チャクラヴァーラ
— 中世インドのペル方程式の解法—について

佐藤　文広
(津田塾大学数学・計算機科学研究所/立教大学)

インドでは，遅くとも 5 世紀頃には 1 次不定方程式が，遅くとも 7 世紀には 2 次不定方程式（ペル方程式）が研究されていた.[*1] D を平方数ではない正整数とし，方程式

$$x^2 - Dy^2 = 1$$

を**ペル方程式**という．インドでは，7 世紀から 11 世紀までのどこかの時点で，**円環法** (**cakravāla**, **チャクラヴァーラ**，“cakra”=車輪，円板）と呼ばれるペル方程式の解法アルゴリズム（オイラー・ラグランジュによる二元二次形式論や $\sqrt{D}$ の連分数展開を利用する今日の方法に通ずるものである）が発見されていた．本稿では，まず，チャクラヴァーラに先行するインド数学の重要な成果であるクッタカとバーヴァナーに簡単に触れた (§1, §2) 後，チャクラヴァーラとはどのような方法であるかを説明し（§3)，チャクラヴァーラをめぐる議論（の一部）を紹介し (§4)，最後 (§5) に，チャクラヴァーラと二元二次形式のガウスの簡約理論，オイラー・ラグランジュによる連分数を利用したペル方程式の解法との関係，元来のチャクラヴァーラが正しく解法を与えていることの初等的証明（Bauval による）を解説する.

チャクラヴァーラについては以前から関心を持っていたが，実際に調べ始めた直接的なきっかけは，[Katz and Parshall, 2014] という代数学史の本を翻訳した際に，チャクラヴァーラの方法によって必ずペル方程式の解が得られることの証明は「19 世紀まで得られなかった」との記述に出会ったことである．通常，その証明は 18 世紀のラグランジュに帰すことが多く，19 世紀とは誰のことか想像が付かなかったので，翻訳の正確を期すために調査を始めた次第である.[*2]

チャクラヴァーラの真の創始者は判然とせず，「7 世紀から 11 世紀までのどこかの時点で」と上で記載したのは，628 年頃の作品と見られるブラフマグプタ（598–670）の『ブラーフマスプタシッダーンタ』にはペル方程式の部分的解法のみが記述されており，一方，1073 年に書かれたと推定さ

[*1] インド数学史全般については [林，2020] を参照されたい．多くの原典の和訳（と解説）が [矢野，1980], [楠葉・林・矢野，1997], [林，2016], [林，2019] にあり，大変貴重である．洋書では [Plofker, 2009] がインド数学の通史である．[Plofker, 2007] にも，原典からの抜粋が多数英訳されている．本稿の主題のチャクラヴァーラについては，[ヴェイユ 1987, pp. 21–25] にある程度詳しい紹介がある.

[*2] この疑問への私なりの解答は，p. 10.

れる文献でジャヤデーヴァ[*3]によるものとして，また有名な天文学者で数学者のバースカラ II の『ビージャガニタ』(1150 年) で，チャクラヴァーラの完全なアルゴリズムが書き残されているからである．これは，フェルマに始まるヨーロッパでのペル方程式の研究に少なくとも 600 年近く先行しているので，「ペル方程式」は（ペルがこの方程式についてほとんど寄与していないというよく知られた事実をさておいても）「ジャヤデーヴァ・バースカラ方程式」と呼ぶべきだという，それなりにもっともな意見もある ([Selenius, 1975, p. 168], [林，2020，p.290])．

チャクラヴァーラの基礎となった重要な先行結果は，1 次不定方程式 $ax + by = c$ の解法である**クッタカ**（**kuṭṭaka**,「粉砕法」と訳される）と，今日では二元二次形式の合成の先駆けと見ることができるブラフマグプタの**バーヴァナー** (**bhāvanā**) である．まず，この 2 つについて説明しておこう．

1　クッタカ

クッタカの数学的内容は，本質的には，いわゆる拡張ユークリッドアルゴリズムによって $ax + by = c$ $(a, b, c \in \mathbb{Z})$ の整数解を求める方法である．[*4]　アールヤバタ (476–) の『アールヤバティーヤ』の第 2 章詩節[*5] 32 , 33 を [矢野，1980, pp. 108–109] の訳で引用してみる．

> 32.　大きい余りを生ずる除数を，小さい余りを生ずる除数で割るがよい．(この第 1 の割り算の商はいつも捨てる．）余り（と除数) を相互に割り，(その割り算の余りが十分小さくなるまで割り算を続け商の蔓が偶数個になるようにしておく．最後の余りに）想定数をかけ，最初の余りの差に加えて (最後の除数で割ってきれいになるような想定数を見い出し，商の蔓の下に順に想定数と最後の商を置く．このようにして商の蔓を完成した後で）
>
> 33.　下（から二番目）の数を上の数にかけ，最下位の数を加える．(この操作を蔓の一番上まで続けて第二の蔓を作る．一番上に生じた数を）小さい余りを生ずる除数で割り，その余りに大きい余りを生ずる除数をかけ，大きい余りを加えると，二つの除数に対応するアグラになる．

ここでも見られるように，古代インドの文献では解かれるべき問題設定などは，必ずしも，誰にでも分かるようには定式化されておらず，詳細は師から弟子への口伝で伝えられたとみられる．

扱っている問題は

$$N = ax + R_1 = by + R_2 \quad (R_1 > R_2)$$

[*3] ジャヤデーヴァについては，[Shukla, 1954] を見よ．

[*4] とは言っても，クッタカがギリシアから，ないしは，ギリシアとの共通の起源から伝播したということを示す史料はない．また，ユークリッドの互除法を 1 次不定方程式の解法として説明するギリシアの史料もないようである．実際，[Dickson, 1920, Chapter 2] の冒頭の節 “Solutions of $ax + by = c$” はインドのクッタカの解説から始めてられている．次いで取り上げられているのは，17 世紀の Bachet によるものである．

[*5] インドの古典サンスクリットの数学文献は韻文で書かれた詩節からなっている。[プロフカー，2014] を見よ。

を満たす自然数 N（のうちで最小のもの）を求めることである（中国の剰余問題である）．これを，

$$(*) \qquad y = \frac{ax + c}{b}, \quad c = R_1 - R_2$$

の形の不定方程式と見て解いている．大きい余りとは R_1, それを生ずる除数とは a，小さい余りとは R_2, それを生ずる除数とは b のことである．最後に出てくるアグラとは，N のことである．雑に言うと，詩節 32 では，a と b に互除法を適用する過程を，詩節 33 では，その計算に基づいて問題の不定方程式の解を求める過程を説明している．クッタカは今回の主題ではないので，これ以上の詳細は付録 A.1 に譲る (pp. 27–31)．a, b が互除法によって，どんどん細かく割られていくことから「クッタカ」（粉砕法）と名づけられたと考えられる．

なお，ブラフマグプタやバースカラ II では，不定方程式 $(*)$ に現れる a, b, c, x, y を，それぞれ，**被除数** (**bhājya**), **除数** (**bhājaka**), **付数** (**kṣepa**), **乗数** (**guṇaka**), **商** (**labdhi**) と呼んでいる．

2　ブラフマグプタのバーヴァナー

ブラフマグプタは『ブラフマスプタシッダーンタ』で

$$Dx^2 + m = y^2$$

の形の不定方程式を **平方始原** (**vargaprakṛti**) という名前のもとで扱っている（[伊東，1987, pp. 419–423]，[林，2020, pp. 244–246] を見よ）．この方程式の D, m, x, y をそれぞれ，**始原数** (**prakṛti**)，**付数** (**kṣepa**)，**前根** (**ādyamūla, ptrathamamūla**) または**短根** (**kaniṣṭapada**)，**後根** (**antyamūla**) または**長根** (**jeyeṣṭapada**) と呼んでいる（というより，このように呼ばれたるものを我々は D, m, x, y によって上のように解釈している，と言うべきであろうか）．中世インドにおいてこの種の不定方程式の研究の一つの動機は，$\sqrt{D}$ のよい近似分数を求めるという問題にあったと言われている．（古代インドの『シュルバストートラ』に見られる正方形の対角線の長さの近似計算と $2x^2 + 1 = y^2$ との関係，より良い近似値を求める工夫がブラフマグプタのバーヴァナーと関係し得ることは，付録 A.2 pp. 31 – 33 を見よ．）

さて，バーヴァナー（生成，合成）とは，上の形の 2 次不定方程式の解 2 個から新しい解を生成する手段であり，その基本原理は次の恒等式である．

規則 1　$y_j^2 = Dx_j^2 + m_j$ $(j = 1, 2)$ のとき，

$$y = Dx_1x_2 \pm y_1y_2, \quad x = x_1y_2 \pm x_2y_1, \quad m = m_lm_2 \quad \text{（複号同順）}$$

とおくと，

$$y^2 = Dx^2 + m$$

が成り立つ．（ここで，符号を $+$ に取ったものを**和合成**，$-$ に取ったものを**差合成**という．）

言い換えれば，

$$(y_1^2 - Dx_1^2)(y_2^2 - Dx_2^2) = (Dx_1x_2 \pm y_1y_2)^2 - D(x_1y_2 \pm x_2y_1)^2$$

が成り立っている．これは，しばしば，**ブラフマグプタの公式**と呼ばれており，二次体のノルムの乗法性や二元二次形式の合成の先駆けと位置付けられることはよく知られている通りである．

いま，D を固定して，$y^2 = Dx^2 + m$ の関係が成り立つとき，$(x, y; m)$ と記すことにする．このとき，規則 1 は 2 つの解の合成演算

$$(x_1, y_1; m_1) \boxplus (x_2, y_2; m_2) := (x_1y_2 + x_2y_1, Dx_1x_2 + y_1y_2; m_1m_2),$$
$$(x_1, y_1; m_1) \boxminus (x_2, y_2; m_2) := (x_1y_2 - x_2y_1, Dx_1x_2 - y_1y_2; m_1m_2)$$

を与えている．

次の 2 つの規則は，付数が ± 4 となる解が得られているとき，付数が 1 となる解を生成する方法を与えている．

規則 4　$q^2 = Dp^2 + 4$ のとき，$\left(\frac{p(q^2-1)}{2}, \frac{q(q^2-3)}{2}\right)$ は $Dx^2 + 1 = y^2$ の解である．

規則 5　$Dp^2 - 4 = q^2$ で $r = \frac{1}{2}(q^2 + 3)(q^2 + 1)$ のとき，$(pqr, (q^2 + 2)(r - 1))$ は $Dx^2 + 1 = y^2$ の解である．

規則 4 は $(p, q; 4)^{\boxplus 3}$ を，規則 5 は $(p, q; -4)^{\boxplus 6}$ を，それぞれ計算することによって得られる．

さらに，付数が $\pm 1, \pm 2$ の場合からも，付数 1 の場合の解が得られることも，当然ながら，気づかれていた．

これらの「合成」規則によって，すでに得られた解から多くの解が生成されることは，注釈者たちによって述べられているところである．バースカラ II の『ビージャガニタ』では，

> 短長付数を置き，それらの下に同じそれらあるいは他のものを順に入れ，これらから生成により多くの根が得られる．だから，それらの生成が今から述べられる．……（[林，2016, p. 236]，強調は筆者．）

と前置きして，上の規則 1 にあたるものが説明されている．

ブラフマグプタの例

次の（[Katz-Parshall, 2014] で取り上げられた）ブラフマグプタによる例をみよう．

> “平方に 92 をかけ，1 を加えたものが，また平方である．この数を 1 年以内に計算できるならば，そのものは計算家である．”

ブラフマグプタの規則は，次のように始まる：

> “根を 2 回 (上下に）置く:その平方に乗数をかけ，それに適当な数を（それが平方となるように）加え，または，減じたものの根もそうする．”

言い換えると，任意の数，例えば 1 をとり，$92 \cdot 1^2 + b_0$ が平方となるような b_0 を目の子で見つける．$b_0 = 8$ とすれば，$92 \cdot 1^2 + 8 = 100 = 10^2$ である．これで $Dx_0^2 + b_0 = y_0^2$ となるような数 x_0, b_0, y_0 が見つかったわけである．すなわち，$(1, 10)$ は付数 8 に対する解である．

そこで，ブラフマグプタはこの解を 2 行にわたって書く：

$$\begin{matrix} x_0 & y_0 & b_0 \\ x_0 & y_0 & b_0 \end{matrix}$$

$$\begin{matrix} 1 & 10 & 8 \\ 1 & 10 & 8 \end{matrix}$$

彼の規則の説くところは

> “前根 (の組) の積に乗数をかけ後根 (の組) の積を加える．これが（新しい）後根である．(前根，後根を) 稲妻型にかけあわせた和が（新しい）前根である．(新しい）付数は付数の積である．この (新しい）2 つの根を（もとの）付数で割れば，付数 1（に対する根）となる．”

