平方根の連分数とペル方程式

Continued Fractions of Square Root
and
Pell's Equation

第 4 版

$$\sqrt{m} = [n, \overline{n_1, n_2, ..., n_r, 2n}]$$

$$\frac{p}{q} = [n, n_1, n_2, ..., n_r]$$

$$p^2 - mq^2 = \pm 1$$

有澤健治著

目次

はじめに

ここでは平方根の連分数展開に関する話題を扱う[1]。話は連分数の基礎から始まるが、入門的な解説書ではない。どちらかと言えば研究書である。原則として、全ての主張について証明が添えられている。また、分かりやすくするために、必ず例が示されている。

易しくシンプルな証明を心がけた。そのために、多くの定理について既存の証明が改善されている。行列の知識は非常に役に立つ。煩雑な計算が透明に理解されるのである。読者は、簡単な行列 (2 行 2 列行列) の知識を持っていることが想定されている。また初等的な合同式も説明に使用されている。

第 1 章と第 2 章は、連分数論の基礎知識に充てられている。内容的にはよく知られたものだと思えるが、ここで導入された関数などは、後の章の理解には不可欠だと思えるので、連分数論をよく知っている読者もざっと目を通すのが良いだろう。

次に、新しい内容が盛り込まれていると信じる章を簡単に紹介しておく。

- 第 2 章の連分数の循環に関する議論は、主張されている内容は、よく知られているものであるが、筆者の独自の視点から再証明を試みた。かなり分かり易すくなったと思うが、成功しているか否かの判断は読者に任せる。

[1]「連分数」なのか「連分数展開」なのか迷うところであるが、ここでは「展開」はあくまで動詞として使っている。従って「連分数展開」とは「連分数への展開」の意味である。高木も同じ立場を採っているように思える。英語では連分数は continued fractions である。Hardy-Wright は continued fractions を expansion と関係づけていない。英語の文献には “continued fractions expansion” の言い方は見かける

- 第 3 章の「二次無理数の連分数の周期」は、周期に関する最近の研究成果を紹介している。周期を、或る集合の位数と関係させて論じているのが新しい。また、この章の「平方根の連分数の周期構造」には、新しい内容が含まれている。
- 第 4 章の「平方根の連分数の逆問題」は、新しい問題提起とその解だと思うが、既に誰かがやっているかも知れない。
- 第 5 章の「Pell 方程式」は、Pell 方程式の解法を論じている。この章は以下の理由で、特に重要である。

連分数の歴史は非常に古く、新しい定理を見つけることは非常に難しい。新しいと思っても、よく調べると既存の定理の再発見であったと覚悟しなくてはならない。

第 5 章の定理 2 が、筆者が経験した、そうした再発見の例である。この定理は、平方根の連分数と Pell 方程式の解との美しい関係を述べている。両者に関係があることは古くから知られていたが、その関係を簡潔明瞭に言い表したのが定理 2 である。この定理はまだ殆ど知られていないはずである。と言うのは、平方根の連分数の周期を論じる中で Pell 方程式に触れている 2017 年の Saradha[19] の論文があるが、この定理には触れていない。ところが、この定理は 2014 年の Dummit[20] の論文に載っているのである。長くなるとの理由で、証明は添えられていない。この定理を紹介した 2016 年の Lahn-Spiegel[21] の論文が存在するが、単なる Dummit の紹介で、証明は添えられていない。従って、筆者のこの記事が、定理 2 の完全な証明を添えた、現状では唯一の著作と考えてよいであろう。

本書第 2 版では、第 5 章に拡張 Pell 方程式 $x^2 - my^2 = \pm 4$ の新しい解法を添えておいた。これは定理 2 の Pell 方程式 $x^2 - my^2 = \pm 1$ の解法のアイデアを拡張 Pell 方程式に適用したもので、まだ全く知られていないはずである。

本書第 3 版では、第 6 章に一般 Pell 方程式 $x^2 - my^2 = \pm d$ を追加した。最近のものと思われる Conrad の解法を紹介するとともに、この方法のアイデアを活かし、Conrad の欠点を含まない新しい解法を提示した。これも、まだ全く知られていないはずである。

この書を書くにあたって、筆者が主に参考にしたテキストは、Dirichlet-Dedekind の『整数論講義』、高木貞治の『初等整数論講義』、Hardy-Wright の “An Introduction to the Theory of Numbers” および Sierpinski の “Elementary Theory of Numbers” の 4 冊である。

Dirichlet-Dedekind と高木貞治の目標はイデアル論にあり、そのために連分数論と Pell 方程式の理解だけを目標にした場合には、些か荷が重いかも知れない。なお、高木貞治は Dirichlet-Dedekind の証明の冗長な部分に対して、多くの改良を行っている。また彼の著書に現れる道草の中には、数学に対する彼の考えが滲み出ていて、非常に面白い。

Hardy-Wright は、従来の整数論で行われている連分数の計算方法を大胆に見直し、改良している。彼のアプローチは整数論の分野で支持されているのであろう。連分数に関する現在の論文の多くは、彼のスタイルで書かれている。従って、ここでも Hardy-Wright 流を採用している。しかし、彼が Gauss の強力な計算ツール (本書で $H(...)$ と名付けられた関数) を捨てたのはやり過ぎだと思う。

Sierpinski は計算が大好きらしく、面白い知識を披露している。例えば、互除法における割り算の回数の上限は、分母を 10 進数で表した桁数に 5 を掛けて得られるとする Lamé による定理の紹介である。もちろん面白い定理ではあるが、この性質を 10 進数と関係づける定理の述べ方に眉をひそめる者もいるだろう [2]。

[2] 付録 A に、Fibonacci 数を使って上限が示されている

■ 本文の中では、次の記号を断りなく使う。

式	意味
$3 \cdot 5$	3×5
$a \mid b$	a は b を割り切る
$a \nmid b$	a は b を割り切らない
$\gcd(a, b, ...)$	$a, b, ...$ の最大公約数
$[x]$	Gauss の整数化記号 ($0 \leq x - [x] < 1$)
$\|M\|$	集合 M の位数 (要素の個数) (M は任意の集合とする)
N	自然数の集合
$N(\xi)$	代数的数 ξ のノルム (5.2 章参照)
Z	整数の集合
Q	有理数の集合

■ 3 つの連続するピリオド列 "..." あるいはドット列 "$\cdots$" は省略記号として使われている。省略の中身は文脈による。

■ 特に断らない限り、括弧は以下の規則で使用されている。

- 式の中の丸括弧は (そして丸括弧だけが) 計算の優先順位を表す
- $(a, b, c, ...)$ のような複数のデータを含む丸括弧は、順序が意味を持つデータの集まりとして
- { ... } のような波括弧 (curly bracket) は集合の意味で
- $[a, b, c, ...]$ のように、角括弧の中に複数のデータが含まれる場合には連分数として

■ 特に断らない限り、ギリシャ文字は無理数に、ローマ文字は整数に対して使われている。

最後に、計算機の発展との関係を述べたい。計算機によって膨大なデータが簡単に手に入るようになった。Pell 方程式においても、計算機が吐き出す結果を眺めると様々な法則性が見えてくる。昔の天才も気付かなかった法則性が見えるのである。証明の目標が立てやすくなり、新しい定理を効率よく発見可能になっている。この点で我々は幸せな時代に生きている。

整数論に興味があるならば、Python を習得するのが良いだろう。Python はシンプルにして強力な、可読性に富みプログラムしやすい言語である。Python は、まるで整数論のために設計された感がある。Python の設計者は整数論のニーズをよく知っていると思える。何と言っても、整数演算が優れている。任意桁数の整数演算を行うので、安心して大きな整数を計算できるである。

何度も読み直して校正は重ねたが、それでも至らない所もあるだろう。問題点や改善点、あるいは説明の足りない所などがあれば、筆者にメールを送って頂ければ幸いである。

2018 年 6 月 22 日　初版
2018 年 8 月 25 日　第 2 版
2018 年 9 月 28 日　第 3 版
2019 年 03 月 03 日　第 4 版

愛知大学名誉教授　有澤健治

arisawa@aichi-u.ac.jp
http://ar.nyx.link/cf/

R. 190303

Chapter 1

連分数の基礎

1.1 互除法

最大公約数の計算は互除法が効率の良いアルゴリズムとして有名である[1]。この方法によると、6201 と 11349 の最大公約数は以下の様に除算を繰り返して求まる。
(右側に計算プロセスを式で示す。掛け算の記号を '×' ではなく、'·' で示した)

11349 を 6201 で割った剰余を計算して 5148 を得る。	$11349 = 1 \cdot 6201 + 5148$
6201 を 5148 で割った剰余を計算して 1053 を得る。	$6201 = 1 \cdot 5148 + 1053$
5148 を 1053 で割った剰余を計算して 936 を得る。	$5148 = 4 \cdot 1053 + 936$
1053 を 936 で割った剰余を計算して 117 を得る。	$1053 = 1 \cdot 936 + 117$
936 を 117 で割った剰余を計算して 0 を得る。	$936 = 8 \cdot 117 + 0$

剰余が 0 になった所で計算を止め、117 を答 (最大公約数) とする。

この計算法の基本的なアイデアは、a を b で割った剰余を c とすると、a と b の約数は b と c の約数でもあることの発見に基づいている。つまり $a = a'd,\ b = b'd$ とすると $a = nb + c$ は $(a' - nb')d = c$ であるから c も d で割り切れる。従って d は b と c の共通の約数 (公約数) である。先の例で言えば、

[1] 計算の対象となっている数字が急速に小さくなって行くことは直感的に明らかであるが、効率の数学的な評価に関しては、付録 A を見よ

11349 と 6201 の公約数は 6201 と 5148 との公約数でもある。この操作を繰り返して、ついには 117 と 0 との自明な公約数 117 に辿り着くのである [2]。これが最大の公約数であることは明らかである。

互除法の計算を (連分数との関係で多少拡張して) 纏めると次のようになる:

$$\left.\begin{aligned} x_0 &= n_0 x_1 + x_2 \\ &\cdots \\ x_{l-1} &= n_{l-1} x_l + x_{l+1} \\ x_l &= n_l x_{l+1} + 0 \end{aligned}\right\} \tag{1.1}$$

ただし $x_1 \geq 1$ としている。x_0 は負でもよい。$x_2, x_3, ...$ は剰余であるから、$x_1 > x_2 > x_3 > \cdots > x_{l+1} > 0$ である。剰余が 0 になったら計算を止める。$x_{l+2} = 0$ と考えればよい。$n_1, ..., n_l \geq 1$ であるが、n_0 は負でもよい。$x_1, ..., x_l$ の中には 1 は現れない。x_{l+1} は 1 であってもよい。x_{l+1} が最大公約数である。先の例では $x_0 = 11349,\ x_1 = 6201,\ l = 4,\ x_5 = 117$ である。

さて、分数 11349/6201 を次のように連分数

$$\frac{11349}{6201} = 1 + \frac{5148}{6201} = 1 + \frac{1}{\frac{6201}{5148}} = 1 + \frac{1}{1 + \frac{1053}{5148}} = 1 + \frac{1}{1 + \frac{1}{4 + \frac{936}{1053}}} = \cdots$$

で表すこともできるが、この表現方法 (文字通りの連分数表示) は煩雑で、紙面を要し、計算が面倒で、見通しが悪い。従って、ここでは、このような連分数表示を採用しない。代わりに、Hardy-Wright に従って、簡単に $11349/6201 = [1, 1, 4, 1, 8]$ のように表記する。式 (1.1) との関係では $x_0/x_1 = [n_0, n_1, ..., n_l]$ である。そして、これを連分数と呼ぶこととする。角括弧の中の数字列 $n_0, n_1, ..., n_l$ は連分数の商と呼ばれる [3]。この表記法はシンプルであるが、詳細が省かれているので、使いこなすには多少の慣れと知識が必要である。

[2] 0 は 117 で割り切れる

[3] Hardy-Wright: “the partial quotients, or simply the quotients, of the continued fraction”

1.2 有理数の連分数展開

連分数を $[n_1, n_2, ..., n_l]$ 書くと、この計算プロセスは次の再帰式で纏めることができる。

式 (1.1) は分数形式で

$$\frac{x_k}{x_{k+1}} = n_k + \frac{x_{k+2}}{x_{k+1}} \quad (k = 1, 2, ..., l-1)$$
$$\frac{x_l}{x_{l+1}} = n_l$$

となる。

そして $x_k/x_{k+1} = [n_k, ..., n_l]$ である。従って

$$\begin{aligned} [n_k, ..., n_l] &= n_k + \frac{1}{[n_{k+1}, ..., n_l]} \qquad (k = 1, 2, ..., l-1) \\ [n_l] &= n_l \end{aligned} \tag{1.2}$$

である。

例 1. $[1, 1, 4, 1, 8]$ は次のように逆順に求まっていく。

$$[8] = 8, \quad [1, 8] = 1 + \frac{1}{8} = \frac{9}{8}, \quad [4, 1, 8] = 4 + \frac{8}{9} = \frac{44}{9},$$
$$[1, 4, 1, 8] = 1 + \frac{9}{44} = \frac{53}{44}, \quad [1, 1, 4, 1, 8] = 1 + \frac{44}{53} = \frac{97}{53}$$

連分数 $[1, 1, 4, 1, 8]$ は $11349/6201$ から生成されたにも関わらず、計算で得られたのは $97/53$ である。これは $11349/6201$ の既約分数であるる

ところで、ここでは、連分数の添字を 1 から始めている。0 から始めるか、1 から始めるかに関しては決まりは無い。問題に応じて、適切な方を採用すればよい。筆者は、連分数の最初の商の特殊性を強調したい場合には 0 から開始し、そうでない場合には 1 から開始している。

得られた結果を少し別な視点から見直してみよう。互除法の逆問題を考えてみる。すなわち、与えられた連分数の商 (ここでは $1, 1, 4, 1, 8$) を生成する 2 数を求める問題として考えてみる。

2 数、例えば 11349 と 6201 から最大公約数 117 を取り除いた数 97 と 53 からも、連分数の商 $1, 1, 4, 1, 8$ が生成される。これも $97/53$ の連分数と言い

$[1,1,4,1,8]$ で表す。$11349/6201 = 97/53$ であるから、混乱は発生しない。一般的に言えば、互いに素な自然数を p と q とすると、両者に共通の因子 d を掛けた pd と qd からも同じ連分数の商が生成される。従って逆問題は、与えられた連分数の商を生成する互いに素な 2 数を求めれば十分である。

97 と 53 について、このことを確認しよう。図 1.1 に連分数の商を生成する計算プロセスを簡潔に示す。x の欄が割り算の分子と分母の列であり、剰余から生成されていく。n の欄が連分数の商である。例えば 97/53 の商が、97 の右に書かれた 1 であり、その剰余が 53 の下に書かれた 44 である。以下同様である。剰余が 0 になって止める。0 の手前が 1 であることで、97 と 53 が互いに素であることが確認できる。

x	n
97	1
53	1
44	4
9	1
8	8
1	
0	

図 1.1: 互除法 97 と 53

x	n
x_1	1
x_2	1
x_3	4
x_4	1
x_5	8
1	
0	

図 1.2: 互除法の逆問題

図 1.2 に図 1.1 の逆問題を示す。$x_6 = 1$ にすることによって、互いに素な x_1 と x_2 が得られるはずである。x_1 から x_5 までが求める箇所である。逆問題では、$x_5, x_4, ..., x_1$ の順に計算していく。慣れれば図 1.2 から直接 $x_5, ..., x_1$ を計算できるが、そうでなければ、例 1 のように、連分数の計算ルール、式 (1.2) の $[n_k, ..., n_l] = n_k + 1/[n_{k+1}, ..., n_l]$ を使って、逆順に求めることもできる。しかし、以下では互除法の規則、式 (1.1) を使って、$x_5, x_4, ..., x_1$ を求めてみよう。

$x_6 = 1$ から $x_5 = n_5 = 8$ を得る。そして $x_4 = 1 \cdot 8 + 1 = 9$ を得る。同様に $x_3 = 4 \cdot 9 + 8 = 44,\ x_2 = 1 \cdot 44 + 9 = 53,\ x_1 = 1 \cdot 53 + 44 = 97$ と計算されて行く。

この計算例から分かるように x_k は $n_k, n_{k+1}, ..., n_l$ の関数である。そこで

$x_k = H(n_k, n_{k+1}, ..., n_l)$ と書くことにする[4]。すると関数 H は次のように再帰的に定義される。

$$H() = 1, \quad H(n_l) = n_l$$
$$H(n_k, ..., n_l) = n_k H(n_{k+1}, ..., n_l) + H(n_{k+2}, ..., n_l) \qquad (k = l-1, ..., 1) \tag{1.3}$$

例 2.

$$H(a) = a, \quad H(a,b) = ab + 1, \quad H(a,b,c) = abc + a + c,$$
$$H(a,b,c,d) = abcd + ab + cd + ad + 1$$

$x_1 = H(n_1, n_2, ..., n_l),\ x_2 = H(n_2, ..., n_l)$ であるから H と連分数とは次の関係がある:

$$[n_1, n_2, ..., n_l] = \frac{H(n_1, n_2, ..., n_l)}{H(n_2, ..., n_l)}$$

関数 H は次の性質を持つ。

$$H(n_1, n_2, ..., n_{l-1}, n_l) = H(n_l, n_{l-1}, ..., n_2, n_1) \tag{1.4}$$
$$H(n_1, n_2, ..., n_{l-1}, n_l) = n_l H(n_1, n_2, ..., n_{l-1}) + H(n_1, n_2, ..., n_{l-2}) \tag{1.5}$$

この証明は少し長くなるので、付録 C に示す。また同じ付録に次の重要な性質

$$\begin{vmatrix} H(n_1, ..., n_l) & H(n_1, ..., n_{l-1}) \\ H(n_2, ..., n_l) & H(n_2, ..., n_{l-1}) \end{vmatrix} = (-1)^l$$

が示されている。

$p_l, q_l, p_{l-1}, q_{l-1}$ を

$$\begin{pmatrix} p_l & p_{l-1} \\ q_l & q_{l-1} \end{pmatrix} = \begin{pmatrix} H(n_1, ..., n_l) & H(n_1, ..., n_{l-1}) \\ H(n_2, ..., n_l) & H(n_2, ..., n_{l-1}) \end{pmatrix}$$

で定義すると $p_l q_{l-1} - p_{l-1} q_l = (-1)^l$ で、$\gcd(p_l, q_l) = 1$ および $\gcd(p_{l-1}, q_{l-1}) =$

[4] この関数は Gauss によって導入された。彼は基本的な関数であると考えたのであろう。名前を与えずに、単に "$[n_k, n_{k+1}, ..., n_l]$" のように、角括弧を使って表した。Dirichlet-Dedekind や高木は Gauss の意味で角括弧を使っている。Hardy-Wright は、Gauss の角括弧は不要と考え、角括弧を連分数を表すのに使った。ここでも Hardy-Wright に従って、角括弧で連分数を表す。しかし、Gauss の角括弧を完全に捨て去るのは惜しい。そこで同じことを、関数 $H(n_k, n_{k+1}, ..., n_l)$ を定義して、Gauss の考えた計算規則を残すことにしたのである。

1 である。そして

$$p_l/q_l = [n_1, ..., n_l], \quad p_{l-1}/q_{l-1} = [n_1, ..., n_{l-1}]$$

となる。

これは $p_l, q_l, p_{l-1}, q_{l-1}$ が関数 H によって定義されている場合の関係式である。しかし $[n_1, ..., n_l]$ と $[n_1, ..., n_{l-1}]$ だけが求まっている場合にはどうか? 関心を分母が正の分数に限定すれば

$$p_l/q_l = [n_1, ..., n_l], \quad p_{l-1}/q_{l-1} = [n_1, ..., n_{l-1}]$$

となる既約分数 p_l/q_l と p_{l-1}/q_{l-1} が一意に定まる。そして、それらは H から求めたものと一致するはずである。

従って次の重要な定理を得た。

定理 1. p_l/q_l、p_{l-1}/q_{l-1} を

$$p_l/q_l = [n_1, n_2, ..., n_{l-1}, n_l],\ p_{l-1}/q_{l-1} = [n_1, n_2, ..., n_{l-1}]$$

となる (分母が正の) 既約分数とする。すると

$$p_l q_{l-1} - q_l p_{l-1} = (-1)^l$$

である。

注釈 1 分数の表現で、分母に負数を許すと、一意に分数を表現できない。このことは定理 1 では特に問題で、符号が定まらないのである。従って $[n_1, n_2, ..., n_l]$ を p/q と置く場合、「p/q は分母が正で既約」の断り書きが必要である。しかし、この断り書きは面倒である。原則として省きたい。我々が既約分数を使いたい実際上のニーズは、分数表現の一意性が欲しいからであり、その点で、「既約分数」と言えば、「分母が正」を暗黙に意味していた方が都合が良いのである。なお、高木も Hardy-Wright も注意深い言い回しで、ここで述べた符号問題を回避している。

例 3. $[1, 1, 4, 1, 8] = 1 + 1/[1, 4, 1, 8] = 97/53,\ [1, 1, 4, 1] = 11/6$ である。確かに $97 \cdot 6 - 53 \cdot 11 = -1$ が成立している。

この定理により、不定方程式 $px - qy = \pm 1$ の特殊解が得られる。例えば $97x - 53y = \pm 1$ の不定方程式の解の一つは $(x, y) = (6, 11)$ である。$p > q$ の

場合 p/q を連分数 $[n_1, n_2, ..., n_{l-1}, n_l]$ に展開し、$y/x = [n_1, n_2, ..., n_{l-1}]$ から解を得る。$p < q$ の場合には、(p, q) の役割を入れ替える。

$p > q > 0$ として、p/q の連分数を $[n_1, n_2, ..., n_l]$ としよう。また $p_k/q_k = [n_1, n_2, ..., n_k]$ とする。$p_l/q_l = p/q$ である。すると、$p_1/q_1, p_2/q_2, ..., p_l/q_l$ は、どのように p/q に近づいて行くのだろうか?

定理 1 より

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^k}{q_{k-1}q_k} \tag{1.6}$$

である。つまり、k が偶数なら $p_k/q_k - p_{k-1}/q_{k-1}$ は正、奇数なら負であり、振動する:

$$\frac{p_1}{q_1} \nearrow \frac{p_2}{q_2} \searrow \frac{p_3}{q_3} \nearrow \frac{p_4}{q_4} \searrow \cdots$$

そして振幅は急速に小さくなって行く。また

$$\begin{aligned}\frac{p_k}{q_k} &= \frac{H(n_1, n_2, ..., n_k)}{H(n_2, ..., n_k)} = \frac{n_k H(n_1, n_2, ..., n_{k-1}) + H(n_1, n_2, ..., n_{k-2})}{n_k H(n_2, ..., n_{k-1}) + H(n_2, ..., n_{k-2})} \\ &= \frac{n_k p_{k-1} + p_{k-2}}{n_k q_{k-1} + q_{k-2}}\end{aligned} \tag{1.7}$$

であり、$n_k > 0$ であるから、p_k/q_k は p_{k-1}/q_{k-1} と p_{k-2}/q_{k-2} の間にある。従って

$$\frac{p_1}{q_1} < \frac{p_3}{q_3} < \frac{p_5}{q_5} < \cdots, \qquad \frac{p_2}{q_2} > \frac{p_4}{q_4} > \frac{p_6}{q_6} > \cdots$$

となり、奇数の列と偶数の列は共に p/q に向かって、増加あるは減少して行く。

例 4. $p/q = [1, 1, 4, 1, 8]$ の場合には、

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}, \frac{p_4}{q_4}, \frac{p_5}{q_5} = \frac{1}{1}, \frac{2}{1}, \frac{9}{5}, \frac{11}{6}, \frac{97}{53}$$

であり、次のように振動する:

$$\frac{1}{1} \nearrow \frac{2}{1} \searrow \frac{9}{5} \nearrow \frac{11}{6} \searrow \frac{97}{53}$$

なお、式 (1.7) は、前方から連分数の値を計算するのに役に立つ。例で示そう。

$$[1] = \frac{1}{1}, \quad [1,1] = \frac{2}{1}, \quad [1,1,4] = \frac{1+2\cdot 4}{1+1\cdot 4} = \frac{9}{5}$$

$$[1,1,4,1] = \frac{2+9\cdot 1}{1+5\cdot 1} = \frac{11}{6}, \quad [1,1,4,1,8] = \frac{9+11\cdot 8}{5+6\cdot 8} = \frac{97}{53}$$

見て分かるように、なかなか効率良く求まるのである。

注意 1

$$[n_1, n_2, ..., n_l + \frac{1}{n_{l+1}}] = [n_1, n_2, ..., [n_l, n_{l+1}]] = [n_1, n_2, ..., n_l, n_{l+1}]$$

である [5]。特に $n_{l+1} = 1$ の場合には

$$[n_1, n_2, ..., n_l + 1] = [n_1, n_2, ..., n_l, 1]$$

である。このことは、連分数を整数だけで展開した場合、2 通りに表されることを意味している。例えば $[1,2,3] = [1,2,2,1]$ である。

1.3 無理数の連分数展開

有理数の連分数は有限の長さで終了するが、無理数の場合には無限に続く [6]。ω $(\omega > 1)$ を無理数とする。この連分数を $\omega = [n_1, n_2, n_3, ...]$ とする。n_k は (原理的には) 以下のように求まっていく。

$$(\omega_1 - n_1)\omega_2 = 1, \quad (\omega_2 - n_2)\omega_3 = 1, \quad (\omega_3 - n_3)\omega_4 = 1, \quad \cdots$$

ここに $\omega_1 = \omega$ とした。また n_k は

$$n_k \leq \omega_k < n_{k+1}$$

となる整数である。ω_{k-1} が無理数なら ω_k も無理数である。従って等号が成立することはない。また $0 < \omega_k - n_k < 1$ で、この下で $\omega_k > 1$ となる。故に $n_k \geq 1$ である。ω_k を使うと、

$$\omega = [n_1, n_2, n_3, ..., n_k, \omega_{k+1}]$$

[5] 付録 C に証明がある。

[6] 無理数の発見は古代ギリシャにさかのぼり、ピタゴラス学派によると言われている。ユークリッドの『原論 (第 10 巻)』では、互助法のアルゴリズムが停止するか否かによって、有理数と無理数を区別している。連分数は互除法に過ぎないので、連分数の有限/無限の問題は BC300 年頃には既に見つかっていたことになる。なお 10 巻はティアイテトスによると言われている。連分数は Lagrange によって開拓された (高木 p.169)

となる。$n_1, n_2, n_3, ..., n_k$ を部分商、ω_{k+1} を終項と言う[7]。

定理 2. ω $(\omega > 1)$ を無理数とする。この連分数を $[n_1, n_2, n_3, ...]$ とする。また $p_k/q_k = [n_1, n_2, n_3, ..., n_k]$ とする。すると

$$|\omega - \frac{p_k}{q_k}| < \frac{1}{q_k q_{k+1}}$$

であり、従って連分数は ω に収束する:

$$\lim_{k\to\infty} |\omega - \frac{p_k}{q_k}| = 0$$

証明:

$$\omega = [n_1, n_2, n_3, ..., n_k, \omega_{k+1}]$$

とすると

$$\omega = \frac{H(n_1, n_2, n_3, ..., n_k, \omega_{k+1})}{H(n_2, n_3, ..., n_k, \omega_{k+1})}$$

である。そこで (簡単のために)

$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} H(n_1, n_2, n_3, ..., n_k) & H(n_1, n_2, n_3, ..., n_{k-1}) \\ H(n_2, n_2, n_3, ..., n_k) & H(n_2, n_3, ..., n_{k-1}) \end{pmatrix}$$

と置くと

$$\omega = \frac{p_k \omega_{k+1} + p_{k-1}}{q_k \omega_{k+1} + q_{k-1}}$$

である。そして $\omega_{k+1} > 0$ 故、ω は p_k/q_k と p_{k-1}/q_{k-1} の間にある。従って、式 (1.6) より直ちに

$$|\omega - \frac{p_{k-1}}{q_{k-1}}| < \frac{1}{q_k q_{k-1}}$$

が得られる。ここで k を $k+1$ に置き換えると、定理の不等式が得られる。

q_k は (p_k も) k の増加関数である。従って $k \to \infty$ で $q_k q_{k+1} \to \infty$ であり、連分数の収束が証明される。 □

[7] 高木 p.131

Chapter 2

二次無理数の連分数展開

2.1 簡単な計算法

ここでは平方根に対する連分数の簡単な計算法について考察してみる。

実数 θ を与える。$\theta_0 = \theta$ とし、式

$$\theta_k = \frac{1}{\theta_{k-1} - n_{k-1}} \qquad (k = 1, 2, 3, ...) \tag{2.1}$$

に基づいて θ_k と n_k を再帰的に求める。ここに n_k は $n_k \leq \theta_k < n_k + 1$ なる整数とする。このような整数はガウスの整数化記号を使って $n_k = [\theta_k]$ と書かれることが多い。ここでもこの記法を使う。また停止条件は $\theta_k = 0$ とする。その結果得られる数列 $n_0, n_1, n_2, ...$ を θ の連分数と言う [1]。

しばしば θ を、その連分数で表記する必要に迫られる。その場合は様々な書き方があるが、ここでは Hardy-Wright に従い、角カッコで囲って、$\theta = [n_0, n_1, n_2, ...]$ のように書くことにする [2]。$n_1, n_2, ...$ は自然数である。すなわち $n_k > 0$ $(k > 0)$ である。n_0 は特殊で、整数ではあるが、$n_0 \leq 0$ を許す。ただし以下の点で Hardy-Wright の記法を変更する。

[1] 実数とその連分数との対応は、連分数の長さが有限であれば自明なのであるが、無限の場合には収束の問題など基本的な問題を解決する必要がある。前節 1 定理 2 で収束が証明されている。また高木 [2] にも解説がある

[2] この記号もガウスによるが、ガウスは別の意味で使っている。この他に多様な変種がある

- 繰り返しの範囲を上線で示す。つまり $[n_0, n_1, ..., n_k, \overline{n_{k+1}, n_{k+2}, ..., n_{k+r}}]$ のように書く [3]。
- Gauss の整数化記号と区別するために、長さが 1 の場合には $[x,]$ のように “,” を追加する [4]。

連分数については以下のことが知られている。

(a) θ が有理数なら連分数は有限の長さで停止する

(b) θ が無理数なら連分数は停止しない

(c) θ が 2 次無理数であれば連分数は循環する [5]

このうち、(a),(b) については前節でとりあげた。(c) については、以下に続く節で証明する。

詳細な証明は後回しにして、ここでは計算法の概要だけを説明する。式 (2.1) を

$$n_k = [\theta_k], \quad (\theta_k - n_k)\theta_{k+1} = 1 \qquad (k = 0, 1, 2, ...) \tag{2.2}$$

と書き換える。この式で θ_k を基に θ_{k+1} を順に決めて行く。すると θ_0 の正負に関わらず、式 (2.2) で得られる θ_k, n_k $(k \geq 1)$ について関係

$$\theta_k > 1, \quad n_k > 0, \quad 0 < \theta_k - n_k < 1,$$

が成立していることが容易に分かる。

証明: $k \geq 0$ について $0 < \theta_k - n_k < 1$ は $n_k = [\theta_k]$ とガウスの整数化記号の定義から得られる。その結果、式 (2.2) の $(\theta_k - n_k)\theta_{k+1} = 1$ より $\theta_{k+1} > 1$ が $k \geq 1$ に対して得られる。 □

2 次無理数を扱う場合には、式 (2.2) の方が計算はやり易い。理由は、2 次無理数の場合には θ_k が

$$\theta_k = \frac{\sqrt{m} + b_k}{a_k} \tag{2.3}$$

のように、2 つの自然数 a_k, b_k の組で表現でき、この表現形式を式 (2.2) に適用した

$$(\frac{\sqrt{m} + b_k}{a_k} - n_k)(\frac{\sqrt{m} + b_{k+1}}{a_{k+1}}) = 1 \tag{2.4}$$

[3] Hardy-Wright は繰り返しの範囲を 2 つの上点で表している

[4] しかし実際にはこの記法は使われないであろう

[5] Lagrange の定理と言う

との相性が良いことにある。すなわち $b_{k+1} = n_k a_k - b_k$ によって b_{k+1} を決める。その際には、$b_{k+1} < \sqrt{m}$ の条件の下で n_k をできだけ大きくとる。b_{k+1} が定まると、式 (2.4) は

$$\frac{m - b_{k+1}^2}{a_k a_{k+1}} = 1$$

となる。従って a_{k+1} は $a_{k+1} = (m - b_{k+1}^2)/a_k$ から決めればよい。その結果、どの $k\ (\geq 1)$ でも次の関係が成立することになる:

$$0 < b_k < \sqrt{m}, \quad \frac{\sqrt{m} + b_k}{a_k} > 1, \quad 0 < \frac{\sqrt{m} - b_k}{a_k} < 1, \quad a_k \mid (m - b_k^2) \quad (2.5)$$

実際に計算を行う場合には、最初に $0 < b < \sqrt{m}$ なる b と $m - b^2$ を計算しておくのが良い。

例を $\sqrt{7}$ にとると $b = 1, 2$ である。次のような表を作っておく。

$\sqrt{m} - b$	$m - b^2$
$\sqrt{7} - 1$	6
$\sqrt{7} - 2$	3

この下で式 (2.4) の $a_k, b_k, n_k\ (k = 1, 2, ...)$ を満たして行く:

$$(\frac{\sqrt{7}+0}{1} - 2)(\frac{\sqrt{7}+2}{3}) = 1$$
$$(\frac{\sqrt{7}+2}{3} - 1)(\frac{\sqrt{7}+1}{2}) = 1$$
$$(\frac{\sqrt{7}+1}{2} - 1)(\frac{\sqrt{7}+1}{3}) = 1$$
$$(\frac{\sqrt{7}+1}{3} - 1)(\frac{\sqrt{7}+2}{1}) = 1$$
$$(\frac{\sqrt{7}+2}{1} - 4)(\frac{\sqrt{7}+2}{3}) = 1$$

これから $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$ を得る。この計算例で分かるように、この書き方の利点は、紙面を節約できるばかりではなく、計算のプロセスを目の子で追っていけることにある。

計算機による計算では $n_k = [(\sqrt{m} + b_k)/a_k]$ を $n_k = [(n_0 + b_k)/a_k]$ で置き換えても構わない。

証明: なぜなら $n_k \leq (\sqrt{m}+b_k)/a_k < n_k+1$ であるから $n_k a_k \leq \sqrt{m}+b_k < (n_k+1)a_k$ となる。また $n_0 = [\sqrt{m}]$ より $n_0 \leq \sqrt{m} < n_0+1$ つまり $n_0+b_k \leq \sqrt{m}+b_k < n_0+b_k+1$ である。従って $n_k a_k < n_0+b_k+1$ つまり $n_k a_k \leq n_0+b_k$ と $n_0+b_k < (n_k+1)a_k$ を得る。故に $n_k \leq (n_0+b_k)/a_k < n_k+1$ すなわち $n_k = [(n_0+b_k)/a_k]$ となる。 □

故に、計算機を使う場合には、次のアルゴリズムで計算を進めれば良い。

$$n_0 = [\sqrt{m}], \quad a_0 = 1, \quad b_0 = 0 \tag{2.6}$$

$$b_k = n_{k-1}a_{k-1} - b_{k-1}, \quad a_k = \frac{m-b_k^2}{a_{k-1}}, \quad n_k = [\frac{n_0+b_k}{a_k}] \qquad (k = 1, 2, ...) \tag{2.7}$$

ここに述べた計算方法がうまく働くためには以下のことが証明されなくてはならない。

- $\sqrt{m} > b_k > 0$ $(k = 1, 2, ...)$ となること
- $a_{k-1} \mid (m - b_k^2)$ $(k = 2, 2, ...)$ となること
- 循環が発生し、そこで停止すること

これらの問題は、多少の一般化を含む形で、次節で扱われる。

連分数の計算は、結局、実数 ξ から $\xi - [\xi]$ を求めること、$\xi - [\xi]$ の逆数を求めることの繰り返しである。従って、以下ではこの二つの基本操作に対して次のように名前を与え、同時に操作の記号的な表現を示しておく。

定義: 最小化 (min): $b \in Z$ に対して最小化の操作を

$$(\frac{\sqrt{m}+b}{a}) \xrightarrow[n]{\min} (\frac{\sqrt{m}-b'}{a})$$

と書く。ここに

$$n = \left[\frac{\sqrt{m}+b}{a}\right], \quad b' = na - b$$

である。故に

$$0 < (\frac{\sqrt{m}-b'}{a}) < 1$$

である。

b は一般に正整数である。

定義: 逆数化 (inv): $b \in Z$ に対して逆数化の操作を

$$(\frac{\sqrt{m}-b}{a}) \xrightarrow{\text{inv}} (\frac{\sqrt{m}+b}{a'}) \tag{2.8}$$

と書く。ここに

$$aa' = m - b^2$$

である。逆数との積は 1 である。つまり

$$(\frac{\sqrt{m}-b}{a})(\frac{\sqrt{m}+b}{a'}) = 1$$

従って

$$0 < (\frac{\sqrt{m}-b}{a}) < 1 \qquad \Longrightarrow \qquad (\frac{\sqrt{m}+b}{a'}) > 1$$

である。

b は一般に正整数である。

例えば $m = 7$ であれば

$$\begin{aligned}
(\frac{\sqrt{7}+0}{1}) &\xrightarrow[2]{\min} (\frac{\sqrt{7}-2}{1}) \xrightarrow{\text{inv}} (\frac{\sqrt{7}+2}{3}) \\
(\frac{\sqrt{7}+2}{3}) &\xrightarrow[1]{\min} (\frac{\sqrt{7}-1}{3}) \xrightarrow{\text{inv}} (\frac{\sqrt{7}+1}{2}) \\
(\frac{\sqrt{7}+1}{2}) &\xrightarrow[1]{\min} (\frac{\sqrt{7}-1}{2}) \xrightarrow{\text{inv}} (\frac{\sqrt{7}+1}{3}) \\
(\frac{\sqrt{7}+1}{3}) &\xrightarrow[1]{\min} (\frac{\sqrt{7}-2}{3}) \xrightarrow{\text{inv}} (\frac{\sqrt{7}+2}{1}) \\
(\frac{\sqrt{7}+2}{1}) &\xrightarrow[4]{\min} (\frac{\sqrt{7}-2}{1}) \xrightarrow{\text{inv}} (\frac{\sqrt{7}+2}{3})
\end{aligned}$$

のように、最小化と逆数化を繰り返して、連分数が得られる。

2.2 幾つかの補題

定義: 集合 S: $S(m)$ は $\dfrac{\sqrt{m}+b}{a}$ $(b \in Z, a \in N)$ なる数の集合で、かつ $S(m)$ の元は次の条件が満たされているとする。

$$\sqrt{m} > |b| > 0 \quad \text{and} \quad a \mid (m - b^2)$$

m を与えた時、(b, a) の範囲は有限に収まるので、$S(m)$ は有限集合である。また $S(m)$ の元は全て正である。

以下では、誤解が発生しない限り、$S(m)$ を簡単に S と書く。必要とあれば $S(5)$ のように、簡略しない書き方をする。

定義: 集合 S^- と S^+:

- $S^- = \{\xi \in S; \xi < 1\}$
- $S^+ = \{\xi \in S; \xi > 1\}$

例 1. $m = 5$ の場合の S^- と S^+ の例を次に示す。

$$S^- \quad \frac{\sqrt{5}+1}{4} \quad \frac{\sqrt{5}-1}{2} \quad \frac{\sqrt{5}-1}{4} \quad \frac{\sqrt{5}-2}{1}$$

$$S^+ \quad \frac{\sqrt{5}-1}{1} \quad \frac{\sqrt{5}+1}{2} \quad \frac{\sqrt{5}+1}{1} \quad \frac{\sqrt{5}+2}{1}$$

上段に S^- の元、下段に S^+ の元を示してある。上段の元と下段の元を掛けると 1 になるように配置されている。

定義: 写像 f: 逆数化と最小化の合成操作を f とする。例えば

$$\frac{\sqrt{7}-1}{2} \xrightarrow{f} \frac{\sqrt{7}-2}{3}$$

である。f は S^- から S^- への写像である。この写像を k 繰り返す写像を f^k とする。写像の出発点を $\xi_0 = \sqrt{m} - [\sqrt{m}]$ とし f^k $(k = 0, 1, 2, ...)$ を計算すると、(S^- が有限集合なので) どこかで $f^k(\xi_0) = f^{k'}(\xi_0)$ となる k と k' が存在する。つまり $\sqrt{m}$ の連分数は循環する。

$\sqrt{m}$ の連分数の循環性の証明は、このように易しいのであるが、実はもっと強い主張「ξ_0 が循環する」が成立する。つまり $\xi_0 = f^l(\xi_0)$ となる l が存在する。これを純循環という[6]。以下に幾つかの補題を通じて、この事を証明する。

[6]高木 p.205

補題 1. 逆数化で $S^+ \Leftrightarrow S^-$、すなわち

- $\xi \in S^- \quad \Rightarrow \quad \xi^{-1} \in S^+$
- $\xi \in S^+ \quad \Rightarrow \quad \xi^{-1} \in S^-$

