Pell 方程式

MATHEMATICS.PDF

2010-10-29

目 次

参考文献

[1] 高木貞治: 初等整数論講義 第 2 版, 岩波書店, 1971

[2] 和田秀男: 数の世界—整数論への道 , 岩波書店, 1981.

[3] 木田祐司, 牧野潔夫: UBASIC によるコンピュータ整数論, 日本評論社, 1994.

[4] K. H. Rosen: Elementary Number Theory and Its Applications, Addison-Wesley, 1984

1　Diophantus 方程式 $x^2 - my^2 = r$ について

この節では, Diophantus 方程式[1)]

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

の整数解について考察する. ただし, m, r は整数とする.

$m = r = 0$ のとき, $(0, t)$ (t は任意の整数) がすべての整数解である.

$m = 0$ かつ $r < 0$ のとき, 方程式 (1) は整数解を持たない.

$m = 0$ かつ $r > 0$ のとき, r が平方数ならば, $(\pm\sqrt{r}, t)$ (t は任意の整数) がすべての整数解である. r が平方数でなければ, 整数解はない.

$m < 0$ かつ $r = 0$ のとき, 方程式 (1) の整数解は $(x, y) = (0, 0)$ のみである.

$m < 0$ かつ $r < 0$ のとき, 方程式 (1) は整数解を持たない.

$m < 0$ かつ $r > 0$ のとき, (x, y) を方程式 (1) の整数解とすると,

$$|x|^2 = x^2 \leq x^2 - my^2 = r,$$
$$|m||y|^2 = -my^2 \leq x^2 - my^2 = r.$$

ゆえに, $|x| \leq \sqrt{r}$, $|y| \leq \sqrt{r/|m|}$. したがって, 整数解は有限個である.

$m > 0$ かつ $r = 0$ のとき, m が平方数ならば, $(\pm\sqrt{m}t, t)$ (t は任意の整数) がすべての整数解である. m が平方数でなければ, 整数解はない.

残りは $m > 0$ かつ $r \neq 0$ のときであるが, m が平方数のとき, すなわち, ある整数 m_1 が存在して $m = m_1^2$ と書けるとき,

$$r = x^2 - my^2 = x^2 - m_1^2 y^2 = (x + m_1 y)(x - m_1 y).$$

しかも, $x + m_1 y$, $x - m_1 y$ はともに整数である. よって, 方程式 (1) の整数解は, r のある 2 つの整数の積への分解 $r = r_1 r_2$ に対する連立 1 次方程式

$$x + m_1 y = r_1,$$
$$x - m_1 y = r_2$$

の整数解である. r_1, r_2 の組は有限個であり, 各々の r_1, r_2 の組に対して上の連立 1 次方程式の整数解は高々1 つであるから, 方程式 (1) の整数解は有限個である.

以後, m, r について,

- $m > 0$ かつ m は平方数でない
- $r \neq 0$

という条件を仮定する.

[1)] 整数解や有理数解について考察する場合に, 多項式の方程式を Diophantus 方程式 (Diophantine equation) という.

方程式 (1) の整数解のうち, $x=0$ または $y=0$ であるようなものは**自明な解**と呼ばれる. r が平方数のとき, 自明な解は $(\pm\sqrt{r},0)$ である. $-r/m$ が平方数のとき, 自明な解は $(0,\pm\sqrt{-r/m})$ である. それ以外のとき, 自明な解は存在しない.

自明でない整数解のうち, x, y がともに正の整数であるような解を**正整数解**という. (x,y) が方程式 (1) の整数解ならば, $(x,-y)$, $(-x,y)$, $(-x,-y)$ もまた (1) の整数解である. よって, 正整数解についてのみ考えれば十分である.

[定理 1.1] (x,y), (x',y') を方程式 (1) の 2 つの正整数解とする. このとき, 次の 3 つの条件はすべて同値である:

(i) $x'<x$ または $y'<y$

(ii) $x'<x$ かつ $y'<y$

(iii) $x+y\sqrt{m}<x'+y'\sqrt{m}$

また,

$$(x,y)=(x',y') \Leftrightarrow x=x' \text{ または } y=y',$$
$$(x,y)\neq(x',y') \Leftrightarrow (x'<x \text{ かつ } y'<y) \text{ または } (x<x' \text{ かつ } y<y')$$

が成り立つ.

[証明] (i)⇒(ii)　$x^2-my^2=x'^2-my'^2$ より, $x^2-x'^2=m(y^2-y'^2)$ だから,

$$(x-x')(x+x')=m(y-y')(y+y'). \tag{2}$$

$x'<x$ とすると, x, x' はともに正なので, 式 (2) の左辺は正. よって, 右辺も正である. y, y', m はすべて正なので, $y'<y$ が得られる. ゆえに, $x'<x$ かつ $y'<y$ が成り立つ. 同様に, $y'<y$ とすると, 式 (2) の右辺は正. よって, 左辺も正で, $x'<x$ が得られる.

(ii)⇒(iii)　明らか.

(iii)⇒(i)　対偶を示せばよい. $x\leq x'$ かつ $y\leq y'$ ならば, $x+y\sqrt{m}\leq x'+y'\sqrt{m}$.

また, 後半の 1 番目の同値について, ⇒ は明らか. ⇐ については, $x=x'$ とするとき, もし仮に $y'<y$ とすると, (i)⇒(ii) より $x'<x$ でなければならず, 矛盾が生じる. $y<y'$ のときも同様である. ゆえに, $y=y'$ でなければならない. また, $y=y'$ とするときも, 同様の議論により $x=x'$ がいえる.

後半の 2 番目の同値については, 先に示した同値 (i)⇔(ii) より,

$$\begin{aligned}(x,y)\neq(x',y') &\Leftrightarrow x\neq x' \text{ または } y\neq y'\\ &\Leftrightarrow (x'<x \text{ または } x<x') \text{ または } (y'<y \text{ または } y<y')\\ &\Leftrightarrow (x'<x \text{ または } y'<y) \text{ または } (x<x' \text{ または } y<y')\\ &\Leftrightarrow (x'<x \text{ かつ } y'<y) \text{ または } (x<x' \text{ かつ } y<y').\end{aligned}$$

□

定理 1.1 より, 方程式 (1) の正整数解 (a,b) について, 次の 3 つの条件はすべて同値である:

(i) 任意の正整数解 (x,y) に対して, $a \leq x$ または $b \leq y$

(ii) 任意の正整数解 (x,y) に対して, $a \leq x$ かつ $b \leq y$

(iii) 任意の正整数解 (x,y) に対して, $a + b\sqrt{m} \leq x + y\sqrt{m}$

条件 (i), (ii), (iii) のいずれか (したがって, すべて) を満たす正整数解 (a,b) を**最小解**という.

また, (a,b) が最小解であるとき, 任意の正整数解 (x,y) に対して,

$$(x,y) = (a,b) \Leftrightarrow x = a \text{ または } y = b,$$
$$(x,y) \neq (a,b) \Leftrightarrow a < x \text{ かつ } b < y$$

が成り立つ.

Pell 方程式とは, 方程式 (1) のうちで $r = 1$ のものいう. この文書では, 説明の便宜上 $r = \pm 1$ の場合を Pell 方程式と呼ぶことにする[2)].

[定理 1.2] m, r, s を整数とする. (x,y) を方程式 $x^2 - my^2 = r$ の整数解とし, (z,w) を方程式 $x^2 - my^2 = s$ の整数解とする. このとき, $(xz + myw, xw + yz)$, $(xz - myw, xw - yz)$ は方程式 $x^2 - my^2 = rs$ の整数解である.

[証明] 以下の式において, $\pm$ は複号同順とする.

$$\begin{aligned}
&(xz \pm myw)^2 - m(xw \pm yz)^2 \\
&\quad = (x^2z^2 \pm 2mxyzw + m^2y^2w^1) - m(x^2w^2 \pm 2xyzw + y^2z^2) \\
&\quad = (x^2 - my^2)z^2 - (x^2 - my^2)mw^2 \\
&\quad = (x^2 - my^2)(z^2 - mw^2) \\
&\quad = rs.
\end{aligned}$$

ゆえに, $(xz + myw, xw + yz)$, $(xz - myw, xw - yz)$ は方程式 $x^2 - my^2 = rs$ の解である. これらが整数解であることは明らかである. □

[注意 1.3] 方程式 (1) の正整数解の 1 つを (x_0, y_0) とする. Pell 方程式 $x^2 - my^2 = 1$ の正整数解を (z,w) とすると, 上の定理より $(x_0z + my_0w, x_0w + y_0z)$ も方程式 (1) の正整数解になる. 後に述べるように, 方程式 $x^2 - my^2 = 1$ の正整数解は無数にある. しかも, 2 つの正整数解 (z,w), (z',w') について,

$$\begin{aligned}
&z' < z \text{ かつ } w' < w \\
&\quad \Rightarrow x_0z' + my_0w' < x_0z + my_0w \\
&\qquad \text{かつ } x_0w' + y_0z' < x_0w + y_0z.
\end{aligned}$$

[2)] $r = \pm 4$ の場合も Pell 方程式と呼ばれることがある. この場合は, 2 次体の単数との関連で重要である.

したがって, 方程式 (1) の正整数解がもし存在すれば, それらは無数に存在する.

[注意 1.4] r を正の整数とする. (x, y) を Pell 方程式 $x^2 - my^2 = 1$ の正整数解とすると, (rx, ry) は方程式 $x^2 - my^2 = r^2$ の正整数解である.

ただし, (a, b) が方程式 $x^2 - my^2 = 1$ の最小解であっても, (ra, rb) は必ずしも方程式 $x^2 - my^2 = r^2$ の最小解とは限らない. 例えば, 方程式 $x^2 - 5y^2 = 1$ の最小解は $(9, 4)$ であるが, 方程式 $x^2 - 5y^2 = 4$ の最小解は $(3, 1)$ である.

[注意 1.5] p を奇素数とし, $p \mid m$ かつ $p \nmid r$ であるとする. r が p を法として平方非剰余[3] であるとき, 方程式 $x^2 - my^2 = r$ は整数解を持たない.

なぜなら, もし仮に整数解 (x, y) が存在すると, $x^2 - my^2 = r$ から $x^2 \equiv r \pmod{p}$ が得られる. これは, r が p を法として平方非剰余であることに反する.

2 連分数展開による解法

実数 α の連分数展開

$$\alpha = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

の最初の $n+1$ 項を既約分数 p_n/q_n で

$$\frac{p_n}{q_n} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

のように表すとき, p_n/q_n を α の n 番目の**近似分数**という.