言い換えると，「後根」y の新しい値として $y_1 = Dx_0^2 + y_0^2$ をとっている．具体的には $y_1 = 92 \cdot 1^2 + 10^2 = 192$ である．「前根」x の新しい値は $x_1 = x_0y_0 + x_0y_0 = 2x_0y_0$ であり，したがって，$x_1 = 20$ である．新しい付数は $b_1 = b_0^2 = 64$ である．したがって，$(x_1, y_1) = (20, 192)$ は $b_1 = 64$ に対する解，すなわち，$92 \cdot 20^2 + 64 = 192^2$ が成り立っている．ブラフマグプタは x_1, y_1 を $b_0 = 8$ で割って，$(\frac{5}{2}, 24)$ を得る．これは，x が整数でないので解に適していないが，配列による同じ技巧を再度適用して，付数 1 に対する整数解 $(120, 1151)$, すなわち，$92 \cdot 120^2 + 1 = 1151^2$ を得ている．（[Katz and Parshall, 2014, pp.122–123].）

これを，すでに導入した記号法で書こう：$D = 92$ とする．$92 \cdot 1^2 + 8 = 10^2$ であるから，$(1, 10; 8)$ である．このとき，

$$(1, 10; 8) \boxplus (1, 10; 8) = (20, 92 + 100; 64) = (20, 192; 8^2) \quad \therefore \left(\frac{5}{2}, 24; 1\right)$$

が成り立つ．これは整数解ではないが，もう一度，自分自身と合成すると，

$$\left(\frac{5}{2}, 24; 1\right) \boxplus \left(\frac{5}{2}, 24; 1\right) = \left(120, 92 \cdot \frac{25}{4} + 24^2; 1\right) = (120, 1151; 1)$$

が得られる．

$83x^2 + 1 = y^2$ では，$83 \cdot 1^2 - 2 = 9^2$ であるから，

$$(1, 9; -2) \boxplus (1, 9; -2) = (18, 83 \cdot 1 + 81; 4) = (18, 164; 4)$$

となり，$(9, 82; 1)$ という（最小）正整数解が得られる．合成規則をさらに繰り返し適用すれば，非常に大きな解が容易に得られる．例えば，

$$\begin{aligned} &(9, 82; 1)^{\boxplus 2} = (1476, 13447; 1), \\ &(9, 82; 1)^{\boxplus 4} = (39695544, 361643617; 1), \\ &(9, 82; 1)^{\boxplus 6} = (1067571958860, 9726043422151; 1), \\ &(9, 82; 1)^{\boxplus 7} = (175075291425879, 1595011813884802; 1). \end{aligned}$$

3　チャクラヴァーラ

チャクラヴァーラのアルゴリズムは，初期解 $(p_1, q_1; m_1)$ から始めて，解 $(p_n, q_n; m_n)$ が与えられたとき，それから新しい解 $(p_{n+1}, q_{n+1}; m_{n+1})$ を構成し，最終的に $(p, q; 1)$ の形の解を得るものである．

チャクラヴァーラのアルゴリズム

初期解は，多くの場合，

$$(p_1, q_1; m_1) = (1, q_1, q_1^2 - D)$$

の形で，$\left|q_1^2 - D\right|$ が最小となるように $q_1 > 0$ が選ばれている．

では，$(p_n, q_n; m_n)$ が与えられたとして新しい解 $(p_{n+1}, q_{n+1}; m_{n+1})$ を構成するステップを説明しよう．p_n, q_n は互いに素としよう（$p_1 = 1$ だから初期解はこの条件を満たしている）．このとき，u をパラメータとして

$$(1, u; u^2 - D) \boxplus (p_n, q_n; m_n) = (q_n + p_n u, Dp_n + q_n u; (u^2 - D)m_n)$$

を考える．これより，

$$(p_{n+1}, q_{n+1}; m_{n+1}) = \left(\frac{q_n + p_n u}{m_n}, \frac{Dp_n + q_n u}{m_n}; \frac{u^2 - D}{m_n}\right)$$

とおく．ここで，$\mathrm{GCD}(p_n, m_n) \neq 1$ だったならば，$Dp_n^2 + m_n = q_n^2$ より $\mathrm{GCD}(p_n, q_n) \neq 1$ となり仮定に反するから，$\mathrm{GCD}(p_n, m_n) = 1$ である．したがって，（**クッタカにより**）$p_{n+1} = \dfrac{q_n + p_n u}{m_n}$ が整数となるように，パラメータ u を選ぶことができる．バースカラ II は次のように述べている：

> [平方始原の] 短根，長根，付数を [クッタカの] 被除数，付数，除数[*6]とみなして，その乗数を次のように想定すべきである，すなわち，（その）乗数の平方が，始原数から引かれるか，あるいは始原数を引かれたとき，残りが小さくなるように．
>
> それを付数で割ったものが付数である．ただし，始原数から引かれた場合には（正負を）逆にする．（その）乗数に対する商が短根である．それから長（根が得られる）．これを繰り返す．
>
> 前の根と付数を除去して．これを円環法と呼ぶ．このようにして，四と二と一を加えた場合の整数根二つが生ずる．
>
> 四と二を付数とする二根からルーパ [単位 1 のこと] を付数とするもののための生成が（行われるべきである）．([林，2016, p. 248])

この説明の最初の 2 段落が，上で紹介した新しい解を構成する手続きを述べている．第 1 段落で「残りが小さくなるように」とあるのはいささかあいまいであるが，上の記号で

[*6] p. 3 を見よ．

$|u^2 - D|$ が最小となる，したがって，次の段階の付数の絶対値が最小となるようにとる

と理解できる．ただし，バースカラ II は，ここで

u は正整数のみを考える

ことにしていると思われる．[*7] 第 3 段落は，この手続きを繰り返すと，付数 m が（必ず）$\pm 1, \pm 2, \pm 4$ の解が得られることを主張している．ここまでくれば，$m = 1$ となる解がバーヴァナーによって得られることはブラフマグプタの規則で示されており，それが第 4 段落の意味するところである．実は，上の手続きを繰り返せば，必ず $m = 1$ となる解に到達できるのだが，$m = -1, \pm 2, \pm 4$ の解が得られたならば，ブラフマグプタの規則を用いる方が計算上の近道となる．その一方で，理論的構造はかえって見にくくなることに注意しよう．

バースカラ II の例

$61x^2 + 1 = y^2$ の解法を調べてみよう（原典の訳は，[林，2016, p. 254–255]）．初期解 $(1, 8; 3)$ から出発する．このとき u は $8 + u$ が 3 で割り切れるように取る．$u = 3k + 1$ の形である．$\sqrt{61} = 7.81...$ であるから，これに最も近い u として $u = 7$ がとれる．[*8] 第 2 の解は

$$\left(\frac{8 + 1 \cdot 7}{3}, \frac{8 \cdot 7 + 61}{3}; \frac{7^2 - 61}{3}\right) = \left(\frac{15}{3}, \frac{117}{3}; \frac{-12}{3}\right) = (5, 39; -4)$$

となる．付数が -4 となったので，バースカラ II は，ここで，バーヴァナー（規則 5）を利用して解を出すのだが[*9]，ここでは，巡回性を確認するためにさらに先に進める．次には，$39 + 5u$ が 4 で割れるように取るのだが，$u = 4k - 7$ の形になる（-7 は先の u の -1 倍である．）$u = 9$ とで

[*7] このことは，これまでの文献で必ずしも明確に指摘されていない（はっきり $u > 0$ としているのは [Bauval, 2014] である）．[Datta and Singh, 1938 (Part II), p. 163] では，u は “arbitrary integral number” でよいといい，正負の指定はしていない．[Ayyangar, 1929-1930] でも 負でもよいと考えられている．しかし，実際のところ，バースカラ II（[林，2016]）でも [Datta and Singh, 1938 (Part II)] でも u を負に取る例は与えられていない．以下の $D = 61$ の例で，具体的に負に取ったときの問題点を例示する．

[*8] ここで $u = -3 \times 3 + 1 = -8$ とすれば，$u^2 - D = 64 - 61 = 3$ で $7^2 - 61 = -12$ より絶対値が小さい．したがって，u として負の整数も許容するならば，$u = -8$ と取ることになる．しかし，このとき，次の解は，

$$\left(\frac{8 + 1 \cdot (-8)}{3}, \frac{8 \cdot (-8) + 61}{3}, \frac{(-8)^2 - 61}{3}\right) = (0, -1; 1)$$

となり，解法としては機能しなくなる．もちろん，バースカラ II はこのようには取ってはいない．クッタカの解として負の数をとるという考え方はなかったので，あえて，正整数をとると言う必要なかったのであろうか．一般的に言うと，u として負の整数を許容すると，チャクラヴァーラのステップを逆行するケースが発生し，解に到達しなくなる可能性があるのである（p. 11 を見よ）．Ayyangar はこのような場合を例外として排除するが，アルゴリズムとしては曖昧さが残る．

[*9] ヴェイユは計算を「ちょいと近道をする程度」と言っているが，以下のように，手計算をしようとしたら，これは大いなる近道である．p. 28 で見るように，アールヤバタによるクッタカの説明においても，アルゴリズムを目視で解が出るようになるところで止めており，インドの数学はとことん計算志向である．

きる．このとき，第 3 の解として，

$$\left(\frac{39+5\cdot 9}{-4}, \frac{39\cdot 9+61\cdot 5}{-4}; \frac{9^2-61}{-4}\right)$$
$$= \left(\frac{84}{-4}, \frac{656}{-4}; \frac{20}{-4}\right) = (-21, -164; -5) \sim (21, 164; -5)$$

を得る．次は，$164+21u$ が 5 で割り切れるようにするのだが，$u = 5k-9$ の形になる．よって，$u = 6$ とする．このとき，第 4 の解として，

$$\left(\frac{164+21\cdot 6}{-5}, \frac{164\cdot 6+61\cdot 21}{-5}; \frac{6^2-61}{-5}\right)$$
$$= \left(\frac{290}{-5}, \frac{2265}{-5}; \frac{-25}{-5}\right) = (, -58, -453; 5) \sim (58, 453; 5)$$

を得る．以下同様に進めると 13 ステップ後に $m = 1$ に到達し循環する．

そのサイクルは

$$\begin{aligned}
&(p, q; m, u) = (1, 8; 3, 8)\\
&\longmapsto (5, 39; -4, 7) \longmapsto (21, 164; -5, 9) \longmapsto (58, 453; 5, 6)\\
&\longmapsto (195, 1523; 4, 9) \longmapsto (722, 5639; -3, 7)\\
&\longmapsto (3805, 29718; -1, 8) \longmapsto (60158, 469849; -3, 8)\\
&\longmapsto (296985, 2319527; 4, 7) \longmapsto (1248098, 9747957; 5, 9)\\
&\longmapsto (3447309, 26924344; -5, 6) \longmapsto (11590025, 90520989; -4, 9)\\
&\longmapsto (42912791, 335159612; 3, 7) \longmapsto (226153980, 1766319049; \mathbf{1}, 8)\\
&\longmapsto (3575550889, 27925945172; 3, 8)
\end{aligned}$$

この計算により，$61x^2+1 = y^2$ の解として，

$$61\cdot 226153980^2 + 1 = 1766319049^2$$

が得られた．

注意: この例で i 番目の解における m, u を m_i, u_i とおき，$m_0 = 1, u_1, m_1, u_2, m_2, \ldots, u_{14}, m_{14} = 1$ と並べた数列を考える．すなわち，

$$1, 8, 3, 7, -4, 9, -5, 6, 5, 9, 4, 7, -3, 8, -1, 8, -3, 7, 4, 9, 5, 6, -5, 9, -4, 7, 3, 8, 1$$

を考える．この数列は，

- $m = -1$ となったあとは，付数 m の符号が反転し，補助数 u が繰り返している；
- 全体として回文になっている．すなわち，右から読んでも，左から読んでも同じ数列である；

という性質を持っていることに注意が引かれる．後に，これが一般的現象であることを示す (p. 26).

4　チャクラヴァーラをめぐる論点

チャクラヴァーラがどのように機能するかを具体例で見てみたが，このアルゴリズムについて，理論的には次のような問題が生ずる．

(A) $p_{n+1} = \frac{q_n+p_nu}{m_n}$ が整数となるようにパラメータ u を選んだのだったが，このとき，q_{n+1}, m_{n+1} も整数となり必ず整数解を与えているのか? また，p_{m+1}, q_{m+1} は互いに素で，次のステップに進むことができるのか?

(B) チャクラヴァーラ＝円環法と言っているが，何を円環と見ることができるのか（何が循環しているのか）？

(C) どのような D に対しても，チャクラヴァーラの手続きを繰り返せば，必ず $m = 1$ となる解が得られることが示せるのか?

