ユークリッドの互除法と不定方程式（平成１６年）

ユークリッドの互除法は，現在、我が国の初等・中等教育から，ほとんど疎外されている．代数学，なかでも数論における「ユークリッドの互除法」の果たす役割を考えなおし，初等教育の段階から指導する必要を感じている．

「整数が素因数分解出来れば，ユークリッドの互除法はいらない.」いまの教育現場の考え方のように思えてしかたがない.

1. ユークリッドの互除法

補助定理１

$(a,\ b)$ ： a と b の最大公約数とする.

a をbで割った商をk, 余りを c とすると，

$$(a,\ b) = (b,\ c)$$

（証明） $a,\ b$ の公約数を k とおくと

$a = ka'$, $b = kb'$ ただし， $(a',\ b') = 1$

$a = kb + c$ だから，$c = a - kb = k(a' - kb')$

∴ $a,\ b$ の公約数は $b,\ c$ の公約数である.

同様にして， $b,\ c$ の公約数は $a,\ b$ の公約数である.

$a,\ b$ の公約数の集合 $=$ $b,\ c$ の公約数の集合

$$\therefore\ (a,\ b) = (b,\ c)$$

定理（ユークリッドの互除法）

a をbで割った余りをcとし， b を c で割った余りをd と以下続けると，

$$(a,\ b) = (b,\ c) = (c,\ d) = \cdots\cdots = (l,\ 0)$$ ただし、$a > b > c > d > \cdots > l$

l が $a,\ b$ の最大公倍数である.

補助定理２

$(a,\ b) = (b,\ a)$ ……①

$(a,\ b) = (a-b,\ b)$ ……②

（証明） ①は自明

②について

$a,\ b$ の公約数を k とする．

$a = ka',\quad b = kb' \quad (a',\ b'$ ： 整数$)$

$\therefore\ a-b = k(a'-b')$

よって， $a-b$ と b の公約数は k となる．

逆に， $a-b$ と b の公約数を d とすると，

$a-b = db',\ b = db'' \quad (b',\quad b''$ ： 整数$)$

$a = b + db' = d(b'' + b')$

よって， a と b の公約数の全体は $a-b$ と b の公約数の全体は等しい．

$\therefore\ (a,\ b) = (a-b,\ b)$

古代中国ノ算書「九章算術」は，後漢の初頭（一世紀）頃，従来からあった中国の数学を集大成して出来上がったものである．方田の章六題に，次のようにユークリッドの互助法を用いて，分母分子の最大公約数を求めている．

「また、九十一分の四十九がある。問うに、これを約すといくらか。」「答えて曰く、別に分母分子の数を置き（副置）、小さい数を大きい数からこもごも減じて、（更相減損）等数を求める。等数で分母分子を約す。」

（副置分母子之数、以少減多、更相減損、求其等也、以等数約之）

49　49　7　7　7　7　7　7

91　42　42　35　28　21　14　7

ユークリッド原論第７巻２題には、「互いに素でない２数が与えられたとき、それらの最大公約数を見いだすこと。」がある。２数と単位数が線分として扱われている。２線分の差で小の線分を引き、その差が単位線分を残すまで続ける。その差が、元の２数の約数のとき、この差を最大公約数とする。

（注）ユークリッドの互除法は、英語で *Euclid's algorithm* といい、ギリシャ語では、*Antanairesis* といい、反復減法という意味をもつと云われる。

