (2) above on ν_n, viz that $|\nu_n^2 - D|$ is least in the congruence class (mod m_n) does *not* imply that the choice of ν_n is unique. This is behind the phenomenon of *twin successors* and sequences as first pointed out in [B]. This produces sequences which split and then join up (locally) with, however, the same common fundamental solution of the Brahmagupta-Fermat-Pell equation. Explicit examples show this and these will be found in Section 3. In particular, as mentioned earlier, the cases $D = 29$, 97, 58 exhibit twin successors and are worked out in detail. The other examples which are worked out are for $D = 61$, 67 (unique successors) with solutions due to *Bhāskarachaya* himself, and in section 5 the additional cases $D = 13$, 41 to illustrate the occurence of short periods in continued fractions. The phenomenon of twin successors and sequences have their counterparts in the semi-regular continued fractions which are derived from the algorithm in Section 5.

Section 4 is devoted to results which were obtained in [B]. We adopt the terminology in [B] and call (m_n, ν_n, m_{n+1}) a *step* if it satisfies the conditions (1) and (2) given above. Proposition 4.3 gives equivalent characterisations of a step. A step (m_n, ν_n, m_{n+1}) is *reduced* if the reverse triple (m_{n+1}, ν_n, m_n) is also a step. Thus $|\nu_n^2 - D|$ is least both in the congruence class (mod m_n) and the congruence class (mod m_{n+1}). Theorem 4.6

positive equation are given and the premises of the theorem of [MS] can be verified.

[4] This is very much as in the case of the reduction theory of Gauss (see Dirichlet [D, Chapter 4]).

shows that the successor of every step is reduced. The first step is seen to be reduced and therefore every step of the algorithm is reduced. This leads to Theorem 4.8 which proves that the number of steps is finite and produces a cycle. Proposition 4.3 and Theorem 4.6 closely follow results obtained in [B, Proposition 1, Theorem 2]. In Appendices 1 and 2 detailed proofs are given of Proposition 4.3 and Theorem 4.6. These are amplified versions of the proofs given in [B, Proposition 1 and Theorem 2]. Given the brevity of the proofs in [B] we hope this will be useful.

In Section 5, we adopt some of the considerations in Gauss [DA] and Dirichlet [D], Chapter 4, but now in the framework of the analysis of the *Chakravāla* algorithm in Section 4. After the work of Fermat (see [W]), Lagrange ([L], see [W]), Legendre ([Le], see [W]) and Gauss ([G-DA], see [D]) were the first to consider binary quadratic form representation of integers. Lagrange introduced the notion of equivalent forms under $GL(2,\mathbb{Z})$ transformations, and a reduction theory of quadratic forms which is efficient for the positive definite case and leads to easy proofs of the various Fermat theorems on the sums of squares. This culminated in the great work of Gauss ([G-DA]) who, in particular, gave a complete theory of reduction for indefinite binary quadratic forms and this leads to the solution of (1.1). Gauss's work is covered in the Dirichlet lectures [D], edited and supplemented by Dedekind, and this constitutes our principal reference. The modular group $SL(2,\mathbb{Z})$ (whose elements Gauss called *proper substitutions*) plays an important role in Gauss's theory and this will be the case in our context.

We consider the step (m,ν,m') as an indefinite binary quadratic form with integer coefficients (in the notation of Gauss)

$$Q(x,y) = mx^2 + 2\nu xy + m'y^2$$

where ν is chosen so that $|\nu^2 - D|$ is least in the congruence class (mod m) (see section 4). The discriminant of this form is $\Delta(Q) = 4(\nu^2 - mm') = 4D$ where we take $D > 0$, non-square and fixed. Forms with the above property for the middle coefficent may be called *best* forms (mod m). Such forms are steps (in the sense of Section 4) and they are reduced and are thus also best (mod m'). Note that the determinant of this form is $\det Q = mm' - \nu^2 = -D$ and thus the form is indefinite.

The condition that ν is best (mod m) can be restated in terms of the roots of the quadratic form $Q(\omega,1)$

$$Q(\omega,1) = m\omega^2 + 2\nu\omega + m' = 0$$

The *principal* root is

$$\omega_+ = \frac{-\nu + \sqrt{D}}{m}$$

and its conjugate is

$$\omega_- = \frac{-\nu - \sqrt{D}}{m}$$

Proposition 5.1 states that the necessary and sufficient condition that ν is best (mod m) is

$$|\omega_+| < 1$$

provided $|m| < \sqrt{D}$. Thus ω_+ is a proper fraction. It can be shown (see Remark 5.3) that the other root ω_- satisfies $|\omega_-| > 1$. These two conditions figure in the reduction theory of Gauss, where in addition there is a third condition, namely that the roots have opposite signs (see [D], §74).

From Theorem 4.6 and Corollary 4.7 the step (m, ν, m') is reduced (reduced form) and thus (m', ν, m) is also a step (reduced form). Hence ν is best both (mod m) and (mod m'). Moreover $|m'| < \sqrt{D}$. We will refer to (m', ν, m) as the *reversed* step.

The quadratic form corresponding to the reversed step is the reversed form

$$Q^{(r)}(x, y) = m'x^2 + 2\nu xy + my^2$$

whose principal root is

$$\omega_+^{(r)} = \frac{-\nu + \sqrt{D}}{m'}$$

and since ν is best (mod m'), and $|m'| < \sqrt{D}$, we have by Proposition 5.1

$$|\omega_+^{(r)}| < 1$$

The modular group $SL(2, \mathbb{Z})$ acts on quadratic forms by acting on the form matrix (Section 5 and [D], §54, §63). There is a modular transformation S_δ (see equation (5.16) below) which maps a step (considered as a reduced form) to the successor form

$$S_\delta : (m, \nu, m') \to (m', \nu', m'')$$

where $\nu + \nu' = -\delta m'$ and δ is an integer. Thus $\nu' \equiv -\nu$ (mod m'). For the successor form (m', ν', m'') to be a step (reduced form) we must have $|\omega'_+| < 1$. Here ω'_+ is the principal root of the quadratic form (m', ν', m''). This fixes δ but *not* uniquely. There can be twin successors as explained earlier. This is the content of Theorem 5.4. It is shown in Section 5 that the cyclic algorithm then arises naturally. The modular group $SL(2, \mathbb{Z})$ acts naturally on roots of forms (Section 5 and [D], §73) and thus on roots of steps which are reduced forms. The action of the transformation S_δ on principal roots is given in section 5. Its

iteration leads to semi-regular continued fractions (SRCF) which are convergent (Proposition 5.5, Lemma 5.6 and Proposition 5.7) and are periodic. The $SL(2,\mathbb{Z})$ automorphisms of the quadratic form constitute a subgroup (its elements are called *automorphs*) which act on the roots. As shown in [D, §62] there is a $1-1$ correspondence between the elements of this subgroup and solutions of the Brahmagupta-Fermat-Pell equation. The periodicity of the SRCF (together with symmetry properties of Lemma 5.11) provide us with such automorphs and thus all solutions of the Brahmagupta-Fermat-Pell equation. The solutions obtained at the end of the first cycle are fundamental: positive and least. This is shown in Section 5 (see Proposition 5.12) Although not strictly necessary, we nevertheless give for comparison the transformation to regular continued fractions (RCF) together with the (same) fundamental solutions. This involves cycles with longer period lengths. However for the RCF the non-uniqueness of successors disappears. We give a number of examples. Appendix 3 contains the proof of Lemma 5.6, and in Appendix 4 we give a proof of Lemma 5.11 which gives a generalisation to the SRCF of the Galois inverse period theorem and its symmetry consequences, needed earlier.

Remark 1.1. The history of this equation can be found in the book by André Weil, [W]. The work in number theory of the early Indian mathematicians and astronomers (Aryabhata, Brahmagupta, Bhaskara II (Bhaskaracharya) and others) and then the later European contributions (Fermat, Brouncker, Euler, Lagrange, and Legendre) is recounted in this book. For Gauss's theory (not covered in [W]) see the beautiful Dirichlet lectures [D], posthumously edited and supplemented by Dedekind.

Remark 1.2. A basic text which gives an account of the Indian work (500 CE- 1400 CE) with translations of the relevant passages from the Sanskrit is Datta and Singh: [DS].

Remark 1.3 A brief historic account of work related to this equation can be found in [MT].

Remark 1.4. I bring to the reader's attention two interesting books on the history of Indian Mathematics by Divakaran [Di] and Plofker [Pl]. I have profited from them.

Acknowledgements: I wish to thank P. P. Divakaran for stimulating my interest in this subject. This has led to the present study. I thank Erhard Seiler for his continuing interest as well as for his efforts towards procuring for me some works of Selenius ([Se1] and [Se2]) which are not easily available. I am grateful to Sergey Alexandrov and Jean-Bernard Zuber for reading these notes and for their pertinent questions and comments.

2. Brahmagupta's composition law and applications

Let D be a positive, non-square integer. Let m be an integer. Througout the following the triple $(x, y; m)$ will denote an integer solution of

$$Dx^2 + m = y^2 \tag{2.1}$$

Proposition 1.1: The Brahmagupta Composition law (628 CE)

Let $(x_j, y_j; m_j)$ be two such triples. There exists a composition

$$(x_1, y_1; m_1) \bullet (x_2, y_2; m_3) = (x_3, y_3; m_3) \tag{2.2}$$

such that

$$\begin{aligned} x_3 &= x_1 y_2 + x_2 y_1 \\ y_3 &= D x_1 x_2 + y_1 y_2 \\ m_3 &= m_1 m_2 \end{aligned} \tag{2.3}$$

Proof : For $j = 1, 2$ we write

$$y_j^2 - D x_j^2 = (y_j + \sqrt{D} x_j)(y_j - \sqrt{D} x_j)$$

We have

$$(y_1 + \sqrt{D} x_1)(y_2 + \sqrt{D} x_2) = (y_1 y_2 + D x_1 x_2) + \sqrt{D}(x_1 y_2 + x_2 y_1)$$

Similarly

$$(y_1 - \sqrt{D} x_1)(y_2 - \sqrt{D} x_2) = (y_1 y_2 + D x_1 x_2) - \sqrt{D}(x_1 y_2 + x_2 y_1)$$

Multiplying out the last two equations gives

$$m_1 m_2 = (y_1^2 - D x_1^2)(y_2^2 - D x_2^2) = (D x_1 x_2 + y_1 y_2)^2 - D(x_1 y_2 + x_2 y_1)^2 \tag{2.4}$$

■

Remark :The last equation is an algebraic identitity: Brahmagupta's identity. Since this is an algebraic identity, D can be arbitrary. Choosing e.g. $D = -1$ we get Diophantus's identity.

Proposition 1.2: (after Brahmagupta):

If the equation

$$D x^2 + 1 = y^2 \tag{2.5}$$

where D is a nonsquare, positive integer, has one positive integer solution (x_1, y_1) , then it has infinitely many positive solutions (x_n, y_n), for all integers $n \geq 1$. The (x_n, y_n) are generated by the formula

$$y_n + x_n\sqrt{D} = (y_1 + x_1\sqrt{D})^n$$

Proof: The proof is by iteration of the composition law of Proposition 1.1 applied to the integer triple $(x, y; 1)$. Define the quadratic ring

$$\mathbb{Z}(\sqrt{D}) = \{\eta = y + \sqrt{D}x : \ y, x \in \mathbb{Z}\}$$

The ring has a norm $\mathcal{N}(\eta)$ defined by

$$\mathcal{N}(\eta) = \eta\bar{\eta} = (y + \sqrt{D}x)(y - \sqrt{D}x) = y^2 - Dx^2$$

Thus the integer triple $(x, y; 1)$ corresponds to a unit of the ring: $\mathcal{N}(\eta) = 1$.

More generally we obtain an infinite number of solutions $(x_n, y_n; 1)$, as follows: Let $n \geq 1$.

$$\eta_n = y_n + \sqrt{D}x_n = (y_1 + \sqrt{D}x_1)^n = \eta_1^n$$

where $\eta_1 = y_1 + \sqrt{D}x_1$ is a unit. Then its norm is

$$\mathcal{N}(\eta_n) = \eta_n\bar{\eta}_n = (\eta_1\bar{\eta}_1)^n = 1$$

and thus $(x_n, y_n; 1)$ are solutions. If $(x_1, y_1; 1)$ is a positive solutions then all $(x_n, y_n; 1)$ are positive solutions. Thus Proposition 1.2 implies that there are an infinite number of positive solutions. Of the solution set $\{(x_n, y_n; 1)\}$ one of them is the smallest because the solutions grow with increasing integer values of x (equivalently y) as is easy to show. ∎

Suppose now we have found *all* the positive solutions. Then, by the above argument, one of them is the smallest labelled $(x_D, y_D; 1)$. This is the *fundamental solution* and $\eta_D = y_D + x_D\sqrt{D}$ is the the fundamental unit. All other units are generated by the formula η_D^n, for all $n \geq 1$ as the next proposition shows.

Ordering units: Recall that a unit of a quadratic ring is an element $\eta = y + x\sqrt{D}$ where y, x are integers and $\eta\bar{\eta} = 1$. Here $\bar{\eta}$ is the conjugate $\bar{\eta} = y - x\sqrt{D}$. We can order the units by ordering the integers y or equivalently the integers x since $\eta\bar{\eta} = 1$ implies $y^2 = Dx^2 + 1$. Thus we can say that the fundamental unit η_D is the smallest unit.

Proposition 1.3 (after Dirichlet) : All units are generated from the fundamental unit η_D by the formula η_D^n, for all $n \geq 1$ and there are no others.

Proof: That η_D^n are units follows from Proposition1.2, $\eta_D^n\bar{\eta_D}^n = (\eta_D\bar{\eta}_D)^n = 1$. We now prove that there are no others. The following argument is borrowed in essence from [D, §85]. Suppose $\eta = t + u\sqrt{D}$ is a unit not in the list η_D^n, all $n \geq 1$. Then for some n,

$$\eta_D^n < \eta < \eta_D^{n+1}$$

Set $\eta' = \eta\bar{\eta_D}^n$. Plainly, η' is a unit, since $\eta'\bar{\eta}' = (\eta\bar{\eta})(\bar{\eta}_D^n\eta_D^n) = 1$.
Then

$$\bar{\eta_D}^n\eta_D^n < \eta\bar{\eta_D}^n < \bar{\eta_D}^n\eta_D^n\eta_D$$

or

$$1 < \eta' < \eta_D$$

which contradicts the assumption that η_D is a fundamental unit. ∎

Remark: The *Chakravāla* algorithm (see later), like those of Lagrange and Gauss, solves the equation for all positive, non-square D and gives all the positive periodic solutions. At the end of the first period the algorithm gives the fundamental solution (x_D, y_D). That this is so is shown in section 5, Proposition 5.12. The formula

$$y_n + x_n\sqrt{D} = (y_D + x_D\sqrt{D})^n$$

then generates all the solutions and there are no others as proved in Propositions 1.2 and 1.3. The fundamental solution is unique: the *Chakravāla*, Lagrange and Gauss algorithms give the same fundamental solution, as follows from Proposition 1.3.

For completeness, we now give two elementary applications of the composition law, both due to Brahmagupta. These are borrowed from [DS, Part 2].

Example 1 : Solve in integers

$$83x^2 + 1 = y^2 \tag{2.6}$$

Solution : Notice that the triple $(x = 1, y = 9; m = -2)$ is a solution to

$$83x^2 - 2 = y^2 \tag{2.7}$$

Composing this triple with itself gives

$$(1, 9; -2) \bullet (1, 9; -2)) = (18, 164; 4) = (x', y'; m')$$

which is a solution to

$$83x'^2 + 4 = y'^2$$

Dividing out by 4 gives

$$83(\frac{x'}{2})^2 + 1 = (\frac{y'}{2})^2$$

Thus the triple $(9, 82; 1)$ is an integer solution to (2.6). ∎

Example 2: Solve in integers

$$92x^2 + 1 = y^2 \tag{2.8}$$

Solution : Suppose $x = 1, y = 10, m = 8$. By composing with itself

$$(1, 10; 8) \bullet (1, 10; 8) = (20, 192; 64) = (x', y'; m')$$

In other words, with the above values,

$$92x'^2 + 64 = y'^2$$

Now division by 8^2 gives

$$92(\frac{x'}{8})^2 + 1 = (\frac{y'}{8})^2$$

Therefore $(x'' = x'/8 = 5/2, y'' = y'/8 = 24; 1)$ satisfies the beginning equation. Composing withitself gives

$$(x'', y''; 1) \bullet (x'', y''; 1) = (120, 1151; 1)$$

Thus (120, 1151 ;1) is an integer solution. ∎

Remark : Before taking up the *Chakravāla* algorithm, we will state a result due to Brahmagupta which shows that for four cases when integer solutions of the auxiliary equation (2.2) are given, then the integer solutions of (1.1) can be straight away obtained. In the *Chakravāla* algorithm (to be given later), as a shortcut, one can stop when one of these cases arise without going to the end of the cycle. The proof (which is based on the composition law) is sketched in [W] (Chapter1) and given in more detailed fashion in [DS], Part 2, pages 157-160. We do not give the proof here because in the *Chakravāla* or cyclic algorithm which is the subject of the present study it is not necessary to make use this theorem. However it is useful to know it, because in many instances it cuts short the work without going to the end of the period.

Proposition 1.4: (Brahmagupa)

Existence of integer solutions a, b of

$$Da^2 + m = b^2$$

for $m = -1, \pm 2, \pm 4$ imply the existence of integer solutions $(x, y; 1)$ of

$$Dx^2 + 1 = y^2$$

1: For $m = -1$: we have the integer triple $(2ab, 2b^2 + 1; 1)$

2: For $m = \pm 2$: we have the integer triple $(ab, b^2 \mp 1; 1)$

3: $m = 4$, b even : we have the integer triple $(\frac{ab}{2}, \frac{b^2}{2} - 1; 1)$.

4: $m = 4$, b odd: we have the integer triple $(\frac{a}{2}(b^2 - 1), \frac{b}{2}(b^2 - 3); 1)$.

5. $m = -4$: we have the integer triple $(\frac{ab}{2}(b^2+3)(b^2+1), (b^2+2)[\frac{1}{2}(b^2+3)(b^2+1) - 1]; 1)$

3. The Chakravāla algorithm of Bhāskara II (1150 CE)

We want to solve the Brahmagupta-Fermat-Pell equation (1.1) which we repeat

$$Dx^2 + 1 = y^2 \tag{3.1}$$

where D is a positive non-square integer.

Consider the associated equation

$$Da^2 + m = b^2 \tag{3.2}$$

where the members of the triple $(a, b; m)$ are relatively prime integers. The following Lemma will be used repeatedly to produce the recursion.

Lemma 3.1 (*Bhāskara* II) (see [DS], part 2):

Let ν be any positive integer. Then

$$D\big(\frac{(a\nu + b}{m}\big)^2 + \frac{(\nu^2 - D)}{m} = (\frac{Da + b\nu}{m})^2 \tag{3.3}$$

Proof
We have the identitity

$$D\ 1^2 + (\nu^2 - D) = \nu^2 \tag{3.4}$$

We compose the triple $(a, b; m)$ with the triple $(1, \nu; (\nu^2 - D)$ according to Brahmagupta's composition law (Proposition 1.1) to get the triple $(a\nu + b, Da + b\nu; m(\nu^2 - D)$. In other words

$$D(a\nu + b)^2 + m(\nu^2 - D) = \big(Da + b\nu\big)^2$$

Now divide the previous eqation by m^2 to get

$$D\big(\frac{(a\nu+b)}{m}\big)^2+\frac{(\nu^2-D)}{m}=\big(\frac{Da+b\nu}{m}\big)^2 \tag{3.5}$$

which proves the lemma. ∎

We now describe the *Chakravāla* algorithm of Bhāskara II for solving (3.1). In an intermediate step, Bhāskara solved a linear Diophantine equation by the pulverizer or *kuttāka* method (see [DS], part 2) of Aryabhata and Brahmagupta. However, as noticed in [A1] and [W, page 23], this is equivalent in the present context to a congruence condition.

We will solve the auxiliary equation (3.2) iteratively to obtain a sequence of quadruples $(a_n, b_n; m_n, \nu_n)$ where the three members of the triple $(a_n, b_n; m_n)$ consists of relatively prime (coprime) integers. ν_n is a positive integer. We use the standard notation: if a, b are integers then $a|b$ means a divides b. Two integers a, b are relatively prime if $\gcd(a, b) = 1$. It is convenient to state again (3.2)

$$Da_n^2+m_n=b_n^2 \tag{3.6}$$

The positive integers ν_n play an auxiliary role, but are needed for the algorithm to be defined.

The *Chakravāla* algorithm

To start the algorithm we choose:

$$a_0=0, b_0=1; m_0=1, \nu_{-1}=0 \tag{3.7}$$

The subsequent steps are defined as follows:

1. Choose $\nu_n \equiv -\nu_{n-1}$ (mod m_n) and amongst these ν_n choose ν_n such that $|\nu_n^2 - D|$ is least in the congruence class (mod m_n). We then say (following the convenient terminology in [B]) that the positive integer ν_n is **best** (mod m_n).

Remark 1: By definition of the choice of ν_n, $m_n|(\nu_n + \nu_{n-1})$.

Remark 2: There may be more than one choice of ν_n which is best, as remarked in [B]. This will be illustrated for the cases $D = 29,\ 97,\ 58$.

2. Suppose after n iterations we have the quadruple $(a_n, b_n; m_n, \nu_n)$ where $(a_n, b_n; m_n)$ are relatively prime integers. Then applying *Bhāskara's Lemma* composing the triples $(a_n, b_n; m_n)$ and $(1, \nu_n; (\nu_n^2 - D)$ gives us the recursion

$$a_{n+1}=\frac{(a_n\nu_n+b_n)}{m_n} \tag{3.8}$$

$$b_{n+1} = \frac{Da_n + b_n\nu_n}{m_n} \tag{3.9}$$

$$m_{n+1} = \frac{(\nu_n^2 - D)}{m_n} \tag{3.10}$$

(3.8), (3.9) and (3.10) imply the recurrence relations:

$$a_{n+2} = a_{n+1}\frac{(\nu_{n+1} + \nu_n)}{m_{n+1}} - a_n \tag{3.11}$$

$$b_{n+2} = b_{n+1}\frac{(\nu_{n+1} + \nu_n)}{m_{n+1}} - b_n \tag{3.12}$$

Now $m_{n+1} \mid (\nu_{n+1} + \nu_n)$. Therefore the coefficients in (3.11) and (3.12) are integers.