が問題となる．中世インドの文献には，これらについて説明は与えられていない．

問題 (A)

問題 (A) は簡単である．インド数学史の大著 [Datta and Singh, 1938 (Part II), p. 172] では，バースカラ II 自身も証明を知っていただろうと推測している．しかし，このことの証明が文献に現れたのは，[Hankel, 1874, p. 201] が最初のようである．

【(A) の証明】

$$p_n \cdot \frac{Dp_n + q_nu}{m_n} = \frac{Dp_n^2 + p_nq_nu}{m_n} = \frac{q_n^2 - m_n + p_nq_nu}{m_n} = q_n \cdot \frac{q_n + p_nu}{m_n} - 1$$

であるから，u の取り方により，これは整数である．また，$\mathrm{GCD}(p_n, m_n) = 1$ であったから，$q_{n+1} = \frac{Dp_n+uq_n}{m_n}$ も整数であり，したがって，

$$m_{n+1} = \frac{u^2 - D}{m_n} = \left(\frac{Dp_n + uq_n}{m_n}\right)^2 - D \cdot \left(\frac{q_n + p_nu}{m_n}\right)^2$$

も整数である．また，

$$p_{n+1}q_n - p_nq_{n+1} = \frac{q_n(q_n + p_nu) - p_n(Dp_n + uq_n)}{m_n} = \frac{q_n^2 - Dp_n^2}{m_n} = \frac{m_n}{m_n} = 1 \tag{4.1}$$

だから，$\mathrm{GCD}(p_{n+1}, q_{n+1}) = 1$ である．　□

注意：　冒頭で，[Katz and Parshall, 2014, p. 126] に (C) の証明は「19 世紀まで得られなかった」との記述があるが誰の仕事を指すのか不明であったことが，チャクラヴァーラを勉強し始めるきっかけだったと書いたが，なぜこのような記述がなされたのかについての解答は次のようなものだと推測する．

- [Katz and Parshall, 2014, p. 126] にこのことの典拠は示されていないが，インドの数学についての彼らの記述は [Plofker, 2007], [Plofker, 2009] に大いに依拠している．
- [Plofker, 2009, p. 195, 脚注 36] には，

  “円環法が常に，ついには k_i [ここでの記号では m_n] として求めたい値である 1 を生成するという事実 [すなわち，(C)] の証明をバースカラは与えていない．実際，これは 19 世紀の H. Hankel の研究まで証明されることはなかった．[Datta and Singh, 1938 (Part II), p. 172] を見よ．”

  と書かれている．これが，Katz-Parshall の主張のもととなったのであろう．
- [Datta and Singh, 1938 (Part II), p. 172] に “Hankel's Proof” というものが確かに書かれているが，しかし，それは，上に述べた (A) の証明であって，(C) の証明ではない．Plofker の理解は誤りである．
- したがって，[Katz and Parshall, 2014, p. 126] の記述は Plofker の誤読を踏襲してしまったものと推測される．Plofker が名前を挙げている Hankel 自身は (C) の証明を Lagrange に帰している（[Hankel, 1874, p. 202]）．これが通説であろう．

問題 (B) を論ずる前に，**クッタカの除去**について説明しておこう．すなわち，上で (p. 6) パラメータ u の選び方にクッタカを利用するように述べたが，実はクッタカは必要ないのである．このことは，[Ayyangar, 1929 – 30], [ヴェイユ，1987, p.24] で指摘されているが，そこでヴェイユは，

> 全く不可思議なことなのだが，我々のインド人著者たちは誰一人として（さらには 16 世紀に至るまでの注釈者たちでさえ）このことには気づいていなかったように思われる；彼らはそれに言及していないばかりか，x [ここでは u] を選ぶに当たっては，一様にクッタカに訴えている；数値例をたっぷりと持っていたのだから，クッタカの必要がないことは容易に見ぬけてよさそうなものだが …

ともいう．（このことを最初に指摘したのが誰かはよくわからない．[Datta-Singh, 1935; 1938] にも [Hankel, 1874] にもその指摘はない．[Dutta, 2010] は [Ayyangar, 1929 – 30] が指摘したと書いている）．さて，クッタカを使う必要がないとは次のような事情による．

チャクラヴァーラの出発点となる解 $(p_1, q_1; m_1) = (1, q_1; q_1^2 - D)$ をとる．このとき，u としては，$q_1 + u$ が m_1 で割り切れるように取る，すなわち，$u = m_1 t - q_1$（$t \in \mathbb{Z}$ は $|u^2 - D|$ が小さくなるように取ればよい）とクッタカを使うまでもなく解ける．一般に，$(p_{n-1}, q_{n-1}; m_{n-1})$ から $(p_n, q_n; m_n)$ を定める際に取るパラメータを $u = u_n$ と記すことにする．このとき

$$(p_n, q_n; m_n) = \left(\frac{q_{n-1} + p_{n-1}u_n}{m_{n-1}}, \frac{Dp_{n-1} + q_{n-1}u_n}{m_{n-1}}; \frac{u_n^2 - D}{m_{n-1}} \right)$$

から $(p_{n+1}, q_{n+1}; m_{n+1})$ を定めるには，$q_n + p_n u$ が m_n で割り切れるように u を選び $u = u_{n+1}$

としなくてはならないが,

$$\begin{aligned} p_n u_n - q_n &= \frac{q_{n-1} + p_{n-1}u_n}{m_{n-1}} \cdot u_n - \frac{Dp_{n-1} + q_{n-1}u_n}{m_{n-1}} \\ &= \frac{p_{n-1}(u_n^2 - D)}{m_{n-1}} = p_{n-1}m_n \end{aligned}$$

であるから，$u\,(= u_{n+1}) = m_n t - u_n$ の形の数の中から $|u^2 - D|$ が小さいものをとればよい．ここでクッタカ法を利用する必要はないのである．まったく，ヴェイユの言う通りで，数値例を多数見ていれば，u の属す法 m の合同類の形は計算することなく決まっていることに気付く方が普通に思えてくる．

この事実の重要性は次の点にある：

> u_{n+1} の決定に p_n, q_n の値は関わらず，u_n, m_n（と D）のみで定まる．すなわち，
>
> (4.2) $\quad (u, m) \longmapsto (u', m'), \quad \begin{cases} u' \equiv -u \pmod{m} \text{ で } {u'}^2 \text{ は } D \text{ に最も近い正整数}, \\ m' = \frac{(u')^2 - D}{m} \end{cases}$
>
> と与えられる．

注意： (1) 上の条件で u' が一意的に定まるわけではない．例えば，$D = 58$ の場合，初期解 $(p_1, q_1; m_1) = (1, 8; 6)$ から $u' = u_1 \equiv 4 \pmod{6}$ が出てくるが $58 - 4^2 = 10^2 - 58 = 42$ であり，$u' = 4, 10$ を区別する原理はない．この点には注意が必要である（例 5.3.7, §5.3.4 を見よ）．

(2) もし u として負の整数も許したとすると，u'' を決定する際に，$u'' \equiv -u'$ となり，u'' として u をとることになるという場合が発生しうる．このようにとってしまうとチャクラヴァーラのステップが逆行することになり，解が得られなくなる．アルゴリズムの定式化においては，このことを何らかの形で回避するようにしなければならない．

(B) 何が循環しているのか

[ヴェイユ，1987, p. 25] では

> “… [チャクラヴァーラのプロセスを] 続ければ，「付加因子」[ここでは「付数」と呼んだ] $m, m', m'', \ldots$ が繰り返し周期的に現れ，その本性が自然に浮かび上がってくることになる；この現象は $\sqrt{N}$ [ここの記号では $\sqrt{D}$] の連分数の周期性に対応している”

とある．この引用はチャクラヴァーラで循環するのは付数であるような印象を与えるが，実際に，循環するのは，(m, u) の組と考えるべきである．

(m, u) が循環することを見るために，まず，チャクラヴァーラのプロセスで現れる付数 m を評価しよう．$q_1 = [\sqrt{D}]$，すなわち，$\sqrt{D} - 1 < q_1 < \sqrt{D}$ と選んだとしよう．このとき，$q_1^2 < D < (q_1 + 1)^2 = q_1^2 + 2q_1 + 1$ だから，u_1^2 を　q_1^2 と $(q_1 + 1)^2$ の D に近い方とすれ

ば，$\left|u_1^2 - D\right| \leq q_1 + \frac{1}{2}$ であり，$u_1^2 - D$ は整数だから，$\left|u_1^2 - D\right| \leq q_1 < \sqrt{D}$ である．よって，$|m_1| = |u_1^2 - D| < \sqrt{D}$ である．

一般に $n \geq 1$ に対し $|m_n| < \sqrt{D}$ が成立つ（系 5.3.9 を見よ）．したがって，チャクラヴァーラのプロセスで現れる付数 m_n で相異なるものは有限個しかない．

u_{n+1} は法 m_n で定まり，$\pm\sqrt{D}$ に近くとるのであるから，$|u_n| < \frac{3}{2}\sqrt{D}$ $(n \geq 1)$ の範囲にある．よって，登場する (m, u) も相異なるものは有限個である．したがって，チャクラヴァーラのステップを繰り返すと，いつか (m, u) のサイクルができる．サイクルができたとたんにその後の m と u のペアは同じサイクルを繰り返すことが分かる．ここで，先の $61x^2 + 1 = y^2$ の例の計算を見るとよく分かるが，上で述べたように，m だけが元に戻ったからといってサイクルが成立したわけではないことには注意しよう．

【$m = 1$ で循環することの証明】　ひとたび $m = 1$ になると次から繰り返しが始まることにも注意しておこう．一般に，チャクラヴァーラの出発点として u_1^2 が D に最も近い整数 u_1) をとり，初期解 $(u_1, 1, u_1^2 - D)$ からスタートしたとする．このときのデータは $(m, u) = (u_1^2 - D, u_1)$ である．ある時点で $m = 1$ となる解に到達したとする．このとき，$p + qu$ は常に $m = 1$ で割れるから，u としては，出発点で利用した u_1 をとることができ，新しい付数は $\frac{u_1^2 - D}{1} = u_1^2 - D$ となり，出発点と同じ $(m, u) = (u_1^2 - D, u_1)$ に戻っている．□

したがって，

(C)　チャクラヴァーラの手続きを繰り返すことで，必ず，$m = 1$ がいつか現れる

が示されれば，$(u, m) = (u_1, u_1^2 - D)$ から始まるサイクル中に現れる (u, m) 達だけが純循環となる．

さて，チャクラヴァーラ（円環法）という名称から，このようなサイクルの成立を見てとっているはずであるが，上で述べたように，バースカラ II では計算を簡略化する規則 4,5 (p. 4) 等を適用するため，かえって巡回性が明瞭になっていないきらいがある．

またこの (m, u) の巡回性は，各段階で u をそのつど（p_n, q_n の情報を含む）クッタカによって求めるのではなく，以前の段階で得られている m, u のみから求められるという認識があって，初めて確認されることに注意しよう．u を決定する 1 次不定方程式 $m_n x = q_n + p_n u$ は係数が確実に増大し，巡回性を示す対象ではないからである．したがって，インドの数学者が円環法のサイクルの存在を理論的に理解できていたならば，クッタカが不要であることの重要性を認めて記録していたに違いない．$m = 1$ になると循環が始まることの上の説明のようなことは気付いていたと思われるが，巡回性はインドの数学者にとって理論的把握というよりは経験的真理にとどまるものであったことを示すものであろう．

問題 (C) とチャクラヴァーラの現代的解釈

ペル方程式（より一般に二元二次形式）の解法は，17 世紀以降，ヨーロッパにおいて，フェルマ，ウォリス，ブランカー，オイラー，ラグランジュによって発展するが，これらを跡付けていくことは [ヴェイユ，1987] を見てほしい．

ここでは，チャクラヴァーラの方法によって常にペル方程式を解くことができる（問題 (C)）ことの証明をめぐる議論を紹介する．それはチャクラヴァーラとは何かという解釈の問題ということもできる．[Selenius, 1975] は 19 世紀以来のインド数学に触れた数学史書における諸説を整理している．それによると，20 世紀初頭までのほとんどの数学史書は，チャクラヴァーラとラグランジュの理論とを同一視し，チャクラヴァーラの方法の正当性を示したのは，ラグランジュであるとしている．しかし，[Ayyangar, 1929–30] を嚆矢として，ラグランジュの方法とチャクラヴァーラの差異を強調し，その通説に異議を唱える論者もいる（例えば，[Selenius, 1975], [Dutta, 2010, p. 153] など）[*10]．

その議論の要点は，p. 11 の (♯) で与えた u' を決定する条件に関わっている．バースカラ II の記述では，$u' \equiv -u \pmod{m}$ という合同条件の下で

M.1 $\left|u'^2 - D\right|$ が最小となるような正整数 u' を選ぶ

ことを指示しているように読める．（ここで，u は負でも良いとする考え方もあるが，そこには問題点も生ずることは，脚注 *7, *8, および，p. 11 の注意 (2) で指摘した．）

しかし，同じ合同条件の下で

M.2 $\left|\sqrt{D} - u'\right|$ が最小になるような整数 u' を選ぶ
M.3 $u' < \sqrt{D}$ かつ $\sqrt{D} - u'$ が最小になるような整数 u' を選ぶ

という条件でも同様に機能するアルゴリズムが得られるのではないかと思われる．（p. 11 の注意 1 で例を挙げたが，M.1 では u' に相異なる 2 つの選択肢が生ずる可能性がある．M.2, M.3 ではそのようなことはなく，また，u' を負に取ることから生ずる問題もなく，むしろアルゴリズムとして明解である．）結論的に言うと，

- M.3 のアルゴリズムは，$\sqrt{D}$ の正則連分数展開を用いるラグランジュの方法，ガウスによる判別式が正の二元二次形式の簡約理論による方法と数学的には同等である．
- チャクラヴァーラのアルゴリズム M.1 は M.3 よりも早く $Dx^2 + 1 = y^2$ の解に到達するというメリットはある．（M.1 と M.2 はさほどの違いはなく，M.2 の立場をとれば計算が簡単になることは，ブランカー，ウォリスも気付いていたという [ヴェイユ，1987, p. 97]．）
- 　したがって，チャクラヴァーラの方法は，細かいことを言えば，（ブランカー，ウォリス，オイラー,）ラグランジュの方法と違うことは確かであるが，その差異をどれほど大きなも

[*10] [Dutta, 2010, p. 153] は [Ayyangar, 1929–30] が元来のチャクラヴァーラの方法の正当性を証明した最初の文献としているが，その証明には瑕疵がある．その点は後に説明する (p. 19).