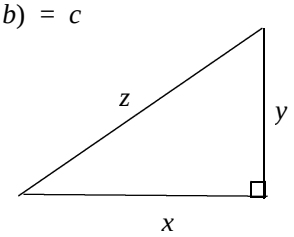
2. 不定方程式

1) *Diophantos* の方程式　　$ax + by = c$　ただし、$(a, b) = c$

2) *Pell* の方程式　　$x^2 - Ny^2 = m$

3) *Pythagoras* 数　　$x^2 + y^2 = z^2$

ただし、x, y, z は正の整数



Diophantos の方程式

$(a, b) = c$　のとき　$ax + by = c$　を満足する整数 x, y が存在する。

（証明）　$a = a_1, b = a_2$ とおき、ユークリッドの互除法により

$$a_1 = k_1a_2 + a_3 \quad (0 < a_3 < a_2) \quad \cdots\cdots\cdots\cdots\cdots(1)$$

$$a_2 = k_2a_3 + a_4 \quad (0 < a_4 < a_3) \quad \cdots\cdots\cdots\cdots\cdots(2)$$

$$a_3 = k_3a_4 + a_5 \quad (0 < a_5 < a_4) \quad \cdots\cdots\cdots\cdots\cdots(3)$$

$$\cdots\cdots\cdots\cdots$$

$$a_{n-1} = k_{n-1}a_n + a_{n+1} \quad (0 < a_{n+1} < a_n) \quad \cdots\cdots\cdots\cdots(4)$$

$$a_n = k_n a_{n+1} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(5)$$

(1),(2) より　$a_4 = -ak_2 + b(1 + k_1k_2)$ ……(6)

(3),(6) より　$a_5 = a(1 + k_2k_3) - b(k_1 + k_3 + k_1k_2k_3)$

以下、同じようにして、

$$a_{n+1} = ax + by \quad \text{ただし、} x, y : \text{整数}$$

a_{n+1} は a, b の最大公約数 $(a, b) = c$ である。

アールヤバティーヤの解法

Diophantos　方程式の解法を記した最古の書は、古代インドの天文学書「アールヤバティーヤ」だと言われている。その解法は、次のようになものであったとされている。

(A)　　$ax + c = by$　ただし、$(a, b) = c$

(1)　　b を a で割り、商を q 余りを r とすると、

$$b = aq + r \quad (r < a) \qquad \therefore \quad ax + c = (qa + r)\, y$$

(2)　　$x = qy + z$　　とおく。

(B)　　$az + c = ry$

以下、未知数の係数をユークリッドの互除法を用いて、次々と小さくしていくと、最後には次の方程式に達する。

(C)　　$1 \cdot v + c = sw$ または $1 \cdot v - c = sw$

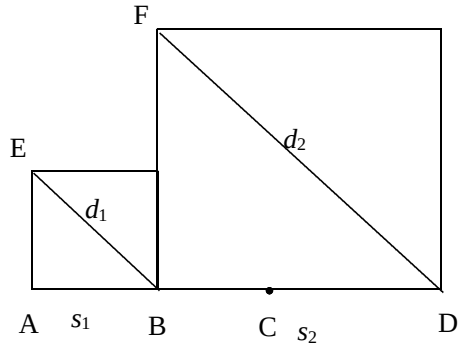
(C)から逆算することで、x, y が w の整式で表される、現代の我々の解法と同じである。

Pell の方程式　　$x^2 - 2y^2 = 1$

この方程式の解 $\sqrt{2}$ の近似分数は、*B.C.400* 年頃古代インドやギリシャで求められている。

古代インドの *Bandhayana* は、$\frac{17}{12}, \frac{577}{408}$ を得ている。

プロクロス（４１０～４８５）によると、ピタゴラス学派は、次の作図を行っていると記している。(図 *1*)



(図 *1*)

辺 *AB* を次のように延長して、

BC = AB,　CD = EB とする。

$$AD^2 + CD^2 = (AB + BD)^2 + (BD - AB)^2$$
$$= 2AB^2 + 2BD^2$$

$CD^2 = EB^2 = 2AB^2$ だから

$$AD^2 = 2BD^2 = FD^2$$

$\therefore$ BD = AB + EB,　FD = AD = 2AB + EB

AB = s_1, BD = s_2, EB = d_1, FD = d_2 とおくと $s_2 = s_1 + d_1$, $d_2 = 2s_1 + d_1$