証明: $\xi \in S^-$ であれば $\xi = (\sqrt{m} - b)/a$ で

$$(\frac{\sqrt{m} - b}{a})(\frac{\sqrt{m} + b}{a'}) = 1$$

である。ここに $aa' = m - b^2$ である。集合 S^- の条件より、このような a' は存在する。従って $\xi^{-1} \in S^+$ である。後半も同様に証明される。 □

注意: この補題の証明では $b > 0$ なることは要求されていない。例えば

$$\frac{\sqrt{5}+1}{4} < 1, \quad \frac{\sqrt{5}-1}{1} > 1, \quad (\frac{\sqrt{5}+1}{4})(\frac{\sqrt{5}-1}{1}) = 1$$

である。

補題 2. $\xi \in S^+$, $\xi' = \xi - [\xi]$ とすると $\xi' \in S^-$ である。詳しくは $\xi = (\sqrt{m} + b)/a$, $\xi' = (\sqrt{m} - b')/a$ とすると、$0 < \xi' < 1$ の他に、次が成り立つ。

(a) $0 < b' < \sqrt{m}$

(b) $a \mid (m - b'^2)$

(c) $(\sqrt{m} + b')/a > 1$

証明: $n = [\xi]$ と置く。$\xi > 1$ より $n \geq 1$ であり、$b' = na - b$ である。

まず (b) を証明する。

$$m - b'^2 = m - (na - b)^2 = m - b^2 - na(na - 2b)$$

であるから $a \mid (m - b^2)$ ならば $a \mid (m - b'^2)$ である。そして S^+ の条件から $a \mid (m - b^2)$ が成立している。

次に (c) を証明する。

$$\sqrt{m} + b' - a = \sqrt{m} + na - b - a = \sqrt{m} - b + (n-1)a > 0$$

ここで、最後の不等関係は $n \geq 1$ と S^+ の条件 $\sqrt{m} > |b| > b$ から得る。

最後に (a) を証明する。$0 < \xi' < 1$ と (c) より

$$0 < \frac{\sqrt{m} - b'}{a} < 1 < \frac{\sqrt{m} + b'}{a}$$

である。これから $\sqrt{m} > b' > 0$ が得られる。 □

注意: $\xi' = (\sqrt{5}+1)/4$ は $\xi' < 1$ であり、従って $\xi' \in S^-$ であるが、$\xi' = \xi - [\xi]$ となる ξ が S^+ の中に存在しない。同様なことは $\xi' = (\sqrt{5}-1)/4$ についても言える。他方 $(\sqrt{5}+2)/1$, $(\sqrt{5}+1)/1$, $(\sqrt{5}-1)/1$ はどれも S^+ の元であり、共に $(\sqrt{5}-2)/1$ に最小化される。

補題 3. 数 $(\sqrt{m}-b)/a \in S^-$ において、$(\sqrt{m}+b)/a > 1$ であれば、

$$\frac{\sqrt{m}+b'}{a} = \frac{\sqrt{m}-b}{a} + n \quad \text{and} \quad \frac{\sqrt{m}+b'}{a} > 1 \quad \text{and} \quad \sqrt{m} > b' \tag{2.9}$$

となる最大の自然数 n が存在する。さらに、このときの b' について、次が成り立つ。

(a) $b' > 0$

(b) $(\sqrt{m}-b')/a < 1$

証明: 最初に、最大の自然数 n の存在を示す。n には上限があるので自然数の存在を示せばよい。$n = 1$ が条件を満たすことを確認する。$0 < (\sqrt{m}-b)/a$ 故

$$1 < \frac{\sqrt{m}-b}{a} + 1 = \frac{\sqrt{m}+(a-b)}{a} = \frac{\sqrt{m}+b'}{a}$$

ここに $b' = a-b$ である。他方 $(\sqrt{m}+b)/a > 1$ であるから、$\sqrt{m} > a-b = b'$ が成立する。

従って $\sqrt{m} > b' = na-b$ を満たす最大の b' が存在し、$\sqrt{m} < b'+a$ である。これから、まず (b) が示される。最後に (a) は、(2.9) と (b) の組 $(\sqrt{m}-b')/a < 1 < (\sqrt{m}+b')/a$ から示される。 □

注意: 「最大」の条件を外すと、式 (2.9) の n は 1 つとは限らない。例えば $(m,b,a) = (12,3,1)$ の組では $n = 4,5,6$ が条件 (2.9) を満たす。

定義: 最大の数: 数 $(\sqrt{m}+b)/a \in S$ が $b+a > \sqrt{m}$ を満たす時「$(\sqrt{m}+b)/a$ は最大の数」と言うことにする。

注釈 1 「最大の数」とは、

$$(\sqrt{m}+b)/a \in S \quad \text{and} \quad (\sqrt{m}+b)/a+1 \notin S$$

となる数でもある。

注釈 2 $b+a>\sqrt{m}$ の関係は $(\sqrt{m}-b)/a<1$ と同じである。

補題 4. 数 $(\sqrt{m}-b)/a\in S^-$ の逆数を $(\sqrt{m}+b)/a'$ とする。もしも $(\sqrt{m}+b)/a>1$ ならば $(\sqrt{m}+b)/a'$ は最大の数である。*(*従って $(\sqrt{m}-b)/a'<1$ が成り立つ*)*

証明: まず $(\sqrt{m}-b)/a<1<(\sqrt{m}+b)/a$ より $b>0$ であり、$0<(\sqrt{m}-b)/a$ より $\sqrt{m}>b$ であることに留意しておく。

$$1=(\frac{\sqrt{m}-b}{a})(\frac{\sqrt{m}+b}{a'})=(\frac{\sqrt{m}+b}{a})(\frac{\sqrt{m}-b}{a'})$$

従って

$$1<\frac{\sqrt{m}+b}{a}\quad\Rightarrow\quad 0<\frac{\sqrt{m}-b}{a'}<1\quad\Rightarrow\quad \sqrt{m}<b+a'$$

□

定義: 演算 ξ^*: $\xi=(\sqrt{m}+b)/a\in S$ に対して $\xi^*=(\sqrt{m}-b)/a$ とする。b は負でもよい。

定義: 集合 T^- と T^+:

$$T^-=\{\xi\in S^-;\xi^*>1\}$$
$$T^+=\{\xi\in S^+;\xi^*<1\}$$

注釈 3 T^- の元は S^+ の元を最小化しても得られる (補題 2)。T^+ の元は S^- の元を最大化しても得られる (補題 3)。

注釈 4 集合 T^- と T^+ は、連分数の循環において本質的な役割を演じるのであるが、$\xi\in T^-$ のための条件としては、$\xi=(\sqrt{m}-b)/a$ としたときに $b>0$ だけでは不足である。$(\sqrt{5}-1)/4\notin T^-$ の例がある。

補題 5. $(\sqrt{m}-b)/a\in T^-$ あるいは $(\sqrt{m}+b)/a\in T^+$ とすると、どちらも

- $0<b<\sqrt{m}$
- $a\mid(m-b^2)$
- $0<(\sqrt{m}-b)/a<1,\quad(\sqrt{m}+b)/a>1$

となる。

証明: これらは補題 2 と補題 3、および T^-、T^+ の定義から明らか。 □

補題 6. 以下の写像はどれも全単射である。

(a) $T^- \overset{\text{inv}}{\longleftrightarrow} T^+$

(b) $T^+ \overset{\text{min}}{\longrightarrow} T^-$

証明: (a) の $T^- \overset{\text{inv}}{\longrightarrow} T^+$ の証明は次のようにすればよい。$aa' = m - b^2$ であれば

$$(\frac{\sqrt{m}-b}{a})(\frac{\sqrt{m}+b}{a'}) = (\frac{\sqrt{m}-b}{a'})(\frac{\sqrt{m}+b}{a}) = 1$$

が成り立つ。T^- の定義により $(\sqrt{m}-b)/a \in T^-$ なら

$$(\sqrt{m}-b)/a < 1, \quad (\sqrt{m}+b)/a > 1$$

である。従って

$$(\sqrt{m}+b)/a' > 1, \quad (\sqrt{m}-b)/a' < 1$$

つまり $(\sqrt{m}+b)/a' \in T^+$ である。$T^+ \overset{\text{inv}}{\longrightarrow} T^-$ も同様に証明される。従って全単射でもある。

(b) は補題 2 と補題 3 から明らか □

補題 7.

$$\xi \in T^- \quad \Longrightarrow \quad f(\xi) \in T^-$$

すなわち f は T^- から T^- への全単射である。

証明: 写像 $f(\xi)$ は、ξ の逆数を求めて、その結果を最小化して得られる。従って補題 6 によって f は T^- から T^- への全単射である。 □

定理 1. $\xi \in T^-$ とすると $\xi = f^l(\xi)$ となる自然数 $l \geq 1$ が存在する。

証明: f が T^- から T^- への写像であることと、T^- は有限集合であることから $f^k(\xi) = f^{k'}(\xi)$ $(k < k')$ となる自然数 k と k' が存在する。また補題 7 によって f は全単射であるから $f^k(\xi) = f^{k'}(\xi)$ ならば $f^{k-1}(\xi) = f^{k'-1}(\xi)$ が成

立し、結局 $\xi = f^0(\xi) = f^{k-k}(\xi) = f^{k'-k}(\xi)$ である。従って $l = k' - k$ と置けばよい。 □

$\xi \in T^-$ としよう。すると定理 1 より $\xi = f^l(\xi)$ となる自然数が l が存在する。f は逆数化、最小化の合成写像である。ξ の連分数なので、$\theta_0 = \xi$ と置く。連分数の計算手順は

$$n_k = [\theta_k], \quad \xi_k = \theta_k - n_k, \quad \theta_{k+1} = 1/\xi_k \qquad (k = 0, 1, 2, ...)$$

である。$0 < \xi < 1$ なので、$n_0 = [\theta_0] = [\xi] = 0$ である。従って $\xi_0 = \theta_0$ である。この後 $\theta_1 = 1/\xi_0$ と続く。そして、$\theta_l = 1/\xi_{l-1}$, $\theta_{l+1} = 1/\xi_l$ であるが、$\xi_l = \xi_0$ 故 $\theta_{l+1} = \theta_1$ である。従って $n_{l+1} = n_l$ となり、$\xi = [0, \overline{n_1, n_2, ..., n_l}]$ となる。

$\theta_0 = \sqrt{m}$ の場合、$n_0 = [\sqrt{m}]$, $\xi = \theta - n_0$ とすると $\xi \in T^-$ である。従って $\sqrt{m} = [n_0, \overline{n_1, n_2, ..., n_l}]$ となる。$\sqrt{m}$ の連分数は、後に詳細に分析する。

2.3 遷移図

この節では b を正または負の整数、a を自然数とする。$\sqrt{m}$ の連分数の計算プロセスの中では $(\sqrt{m}+b)/a$ の形の数が発生する。そこで $(\sqrt{m}+b)/a$ を (b,a) で表し、計算プロセスの中で (b,a) がどのように遷移するかを見てみよう。幾つかの例を図 2.1 から図 2.4 に示す。横軸が b で、縦軸が a である。図では T^- と T^+ の元が、①や2のように、数字を丸や四角の図形で囲って示されている。

操作 f は、逆数化と、最小化の合成である。逆数化では (b,a) $(b<0)$ から $(-b,(m-b^2)/a)$ を求める。最小化では (b,a) $(b>0)$ から $(-b',a)$ を求めるが、b' は条件 $0<b'=na-b<\sqrt{m}$ を満たす最大の数である。図との関係では、写像 f を逆数化と最小化に分解したほうが分かりやすい。T^- の元に作用した場合には逆数化、T^+ の元に作用した場合には最小化を表す写像を g とする。すると $T=T^-\cup T^+$ の元は g によって T のどれかに移る。$\xi\in T$ に g の作用を繰り返すと、やがては ξ に戻る。g による推移関係によって T の元は類を作る。図では同じ類に属する T の元を同じ図形で囲っている。数字は g によって推移する順序を表している。例えば①に g を作用させると②に移る。

図を例に具体的に説明しよう。図 2.1 (m=5) は T の中に 2 つの独立した循環を含む:

$$(\frac{\sqrt{5}-2}{1})\xrightarrow{\text{inv}}(\frac{\sqrt{5}+2}{1})\xrightarrow[4]{\min}(\frac{\sqrt{5}-2}{1})$$
$$(\frac{\sqrt{5}-1}{2})\xrightarrow{\text{inv}}(\frac{\sqrt{5}+1}{2})\xrightarrow[1]{\min}(\frac{\sqrt{5}-1}{2})$$

他方、図 2.2 (m=6) は 1 つの循環で T の全てを巡回する:

$$(\frac{\sqrt{6}-2}{1})\xrightarrow{\text{inv}}(\frac{\sqrt{6}+2}{2})\xrightarrow[2]{\min}(\frac{\sqrt{6}-2}{2})\xrightarrow{\text{inv}}(\frac{\sqrt{6}+2}{1})\xrightarrow[4]{\min}(\frac{\sqrt{6}-2}{1})$$

集合 S の元が全て遷移図に現れるわけではない。例えば $(\sqrt{7}-1)/6$ は最小数ではあるが、$(\sqrt{7}+1)/6<1$ なので、図 2.3 に現れていない。図 2.4 における $(\sqrt{8}-1)/7$ も同様である。

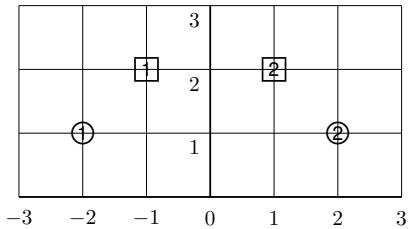


図 2.1: 遷移図: $m = 5$

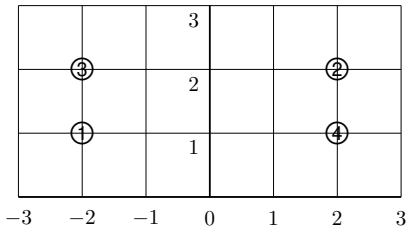


図 2.2: 遷移図: $m = 6$

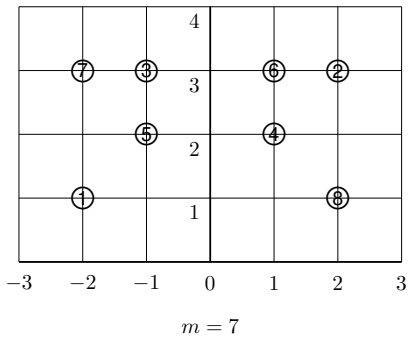


図 2.3: 遷移図: $m = 7$

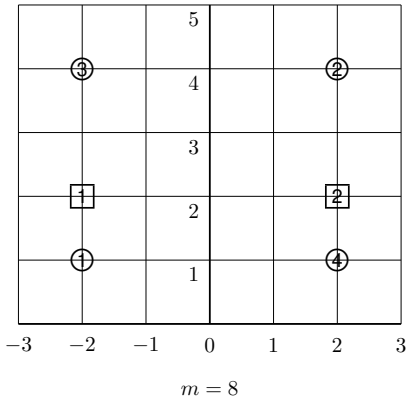


図 2.4: 遷移図: $m = 8$

2.4 幾つかの例

話を抽象化しないために、最初に幾つかの例を挙げる。例を計算しているうちに、コツが掴め、問題意識が湧くであろう。

例 1. $\dfrac{\sqrt{5}+1}{3}$

$(\sqrt{5}+1)/3 > 1,\ 5-1^2 > 0$ ではあるが $3 \mid (5-1^2)$ ではない。そこで

$$(\frac{\sqrt{5}+1}{3}) = (\frac{3(\sqrt{5}+1)}{9}) = (\frac{\sqrt{45}+3)}{9})$$

と変形する。すると $9 \mid (45-3^2)$ なので $(\sqrt{45}+3)/9 \in T^+(45)$ となる。従って循環は示されたが、実際に様子を確認してみる。

$$(\frac{\sqrt{45}+3)}{9}) \xrightarrow[1]{\min} (\frac{\sqrt{45}-6)}{9}) \xrightarrow{\text{inv}} (\frac{\sqrt{45}+6}{1}) \xrightarrow[12]{\min} (\frac{\sqrt{45}-6}{1}) \xrightarrow{\text{inv}} (\frac{\sqrt{45}+6}{9})$$
$$\xrightarrow[1]{\min} (\frac{\sqrt{45}-3}{9}) \xrightarrow{\text{inv}} (\frac{\sqrt{45}+3}{4}) \xrightarrow[2]{\min} (\frac{\sqrt{45}-5}{4}) \xrightarrow{\text{inv}} (\frac{\sqrt{45}+5}{5}) \xrightarrow[2]{\min} (\frac{\sqrt{45}-5}{5})$$
$$\xrightarrow{\text{inv}} (\frac{\sqrt{45}+5}{4}) \xrightarrow[2]{\min} (\frac{\sqrt{45}-3}{4}) \xrightarrow{\text{inv}} (\frac{\sqrt{45}+3}{9})$$

例 2. $\dfrac{\sqrt{2}+6}{4}$

$$(\frac{\sqrt{2}+6}{4}) \xrightarrow[1]{\min} (\frac{\sqrt{2}+2}{4}) = (\frac{2(\sqrt{2}+2)}{8}) = (\frac{\sqrt{8}+4}{8}) \xrightarrow{\text{inv}} (\frac{4-\sqrt{8}}{1})$$
$$\xrightarrow[1]{\min} (\frac{3-\sqrt{8}}{1}) \xrightarrow{\text{inv}} (\frac{3+\sqrt{8}}{1}) \xrightarrow[5]{\min} (\frac{\sqrt{8}-2}{1}) \in T^-(8)$$

例 3. $\dfrac{\sqrt{2}+7}{5}$

$$(\frac{\sqrt{2}+7}{5}) \xrightarrow[1]{\min} (\frac{\sqrt{2}+2}{5}) = (\frac{5(\sqrt{2}+2)}{25}) = (\frac{\sqrt{50}+10}{25}) \xrightarrow{\text{inv}} (\frac{10-\sqrt{50}}{2})$$
$$\xrightarrow[1]{\min} (\frac{8-\sqrt{50}}{2}) \xrightarrow{\text{inv}} (\frac{8+\sqrt{50}}{7}) \xrightarrow[2]{\min} (\frac{\sqrt{50}-6}{7}) \in T^-(50)$$

例 4. $\dfrac{\sqrt{3}+9}{6}$

$$(\frac{\sqrt{3}+9}{6}) \xrightarrow[1]{\min} (\frac{\sqrt{3}+3}{6}) \xrightarrow{\text{inv}} (\frac{3-\sqrt{3}}{1}) \xrightarrow[1]{\min} (\frac{2-\sqrt{3}}{1}) \xrightarrow{\text{inv}} (\frac{2+\sqrt{3}}{1})$$
$$\xrightarrow[4]{\min} (\frac{\sqrt{3}-2}{1}) \in T^{-}(3)$$

2.5 二次無理数の連分数の循環性

2 次無理数 θ の連分数は式 (2.2)、すなわち $\theta_0 = \theta$ として

$$n_k = [\theta_k], \quad (\theta_k - n_k)\theta_{k+1} = 1 \qquad (k = 0, 1, 2, ...)$$

で計算される。以下、$\eta_k = \theta_k - [\theta_k]$ と置く。すると $0 < \eta_k < 1$ である。この節の目標は、この計算過程で発生する数の列 $\eta_0, \eta_1, \eta_2, ...$ が、いずれ T^{-} に入り込むことを示すことにある。

$\theta = (b \pm \sqrt{m})/a$ とする。a と m は自然数、b は整数である。$\sqrt{m}$ は無理数とする。$m - b^2$ は負でも構わない。

以下では $a \mid (m - b^2)$ とする。この条件はきついように思われるかも知れないが、全く一般性を失わない。なぜなら $a \nmid (m - b^2)$ であれば $(m - b^2)/a = d/c$ となる d と c を導入して $a' = ac,\ b' = bc,\ m' = mc^2$ とすれば

$$(b \pm \sqrt{m})/a = (bc \pm \sqrt{mc^2})/(ac) = (b' \pm \sqrt{m'})/a'$$

となり、しかも $(m' - b'^2)/a' = (c^2(m - b^2))/(ac) = d$ 故 $a' \mid (m' - b'^2)$ となるからである。d/c は通分しておいて構わない。

例 1. $\theta = \dfrac{5 + \sqrt{11}}{6}$ これは $(a, b, m) = (6, 5, 11)$ に相当する。$b^2 - m = 14$ は 6 では割り切れない。$14/6 = 7/3$ 故 $\dfrac{5 + \sqrt{11}}{6} \cdot \dfrac{3}{3} = \dfrac{15 + \sqrt{99}}{18}$ を作る。今度は $\dfrac{15^2 - 99}{18} = \dfrac{7}{1}$ である。

逆数の計算結果と、それをさらに最小化した結果を表 2.1 に示す。$\eta = \eta_0$ で、ここから出発する。$0 < \eta < 1$ である。a' は $aa' = |m - b^2|$ を満たす正整数である。b' は b から a' を (幾つか) 引いて得られる整数である。詳しくは $n = [\theta'] \geq 1,\ b' = b - na'$ である。従って $b' < b$ である。

表 2.1: 状態遷移表

TYPE	η	$m-b^2$	$\theta'=\eta^{-1}$	$\eta'=\theta'-[\theta']$	η' の TYPE
(A)	$\dfrac{b+\sqrt{m}}{a}$	$m>b^2$	$\dfrac{-b+\sqrt{m}}{a'}$	$\dfrac{-b'+\sqrt{m}}{a'}$	T^-
(B)	$\dfrac{b+\sqrt{m}}{a}$	$m<b^2$	$\dfrac{b-\sqrt{m}}{a'}$	$\dfrac{b'-\sqrt{m}}{a'}$	(D)
(C)	$\dfrac{b-\sqrt{m}}{a}$	$m>b^2$			
(D)	$\dfrac{b-\sqrt{m}}{a}$	$m<b^2$	$\dfrac{b+\sqrt{m}}{a'}$	$\dfrac{b'+\sqrt{m}}{a'}$	(A) or (B)

TYPE (A) $(b+\sqrt{m})/a$ は S^- の元であるが (S^- の定義)、そのままでも T^- の元であるかも知れない。そうでなければ逆数 θ' は S^+ の元であり (補題 1)、その最小化 η' は T^- の元である (補題 2 と T^- の定義)。

TYPE (B) $\eta>0$ であるから、条件 $m<b^2$ の下では $b>0$ である。結局 $b>\sqrt{m}$ である。$0<\eta'<1$ であるから、$b'>\sqrt{m}$ である。従って η' は TYPE(D) である。

TYPE (C) 条件 $m>b^2$ の元では $b-\sqrt{m}<0$ であり、$\eta>0$ の条件と矛盾する。従って、このタイプは発生しない。

TYPE (D) $\eta>0$ であるから $b>0$ であるが、条件 $m<b^2$ によって、$b>\sqrt{m}$ である。η' のタイプは、m と b'^2 との大小によって 2 つの可能性がある。$m>b'^2$ なら η' は TYPE (A) であり、T^- に入って、そこで循環する。$m<b'^2$ ならば TYPE (B) であるが、その後、さらに TYPE (D) に行く。従って TYPE (B) と TYPE (D) との中での循環が発生しないことを証明する必要がある。証明は次のようにやればよいであろう。仮に循環が発生したとして、それを

$$\frac{b_0\pm\sqrt{m}}{a_0}\to\frac{b_1\mp\sqrt{m}}{a_1}\to\frac{b_2\pm\sqrt{m}}{a_2}\to\cdots$$

しよう。整数 b_k $(k=0,1,2...)$ には下限がある: $b_k>-\sqrt{m}$。他方 $b_0>b_1>b_2>\cdots$ である。しかし、これは不可能である。

例 2. $\eta = \dfrac{3+\sqrt{5}}{6}$ から出発する。$\dfrac{3^2-5}{6} = \dfrac{2}{3}$ 故、$\eta = \dfrac{3+\sqrt{5}}{6} \cdot \dfrac{3}{3} = \dfrac{9+\sqrt{45}}{18}$ と修正しておく。これは TYPE(B) である。

$$\left(\frac{9+\sqrt{45}}{18}\right) \xrightarrow{\text{inv}} \left(\frac{9-\sqrt{45}}{2}\right) \xrightarrow[1]{\min} \left(\frac{7-\sqrt{45}}{2}\right) \qquad \text{TYPE(D)}$$

$$\left(\frac{7-\sqrt{45}}{2}\right) \xrightarrow{\text{inv}} \left(\frac{7+\sqrt{45}}{2}\right) \xrightarrow[6]{\min} \left(\frac{-5+\sqrt{45}}{2}\right) \qquad \text{TYPE(A)}$$

$\dfrac{-5+\sqrt{45}}{2}$ は T^- の元である。

Chapter 3

二次無理数の連分数の周期

3.1 T^- の位数

定義: 記号 $|M|$: 集合 M の位数を $|M|$ で表す。M は任意の集合である。

例えば $|T^-(m)|$ は集合 $T^-(m)$ の位数である。

3.1.1 S の位数

$S(m)$ の元 $(\sqrt{m}+b)/a$ は、m を与えたときに、a と b で決まる。b は $\sqrt{m} > |b| > 0$、a は $a \mid (m-b^2)$ で決まったので

$$|S(m)| = 2\sum_{b=1}^{[\sqrt{m}]} d(m-b^2)$$

である。ここに $d(n)$ は n の約数の個数である。例えば $n=6$ の約数は $1,2,3,6$ なので $d(6)=4$ である。2 倍してあるのは b は 正負を許すからである。

3.1.2 S^- の位数

$S(m) = S^-(m) \cup S^+(m),\ S^-(m) \cap S^+(m) = \emptyset,\ |S^-(m)| = |S^+(m)|$ であるから

$$|S^-(m)| = \sum_{b=1}^{[\sqrt{m}]} d(m - b^2) \tag{3.1}$$

である。

このような回りくどい言い方をしたのは $\xi \in S$ かつ $\xi < 1$ のような条件を式に反映させるのが面倒だからである。

3.1.3 T^- の位数

T^- の元を、T^- の定義どおりに「$\xi \in S$ かつ $\xi < 1$ かつ $\xi^* > 1$」で調べるのは面倒である。そこでアプローチを工夫する。

$m - b^2 = ac$ とすると

$$(\frac{\sqrt{m} - b}{a})(\frac{\sqrt{m} + b}{c}) = (\frac{\sqrt{m} - b}{c})(\frac{\sqrt{m} + b}{a}) = 1$$

である。故に $(\sqrt{m} - b)/a > 1$ であれば $(\sqrt{m} + b)/c < 1$ であるから、$(\sqrt{m} - b)/c < 1$ であったとしても $(\sqrt{m} - b)/c \notin T^-$ である。

$b_0 = [\sqrt{m}]$ とする。すると条件 $(\sqrt{m} - b)/a < 1$ から $b_0 - b < a$ を得る。従って、各 $b = 1, 2, ..., b_0$ に対して、可能な a は次の条件から決まる。

- $a \mid (m - b^2)$
- $b_0 - b < a$ and $b_0 - b < c$ 但し $c = (m - b^2)/a$

例 1. $m = 7$:
このとき $b_0 = 2,\ b = 1, 2$
$b = 1$ で $m - b^2 = 6 = ac = (1 \cdot 6),\ 2 \cdot 3,\ 3 \cdot 2,\ (6 \cdot 1)$
$b = 2$ で $m - b^2 = 3 = ac = 1 \cdot 3,\ 3 \cdot 1$
$|T^-(7)| = 4$
注: (...) は条件から外れているもの

例 2. $m = 8$:
このとき $b_0 = 2,\ b = 1, 2$
$b = 1$ で $m - b^2 = 7 = ac = (1 \cdot 7),\ (7 \cdot 1)$
$b = 2$ で $m - b^2 = 4 = ac = 1 \cdot 4,\ 2 \cdot 2,\ 4 \cdot 1$
$|T^-(8)| = 3$
注: (...) は条件から外れているもの

例 3. $m = 13$:
このとき $b_0 = 3,\ b = 1, 2, 3$
$b = 1$ で $m - b^2 = 12 = ac = (1 \cdot 12),\ (2 \cdot 6),\ 3 \cdot 4, ...$
$b = 2$ で $m - b^2 = 9 = ac = (1 \cdot 9),\ 3 \cdot 3, ...$
$b = 3$ で $m - b^2 = 4 = ac = 1 \cdot 4,\ 2 \cdot 2, ...$
注: $a \leq c$ だけを書いた。この場合の計算法は $|T^-(13)| = 2 \cdot 2 + 1 \cdot 2 = 6$
注: (...) は条件から外れているもの

例 4. $m = 19$:
このとき $b_0 = 4,\ b = 1, 2, 3, 4$
$b = 1$ で $m - b^2 = 18 = ac = (1 \cdot 18),\ (2 \cdot 9),\ (3 \cdot 6), ...$
$b = 2$ で $m - b^2 = 15 = ac = (1 \cdot 15),\ 3 \cdot 5, ...$
$b = 3$ で $m - b^2 = 10 = ac = (1 \cdot 10),\ 2 \cdot 5, ...$
$b = 4$ で $m - b^2 = 3 = ac = 1 \cdot 3, ...$
注: $a \leq c$ だけを書いた。この場合の計算法は $|T^-(19)| = 2 \cdot 3 + 1 \cdot 0 = 6$
注: (...) は条件から外れているもの

3.1.4 T^- の位数と S^- の位数との比較

表 3.1 に $|S^-(m)|$ と $|T^-(m)|$ の例を m の幾つかの値について示す。

表 3.1: $|S^-(m)|$ と $|T^-(m)|$ の例

m	2	3	5	6	7	8	10	11	12	13	14	15	17	18	19
$\|S^-(m)\|$	1	2	4	4	6	5	8	8	8	12	8	10	12	11	16
$\|T^-(m)\|$	1	2	2	2	4	3	4	2	4	6	4	4	4	3	6

見て分かるように、$|T^-(m)|$ は $|S^-(m)|$ に比べてかなり小さい。m が大きくなるに従って、違いは顕著になるように見える。しかし、それは見かけ上のことである。観察によると 2 から m における $|T^-(m)|/\sqrt{m}$ の最大値は、m の緩やかな増加関数である。この最大値が更新されたときの m と $|S^-(m)|$ と $|T^-(m)|$ の値の一部を表 3.2 に示す。"ratio" の欄には $100|T^-(m)|/|S^-(m)|$ も書かれている。この比率が $m \to \infty$ で 0 になるのか、それとも有限の値に留まるのかははっきりしない。

表 3.2: $|S^-(m)|$ と $|T^-(m)|$ の比率

m	$\|S^-(m)\|$	$\|T^-(m)\|$	ratio(%)
2	1	1	100
3	2	2	100
7	6	4	66
13	12	6	50
109	74	22	29
244	130	40	30
601	262	64	24
1009	398	92	23
2041	656	140	21
5569	1306	252	19
10921	2060	376	18
21961	3272	564	17
53881	5972	956	16
87481	8122	1256	15

3.2 T^- の位数と連分数の周期

$\sqrt{m}$ を連分数に展開したときの周期を $l(m)$ 、$T^-(m)$ の位数を $|T^-(m)|$ としよう。θ_k を式 (2.1) で定義される実数とすれば、$\theta_1, \theta_2, ... \in T^-(m)$ であり、従って $l(m) \leq |T^-(m)|$ の関係がある。

この周期が更新されたときの m の値と、の関係を表 3.3 に示す。$|T^-(m)|$ と $l(m)$ が一致しているか否かによって 'Y' あるいは 'N' と記されている。$n = [\sqrt{m}]$ である。

連分数の周期は、m が増えるとともに、ところどころ大きな値をとることがあるが、この現象は、$\theta_1, \theta_2, ...$ たちが時々 $T^-(m)$ の全ての要素を渡ることから発生していることがこの表から読み取れる。

表 3.3: 連分数周期と T^- の位数

m	$\|T^-(m)\| = l(m)$?	$\|T^-(m)\|$	$l(m)$	n
2	Y	1	1	1
3	Y	2	2	1
7	Y	4	4	2
13	N	6	5	3
19	Y	6	6	4
31	Y	8	8	5
43	Y	10	10	6
46	Y	12	12	6
94	Y	16	16	9

Beceanu [16] は連分数周期に関する詳細な計算機実験の結果を紹介している。彼は $l(m)/\sqrt{m}$ の振る舞いに注目する。m が大きくなるに従って、この最大値はゆっくりと更新されていく。それでは $\sqrt{m}$ の代わりに $\sqrt{m}\log(m)$ を使ったらどうか? しかし結果は芳しくない。今度は $\sqrt{m}\log(m)$ は $l(m)$ に比べて、(大きな m では) あまりにも大きくなる [1]。

実験が示唆する $l(m)$ の大きさを理論は提供できないでいる。実験と理論と

[1] 筆者の実験では $\sqrt{m}\log\log(m)$ でも同様である

の乖離が大きすぎるのである。最近の理論的な発展のレビューは Saradha [19] にある。ここでは、この問題に、これ以上深入りしない。

Beceanu は、$l(m)$ の振る舞いを式 (3.1) との関係で論じているために [2]、成功したとは言えない。$l(m)$ は $|S^-(m)|$ とではなく $|T^-(m)|$ と比較すべきである。結果を表 3.4 に示す。m は 2 から 10^7 まで試している。Beceanu は、この 4 倍までの表を提示しているが、そこまでは必要はないだろう。表 3.3 との違いは、表 3.4 では $l(m)/\sqrt{m}$ の値が更新されたときの m が表に示されている点にある。m が非常に大きい場合も、$|T^-(m)|$ が $l(m)$ に反映されていることが分かる。

表 3.4 を見る限り $|T^-(m)| = l(m)$ となる m が無限個ありそうではあるが、筆者はまだ証明に成功していない。

表 3.4: 連分数周期と T^- の位数

m	$\|T^-(m)\| = l(m)$?	$\|T^-(m)\|$	$l(m)$	n
2	Y	1	1	1
3	Y	2	2	1
7	Y	4	4	2
43	Y	10	10	6
46	Y	12	12	6
211	Y	26	26	14
331	Y	34	34	18
631	Y	48	48	25
919	Y	60	60	30
1726	Y	88	88	41
4846	Y	152	152	69
7606	Y	194	194	87
10399	Y	228	228	101
10651	Y	234	234	103
10774	Y	238	238	103
18379	Y	322	322	135

[2] Beceanu のプログラムの $d(n)$ には 1 と n が含まれていない

19231	Y	332	332	138
32971	Y	438	438	181
48799	Y	544	544	220
61051	Y	614	614	247
78439	Y	696	696	280
82471	Y	716	716	287
111094	Y	834	834	333
162094	Y	1016	1016	402
187366	Y	1106	1106	432
241894	Y	1262	1262	491
257371	Y	1318	1318	507
289111	Y	1400	1400	537
294694	Y	1438	1438	542
799621	N	3174	2383	894
969406	Y	2664	2664	984
1234531	Y	3030	3030	1111
1365079	Y	3196	3196	1168
1427911	Y	3308	3308	1194
1957099	Y	3898	3898	1398
2237134	Y	4212	4212	1495
2847079	Y	4784	4784	1687
5715319	Y	6892	6892	2390

Balková-Hrušková [18] は次のように述べている。m の全域で成立する連分数の周期 $l(m)$ の上限に関して、定理としては $l(m) \leq 2m$ が知られている。しかし、この評価はあまりにも現実とかけ離れている。代わりに $l(m) \leq 2n$ が ($m \leq 1000$ までの観察に基いて) 予想されていたものの、この予想は $m = 1726$ で破れている。ここに $n = [\sqrt{m}]$ である。詳細は表 3.4 からも確認できる。m が大きくなるに従って、$l(m) \leq 2m$ の破れが酷くなっていくのが分かるであろう。

証明されている関係 $l(m) \leq 2m$ は、ほんの少しだけ改善できる。すなわち $l(m) < m$ が成り立つ。

補題 1. n を自然数とすると $d(n) \leq 2[\sqrt{n}]$

証明: $a_1, a_2, ..., a_l$ を $\sqrt{n}$ 以下の n の約数とする。明らかに $l \leq [\sqrt{n}]$ である。各 a_k には $a_k b_k = n$ なる b_k が存在して、b_k もまた n の約数である。従って n が平方数でなければ $d(n) = 2l \leq 2[\sqrt{n}]$、平方数であれば $d(n) = 2l-1 \leq 2[\sqrt{n}]-1$ であり、どちらにせよ補題の主張が成立する。 □

補題 2. $|S^-(m)| < m$

証明:

$$|S^-(m)| = \sum_{b=1}^{[\sqrt{m}]} d(m-b^2) \leq 2 \sum_{b=1}^{[\sqrt{m}]} [\sqrt{m-b^2}] \leq 2 \sum_{b=1}^{[\sqrt{m}]} \sqrt{m-b^2} < \frac{\pi}{4} m$$

ここで最後の不等関係は $\sum_{b=1}^{[\sqrt{m}]} \sqrt{m-b^2}$ が、半径 $\sqrt{m}$ の $1/4$ 円に含まれることから発生する。 □

定理 1. $\sqrt{m}$ の連分数の周期は m より小さい。

証明:

$$l(m) \leq |T^-(m)| \leq |S^-(m)| < m$$

□

次に Hardy-Wright にある定理を (証明なしに) 紹介する [3]。

補題 3.

$$\overline{\lim}_{n\to\infty} \frac{\log d(n) \log\log n}{\log n} = \log 2$$

後の証明を容易にするために、この補題の言い方を多少変形する。$d(n)$ の代わりに $\hat{d}(n)$ を導入する。

$$\hat{d}(n) = \max(d(1), d(2), ..., d(n))$$

すると $\hat{d}(n)$ は n について増加関数である。

[3]証明は Hardy-Wright p.262 に書かれている。なお、Ramanujan [12] p.44 に、もう少し詳しい結果が載っている

補題 3a.

$$\lim_{n\to\infty} \frac{\log \hat{d}(n) \log\log n}{\log n} = \log 2 \tag{3.2}$$

証明: Hardy-Wright は補題 3 の証明にあたって

$$\log d(n) \leq \frac{(1+\epsilon)\log 2 \log n}{\log\log n}$$

を導いている。この $d(n)$ は $\hat{d}(n)$ に置き換えてよい。(右辺は n の増加関数だから)

また彼らは $n = 2\cdot 3\cdot 5\cdots P$ (P は素数) のとき

$$\log d(n) > \frac{(1-\epsilon)\log 2 \log n}{\log\log n}$$

を導いている。この $d(n)$ も $\hat{d}(n)$ に置き換えてよい。($\hat{d}(n) \geq d(n)$ だから) □

式 (3.2) で $\alpha_n = (\log 2)/(\log\log n)$ と置くと、

$$\lim_{n\to\infty} \frac{\hat{d}(n)}{n^{\alpha_n}} = 1$$

を得る。α_n は非常にゆっくりとした減少関数で $n\to\infty$ で $\alpha_n \to 0$ である。

そこで $\hat{d}(n)$ を使うと [4]

$$|S^-(m)| = \sum_{b=1}^{[\sqrt{m}]} d(m-b^2) < [\sqrt{m}]\hat{d}(m) < \sqrt{m}\hat{d}(m) \tag{3.3}$$

従って

$$1 \geq \lim_{m\to\infty} \frac{|S^-(m)|}{\sqrt{m}\hat{d}(m)} = \lim_{m\to\infty} \frac{|S^-(m)|}{\sqrt{m}\hat{d}(m)} \frac{\hat{d}(m)}{m^{\alpha_m}} = \lim_{m\to\infty} \frac{|S^-(m)|}{\sqrt{m}m^{\alpha_m}}$$

つまり

$$\lim_{m\to\infty} \frac{l(m)}{\sqrt{m}m^{\alpha_m}} \leq 1$$

を得る [5]。

[4] 式 (3.3) の中の $\hat{d}(n)$ を $d(n)$ で置き換えると、この式の不等関係は成立しない。また $\overline{\lim}$ を含む証明は非常にややこしいので、素直な関数 $\hat{d}(n)$ を使って、$\overline{\lim}$ の使用を避けたのである。

[5] Hickerson [13] に同様な評価がある。

3.3 平方根の連分数の周期構造

連分数を $[n_0, n_1, n_2, ...]$ と表記する。また繰り返しの範囲を上線で示す。

定義: 代数共役: $\xi = x + y\sqrt{m}\ (x, y \in Q)$ なる数 ξ に対して、$x - y\sqrt{m}$ を ξ の代数共役と言う [6]。

代数共役は複素共役と同様に、同型写像である。

定理 2. $n_0 = [\sqrt{m}]$ とする。次が成立する [7]。

(a) $\sqrt{m}$ は $[n_0, \overline{n_1, n_2, ..., n_{r-1}, n_r, 2n_0}]$ の周期構造を持つ

(b) $n_k \leq n_0 \quad (k = 1, 2, ..., r)$

(c) $[n_0, \overline{n_1, n_2, ..., n_{r-1}, n_r, 2n_0}) = [n_0, \overline{n_r, n_{r-1}, ..., n_2, n_1, 2n_0}]$

(d) もしも $\sqrt{m} = [n_0, \overline{n_1, n_2, ..., n_{r-1}, n_r, 2n_0}]$ となる m が存在すれば、$n_1, n_2, ..., n_{r-1}, n_r$ を同じにする m が無数に存在する。

証明: (a) の証明: $\theta_0 = \sqrt{m}$ とし、θ_k は式 (2.1)、すなわち

$$\theta_k = (\theta_{k-1} - [\theta_{k-1}])^{-1} \quad (k = 1, 2, ...)$$

で与えられるとする。以下では

$$n_k = [\theta_k],\ \eta_k = \theta_k - n_k \quad (k = 0, 1, 2, ...)$$

とする。

$\eta_1 = \sqrt{m} - n_0$ は $T^-(m)$ の元であり、従って $T^-(m)$ の中で循環する (第 2 章:定理 1)。つまり $\eta_1 = \eta_{l+1}$ となる $l\ (> 0)$ が存在する。このような l は無数に存在するが、最小なものを選ぶ。

---

[6] どうやら「代数共役」は市民権を得ていないらしい。高木は詳しく「2 次無理数の共役」あるいは単に「共役」を、Hardy-Wright は簡単に「共役 (conjugate)」としている。高木は複素共役の記号と 2 次無理数の共役の記号を区別しているが、Hardy-Wright は共に上線で表している。区別する理由も無いと言うのだろう。しかし、ここでは複素共役と区別して、「代数共役」としておく。2 次体の中で議論しているのだから、これでよいのではないか?

