

科学・技術の世界 – Fermat の大定理を巡って –

第八回 平成17年6月6日(火)

連分数の記法

$$\begin{aligned} & b_0 + \frac{c_1}{b_1 + \frac{c_2}{b_2 + \frac{c_3}{b_3 + \frac{c_4}{b_4 + \dots}}}} \\ &= b_0 + \frac{c_1}{b_1 +} \frac{c_2}{b_2 +} \frac{c_3}{b_3 +} \frac{c_4}{b_4 +} \dots \end{aligned}$$

文字の対応を各自確認すること.

連分数展開 (1/3)

$\sqrt{N}$ の連分数展開は次の三つの操作の繰り返しでできる.

- 整数部分を取り出す.
- 逆数を取る.
- 有理化する.

例. $\sqrt{7}$ の連分数展開を計算する.

$$\begin{aligned}\sqrt{7} &= 2 + (\sqrt{7} - 2) \Leftarrow \text{整数部分を取る} \\ &= 2 + \frac{1}{0 + \frac{1}{\sqrt{7} - 2}} \Leftarrow \text{逆数を取る} \\ &= 2 + \frac{1}{0 + \frac{\sqrt{7} + 2}{3}} \Leftarrow \text{有理化する}\end{aligned}$$

連分数展開 (2/3)

$$\begin{aligned}\sqrt{7} &= 2 + \frac{1}{0+} \left(1 + \frac{\sqrt{7}-1}{3} \right) \\ &= 2 + \frac{1}{1+} \frac{3}{\sqrt{7}-1} \\ &= 2 + \frac{1}{1+} \frac{\sqrt{7}+1}{2} \\ &= 2 + \frac{1}{1+} \frac{1}{1+} \frac{\sqrt{7}+1}{3} \\ &= 2 + \frac{1}{1+} \frac{1}{1+} \frac{1}{1+} \frac{\sqrt{7}+2}{1}\end{aligned}$$

連分数展開 (3/3)

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

となり, 後は繰り返しが表れるので, 求める連分数展開は

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

となる.

解の合成(1/2)

方程式

$$X^2 - NY^2 = m_1, \quad X^2 - NY^2 = m_2$$

の解 (x_1, y_1) および (x_2, y_2) が存在すれば, 方程式

$$X^2 - NY^2 = m_1 m_2$$

の解

$$(x_1 x_2 + N y_1 y_2, x_1 y_2 + x_2 y_1)$$

が存在することがわかる. これを 解 $(x_1, y_1), (x_2, y_2)$ の合成と呼ぶ.

解の合成(2/2)

例. 方程式 $x^2 - 21y^2 = 4$ の解として,
 $(x, y) = (5, 1)$ が取れる. この解の自分自身との合
成を取ると, $(46, 10)$ を得るが, これは
 $x^2 - 21y^2 = 16$ の解である. 公約数で割ったもの
 $(23, 5)$ は再び $x^2 - 21y^2 = 4$ の解となる. これとは
じめの解 $(5, 1)$ を合成すると $(220, 48)$ が得られ, 公
約数 4 で割ったもの $(55, 12)$ は $x^2 - 21y^2 = 1$ の解
となる.

Pell 方程式の解法その 1 (1/11)

$x^2 - 13y^2 = 1$ を解いてみよう.

- $p_0 = [\sqrt{13}] = 3, q_0 = 1$ とおく.
- $\sqrt{13}$ の連分数展開を考える.

$$\sqrt{13} = 3 + \frac{1}{1 + \frac{\sqrt{13} - 1}{4}}$$

- (p_1, q_1) を $(3, 1)$ と $(1, 1)$ の合成を取って公約数で約分したものとする. すると $(p_1, q_1) = (4, 1)$ となり, $p_1^2 - 13q_1^2 = 3$ となる.