$p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$ と定めると, $n = 0, 1, 2, \ldots$ に対して,

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n q_{n-1} + q_{n-2}. \end{aligned} \tag{3}$$

また, $n = -2, -1, 0, \ldots$ に対して,

$$p_{n+1} q_n - p_n q_{n+1} = (-1)^n.$$

特に, $\gcd(p_n, q_n) = 1$ が成り立つ. なぜなら, もし仮に p_n, q_n の両方を割る素数 p が存在すれば, 上式の左辺は p の倍数であるが, 右辺は $(-1)^n$ のため不可能である.

m が平方数でない正の整数であって, r が $0 < |r| < \sqrt{d}$ を満たすとき, Diophantus 方程式 (1) の正整数解 (x, y) で $\gcd(x, y) = 1$ を満たすものがもし存在すれば, 以下に述べる定理 2.5 により, それは $\sqrt{m}$ の近似分数の分子 p_n と分母 q_n に現れる. 漸化式 (3) を用いて (p_n, q_n) を帰納的に計算すると, $p_n^2 - mq_n^2 = r$ を満たすものが飛び飛びの番号で現れる. 以下に述べる定理 2.1 により, 正整数解は小さい順に現れる.

[3] 素数 p で割れない整数 r について, $r \equiv x^2 \pmod{p}$ を満たす整数 x が存在するとき, r は p を法として平方剰余であるといい, そうでないとき, 平方非剰余であるという.

［定理 2.1］すべての整数 $n \geq 1$ に対して $a_n \geq 1$ であるとする. このとき, すべての整数 $n \geq 1$ に対して

(i) $n \leq q_n$

(ii) $q_n < q_{n+1}$

が成り立つ. さらに, $a_0 \geq 1$ であれば, すべての整数 $n \geq 1$ に対して

(iii) $n < p_n$

(iv) $p_n < p_{n+1}$

が成り立つ.

［証明］(i)　n に関する数学的帰納法により証明する. まず, $q_{-2} = 1$, $q_{-1} = 0$ より,

$$q_0 = a_0 q_{-1} + q_{-2} = 1.$$

これと $a_1 \geq 1$, $a_2 \geq 1$ より,

$$\begin{aligned} q_1 &= a_1 q_0 + q_{-1} = a_1 \geq 1, \\ q_2 &= a_2 q_1 + q_0 = a_1 a_2 + 1 \geq 2. \end{aligned}$$

$n \geq 3$ のとき, $1 \leq k < n$ なるすべての番号 k について $k \leq q_k$ であると仮定すると, $a_n \geq 1$ より

$$\begin{aligned} q_n &= a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} \\ &\geq (n-1) + (n-2) = 2n - 3 \\ &\geq n. \end{aligned}$$

以上より, すべての整数 $n \geq 1$ に対して $n \leq q_n$ が成り立つことが示された.

(ii)　まず,

$$\begin{aligned} q_1 &= a_1 q_0 + q_{-1} = a_1, \\ q_2 &= a_2 q_1 + q_0 = a_1 a_2 + 1. \end{aligned}$$

$a_1 \geq 1$, $a_2 \geq 1$ より, $q_1 < q_2$ が成り立つ.

$n \geq 3$ のとき, $a_n \geq 1$ であり, (i) より $n - 2 \leq q_{n-2}$ であるから,

$$q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + (n-2) > q_{n-1}.$$

(iii)　n に関する数学的帰納法により証明する. まず, $p_{-2} = 0$, $p_{-1} = 1$ より,

$$p_0 = a_0 p_{-1} + p_{-2} = a_0 \geq 1.$$

これと $a_1 \geq 1$, $a_2 \geq 1$ より,

$$p_1 = a_1 p_0 + p_{-1} = a_1 a_0 + 1 \geq 2,$$
$$p_2 = a_2 p_1 + p_0 = a_2(a_1 a_0) + a_0 \geq 3.$$

$n \geq 3$ のとき, $1 \leq k < n$ なるすべての番号 k について $k < p_k$ であると仮定すると, $a_n \geq 1$ より

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2} \geq p_{n-1} + p_{n-2} \\ &> (n-1) + (n-2) = 2n - 3 \\ &\geq n. \end{aligned}$$

以上より, すべての整数 $n \geq 1$ に対して $n < p_n$ が成り立つことが示された.

(iv)　まず,

$$p_1 = a_1 p_0 + p_{-1} = a_1 a_0 + 1,$$
$$p_2 = a_2 p_1 + p_0 = a_2(a_1 a_0) + a_0.$$

$a_0 \geq 1$, $a_1 \geq 1$, $a_2 \geq 1$ より, $p_1 < p_2$ が成り立つ.

$n \geq 3$ のとき, $a_n \geq 1$ であり, (iii) より $n - 2 < p_{n-2}$ であるから,

$$p_n = a_n p_{n-1} + p_{n-2} > p_{n-1} + (n-2) > p_{n-1}.$$

□

[補題 2.2] α を無理数, x/y を既約分数とするとき,

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{2y^2}$$

ならば, x/y は α の近似分数である.

[証明] 高木 [1], 第 2 章 §24 問題 3 あるいは Rosen [4], §10.3, Theorem 10.18 を参照. □

[注意 2.3] 定理の主張の逆は必ずしも成立しない. すなわち, すべての近似分数が不等式を満たすとは限らない.

[補題 2.4] $\alpha > 0$ を無理数, x/y を既約分数とするとき, x/y が α の近似分数ならば, y/x は $1/\alpha$ の近似分数である.

[証明] まず, $\alpha > 1$ のとき, α の連分数展開を

$$\alpha = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

とすると, $1/\alpha$ の連分数展開は

$$\frac{1}{\alpha} = 0 + \frac{1}{a_0} + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

となる. ここで, $\alpha > 1$ より $a_0 \geq 1$ であることに注意せよ. x/y を α の n 番目の近似分数とすると,

$$\frac{x}{y} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

である. このとき, y/x は

$$\frac{y}{x} = 0 + \frac{1}{a_0} + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

となり, $1/\alpha$ の $n+1$ 番目の近似分数である.

$0 < \alpha < 1$ のときは, $\alpha > 1$ の場合を $1/\alpha$ に適用すればよい. つまり, $1/\alpha$ の連分数展開を

$$\frac{1}{\alpha} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

とすれば, $1/(1/\alpha) = \alpha$ の連分数展開は

$$\alpha = 0 + \frac{1}{a_0} + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

となる. x/y を α の n 番目の近似分数とすれば, y/x は $1/\alpha$ の $n-1$ 番目の近似分数である. □

[定理 2.5] m を平方数でない正の整数とし, r を $0 < |r| < \sqrt{d}$ なる整数とする. さらに, (x, y) を Diophantus 方程式

$$x^2 - my^2 = r$$

の正整数解で $\gcd(x, y) = 1$ なるものとする. このとき, x/y は $\sqrt{m}$ の近似分数である.

[証明] $0 < r < \sqrt{m}$ のとき,

$$(x - \sqrt{m}y)(x + \sqrt{m}y) = x^2 - my^2 = r > 0.$$

これと $x + y\sqrt{m} > 0$ より, $x - y\sqrt{m} > 0$. この両辺に $2y\sqrt{m}$ を加えると,

$$x + y\sqrt{m} > 2y\sqrt{m}.$$

よって,

$$\begin{aligned}\left|\sqrt{m} - \frac{x}{y}\right| &= \left|\frac{x - y\sqrt{m}}{y}\right| = \left|\frac{x^2 - my^2}{y(x + y\sqrt{m})}\right| \\ &= \frac{r}{y(x + y\sqrt{m})} < \frac{r}{y(2y\sqrt{m})} \\ &= \frac{r}{2y^2\sqrt{m}}.\end{aligned}$$

さらに, $r < \sqrt{m}$ より,

$$\frac{r}{2y^2\sqrt{m}} < \frac{\sqrt{m}}{2y^2\sqrt{m}} < \frac{1}{2y^2}.$$

ゆえに,

$$\left|\sqrt{m} - \frac{x}{y}\right| < \frac{1}{2y^2}.$$

m は平方数でないから, $\sqrt{m}$ は無理数である. したがって, 補題 2.2 より, x/y は $\sqrt{m}$ の近似分数である.

$-\sqrt{m} < r < 0$ のとき, $x^2 - my^2 = r$ の両辺を $-m$ で割ると,

$$y^2 - \frac{1}{m} \cdot x^2 = -\frac{r}{m}.$$

$r > 0$ のときと同様の議論によって, y/x が $1/\sqrt{m}$ の近似分数であることがいえる. したがって, 補題 2.4 より, $x/y = 1/(y/x)$ は $\sqrt{m} = 1/(1/\sqrt{m})$ の近似分数である. □

[注意 2.6] r が平方因子を持たないとき, Diophantus 方程式 $x^2 - my^2 = r$ のすべての正整数解 (x, y) について $\gcd(x, y) = 1$ が成り立つ. なぜなら, もし x, y を同時に割る素数 p が存在すれば, 左辺は p^2 の倍数であるが, これは右辺の r は平方因子を持たないことに矛盾する. したがって, このとき, 正整数解は (もし存在すれば) すべて $\sqrt{m}$ の近似分数になっている.

また, もし方程式 $x^2 - my^2 = r$ が $g = \gcd(x, y) > 1$ なる整数解 (x, y) を持つならば, r は g^2 の倍数でなければならず, $(x/g)^2 - m(y/g)^2 = r/g^2$ を満たす.

3 $\sqrt{m}$ の連分数展開

[補題 3.1] α を無理数, n を正の整数とする. このとき,

(i) $\lfloor \alpha + n \rfloor = \lfloor \alpha \rfloor + n$

(ii) $\left\lfloor \dfrac{\alpha}{n} \right\rfloor = \left\lfloor \dfrac{\lfloor \alpha \rfloor}{n} \right\rfloor$

が成り立つ. ただし, $\lfloor \alpha \rfloor$ は α 以下の整数で最大のものである.