[7] これらの定理は Sierpinski [4] にも載っている。しかし (b) に関しては弱い主張 $n_k < 2n_0$ となってる。Balková-Hrušková [18] には (b) の $n_k \leq n_0$ は observation として紹介されている。証明されていないとのこと。さして難しくはないのに不思議である。(d) の証明は Sierpinski [4] にある。元の証明は Kraïtchik [11] に載っていたらしい。(c) は Galois' Theorem とも呼ばれている [17, 18]。Waerden [10] によると、Galois の最初の論文が連分数に関するもので、その中で証明されたらしい

$\eta_k = (\sqrt{m} - b_k)/a_{k-1}$ と置く。すると、$a_1, a_2, ..., a_{l-1}$ の中には 1 は現れない。なぜなら、仮に $a_k = 1$ $(1 \leq k < l)$ としよう。すると $b_{k+1} = n_k - b_k$ であり、n_k は $b_{k+1} \leq n_0$ の条件下で最大になるように選ばれる。従って、そのときの b_{k+1} は n_0 である。従って

$$\eta_{k+1} = (\sqrt{m} - n_{k+1})/a_k = (\sqrt{m} - n_0)/1 = \eta_1$$

となり、l が $\eta_{l+1} = \eta_1$ となる最小の自然数であるとする当初の仮定に反する。

従って連分数 $a_1, a_2, ...$ の列の中で、最初に現れた 1 から元に戻る。そして $a_l = 1,\ b_1 = n_0$ である。次に $b_l = n_0$、従って $n_l = 2n_0$ を示す。この証明は長くなる。

$(\sqrt{m} + b)/a - n = (\sqrt{m} - b')/a$ の代数共役をとると、$(-\sqrt{m} + b)/a - n = (-\sqrt{m} - b')/a$ である。従って $(\sqrt{m} - b)/a = (\sqrt{m} + b')/a - n$ である。また

$$(\frac{\sqrt{m} - b'}{a})(\frac{\sqrt{m} + b'}{a'}) = 1$$

の代数共役は

$$(\frac{\sqrt{m} + b'}{a})(\frac{\sqrt{m} - b'}{a'}) = 1$$

である。つまり、代数共役を取ることによって

$$\xrightarrow[]{\text{inv}} \frac{\sqrt{m} + b}{a} \xrightarrow[n]{\text{min}} \frac{\sqrt{m} - b'}{a} \xrightarrow[]{\text{inv}} \frac{\sqrt{m} + b'}{a'} \xrightarrow[n']{\text{min}}$$

が

$$\xleftarrow[]{\text{inv}} \frac{\sqrt{m} - b}{a} \xleftarrow[n]{\text{min}} \frac{\sqrt{m} + b'}{a} \xleftarrow[]{\text{inv}} \frac{\sqrt{m} - b'}{a'} \xleftarrow[n']{\text{min}}$$

に反転する。

さて θ_l から θ_1 へ遷移する場面、すなわち $\theta_1 = (\theta_l - n_l)^{-1}$ の近くでは次のようになっている。

$$\xrightarrow[n_{l-1}]{\text{min}} \frac{\sqrt{m} - b_l}{a_{l-1}} \xrightarrow[]{\text{inv}} \frac{\sqrt{m} + b_l}{a_l} \xrightarrow[n_l]{\text{min}} \frac{\sqrt{m} - b_1}{a_l} \xrightarrow[]{\text{inv}} \frac{\sqrt{m} + b_1}{a_1} \xrightarrow[n_1]{\text{min}} \tag{3.4}$$

$$\xleftarrow[n_{l-1}]{\text{min}} \frac{\sqrt{m} + b_l}{a_{l-1}} \xleftarrow[]{\text{inv}} \frac{\sqrt{m} - b_l}{a_l} \xleftarrow[n_l]{\text{min}} \frac{\sqrt{m} + b_1}{a_l} \xleftarrow[]{\text{inv}} \frac{\sqrt{m} - b_1}{a_1} \xleftarrow[n_1]{\text{min}} \tag{3.5}$$

循環しているので $a_{l+k} = a_k,\ b_{l+k} = b_k,\ n_{l+k} = n_k$ である。

$\theta = \sqrt{m}$ の場合には $\eta_0 = \eta_l = (\sqrt{m} - n_0)/1$ で、従って $a_l = 1,\ b_1 = n_0$ となっている。その場合には式 (3.5) によって $b_l = b_1 = n_0,\ n_l = 2n_0$ となる。

(b) の証明:

$$\frac{\sqrt{m}+b_k}{a_k} - n_k = \frac{\sqrt{m}-b_{k+1}}{a_k}$$

従って $b_k + b_{k+1} = n_k a_k$ である。他方、第 2.2 節:補題 5 によると b_k $(k = 1, 2, ..., r)$ はどれも $0 < b_k < \sqrt{m}$ すなわち $0 < b_k \leq n_0$ を満たす。従って $b_k + b_{k+1} \leq 2n_0$ であり、$a_k = 1$ は $k = l$ でのみ発生し、$n_k = n_l = 2n_0$ である。$a_k \geq 2$ の場合には $n_k a_k \leq 2n_0$ より $n_k \leq n_0$ を得る。

(c) の証明:

また式 (3.4) の $(\sqrt{m} - b_1)/a_l$ と式 (3.5) の $(\sqrt{m} - b_l)/a_l$ は同じなので、式 (3.4) によって辿って得られる $n_1, n_2, ...$ と、式 (3.5) によって辿って得られる $n_{l-1}, n_{l-2}, ...$ とは同じ数字列となる。

(d) の証明:

次節で、具体的に解を構成することによって、証明する予定である。その中で解が存在する条件も示される。 □

注釈: この定理の別証を第 5 章の定理 1 に載せておく。

Chapter 4

平方根の連分数の逆問題

連分数の表記法　ここでは Hardy-Wright に従い、連分数を $[n_0, n_1, ...]$ で表す。また繰り返しの範囲を上線で示す。
つまり $[n_0, n_1, ..., n_k, \overline{n_{k+1}, n_{k+2}, ..., n_{k+r}}]$ のように書く。
　しかし、このままでは $[n]$ が Gauss の整数化の記法と紛らわしいので、連分数の場合には $[n,]$ と書くことにしよう。

目標　ここでは平方根 $\sqrt{m}$ の連分数を扱うので、

$$\sqrt{m} = [n, \overline{n_1, n_2, ..., n_r, 2n}] \tag{4.1}$$

としてよい。我々の目標は $n_1, n_2, ..., n_r$ を与えて、m を求めることにある。

4.1　解法: $r = 0$

$r = 0$ のパターンは $\sqrt{m} = [n, \overline{2n}]$ である。$\sqrt{m} = [n, \theta_1],\ \theta_1 = [2n, \theta_1]$ であるから、次の式が得られる:

$$(\sqrt{m} - n)\theta_1 = 1 \tag{4.2}$$

$$(\theta_1 - 2n)\theta_1 = 1 \tag{4.3}$$

θ_1 を ξ と置くと式 (4.2) および式 (4.3) から、各々

$$(m - n^2)\xi^2 - 2n\xi - 1 = 0$$
$$\xi^2 - 2n\xi - 1 = 0$$

を得る。この 2 つの式を比較して、

$$m = n^2 + 1 \quad (n = 1, 2, 3, ...) \tag{4.4}$$

を得る。つまり $m = 2, 5, 10, 17, ...$ である。

4.2 解法: $r = 1$

$r = 1$ のパターンは $\sqrt{m} = [n, \overline{c, 2n}]$ である。このパターンは m が小さい場合には出現頻度が非常に高い。$\sqrt{m} = [n, \theta_1],\ \theta_1 = [c, 2n, \theta_1]$ であるから、$\theta_1 = [c, \theta_2],\ \theta_2 = [2n, \theta_1]$ と書き換えて、次の式が得られる:

$$(\sqrt{m} - n)\theta_1 = 1 \tag{4.5}$$
$$(\theta_1 - c)\theta_2 = 1$$
$$(\theta_2 - 2n)\theta_1 = 1$$

簡単のため θ_1 を ξ とする。逆方向から計算していくほうが楽である。

$$\theta_2 = 2n + \frac{1}{\xi} = \frac{2n\xi + 1}{\xi}, \quad \xi = c + \frac{1}{\theta_2} = c + \frac{\xi}{2n\xi + 1} = \frac{c(2n\xi + 1) + \xi}{2n\xi + 1}$$

これから

$$2n\xi^2 - 2nc\xi - c = 0 \tag{4.6}$$

を得る。他方、式 (4.5) からは

$$a\xi^2 - 2n\xi - 1 = 0, \quad a = m - n^2 \tag{4.7}$$

が得られる。この 2 つの式を比較すると、

$$ac = 2n \tag{4.8}$$

を得る。

$m = n^2 + a$ であるから、$a = 1$ のケースは既に $\sqrt{m} = [n, \overline{2n}]$ で扱われている。従って $a \geq 2$ としてよい。つまり c は $c \leq n$ を満たす必要がある。従って $\sqrt{m} = [n, c, 2n]$ となる m が存在するためには $c \mid (2n)$ で、その場合 $a = (2n)/c$

と置いて、$m = n^2 + a$ である。

あるいは次のように考えてもよい。c を与えたとき、解 (a, n) は、c が奇数の場合、$a \mid (2n)$ の条件より、$(a, n) = (2k, ck)$ である。このとき $m = k(kc^2 + 2)$ となる。他方 c が偶数の場合、$c = 2d$ と置いて、式 (4.8) より $n = ad$ を得る。従って、$(a, n) = (k, kd)$ である。条件 $a \geq 2$ より $k \geq 2$ である。このとき $m = k(kd^2 + 1)$ となる。

逆に m からの連分数の計算は $m = n^2 + a$ $(a \geq 2)$ として $a \mid 2n$ であれば $c = (2n)/a$ と置いて $[n, c, 2n]$ が答となる。

各 c について無限個の解がある。c 毎に、最初の 3 つの k から生じる a, n, m を表に示す。c が奇数であれば、k は 1 から始まり、偶数なら 2 から始まる。

c	k	a	n	m
1	1	2	1	3
1	2	4	2	8
1	3	6	3	15
2	2	2	2	6
2	3	3	3	12
2	4	4	4	20
3	1	2	3	11
3	2	4	6	40
3	3	6	9	87
4	2	2	4	18
4	3	3	6	39
4	4	4	8	68

得られた結果を、m が小さい方から書くと、$m = 3, 6, 8, 11, 12, 15, ...$ となる。

4.3 解法: $r \geq 2$

式 (4.1) を

$$\sqrt{m} = [n, \xi], \quad \xi = \overline{[n_1, n_2, ..., n_r, 2n]} \tag{4.9}$$

と書き換える。すると

$$\sqrt{m} = n + \frac{1}{\xi} \tag{4.10}$$

であるから、まず

$$(m - n^2)\xi^2 - 2n\xi - 1 = 0 \tag{4.11}$$

を得る。そこで $a = m - n^2$ と置くと、

$$a\xi^2 - 2n\xi - 1 = 0 \tag{4.12}$$

となる。a と n が求まると $m = n^2 + a$ で m が得られる。

次に n を求めるために、式 (4.9) から ξ についてのもう一つの方程式を導く。

$$\xi = [n_1, n_2, ..., n_r, 2n, \xi]$$

であるから

$$\begin{aligned}\xi &= \frac{H(n_1, n_2, ..., n_r, 2n.\xi)}{H(n_2, ..., n_r, 2n, \xi)} \\ &= \frac{H(n_1, n_2, ..., n_r, 2n)\xi + H(n_1, n_2, ..., n_r)}{H(n_2, n_2, ..., n_r, 2n)\xi + H(n_2, n_2, ..., n_r)}\end{aligned}$$

となる (付録 C)。従って ξ についての方程式を立てると

$$A\xi^2 - B\xi - C = 0$$

ここに

$$\begin{aligned}A &= H(n_2, n_3, ..., n_r, 2n) \\ B &= H(n_1, n_2, ..., n_r, 2n) - H(n_2, n_2, ..., n_r) \\ C &= H(n_1, n_2, ..., n_r)\end{aligned}$$

であるが、$r \geq 2$ として $2n$ を外に出すと

$$\begin{aligned}A &= 2nH(n_2, n_3, ..., n_r) + H(n_2, n_3, ..., n_{r-1}) \\ B &= 2nH(n_1, n_2, ..., n_r) + H(n_1, n_2, ..., n_{r-1}) - H(n_2, n_3, ..., n_r) \\ C &= H(n_1, n_2, ..., n_r)\end{aligned} \tag{4.13}$$

となる。ところが

$$H(n_1, n_2, ..., n_{r-1}) = H(n_2, n_3, ..., n_r)$$

である。

証明: 関数 H の性質より $H(n_2, n_3, ..., n_r) = H(n_r, ..., n_3, n_2)$ である。他方 $n_1, n_2, ..., n_{r-1}, n_r$ の対称性 (第 3.3 節:定理 2) より

$$H(n_r, ..., n_3, n_2) = H(n_1, n_2, n_3, ..., n_{r-1})$$

となる。 □

従って ξ は

$$A\xi^2 - 2nC\xi - C = 0$$
$$A = 2nH(n_2, n_3, ..., n_r) + H(n_2, n_3, ..., n_{r-1})$$
$$C = H(n_1, n_2, ..., n_r)$$

を満たす。この結果と、式 (4.12) に C を掛けた

$$aC\xi^2 - 2nC\xi - C = 0$$

を比較して $aC = A$ すなわち

$$aH(n_1, n_2, ..., n_r) = 2nH(n_2, n_3, ..., n_r) + H(n_2, n_3, ..., n_{r-1}) \qquad (4.14)$$

を得る。

従って目標は a, n についての不定方程式 (4.14) を解くことにある。簡潔に書くために

$$p_k = H(n_1, n_2, ..., n_k), \quad q_k = H(n_2, n_3, ..., n_k) \qquad (1 \le k \le r) \qquad (4.15)$$

と置くと、式 (4.14) は

$$ap_r = 2nq_r + q_{r-1} \qquad (4.16)$$

となる。そこで最初に、x, y に関する次の不定方程式の解の、一般的性質を明らかにしておく。

$$xp_r - yq_r = q_{r-1} \qquad (4.17)$$

以下の議論に次の補題が役に立つ。

補題 1. $n_1, n_2, ..., n_r > 0$ であれば $p_k, q_k > 0$ である。

証明: これは関数 H の一般的性質である。実際 p_r については、$H(n_1) > 0$, $H(n_1, n_2) > 0$ と

$$H(n_1, n_2, ..., n_r) = n_r H(n_1, n_2, ..., n_{r-1}) + H(n_1, n_2, ..., n_{r-2})$$

の関係から再帰的に正であることが示される。q_r についても同様である。 □

補題 2. $n_1, n_2, ..., n_r \geq 1$ であれば $p_r > p_{r-1}, \quad q_r > q_{r-1}$ である。

証明:

$$\begin{aligned} p_r - p_{r-1} &= H(n_1, ..., n_r) - H(n_1, ..., n_{r-1}) \\ &= H(n_1, ..., n_{r-1})(n_r - 1) + H(n_1, ..., n_{r-2}) > 0 \end{aligned}$$

$q_r - q_{r-1}$ についても同様である。 □

補題 3. 次の不等関係が成り立つ:

$$p_r > q_r > q_{r-1}$$

証明: $n_1, ..., n_r$ は正である。従って

$$\begin{aligned} p_r &= H(n_1, ..., n_r) = n_1 H(n_2, ..., n_r) + H(n_3, ..., n_r) > H(n_2, ..., n_r) = q_r \\ q_r &= H(n_2, ..., n_r) = H(n_2, ..., n_{r-1}) n_r + H(n_2, ..., n_{r-2}) \\ &> H(n_2, ..., n_{r-1}) = q_{r-1} \end{aligned}$$

である。 □

補題 4. x, y を

$$x p_r - y q_r = q_{r-1}$$

の整数解とする。その下で次が成り立つ:

(a) $x \geq 0$ とすると、$x \leq y$ である
(b) $x \leq q_r$ とすると、$y < p_r$ である
(c) $y \geq 0$ とすると、$0 < x \leq y$ である
(d) $0 \leq y \leq p_r$ とすると、$0 < x \leq q_r$ である

証明: (a) 補題の式を

$$x(p_r - q_r) + (x - y) q_r = q_{r-1}$$

と変形する。$x \geq 0$ と $p_r > q_r$ 故 $(x - y) q_r \leq q_{r-1}$ であり、また $q_r > q_{r-1}$ 故 $x \leq y$ を得る。

(b) 補題の式を

$$(x - q_r) p_r + (p_r - y) q_r = q_{r-1}$$

と変形する。$x \leq q_r$ より $(p_r - y)q_r \geq q_{r-1}$ であり、また $q_r > q_{r-1}$ 故 $p_r > y$ を得る。

(c) $x > 0$ は明らかである。補題の式を

$$(x - y)p_r + y(p_r - q_r) = q_{r-1}$$

と変形する。$p_r > q_r$ 故 $(x - y)p_r \leq q_{r-1}$ であり、また $p_r > q_{r-1}$ 故 $x \leq y$ を得る。

(d) $x > 0$ は明らかである。補題の式を

$$(x - q_r)p_r + (p_r - y)q_r = q_{r-1}$$

と変形する。$p_r \geq y$ より $(x - q_r)p_r \leq q_{r-1}$ であり、また $p_r > q_{r-1}$ 故 $x \leq q_r$ を得る。 □

式 (4.15) で与えられる p_k, q_k に関して、次の恒等式が存在する [1]。

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^k \qquad (2 \leq k \leq r) \tag{4.18}$$

$$p_k q_{k-2} - q_k p_{k-2} = (-1)^{k+1} n_k \qquad (3 \leq k \leq r) \tag{4.19}$$

この恒等式は $n_1, n_2, ..., n_r$ の対称性の有無に関わらず成立する。

この恒等式から次の重要な性質が読み取れる: $p_k q_{k-1}$ と $q_k p_{k-1}$ は互いに素である。

対称性がある場合には

$$p_{r-1} = q_r \tag{4.20}$$

である。これと式 (4.18) から

$$p_r q_{r-1} - q_r^2 = (-1)^r \tag{4.21}$$

を得る。ここから得られる p_r, q_r, q_{r-1} の偶奇関係を表に示す。

[1] この恒等式は Appendix C で証明されている。比較するときは Appendix C の方は Hadry-Wright に従って $p_n = H(a_0, a_1, ..., a_n)$ となっているが、ここでは $p_n = H(a_1, ..., a_n)$ となっていることに注意しなくてはならない

表 4.1: 偶奇表 1

p_r	q_r	q_{r-1}
奇	奇	偶
奇	偶	奇
偶	奇	奇
偶	奇	偶

x_0, y_0 を不定方程式 (4.17) の一つの解 (特殊解) とする。すなわち x_0, y_0 は

$$x_0 p_r - y_0 q_r = q_{r-1} \tag{4.22}$$

を満たすとする。すると

$$(x - x_0)p_r - (y - y_0)q_r = 0$$

であるから、方程式 (4.17) の任意の解は

$$x = x_0 + kq_r, \quad y = y_0 + kp_r \qquad (k \in Z)$$

が得られる。

式 (4.21) の両辺に q_{r-1} を掛けると

$$p_r q_{r-1}^2 - q_{r-1} q_r^2 = (-1)^r q_{r-1}$$

を得る。この恒等式は特殊解 x_0, y_0 を求めるために使える。これと式 (4.22) を比較して

$$x_0 = (-1)^r q_{r-1}^2, \quad y_0 = (-1)^r q_{r-1} q_r \tag{4.23}$$

とすればよい。従って一般解は

$$x = kq_r + (-1)^r q_{r-1}^2, \quad y = kp_r + (-1)^r q_{r-1} q_r \quad (k \in Z) \tag{4.24}$$

である。

a, n についての不定方程式 (4.16) を解くには、次の条件を全て満たす解 x, y が必要である。

(a) $x > 0,\ y > 0$

(b) y は偶数である

(c) $n_{\max} \leq y/2$

ここに $n_{\max} = \max(n_1, n_2, ..., n_r)$ である。そのような解が得られれば $a = x,\ n = y/2$ である。

$q_{r-1}q_r$ が奇数の場合には、表 4.1 によって、p_r は偶数である。従って y を偶数とする k は存在しない。他方 $q_{r-1}q_r$ 、y が偶数となるように、次のように k を選ぶことができる:

- p_r が偶数であれば、k の偶奇に関わらず y は偶数となる
- p_r が奇数であれば、k を偶数に選ぶ

k を正の方向に大きくすると $y \to +\infty$、逆に負の方向に大きくすると $y \to -\infty$ となるから $y \geq 2n_{\max}$ とする最小の k が存在する。そのときの x, y の組を x_1, y_1 とすると、$p_r, q_r, q_{r-1} > 0$ なので、式 (4.17) によって x_1 は正である。従って

$$a = kq_r + x_1, \quad 2n = kp_r + y_1, \quad (k \geq 0) \tag{4.25}$$

となる。ここに、y_1 は偶数である。p_r が奇数の場合には、k を偶数に選ぶ必要がある。

以上より、次の定理が得られた。

定理 1. 数列 $n_1, n_2, ..., n_r$ は対称性 $(n_1, n_2, ..., n_r) = (n_r, ..., n_2, n_1)$ を持っているとする。また p_r, q_r, q_{r-1} は式 (4.15) で与えられているとする。そのとき、不定方程式 (4.16) の解 (a, n) が存在するための必要充分条件は

$$q_{r-1}q_r \equiv 0 \pmod 2 \tag{4.26}$$

である。

ところで n と a は独立していないのである。なぜなら $n = [\sqrt{m}],\ m = n^2 + a$ である。$(n+1)^2 > m$ であるから $2n + 1 > a$ でなくてはならない。つまり $y \geq x$ の必要がある。これが成立していることは補題 4 で示されている。

結局、条件式 (4.26) を考慮に入れると、表 4.1 に代って次の表を得る。

表 4.2: 偶奇表 2

p_r	q_r	q_{r-1}	k
奇	奇	偶	偶
奇	偶	奇	偶
偶	奇	偶	偶/奇

結局 a, n を手に入れる計算プロセスは次のようになろう。(条件を満たさない場合には、次のステップに行く)

(S1) p_r, q_r, q_{r-1} および $n_{\max}$ を計算する
(S2) $0 < x < q_r,\ 0 < y < p_r$ を満たす x, y を
$x \equiv (-1)^r q_{r-1}^2 \pmod{q_r}, \quad y \equiv (-1)^r q_{r-1} q_r \pmod{p_r}$
から算出する
(S3) $y < 2n_{\max}$ なら x に q_r を、y に p_r を加える
(S4) y が奇数なら x に q_r を、y に p_r を加える
(S5) y が偶数なら (S7) へ行く
(S6) 解は存在しない。計算を止める
(S7) $a = x,\ n = y/2$ として終わる

さて Balková-Hrušková [18] は、$\sqrt{m}$ の連分数の周期が奇数の場合には $a \equiv 3 \pmod 4$ の解が存在しないことを、観察結果から予想している。証明はされていないと言う。ここで、この予想が正しいことを証明しよう。

余題 1. r が偶数の場合、$a \not\equiv 3 \pmod 4$ である [2]。

証明: r が偶数の場合には、式 (4.24) は

$$x = kq_r + q_{r-1}^2, \quad y = kp_r + q_{r-1}q_r \quad (k \in Z)$$

となる。

[2] Pell 方程式を使った別証明が第 5.3 節:定理 2 にある。

q_{r-1} が奇数の場合、q_r は偶数である。従って表 4.2 より、p_r は奇数である。従って k は偶数になる。$q_{r-1} = 2k' + 1$ と置こう。すると

$$x = kq_r + q_{r-1}^2 = kq_r + (2k' + 1)^2 \equiv 0 + 1 \pmod 4$$

従って $a = x \not\equiv 3 \pmod 4$ である。

q_{r-1} が偶数かつ p_r が奇数の場合には、表 4.2 より、k は偶数、q_r は奇数になる。従って x は偶数、つまり $a = x \not\equiv 3 \pmod 4$ である。

q_{r-1} が偶数かつ p_r が偶数のケースは、r が偶数の場合には発生しない。なぜなら、表 4.2 より q_r は奇数である。他方、式 (4.21) は

$$p_r q_{r-1} = q_r^2 + 1$$

となる。この式の左辺は 4 の倍数である。右辺は $q_r = 2k + 1$ と置けば分かるように、4 の倍数にはならない。

以上によって、$r \geq 2$ の場合に余題の主張が証明されたが、$r = 0$ の場合には $a = 1$ であるから余題の主張は成立している。 □

補足 1 式 (4.17) を引用する:

$$xp_r - yq_r = q_{r-1}$$

この式の一般解は

$$x = kq_r + (-1)^r q_{r-1}^2, \quad y = kp_r + (-1)^r q_{r-1} q_r \quad (k \in Z)$$

であった。そして逆問題を解くには、x, y が自然数となる最小解が必要であった。原理的には、そのような解は合同式

$$y \equiv (-1)^r q_{r-1} q_r \pmod{p_r} \tag{4.27}$$

から $y > 0$ となる最小の y と、そのときの k を求めて、その k を x に適用すればよかったのである。補題 4 によると、そうして得られる x は $0 < x \leq q_r$ を満たしている。従って、この不等式を満たす x を見つければよいのである。

次の合同式から得られる x は $0 < x < q_r$ を満たしている。

$$x \equiv (-1)^r q_{r-1}^2 \pmod{q_r} \tag{4.28}$$

q_r と q_{r-1} は互いに素であるから、$x = 0$ にはならない。つまり、合同式 (4.27,4.28) から得られる正の最小の x, y で構わない。

合同式 (4.28) からは $x = kq_r + (-1)^r q_{r-1}^2$ を満たす k が、合同式 (4.27) からは $y = k'p_r + (-1)^r q_{r-1}q_r$ を満たす k' が得られる。しかし一般的に言えば $k = k'$ となる保証は無い。

$$k = [(-1)^r \frac{q_{r-1}^2}{q_r}], \quad k' = [(-1)^r \frac{q_{r-1}q_r}{p_r}]$$

であるから、$k = k'$ となるには

$$[(-1)^r \frac{q_{r-1}^2}{q_r}] = [(-1)^r \frac{q_{r-1}q_r}{p_r}]$$

となる必要がある。そして、この条件は

$$[\frac{q_{r-1}^2}{q_r}] = [\frac{q_{r-1}q_r}{p_r}] \tag{4.29}$$

に等しい。

注: 任意の実数 ω に対して、$n = [\omega]$ としたとき $n \leq \omega < n+1$ となる。従って q を自然数、p を $q \nmid p$ である整数とすると、$n = [\frac{p}{q}]$ なる n によって、$nq < p < nq + q$ である。すなわち $p = nq + r$ となる n と r $(0 < r < q)$ が p の正負に関わらず存在する。

$n' = [-\frac{p}{q}]$ とする。すると $-p = n'q + r'$ となる r' $(0 < r' < q)$ が存在する。従って $0 = (n + n')q + (r + r')$ である。そして $0 < r + r' < 2q$ であるから、$n + n' = -1$ である。従って $[\frac{p}{q}] + [-\frac{p}{q}] = -1$ である。

例えば $[-\frac{5}{3}] = -1 - [\frac{5}{3}] = -1 - 1 = -2$ である。

式 (4.29) は任意の $n_1, n_2, ..., n_r$ $(r \geq 2)$ に対しては成立しないことは、例えば $n_1, n_2, ..., n_r = 2, 3, 5$ を試してみれば分かる。この場合には、$(p_3, q_3, q_2) = (37, 16, 3)$ で、従って $[q_{r-1}^2/q_r] = [9/16] = 0$、$[(q_{r-1}q_r)/p_r] = [48/37] = 1$ であり、式 (4.29) が成り立たない。$n_1, n_2, ..., n_r$ の対称性が等式 (4.29) を可能にしているのである。

ここでは等式 (4.29) の証明に間接的な方法がとられた。直接的に証明するのは難しそうである。

4.4 計算例

n_k $(k = 1, ..., r)$ を与えて p_k と q_k を計算するアルゴリズムを示す。

$$p_0 = 1, \quad p_1 = n_1, \quad q_0 = 0, \quad q_1 = 1, \quad q_2 = n_2$$

$$p_k = n_k p_{k-1} + p_{k-2}, \quad q_k = n_k q_{k-1} + q_{k-2} \qquad (k = 2, ..., r)$$

但し、再帰式を統一的に理解するために、便宜的に $q_0 = 0$ と置いた。

p_k と q_k を再帰的に求めるには、次のような表を作って、左から順に (“?” と書いたところを) 埋めていく。

k	0	1	2	3	...	$r-1$	r
n_k	*	n_1	n_2	n_3	...	n_{r-1}	n_r
p_k	1	n_1	?	?	...	?	?
q_k	0	1	n_2	?	...	?	?

ここに、“*” は空欄を表している。

4.4.1 例 1

k	0	1	2	3	4	5
n_k	*	2	3	4	3	2
p_k	1	2	7	30	97	224
q_k	0	1	3	13	42	97

つまり

$$p_r = 224, \quad q_r = 97, \quad q_{r-1} = 42$$

で、$q_r q_{r-1}$ が偶数だから解を持つ:

$$x \equiv -42^2 \equiv 79 \pmod{97}, \qquad y \equiv -42 \cdot 97 \equiv 182 \pmod{224}$$

故に $n = 91,\ a = 79$ となり $m = 91^2 + 79 = 8360$ である。

4.4.2 例 2

k	0	1	2	3	4	5	6
n_k	*	2	3	4	4	3	2
p_k	1	2	7	30	127	411	949
q_k	0	1	3	13	55	178	411

つまり

$$p_r = 949, \quad q_r = 411, \quad q_{r-1} = 178$$

で、$q_r q_{r-1}$ が偶数だから次の解を持つ:

$$x \equiv 178^2 \equiv 37 \pmod{411}, \qquad y \equiv 178 \cdot 411 \equiv 85 \pmod{949}$$

であるが、しかし、この y は奇数である。従って x, y に各々 q_r, p_r を追加する必要がある。その結果 $x = 448,\ y = 1034$ を得る。これから $n = 517,\ a = 448$ となり $m = 517^2 + 448 = 267737$ である。

4.4.3 例 3

k	0	1	2	3
n_k	*	1	2	1
p_k	1	1	3	4
q_k	0	1	2	3

つまり

$$p_r = 4, \quad q_r = 3, \quad q_{r-1} = 2$$

で、$q_r q_{r-1}$ が偶数だから次の解を持つ:

$$x \equiv -2^2 \equiv 2 \pmod{3}, \qquad y \equiv -2 \cdot 3 \equiv 2 \pmod{4}$$

しかし $n = y/2 = 1$ は n_k の最大値 2 に満たない。従って x, y に各々 q_r, p_r を追加する必要がある。その結果 $x = 5,\ y = 6$ を得る。これから $n = 3,\ a = 5$ となり $m = 3^2 + 5 = 14$ である。

4.4.4 例 4

k	0	1	2	3	4	5
n_k	*	1	2	1	2	1
p_k	1	1	3	4	11	15
q_k	0	1	2	3	8	11

つまり

$$p_r = 15, \quad q_r = 11, \quad q_{r-1} = 8$$

で、$q_r q_{r-1}$ が偶数だから次の解を持つ: $r = 5$ で

$$x \equiv -8^2 \equiv 2 \pmod{11}, \qquad y \equiv -8 \cdot 11 \equiv 2 \pmod{15}$$

しかし $n = y/2 = 1$ は n_k の最大値 2 に満たない。従って x, y に各々 q_r, p_r を追加する必要がある。その結果 $x = 13,\ y = 17$ を得る。

しかし $y = 17$ は奇数である。従って x, y に各々 q_r, p_r を追加する必要がある。その結果 $x = 24,\ y = 32$ を得る。これから $n = 16,\ a = 24$ となり $m = 16^2 + 24 = 280$ である。

4.5 特殊ケース

4.5.1 $\sqrt{m} = [n, 1, 1, 1, ..., 2n]$

これは $n_1 = n_2 = \cdots = n_r = 1$ のケースである。$r = 0$ の場合は既に第 4.1 節で、$r = 1$ の場合は第 4.2 節で解決されており、ここでは $r \geq 2$ の場合を扱う。その場合、第 4.3 節で得られた成果を活用できる。

目標は不定方程式

$$xp_r - yq_r = q_{r-1}$$

の解で y が偶数のものを見つけることにあった。見つかれば $a = x,\ n = y/2,\ m = n^2 + a$ として m が求まる。ここに

$$p_k = H(n_1, n_2, ..., n_k)\ (0 \leq k \leq r), \qquad q_k = H(n_2, ..., n_k)\ (1 \leq k \leq r)$$

である。

$H() = 1,\ H(1) = 1$ と公式

$$H(n_1, n_2, ..., n_k) = n_k H(n_1, n_2, ..., n_{k-1}) + H(n_1, n_2, ..., n_{k-2})$$

により

$$p_0 = 1, \quad p_1 = 1$$
$$p_k = p_{k-1} + p_{k-2} \quad (k = 2, 3, 4, ..., r)$$

および、$H(n_2, ..., n_k) = n_k H(n_2, ..., n_{k-1}) + H(n_2, ..., n_{k-2})$ により

$$q_1 = 1, \quad q_2 = 1$$
$$q_k = q_{k-1} + q_{k-2} \quad (k = 3, 4, ..., r)$$

が成り立つ。つまり p_k も q_k も Fibonacci 数である。以下 Fibonacci 数を F_k $(k = 1, 2, 3...)$ で表す。習慣的な Fibonacci 数のインデックス k は 1 から始まる [3]。ここでも、この習慣に従う。すると $p_k = F_{k+1},\ q_k = F_k$ である。

解 m が存在するための条件は

$$q_{r-1}q_r = F_{r-1}F_r \equiv 0 \pmod 2$$

である。言い換えれば $F_{r-1}F_r$ が奇数であれば解は存在しない。

明らかに、

$$F_{3k+0}, F_{3k+1}, F_{3k+2} \equiv 0, 1, 1 \pmod 2 \quad (k = 0, 1, 2, 3, ...)$$

つまり

$$r \equiv 2 \pmod 3$$

の場合には m は存在しない [4]。あるいは p_r m は存在しないと言い換えてもよい。

$m = n^2 + a$ を Fibonacci 数を使って表そう。$x = a,\ y = 2n$ とすれば、$x,\ y$ は式 (4.24)、すなわち

$$x = kq_r + (-1)^r q_{r-1}^2, \quad y = kp_r + (-1)^r q_{r-1}q_r \quad (k \in Z)$$

[3] 例えば Hardy-Wright [3] 、Sierpinski [4]

[4] この結果は、文献 [11] では、observation として紹介されている

で与えられる。この特殊なケースでは、これは

$$x = kF_r + (-1)^r F_{r-1}^2, \quad y = kF_{r+1} + (-1)^r F_{r-1}F_r \quad (k \in Z) \tag{4.30}$$

となる。

y が正の偶数となる最小の x, y を求めよう。次の補題が役に立つ。

補題 5.

$$F_{r+1}F_{r-1} - F_r^2 = (-1)^r \tag{4.31}$$

$$F_{r+1}F_{r-2} - F_rF_{r-1} = (-1)^{r+1} \tag{4.32}$$

証明: 式 (4.18) を引用する:

$$p_kq_{k-1} - q_kp_{k-1} = (-1)^k \qquad (2 \le k \le r)$$

$$p_kq_{k-2} - q_kp_{k-2} = (-1)^{k+1}n_k \qquad (3 \le k \le r)$$

この恒等式は $n_1, n_2, ..., n_r$ の対称性の有無に関わらず成立する。$q_k = F_k,\ p_{k-1} = F_k$ に注意し、$k = r$ を代入し、$n_r = 1$ であることから、補題の関係が得られる。 □

そこで式 (4.30) において、仮に $k = (-1)^{r+1}F_{r-2}$ とすると

$$x = (-1)^r(-F_{r-2}F_r + F_{r-1}^2) = (-1)^r\{-(-1)^{r-1}\} = 1$$

$$y = (-1)^r(-F_{r-2}F_{r+1} + F_{r-1}F_r) = (-1)^r\{-(-1)^{r+1}\} = 1$$

である。これは x, y を正にする最小の組であるが、 y は偶数ではない。そこで $k = (-1)^{r+1}F_{r-2} + k'$ と置いてみる。すると

$$x = k'F_r + 1, \quad y = k'F_{r+1} + 1$$

となる。F_{r+1} が偶数であれば、y を偶数とする k' は存在しない。F_r が奇数であれば、k' を奇数に選ぶ。その下で $a = x,\ n = y/2$ である。

例 1. $k' = 1$ とすると、$r = 2$ では解は存在しない。$r = 3$ で $m = 7$、$r = 4$ で $m = 13$、$r = 5$ では存在しない、$r = 6$ で $m = 58$ である。$r = 1$ は、この証明の適用外であるが、存在が確認できる。

4.5.2 $\sqrt{m} = [n, c, c, c, ..., 2n]$

これは $n_1 = n_2 = \cdots = n_r = c$ のケースである。$r = 0$ の場合は既に第 4.1 節で、$r = 1$ の場合は第 4.2 節で解決されており、ここでは $r \geq 2$ の場合を扱う。その場合、第 4.3 節で得られた成果を活用できる。

目標は不定方程式

$$xp_r - yq_r = q_{r-1}$$

の解で y が偶数のものを見つけることにあった。見つかれば $a = x,\ n = y/2,\ m = n^2 + a$ として m が求まる。ここに

$$p_k = H(n_1, n_2, ..., n_k)\ (0 \leq k \leq r), \qquad q_k = H(n_2, ..., n_k)\ (1 \leq k \leq r)$$

である。

$H() = 1,\ H(c) = c$ と公式

$$H(n_1, n_2, ..., n_k) = n_k H(n_1, n_2, ..., n_{k-1}) + H(n_1, n_2, ..., n_{k-2})$$

により

$$p_0 = 1, \quad p_1 = c$$
$$p_k = cp_{k-1} + p_{k-2} \quad (k = 2, 3, 4, ..., r)$$

が成り立つ。同様に q_k に対しては

$$q_1 = 1, \quad q_2 = c$$
$$q_k = cq_{k-1} + q_{k-2} \quad (k = 3, 4, ..., r)$$

である。従って $q_k = p_{k-1}$ である。

参考のために、最初のいくつかを挙げておく:

$$q_1 = 1, \quad q_2 = c, \quad q_3 = c^2{+}1, \quad q_4 = c^3{+}2c, \quad q_5 = c^4{+}3c^2{+}1, \quad q_6 = c^5{+}4c^3{+}3c$$

解の存在は $q_{r-1}q_r$ の偶奇で決まる。c が奇数の場合には

$$q_1 \equiv q_2 \equiv 1 \pmod 2$$
$$q_k \equiv q_{k-1} + q_{k-2} \pmod 2 \quad (k = 3, 4, ...)$$
$$q_1, q_2, q_3, q_4, q_5, q_6, ... \equiv 1, 1, 0, 1, 1, 0, ... \pmod 2$$

従って $r \equiv 2 \pmod 3$ の場合には解は存在しない。c が偶数の場合には

$$q_1 \equiv 1 \quad q_2 \equiv 0 \pmod 2$$
$$q_k \equiv q_{k-2} \pmod 2 \quad (k = 3, 4, ...)$$
$$q_k \equiv 1 \pmod 2 \quad (k = 1, 3, 5, ...)$$
$$q_k \equiv 0 \pmod 2 \quad (k = 2, 4, 6, ...)$$

従って任意の r について解が存在する。

次に y が正の偶数となる最小の x, y を求めよう。$x = a,\ y = 2n$ とすれば、$x,\ y$ は式 (4.24)、すなわち

$$x = kq_r + (-1)^r q_{r-1}^2, \quad y = kp_r + (-1)^r q_{r-1} q_r \quad (k \in Z)$$

で与えられる。そこで仮に $k = (-1)^{r+1} q_{r-2}$ を試すと

$$x = (-1)^r(-q_{r-2}q_r + q_{r-1}^2)$$
$$y = (-1)^r(-q_{r-2}p_r + q_{r-1}q_r)$$

ここで次の補題が役に立つ。

補題 6.

$$q_r q_{r-2} - q_{r-1}^2 = (-1)^{r+1}$$
$$p_r q_{r-2} - q_r q_{r-1} = (-1)^{r+1} c$$

証明: 式 (4.18) を引用する:

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^k \qquad (2 \le k \le r)$$
$$p_k q_{k-2} - q_k p_{k-2} = (-1)^{k+1} n_k \qquad (3 \le k \le r)$$

この恒等式は $n_1, n_2, ..., n_r$ の対称性の有無に関わらず成立する。$k = r - 1$ を代入する。$p_{r-1} = q_r,\ p_{r-2} = q_{r-1}$ であることから第 1 の式を得る。第 2 の式は、$k = r$ を代入する。$p_{r-2} = q_{r-1},\ n_k = c$ であることから 第 2 の式を得る。 □

従って、この補題によって、$x = 1,\ y = c$ である。c、これで目的の x, y を得たのであるが、しかしながら、ここから得られるのは $a = 1,\ n = y/2$ の解であり、第 4.1 節で $r = 0$ のケースとして、既に終わっている。従って c の偶奇に関わらず、もう少し計算が必要である。$k = (-1)^{r+1} q_{r-2} + k'$ と置いてみ

る。すると

$$x = k'q_r + 1, \quad y = k'p_r + c$$

となる。$k' \geq 1$ とする。c が偶数の場合は、y を偶数とする k' は必ず存在する。他方 c が奇数の場合には、p_r が偶数であれば、y は偶数にはならない。p_r が奇数であれば、y を偶数に選ぶことが可能である。

いくつかの c と r について、最小の m を次の表に載せる。

c	$r=2$	$r=3$	$r=4$	$r=5$	$r=6$
1	None	7	13	None	58
2	41	55	925	1326	29041
3	None	335	3170	None	355577
4	370	1462	94394	420210	29978210
5	None	4927	124745	None	89362850

以上では (正攻法をとったために) 回りくどい計算によって、驚くほどシンプルな結果を導いた: 最小の正の (x, y) の組は $(1, c)$ である。

実はこの結果は、自明なほど簡単な論理で導き出せる。

我々が欲しいのは次の不定方程式の最小解である:

$$xp_r - yq_r = q_{r-1}$$

ここに $q_{r-1} = H(n_2, n_3, ..., n_{r-1})$ である。他方では我々は、恒等式

$$p_r = n_1 q_r + H(n_3, n_4, ..., n_r)$$

を知っている。従って

$$H(n_2, n_3, ..., n_{r-1}) = H(n_3, n_4, ..., n_r)$$

であれば、最小解 $(x, y) = (1, n_1)$ を得たことになる。特に $n_1, n_2, ..., n_r$ が全て c の場合には、この条件が成立している。これから $(x, y) = (1, c)$ が得られる。

Chapter 5

Pell 方程式

5.1 Pell 方程式とは

Pell 方程式の解を求める問題とは、平方数ではない自然数 m を与えて方程式

$$x^2 - my^2 = \pm 1 \tag{5.1}$$

を満たす非負整数 x, y を求める問題である [1]。$(x, y) = (1, 0)$ は自明な解である。

通常は式 (5.1) の右辺が $+1$ のものを Pell 方程式と呼んでいるが [2]、ここでは ± 1 とする。その方が数学的には理にかなっているからである。

この章の目標は、Pell 方程式の新しい解法を述べた幾つかの定理 (定理 2、定理 2a、定理 4) を証明することにある [3]。必要な議論の内容は、定理を除いて、ほぼ高木 [2] に沿っている。様々な予備概念も、ほぼ高木に沿っている。しかし、高木は整数論の教科書として広く議論をしているのに対して、ここでは目標を Pell 方程式の解法の理解に絞っている。従って高木に比べて、扱っている

[1]「非負整数」ではなく「整数」と言ってもよいのであるが、得られた解に "±" を付けるのが煩わしいので、このような言い方をした

[2]高木 p.317 によると、この方程式に Pell の名前が付いたのは Euler の誤解に基づいているとのこと。Fermat が既に扱っている。さらに、インドの数学者は解法も知っていたらしい

[3]定理 2 と同等な主張は Evan Dummit [20] に見出される。しかし彼は、証明が長くなるとの理由で、証明を載せていない。確かに長くなる!