のと考えるかは，趣味の問題のように感じられる．実際，インドの原典では，そのような点について細かい議論をしてはいない．

- Ayyangar, Selenius のような論者は，いずれも，チャクラヴァーラに連分数による現代的解釈を与えた上で，ラグランジュとの違いを（u' の選択の問題というより），通常の正則連分数展開を用いるのか，非正則な連分数展開を用いるのかの違いとして捉えて，いかなる連分数論がチャクラヴァーラを正確に表現しているのかという問題の立て方をしている．しかし，チャクラヴァーラとフェルマ以降ヨーロッパで発達したペル方程式の理論との本質的違いは，
  - チャクラヴァーラでは，考えている二元二次形式 $y^2 - Dx^2$ は固定され，解を変換することで $y^2 - Dx^2$ がとる値 m を小さくしていくと考えており，
  - 近代的理論では，二元二次形式そのものの変換=被約化（ないしは、その根の変換=連分数展開）を考えている

  という視点の違いにこそあると見るべきだと考える．このことに比べれば，u' の選択の仕方からくるアルゴリズムの違いやそれに対応する連分数論の違いは二義的であろう．

5 チャクラヴァーラの数学的構造

5.1 二元二次形式の簡約理論との関係

以下では，記号を簡潔にするために，2×2 行列 S と $2 \times r$ 行列 T $(r = 1, 2)$ に対して

$$S[T] := {}^tTST$$

とおく．また，$T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}$ のとき，

$$S[T] = S \begin{bmatrix} t_1 & t_2 \\ t_3 & t_4 \end{bmatrix}$$

と T の ( ) を省略することにする．

一般に $Dx^2 + m = y^2$ の形の不定方程式を考えるが，目標は $m = 1$ となる解，すなわち，

$$Dx^2 + 1 = y^2 \quad D \text{ は平方数でない正整数}$$

の正整数解であった．以下，$(x, y; m)$ と書いたときには，$Dx^2 + m = y^2$ が成り立っているとする．チャクラヴァーラのアルゴリズムは次のようなものであった：

C.1（簡単のため）自明な初期解 $(p_0, q_0; m_0) = (0, 1; 1)$ から出発する．また $u_0 = 0$ とおく．

C.2 $(p_n, q_n; m_n), u_n$ $(n \geq 0)$ が与えられたとき，u_{n+1} を

$$u_{n+1} \equiv -u_n \pmod{m_n}$$

となるように取る．ここで，u_{n+1}^2 が何らかの意味で D に近くなるようにするのだが，当面，そのやり方は特に指定しないことにする．

C.3 $(p_{n+1}, q_{n+1}; m_{n+1})$ は

$$p_{n+1} := \frac{q_n + p_n u_{n+1}}{m_n}, \quad q_{n+1} := \frac{Dp_n + q_n u_{n+1}}{m_n}, \quad m_{n+1} := \frac{u_{n+1}^2 - D}{m_n}$$

と定義される．

上のように自明な初期解から始めると，次の段階が

$$(p_1, q_1; m_1) = (1, u_1; u_1^2 - D)$$

とこれまでの節で初期解と呼んでいたものになる．

さて，p_n, q_n は次第に増大していくが，すでに説明したように，(u_n, m_n) は周期的になる．ここで，(u_n, m_n) に m_{n-1} を付け加えて $n \geq 0$ に対し，2×2 対称行列

$$S_n = \begin{pmatrix} m_n & u_n \\ u_n & m_{n-1} \end{pmatrix},$$

ないしは，S_n に付随する二元二次形式

$$f_n(X, Y) = m_n X^2 + 2u_n XY + m_{n-1} Y^2$$

を考えよう．ただし，$m_{-1} = -D$，すなわち，$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & -D \end{pmatrix}$, $f_0(X, Y) = X^2 - DY^2$ とする．このとき，$\det S_n = -(u_n^2 - m_{n-1}m_n) = -D$，言い換えると，$f_n(X, Y)$ の判別式はすべて D である．

さて，$u_{n+1} + u_n \equiv 0 \pmod{m_n}$ であったから，

$$u_{n+1} + u_n = \ell_{n+1} m_n \quad (\exists \ell_{n+1} \in \mathbb{Z})$$

と表すことができる．この ℓ_{n+1} を用いると，

$$\begin{aligned} S_n \begin{bmatrix} \ell_{n+1} & 1 \\ -1 & 0 \end{bmatrix} &= \begin{pmatrix} \ell_{n+1} & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} m_n & u_n \\ u_n & m_{n-1} \end{pmatrix} \begin{pmatrix} \ell_{n+1} & 1 \\ -1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} m_{n-1} - 2\ell_{n+1}u_n + m_n \ell_{n+1}^2 & -u_n + \ell_{n+1} m_n \\ -u_n + \ell_{n+1} m_n & m_n \end{pmatrix} \\ &= \begin{pmatrix} m_{n+1} & u_{n+1} \\ u_{n+1} & m_n \end{pmatrix} = S_{n+1} \end{aligned}$$

となる．$\begin{pmatrix} \ell_{n+1} & 1 \\ -1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$ であるから，（u_{n+1} の取り方の指定は保留しておくと）チャクラヴァーラのアルゴリズムは，S_n をそれと狭義同値（ガウスの用語では正式同値）な S_{n+1} へと変換することになっている．この変換 $S_n \longmapsto S_{n+1}$ を**被約化写像**と呼ぶことにしよう．

● **アルゴリズム M.3 とガウスの簡約理論**

判別式が正（で非平方数）の二元二次形式の簡約理論は, ガウスの *"Disquisitiones Arithmeticae"* の 第 5 章 183 条から 205 条で扱われている（[ガウス，1995, pp. 167–204]）．ガウスは判別式 $D > 0$ の二元二次形式に対し，

$$S = \begin{pmatrix} a' & b \\ b & a \end{pmatrix} \longmapsto S' = \begin{pmatrix} a'' & b' \\ b' & a' \end{pmatrix}, \quad \begin{cases} b' \equiv -b \pmod{a'}, \sqrt{D} - |a'| < b' < \sqrt{D}, \\ a'' := \frac{(b')^2 - D}{a'} \end{cases}$$

という被約化写像を考えた. これは $S = S_n$ に適用すれば, 上の C.2 において u_{n+1} を $\sqrt{D} - |m_n| < u_{n+1} < \sqrt{D}$ ととったものであるから，p. 13 のアルゴリズム M.3 そのものである．

ガウスは

$$S = \begin{pmatrix} a' & b \\ b & a \end{pmatrix} \text{が}\textbf{被約} \quad \Longleftrightarrow 0 < \sqrt{D} - b < |a| < \sqrt{D} + b$$

と定義し，

- D を固定したとき，判別式 D の被約形式は有限個しか存在しない;
- 判別式 D の任意の S は被約化写像を繰り返すことで，必ず被約形式に到達する;
- 被約化写像は，被約形式を被約形式に移し，異なる被約形式は異なる被約形式に移される．
- したがって，被約化写像を繰り返すことで，判別式 D の被約形式のなす有限集合は純循環するサイクルに分割される．異なるサイクルに属す二元二次形式は狭義同値ではない．

等の性質を証明した．

$S_0 = \begin{pmatrix} 1 & 0 \\ 0 & -D \end{pmatrix}$ に被約化写像を施したものは $S_1 = \begin{pmatrix} u_1^2 - D & u_1 \\ u_1 & 1 \end{pmatrix}$ で，M.3 の条件下では $u_1 = [\sqrt{D}]$ であるから，S_1 はガウスの意味で被約になっている．したがって，アルゴリズム M.3 によって被約化写像を繰り返し適用すれば，ある $p \geq 1$ に対し，$S_{p+1} = S_1$, したがって，$m_p = 1$ となり，ペル方程式の解が見つかることになる．

5.2 連分数展開との関係

次に，この二元二次形式（二次対称行列）の被約化写像を，2 次無理数の連分数展開と結び付けよう．一般に

$$f(X, Y) = aX^2 + 2bXY + cY^2 = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{bmatrix} X \\ Y \end{bmatrix}$$

を判別式 $D = b^2 - ac > 0$ が非平方数である整数係数二元二次形式とする．$f(X, 1) = aX^2 + 2bX + c = 0$ の二根 $\frac{-b \pm \sqrt{D}}{a}$ のうち，$\alpha := \frac{-b + \sqrt{D}}{a}$ をその**第 1 根**，$\beta := \frac{-b - \sqrt{D}}{a}$ をその**第 2 根**と呼ぶ．ここで，$U \in GL_2(\mathbb{Z})$ として，$f(X, Y)$ を

$$f'(X, Y) := a'X^2 + 2b'XY + c'Y^2, \quad \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} = (\det U) \begin{pmatrix} a & b \\ b & c \end{pmatrix} [U]$$

に変換し（$\det U$ 倍に注意），α', β' をその第 1 根，第 2 根とすると，

$$\alpha = U \cdot \alpha' := \frac{p\alpha' + q}{r\alpha' + s}, \quad \beta = U \cdot \beta' := \frac{p\beta' + q}{r\beta' + s}, \quad U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

が成り立つことが知られている．

通常の正則連分数展開とチャクラヴァーラのアルゴリズムを結び付けるには，上の S_n とは異なる対称行列

$$T_n = \begin{pmatrix} |m_n| & -u_n \\ -u_n & -|m_{n-1}| \end{pmatrix} \quad (n \geq 0)$$

を用いると便利である．$(-1)^{n-1} m_n > 0$ であるから，S_n とは

$$T_n = \begin{pmatrix} (-1)^{n-1} m_n & -u_n \\ -u_n & (-1)^{n-1} m_{n-1} \end{pmatrix} = (-1)^{n-1} S_n \begin{bmatrix} (-1)^n & 0 \\ 0 & 1 \end{bmatrix}$$

という関係にある．

整数 l_{n+1} を $u_n + u_{n+1} = l_{n+1}|m_n|$ となるようにとる．$l_{n+1} = (-1)^{n+1}\ell_{n+1}$ の関係がある．この l_{n+1} を用いると，T_n と T_{n+1} の関係が

$$-T_n \begin{bmatrix} l_{n+1} & 1 \\ 1 & 0 \end{bmatrix} = T_{n+1} \tag{5.3}$$

と表せる．（左辺の $-$ は $\det \begin{pmatrix} l_{n+1} & 1 \\ 1 & 0 \end{pmatrix} = -1$ から来ている．）ここで，T_n（に付随する二次方程式）の第 1 根を α_n とすると，

$$\alpha_n = \frac{u_n + \sqrt{D}}{|m_n|}$$

であり，α_n と α_{n+1} の間には，(5.3) により

$$\alpha_n = \begin{pmatrix} l_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \cdot \alpha_{n+1} = l_{n+1} + \frac{1}{\alpha_{n+1}}$$

という関係がある．ここで，u_{n+1} は M.3 のアルゴリズムに従って選ばれているとすると，

$$\sqrt{D} - |m_n| < u_{n+1} < \sqrt{D}$$

であり，これを変形すると，

$$0 < \frac{-u_{n+1} + \sqrt{D}}{|m_n|} < 1$$

となる．一方，$u_n + u_{n+1} = l_{n+1}|m_n|$ を用いると，

$$\alpha_n - l_{n+1} = \frac{u_{n+1} + \sqrt{D}}{|m_n|} - l_{n+1} = \frac{-u_{n+1} + \sqrt{D}}{|m_n|}$$

となるから，

$$0 < \alpha_n - l_{n+1} < 1, \quad \text{したがって}, \quad l_{n+1} = [\alpha_n]$$

が得られる．すなわち，$\alpha_0 = \sqrt{D}, \alpha_1, \alpha_2, \ldots$ は $\sqrt{D}$ の連分数展開を与えている．以上で，M.3 のアルゴリズムによるチャクラヴァーラは，$\sqrt{D}$ の連分数展開によるラグランジュの解法とも同等であることも分かった．

注意： u_{n+1} を M.2 のアルゴリズムで決定するならば，[Minnigerode, 1887], [Hurwitz, 1889] で扱われたタイプの連分数展開に対応する．M.1 のアルゴリズムに対応する連分数展開は，Ayyangar, Selenius によって研究されている（関連文献は [Selenius, 1975] の文献表を見よ．[Matthews, Robertson, and White, 2010] も見よ）．

5.3 M.1 に基づくチャクラヴァーラの巡回性の証明

もともとのチャクラヴァーラの方法（M.1）によるペル方程式の解法の正当化は，[Ayyangar, 1929–1930] でなされているが，その証明には，とくに，u_{n+1} に 2 通りの選択肢が存在するときが十分には扱われていない．[Bauval, 2014] はそのギャップを埋め，既存の二元二次形式論や連分数論を用いない（そうは言っても，証明の基本的考え方はガウスの簡約理論と実質的に同じであるが）初等的な証明を与えている．以下では，Bauval の証明を多少補足を加えながら，紹介する．

5.3.1 法 m の最良平方近似

D を正整数で平方数ではないとする．m を 0 と異なる整数とする．整数 $u > 0$ が D の**法 m の最良平方近似**であるとは，与えられた法 m の合同類の中で $|u^2 - D|$ が最小となるような u のことを言う．$|m| < \sqrt{D}$ のとき，法 m の最良平方近似は

$$0 < u_1 < \sqrt{D} < u_2 = u_1 + |m|$$

となる u_1, u_2 のいずれかである．m が偶数ならば，$D - u_1^2 = u_2^2 - D$ となることがある．実際，

$$D - u_1^2 = u_2^2 - D \Longleftrightarrow D = u_1^2 + |m|u_1 + \frac{m^2}{2}$$

であるから，m が偶数ならこのようなことが起こり得る．D, m が指定されているとき，このようなことは 1 回しか起こらないことに注意．このような場合を**例外ケース**といおう．

定理 5.3.1 m が 0 と異なる整数, u が正整数で

$$|m| < \sqrt{D}, \quad u^2 - D \equiv 0 \pmod{m}$$

が成り立つとする．このとき $m' = \frac{u^2 - D}{m}$ とおくと，次は同値である．

(1) u は法 m の最良平方近似.