[証明] (i) $a = \lfloor \alpha \rfloor$ とおくと, ある実数 β が存在して, $\alpha = a + \beta$ かつ $0 \leq \beta < 1$. よって,

$$\alpha + n = a + n + \beta.$$

したがって,

$$\lfloor \alpha + n \rfloor = a + n = \lfloor \alpha \rfloor + n.$$

(ii) $a = \lfloor \alpha/n \rfloor$ とおくと, $a \leq \alpha/n$ より, $na \leq \alpha$ となる. na は整数だから, $na \leq \lfloor \alpha \rfloor$. よって,

$$a = \frac{na}{n} \leq \frac{\lfloor \alpha \rfloor}{n} \leq \frac{\alpha}{n}.$$

1 番目の不等式から $\lfloor \alpha/n \rfloor \leq \lfloor \lfloor \alpha \rfloor /n \rfloor$ が得られ, 2 番目の不等式から $\lfloor \lfloor \alpha \rfloor /n \rfloor \leq \lfloor \alpha/n \rfloor$ が得られる. これらから, 求める等式が得られる. □

[定理 3.2] $\sqrt{m}$ の連分数展開を

$$\sqrt{m} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots \tag{4}$$

とし, p_n/q_n を n 番目の近似分数とする. $S_0 = 0$, $T_0 = 1$ とし,

$$\begin{aligned} \alpha_n &= \frac{\sqrt{m} + S_n}{T_n}, \\ A_n &= \left\lfloor \frac{\lfloor \sqrt{m} \rfloor + S_n}{T_n} \right\rfloor, \\ S_{n+1} &= A_n T_n - S_n, \\ T_{n+1} &= \frac{m - S_{n+1}^2}{T_n} \end{aligned}$$

によって α_n, A_n, S_n, T_n を順次定める. このとき,

(i) $\alpha_n = a_n + 1/\alpha_{n+1}$, $\lfloor \alpha_n \rfloor = A_n = a_n$ $(n = 0, 1, 2, \ldots)$

(ii) S_n, T_n は整数 $(n = 0, 1, 2, \ldots)$

(iii) $0 < S_n < \sqrt{m}$ $(n = 1, 2, \ldots)$, $0 < T_n < 2\sqrt{m}$ $(n = 0, 1, 2, \ldots)$

(iv) $p_n^2 - m q_n^2 = (-1)^{n+1} T_{n+1}$ $(n = 0, 1, 2, \ldots)$

が成り立つ.

[証明] (i)　補題 3.1 を適用すると,

$$\lfloor \alpha_n \rfloor = \left\lfloor \frac{\sqrt{m} + S_n}{T_n} \right\rfloor = \left\lfloor \frac{\lfloor \sqrt{m} + S_n \rfloor}{T_n} \right\rfloor = \left\lfloor \frac{\lfloor \sqrt{m} \rfloor + S_n}{T_n} \right\rfloor = A_n.$$

任意の整数 $n \geq 0$ に対して,

$$\begin{aligned} \alpha_n - A_n &= \frac{\sqrt{m} + S_n}{T_n} - A_n = \frac{\sqrt{m} - (A_n T_n - S_n)}{T_n} \\ &= \frac{\sqrt{m} - S_{n+1}}{T_n} = \frac{(\sqrt{m} - S_{n+1})(\sqrt{m} + S_{n+1})}{T_n(\sqrt{m} + S_{n+1})} \\ &= \frac{m - S_{n+1}^2}{T_n(\sqrt{m} + S_{n+1})} = \frac{T_{n+1}}{\sqrt{m} + S_{n+1}} \\ &= \frac{1}{\alpha_{n+1}}. \end{aligned}$$

すなわち,

$$A_n = \lfloor \alpha_n \rfloor, \quad \alpha_n = A_n + \frac{1}{\alpha_{n+1}}.$$

$\alpha_0 = \sqrt{m}$ だから, $\sqrt{m}$ の連分数展開

$$\sqrt{m} = A_0 + \frac{1}{A_1} + \frac{1}{A_2} + \cdots + \frac{1}{A_n} + \cdots$$

が得られる. 無理数の連分数展開は一意的[4]だから, すべての整数 $n \geq 0$ に対して $A_n = a_n$ が成り立つ.

(ii)　n に関する数学的帰納法により証明する.

$n = 0$ のとき, $S_0 = 0$, $T_0 = 1$ より明らか.

$n = 1$ のとき,

$$S_1 = a_0 T_0 - S_0 = a_0 \in \mathbb{Z},$$
$$T_1 = \frac{m - S_1^2}{T_0} = m - a_0^2 \in \mathbb{Z}.$$

一般に, $n \geq 2$ のとき, $0 \leq k < n$ なる整数 k について主張が正しいと仮定する.

$S_n \in \mathbb{Z}$ は, S_n の定義からすぐにわかる.

$T_{n-1} = (m - S_{n-1}^2)/T_{n-2}$ より,

$$\frac{m - S_{n-1}^2}{T_{n-1}} = T_{n-2} \in \mathbb{Z}.$$

これより,

$$\begin{aligned} T_n = \frac{m - S_n^2}{T_{n-1}} &= \frac{m - (a_{n-1}T_{n-1} - S_{n-1})^2}{T_{n-1}} \\ &= \frac{m - (a_{n-1}^2 T_{n-1}^2 - 2a_{n-1}S_{n-1}T_{n-1} + S_{n-1}^2)}{T_{n-1}} \\ &= a_{n-1}^2 T_{n-1} - 2a_{n-1}S_{n-1} + \frac{m - S_{n-1}^2}{T_{n-1}} \in \mathbb{Z}. \end{aligned}$$

よって, n のときも主張は正しい.

(iii)　まず, n に関する数学的帰納法によって, $\sqrt{m} - S_n > 0$ かつ $T_n > 0$ を証明する.

$n = 0$ のとき, $S_0 = 0$, $T_0 = 1$ より, 主張は正しい.

$n = 1$ のとき, $a_0 = \lfloor \sqrt{m} \rfloor$, $S_1 = a_0$, $T_1 = m - a_0^2$ より, 主張は正しい. ここで, m は平方数ではないので, $m > a_0^2$ である.

一般に, $n \geq 2$ のとき, $0 \leq k < n$ なる整数 k について主張が正しいと仮定する. $T_{n-1} > 0$ より,

$$\begin{aligned} S_n &= a_{n-1}T_{n-1} - S_{n-1} \\ &< \alpha_{n-1}T_{n-1} - S_{n-1} \\ &= (S_{n-1} + \sqrt{d}) - S_{n-1} \\ &= \sqrt{d}. \end{aligned}$$

すなわち, $\sqrt{d} - S_n > 0$ が成り立つ.

もし仮に $T_n < 0$ とすると,

$$T_n = \frac{m - S_n^2}{T_{n-1}} = \frac{(\sqrt{m} - S_n)(\sqrt{m} + S_n)}{T_{n-1}}$$

[4] 高木 [1], 第 2 章 §20 定理 2.3 を参照.

において, 帰納法の仮定 $T_{n-1} > 0$ と先に示した $\sqrt{m} - S_n > 0$ より, $\sqrt{m} + S_n < 0$ でなければならない. このとき,

$$a_{n-1}T_{n-1} - S_{n-1} = S_n < -\sqrt{m}.$$

よって,

$$a_{n-1}T_{n-1} < S_{n-1} - \sqrt{m}.$$

再び帰納法の仮定より $T_{n-1} > 0$ だから,

$$0 < S_{n-1} - \sqrt{m}.$$

ところが, これは帰納法の仮定 $\sqrt{m} - S_{n-1} > 0$ に反する. したがって, $T_n > 0$ でなければならない.

以上より, すべての整数 $n \geq 0$ に対して, $\sqrt{m} - S_n > 0$ かつ $T_n > 0$ が示された.

任意の整数 $n \geq 0$ に対して, $\sqrt{m} - S_n > 0$, $\sqrt{m} - S_{n+1} > 0$, および $S_{n+1} = a_nT_n - S_n$ より,

$$T_n \leq a_nT_n = S_{n+1} + S_n < 2\sqrt{m}.$$

最後に, $S_n > 1$ を各整数 $n \geq 1$ に対して証明する. まず, $S_1 = a_0 > 0$ である. $n \geq 2$ のとき, $\alpha_n = 1/(\alpha_{n-1} - a_{n-1}) > 1$ より,

$$1 < \frac{\sqrt{m} + S_n}{T_n}.$$

両辺に $\sqrt{m} - S_n (> 0)$ を掛けると,

$$\sqrt{m} - S_n < \frac{m - S_n^2}{T_n} = T_{n-1}.$$

$\alpha_{n-1} = 1/(\alpha_{n-2} - a_{n-2}) > 1$ より, $a_{n-1} \geq 1$ だから,

$$T_{n-1} \leq a_{n-1}T_{n-1}.$$

さらに, $\sqrt{m} - S_{n-1} > 0$ より,

$$a_{n-1}T_{n-1} = S_{n-1} + S_n < \sqrt{m} + S_n.$$

ゆえに,

$$\sqrt{m} - S_n < \sqrt{m} + S_n.$$

これより, $2S_n > 0$. したがって, $S_n > 0$.

(iv)　(i) より

$$\sqrt{m} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \frac{1}{\alpha_{n+1}}$$

であるから,

$$\sqrt{m} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}$$

が成り立つ[5]. $\alpha_{n+1} = (\sqrt{m} + S_{n+1})/T_{n+1}$ より,

$$\sqrt{m} = \frac{(\sqrt{m} + S_{n+1})p_n + T_{n+1}p_{n-1}}{(\sqrt{m} + S_{n+1})q_n + T_{n+1}q_{n-1}}.$$

分母を払って整理すると,

$$mq_n + (S_{n+1}q_n + T_{n+1}q_{n-1})\sqrt{m} = (S_{n+1}p_n + T_{n+1}p_{n-1}) + p_n\sqrt{m}.$$

m は平方数でないので, $\sqrt{m}$ は無理数である. ゆえに,

$$mq_n = S_{n+1}p_n + T_{n+1}p_{n-1},$$
$$p_n = S_{n+1}q_n + T_{n+1}q_{n-1}.$$

よって, 最初の式の両辺に q_n を掛け, 2 番目の式の両辺に p_n を掛けると,

$$mq_n^2 = S_{n+1}p_nq_n + T_{n+1}p_{n-1}q_n,$$
$$p_n^2 = S_{n+1}p_nq_n + T_{n+1}p_nq_{n-1}.$$

ゆえに,

$$\begin{aligned} p_n^2 - mq_n^2 &= T_{n+1}(p_{n-1}q_n - p_nq_{n-1}) \\ &= (-1)^{n-1}T_{n+1} = (-1)^{n+1}T_{n+1}. \end{aligned}$$

□

[注意 3.3] a_n を計算するとき, 実数列 α_n の値を求める必要はなく, 整数列 A_n, S_n, T_n のみ計算すればよい.

4 循環連分数と 2 次無理数

連分数の展開が途中から循環するものを**循環連分数**という. 特に, 最初から循環しているものを**純循環連分数**という. 循環の最小の周期のことを, その連分数の**周期**という.