Theorem 3.2 :

$a_{n+1}, b_{n+1}, m_{n+1}$ are relatively prime integers.

Proof: By assumption a_n, b_n, m_n are relatively prime integers.

1. We will first prove that a_{n+1} is an integer. To this end first eliminate b_n between (3.8) and (3.9). We get

$$m_n(b_{n+1} - \nu_n a_{n+1}) = a_n(D - \nu_n^2) \tag{3.13}$$

whence

$$(b_{n+1} - \nu_n a_{n+1}) = -m_{n+1}a_n \tag{3.14}$$

$$b_n - \nu_{n-1}a_n = -m_n a_{n-1} \tag{3.15}$$

From (3.8) we get

$$a_{n+1}m_n = a_n\nu_n + b_n = a_n(\nu_n + \nu_{n-1}) + (b_n - a_n\nu_{n-1})$$

Dividing the last equation by m_n and using (3.15) we get

$$a_{n+1} = \frac{a_n(\nu_n + \nu_{n-1})}{m_n} - a_{n-1} \tag{3.16}$$

Since a_n, a_{n-1} are integers and $m_n|(\nu_n + \nu_{n-1})$ we have a_{n+1} is an integer.

2. Next we prove that b_{n+1}, m_{n+1} are integers. From (3.13)

$$\frac{m_n}{a_n}(b_{n+1} - \nu_n a_{n+1}) = (D - \nu_n^2) \tag{3.17}$$

Now m_n and a_n are relatively prime. The right hand side of (3.17) is an integer. Therefore $a_n|(b_{n+1} - \nu_n a_{n+1})$. Hence

$$\frac{b_{n+1} - \nu_n a_{n+1}}{a_n} = \frac{D - \nu_n^2}{m_n} = -m_{n+1} = \text{integer}$$

Therefore

$$b_{n+1} = \nu_n a_{n+1} - a_n m_{n+1} = \text{integer} \tag{3.18}$$

We have thus proved that b_{n+1} and m_{n+1} are integers.

3. Next we prove that $a_{n+1}, b_{n+1}, m_{n+1}$ are pairwise relatively prime. From (3.8) we obtain

$$\begin{aligned} m_n a_{n+1} b_n &= (a_n \nu_n + b_n) b_n = a_n \nu_n b_n + b_n^2 \\ &= a_n \nu_n b_n + (D a_n^2 + m_n) \\ &= a_n(\nu_n b_n + D a_n) + m_n \\ &= a_n m_n b_{n+1} + m_n \end{aligned}$$

where in the last step we have used (3.9). Now dividing out by m_n we obtain

$$a_{n+1} b_n - a_n b_{n+1} = 1 \tag{3.19}$$

.

From (3.19) we see that a_{n+1}, b_{n+1} are relatively prime and $(a_{n+1}, b_{n+1}, m_{n+1})$ are relatively prime. The theorem has been proved ∎

The analysis of this algorithm will be given in Section 4. We make some prelimnary observations. ν_n has been chosen such that ν_n^2 is nearest to D as possible in absolute value, within the congruence class (mod $\mathrm{m_n}$). The condition $|m_n| < \sqrt{D}$ is shown in Section 4 to hold uniformly. Recall $m_n m_{n+1} = \nu_n^2 - D$. It follows that $|\nu_n^2 - D| < D$ whence we obtain the bound $0 < \nu_n < \sqrt{2D}$

To display the cyclical structure of the algorithm it will be enough to record the evolution of the triple (m_n, ν_n, m_{n+1}). The triple represents (Gaussian notation) the binary quadratic form

$$Q_n(x, y) = m_n x^2 + 2\nu_n xy + m_{n+1} y^2 \tag{3.20}$$

and the discriminant of the form is by its definition $\Delta(Q_n) = 4(\nu_n^2 - m_n m_{n+1}) = 4D$. The quadratic form can be represented by the matrix

$$Q_n = \begin{pmatrix} m_n & \nu_n \\ \nu_n & m_{n+1} \end{pmatrix} \tag{3.21}$$

whence the determinant of the form is $\det(Q_n) = m_n m_{n+1} - \nu_n^2 = -D$, showing that the form is indefinite. The number D is positive, non square and fixed. Since the coefficients are integers with the above uniform bounds, the number of possible triples (or forms) (m_n, ν_n, m_{n+1}) of fixed discriminant is finite. Therefore the successive forms must eventually repeat themselves. This is the origin of the cyclical structure of the *Cakravāla* algorithm which will be proved in Section 4.

If the cyclic algorithm leads to one of the cases $m = \pm 1, \pm 2, \pm 4$, then as a shortcut we can apply Brahmagupta's Theorem 3. Independently of this, as shown later, this algorithm always gives an integer solution of (3.1). If not stopped artificially to exploit the above short cut, the full sequence leading to the solution will display the cyclical structure. We give a few examples which display these features. The cases in examples 3.1 and 3.2 were solved by $Bh\alpha skaraII$ (see [DS]). Example 3.3, mentioned in [B], illustrates the possibility of twin successors and thus of a sequence splitting into two sequences which join up in the cycle. Examples 3.4, and 3.5 also illustrates this point.

Example 3.1 (*Bhāskara II*, 1150 CE) (see [DS, part 2]):
Solve in integers the case $D = 61$:

$$61x^2 + 1 = y^2$$

.

The auxiliary equation is:

$$61a^2 + m = b^2$$

Step 0:

$$\nu_{-1} = 0, a_0 = 0, b_0 = 1, m_0 = 1$$

.
This is the trivial solution.

Step 1: $(a_1, , b_1, m_1, \nu_0)$. We must have $m_0|(\nu_0 + \nu_{-1})$. Using the values from step 0, we have ν_0 is any integer such that $|\nu_0^2 - 61|$ is least. This gives $\nu_0 = 8$. Thus $m_1 = \nu_0^2 - 61 = 3$ and $a_1 = 1, b_1 = 8$. We thus have

$$a_1 = 1, b_1 = 8, m_1 = 3, \nu_0 = 8$$

Step 2: (a_2, b_2, m_2, ν_1). Must have $m_1|(\nu_1 + \nu_0)$. This implies $3|(\nu_1 + 8)$, and $|\nu_1^2 - 61|$ is least. Therefore $\nu_1 = 7$, $m_2 = \frac{\nu_1^2 - 61}{3} = -4$, $a_2 = (7 + 8)/3 = 5$, $b_2 = (61 + b_1\nu_1)/3 = (61 + 56)/3 = 39$. We thus have

$$a_2 = 5, b_2 = 39, m_2 = -4, \nu_1 = 7$$

Proceeding in this way we have to obtain $(a_{n+1}, b_{n+1}, m_{n+1}, \nu_n)$ until $n = 13$ when we get the desired result $(m_{14} = 1)$.

$$(a_{14} = 226153980, b_{14} = 1766319049, m_{14} = 1, \nu_{13} = 8)$$

To display the cyclical structure of the *Cakravāla* it is enough to record the sequence (m_n, ν_n, m_{n+1}). Starting with $n = 0$, the full cycle ends at $n = 13$, in other words after 14 steps. We have

$$\{(1, 8, 3), (3, 7, -4), (-4, 9, -5), (-5, 6, 5), (5, 9, 4)(4, 7, -3), (-3, 8, -1);$$
$$(-1, 8, -3), (-3, 7, 4), (4, 9, 5), (-5, 6, -5), (-5, 9, -4), (-4, 7, 3), (3, 8, 1)\} \tag{3.22}$$

The sequence reverses itself after 7 steps (marked with a semi colon). From step 8 each member is the reverse of the previous one, to end up finally at step 14 which is the reverse of the first step and gives $m_{14} = 1$.

Boundedness of m_n, ν_n: Observe in the above cycle that the maximum value of $|m_n|$ is 5. We have $|m_n| < \sqrt{D}$, where $D = 61$ for all n in the cycle. Moreover the maximum value of ν_n is $9 < \sqrt{2 \times 61}$. Thus $\nu_n < \sqrt{2D}$.

Remark : Just after 2 steps we get $m = -4$, so we could have applied Brahmagupta's Proposition 1.3 to the triple
$(a = a_2 = 5,\ b = b_2 = 39; m = m_2 = -4)$ to obtain

$$x = ab\frac{1}{2}(b^2 + 3)(b^2 + 1) = 226153980$$

$$y = (b^2 + 2)\Big(\frac{1}{2}(b^2 + 3)(b^2 + 1) - 1\Big) = 1766319049$$

as the least solution of $61x^2 + 1 = y^2$. This short cut however breaks the cycle.

Example 3.2, (*Bhāskara II*). Solve in integers the case $D = 67$:

$$67x^2 + 1 = y^2$$

.
The auxiliary equation is:

$$67a^2 + m = b^2$$

0 : $(a_0 = 0, b_0 = 1, m_0 = 1, \nu_{-1} = 0)$.

1: $m_0|(\nu_0 + \nu_{-1}) \Rightarrow 1|\nu_0$. Therefore ν_0 is any integer: $|\nu_0^2 - 67|$ is least. $\nu_0 = 8$ We get

$$(a_1 = 1, b_1 = 8, m_1 = -3, \nu_0 = 8)$$

2 : $m_1|(\nu_1 + \nu_0) \Rightarrow ((-3)|(\nu_1 + 8)$. Possible choices are $\nu_1 = 4, 7, 10.....$ Of these we must have $|\nu_1^2 - 67|$ is least. This gives $\nu_1 = 7$. $m_2 = \frac{\nu_1^2 - 67}{-3} = 6$. $a_2 = -5, b_2 = -41$. Taking absolute values we get

$$(a_2 = 5, b_2 = 41, m_2 = 6, \nu_1 = 7)$$

3. $m_2|(\nu_2 + \nu_1) \Rightarrow 6|(\nu_2 + 7)$, and $|\nu_2^2 - 67|$ least. This gives $\nu_2 = 5$ and $m_3 = \frac{\nu_2^2 - 67}{6} = -7$. We get

$$(a_3 = 11, b_3 = 90, m_3 = -7, \nu_2 = 5$$

4. $m_3|(\nu_3+\nu_2) \Rightarrow (-7)|(\nu_3+5)$, and $|\nu_3^2-67|$ least. This gives $\nu_3 = 9$ and $m_4 = \frac{\nu_3^2 - 67}{(-7)} = -2$. We get

$$(a_4 = 27, b_4 = 221, m_4 = -2, \nu_3 = 9)$$

We have taken absolute values for a_4, b_4.

Henceforth we record only the sequence

$$(m_n, \nu_n, m_{n+1})$$

to display the cyclical nature of the algorithm.

5. (m_4, ν_4, m_5) :
$m_4|(\nu_4 + \nu_3) \Rightarrow (-2)|(\nu_4 + 9)$, and $|\nu_4^2 - 67|$ least. This gives $\nu_4 = 9$ and $m_5 = \frac{\nu_4^2 - 67}{(-2)} = \frac{81-67}{(-2)} = -7$. Therefore we have obtained the triple

$$(m_4 = -2, \nu_4 = 9, m_5 = -7)$$

6. (m_5, ν_5, m_6) :
$m_5|(\nu_5 + \nu_4) \Rightarrow (-7)|(\nu_5 + 9)$, and $|\nu_5^2 - 67|$ least. This gives $\nu_5 = 5$ and $m_6 = \frac{\nu_5^2 - 67}{(-7)} = \frac{25-67}{(-7)} = 6$. Therefore we have obtained the triple

$$(m_5 = -7, \nu_5 = 5, m_6 = 6)$$

7. (m_6, ν_6, m_7) :

$m_6|(\nu_6 + \nu_5) \Rightarrow 6|(\nu_6 + 5)$, and $|\nu_6^2 - 67|$ least. This gives $\nu_6 = 7$ and $m_7 = \frac{\nu_6^2 - 67}{m_6} = \frac{49-67}{6} = -3$. Therefore we have obtained the triple

$$(m_6 = 6, \nu_6 = 7, m_7 = -3)$$

8. (m_7, ν_7, m_8) :

$m_7|(\nu_7+\nu_6) \Rightarrow (-3)|(\nu_7+7)$, and $|\nu_7^2-67|$ least. This gives $\nu_7=8$ and $m_8=\frac{\nu_6^2-67}{m_7}=\frac{64-67}{-3}=1$. Therefore we have obtained the triple

$$(m_7=-3, \nu_7=8, m_8=1)$$

Thus the solution has been reached in Step 8:

$$(a_8=5967, b_8=48842, m_8=1)$$

.

Remark : Since we reached $m_4=-2$ in Step 4, a short cut via Brahmagupta's Theorem 3 already gives $(x=5967, y=48842, m=1)$.

The full sequence (m_n, ν_n, m_{n+1}) which displays the cyclical nature is

$$\{(1,8,-3),(-3,7,6),(6,5,-7),(-7,9,-2);\ (-2,9,-7),(-7,5,6),(6,7,-3),(-3,8,1)\} \tag{3.23}$$

From step 5 onwards the sequence reverses itself. This is a typical feature of the *Cakravāla* cycle. Once again we observe for all n in the cycle $|m_n|<\sqrt{D}$ since the maximum value of $|m_n|$ in the cycle is 7 and $7<\sqrt{67}$. Moreover $0<\nu_n<\sqrt{2D}$, since the maximum value of ν_n is 9 and $9<\sqrt{2\times 67}$.

Twin successors:

Bauval [B] pointed out the possibility of local splitting and joining of a *Cakravāla* sequence. When $|m|<\sqrt{D}$, m is even and ν is best (mod m), this occurs when ν has two values $\nu_\pm$ which are equidistant from D. We have

$$0<\nu_+^2-D=D-\nu_-^2$$

Twin successors are of the form (see Section 4, Lemma 4.2) $(m, \nu_\pm, m')$ where m is even and $\nu_\pm$ is best (mod m) , and

$$\nu_\pm=|m'|\pm\frac{|m|}{2}$$

$$|m'|^2+\frac{|m|^2}{4}=D$$

.

This leads to twin sequences. This possibility was absent in the Ayyangar analysis. We will first see this from an illustrative example when $D = 29$, see[B]. Further examples are when $D = 97$ and when $D = 58$.

Example 3.3 : Solve in integers the equation

$$29x^2 + 1 = y^2$$

The auxiliary equation is

$$29a^2 + m = b^2$$

We proceed as earlier to obtain the sequence (m_n, ν_n, m_{n+1}).

0 :

$$(a_0 = 0, b_0 = 1, m_0 = 1, \nu_{-1} = 0)$$

1 : (m_0, ν_0, m_1):

To obtain ν_0 the only condition to meet in this case is $|\nu_0^2 - 29|$ is least. This gives $\nu_0 = 5$.

$$m_1 = \frac{\nu_0^2 - 29}{m_0} = -4$$

Thus we obtain the triple

$$(m_0, \nu_0, m_1) = (1, 5, -4)$$

2: (m_1, ν_1, m_2):

$m_1|(\nu_1 + \nu_0) \Rightarrow 4|(\nu_1 + 5)$, The possible values are $\nu_1 = 3, 7, 11, ...$ We have to have $|\nu_1^2 - 29|$ is least. This happens for both $\nu_1 = \nu_- = 3$ and $\nu_1 = \nu_+ = 7$. In fact

$$\nu_- = 3 \ : |9 - 29| = 20$$

1

$$\nu_+ = 7 \ : |49 - 29| = 20$$

So we can choose either of the values and thus the sequence is *split*. This leads to twin successors

1. $\nu_- = 3$. Then

$$m_2 = \frac{\nu_-^2 - 29}{m_1} = \frac{-20}{-4} = 5$$

$$(m_1, \nu_1 = \nu_1 = \nu_-, m_2) = (-4, 3, 5)$$

2. $\nu_+ = 7$. Then

$$m_2 = \frac{\nu_+^2 - 29}{m_1} = \frac{20}{-4} = -5$$

$$(m_1, \nu_1 = \nu_+, m_2) = (-4, 7, -5)$$

Observe that m_1 is even, $\nu_\pm = |m_2| \pm \frac{|m_1|}{2}$, and $29 = m_2^2 + \frac{m_1^2}{4}$, thus verifying the assertions preceding this example. Thus choices $\nu_1 = \nu_\pm$ have led to *twin successors*:

$$(1, 5, -4) \nearrow (-4, \nu_- = 3, 5) : \text{ sequence } 1$$

$$(1, 5, -4) \searrow (-4, \nu_+ = 7, -5) : \text{ sequence } 2$$

(ν_- sequence: Successor of $(m_1, \nu_-, m_2) = (-4, 3, 5)$ is (m_2, ν_2, m_3).

We obtain $\nu_2 : m_2|(\nu_2 + \nu_-) \Rightarrow 5|(\nu_2 + 3)$. Then possible choices $\nu_2 =, 2, 7, 12, ...$ Of these $\nu_2 = 7 = \nu_+$ makes $|\nu_2^2 - 29|$ least. Then

$$m_3 = \frac{\nu_+^2 - 29}{m_2} = \frac{20}{5} = 4$$

and thus

$$(m_2, \nu_2 = \nu_+, m_3) = (5, 7, 4)$$

and thus successor of (m_1, ν_-, m_2) is (m_2, ν_+, m_3). In section 4 we will see that is a general feature.

We have $\nu_3 : m_3|(\nu_3 + \nu_2) \Rightarrow 4|(\nu_3 + 7)$. Then possible choices $\nu_3 = 1, 5, 9, ...$ Of these $\nu_3 = 5$ makes $|\nu_3^2 - 29|$ least. Then

$$m_4 = \frac{\nu_3^2 - 29}{m_3} = \frac{-4}{4} = -1$$

Thus

$$(m_3, \nu_3, m_4) = (4, 5, -1)$$

We have so far obtained for for the ν_- sequence:

$$(1, 5, -4), (-4, \nu_- = 3, 5), (5, \nu_+ = 7, 4), (4, 5, -1);$$

ν_+ sequence : The successor of $(m_1, \nu_{1+}, m_2) = (-4, 7, -5)$ is (m_2, ν_2, m_3)
$\nu_2 : m_2|(\nu_2 + \nu_{1+}) \Rightarrow 5|(\nu_2 + 7)$. Possible choices $\nu_2 = 3, 8, ...$ Of these $\nu_2 = \nu_- = 3$ makes $|\nu_2^2 - 29|$ least. Then

$$m_3 = \frac{-20}{-5} = 4$$

and we obtain for the triple (m_2, ν_2, m_3):

$$(-5, \nu_- = 3,\ 4)$$

Thus the successor of (m_1, ν_+, m_2) is (m_2, ν_-, m_3).

$\nu_3 : m_3|(\nu_3 + \nu_-) \Rightarrow 4|(\nu_3 + 3)$. Possible choices $\nu_3 = 5, 9, ...$ Of these $\nu_3 = 5$ makes $|\nu_3^2 - 29|$ least. Then

$$m_4 = \frac{-4}{4} = -1$$

and we obtain for the triple (m_3, ν_3, m_4):

$$(4, 5, -1)$$

Thus for the ν_+ sequence we have obtained so far

$$(1, 5, -4), (-4, \nu_+ = 7, -5), (-5, \nu_- = 3, 4), (4, 5, -1);$$

At $(4, 5, -1)$ the two sequences have merged. After the ν_+ and ν_- have merged the sequences reverse to complete the cycle. The same phenomenon of twin successors, local splitting and merging is met in the reverse parts. Therefore we have 4 cycles. The point where the sequences reverse is indicated by a semi-colon.

The completed sequence ν_- cycles are

$$\{(1, 5, -4), (-4, \nu_-, 5), (5, \nu_+, 4), (4, 5, -1);$$
$$(-1, 5, 4), (4, \nu_+, 5), (5, \nu_-, -4), (-4, 5, 1)\} \tag{3.24}$$

ν_- bis cycle :

$$(1, 5, -4), (-4, \nu_-, 5), (5, \nu_+, 4), (4, 5, -1); (-1, 5, 4), (4, \nu_-, -5), (-5, \nu_+, -4), (-4, 5, 1)$$

The completed ν_+ cycle is

$$\{(1, 5, -4), (-4, \nu_+, -5), (-5, \nu_-, 4), (4, 5, -1);$$
$$(-1, 5, 4), (4, \nu_-, -5), (-5, \nu_+, -4), (-4, 5, 1)\} \tag{3.25}$$

and ν_+ bis cycle :

$$(1,5,-4),(-4,\nu_+,-5),(-5,\nu_-,4),(4,5,-1);(-1,5,4),(4,\nu_+,5),(5,\nu_-,-4),(-4,5,1)$$

which shows the cyclical nature of the twin sequences. Finally observe that after 4 steps the two sequences above have merged at the triple $(4,5,-1)$. Working through the algorithm gives us the common solution $(a_4 = 13, b_4 = 70; -1)$ to the equation

$$29\,a^2 - 1 = b^2$$

where $a = a_4$ and $b = b_4$. The full cycle is however reached after 8 steps when we obtain as the common solution $(a_8 = 1820,\ b_8 = 9801; 1)$. This is most easily seen by applying a shortcut which is Brahmagupta's composition after 4 steps:

$$(a,b;-1)\bullet(a,b;-1) = (2ab,\ 29a^2+b^2;1) = (1820,\ 9801;1)$$

where $a = a_4 = 13,\ b = b_4 = 70$. This is the common solution at the end of the cycle where the two sequences have merged again.