(2) $m'^2 + \frac{m^2}{4} \leq D$.

(3) $u \geq |m'| + \epsilon \cdot \frac{|m|}{2}$, $\epsilon = \begin{cases} 1 & (u^2 > D) \\ -1 & (u^2 < D) \end{cases}$.

【証明】 条件は m の正負に無関係であるから，$m > 0$ で $m' = \left|\frac{u^2-D}{m}\right| > 0$ として絶対値符号を外した形で証明すれば十分である．

(i) $u > \sqrt{D}$ のとき：

$$\begin{aligned}(1) &\Longleftrightarrow u^2 - D \le D - (u-m)^2 \Longleftrightarrow u^2 - D \le mu - \frac{m^2}{2} \\ &\Longleftrightarrow mm' \le m\left(u - \frac{m}{2}\right) \Longleftrightarrow (3) \Longleftrightarrow u^2 \ge m'^2 + mm' + \frac{m^2}{4} \\ &\Longleftrightarrow (2)\end{aligned}$$

である．（最後の同値では，$mm' = u^2 - D$ を用いた．）

(ii) $u < \sqrt{D}$ のとき：

$$(1) \Longleftrightarrow D - u^2 \le (u+m)^2 - D \Longleftrightarrow D - u^2 \le mu + \frac{m^2}{2}$$

である．この右辺の不等式について

$$\begin{aligned}&\text{右辺} \Longleftrightarrow mm' \le m\left(u + \frac{m}{2}\right) \Longleftrightarrow (3) \\ &\text{右辺} \Longleftrightarrow u^2 + mu + \frac{m^2}{2} - D \ge 0 \quad (D > m^2 \text{ より } u = 0 \text{ で左辺は負}) \\ &\Longleftrightarrow u \ge -\frac{m}{2} + \sqrt{D - \frac{m^2}{4}}\ (> 0) \\ &\Longleftrightarrow u^2 \ge D - m\sqrt{D - \frac{m^2}{4}} \Longleftrightarrow m\sqrt{D - \frac{m^2}{4}} \ge D - u^2\ (= mm') \\ &\Longleftrightarrow D \ge m'^2 + \frac{m^2}{4} \Longleftrightarrow (2)\end{aligned}$$

となる． □

この定理は [Ayyangar, 1929–1930] にあるのだが，そこでは，(2) の条件が $\le$ でなく $<$ となっており，不備があった．等号となる場合は後の命題 5.3.5 にあるように，最良平方近似が 1 つに定まらない場合である．

定義 5.3.2　整数 m と正整数 u の組 (m, u) について，

$$|m| < \sqrt{D} \text{ で } u \text{ が } D \text{ の法 } m \text{ の最良平方近似}$$

のとき (m, u) を **nice pair** という．さらに，$m' = \frac{u^2-D}{m}$ について，(m', u) も nice pair（すなわち，u が D の法 m' の最良平方近似でもある）ならば，(m, u, m') を **reduced triple** という．

補題 5.3.3　(m, u) が nice ならば $|m'| < \sqrt{D}$ であり，さらに $|m'| \ge |m|$ ならば，(m, u, m') は reduced triple である．

【証明】 定理 5.3.1 の (2) により，$|m'| < \sqrt{D}$ は直ちに従う．合同条件 $u^2 - D \equiv 0 \pmod{m}'$ は m' の定義により自動的に成り立っている．$|m'| \ge |m|$ ならば　$m^2 + \frac{m'^2}{4} \le m'^2 + \frac{m^2}{4} \le D$ だから，定理 5.3.1 の条件 (2) により (m', u) も nice である． □

系 5.3.4　u_0 を法 1 の最良平方近似とすると，$(1, u_0, u_0^2 - D)$ は reduced triple である．

【証明】 仮定は $(1, u_0)$ が nice であることを言っている．$m = 1 < |m'| = |u_0^2 - D|$ だから，上の補題より，$(1, u_0, u_0^2 - D)$ は reduced triple である．　□

命題 5.3.5　m は整数で，$\sqrt{D} > |m| \neq 0$ だとする．このとき，次は同値である:

(1)　ある法 m の剰余類の中に，D の法 m の最良平方近似が 2 つ存在する．

(2)　ある正整数 v が存在し，$D = v^2 \pm |m|v + \frac{m^2}{2}$ と表せる．

(3)　法 m の最良平方近似 u に対し，$m' = \frac{u^2 - D}{m}$ とおいたとき，$m'^2 + \frac{m^2}{4} = D$ が成り立つ．

【証明】 (1) $\Longrightarrow$ (2)：2 つの最良平方近似は，$0 < v < \sqrt{D} < v' = v + |m|$ となる v, v' である．どちらも最良平方近似であるから，$D - v^2 = (v + |m|)^2 - D$ である．整理すると，$2D = 2v^2 + 2|m|v + |m|^2$ である．よって，$D = v^2 + |m|v + \frac{m^2}{2}$ と表せた．仮に大きい方を v と置いたとき，小さい方は $v - |m|$ となる．このときには，$D = v^2 - |m|v + \frac{m^2}{2}$ となる．

(2) $\Longrightarrow$ (1)：条件 (2) を符号が $+$ で満足する $v > 0$ が存在したとすると，上の変形の逆をたどって，$D - v^2 = (v + |m|)^2 - D$ となる．$v > 0$ であるから，どちらも正であって，$0 < v < \sqrt{D} < v + |m|$ となる．よって，$v, v + |m|$ はともに法 m の最良平方近似である．符号が $-$ で (2) を満足する $v > 0$ があったときには，$v, v - |m|$ が法 m の最良平方近似となる．

(1) $\Longrightarrow$ (3)：$v, v' = v + |m|$ がともに最良平方近似だとする．このとき $m' = \frac{v^2 - D}{m}$, $m'' = \frac{v'^2 - D}{m}$ とすると，$m'' = -m'$ である．また，

$$m' = \frac{v^2 - D}{m} = \frac{-|m|v - \frac{m^2}{2}}{m} = -\mathrm{sgn}(m)v - \frac{m}{2}$$

と与えられる．よって，

$$\begin{aligned} m''^2 + \frac{m^2}{4} &= m'^2 + \frac{m^2}{4} \\ &= v^2 + |m|v + \frac{m^2}{4} + \frac{m^2}{4} = v^2 + |m|v + \frac{m^2}{2} = D \end{aligned}$$

が成り立つ．

(3) $\Longrightarrow$ (2)：$D = \left(\frac{u^2 - D}{m}\right)^2 + \frac{m^2}{4}$ だとすると，

$$m^2 D = u^4 - 2u^2 D + D^2 + \frac{m^4}{4}, \quad \text{したがって,} \quad D^2 - (m^2 + 2u^2)D + u^4 + \frac{m^4}{4} = 0$$

となる．これを解くと，

$$\begin{aligned} D &= \frac{1}{2}\left((m^2 + 2u^2) \pm \sqrt{(m^2 + 2u^2)^2 - 4\left(u^4 + \frac{m^4}{4}\right)}\right) \\ &= \frac{1}{2}\left((m^2 + 2u^2) \pm \sqrt{4m^2u^2}\right) = \frac{m^2}{2} \pm |m|u + u^2 \end{aligned}$$

となる．　□

系 5.3.6　D の法 m の最良平方近似 u に対し，$\left(\frac{u^2-D}{m}\right)^2+\frac{m^2}{4}<D$ ならば u はただ一つの法 m の最良平方近似である．

【証明】 命題 5,3,1, 5.3.5 より明らか．　□

5.3.2　チャクラヴァーラアルゴリズム

前節の用語を用いると，M.1 に基づくチャクラヴァーラのアルゴリズムは次のようなものである：

C.1（簡単のため）自明な初期解 $(p_0,q_0;m_0)=(0,1;1)$ から出発する．また $u_0=0$ とおく．

C.2 $(p_n,q_n;m_n),u_n$ $(n\geq 0)$ が与えられたとき，u_{n+1} を D の法 m_n の最良平方近似で，

$$u_{n+1}\equiv -u_n \pmod{m_n}$$

を満たすものとする．

C.3 $(p_{n+1},q_{n+1};m_{n+1})$ は

$$p_{n+1}:=\frac{q_n+p_nu_{n+1}}{m_n},\quad q_{n+1}:=\frac{Dp_n+q_nu_{n+1}}{m_n},\quad m_{n+1}:=\frac{u_{n+1}^2-D}{m_n}$$

と定義される．

このとき，三つ組 $(m_0,u_1,m_1),(m_1,u_2,m_2),\ldots,(m_{n-1},u_n,m_n),\ldots$ は実質的には前節の対称行列 $S_1,S_2,\ldots,S_n,\ldots$ の系列であるが，対称行列としての性質は一切用いない．

例 5.3.7　アルゴリズムが一意的に定まらない，すなわち，C.2 で最良平方近似が 2 つ現れる例外ケースの振る舞いを例で調べておく．

$D=29$ とする．$u_0=0$, $m_0=1$ からスタートする．

- $(u_1,m_1)=(5,-4)$.
  $(\because)$ $u_2\equiv 0 \pmod 1$ で 29 の最良平方近似．$5^2=25<29<6^2=36$ だから，$u_1=5$. $m_1=(5^2-29)/1=-4$.
- $(u_2^+,m_2^+)=(7,-5)$, $(u_2^-,m_2^-)=(3,5)$.
  $(\because)$ $u_2^{\pm}\equiv -1 \pmod 4$ で 29 の最良平方近似．$3^2=9<29<7^2=49$ だから，$3,7$ はどちらも最良平方近似．そこで，$u_2^+=7$. $u_2^-=3$ とおく．このとき，$m_2^+=(7^2-29)/(-4)=-5$. $m_2^-=(3^2-29)/(-4)=5$.
- $(u_3^+,m_3^+)=(3,4)$, $(u_3^-,m_3^-)=(7,4)$.
  $(\because)$ $u_3^+\equiv -7\equiv 3 \pmod 5$ で 29 の最良平方近似．$3^2=9<29<8^2=64$ だから，$u_3^+=3$, $m_3^+=(3^2-29)/(-5)=4$. $u_3^-\equiv -3\equiv 2 \pmod 5$. $2^2=4<29<7^2=49$ だから，$u_3^-=7$. $m_3^-=(7^2-29)/5=4$.
- $(u_4^+,m_4^+)=(u_4^-,m_4^-)=(5,-1)$.
  $(\because)$ $u_4^+\equiv -3\equiv 1 \pmod 4$, $u_4^-\equiv -7\equiv 1 \pmod 4$, $5^2=25<29<10^2=100$ だから，$u_4^+=u_4^-=5$, $m_4^+=m_4^-=(5^2-29)/4=-1$.

よって,

m_0	u_1	m_1	u_2^+ u_2^-	m_2^+ m_2^-	u_3^+ u_3^-	m_3	u_4	m_4
1	5	-4	7 3	-5 5	3 7	4	5	-1

となった.

5.3.3 基本定理

チャクラヴァーラのアルゴリズムに出てくる (m_n, u_{n+1}) は，u_{n+1} の定義により，すべて定義 5.3.2 の意味での nice pair である．次が基本定理である．

定理 5.3.8 (m, u, m') が reduce triple だとする．すなわち,

(a) $|m| < \sqrt{D}$, $u^2 \equiv D \pmod{m}$, $mm' = u^2 - D$.