$\therefore \quad s_{n+1} = s_n + d_n, \quad d_{n+1} = 2s_n + d_n$

$s_1 = 1, \quad d_1 = 1$　とすると

$$\begin{cases} s_1 = 1 \\ d_1 = 1, \end{cases} \quad \begin{cases} s_2 = 2 \\ d_2 = 3, \end{cases} \quad \begin{cases} s_3 = 5 \\ d_3 = 7, \end{cases} \quad \begin{cases} s_4 = 12 \\ d_4 = 17, \end{cases} \quad \cdots\cdots \quad \therefore \quad \frac{d_4}{s_4} = \frac{17}{12}, \ \frac{d_8}{s_8} = \frac{577}{408}$$

ユークリッドの互除法との関係

古代中国の九章算術では、数の間の変換「更相減損」を行って、最大公約数を求めた。その変換は、次のように ST または TS と表される。

$$x > y \ \text{のとき} \quad (x,\ y) \xrightarrow{S} (x-y,\ y)$$

$$x < y \ \text{のとき} \quad (x,\ y) \xrightarrow{T} (x,\ y-x)$$

のとき

$$\text{ST:} \quad (x,\ y) \xrightarrow{S} (x-y,\ y) \xrightarrow{T} (x-y,\ 2y-x)$$

$$\text{TS:} \quad (x,\ y) \xrightarrow{T} (x,\ y-x) \xrightarrow{S} (2x-y,\ y-x)$$

一方、ピタゴラス学派による変換は、正方形の辺（数） s と対角辺（数） d の間の変換 BA は、次のようにと表される。

$$\text{BA:} \quad (s\ ,\ d) \xrightarrow{B} (s,\ s+d) \xrightarrow{A} (2s+d,\ s+d)$$

２つの１次変換 BA, ST は、次のように表されるから、

$$\text{BA:} \quad \begin{cases} d' = 2s + d \\ s' = s + d \end{cases} \quad \cdots\cdots\cdots\cdots(1)$$

$$\text{ST:} \quad \begin{cases} x' = x - y \\ y' = -x + 2y \end{cases} \quad \cdots\cdots\cdots(2)$$

(*1*)は(*2*)の逆変換であることが分る。

（注）ピタゴラス学派は、ユークリッド原論 *II.10* を用いてこの作図を証明したといわれている。

Pell の方程式 $x^2 - 3y^2 = 1$

アルキメデス（*B.C.3*世紀）は、 $\sqrt{3}$ の近似分数として $\frac{265}{153}, \frac{1351}{780}$ を得た。その求め方は、次の近似式によるものと推測されている。

$$a \pm \frac{b}{2a \pm 1} < \sqrt{a^2 \pm b} < a \pm \frac{b}{2a} \quad \text{(複号同順)} \cdots\cdots\cdots\cdots (*)$$

$\sqrt{3}$ の計算

(a) $\dfrac{5}{3} < \sqrt{3} < \dfrac{7}{4}$

$1 < \sqrt{3} < \sqrt{4}$ で、$\sqrt{3}$ の近似値を 2 として、$\sqrt{3} = \sqrt{2^2-1}$ と変形して、不等式（$*$）を用いると、$2 - \dfrac{1}{2\times 2-1} < \sqrt{2^2-1} < 2 - \dfrac{1}{2\times 2}$

$$\therefore \frac{5}{3} < \sqrt{3} < \frac{7}{4}$$

(b) $\dfrac{19}{11} < \sqrt{3} < \dfrac{26}{15}$

$\dfrac{5}{3} < \sqrt{3} < \dfrac{7}{4}$ より、分母を払い $5 < \sqrt{27} < \dfrac{21}{4}$

$\sqrt{27}$ の近似値を 5 として、$\sqrt{27} = \sqrt{5^2+2}$ と変形して、不等式（$*$）を用いると、$5 + \dfrac{2}{2\times 5+1} < \sqrt{5^2+2} < 5 + \dfrac{2}{2\times 5}$

$$\frac{57}{11} < 3\sqrt{3} < \frac{26}{5} \quad \therefore \frac{19}{11} < \sqrt{3} < \frac{26}{15}$$