Pell 方程式の解法その 1 (2/11)

- $\sqrt{13}$ の連分数展開をもう一段階進める.

$$\sqrt{13} = 3 + \frac{1}{1+} \frac{1}{1+} \frac{\sqrt{13} - 2}{3}$$

- (p_2, q_2) を $(4, 1)$ と $(2, 1)$ の合成を公約数で約分したものとする. すると $(p_2, q_2) = (7, 2)$ となり, $p_2^2 - 13q_2^2 = -3$ となる.
- $\sqrt{13}$ の連分数展開をもう一段階進める.

$$\sqrt{13} = 3 + \frac{1}{1+} \frac{1}{1+} \frac{1}{1+} \frac{\sqrt{13} - 1}{3}$$

Pell 方程式の解法その 1 (3/11)

- (p_3, q_3) を $(7, 2)$ と $(1, 1)$ の合成を公約数で約分したものとする. すると $(p_3, q_3) = (11, 3)$ となり, $p_3^2 - 13q_3^2 = 4$ となる.
- $\sqrt{13}$ の連分数展開をもう一段階進める.

$$\sqrt{13} = 3 + \frac{1}{1+} \frac{1}{1+} \frac{1}{1+} \frac{1}{1+} \frac{\sqrt{13} - 3}{4}$$

- (p_4, q_4) を $(11, 3)$ と $(3, 1)$ の合成を公約数で約分したものとする. すると $(p_4, q_4) = (18, 5)$ となり, $p_4^2 - 13q_4^2 = -1$ となる.

Pell 方程式の解法その 1 (4/11)

- $\sqrt{13}$ の連分数展開をもう一段階進める.

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

- 元々の $x^2 - 13y^2 = 1$ の解は, 前項で得られた $x^2 - 13y^2 = -1$ の解 $(18, 5)$ を自分自身と合成した $(649, 180)$ が求めるものとなる.

Pell 方程式の解法その 1 (5/11)

先週から計 4 つの方程式を解いたが, その手法をまとめると次のようになる.

- $p_0 = [\sqrt{N}]$, $q_0 = 1$ とおく.
- $\sqrt{N}$ の連分数展開で n 回目に整数部分を取り出した所を

$$\sqrt{N} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots + \frac{1}{a_n + \frac{\sqrt{N} - x_n}{m_n}}}}$$

とし, (p_{n-1}, q_{n-1}) と $(x_n, 1)$ を合成したものを (P_n, Q_n) とする. さらに次のように定める.

$$(p_n, q_n) = (P_n/m_n, Q_n/m_n)$$

Pell 方程式の解法その 1 (6/11)

前項の定義からは (p_n, q_n) が整数とは限らない. しかし, 以下の補題によって各 (p_n, q_n) はすべて整数となることがわかる.

補題 1 (1) $p_{n-1}^2 - Nq_{n-1}^2 = (-1)^n m_n$

(2) $N - x_n^2, Q_n, P_n$ はすべて m_n で割り切れる.

証明. 帰納法による. $n = 1$ のとき,

$$\sqrt{N} = p_0 + \frac{1}{0+} \frac{\sqrt{N} + p_0}{N - p_0^2}$$

から $-m_1 = N - p_0^2$ となり, (1) は成立する.

Pell 方程式の解法その 1 (7/11)

次に $p_0 \equiv -x_1 \pmod{m_1}$ に注意すると,

$$N - x_1^2 \equiv N - p_0^2 \equiv 0 \pmod{m_1}$$

$$Q_1 \equiv p_0 + x_1 q_0 \equiv p_0 - p_0 \cdot 1 \equiv 0 \pmod{m_1}$$

となる. 残りの P_1 に関しては

$$P_1^2 = NQ_1^2 + (N - x_1^2)m_1$$

から m_1 で割り切れることがわかる.

Pell 方程式の解法その 1 (8/11)

帰納法の二段階目として $n = k$ で補題が成立すると仮定する. $\sqrt{N}$ の連分数展開を 1 Step 進めると,

$$\begin{aligned}\sqrt{N} &= p_0 + \frac{1}{a_1 +} \cdots \frac{1}{a_k +} \frac{\sqrt{N} - x_k}{m_k} \\ &= p_0 + \frac{1}{a_1 +} \cdots \frac{1}{a_k +} \frac{1}{a_{k+1} +} \frac{\sqrt{N} + x_k}{m_{k+1}}\end{aligned}$$

ここで $m_{k+1} = (N - x_k^2)/m_k$ である. 帰納法の仮定から m_{k+1} は整数であることに注意しよう. 定義から (P_k, Q_k) は次の方程式を満す.