Example 3.4: $D = 97$. This will illustrate once more twin successors. We will record the steps (m_n, ν_n, m_{n+1}), the solution of the Brahmagupta-Fermat equation will be found in Section 5. We start with $\nu_{-1} = 0,\ m_0 = 1$.
1. (m_0, ν_0, m_1). Since $m_0 = 1$, the only condition to meet is that $|\nu_0^2 - 97|$ is least. This gives $n_0 = 10$ and $m_1 = \nu_0^2 - 97 = 3$.Thus

$$(m_0, \nu_0, m_1) = (1, 10, 3)$$

2. (m_1, ν_1, m_2). We must have $3|(10 + \nu_1)$. This gives $\nu_1 = 2, 5, 8, 11, 14, ...$ as possible choices. $\nu_1 = 11$ makes $|\nu_1^2 - 97|$ least. This gives $m_2 = \frac{\nu_1^2 - 97}{m_1} = \frac{24}{3} = 8$ Therefore

$$(m_1, \nu_1, m_2) = (3, 11, 8)$$

3. (m_2, ν_2, m_3). We must have $8|(11 + \nu_1)$. This gives $\nu_2 = 5, 13, ...$ as possible choices. Both the choices $\nu_2 = 5, 13$ make $|\nu_2^2 - 97|$ least. In fact $|5^2 - 97| = 72$ and $|13^2 - 97| = 72$. Define

$$\nu_{2,+} = 13,\ \nu_{2,-} = 5$$

Then ν_+^2 and ν_-^2 are equidistant from 97 in absolute value. This leads to twin sequences as follows.
4. ν_+ *branch* : For the choice $\nu_2 = \nu_+ = 13$ we have $m_3 = \frac{\nu_+^2 - 97}{8} = \frac{72}{8} = 9$. Therefore

$$(m_2, \nu_2, m_3) = (8, \nu_{2,+} = 13, 9)$$

$(m_3 = 9, \nu_3, m_4)$. We must have $m_3|(\nu_3 + 13)$ This gives $\nu_3 = 5, 14, ...$ and it is seen that $\nu_3 = 5$ makes $|\nu_3^2 - 97|$ least. Thus $\nu_3 = \nu_-$ Therefore $m_4 = \frac{\nu_3^2 - 97}{m_3} = \frac{5^2 - 97}{9} = -\frac{72}{9} = -8$. Therefore

$$(m_3, \nu_3, m_4) = (9, \nu_{2,-} = 5, -8)$$

5. $(m_4 = -8, \nu_4, m_5)$. We must have $8|(\nu_4 + 5)$. This gives $\nu_4 = 3, 11, 19, ...$ as possible choices. $|\nu_4^2 - 97|$ is least for the choice $\nu_4 = 11$. Thus $m_5 = \frac{\nu_4^2 - 97}{m_4} = \frac{121 - 97}{-8} = \frac{24}{-8} = -3$. Therefore

$$(m_4, \nu_4, m_5) = (-8, 11, -3)$$

6. $(m_5 = -3, \nu_5, m_6)$. We must have $3|(\nu_5 + 11)$. This gives $\nu_5 = 1, 4, 10, 13, ...$ as possible choices. $|\nu_5^2 - 97|$ is least for the choice $\nu_5 = 10$. Thus $m_6 = \frac{\nu_5^2 - 97}{m_4} = \frac{100 - 97}{-3} = -1$. Therefore

$$(m_5, \nu_5, m_6) = (-3, 10, -1)$$

We have thus obtained for the ν_+ branch:

$$(1, 10, 3), (3, 11, 8), (8, \nu_+ = 13, 9), (9, \nu_- = 5, -8), (-8, 11, -3), (-3, 10, -1); \qquad (3.26)$$

ν_- *branch*: We have

$$(m_0 = 1, \nu_0 = 10, m_1 = 3), (m_1 = 3, \nu_1 = 11, m_2 = 8), (m_2, \nu_2 = \nu_- = 5, m_3 = -9)$$

where the last integer comes from $m_3 = \frac{25 - 97}{8} = -9$.
$(m_3 = -9, \nu_3, m_4)$. We must have $m_3|(\nu_3 + 5)$, or $9|(\nu_3 + 5)$. Possible choices are $\nu_3 = 4, 13, 22, ...$ The choice $\nu_3 = 13 = \nu_+$ makes $|n_3^2 - 97|$ least. Whence $m_4 = \frac{169 - 97}{-9} = -8$. Thus

$$(m_3, \nu_3, m_4) = (-9, \nu_+ = 13, -8)$$

$(m_4 = -8, \nu_4, m_5)$. We must have $m_4|(\nu_4 + \nu_3)$, or $8|(\nu_4 + 13)$. Possible choices are $\nu_4 = 3, 11, 19, ...$ Of these choices $\nu_4 = 11$ makes $|\nu_4^2 - 97|$ least. We have $m_5 = \frac{121 - 97}{-8} = -3$. Thus

$$(m_4, \nu_4, m_5) = (-8, 11, -3)$$

$(m_5 = -3, \nu_5, m_6)$. We must have $m_5|(\nu_5 + \nu_4)$, or $3|(\nu_5 + 11)$. Possible choices are $\nu_5 = 1, 4, 7, 10, 13, ...$ Of these choice $\nu_5 = 10$ makes $|\nu_4^2 - 97|$ least. We have $m_6 = \frac{\nu_5^2 - 97}{m_5} = \frac{100 - 97}{-3} = -1$. Thus

$$(m_5, \nu_5, m_6) = (-3, 10, -1)$$

We have thus obtained so far for the ν_- branch

$$(1,10,3),(3,11,8),(8,\nu_- = 5,-9),(-9,\nu_+ = 13,-8),(-8,11,-3),(-3,10,-1); \quad (3.27)$$

Observe that the ν_+ branch given by (3.26) and the ν_- branch given by (3.27) have merged at the step $(-3, 10, -1)$. After the ν_+ and ν_- have merged the sequences reverse to complete the cycle. The same phenomenon of twin successors, local splitting and merging is met in the reverse parts. Therefore we have 4 cycles. They are
ν_+ cycle

$$(1,10,3),(3,11,8),(8,\nu_+ = 13,9),(9,\nu_- = 5,-8),(-8,11,-3),(-3,10,-1);$$

$$(-1,10,-3),(-3,11,-8),(-8,\nu_- = 5,9),(9,\nu_+ = 13,8),(8,11,3),((3,10,1) \quad (3.28)$$

ν_+ bis cycle

$$(1,10,3),(3,11,8),(8,\nu_+ = 13,9),(9,\nu_- = 5,-8),(-8,11,-3),(-3,10,-1);$$

$$(-1,10,-3),(-3,11,-8),(-8,\nu_+ = 13,-9),(-9,\nu_- = 5,8),(8,11,3),(3,10,1) \quad (3.29)$$

ν_- cycle

$$(1,10,3),(3,11,8),(8,\nu_- = 5,-9),(-9,\nu_+ = 13,-8),(-8,11,-3),(-3,10,-1);$$

$$(-1,10,-3),(-3,11,-8),(-8,\nu_+ = 13,-9),(-9,\nu_- = 5,8),(8,11,3),(3,10,1) \quad (3.30)$$

ν_- bis cycle

$$(1,10,3),(3,11,8),(8,\nu_- = 5,-9),(-9,\nu_+ = 13,-8),(-8,11,-3),(-3,10,-1);$$

$$(-1,10,-3),(-3,11,-8),(-8,\nu_- = 5,9),(9,\nu_+ = 13,8)8,11,3),(3,10,1) \quad (3.31)$$

These 4 cycles produce the same solution $(6377352, 62809633; 1)$ of the Brahmagupta-Fermat equation which can be seen from the algorithm. This will be seen again in Section 5.

Example 3.5: $D = 58$. This is our final example of twin successors. We will record the steps (m_n, ν_n, m_{n+1}), the solution of the Brahmagupta-Fermat equation will be found in Section 5. We start with $\nu_{-1} = 0$, $m_0 = 1$.
1. (m_0, ν_0, m_1). Since $m_0 = 1$, the only condition to meet is that $|\nu_0^2 - 58|$ is least. This gives $n_0 = 8$ and $m_1 = \nu_0^2 - 58 = 6$.Thus

$$(m_0, \nu_0, m_1) = (1, 8, 6)$$

2. (m_1, ν_1, m_2). We must have $6|(8+\nu_1)$. This gives $\nu_1 = 4, 10, 16, ...$ as possible choices. Both the choices $\nu_1 = 4, 10$ make $|\nu_1^2 - 58|$ least. In fact $|4^2 - 58| = 42$ and $|10^2 - 58| = 42$. Define

$$\nu_{1,+} = 10,\ \nu_{1,-} = 4$$

Then ν_+^2 and ν_-^2 are equidistant from 58 in absolute value. This leads to twin sequences as follows.

3. ν_- *branch* : For the choice $\nu_1 = \nu_- = 4$ we have $m_2 = \frac{\nu_+^2 - 58}{6} = \frac{-42}{6} = -7$. Therefore

$$(m_1, \nu_1, m_2) = (6, \nu_- = 4, -7)$$

$(m_2 = -7, \nu_2, m_3)$. We must have $m_2|(\nu_1 + \nu_2)$, or $7|(4 + \nu_2)$. This gives $\nu_2 = 3, 10, ...$ and it is seen that $\nu_2 = 10$ makes $|\nu_2^2 - 58|$ least. Thus $\nu_2 = \nu_+ = 10$ Therefore $m_3 = \frac{\nu_2^2 - 58}{m_3} = \frac{10^2 - 58}{m_2} = \frac{42}{-7} = -6$. Therefore

$$(m_2, \nu_2, m_3) = (-7, \nu_+ = 10, -6)$$

4. $(m_3 = -6, \nu_3, m_4)$. We must have $6|(10 + \nu_3)$. This gives $\nu_3 = 2, 8, 14, ...$ as possible choices. $|\nu_3^2 - 58|$ is least for the choice $\nu_3 = 8$. Thus $m_4 = \frac{\nu_3^2 - 58}{m_3} = \frac{64-58}{-6} = \frac{6}{-6} = -1$. Therefore

$$(m_3, \nu_3, m_4) = (-6, 8, -1)$$

5. $(m_4 = -1, \nu_4, m_5)$. We must have $-1|(\nu_4 + 8)$. This gives $\nu_4 = 1, 2, 3, 4, ...7, 8, 9, ...$ as possible choices. $|\nu_4^2 - 58|$ is least for the choice $\nu_4 = 8$. Thus $m_5 = \frac{\nu_4^2 - 58}{m_4} = \frac{64-58}{-1} = -6$. Therefore

$$(m_4, \nu_4, m_5) = (-1, 8, -6)$$

At this point the sequence has already reversed. The complete sequences are:

ν_- cycle

$$\begin{aligned}&(1, 8, 6), (6, \nu_- = 4, -7), (-7, \nu_+ = 10, -6), (-6, 8, -1);\\ &(-1, 8, -6), (-6, \nu_+ = 10, -7), (-7, \nu_- = 4, 6), (6, 8, 1)\end{aligned} \tag{3.32}$$

ν_- bis cycle

$$\begin{aligned}&(1, 8, 6), (6, \nu_- = 4, -7), (-7, \nu_+ = 10, -6), (-6, 8, -1);\\ &(-1, 8, -6), (-6, \nu_- = 4, 7), (7, \nu_+ = 10, 6), (6, 8, 1)\end{aligned}$$

.
In a similar way we compute the the other of the twin sequences.

ν_+ cycle:

$$(1,8,6),(6,\nu_+=10,7),(7,\nu_-=4,-6),(-6,8,-1);$$

$$(-1,8,-6),(-6,\nu_-=4,7),(7,\nu_+=10,6),(6,8,1) \tag{3.33}$$

.
ν_+ bis cycle

$$(1,8,6),(6,\nu_+=10,7),(7,\nu_-=4,-6),(-6,8,-1);$$

$$(-1,8,-6),(-6,\nu_+=10,-7),(-7,\nu_-=4,6),(6,8,1)$$

The two sequences merge at the midpoint, $(-6,8,-1)$, and then reverse to complete the cycles. Working through the algorithm we obtain from the twin sequences the same fundamental solution $(2574,19603);1)$ to the Brahmagupta-Fermat- Pell equation. This will be seen again in Section 5, from the periodic semi-regular continued fraction engendered by this algorithm.

4. The Chakravāla algorithm produces a cycle after a finite number of steps.

This section is based principally on the work of Bauval, [B].

Definition 4.1: Best (mod m)

Let $D>0$ be a non-square integer. Let $\nu>0$, and m be integers. Then following Bauval [B] we say that ν is **best (mod m)** if in the congruence class (mod m), ν^2 is nearest to D in absolute value. In other words for all $\nu'>0$, and $\nu'\equiv\nu \pmod m$

$$|D-\nu^2|\leq|D-\nu'^2] \tag{4.1}$$

If $|m|<\sqrt{D}$, then ν is best if ν is one of two positive integers ν_1 and ν_2 such that

$$\nu_1^2<D<\nu_2^2=(\nu_1+|m|)^2 \tag{4.2}$$

If only one is best, then we say it is **strictly best**.

If m is even and ν_1 and ν_2 are both best then

$$D-\nu_1^2=\nu_2^2-D \tag{4.3}$$

.

Lemma 4.2 (Twins):

Suppose m is even and $\nu_1 = \nu_-$, $\nu_2 = \nu_+$ are both best (mod m). Then we have **twins** $(m, \nu_\pm, m')$ satisfying

$$\nu_\pm = |m'| \pm \frac{|m|}{2} \tag{4.4}$$

and

$$D = |m'|^2 + \frac{|m|^2}{4} \tag{4.5}$$

Proof: Since $\nu_1 = \nu_-, \nu_2 = \nu_+$ are both best, we have

$$D - \nu_-^2 = \nu_+^2 - D = |m||m'| \tag{4.6}$$

where

$$\nu_-^2 < D < \nu_+^2 = (\nu_- + |m|)^2 \tag{4.7}$$

Therefore

$$|m||m'| = (\nu_- + |m|)^2 - D = \nu_-^2 + |m|^2 + 2\nu_-|m| - D$$

whence

$$|m||m'| = -|m||m'| + |m|^2 + 2\nu_-|m|$$

Dividing out by $2|m|$ we obtain

$$\nu_- = |m'| - \frac{|m|}{2} \tag{4.8}$$

and

$$\nu_+ = \nu_- + |m| = |m'| + \frac{|m|}{2} \tag{4.9}$$

which proves (4.4). Now square each of (4.8) and (4.9) and then add the squares to get

$$D = \frac{1}{2}(\nu_-^2 + \nu_+^2) = |m'|^2 + \frac{|m|^2}{4}$$

which proves (4.5). ∎

Proposition 4.3 , (after Bauval [B], Proposition 1) : Suppose $|m| < \sqrt{D}$, $\nu^2 - D = \varepsilon|m||m'|$ where $\varepsilon = 1$ if $\nu^2 > D$ and $\varepsilon = -1$ if $\nu^2 < D$ (which follows from $\nu^2 - D = mm'$). Suppose also ν is best (mod m). Then the following inequalities are equivalent

(1) ν is best (mod m)

$$(2) \qquad |m'|^2 + \frac{|m|^2}{4} \leq D \tag{4.10}$$

$$(3) \qquad \nu \geq |m'| + \varepsilon\frac{|m|}{2} \tag{4.11}$$

(2) $\Rightarrow |m'| < \sqrt{D}$.

Proof of Proposition 4.3: This is given in Appendix 1. ∎

The above implies that in the *Chakravāla* recursion $|m_n| < \sqrt{D}$ for all positive integers n.

Remark: The same inequalities also figure in Ayyangar [A1], page 237, but the his derivation of (2) from (3) by a squaring argument is false when $\varepsilon = -1$. See equation (14), p 237 of [A1]. Various errors in [A1] are pointed out in [B].

Definition 4.4: Steps and Reduced steps: We shall say, following Bauval [B], that the triple (m, ν, m') is a **step** if $|m| < \sqrt{D}$, $|\nu^2 - D| = |m||m'|$ and ν is best (mod m). If ν is also best (mod m'), then we have a **reduced step**. If (m, ν, m') is a reduced step then clearly (m', ν, m) is a step. If (m, ν, m') is a reduced step then both

$$|m'|^2 + \frac{|m|^2}{4} \leq D \tag{4.12}$$

$$|m|^2 + \frac{|m'|^2}{4} \leq D \tag{4.13}$$

Corollary 4.5: Let (m, ν, m') be a step. If $|m'| \geq |m|$ then the step is reduced.

Proof of Corollary 4.5: The inequality (4.10) for the step can be rewritten as

$$\frac{3}{4}(|m'|^2 - m^2) + |m|^2 + \frac{|m'|^2}{4} \leq D$$

Since $|m'| \geq |m|$, we get

$$|m|^2 + \frac{|m'|^2}{4} \leq D \tag{4.14}$$

which proves the Corollary.

Theorem 4.6 (after Bauval [B], Theorem 2): The successor of **any** step is **reduced**: If (m, ν, m') is a step and (m', ν', m'') is a successive step, we have $|m| < \sqrt{D}$ and $|m'| < \sqrt{D}$, $\varepsilon|m||m'| = \nu^2 - D$, $\varepsilon|m'||m''| = \nu'^2 - D$, $m'|(\nu + \nu')$ and

$$(1) \quad |m'|^2 + \frac{m^2}{4} \leq D \tag{4.15}$$

$$(2) \quad |m''|^2 + \frac{m'^2}{4} \leq D \tag{4.16}$$

then

$$(3) \quad |m'|^2 + \frac{m''^2}{4} \leq D \tag{4.17}$$

and thus the successor step (m', ν', m'') is a reduced step.

Corollary 4.7: *All steps are reduced*:

The first step (m_0, ν_0, m_1), where $m_0 = 1$ is easily seen to be reduced. By Proposition 4.3, $|m_1|^2 + \frac{|m_0|^2}{4} \leq D$, and $|m_1| < \sqrt{D}$. Furthermore $|m_0|^2 + \frac{|m_1|^2}{4} \leq 1 + \frac{D}{4} \leq D$, since $D \geq 2$. Hence the first step is reduced and therefore by Theorem 4.6 *all steps are reduced*.

Proof of Theorem 4.6: The proof is given in Appendix 2.

Lemma 4.8: Twin succesors

Suppose m is even and both $\nu_\pm = |m'| \pm \frac{|m|}{2}$ are best (mod m) as in Lemma 4.2. Then the successor step of $(m, \nu_\pm, m')$ is $(m', \nu_\mp, -m)$.

Proof: By Theorem 4.6 and Corollary 4.7, all steps are reduced. Thus each step $(m, \nu_\pm, m')$ is reduced and thus each of $\nu_\pm$ is best (mod m) as well as being best (mod m'). From this it can be shown that the successor step of (m, ν_+, m') is (m', ν_-, m''). Indeed, let the successor step of (m, ν_+, m') be (m', ν', m''). Then ν' is best (mod m'). Moreover ν_- is best (mod m'), since the step (m, ν_-, m') is reduced. The solution is $\nu' = \nu_-$.

Consider the successor step (m', ν_-, m''). Again, since by Theorem 4.6 and Corollary 4.7, all steps are reduced, we have that (m', ν_-, m'') is a reduced step. Therefore ν_- is best (mod m') and best (mod m''). Since ν_- is best (mod m), from Lemma 4.2, and also best (mod m') since (m, ν, m') is a reduced step, it follows that $m'' = \varepsilon m$, where $\varepsilon = \pm 1$, and the step $(m', \nu_-, \varepsilon m)$ is the successor of the step (m, ν_+, m'). It remains to fix the sign factor ε. Now $m'm = \nu_+^2 - D$, and from (4.7) $\nu_+^2 > D$. Therefore m and m' have the same sign. Since $m''m' = \nu_-^2 - D$ and $\nu_-^2 < D$, $m'' = \varepsilon m$ has the opposite sign of m' and therefore opposite sign of m. Thus $\varepsilon = -1$. Therefore we have proved that the step

(m, ν_+, m') has as successor step $(m', \nu_-, -m)$. Similarly we prove that the step(m, ν_-, m') has as successor step $(m', \nu_+, -m)$. ∎

Theorem 4.9: *The Chakravāla algorithm produces a finite sequence which is a cycle* :

Proof: The algorithm produces the sequence of steps (m_n, ν_n, m_{n+1}). From Proposition 4.3 we have $|m_n| < \sqrt{D}$ for all n. From this and $m_n m_{n+1} = \nu_n^2 - D$ we have $|\nu_n^2 - D| < D$, whence $0 < \nu_n < \sqrt{2D}$ for all n. Therefore the number of possible steps is finite. From Theorem 4.6 we have that if (m_n, ν_n, m_{n+1}) is a step, then its reverse (m_{n+1}, ν_n, m_n) is also a step. Therefore the total number of steps is even, say $2r$. The $2r$ steps complete a cycle. The mid point, before reversal, is reached after r steps. We now have two cases.