[例 4.1] $\sqrt{7}$ の連分数展開は

$$\sqrt{7} = 2 + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \frac{1}{4} + \cdots$$

である. 右辺は循環連分数であり, 周期は 4 である.

$\lfloor\sqrt{7}\rfloor + \sqrt{7}$ の連分数展開は

$$\lfloor\sqrt{7}\rfloor + \sqrt{7} = 4 + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \frac{1}{4} + \cdots$$

である. 右辺は純循環連分数であり, 周期は 4 である.

[5] n に関する数学的帰納法で証明できる. 例えば, 高木 [1], 第 2 章 §19 を参照.

整数係数の 2 次方程式

$$ax^2 + by^2 + c = 0, \quad \gcd(a, b, c) = 1 \tag{5}$$

において, その判別式

$$D = b^2 - 4ac$$

が平方数でないとき, (5) の解 θ は無理数である. このとき, θ を判別式 D に属する **2 次無理数**という. また, D を θ の**判別式**という.

方程式 (5) の解は

$$\theta = \frac{-b + \sqrt{D}}{2a}, \quad \overline{\theta} = \frac{-b - \sqrt{D}}{2a}$$

である. これらを互いに**共役**な 2 次無理数という.

以後, 2 次無理数というときには, 実数であるものだけを考える.

[例 4.2] m を平方数でない正の整数とすると, $\sqrt{m}$ は 2 次方程式 $x^2 - m = 0$ の解で, その判別式は $4m$ である. もう 1 つの解は $-\sqrt{m}$ であり, $\sqrt{m}$ と $-\sqrt{m}$ は互いに共役な 2 次無理数である.

また, $\lfloor\sqrt{m}\rfloor + \sqrt{m}$ は 2 次方程式 $(x - \lfloor\sqrt{m}\rfloor)^2 - m = 0$ の解で, その判別式は同じく $4m$ である. もう 1 つの解は $\lfloor\sqrt{m}\rfloor - \sqrt{m}$ であり, 2 つの解は互いに共役な 2 次無理数である.

$\sqrt{m}$ と $\lfloor\sqrt{m}\rfloor + \sqrt{m}$ は同じ判別式に属する 2 次無理数である.

(実の)2 次無理数 θ とそれと共役な $\overline{\theta}$ について, 不等式

$$-1 < \overline{\theta} < 0, \quad 1 < \theta$$

が成り立つとき, θ を**簡約された 2 次無理数**という.

[補題 4.3] (i) 2 次無理数は循環連分数に展開される.

(ii) 循環連分数は 2 次無理数である.

(iii) 簡約された 2 次無理数は純循環連分数に展開される.

(iv) 純循環連分数は簡約された 2 次無理数である.

[証明] 高木 [1], 第 3 章定理 3.3, 定理 3.6, 定理 3.6′, §32 問題 2 を参照. □

[例 4.4] m を平方数でない正の整数とする. $\sqrt{m}$ は 2 次無理数なので, 循環連分数に展開される.

また, $\lfloor\sqrt{m}\rfloor + \sqrt{m}$ は

$$-1 < \lfloor\sqrt{m}\rfloor - \sqrt{m} < 0, \quad 1 < \lfloor\sqrt{m}\rfloor + \sqrt{m}$$

を満たすので, 簡約された 2 次無理数である. よって, その連分数展開は純循環である.

$\sqrt{m}$ の連分数展開を

$$\sqrt{m} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

とすると, $a_0 = \lfloor \sqrt{m} \rfloor$ なので, $\lfloor \sqrt{m} \rfloor + \sqrt{m}$ の連分数展開は

$$\lfloor \sqrt{m} \rfloor + \sqrt{m} = 2a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

となる. 両者の連分数展開は最初の項 (a_0 と $2a_0$) を除いてすべて一致する. よって, 連分数展開の周期は一致する. しかも, 後者の連分数展開は純循環, すなわち最初から循環しているので, その周期を n_0 とすれば, $\sqrt{m}$ の連分数展開は a_1 から a_{n_0+1} までのパターンを延々と繰り返すことがわかる.

5 Pell 方程式 $x^2 - my^2 = \pm 1$ の正整数解の一般項

m を平方数でない正の整数とし, a, b を正の整数とする. $x_0 = 1$, $y_0 = 0$ とおき,

$$\begin{aligned} x_n &= ax_{n-1} + bmy_{n-1}, \\ y_n &= bx_{n-1} + ay_{n-1} \end{aligned} \qquad (n = 0, 1, 2, \ldots) \tag{6}$$

とおく.

[補題 5.1] (x_n, y_n) の一般項は

$$\begin{aligned} x_n &= \frac{1}{2}\left((a + b\sqrt{m})^n + (a - b\sqrt{m})^n\right), \\ y_n &= \frac{1}{2\sqrt{m}}\left((a + b\sqrt{m})^n - (a - b\sqrt{m})^n\right). \end{aligned}$$

[証明] 式 (6) を行列で表せば,

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a & bm \\ b & a \end{pmatrix} \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} = \cdots = \begin{pmatrix} a & bm \\ b & a \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

$P = \begin{pmatrix} 1/2 & 1/2 \\ -1/(2\sqrt{m}) & 1/(2\sqrt{m}) \end{pmatrix}$ とおくと, $P^{-1} = \begin{pmatrix} 1 & -\sqrt{m} \\ 1 & \sqrt{m} \end{pmatrix}$ であり,

$$P^{-1} \begin{pmatrix} a & bm \\ b & a \end{pmatrix} P = \begin{pmatrix} a - b\sqrt{m} & 0 \\ 0 & a + b\sqrt{m} \end{pmatrix}$$

と対角化できる.

$$\begin{pmatrix} a & bm \\ b & a \end{pmatrix}^n = P \begin{pmatrix} (a - b\sqrt{m})^n & 0 \\ 0 & (a + b\sqrt{m})^n \end{pmatrix} P^{-1}$$

だから,

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} \dfrac{1}{2}\left((a + b\sqrt{m})^n + (a - b\sqrt{m})^n\right) \\ \dfrac{1}{2\sqrt{m}}\left((a + b\sqrt{m})^n - (a - b\sqrt{m})^n\right) \end{pmatrix}.$$

これが求める一般項である. □

[補題 5.2] すべての整数 $n \geq 1$ に対して

$$x_n \pm y_n\sqrt{m} = (a \pm b\sqrt{m})^n.$$

ただし, $\pm$ は複号同順とする.

[証明] n に関する数学的帰納法により証明する.

$n = 1$ のときは明らか.

$n-1$ のとき定理の主張が正しいと仮定すると, 漸化式 (6) から

$$\begin{aligned}(a \pm b\sqrt{m})^n &= (a \pm b\sqrt{m})(a \pm b\sqrt{m})^{n-1} \\ &= (a \pm b\sqrt{m})(x_{n-1} \pm y_{n-1}\sqrt{m}) \\ &= (ax_{n-1} + bmy_{n-1}) \pm (bx_{n-1} + ay_{n-1})\sqrt{m} \\ &= x_n \pm y_n\sqrt{m}.\end{aligned}$$

よって, n のときも主張は正しい. □

[補題 5.3] 任意の整数 $n \geq 1$ に対して, $x_n < x_{n+1}$, $y_n < y_{n+1}$ が成り立つ.

[証明] n に関する数学的帰納法により証明する.

最初に, $a \geq 1$, $b \geq 1$, $m \geq 1$ に注意しておく.

$n = 1$ のとき, 漸化式 (6) より,

$$\begin{aligned}x_2 &= ax_1 + bmy_1 = a^2 + mb^2 > a = x_1, \\ y_2 &= bx_1 + ay_1 = 2ab > b = y_1.\end{aligned}$$

$1 \leq k \leq n-1$ なる任意の整数 k に対して定理の主張が正しいと仮定すると,

$$\begin{aligned}1 \leq a = x_1 < x_2 < \cdots < x_{n-1}, \\ 1 \leq b = y_1 < y_2 < \cdots < y_{n-1}.\end{aligned}$$

これより,

$$\begin{aligned}x_n &= ax_{n-1} + bmy_{n-1} > x_{n-1}, \\ y_n &= bx_{n-1} + ay_{n-1} > y_{n-1}\end{aligned}$$

となり, n のときにも正しいことがいえる. □

[定理 5.4] (i) (a, b) を Pell 方程式 $x^2 - my^2 = 1$ の正整数解とするとき, 漸化式 (6) で定まる (x_n, y_n) $(n \geq 1)$ もその正整数解である.

(ii) (a, b) を Pell 方程式 $x^2 - my^2 = -1$ の正整数解とするとき, 漸化式 (6) で定まる (x_n, y_n) $(n \geq 1)$ は, n が奇数のとき方程式 $x^2 - my^2 = -1$ の正整数解であり, n が偶数のとき方程式 $x^2 - my^2 = 1$ の正整数解である.

[証明] 補題 5.2 より,

$$\begin{aligned} x_n^2 - my_n^2 &= (x_n + y_n\sqrt{m})(x_n - y_n\sqrt{m}) \\ &= (a + b\sqrt{m})^n (a - b\sqrt{m})^n \\ &= (a^2 - mb^2)^n. \end{aligned}$$

(i) $a^2 - mb^2 = 1$ より,

$$x_n^2 - my_n^2 = 1.$$

よって, (x_n, y_n) は方程式 $x^2 - my^2 = 1$ の正整数解である.

(ii) $a^2 - mb^2 = -1$ より,

$$x_n^2 - my_n^2 = (-1)^n.$$

よって, (x_n, y_n) は, n が奇数のとき方程式 $x^2 - my^2 = -1$ の正整数解であり, n が偶数のとき方程式 $x^2 - my^2 = 1$ の正整数解である. □

[定理 5.5] (a, b) を Pell 方程式 $x^2 - my^2 = -1$ の最小解とするとき, 漸化式 (6) で定まる (x_n, y_n) $(n \geq 1)$ が Pell 方程式 $x^2 - my^2 = \pm 1$ の正整数解のすべてである.

[証明] 定理 5.4 より, (x_n, y_n) $(n \geq 1)$ が Pell 方程式 $x^2 - my^2 = \pm 1$ の正整数解であること, より詳しく述べると

$$x_n^2 - my_n^2 = (-1)^n \quad (n = 1, 2, \ldots)$$

であることが既に示されている. あとは, 正整数解が (x_n, y_n) $(n \geq 1)$ 以外に存在しないことを示せばよい.

(x, y) を Pell 方程式 $x^2 - my^2 = \pm 1$ の任意の正整数解とし,

$$x^2 - my^2 = (-1)^e$$

とする. ここで, $e = 0$ または 1 である.