(b) u は D の法 m の最良平方近似,

(c) u は D の法 m' の最良平方近似,

とすると，このとき，u' を合同類 $-u + m'Z$ に属す D の法 m' の最良平方近似とし，$m'' = \frac{u'^2 - D}{m'}$ とすると，(m', u', m'') も reduced triple である．すなわち,

(a′) $|m'| < \sqrt{D}$, $u'^2 \equiv D \pmod{m'}$, $m'm'' = u'^2 - D$.

(b′) u' は D の法 m' の最良平方近似,

(c′) u' は D の法 m'' の最良平方近似,

【証明】 証明すべきことは，最後の条件 (c′) のみである．仮定 (b), (b′) と定理 5.3.1 (2) により,

$$m'^2 + \frac{m^2}{4} \le D, \quad m''^2 + \frac{m'^2}{4} \le D$$

である．$|m| \ge |m''|$ なら第 1 の不等式より，$|m''| \ge |m'|$ ならば第 2 の不等式より不等式 $m'^2 + \frac{m''^2}{4} \le D$ が得られるから，定理 5.3.1 (2) によって (c′) が成立つ．そこで，$|m| < |m''| < |m'|$ の場合を考える．

$$mm' = u^2 - D, \quad m'm'' = u'^2 - D, \quad \ell := \frac{u + u'}{m'}$$

とする．ℓ は仮定により整数である．このとき,

$$m'\ell(u' - u) = u'^2 - u^2 = m'(m'' - m)$$

であるから,

$$u' = \frac{1}{2}\left(m'\ell + \frac{m'' - m}{\ell}\right), \quad u = \frac{1}{2}\left(m'\ell - \frac{m'' - m}{\ell}\right)$$

となる.

$$\epsilon = \mathrm{sgn}(m), \quad \epsilon' = \mathrm{sgn}(m'), \quad \epsilon'' = \mathrm{sgn}(m'')$$

とおくと，$\ell m' = u + u' > 0$ だから，$\mathrm{sgn}(\ell) = \epsilon'$ である.

$|m''| > |m|$ により，u' は

$$u' = \frac{1}{2}\left(m'\ell + \frac{m''-m}{\ell}\right) = \frac{m'\ell}{2} + \frac{1}{2}\left(\frac{\epsilon''|m''| - \epsilon|m|}{\epsilon'|\ell|}\right)$$
$$\geq \frac{|m'||\ell|}{2} + \frac{1}{2}\left(\frac{\epsilon''|m''| - \epsilon'|m''|}{\epsilon'|\ell|}\right) = \frac{|m'||\ell|}{2} + \frac{|m''|}{2}\left(\frac{(\epsilon'\epsilon''-1)}{|\ell|}\right)$$

と評価される．一方，u は法 m の最小近似であるから，定理 5.3.1 (3) により，

$$u > |m'| + \epsilon\epsilon' \cdot \frac{|m|}{2}$$

である．よって，上で求めた u の表示式を合わせると，

$$\frac{1}{2}\left(|m'||\ell| - \frac{\epsilon'\epsilon''|m''| - \epsilon\epsilon'|m|}{|\ell|}\right) > |m'| + \epsilon\epsilon' \cdot \frac{|m|}{2}$$

となる．ここで，$|\ell| = 1$ だったとすると，

$$\frac{1}{2}\left(|m'| - (\epsilon'\epsilon''|m''| - \epsilon\epsilon'|m|\right) > |m'| + \epsilon\epsilon' \cdot \frac{|m|}{2},$$

したがって，

$$-\frac{\epsilon'\epsilon''|m''|}{2} > \frac{|m'|}{2}$$

となるが，これは $|m'| > |m''|$ に矛盾する．よって，$|\ell| \geq 2$ である．また，$\epsilon'\epsilon'' = +1$ のときには，$|\ell| = 2$ とすると，

$$-\frac{|m''| - \epsilon\epsilon'|m|}{4} > \frac{|m|}{2}, \quad \text{したがって,} \quad \frac{\epsilon\epsilon'|m|}{4} > \frac{|m|}{2} + \frac{|m''|}{4} > \frac{|m|}{2}$$

となるが，これも矛盾である．よって，$\epsilon'\epsilon'' = +1$ のときは，$|\ell| \geq 3$ である．さて，上の u' の評価式に戻ると，$|\ell| \geq 2$ であるから，

$$\epsilon'\epsilon'' = -1 \Longrightarrow u' \geq \frac{|m'||\ell|}{2} - \frac{|m''|}{|\ell|} \geq |m'| - \frac{|m''|}{2}$$
$$\epsilon'\epsilon'' = 1 \Longrightarrow u' \geq \frac{|m'||\ell|}{2} \geq \frac{3|m'|}{2} = |m'| + \frac{|m'|}{2} > |m'| + \frac{|m''|}{2}$$

となる（後者の場合は，$|\ell| \geq 3$ と $|m'| > |m''|$ の仮定を用いた）．すなわち，$u' \geq |m'| + \epsilon'\epsilon'' \cdot \frac{|m''|}{2}$ が得られた．定理 5.3.1 の条件 (3) により，これは u' が法 m'' の最良平方近似であることを示している． □

系 5.3.9 λ を D の（法 1 の）最良平方近似だとする．初期 triple $(m_0, u_1, m_1) = (\lambda, \lambda^2 - D)$ からチャクラヴァーラのアルゴリズムによって得られる triple (m_i, u_{i+1}, m_{i+1}) はすべて reduced triple である．特に，$|m_i| < \sqrt{D}$ $(i \geq 1)$ である．

【証明】 系 5.3.4 によって，初期 triple $(m_0, u_1, m_1) = (\lambda, \lambda^2 - D)$ は reduced である．したがって，定理 5.3.8 によって，以後得られるすべての triple (m_i, u_{i+1}, m_{i+1}) は reduced である．最後の主張は，定理の (a′) から従う． □

補題 5.3.10　初期 triple $(m_0, u_1, m_1) = (1, \lambda, \lambda^2 - D)$ からスタートするチャクラヴァーラのアルゴリズムによって，$(m_{i-1}, u_i, m_i) \rightarrowtail (m_i, u_{i+1}, m_{i+1})$ が得られたとき，チャクラヴァーラのアルゴリズムによって $(m_{i+1}, u_{i+1}, m_i) \rightarrowtail (m_i, u_i, m_{i-1})$ も得られる．

【証明】　定理 5.3.8 によって，u_i は法 m_i の最良平方近似であるから，$u_i + u_{i+1} \equiv 0 \pmod{m_i}$ であればよいが，これは仮定に含まれている．　□

補題 5.3.10 で示されたチャクラヴァーラのアルゴリムは反転することができるという事実に，reduced という条件の重要性が現れている．

5.3.4　例外ケースが現れる場合

いま，u_i, m_i が定まったとき，法 m_i の最良平方近似として $u_{i+1}^{\pm}$ の 2 つがとれたとする．このとき，$m_0, u_1, m_1, \ldots, m_{n-1}, u_n, m_n, \ldots$ と交互に並べた数列（以下，(m,u)**-系列**という）は

$$\ldots, u_i, m_i, \ \begin{matrix} u_{i+1}^{+} \\ u_{i+1}^{-} \end{matrix}, \ \begin{matrix} m_{i+1}^{+} \\ m_{i+1}^{-} \end{matrix}, \ \begin{matrix} u_{i+2}^{+} \\ u_{i+2}^{-} \end{matrix}, \ldots$$

の形になる．このとき，

$$u_{i+1}^{+} - u_{i+1}^{-} = |m_i|, \quad m_{i+1}^{\pm} = \pm m_{i+1}, \quad (u_{i+1}^{\pm})^2 - D = \pm m_i m_{i+1},$$
$$u_{i+1}^{\pm} + u_i \equiv 0 \pmod{m_i}$$

が成り立っている．よって，

$$(u_{i+1}^{+} - u_{i+1}^{-})(u_{i+1}^{+} + u_{i+1}^{-}) = (u_{i+1}^{+})^2 - (u_{i+1}^{-})^2 = 2m_i m_{i+1}$$

であるから，

$$u_{i+1}^{+} + u_{i+1}^{-} = 2\mathrm{sgn}(m_i) m_{i+1} \equiv 0 \pmod{m_{i+1}}$$

となる．$u_{i+2}^{\pm}$ は $u_{i+2}^{\pm} + u_{i+1}^{\pm} \equiv 0 \pmod{m_{i+1}}$ を満たす D の法 m_{i+1} の最小平方剰余であるが，上で示したことにより，$u_{i+2}^{\pm} \equiv u_{i+1}^{\mp} \pmod{m_{i+1}}$ であり，定理 2 により，$u_{i+i}^{\pm}$ は法 m_{i+1} の最小平方剰余であるから，$u_{i+2}^{\pm} = u_{i+1}^{\mp}$ である．また，

$$m_{i+2}^{\pm} = \frac{(u_{i+2}^{\pm})^2 - D}{m_{i+1}^{\pm}} = \frac{(u_{i+1}^{\mp})^2 - D}{\pm m_{i+1}} = -m_i$$

となる．したがって，(m,u)-系列は

$$\ldots, u_i, m_i, \ \begin{matrix} u_{i+1}^{+} \\ u_{i+1}^{-} \end{matrix}, \ \begin{matrix} m_{i+1} \\ -m_{i+1} \end{matrix}, \ \begin{matrix} u_{i+1}^{-} \\ u_{i+1}^{+} \end{matrix}, -m_i, \ldots$$

と延長される．このとき，次のステップ $(\pm m_{i+1}, u_{i+1}^{\mp}, -m_i) \rightarrowtail (-m_i, \nu, \mu)$ は，

$$\nu + u_{i+1}^{\mp} \equiv 0 \pmod{m_i}, \quad \nu = \text{法 } m_i \text{ の最良平方近似}, \quad \mu = \frac{\nu^2 - D}{-m_i}$$

で定まる．このとき，$\nu = u_i$ は第 1 の合同式を満たしており，第 2 の最良近似性は定理 2 から従い，$\mu = -m_{i-1}$ となる．よって，(m,u)-系列は，

$$\ldots, m_{i-1}, u_i, m_i, \begin{matrix} u_{i+1}^+ \\ u_{i+1}^- \end{matrix}, \begin{matrix} m_{i+1} \\ -m_{i+1} \end{matrix}, \begin{matrix} u_{i+1}^- \\ u_{i+1}^+ \end{matrix}, -m_i, u_i, -m_{i-1}, \ldots$$

となる．系 5.3.10 により，チャクラヴァーラのアルゴリズムは

$$(m_i, u_i, m_{i-1}) \rightarrowtail (m_{i-1}, u_{i-1}, m_{i-2}) \rightarrowtail \cdots \rightarrowtail (\lambda^2 - D, \lambda, 1)$$

となるが，

(♭) $$(m, u', m') \rightarrowtail (m', u'', m'') \Longrightarrow (-m, u', -m') \rightarrowtail (-m', u'', -m'')$$

であるから，上の (m,u)-系列は

$$1, u_1, m_1, u_2, \ldots, m_{i-1}, u_i, m_i, \begin{matrix} u_{i+1}^+ \\ u_{i+1}^- \end{matrix}, \begin{matrix} m_{i+1} \\ -m_{i+1} \end{matrix}, \begin{matrix} u_{i+1}^- \\ u_{i+1}^+ \end{matrix}, -m_i, u_i, -m_{i-1}, \ldots, u_2, -m_1, u_1, -1$$

となる．したがって，例外ケースが一度発生すると，そこからは，m_i の符号を反転させながら，(m,u)-系列を逆にたどり，$m = -1$ に到達する．これは，例 5.3.7 で見たパターンが一般的なものであることを示している．

補題 5.3.11　ある n に対し，$m_n = -1 = -m_0$ となると，以下，$u_{n+i} = u_i$, $m_{n+i} = -m_i$ $(\forall i \geq 1)$ となる．とくに，$m_{2n} = 1$ を得る．

【証明】 アルゴリズムが $(u_{n-1}, m_{n-1}) \rightarrowtail (u_n, m_n)$ で $m_n = -1$ を与えたとする．このとき，定理 2 により u_{n+1} は (法 1 の) 最良平方近似である．したがって，$u_{n+1} = u_1$ であるよって，$m_{n+1} = -u_1^2 - D = -m_1$ である．以下，(♭) により，主張が従う．　□

以上をまとめると，$m_i = \pm 1$ となる以前に例外ケースが発生すれば，ある n に対して $m_n = -1$ となり，付数の符号を反転させた形でもう一度同じ系列をたどって，$m_{2n} = 1$ が得られる．