範囲が狭い。証明法も単刀直入であり、余計な知識を要求しない。

式 (5.1) は

$$(x+y\sqrt{m})(x-y\sqrt{m})=\pm 1 \tag{5.2}$$

と書き換えられる。この式の右辺が -1 の解 x, y が求まれば

$$(x+y\sqrt{m})(x-y\sqrt{m})=-1$$

であるから、$+1$ の解は

$$\begin{aligned}1&=(x+y\sqrt{m})^2(x-y\sqrt{m})^2=(x^2+my^2+2xy\sqrt{m})(x^2+my^2-2xy\sqrt{m})\\&=(x^2+my^2)^2-(2xy)^2m\end{aligned} \tag{5.3}$$

とすることによって求めることができる。このように両者が関わっているので、$+1$ の場合に解を限定すると数学的には煩雑になってしまう。

方程式 (5.2) の一つの解 x, y が求まれば、$(x+y\sqrt{m})^n(x-y\sqrt{m})^n=\pm 1$ であるから、$n=2$ で行ったのと同様にして、$n>1$ の任意の n に対して新たな解を構成できる。つまり解が存在するなら、無限個の解が存在することが分かる。

Pell 方程式

$$x^2-my^2=-1 \tag{5.4}$$

の解は必ずしも存在しない。例えば $m\equiv 3 \pmod 4$ の場合には存在しない。なぜなら、$x^2\equiv 0,1 \pmod 4$ および $y^2\equiv 0,1 \pmod 4$ であるから $x^2+y^2\equiv 0,1,2 \pmod 4$ であるが、他方では式 (5.4) から、$x^2+y^2\equiv 3 \pmod 4$ であり矛盾する。同様な理由で $m\equiv 0 \pmod 4$ の場合にも存在しない。

式 (5.4) の解は、任意の m に対しては必ずしも存在しないが、存在する例としては、$m=n^2+1$ $(n=1,2,3,...)$ の場合が挙げられる。この場合には、$x=n,\ y=1$ の解を持っている。これ以外の m で、式 (5.4) の解を持つパターンは多くはない。付録 B には平方根の連分数 $(m<100)$ が載っている。後に述べる定理 2 と突き合わせると、連分数の周期が奇数のものが、式 (5.4) に対応している。例えば $m=41$ の場合には解を持つ。そのときの解は定理 2 により $(x,y)=(32,5)$ である。

5.2 基礎概念

定義: 集合 $Q(\sqrt{m})$: 集合 $\{x+y\sqrt{m};\ x,y\in Q\}$ を $Q(\sqrt{m})$ で表す。ここでは m は正で平方数ではないとする。$Q(\sqrt{m})$ は体をなす。

定義: 代数共役: $\xi=x+y\sqrt{m}\in Q(\sqrt{m})$ なる数 ξ に対して、平方根の符号を反転した $x-y\sqrt{m}$ を ξ の代数共役と言い $\overline{\xi}$ で表す[4]。

この上線の使い方は、複素共役と紛らわしいのであるが、複素共役の拡張になっている。ここでは複素数を扱わないので紛れる心配はないが、そもそも複素共役のためだけの上線は要らないのであろう。

上線はあくまで与えられた $Q(\sqrt{m})$ の元に対して定義されているのであって、任意の平方根の符号反転を行うものではない。仮に平方根の符号反転演算子だとすると $\overline{\sqrt{2\cdot 3}}\neq\overline{\sqrt{2}}\cdot\overline{\sqrt{3}}$ となるので、上線の持つ重要な性質: $\overline{\xi_1\xi_2}=\overline{\xi_1}\,\overline{\xi_2}$ が失われる。

定義: ノルム $N(\xi)$: $\xi=x+y\sqrt{m}\in Q(\sqrt{m})$ なる数 ξ に対して、$N(\xi)=\xi\overline{\xi}=x^2-my^2$ を定義する。$N(\xi)$ を ξ のノルムと言う。ノルムは負になり得る。

定義: 集合 $Z(\omega)$: ω を無理数として集合 $Z(\omega)$ を次で定義する。

$$\{x+y\omega;\ x,y\in Z\}$$

我々の目標である Pell 方程式 (5.1) との関係では、$Z(\sqrt{m})$ だけが理解されていればよいのである。それにも関わらず議論の範囲を広げたのは、第 5.5 節で、拡張 Pell 方程式 (5.6) を扱う予定だからである。

定義: 代数的整数: ここでは代数的整数を 2 次に限定する。2 次の代数的整数とは $\xi^2+b\xi+c=0\ (b,c\in Z)$ を満たす無理数である。

[4]「代数共役」の用語に関しては、第 3.3 の脚注 6 を見よ。Hardy-Wright も上線で代数共役を表している

代数的整数を次のように言い換えてもよい: ω が代数的整数であるとは $\omega^2 \in Z(\omega)$ となる無理数 ω のことである。

ξ が代数的整数であれば $\xi = \dfrac{-b \pm \sqrt{D}}{2}$, $D = b^2 - 4c$ で表される。逆に $\xi = \dfrac{-b \pm \sqrt{m}}{2}$ で表される数はどのようなときに代数的整数となるか?

例 1. (a) $\omega = \dfrac{1+\sqrt{3}}{2}$ は代数的整数ではない。なぜなら $2\omega^2 - 2\omega - 1 = 0$ だから。(b) $\omega = \dfrac{1+\sqrt{5}}{2}$ は代数的整数である。なぜなら $\omega^2 - \omega - 1 = 0$ だから。

$\omega = \dfrac{1+\sqrt{m}}{2}$ より $4\omega^2 - 4\omega - (m-1) = 0$ を得る。従って ω が代数的整数となる必要十分条件は $m \equiv 1 \pmod 4$ である。

補題 1. ω が代数的整数ならば $Z(\omega)$ は環をなす。

証明: 加減算で $Z(\omega)$ が閉じていることは明らかである。乗法で閉じていることは次のように分かる。

$\xi_1, \xi_2 \in Z(\omega)$ とすると、$\xi_1 = x_1 + y_1\omega$, $\xi_2 = x_2 + y_2\omega$ と置ける。$\xi = \xi_1\xi_2 = x_1x_2 + y_1y_2\omega^2 + (x_1y_2 + y_1x_2)\omega$ であるが、$\omega^2 \in Z(\omega)$ であるから、補題の主張を得る。 □

補題 2. ω が代数的整数ならば $Z(\omega)$ の無理数の元もまた代数的整数である。

証明: $\rho \in Z(\omega) \Rightarrow \rho^2 \in Z(\rho)$ を示せばよい。$\omega^2 = u\omega + v$ とする。$\rho = x + y\omega$ とすると、

$$(\rho - x)^2 = y^2\omega^2 = y^2(u\omega + v) = uy(y\omega) + vy^2 = uy(\rho - x) + vy^2$$

であり、従って

$$\rho^2 = 2x\rho - x^2 + uy(\rho - x) + vy^2 \in Z(\rho)$$

である。 □

定義: 集合 $Z^*(\sqrt{m})$: ω を

$$\omega = \begin{cases} \sqrt{m/4} & \text{for} \quad m \equiv 0 \pmod 4 \\ \dfrac{1+\sqrt{m}}{2} & \text{for} \quad m \equiv 1 \pmod 4 \\ \sqrt{m} & \text{for} \quad m \equiv 2,3 \pmod 4 \end{cases} \tag{5.5}$$

として $Z^*(\sqrt{m}) = Z(\omega)$ で定義する [5]。

すると (a) ω は代数的整数である。(b) $Z^*(\sqrt{m})$ は環をなし、その元は代数的整数である。また (c) $\xi \in Z^*(\sqrt{m})$ であれば $\overline{\xi} \in Z^*(\sqrt{m})$ である。

証明: (a) と (b) は既に証明済み。(c) は $m \not\equiv 1 \pmod 4$ の場合には自明。$m \equiv 1 \pmod 4$ の場合には $\overline{\omega} = -\omega + 1$ の関係より得る。 □

補注: この定義によると $Z(\sqrt{m}) \subset Z^*(\sqrt{m})$ である。

定義: 単数: ϵ が $Z^*(\sqrt{m})$ の単数とは $\epsilon\overline{\epsilon} = \pm 1$ となる $Z^*(\sqrt{m})$ の元である。ε が $Z(\sqrt{m})$ の単数とは $\varepsilon\overline{\varepsilon} = \pm 1$ となる $Z(\sqrt{m})$ の元である。± 1 は自明な単数である。

注意: 単数の本来の意味 (定義) は 1 の約数である代数的整数のことである。これは結局、ここで定義したことと同じ。

定義: 単数の集合 $U(\sqrt{m})$ と $U^*(\sqrt{m})$: $U(\sqrt{m})$ と $U^*(\sqrt{m})$ で各々 $Z(\sqrt{m})$ と $Z^*(\sqrt{m})$ の単数の集合を表すことする。

$Z(\sqrt{m}) \subset Z^*(\sqrt{m})$ であるから、$U(\sqrt{m}) \subset U^*(\sqrt{m})$ である。

補題 3. $U(\sqrt{m})$ および $U^*(\sqrt{m})$ は群をなす。これらの群の単位元は 1 である。

証明: いずれも環をなすことから、乗法に関して閉じていることは既に証明されている。従って逆元のみを問題にすればよい。

式 (5.5) の ω を使って $\xi \in Z(\omega)$ とする。単数条件から $\xi\overline{\xi} = e = \pm 1$ である。従って $\xi^{-1} = e\overline{\xi} \in Z(\omega)$ である。 □

[5] 高木も Hardy-Wright も $m \equiv 0 \pmod 4$ のケースを扱わない。そもそも m は平方因子を含まないとしているのである。そのような条件付はイデアルを論じるときには必要になる。しかし、我々の目的には困るので全てのケースを含むようにした

正の単数 $Z(\sqrt{m})$ の正の単数は乗法に関して群をなす。$\varepsilon = x + y\sqrt{m}\ (x, y > 0)$ とすると $\varepsilon^{-1} = |x - y\sqrt{m}|$ である。$x+y\sqrt{m}$ を正の単数として $x+y\sqrt{m} > 1$ なら $x, y > 0$、$x + y\sqrt{m} < 1$ なら x, y は異符号である。$Z^*(\sqrt{m})$ の正の単数についても同様である。

$Z(\sqrt{m})$ の単数は Pell 方程式 (5.1) の解でもある。不定方程式

$$x^2 - my^2 = \pm 4 \tag{5.6}$$

を拡張 Pell 方程式と言おう。この解を x, y とすると $\theta = (x + y\sqrt{m})/2$ は $\theta\overline{\theta} = \pm 1$ を満たし、また代数的整数である。

補題 4. 拡張 Pell 方程式の解を x, y とすると $(x + y\sqrt{m})/2 \in Z^*(\sqrt{m})$ である。

証明: $m \equiv 0 \pmod 4$ の場合: $m = 4m'$ として、式 (5.6) は $x^2 - 4m'y^2 = \pm 4$ となる。従って x は偶数であり、$x = 2x'$ とする。すると方程式は $x'^2 - m'y^2 = \pm 1$ となり、

$$(x + y\sqrt{m})/2 = x' + y\sqrt{m'} \in Z(\sqrt{m'}) = Z^*(\sqrt{m})$$

$m \equiv 1 \pmod 4$ の場合: $\dfrac{x + y\sqrt{m}}{2} = x' + y' \cdot \dfrac{1 + \sqrt{m}}{2}$ と置くと $x = 2x' + y',\ y = y'$ を得るが、$x^2 \equiv y^2 \pmod 4$ なので x, y は共に偶数あるいは共に奇数である。従って $2x' = x - y$ から定まる x' は整数である。y' も整数であるから $\dfrac{x + y\sqrt{m}}{2} \in Z^*(\sqrt{m})$ である。

$m \equiv 2, 3 \pmod 4$ の場合: $x^2 \equiv my^2 \pmod 4$ なので x, y は共に偶数である。そこで $x = 2x',\ y = 2y'$ と置くと、

$$\frac{x + y\sqrt{m}}{2} = x' + y'\sqrt{m} \in Z(\sqrt{m}) = Z^*(\sqrt{m})$$

となる。以上より全ての場合において補題の主張が証明された。 □

目標式 (5.1) との関係で、この節では、単数の範囲を $Z(\sqrt{m})$ の単数に限定することがある。このことは $m \not\equiv 0 \pmod 4$ の場合に $Z(\sqrt{m})$ の単数を考察から外すことを意味しない。

$N(\xi) = \pm 1$ は $x^2 - my^2 = \pm 1$ であるから、Pell 方程式 (5.1) を解く問題は、自明でない $Z(\sqrt{m})$ の単数を求める問題に置き換えられる。拡張 Pell 方程式 (5.6) を解く問題の場合も $Z^*(\sqrt{m})$ の単数を求める問題に置き換えられる。

例 2. $3+\sqrt{8}$ は $Z(\sqrt{8})$ の単数である。$1/(3+\sqrt{8}) = 3-\sqrt{8}$ で、これもまた $Z(\sqrt{8})$ の単数である。これらのノルムは 1 である。$(x,y) = (3,1)$ は Pell 方程式 $x^2 - 8y^2 = 1$ の解である。

例 3. $2+\sqrt{5}$ は $Z(\sqrt{5})$ の単数である。$1/(2+\sqrt{5}) = \sqrt{5}-2$ で、これもまた $Z(\sqrt{5})$ の単数である。これらのノルムは -1 である。$(x,y) = (2,1)$ は Pell 方程式 $x^2 - 5y^2 = -1$ の解である。

例 4. $\epsilon = (1+\sqrt{5})/2$ は $\epsilon\bar{\epsilon} = -1$ を満たし、$Z^*(\sqrt{5})$ の単数である。$\epsilon_2 = \epsilon^2 = (3+\sqrt{5})/2$ は $\epsilon_2\bar{\epsilon}_2 = 1$ を満たし、$Z^*(\sqrt{5})$ の単数である。右辺の符号が $+$ になったのは当然である。$\epsilon_3 = \epsilon^3 = 2+\sqrt{5}$ は $\epsilon_3\bar{\epsilon}_3 = -1$ を満たし、$Z^*(\sqrt{5})$ の単数であるばかりか、$Z(\sqrt{5})$ の単数でもある。$Z(\sqrt{5})$ の単数になったのは偶然ではない。

例 5. $\theta = (1+\sqrt{10})/3$ は $N(\theta) = -1$ ではあるが、単数ではない。なぜなら $3\theta^2 - 2\theta - 3 = 0$ で、代数的整数の要件を満たさない。

定義: 2 次の無理数の原始 2 次式と判別式: ξ は $a\xi^2 + b\xi + c = 0$ の根とする。a, b, c の最大公約数は除去できるので $\gcd(a,b,c) = 1$ として構わない。その時の 2 次式を ξ の原始 2 次式と言う。ここでは $a > 0$ としておく [6]。ξ の原始 2 次式の $D = b^2 - 4ac$ を ξ の判別式と言う [7]。

D が偶数であれば、b も偶数である。従って $D \equiv 0 \pmod 4$ となる。D が奇数であれば b も奇数であり、従って $D \equiv 1 \pmod 4$ となる。次の補題から判別式の重要性が理解できる。

補題 5. X を 2 次の無理数の集合とする。$\xi \in X$ に対する変換 (a),(b) を

(a) $\xi \quad \longrightarrow \quad \xi' = \xi - n \quad (n \in Z)$

(b) $\xi \quad \longrightarrow \quad \xi' = 1/\xi$

として定義する。ξ が満たす 2 次式 $a\xi^2 + b\xi + c = 0$ が $a'\xi'^2 + b'\xi' + c' = 0$ に変換されるとすると

(1) $\gcd(a,b,c) = \gcd(a',b',c')$

[6] 高木 p.197. 高木は $a > 0$ の条件を付けていない。他方 Hardy-Wright は $a > 0$ の条件を付けている (p.205)。ここでは Hardy-Wright の定義を採用する

[7] 高木 p.196

(2) $b^2 - 4ac = b'^2 - 4a'c'$

(3) $b \equiv b' \pmod 2$

証明: この補題の主張は、変換 (b) に対しては自明である。そこで変換 (a) のみを吟味する。

$$\begin{aligned} a\xi^2 + b\xi + c &= a(\xi' + n)^2 + b(\xi' + n) + c \\ &= a\xi'^2 + (2an + b)\xi' + (an^2 + bn + c) \end{aligned}$$

従って $a' = a,\ b' = 2an + b,\ c' = an^2 + bn + c$ となる。これから

$$b \equiv b' \pmod 2$$

を得る。また最大公約数の計算規則を使えば

$$\begin{aligned} \gcd(a', b', c') &= \gcd(a, 2an + b, an^2 + bn + c) = \gcd(a, b, an^2 + bn + c) \\ &= \gcd(a, b, c) = 1 \end{aligned}$$

となる。ξ の判別式を D、ξ' の判別式を D' とすると、

$$D' = (2an + b)^2 - 4a(an^2 + bn + c) = b^2 - 4ac = D$$

となる。 □

注意: この補題において (3) は蛇足である。なぜなら b の偶奇は判別式の偶奇に一致するからである。

補注: 連分数の計算は、変換 (a)、(b) の繰り返しである。そこで生成される無理数は、(1)、(2)、(3) の性質を保っているのである。特に、$\sqrt{m}$ の判別式は $D = 4m$ である。従って $\sqrt{m}$ の連分数の計算の途中で生成される無理数の判別式はすべて $4m$ である。

$m = 4n + 1\ (n \in N)$ として $\xi = (\sqrt{m} + 1)/2$ の連分数の計算を考えよう。ξ の原始 2 次式は $\xi^2 - \xi - n = 0$ であり、ξ の判別式は m である。ξ の原始 2 次式から生成される 2 次式 $a'\xi'^2 + b'\xi' + c' = 0$ は $\gcd(a', b', c') = 1$ を保つ。判別式は m を保ち、また b' は奇数を保つ。従って ξ' を $(\sqrt{m} + b)/a$ として表すと、$b\ (= b')$ は奇数、$a\ (= 2a')$ は偶数である。

定義: モジュラー変形: 実数 ω の変形 $\omega' = (r\omega+s)/(t\omega+u)$ を ω のモジュラー変形と言う。ここに r, s, t, u は整数で、$ru-st = \pm 1$ とする。以下、$e = ru-st$ とする [8]。

条件 $ru - st = e$ は行列式を使って $\begin{vmatrix} r & s \\ t & u \end{vmatrix} = e$ とも表現できる。従って、モジュラー変形 $(r\omega + s)/(t\omega + u)$ に行列 $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ を対応させるのは魅力的なアイデアである。このアイデアを検討してみよう。

モジュラー変形 $\omega' = (r\omega + s)/(t\omega + u)$ とモジュラー変形 $\omega' = (-r\omega - s)/(-t\omega-u)$ は同一の変形である。従って $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ と、符号を反転した $\begin{pmatrix} -r & -s \\ -t & -u \end{pmatrix}$ は同一のモジュラー変形を表していると考える必要がある。

モジュラー変形を繰り返すと、またモジュラー変形になる。すなわち

$$\omega' = (r\omega + s)/(t\omega + u), \quad \omega'' = (r'\omega' + s')/(t'\omega' + u')$$

とすると

$$\omega'' = ((r'r + s't)\omega + r's + s'u)/((t'r + u't)\omega + t's + u'u)$$

となる。つまり、モジュラー変形を繰り返して得られた結果は、対応する行列の積に一致している:

$$\begin{pmatrix} r'r + s't & r's + s'u \\ t'r + u't & t's + u'u \end{pmatrix} = \begin{pmatrix} r' & s' \\ t' & u' \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

従って

$$\begin{vmatrix} r'r + s't & r's + s'u \\ t'r + u't & t's + u'u \end{vmatrix} = \begin{vmatrix} r' & s' \\ t' & u' \end{vmatrix} \begin{vmatrix} r & s \\ t & u \end{vmatrix} = e'e$$

である。つまり、モジュラー変形を繰り返して得られる変形はモジュラー変形であることが容易に分かる。

恒等変形は $\omega' = (1\omega + 0)/(0\omega + 1)$ あるいは $\omega' = (-1\omega + 0)/(0\omega - 1)$ であり、これらは行列 $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ に対応している。つまり、符号の違いに関わらず、共に単位行列と見なす必要がある。

[8] 高木 p.173. の定義に従う

符号が定まらないことは、逆変形によく現れている。$\omega' = (r\omega + s)/(t\omega + u)$ の逆変形は逆写像 $\omega = (-u\omega' + s)/(t\omega' - r)$ あるいは $\omega = (u\omega' - s)/(-t\omega' + r)$ であり、これの行列表現は、それぞれ $\begin{pmatrix} -u & s \\ t & -r \end{pmatrix}$ と $\begin{pmatrix} u & -s \\ -t & r \end{pmatrix}$ である。つまり、この 2 つは同じモジュラー変形を表している。他方では

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}^{-1} = e \begin{pmatrix} u & -s \\ -t & r \end{pmatrix}$$

であるが、e の符号に関わらず同一の逆変形を表していると見なす必要がある。

注意: それでもモジュラー変形は ω に対して一意には定まらない。例えば $\omega = \sqrt{2},\ \omega' = \sqrt{2} + 1$ とすると $(r, s, t, u) = (1, 1, 0, 1)$ であるが、他方 $(r, s, t, u) = (0, 1, 1, -1)$ も可能である。e の値は、前者は 1 で、後者は -1 である [9]。この例は $(\sqrt{2}+1)/1 = 1/(\sqrt{2}-1)$ から来ている。同様な例、あるいはもっと複雑な例も、いくらでも作れるだろう。

定義: 変形行列: 写像 $(r\omega + s)/(t\omega + u)$ に対応する行列 $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ を ω の変形行列と言うことにしよう。

例 6. $\eta = \theta - n$ の変形行列は $\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ である。これを図式的に

$$\eta \xleftarrow{\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}} \theta$$

と書こう。$\theta' = 1/\eta$ は

$$\theta' \xleftarrow{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}} \eta$$

である。矢印を左向きにしたのは、行列演算と関係がある。この 2 つの合成操作は

$$\theta' \xleftarrow{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}} \theta$$

[9] 高木 p.176

で、これは

$$\theta' \xleftarrow{\begin{pmatrix} 0 & 1 \\ 1 & -n \end{pmatrix}} \theta$$

に等しい。θ から θ' への変換は

$$\begin{pmatrix} 0 & 1 \\ 1 & -n \end{pmatrix}^{-1} = \begin{pmatrix} n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

で、これは $\theta = [n, \theta']$ に相当する。

θ を連分数に展開すると $\theta = [n_1, n_2, n_3, ...]$ であるから $\theta' = [n_2, n_3, ...]$ と置くと $\theta = [n_1, \theta']$ である。つまり、θ' は θ の連分数の計算において、最初に現れる数である。

補題 6. $\omega' = [n_1, n_2, ..., n_l, \omega]$ とする。すると $[n_1, n_2, ..., n_l, \omega]$ は ω のモジュラー変形である。この変形行列を M とすると $|M| = (-1)^l$ となる。

証明: $l = 1$ の場合には $\omega' = [n_1, \omega] = n_1 + 1/\omega = (n_1\omega + 1)/\omega$ 故 $[n_1, \omega]$ はモジュラー変形であり、変形行列は $\begin{pmatrix} n_1 & 1 \\ 1 & 0 \end{pmatrix}$ となる。

$l \geq 2$ の場合には、付録 C の定理 6 より、自然数 r, s, t, u を

$$r/t = [n_1, n_2, ..., n_l], \quad s/u = [n_1, n_2, ..., n_{l-1}]$$

で定義する。ここに $r/t,\ s/u$ は (分母が正の) 既約分数とする。すると、

$$[n_1, n_2, ..., n_l, \omega] = \frac{s + r\omega}{u + t\omega}$$

であるから、変形行列は $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ となる。なお付録 C の定理 5 より $\begin{vmatrix} r & s \\ t & u \end{vmatrix} = (-1)^l$ である。 □

この補題は、モジュラー変形と連分数との関係に注意を促すために添えた。補題を証明するだけであれば、もっと簡単にやれる。

例 7. モジュラー変形を $\omega' = [2, 3, 5, \omega]$ とする。付録 C の定理 6 を使うと効率

よく変形行列を計算できる:

$$[2] = \frac{2}{1}, \quad [2,3] = 2 + \frac{1}{3} = \frac{7}{3}, \quad [2,3,5] = \frac{2 + 7 \cdot 5}{1 + 3 \cdot 5} = \frac{37}{16}$$

$$[2,3,5,\omega] = \frac{7 + 37\omega}{3 + 16\omega}$$

従って変形行列は $\begin{pmatrix} 37 & 7 \\ 16 & 3 \end{pmatrix}$ である。故に $\omega' = (37\omega + 7)/(16\omega + 3)$ となる。なお $\begin{vmatrix} 37 & 7 \\ 16 & 3 \end{vmatrix} = -1$ となる。符号は $l = 3$ に対応している。

定義: 自己変形: θ を 2 次無理数とする。$\theta = (r\theta + s)/(t\theta + u)$ でかつ $ru - st = \pm 1$ となる (r, s, t, u) の組を θ の自己変形という。つまり自己変形とは自分自身に変形するモジュラー変形である。その場合には θ は必然的に 2 次無理数となる。$(r, s, t, u) = (1, 0, 0, 1)$ は自明な自己変形である。我々は自明でない自己変形に関心がある。

補題 7. 2 次無理数 θ の自己変形

$$\theta = \frac{r\theta + s}{t\theta + u}, \quad ru - st = e = \pm 1 \tag{1}$$

を基に $p^2 - Dq^2 = 4e$ の解が求まる。ここに D は θ の判別式である。

証明: 求め方を示す。式 (1) より

$$t\theta^2 + (u - r)\theta - s = 0 \tag{2}$$

である。θ が 2 次無理数であるから、$ts \neq 0$ である。$q = \gcd(t, u - r, s)$ として $a = t/q,\ b = (u - r)/q,\ c = -s/q$ と置くと

$$a\theta^2 + b\theta + c = 0 \quad (ac \neq 0,\ \gcd(a, b, c) = 1) \tag{3}$$

となる。式 (3) から θ の判別式 $D = b^2 - 4ac$ が得られる。ここで $p = u + r$ と置くと、$2u = p + bq,\ 2r = p - bq$ である。従って、纏めると

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} (p - bq)/2 & -cq \\ aq & (p + bq)/2 \end{pmatrix} \tag{4}$$

である。従って

$$ru - st = (p^2 - b^2q^2)/4 + acq^2 = (p^2 - Dq^2)/4 \tag{5}$$

となる。故に $p^2 - Dq^2 = 4e$ である。 □

補注: $D = 4m$ の場合には、p は偶数となる。従って $p = 2p'$ と置いてよい。その場合には $Z(\sqrt{m})$ の単数 $p'^2 - mq^2 = e$ が求まっている。

例 8. $\theta = \dfrac{5\theta + 3}{3\theta + 2}$ とすると、$p = 5 + 2 = 7$ である。また $3\theta^2 - 3\theta - 3 = 0$ から $q = 3$ および $\theta^2 - \theta - 1 = 0$ を得て $D = 5$ である。確かに $p^2 - 5q^2 = 7^2 - 5 \cdot 3^2 = 4$ である。

自己変形はモジュラー変形と同様に行列で表現できる。もちろん、モジュラー変形と同じ注意が要求される。

補題 8. 自己変形

$$\theta = (r\theta + s)/(t\theta + u), \quad e = ur - st = \pm 1$$

の分母 $\rho = t\theta + u$ は $Z^*(\sqrt{D})$ の単数である。ここに D は θ の判別式である [10]。

証明: 補題 7 の式 (4) より

$$\rho = t\theta + u = aq\theta + \frac{p + bq}{2}$$

他方、補題 7 の式 (3) より $a\theta = \dfrac{-b + \sqrt{D}}{2}$ であるから

$$\rho = \frac{q(-b + \sqrt{D})}{2} + \frac{p + bq}{2} = \frac{p + q\sqrt{D}}{2}$$

また補題 7 の式 (5) より

$$\rho\overline{\rho} = \frac{p^2 - Dq^2}{4} = e$$

となり、ρ は $Z^*(\sqrt{D})$ の単数の条件を満たす (補題 4)。 □

補注: $D = 4m$ の場合には、p は偶数となる。従って $p = 2p'$ と置いてよい。その場合には $Z(\sqrt{m})$ の単数 $p'^2 - mq^2 = e$ が求まっている。

例 9. 自己変形を $\dfrac{4\theta + 3}{3\theta + 2}$ とする。$e = -1$ である。また自己変形の分母は $\rho = 3\theta + 2$ である。$3\theta^2 - 2\theta - 3 = 0$ より $D = 40$ および $\theta = \dfrac{2 + \sqrt{40}}{3 \cdot 2} = \dfrac{1 + \sqrt{10}}{3}$ を得る。これから $Z(\sqrt{10})$ の単数 $\rho = 3\theta + 2 = 3 + \sqrt{10}$ が得られた。

[10] 高木 p.212 の「問題 1」に相当する。この補題は自己変形と単数を結びつける基本的な命題である

自己変形から 2 次の無理数と、(その判別式を D として) $Z^*(\sqrt{D})$ の単数が得られるが、逆に、次の補題に示すように、判別式が D の 2 次の無理数と $Z^*(\sqrt{D})$ の単数から自己変形が得られる。

補題 9. θ を 2 次の無理数とし, 整数 a, b, c によって

$$a\theta^2 + b\theta + c = 0 \quad (a \neq 0) \tag{1}$$

と表されるとする。θ の判別式を

$$D = b^2 - 4ac \tag{2}$$

とする。そして整数 p, q は

$$p^2 - Dq^2 = 4e \quad (e = \pm 1, q \neq 0) \tag{3}$$

を満たすとする。すると、

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} (p - bq)/2 & -cq \\ aq & (p + bq)/2 \end{pmatrix} \tag{4}$$

で r, s, t, u を定義すると、θ は

$$\theta = \frac{r\theta + s}{t\theta + u} \tag{5}$$

を満たし、この式は θ の自己変形である。

証明: 式 (4) と (3) より

$$ru - st = (p^2 - b^2q^2)/4 + acq^2 = (p^2 - Dq^2)/4 = e \tag{6}$$

である。また式 (4) と式 (1) より

$$\theta(t\theta + u) - (r\theta + s) = t\theta^2 + (u - r)\theta - s = q(a\theta^2 + b\theta + c) = 0 \tag{7}$$

を得る。ところが $a \neq 0,\ q \neq 0$ であるから $t \neq 0$ であり、また θ は無理数なので $t\theta + u$ は 0 にはなり得ない。従って

$$\theta = \frac{r\theta + s}{t\theta + u} \tag{8}$$

である。r と u が整数になることは次のように示される。

式 (2) より $D \equiv b^2 \pmod 4$ であるから、式 (3) より $p^2 \equiv (bq)^2 \pmod 4$ を得る。従って p と bq は共に偶数、あるいは共に奇数であり、r, u は整数となる。 □

すなわち、自己変形と単数は与えられた θ の下に 1 対 1 に対応しているの

である。

補注: 補題の式 (1) において、b が偶数の場合は次のようになる。式 (1) に代わって

$$a\theta^2 + 2b\theta + c = 0 \quad (a \neq 0) \tag{1'}$$

式 (2) に代わって

$$D = 4m,\ m = b^2 - ac \tag{2'}$$

式 (3) に代わって

$$p^2 - mq^2 = e \quad (e = \pm 1, q \neq 0) \tag{3'}$$

式 (4) に代わって

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} p - bq & -cq \\ aq & p + bq \end{pmatrix} \tag{4'}$$

式 (5) はそのままである。

例 10. 単数を $\varepsilon = 3 + \sqrt{8}$ とする。$(p, q) = (3, 1)$ である。$\theta = \sqrt{8}$ とすれば $\theta^2 - 8 = 0$ 故、補注を使うのが楽である。$(a, b, c) = (1, 0, -8)$ となる。$p - bq = 3,\ p + bq = 3, aq = 1, cq = -8$ であるから $\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix}$ である。

他方 $\theta = \sqrt{8} - 2$ とすれば、θ は $\theta^2 + 4\theta - 4 = 0$ を満たし、補注のケースである。同様にやっていけるが、他の方法をとろう。$\theta + 5 = 3 + \sqrt{8}$ が単数なので、

$$\theta(\theta + 5) = \theta^2 + 5\theta = -4\theta + 4 + 5\theta = \theta + 4$$

従って $\theta = (\theta + 4)/(\theta + 5)$ が θ の自己変形である。この方法は θ が代数的整数の場合に使える。

θ を与えたとしても自己変形は一意には決まらない。実際 $\theta = \sqrt{8}$ を例にとると、単数 $3+\sqrt{8}$ を基にして、次のように自己変形を作ることができる: $(3+\sqrt{8})^2 = 17 + 6\sqrt{8},\ (17 + 6\sqrt{8})\sqrt{8} = 17\sqrt{8} + 48$ より $\theta = (17\sqrt{8} + 48)/(6\sqrt{8} + 17)$ もまた $\theta = \sqrt{8}$ の自己変形である。

ここで自己変形のなす群と単数のなす群との乗算における対応関係を確認する。

補題 10. $(r\theta+s)/(t\theta+u)$ と $(r'\theta+s')/(t'\theta+u')$ が共に θ の自己変形とする。すると 2 つの自己変形を繰り返すと

$$\begin{pmatrix} r & s \\ t & u \end{pmatrix}\begin{pmatrix} r' & s' \\ t' & u' \end{pmatrix}=\begin{pmatrix} rr'+st' & rs'+su' \\ tr'+ut' & ts'+uu' \end{pmatrix}$$

となるが、生成された自己変形の分母 $(tr'+ut')\theta+(ts'+uu')$ は、基になった自己変形の分母 $t\theta+s$ と $t'\theta+s'$ の積に等しい。

証明: 行列の積が自己変形であることは明らか。そこで $(tr'+ut')\theta+(ts'+uu')=(t\theta+s)(t'\theta+s')$ を示す。2 つの自己変形の分母の積は

$$(t\theta+s)(t'\theta+s')=tt'\theta^2+(ut'+tu')\theta+uu'$$

であるが、ここで $t'\theta^2=(r'-u')\theta+s'$ を利用する。すると

$$\begin{aligned} tt'\theta^2+(ut'+tu')\theta+uu' &= t((r'-u')\theta+s')+(ut'+tu')\theta+uu' \\ &= (tr'+ut')\theta+ts'+uu' \end{aligned}$$

で求める結果を得る。 □

定義: 簡約 2 次無理数: 2 次無理数 θ が不等式 $\theta>1,\ 0>\overline{\theta}>-1$ を満たすとき、θ を簡約 2 次無理数と言う [11]。

定義: 純循環: 純循環とは、循環が最初の部分商から始まるのを言う [12]。連分数の表記では $\theta=[n_1,n_2,...,n_l,\theta]$ の形になる。

注釈: 簡約 2 次無理数は既に第 2 章で集合 T^+ の要素として扱われて、純循環することが証明されている。

補題 11. θ は簡約 2 次無理数とする。$\xi=\dfrac{1}{\theta-[\theta]}$ とすれば ξ も簡約 2 次無理数である。

証明: 証明を分かりやすくするために $\theta^*=-\overline{\theta},\ \xi^*=-\overline{\xi}$ とする。すると条件 $\theta>1$ と $0<\theta^*<1$ の下に $\xi>1$ と $0<\xi^*<1$ を示せばよい。

[11] 河田 p.112。高木は丁寧に「簡約された二次無理数」と言う (p.200)
[12] 高木 p.205

$n = [\theta] \geq 1$ とする。$\xi = 1/(\theta - n) > 1$ は明らか。$0 < \theta^* < 1$ であるから、$n < \theta^* + n < n + 1$ より $\dfrac{1}{n} > \dfrac{1}{\theta^* + n} > \dfrac{1}{n+1}$ である。ところが $\dfrac{1}{\xi^*} = \theta^* + n$ であるから $\dfrac{1}{n} > \xi^* > \dfrac{1}{n+1}$ である。故に $0 < \xi^* < 1$ が成り立つ。 □

補題 12. θ は簡約 2 次無理数とする。

$$\theta = [n_1, n_2, ..., n_{l-1}, n_l, \theta] = [\overline{n_1, n_2, ..., n_{l-1}, n_l}] \tag{1}$$

とすれば $\eta = -1/\overline{\theta}$ に対して

$$\eta = [n_l, n_{l-1}, ..., n_2, n_1, \eta] = [\overline{n_l, n_{l-1}, ..., n_2, n_1}] \tag{2}$$

となる。

証明: $n_1, n_2, ..., n_l$ は

$$\theta_1 = \theta, \quad n_k = [\theta_k], \quad \frac{1}{\theta_{k+1}} = \theta_k - n_k \quad (k = 1, 2, ..., l-1, l) \tag{3}$$

