ユークリッドの互除法

2 数の最大公約数を求めるとき、多くの場合、2 数を同時に割れる数を順次見つける方法をとるだろう。運が良ければ一発で最大公約数が見つかるし、そうでなくとも公約数で割っているうちに目的の数に行き着くものだ。それが最大公約数であることは、割り算の後に残った 2 数が互いに素であることから分かる。

しかし、ここでは別の方法で最大公約数を求めてみよう。それは次の**アルゴリズム**で求められる。

> ♠ a, b $(a > b)$ の最大公約数：
>
> 1) $a = \underline{b}q + c$ $(0 \leqq c < \underline{b})$ を満たす q, c を求める。
>
> 2) $b = \underline{c}q' + d$ $(0 \leqq d < \underline{c})$ を満たす q', d を求める。
>
> 3) $c = \underline{d}q'' + e$ $(0 \leqq e < \underline{d})$ を満たす q'', e を…（以下繰り返し）。
>
> 0) 余りにあたる数（c, d, e など）が 0 になった時点の、
>
> 除数にあたる数（$\underline{b}$, $\underline{c}$, $\underline{d}$ など）が最大公約数である。

まずは、具体的な数で試してみよう。下線はアルゴリズムとの対比で書き入れてある。60 と 36 の最大公約数は

$$\begin{aligned} 1) \quad 60 &= \underline{36} \times 1 + 24 \\ 2) \quad 36 &= \underline{24} \times 1 + 12 \\ 0) \quad 24 &= \underline{12} \times 2 \end{aligned}$$

より、12 であることが分かり、もちろん正しい。また、53 と 36 の最大公約数であれば

$$\begin{aligned} 1) \quad 53 &= \underline{36} \times 1 + 17 \\ 2) \quad 36 &= \underline{17} \times 2 + 2 \\ 3) \quad 17 &= \underline{2} \times 8 + 1 \end{aligned}$$

より、最大公約数は 1、すなわち 53 と 36 は互いに素である。ここで、最後に $0)\ 2 = \underline{1} \times 2$ を書かなかったのは、余りが $+1$ になれば次の余りは 0 になることは決まっている。つまり、実質的に $+1$ が出たところでアルゴリズムは終了して、2 数は互いに素であることが分かるのである。

この方法は**ユークリッドの互除法**と呼ばれ、非常に使い勝手の良い方法である[1]。少し練習すればすぐに慣れると思われるが、Microsoft Excel でも手順を再現できる。次のようにして、A1 セル

[1] ユークリッド（330?B.C.–275?B.C.）：アレクサンドリアのエウクレイデスのこと。ギリシアの数学者、天文学者。

と B1 セルに 2 数を入力すればよいだろう。“↓下へコピーする” のは各列とも 2 行目の式で、1 行目はコピーしない。

◇	A	B	C	D	E	F
1	正の整数を入力	正の整数を入力	(※ C1)	(※ D1)	(※ E1)	(※ F1)
2			(※ C2)	(※ D2)	(※ E2)	(※ F2)
3			↓下へコピーする	↓下へコピーする	↓下へコピーする	↓下へコピーする
4			↓	↓	↓	↓
5			↓	↓	↓	↓
6			↓	↓	↓	↓

※ セルの式
(C1)　=A1&” =”
(D1)　=B1
(E1)　=”× ”&INT(A1/B1)& ” +”
(F1)　=MOD(A1,B1)
(C2)　=IF(F1=0,”* gcd is ”&D1,D1&” =”)
(D2)　=F1
(E2)　=”× ”&INT(D1/F1)&” +”
(F2)　=MOD(D1,F1)

ユークリッドの互除法の証明

それでは、なぜユークリッドの互除法で最大公約数が求められるのかを示すことにしよう。示すべきことは

> 自然数 a, b $(a > b)$ に対して、a を b で割った余りを $r(\neq 0)$ とするとき、
> a, b の最大公約数と、b, r の最大公約数は等しい

である。このように言うと、1 行目の式からすぐに最大公約数が分かりそうなものだが、そうではない。たしかに、その式には最大公約数が隠れているのだが、はっきり見えるわけではない。それがはっきりするためには、式が割り切れる形になるか、余りが 1 である形になる必要がある。式の変形は、最初から最後まで、最大公約数が式中にあることを保障するものなのである。では、証明を試みよう。