$a + b\sqrt{m} > 1$ だから, ある整数 $k \geq 0$ が存在して

$$(a + b\sqrt{m})^k < x + y\sqrt{m} \leq (a + b\sqrt{m})^{k+1}.$$

辺々を $(a + b\sqrt{m})^k$ で割ると,

$$1 < \frac{x + y\sqrt{m}}{(a + b\sqrt{m})^k} \leq a + b\sqrt{m}.$$

$(a-b\sqrt{m})(a+b\sqrt{m})=a^2-mb^2=-1$ より,

$$\frac{1}{(a+b\sqrt{m})^k}=(-1)^k(a-b\sqrt{m})^k=(-1)^k(x_k-y_k\sqrt{m})$$

であるから,

$$1<(-1)^k(x+y\sqrt{m})(x_k-y_k\sqrt{m})\leq a+b\sqrt{m}.$$

ここで,

$$\begin{aligned}s+t\sqrt{m}&=(-1)^k(x+y\sqrt{m})(x_k-y_k\sqrt{m})\\&=(-1)^k\left((xx_k-myy_k)+(yx_k-xy_k)\sqrt{m}\right)\\&=(-1)^k(xx_k-myy_k)+(-1)^k(yx_k-xy_k)\sqrt{m}\end{aligned}$$

とおくと,

$$s-t\sqrt{m}=(-1)^k(xx_k-myy_k)-(-1)^k(yx_k-xy_k)\sqrt{m}$$

であるから,

$$\begin{aligned}s^2-mt^2&=(xx_k-myy_k)^2-m(yx_k-xy_k)^2\\&=(x^2-my^2)(x_k^2-my_k^2)\\&=(-1)^{k+e}.\end{aligned}$$

この式と $1<s+t\sqrt{m}$ を用いると,

$$0<(-1)^{k+e}(s-t\sqrt{m})<1.$$

$k+e$ が偶数のとき,

$$0<s-t\sqrt{m}<1.$$

$k+e$ が奇数のとき,

$$-1<s-t\sqrt{m}<0.$$

いずれにせよ,

$$\begin{aligned}s&=\frac{1}{2}\left((s+t\sqrt{m})+(s-t\sqrt{m})\right)>0,\\t&=\frac{1}{2\sqrt{m}}\left((s+t\sqrt{m})-(s-t\sqrt{m})\right)>0.\end{aligned}$$

よって, (s,t) は Pell 方程式 $x^2-my^2=\pm1$ の正整数解である. (a,b) が最小解であることと $s+t\sqrt{m}\leq a+b\sqrt{m}$ より,

$$s=a,\quad t=b.$$

ゆえに,

$$\begin{aligned} x+y\sqrt{m} &= \frac{s+t\sqrt{m}}{(-1)^k(x_k-y_k\sqrt{m})} \\ &= (s+t\sqrt{m})(x_k+y_k\sqrt{m}) \\ &= (a+b\sqrt{m})(a+b\sqrt{m})^k \\ &= (a+b\sqrt{m})^{k+1} \\ &= x_{k+1}+y_{k+1}\sqrt{m}. \end{aligned}$$

したがって, (x_n, y_n) $(n \geq 1)$ 以外に正整数解はない. □

[注意 5.6] 記号を上の定理の通りとするとき, 補題 5.3 により, $(x_2, y_2) = (a^2+mb^2, 2ab)$ が Pell 方程式 $x^2 - my^2 = 1$ の最小解である.

[注意 5.7] (a, b) を Pell 方程式 $x^2 - my^2 = 1$ の最小解とするとき, 漸化式 (6) で定まる (x_n, y_n) $(n \geq 1)$ がその正整数解のすべてであることも, 同様の議論により証明できる.

[例 5.8] $m = 2$ のとき, Pell 方程式 $x^2 - 2y^2 = -1$ の最小解は $(1, 1)$ である.

Pell 方程式 $x^2 - 2y^2 = \pm 1$ の正整数解 (x_n, y_n) の一般項は

$$\begin{aligned} x_n &= \frac{1}{2}\left((1+\sqrt{2})^n + (1-\sqrt{2})^n\right), \\ y_n &= \frac{1}{2\sqrt{2}}\left((1+\sqrt{2})^n - (1-\sqrt{2})^n\right). \end{aligned}$$

6 Pell 方程式 $x^2 - my^2 = \pm 1$ の最小解の計算方法

この節では, Pell 方程式

$$x^2 - my^2 = \pm 1 \tag{7}$$

の最小解の計算方法について考察する. ただし, m は平方数でない 2 以上の整数とする.

[定理 6.1] (x, y), (x', y') を方程式 (7) の 2 つの正整数解とする. このとき, 次の 3 つの条件はすべて同値である:

(i) $x' < x$ または $y' < y$

(ii) $x' < x$ かつ $y' < y$

(iii) $x + y\sqrt{m} < x' + y'\sqrt{m}$

また,

$$(x,y)=(x',y') \Leftrightarrow x=x' \text{ または } y=y',$$
$$(x,y)\neq(x',y') \Leftrightarrow (x'<x \text{ かつ } y'<y) \text{ または } (x<x' \text{ かつ } y<y')$$

が成り立つ.

[証明] (i)⇒(ii)　$x'<x$ ならば,

$$\begin{aligned} my'^2 &= x'^2 \pm 1 \leq x'^2+1 \\ &= x'^2+2x'+1-2x' \\ &< (x'+1)^2-1 \leq x^2-1 \\ &\leq my^2. \end{aligned}$$

ゆえに, $y'<y$. 逆に, $y'<y$ ならば,

$$\begin{aligned} x'^2 &= my'^2 \pm 1 \leq my'^2+1 \\ &= m(y'^2+2y'+1)-(2my'+m-1) \\ &< m(y'+1)^2-1 \leq my^2-1 \\ &\leq x^2. \end{aligned}$$

ゆえに, $x'<x$.

(ii)⇒(iii)　明らか.

(iii)⇒(i)　対偶を示せばよい. $x\leq x'$ かつ $y\leq y'$ ならば, $x+y\sqrt{m}\leq x'+y'\sqrt{m}$.

後半の同値の証明は, 定理 1.1 と全く同じである. □

[注意 6.2] 方程式の右辺が ±1 でない場合に, 上の定理の (i)⇒(ii) が必ずしも成立しない例として, 方程式 $x^2-5y^2=-4$ の正整数解 $(1,1)$ と方程式 $x^2-5y^2=4$ の正整数解 $(3,1)$ がある.

定理 6.1 により, 2 つの Pell 方程式 $x^2-my^2=1$ と $x^2-my^2=-1$ の両方を合わせて最小の正整数解を考えることができる. これを方程式 $x^2-my^2=\pm1$ の**最小解**と呼ぶことにする.

(x,y) が Pell 方程式 (7) の整数解ならば, $\gcd(x,y)=1$ である. なぜなら, もし仮に x, y をともに割る素数 p が存在すれば, (7) の左辺は p^2 の倍数になる. ところが, 右辺は ±1 なので, これは不可能である.

定理 2.5 により, Pell 方程式 (7) のすべての正整数解は, $\sqrt{m}$ を連分数展開したときの近似分数の分子と分母に現れる. つまり, 漸化式 (3) を順次計算して $p_n^2-mq_n^2=\pm1$ を満たす (p_n,q_n) が現れたら, それが Pell 方程式 (7) の正整数解である.

定理 3.2 によると, $T_{n+1} > 1$ より,

$$\begin{aligned}&(p_n, q_n) \text{ は Pell 方程式 (7) の正整数解}\\ &\Leftrightarrow (-1)^{n+1} T_{n+1} = \pm 1\\ &\Leftrightarrow T_{n+1} = 1\end{aligned}$$

が成り立つ.

次の定理は, Pell 方程式 (7) の整数解の存在を保証する.

[定理 6.3] α_n, S_n, T_n 等の記号は定理 3.2 の通りとする.

$\sqrt{m}$ の連分数展開の周期を n_0 (≥ 1) とする. このとき,

(i) $T_{n_0 j+i} = T_i$ $(i = 0, 1, 2, \ldots, n_0 - 1;\ j = 0, 1, 2, \ldots)$. 特に, $T_{n_0 j} = 1$ $(j = 0, 1, 2, \ldots)$.

(ii) $T_{n+1} = 1$ ならば, $n_0 \mid n + 1$

が成り立つ.

[証明] (i) $\sqrt{m}$ の連分数展開を

$$\sqrt{m} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

とすると, $a_0 = \lfloor \sqrt{m} \rfloor$ なので, $\lfloor \sqrt{m} \rfloor + \sqrt{m}$ の連分数展開は

$$\lfloor \sqrt{m} \rfloor + \sqrt{m} = 2a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

となる. このとき, $S_0 = 0$ と置く代わりに $S_0 = \lfloor \sqrt{m} \rfloor$ と置くことにより, $\lfloor \sqrt{m} \rfloor + \sqrt{m}$ に関して定理 3.2 の (i), (ii), (iii) が成り立つことが, $\sqrt{m}$ のときと同様に証明できる. しかも, 両者の α_n, S_n, T_n の値が, S_0 と α_0 を除いてすべて一致する. さらに, $\lfloor \sqrt{m} \rfloor + \sqrt{m}$ は

$$-1 < \lfloor \sqrt{m} \rfloor - \sqrt{m} < 0, \quad 1 < \lfloor \sqrt{m} \rfloor + \sqrt{m}$$

を満たすので, 簡約された 2 次無理数である. ゆえに, その連分数展開は純循環である (補題 4.3). $\sqrt{m}$ と $\lfloor \sqrt{m} \rfloor + \sqrt{m}$ の連分数展開は最初の項を除いてすべて一致する. よって, 両者の連分数展開の周期は一致する. すなわち, $\lfloor \sqrt{m} \rfloor + \sqrt{m}$ の連分数展開の周期は n_0 である. したがって, $\alpha_0 = \alpha_{n_0 j}$ $(j = 1, 2, \ldots)$ が成り立つ. さらに,

$$\lfloor \sqrt{m} \rfloor + \sqrt{m} = \alpha_0 = \alpha_{n_0 j} = \frac{\sqrt{m} + S_{n_0 j}}{T_{n_0 j}}.$$

両辺に $T_{n_0 j}$ を掛けると,

$$T_{n_0 j} \lfloor \sqrt{m} \rfloor + T_{n_0 j} \sqrt{m} = S_{n_0 j} + \sqrt{m}.$$

m は平方数でないので, $\sqrt{m}$ は無理数である. したがって, $T_{n_0 j} = 1 (= T_0)$, $S_{n_0 j} = \lfloor \sqrt{m} \rfloor (= S_0)$ が得られる.