によって再帰的に決まる自然数列である。ここに $\theta_{l+1} = \theta_1$ とする。$\theta_k^* = -\overline{\theta}_k$ と置くと、この下で $\theta_k > 1,\ 0 < \theta_k^* < 1\ (k = 1, 2, ...)$ が成り立つ (補題 11)。従って $\eta_k = 1/\theta_k^*$ と置けば $\eta_k > 1,\ 0 < \eta_k^* < 1\ (k = 1, 2, ...)$ が成り立つ。ここに $\eta_k^* = -\overline{\eta}_k$ とした。そして

$$\eta_{l+1} = \eta_1 = \eta, \quad \frac{1}{\eta_k} = \eta_{k+1} - n_k \quad (k = l, l-1, ..., 2, 1)$$

となる。$\eta_k > 1\ (k = 1, 2, ...)$ 故 $0 < \eta_{k+1} - n_k < 1$ である。従って $[\eta_{k+1}] = n_k$ が成り立つ。故に

$$\eta = [n_l, n_{l-1}, ..., n_2, n_1, \eta]$$

となる。 □

次の定理は既に第 2 章の定理 2 で証明されているが、別証を載せる。

定理 1. $\omega = \sqrt{m},\ n_0 = [\omega]$ とすると次が成立する。

(a) ω は $[n_0, \overline{n_1, n_2, ..., n_{r-1}, n_r, 2n_0}]$ の周期構造を持つ

(b) $[n_0, \overline{n_1, n_2, ..., n_{r-1}, n_r, 2n_0}) = [n_0, \overline{n_r, n_{r-1}, ..., n_2, n_1, 2n_0}]$

(c) $n_k \leq n_0 \quad (k = 1, 2, ..., r)$

証明: $\omega = \sqrt{m}$ とする。すると $\omega > 1,\ \omega + \overline{\omega} = 0$ である。$n_0 = [\omega]$ とすると

$n_0 \geq 1$ である。そこで $\theta_1 = \dfrac{1}{\omega - n_0}$ と置くと、$\theta_1 > 1$ である。また

$$-\frac{1}{\overline{\theta}_1} = n_0 - \overline{\omega} = n_0 + \omega > 1$$

であるから $-1 < -\overline{\theta}_1 < 0$ となり、θ_1 は簡約無理数である。従って $\eta_1 = -1/\overline{\theta}_1$ とすると補題 12 によって

$$\omega = [n_0, \theta] \tag{1}$$

$$\theta_1 = [n_1, n_2, ..., n_{l-1}, n_l, \theta_1] \tag{2}$$

$$\eta_1 = [n_l, n_{l-1}, ..., n_2, n_1, \eta_1] \tag{3}$$

が成り立つ。また

$$\frac{1}{\theta_1} = \omega - n_0, \quad \eta_1 = -\overline{\omega} + n_0$$

である。これと $\omega + \overline{\omega} = 0$ より

$$\frac{1}{\theta_1} - \eta_1 = -2n_0$$

故に

$$\eta_1 = 2n_0 + \frac{1}{\theta_1} = [2n_0, \theta_1]$$

である。これと式 (3) を比較して $2n_0 = n_l$ および

$$\begin{aligned} \theta_1 &= [n_{l-1}, ..., n_2, n_1, \eta_1] = [n_{l-1}, ..., n_2, n_1, [2n_0, \theta_1]] \\ &= [n_{l-1}, ..., n_2, n_1, 2n_0, \theta_1] \end{aligned} \tag{4}$$

を得る。これを式 (2) と比較して $(n_{l-1}, ..., n_2, n_1) = (n_1, n_2, ..., n_{l-1})$ を得る。最後に式 (2) と式 (4) より ($r = l - 1$ と置いて) 定理の (a) と (b) の主張を得る。

(c) の証明: $\theta_k = \dfrac{\sqrt{m} + b_k}{a_k}$ とすると

$$\frac{\sqrt{m} + b_k}{a_k} - n_k = \frac{\sqrt{m} - b_{k+1}}{a_k} \quad (k = 1, 2, ..., r)$$

である。従って $b_k + b_{k+1} = n_k a_k$ である。他方、b_k $(k = 1, 2, ..., r)$ はどれも $0 < b_k < \sqrt{m}$ すなわち $0 < b_k \leq n$ を満たす。ここに $n_0 = [\sqrt{m}]$ である。従って $b_k + b_{k+1} \leq 2n_0$ である。$a_k \geq 2$ の場合には $n_k a_k \leq 2n_0$ より $n_k \leq n_0$ を得る。他方 $a_k = 1$ の場合には n_k を $b_{k+1} = n_0$ となるように選ぶことができる。つまり $\sqrt{m} - n_0$ が生成され、ここで循環する ($\theta_1 = 1/(\sqrt{m} - n_0)$ に戻る)。 □

5.3 Pell 方程式と連分数

Pell 方程式は連分数と深く関わっている。そのことを以下で示そう。

$\theta = \sqrt{m}$ とし、式

$$\theta_k = \frac{1}{\theta_{k-1} - [\theta_{k-1}]} \qquad (k = 1, 2, ...)$$

に基いて θ_k を再帰的に求める。但し $\theta_0 = \theta$ とする。

$\sqrt{m}$ の連分数を

$$\sqrt{m} = [n_0, \overline{n_1, n_2, ..., n_l}]$$

とする。ここに $n_k = [\theta_k]$ である。

その連分数が $k = l+1$ で循環し $k = 1$ に戻るとせよ。すなわち、$\theta_{l+1} = \theta_1$ とする。すると $\theta_1 = [n_1, n_2, ..., n_l, \theta_1]$ であり、θ_1 の自己変形を表している。従って $\theta_1 = (r\theta_1 + s)/(t\theta_1 + u),\ ru - st = (-1)^l$ となる r, s, t, u が存在する (補題 6)。

ここで $\eta = \sqrt{m} - n$ と置くと $\theta_1 = 1/\eta$ である。そして θ_1 の自己変形から η の自己変形 $\eta = (u\eta + t)/(s\eta + r)$ が得られる。補題 8 より $s\eta + r$ は単数であり、$N(s\eta + r) = ru - st$ である。これより

$$\begin{aligned} N(r + s\eta) &= (r + s\eta)(r + s\overline{\eta}) = r^2 + sr(\eta + \overline{\eta}) + s^2\eta\overline{\eta} \\ &= r^2 - 2nsr - s^2(m - n^2) = (r - sn)^2 - ms^2 = (-1)^l \end{aligned} \qquad (5.7)$$

が得られる。従って $x = ns - r,\ y = s$ が Pell 方程式の解である [13]。

注釈 1 ここで得られた主張の意義は、平方数でない任意の自然数 m に対して、Pell 方程式の自明でない解が存在すること、従って $Z(\sqrt{m})$ に ± 1 でない単数が存在すること、従ってまた $Z(\sqrt{m})$ の任意の元に対して、自明でない自己変形が存在することが示されたことにある。解の構成法が示されているが、以下に示す定理 2 の方が扱いやすい。

ここで、Pell 方程式の解が得られるまでの議論の流れを俯瞰しよう。

連分数 $\iff$ 自己変形 $\iff$ 単数 $\iff$ Pell 方程式

[13] 高木 p.215 に、本質的にこれと同等な証明がある

従って、この段階でも、連分数を基に Pell 方程式の解を得ることができる。以下に、その計算例を挙げる。

例 1. Pell 方程式 $x^2 - 8y^2 = \pm 1$

$m = 8,\ \sqrt{8} = [2, \overline{1, 4}],\ l = 2,\ n_0 = 2$ のケースである。
付録 C の定理 6 を使うと、次のように効率よく自己変形を計算できる。

$$[1] = 1/1, \quad [1, 4] = 5/4, \quad \theta_1 = [\overline{1, 4}] = [1, 4, \theta_1] = \frac{1 + 5\theta_1}{1 + 4\theta_1}$$

従って、変形行列は $\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 4 & 1 \end{pmatrix}$ である。従って式 (5.7) を使うと

$$x = r - ns = 5 - 2 \cdot 1 = 3, \quad y = s = 1$$

となる。

別解: 式 (5.7) の世話にならなくても次のようにやっていける。
θ_1 の自己変形 $\theta_1 = (5\theta_1 + 1)/(4\theta_1 + 1)$ より方程式 $4\theta_1^2 - 4\theta_1 - 1 = 0$ が得られる。そして自己変形の分母 $4\theta_1 + 1$ は単数である。方程式を解くと $\theta = (2 \pm \sqrt{8})/4$ 故、分母 $4\theta_1 + 1 = 3 \pm \sqrt{8}$ である。ここから直ちに Pell 方程式の解が得られる。

この計算例を見て分かるように、このままでは Pell 方程式の解を導くプロセスは些か煩雑である。しかし $\sqrt{m}$ の連分数論の成果を援用すると、次の美しい定理が得られる。

定理 2. $n = [\sqrt{m}]$ とすると $\sqrt{m} = [n, \overline{n_1, n_2, ..., n_r, 2n}]$ となる (定理 1)。そこで $p/q = [n, n_1, n_2, ..., n_r]$ とすると

$$p^2 - mq^2 = (-1)^{r+1}$$

である [14]。

証明:

$$\theta_1 = 1/(\sqrt{m} - n), \quad \theta_1 = [n_1, n_2, ..., n_r, 2n, \theta_1]$$

とすると $\theta_1 = (r\theta_1 + s)/(t\theta_1 + u),\ ru - st = (-1)^{r+1}$ と表せる (補題 6)。そ

[14] この美しい定理は、最近の文献に見つかった [20, 21]。いずれも証明は省かれているが、Dummit [20] は証明したと思える。筆者と同じ道を歩んだことが推測されるからである。なお Lahn-Spiegel [21] は単なる Dummit の紹介である

して

$$r = H(n_1, n_2, ..., n_r, 2n), \quad s = H(n_1, n_2, ..., n_r)$$

である (付録 C 定理 6)。ここで定理 1

$$(n_1, n_2, ..., n_{r-1}, n_r) = (n_r, n_{r-1}, ..., n_2, n_1)$$

と、付録 C 定理 1 を使って

$$r = H(n_1, n_2, ..., n_r, 2n) = H(2n, n_r, ..., n_2, n_1) = H(2n, n_1, n_2, ..., n_r)$$

が得られる。従って

$$\frac{r}{s} = \frac{H(2n, n_1, n_2, ..., n_r)}{H(n_1, n_2, ..., n_r)} = [2n, n_1, n_2, ..., n_r] = n + [n, n_1, n_2, ..., n_r]$$
$$= n + \frac{p}{q}$$

である。つまり $s = q$, $r = p + nq = p + ns$ である。これと、式 (5.7) より、求める結果を得る。 □

例 2. $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$ の場合 $p/q = [2, 1, 1, 1]$ を計算すればよい。

$[1, 1] = 1 + 1/1 = 2/1$, $[1, 1, 1] = 1 + 1/2 = 3/2$, $[2, 1, 1, 1] = 2 + 2/3 = 8/3$

従って $p/q = 8/3$ である。これから $p^2 - 7q^2 = 1$ が確認できる。なお Pell 方程式の右辺は、$l = r + 1 = 4$ 故 $(-1)^l = 1$ と一致している。

注釈 2 定理 2 は覚えやすく計算しやすい。Pell 方程式の解 x, y は $\sqrt{m}$ の、特に良い近似分数 x/y を表していると見ることができる。$\sqrt{m}$ の連分数は良い近似分数を与えるが、定理 2 は特に良い近似が現れる場所を示しているのである。証明においては $(n_1, n_2, ..., n_r)$ の対称性だけが仮定されており、これらが $2n$ より小さいことは使われていない。従って例えば $p/q = [2, 1]$ だけではなく、$p/q = [2, 1, 4, 1]$ も $p/q = [2, 1, 4, 1, 4, 1]$ も $m = 8$ の Pell 方程式を満たすのである。

注釈 3 先に $m \equiv 3 \pmod 4$ の場合には式 (5.4) の解が存在しないことを指摘しておいた。このことと定理 2 から、$\sqrt{m}$ の連分数の周期 $(r + 1)$ は、$m \equiv 3$

(mod 4) の場合には、奇数にはならないことが分かる。同じ理由で、$m \equiv 0 \pmod 4$ の場合にも、連分数の周期は奇数にはならない。ところで、第 4.3 節: 余題 1 では、r が偶数の場合 (つまり連分数の周期が奇数の場合)、$m = n^2 + a$ の a は $a \not\equiv 3 \pmod 4$ であることが示されている。$n^2 \equiv 0, 1 \pmod 4$ であるから、$n^2 \equiv 0 \pmod 4$ の場合には $m \not\equiv 3 \pmod 4$、$n^2 \equiv 1 \pmod 4$ の場合には $m \not\equiv 0 \pmod 4$ が得られる。つまり、連分数の周期と 4 による m の剰余との関係 (の一部) が直接的に証明されていたのである。

定理 2 によって、Pell 方程式の全ての解が得られることが定理 2a で示される。

5.4 Pell 方程式の基本解

平方数でない任意の自然数 m に対して、Pell 方程式 (5.1) の解が存在することを示した。ここで、ようやく基本単数の概念を持ち出すことができる [15]。

定義: 基本単数: ε を $1 < \varepsilon$ の条件を満たす $Z(\sqrt{m})$ の単数とする。Pell 方程式の解 (x, y) が存在するので、このような単数は $\varepsilon = x + y\sqrt{m}$ とすれば得られる。$Z(\sqrt{m})$ の元 $\varepsilon' = x' + y'\sqrt{m}$ で $\varepsilon' \leq \varepsilon$ を満たすものは少なくとも 1 つは存在し、また高々有限個しか存在しない。なぜなら x', y' は非負整数だからである。従って $1 < \varepsilon'$ の条件を満たす $Z(\sqrt{m})$ の最小の単数が存在する。この単数を $Z(\sqrt{m})$ 基本単数という。

$3+\sqrt{8}$ は $Z(\sqrt{m})$ 基本単数である。実際、正の単数で $1 < x+y\sqrt{8} < 3+\sqrt{8}$ を満たしているのは存在しない。

補題 13. ε_0 を $Z(\sqrt{m})$ の基本単数とする。このとき、$Z(\sqrt{m})$ のどの単数 $\varepsilon > 1$ も ε_0^n で表される。ここに n は非負整数である。

証明: $1 < \varepsilon_0$ であるから $\varepsilon > 1$ に対して $\varepsilon_0^n \leq \varepsilon < \varepsilon_0^{n+1}$ となる n が存在する。これから $1 \leq \varepsilon/\varepsilon_0^n < \varepsilon_0$ である。$\varepsilon/\varepsilon_0^n$ は $Z(\sqrt{m})$ の単数であるが、ε_0 は $1 < \varepsilon_0$ の条件を満たす最小の単数であったので、$\varepsilon = \varepsilon_0^n$ でなくてはならない。 □

[15]「基本単数」の存在証明は、連分数論から、あるいは、イデアル論から攻めることができる。高木は両方を紹介している

$\sqrt{m}=[n_0,\theta]$, $\theta=[n_1,n_2,...]$ とし、$n_1,n_2,...$ が周期 l を持つとする。すなわち、$n_{l+k}=n_k$ $(k=1,2,...)$ とする。$\sqrt{m}$ の判別式は $D=4m$ である。従って θ の判別式も $4m$ である。この自己変形を

$$\theta=[n_1,n_2,...,n_l,\theta],\quad \theta=\frac{r\theta+s}{t\theta+u},\quad ru-ts=\pm1$$

とする。すると $t\theta+u$ は $Z(\sqrt{m})$ の単数であった (補題 8)。

自己変形を k 回繰り返す、すなわち、

$$\theta=[n_1,n_2,...,n_l,n_{l+1},n_{l+2},...,n_{kl},\theta]$$

とすると変形行列は

$$\begin{pmatrix} r_k & s_k \\ t_k & u_k \end{pmatrix}=\begin{pmatrix} r & s \\ t & u \end{pmatrix}^k$$

である。$t_k\theta+u_k$ は単数であり、$t_k\theta+u_k=(t\theta+u)^k$ である (補題 10)。

例 1. $\theta=\dfrac{\sqrt{10}+1}{3}$ とすると $\theta=[1,2,1,\theta]$ である。すると $\theta=\dfrac{4\theta+3}{3\theta+2}$ となり $\begin{pmatrix} 4 & 3 \\ 3 & 2 \end{pmatrix}$ が自己変形行列である。2 周期まで計算すると、(長い計算の後に)

$$\theta=[1,2,1,1,2,1,\theta]=\frac{25\theta+18}{18\theta+13}$$

であることが分かる。これから得られる自己変形行列は $\begin{pmatrix} 25 & 18 \\ 18 & 13 \end{pmatrix}$ であるが、同じ結果は $\begin{pmatrix} 4 & 3 \\ 3 & 2 \end{pmatrix}^2=\begin{pmatrix} 25 & 18 \\ 18 & 13 \end{pmatrix}$ からも簡単に得られる。

$\varepsilon=3\theta+2=\sqrt{10}+3$ は $\varepsilon\overline{\varepsilon}=-1$ を満たし、確かに $Z(\sqrt{10})$ の単数である。$\varepsilon'=18\theta+13=6\sqrt{10}+19$ も $\varepsilon'\overline{\varepsilon}'=1$ を満たし、確かに $Z(\sqrt{10})$ の単数である。そして $\varepsilon'=\varepsilon^2$ の関係が成立している。

例 2. $\omega=\sqrt{10}$ とすると $\omega=[3,\overline{6}]$, $\theta=[6,\theta]=\dfrac{6\theta+1}{1\theta+0}$ である。ここに自己変形は最小周期を採用した。これから単数 $\varepsilon=1\theta+0=\omega+3$ を得る。$\varepsilon^2=6\omega+19$ で、この自己変形は $\theta=[6,6,\theta]=\dfrac{19\theta+60}{6\theta+19}$ である。もちろん、どちらの自己変形からも、同一の θ、従って同一の連分数が得られる。この事情は ε^k $(k\geq1)$ で変わらない。

補題 14. $\sqrt{m}$ の連分数の最小周期から得られた自己変形を $\theta = \dfrac{r\theta + s}{t\theta + u}$ とすると、$t\theta + u$ は $Z(\sqrt{m})$ の基本単数である。

証明: $Z(\sqrt{m})$ の基本単数を ε_0 とする。θ と ε_0 から自己変形を作ることができる (補題 9)。これを $\theta = \dfrac{r_0\theta + s_0}{t_0\theta + u_0}$ としよう。

既に $t\theta + u$ が $Z(\sqrt{m})$ の単数であることは証明されている (補題 8)。またどの単数 ε も基本単数 ε_0 によって $\varepsilon_0^k = \varepsilon$ $(k \geq 1)$ と表されることも証明されている (補題 13)。さらに、既に示したように ε の自己変形行列は $\begin{pmatrix} r & s \\ t & u \end{pmatrix} = \begin{pmatrix} r_0 & s_0 \\ t_0 & u_0 \end{pmatrix}^k$ となる。これは基本単数を与える連分数の周期の k 倍の自己変形である。ε は最小周期から得たのであったから $k = 1$ である。つまり ε は基本単数である。 □

定義: Pell 方程式の基本解: 基本単数に対応する Pell 方程式の解を「Pell 方程式の基本解」と言うことにする。Pell 方程式の基本解から基本単数が求まり、その基本単数のべき乗から Pell 方程式の全ての解が求まる。

例 3. $3 + \sqrt{8}$ は $Z(\sqrt{m})$ の基本単数である。従って $(x, y) = (3, 1)$ は Pell 方程式 $x^2 - 8y^2 = \pm 1$ の基本解である。$(3 + \sqrt{8})^k$ から Pell 方程式 $x^2 - 8y^2 = \pm 1$ の全ての解が求まる。

定理 2 を強めた次の定理が成立する。

定理 2a. $n = [\sqrt{m}]$、$\sqrt{m} = [n, n_1, n_2, ...]$ 、l を連分数の周期とする。すると $n_l = 2n$ で $n, n_1, n_2, ..., n_{l-1}$ のどれも $2n$ より小さい (定理 1)。

そこで、$p_k/q_k = [n, n_1, n_2, ..., n_{kl-1}]$ $(k = 1, 2, ...)$ とすると

$$p_k^2 - mq_k^2 = (-1)^{kl}$$

である。そして、(p_1, q_1) は Pell 方程式の基本解である。また、基本単数を ε_0 とすると、(p_k, q_k) は、単数 ε_0^k に対応した Pell 方程式の解である。

証明: $Z(\sqrt{m})$ の基本単数を ε_0 とする。また $\theta_1 = 1/(\sqrt{m} - n)$ とする。すると自己変形 $\theta_1 = [n_1, n_2, ..., n_r, 2n, \theta_1]$ は基本単数に対応する (補題 14)。$p_1/q_1 =$

$[n, n_1, n_2, ..., n_r]$ が Pell 方程式を満たすことは定理 2 で証明済みであるが、これは Pell 方程式の基本解である。同様にして $p_k/q_k = [n, n_1, n_2, ..., n_{kl-1}]$ $(k = 1, 2, ...)$ は ε_0^k に対応する解であることを示せる。 □

Pell 方程式の解の基本性、あるいは単数の基本性の判定は面倒であった。しかし、この定理が綺麗に、この問題を解決してくれるのである。

例 4. Pell 方程式 $p^2 - 7q^2 = \pm 1$ の解は $\sqrt{7} = [2, \overline{1, 1, 1, 4}]$ であるから、$p/q = [2, 1, 1, 1]$ を計算し、$p/q = 8/3$ として求まる。この $(p, q) = (8, 3)$ は Pell 方程式の基本解である。また、$8 + 3\sqrt{7}$ は $Z(\sqrt{7})$ の基本単数でもある。

例 5. $(p, q) = (15, 4)$ は $p^2 - 14q^2 = 1$ の解である。p/q の連分数 $[3, 1, 3]$ は必要な対称性を持っていないが変形して、$p/q = [3, 1, 2, 1]$ となる。これは必要な対称性を持っており、$\sqrt{14} = [3, \overline{1, 2, 1, 6}]$ から派生していることが分かる。従って $(p, q) = (15, 4)$ は基本解である。

例 6. $(p, q) = (17, 12)$ は $p^2 - 2q^2 = 1$ の解である。$p/q = [1, 2, 2, 2]$ は $\sqrt{2} = [1, \overline{2, 2, 2, 2}]$ に対応する。ところが $[1, \overline{2, 2, 2, 2}] = [1, \overline{2}]$ であり、$[1, \overline{2}]$ からは $p/q = [1]$ を得る。従って、$(p, q) = (17, 12)$ は基本解ではない。基本解は $p/q = [1]$ から得られる $(p, q) = (1, 1)$ である。従って $Z(\sqrt{2})$ の基本単数は $1 + \sqrt{2}$ である。なお $17 + 12\sqrt{2} = (1 + \sqrt{2})^4$ である。

5.5 拡張 Pell 方程式

Pell 方程式を 2 つのタイプに分ける:

$$\text{T1} \quad x^2 - my^2 = \pm 1$$

$$\text{T2} \quad x^2 - my^2 = \pm 4$$

$x^2 - my^2 = \pm 4$ において $m \equiv 1 \pmod 5$ の場合だけが新しい問題を提起する。なぜなら $x^2 \equiv my^2 \pmod 4$ であるから

(a) $m \equiv 0 \pmod 4$ の場合、$x = 2x'$, $m = 4m'$ と置いて $x'^2 - m'y^2 = \pm 1$;

(b) $m \equiv 2, 3 \pmod 4$ の場合、$x \equiv y \equiv 0 \pmod 2$ である。故に $x = 2x'$, $y = 2y$ と置いて $x'^2 - my'^2 = \pm 1$;

故に $m \equiv 1 \pmod 4$ を除いて、いずれも T1 に還元できる。従って以下では $m \equiv 1 \pmod 4$ とする。

既に示したように、T2 の Pell 方程式は、判別式 m の無理数 θ と、それが満たす自己変形 M を見つければ解ける。M は θ を連分数に展開すれば得られるので、結局 θ を見つけることに帰着する。

問題 1. $\omega = \dfrac{1+\sqrt{m}}{2}$ の判別式は m であることを示せ。

答: $4\omega^2 - 4\omega - (m-1) = 0$ であるが、$m \equiv 1 \pmod 4$ であるから $(m-1) = 4m'$ と置いて $\omega^2 - \omega - m' = 0$ を得る。従って判別式は $D = 1 + 4m' = m$ である。

問題 2. 問題 1 において、$m = 5, 13, 17, 21, 29, 33, 37$ の場合の ω の連分数を求めよ。

答: CASE $m = 5$: $\omega = [\overline{1}]$

CASE $m = 13$: $\omega = [2, \overline{3}]$

CASE $m = 17$: $\omega = [2, \overline{1, 1, 3}]$

CASE $m = 21$: $\omega = [2, \overline{1, 3}]$

CASE $m = 29$: $\omega = [3, \overline{5}]$

CASE $m = 33$: $\omega = [3, \overline{2, 1, 2, 5}]$

CASE $m = 37$: $\omega = [3, \overline{1, 1, 5}]$

$m = 17$ について詳しく書くと次のようになる。

$$\left(\frac{\sqrt{17}+1}{2} - 2\right)\left(\frac{\sqrt{17}+3}{4}\right) = 1$$

$$\left(\frac{\sqrt{17}+3}{4} - 1\right)\left(\frac{\sqrt{17}+1}{4}\right) = 1$$

$$\left(\frac{\sqrt{17}+1}{4} - 1\right)\left(\frac{\sqrt{17}+3}{2}\right) = 1$$

$$\left(\frac{\sqrt{17}+3}{2} - 3\right)\left(\frac{\sqrt{17}+3}{4}\right) = 1$$

定理 3. $\omega = \dfrac{\sqrt{m}+1}{2}$, $n_0 = [\omega]$ とすると次が成立する。

(a) ω は $[n_0, \overline{n_1, n_2, ..., n_{r-1}, n_r, 2n_0 - 1}]$ の周期構造を持つ

(b) $[n_0, \overline{n_1, n_2, ..., n_{r-1}, n_r, 2n_0 - 1}) = [n_0, \overline{n_r, n_{r-1}, ..., n_2, n_1, 2n_0 - 1}]$

(c) $n_k \leq n_0 \quad (k = 1, 2, ..., r)$

証明: $\omega = \dfrac{\sqrt{m}+1}{2}$ とする。すると $\omega > 1$, $\omega + \overline{\omega} = 1$ である。$n_0 = [\omega]$ とすると $n_0 \geq 1$ である。そこで $\theta = \dfrac{1}{\omega - n_0}$ と置くと、$\theta > 1$ である。また

$$-\frac{1}{\overline{\theta}} = n_0 - \overline{\omega} = n_0 - (1 - \omega) = n_0 - 1 + \omega > 1$$

であるから $-1 < \overline{\theta} < 0$ となり、θ は簡約された 2 次無理数である。従って $\eta = -1/\overline{\theta}$ とすると、補題 12 によって

$$\omega = [n_0, \theta] \tag{1}$$

$$\theta = [n_1, n_2, ..., n_{l-1}, n_l, \theta] \tag{2}$$

$$\eta = [n_l, n_{l-1}, ..., n_2, n_1, \eta] \tag{3}$$

が成り立つ。また

$$\frac{1}{\theta} = \omega - n_0, \quad \eta = -\overline{\omega} + n_0$$

である。これと $\omega + \overline{\omega} = 1$ より

$$\frac{1}{\theta} - \eta = 1 - 2n_0$$

故に

$$\eta = 2n_0 - 1 + \frac{1}{\theta} = [2n_0 - 1, \theta]$$

である。これと式 (3) を比較して $2n_0 - 1 = n_l$ および

$$\begin{aligned} \theta &= [n_{l-1}, ..., n_2, n_1, \eta] = [n_{l-1}, ..., n_2, n_1, [2n_0 - 1, \theta]] \\ &= [n_{l-1}, ..., n_2, n_1, 2n_0 - 1, \theta] \end{aligned} \tag{4}$$

を得る。これを式 (2) と比較して $(n_{l-1}, ..., n_2, n_1) = (n_1, n_2, ..., n_{l-1})$ と $n_l = 2n_0 - 1$ を得る。最後に式 (2) と式 (4) より ($r = l - 1$ と置いて) 定理の (a) と (b) の主張を得る。

(c) の証明: $\theta_k = \dfrac{\sqrt{m} + b_k}{a_k}$ とすると

$$\frac{\sqrt{m} + b_k}{a_k} - n_k = \frac{\sqrt{m} - b_{k+1}}{a_k} \quad (k = 1, 2, ..., r)$$

従って $b_k + b_{k+1} = n_k a_k$ である。他方、b_k $(k = 1, 2, ..., r)$ はどれも $0 < b_k < \sqrt{m}$ すなわち $0 < b_k \leq n$ を満たす。ここに $n = [\sqrt{m}]$ である。従って $b_k + b_{k+1} \leq 2n$ である。$m \equiv 1 \pmod 4$ の場合には $a_k = 1$ は発生しない。

a_k は偶数だからである (補題 5 の補注)。$a_k \geq 2$ の場合には $n_k a_k \leq 2n$ より $n_k \leq n$ を得る。 □

問題 3. 問題 2 の結果を利用して、$m = 5, 13, 17, 21, 29, 33, 37$ の場合について、拡張 Pell 方程式 $x^2 - my^2 = \pm 4$ の解を求めよ。

答: CASE $m = 5$: $\omega = [1, \theta]$, $\theta = [1, \theta]$ として、θ の自己変形 $\theta = (\theta+1)/\theta$ を得る。$\theta = (\sqrt{5}+1)/2$ で、自己変形の分母である θ が単数である。実際 $\theta\overline{\theta} = -1$ を満たしている。従って $(x, y) = (1, 1)$ である。

CASE $m = 13$: $\omega = [2, \theta]$, $\theta = [3, \theta]$ として、θ の自己変形 $\theta = (3\theta + 1)/\theta$ を得る。$\theta = (\sqrt{13} + 3)/2$ で、自己変形の分母である θ が単数である。実際 $\theta\overline{\theta} = -1$ を満たしている。従って $(x, y) = (3, 1)$ である。

CASE $m = 17$: $\omega = [2, \theta]$, $\theta = [1, 1.3, \theta]$ として、θ の自己変形 $\theta = (7\theta + 2)/(4\theta+1)$ を得る。$\theta = (\sqrt{17}+3)/4$ で、自己変形の分母である $4\theta+1 = 4+\sqrt{17}$ が単数である。実際 $(4\theta + 1)(4\overline{\theta} + 1) = (4 + \sqrt{17})(4 - \sqrt{17}) = -1$ を満たしている。しかし、これは $Z(\sqrt{17})$ の単数になっている。$4 + \sqrt{17} = 3 + 2\omega$ であるから、これは $Z^*(\sqrt{17})$ の単数でもある。これは拡張 Pell 方程式 T2 において、x, y が共に偶数の場合に該当する。

m	m	$(\mathrm{mod}\ 8)$	ω	Pell eq.
5		5	$\omega = [\overline{1}] = [1, \overline{1}]$	$1^2 - 5 \cdot 1^2 = -4$
13		5	$\omega = [2, \overline{3}]$	$3^2 - 13 \cdot 1^2 = -4$
17		1	$\omega = [2, \overline{1, 1, 3}]$	$4^2 - 17 \cdot 1^2 = -1$
21		5	$\omega = [2, \overline{1, 3}]$	$5^2 - 21 \cdot 1^2 = +4$
29		5	$\omega = [3, \overline{5}]$	$5^2 - 29 \cdot 1^2 = -4$
33		1	$\omega = [3, \overline{2, 1, 2, 5}]$	$23^2 - 33 \cdot 4^2 = +1$
37		5	$\omega = [3, \overline{1, 1, 5}]$	$6^2 - 37 \cdot 1^2 = -1$

符号は循環部分の周期と関係していることが読み取れる。この方法で得られた単数は $Z(\sqrt{m})$ の単数になる場合があった。これはどのような場合か? これに関係して次の補題がある。

補題 15. $m \equiv 1\ (\mathrm{mod}\ 8)$ とすると、$Z^*(\sqrt{m})$ における単数は $Z(\sqrt{m})$ の単数でもある。

証明: $\epsilon = (x + y\sqrt{m})/2$ を $Z^*(\sqrt{m})$ の単数とすると、$x^2 - my^2 = \pm 4$ である。$m \equiv 1 \pmod 4$ でもあるので、$x^2 \equiv y^2 \pmod 4$、つまり x, y は共に偶数あるいは共に奇数である。他方 $x^2 \equiv y^2 \pm 4 \pmod 8$ であるが、この合同式は x, y が共に奇数の場合には成立しない。つまり x, y は共に偶数である。このことは ϵ は $Z(\sqrt{m})$ の単数でもあることを意味する。 □

補題 16. $m \equiv 5 \pmod 8$ とする。$Z^*(\sqrt{m})$ における単数を ϵ とすると ϵ^3 は $Z(\sqrt{m})$ の単数である。

証明: $\epsilon = (x + y\sqrt{m})/2$ とすると $x^2 - my^2 = \pm 4$ である。$m \equiv 1 \pmod 4$ でもあるので、$x^2 \equiv y^2 \pmod 4$、つまり $x \equiv y \pmod 2$ である。ϵ^3 を計算すると

$$\epsilon^3 = \frac{x(x^2 + 3my^2) + y(3x^2 + my^2)\sqrt{m}}{8}$$

x, y が共に奇数として

$$x(x^2 + 3my^2) \equiv x(1 + 3m) \equiv 16x \equiv 0 \pmod 8$$
$$y(3x^2 + my^2) \equiv y(3 + m) \equiv 8y \equiv 0 \pmod 8$$

従って $\epsilon^3 \in Z(\sqrt{m})$ である。

x, y が共に偶数の場合には ϵ は既に $Z(\sqrt{m})$ の単数であり、従って $\epsilon^3 \in Z(\sqrt{m})$ である。 □

ここで、第 5.3 節「Pell 方程式と連分数」の最初に紹介した Pell 方程式の解法を、拡張 Pell 方程式に適用してみよう。

$\omega = (\sqrt{m} + 1)/2$ として、$\omega = [n, \overline{n_1, n_2, ..., n_l}]$ とすると、$\omega = [n, \theta]$, $\theta = [n_1, n_2, ..., n_l, \theta]$ と書けた。θ の自己変形を $\theta = (r\theta + s)/(t\theta + u)$ とすると $\eta = 1/\theta$ の自己変形は $\eta = (u\eta + t)/(s\eta + r)$ である。そして

$$\eta = \frac{\sqrt{m} + 1}{2} - n = \frac{\sqrt{m} - (2n - 1)}{2}$$

である。従って $\eta+\overline{\eta}=-(2n-1),\ \eta\overline{\eta}=((2n-1)^2-m)/4$ が成り立ち

$$\begin{aligned}N(s\eta+r)&=(r^2+sr(\eta+\overline{\eta})+s^2\eta\overline{\eta})\\&=r^2-(2n-1)sr+s^2\cdot\frac{(2n-1)^2-m}{4}\\&=(r-\frac{2n-1}{2}\cdot s)^2-\frac{m}{4}\cdot s^2\end{aligned}$$

となるが、自己変形の分母は単数であった。故に

$$(2r-(2n-1)s)^2-ms^2=\pm4$$

が成り立つ。

例 1. $m=21$ とすると、$\omega=[2,\theta],\ \theta=[1,3,\theta]=(4\theta+1)/(3\theta+1)$ である。従って $(n,r,s)=(2,4,1)$ となり、

$$(8-3\cdot1)^2-21\cdot1^2=+4$$

で、確かに、拡張 Pell 方程式の解になっている。

例 2. $m=33$ とすると、$\omega=[3,\theta],\ \theta=[2,1,2,5,\theta]=(43\theta+8)/(16\theta+3)$ である。従って $(n,r,s)=(3,43,8)$ となり、

$$(2\cdot43-5\cdot8)^2-33\cdot8^2=+4$$

となるが、通約できて

$$(43-5\cdot4)^2-33\cdot4^2=+1$$

を得る。

定理 4. m を $m\equiv1\pmod4$ なる自然数とする。また ω を

$$\omega=\frac{\sqrt{m}+1}{2}=[n,\overline{n_1,n_2,...,n_r,2n-1}]$$

とすると

$$\frac{p}{q}=[n,n_1,n_2,...,n_r]$$

によって定義した既約分数 p/q は

$$(2p-q)^2-mq^2=(-1)^{r+1}\cdot4$$

を満たす。

証明: 自己変形を

$$\omega = [n, \theta], \quad \theta = [n_1, n_2, ..., n_r, 2n-1, \theta] = \frac{r\theta + s}{t\theta + u}, \quad \eta = \frac{1}{\theta}$$

とすると、$\omega = n + \eta$ であるから

$$\eta = \frac{u\eta + t}{s\eta + r}, \quad \eta = \omega - n = \frac{\sqrt{m} - (2n-1)}{2}$$

を得る。付録 C 定理 6、付録 C 定理 1 を使って

$$\begin{aligned} r &= H(n_1, n_2, ..., n_r, 2n-1) = H(2n-1, n_r, ..., n_2, n_1) \\ &= H(2n-1, n_1, n_2, ..., n_r) \\ s &= H(n_1, n_2, ..., n_r) \end{aligned}$$

である。従って付録 C 定理 4 より

$$\begin{aligned} \frac{r}{s} &= \frac{H(2n-1, n_1, n_2, ..., n_r)}{H(n_1, n_2, ..., n_r)} = [2n-1, n_1, n_2, ..., n_r] \\ &= n - 1 + [n, n_1, n_2, ..., n_r] = n - 1 + \frac{p}{q} \end{aligned}$$

となる。従って

$$\begin{aligned} &s = q, \quad r = p + (n-1)q \\ &s\eta + r = q \cdot \frac{\sqrt{m} - (2n-1)}{2} + p + (n-1)q = \frac{(2p-q) + q\sqrt{m}}{2} \end{aligned}$$

となるが、$s\eta + r$ は自己変形の分母だから単数である。故に

$$(2p-q)^2 - mq^2 = \pm 4$$

である。連分数の長さが偶数なら正、奇数なら負である (補題 6)。 □

例 3. $m = 5$ の場合、$\omega = [\overline{1}]$, $p/q = [1]$ より $(p, q) = (1, 1)$ である。従って

$$(2-1)^2 - 5 \cdot 1^2 = -4$$

例 4. $m = 6$ の場合には $m \not\equiv 1 \pmod 4$ であるから定理 4 の適用外である。無理をするとどうなるか? まず ω の連分数展開は面倒である。$\dfrac{\sqrt{6}+1}{2} = \dfrac{\sqrt{24}+2}{4}$ と書き換える必要がある。その場合 $\omega = [\overline{1, 1, 2, 1}]$ となり定理の方法が適用できない。ではどうすれば拡張 Pell 方程式 $x^2 - 6y^2 = \pm 4$ の解を求めることができるか? $x = 2p$, $y = 2q$ と置いて $p^2 - 6q^2 = \pm 1$ を求める。この解は $(p, q) = (5, 2)$ である。

例 5. $m = 13$ の場合、$\omega = [2, \overline{3}]$, $p/q = [2] = 2/1$ である。従って

$$(4-1)^2 - 13 \cdot 1^2 = -4$$

例 6. $m = 17$ の場合、$\omega = [2, \overline{1, 1, 3}]$, $p/q = [2, 1, 1] = 5/2$ である。従って

$$(10-2)^2 - 17 \cdot 2^2 = -4 \quad \text{or} \quad 4^2 - 17 \cdot 1^2 = -1$$

例 7. $m = 21$ の場合、$\omega = [2, \overline{1, 3}]$, $p/q = [2, 1] = 3/1$ である。従って

$$(6-1)^2 - 21 \cdot 1^2 = +4$$

例 8. $m = 29$ の場合、$\omega = [3, \overline{5}]$, $p/q = [3] = 3/1$ である。従って

$$(6-1)^2 - 29 \cdot 1^2 = -4$$

例 9. $m = 33$ の場合、$\omega = [3, \overline{2, 1, 2, 5}]$, $p/q = [3, 2, 1, 2] = 27/8$ である。従って

$$(54-8)^2 - 33 \cdot 8^2 = +4 \quad \text{or} \quad 23^2 - 33 \cdot 4^2 = +1$$

例 10. $m = 37$ の場合、$\omega = [3, \overline{1, 1, 5}]$, $p/q = [3, 1, 1] = 7/2$ である。従って

$$(14-2)^2 - 37 \cdot 2^2 = -4 \quad \text{or} \quad 6^2 - 37 \cdot 1^2 = -1$$

重要な問題が残されている。

基本単数の存在 $m \equiv 1 \pmod 4$ として、$Z^*(\sqrt{m})$ の基本単数は存在するか?

YES: この問題は $Z(\sqrt{m})$ に関して補題 13 で扱われている。同様に存在が証明される。$Z(\sqrt{m})$ の単数は $Z^*(\sqrt{m})$ の単数でもあるから [16]、$Z(\sqrt{m})$ の単数 ε は $\varepsilon = \epsilon_0^k$ $(k \in N)$ で表されることになる。ここに ϵ_0 は $Z^*(\sqrt{m})$ の基本単数である。

連分数の最小周期と基本単数の関係 $m \equiv 1 \pmod 4$ として、$\dfrac{\sqrt{m}+1}{2}$ の連分数の最小周期から得られる単数は $Z^*(\sqrt{m})$ の基本単数か?