Case 1: Each step has a unique successor. We then have a sequence of r successive steps and then the reversed sequence of r steps to complete a cycle. Thus the cycle is

$$(1, \nu_0, m_1), (m_1, \nu_1, m_2), ..., (m_{r-2}, \nu_{r-2}, m_{r-1}), (m_{r-1}, \nu_{r-1}, m_r);$$

$$(m_r, \nu_{r-1}, m_{r-1}), (m_{r-1}, \nu_{r-2}, m_{r-2}), ..., (m_2, \nu_1, m_1), (m_1, \nu_0, 1)$$

Case 2: A step has a twin successor. In this case we have twin sequences. By Lemma 4.8, the successor of $(m, \nu_\pm, m')$ is $(m', \nu_\mp, -m)$ where $\nu_\pm = |m'| \pm \frac{|m|}{2}$. Moreover, following the argument in [B], a twin successor can only occur once before the midpoint of the cycle. Assume that the twin successor occurs at the j-th step. We then have two sequences. For each sequence we indicate by a semicolon the step at which the sequence is reversed. The two sequences merge at the $(j+3)$rd step. Thus the split is local. See the illustrative Examples 3.3 ($D = 29$), 3.4 ($D = 97$) and 3.5 (D=58).

$$(1, \nu_0, m_1), (m_1, \nu_1, m_2), ..., (m_{j-1}, \nu_{j-1}, m), (m, \nu_+, m')(m', \nu_-, -m), (-m, \nu_{j+2}, m_{j+3});$$

$$(m_{j+3}, \nu_{j+2}, -m)(-m, \nu_-, m')(m', \nu_+, m)(m, \nu_{j-1}, m_{j-1}), ..., (m_2, \nu_1, m_1), (m_1, \nu_0, 1)$$

and

$$(1, \nu_0, m_1), (m_1, \nu_1, m_2), ..., (m_{j-1}, \nu_{j-1}, m), (m, \nu_-, m')(m', \nu_+, -m), (-m, \nu_{j+2}, m_{j+3});$$

$$(m_{j+3}, \nu_{j+2}, -m)(-m, \nu_+, m')(m', \nu_-, m)(m, \nu_{j-1}, m_{j-1}), ..., (m_2, \nu_1, m_1), (m_1, \nu_0, 1)$$

∎

5. The Chakravāla algorithm and it's semi-regular continued fractions

We will consider the action of modular transformations on steps. A modular transformation is the action of the group $SL(2, \mathbb{Z})$. For this it is useful to identify the step (m_n, ν_n, m_{n+1}) with the binary quadratic form

$$Q_n(x,y) = m_n x^2 + 2\nu_n xy + m_{n+1}y^2 \tag{5.1}$$

with an extra condition: the middle coefficient ν_n is *best*, i.e. $|\nu_n^2 - D|$ is least in the modulus class (mod m_n). Such forms can be called *best forms*. $\Delta(Q_n) = 4D$ is the discriminant of the form, and this is by definition

$$\Delta(Q_n) = 4(\nu_n^2 - m_n m_{n+1}) = 4D$$

The main reason, in this context, for the quadratic form interpretation is for studying the action of the modular group $SL(2,\mathbb{Z})$. It has been known, since Gauss, that the modular group, and some particular transformations engender the evolution of the forms $(m,\nu,m') \to (m',\nu',m'')$. Additional conditions have to be imposed to ensure *reducibility* to impose boundedness of forms. Furthermore reduced forms are reversible: if (m,ν,m') is a reduced form so is (m',ν,m''). This leads to periodicity. The Gauss reduction condition is in terms of the roots of the quadratic form. On the other hand the *best* forms of the *Chakravāla* algorithm are also reduced (Theorem 4.6 and Corrolary 4.7). We shall see in the following that the *Chakravāla* algorithm is also produced by $SL(2,\mathbb{Z})$ action supplemented by the *best* condition. We shall also see that the *best* condition is equivalent to a condition on roots of the quadratic form (but different from those of Gauss). The best forms are bounded and periodic, and the action of the modular group on the roots leads to periodic semi-regular continued fractions. The modular group action and the *Chakravāla* periodic semi-regular continued fractions lead to automorphisms of the quadratic form. Each such automorphism (automorph) gives (as in the classical theory of Gauss) a a solution of the Brahmagupta-Fermat-Pell equation. The solution obtained at the end of the first cycle is fundamental: it is positive and least. This is proved in Proposition 5.12. The tranformation to regular continued fractions turns out to be unnecessary. This transformation is also given for completeness but the periods are much longer than those of the semiregular continued fractions.

Remark: In the following we use the terms steps and best forms equivalently.

The quadratic form can be represented by the matrix

$$Q_n = \begin{pmatrix} m_n & \nu_n \\ \nu_n & m_{n+1} \end{pmatrix} \tag{5.2}$$

whence the determinant of the form is $\det(Q_n) = m_n m_{n+1} - \nu_n^2 = -D$, showing that the form is indefinite. The number $D > 0$ is not a square and is fixed. Since the coefficients are integers with uniform bounds (Theorem 4.9) , the number of possible forms (m_n, ν_n, m_{n+1}) of fixed discriminant is finite. Therefore the successive forms eventually repeat themselves. We have proved earlier (Theorem 4.6) that every best form ($\equiv$ *step*)

arising in the Chakravala process is reduced. This leads (Theorem 4.8) to finite sequences which are cyclical.

5.1 Action of the modular group $SL(2,Z)$ on $steps \equiv best\ forms$

Let (a,b,c) with integer entries represent the quadratic form

$$Q(a,b,c) = ax^2 + 2bxy + cy^2 \tag{5.3}$$

Then $Q(a,b,c)$ can be represented by the matrix

$$Q(a,b,c) = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \tag{5.4}$$

with

$$\Delta(Q) = -4\det Q = 4(b^2 - ac) = 4D \tag{5.5}$$

The matrix $M \in SL(2,Z)$

$$M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{5.6}$$

with

$$\det M = \alpha\delta - \beta\gamma = 1$$

acts on the form (a,b,c)

$$(a,b,c) \to (a',b',c') \tag{5.7}$$

by its action on the on the matrix Q representing the quadratic form

$$Q(a,b,c) \to Q'(a',b'c') = M^T Q(a,b,c) M = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} \tag{5.8}$$

with transformed coefficients

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \tag{5.9}$$

$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta \tag{5.10}$$

$$c' = a\beta^2 + 2b\delta\beta + c\delta^2 \tag{5.11}$$

By computation we find that the discriminant $\Delta(Q')$ of Q' satisfies

$$\Delta(Q') = (\alpha\delta - \beta\gamma)^2\Delta(Q) = \Delta(Q) \tag{5.12}$$

so that modular transformations leaves the discriminant invariant.

Right neighbouring forms

Definition 5.0: Following Dirichlet ([D], page 107) we will say that (a, b, c) has a right neighboring form (a', b', c') if the following three conditions are satisfied : that the discriminant is the same, that $a' = c$ and $b' \equiv -b \pmod{a'}$. The last condition means that $b + b'$ is divisible by a'. In other words that for an integer δ we have $b + b' = -a'\delta$. These conditions are fulfilled by the choice of the modular transformation S_δ below.

Let δ be an integer. Consider the $SL(2, \mathbb{Z})$ matrix

$$S_\delta = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix} \tag{5.13}$$

Under the transformation $S_\delta : \ (a, b, c) \to (a', b', c')$
we get

$$a' = c, \ b' = -b - c\delta, \ c' = a + 2b\delta + c\delta^2$$

We thus have the map after re-labelling

$$S_\delta : \ (a, b, a') \to (a', b', a'')$$

where

$$b' = -b - a'\delta, \ a'' = a + 2b\delta + a'\delta^2 \tag{5.14}$$

Thus (a', b', a'') is a right neighbouring form of (a, b, a').

5.2 Modular transformations of steps/best forms to steps/best forms..

The previous developments ((5.13) - (5.14)) apply directly to a *Chakravāla* step (m, ν, m') considered as a best form. Under the modular transformation S_δ given by (5.13) we have

$$S_\delta : (m, \nu, m') \to (m', \nu', m'') \tag{5.15}$$

where S_δ is the matrix

$$S_\delta = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix} \tag{5.16}$$

We identify (a, b, a') with (m, ν, m') and (a', b', a'') with (m', ν, m''). Then from (5.14) we get

$$\frac{\nu + \nu'}{m'} = -\delta \tag{5.17}$$

Since δ is an integer this means

$$\nu' \equiv -\nu \,(\mathrm{mod}\, m') \tag{5.18}$$

Moreover we obtain from (5.14), the above identification and (5.17)

$$m'' = m - \frac{\nu + \nu'}{m'}(\nu - \nu') \tag{5.19}$$

From (5.19) and $mm' = \nu^2 - D$ since (m, ν, m') is a step, we get

$$m'' = \frac{\nu^2 - D}{m'} \tag{5.20}$$

(5.20) also follows from the fact that the discriminant is left invariant under modular transformations:

$$\nu^2 - mm' = \nu'^2 - m'm'' = D \tag{5.21}$$

The form (m', ν', m'') is a right neighbour of the step according to Definition 5.0 and thus $\nu' = -\nu - m'\delta$ for any integer δ. *We now pick this integer δ by demanding that ν' is best (mod m') (see Definition 4.1).* In other words, ν' is nearest to ν in the $|\cdot|$ norm in the congruence class mod (m'). This ensures that the right neighbour (m', ν', m'') is a *Successor Step* of the *Chakravāla* algorithm and thus *reduced* by Theorem 4.6. However *the choice of δ is not unique so that there may be more than one successor step.* To see this, remark that

$$\delta = -\frac{\nu + \nu'}{m'}$$

and two choices of ν' may be equally best (mod m') as shown earlier.

We now give an equivalent condition in terms of the roots of quadratic forms for a right neighbour of the Chakravala step (as defined above) to be a successor step (and thus a reduced step).

We consider the roots of the quadratic form (m, ν, m')

$$m\omega^2 + 2\nu\omega + m' = 0 \tag{5.22}$$

The roots are

$$\omega = \frac{-\nu \pm \sqrt{D}}{m} \tag{5.23}$$

Define

$$\omega_+ = \frac{-\nu + \sqrt{D}}{m} \tag{5.24}$$

to be the first or *principal* root.

Proposition 5.1: Let (m, ν, m') be a quadratic form. Assume $D > 0$ is a non-square integer, $\nu > 0$ is an integer and $|m| < \sqrt{D}$. Then the condition ν is *best* (mod m) (see Definition 4.1) is equivalent to the condition that the principal root $|\omega_+| < 1$.

Proof: ν is best (mod m) implies that $|\nu^2 - D|$ is least in the congruence class (mod m). Assume $|m| < \sqrt{D}$. Then ν is ν_1 or ν_2 where

$$0 < \nu_1 < \sqrt{D} < \nu_2 = \nu_1 + |m| \tag{5.25}$$

Suppose $\nu = \nu_1$. Then

$$0 < \nu < \sqrt{D} < \nu + |m| \tag{5.26}$$

Therefore

$$|\omega_+| = \frac{|-\nu + \sqrt{D}|}{|m|} < \frac{|m|}{|m|} = 1 \tag{5.27}$$

Suppose $\nu = \nu_2$. Then

$$\nu - |m| < \sqrt{D} < \nu \tag{5.28}$$

or

$$0 < \nu - \sqrt{D} < |m| \tag{5.29}$$

Therefore

$$|\omega_+| = \frac{|\nu - \sqrt{D}|}{|m|} < \frac{|m|}{|m|} = 1 \tag{5.30}$$

Therefore in both cases $\nu = \nu_1$ or $\nu = \nu_2$ we have $|\omega_+| < 1$. Thus ν is best in the congruence class (mod m) $\Rightarrow |\omega_+| < 1$.

Conversely suppose $|\omega_+| < 1$. Therefore

$$|-\nu + \sqrt{D}| < |m| \tag{5.31}$$

Suppose $\nu < \sqrt{D}$. Then from (5.31)

$$0 < -\nu + \sqrt{D} < |m|$$

and hence

$$\nu < \sqrt{D} < \nu + |m| \tag{5.32}$$

Suppose $\nu > \sqrt{D}$. Then from (5.31) we have

$$0 < \nu - \sqrt{D} < |m|$$

and hence

$$\nu - |m| < \sqrt{D} < \nu \tag{5.33}$$

Therefore the condition $|\omega_+| < 1 \Rightarrow \nu$ is best mod m. This completes the proof that the condition $|\omega_+| < 1$ and the condition that ν is best in the congruence class (mod m) are equivalent. ∎

Corollary 5.2: The condition $|\omega_+| < 1$ implies that the form (m, ν, m') is *reduced*. For, Proposition 5.1 says that ν is best (mod m) and therefore (m, ν, m') is a step. Theorem 4.6 and its corollary then says this step is reduced and equivalently the form is reduced.

Remark 5.3: Comparison with Gauss reduction, see [D]

1. Besides the above reduction condition $|\omega_+| < 1$, we have trivially $|\omega_-| > 1$ where (using $\nu > 0$)

$$|\omega_-| = \frac{|\nu + \sqrt{D}|}{|m|} = \frac{\nu + \sqrt{D}}{|m|}$$

In fact since $|m| \leq \sqrt{D}$ (see Section 4) and $\nu > 0$ we have

$$|\omega_-| > \frac{\sqrt{D}}{\sqrt{D}} = 1$$

$|\omega_+| < 1$ and $|\omega_-| > 1$ are also two of the conditions of Gauss reduction (see Dirichlet-Dedekind [D] Chapter 4, §74). However, Gauss has a third condition, namely the roots ω_+ and ω_- have opposite signs. As a consequence in the Gauss reduction $0 < \nu < \sqrt{D}$. Furthermore, as a consequence for the Gauss reduced form (m, ν, m'), the outer members m, m' have opposite signs. In the *Chakravāla* reduction this third condition of Gauss (namely that the roots ω_+ and ω_- have opposite signs) is absent. In the Gauss theory a reduced form has exactly one reduced form as a right neighbour (see [D], §77). A *Chakravāla* reduced form has at least one and at most two reduced forms as right neighbour(s) (the latter case coresponds to twin successors of Section 4). As pointed out

there it is possible to encounter *local* splitting and merging of sequences (see Lemma 4.2 in Section 4 and the examples for $D = 29,\ 97,\ 58$ in section 3). However the solution of the Brahmagupta-Fermat-Pell equation remains the same (see later) for the complete cycles of the split/merged sequences.

Theorem 5.4:

Let (m, ν, m') be a *Chakravāla* step. Let S_δ be the modular map (5.15) and (5.13):

$$S_\delta :\ (m, \nu, m') \to (m', \nu', m'')$$

where S_δ is given by (5.13)

$$S_\delta = \begin{pmatrix} 0 & 1 \\ -1 & \delta \end{pmatrix} \tag{5.34}$$

where δ is an integer. The map S_δ gives (m', ν', m'') as a right neighbour with $\nu' = -\nu - m'\delta$.
Let ω'_+ be the principal root of

$$m'\omega'^2 + 2\nu'\omega' + m'' = 0$$

$$\omega'_+ = \frac{-\nu' + \sqrt{D}}{m'} \tag{5.35}$$

Then the right neighbour (m', ν', m'') with $\nu' = -\nu - m\delta$ is a step if and only if $|\omega'_+| < 1$. Then ν' is best (mod m') and this fixes the integer δ.
As a consequence by Theorem 4.6 the successor step (m', ν', m'') *is a* **reduced** *step i.e.* (m'', ν', m') *is also a step.*

Proof: The map S_δ is given by (5.15) et seq till (5.20). (m', ν', m'') is a right neighbour of the step (m, ν, m'). The latter being a step implies $|m| < \sqrt{D}$ and then Proposition 4.3 implies that $|m'| < \sqrt{D}$. As a right neighbour $\nu' \equiv -\nu$ (mod m'), and from the map S_δ we have $\nu' = -\nu - m'\delta$, where δ is the integer in S_δ Amongst all these ν' one is to be chosen as follows: Let ω'_+ be the principal root given by (5.35). Suppose $|\omega'_+| < 1$ Then by Proposition 5.1 (applied to ω'_+) , ν' is best (mod m'). Therefore (m', ν', m'') is a successor step and thus, by Theorem 4.6, is a reduced step. Conversely suppose (m', ν', m'') is a step. Then ν' is best (mod m'). Therefore by Proposition 5.1, $|\omega'_+| < 1$. ∎

5.3 Action of the modular group on roots of quadratic forms
If $Q(x, y) = ax^2 + 2bxy + cy^2$ and $Q'(x', y') = a'x'^2 + 2b'x'y' + cy'^2$ is its modular transform, then $Q(x, y) = Q'(x', y')$ identically. If Q is represented by the matrix in (5.4), then $Q' = M^T QM$ where M is given by (5.6). If $\xi = (x, y)$ represented as a column vector and $\xi' = (x', y')$, then $(\xi, Q\xi) = (\xi', Q'\xi')$. Hence $\xi = M\xi'$. Thus

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \tag{5.36}$$

Therefore

$$x = \alpha x' + \beta y',\ y = \gamma x' + \delta y' \tag{5.37}$$

whence

$$\frac{x}{y} = \frac{\alpha(\frac{x'}{y'}) + \beta}{\gamma(\frac{x'}{y'}) + \delta}$$

The roots ω, ω' of the quadratic forms $Q(x, y)$, $Q'(x', y')$ are just the values of the ratios $\frac{x}{y}$ and $\frac{x'}{y'}$ where these forms vanish. Therefore

$$\omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta} \tag{5.38}$$

Inverting this we get

$$\omega' = \frac{\delta\omega - \beta}{-\gamma\omega + \alpha} \tag{5.39}$$

Let ω_+, ω'_+ be the principal roots, where

$$\omega_+ = \frac{-b + \sqrt{D}}{a}$$

As a consequence of (5.39) we get

$$\omega'_+ = \frac{-b' + \sqrt{D}}{a'}$$

Thus principal roots are transformed to principal roots.

5.4 Action of modular group on roots of *Cakravāla* steps and semi-regular continued fractions

Let (m, ν, m') be a *Cakravāla* step. Let S_δ be the modular map (5.15):

$$S_\delta :\ (m, \nu, m') \to (m', \nu', m'')$$

(m, ν, m') is a step and therefore by Propsition 5.1, its principal root $|\omega_+| < 1$. By Theorem 5.2, (m', ν', m'') is a step if and only if its principal root satisfies $|\omega'_+| < 1$. Thus ω_+ and $|\omega'_+| < 1$ are proper fractions. Now specialising the action of the modular group on roots of quadratic forms given by (5.39) to S_δ we get

$$\omega_+ = \frac{1}{\delta - \omega'_+} \tag{5.40}$$

For $n \geq 0$ take the sequence of modular maps

$$S_{\delta_n} : (m_n, \nu_n, m_{n+1}) \to (m_{n+1}, \nu_{n+1}, m_{n+2}) \tag{5.41}$$

where

$$\delta_n = -\frac{\nu_n + \nu_{n+1}}{m_{n+1}} \tag{5.42}$$

and (m_n, ν_n, m_{n+1}) is a step and thus $|\omega_{+,n}| < 1$. Then $(m_{n+1}, \nu_{n+1}, m_{n+2})$ is a step $\iff$ $|\omega_{+,n+1}| < 1$. By Proposition 5.1, ν_{n+1} is best mod m_{n+1}. This fixes (but not uniquely) ν_{n+1} $(= -\nu_n \bmod m_{n+1})$. This fixes in turn the integer δ_n and thus the map S_{δ_n}. We now get from (5.40) with $\omega_+ = \omega_{+,n}$, $\omega'_+ = \omega_{+,n+1}$

$$\omega_{+,n} = \frac{1}{\delta_n - \omega_{+,n+1}} \tag{5.43}$$

Semi-Regular Continued Fraction (SRCF):

Henceforth we simplify notation by writing $\omega = \omega_+$ for the principal root. From (5.43) we have by iteration the continued fraction

$$\omega_n = \frac{1|}{|\delta_n} + \frac{-1|}{|\delta_{n+1}} + \frac{-1|}{|\delta_{n+2}} + ... \tag{5.44}$$

$$= \cfrac{1}{\delta_n + \cfrac{-1}{\delta_{n+1} + \cfrac{-1}{\delta_{n+2} + ...}}}$$

Proposition 5.5 :

The continued fraction given by (5.44) (starting with $n = 0$) can be transformed into a standard form of a *semi-regular continued fraction (SRCF)* (or $half - regular$ in the sense of Perron [P], Chapter 5, §35, page 149 et seq)

$$\omega_0 = \frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ...\frac{\varepsilon_n|}{|k_n} + ... \tag{5.45}$$

$$= \cfrac{\varepsilon_0}{k_0 + \cfrac{\varepsilon_1}{k_1 + \cfrac{\varepsilon_2}{k_2 + ...\cfrac{\varepsilon_n}{k_n + ...}}}}$$

where the integers

$$k_n = |\delta_n| \geq 2 \tag{5.46}$$

and the $\varepsilon_n = \pm 1$ are as follows:

$$k_n = |\delta_n|,\ \varepsilon_n = -(\text{sign}\ \delta_{n-1} \times \text{sign}\ \delta_n)1,\ \varepsilon_0 = (\text{sign}\ \delta_0)1 \tag{5.47}$$

$k_n \geq 2 \Rightarrow$

$$k_n + \varepsilon_{n+1} \geq 1 \tag{5.48}$$

and therefore the infinite irregular continued fraction (5.45) is a *Semi-Regular Continued Fraction (SRCF)*, (see Perron, [P], §35, page 149 et seq).

Remark: This may be called *Bhāskara's* continued fraction as it has been derived directly from his algorithm and should be distinguished from the NSCF in [A2]. We simply refer to it as the SRCF in the following.

Proof: We have $k_n = |\delta_n|$. Define $\varepsilon'_n = -\frac{|\delta_n|}{\delta_n} = -\frac{k_n}{\delta_n}$. Therefore $\varepsilon'_n = -\text{sign}\ \delta_n$. Now substituting $\delta_n = -\frac{k_n}{\varepsilon'_n}$ in (5.43) we get

$$\omega_n = \frac{-\varepsilon'_n}{k_n + \varepsilon'_n \omega_{n+1}} \tag{5.49}$$

We set $\varepsilon'_{-1} = 1$. Define $\varepsilon_n = -\varepsilon'_{n-1}\varepsilon'_n$. Then $\varepsilon_0 = -\varepsilon'_0$. We have

$$\varepsilon_n = -(\text{sign}\ \delta_{n-1} \times \text{sign}\ \delta_n)1,\ \varepsilon_0 = (\text{sign}\ \delta_o)1 \tag{5.50}$$

Now we obtain a recursion relation for the SRCF. From (5.49), multiplying both sides by ε'_{n-1} and setting

$$\xi_n = \varepsilon'_{n-1}\omega_n \tag{5.51}$$

we get

$$\xi_n = \frac{\varepsilon_n}{k_n + \xi_{n+1}} \tag{5.52}$$

with $\xi_0 = \omega_0$. Iterating (5.52) we have the complete quotient

$$\xi_n = \frac{\varepsilon_n|}{|k_n} + \frac{\varepsilon_{n+1}|}{|k_{n+1}} + \text{.....} \tag{5.53}$$

Starting from $n = 0$ we get the SRCF

$$\omega_0 = \xi_0 = \frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ... + \frac{\varepsilon_n|}{|k_n} + ... \tag{5.54}$$

Thus (5.45) and (5.47) have been proved. That $k_n \geq 2$ is the statement of Lemma 5.6 below and is proved in Appendix 3. The proof of Proposition 5.3 is complete. ∎

Lemma 5.6: Let (m, ν, m') and (m', ν', m'') be any two successive steps. By definition

$$\delta = -\frac{\nu + \nu'}{m'}$$

Define

$$k = |\delta| = \frac{\nu + \nu'}{|m'|}$$

Then

$$k \geq 2$$

The proof which depends on the fact that all steps are reduced (Theorem 4.6 and Corollary 4.7) is given in Appendix 3.

Proposition 5.7: A semi-regular continued fraction

$$\omega_0 = \frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ...\frac{\varepsilon_n|}{|k_n} + ... \tag{5.55}$$

where $\varepsilon_n = \pm 1$ and $k_n \geq 2$ converges.