(c) $\dfrac{265}{153} < \sqrt{3} < \dfrac{1351}{780}$

$\dfrac{19}{11} < \sqrt{3} < \dfrac{26}{15}$ より、分母を払って $\dfrac{285}{11} < \sqrt{675} < 26$

$\sqrt{675}$ の近似値が 26 として、$\sqrt{675} = \sqrt{26^2-1}$ と変形し、不等式（$*$）を用いると、$26 - \dfrac{1}{2\times 26-1} < \sqrt{26^2-1} < 26 - \dfrac{1}{2\times 26}$

$$\frac{1325}{51} < 15\sqrt{3} < \frac{1351}{52} \quad \therefore \frac{265}{153} < \sqrt{3} < \frac{1351}{780}$$

（注）近似を左右交互に行っている。

（注）我々は、連分数で次のように計算する。

$$\sqrt{3} = 1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{1} + \frac{1}{2} + \cdots$$

ブラフマグプタ（７世紀）の解法

pell の方程式　$x^2 - Ny^2 = m$　$(m \neq 0)$ について、次の恒等式が成り立つ

$$(x^2 - Ny^2)(z^2 - Nt^2) = (xz \pm Nyt)^2 - N(xt \pm yz)^2 \quad (\text{B}rahmagupta\text{の恒等式})$$

$$\because \quad (x^2 - Ny^2)(z^2 - Nt^2) = x^2z^2 + N^2y^2t^2 - N(x^2t^2 + y^2z^2)$$

$$= (xz \pm Nyt)^2 - N(xt \pm yz)^2$$

（注）　$p^2 - Nq^2 = m, \quad r^2 - Ns = n \quad \Rightarrow (pr \pm Nqs)^2 - N(ps \pm qr)^2 = mn$

$(x, y) = x^2 - Ny^2$　と置くと、

$$(p, q)(r, s) = (pr + Nqs, ps + qr)$$

(p_n, q_n) を、次のように置くと、

$$(p_0, q_0) = (r, s), \qquad (p_k, q_k) = (p, q)(p_{k-1}, q_{k-1})$$

$$(p_1, q_1) = (1, 1)$$

$$(p_2, q_2) = (2p_1 + 3q_1, p_1 + 2q_1) = (5, 3)$$

$$(p_3, q_3) = (2p_2 + 3q_2, p_2 + 2q_2) = (19, 11)$$

$$(p_4, q_4) = (2p_3 + 3q_3, p_3 + 2q_3) = (71, 41)$$

$$(p_5, q_5) = (2p_4 + 3q_4, p_4 + 2q_4) = (256, 153)$$

……

(p_n, q_n) は $x^2 - 3y^2 = -2$ の解だから $265^2 - 3 \times 153^2 = -2$

$$(p_1, q_1) = (2, 1)$$

$$(p_2, q_2) = (2p_1 + 3q_1, p_1 + 2q_1) = (7, 4)$$

$$(p_3, q_3) = (2p_2 + 3q_2, p_2 + 2q_2) = (36, 15)$$

$$(p_4, q_4) = (2p_3 + 3q_3, p_3 + 2q_3) = (362, 209)$$

$$(p_5, q_5) = (2p_4 + 3q_4, p_4 + 2q_4) = (1351, 780)$$

……

(p_n, q_n) は $x^2 - 3y^2 = 1$ の解だから $1351^2 - 3 \times 780^2 = 1$

$x^2-Ny^2 = m$　と置くと

$$\frac{x}{y}-\sqrt{N}=\frac{1}{y}\frac{m}{x+y\sqrt{N}}$$

m に対して x, y が大ならば、$\frac{x}{y}$ が $\sqrt{N}$ の近似値となるから

$265^2-3\times 153^2 = -2$,　$1351^2-3\times 780^2 = 1$　から $\sqrt{3}$ の近似値 $\frac{265}{153}$, $\frac{1351}{780}$ が考えられる。