YES: この問題も $Z(\sqrt{m})$ に関して補題 14 で扱われている。証明もこれと同様に進む。

[16] $m \pmod 4$ の値に関わらず $Z^*(\sqrt{m})$ は $Z(\sqrt{m}) \subset Z^*(\sqrt{m})$ となるように定義されたのである

例 11. $m = 13$ の場合、$\omega = [2, \overline{3}]$ の循環の第 1 節から $p/q = [2] = 2/1$ が得られる。従って $x = 2p - q = 3,\ y = q = 1$ より

$$\epsilon_0 = \frac{x + y\sqrt{13}}{2} = \frac{3 + \sqrt{13}}{2}$$

が $Z^*(\sqrt{13})$ の基本単数である。従って $\epsilon_0^2 = \dfrac{11 + 3\sqrt{13}}{2}$ も $Z^*(\sqrt{13})$ の単数である。これから拡張 Pell 方程式の他の解 $11^2 - 13 \cdot 3^2 = 4$ が得られる。

同じ結果は ω の循環の最初の 2 つの節を使って

$$p/q = [2, 3] = 7/3, \quad x = 2p - q = 11, \quad y = q = 3$$

としても得られる。

例 12. $m = 21$ の場合、$\omega = [2, \overline{1, 3}]$ の循環の第 1 節から $p/q = [2, 1] = 3/1$ が得られる。従って $x = 2p - q = 5,\ y = q = 1$ より

$$\epsilon_0 = \frac{x + y\sqrt{21}}{2} = \frac{5 + \sqrt{21}}{2}$$

が $Z^*(\sqrt{21})$ の基本単数である。従って $\epsilon_0^2 = \dfrac{23 + 5\sqrt{21}}{2}$ も $Z^*(\sqrt{21})$ の単数である。これから拡張 Pell 方程式の他の解 $23^2 - 21 \cdot 5^2 = 4$ が得られる。

同じ結果は ω の循環の最初の 2 つの節を使って

$$p/q = [2, 1, 3, 1] = 14/5, \quad x = 2p - q = 23, \quad y = q = 5$$

としても得られる。

Chapter 6

一般 Pell 方程式

6.1 一般 Pell 方程式とは

ここでは $m, d \in N$ を与え

$$x^2 - my^2 = k\ (= \pm d) \quad (x, y \in Z) \tag{6.1}$$

のタイプの方程式を考える。m は平方数ではないとしている。

例えば $m = 5,\ d = 20$ を与えると、$(x, y) = (0, 2),\ (5, 1),\ (5, 3),\ (10, 4),\ (15, 7)$ などの解を得る。そのときの k は $+20$ または -20 となるが、どちらも解とする。どちらの解であるかを明示するために、この章の例題では解を $(x, y, k) = (0, 2, -20), (5, 1, 20), (5, 3, -20), (10, 4, 20), (15, 7, -20)$ のように k の値も表示している。k を与えて方程式を解いているのではないことを注意しておく [1]。

$d = 1$ は通常の Pell 方程式で、$d = 4$ は拡張 Pell 方程式である。それらの解法は既に分かっている。ここで考えようとしている問題は、そのどちらにも属さない方程式で、ここでは一般 Pell 方程式と呼ぼう [2]。この場合には、解が存在する条件は何か? 存在するとすれば、どのように求めるか?

[1] 通常のテキストや論文などでは k を与えて解こうとしている。しかし、この問題の特性を考えると $+d$ と $-d$ の解は切り離し難いのである

[2] 英文の文献では generalized Pell's equation と呼ばれている。日本語では河田の「一般の Pell 方程式」がある [6]

式 (6.1) の x, y を実数と考え、グラフを描くと双曲線になる (図 6.1)。整数解はこの双曲線の上にある。この双曲線は x 軸と y 軸に対称であり、整数解の分布もまた x 軸と y 軸に対称である。(次節で紹介する解法 I では解の分布についての、この簡単な性質が利用されていない。後に紹介する Conrad の方法と解法 II ではフルに利用されている)

式 (6.1) を

$$(x - \sqrt{m}y)(x + \sqrt{m}y) = k \tag{6.2}$$

と変形する。すると式 (6.1) を解く問題は、$\xi\overline{\xi} = k$ となる $Z(\sqrt{m})$ の元 $\xi = x + \sqrt{m}y$ を見つける問題であると考えることができる [3]。

そのような解が見つかったとせよ。それを θ とする。$Z(\sqrt{m})$ の基本単数を ε_0 とする。$\varepsilon_0\overline{\varepsilon}_0 = \pm 1$ である。$\xi = \pm\theta\varepsilon_0^n$ $(n \in Z)$ とすると、

$$\xi\overline{\xi} = \theta\overline{\theta}(\varepsilon_0\overline{\varepsilon}_0)^n = k(\varepsilon_0\overline{\varepsilon}_0)^n$$

であるから、$\varepsilon_0\overline{\varepsilon}_0 = +1$ の場合には ξ は n に関わらず $\xi\overline{\xi} = k$ を満たすが、$\varepsilon_0\overline{\varepsilon}_0 = -1$ の場合には ξ は n の偶奇に従って $\xi\overline{\xi} = +k$ または $\xi\overline{\xi} = -k$ を満たす。基本単数は常に存在するので、式 (6.1) に解が存在するなら、無限個の解が存在するのである。

図 6.1 に $x^2 - 5y^2 = \pm 20$ の双曲線と、整数解 (黒丸) を例として示す。また双曲線の漸近線 $x + \sqrt{5}y = 0$ と $x - \sqrt{5}y = 0$ も参考のために描かれている。当然のことであるが、整数解 (黒丸) は x 軸と y 軸に対称に分布している。図に見える $x, y \geq 0$ の整数解は $(x, y) = (0, 2),\ (5, 1),\ (5, 3),\ (10, 4),\ (15, 7)$ である。

[3] $Z(\sqrt{m})$ は第 5.2 節で定義されている

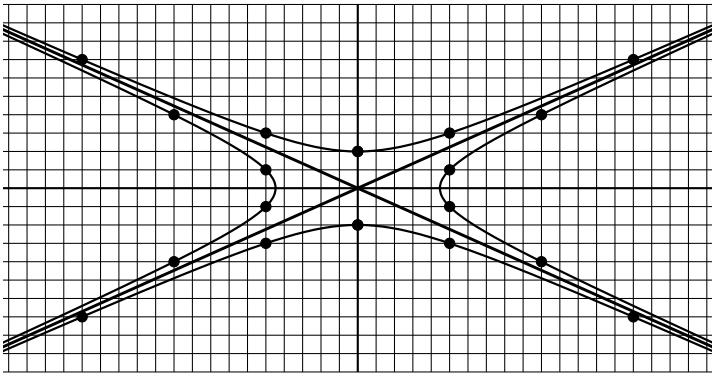


図 6.1: 解の分布例

解 $(0,2)$ は $2\sqrt{5}$ に対応している。$Z(\sqrt{5})$ の基本単数は $\varepsilon_0 = 2+\sqrt{5}$ である。$2\sqrt{5}\varepsilon_0 = 10+4\sqrt{5}$ で、座標点 $(10,4)$ が得られる。また $2\sqrt{5}\varepsilon_0^{-1} = 10-4\sqrt{5}$ で、座標点 $(10,-4)$ が得られる。

解 $(5,1)$ は $5+\sqrt{5}$ に対応している。$(5+\sqrt{5})\varepsilon_0 = 15+7\sqrt{5}$ である。また $(5+\sqrt{5})\varepsilon_0^{-1} = -5+3\sqrt{5}$ である。

解 $(5,3)$ は $5+3\sqrt{5}$ に対応している。$(5+3\sqrt{5})\varepsilon_0 = 25+11\sqrt{5}$ であるが、これは図からはみ出ている。$(5+3\sqrt{5})\varepsilon_0^{-1} = 5-\sqrt{5}$ 及び $(5+3\sqrt{5})\varepsilon_0^{-2} = -15+7\sqrt{5}$ が図に見える。

この例で分かるように、式 (6.1) の解の相互の関係を見るときに、基本単数が重要な役割を演じている。さらに、$k=-d$ の解から $k=+d$ の解が得られる (あるいはその逆) ことがあるのだから、$k=+d$ の解と $k=-d$ の解を切り離してはならないことが分かる。

式 (6.1) の解について考えるときは $x+\sqrt{m}y>0$ の領域だけに注目して構わない。残りの領域の解は x,y の符号を反転して得られる。$x+\sqrt{m}y>0$ の領域の解は $Z(\sqrt{m})$ の正の単数で結ばれている。そして正の単数は基本単数 ε_0 によって ε_0^n $(n \in Z)$ で表せるのであった。

ここで「同伴」を次のように定義する。

定義: 同伴: 実数 ξ と ξ' が $U(\sqrt{m})$ にて同伴であるとは、$\xi/\xi' \in U(\sqrt{m})$ であること。($U(\sqrt{m})$ とは $Z(\sqrt{m})$ の単数の集合であった)

同様に「$U^*(\sqrt{m})$ にて同伴」が定義される。($U^*(\sqrt{m})$ とは $Z^*(\sqrt{m})$ の単数の集合であった [4])

注意: 通常のテキストでは、同伴を $Z^*(\sqrt{m})$ の単数によって定義している [5]。しかし、そのような広い「同伴」は式 (6.1) に関する限り適切ではない。そこで、考えている単数の集合を明示することにしたのである。

$\theta\overline{\theta} = \pm d$ を満たす θ に、$U(\sqrt{m})$ にて同伴な無数の $\xi(= \pm\theta\varepsilon_0^n)$ もまた $\xi\overline{\xi} = \pm d$ を満たすのである。これらは一つの類をなしている。$U^*(\sqrt{m})$ にて同伴な場合も同様であるが、その場合 $Z(\sqrt{m})$ の基本単数 ε_0 を $Z^*(\sqrt{m})$ の基本単数 ϵ_0 に代える必要がある。

図 6.1 の $x + \sqrt{5}y > 0$ の領域では 9 個の整数解 (黒丸) が存在し、同伴関係によって次の 3 つに分類される:

$$(0,2) \sim (10,4) \sim (10,-4)$$
$$(5,1) \sim (15,7) \sim (-5,3)$$
$$(5,3) \sim (5,-1) \sim (-15,7)$$

ここに $U(\sqrt{5})$ による同伴関係を $\sim$ で表している。従って $x^2 - 5y^2 = \pm 20$ の全ての整数解は $Z(\sqrt{5})$ の単数 $\varepsilon_0 = 2 + \sqrt{5}$ を使って

$$\pm\sqrt{5}\varepsilon_0^n, \quad \pm(5+\sqrt{5})\varepsilon_0^n, \quad \pm(5+3\sqrt{5})\varepsilon_0^n \quad (n \in Z)$$

を計算して得られる。

こうした分類は絶対的なものではない。もしも同伴関係を $U^*(\sqrt{5})$ で定義すると、基本単数が変化する。$Z^*(\sqrt{5})$ の基本単数を ϵ_0 としよう。すると

$$\epsilon_0 = (1+\sqrt{5})/2, \quad \varepsilon_0 = \epsilon_0^3$$
$$2\sqrt{5}\epsilon_0 = 5+\sqrt{5}, \quad (5+\sqrt{5})\epsilon_0 = 5+3\sqrt{5}$$

であるから、今度はここに挙げた解は全て同伴となる。従って、この場合、全ての解は $\pm 2\sqrt{5}\epsilon_0^n$ $(n \in Z)$ の計算から得られる。つまり、同伴関係によって解

[4] $Z^*(\sqrt{m})$ は第 5.2 節で定義されている
[5] 例えば、高木 p.272

を分類する場合、単数集合として何を使っているのか、はっきりさせる必要があるのである。

我々は一般 Pell 方程式 (6.1) の、次の特性を持つ解の組 S が欲しいのである。

(a) S の中に、同伴な 2 つの元は存在しない
(b) 方程式 (6.1) の全ての解が、S の元に単数を乗じて生成される

これらの 2 つの特性を持つ解の組を一般 Pell 方程式の**代表解の組**と呼ぶことにしよう。また代表解の組の要素を**代表解**と呼ぶことにしよう[6]。

6.2 解法 I

補題 1. 自然数 d と、平方数ではない自然数 m を与える。$Z(\sqrt{m})$ の元 θ が

$$\theta\overline{\theta} = \pm d \tag{1}$$

を満たしているとする。以下、この θ を式 (1) の解と呼ぶ。

すると θ の $U(\sqrt{m})$ における同伴解 θ_0 で

$$\sqrt{d} \leq \theta_0 < \varepsilon_0\sqrt{d}$$

を満たすものが一つだけ存在する。ここに ε_0 は $Z(\sqrt{m})$ の基本単数である。

証明: $\theta' = \pm\varepsilon_0^n\theta$ $(n \in Z)$ はどれも $U(\sqrt{m})$ における θ の同伴解である。そのうち、$\theta' \geq \sqrt{d}$ となる最小の θ' を選び、それを θ_0 とする。すると $\theta_0 < \varepsilon_0\sqrt{d}$ が成り立つ。なぜなら、仮に $\theta_0 \geq \varepsilon_0\sqrt{d}$ とすると $\varepsilon_0 > 1$ 故

$$\theta_0 > \frac{\theta_0}{\varepsilon_0} \geq \sqrt{d}$$

となる。そして

$$\frac{\theta_0}{\varepsilon_0} = \pm\theta_0\overline{\varepsilon}_0$$

である。この $\pm$ の符号は $N(\varepsilon_0) = \varepsilon_0\overline{\varepsilon}_0 = \pm 1$ の符号に対応している。$+1$ の場合には $\overline{\varepsilon}_0 > 0$ であるが、-1 の場合には $\overline{\varepsilon}_0 < 0$ である。何れにせよ、

[6]「代表解」は筆者の造語である。「代表解」は、高木 p.224 の「根原解」(現代なら「根源解」と書くのだろう) と似ているが、根原解は解の存在範囲を予め限定しているのに対して、代表解では目標に応じて柔軟に存在範囲を設定している

$\theta_0' = \theta_0/\varepsilon_0 = \pm\theta_0\bar{\varepsilon}_0 \in Z(\sqrt{m})$ は $\theta_0' \geq \sqrt{d}$ と $N(\theta_0') = \pm 1$ を満たし、θ_0 より小さい。つまり最初の仮定に反する。

「一つだけ」は次のように示される。仮に θ の同伴解 θ' で $\theta_0 < \theta' < \varepsilon_0\sqrt{d}$ となるものが存在するとすれば、θ' は $Z(\sqrt{m})$ の単数 ε を使って $\theta' = \varepsilon\theta_0$ と表されることとなる。すると $\theta_0 < \varepsilon\theta_0 < \varepsilon_0\sqrt{d}$ である。ところが θ_0 は $\theta_0 \geq \sqrt{d}$ を満たすように選ばれたのであった。従って $\varepsilon < \varepsilon_0\sqrt{d}/\theta_0 < \varepsilon_0$ となるが、これは ε_0 が基本単数であるとする前提に反する。 □

この補題は代表解の組を $\sqrt{d} \leq x + \sqrt{m}y < \varepsilon_0\sqrt{d}$ の範囲に求めるのに使える。

定理 1. 自然数 d と、平方数ではない自然数 m を与えた不定方程式

$$x^2 - my^2 = k \ (= \pm d) \tag{1}$$

が自然数解を持つとする。すると $N(\varepsilon_0) = +1$ の場合は

$$\begin{aligned} 0 \leq y < q\sqrt{d} \qquad & \text{if} \quad k > 0 \\ \sqrt{d/m} \leq y < p\sqrt{d/m} \qquad & \text{if} \quad k < 0 \end{aligned} \tag{2}$$

$N(\varepsilon_0) = -1$ の場合は

$$\begin{aligned} 0 \leq y < p\sqrt{d/m} \qquad & \text{if} \quad k > 0 \\ \sqrt{d/m} \leq y < q\sqrt{d} \qquad & \text{if} \quad k < 0 \end{aligned} \tag{3}$$

の範囲に代表解を求めることができる。ここに ε_0 は $Z(\sqrt{m})$ の単数で $\varepsilon_0 = p + q\sqrt{m}$ としている。

証明: x, y を実数として、双曲線 $x^2 - my^2 = k$ $(k = \pm d)$ と直線 $x + \sqrt{m}y = c$ との交点を調べよう。与えられた c と d に対して、この交点は (存在するとすれば) $k = +d$ と $k = -d$ の各々について唯 1 点が定まる。これを $P(c)$ と $Q(c)$ としよう。

$x, y \geq 0$ の領域に代表解を見出そう。そこで、以下では $x, y \geq 0$ とする。この領域において、この双曲線のグラフは増加関数である。

この領域の中で、双曲線と直線が交点を持つ最小の c を c_0 とする。すると $c_0 = \sqrt{d}$ で、そのときは、直線 $x + \sqrt{m}y = c_0$ は $k = +d$ の双曲線と $k = -d$ の双曲線の両方に ($x, y \geq 0$ の領域境界で) 交点を持つ (図 6.2)。そこで $P_0 = P(c_0)$, $Q_0 = Q(c_0)$ とする。$P_0 = (\sqrt{d}, 0)$, $Q_0 = (0, \sqrt{d/m})$ である。

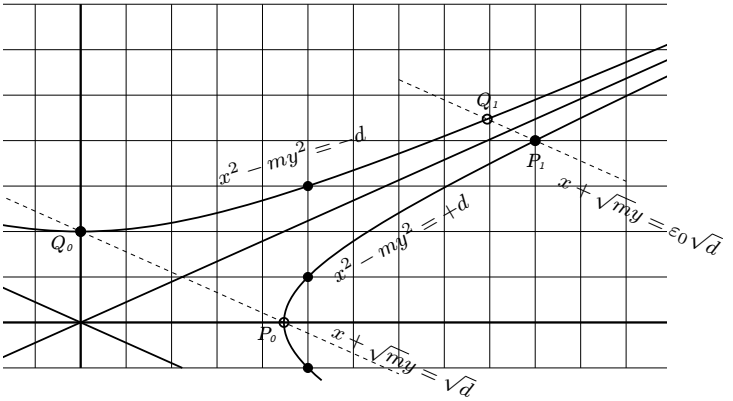


図 6.2: $x, y \geq 0$ における代表解の範囲

ε_0 を $Z(\sqrt{m})$ の基本単数とする。$\varepsilon_0 > 1$ に注意しておく。また $N(\varepsilon_0^n) = \pm 1$ $(n \in Z)$ である。

$n \geq 0$ に対して $c_n = c_0\varepsilon_0^n$, $P_n = P(c_n)$, $Q_n = Q(c_n)$ とする。P_1, Q_1 を求めよう。

$$(x + \sqrt{m}y)(x - \sqrt{m}y) = k, \quad x + \sqrt{m}y = c_1$$

を解くと

$$x = \frac{1}{2}(c_1 + \frac{k}{c_1}), \quad y = \frac{1}{2\sqrt{m}}(c_1 - \frac{k}{c_1})$$

を得る。$k = \pm d$ 故、これで 2 点が求まる。

簡単のために $r = q\sqrt{m}$ と置く。$\varepsilon_0 = p + r$ とすると、$2p = \varepsilon_0 + \bar{\varepsilon}_0$, $2r = \varepsilon_0 - \bar{\varepsilon}_0$ である。$k > 0$ の場合、

$$2x = c_1 + \frac{d}{c_1} = \sqrt{d}(\varepsilon_0 + \frac{1}{\varepsilon_0})$$

$$2y\sqrt{m} = c_1 - \frac{d}{c_1} = \sqrt{d}(\varepsilon_0 - \frac{1}{\varepsilon_0})$$

$k<0$ の場合、

$$2x = c_1 - \frac{d}{c_1} = \sqrt{d}(\varepsilon_0 - \frac{1}{\varepsilon_0})$$
$$2y\sqrt{m} = c_1 + \frac{d}{c_1} = \sqrt{d}(\varepsilon_0 + \frac{1}{\varepsilon_0})$$

となる。

また $N(\varepsilon_0) = +1$ の場合

$$\varepsilon_0 + \frac{1}{\varepsilon_0} = \varepsilon_0 + \overline{\varepsilon}_0 = 2p$$
$$\varepsilon_0 - \frac{1}{\varepsilon_0} = \varepsilon_0 - \overline{\varepsilon}_0 = 2r$$
$$P_1 = (p\sqrt{d},\ r\sqrt{d/m}), \quad Q_1 = (r\sqrt{d},\ p\sqrt{d/m})$$

他方 $N(\varepsilon_0) = -1$ の場合

$$\varepsilon_0 + \frac{1}{\varepsilon_0} = \varepsilon_0 - \overline{\varepsilon}_0 = 2r$$
$$\varepsilon_0 - \frac{1}{\varepsilon_0} = \varepsilon_0 + \overline{\varepsilon}_0 = 2p$$
$$P_1 = (r\sqrt{d},\ p\sqrt{d/m}), \quad Q_1 = (p\sqrt{d},\ r\sqrt{d/m})$$

である。

従って、不定方程式 (1) の自然数解が存在するとすれば、双曲線の区間 P_0, P_1 あるいは区間 Q_0, Q_1 に存在しなくてはならないので、定理の式 (2),(3) を得る。 □

図 6.2 では、$x^2 - 5y^2 = \pm 20$ が例示されている。

原理的な話としては、定理 1 で十分に問題が解決されているのである。以下に適用例を挙げる。

例 1. $x^2 - 2y^2 = k = \pm 7$

計算に必要なパラメータを整理すると次のようになる。

$$m = 2,\ d = 7,\ \varepsilon_0 = 1 + \sqrt{2},\ N(\varepsilon_0) = -1,\ p = 1,\ q = 1$$

定理 1 式 (3) より、$k = +7$ の場合 $0 \le y < \sqrt{7/2}$ となる。故に $y = 0, 1$ を試せばよい。$k = -7$ の場合 $\sqrt{7/2} \le y < \sqrt{7}$ となる。故に $y = 2$ を試せばよい。x は $x^2 = 2y^2 \pm 7$ から求める。結果は $(x, y, k) = (3, 1, 7), (1, 2, -7)$

例 2. $x^2 - 3y^2 = k = \pm 6$

計算に必要なパラメータを整理すると次のようになる。

$$m = 3,\ d = 6,\ \varepsilon_0 = 2 + \sqrt{3},\ N(\epsilon_0) = +1,\ p = 2,\ q = 1$$

定理 1 式 (2) より、$k = +6$ の場合 $0 \leq y < \sqrt{6}$ となる。故に $y = 0, 1, 2$ を試せばよい。$k = -6$ の場合 $\sqrt{6/3} \leq y < 2\sqrt{6/3}$ となる。故に $y = 2$ を試せばよい。x は $x^2 = 3y^2 \pm 6$ から求める。結果は $(x, y, k) = (3, 1, 6)$

別解: $x = 3x'$ と置いて、$y^2 - 3x'^2 = k = \mp 2$ を得る。この $+2$ の解は存在しない。-2 の解は $(x', y) = (1, 1)$ である。従って例題の解は $(x, y, k) = (3, 1, 6)$ である。

補注 1: $x^2 - 3y^2 = \pm 2$ と $x^2 - 3y^2 = \pm 3$ を別々に解けばよいと考えるかも知れない。$x^2 - 3y^2 = \pm 2$ から $N(1 + \sqrt{3}) = -2$ 、$x^2 - 3y^2 = \pm 3$ から $N(\sqrt{3}) = -3$ を得るが、この方法で $N(3 + \sqrt{3}) = 6$ が得られる。問題は、この方法が適用可能な条件がはっきりしないことにある [7]。

補注 2: $x^2 - 3y^2 = k$ の解は、k が次の場合には存在しない:
$k \equiv 3 \pmod 4$ の場合: なぜなら $x^2 + y^2 \not\equiv 3 \pmod 4$
$k \equiv 2 \pmod 3$ の場合: なぜなら $x^2 \not\equiv 2 \pmod 3$

以上より、次の k では解が存在しない: $k = 2, 3, \pm 5, \pm 7, 8, 11, 14, \pm 17, ...$

例 3. $x^2 - 5y^2 = k = \pm 20$

計算に必要なパラメータを整理すると次のようになる。

$$m = 5,\ d = 20,\ \varepsilon_0 = 2 + \sqrt{5},\ N(\varepsilon_0) = -1,\ p = 2,\ q = 1$$

定理 1 式 (3) より、$k = +20$ の場合 $0 \leq y < 2\sqrt{20/5}$ となる。故に $y = 0, 1, 2, 3$ を試せばよい。$k = -20$ の場合 $\sqrt{20/4} \leq y < \sqrt{20}$ となる。故に $y = 3, 4$ を試せばよい。x は $x^2 = 5y^2 \pm 20$ から求める。結果は $(x, y, k) = (0, 2, -20), (5, 1, 20), (5, 3, -20)$

補注 1: $x^2 - 5y^2 = k$ の解は、k が次の場合には存在しない:
$k \equiv 2 \pmod 4$ の場合: なぜなら $x^2 - y^2 \not\equiv 2 \pmod 4$
$k \equiv 2, 3 \pmod 5$ の場合: なぜなら $x^2 \not\equiv 2, 3 \pmod 5$

[7] $x^2 - 2y^2 = \pm 5$ は解を持たないが $x^2 - 2y^2 = \pm 25$ は解を持っている。この問題の解明にはイデアル論が要求されるのであろう

以上より、次の k では解が存在しない:
$k = \pm 2,\ \pm 3,\ \pm 6,\ \pm 7,\ \pm 8,\ \pm 10,\ \pm 12,\ \pm 13,\ \pm 14,\ \pm 17,\ \pm 18,\ ...$

補注 2: この例 3 は第 6.1 節で詳しく解説されている。また図 6.1 もこの例を扱っている。さらに例 9 では $Z^*(\sqrt{5})$ の中で、この方程式が解かれている。

例 4. $x^2 - 6y^2 = k = \pm 25$

計算に必要なパラメータを整理すると次のようになる。

$$m = 6,\ d = 25,\ \varepsilon_0 = 5 + 2\sqrt{6},\ N(\varepsilon_0) = +1,\ p = 5,\ q = 2$$

定理 1 式 (2) より、$k = +25$ の場合 $0 \leq y < 2\sqrt{25}$ となる。故に $y = 0, 1, 2, ..., 9$ を試せばよい。$k = -25$ の場合 $\sqrt{25/6} \leq y < 5\sqrt{25/6}$ となる。故に $y = 2, 3, ..., 10$ を試せばよい。これから

$$(x, y, k) = (5, 0, 25), (7, 2, 25), (11, 4, 25)$$

が得られる。

この例を出したのは、右辺が平方数の場合、あるいは平方因子を含む場合に犯しがちな誤り、すなわち x, y からその平方因子を除去して、不定方程式を簡略化する誘惑を防ぐためである。$x = 5x',\ y = 5y'$ と置くと、$x'^2 - 6y'^2 = 1$ となり、これから代表解 $x' = 1,\ y' = 0$ を得るので、$x = 5,\ y = 0$ が $x^2 - 6y^2 = \pm 25$ の代表解であると思うかも知れない。しかし、これは代表解の一部に過ぎない。

6.2.1 $x^2 - my^2 = k = \pm 4d$

$m \equiv 0, 2, 3 \pmod 4$ の場合には、易しい問題に還元できる。なぜなら x, y は次の合同式

$$x^2 \equiv my^2 \pmod 4$$

を満たさなくてはならない。

CASE $m \equiv 0 \pmod 4$: x は偶数。$m = 4m',\ x = 2x'$ と置くと、式 $x^2 - my^2 = \pm 4d$ は $x'^2 - m'y^2 = d$ に還元できる。

CASE $m \equiv 1 \pmod 4$: $x^2 \equiv y^2 \pmod 4$ ゆえ、x, y は共に偶数あるいは共に奇数。この場合、$\theta = (x + \sqrt{m}y)/2$ と置いて、式 $x^2 - my^2 = \pm 4d$ の代わりに $N(\theta\overline{\theta}) = \pm d$ となる θ を求める。

CASE $m \equiv 2, 3 \pmod 4$: x, y 共に偶数。$x = 2x',\ y = 2y'$ と置くと、式 $x^2 - my^2 = \pm 4d$ は $x'^2 - my'^2 = \pm d$ に還元できる。

例 5. $x^2 - 8y^2 = k = \pm 20$

$x = 2x'$ と置くと、$x'^2 - 2y^2 = \pm 5$ となるが、解はない。

例 6. $x^2 - 8y^2 = k = \pm 28$

$x = 2x'$ と置くと、$x'^2 - 2y^2 = \pm 7$ となる。これは $(x', y, k) = (3, 1, 7), (1, 2, -7)$ に解を持つ。従って代表解の組は $(x, y, k) = (6, 1, 28), (2, 2, -28)$ と考えたくなるが、これは $U(\sqrt{2})$ における代表解の組である。(あるいは $U^*(\sqrt{8})$ における代表解の組であると言ってもよい)

$U(\sqrt{8})$ における代表解の組は定理 1 を直接適用して得られる

$$(x, y, k) = (6, 1, 28), (2, 2, -28), (10, 3, 28), (10, 4, -28)$$

である。なぜなら $Z(\sqrt{8})$ の基本単数は $\varepsilon_0 = 3 + \sqrt{8}$ であり、同伴は $U(\sqrt{8})$ に基づいて考える必要がある。すると、ここに挙げた 4 つの、同伴ではない解が存在することになる。ところが $x'^2 - 2y^2 = \pm 7$ の解を求めると、$U(\sqrt{2})$ に基づいて同伴を処理することになる。実際

$$(6 + \sqrt{8})(1 + \sqrt{2}) = 10 + 4\sqrt{8}, \quad (2 + 2\sqrt{8})(1 + \sqrt{2}) = 10 + 3\sqrt{8}$$

となっている。

従って、この場合には、次のように言えば正しい: 解は

$$x + \sqrt{8}y = \pm(6 + \sqrt{8})(1 + \sqrt{2})^n \quad (n \in Z)$$
$$x + \sqrt{8}y = \pm(2 + 2\sqrt{8})(1 + \sqrt{2})^n \quad (n \in Z)$$

で表されると。

例 7. $x^2 - 6y^2 = k = \pm 20$

$x = 2x',\ y = 2y'$ と置くと、$x'^2 - 6y'^2 = \pm 5$ となる。$\varepsilon_0 = 5 + 2\sqrt{6},\ N(\varepsilon_0) = 1$ である。これを解くと、$(x', y', k) = (1, 1, 5), (7, 3, 5)$ で、従って $(x, y, k) = (2, 2, 20), (14, 6, 20)$ を得る。

補題 2. 自然数 d と、平方数ではない自然数 m を与える。$Z^*(m)$ の元 θ が

$$\theta\overline{\theta} = \pm d \tag{1}$$

を満たしているとする。以下、この θ を式 (1) の解と呼ぶ。

すると θ の $U^*(\sqrt{m})$ における同伴解 θ_0 で

$$\sqrt{d} \le \theta_0 < \epsilon_0\sqrt{d}$$

を満たすものが一つだけ存在する。ここに ϵ_0 は $Z^*(\sqrt{m})$ の基本単数である。

証明: この証明は、補題 1 の証明と基本的に同じである。単に $Z(\sqrt{m})$ を $Z^*(\sqrt{m})$ に、ε_0 を ϵ_0 に置き換えればよい。 □

この補題は代表解の組を $\sqrt{d} \le x + \sqrt{m}y < \epsilon_0\sqrt{d}$ の範囲に求めるのに使える。

定理 2. m は平方数ではない自然数で、$m \equiv 1 \pmod 4$ とする。また d を自然数とする。不定方程式

$$x^2 - my^2 = \pm 4d \tag{1}$$

は自然数解を持つとする。すると $N(\epsilon_0) = +1$ の場合は

$$\begin{aligned} 0 \le y < q\sqrt{d} \qquad & \text{if} \quad k > 0 \\ 2\sqrt{d/m} \le y < p\sqrt{d/m} \qquad & \text{if} \quad k < 0 \end{aligned} \tag{2}$$

$N(\epsilon_0) = -1$ の場合は

$$\begin{aligned} 0 \le y < p\sqrt{d/m} \qquad & \text{if} \quad k > 0 \\ 2\sqrt{d/m} \le y < q\sqrt{d} \qquad & \text{if} \quad k < 0 \end{aligned} \tag{3}$$

の範囲に代表解を求めることができる [8]。ここに ϵ_0 は $Z^*(\sqrt{m})$ の単数で $\epsilon_0 = (p + q\sqrt{m})/2$ としている。

証明: 証明の方法は定理 1 とほとんど同じなので、違う部分のみを書く。同様に $r = q\sqrt{m}$ と置く。

まず単数の形が違うので、今度は

$$\epsilon_0 + \overline{\epsilon}_0 = p, \quad \epsilon_0 - \overline{\epsilon}_0 = r$$

[8] この定理の式 (2) と等価な記述は、高木 p.224 にある。高木はこれを「根原解」と名付けたのである

となる。$P_0,\ Q_0$ は定理 1 と同じである。しかし $P_1,\ Q_1$ は、直線 $x+\sqrt{m}y=\epsilon_0\sqrt{d}$ と双曲線 $x^2-my^2=\pm 4d$ との交点に選ばなくてはならない。

$N(\epsilon_0)=+1$ の場合:

$$\epsilon_0+\frac{1}{\epsilon_0}=\epsilon_0+\overline{\epsilon}_0=p$$
$$\epsilon_0-\frac{1}{\epsilon_0}=\epsilon_0-\overline{\epsilon}_0=r$$
$$P_1=(p\sqrt{d},\ r\sqrt{d/m}),\quad Q_1=(r\sqrt{d},\ p\sqrt{d/m})$$

$N(\epsilon_0)=-1$ の場合:

$$\epsilon_0+\frac{1}{\epsilon_0}=\epsilon_0-\overline{\epsilon}_0=r$$
$$\epsilon_0-\frac{1}{\epsilon_0}=\epsilon_0+\overline{\epsilon}_0=p$$
$$P_1=(r\sqrt{d},\ p\sqrt{d/m}),\quad Q_1=(p\sqrt{d},\ r\sqrt{d/m})$$

従って、以上により定理の主張を得る。 □

例 8. $x^2-5y^2=k=\pm 16$

計算に必要なパラメータを整理すると次のようになる。

$$m=5,\ d=4,\ \epsilon_0=(1+\sqrt{5})/2,\ N(\epsilon_0)=-1,\ p=1,\ q=1$$

定理 2 式 (3) より、$k=+16$ の場合 $0\le y<\sqrt{4/5}$ となる。故に $y=0$ である。$k=-16$ の場合 $2\sqrt{4/5}\le y<\sqrt{4}$ となる。故に この範囲に y の整数値はない。x は $x^2=5y^2\pm 16$ から求める。結果は $(x,y,k)=(4,0,16)$ 従って $(x,y,k)=(4,0,16)$ だけが $U^*(\sqrt{5})$ における代表解である。他の解はこれから求まる。例えば $4\epsilon_0=2+2\sqrt{5},\ (2+2\sqrt{5})\epsilon_0=6+2\sqrt{5}$ であるが、これらは $x^2-5y^2=\pm 16$ の $U(\sqrt{5})$ における代表解である。

例 9. $x^2-5y^2=k=\pm 20$

$\epsilon_0=(1+\sqrt{5})/2,\ N(\epsilon_0)=-1$ なので $k=+20$ の場合には $0\le y<\sqrt{5/5}$ である。しかし $y=0$ は解にはならない。$k=-20$ の場合には $2\sqrt{5/5}\le y<\sqrt{5}$ であり、$y=2$ を試せばよい。解 $(x,y)=(0,2)$ を得る。これだけが $U^*(\sqrt{5})$ における代表解である。他の解はこれから求まる。例えば $2\sqrt{5}\epsilon_0=5+\sqrt{5},\ (5+\sqrt{5})\epsilon_0=5+3\sqrt{5}$ であるが、これらは $x^2-5y^2=\pm 20$ の $U(\sqrt{5})$ における代表解である。

この結果は定理 1 を使った例 3 と比較すべきである。

6.3 Conrad の方法

以下に Conrad の論文 [22, 23] に載っていた定理を紹介する [9]。この定理に基づいて計算すると、$Z(\sqrt{m})$ の基本単数が正の場合には、定理 1 に比べて、試行回数が著しく改善される。他方幾つかの欠点を抱えている。また証明法も複雑で、素直ではないので、証明は省略する。代わりに、Conrad の欠点を除去した定理と証明を定理 4 として、次の節で紹介する。

解の分布は x 軸と y 軸に対称であった。定理 1 では、この事実が利用されていなかった。Conrad の定理は、この対称性を利用すれば探索範囲を著しく改善できることを示している。

定理 3. ε を $N(\varepsilon) = 1,\ \varepsilon > 1$ を満たす $Z(\sqrt{m})$ の最小の単数とする。すると $x^2 - my^2 = \pm d$ を満たす解は

$$|x| \leq \sqrt{d\varepsilon}, \quad |y| \leq \sqrt{d\varepsilon/m} \tag{1}$$

の範囲に存在する解を基に $(x + \sqrt{m}y)\varepsilon^n\ (n \in Z)$ によって得られる。

証明: 証明は長くなるので省略する □

この定理 3 と定理 1 を比較しよう。$Z(\sqrt{m})$ の基本単数 $\varepsilon_0 = p + q\sqrt{m}$ で表すと、定理 1 では、y は $N(\varepsilon_0) = +1$ の場合には $0 \leq y < p\sqrt{d/m}$ の範囲に、$N(\varepsilon_0) = -1$ の場合には $0 \leq y < q\sqrt{d}$ の範囲にあるのであった。

他方、この定理 3 の ε は、ε_0 を使って表すと

$$\varepsilon = \begin{cases} \varepsilon_0 & \text{if } N(\varepsilon_0) = +1 \\ \varepsilon_0^2 & \text{if } N(\varepsilon_0) = -1 \end{cases}$$

[9] 論文と言うより、ネット上の記事である。何らかの理由で投稿を見送ったのであろう。考えられるのは Robertson の論文 [24, 25] である。Conrad の記事 [23] には発行年が書かれていないが、2016 年にネットに上がっていることが Firefox を使えば分かる。Robertson の論文は 2004 年と 2014 年であり、この論文には定理 4 の特殊ケース $N(\varepsilon_0) = +1$ と等価な式が載っている。Conrad の方法は、この式を超えていないので、投稿を見送った可能性が高い。それにも関わらず、Conrad を採り上げたのは、筆者自身は定理 1 と定理 2 を書き上げたあと Conrad に触発され、定理 4 と定理 5 を書いた。そして第 6 章を仕上げたあとで、Robertson の論文を見つけた。そのために脚注で補足することにしたのである

である。

多くの場合、$\sqrt{\varepsilon_0} < p$ であり、p が大きくなると、この違いは大きい。従って $N(\varepsilon_0) = +1$ の場合には、定理 3 は y の上限の評価を大きく改善する。

しかし、$N(\varepsilon_0) = -1$ の場合には事情は異なる。この場合の定理 3 の y の上限は $\varepsilon_0\sqrt{d/m}$ である。$q\sqrt{m} \leq \varepsilon_0$ 故、$q\sqrt{d} = q\sqrt{m}\sqrt{d/m} \leq \varepsilon_0\sqrt{d/m}$ である。従って、定理 3 は y の上限の評価を悪くする。

Conrad の定理はもう一つの欠点を抱えている。式 (1) の解を $x + \sqrt{m}y \geq 0$ の範囲に制限したとしても、示された範囲の解の中に同伴解が存在しないと言う保証が無いことである。

例 10. $x^2 - 7y^2 = 57$

$\varepsilon_0 = 8 + 3\sqrt{7},\ N(\varepsilon_0) = 1$ である。定理 1 では $0 \leq y < 3\sqrt{57} = 22.6$、他方定理 3 では $0 \leq y < \sqrt{57\varepsilon_0/7} = 11.4$ となる。

定理 1 から得られる解 (代表解の組) は

$$(x, y) = (8, 1), (13, 4), (20, 7), (43, 16)$$

に対して、定理 3 から得られる解は

$$(x, y) = (\pm 8, \pm 1), (\pm 13, \pm 4), (\pm 20, \pm 7)$$

である。定理 1 では代表解の組を求めているのに対して、Conrad の方は式 (1) を満たす解を条件式 (1) の範囲で求めているために $\pm$ が付加されている。ところが $20 + 7\sqrt{7} = (13 - 4\sqrt{7})(8 + 3\sqrt{7})$ であることから分かるように、定理 3 の解には $x + \sqrt{7}y \geq 0$ の範囲にも同伴のものが含まれている。このことは、条件式 (1) の y の範囲が広すぎることを意味している。

例 11. $x^2 - 34y^2 = k = \pm 18$

$\sqrt{34} = [5, \overline{1, 4, 1, 10}]$ より $p/q = [5, 1, 4, 1]$ とすると、$p = 35,\ q = 6$ である。これから $\varepsilon_0 = 35 + 6\sqrt{34},\ N(\varepsilon_0) = 1$ を得る。従って定理 1 を使うと $0 \leq y < 35\sqrt{18/34}$ の範囲が得られる。故に $y = 1, 2, ..., 25$ を試せばよい。結果は $(x, y, k) = (18, 3, 18), (4, 1, -18), (64, 11, -18)$ である。