Pell 方程式の解法その 1 (9/11)

$$P_k^2 - NQ_k^2 = (-1)^{k+1}(N - x_k^2)m_k$$

これと $(p_k, q_k) = (P_k/m_k, Q_k/m_k)$ から

$$p_k^2 - Nq_k^2 = (-1)^{k+1}m_{k+1}$$

がわかる. 次に (2) であるが,

$$x_{k+1} \equiv -x_k \pmod{m_{k+1}}$$

であること, および

$$P_k = p_{k-1}x_k + Nq_{k-1}, \quad Q_k = p_{k-1} + x_kq_{k-1}$$

に注意する.

Pell 方程式の解法その 1 (10/11)

$$N - x_{k+1}^2 \equiv N - x_k^2 \pmod{m_{k+1}}$$

であるが, $m_{k+1} = (N - x_k^2)/m_k$ より上の式は 0 に等しい. また $x_{k+1} = -x_k + lm_{k+1}$ から,

$$\begin{aligned} m_k Q_{k+1} &= P_k + x_{k+1} Q_k = P_k - x_k Q_k + lm_{k+1} Q_k \\ &= (p_{k-1} x_k + N q_{k-1}) - x_k (p_{k-1} + x_k q_{k-1}) \\ &\quad + lm_{k+1} Q_k \\ &= (N - x_k^2) q_{k-1} + lm_{k+1} Q_k \\ &= m_k m_{k+1} q_{k-1} + lm_{k+1} Q_k \end{aligned}$$

Q_k は m_k で割り切れるので, Q_{k+1} は m_{k+1} で割り切れる. □

Pell 方程式の解法その 1 (11/11)

補題から, これまでに紹介してきた方法で (p_n, q_n) を計算していくと, 次のことがわかる.

$p_n^2 - Nq_n^2 = (-1)^{n+1}m_n$ の m_n は
 $N - (x_n)^2$ の約数. 従って組 (m_n, x_n) は有限個の可能性しかない.

これから数の組からなる列 (x_n, m_n) を考えると, n を十分大きくすれば $m_n = 1$ となる n となるものがある可能性は十分ある. このような n が見い出せれば, (p_n, q_n) またはそれを自分自身と合成したものが解となる. これがインドで考えられた Pell 方程式の解法である.

が, この方法ではいつも確実に解が求められるか不安が残るのもまた事実である.

Pell 方程式の解法その 2 (1/9)

ここから Fermat らの見い出した解法を紹介する.
本質的にはこれまでのものと同一であることに注意して欲しい.

まず

$$F_0(X_0, Y_0) = X_0^2 - NY_0^2$$

とおく. ここから以下の手続きで多項式
 $F_i(X_i, Y_i), i = 1, 2, \dots$ を構成する.

- (a) $F_i(t, 1) = 0$ の正の解をこえない最大の整数を m_i とする.
- (b) $X_i = m_i X_{i+1} + Y_{i+1}, Y_i = X_{i+1}$ とおく.
- (c) $F_{i+1}(X_{i+1}, Y_{i+1}) = -F_i(X_i, Y_i)$ と定める.

Pell 方程式の解法その 2 (2/9)

この定義に従うと,

$$F_i(X_i, Y_i) = AX_i^2 - 2BX_iY_i - CY_i^2$$

としたとき,

$$\begin{aligned} F_{i+1}(X_{i+1}, Y_{i+1}) &= -(A(m_i X_{i+1} + Y_{i+1}))^2 \\ &\quad - 2B(m_i X_{i+1} + Y_{i+1})X_{i+1} - CX_{i+1}^2 \\ &= -(Am_i^2 - 2Bm_i - C)X_{i+1}^2 \\ &\quad - 2(Am_i - B)X_{i+1}Y_{i+1} - AY_{i+1}^2 \end{aligned}$$

となる. 係数の変化に注意すること.