5.3.5　例外ケースが現れない場合

初期 triple $(m_0, u_1, m_1) = (1, \lambda, \lambda^2 - D)$ からチャクラヴァーラのアルゴリズムをスタートして得られる (reduced) triples (m_{i-1}, u_i, m_i) には，例外ケースが現れないとする．このとき，定理 5.3.1, 5.3.8 により，$|m_i| < \sqrt{D}$ であり，$0 < u_i < \frac{3}{2}\sqrt{D}$ であるから，現れる triple は有限個しか存在せず，必ず，ある正整数 k, p に対して

$$(m_{i+p-1}, u_{i+p}, m_{i+p}) = (m_{i-1}, u_i, m_i) \quad (i \geq k)$$

となる．k, p をこの条件を満たす最小正整数と取っておく．ここで，$k > 1$ だとする．このとき，

$$(m_{k-2}, u_{k-1}, m_{k-1}) \rightarrowtail (m_{k-1}, u_k, m_k) \leftarrowtail (m_{k+p-1}, u_{k+p}, m_{k+p})$$

となっている．この対応は逆転させられるから，

$$(m_{k-1}, u_{k-1}, m_{k-2}) \leftarrowtail (m_k, u_k, m_{k-1}) \rightarrowtail (m_{k+p}, u_{k+p}, m_{k+p-1})$$

となり，逆方向には，例外ケースが現れ，§5.3.4 の結果により，$(m_{k-3}, u_{k-3}, m_{k-4})$ において，合流する．再度逆転させたもともとのチャクラヴァーラのプロセスを考えると，$(m_{k-4}, u_{k-3}, m_{k-3})$ において，例外ケースが現れることとなり，これは仮定に反する．よって，$k = 1$, すなわち，

$$(m_p, u_{1+p}, m_{1+p}) = (m_0, u_1, m_1), \quad m_p = 1$$

で周期 p で初期 triple に回帰している．

以上をまとめると，

定理 5.3.12 D が非平方数のとき，チャクラヴァーラのプロセスによって，必ず，$Dx^2 + 1 = y^2$ の正整数解が得られる．

5.3.6 回文性

先に，p. 9 で $D = 61$ に対して (m, u)-系列の回文性について注意した．この回文性が一般的現象であることを示そう．

λ を D の法 1 の最小平方剰余とする．そして，$m_0 = 1$, $u_1 = \lambda$, $m_1 = \lambda^2 - D$ からチャクラヴァーラのアルゴリズムを進行させる．定理 5.3.12 により，チャクラヴァーラのアルゴリズムによって，必ず，ある p に対して $m_p = 1$ となる．このとき，(m, u)-系列は

$$\begin{array}{cccccccc} m_0 & u_1 & m_1 & \cdots\cdots\cdots\cdots & m_{p-1} & u_p & m_p \\ 1 & \lambda & \lambda^2 - D & \cdots\cdots\cdots\cdots & ? & ? & 1 \end{array}$$

の形になっている. 系 5.3.9 により, (m_{p-1}, u_p, m_p) は reduced triple であるから, u_p は法 $m_p = 1$ での最小平方近似である, したがって, $u_p = \lambda = u_1$ ととれ, $m_{p-1} = (u_p^2 - D)/m_p = \lambda^2 - D = m_1$. したがって，補題 5.3.10 によって，$(m, u)$-系列の順序を逆転させたものもチャクラヴァーラのアルゴリズムで得られるものとなるが，初期値が同じになるので，系列に分岐が生ずることがない，すなわち，例外ケースが現れない場合には，(m, u)-系列は順序を逆転させたものと一致する．これが，回文性である．（実例は p. 8 の $D = 61$ の場合を見よ。）

例外ケースが現れる場合には，$m_n = 1$ に到達する複数の経路がとれるが，順序を逆転させたものは，そのどれかと一致する．例えば、p. 22 で見た $D = 29$ の場合には、(m, u)-系列は

$$1, 5, -4, \frac{7}{3}, \frac{-5}{5}, \frac{3}{7}, 4, 5, -1, 5, 4, \frac{7}{3}, \frac{5}{-5}, \frac{3}{7}, -4, 5, 1$$

である。

● 付録

A.1 アールヤバタのクッタカ（『アールヤパティーヤ』の第 2 章詩節 32，33）

§1 で引用した『アールヤバティーヤ』のクッタカについての詩節 32, 33 を再掲する．

32. 大きい余りを生ずる除数を，小さい余りを生ずる除数で割るがよい．(この第 1 の割り算の商はいつも捨てる．）余り（と除数) を相互に割り，(その割り算の余りが十分小さくなるまで割り算を続け商の蔓が偶数個になるようにしておく．最後の余りに）想定数をかけ，最初の余りの差に加えて (最後の除数で割ってきれいになるような想定数を見い出し，商の蔓の下に順に想定数と最後の商を置く．このようにして商の蔓を完成した後で）

33. 下（から二番目）の数を上の数にかけ，最下位の数を加える．(この操作を蔓の一番上まで続けて第二の蔓を作る．一番上に生じた数を）小さい余りを生ずる除数で割り，その余りに大きい余りを生ずる除数をかけ，大きい余りを加えると，二つの除数に対応するアグラになる．([矢野，1980, pp. 108–109])

[矢野，1980] では訳者矢野道雄氏によるかなり詳しい注が付されている．それを参考に，この 2 つの詩節が拡張ユークリッドアルゴリズムによって $ax + by = c$ の形の 1 次不定方程式を解くアルゴリズムを記述していることを説明しよう．

解くべき問題は

$$N = ax + R_1 = by + R_2$$

を満たす自然数 N（のうちで最小のもの）を求めることである．最後に出てくるアグラとは，N のことである．この形のクッタカを「アグラを伴うクッタカ」といい，p. 6 では $y = \frac{ax+b}{c}$ の整数解を求めようとしていたが，この形のクッタカを「アグラを伴わないクッタカ」という．結局のところ，アグラを伴うクッタカも $y = \frac{ax+(R_1-R_2)}{b}$ と考えるので，実質的な区別ではない．ここで $R_1 > R_2$ のとき，a を大きい余りを生ずる除数，b を小さい余りを生ずる除数という．a を b で割った余り r_1 で b を割り，その余り r_2 で r_1 を割る．以下同様に

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\vdots \\ r_{2k-1} &= q_{2k+1} r_{2k} + r_{2k+1} \end{aligned}$$

と互除法の計算を行う．詩節 32 は，この計算を記録する方法を示している．すなわち，

最初の商 q_1 をすて，残りの商を

$$\begin{matrix} q_2 \\ q_3 \\ \vdots \\ q_{2k+1} \end{matrix}$$

と偶数個の商を並べる．

これが, 詩節 32 の 3 行目に出てくる「商の蔓」である．「最後の余り」r_{2k+1} に「想定数」x_{2k} をかけ，「最初の余りの差」$c = R_1 - R_2$ を加え，「最後の除数」r_{2k} で割る．すなわち，$x_{2k+1} = \frac{r_{2k+1}x_{2k}+c}{r_{2k}}$ を考え，これが整数となるように（「きれいになるように」）想定数 x_{2k} をとる．そして，蔓に

$$\begin{matrix} q_2 \\ q_3 \\ \vdots \\ q_{2k+1} \\ x_{2k} \\ x_{2k+1} \end{matrix}$$

と付け加える．これが，完成された「商の蔓」である．以上が詩節 32 の内容である．「想定数」x_{2k} をとるというところは，互除法の過程で不定方程式の係数を十分小さくでき，解が目視で見てとれるようになったら，そこでやめてよいということを言っている．理論的には余りが 0 となるまで互除法を継続すべきであるが，答えが分かるならばそこまででよい，という計算重視の考え方に立っている．

ここで，互除法のステップに従って，解くべき不定方程式 $y = \frac{ax+c}{b}$ $(c = R_1 - R_2)$ を書き換えていくと，

$$\begin{aligned} y &= \frac{ax+c}{b} = q_1 x + x_1, \quad x_1 = \frac{r_1 x + c}{b}, \\ x &= \frac{bx_1 - c}{r_1} = q_2 x_1 + x_2, \quad x_2 = \frac{r_2 x_1 - c}{r_1}, \\ &\vdots \\ x_{n-1} &= \frac{r_{n-1}x_n + (-1)^n c}{r_n} = q_{n+1}x_n + x_{n+1}, \\ x_n &= \frac{r_n x_{n-1} + (-1)^{n-1} c}{r_{n-1}}, \\ &\vdots \end{aligned}$$

となる．ここで，$x = x_0$, $y = x_{-1}$, $b = r_0$, $a = r_{-1}$ と置けば，最後の一般式は，$n = 0, -1$ に対して，それぞれ第 2 式，第 1 式となり，成立している．

さて，ある n に対し，

(♭) $$x_n = \frac{r_n x_{n-1} + (-1)^{n-1} c}{r_{n-1}}$$

をみたす x_{n-1}, x_n が求められれば，漸化式

(♯) $$x_{n-2} = q_n x_{n-1} + x_n$$

を用いて遡ることにより，$x = x_0$, $y = x_{-1}$ を求め，したがって $N = ax + R_1$ も求めることができる．

以上の記号を用いると，詩節 32 の「商の蔓」の構成の細かな部分が理解できる．

- 想定数 x_n から遡って解 $x = x_0$ を求めるための漸化式 (♯) は商 $q_n, q_{n-1}, \ldots, q_2$ で定まるから，詩節 32 の「商の蔓」では,，「第 1 の割り算の商 (q_1) はいつも捨て」た上で，商 q_i $(i \geq 2)$ のみ記録すればよい．
- 「商の蔓が偶数個になるように」する（n が奇数になるようにする）のは，漸化式 (♭) における c の係数 $(-1)^{n-1}$ が 1 になるようにするためである．そうすれば,「最初の余りの差を加えて」と書けるのである．（もちろん，奇数の長さの蔓の場合には,「最初の余りの差を減ずる」とすればよいだけである．）

詩節 33 の第 2 の蔓の構成は第 1 の蔓を利用して漸化式を遡りながら解いていく過程を述べている．まず，第 1 文では，下図の x_{2k-1} を計算せよと言っている．

$$\begin{array}{cc} q_2 & \\ q_3 & \\ \vdots & \vdots \\ q_{2k+1} & x_{2k-1} = q_{2k+1}x_{2k} + x_{2k+1} \\ x_{2k} & x_{2k} \\ x_{2k+1} & x_{2k+1} \end{array}$$

以下，同様に，漸化式 (♯) を解き，遡って x_i を計算していくと，

$$\begin{array}{cc} q_2 & x_0 = x \\ q_3 & x_1 \\ \vdots & \vdots \\ q_{2k+1} & x_{2k-1} \\ x_{2k} & x_{2k} \\ x_{2k+1} & x_{2k+1} \end{array}$$

と「第 2 の蔓」が完成する．ここで得られた $x = x_0$ に対し，詩節 33 の後半では，b で割った余りに a をかけ，R_1 を加えると，N を得るとしている．b で割らずとも，$ax + R_1$ とすれば解が一つは得られるが，この解は想定数の取り方に依存しており一般には最小正整数解を与えることはない．N の最小正整数解を得るために x を b で割って，その余りに置き換えているのである．

例： $y = \frac{257x+3}{53}$ を考える．互除法の計算をすると，

$$
\begin{aligned}
& & a = r_{-1} = 257, \quad & b = r_0 = 53, \\
257 &= 4 \cdot 53 + 45, & q_1 = 4, \quad & r_1 = 45 \\
53 &= 1 \cdot 45 + 8, & q_2 = 1, \quad & r_2 = 8 \\
45 &= 5 \cdot 8 + 5, & q_3 = 5, \quad & r_3 = 5 \\
8 &= 1 \cdot 5 + 3, & q_4 = 1, \quad & r_4 = 3 \\
5 &= 1 \cdot 3 + 2, & q_5 = 1, \quad & r_5 = 2 \\
3 &= 1 \cdot 2 + 1, & q_6 = 1, \quad & r_6 = 1 \\
2 &= 2 \cdot 1 + 0, & q_7 = 2, \quad & r_7 = 0
\end{aligned}
$$

となる．このとき，$x_7 = \frac{r_7 x_6 + 3}{1} = 3$ で $x_6 = t$ は任意定数である．（この任意定数はいろいろにとれるので，適当に定めてそれを「想定数」と呼んだわけである．）第 1 の蔓は

$$
\begin{aligned}
q_2 &= 1 \\
q_3 &= 5 \\
q_4 &= 1 \\
q_5 &= 1 \\
q_6 &= 1 \\
q_7 &= 2 \\
x_6 &= t \\
x_7 &= 3
\end{aligned}
$$

となる．第 2 の蔓は第 1 の蔓から

$$
\begin{aligned}
q_2 &= 1 \\
q_3 &= 5 \\
q_4 &= 1 \\
q_5 &= 1 \\
q_6 &= 1 \\
q_7 &= 2 \\
x_6 &= t \\
x_7 &= 3
\end{aligned}
\quad \longmapsto \quad
\begin{aligned}
x_0 &= 1 \cdot (45t + 51) + (8t + 9) = 53t + 60 \\
x_1 &= 5 \cdot (8t + 9) + (5t + 6) = 45t + 51 \\
x_2 &= 1 \cdot (5t + 6) + (3t + 3) = 8t + 9 \\
x_3 &= 1 \cdot (3t + 3) + (2t + 3) = 5t + 6 \\
x_4 &= 1 \cdot (2t + 3) + t = 3t + 3 \\
x_5 &= 2t + 3 \\
x_6 &= t \\
x_7 &= 3
\end{aligned}
$$