Conrad の方法では $|y|$ の範囲は $|y| = 0, 1, ..., 6$ になる。
なぜなら $u = (35 + 6\sqrt{34})$ 故　$|y| \leq \sqrt{18u/34} = 6.09$ である。条件式 (1) を満たす解は $(x, y) = (\pm 4, \pm 1), (\pm 18, \pm 3)$ である。なお定理 1 の結果の $(x, y) = (64, 11)$ は $(x, y) = (4, -1)$ から得られる。

例 12. $x^2 - 5y^2 = k = \pm 20$

$$m = 5, \quad d = 20, \quad \varepsilon_0 = 2 + \sqrt{5}, \quad \varepsilon = \varepsilon_0^2, \quad |y| \leq \varepsilon_0 \sqrt{d/m} = 8.47$$

この結果は、例 3 の定理 1 を使った場合の試行範囲 $0 \leq y \leq 4$ に比べても悪くなっている。

6.4 解法 II

ここでは Conrad の方法の欠点を含まない新しい方法を紹介する。

定理 1 により得られる解は、この (a) と (b) を満たしている。Conrad の方法は、$Z(\sqrt{m})$ の基本単数が正の場合には、定理 1 に比べて、試行回数を大きく改善する。しかしながら基本単数が負の場合は、逆に、悪くなる。さらにもっと悪いことには代表解の組の条件 (a) を満たしていない。従って Conrad の方法で解を求めても、さらに条件 (a) を満たすように、解を選別しなくてはならないのである。定理 4 による解法 II は、こうした問題点を解決している。

補題 3. 自然数 d と、平方数ではない自然数 m を与える。$Z(\sqrt{m})$ の元 θ が

$$\theta\overline{\theta} = \pm d \tag{1}$$

を満たしているとする。以下、この θ を式 (1) の解と呼ぶ。

すると θ の $U(\sqrt{m})$ における同伴解 θ_0 で

$$\sqrt{d/\varepsilon_0} \leq \theta_0 < \sqrt{d\varepsilon_0}$$

を満たすものが一つだけ存在する。ここに ε_0 は $Z(\sqrt{m})$ の基本単数である。

証明: $\theta' = \pm\varepsilon_0^n\theta$ $(n \in Z)$ はどれも $U(\sqrt{m})$ における θ の同伴解である。そのうち、$\theta' \geq \sqrt{d/\varepsilon_0}$ となる最小の θ' を選び、それを θ_0 とする。すると $\theta_0 < \sqrt{d\varepsilon_0}$ が成り立つ。なぜなら、仮に $\theta_0 \geq \sqrt{d\varepsilon_0}$ とすると $\varepsilon_0 > 1$ 故

$$\theta_0 > \frac{\theta_0}{\varepsilon_0} \geq \sqrt{d/\varepsilon_0}$$

となる。そして

$$\frac{\theta_0}{\varepsilon_0} = \pm\theta_0\overline{\varepsilon}_0$$

である。この $\pm$ の符号は $N(\varepsilon_0) = \varepsilon_0\overline{\varepsilon}_0 = \pm 1$ の符号に対応している。$+1$ の場合には $\overline{\varepsilon}_0 > 0$ であるが、-1 の場合には $\overline{\varepsilon}_0 < 0$ である。何れにせよ、

$\theta_0' = \theta_0/\varepsilon_0 = \pm\theta_0\bar{\varepsilon}_0 \in Z(\sqrt{m})$ は $\theta_0' \geq \sqrt{d/\varepsilon_0}$ と $N(\theta_0') = \pm 1$ を満たし、θ_0 より小さい。つまり最初の仮定に反する。

「一つだけ」は次のように示される。仮に θ の同伴解 θ' で $\theta_0 < \theta' < \sqrt{d\varepsilon_0}$ となるものが存在するとすれば、θ' は $Z(\sqrt{m})$ の単数 ε を使って $\theta' = \varepsilon\theta_0$ と表されることとなる。すると $\theta_0 < \varepsilon\theta_0 < \sqrt{d\varepsilon_0}$ である。ところが θ_0 は $\theta_0 \geq \sqrt{d/\varepsilon_0}$ を満たすように選ばれたのであった。従って $\varepsilon < \sqrt{d\varepsilon_0}/\theta_0 < \varepsilon_0$ となるが、これは ε_0 が基本単数であるとする前提に反する。 □

この補題は代表解の組を $\sqrt{d/\varepsilon_0} \leq x + \sqrt{m}y < \sqrt{d\varepsilon_0}$ の範囲に求めるのに使える。

定理 4. ε_0 は $Z(\sqrt{m})$ の基本単数で $\varepsilon_0 = p + q\sqrt{m}$ とする。すると $x^2 - my^2 = k\ (= \pm d)$ の代表解は、$r = q\sqrt{m}$ として、a, b を

$$a = \begin{cases} \sqrt{d(p+1)/2} & \text{if} \quad N(\varepsilon_0) = +1 \\ \sqrt{d(r+1)/2} & \text{if} \quad N(\varepsilon_0) = -1 \end{cases}$$

$$b = \begin{cases} \sqrt{d(p-1)/2} & \text{if} \quad N(\varepsilon_0) = +1 \\ \sqrt{d(r-1)/2} & \text{if} \quad N(\varepsilon_0) = -1 \end{cases}$$

と置くと

$$-\frac{b}{\sqrt{m}} \leq y < \frac{b}{\sqrt{m}} \qquad \text{if } k > 0 \qquad (1)$$

$$\sqrt{\frac{d}{m}} \leq y \leq \frac{a}{\sqrt{m}} \quad (-b \leq x < b) \qquad \text{if } k < 0 \qquad (2)$$

の範囲に求めることができる [10]。

証明: 証明は定理 1 とほぼ同じ。定理 1 との違いだけを述べる。$c_0 = \sqrt{d/\varepsilon_0},\ c_1 = \sqrt{d\varepsilon_0}$ とする。代表解の存在範囲は、直線 $x + \sqrt{m}y = c_0$ と直線 $x + \sqrt{m}y = c_1$ に囲まれた領域である。そこで直線 $x + \sqrt{m}y = c_0$ と、双曲線 $x^2 - my^2 = \pm d$ の交点を各々 $P_0,\ Q_0$ とし、また直線 $x + \sqrt{m}y = c_1$ と、双曲線 $x^2 - my^2 = \pm d$

[10] Robertson の論文に $N(\varepsilon_0) = +1$ のケースが載っている [24, 25]。高木もそうであるが、Conrad も Robertson も基本単数が -1 のケースの扱いが悪い。簡単に理論の中に組み込めるのに不思議である

の交点を各々 $P_1,\ Q_1$ とする (図 6.3)。すると

$$P_0 = (a, -\frac{b}{\sqrt{m}}), \quad Q_0 = (-b,\ \frac{a}{\sqrt{m}})$$
$$P_1 = (a, +\frac{b}{\sqrt{m}}), \quad Q_1 = (+b,\ \frac{a}{\sqrt{m}})$$

となる。P_0 と P_1 は x 軸に対称に、Q_0 と Q_1 は y 軸に対称になることに注目しよう。ここに a, b は

$$a = \frac{\sqrt{d}}{2}(\sqrt{\varepsilon_0} + \frac{1}{\sqrt{\varepsilon_0}}), \quad b = \frac{\sqrt{d}}{2}(\sqrt{\varepsilon_0} - \frac{1}{\sqrt{\varepsilon_0}})$$

である。そして $r = q\sqrt{m}$ と置くと

$$(\sqrt{\varepsilon_0} + \frac{1}{\sqrt{\varepsilon_0}})^2 = \varepsilon_0 + \frac{1}{\varepsilon_0} + 2 = \begin{cases} \varepsilon_0 + \overline{\varepsilon}_0 + 2 = 2p + 2 & \text{if} \quad N(\varepsilon_0) = +1 \\ \varepsilon_0 - \overline{\varepsilon}_0 + 2 = 2r + 2 & \text{if} \quad N(\varepsilon_0) = -1 \end{cases}$$

$$(\sqrt{\varepsilon_0} - \frac{1}{\sqrt{\varepsilon_0}})^2 = \varepsilon_0 + \frac{1}{\varepsilon_0} - 2 = \begin{cases} \varepsilon_0 + \overline{\varepsilon}_0 - 2 = 2p - 2 & \text{if} \quad N(\varepsilon_0) = +1 \\ \varepsilon_0 - \overline{\varepsilon}_0 - 2 = 2r - 2 & \text{if} \quad N(\varepsilon_0) = -1 \end{cases}$$

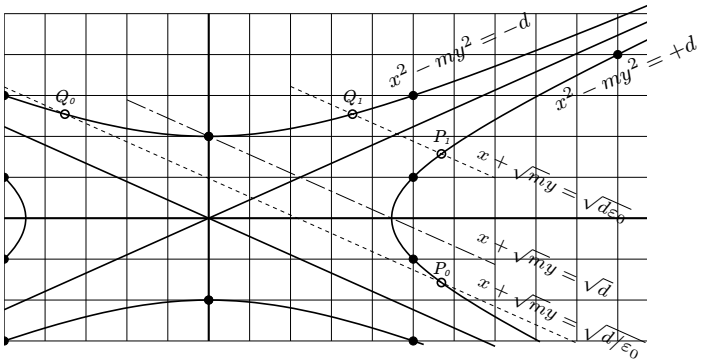


図 6.3: 代表解の範囲例 $(m, d) = (5, 20)$

従って定理の主張を得る。なお、この範囲にある解は同伴にならないことは補題 3 から明らか。 □

補注: 式 (1) において $b/\sqrt{m}$ が整数の場合にだけ等号が必要になる。この式は $-b/\sqrt{m} < y \leq b/\sqrt{m}$ でもよい。式 (2) においても $a/\sqrt{m}$ が整数の場合にだけ「$(-b \leq x < b)$」の部分が必要になる。その場合、等号はどちらに付いてもよい。

図 6.3 には例として $x^2 - 5y^2 = \pm 20$ が描かれている。整数解は黒丸で示されている。白丸は P_0, P_1, Q_0, Q_1 である。P_0, Q_0 は、直線 $x + \sqrt{m}y = \sqrt{d/\varepsilon_0}$ (破線で示されている) と双曲線との交点である。また P_1, Q_1 は、直線 $x + \sqrt{m}y = \sqrt{d\varepsilon_0}$ (破線で示されている) と双曲線との交点である。参考のために、直線 $x + \sqrt{m}y = \sqrt{d}$ も一点破線で示されている。

定理 4 は定理 1 の良い面を引き継いでおり、さらに Conrad を次の点で改善している。

- $N(\varepsilon_0) = -1$ の場合も試行範囲を大きく狭めている
- 同伴解を含まない

例 13. $x^2 - 5y^2 = \pm 20$

$$m = 5, \quad d = 20, \quad \varepsilon_0 = 2 + \sqrt{5}, \quad N(\varepsilon_0) = -1, \quad r = \sqrt{5}$$
$$a = \sqrt{10(r+1)}, \quad b = \sqrt{10(r-1)}$$
$$a/\sqrt{m} = 2.54, \quad b/\sqrt{m} = 1.57, \quad \sqrt{d/m} = 2$$

従って $k > 0$ では $|y| = 0, 1$ を試し $(x, y) = (5, \pm 1)$ を得る。また $k < 0$ では $y = 2$ を試し $(x, y) = (0, 2)$ を得る。

例 14. $x^2 - 73y^2 = k = \pm 8$

$$m = 73, \quad d = 8, \quad \varepsilon_0 = 1068 + 125\sqrt{73}, \quad N(\varepsilon_0) = -1, \quad r = 125\sqrt{73}$$
$$a = \sqrt{4(r+1)}, \quad b = \sqrt{4(r-1)}$$
$$a/\sqrt{m} = 7.65, \quad b/\sqrt{m} = 7.65, \quad \sqrt{d/m} = 0.33$$

従って $k > 0$ で $|y| = 0, 1, ..., 7$ を、$k < 0$ で $y = 1, 2, ..., 7$ を試せばよいが、これから $x = 9,\ y = \pm 1$ を得る。

補題 4. 自然数 d と、平方数ではない自然数 m を与える。$Z^*(m)$ の元 θ が

$$\theta\overline{\theta} = \pm d \tag{1}$$

を満たしているとする。以下、この θ を式 (1) の解と呼ぶ。

すると θ の $U^*(\sqrt{m})$ における同伴解 θ_0 で

$$\sqrt{d/\epsilon_0} \le \theta_0 < \sqrt{d\epsilon_0}$$

を満たすものが一つだけ存在する。ここに ϵ_0 は $Z^*(\sqrt{m})$ の基本単数である。

証明: この証明は、補題3の証明と基本的に同じである。単に $Z(\sqrt{m})$ を $Z^*(\sqrt{m})$ に、ε_0 を ϵ_0 に置き換えればよい。 □

この補題は不定方程式 $x^2 - my^2 = \pm 4d$ の代表解の組を $2\sqrt{d/\epsilon_0} \le x + \sqrt{m}y < 2\sqrt{d\epsilon_0}$ の範囲に求めるのに使える。

定理 5. m は平方数ではない自然数で、$m \equiv 1 \pmod 4$ とする。また d を自然数とする。ϵ_0 は $Z^*(\sqrt{m})$ の基本単数で $\epsilon_0 = (p + q\sqrt{m})/2$ とする。すると $x^2 - my^2 = k\ (= \pm 4d)$ の代表解は、$r = q\sqrt{m}$ として、a, b を

$$a = \begin{cases} \sqrt{d(p+2)} & \text{if} \quad N(\epsilon_0) = +1 \\ \sqrt{d(r+2)} & \text{if} \quad N(\epsilon_0) = -1 \end{cases}$$

$$b = \begin{cases} \sqrt{d(p-2)} & \text{if} \quad N(\epsilon_0) = +1 \\ \sqrt{d(r-2)} & \text{if} \quad N(\epsilon_0) = -1 \end{cases}$$

と置くと

$$-\frac{b}{\sqrt{m}} \le y < \frac{b}{\sqrt{m}} \qquad \text{if } k > 0 \qquad (1)$$

$$2\sqrt{\frac{d}{m}} \le y \le \frac{a}{\sqrt{m}} \quad (-b \le x < b) \qquad \text{if } k < 0 \qquad (2)$$

の範囲に求めることができる。

証明: 証明は定理 1 とほぼ同じ。定理 1 との違いだけを述べる。

$c_0 = \sqrt{d/\epsilon_0},\ c_1 = \sqrt{d\epsilon_0}$ とする。代表解の存在範囲は、直線 $x + \sqrt{m}y = 2c_0$ と直線 $x + \sqrt{m}y = 2c_1$ に囲まれた領域である。そこで直線 $x + \sqrt{m}y = 2c_0$ と、双曲線 $x^2 - my^2 = \pm 4d$ の交点を各々 $P_0,\ Q_0$ とし、また直線 $x + \sqrt{m}y = 2c_1$

と、双曲線 $x^2 - my^2 = \pm 4d$ の交点を各々 $P_1,\ Q_1$ とする (図 6.4)。すると

$$P_0 = (a, -\frac{b}{\sqrt{m}}), \quad Q_0 = (-b,\ \frac{a}{\sqrt{m}})$$
$$P_1 = (a, +\frac{b}{\sqrt{m}}), \quad Q_1 = (+b,\ \frac{a}{\sqrt{m}})$$

となる。P_0 と P_1 は x 軸に対称に、Q_0 と Q_1 は y 軸に対称になることに注目しよう。ここに a, b は

$$a = \sqrt{d}(\sqrt{\epsilon_0} + \frac{1}{\sqrt{\epsilon_0}}), \quad b = \sqrt{d}(\sqrt{\epsilon_0} - \frac{1}{\sqrt{\epsilon_0}})$$

である。そして $r = q\sqrt{m}$ と置くと

$$(\sqrt{\epsilon_0} + \frac{1}{\sqrt{\epsilon_0}})^2 = \epsilon_0 + \frac{1}{\epsilon_0} + 2 = \begin{cases} \epsilon_0 + \bar{\epsilon}_0 + 2 = p + 2 & \text{if} \quad N(\epsilon_0) = +1 \\ \epsilon_0 - \bar{\epsilon}_0 + 2 = r + 2 & \text{if} \quad N(\epsilon_0) = -1 \end{cases}$$

$$(\sqrt{\epsilon_0} - \frac{1}{\sqrt{\epsilon_0}})^2 = \epsilon_0 + \frac{1}{\epsilon_0} - 2 = \begin{cases} \epsilon_0 + \bar{\epsilon}_0 - 2 = p - 2 & \text{if} \quad N(\epsilon_0) = +1 \\ \epsilon_0 - \bar{\epsilon}_0 - 2 = r - 2 & \text{if} \quad N(\epsilon_0) = -1 \end{cases}$$

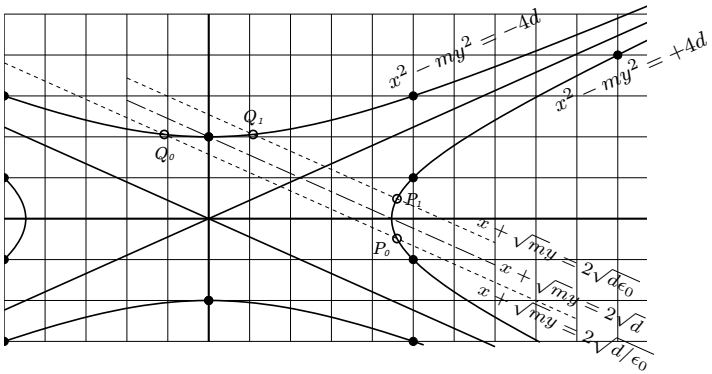


図 6.4: 代表解の範囲 $(m, d) = (5, 5)$

従って定理の主張を得る。なお、この範囲にある解は同伴にならないことは補題 3 から明らか。 □

補注: 式 (1) において $b/\sqrt{m}$ が整数の場合にだけ等号が必要になる。この式は $-b/\sqrt{m} < y \leq b/\sqrt{m}$ でもよい。式 (2) においても $a/\sqrt{m}$ が整数の場合にだけ「$(-b \leq x < b)$」の部分が必要になる。その場合、等号はどちらに付いてもよい。

例 15. $x^2 - 61y^2 = \pm 12$

計算に必要なパラメータを整理すると次のようになる。

$$m = 61,\ d = 3,\ \epsilon_0 = (39 + 5\sqrt{61})/2,\ N(\epsilon_0) = -1,\ p = 39,\ q = 5$$

ϵ_0 の値は、付録 A に載っている。これから

$$b/\sqrt{m} = 1.35,\ a/\sqrt{m} = 1.42,\ 2\sqrt{d/m} = 0.44$$

を得る。従って $k > 0$ の場合には $y = 0, 1$ を、$k < 0$ の場合には $y = 1$ 試せばよいことが分かる。結果は $(x, y, k) = (\pm 7, 1, -12)$ である。

この例題を他の方法と比較しよう。まず定理 1 を使った場合には

$$m = 61,\ d = 12,\ \varepsilon_0 = 29718 + 3805\sqrt{61},\ N(\varepsilon_0) = -1,\ p = 29718,\ q = 3805$$

である。ε_0 の値は、付録 D に載っている。この値が、かくも大きくなるのは $\sqrt{61}$ の連分数の周期が長いからである (付録 B)。定理 1 の式 (3) を使って y の範囲を求めると $k > 0$ の場合、$y = 0, 1, 2, ..., 13180$ を試さなくてはならない。また $k < 0$ の場合も, $y = 1, 2, ..., 13180$ である。これらの合計が、たったの 3 つに減少したのであるから、定理 5 の凄さが分かるであろう。

次に定理 2 と比較しよう。定理 2 では定理 5 と同じパラメータ

$$m = 61,\ d = 3, \epsilon_0 = (39 + 5\sqrt{61})/2,\ N(\epsilon_0) = -1,\ p = 39,\ q = 5$$

が使われる。結局 $k > 0$ の場合 $y = 0, 1, 2, ..., 8$ を、$k < 0$ の場合も $y = 1, 2, ..., 8$ を試すことになる。定理 1 に比べると驚異的に改善されているが、定理 5 には及ばない。

もしも $N(\epsilon) = 1$ の単数の利用に拘るなら、そのような単数で効率的に計算できるものは $\varepsilon = \epsilon_0^2 = (1523 + 196\sqrt{61})/2$ であり、計算に必要なパラメータは今度は $m = 61,\ d = 3,\ p = 1523,\ q = 196$ となる。従って $k > 0$ の場合には $y = 0, 1, 2, ..., 339$ を、$k < 0$ の場合も $y = 1, 2, ..., 337$ を試すことになる。

次に Conrad の方法 (定理 3) と比較しよう。Conrad の方法では $N(\varepsilon) = +1$ の単数が要求される。そのような単数で効率的に計算できるものは $\varepsilon = \varepsilon_0^2$ で

あり、これは $\varepsilon = 1766319049 + 226153980\sqrt{61}$ である。従って、試すべき y は $y = 0, 1, 2, ..., 26361$ となるが、定理 1 よりも悪くなっている。

次に定理 4 と比較しよう。計算に必要なパラメータは

$$m = 61,\ d = 12,\ \varepsilon_0 = 29718 + 3805\sqrt{61},\ N(\varepsilon_0) = -1,\ p = 29718,\ q = 3805$$

である。これから

$$r = q\sqrt{m} = 3805\sqrt{61},\ a = \sqrt{6(r+1)},\quad b = \sqrt{6(r-1)}$$
$$a/\sqrt{m} = 54.07,\quad b/\sqrt{m} = 54.06,\quad \sqrt{d/m} = 0.44$$

を得る。その結果 $k > 0$ で $y = 0, 1, 2, ..., 54$ を、$k < 0$ でも $y = 1, 2, ..., 54$ を試すことになる。

もしも $N(\varepsilon) = 1$ の単数の利用に拘るなら、そのような単数で効率的に計算できるものは $\varepsilon = \varepsilon_0^2$ であり、これは $\varepsilon = 1766319049 + 226153980\sqrt{61}$ である。この場合

$$p = 1766319049,\quad a = \sqrt{6(p+1)},\quad b = \sqrt{6(p-1)}$$
$$a/\sqrt{m} = 13180.91,\quad b/\sqrt{m} = 13180.91,\quad \sqrt{d/m} = 0.44$$

となる。これから $k > 0$ で $y = 0, 1, 2, ..., 13180$ を、$k < 0$ でも $y = 1, 2, ..., 13180$ を試すことになる。これは (結果的には) 定理 1 と変わらない。

6.5 補足

一般 Pell 方程式 $x^2 - my^2 = k\ (= \pm d)$ の代表解の例を付録 F に載せておく。ここには $m = 2, ..., 10$ の各々について $d = 2, ..., 50$ の代表解が載っている。もっと多くの例 ($m = 2, ..., 99,\ d = 2, ..., 999$) が筆者のサーバにあるが [11]、興味を持たれた読者は、それも参照されたい。

得られた結果を眺めていると幾つかの事に気がつく。例えば

(a) k が素数のときは代表解の個数は 2 を超えない。

(b) k_1, k_2 を相異なる素数として、$k = k_1 k_2$ の解が存在し $k = k_1$ の解が存在すれば $k = k_2$ の解も存在する。

[11] http://ar.nyx.link/cf/

などである。(a) の性質はイデアル論を使えば容易に証明できる。(b) の性質の証明には環論に関するもう少し深い議論が要求される。ここでは、k と代表解の有無の関係を問題にするが、比較的容易に証明できる範囲に議論を留めておく [12]。

証明を容易にするために θ' を次のように定義する: $\theta = x + y\sqrt{m} \in Q(\sqrt{m})$ について $\theta\overline{\theta} > 0$ なら $\theta' = \overline{\theta} = x - y\sqrt{m}$ とし、$\theta\overline{\theta} < 0$ なら $\theta' = -\overline{\theta} = -x + \sqrt{m}$ とする。あるいは、符号関数 $\mathrm{sgn}(x)$ を使って 2 つのケースを纏めると $\theta' = \mathrm{sgn}(\theta\overline{\theta})\overline{\theta}$ である [13]。

すると $\theta\theta' > 0$ であり、特に $\theta = \theta'$ であれば $\theta = x$ あるいは $\theta = y\sqrt{m}$ である。また方程式 $x^2 - my^2 = k$ は $\theta\theta' = |k|$ である。

補題 5. 次の関係が成立する:

(a) $a' = a \quad (a \in Q)$
(b) $(\theta')' = \theta$
(c) $(\alpha\beta)' = \alpha'\beta'$

証明: (a) は自明。(b) と (c) は

$$(\theta')' = (\mathrm{sgn}(\theta\overline{\theta})\overline{\theta})' = \mathrm{sgn}(\theta\overline{\theta})^2\overline{\overline{\theta}} = \theta$$
$$(\alpha\beta)' = \mathrm{sgn}(\alpha\beta\overline{\alpha\beta})\overline{\alpha\beta} = \mathrm{sgn}(\alpha\overline{\alpha})\overline{\alpha}\,\mathrm{sgn}(\beta\overline{\beta})\overline{\beta} = \alpha'\beta'$$

である。 □

そこで定理 4 に戻り、$Z(\sqrt{m})$ における方程式 $\theta\theta' = |k|$ の解の一つを θ とする。一般性を失わずに $\theta' \le \theta$ と考えてよい。もしも $\theta' > \theta$ となっていれば、θ と θ' を入れ替えればよい。そこで以下では $\theta' \le \theta$ とする。補題 3 により

$$\sqrt{\frac{|k|}{\varepsilon_0}} \le \theta' \le \theta < \sqrt{|k|\varepsilon_0}$$

である。

[12] 代表解の個数との関係の方が面白いであろうが、イデアル論の中で論じるほうが自然であろう
[13] $\sqrt{m}$ は無理数であるとしている。すると $\theta\overline{\theta} = 0$ の場合は $\theta = \overline{\theta} = 0$ であり、$\theta' = \mathrm{sgn}(\theta\overline{\theta})\overline{\theta}$ は自然に成立する。

$\theta\theta' = |k|$ であるから、$\theta' < \theta$ の場合には $\theta' < \sqrt{|k|} < \theta$ である。故に θ と θ' が共に代表解の領域に含まれていれば

$$\frac{1}{\sqrt{\varepsilon_0}} < \frac{\theta'}{\sqrt{|k|}} < 1 < \frac{\theta}{\sqrt{|k|}} < \sqrt{\varepsilon_0}$$

が成り立つ。$\theta' = \theta$ の場合には、

$$\frac{1}{\sqrt{\varepsilon_0}} < \frac{\theta'}{\sqrt{|k|}} = 1 = \frac{\theta}{\sqrt{|k|}} < \sqrt{\varepsilon_0}$$

が成り立つ。

$1/\sqrt{\varepsilon_0} = \theta'/\sqrt{|k|}$ の場合には、$\theta\theta' = |k|$ の条件から、$\sqrt{\varepsilon_0} = \theta/\sqrt{|k|}$ となり、θ が代表解の領域に入らない。この場合、$\theta \sim \theta'$ である。なぜなら $\theta = \theta'\varepsilon_0$ が成り立つ。θ' が領域境界にあり、そのために θ が領域に含まれないのである。

特殊なケース $\theta = \theta'$ および $1/\sqrt{\varepsilon_0} = \theta'/\sqrt{|k|}$ を発生させる k の特徴を調べよう。$\theta = \theta'$ の場合には $|k| = x^2$ あるいは $|k| = my^2$ である。従って k あるいは k/m が平方数であるか否かによって容易に判別できる。しかし $1/\sqrt{\varepsilon_0} = \theta'/\sqrt{|k|}$ は少し複雑である。

$Z(\sqrt{m})$ の基本単数を $\varepsilon_0 = p + q\sqrt{m}$ とする。$\theta = x + y\sqrt{m}$ について $\theta = \theta'\varepsilon_0$ となる条件は

$$(p+1)y = qx, \quad (p-1)x = mqy \qquad \text{if } \theta\overline{\theta} > 0$$

$$(p-1)y = qx, \quad (p+1)x = mqy \qquad \text{if } \theta\overline{\theta} < 0$$

である。従って $xy \neq 0$ であれば、何れの場合も $p^2 - 1 = mq^2$ すなわち $N(\varepsilon_0) = 1$ が必要である。

$\theta\overline{\theta} > 0$ の場合は $x = (p+1)t,\ y = qt$ と置く、$\theta\overline{\theta} < 0$ の場合は $x = (p-1)t,\ y = qt$ と置く。これから $N(\varepsilon_0) = 1$ を考慮して

$$k = \theta\overline{\theta} = \begin{cases} 2(p+1)t^2 & \text{for } \theta\overline{\theta} > 0 \\ -2(p-1)t^2 & \text{for } \theta\overline{\theta} < 0 \end{cases}$$

が得られる。t は x, y が共に整数となる有理数から選ばれる。

例 1. $m = 7$ の場合 $\varepsilon_0 = 8 + 3\sqrt{7}$、従って $p = 8,\ q = 3,\ e = +1$ である。$k > 0$ の場合 $x = 9t,\ y = 3t$ 故、$t = n/3\ (n = 1, 2, 3, ...)$ と置くと、$k = 2n^2$ を得る。$k < 0$ の場合 $x = 7t,\ y = 3t$ 故、$t = n\ (n = 1, 2, 3, ...)$ と置くと、$k = -14n^2$ を得る

補題 6. 一般 Pell 方程式 $x^2 - my^2 = k$ が解 (x, y) を持つような k の集合を $S(m)$ とする。すると $a, b \in S(m)$ ならば $ab \in S(m)$ である。

証明: $a, b \in S(m)$ とすると、$\alpha\overline{\alpha} = a,\ \beta\overline{\beta} = b$ となる $\alpha, \beta \in Z(\sqrt{m})$ が存在する。すると $\alpha\overline{\alpha}\beta\overline{\beta} = ab$ であるから

$$\gamma_1 = \alpha\beta, \quad \gamma_2 = \alpha\overline{\beta}, \quad \gamma_3 = \overline{\alpha}\beta, \quad \gamma_4 = \overline{\alpha}\overline{\beta}$$

は $\gamma_i\overline{\gamma}_i = ab$ を満たす。つまり $ab \in S(m)$ である。 □

補題 3 に基づいて、一般 Pell 方程式 $x^2 - my^2 = k$ の代表解の組を

$$\frac{1}{\sqrt{\varepsilon_0}} \leq \frac{\theta}{\sqrt{|k|}} < \sqrt{\varepsilon_0} \tag{6.3}$$

の領域に求める。ここに ε_0 は $Z(\sqrt{m})$ の単数であり $\theta = x + y\sqrt{m}$ とした。方程式は $\theta\overline{\theta} = k$ と等価である。この領域に θ が存在する k の集合を $S_0(m)$ とする。 $S_0(m) \subset S(m)$ である。$S_0(m)$ の例を次の表に示す [14]:

表 6.1: 集合 $S_0(m)$

m	$N(\varepsilon_0)$	$S_0(m)$
2	-1	$-2, 4, -7, -8, 9, 14, 16, -17, -18, 23, 25, -28, -31, -32, ...$
3	$+1$	$-2, -3, 4, 6, -8, 9, -11, -12, 13, 16, -18, 22, -23, 24, 25, ...$
5	-1	$\pm4, -5, 9, 11, \pm16, -19, \pm20, 25, -29, 31, \pm36, -41, \pm44, ...$
6	$+1$	$-2, 3, 4, -5, -6, -8, 9, 10, 12, -15, 16, -18, 19, -20, -23, ...$
7	$+1$	$2, -3, 4, -6, -7, 8, 9, -12, -14, 16, 18, -19, 21, -24, 25, ...$
8	$+1$	$\pm4, -7, \pm8, 9, \pm16, 17, -23, 25, \pm28, -31, \pm32, \pm36, 41, ...$
10	-1	$4, -6, \pm9, -10, 15, 16, -24, 25, 26, -31, \pm36, \pm39, -40, ...$

$S(m)$ は $S_0(m)$ から次のように得られる。$N(\varepsilon_0)$ が $+1$ であれば $S(m) = S_0(m)$ である。なぜなら単数 ε_0 を θ に乗じても k は変化しないから。しかし -1 であれば $S(m)$ の元は全て $\pm$ を要する。なぜなら単数 ε_0 を θ に乗じると k の符号は変化するから。

定理 6. $a, b \in S_0(m)$ ならば $ab \in S_0(m)$ である。

証明: $a, b \in S_0(m)$ 故、$\alpha\overline{\alpha} = a,\ \beta\overline{\beta} = b$ となる $\alpha, \beta \in Z(\sqrt{m})$ が存在する。

[14] この表は付録 F より得られる

$\alpha' \leq \alpha$, $\beta' \leq \beta$ とすると、

$$\sqrt{\frac{|a|}{\varepsilon_0}} \leq \alpha' \leq \sqrt{|a|}$$

$$\sqrt{|b|} \leq \beta < \sqrt{|b|\varepsilon_0}$$

となる。従って $\sqrt{|ab|/\varepsilon_0} \leq \alpha'\beta < \sqrt{|ab|\varepsilon_0}$ となる。同様に $\sqrt{|ab|/\varepsilon_0} \leq \alpha\beta' < \sqrt{|ab|\varepsilon_0}$ も得られる。従って $\gamma = \alpha'\beta$ または $\gamma = \alpha\beta'$ と置くと $\sqrt{|ab|/\varepsilon_0} \leq \gamma < \sqrt{|ab|\varepsilon_0}$ である。そして $\gamma\gamma' = \alpha\alpha'\beta\beta' = |ab|$ であるから $\gamma\overline{\gamma} = ab$ であり $ab \in S_0(m)$ である。 □

例 2. $x^2 - 7y^2 = \pm 6$ について考えてみよう。表から $x^2 - 7y^2 = 2$ の解と $x^2 - 7y^2 = -3$ の解が存在することが分かる。この場合、定理 6 は $x^2 - 7y^2 = (2) \cdot (-3) = -6$ の解も存在することを主張している。実際、この主張は、表 6.1 から確認できる。

付録

A 有理数の連分数

ここでは有理数の連分数 $p/q = [n_1, n_2, ..., n_l]$ について考えてみる。

問題 p を与えて、その下で q を $q = 2, ..., p-1$ と変える。すると連分数の長さ l を最大にする q は p といかなる関係にあるか? また、そのときの l は p といかなる関係にあるか?

この疑問に答えるために、$p = 19$ と $q = 2, ..., 18$ の連分数の計算例を示す。計算の方法は本文の互除法の式 (1.1) に基づいている。この例は、この問題を考える上でのヒントになろう。

```
19 2 [9, 2]
19 3 [6, 3]
19 4 [4, 1, 3]
19 5 [3, 1, 4]
19 6 [3, 6]
19 7 [2, 1, 2, 2]
19 8 [2, 2, 1, 2]
19 9 [2, 9]
19 10 [1, 1, 9]
19 11 [1, 1, 2, 1, 2]
19 12 [1, 1, 1, 2, 2]
19 13 [1, 2, 6]
19 14 [1, 2, 1, 4]
19 15 [1, 3, 1, 3]
19 16 [1, 5, 3]
19 17 [1, 8, 2]
19 18 [1, 18]
```

連分数の計算結果を $[n_0, n_1, ..., n_l]$ とすると、この例では、どれも $n_l \neq 1$ である。実は、これは一般的な性質である。理由は明らかである。式 (1.1) の一部を引用すると

$$x_{l-1} = n_{l-1}x_l + x_{l+1}$$

$$x_l = n_l x_{l+1} + 0$$

であるが、仮に $n_l = 1$ とすると、$x_l = x_{l+1}$ となり、x_{l+1} が x_l による除算の剰余であることから発生する制限 $x_l > x_{l+1} \geq 0$ と両立しないからである。

次に、与えられた p の下で、最大長を生成する q の例を次に示す。一般に、そのような複数の q が存在する。例えば $p = 19$ の場合には、$q = 11$ と $q = 12$ で最大長が生成される。その場合には、そのうちの 1 つが例示されている。p が Fibonacci 数 $(1, 1, 2, 3, 5, 8, 13, ...)$ の場合には、最大長を生成する q は手前の Fibonacci 数である。他の q は最大長を生成しない。p が増加していくときの、最大長の更新は Fibonacci 数と深く関係しているのである。

```
5 3 [1, 1, 2]
6 4 [1, 2]
7 4 [1, 1, 3]
8 5 [1, 1, 1, 2]
9 5 [1, 1, 4]
10 6 [1, 1, 2]
11 7 [1, 1, 1, 3]
12 7 [1, 1, 2, 2]
13 8 [1, 1, 1, 1, 2]
14 9 [1, 1, 1, 4]
15 11 [1, 2, 1, 3]
16 9 [1, 1, 3, 2]
17 10 [1, 1, 2, 3]
18 11 [1, 1, 1, 1, 3]
19 11 [1, 1, 2, 1, 2]
20 11 [1, 1, 4, 2]
21 13 [1, 1, 1, 1, 1, 2]
22 13 [1, 1, 2, 4]
23 14 [1, 1, 1, 1, 4]
24 13 [1, 1, 5, 2]
25 14 [1, 1, 3, 1, 2]
26 15 [1, 1, 2, 1, 3]
27 17 [1, 1, 1, 2, 3]
28 17 [1, 1, 1, 1, 5]
29 18 [1, 1, 1, 1, 1, 3]
```

連分数が、互除法によって発生したことを無視して、付録 C に解説されている形式的算法に従うとすれば、先に「$n_l \neq 1$」とした部分は訂正しなくてはならない: $n_l > 1$ の場合には、$[n_1, n_2, ..., n_l]$ は $[n_1, n_2, ..., n_l - 1, 1]$ と同じである。連分数の計算規則に従うと、両者は同じになるのである。例えば $[1, 1, 1, 1, 1, 2] = [1, 1, 1, 1, 1, 1, 1]$ である。その結果、連分数の商が全て 1 になるものは、この例では $5/3, 8/5, 13/8, 21/13$ である。これらは Fibonacci 数列になってる。

定義 $l(p,q)$ を p/q の連分数の長さとする。

その際、連分数は長い方に規格化されているとする[1]。例えば $l(5,3)=4$ である。互除法の除算の回数は $l(p,q)$ より、1 回少ない。

r を剰余 $p=aq+r\ (0<r<q)$ とすると、$l(p,q)=1+l(q,r)$ である。

補題 1 $a_1=a_2=\cdots=a_k=1$ として、$[a_k,a_{k-1},...,a_1]$ を p_k/q_k と置く。ここに p_k,q_k は自然数で、互いに素としてよい。すると $q_k=p_{k-1}$ で

$$p_0=p_1=1$$
$$p_k=p_{k-1}+p_{k-2}\quad(k=2,3,...)$$

となる。すなわち $p_0,p_1,p_2,p_3,...$ は Fibonacci 数列である。

証明:

$$\frac{p_k}{q_k}=[a_k,a_{k-1},...,a_1]=a_k+\frac{1}{[a_{k-1},...,a_1]}=a_k+\frac{q_{k-1}}{p_{k-1}}=\frac{a_kp_{k-1}+q_{k-1}}{p_{k-1}}$$

故に、$q_k=p_{k-1}$ で $p_k=a_kp_{k-1}+q_{k-1}$ である。これから $p_k=a_kp_{k-1}+p_{k-2}$ が得られる。 □

以下 Fibonacci 数列を $F_1,F_2,F_3,...\ (F_1=F_2=1)$ とする。$l(F_{k+1},F_k)=l(F_k,F_{k-1})+1$ であり、$l(F_2,F_1)=1$ であるから、$l(F_{k+1},F_k)=k$ が成り立つ。

定理 1 $F_n\le p<F_{n+1}\ (n\ge 3)$ とする。すると $0<q<p$ であれば $l(p,q)\le l(F_n,F_{n-1})$ である[2]。

証明: n についての数学的帰納法で証明する。

$n=3$ では $F_3\le p<F_4$ すなわち $2\le p<3$ で、$p=2$ である。このとき $q=1$ で $l(p,q)=l(2,1)=[1,1]$ である。他方 $l(F_3,F_2)=l(2,1)$ で帰納法の仮定を満たす。

[1]短い方に規格化した方が、通常の感覚と一致するので、分かり易いかも知れないが、今度は証明の述べ方がややこしくなる

[2]これと同等な定理はどこかに既にあると思える。と言うのは、互除法の効率の問題は、アルゴリズム分野の基本的な問題であり、Knuth[7] には、Fibonacci 数と関係していることが指摘されているからである

そこで $n > 3$ とし、$n = k$ で帰納法の仮定を満たすとする。すなわち、次の命題 $P(n, p, q)$ が $n = k$ で成立しているとする。

$$P(n,p,q): \quad F_n \le p < F_{n+1} \quad \text{and} \quad 0 < q < p \quad \Longrightarrow \quad l(p,q) \le l(F_n, F_{n-1})$$