(ii)　$T_{n+1}=1$ とすると,

$$\alpha_{n+1}=S_{n+1}+\sqrt{m}.$$

α_{n+1} は $\lfloor\sqrt{m}\rfloor+\sqrt{m}$ の純循環な連分数展開の途中に現れるものなので, α_{n+1} の連分数展開も純循環である. したがって, α_{n+1} は簡約された 2 次無理数である (補題 4.3). ゆえに,

$$-1<S_{n+1}-\sqrt{m}<0.$$

よって, $S_{n+1}=\lfloor\sqrt{m}\rfloor$ となり, $\alpha_{n+1}=\alpha_0$ が得られる. これは, $n_0 \mid n+1$ を意味する. □

n_0 を $\sqrt{m}$ の連分数展開の周期とする.

$n+1$ が n_0 の倍数でないとき, (p_n, q_n) は $x^2-my^2=\pm1$ の解ではない.

$n+1$ が n_0 の倍数であるとき, すなわち $n+1=n_0 j$ $(j=1, 2, \ldots)$ のとき,

$$p_{n_0 j-1}^2-mq_{n_0 j-1}^2=(-1)^{n_0 j}T_{n_0 j}=(-1)^{n_0 j}.$$

n_0 が偶数の場合,

- $(p_{n_0 j-1}, q_{n_0 j-1})$ $(j=1, 2, \ldots)$ が $x^2-my^2=1$ のすべての正整数解

となる. 定理 2.1 により, 正整数解は小さい順に現れるので, $j=1$ のときの解 (p_{n_0-1}, q_{n_0-1}) が最小解である. 方程式 $x^2-my^2=-1$ には整数解がない.

n_0 が奇数の場合,

- $(p_{n_0(2i-1)-1}, q_{n_0(2i-1)-1})$ $(i=1, 2, \ldots)$ が $x^2-my^2=-1$ の正整数解
- $(p_{n_0(2i)-1}, q_{n_0(2i)-1})$ $(i=1, 2, \ldots)$ が $x^2-my^2=1$ の正整数解

である. $i=1$ のときの解 (p_{n_0-1}, q_{n_0-1}) および (p_{2n_0-1}, q_{2n_0-1}) が, それぞれの方程式の最小解である.

最後に, 方程式 $x^2-my^2=\pm1$ の最小解を計算する手順をまとめると, 以下のとおりである:

[手順 6.4] m を平方数でない正の整数とする. $\sqrt{m}$ の連分数展開を定理 3.2 によって求めるとき, $T_{n+1}=1$ となれば, (p_n, q_n) が, 方程式 $x^2-my^2=\pm1$ の最小解である.

7　方程式 $x^2-my^2=\pm4$ の正整数解の一般項

m を平方数でない正の整数とする.

(x, y) を方程式 $x^2-my^2=\pm4$ の任意の整数解とする.

$m\equiv0 \pmod 4$ のとき,

$$x^2\equiv0 \pmod 4.$$

すなわち, x^2 は 4 の倍数, したがって, x は偶数である. $m=4m_1$, $x=2x'$ とおくと, m_1, x' は整数であり, (x', y) は $x'^2-m_1y^2=\pm1$ を満たす.

逆に, 方程式 $x^2 - m_1 y^2 = \pm 1$ の任意の整数解 (x', y') は, $(2x')^2 - m(y')^2 = \pm 4$ を満たす.

したがって, m が 4 の倍数のとき, 方程式 $x^2 - my^2 = \pm 4$ の整数解は, 方程式 $x^2 - m_1 y^2 = \pm 1$ の整数解を求めることに帰着する.

$m \equiv 2 \pmod 4$ のとき, すなわち $2 \mid m$ かつ $4 \nmid m$ のとき, $m = 2m_2$ とおくと, $2 \nmid m_2$ であって,

$$x^2 = 2m_2 y^2 \pm 4.$$

よって, x は 2 の倍数である. $x = 2x'$ とおくと,

$$m_2 y^2 = 2x'^2 \pm 2.$$

$2 \nmid m_2$ だから, $2 \mid y$ でなければならない. $y = 2y'$ とおくと, (x', y') は $x'^2 - m_2 y'^2 = \pm 1$ を満たす.

逆に, 方程式 $x^2 - my^2 = \pm 1$ の任意の整数解 (x', y') は, $(2x')^2 - m(2y')^2 = \pm 4$ を満たす.

したがって, m が 4 の倍数のとき, 方程式 $x^2 - my^2 = \pm 4$ の整数解は, 方程式 $x^2 - m_2 y^2 = \pm 1$ の整数解を求めることに帰着する.

$m \equiv 3 \pmod 4$ のとき,

$$x^2 - 3y^2 \equiv 0 \pmod 4.$$

もし仮に x が奇数だとすると, $x^2 \equiv 1 \pmod 4$ より

$$3y^2 \equiv 1 \pmod 4.$$

任意の整数 y に対して $y^2 \equiv 0, 1 \pmod 4$ だから, これは不可能である. ゆえに, x は偶数でなければならない. したがって, y も偶数である. $x = 2x'$, $y = 2y'$ とおくと, x', y' は整数であり, (x', y') は $x'^2 - my'^2 = \pm 1$ を満たす.

逆に, 方程式 $x^2 - my^2 = \pm 1$ の任意の整数解 (x', y') は, $(2x')^2 - m(2y')^2 = \pm 4$ を満たす.

したがって, $m \equiv 3 \pmod 4$ のとき, 方程式 $x^2 - my^2 = \pm 4$ の整数解は, 方程式 $x^2 - my^2 = \pm 1$ の整数解を求めることに帰着する.

$m \equiv 1 \pmod 8$ のとき,

$$x^2 - y^2 \equiv 4 \pmod 8.$$

もし仮に x が奇数だとすると, $x^2 \equiv 1 \pmod 8$ より

$$y^2 \equiv 5 \pmod 8.$$

任意の整数 y に対して $y^2 \equiv 0, 1, 4 \pmod 8$ だから, これは不可能である. ゆえに, x は偶数でなければならない. したがって, y も偶数である. $x = 2x'$, $y = 2y'$ とおくと, x', y' は整数であり, (x', y') は $x'^2 - my'^2 = \pm 1$ を満たす.

逆に, 方程式 $x^2 - my^2 = \pm 1$ の任意の整数解 (x', y') は, $(2x')^2 - m(2y')^2 = \pm 4$ を満たす.

したがって, $m \equiv 1 \pmod 8$ のとき, 方程式 $x^2 - my^2 = \pm 4$ の整数解は, 方程式 $x^2 - my^2 = \pm 1$ の整数解を求めることに帰着する.

ここまでの議論と, Pell 方程式 $x^2 - my^2 = \pm 1$ に関する結果とから, 次の定理が得られる.

[定理 7.1] m を平方数でない正の整数, (a, b) を Pell 方程式 $x^2 - my^2 = \pm 1$ の最小解をとする. また, $x_0 = 1$, $y_0 = 0$ とおき,

$$\begin{aligned} x_n &= ax_{n-1} + bmy_{n-1}, \\ y_n &= bx_{n-1} + ay_{n-1} \end{aligned} \qquad (n = 0, 1, 2, \ldots)$$

とおく.

(i) $m \equiv 0 \pmod 4$ のとき, $(2x_n, y_n)$ が方程式 $x^2 - my^2 = \pm 4$ の正整数解のすべてであり, その最小解は $(2a, b)$ である.

(ii) $m \equiv 2, 3 \pmod 4$ または $m \equiv 1 \pmod 8$ のとき, $(2x_n, 2y_n)$ が方程式 $x^2 - my^2 = \pm 4$ の正整数解のすべてであり, その最小解は $(2a, 2b)$ である.

以上より, $m \equiv 5 \pmod 8$ のときが本質的だとわかる.

[定理 7.2] m を平方数でも 4 の倍数でもない正の整数とする. このとき, 方程式

$$x^2 - my^2 = \pm 4$$

の任意の整数解 (x, y) について,

$$x \equiv y \pmod 2$$

が成り立つ.

[証明] (x, y) を方程式 $x^2 - my^2 = \pm 4$ の整数解とすると,

$$x^2 - my^2 \equiv 0 \pmod 4.$$

$m \equiv 1$ または $3 \pmod 4$ のとき,

$$x^2 \pm y^2 \equiv 0 \pmod 4.$$

これより, $x^2 \pm y^2 \equiv 0 \pmod 2$. よって,

$$x \equiv x^2 \equiv \pm y^2 \equiv y^2 \equiv y \pmod 2.$$

$m \equiv 2 \pmod 4$ のとき,

$$x^2 - 2y^2 \equiv 0 \pmod 4.$$

これより, $x^2 - 2y^2 \equiv 0 \pmod 2$, すなわち $x^2 \equiv 0 \pmod 2$. よって, x は 2 で割れ, x^2 は 4 で割れる. したがって, $my^2 = x^2 \pm 4$ が 4 で割れる. もし仮に y が 2 で割れないとすると, m が 4 で割れて仮定に反する. ゆえに, y は 2 で割れなければならない. □

a, b を正の整数とする．$x_0 = 2$, $y_0 = 0$ とおき，

$$\begin{aligned} x_n &= \frac{1}{2}(ax_{n-1} + by_{n-1}m), \\ y_n &= \frac{1}{2}(ay_{n-1} + bx_{n-1}) \end{aligned} \qquad (n = 1, 2, \ldots) \tag{8}$$

とおく．

［補題 7.3］ (x_n, y_n) の一般項は

$$\begin{aligned} x_n &= \frac{1}{2^n}\left((a + b\sqrt{m})^n + (a - b\sqrt{m})^n\right), \\ y_n &= \frac{1}{2^n\sqrt{m}}\left((a + b\sqrt{m})^n - (a - b\sqrt{m})^n\right). \end{aligned}$$

［証明］ 漸化式 (8) を行列で表せば，

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \frac{1}{2}\begin{pmatrix} a & bm \\ b & a \end{pmatrix}\begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} = \cdots = \frac{1}{2^n}\begin{pmatrix} a & bm \\ b & a \end{pmatrix}^n \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

$P = \begin{pmatrix} 1/2 & 1/2 \\ -1/(2\sqrt{m}) & 1/(2\sqrt{m}) \end{pmatrix}$ とおくと，$P^{-1} = \begin{pmatrix} 1 & -\sqrt{m} \\ 1 & \sqrt{m} \end{pmatrix}$ であり，

$$P^{-1}\begin{pmatrix} a & bm \\ b & a \end{pmatrix} P = \begin{pmatrix} a - b\sqrt{m} & 0 \\ 0 & a + b\sqrt{m} \end{pmatrix}$$