[証明？] a を b で割った余りが r であるとは、商を q として、等式 $a = bq + r$ が成り立つことである。a, b の最大公約数を G とすれば、等式は $a'G = b'Gq + r$（ただし、a', b' は互いに素）であるから

$$(a' - b'q)G = r$$

が成り立つ。左辺は G の倍数であるから、r も G の倍数でなければならず、$r = r'G$ と書ける。したがって $b = b'G$、$r = r'G$ より、b, r の最大公約数も G である。（証明？終り）

末尾に？を付けたように、これには不備があり証明になっていない。不備は一番最後のところ、「$b = b'G$、$r = r'G$ より、b, r の最大公約数も G」の一節である。この場合、言えるのは「b, r の “公約数” は G」であって “最大公約数” ではない。なぜなら、b', r' が互いに素であることを示していないからである。

ならば、そのことが示せればよいのだが、この流れから b', r' が互いに素であることを示すのは厳しい。そこで、以下の証明でどうだろう。

> [証明] $a = bq + r$ において、a, b の最大公約数を G、b, r の最大公約数を H とする。
>
> b, r は最大公約数 H を持つので $a = (b'q + r')H$ と書ける。右辺は H の倍数だから、a も H の倍数—すなわち a は（b の約数でもある）約数 H を持つ。したがって、（単に a, b に共通の約数 H は、a, b の最大公約数 G より大きくないので）$H \leqq G$ ...(1) が成り立つ。
>
> また、$r = a - bq$ において、a, b は最大公約数 G を持つので $r = (a' - b''q)G$ と書ける。右辺は G の倍数だから、r も G の倍数—すなわち r は（b の約数でもある）約数 G を持つ。したがって、（単に r, b に共通の約数 G は、b, r の最大公約数 H より大きくないので）$G \leqq H$ ...(2) が成り立つ。
>
> (1), (2) より $G = H$、すなわち、a, b の最大公約数は、b, r の最大公約数に等しい。（証明終り）

(1) については、

$$P_1 : \ a \text{ が最大公約数 } G \text{ を持つ} \quad \Rightarrow \quad Q_1 : \ a \text{ は約数 } H \text{ を持つ}$$

ことを示したので、$P_1 \Rightarrow Q_1$ は真である。よって、Q_1 は P_1 であるための十分条件となる。しかし、ここで示したのは a が約数 G, H を持つことだけで、G と H が同じ値かどうかは分からない。したがって、$H \leqq G$ が言えるだけである。

(2) については、

$$P_2 : \ r \text{ が最大公約数 } H \text{ を持つ} \quad \Rightarrow \quad Q_2 : \ r \text{ は約数 } G \text{ を持つ}$$

こと、すなわち r が約数 H, G を持つことだけで、H と G が同じ値かどうかは分からない。したがって、$G \leqq H$ が言えるだけである。

しかし、(1)、(2) を合わせて考えると $G = H$ が言えるのである。

不定方程式

53 と 36 の最大公約数をユークリッドの互除法で求めたところに戻ってみよう。ここで 1), 2), 3) を

$$\begin{aligned} 1')\ 17 &= 53 - \underline{36} \times 1 \\ 2')\ \ 2 &= 36 - \underline{17} \times 2 \\ 3')\ \ 1 &= 17 - \underline{2} \times 8 \end{aligned}$$

と見直し、1′) の右辺を 3′) の 17 に代入し、1′) の右辺を 2′) の $\underline{17}$ に代入した上で 2′) の右辺を 3′) の $\underline{2}$ に代入すると、

$$\begin{aligned} 1 &= (53 - \underline{36} \times 1) - \{36 - (53 - \underline{36} \times 1) \times 2\} \times 8 \\ &= 53 \times 17 + 36 \times (-25) \end{aligned}$$

のように整理することができる。

この様子を一般的に言ってみよう。互いに素である 2 数 a、b（$a > b$）にユークリッドの互除法を用いると、$a = bq + c$ は必ず $x = yr + 1$ となる。最後に現れる x と y は、a、b を用いながら順次変形されたものだから、前の式を代入すれば $1 = a \times m + b \times n$（$m$, n は整数）の形にすることができる。言い換えれば、a, b が互いに素であるとき、$am + bn = 1$ を満たす整数 m, n が必ず存在するということである。

したがって、方程式 $ax + by = 1$ には間違いなく解が存在している。一般に $ax + by = k$ の形の方程式は**不定方程式**と呼ばれる。

不定方程式を解く

一般的な不定方程式 $ax + by = k$ を解いてみたい。しかし、実際に解くのは $ax + by = 1$ でよい。なぜなら、$ax + by = 1$ を解いて $am + bn = 1$ となる m, n を求めることができたら、それらを k 倍した mk, nk が $a(mk) + b(nk) = k$ の解だからである。