$n = k + 1$ として $F_{k+1} \le p < F_{k+2}$ で $0 < q < p$ とする。

CASE A: $q < F_{k+1}$

この場合、$F_{k'} \le q < F_{k'+1}$ となる k' $(k' \le k)$ が存在する。r を剰余 $p = aq + r$ $(0 < r < q)$ とする。$l(p,q) = 1 + l(q,r)$ であるが帰納法の仮定から $l(q,r) \le l(F_{k'}, F_{k'-1})$ である。従って $l(q,r) \le 1 + l(F_{k'}, F_{k'-1}) = l(F_{k'+1}, F_{k'}) \le l(F_{k+1}, F_k)$ である。すなわち $q < F_{k+1} \le p < F_{k+2}$ の場合には $P(k+1, p, q)$ は真である。

CASE B: $F_{k+1} \le q$

$p - q < F_{k+2} - F_{k+1} = F_k$ である。従って剰余 r は $r = p - q$ で $l(p,q) = 1 + l(q,r)$ であるが、$r < F_k < F_{k+1} < q < F_{k+2}$ 故、CASE A の議論を $P(k+1, q, r)$ として適用できる。 □

B 平方根の連分数

$\sqrt{m}$ を連分数に展開するプログラム例を Python3 で示す。

```
#! /usr/bin/env python3
# continued fractions of sqrt(m)
from math import sqrt

def cfrac(m):
  r0 = sqrt(m)
  r = round(r0)
  if r*r == m:
    return r,None
  n0 = int(r0)
  n,a,b = n0,1,0
  cf=[]
  while True:
    b = n*a -b
    a = (m-b*b)//a
    n = (n0+b)//a
    cf.append(n)
    if a == 1:
      break
  return n0,cf

for m in range(2,100):
  r = round(sqrt(m))
  n0,cf=cfrac(m)
  print(m,n0,cf)
```

次は実行結果のリストである。$2 \leq m < 100$ を示してある。出力フィールドの意味は次の通りである:

m n_0 [連分数の循環部分]

ここに $n_0 = [\sqrt{m}]$ である。例えば

```
7 2 [1, 1, 1, 4]
```

と書かれている行は $m = 7$ の結果で、その連分数は $[2, \overline{1, 1, 1, 4}]$ である。

```
2 1 [2]
3 1 [1, 2]
4 2 None
5 2 [4]
6 2 [2, 4]
7 2 [1, 1, 1, 4]
8 2 [1, 4]
9 3 None
10 3 [6]
11 3 [3, 6]
12 3 [2, 6]
13 3 [1, 1, 1, 1, 6]
14 3 [1, 2, 1, 6]
15 3 [1, 6]
16 4 None
17 4 [8]
18 4 [4, 8]
19 4 [2, 1, 3, 1, 2, 8]
20 4 [2, 8]
21 4 [1, 1, 2, 1, 1, 8]
22 4 [1, 2, 4, 2, 1, 8]
23 4 [1, 3, 1, 8]
24 4 [1, 8]
25 5 None
26 5 [10]
27 5 [5, 10]
28 5 [3, 2, 3, 10]
29 5 [2, 1, 1, 2, 10]
30 5 [2, 10]
31 5 [1, 1, 3, 5, 3, 1, 1, 10]
32 5 [1, 1, 1, 10]
33 5 [1, 2, 1, 10]
34 5 [1, 4, 1, 10]
35 5 [1, 10]
36 6 None
37 6 [12]
38 6 [6, 12]
39 6 [4, 12]
40 6 [3, 12]
41 6 [2, 2, 12]
42 6 [2, 12]
43 6 [1, 1, 3, 1, 5, 1, 3, 1, 1, 12]
44 6 [1, 1, 1, 2, 1, 1, 1, 12]
45 6 [1, 2, 2, 2, 1, 12]
```

```
46 6 [1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12]
47 6 [1, 5, 1, 12]
48 6 [1, 12]
49 7 None
50 7 [14]
51 7 [7, 14]
52 7 [4, 1, 2, 1, 4, 14]
53 7 [3, 1, 1, 3, 14]
54 7 [2, 1, 6, 1, 2, 14]
55 7 [2, 2, 2, 14]
56 7 [2, 14]
57 7 [1, 1, 4, 1, 1, 14]
58 7 [1, 1, 1, 1, 1, 1, 14]
59 7 [1, 2, 7, 2, 1, 14]
60 7 [1, 2, 1, 14]
61 7 [1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14]
62 7 [1, 6, 1, 14]
63 7 [1, 14]
64 8 None
65 8 [16]
66 8 [8, 16]
67 8 [5, 2, 1, 1, 7, 1, 1, 2, 5, 16]
68 8 [4, 16]
69 8 [3, 3, 1, 4, 1, 3, 3, 16]
70 8 [2, 1, 2, 1, 2, 16]
71 8 [2, 2, 1, 7, 1, 2, 2, 16]
72 8 [2, 16]
73 8 [1, 1, 5, 5, 1, 1, 16]
74 8 [1, 1, 1, 1, 16]
75 8 [1, 1, 1, 16]
76 8 [1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16]
77 8 [1, 3, 2, 3, 1, 16]
78 8 [1, 4, 1, 16]
79 8 [1, 7, 1, 16]
80 8 [1, 16]
81 9 None
82 9 [18]
83 9 [9, 18]
84 9 [6, 18]
85 9 [4, 1, 1, 4, 18]
86 9 [3, 1, 1, 1, 8, 1, 1, 1, 3, 18]
87 9 [3, 18]
88 9 [2, 1, 1, 1, 2, 18]
89 9 [2, 3, 3, 2, 18]
```

```
90 9 [2, 18]
91 9 [1, 1, 5, 1, 5, 1, 1, 18]
92 9 [1, 1, 2, 4, 2, 1, 1, 18]
93 9 [1, 1, 1, 4, 6, 4, 1, 1, 1, 18]
94 9 [1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18]
95 9 [1, 2, 1, 18]
96 9 [1, 3, 1, 18]
97 9 [1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18]
98 9 [1, 8, 1, 18]
99 9 [1, 18]
```

C 連分数の形式的算法

ここでは Hardy-Wright に従って記法 $[a_1, a_2, a_3, ...]$ を扱う[1]。また、ここでは $a_1, a_2, a_3, ... \in K$ で、K は任意の可換体とし、形式的算法のみを議論する。

形式算法では収束の問題を扱えないので、長さは有限である。また、表現の一意性も担保できない。しかし、形式的算法の中だけで証明できる重要な定理がある。

定義 1

$$[a_1] = a_1, \quad [a_1, a_2, ..., a_n] = a_1 + \frac{1}{[a_2, a_2, ..., a_n]} \quad (n \geq 2) \tag{1}$$

次のように定義してもよいだろう[2]。

定義 1a

$$[a] = a, \quad [a, b] = a + \frac{1}{b}, \quad [a_1, a_2, a_3, ...] = [a_1, [a_2, a_3, ...]]$$

定義 1a のメリットは、次の関係が自明になることにある。

$$[a_1, a_2, a_3, ..., [b_1, b_2, b_3, ...]] = [a_1, a_2, a_3, ..., b_1, b_2, b_3, ...] \tag{2}$$

つまり括弧の中の末尾に括弧は許されるが、その括弧は外してもよい[3]。

証明: すなわち

$$[a_1, a_2, a_3, ...] = [a_1, [a_2, a_3, ...]] = [a_1, [a_2, [a_3, ...]]] = [a_1, a_2, [a_3, ...]]$$

等々、帰納法を使えばよい。 □

注意: $[a_1, a_2, a_3, ..., a_n]$ において $n = 1$ の場合、すなわち $[a_1]$ は Gauss の整数化記号 $[x]$ と紛らわしい。そこで、$[x]$ が連分数を表している場合には ",” を追加して $[x,]$ と書くことにする。実際には、そのようなケースは殆ど発生しないだろうが...

---

[1] Dirichlet-Dedekind は 角括弧を定義 1 の $H(a, b, c, ...)$ の意味に使う。これは Gauss に拠るらしい。高木も同様である。他方 Dirichlet-Dedekind と Sierpinski は連分数を丸括弧で表現する。Hardy-Wright も Sierpinski も $H(a, b, c, ...)$ 相当の関数を定義しない。

[2] もちろん、両者は同値である

[3] Hardy-Wright p.130

例 1 $[2,3,5,7]$ の計算。定義そのままに、後方から計算してみる。

$$[7]=7,\quad [5,7]=5+\frac{1}{7}=\frac{36}{7},\quad [3,5,7]=3+\frac{7}{36}=\frac{115}{36}$$
$$[2,3,5,7]=2+\frac{36}{115}=\frac{266}{115}$$

定理 6 を使って、前方から計算することもできる (例 4)。

例 2

$$[a,b,c]=a+\frac{1}{[b,c]}=a+\frac{c}{bc+1}=\frac{a(bc+1)+c}{ab+1}=\frac{abc+a+c}{ab+1}$$
$$[a,b,c,d]=a+\frac{1}{[b,c,d]}=a+\frac{bc+1}{bcd+b+d}=\frac{a(bcd+b+d)+bc+1}{bcd+b+d}$$
$$=\frac{abcd+ab+ad+bc+1}{bcd+b+d}$$

定義 2 関数 $H(a_1,a_2,a_3,...,a_n)$ を

$$\begin{aligned}&H()=1,\quad H(a_1)=a_1,\quad H(a_1,a_2)=a_1a_2+1,\\&H(a_1,a_2,a_3,...,a_n)=a_1H(a_2,a_3,...,a_n)+H(a_3,...,a_n)\end{aligned}\tag{3}$$

で再帰的に定義する [4]。

例 3

$$\begin{aligned}&H()=1,\quad H(a)=a,\quad H(a,b)=ab+1,\quad H(a,b,c)=abc+a+c,\\&H(a,b,c,d)=abcd+ab+ad+cd+1\end{aligned}\tag{4}$$

以下の証明において、紙面の節約のために $A_k=\begin{pmatrix}a_k & 1\\ 1 & 0\end{pmatrix}$ を定義しておく。すると

[4]関数 $H(a_1,...,a_n)$ は Gauss の記法 $[a_1,...,a_n]$ に相当するが、$n=0$ も含めて拡張してある。なお、Dirichlet-Dedekind が Gauss 記法を導入する際に、文字 "H" を便宜的に使ったので、それを借用した

補題 1

$$\begin{pmatrix} H(a_1,...,a_n) & H(a_1,...,a_{n-1}) \\ H(a_2,...,a_n) & H(a_2,...,a_{n-1}) \end{pmatrix} = A_1 A_2 \cdots A_n \tag{5}$$

である。

証明: 定義 2 より

$$\begin{pmatrix} H(a_1,...,a_n) \\ H(a_2,...,a_n) \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} H(a_2,...,a_n) \\ H(a_3,...,a_n) \end{pmatrix} = A_1 A_2 \cdots A_n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

ここで

$$\begin{pmatrix} H(a_n) \\ H() \end{pmatrix} = \begin{pmatrix} a_n \\ 1 \end{pmatrix} = \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

を利用した。また

$$\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

に注意すると

$$\begin{pmatrix} H(a_1,...,a_n) & H(a_1,...,a_{n-1}) \\ H(a_2,...,a_n) & H(a_2,...,a_{n-1}) \end{pmatrix} = A_1 A_2 \cdots A_n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

が得られる。これから補題の主張が得られる。 □

定理 1

$$H(a_1,a_2,...,a_{n-1},a_n) = H(a_1,a_2,...,a_{n-1})a_n + H(a_1,a_2,...,a_{n-2}) \tag{6}$$

$$H(a_1,a_2,...,a_{n-1},a_n) = H(a_n,a_{n-1},...,a_2,a_1) \tag{7}$$

証明: 式 (6) は

$$\begin{pmatrix} H(a_1,a_2,...,a_{n-1},a_n) & H(a_1,a_2,...,a_{n-1}) \\ H(a_2,...,a_{n-1},a_n) & H(a_2,...,a_{n-1}) \end{pmatrix}$$
$$= \begin{pmatrix} H(a_1,a_2,...,a_{n-1}) & H(a_1,a_2,...,a_{n-2}) \\ H(a_2,...,a_{n-1}) & H(a_2,...,a_{n-2}) \end{pmatrix} A_n$$

から得られる。また、転置行列を肩付きの t で表すと、式 (7) は

$$\begin{pmatrix} H(a_n, a_{n-1}, ..., a_2, a_1) & H(a_n, a_{n-1}, ..., a_2) \\ H(a_{n-1}, ..., a_2, a_1) & H(a_{n-1}, ..., a_2) \end{pmatrix}^{\mathrm{t}} \\ = (A_n A_{n-1} \cdots A_2 A_1)^{\mathrm{t}} = A_1 A_2 \cdots A_{n-1} A_n$$

から得られる。 □

定理 2 $n \geq 2$ として

$$\begin{vmatrix} H(a_1, ..., a_n) & H(a_1, ..., a_{n-1}) \\ H(a_2, ..., a_n) & H(a_2, ..., a_{n-1}) \end{vmatrix} = (-1)^n$$

証明: 補題 1 から自明。 □

定理 2 の系 $H(a_1, ..., a_n)$ と $H(a_2, ..., a_n)$ は互いに素である。また $H(a_1, ..., a_n)$ と $H(a_1, ..., a_{n-1})$ も互いに素である。

定理 3 $n \geq 3$ として

$$\begin{vmatrix} H(a_1, ..., a_n) & H(a_1, ..., a_{n-2}) \\ H(a_2, ..., a_n) & H(a_2, ..., a_{n-2}) \end{vmatrix} = (-1)^{n-1} a_n$$

証明:

$$\begin{pmatrix} H(a_1, ..., a_n) \\ H(a_2, ..., a_n) \end{pmatrix} = A_1 A_2 \cdots A_{n-2} A_{n-1} A_n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{8}$$

である。また

$$\begin{pmatrix} H(a_1, ..., a_{n-2}) \\ H(a_2, ..., a_{n-2}) \end{pmatrix} = A_1 \cdots A_{n-2} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{9}$$

である。そして

$$\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_n \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} a_{n-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

であるから、式 (8) を第 1 の関係を使って、式 (9) を第 2 の関係を使って変形すると

$$\begin{pmatrix} H(a_1,...,a_n) & H(a_1,...,a_{n-2}) \\ H(a_2,...,a_n) & H(a_2,...,a_{n-2}) \end{pmatrix} = A_1 \cdots A_{n-2} A_{n-1} \begin{pmatrix} a_n & 0 \\ 1 & 1 \end{pmatrix}$$

となり、定理の主張が得られる。 □

定理 4 次の関係が成立する。

$$[a_1, a_2, ..., a_n] = \frac{H(a_1, a_2, ..., a_n)}{H(a_2, ..., a_n)} \tag{10}$$

証明: $n = 1$ では成立している。$n > 1$ では、角括弧の中の a たちの個数に関する、数学的帰納法で示される。個数が $n-1$ で成立しているとすれば

$$\begin{aligned} [a_1, a_2, ..., a_n] &= a_1 + \frac{1}{[a_2, ..., a_n]} = \frac{a_1 H(a_2, ..., a_n) + H(a_3, ..., a_n)}{H(a_2, ..., a_n)} \\ &= \frac{H(a_1, a_2, ..., a_n)}{H(a_2, ..., a_n)} \end{aligned}$$

□

定理 5 $a_1, ..., a_n$ を整数として

$$[a_1, ..., a_n] = \frac{p_n}{q_n}, \quad [a_1, ..., a_{n-1}] = \frac{p_{n-1}}{q_{n-1}}$$

とする。$p_n/q_n,\ p_{n-1}/q_{n-1}$ が (分母が正の) 既約分数であれば

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^n$$

となる。

証明: 分母が正の既約分数の一意性と、定理 2 と定理 2 の系、および定理 4 より明らか。 □

定理 6 $a_1, ..., a_n$ を整数として

$$[a_1, ..., a_{n-1}] = \frac{p_{n-1}}{q_{n-1}}, \quad [a_1, ..., a_n] = \frac{p_n}{q_n}$$

とする。ここに $p_n/q_n,\ p_{n-1}/q_{n-1}$ は (分母が正の) 既約分数とする。すると、任意の可換体の元 θ に対して

$$[a_1, ..., a_n, \theta] = \frac{p_{n-1} + p_n \theta}{p_{q-1} + q_n \theta}$$

となる。

証明: 正整数からなる既約分数の一意性と、定理 1 と定理 4 より

$$[a_1, ..., a_n, \theta] = \frac{H(a_1, ..., a_n, \theta)}{H(a_2, ..., a_n, \theta)} = \frac{H(a_1, ..., a_n)\theta + H(a_1, ..., a_{n-1})}{H(a_2, ..., a_n)\theta + H(a_2, ..., a_{n-1})}$$
$$= \frac{p_n\theta + p_{n-1}}{q_n\theta + q_{n-1}}$$

□

例 4 定理 6 を使うと、連分数を前方から計算できるばかりか、連分数の末尾に未知数が含まれているような場合も、効率よく計算できる。例えば $[2, 3, 5, \theta]$ の場合には次のように計算する。

$$[2] = \frac{2}{1}, \quad [2, 3] = 2 + \frac{1}{3} = \frac{7}{3}, \quad [2, 3, 5] = \frac{2 + 7 \cdot 5}{1 + 3 \cdot 5} = \frac{37}{16}$$
$$[2, 3, 5, \theta] = \frac{7 + 37\theta}{3 + 16\theta}$$

D Pell 方程式の基本解

以下に Pell 方程式 $x^2 - my^2 = e\ (e = \pm 1)$ の基本解を $m,\ x,\ y,\ e$ の順に示す。

2 1 1 -1
3 2 1 1
5 2 1 -1
6 5 2 1
7 8 3 1
8 3 1 1
10 3 1 -1
11 10 3 1
12 7 2 1
13 18 5 -1
14 15 4 1
15 4 1 1
17 4 1 -1
18 17 4 1
19 170 39 1
20 9 2 1
21 55 12 1
22 197 42 1
23 24 5 1
24 5 1 1
26 5 1 -1
27 26 5 1
28 127 24 1
29 70 13 -1
30 11 2 1
31 1520 273 1
32 17 3 1
33 23 4 1
34 35 6 1
35 6 1 1
37 6 1 -1
38 37 6 1
39 25 4 1
40 19 3 1
41 32 5 -1
42 13 2 1
43 3482 531 1
44 199 30 1
45 161 24 1
46 24335 3588 1
47 48 7 1
48 7 1 1
50 7 1 -1
51 50 7 1
52 649 90 1
53 182 25 -1
54 485 66 1
55 89 12 1
56 15 2 1
57 151 20 1
58 99 13 -1
59 530 69 1
60 31 4 1
61 29718 3805 -1
62 63 8 1
63 8 1 1
65 8 1 -1
66 65 8 1
67 48842 5967 1
68 33 4 1
69 7775 936 1
70 251 30 1
71 3480 413 1
72 17 2 1
73 1068 125 -1
74 43 5 -1
75 26 3 1
76 57799 6630 1
77 351 40 1
78 53 6 1
79 80 9 1
80 9 1 1
82 9 1 -1
83 82 9 1
84 55 6 1
85 378 41 -1
86 10405 1122 1
87 28 3 1
88 197 21 1
89 500 53 -1
90 19 2 1
91 1574 165 1
92 1151 120 1
93 12151 1260 1
94 2143295 221064 1
95 39 4 1
96 49 5 1
97 5604 569 -1
98 99 10 1
99 10 1 1

E 拡張 Pell 方程式の基本解

以下に $\omega = \dfrac{\sqrt{m}+1}{2}$ $(m = 4n+1)$ の連分数と、それから得られた拡張 Pell 方程式の基本解を載せる。

出力フィールドの意味は次の通りである:

$$m \quad n_0 \quad [\text{ 連分数の循環部分 }] \quad x \quad y \quad (x^2 - my^2)$$

ここに $n_0 = [\omega]$ である。例えば

```
33 3 [2, 1, 2, 5] 23 4 1
```

と書かれている行は $m = 33$ の結果で、その場合の ω の連分数は $[3, \overline{2,1,2,5}]$ となる。拡張 Pell 方程式 $x^2 - my^2 = \pm 4$ を満たす基本解 x, y は、$p/q = [3,2,1,2]$ より求めた p, q によって、$x = 2p - q, y = q$ として得られるが、表には、通約した結果が書かれている。(長くなる行は 2 行に分けて書かれている)

```
5 1 [1] 1 1 -4
13 2 [3] 3 1 -4
17 2 [1, 1, 3] 4 1 -1
21 2 [1, 3] 5 1 4
29 3 [5] 5 1 -4
33 3 [2, 1, 2, 5] 23 4 1
37 3 [1, 1, 5] 6 1 -1
41 3 [1, 2, 2, 1, 5] 32 5 -1
45 3 [1, 5] 7 1 4
53 4 [7] 7 1 -4
57 4 [3, 1, 1, 1, 3, 7] 151 20 1
61 4 [2, 2, 7] 39 5 -4
65 4 [1, 1, 7] 8 1 -1
69 4 [1, 1, 1, 7] 25 3 4
73 4 [1, 3, 2, 1, 1, 2, 3, 1, 7] 1068 125 -1
77 4 [1, 7] 9 1 4
85 5 [9] 9 1 -4
89 5 [4, 1, 1, 1, 1, 4, 9] 500 53 -1
93 5 [3, 9] 29 3 4
97 5 [2, 2, 1, 4, 4, 1, 2, 2, 9] 5604 569 -1
101 5 [1, 1, 9] 10 1 -1
105 5 [1, 1, 1, 1, 1, 9] 41 4 1
109 5 [1, 2, 1, 1, 2, 1, 9] 261 25 -4
113 5 [1, 4, 2, 2, 4, 1, 9] 776 73 -1
117 5 [1, 9] 11 1 4
125 6 [11] 11 1 -4
```

```
129 6 [5, 1, 1, 2, 3, 2, 1, 1, 5, 11] 16855 1484 1
133 6 [3, 1, 3, 11] 173 15 4
137 6 [2, 1, 5, 5, 1, 2, 11] 1744 149 -1
141 6 [2, 3, 2, 11] 95 8 1
145 6 [1, 1, 11] 12 1 -1
149 6 [1, 1, 1, 1, 11] 61 5 -4
153 6 [1, 2, 5, 1, 5, 2, 1, 11] 2177 176 1
157 6 [1, 3, 3, 1, 11] 213 17 -4
161 6 [1, 5, 2, 2, 1, 2, 2, 5, 1, 11] 11775 928 1
165 6 [1, 11] 13 1 4
173 7 [13] 13 1 -4
177 7 [6, 1, 1, 2, 1, 3, 1, 2, 1, 1, 6, 13] 62423 4692 1
181 7 [4, 2, 2, 4, 13] 1305 97 -4
185 7 [3, 3, 13] 68 5 -1
189 7 [2, 1, 2, 13] 55 4 1
193 7 [2, 4, 6, 1, 2, 1, 1, 1, 1, 2, 1, 6, 4, 2, 13] 1764132 126985 -1
197 7 [1, 1, 13] 14 1 -1
201 7 [1, 1, 2, 3, 6, 1, 3, 1, 6, 3, 2, 1, 1, 13] 515095 36332 1
205 7 [1, 1, 1, 13] 43 3 4
209 7 [1, 2, 1, 2, 6, 1, 6, 2, 1, 2, 1, 13] 46551 3220 1
213 7 [1, 3, 1, 13] 73 5 4
217 7 [1, 6, 2, 3, 4, 1, 1, 1, 1, 1, 4, 3, 2, 6, 1, 13]
      3844063 260952 1
221 7 [1, 13] 15 1 4
229 8 [15] 15 1 -4
233 8 [7, 1, 1, 3, 3, 1, 1, 7, 15] 23156 1517 -1
237 8 [5, 15] 77 5 4
241 8 [3, 1, 4, 2, 2, 1, 1, 1, 7, 7, 1, 1, 1, 2, 2, 4, 1, 3, 15]
      71011068 4574225 -1
245 8 [3, 15] 47 3 4
249 8 [2, 1, 1, 3, 2, 1, 7, 5, 7, 1, 2, 3, 1, 1, 2, 15]
      8553815 542076 1
253 8 [2, 4, 1, 4, 2, 15] 1861 117 4
257 8 [1, 1, 15] 16 1 -1
261 8 [1, 1, 2, 1, 2, 1, 1, 15] 727 45 4
265 8 [1, 1, 1, 3, 2, 2, 3, 1, 1, 1, 15] 6072 373 -1
269 8 [1, 2, 2, 1, 15] 82 5 -1
273 8 [1, 3, 5, 3, 1, 15] 727 44 1
277 8 [1, 4, 1, 1, 1, 1, 4, 1, 15] 2613 157 -4
281 8 [1, 7, 2, 3, 1, 2, 1, 1, 2, 1, 3, 2, 7, 1, 15] 1063532 63445 -1
285 8 [1, 15] 17 1 4
293 9 [17] 17 1 -4
297 9 [8, 1, 1, 3, 1, 3, 1, 1, 8, 17] 48599 2820 1
301 9 [5, 1, 2, 1, 1, 1, 2, 1, 5, 17] 22745 1311 4
```

F 一般 Pell 方程式の解の例

以下に $m = 2, 3, 5, 6, 7, 8, 10$ における一般 Pell 方程式 $x^2 - my^2 = \pm d$ の解を $d = 2, ..., 41$ について載せる。

出力フィールドの意味は次の通りである:

$$m \quad d \quad [\ \text{(代表解), (代表解),...]}$$

ここに (代表解) は $(x, y, x^2 - my^2)$ の組である。

例えば

```
2 7 [(-1, 2, -7), (1, 2, -7)]
```

と書かれている行は $m = 2,\ d = 7$ の結果で、その場合の代表解は 2 つあり、一つは $x = -1,\ y = 2,\ x^2 - 2y^2 = -7$ もう一つは $x = 1,\ y = 2,\ x^2 - 2y^2 = -7$ であることを意味している。

F.1 $m = 2$

```
2 2 [(0, 1, -2)]
2 3 []
2 4 [(2, 0, 4)]
2 5 []
2 6 []
2 7 [(-1, 2, -7), (1, 2, -7)]
2 8 [(0, 2, -8)]
2 9 [(3, 0, 9)]
2 10 []
2 11 []
2 12 []
2 13 []
2 14 [(4, -1, 14), (4, 1, 14)]
2 15 []
2 16 [(4, 0, 16)]
2 17 [(-1, 3, -17), (1, 3, -17)]
2 18 [(0, 3, -18)]
2 19 []
2 20 []
2 21 []
2 22 []
2 23 [(5, -1, 23), (5, 1, 23)]
2 24 []
```

```
2 25 [(5, 0, 25)]
2 26 []
2 27 []
2 28 [(-2, 4, -28), (2, 4, -28)]
2 29 []
2 30 []
2 31 [(-1, 4, -31), (1, 4, -31)]
2 32 [(0, 4, -32)]
2 33 []
2 34 [(6, -1, 34), (6, 1, 34)]
2 35 []
2 36 [(6, 0, 36)]
2 37 []
2 38 []
2 39 []
2 40 []
2 41 [(7, -2, 41), (7, 2, 41)]
2 42 []
2 43 []
2 44 []
2 45 []
2 46 [(-2, 5, -46), (2, 5, -46)]
2 47 [(7, -1, 47), (7, 1, 47)]
2 48 []
2 49 [(-1, 5, -49), (1, 5, -49), (7, 0, 49)]
2 50 [(0, 5, -50)]
```

F.2 m=3

```
3 2 [(-1, 1, -2)]
3 3 [(0, 1, -3)]
3 4 [(2, 0, 4)]
3 5 []
3 6 [(3, -1, 6)]
3 7 []
3 8 [(-2, 2, -8)]
3 9 [(3, 0, 9)]
3 10 []
3 11 [(-1, 2, -11), (1, 2, -11)]
3 12 [(0, 2, -12)]
3 13 [(4, -1, 13), (4, 1, 13)]
```

```
3 14 []
3 15 []
3 16 [(4, 0, 16)]
3 17 []
3 18 [(-3, 3, -18)]
3 19 []
3 20 []
3 21 []
3 22 [(5, -1, 22), (5, 1, 22)]
3 23 [(-2, 3, -23), (2, 3, -23)]
3 24 [(6, -2, 24)]
3 25 [(5, 0, 25)]
3 26 [(-1, 3, -26), (1, 3, -26)]
3 27 [(0, 3, -27)]
3 28 []
3 29 []
3 30 []
3 31 []
3 32 [(-4, 4, -32)]
3 33 [(6, -1, 33), (6, 1, 33)]
3 34 []
3 35 []
3 36 [(6, 0, 36)]
3 37 [(7, -2, 37), (7, 2, 37)]
3 38 []
3 39 [(-3, 4, -39), (3, 4, -39)]
3 40 []
3 41 []
3 42 []
3 43 []
3 44 [(-2, 4, -44), (2, 4, -44)]
3 45 []
3 46 [(7, -1, 46), (7, 1, 46)]
3 47 [(-1, 4, -47), (1, 4, -47)]
3 48 [(0, 4, -48)]
3 49 [(7, 0, 49)]
3 50 [(-5, 5, -50)]
```

F.3 m=5

```
5 2 []
```

```
5 3 []
5 4 [(-1, 1, -4), (1, 1, -4), (2, 0, 4)]
5 5 [(0, 1, -5)]
5 6 []
5 7 []
5 8 []
5 9 [(3, 0, 9)]
5 10 []
5 11 [(4, -1, 11), (4, 1, 11)]
5 12 []
5 13 []
5 14 []
5 15 []
5 16 [(-2, 2, -16), (2, 2, -16), (4, 0, 16)]
5 17 []
5 18 []
5 19 [(-1, 2, -19), (1, 2, -19)]
5 20 [(0, 2, -20), (5, -1, 20), (5, 1, 20)]
5 21 []
5 22 []
5 23 []
5 24 []
5 25 [(5, 0, 25)]
5 26 []
5 27 []
5 28 []
5 29 [(-4, 3, -29), (4, 3, -29)]
5 30 []
5 31 [(6, -1, 31), (6, 1, 31)]
5 32 []
5 33 []
5 34 []
5 35 []
5 36 [(-3, 3, -36), (3, 3, -36), (6, 0, 36)]
5 37 []
5 38 []
5 39 []
5 40 []
5 41 [(-2, 3, -41), (2, 3, -41)]
5 42 []
5 43 []
5 44 [(-1, 3, -44), (1, 3, -44), (7, -1, 44), (7, 1, 44), (8, -2, 44), (8, 2, 44
5 45 [(0, 3, -45)]
5 46 []
```

```
5 47 []
5 48 []
5 49 [(7, 0, 49)]
5 50 []
```

F.4 m=6

```
6 2 [(-2, 1, -2)]
6 3 [(3, -1, 3)]
6 4 [(2, 0, 4)]
6 5 [(-1, 1, -5), (1, 1, -5)]
6 6 [(0, 1, -6)]
6 7 []
6 8 [(-4, 2, -8)]
6 9 [(3, 0, 9)]
6 10 [(4, -1, 10), (4, 1, 10)]
6 11 []
6 12 [(6, -2, 12)]
6 13 []
6 14 []
6 15 [(-3, 2, -15), (3, 2, -15)]
6 16 [(4, 0, 16)]
6 17 []
6 18 [(-6, 3, -18)]
6 19 [(5, -1, 19), (5, 1, 19)]
6 20 [(-2, 2, -20), (2, 2, -20)]
6 21 []
6 22 []
6 23 [(-1, 2, -23), (1, 2, -23)]
6 24 [(0, 2, -24)]
6 25 [(5, 0, 25), (7, -2, 25), (7, 2, 25)]
6 26 []
6 27 [(9, -3, 27)]
6 28 []
6 29 [(-5, 3, -29), (5, 3, -29)]
6 30 [(6, -1, 30), (6, 1, 30)]
6 31 []
6 32 [(-8, 4, -32)]
6 33 []
6 34 []
6 35 []
```

```
6 36 [(6, 0, 36)]
6 37 []
6 38 [(-4, 3, -38), (4, 3, -38)]
6 39 []
6 40 [(8, -2, 40), (8, 2, 40)]
6 41 []
6 42 []
6 43 [(7, -1, 43), (7, 1, 43)]
6 44 []
6 45 [(-3, 3, -45), (3, 3, -45)]
6 46 [(10, -3, 46), (10, 3, 46)]
6 47 [(-7, 4, -47), (7, 4, -47)]
6 48 [(12, -4, 48)]
6 49 [(7, 0, 49)]
6 50 [(-10, 5, -50), (-2, 3, -50), (2, 3, -50)]
```

F.5 m=7

```
7 2 [(3, -1, 2)]
7 3 [(-2, 1, -3), (2, 1, -3)]
7 4 [(2, 0, 4)]
7 5 []
7 6 [(-1, 1, -6), (1, 1, -6)]
7 7 [(0, 1, -7)]
7 8 [(6, -2, 8)]
7 9 [(3, 0, 9), (4, -1, 9), (4, 1, 9)]
7 10 []
7 11 []
7 12 [(-4, 2, -12), (4, 2, -12)]
7 13 []
7 14 [(-7, 3, -14)]
7 15 []
7 16 [(4, 0, 16)]
7 17 []
7 18 [(5, -1, 18), (5, 1, 18), (9, -3, 18)]
7 19 [(-3, 2, -19), (3, 2, -19)]
7 20 []
7 21 [(7, -2, 21), (7, 2, 21)]
7 22 []
7 23 []
7 24 [(-2, 2, -24), (2, 2, -24)]
```

```
7 25 [(5, 0, 25)]
7 26 []
7 27 [(-6, 3, -27), (-1, 2, -27), (1, 2, -27), (6, 3, -27)]
7 28 [(0, 2, -28)]
7 29 [(6, -1, 29), (6, 1, 29)]
7 30 []
7 31 [(-9, 4, -31), (9, 4, -31)]
7 32 [(12, -4, 32)]
7 33 []
7 34 []
7 35 []
7 36 [(6, 0, 36), (8, -2, 36), (8, 2, 36)]
7 37 [(10, -3, 37), (10, 3, 37)]
7 38 [(-5, 3, -38), (5, 3, -38)]
7 39 []
7 40 []
7 41 []
7 42 [(7, -1, 42), (7, 1, 42)]
7 43 []
7 44 []
7 45 []
7 46 []
7 47 [(-4, 3, -47), (4, 3, -47)]
7 48 [(-8, 4, -48), (8, 4, -48)]
7 49 [(7, 0, 49)]
7 50 [(15, -5, 50)]
```

F.6 m=8

```
8 2 []
8 3 []
8 4 [(-2, 1, -4), (2, 0, 4)]
8 5 []
8 6 []
8 7 [(-1, 1, -7), (1, 1, -7)]
8 8 [(0, 1, -8), (4, -1, 8)]
8 9 [(3, 0, 9)]
8 10 []
8 11 []
8 12 []
8 13 []
```

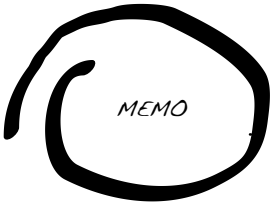
```
8 14 []
8 15 []
8 16 [(-4, 2, -16), (4, 0, 16)]
8 17 [(5, -1, 17), (5, 1, 17)]
8 18 []
8 19 []
8 20 []
8 21 []
8 22 []
8 23 [(-3, 2, -23), (3, 2, -23)]
8 24 []
8 25 [(5, 0, 25)]
8 26 []
8 27 []
8 28 [(-2, 2, -28), (2, 2, -28), (6, -1, 28), (6, 1, 28)]
8 29 []
8 30 []
8 31 [(-1, 2, -31), (1, 2, -31)]
8 32 [(0, 2, -32), (8, -2, 32)]
8 33 []
8 34 []
8 35 []
8 36 [(-6, 3, -36), (6, 0, 36)]
8 37 []
8 38 []
8 39 []
8 40 []
8 41 [(7, -1, 41), (7, 1, 41)]
8 42 []
8 43 []
8 44 []
8 45 []
8 46 []
8 47 [(-5, 3, -47), (5, 3, -47)]
8 48 []
8 49 [(7, 0, 49), (9, -2, 49), (9, 2, 49)]
8 50 []
```

F.7 m=10

```
10 2 []
```

```
10 3 []
10 4 [(2, 0, 4)]
10 5 []
10 6 [(-2, 1, -6), (2, 1, -6)]
10 7 []
10 8 []
10 9 [(-1, 1, -9), (1, 1, -9), (3, 0, 9)]
10 10 [(0, 1, -10)]
10 11 []
10 12 []
10 13 []
10 14 []
10 15 [(5, -1, 15), (5, 1, 15)]
10 16 [(4, 0, 16)]
10 17 []
10 18 []
10 19 []
10 20 []
10 21 []
10 22 []
10 23 []
10 24 [(-4, 2, -24), (4, 2, -24)]
10 25 [(5, 0, 25)]
10 26 [(6, -1, 26), (6, 1, 26)]
10 27 []
10 28 []
10 29 []
10 30 []
10 31 [(-3, 2, -31), (3, 2, -31)]
10 32 []
10 33 []
10 34 []
10 35 []
10 36 [(-2, 2, -36), (2, 2, -36), (6, 0, 36)]
10 37 []
10 38 []
10 39 [(-1, 2, -39), (1, 2, -39), (7, -1, 39), (7, 1, 39)]
10 40 [(0, 2, -40)]
10 41 [(9, -2, 41), (9, 2, 41)]
10 42 []
10 43 []
10 44 []
10 45 []
10 46 []
```

```
10 47 []
10 48 []
10 49 [(7, 0, 49)]
10 50 []
```


MEMO

参考文献

[1] P.G.L.Dirichlet, J.W.R.Dedekind (酒井孝一訳):『整数論講義』(共立出版, 1970)

[2] 高木貞治:『初等整数論講義』(共立出版, 1995)

[3] G.H.Hardy, E.M.Wright: “An Introduction to the Theory of Numbers” (Oxford Science Publication,1979)

[4] W.Sierpinski: “Elementary Theory of Numbers” (North-Holand PWN-Polish Scientific Publishers, 2012)

[5] William J.LeVeque: “Topics in Number Theory — Vol.I and II” (Dover Publications Inc., 2002)

[6] 河田敬義:『数論 I』(岩波講座 基礎数学 1978)

[7] Knuth(広瀬健訳):『基本算法 (1)』(サイエンス社, 1978)

[8] Euclid (斎藤憲訳, 解説):『エウクレイデス全集 (第 2 巻) 原論 VII-X』(東京大学出版会、2015)

[9] van der Waerden (銀林浩訳): 『現代代数学 1』(東京図書, 1937)

[10] van der Waerden (加藤明史訳): 『代数学の歴史』(現代数学社, 1985)

[11] M.Kraïtchik: “Théorie des nombres II” (Paris 1926).

[12] Srinivasa Ramanujan (edited by G.H.Hardy, P.V.Seshu Aiyar & B.M.Wilson): “Collected Papers of Srinivasa Ramanujan” (Cambridge University Press, 1927)

[13] Dean R.Hickerson: “Length of Period of Simple Continued Fraction Expansion of $\sqrt{d}$” (Pacific Journal of Mathematics Vol. 46, No. 2, 1973, `https://msp.org/pjm/1973/46-2/pjm-v46-n2-p11-s.pdf`)

[14] John H.E.Cohn: “The Length of the Period of the Simple Continued Fraction of $d^{1/2}$” (Pacific Journal of Mathematics Vol. 71, No. 1, 1977, `https://msp.org/pjm/1977/71-1/pjm-v71-n1-p03-s.pdf`)

[15] William F. Hammond: “Continued Fractions and the Euclidean Algorithm” (University at Albany, 1997, https://www.albany.edu/~hammond/gellmu/examples/confrac.pdf)

[16] Marius Beceanu: “Period of the Continued Fraction of $\sqrt{m}$” (http://web.math.princeton.edu/mathlab/jr02fall/Periodicity/mariusjp.pdf, 2003)

[17] Seung Hyun Yang: “Continued Fractions and Pell’s Equation” (http://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Yang.pdf, 2008)

[18] Ľubomíra Balková, Aranka Hrušková: “Continued Fractions of Quadratic Numbers” (https://arxiv.org/pdf/1302.0521.pdf, 2013)

[19] N. Saradha: “On the Length of the Period of a Real Quadratic Irrational (Indian J. Pure Appl. Math. 48(3), 2017, http://www.insa.nic.in/writereaddata/UpLoadedFiles/IJPAM/Vol48_2017_3_ART02.pdf)

[20] Evan Dummit: “Continued Fractions and Diophantine Equations” (https://math.la.asu.edu/~dummit/docs/numthy_6_continued_fractions_and_diophantine_equations.pdf, 2014)

[21] Max Lahn, Jonathan Spiegel: “Continued Fractions and Pell’s Equation” (http://davidlowryduda.com/wp-content/uploads/2016/05/LahnSpiegel-FinalProject.pdf, 2016)

[22] Keith Conrad: “Generalized Pell equation” (http://math.stanford.edu/~conrad/154Page/handouts/genpell.pdf)

[23] Keith Conrad: “Pell’s Equation, II” (http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/pelleqn2.pdf)

[24] John P. Robertson: “Solving the generalized Pell equation $x^2 - Dy^2 = N$” (http://www.jpr2718.org/pell.pdf, 2004)

[25] John P. Robertson: “Fundamental Solutions to Generalized Pell Equations” (http://www.jpr2718.org/FundSoln.pdf, 2014)