Proof: This is the Tietze convergence theorem, given in Perron [P], Chapter 5, §35, page 149, Satz 1. This theorem was proved under the weaker condition $k_n \geq 1$, and $k_n + \varepsilon_{n+1} \geq 1$ for all $n \geq 0$. This condition is obviously satisfied if $k_n \geq 2$. The proof is quite easy under the condition $k_n \geq 2$ of Proposition 5.5 and we shall give it. To this end define the convergents

$$\frac{p_n}{q_n} = \frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ...\frac{\varepsilon_{n-1}|}{|k_{n-1}} \tag{5.56}$$

for all $n \geq 1$. Then p_n, q_n satisfy recurrence relations for all $n \geq 1$. These are conveniently written in matrix form

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} k_{n-1} & 1 \\ \varepsilon_{n-1} & 0 \end{pmatrix} \tag{5.57}$$

where $p_0 = 0$, $p_{-1} = 1$ and $q_0 = 1$, $q_{-1} = 0$. We obtain for $n \geq 1$,

whence

$$\frac{p_n}{q_n} = \frac{k_{n-1}p_{n-1} + \varepsilon_{n-1}p_{n-2}}{k_{n-1}q_{n-1} + \varepsilon_{n-1}q_{n-2}} \tag{5.58}$$

Iterating the matrix recurrence relation we get

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} k_0 & 1 \\ \varepsilon_0 & 0 \end{pmatrix} \begin{pmatrix} k_1 & 1 \\ \varepsilon_1 & 0 \end{pmatrix} ..... \begin{pmatrix} k_{n-1} & 1 \\ \varepsilon_{n-1} & 0 \end{pmatrix} \tag{5.59}$$

Taking determinants

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}\varepsilon_0\varepsilon_1....\varepsilon_{n-1} \tag{5.60}$$

Dividing both sides by $q_n q_{n-1}$ we get

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = (-1)^{n+1}\ \frac{\varepsilon_0\varepsilon_1....\varepsilon_{n-1}}{q_n q_{n-1}} \tag{5.61}$$

From the matrix recurrence relation we have for all $n \geq 1$,

$$q_n = k_{n-1}q_{n-1} + \varepsilon_{n-1}q_{n-2} \tag{5.62}$$

where $q_0 = 1,\ q_{-1} = 0$

Lemma 5.8: *q_n is a positive strictly monotonic increasing sequence.*

Proof: Assume $q_{n-1} > q_{n-2} > 0$. Then we have, using $k_n \geq 2$,

$$\begin{aligned} q_n - q_{n-1} &= (k_{n-1} - 1)q_{n-1} + \varepsilon_{n-1}q_{n-2} \\ &> (k_{n-1} - 1)q_{n-2} + \varepsilon_{n-1}q_{n-2} \\ &> q_{n-2} + \varepsilon_{n-1}q_{n-2} = (1 + \varepsilon_{n-1})q_{n-2} \geq 0 \end{aligned}$$

Therefore $q_n > q_{n-1} > 0$. For $n = 1$, $q_1 = k_0 \geq 2$ and therefore $q_1 > 0$. For $n = 2$,

$$\begin{aligned} q_2 - q_1 &= (k_1 - 1)q_1 + \varepsilon_1 \\ &\geq q_1 + \varepsilon_1 = k_0 + \varepsilon_1 > 0 \end{aligned}$$

Therefore by induction for all $n \geq 1$ we have $q_n > q_{n-1} > 0$ for all $n \geq 1$. ∎

Let $m \geq 1$ be any fixed integer. From (5.61) we have, by using a telescopic sum and that q_n is strictly monotonic increasing,

$$\left|\frac{p_{n+m}}{q_{n+m}} - \frac{p_n}{q_n}\right| \leq \sum_{j=1}^{m}\left|\frac{p_{n+j}}{q_{n+j}} - \frac{p_{n+j-1}}{q_{n+j-1}}\right| \leq \sum_{j=1}^{m} \frac{1}{q_{n+j}q_{n+j-1}} \leq \frac{m}{q_{n+1}q_n} \tag{5.63}$$

Since $q_n > 0$ is strictly monotonic increasing, we have $q_n \to \infty$ as $n \to \infty$ and hence

$$\Big|\frac{p_{n+m}}{q_{n+m}} - \frac{p_n}{q_n}\Big| \to 0$$

Therefore $\{\frac{p_n}{q_n}\}$ is a Cauchy sequence and thus converges. The limit defines ω_0. ∎

Lemma 5.9: For $n \geq 1$ we have

$$q_n \geq n \tag{5.64}$$

Proof: The conditions of Satz 1 in the convergence theorem of Perron [P], Chapter 5, §35, page 149, are true here because $k_n \geq 2$. The lemma follows from equations (9) and (10) on page 151 of [P]. ∎

Remark: A simple inductive proof of (5.64) is given by A. Offer in his Lemma 6 , [O].

In a semi-regular continued fraction the convergents do not have a fixed sign. Therefore it is useful for later purposes (see the proof of Proposition 5.12) to have a uniform bound.

Lemma 5.10: The sequence of convergents $\{\frac{p_n}{q_n}\}$ *is uniformly bounded* :

Proof: From (5.61),

$$\frac{p_n}{q_n} = \sum_{j=1}^{n} (-1)^{j+1} \, \frac{\varepsilon_0 \varepsilon_1 .... \varepsilon_{j-1}}{q_j q_{j-1}} \tag{5.65}$$

Using the bound (5.64) in Lemma 5.9, we have that the sequence $\{\frac{p_n}{q_n}\}$ is uniformly bounded above by

$$|\frac{p_n}{q_n}| \leq 1 + \frac{1}{2} + \sum_{j=3}^{n} \frac{1}{q_{j-1}^2} < 1 + \frac{1}{2} + \sum_{j=2}^{\infty} \frac{1}{j^2} = \frac{1}{2} + \zeta(2) \tag{5.66}$$

where ζ is the Riemann zeta function and $\zeta(2) = \frac{\pi^2}{6}$. ∎

Remark: (5.66) is a very rough bound as it ignores all cancellations, but it suffices for our purpose as we shall see later. In practice, it is seen that $|\frac{p_n}{q_n}|$ is a proper fraction less than 1, and this may seem intuitively obvious since we are approximating an irrational ω_0 and $|\omega_0| < 1$. See the examples at the end of this section.

Periodicity:

The SRCF of the *Chakravāla* algorithm is periodic because it corresponds to a reduced step cycle with period length $2r$ (Theorem 4.8). Therefore $\delta_{n+2r} = \delta_n$ which implies $k_{n+2r} = k_n$. Moreover $\varepsilon'_{n+2r} = \varepsilon'_n$ and hence $\varepsilon_{n+2r} = \varepsilon_n$. We thus have in a period of length $2r$

$$\omega_0 = \star \frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ... \frac{\varepsilon_{2r-1}|}{|k_{2r-1}} \star + \tag{5.67}$$

The asterisks mark the beginning and end of a cycle. Within this cycle of period $2r$ we may have a cycle of shorter period. An argument in [D], §83, page 140, shows that the case that the SRCF period is shorter than the step period $2r$ can only occur if r is odd. We have as illustrated below

$$\varepsilon_{2r+i} = \varepsilon_i, \;\; k_{2r+i} = k_i : \; \forall i \geq 0 \tag{5.68}$$

Moreover if in addition r is odd and only if r is odd

$$k_{r+i} = k_i, \; \varepsilon_{r+i} = \varepsilon_i : \; \forall i \geq 0$$

Additional symmetries follow from a generalisation to SRCF of the Galois theorem on inverse periodicity for RCF (regular continued fractions) given in Perron ([P], §23, Satz 6, page 83 and §24, page 87)

Lemma 5.11: *Generalized Galois inverse periodicity for SRCF*:
We have

$$\zeta_0 = \sqrt{D} + \nu_0 = 2\nu_0 + \omega_0 = 2\nu_0 + \star \frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ... \frac{\varepsilon_{2r-2}|}{|k_{2r-2}} + \frac{\varepsilon_{2r-1}|}{|k_{2r-1}} \star \tag{5.69}$$

On the other hand by inverse periodicity we get

$$= k_{2r-1} + \star \frac{\varepsilon_{2r-1}|}{|k_{2r-2}} + \frac{\varepsilon_{2r-2}|}{|k_{2r-3}} + ... + \frac{\varepsilon_1|}{|k_0} + \frac{\varepsilon_0|}{|k_{2r-1}} \star \tag{5.70}$$

Proof: This is given in Appendix 4. ∎

From (5.69) and (5.70) we have the following Galois symmetry relations

$$\varepsilon_i = \varepsilon_{2r-1-i} : \; 0 \leq i \leq 2r-1 \tag{5.71}$$

$$k_i = k_{2r-2-i} : \; 0 \leq i \leq 2r-2 \tag{5.72}$$

$$k_{2r-1} = 2\nu_0 \tag{5.73}$$

As an immediate consequence of (5.71), we see that the sequence $\varepsilon_0, \varepsilon_1, ..., \varepsilon_{2r-1}$ can be written as

$$\varepsilon_0, \varepsilon_1, ..., \varepsilon_{r-1}, \varepsilon_{r-1}, \varepsilon_{r-2}, ..., \varepsilon_1, \varepsilon_0$$

Therefore,

$$\varepsilon_0\varepsilon_1.....\varepsilon_{2r-1} = \varepsilon_0^2\varepsilon_1^2.....\varepsilon_{r-1}^2 = 1 \tag{5.74}$$

a result we shall use afterwards.

5.5 Solving the Brahmagupta-Fermat-Pell equation

As shown earlier an $SL(2,\mathbb{Z})$ transformation has a natural action on a quadratic form and therefore on its (principal) roots:

$$\omega \to \omega'$$

$$\omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta} \tag{5.75}$$

where

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2,\mathbb{Z}) \tag{5.76}$$

The $SL(2,\mathbb{Z})$ automorhisms of the quadratic form form a subgroup. Each element of this subgroup has been baptised an *automorph*. Let S_A be an automorph. Then under S_A we have $\omega \to \omega$:

$$\omega = \frac{\alpha\omega + \beta}{\gamma\omega + \delta} \tag{5.77}$$

It is shown in [D, Chapter 4, §62] that there is a $1-1$ correspondence between such automorphs and solutions of the Brahmagupta-Fermat-Pellian equation. The periodicity of the SRCF (5.67) provides us with such an automorph, and thus a solution of the Brahmagupta-Fermat-Pell equation as we will now see. From (5.67) we have

$$\omega_0 = \frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ...\frac{\varepsilon_{2r-1}|}{|(k_{2r-1} + \omega_0)} \tag{5.78}$$

From (5.58) we have

$$\frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ...\frac{\varepsilon_{2r-1}|}{|k_{2r-1}} = \frac{k_{2r-1}p_{2r-1} + \varepsilon_{2r-1}p_{2r-2}}{k_{2r-1}q_{2r-1} + \varepsilon_{2r-1}q_{2r-2}} \tag{5.79}$$

Now $p_{2r-1}, p_{2r-2}, q_{2r-1}, q_{2r-2}$ are independent of k_{2r-1}. Therefore

$$\omega_0 = \frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ...\frac{\varepsilon_{2r-1}|}{|(k_{2r-1} + \omega_0)} = \frac{(k_{2r-1} + \omega_0)p_{2r-1} + \varepsilon_{2r-1}p_{2r-2}}{(k_{2r-1} + \omega_0)q_{2r-1} + \varepsilon_{2r-1}q_{2r-2}} \tag{5.80}$$

In the previous equation we now use (see (5.58))

$$p_{2r} = k_{2r-1}p_{2r-1} + \varepsilon_{2r-1}p_{2r-2}$$
$$q_{2r} = k_{2r-1}q_{2r-1} + \varepsilon_{2r-1}q_{2r-2} \tag{5.81}$$

to get

$$\omega_0 = \frac{\omega_0 p_{2r-1} + p_{2r}}{\omega_0 q_{2r-1} + q_{2r}} \tag{5.82}$$

Claim

$$S_A = \begin{pmatrix} p_{2r-1} & p_{2r} \\ q_{2r-1} & q_{2r} \end{pmatrix} \in SL(2,\mathbb{Z}) \tag{5.83}$$

and therefore (5.82) is an automorph.

Proof: Since the entries are all integers we just have to verify that S_A is unimodular. From (5.60) and Lemma 5.11, (5.74) we have

$$\det S_A = p_{2r-1}q_{2r} - q_{2r-1}p_{2r} = -(-1)^{2r+1}\varepsilon_0\varepsilon_1...\varepsilon_{2r-1} = 1$$

which proves the claim. ∎

Let us write for ease of notation

$$S_A = \begin{pmatrix} p_{2r-1} & p_{2r} \\ q_{2r-1} & q_{2r} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{5.84}$$

which defines $\alpha, \beta, \gamma, \delta$, namely:

$$\alpha = p_{2r-1},\ \beta = p_{2r},\ \gamma = q_{2r-1},\ \delta = q_{2r} \tag{5.85}$$

From (5.82), and the identification (5.85) we get

$$\omega_0 = \frac{\alpha\omega_0 + \beta}{\gamma\omega_0 + \delta} \tag{5.86}$$

From (5.86) we derive

$$\gamma\omega_0^2 + (\delta - \alpha)\omega_0 - \beta = 0 \tag{5.87}$$

On the other hand, $\omega_0 = \omega_{+,0} = \frac{-\nu_0+\sqrt{D}}{m_0}$ is the principal root of the quadratic form (m_0, ν_0, m_1) where $m_0 = 1$. This is a properly primitive form (in the sense of Gauss,see [D], p 104) since its divisor $\sigma = \gcd(m_0, 2\nu_0, m_1) = 1$. We will compare (5.87) with

$$m_0\omega_0^2 + 2\nu_0\omega_0 + m_1 = 0 \tag{5.88}$$

Let u be an integer. The divisor $\sigma = 1$. Hence comparing (5.87) with (5.88) we get

$$\begin{aligned} \gamma &= m_0 u, \\ \delta - \alpha &= 2\nu_0 u, \\ \beta &= -m_1 u \end{aligned} \tag{5.89}$$

We get

$$\delta + \alpha == 2\delta - (\delta - \alpha) = 2\delta - 2\nu_0 u = \text{even integer}$$

Therefore

$$\delta + \alpha = 2t \tag{5.90}$$

where $t =$ integer. From (5.90) and (5.89) we get

$$\begin{aligned} \alpha &= t - \nu_0 u \\ \delta &= t + \nu_0 u \\ \beta &= -m_1 u \\ \gamma &= m_0 u \end{aligned} \tag{5.91}$$

Now use $\alpha\delta - \beta\gamma = 1$. Then from (5.91) we get

$$t^2 - (\nu_0^2 - m_0 m_1)u^2 = 1 \tag{5.92}$$

From the definition of m_1 we have

$$\nu_0^2 - m_0 m_1 = D$$

Therefore

$$t^2 - Du^2 = 1 \tag{5.93}$$

which is the Brahmagupta-Fermat- Pellian equation.

Remark: (5.91) and (5.93) figure in [D], (§62, page 105) , with notational differences and taking account that in our case $\sigma = 1$. These results are due to Gauss (G-DA, §162).

Finally, from (5.91) and the identification (5.85) we get

$$\begin{aligned} p_{2r-1} &= \alpha = t - \nu_0 u \\ p_{2r} &= \beta = -m_1 u \\ q_{2r-1} &= \gamma = m_0 u \\ q_{2r} &= \delta = t + \nu_0 u \end{aligned} \tag{5.94}$$

Since $m_0 = 1$, (5.94) $\Rightarrow$

$$\begin{aligned} u &= q_{2r-1} \\ t &= p_{2r-1} + \nu_0 q_{2r-1} \end{aligned} \tag{5.95}$$

which solves the Brahmagupta-Fermat-Pell equation $t^2 - Du^2 = 1$ from the convergent $\frac{p_{2r-1}}{q_{2r-1}}$ of the SRCF for a full period $2r$.

Fundamental solution:

Proposition 5.12: The solution of the Brahmagupta-Fermat-Pell equation $t^2 - Du^2 = 1$ given by the *Chakravāla* algorithm at the end of the first cycle is fundamental, i.e. it is positive and the least of all the other solutions given at the end of successive cycles.

Proof: The solution is given by (5.95). First we show that the solution is positive for non-square $D \geq 7$. Then we lift this restriction. Observe that

$$u = q_{2r-1} > 0$$

.
On the other hand

$$t \geq q_{2r-1}\Big(\nu_0 - |\frac{p_{2r-1}}{q_{2r-1}}|\Big)$$

From (5.66) of Lemma 5.10 we have the estimate

$$|\frac{p_{2r-1}}{q_{2r-1}}| < \frac{1}{2} + \zeta(2)$$

Now $\zeta(2) = \frac{\pi^2}{6} = 1.644934.....$ It is easily seen that since for $D \geq 7$, $\nu_0 \geq 3$ we have

$$t > 3 - \frac{1}{2} - \frac{\pi^2}{6} > 0$$

For $D = 2, 5, 6$ the partial quotients are positive and therefore $t > 0$ together with $u > 0$. For $D = 3$, $\nu_0 = 2$. Explicit computation (see later) shows $|\frac{p_{2r-1}}{q_{2r-1}}| < 1$. . Therefore $u > 0$, and $t > 0$ for all non-square $D > 0$.

Next we show that this solution is the least. Suppose we have performed n cycles. This corresponds to a period $2nr$. Let u_n, t_n be the solution after n cycles. We have

$$\begin{aligned} u_n &= q_{2nr-1} \\ t_n &= p_{2nr-1} + \nu_0 q_{2nr-1} \end{aligned} \tag{5.96}$$

By the previous argument we have $u_n > 0$ and $t_n > 0$ for $D \geq 7$. For $D = 2, 5, 6$ the partial quotients are positive and therefore $u_n > 0$, $t_n > 0$. For $D = 3$ we have $\nu_0 = 2$ and the

Claim below proves $|\frac{p_{2nr-1}}{q_{2nr-1}}| < 1$ for all $n \geq 1$. Therefore for all non-square $D \geq 2$ we have $u_n > 0$, $t_n > 0$ which establishes that the solutions after each cycle remain positive. Now $u_n = q_{2nr-1}$ is strictly monotonic increasing with increasing n by Lemma 5.8. Moreover the equation $t_n^2 = Du_n^2 + 1$ implies then that t_n is strictly monotonic increasing. Therefore, of this infinite set of solutions, the solution u_1, t_1 after the first cycle is the least and positive. It is thus the fundamental solution. ∎

Let $(t_1, u_1) = (t_D, u_D)$ be the above fundamental solution. Then all the solutions (t_j, u_j), $j \geq 1$, are generated by the composition law of Proposition 1.2 :

$$t_j + u_j\sqrt{D} = (t_D + u_D\sqrt{D})^j$$

.
That these give all the solutions and there are no others was proved in Proposition 1.3.

We will now prove the Claim that was made above.

Claim: For $D = 3$ and all $n \geq 1$ we have $|\frac{p_{2nr-1}}{q_{2nr-1}}| < 1$.

Proof: For $D = 3$ we have $\nu_0 = 2$. From the algorithm we have the period length $2r = 2$ and

$$\omega_0 = \star\frac{-1|}{|4} + \frac{-1|}{|4}\star \tag{5.97}$$

Now $2(n+1)r - 2nr = 2r = 2$. Therefore

$$\frac{p_{2(n+1)r-1}}{q_{2(n+1)nr-1}} = \frac{-1|}{|4} + \frac{-1|}{|4} + \frac{p_{2nr-1}|}{|q_{2nr-1}}$$

whence

$$\frac{p_{2(n+1)r-1}}{q_{2(n+1)r-1}} = -\frac{(4q_{2nr-1} + p_{2nr-1})}{15q_{2nr-1} + 4p_{2nr-1}} \tag{5.98}$$

Assume for $n \geq 1$ that

$$|\frac{p_{2nr-1}}{q_{2nr-1}}| < 1 \tag{5.99}$$

That this assumption is true for $n = 1$ is seen below.
Then from (5.98) we get

$$|\frac{p_{2(n+1)r-1}}{q_{2(n+1)r-1}}| < \frac{4 + |\frac{p_{2nr-1}}{q_{2nr-1}}|}{15 - 4|\frac{p_{2nr-1}}{q_{2nr-1}}|} < \frac{5}{11} < 1 \tag{5.100}$$

From (5.97) we have for $n=1$, $|\frac{p_{2r-1}}{q_{2r-1}}| = |\frac{p_1}{q_1}| = \frac{1}{4} < 1$. Therefore by induction we have for all $n \geq 1$,

$$|\frac{p_{2nr-1}}{q_{2nr-1}}| < 1 \tag{5.101}$$

and the claim has been proved. ∎

A number of examples are given below.

Remark 5.8: From SRCF to RCF

We have seen how from the penultimate convergent at the end of the first full period of the SRCF (corresponding to the Chakravāla cycle) we get the fundamental solution of the Brahmagupta-Fermat-equation. Fundamental solutions can of course also be obtained by converting the SRCF to an RCF (regular continued fraction) where all the partial quotients have +1 as numerator. The RCF has only positive partial quotients and has an increased (even) period length (see below) This accounts for the fact that the computations are longer. Although from the point of view of the *Chakravāla* algorithm this is unnecessary we nevertheless give this transformation for the sake of comparison.

To do this we perform the transformation $\mathcal{T}_1$ of Perron ([P], §37, page 159 et seq) for the SRCF (5.67)

$$\sqrt{D} = \nu_0 + \omega_0 = \nu_0 + \star\frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ...\frac{\varepsilon_{2r-1}|}{|k_{2r-1}} \star + \tag{5.102}$$

The transformation $\mathcal{T}_1$ consists in the following:
Before each partial quotient with ε_j negative insert $\frac{1|}{|1}$ and replace all minus signs by plus. Change the denominators k_j of the partial quotients as follows:

$$\begin{cases} k_j \to k_j : & \text{if } \varepsilon_j = +1, \varepsilon_{j+1} = +1 \\ k_j \to k_j - 1 : & \text{if } \varepsilon_j = +1, \varepsilon_{j+1} = -1 \text{ or } \varepsilon_j = -1, \varepsilon_{j+1} = +1 \\ k_j \to k_j - 2 : & \text{if } \varepsilon_j = -1, \varepsilon_{j+1} = -1. \end{cases} \tag{5.103}$$

Moreover for the cases $\varepsilon_0 = \pm 1$, ν_0 is either unchanged or $\nu_0 \to \nu_0 - 1$ as defined below.