と構成される．よって，$x = x_0 = 53t + 60 = 53(t + 1) + 7$, $y = \frac{257(53t+60)+3}{53} = 4 \cdot (53t + 60) + (45t + 51) = 257t + 291 = 257(t + 1) + 34$ という $y = \frac{257x+3}{53}$ の解が得られる．N を求めるには，$53(t + 1) + 7$ を 53 で割った余り 7 に対して $257 \cdot 7 + 3 = 1802$ として，$N = 1802$ となる．

ここでは，互除法のステップを最後の余りが 0 となるところまで進めたが，アールヤバタは解が分かるところまでで止めてよいとしていた．例えば，第 1 の蔓として $q_5 = 1$ を得たところで止めることにしよう．このとき，x_4, x_5 を $x_5 = \frac{r_5 x_4 + 3}{r_4} = \frac{2x_4+3}{3}$ を満たすように取ればよいから，

$x_4 = 0, x_5 = 1$ ととれる．このとき，第 1 の蔓は

$$\begin{aligned} q_2 &= 1 \\ q_3 &= 5 \\ q_4 &= 1 \\ q_5 &= 1 \\ x_4 &= 0 \\ x_5 &= 1 \end{aligned}$$

となる．よって，第 2 の蔓は，

$$\begin{array}{ll} q_2 = 1 & x_0 = 1 \cdot 6 + 1 = 7 \\ q_3 = 5 & x_1 = 5 \cdot 1 + 1 = 6 \\ q_4 = 1 & x_2 = 1 \cdot 1 + 0 = 1 \\ q_5 = 1 & x_3 = 1 \cdot 0 + 1 = 1 \\ x_4 = 0 & x_4 = 0 \\ x_5 = 1 & x_5 = 1 \end{array}$$

と構成される．よって，$x = x_0 = 7$ を 53 で割った余りは 7 自身であるから $257 \cdot 7 + 3 = 1802$ として，$N = 1802$ となる．もちろん，先の結果と同じ N が得られている．

A.2 インドにおける正方形の対角線の計算

紀元前 6 世紀のものと推測される『アーパスタンパ・シュルバスートラ』（井狩弥介訳）の「祭場（設営の）方法」の説明の I.6 に正方形の対角線の近似値の次の公式がみられる．

> 基準の長さを，その三分の一だけ増大すべし．さらに，それ [三分の一部分] を，みずからの三十四分の一を減じた，（後者の）四分の一だけ（増大すべし）．(この全長が，基準の長さに対してサヴィセーシャ [差を伴うもの]（と名付けられる）．([矢野，1980, p. 392])

これは，正方形の 1 辺を基準の長さ a としたときに，その対角線の長さ δ を

$$\delta = a + \frac{a}{3} + \left(\frac{a}{3} - \frac{a}{3} \cdot \frac{1}{34}\right) \cdot \frac{1}{4} = \left(1 + \frac{1}{3} + \frac{1}{3 \cdot 4} - \frac{1}{3 \cdot 4 \cdot 34}\right) a$$
$$1 + \frac{1}{3} + \frac{1}{3 \cdot 4} - \frac{1}{3 \cdot 4 \cdot 34} = \frac{577}{408} \fallingdotseq 1.414216$$

として与えるものと解釈されている．

この公式の起源としては，バビロニア起源説（ノイゲバウアー，[ヴェルデン，2006, pp.15–20]）があるが，シュルバスートラの数学の内部で導ける（導かれた）としてインドで独立に発見されたと見る見方も存在する（ティボー，林）([林，2020, p. 85])．

では，この導出を [林，2020, pp. 98–104] によって，眺めてみよう．いま，$2a^2 = b^2 - m$ を満たす正整数 a, b と整数 m が見出されたとする．このとき，

$$2 = \left(\frac{b}{a}\right)^2 - \frac{1}{a^2/m}$$

であるから，a が大きく，$|m|$ が小さければ．$\frac{b}{a}$ は $\sqrt{2}$ のよい近似を与えていると考えられる．例えば，$a=12, b=17, m=1$ が取れる．すなわち，$17/12 \doteqdot 1.416667$ が第 1 近似である．上の近似値は，いわば，第 2 近似にあたるものである．それを導くために，$m>0$ として，図 A.2.1 を考えよう．

図 A.2.1 において，BGID は一辺 b の正方形，EHIC は面積 m（一辺 $c=\sqrt{m}$）の正方形，ABCD は $\mathrm{AB}=b-c$, $\mathrm{BC}=b+c$ を 2 辺とする長方形，ONIJ は一辺 $d:=\sqrt{2}a$ の正方形とする．ここで，$\epsilon=\mathrm{BL}=\mathrm{OL}$ とおく．

さて，正方形 BGID から正方形 ONIJ をとりのぞいたグノーモーンを考えると，その面積は $c^2=m$ に等しい．そこで，グノーモーンの面積は，$2b\epsilon-\epsilon^2$ であるから，$2b\epsilon-\epsilon^2=m$, したがって，ϵ が十分小さければ，

$$\epsilon=\frac{m}{2b}+\frac{\epsilon^2}{2b}\doteqdot\frac{m}{2b}$$

という近似式が得られる．したがって，

$$d=b-\epsilon\doteqdot b-\frac{m}{2b}$$

が $d=\sqrt{2}a$ の近似式となる．よって，

$$\sqrt{2}\doteqdot\frac{b}{a}-\frac{m}{2ab}$$

が得られた．これを，上の例 $a=12, b=17, m=1, c=1$ に適用してみよう．このとき，

$$\sqrt{2}\doteqdot\frac{17}{12}-\frac{1}{3\cdot4\cdot34}=1+\frac{1}{3}+\frac{1}{3\cdot4}-\frac{1}{3\cdot4\cdot34}$$

となって，冒頭の近似式が得られるのである．

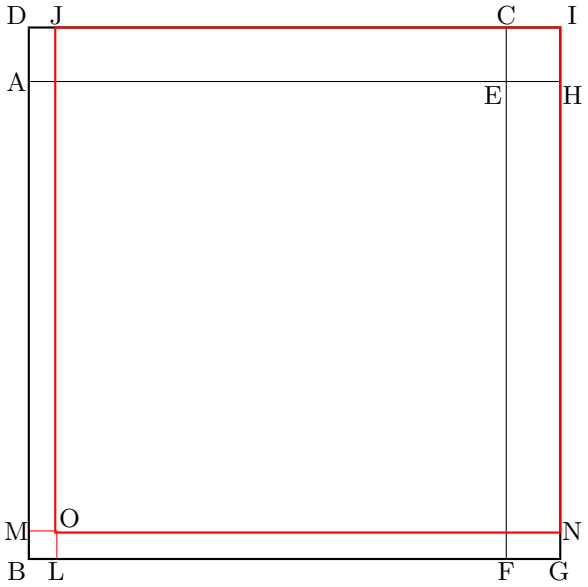

図 A.2.1

$$(\mathrm{BD}=\mathrm{BG}=b,\quad \mathrm{EH}=\mathrm{HI}=\mathrm{HD}=c,\quad \mathrm{JO}=\mathrm{JI}=d=\sqrt{2}a,\quad \mathrm{BL}=\mathrm{OL}=\epsilon)$$

ここで，$2a^2=b^2-m$ から得られた新しい近似値

$$\frac{b}{a}-\frac{m}{2ab}=\frac{2b^2-m}{2ab}=\frac{b^2+2a^2}{2ab}$$

の分母，分子は

$$(b^2+2a^2)^2-2(2ab)^2=(b^2-2a^2)^2=m^2$$

を満たす．実は，$(2ab, b^2+2a^2)$ は (a,b) の二元二次形式の合成（バーヴァナー）の意味での平方であるから，それも当然なのである．したがって，$17^2-2\cdot 12^2=1$ から出発して得られた $(577, 408)$ も $577^2-2\cdot 408^2=1$ を満たしている．

さて，$2x^2=y^2-m$ (m は絶対値の小さい整数）の整数解から得られる有理数 $\frac{y}{x}$ が $\sqrt{2}$ のよい近似値を与えることを動機として，この種の不定方程式に関心が寄せられたとするならば，逆によい近似値が得られたとき，その分母，分子が $2x^2=y^2-m$ の形の不定方程式を満足するかという問もあり得たであろう．上の計算は，そのような発想で近似値を分析することからバーヴァナーのもととなるアイディアが引き出された可能性を示唆しているのかもしれない．

参考文献

[Ayyangar, 1929–30] A. A. Krishnaswamy 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.* **18**, 225–248.

[Bauval, 2014] A. Bauval, An Elementaty Proof of the Halting Property for Chakravala Algorithm, arXive:1406.6809v1 [math.NT] 26 Jun 2014.

[Datta and Singh, 1935; 1938] B. Datta and A.N. Singh, *History of Hindu Mathematics Part I*, Motilal Banarasidass (1935); Part II, Motilal Banarasidass (1938). (reprinted by Asia Publishing House (1962), and Bharatiya Kala Prakashan (2004))

[Dickson, 1920] L. E. Dickson, *History of the Theory of Numbers, Part II, Diophnatine Analysis*, Carnegy Institute of Washington (reprinted by AMS Chelsea Publishing, 1992).

[Duttta, 2005] Amartya Kumar Duttta , Brahmagupta's Bhāvanā: Some Reflections, *Contributions to the History of Indian Mathematics*, Emch at al. (ed.), Hindustan Book Agency, 77–114.

[Duttta, 2010] Amartya Kumar Duttta , Kuṭṭaka, Bhāvanā and Cakravāla, *Studies in the History of Indian Mathematics*, C. S. Seshadri (ed.), Hindustan Book Agency, 145–199.

[Hankel, 1874] Hankel, Hermann, *Zur Geschichite der Mathematik in Alterthum und Mittelealter*, Leibzig: Teubner.

[Hurwitz, 1889] A. Hurwitz, Über eine besondere Art der Kettenbruch-Entwicklung reeller Grössen, *Acta Math.*, **12**, 367–405.

[Katz and Parshall, 2014] V. J. Katz and K. H. Parshall, *Taming the unknown*, Princeton University Press.（邦訳出版予定.）

[Matthews, Robertson, and White, 2010] K. Matthews, J. Robertson, and J. White, Midpoint Criteria for Solving Pell's Equation Using the Nearest Square Continued Fraction, *Mathematics of Comutation* **79**, 485–499.

[Minnigerode, 1887] B. Minnigerode, Über eine neue Methode, die Pellsche Gleichung aufzulösen, *Nachr. König. Gesellsch. Wiss. Göttingen Math.-Phys. Kl.* **23**, 619–652.

[Plofker, 2007] Kim Plofker, Mathematics in India, *The Mathematics of Egypt, Mesopotamia, China, India, and Islam — A Source Book* (V. J. Katz ed.), Princeton University Press, pp. 385–514.

[Plofker, 2009] Kim Plofker, *Mathematics in India*, Princeton University Press.

[Selenius, 1975] Selenius, Clas-Olof, Rationale of the Chakravāla process of Jayadeba and Bhāskara II, *Historia Mathematica* 2, 167–184.

[Shukla, 1954] K. S. Shukla, Ācārya Jayadeva, the mathematician, *Ganita*, Vol. 5, No. 1 (1954), 1 –-20. (reprinted as *Studies in Indian Mathematics and Astronomy* (A. Kolachana et al. (eds.)), Hindustan Book Agency and Springer Nature Singapore, 2019, 133–152.)

[ヴェイユ, 1987] アンドレ・ヴェイユ（足立恒雄・三宅克哉訳),『数論 – 歴史からのアプローチ』, 日本評論社.

[ヴェルデン, 2006] ファン・デル・ヴェルデン (加藤文元・鈴木亮太郎訳),『古代文明の数学』, 日本評論社.

[ガウス, 1995] カール・フリードリッヒ・ガウス（高瀬正仁訳),『ガウス整数論』, 朝倉書店.

[プロフカー, 2014] キム・プロフカー（廣瀬巧訳), サンスクリットの数学的韻文作品, E. Robson, J. Stedall 編『オックスフォード数学史』, 共立出版, pp. 467–482.

[伊東, 1987] 伊東俊太郎編,『中世の数学』(数学の歴史 – 現代数学はどのようにつくられたか– 第 II 巻), 共立出版.

[楠葉・林・矢野, 1997] 楠葉隆徳・林隆夫・矢野道雄訳,『インド数学研究 –数列・円周率・三角法–』, 恒星社厚生閣.

[林, 2016] 林隆夫訳,『インド代数学研究：「ビージャガニタ」+「ビージャパッラヴァ」全訳と注』, 恒星社厚生閣.

[林, 2019] 林隆夫訳,『インド算術研究：「ガニタティラカ」+ シンハティラカ注 全訳と注』, 恒星社厚生閣.

[林, 2020] 林隆夫,『インドの数学 - ゼロの発明』, ちくま学芸文庫.

[矢野, 1980] 矢野道雄編,『インド数学・天文学集』, 科学の名著 1, 朝日出版社.