では、$ax + by = 1$ はどのようにして解くのか。たとえば $53x + 36y = 1$ ならば、53 と 36 に対してユークリッドの互除法を用いて $1 = 53m + 36n$ の形を作ればよいのである。そして、それは先ほどやっている。$1 = 53 \times 17 + 36 \times (-25)$ であった。よって、$53x + 36y = 1$ の解の 1 つは $x = 17$,

$y=-25$ である。しかし、2 個の変数に対して等式は 1 個であるから、この解は唯一のものではない。したがって、$x=17,\ y=-25$ は無数の解のうちの 1 つ、つまり**特殊解**である。

それなら、**一般解**は何であろうか。一般解は次のようにして求められる。元の不定方程式 $53x+36y=1$ と特殊解を代入した $53\cdot 17+36\cdot(-25)=1$ を辺々引いてみる。

$$\begin{array}{rrrrrr} & 53x & + & 36y & = & 1 \\ -) & 53\cdot 17 & + & 36\cdot(-25) & = & 1 \\ \hline & 53(x-17) & + & 36(y+25) & = & 0 \end{array}$$

これより $53(x-17)=-36(y+25)$ が得られる。左辺が 53 の倍数であるなら右辺は $(y+25)$ が 53 の倍数でなければならない。なぜなら、53 と -36 が互いに素であるからだ。同じく、$(x-17)$ は -36 の倍数である。すなわち、$y+25=53n$、$x-17=-36n$ となる。よって、一般解として

$$x=-36n+17,\ y=53n-25 \quad (n \text{ は整数})$$

が求められた。

* * *

不定方程式 $53x+36y=1$ の一般解は $x=-36n+17,\ y=53n-25$（n は整数）であった。n は整数なので、具体的に $n=\cdots,-2,-1,0,1,2,\cdots$ を代入すれば、$(x,\ y)=(89,\ -131),(53,\ -78),(17,\ -25),(-19,\ 28),(-55,\ 81),\cdots$ が求められる。特殊解 $(17,\ -25)$ は、$n=0$ の場合の解であったわけだ。

もし特殊解として $(-19,\ 28)$ を見つけていたら、一般解はどうなったであろうか。それは、$x=-36n-19,\ y=53n+28$ であったはずである。これは最初の一般解と少し違うので、一見すると間違いのように見えてしまう。しかし n は整数なのだから、$n=m-1$ と置き換えても n と m はまったく同じ整数の集合の値である。実際、

$$\begin{aligned} x &= -36n-19 = -36(m-1)-19 = -36m+17 \\ y &= 53n+28 = 53(m-1)+28 = 53m-25 \end{aligned}$$

となって、同じ一般解なのである。▌

ところで、$53x+36y=1$ の特殊解を求める際、53 と 36 に対してユークリッドの互除法を用いた後、$1=\cdots$ の形にする計算が少々ややこしいと感じなかっただろうか。この場合は、3 個の等式の代入で済んだからよいのだが、もっと多くの変形を要する 2 数の値のときは $1=\cdots$ の形に直す苦労は相当である。

このような数値計算が苦手なら、左辺を

$$\begin{aligned} 53x+36y &= 1 \\ 36(x+y)+17x &= 1 \quad (53 \text{ から } 36 \text{ をくくり } 17 \text{ を残す}) \\ 17(3x+2y)+2(x+y) &= 1 \quad (36 \text{ から } 17\times 2 \text{ をくくり } 2 \text{ を残す}) \end{aligned}$$

のように変形するとよい。何をしたかというと、$ax+by$ の小さい係数を使って、大きい係数の一部をくくり出したのである。このとき、くくり出す数はできるだけ大きいほうがよい。そのため、36 からは 17 を 2 回くくり出している。こうすれば方程式の係数は必ず小さくなるので、その時点で $AX+BY=1$ となる X, Y の組を探せばよい。もし、この例でまだ $17X+2Y=1$ となる X, Y の組が見つけられなければ、さらに 17 から 2×8 をくくり出すことになる。

しかし $17X+2Y$ であれば、$17\cdot 1+2\cdot(-8)$ で 1 にできることがすぐに分かるだろう。すなわち

$$\begin{cases} 3x+2y &= 1 \\ x+y &= -8 \end{cases}$$

を解いて、$x=17, y=-25$ が分かるのだ。