と対角化できる．

$$\begin{pmatrix} a & bm \\ b & a \end{pmatrix}^n = P\begin{pmatrix} (a - b\sqrt{m})^n & 0 \\ 0 & (a + b\sqrt{m})^n \end{pmatrix} P^{-1}$$

だから，

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} \dfrac{1}{2^n}\left((a + b\sqrt{m})^n + (a - b\sqrt{m})^n\right) \\ \dfrac{1}{2^n\sqrt{m}}\left((a + b\sqrt{m})^n - (a - b\sqrt{m})^n\right) \end{pmatrix}.$$

これが求める一般項である． □

［補題 7.4］ a, b を正の整数とする．漸化式 (8) で定まる x_n, y_n について，$n = 1, 2, \ldots$ に対して，

$$\frac{x_n \pm y_n\sqrt{m}}{2} = \left(\frac{a \pm b\sqrt{m}}{2}\right)^n.$$

ただし，$\pm$ は複号同順とする．

［証明］ $n = 1$ のとき，

$$x_1 = \frac{a \cdot 2 + b \cdot 0 \cdot m}{2} = a, \quad y_1 = \frac{a \cdot 0 + b \cdot 2}{2} = b.$$

ゆえに,

$$\frac{x_1 \pm y_1\sqrt{m}}{2} = \frac{a \pm b\sqrt{m}}{2} \quad \text{(複号同順)}.$$

$n-1$ のとき, 定理の主張が正しいと仮定すると,

$$\begin{aligned}\left(\frac{a \pm b\sqrt{m}}{2}\right)^n &= \left(\frac{a \pm b\sqrt{m}}{2}\right)\left(\frac{a \pm b\sqrt{m}}{2}\right)^{n-1} \\ &= \left(\frac{a \pm b\sqrt{m}}{2}\right)\left(\frac{x_{n-1} \pm y_{n-1}\sqrt{m}}{2}\right) \\ &= \frac{1}{2}\left(\frac{ax_{n-1} + by_{n-1}m}{2} \pm \frac{ay_{n-1} + bx_{n-1}}{2}\sqrt{m}\right) \\ &= \frac{x_n \pm y_n\sqrt{m}}{2}.\end{aligned}$$

ただし, $\pm$ は複号同順とする. □

[補題 7.5] m, a, b を正の整数とする. m は, $m \equiv 1 \pmod 4$ を満たし, 平方数ではないとする. また, $a \equiv b \pmod 2$ とする. このとき, 漸化式 (8) で定まる x_n, y_n について, $n = 1, 2, \ldots$ に対して,

(i) x_n, y_n は正の整数

(ii) $x_n \equiv y_n \pmod 2$

が成り立つ.

さらに, a, b がともに偶数ならば, すべての整数 $n \geq 1$ に対して x_n, y_n は偶数である.

[証明] (i), (ii) を同時に n に関する数学的帰納法によって証明する.

$n = 1$ のとき,

$$x_1 = \frac{a \cdot 2 + b \cdot 0 \cdot m}{2} = a, \quad y_1 = \frac{a \cdot 0 + b \cdot 2}{2} = b.$$

ゆえに, x_1, y_1 は正の整数であって, $x_1 \equiv y_1 \pmod 2$.

$n-1$ のとき, 定理の主張が正しいと仮定する. $a \equiv b \equiv 0 \pmod 2$ または $x_{n-1} \equiv y_{n-1} \equiv 0 \pmod 2$ のときは, 明らかに

$$ax_{n-1} + by_{n-1}m \equiv 0 \pmod 2,$$
$$ay_{n-1} + bx_{n-1} \equiv 0 \pmod 2.$$

$a \equiv b \equiv 1 \pmod 2$ かつ $x_{n-1} \equiv y_{n-1} \equiv 1 \pmod 2$ のとき, $m \equiv 1 \pmod 4$ より,

$$ax_{n-1} + by_{n-1}m \equiv 1 \cdot 1 + 1 \cdot 1 \cdot 1 = 2 \equiv 0 \pmod 2,$$
$$ay_{n-1} + bx_{n-1} \equiv 1 \cdot 1 + 1 \cdot 1 = 2 \equiv 0 \pmod 2.$$

ゆえに, x_n, y_n は整数である. a, b, x_{n-1}, y_{n-1}, m はすべて正だから, x_n, y_n も正である. また,

$$\begin{aligned} 2(x_n - y_n) &= (ax_{n-1} + by_{n-1}m) - (ay_{n-1} + bx_{n-1}) \\ &\equiv (ax_{n-1} + by_{n-1}) - (ay_{n-1} + bx_{n-1}) \\ &= (a-b)(x_{n-1} - y_{n-1}) \\ &\equiv 0 \pmod 4. \end{aligned}$$

したがって, $x_n \equiv y_n \pmod 2$.

(iii)　n に関する数学的帰納法により証明する.

$n = 1$ のとき, $x_1 = a$, $y_1 = a$ より明らか.

$n-1$ のとき定理の主張が正しいと仮定すると, a, b, x_{n-1}, y_{n-1} はすべて偶数だから, 漸化式 (8) より x_n, y_n も偶数である. □

上の 2 つの補題から, 次の定理が得られる.

[定理 7.6] m, a, b を正の整数とする. m は, $m \equiv 1 \pmod 4$ を満たし, 平方数ではないとする.

(i) (a, b) を方程式 $x^2 - my^2 = 4$ の正整数解とするとき, 漸化式 (8) で定まる (x_n, y_n) $(n \geq 1)$ もその整数解である.

(ii) (a, b) を方程式 $x^2 - my^2 = -4$ の正整数解とするとき, 漸化式 (8) で定まる (x_n, y_n) $(n \geq 1)$ は, n が奇数のとき方程式 $x^2 - my^2 = -4$ の正整数解であり, n が偶数のとき方程式 $x^2 - my^2 = 4$ の正整数解である.

[証明] 補題 7.5 より, すべての整数 $n \geq 1$ に対して, x_n, y_n は正の整数である. また, 補題 7.4 より,

$$\begin{aligned} \frac{x_n^2 - my_n^2}{4} &= \frac{x_n + y_n\sqrt{m}}{2}\,\frac{x_n - y_n\sqrt{m}}{2} \\ &= \left(\frac{a + b\sqrt{m}}{2}\right)^n \left(\frac{a - b\sqrt{m}}{2}\right)^n \\ &= \left(\frac{a + b\sqrt{m}}{2}\,\frac{a - b\sqrt{m}}{2}\right)^n \\ &= \left(\frac{a^2 - mb^2}{4}\right)^n. \end{aligned}$$

(i)　$a^2 - mb^2 = 4$ より,

$$\frac{x_n^2 - my_n^2}{4} = 1.$$

よって, $x_n^2 - my_n^2 = 4$ を満たす.

(ii)　$a^2 - mb^2 = -4$ より,

$$\frac{x_n^2 - my_n^2}{4} = (-1)^n.$$

よって, (x_n, y_n) は, n が奇数のとき $x_n^2 - my_n^2 = -4$ を満たし, n が偶数のとき $x_n^2 - my_n^2 = 4$ を満たす. □

［定理 7.7］ m を平方数でない正の整数とし, $m \equiv 1 \pmod 4$ を満たすとする. また, (a, b) を方程式 $x^2 - my^2 = -4$ の正整数解のうち $(a + b\sqrt{m})/2 > 1$ が最小であるものとする. このとき, 漸化式 (8) で定まる (x_n, y_n) $(n \geq 1)$ が方程式 $x^2 - my^2 = \pm 4$ の正整数解のすべてである.

［証明］ 定理 7.6 より, (x_n, y_n) $(n \geq 1)$ が方程式 $x^2 - my^2 = \pm 4$ の正整数解であること, より詳しく述べると

$$x_n^2 - my_n^2 = (-1)^n 4 \quad (n = 1, 2, \ldots)$$

であることが既に示されている. あとは, 正整数解が (x_n, y_n) $(n \geq 1)$ 以外に存在しないことを示せばよい.

(x, y) を方程式 $x^2 - my^2 = \pm 4$ の任意の正整数解とし,

$$x^2 - my^2 = (-1)^e 4$$

とする. ここで, $e = 0$ または 1 である.

$(a + b\sqrt{m})/2 > 1$ だから, ある整数 $k \geq 0$ が存在して

$$\left(\frac{a + b\sqrt{m}}{2}\right)^k < \frac{x + y\sqrt{m}}{2} \leq \left(\frac{a + b\sqrt{m}}{2}\right)^{k+1}.$$

辺々を $(a + b\sqrt{m})^k/2^k$ で割ると,

$$1 < \frac{2^{k-1}(x + y\sqrt{m})}{(a + b\sqrt{m})^k} \leq \frac{a + b\sqrt{m}}{2}.$$

$(a - b\sqrt{m})(a + b\sqrt{m}) = a^2 - mb^2 = -4$ より,

$$\frac{2^k}{(a + b\sqrt{m})^k} = (-1)^k \left(\frac{a - b\sqrt{m}}{2}\right)^k = (-1)^k \frac{x_k - y_k\sqrt{m}}{2}$$

であるから,

$$1 < \frac{(-1)^k(x + y\sqrt{m})(x_k - y_k\sqrt{m})}{4} \leq \frac{a + b\sqrt{m}}{2}.$$

ここで,

$$\begin{aligned}
\frac{s + t\sqrt{m}}{2} &= \frac{(-1)^k(x + y\sqrt{m})(x_k - y_k\sqrt{m})}{4} \\
&= \frac{(-1)^k\left((xx_k - myy_k) + (yx_k - xy_k)\sqrt{m}\right)}{4} \\
&= (-1)^k \frac{xx_k - myy_k}{4} + (-1)^k \frac{yx_k - xy_k}{4}\sqrt{m}
\end{aligned}$$

とおく. 仮定より $m \equiv 1 \pmod 2$ であり. 定理 7.2 より $x \equiv y$, $x_n \equiv y_n \pmod 2$ であるから, $xx_k - myy_k$, $yx_k - xy_k$ はともに偶数である. ゆえに, s, t は整数である. また,

$$\frac{s - t\sqrt{m}}{2} = (-1)^k \frac{xx_k - myy_k}{4} - (-1)^k \frac{yx_k - xy_k}{4}\sqrt{m}$$