Period of RCF:

Let $\varepsilon_0, \varepsilon_1, ..., \varepsilon_{2r-1}$ be the partial numerators of the SRCF. $2r$ is the length of the full period of the SRCF. Let $\eta = \sharp\{j : \varepsilon_j = -1\}$. Then η is even. It is easy to show that the length of the full period of the RCF is $2r + \eta = 2\rho$.

Remark: This accounts for the fact that the number of steps in the computation of SRCF

convergents is less than those of the corresponding RCF.

Under the transformation $\mathcal{T}_1$ the expression (5.67) for the principal root ω_0 given by a SRCF is now transformed to its RCF and ν_0 changed to ν_0'

$$\mathcal{T}_1 : \sqrt{D} = \nu_0 + \omega_0 = \nu_0' + \omega_0\Big|_{RCF} \tag{5.104}$$

where $\nu_0' = \nu_0$ if $\varepsilon_0 = 1$ and $\nu_0' = \nu_0 - 1$ if $\varepsilon_0 = -1$, and

$$\omega_0\Big|_{RCF} = \star\frac{1|}{|\kappa_0} + \frac{1|}{|\kappa_1} + \frac{1|}{|\kappa_2} + ...\frac{1|}{|\kappa_{2\rho-1}} \star + \tag{5.105}$$

The $\kappa_j \geq 1$ are the integers obtained in the $\mathcal{T}_1$ transformation above.

Claim: ν_0' is the integer part of $\sqrt{D}$.

Proof :Recall that ν_0 is the integer such that ν_0^2 is nearest to D in absolute value in the congruence class (mod 1) (see Definition 4.1 and(4.1), (4.2) with $m_0 = 1$) From its definition (see (5.47) together with $\delta_0 = -\frac{\nu_0+\nu_1}{m_1}$, and $m_1 = \nu_0^2 - D$, we have $\varepsilon_0 = (\text{sign}\delta_o)1 = (-\text{sign}(\nu_0^2 - D))1$. Therefore if $\varepsilon_0 = 1$ then $\nu_0^2 < D$ and nearest to it in which case $\nu_0' = \nu_0$, is the integer part of $\sqrt{D}$. If $\varepsilon_0 = -1$ then $\nu_0^2 > D$ and nearest to it. Hence $(\nu_0 - 1)^2 < D$ and nearest to it. Therefore $\nu_0' = \nu_0 - 1$ is the integer part of $\sqrt{D}$. ∎

We define the convergents of the RCF

$$\frac{P_j}{Q_j} = \frac{1|}{|\kappa_0} + \frac{1|}{|\kappa_1} + \frac{1|}{|\kappa_2} + ...\frac{1|}{|\kappa_{j-1}}$$

P_J, Q_j satisfy the recurrence relation (5.58) where we set all $\varepsilon_j = 1$. In particular

$$P_n = \kappa_{n-1}P_{n-1} + P_{n-2},\ \ Q_n = \kappa_{n-1}Q_{n-1} + Q_{n-2} \tag{5.106}$$

where $P_0 = 0, P_{-1} = 1$, and $Q_0 = 1, Q_{-1} = 0$. Moreover $\kappa_j \geq 1$. Therefore $Q_n \geq Q_{n-1} + Q_{n-2}$, whence $Q_n > Q_{n-1} > 0$. Whence $Q_n \geq 2Q_{n-2}$, and by iteration $Q_{2n} \geq 2^n Q_0 = 2^n$and similarly $Q_{2n+1} \geq 2^n Q_1 \geq 2^n$. Therefore $Q_n \geq 2^{\frac{n-1}{2}}$. As before the sequence $\{\frac{P_n}{Q_n}\}$ is uniformly bounded above by a constant and Cauchy:

$$|\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}| = \frac{1}{Q_{n-1}Q_n} \leq \frac{1}{2^{n-2}} \to 0$$

As a consequence $\frac{P_n}{Q_n} \to \omega_0$.

The solution of the Brahmagupta-Fermat-Pell equation is now obtained exactly as before ((5.78) et seq with obvious changes,($p_j \to P_j$ and $q_j \to Q_j$, $e_j = 1$, $k_j \to \kappa_j$) but now from the convergent $\frac{P_{2\rho-1}}{Q_{2\rho-1}}$ of the RCF which is the ratio of two positive integers. We have to replace (5.95) by

$$\begin{aligned} u &= Q_{2\rho-1} \\ t &= P_{2\rho-1} + \nu_0' Q_{2\rho-1} \end{aligned} \tag{5.107}$$

where $\nu_0' = \nu_0$ if $\varepsilon_0 = 1$ and $\nu_0' = \nu_0 - 1$ if $\varepsilon_0 = -1$. We have proved in the Claim above that ν_0' is the integer part of $\sqrt{D}$. This gives an explicitly positive solution of the Brahmagupta-Fermat-Pell equation from the convergent $\frac{P_{2\rho-1}}{Q_{2\rho-1}}$ of the RCF:

$$t^2 - Du^2 = 1 \tag{5.108}$$

For $n \geq 1$ define

$$\begin{aligned} u_n &= Q_{2n\rho-1} \\ t_n &= P_{2n\rho-1} + \nu_0' Q_{2n\rho-1} \end{aligned} \tag{5.109}$$

As before u_n is positive and strictly monotonic increasing with increasing n. The equation (5.108) then implies that t_n is positive and strictly monotonic increasing. Therefore u_1, t_1 is the fundamental solution. ∎

Remark: Ever since Lagrange the regular continued fraction for $\sqrt{D}$ has been used to prove the existence of fundamental solutions. But, in so far as the Chakravala algorithm is concerned, we have seen that this is not really necessary. The fact that at the end of the first *Chakravāla* cycle the solution is fundamental has been directly proved in Proposition 5.12 at the level of the SRCF which is the natural outcome of this algorithm seen as a reduction theory of quadratic forms.

The RCF solutions are illustrated for the cases $D = 67, 29, 97, 58, 13$ in the Examples 1, 3, 4, 5, 6 below.

Examples:
We consider some illustrative examples of the SRCF (specific to the *Chakravāla* algorithm) for $\omega_{+,0}$ which is the principal root of the form (m_0, ν_0, m_1). We give the corresponding fundamental solution of the Brahmagupta-Fermat equation from the convergent $\frac{p_{2r-1}}{q_{2r-1}}$, where $2r$ is the full period, from (5.95).

From the definition of $\omega_{+,0}$

$$\omega_{+,0} = \frac{-\nu_0 + \sqrt{D}}{m_0}$$

we have, since $m_o = 1$,

$$\sqrt{D} = \{\sqrt{D}\} + \omega_{+,0}$$

where $\{\sqrt{D}\} = \nu_0$, the integer nearest to $\sqrt{D}$ in absolute value in the congruence class (mod 1). [5]

Thus the SRCF of $\omega_{+,0}$ gives the SRCF of $\sqrt{D}$. These examples illustrate also the periodicity of the SRCF. The period length of the cycle is $2r$ which is also the period length of the continued fraction. But when r is odd the SRCF has within its period of length $2r$ a short period of length r in illustration of earlier remarks. We mark by asterisks the beginning and end of a cycle. For $D = 67$, $D = 29$, $D = 97$ and $D = 58$ we have for the SRCF the period length $2r$. For $D = 29$, $D = 97$ and $D = 58$ we have twin successors and local branching and joining as illustrated in Section 3. Correspondingly we will find two SRCF which at the end of the full cycle give the same fundamental solution of the Brahmagupta-Fermat-Pell equation. On the other hand, for $D = 61$, 13, 41 the SRCF have the short period length r. However for the solution of the Brahmagupta-Fermat-Pell equation we will need the full cycle with period $2r$. We point out that of the seven examples below of the SRCF corresponding to the cyclic algorithm, all agree with the NSCF computed by Ayyangar [A2] *except* for those corresponding to the cases $D = 29$, $D = 97$ and $D = 58$ where twin successors occur. In addition we illustrate for the cases $D = 67, 29, 97, 58, 13$, Perron's transformation of the SRCF to the RCF and the ensueing fundamental solution of the Brahmagupta-Fermat equation as explained in Remark 5.8. above. *To each twin SRCF ($D = 29, 97, 58$) corresponds an unique RCF.* Note also that if the period in the RCF is odd, then we must double it to get an even period because we are solving the positive, ($m = 1$), Brahmagupta-Fermat-Pell equation for which the period is even. We then see that the RCF even period is longer than for the SRCF, and sometimes much longer (see e.g example 4 below where the first SRCF period is 12 whereas for the RCF the first even period is 22. Computationaly, the SRCF is faster than the corresponding RCF.

In the following we compute in turn from the complete step cycle given by the cyclic algorithm, the integers $\delta_n = -\frac{\nu_n+\nu_{n+1}}{m_{n+1}}$, $k_n = |\delta_n|$, and $\varepsilon_n = -(\text{sign}\,\delta_n \times \text{sign}\,\delta_{n-1})1$ with $\varepsilon_0 = (\text{sign}\,\delta_0)1$. We will need the convergents

$$\frac{p_n}{q_n} = \frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ...\frac{\varepsilon_{n-1}|}{|k_{n-1}} \tag{5.110}$$

in particular when $n = 2r - 1$ for solving the Brahmagupta Fermat Pell equatuin (see (5.95)).

1. $D = 67$. $\{\sqrt{D}\} = \nu_0 = 8$. The step cycle is given by (2.4).

$$(1, 8, -3), (-3, 7, 6), (6, 5, -7), (-7, 9, -2); (-2, 9, -7), (-7, 5, 6), (6, 7, -3), (-3, 8, 1)$$

[5] ν_0 is *not* in general the same as $[\sqrt{D}]$ the integer part of $\sqrt{D}$.

The step period is $2r = 8$ and $r = 4$ is even. We now compute

$$\star\delta_0 = 5, \delta_1 = -2, \delta_2 = 2, \delta_3 = 9, \delta_4 = 2, \delta_5 = -2, \delta_6 = 5, \delta_7 = -16\star$$

$$k_0 = 5, k_1 = 2, k_2 = 2, k_3 = 9, k_4 = 2, k_5 = 2, k_6 = 5, k_7 = 16$$

$$\varepsilon_0 = 1, \varepsilon_1 = 1, \varepsilon_2 = 1, \varepsilon_3 = -1, \varepsilon_4 = -1, \varepsilon_5 = 1, e_6 = 1, \varepsilon_7 = 1$$

Therefore we obtain (writing ω_0 instead of $\omega_{0,+}$ for simplicity)

$$\sqrt{67} = 8 + \omega_0$$

where

$$\omega_0 = \star\frac{1|}{|5} + \frac{1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|9} + \frac{-1|}{|2} + \frac{1|}{|2} + \frac{1|}{|5} + \frac{1|}{|16}\star$$

after which the same sequence repeats itself. The SRCF period is $q = 2r = 8$. To obtain the solution of the Brahmagupta-Fermat equation we need the following convergent of ω_0:

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}} &= \frac{p_7}{q_7} \\ &= \frac{1|}{|5} + \frac{1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|9} + \frac{-1|}{|2} + \frac{1|}{|2} + \frac{1|}{|5} \\ &= \frac{1106}{5967}\end{aligned}$$

Thus $p_{2r-1} = 1106$ and $q_{2r-1} = 5967$. From (5.95) and $\nu_0 = 8$ we obtain

$$\begin{aligned}u &= q_{2r-1} = 5967, \\ t &= p_{2r-1} + \nu_0 q_{2r-1} = 1106 + 8 \times 5967 = 48842\end{aligned}$$

which gives the fundamental solution of the Brahmagupta-Femat equation

$$t^2 - 67u^2 = 1$$

Perron's transformation $\mathcal{T}_1$ of SRCF to RCF leads to

$$\sqrt{67} = 8 + \star\frac{1|}{|5} + \frac{1|}{|2} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|7} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|2} + \frac{1|}{|5} + \frac{1|}{|16}\star$$

The period of the RCF is $2\rho = 2r + \eta = 8 + 2 = 10$. We have the convergent $\frac{P_{2\rho-1}}{Q_{2\rho-1}} = \frac{1106}{5967}$. The solution of the Brahmagupta-Fermat equation $t^2 - 67u^2 = 1$ is given by

$$u = q_{2\rho-1} = 5967,$$
$$t = p_{2\rho-1} + \nu_0 q_{2\rho-1} = 1106 + 8 \times 5967 = 48842$$

as before.

2. D=61. $\{\sqrt{61}\} = \nu_0 = 8$. The step cycle is given by (3.20).

$$(1,8,3),(3,7,-4),(-4,9,-5),(-5,6,5),(5,9,4),(4,7,-3),(-3,8,-1);$$
$$(-1,8,-3),(-3,7,4),(4,9,5),(5,6,-5),(-5,9,-4),(-4,7,3),(3,8,1)$$

The step period length is $2r = 14$, and thus $r = 7$ which is odd. From this we compute

$$\delta_0 = -5, \delta_1 = 4, \delta_2 = 3, \delta_3 = -3, \delta_4 = -4, \delta_5 = 5, \delta_6 = 16,$$
$$\delta_7 = 5, \delta_8 = -4, \delta_9 = -3, \delta_{10} = 3, \delta_{11} = 4, \delta_{12} = -5, \delta_{13} = -16$$

from which we obtain

$$k_0 = 5, k_1 = 4, k_2 = 3, k_3 = 3, k_4 = 4, k_5 = 5, k_6 = 16;$$
$$k_7 = 5, k_8 = 4, k_9 = 3, k_{10} = 3, k_{11} = 4, k_{12} = 5, k_{13} = 16$$

$$\varepsilon_0 = -1, \varepsilon_1 = 1, \varepsilon_2 = -1, \varepsilon_3 = 1, \varepsilon_4 = -1, \varepsilon_5 = 1, \varepsilon_6 = -1;$$
$$\varepsilon_7 = -1, \varepsilon_8 = 1, \varepsilon_9 = -1, \varepsilon_{10} = 1, \varepsilon_{11} = -1, \varepsilon_{12} = 1, \varepsilon_{13} = -1$$

From the above we see that the step cycle period length is $2r = 14$ whereas the SRCF period length is $q = r = 7$ and thus shorter. We have

$$\sqrt{61} = 8 + \omega_0$$

where

$$\omega_0 = \star\frac{-1|}{|5} + \frac{1|}{|4} + \frac{-1|}{|3} + \frac{1|}{|3} + \frac{-1|}{|4} + \frac{1|}{|5} + \frac{-1|}{|16}\star$$

and for the full period $2r = 14$ we have

$$\omega_0 = \frac{-1|}{|5} + \frac{1|}{|4} + \frac{-1|}{|3} + \frac{1|}{|3} + \frac{-1|}{|4} + \frac{1|}{|5} + \frac{-1|}{|16} + \frac{-1|}{|5} + \frac{1|}{|4} + \frac{-1|}{|3} + \frac{1|}{|3} + \frac{-1|}{|4} + \frac{1|}{|5} + \frac{-1|}{|16}$$

To solve the Brahmagupta-Fermat equation using (5.95) we need the convergent

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}} &= \frac{p_{13}}{q_{13}}\\ &= \frac{-1|}{|5} + \frac{1|}{|4} + \frac{-1|}{|3} + \frac{1|}{|3} + \frac{-1|}{|4} + \frac{1|}{|5} + \frac{-1|}{|16} + \frac{-1|}{|5} + \frac{1|}{|4} + \frac{-1|}{|3} + \frac{1|}{|3} + \frac{-1|}{|4} + \frac{1|}{|5}\\ &= \frac{-42912791}{226153980}\end{aligned}$$

Thus $p_{2r-1} = p_{13} = -42912791$ and $q_{2r-1} = q_{13} = 226153980$. From $\nu_0 = 8$ and (5.95) we obtain

$$\begin{aligned}u &= q_{2r-1} = 226153980,\\ t &= p_{2r-1} + \nu_0 q_{2r-1} = -42912791 + 8 \times 226153980 = 1766319049\end{aligned}$$

which gives the fundamental solution of the Brahmagupta-Fermat equation

$$t^2 - 61u^2 = 1$$

3. $D = 29$. $\{\sqrt{D}\} = 5$. In section 3 we have seen that there are twin sequences which merge. On reversing the same phenomenon take place. We consider the ν_+ and ν_- cycles. To these correspond twin SRCF

$$\begin{aligned}29 &= 5 + \omega_{0,\nu_+}\\ 29 &= 5 + \omega_{0,\nu_-}\end{aligned}$$

of period length $2r = 8$.

ν_- cycle:

$$\begin{aligned}&(1, 5, -4), (-4, \nu_- = 3, 5), (5, \nu_+ = 7, 4), (4, 5, -1);\\ &(-1, 5, 4), (4, \nu_+ = 7, 5), (5, \nu_- = 3, -4), (-4, 5, 1)\end{aligned}$$

$$\delta_0 = 2, \delta_1 = -2, \delta_2 = -3, \delta_3 = 10, \delta_4 = -3, \delta_5 = -2, \delta_6 = 2, \delta_7 = -10$$

$$k_0 = 2, k_1 = 2, k_2 = 3, k_3 = 10, k_4 = 3, k_5 = 2, k_6 = 2, k_7 = 10$$

$$\varepsilon_0 = 1, \varepsilon_1 = 1, \varepsilon_2 = -1, \varepsilon_3 = 1, \varepsilon_4 = 1, \varepsilon_5 = -1, \varepsilon_6 = 1, e_7 = 1$$

$$\omega_{\nu_-} = \star\frac{1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|3} + \frac{1|}{|10} + \frac{1|}{|3} + \frac{-1|}{|2} + \frac{1|}{|2} + \frac{1|}{|10}\star$$

ν_+ cycle:

$$(1,5,-4),(-4,\nu_+=7,-5),(-5,\nu_-=3,4),(4,5,-1);$$
$$(-1,5,4),(4,\nu_-=3,-5),(-5,\nu_+=7,-4),(-4,5,1)$$

$$\delta_0=3,\delta_1=2,\delta_2=-2,\delta_3=10,\delta_4=-2,\delta_5=2,\delta_6=3,\delta_7=-10$$
$$k_0=3,k_1=2,k_2=2,k_3=10,k_4=2,k_5=2,k_6=3,k_7=10$$
$$\varepsilon_0=1,\varepsilon_1=-1,\varepsilon_2=1,\varepsilon_3=1,\varepsilon_4=1,\varepsilon_5=1,\varepsilon_6=-1,\varepsilon_7=1$$

whence

$$\omega_{\nu_+}=\star\frac{1|}{|3}+\frac{-1|}{|2}+\frac{1|}{|2}+\frac{1|}{|10}+\frac{1|}{|2}+\frac{1|}{|2}+\frac{-1|}{|3}+\frac{1|}{|10}\star$$

For the ν_- cycle, we have the convergent

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}}&=\frac{p_7}{q_7}\\&=\frac{1|}{|2}+\frac{1|}{|2}+\frac{-1|}{|3}+\frac{1|}{|10}+\frac{1|}{|3}+\frac{-1|}{|2}+\frac{1|}{|2}\\&=\frac{701}{1820}\end{aligned}$$

For ν_+ cycle , we have the convergent

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}}&=\frac{p_7}{q_7}\\&=\frac{1|}{|3}+\frac{-1|}{|2}+\frac{1|}{|2}+\frac{1|}{|10}+\frac{1|}{|2}+\frac{1|}{|2}+\frac{-1|}{|3}\\&=\frac{701}{1820}\end{aligned}$$

So for both cycles we have $p_{2r-1}=p_7=701$ and $q_{2r-1}=q_7=1820$. So from $\nu_0=5$ and (5.95) we have the common solution for the twin SRCF for $D=29$

$$\begin{aligned}u&=q_{2r-1}=1820,\\t&=p_{2r-1}+\nu_0 q_{2r-1}=701+5\times 1820=9801\end{aligned}$$

which gives the fundamental solution of the Brahmagupta-Fermat-Pell equation

$$t^2-29u^2=1$$

We now perform the Perron transformation (see Remark 5.8) $\mathcal{T}_1 : SRCF \to RCF$. For both the ν_- and ν_+ cycles we get the same RCF:

$$\sqrt{2}9 = 5 + \star\frac{1|}{|2} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|2} + \frac{1|}{|10} + \frac{1|}{|2} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|2} + \frac{1|}{|10}\star$$

The period of the RCF (see Remark 5.8) is $2\rho = 2r + \eta = 8 + 2 = 10$. Computation now gives for the convergent

$$\frac{P_{2\rho-1}}{Q_{2\rho-1}} = \frac{701}{1820} = \frac{p_{2r-1}}{q_{2r-1}}$$

Hence we get the same solution $u = 1820$, $t = 9801$ of the equation $u^2 - 29t^2 = 1$.

4. $D = 97$. $\{\sqrt{D}\} = \nu_0 = 10$. We have twin successors shown in Section 3. We consider the ν_+ and ν_- cycles given in (3.28) and (3.30). The period length is $2r = 12$. Correspondingly we have the SRCF

$$97 = 10 + \omega_{0,\nu_+}$$

$$97 = 10 + \omega_{0,\nu_-}$$

of period length $2r = 12$.