$$\frac{265}{153} < \sqrt{3} < \frac{1351}{780}$$

Pythagoras 数の解法

$(x, y, z) = d \neq 1$ のとき、上式は両辺を d^2 で割ればよいので、$(x, y, z) = 1$ と仮定する。

x, y, z のうち２つが１でない公約数をもつと、残りは１でない公約数をもつ。よって、x, y, z のうちいずれの２つは互いに素となる。

つぎの４通りが考えられる。

(*i*)　*x*: 奇数, *y*: 奇数, *z*: 偶数　　(*ii*)　*x*: 奇数, *y*: 奇数, *z*: 奇数

(*iii*)　*x*: 奇数, *y*: 偶数, *z*: 奇数　　(*iv*)　*x*: 偶数, *y*: 奇数, *z*: 奇数

(*iii*),(*iv*)は、x, y を交換したものだから、同じものと考えられるので、(*i*),(*ii*),(*iii*)の３通りについて考える。

(*i*),(*ii*)について　$x \equiv 1 \pmod 2$,　$y \equiv 1 \pmod 2$

$x^2 \equiv 1 \pmod 4$,　$y^2 \equiv 1 \pmod 4$

$\therefore\ x^2 + y^2 \equiv 2 \pmod 4$

$z^2 \equiv 2 \pmod 4$ でないから、(*i*).(*ii*)は成り立たない。

(*iii*)について、$y^2 = (z + x)(z-x)$ ……(1)

y: 偶数 だから $y^2 \equiv 0 \pmod 4$

x: 奇数, *z*: 奇数 だから、$z + x$, $z-x$: 偶数

$z + x = 2m$, $z-x = 2n$　(m,n: 正整数　$m > n$) とおく ……(2)

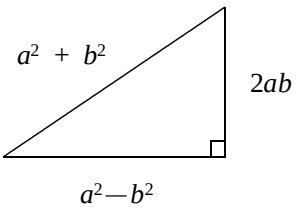
$x = m-n$,　$z = m + n$　(m,n: 互いに素) ……(3)

$(x, z) = 1$ だから $(m, n) = 1$

$\because$ $(m, n) = d \neq 1$ とすると $n = dm$

$x = m(1-d)$, $z = m(1 + d)$

$(x, z) = m \neq 1$



(1),(2)より、 $y^2 = 4mn$ ……(4)

m, n は完全平方数だから、$m = a^2$, $n = b^2$ ……(5)

$m > n$ より $y^2 = 4a^2b^2$

$\therefore$ $y = 2ab$ ……(6)

(3),(5)より、 $x = a^2 - b^2$, $z = a^2 + b^2$ $(a > b)$

$x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$ $(a > b)$ (B*rahmagupta*)

（注）次のものは、よく知られた例である。

1) $a = 2$, $b = 1$ のとき $x = 3$, $y = 4$, $z = 5$

2) $a = 4$, $b = 1$ のとき $x = 15$, $y = 8$, $z = 17$

3) $a = 3$, $b = 2$ のとき $x = 5$, $y = 12$, $z = 13$

4) $a = 4$, $b = 3$ のとき $x = 7$, $y = 24$, $z = 25$

引用文献

［1］ *B. L. van der Waelden: Geometry and Algebra in Ancient Civilizations Springer-Verlag 1983*

［2］ *Thomas L. Heath: The Thirteen Books of Euclid's Element Vol.2 Dover 1956*

［3］ *Thomas L. Heath: A History of Greek Mathematics Vol. 1 Dover 1981*

［4］ *Leonard E. Dickson: History of the Theory of Numbers Vol. II Chelsea 1971*

［5］ 数 論 入 門 １９９９ 北村 泰一 著 槙 書店

［6］ 初等整数論講義 ２０００ 高木 貞治 著 岩波 書店

［7］ アルキメデスを読む １９９９ 上垣 渉 著 日本評論社

［8］ *V. S. Varadarajan: ALGEBRA in ancient and MODERN TIMES, American Mathematical Society, 1998*