であるから,

$$\begin{aligned}\frac{s^2-mt^2}{4} &= \frac{(xx_k-myy_k)^2}{16} - \frac{m(yx_k-xy_k)^2}{16}\\ &= \frac{1}{16}(x^2x_k^2+m^2y^2y_k^2-my^2x_k^2-mx^2y_k^2)\\ &= \frac{1}{16}\left((x^2-my^2)x_k^2-(x^2-my^2)my_k^2\right)\\ &= \frac{1}{16}(x^2-my^2)(x_k^2-my_k^2)\\ &= (-1)^{k+e}.\end{aligned}$$

すなわち,

$$s^2-mt^2=(-1)^{k+e}4.$$

この式と $1<(s+t\sqrt{m})/2$ を用いると,

$$0<(-1)^{k+e}(s-t\sqrt{m})<2<s+t\sqrt{m}.$$

$k+e$ が偶数のとき,

$$0<s-t\sqrt{m}<2.$$

$k+e$ が奇数のとき,

$$-2<s-t\sqrt{m}<0.$$

いずれにせよ,

$$\begin{aligned}s &= \frac{1}{2}\left((s+t\sqrt{m})+(s-t\sqrt{m})\right)>0,\\ t &= \frac{1}{2\sqrt{m}}\left((s+t\sqrt{m})-(s-t\sqrt{m})\right)>0.\end{aligned}$$

よって, (s,t) は方程式 $x^2-my^2=\pm4$ の正整数解である. $(s+t\sqrt{m})/2\le(a+b\sqrt{m})/2$ と (a,b) の最小性より,

$$s=a,\quad t=b.$$

ゆえに,

$$\begin{aligned}\frac{x+y\sqrt{m}}{2} &= \frac{s+t\sqrt{m}}{2}\left(\frac{(-1)^k(x_k-y_k\sqrt{m})}{2}\right)^{-1}\\ &= \frac{s+t\sqrt{m}}{2}\,\frac{x_k+y_k\sqrt{m}}{2}\\ &= \frac{a+b\sqrt{m}}{2}\left(\frac{a+b\sqrt{m}}{2}\right)^{k}\\ &= \left(\frac{a+b\sqrt{m}}{2}\right)^{k+1}\\ &= \frac{x_{k+1}+y_{k+1}\sqrt{m}}{2}.\end{aligned}$$

すなわち,

$$x = x_{k+1}, \quad y = y_{k+1}.$$

したがって, (x_n, y_n) $(n \geq 1)$ 以外に正整数解はない. □

[注意 7.8] 記号を上の定理の通りとするとき, $(x_2, y_2) = ((a^2+mb^2)/2, ab)$ は, 方程式 $x^2-my^2 = 4$ の整数解のうち, $(x+y\sqrt{m})/2$ が最小のものである. したがって, その方程式の最小解である.

[注意 7.9] m についての条件は上の定理と同じで, (a, b) が方程式 $x^2 - my^2 = 4$ の正整数解で正整数解のうち $(a+b\sqrt{m})/2 > 1$ が最小であるとき, 漸化式 (8) で定まる (x_n, y_n) $(n \geq 1)$ がその正整数解のすべてであることも, 同様の議論により証明できる.

[例 7.10] $m = 5$ のとき, Pell 方程式 $x^2 - 5y^2 = -4$ の最小解は $(1, 1)$ である.

方程式 $x^2 - 2y^2 = \pm 4$ の正整数解 (x_n, y_n) の一般項は

$$x_n = \frac{1}{2^n}\left((1+\sqrt{5})^n + (1-\sqrt{5})^n\right),$$
$$y_n = \frac{1}{2^n\sqrt{5}}\left((1+\sqrt{5})^n - (1-\sqrt{5})^n\right).$$

8 方程式 $x^2 - my^2 = \pm 4$ の最小解の計算方法

[定理 8.1] m を平方数でない正の整数とする. (a_1, b_1) を方程式 $x^2 - my^2 = 4$ の最小解とし, (a_2, b_2) を方程式 $x^2 - my^2 = -4$ の最小解とする. このとき, 方程式 $x^2 - my^2 = \pm 4$ の正整数解で $(x+y\sqrt{m})/2 > 1$ が最小となるものは必ず存在する. しかも,

(i) 方程式 $x^2 - my^2 = -4$ に整数解が存在しないときは, (a_1, b_1)

(ii) 方程式 $x^2 - my^2 = -4$ に整数解が存在するときは, (a_2, b_2)

が求めるものである.

[証明] まず, x, y がともに正の整数ならば, $x \geq 1$, $y \geq 1$, $m \geq 2$ より $(x+y\sqrt{m})/2 > 1$ となることに注意せよ.

$m \equiv 5 \pmod 8$ 以外のとき, 定理 7.1 より, 方程式 $x^2 - my^2 = 4$ のすべての正整数解は, Pell 方程式 $x^2 - my^2 = \pm 4$ のすべての正整数解と大小関係を保ちながら 1 対 1 に対応するから, この場合には定理の主張は明らかである.

$m \equiv 5 \pmod 8$ のとき, 方程式 $x^2 - my^2 = 4$ の正整数解の全体を S とし,

$$S_1 = \{x \mid (x, y) \in S\}$$

とおく. S_1 は正の整数の部分集合である.

Pell 方程式 $x^2 - my^2 = 1$ に正整数解 (x, y) が存在することを用いれば, $(2x, 2y)$ は方程式 $x^2 - my^2 = 4$ の正整数解である. ゆえに, S および S_1 は空でない. したがって, S_1 は最小元 a_1 を持つ. 正整数解においては, x と y の両方についての大小と x のみについての大小が対応することから, 最小解 (a_1, b_1) が定まる.

方程式 $x^2 - my^2 = -4$ に整数解がないときは, (a_1, b_1) が求めるものである. 整数解が存在するときは, 正整数解も存在するので, 先に述べたのと同じ議論で最小解 (a_2, b_2) の存在がいえる. このとき, (a_1, b_1) と (a_2, b_2) のどちらかが求めるものである.

もし仮に $x^2 - my^2 = 4$ の最小解 (a_1, b_1) が求めるものならば, 注意 7.9 より $x^2 - my^2 = \pm 4$ のすべての正整数解は $x^2 - my^2 = 4$ の正整数解なので, 方程式 $x^2 - my^2 = -4$ に正整数解が存在することに反する. ゆえに, (a_2, b_2) が求めるものである. □

方程式 $x^2 - my^2 = \pm 4$ の**最小解**とは, $x + y\sqrt{m}$ が最小となる正整数解 (x, y) のことであるとする.

m を平方数でない正の整数とする. $x^2 - my^2 = \pm 4$ の正整数解 (x, y) において, $\gcd(x, y) = 1$ または 2 である. 後者の場合, $(x/2)^2 - m(y/2)^2 = \pm 1$ を満たす.

$m \equiv 5 \pmod 8$ 以外のとき, 定理 7.1 より, $x^2 - my^2 = \pm 4$ の最小解の計算手順は以下のようになる:

[手順 8.2] m を平方数でない正の整数であって, $m \not\equiv 5 \pmod 8$ とする. $\sqrt{m}$ の連分数展開を定理 3.2 によって求めるとき, $T_{n+1} = 1$ となれば,

(i) $m \equiv 0 \pmod 4$ の場合, $(2p_n, q_n)$ が, 方程式 $x^2 - my^2 = \pm 4$ の最小解である.

(ii) $m \equiv 2, 3 \pmod 4$ または $m \equiv 1 \pmod 8$ の場合, $(2p_n, 2q_n)$ が, 方程式 $x^2 - my^2 = \pm 4$ の最小解である.

$m \equiv 5 \pmod 8$ かつ $\sqrt{m} > 4$ のとき, すなわち $m \geq 21$ のとき, 定理 2.5 より, 正整数解 (x, y) が $\gcd(x, y) = 1$ ならば, x, y がそれぞれ $\sqrt{m}$ の近似分数の分子と分母に現れる. $\gcd(x, y) = 2$ ならば, $x/2$, $y/2$ がそれぞれ分子と分母に現れる. 定理 3.2 より,

$$
\begin{aligned}
&(p_n, q_n) \text{ は方程式 } x^2 - my^2 = \pm 4 \text{ の正整数解} \\
&\qquad \Leftrightarrow (-1)^{n+1} T_{n+1} = \pm 4 \Leftrightarrow T_{n+1} = 4, \\
&(2p_n, 2q_n) \text{ は方程式 } x^2 - my^2 = \pm 4 \text{ の正整数解} \\
&\qquad \Leftrightarrow (p_n, q_n) \text{ は方程式 } x^2 - my^2 = \pm 1 \text{ の正整数解} \\
&\qquad \Leftrightarrow (-1)^{n+1} T_{n+1} = \pm 1 \Leftrightarrow T_{n+1} = 1.
\end{aligned}
$$

定理 6.3 より, $T_{n+1} = 1$ となる最初の番号 $n + 1$ は, $\sqrt{m}$ の連分数展開の周期を n_0 としたときの T_{n_0} であった. T_{n+1} の値は周期 n_0 でループするので, $T_{n+1} = 4$ となる番号 $n + 1$ がもしあれば,

$1 \leq n+1 < n_0$ の範囲に少なくとも 1 つ存在する．したがって, $x^2 - my^2 = \pm 4$ の最小解を見つける手順は次のとおりである:

[手順 8.3] m を平方数でない正の整数とし, $m \equiv 5 \pmod 8$ を満たすものとする．$\sqrt{m}$ の連分数展開を定理 3.2 によって求めるとき,

(i) $T_{n+1} = 4$ となれば, (p_n, q_n) が, 方程式 $x^2 - my^2 = \pm 4$ の最小解である．

(ii) $T_{n+1} = 4$ とならばければ, 最後には必ず $T_{n+1} = 1$ となる．そのとき, $(2p_n, 2q_n)$ が, 方程式 $x^2 - my^2 = \pm 4$ の最小解である．

[例 8.4] 方程式 $x^2 - 21y^2 = \pm 4$ の最小解は $(5, 1)$.

方程式 $x^2 - 37y^2 = \pm 4$ の最小解は $(12, 2)$.

$m \equiv 5 \pmod 8$ かつ $\sqrt{m} \leq 4$ のとき, すなわち $m = 5, 13$ のときは, 例外として処理しなければならないが, 最小解はすぐに見つかる．実際, y に 1, 2, ... を代入して $my^2 \pm 4$ が平方数になるものを探す素朴な方法で計算してみれば,

- 方程式 $x^2 - 5y^2 = \pm 4$ の最小解は $(1, 1)$
- 方程式 $x^2 - 13y^2 = \pm 4$ の最小解は $(3, 1)$

であることがわかる．