ν_- cycle:

$$(1, 10, 3), (3, 11, 8), (8, \nu_- = 5, -9), (-9, \nu_+ = 13, -8), (-8, 11, -3), (-3, 10, -1);$$

$$(-1, 10, -3), (-3, 11, -8), (-8, \nu_+ = 13, -9), (-9, \nu_- = 5, 8), (8, 11, 3), (3, 10, 1) \quad (5.111)$$

From this we have

$$\delta_0 = -7, \delta_1 = -2, \delta_2 = 2, \delta_3 = 3, \delta_4 = 7, \delta_5 = 20,$$

$$\delta_6 = 7, \delta_7 = 3, \delta_8 = 2, \delta_9 = -2, \delta_{10} = -7, \delta_{11} = -20$$

From this we have $k_n = |\delta_n|$. Next, we compute ε_n. Recall $\varepsilon_0 = \operatorname{sign}\delta_0$, $\varepsilon_n = -(\operatorname{sign}\delta_n) \times (\operatorname{sign}\delta_{n-1})$. Thus,

$$\varepsilon_0 = -1, \varepsilon_1 = -1, \varepsilon_2 = 1, \varepsilon_3 = -1, \varepsilon_4 = -1, \varepsilon_5 = -1$$

$$\varepsilon_6 = -1, \varepsilon_7 = -1, \varepsilon_8 = -1, \varepsilon_9 = 1, \varepsilon_{10} = -1, \varepsilon_{11} = -1$$

We have the SRCF corresponding to the ν_- cycle

$$\omega_{0,\nu_-} = \star\frac{-1|}{|7} + \frac{-1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|3} + \frac{-1|}{|7} + \frac{-1|}{|20} + \frac{-1|}{|7} + \frac{-1|}{|3} + \frac{-1|}{|2} +$$

$$+\frac{1|}{|2} + \frac{-1|}{|7} + \frac{-1|}{|20}\star$$

The SRCF period is $2r = 12$. We need the convergent $\frac{p_{2r-1}}{q_{2r-1}}$ in order to solve the Brahmagupta-Fermat equation.

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}} &= \frac{p_{11}}{q_{11}} \\ &= \frac{-1|}{|7} + \frac{-1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|3} + \frac{-1|}{|7} + \frac{-1}{|20} + \frac{-1|}{|7} + \frac{-1|}{|3} + \frac{-1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|7} \\ &= \frac{-963887}{6377352}\end{aligned}$$

ν_+ cycle:

$$(1,10,3),(3,11,8),(8,\nu_+ = 13,9),(9,\nu_- = 5,-8),(-8,11,-3),(-3,10,-1);$$

$$(-1,10,-3),(-3,11,-8),(-8,\nu_- = 5,9),(9,\nu_+ = 13,8),(8,11,3),((3,10,1) \qquad (5.112)$$

We have

$$\delta_0 = -7, \delta_1 = -3, \delta_2 = -2, \delta_3 = +2, \delta_4 = +7, \delta_5 = +20,$$

$$\delta_6 = +7, \delta_7 = +2, \delta_8 = -2, \delta_9 = -3, \delta_{10} = -7, \delta_{11} = -20$$

$k_n = |\delta_n|$ and the ε_n are as follows:

$$\varepsilon_0 = -1, \varepsilon_1 = -1, \varepsilon_2 = -1, \varepsilon_3 = 1, \varepsilon_4 = -1, \varepsilon_5 = -1,$$

$$\varepsilon_6 = -1, \varepsilon_7 = -1, \varepsilon_8 = 1, \varepsilon_9 = -1, \varepsilon_{10} = -1, \varepsilon_{11} = -1$$

This gives the SRCF corresponding to the ν_+ cycle:

$$\omega_{0,\nu_+} = \star\frac{-1|}{|7} + \frac{-1|}{|3} + \frac{-1|}{|2} + \frac{1|}{|2} + +\frac{-1|}{|7} + \frac{-1|}{|20} + \frac{-1|}{|7} + \frac{-1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|3} + \frac{-1|}{|7} + \frac{-1|}{|20}\star$$

We compute

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}} &= \frac{p_{11}}{q_{11}}\\ &= \frac{-1|}{|7} + \frac{-1|}{|3} + \frac{-1|}{|2} + \frac{1|}{|2} + + \frac{-1|}{|7} + \frac{-1|}{|20} + \frac{-1|}{|7} + \frac{-1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|3} + \frac{-1|}{|7}\\ &= \frac{-963887}{6377352}\end{aligned}$$

So for both ν_+ and ν_- cycles we have $p_{2r-1} = p_{11} = -963887$ and $q_{2r-1} = q_{11} = 6377352$. Hence from $\nu_0 = 10$ and (5.95) we have the common solution for $D = 97$

$$\begin{aligned}&u = q_{2r-1} = 6377352,\\ &t = p_{2r-1} + \nu_0 q_{2r-1} = -963887 + 10 \times 6377352 = 62809633\end{aligned}$$

This gives the fundametal solution of the Brahmagupta-Fermat-Pell equation

$$t^2 - 97u^2 = 1$$

We now perform the Perron transformation $\mathcal{T}_1 : SRCF \to RCF$ (see Remark 5.8) for both the ν_- and ν_+ cycles. The two RCF coincide and we get

$$\begin{aligned}\sqrt{97} = 9 + \star \frac{1|}{|1} + \frac{1|}{|5} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|5} + \frac{1|}{|1} + \frac{1|}{|18}\\ + \frac{1|}{|1} + \frac{1|}{|5} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|5} + \frac{1|}{|1} + \frac{1|}{|18} \star\end{aligned}$$

The period of the RCF is $2\rho = 2r + \eta = 12 + 10 = 22$. Clearly the period of the RCF is much longer than that of the SRCF and the number of steps to compute the convergents is much increased. Computation gives for the convergent

$$\frac{P_{2\rho-1}}{Q_{2\rho-1}} = \frac{5413465}{6377352}$$

.
whence (see Remark 5.8) we get

$$u = Q_{2\rho-1} = 6377352$$

and

$$t = P_{2\rho-1} + (\nu_0 - 1)Q_{2\rho-1} = 5413465 + 9 \times 6377352 = 62809633$$

which gives the same solution of the Brahmagupta-Fermat equation $u^2-97t^2=1$ as before.

5. $D=58$. $\{\sqrt{D}\}=\nu_0=8$. We have twin successors shown in Section 3, Example 3.5. We consider the ν_+ and ν_- cycles given in (3.32) and (3.33). The period length is $2r=8$. Correspondingly we have the SRCF

$$58=8+\omega_{0,\nu_+}$$

$$58=8+\omega_{0,\nu_-}$$

We compute as before the SRCF from the ν_- and ν_+ cycles. The SRCF corresponding to the ν_- cycle

$$\omega_{0,\nu_-}=\star\frac{-1|}{|2}+\frac{1|}{|2}+\frac{-1|}{|3}+\frac{-1|}{|16}+\frac{-1|}{|3}+\frac{-1}{|2}+\frac{1|}{|2}+\frac{-1|}{|16}\star$$

The SRCF period is $2r=8$. We need the convergent $\frac{p_{2r-1}}{q_{2r-1}}$.

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}}&=\frac{p_7}{q_7}\\&=\frac{-1|}{|2}+\frac{1|}{|2}+\frac{1|}{|3}+\frac{-1|}{|16}+\frac{-1|}{|3}+\frac{-1}{|2}+\frac{1|}{|2}\\&=\frac{-989}{2574}\end{aligned}$$

ν_+ cycle:

The SRCF corresponding to the ν_+ cycle:

$$\omega_{0,\nu_+}=\star\frac{-1|}{|3}+\frac{-1|}{|2}+\frac{1|}{|2}+\frac{-1|}{|16}+\frac{-1|}{|2}+\frac{1|}{|2}+\frac{-1|}{|3}+\frac{-1|}{|16}\star$$

We compute

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}}&=\frac{p_7}{q_7}\\&=\frac{-1|}{|3}+\frac{-1|}{|2}+\frac{1|}{|2}+\frac{-1|}{|16}+\frac{-1|}{|2}+\frac{1|}{|2}+\frac{-1|}{|3}\\&=\frac{-989}{2574}\end{aligned}$$

So for both ν_+ and ν_- cycles we have $p_{2r-1}=p_7=-989$ and $q_{2r-1}=q_7=2574$. Hence from $\nu_0=8$ and (5.95) we have the common solution for $D=58$

$$\begin{aligned}&u=q_{2r-1}=2574,\\&t=p_{2r-1}+\nu_0 q_{2r-1}=-989+8\times 2574=19603\end{aligned}$$

This gives the fundamental solution of the Brahmagupta-Fermat-Pell equation

$$t^2 - 58u^2 = 1$$

Perron's transformation $\mathcal{T}_1$ of the SRCF for the ν_+ and ν_- cycles to the RCF's (see Remark 5.8) lead to the *same* RCF

$$\sqrt{58} = 7 + \star\frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|14} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|14}\star$$

The period of the RCF is $2\rho = 2r + \eta = 8 + 6 = 14$. We have the convergent $\frac{p_{2\rho-1}}{q_{2\rho-1}} = \frac{1585}{2574}$. The solution of the Brahmagupta-Fermat equation $t^2 - 58u^2 = 1$ is given by

$$\begin{aligned} u &= Q_{2\rho-1} = 2574, \\ t &= P_{2\rho-1} + (\nu_0 - 1)Q_{2\rho-1} = 1585 + 7 \times 2574 = 19603 \end{aligned}$$

as before.

6. $D = 13$. $\{\sqrt{D}\} = \nu_0 = 4$. The step cycle is

$$(1, 4, 3), (3, 2, -3), (-3, 4, -1); (-1, 4, -3), (-3, 2, 3), (3, 4, 1)$$

The cycle period is $2r = 6$ and thus $r = 3$ which is odd. We obtain the SRCF by computing first

$$\delta_0 = -2, \delta_1 = 2, \delta_2 = 8, \delta_3 = 2, \delta_4 = -2, \delta_5 = -8$$

after which the sequence repeats itself. Taking absolute values we have the k_n

$$k_0 = 2, k_1 = 2, k_2 = 8, k_3 = 2, k_4 = 2, k_5 = 8$$

Next we compute the ε_n. We have

$$\varepsilon_0 = -1, \varepsilon_1 = 1, \varepsilon_2 = -1, \varepsilon_3 = -1, \varepsilon_4 = 1, \varepsilon_5 = -1$$

Thus

$$\sqrt{13} = 4 + \omega_0$$

$$\omega_0 = \star\frac{-1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|8} + \star$$

The full period $2r = 6$ gives

$$\omega_0 = \star\frac{-1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|8} + \frac{-1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|8}\star$$

To solve the Brahmagupta-Fermat- Pell equation we need the convergent

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}} &= \frac{p_5}{q_5}\\ &= \frac{-1|}{|2} + \frac{1|}{|2} + \frac{-1|}{|8} + \frac{-1|}{|2} + \frac{1|}{|2}\\ &= \frac{-71}{180}\end{aligned}$$

So $p_{2r-1} = p_5 = -71$ and $q_{2r-1} = q_5 = 180$. So from $\nu_0 = 4$ and (5.95) we get

$$\begin{aligned}u &= q_{2r-1} = 180,\\ t &= p_{2r-1} + \nu_0 q_{2r-1} = -71 + 4 \times 180 = 649\end{aligned}$$

which gives the fundamental solution of the Brahmagupta-Fermat equation

$$t^2 - 13u^2 = 1$$

Perron's transformation $\mathcal{T}_1$ of the SRCF to the RCF (see Remark 5.8) leads to

$$\sqrt{13} = 3 + \star\frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|6} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|6}\star$$

The period of the RCF is $2\rho = 2r + \eta = 6 + 4 = 10$. We have the convergent $\frac{p_{2\rho-1}}{q_{2\rho-1}} = \frac{109}{180}$. The solution of the Brahmagupta-Fermat equation $t^2 - 13u^2 = 1$ is given by

$$\begin{aligned}u &= Q_{2\rho-1} = 180,\\ t &= P_{2\rho-1} + (\nu_0 - 1)Q_{2\rho-1} = 109 + 3 \times 180 = 649\end{aligned}$$

as before.

7. $D = 41$. $\{\sqrt{D}\} = \nu_0 = 6$. The step cycle is

$$(1, 6, -5), (-5, 4, 5), (5, 6, -1); (-1, 6, 5), (5, 4, -5), (-5, 6, 1)$$

The cycle period is $2r = 6$ and thus $r = 3$ which is odd. We obtain the SRCF by computing first

$$\delta_0 = 2, \delta_1 = -2, \delta_2 = 12, \delta_3 = -2, \delta_4 = 2, \delta_5 = -12$$

after which the sequence repeats itself. Taking absolute values we have the k_n

$$k_0 = 2, k_1 = 2, k_2 = 12, k_3 = 2, k_4 = 2, k_5 = 12$$

Next we compute the ε_n. We have

$$\varepsilon_0 = 1, \varepsilon_1 = 1, \varepsilon_2 = 1, \varepsilon_3 = 1, \varepsilon_4 = 1, \varepsilon_5 = 1$$

Thus

$$\sqrt{41} = 6 + \omega_0$$

$$\omega_0 = \star\frac{1|}{|2} + \frac{1|}{|2} + \frac{1|}{|12} + \star$$

The full period $2r = 6$ gives

$$\omega_0 = \star\frac{1|}{|2} + \frac{1|}{|2} + \frac{1|}{|12} + \frac{1|}{|2} + \frac{1|}{|2} + \frac{1|}{|12}\star$$

To solve the Brahmagupta-Fermat- Pell equation we need the convergent

$$\begin{aligned}\frac{p_{2r-1}}{q_{2r-1}} &= \frac{p_5}{q_5} \\ &= \frac{1|}{|2} + \frac{1|}{|2} + \frac{1|}{|12} + \frac{1|}{|2} + \frac{1|}{|2} \\ &= \frac{129}{320}\end{aligned}$$

So $p_{2r-1} = p_5 = 129$ and $q_{2r-1} = q_5 = 320$. So from $\nu_0 = 6$ and (5.95) we get

$$\begin{aligned}u &= q_{2r-1} = 320, \\ t &= p_{2r-1} + \nu_0 q_{2r-1} = 129 + 6 \times 320 = 2049\end{aligned}$$

which gives the fundamental solution of the Brahmagupta-Fermat equation

$$t^2 - 41u^2 = 1$$

Appendix 1

Proof of Proposition 4.3 : We have $|m| < \sqrt{D}$. Since ν is best mod m, it is one of two positive integers ν_1 or ν_2 satisfying

$$\nu_1^2 < D < \nu_2^2 = (\nu_1 + |m|)^2 \tag{6.1}$$

Recall also that $\nu^2 - D = \varepsilon|m||m'|$ where $\varepsilon = \pm 1$ according as ν is greater or less than $\sqrt{D}$. We now have two cases according as $\nu > \sqrt{D}$ or $\nu < \sqrt{D}$.

1. Suppose $\nu > \sqrt{D}$. Then $\varepsilon = +1$ and $\nu^2 - D = |m||m'|$. and $\nu_2 = \nu$ in (4.2) and $\nu_1 = \nu - |m|$. We have

$$\nu^2 - D \leq D - (\nu - |m|)^2 = (D - \nu^2) + 2\nu m - |m|^2$$

whence

$$\nu^2 - D \leq \nu|m| - \frac{|m|^2}{2}$$

Use $\nu^2 - D = |m||m'|$ and factor out $|m|$. This gives

$$\nu \geq |m'| + \frac{|m|}{2} \tag{6.2}$$

which proves that (1) (Proposition 4.3) $\Rightarrow$ (3) when $\nu > \sqrt{D}$. Working backwards from (6.2) we can prove (3)$\Rightarrow$ (1) of the proposition. In fact from (6.2) and $\nu^2 - D = |m||m'|$ (since $\nu > \sqrt{D}$) we have

$$\frac{\nu^2 - D}{|m|} = |m'| \leq \nu - -\frac{|m|}{2}$$

whence

$$2(\nu^2 - D) \leq 2|m|\nu - |m|^2 = -(\nu - |m|)^2 + \nu^2$$

whence

$$0 < \nu^2 - D \leq D - (\nu - |m|)^2$$

This implies

$$(\nu - |m|)^2 < D < \nu^2$$

which states that n is best mod m when $\nu > \sqrt{D}$. Thus we have shown that (3) of Proposition $\Rightarrow$ (1). Hence we have shown when $\nu > \sqrt{D}$, we have (1) $\iff$ (3).

We will now show that (3) $\iff$ (2). Squaring inequality (6.2) gives

$$\nu^2 \geq |m'|^2 + |m'||m| + \frac{|m|^2}{4}$$

Now $|m'||m| = \nu^2 - D$. Therefore

$$|m'|^2 + \frac{|m|^2}{4} \leq D \tag{6.3}$$

which is (2) of the Proposition. On the other hand suppose (2) is true. Then we have

$$D + |m||m'| \geq (|m'| + \frac{|m|}{2})^2 \tag{6.4}$$

Since $\nu > \sqrt{D}$ we have $|m||m'| \leq \nu^2 - D$ or $D + |m||m'| \leq \nu^2$. Therefore from (6.4) we get

$$\nu^2 \geq (|m'| + \frac{|m|}{2})^2$$

Now taking square roots we get (6.2). Thus we have proved the chain of implications

$$(1) \iff (3) \iff (2)$$

which proves the Proposition for the case $\nu > \sqrt{D}$.

2. We will now prove the Proposition for the case $\nu < \sqrt{D}$.

Suppose $\nu < \sqrt{D}$. In this case $\varepsilon = -1$ and $\nu^2 - D = -|m||m'|$. Then $\nu_1 = \nu$ in (4.2) and $\nu_2 = \nu + |m|$. We have

$$D - \nu^2 \leq (\nu + |m|)^2 - D = \nu^2 - D + 2\nu|m| + |m|^2 \tag{6.5}$$

Therefore transfering $\nu^2 - D$ to the left and using $\nu^2 - D = -|m||m'|$, we get

$$2|m||m'| \leq 2\nu|m| + |m|^2$$

Dividing out by $2|m|$ we get

$$\nu \geq |m'| - \frac{|m|}{2} \tag{6.6}$$

which proves that (1) $\Rightarrow$ (3) of the Proposition. We now prove that (3) $\Rightarrow$ (1). Starting from (6.6) and $\nu^2 - D = -|m||m'|$ we have

$$D - \nu^2 \geq |m|(\nu + \frac{|m|}{2}) = m|\nu + \frac{|m|^2}{2}$$

or

$$2(D - \nu^2) \geq (\nu + |m|)^2 - \nu^2$$

whence

$$0 < \nu^2 < D < (\nu + |m|)^2$$

which is (1). We have thus proved that when $\nu < \sqrt{D}$, we have (1) $\Rightarrow$ (3) of the Proposition.

We will now prove that (1) $\iff$ (2) when $\nu < \sqrt{D}$.

First we prove (1) $\Rightarrow$ (2). Starting from (6.5)

$$D - \nu^2 \leq \nu|m| + \frac{|m|^2}{2}$$

whence

$$\nu^2 + \nu|m| - D + \frac{|m|^2}{2} \geq 0$$

or

$$(\nu + \frac{|m|}{2})^2 + \frac{|m|^2}{4} - D \geq 0$$

Therefore

$$(\nu + \frac{|m|}{2})^2 > D - \frac{|m|^2}{4} \geq 0$$

Note that $|m| < \sqrt{D}$ implies $D > |m|^2 > \frac{|m|^2}{4}$ and hence $D - \frac{|m|^2}{4} > 0$. All quantities in the previous inequality are positive, so we can take square roots to get

$$\nu \geq \sqrt{D - \frac{|m|^2}{4}} - \frac{|m|}{2}$$

Furthermore, since $D > \frac{|m|^2}{2}$, we have

$$D - \frac{|m|^2}{4} \geq \frac{|m|^2}{2} - \frac{|m|^2}{4} = \frac{|m|^2}{4} > 0$$

Therefore squaring positive quantities we get

$$\nu^2 \geq (\sqrt{D - \frac{|m|^2}{4}} - \frac{|m|}{2})^2 = D - \frac{|m|^2}{4} + \frac{|m|^2}{4} - |m|\sqrt{D - \frac{|m|^2}{4}}$$

Therefore

$$|m|\sqrt{D - \frac{|m|^2}{4}} \geq D - \nu^2 = |m||m'|$$

Dividing out by $|m|$ and then squaring gives us

$$D \geq |m'|^2 + \frac{|m|^2}{4}$$

which proves (2) of the Proposition. Thus (1) $\Rightarrow$ (2).

Next we prove (2) $\Rightarrow$ (1).

Essentially we work backwards. From (2) we have

$$|m|\sqrt{D - \frac{|m|^2}{4}} \geq |m||m'| = D - \nu^2$$

whence

$$\nu^2 \geq (\sqrt{D - \frac{|m|^2}{4}} - \frac{|m|}{2})^2 \tag{6.7}$$

It was established earlier that

$$D - \frac{|m|^2}{4} > \frac{|m|^2}{4}$$

so that

$$\sqrt{D - \frac{|m|^2}{4}} \geq \frac{|m|}{2}$$

Therefore taking square root of (6.7) we get

$$\nu + \frac{|m|}{2} \geq \sqrt{D - \frac{|m|^2}{4}} \tag{6.8}$$

The right hand side is positive. Hence taking the square of (6.8) we get

$$D - \nu^2 \leq \nu|m| + \frac{|m|^2}{2}$$

which is (6.5) and thus

$$0 < \nu^2 < D < (\nu + |m|)^2$$

Therefore we have also shown (2) $\Rightarrow$ (1). Thus (1) $\iff$ (2). Therefore for $\nu < \sqrt{D}$ we have shown by transitivity (1) $\iff$ (2) $\iff$ (3). The proof of Proposition 4.3 is now

complete. ∎

Appendix 2

Proof of Theorem 4.6:

(m, ν, m') is a step and (m', ν', m'') is a successor step. As steps they satisfy (see statement of Theorem 4.3)

$$(1) \quad |m'|^2 + \frac{m^2}{4} \leq D \tag{6.9}$$

$$(2) \quad |m''|^2 + \frac{m'^2}{4} \leq D \tag{6.10}$$

and we have to prove that

$$(3) \quad |m'|^2 + \frac{m''^2}{4} \leq D \tag{6.11}$$

in which case the successor step (m', ν', m'') is a reduced step.

Now (3) follows from (2) if $|m'| \leq |m''|$ by Corollary 4.5. And (3) follows from (1) if $|m''| \leq |m|$. Thus from now on we assume that

$$|m| < |m''| < |m'| \tag{6.12}$$

.