Pell 方程式の解法その 2 (3/9)

さて, $F_0(X_0, Y_0) = X_0^2 - 7Y_0^2$ の場合に F_i がどうなるか見てみよう. $F_0(t, 1) = 0$ の正の解は $\sqrt{7}$ なので, これをこえない最大の整数は 2 となり,

$$F_1(X_1, Y_1) = 3X_1^2 - 4X_1Y_1 - Y_1^2$$

となる. 次に $F_1(t, 1) = 0$ の正の解をこえない最大の整数は 1 なので,

$$F_2(X_2, Y_2) = 2X_2^2 - 2X_2Y_2 - 3Y_2^2.$$

つづいて $F_2(t, 1) = 0$ の正の解をこえない最大の整数は 1 なので,

Pell 方程式の解法その 2 (4/9)

$$F_3(X_3, Y_3) = 3X_3^2 - 2X_3Y_3 - 2Y_3^2$$

となる. 最後に $F_3(t, 1) = 0$ の正の解をこえない最大の整数は 1 なので,

$$F_4(X_4, Y_4) = X_4^2 - 4X_4Y_4 - 3Y_4^2$$

となる.

ここで $F_0(X_0, Y_0) = 1$ をみたす解 (u_0, v_0) があったとする. するとこれまでの式変形から $(u_0, v_0) = (2u_1 + v_1, u_1)$ と (u_1, v_1) を定めれば,

$$F_1(u_1, v_1) = -1$$

が成立する.

Pell 方程式の解法その 2 (5/9)

次に $(u_1, v_1) = (u_2 + v_2, u_2)$ と定めれば,

$$F_2(u_2, v_2) = 1$$

が成立する. つづいて $(u_2, v_2) = (u_3 + v_3, u_3)$ と定めれば,

$$F_3(u_3, v_3) = -1$$

が成立し, $(u_3, v_3) = (u_4 + v_4, u_4)$ とおくと

$$F_4(u_4, v_4) = 1$$

が成立する. ところが式の形から $F_4(X_4, Y_4) = 1$ は自明な解 $(1, 0)$ を持つ.

Pell 方程式の解法その 2 (6/9)

そこで $(u_4, v_4) = (1, 0)$ とおくと,

$$(u_3, v_3) = (1 + 0, 1)$$

$$(u_2, v_2) = (1 + 1, 1)$$

$$(u_1, v_1) = (2 + 1, 2)$$

$$(u_0, v_0) = (2 \cdot 3 + 2, 3) = (8, 3)$$

となり, 方程式 $x^2 - 7y^2 = 1$ の解を得る.

例題. $x^2 - 17y^2 = 1$ の解を求めてみよう. まず

$$F_0(X_0, Y_0) = X_0^2 - 17Y_0^2$$

を考える.

Pell 方程式の解法その 2 (7/9)

$F_0(t, 1) = 0$ の正の解をこえない最大の整数は 4 なので,

$$X_0 = 4X_1 + Y_1, \quad Y_0 = X_1$$

を代入すると,

$$F_1(X_1, Y_1) = X_1^2 - 8X_1Y_1 - Y_1^2$$

次に $F_1(t, 1) = 0$ の正の解をこえない最大の整数は 8 なので,

$$F_2(X_2, Y_2) = X_2^2 - 8X_2Y_2 - Y_2^2$$

となる. ここで $F_0(u_0, v_0) = 1$ となる (u_0, v_0) が存在したとすると,

Pell 方程式の解法その 2 (8/9)

$(u_0, v_0) = (4u_1 + v_1, u_1)$ とおけば,

$$F_1(u_1, v_1) = -1$$

を満し, $(u_1, v_1) = (8u_2 + v_2, u_2)$ とおけば,

$$F_2(u_2, v_2) = 1$$

を満す. ここで $F_2(X_2, Y_2) = 1$ は自明な解 $(1, 0)$ を持つので, $(u_2, v_2) = (1, 0)$ とおけば,

$$(u_2, v_2) = (1, 0)$$

$$(u_1, v_1) = (8, 1)$$

$$(u_0, v_0) = (4 \cdot 8 + 1, 8) = (33, 8)$$

Pell 方程式の解法その 2 (9/9)

$(u_0, v_0) = (33, 8)$ が $x^2 - 17y^2 = 1$ の解となっている.

注. $F_1(X_1, Y_1) = X_1^2 - 8X_1Y_1 - Y_1^2 = -1$ は自明な解 $(X_1, Y_1) = (0, 1)$ を持つが, これを利用しても何も得られない. 理由を考えてみよ.

例題. $x^2 - 35y^2 = 1$ の自明でない整数解を求めよ.