Recall that $\nu^2 - D = \varepsilon|m||m'|$ and $\nu'^2 - D = \varepsilon'|m''||m'|$. Furthermore since $m'|(\nu + \nu')$ we have for some positive integer l,

$$\nu' + \nu = |m'|l \tag{6.13}$$

Therefore

$$|m'|l(\nu' - \nu) = (\nu' + \nu)((\nu' - \nu) = \nu'^2 - \nu^2 = \varepsilon'|m''||m'| - \varepsilon|m||m'|$$

Dividing out by $|m'|$ we get

$$\nu' - \nu = \frac{\varepsilon'|m''| - \varepsilon|m|}{l} \tag{6.14}$$

Adding (6.13) and (6.14), we get

$$2\nu' = |m'|l + \frac{\varepsilon'|m''| - \varepsilon|m|}{l} \tag{6.15}$$

Now $|m| \leq |m''|$ by assumption. Therefore

$$2\nu' = |m'|l + \frac{(\varepsilon' - \varepsilon)|m''|}{l}$$

Now $\varepsilon = \pm 1$. Therefore

$$\nu' \geq \frac{1}{2}\Big(|m'|l + \frac{(\varepsilon' - 1)|m''|}{l}\Big) \tag{6.16}$$

On the other hand, subtracting (6.14) from (6.13), we get

$$\nu = \frac{1}{2}\Big(|m'|l - \frac{\varepsilon'|m''| - \varepsilon|m|}{l}\Big) \tag{6.17}$$

From (6.9), Proposition 4.1 and (6.17) we have

$$\frac{1}{2}\Big(|m'|l - \frac{\varepsilon'|m''| - \varepsilon|m|}{l}\Big) \geq |m'| + \varepsilon\frac{|m|}{2} \tag{6.18}$$

Our strategy is to show first that low values of l are excluded.

1. Suppose $l = 1$. Then from (6.18) we get

$$\frac{1}{2}\Big(|m'| - \varepsilon'|m''| + \varepsilon|m|\Big) \geq |m'| + \varepsilon\frac{|m|}{2}$$

or

$$\frac{1}{2}\Big(|m'| - \varepsilon'|m''|\Big) \geq |m'|$$

or

$$-\varepsilon'|m''| \geq |m'|$$

If $\varepsilon' = 1$, then $|m'| \leq 0$, which is impossible. If $\varepsilon' = -1$, then $|m''| \geq |m'|$ which is contrary to hypothesis (6.12). Therefore

$$l \neq 1$$

2. Suppose $l = 2$. Then from (6.18)

$$\frac{1}{2}\Big(|m'|2 - \frac{\varepsilon'|m''| - \varepsilon|m|}{2}\Big) \geq |m'| + \varepsilon\frac{|m|}{2}$$

or

$$(\varepsilon'|m''| + \varepsilon|m|) \leq 0$$

If $\varepsilon' = 1$, then

$$(|m''| + \varepsilon|m|) \leq 0$$

Then $\varepsilon = 1$ leads to contradiction. If $\varepsilon = -1$ then

$$|m''| \leq |m|$$

which contradicts hypothesis (6.12).Therefore for $\varepsilon' = 1$ we must have $l \neq 2$. Thus

$$\varepsilon' = 1 \Rightarrow l \geq 3$$

.
If $\varepsilon' = -1$, then $l \geq 2$. From (6.16)

$$\nu' \geq \frac{1}{2}\Big(|m'|2 - 2\frac{|m''|}{2}\Big)$$

or

$$\nu' \geq (|m'| - \frac{|m''|}{2}) \tag{6.19}$$

For $\varepsilon' = 1$ we have $l \geq 3$. Therefore

$$\nu' \geq \frac{1}{2}\Big(|m'|l - 2\frac{|m''|}{l}\Big) \geq \frac{1}{2}\Big(|m'|3 - 2\frac{|m''|}{l}\Big)$$

This is true for all $l \geq 3$. Therefore the second term is as small as one pleases. Hence

$$\nu' \geq \frac{3}{2}|m'| = |m'| + \frac{1}{2}|m'|$$

From (6.12), $|m'| \geq |m''|$ and therefore

$$\nu' \geq \frac{3}{2}|m'| \geq |m'| + \frac{1}{2}|m''| \tag{6.20}$$

From (6.19) (case $\varepsilon' = -1$) and (6.20) (case $\varepsilon' = +1$) we get

$$\nu' \geq |m'| + \varepsilon'\frac{1}{2}|m''| \tag{6.21}$$

and this implies from Proposition 4.1

$$|m'|^2 + \frac{|m''|^2}{4} \leq D \tag{6.22}$$

Therefore (m', ν', m'') is a reduced step and thus Theorem 4.3 has been proved. ∎

Appendix 3

Proof of Lemma 5.6:

Let (m, ν, m') and $(m', \nu'', m")$ be two successive steps. From Theorem 4.6 and Corollary 4.7 we have that all steps are reduced. We will show that this implies that $k \geq 2$ where

$$k = \frac{\nu + \nu'}{|m'|}$$

In the proof we will make use of some of the results in Appendix 2 where we gave the proof of Theorem 4.6. Recall that, from Proposition 4.3 beginning paragraph, $\nu^2 - D = \varepsilon|m||m'|$ and similarly $\nu'^2 - D = \varepsilon'|m'||m''|$, where ε, $\varepsilon' = \pm 1$. Furthermore for consistency of notation with Appendix 2 we define $l = k$ so that as in (6.13)

$$\nu + \nu' = |m'|l$$

and we have to prove $l \neq 1$.
We have to consider the following 6 cases :

1. $|m| < |m'| < |m''|$
2. $|m''| < |m'| < |m|$
3. $|m'| < |m| < |m''|$
4. $|m''| < |m| < |m'|$
5. $|m| < |m''| < |m'|$
6. $|m'| < |m''| < |m|$

Suppose $l = 1$. We have proved in Appendix 2, (6.18) and the lines following it, that when $\varepsilon' = 1$, $l \neq 1$. On the other hand, when $\varepsilon' = -1$ we have $|m''| \geq |m'|$, which is contrary to the hypotheses of Cases 2), 4), 5). Therefore $l \neq 1$ in these cases. It remains to consider Cases 6, 1, 3.

Case 6. We shall now show that for Case 6, $l \neq 1$. Suppose $l = 1$. Assume $\varepsilon' = -1$, since otherwise, as earlier, $l \neq 1$. Now by Theorem 4.6 and Corollary 4.7 all steps are reduced. Thus the step (m, ν, m') is reduced. Therefore ν is best mod m and also mod m', since (m', ν, m) is a step. Hence, by Proposition 4.3 and Definition 4.4 we have

$$\nu \geq |m| + \frac{\varepsilon}{2}|m'| \tag{6.23}$$

Combining this with (6.17) we get (by assumption $l = 1$) with $\varepsilon' = -1$ (otherwise $l \neq 1$)

$$\frac{1}{2}\Big(|m'| + |m''| + \varepsilon|m|\Big) \geq |m| + \frac{\varepsilon}{2}|m'| \tag{6.24}$$

whence

$$\frac{1}{2}(1-\varepsilon)|m'| \geq |m|(1-\frac{\varepsilon}{2}) - \frac{1}{2}|m''|$$

or

$$(1-\varepsilon)|m'| \geq |m|(2-\varepsilon) - |m''| \tag{6.25}$$

1. $\varepsilon = 1$. From (6.25) we get $|m| \leq |m''|$ which contradicts Case 6.

2. $\varepsilon = -1$. From (6.25)

$$2|m'| \geq 2|m| + (|m| - |m''|)$$

For Case 6, we have $|m| > |m''|$.
Therefore

$$|m'| \geq |m|$$

which contradicts Case 6. Therefore $l \neq 1$.

It remains to show that for Cases 1 and 3 , $l \neq 1$. We can take $\varepsilon' = -1$ because if $\varepsilon' = 1$ then $l \neq 1$ as shown in Appendix 2. We now consider in turn

Case1. Suppose $l = 1$. (m', ν', m'') is reduced, and therefore ν' is best mod m' and also best mod m''. Hence from Proposition 4.3 we have

$$\nu' \geq |m''| + \varepsilon\frac{|m'|}{2} \tag{6.26}$$

$$\nu' \geq |m'| + \varepsilon\frac{|m''|}{2} \tag{6.27}$$

We also have from (6.15), on taking $l = 1$ and $\varepsilon' = -1$

$$\nu' = \frac{1}{2}(|m'| - |m''| - \varepsilon|m|) \tag{6.28}$$

From (6.28) and (6.27) we get

$$\frac{1}{2}(|m'| - |m''| - \varepsilon|m|) \geq |m'| + \varepsilon\frac{|m''|}{2}$$

or

$$|m'| - |m''| - \varepsilon|m| \geq 2|m'| + \varepsilon|m''|$$

whence

$$-(1+\varepsilon)|m''| \geq |m'| + \varepsilon|m|$$

For $\varepsilon = -1$ we get $|m| \geq |m'|$ which contradicts Case 1. On the other hand if $\varepsilon = 1$ we get $|m| \leq 0$ which is impossible. Therefore $l \neq 1$.

Case 3. Suppose $l = 1$. Assume $\varepsilon' = -1$, otherwise if $\varepsilon' = 1$ then $l \neq 1$ as shown earlier. From (6.28) and (6.26) we have

$$\frac{1}{2}(|m'| - |m''| - \varepsilon|m|) \geq |m''| + \varepsilon\frac{|m'|}{2}$$

or

$$|m'| - |m''| - \varepsilon|m| \geq 2|m''| + \varepsilon|m'|$$

whence

$$(1-\varepsilon)|m'| - \varepsilon|m| \geq 3|m''| \tag{6.29}$$

There are now two possibilities.

1. $\varepsilon = 1$. Then $|m''| \leq 0$, which is impossible.

2. $\varepsilon = -1$. From (6.29) we have

$$2|m'| + |m| \geq 3|m''|$$

Therefore

$$|m| \geq |m''| + 2(m'' - |m'|)$$

For Case 3, we have $|m''| > |m'|$. Therefore from the previous inequality $|m| \geq |m''|$, which contradicts Case 3. Therefore $l \neq 1$. Therefore we have now proved in all the possible cases 1) - 6) that $l \neq 1$. The proof of Lemma 5.6 is complete. ∎

Appendix 4

Generalisation of Galois inverse period theorem and symmetry consequences to semi-regular continued fractions(SRCF)

Proof of (5.71) ,(5.72) and (5.73) :

Perron [P] (§23, pages 82-83) gave a simple proof the Galois inverse period theorem (Satz 6) for regular continued fractions (RCF) and as a consequence obtained in (§24, page

87) additional symmetries for the partial quotients of the RCF. Here, following closely the above considerations in [P], we generalize the Galois inverse period theorem and its symmetry consequences for the partial quotients of the SRCF. A similar generalization is given in [A2], §5.6.1, pages 32-34.

Recall that from (5.24) and (5.67)

$$\vartheta_0 = \sqrt{D} = \nu_0 + \omega_0 = \nu_0 + \star\frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ...\frac{\varepsilon_{2r-1}|}{|k_{2r-1}}\star \tag{6.30}$$

where we have used $m_0 = 1$ and that the SRCF is periodic with period $2r$. $\nu_0 = [\sqrt{D}]$ is the integer closest to $\sqrt{D}$ in absolute value in the congruence class (mod 1). We have the periodicity of the partial quotients by $\varepsilon_{j+2r} = \varepsilon_j$ and $k_{j+2r} = k_j$. It is convenient to make a slight change of notation. We define η_j , κ_j by the equations

$$\eta_j = \varepsilon_{j-1} : \ 1 \leq j \leq 2r \tag{6.31}$$

$$\kappa_j = k_{j-1} : \ 1 \leq j \leq 2r \tag{6.32}$$

$$\kappa_0 = \nu_0 \tag{6.33}$$

with the same periodicity. The SRCF (6.30) now reads with $\kappa_0 = \nu_0$

$$\vartheta_0 = \kappa_0 + \star\frac{\eta_1|}{|\kappa_1} + \frac{\eta_2|}{|\kappa_2} + +....\frac{\eta_{2r}|}{|\kappa_{2r}}\star \tag{6.34}$$

The SRCF (6.34) is generated by the recursion relation

$$\vartheta_j = \kappa_j + \frac{\eta_{j+1}}{\vartheta_{j+1}} : \ 0 \leq j \leq 2r-1 \tag{6.35}$$

and by periodicity

$$\vartheta_{2r} = \kappa_{2r} + \frac{\eta_{2r+1}}{\vartheta_{2r+1}} = \kappa_{2r} + \frac{\eta_1}{\vartheta_1} \tag{6.36}$$

Let $\bar{\vartheta}_j$ be the conjugate of ϑ_j. It obeys the same recursion relation, namely

$$\bar{\vartheta}_j = \kappa_j + \frac{\eta_{j+1}}{\bar{\vartheta}_{j+1}} : \ 0 \leq j \leq 2r-1 \tag{6.37}$$

whence

$$-\frac{\eta_{j+1}}{\bar{\vartheta}_{j+1}} = \kappa_j - \bar{\vartheta}_j \tag{6.38}$$

Define

$$-\frac{\eta_{j+1}}{\bar{\vartheta}_{j+1}} = \zeta_{2r-j} \tag{6.39}$$

From (6.38) and (6.39) we obtain

$$\zeta_{2r-j} = \kappa_j + \frac{\eta_j}{\zeta_{2r-j+1}} \tag{6.40}$$

We rewrite (6.40)

$$\zeta_i = \kappa_{2r-i} + \frac{\eta_{2r-i}}{\zeta_{i+1}} : \ 0 \leq i \leq 2r-1 \tag{6.41}$$

Therefore

$$\zeta_0 = \kappa_{2r} + \frac{\eta_{2r}|}{|\kappa_{2r-1}} + \frac{\eta_{2r-1}|}{|\kappa_{2r-2}} + ... + \frac{\eta_2|}{|\kappa_1} + \frac{\eta_1|}{|\zeta_{2r}} \tag{6.42}$$

From (6.39) and periodicity we obtain

$$\zeta_{2r} = -\frac{\eta_1}{\bar{\vartheta}_1} = -\frac{\eta_{2r+1}}{\bar{\vartheta}_{2r+1}} = \zeta_0 \tag{6.43}$$

From (6.42) and (6.43) we obtain

$$\zeta_0 = \kappa_{2r} + *\frac{\eta_{2r}|}{|\kappa_{2r-1}} + \frac{\eta_{2r-1}|}{|\kappa_{2r-2}} + ... + \frac{\eta_2|}{|\kappa_1} + \frac{\eta_1|}{|\kappa_{2r}}\star \tag{6.44}$$

Reverting back to the original notation in (6.31) and (6.32) we have the analogue for the SRCF of the Galois inverse periodicity

$$\zeta_0 = k_{2r-1} + \star\frac{\varepsilon_{2r-1}|}{|k_{2r-2}} + \frac{\varepsilon_{2r-2}|}{|k_{2r-3}} + ... + \frac{\varepsilon_1|}{|k_0} + \frac{\varepsilon_0|}{|k_{2r-1}}\star \tag{6.45}$$

where from (6.43)

$$\zeta_0 = -\frac{\varepsilon_0}{\bar{\vartheta}_1} \tag{6.46}$$

We now obtain the additional symmetry relations. From

$$\sqrt{D} = \vartheta_0 = \kappa_0 + \star\frac{\eta_1|}{|\kappa_1} + \frac{\eta_2|}{|\kappa_2} + +....\frac{\eta_{2r}|}{|\kappa_{2r}}\star \tag{6.47}$$

we obtain

$$\sqrt{D} - \kappa_0 = \frac{\eta_1}{\vartheta_1}$$

whence

$$\frac{\eta_1}{\sqrt{D}-\kappa_0} = \vartheta_1 = \kappa_1 + \star\frac{\eta_2|}{|\kappa_2} + \frac{\eta_3|}{|\kappa_3} + +....\frac{\eta_{2r}|}{|\kappa_{2r}}\star \tag{6.48}$$

From (6.48) we obtain for the conjugate $\bar{\vartheta}_1$

$$\bar{\vartheta}_1 = -\frac{\eta_1}{\sqrt{D}+\kappa_0}$$

whence

$$-\frac{1}{\bar{\vartheta}_1} = \eta_1(\sqrt{D}+\kappa_0) \tag{6.49}$$

From (6.43) and (6.49) we obtain

$$\zeta_0 = -\frac{\eta_1}{\bar{\vartheta}_1} = (\sqrt{D}+\kappa_0) \tag{6.50}$$

where we have used $\eta_1^2 = 1$. Now from (6.50) and(6.30) we obtain directly (remembering $\kappa_0 = \nu_0$)

$$\zeta_0 = \sqrt{D}+\nu_0 = 2\nu_0+\omega_0 = 2\nu_0 + \star\frac{\varepsilon_0|}{|k_0} + \frac{\varepsilon_1|}{|k_1} + \frac{\varepsilon_2|}{|k_2} + ... + \frac{\varepsilon_{2r-2}|}{|k_{2r-2}} + \frac{\varepsilon_{2r-1}|}{|k_{2r-1}}\star \tag{6.51}$$

We compare ζ_0 given by (6.51) above with ζ_0 given in (6.42):

$$\zeta_0 = k_{2r-1} + \star\frac{\varepsilon_{2r-1}|}{|k_{2r-2}} + \frac{\varepsilon_{2r-2}|}{|k_{2r-3}} + ... + \frac{\varepsilon_1|}{|k_0} + \frac{\varepsilon_0|}{|k_{2r-1}}\star \tag{6.52}$$

to obtain the symmetry relations of (5.71), (5.72) and (5.73) :

$$\varepsilon_i = \varepsilon_{2r-1-i} \ : \ 0 \le i \le 2r-1 \tag{6.53}$$

$$k_i = k_{2r-2-i} \ : \ 0 \le i \le 2r-2 \tag{6.54}$$

$$k_{2r-1} = 2\nu_0 \tag{6.55}$$

The proof of (5.71), (5.72) and (5.73) is complete. ∎

References

[A1] A. A. K. Ayyangar: New Light on Bhaskara's Chakravala or Cyclic Method of solving Indeterminate Equations of the Second Degree in two Variables, J. Indian Math. Soc.

(1929) (1) 18 (2), 232-245.

[A2] A. A. K. Ayyangar: Theory of the Nearest Square Continued Fraction, J. Mysore Univ. (1941) Sect. A 1, 97-117

[B] A. Bauval: An elementary proof of the halting property for the Chakravala algorithm, arXiv:1406.6809

[Bo] W. Bosma: Optimal Continued Fractions, Indigiatones Mathematicae (Proceedings), A 90 (4) 1987, 353-379.

[BK] W. Bosma C. Kraaikamp: Optimal approximatiom by continued fractions, J. Austral. Math. Soc. (Series A) 50 (1991), 481-504.

[D] P. G.L. Dirichlet: Lectures on Number Theory (supplemented by R. Dedekind): American Mathematical Society, History of Mathematics Sources, Volume 16, 1991. Translation by John Stillwell of Vorlesungen über Zahlentheorie by P. G. Lejeune Dirichlet, F. Vieweg und Sohn, Braunschweig, 1863

[Di] P. P. Divakaran: The Mathematics of India (Concepts, Methods, Connections), Hindustan Book Agency (2018), New Delhi, co-published by Springer Verlag, (Sources and Studies in the History of Mathematics and Physical Sciences).

[DS] B. Datta and A. Singh, History of Hindu Mathematics, vols I and II, Bharatiya Kala Prakashan, Delhi (2004, reprint). The original edition (1935, 1938), Asia Publishing House, can be obtained from the Internet Archives.

[FK] E. Fouvry and J Klüners: On the negative Pell equation, Annals of Mathematics (2010), vol 172, 2035-2104.

[G-DA] C. F. Gauss: Disquisisiones Arithmeticae, translated by Arthur A. Clarke, Yale University Press, New Haven and London (2009)

+[L] J. L. Lagrange: Recherche d'Arithmétique, Nouv. Mém. de l'Acad. de Berlin 1773, 1775.

[Le] A. M. Legendre: Essai sur la Théorie des Nombres, Cambridge University Press, Cambridge and New York, (2009). Reprint of second edition, Paris 1808, publisher Courcier.

[M] K.R. Matthews: On the Optimal Continued Fraction expansion of a Quadratic Surd, J. Aust. Math. 93 (2012), 133-156.

[MR] K. R. Matthews and J. P. Robertson: Purely Periodic Nearest Square Continued Fractions, Journal of Combinatorics and Number Theory 2 (2010), 239-244.

[MRW] Keith Mathews, John Robertson and Jim White: Midpoint criteria for solving

Pell's equation using the nearest square continued fraction, Math.Comp. 79 (2010), 485-499.

[MS] R. A. Mollin, A Srinivasan: A note on the negative Pell equation, International Journal of Algebra 4 (2010), 919-222.

[O] A. Offer: Continuants and semi-regular continued fractions, (2008), http://www.numbertheory.org/PDFS/continuant.pdf

[MT]: https://mathshistory.st-andrews.ac.uk/HistTopics/Pell/

[P] O. Perron: Die Lehre von den Kettenbrüchen, B. G. Teubner, Belin and Leipzig (1913). This has been reprinted by Chelsea, New York (1929). A later edition is that of B. G. Teubner Verlag, Stuttgart (1954). We have used the page numbering and the section numbers of the original Teubner edition. This can be downloaded from https://archive.org

[Pl] K. Plofker: Mathematics in India, Princeton University Press, Princeton and Oxford (2009).

[S] P. Stevenhagen: The number of real quadratic fields having units of negative norm, Experimental Mathematics, 2 (2) (1993) , 121- 136.

[Se] C-L Selenius: Rationale of the Chakravala process of Jayadeva and Bhaskara II: Historia Mathematica 2 (1975), 167-184

[Se1] C-L Selenius: Konstruction und Theorie halbregelmässiger Kettenbrüche mit idealer relativer Approximation, Acta Acad. Aboensis (1960), math. phys. 22 (2) , 1-77

[Se2] C-L Selenius: Kettenbrüchtheoretische Erklärung der zyklishen Methode zur Lösung der Bhaskara-Pell-Gleichung, Acta Acad. Aboensis (1963), math. phys. 23 (10) , 1-44

[KS] K. Shukla: Ac$\bar{a}$rya Jayadeva the mathematician, Ganita 5 (1954) 1-20.

[S1] H. Stark: An introduction to Number Theory, The MIT Press (1987), Cambridge, Massachusetts and London, England.

[T] F. Tano: Sur quelques théorèmes de Dirichlet, J. Reine und Angew.Math 105 (1889) 160-169

[W] A. Weil: Number Theory, An approach through history from Hammurapi to Legendre, Birkhaüser (1984), Boston-Basel-Berlin