互除法

松本　眞:m-mat　@　math.sci.hiroshima-u.ac.jp

平成 17 年 7 月 8 日

1　整数の互除法

最大公約数を求めるためにユークリッドの互除法を使うことは良く知られていると思う。しかし、もともとの互除法は、

「比を有理数で近似する」

ために導入されたようである。

いま、基準となる長さの棒 X(長さ x メートル) を用いて、棒 Y の長さ（長さ y メートル）を計ろうとしたとする。つまり、

y/x はどのような値か。

y の中に x が何個（自然数個）取れるかを計算して、

$$y = q_1 x + r_1,$$

q_1 は自然数で $0 \leq r_1 < x$ である。ここで $r_1 = 0$ なら $y/x = q_1$ であり、目的は達成された。$r_1 = 0$ でないとする。

もはや $r_1 < x$ であるから、x の中に r_1 が何個とれるかを考えるよりほかない。

そこで、

$$y_1 := x, x_1 := r_1$$

とおきなおして $y_1 = x$ の中に $x_1 = r_1$ が何個とれるかを計算して

$$y_1 = q_2 x_1 + r_2,$$

とする。以後、帰納的に

$$y_i = q_{i+1}x_i + r_{i+1},$$

$$y_{i+1} := x_i, \quad x_{i+1} = r_{i+1}$$

とおく。$r_{i+1} = 0$ となったら停止する。

この計算は 2×2 行列で見るとわかりやすい。

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} -q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

であり、

$$\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} -q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$$

である。こうして、

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} -q_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

となる。

もし n 回目で割り切れて $r_n = 0$ となれば、一般に $x_i = r_i$ であるから $x_n = 0$ となり、

$$\begin{pmatrix} 0 \\ y_n \end{pmatrix} = A_n \begin{pmatrix} x \\ y \end{pmatrix},$$

ここに

$$A_n = \begin{pmatrix} -q_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -q_1 & 1 \\ 1 & 0 \end{pmatrix}$$

は行列式が $(-1)^n$ の整数行列となる。

レポート問題 1.1. A_n は、行列式が $(-1)^n$ の整数行列となることを証明せよ。(超易問)

さて、

$$A_n = \begin{pmatrix} s & t \\ a & b \end{pmatrix}$$

とおくと、

$$sx + ty = 0, \quad ax + by = y_n$$

が成立する。

$$A_n^{-1} = (-1)^n \begin{pmatrix} b & -t \\ -a & s \end{pmatrix}$$

だから

$$x = (-1)^{n+1} t y_n, y = (-1)^n s y_n$$

となり、y_n は x, y の公約数であるが

$$bs - at = (-1)^n (\text{訂正箇所})$$

より s, t は互いに素なので y_n は最大の公約数 $d = GCD(x, y)$ である。

そしてこのとき、

$$ax + by = d$$

となる a, b も、もとまっている。さらに

$$x/y = -s/t$$

であり、x と y の比が既約分数として求まっている。

2 無理数比の場合

上の議論は、x, y 自身は無理数であっても、比 $x : y$ が整数比であればうまくいく。上のアルゴリズムの進み方は、x と y の比にしか依存しない。

さて、ピタゴラスは無理数を認めなかったが、ユークリッド（紀元前 300 年ごろ）の時代には比 $x : y$ が整数比にならない例がすでに知られていた。それは上の互除法が無限に続いてしまうような例である。

たとえば、上の互除法で、

「一回互除法を行った結果が、比が変わっていない」

すなわち

$$x : y = x_1 : y_1$$

となっているような例を考えよう。

$$y = q_1 x + r, \quad x_1 = r, \quad y_1 = x$$

であるから

$$x : y = y - q_1 x : x$$

となるような例である。たとえば $q_1 = 1$ のときには

$$y^2 - xy - x^2 = 0$$

となり、x, y は正だから

$$y/x = (1 + \sqrt{5})/2(\text{訂正箇所})$$

を得る。このような比では、互除法はとまらない。これが、この比が整数比でないことを証明している。この比は、黄金比と呼ばれる。

レポート問題 2.1. $x : y = 1 : (1 + \sqrt{5})/2$(訂正箇所) に対して互除法を行うと、全ての n に対して $q_n = 1$ となり、終わらないことを示せ。

3 応用その1

直径1メートルの円の周囲の長さを精密に測って、$3.1415926535\cdots$ という値を得たとする。これを有理数で近似しよう。$x = 1, \quad y = 3.1415926535$ に対して互除法を行うと

$$\begin{aligned}
3.1415926535 &= 3 \times 1 + 0.1415926535 \quad q_1 = 3 \\
1 &= 7 \times 0.1415926535 + 0.0088514255 \quad q_2 = 7 \\
0.1415926535 &= 15 \times 0.0088514255 + 0.008821271 \quad q_3 = 15 \\
0.0088514255 &= 1 \times 0.008821271 + 0.0000301545 \quad q_4 = 1
\end{aligned}$$

といった具合になる。

$$A_n = \begin{pmatrix} -q_n & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} -q_1 & 1 \\ 1 & 0 \end{pmatrix}$$

とおくと

$$\begin{aligned}
A_1 &= \begin{pmatrix} -3 & 1 \\ 1 & 0 \end{pmatrix} \\
A_2 &= \begin{pmatrix} -7 & 1 \\ 1 & 0 \end{pmatrix} A_1 = \begin{pmatrix} 22 & -7 \\ -3 & 1 \end{pmatrix} \\
A_3 &= \begin{pmatrix} -15 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 22 & -7 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -333 & 106 \\ 22 & -7 \end{pmatrix} \\
A_4 &= \begin{pmatrix} 355 & -113 \\ -333 & 106 \end{pmatrix}
\end{aligned}$$

といった具合である。

ここから、

$$A_n = \begin{pmatrix} a_{n+1} & b_{n+1} \\ a_n & b_n \end{pmatrix}$$

という形になることが見て取れる。そして、

$$A_n = \begin{pmatrix} -q_n & 1 \\ 1 & 0 \end{pmatrix} A_{n-1} = \begin{pmatrix} -q_n a_{n+1} + a_n & -q_n b_{n+1} + b_n \\ a_{n+1} & b_{n+1} \end{pmatrix}$$

さて、

$$\begin{pmatrix} x \\ y \end{pmatrix} = A_n^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = (-1)^n \begin{pmatrix} b_n & -b_{n+1} \\ -a_n & a_{n+1} \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

である。よって

$$x : y = b_n x_n - b_{n+1} y_n : -a_n x_n + a_{n+1} y_n$$

右辺の比は $b_n : -a_n$ で近似されるので、$a_n x + b_n y$ が x に比して 0 に近い。そこで

$$a_n x + b_n y : x = -a_n b_{n+1} y_n + b_n a_{n+1} y_n : b_n x_n - b_{n+1} y_n = (-1)^n y_n : b_n x_n - b_{n+1} y_n$$

$$|a_n/b_n + y/x| = |1/b_n(b_n x_n/y_n - b_{n+1})|$$

そして、b_n と b_{n+1} の符号が逆であることから

$$|b_n(b_n x_n/y_n - b_{n+1})| > |b_n b_{n+1}|$$

こうして

$$|y/x - (-a_n/b_n)| < 1/|b_n b_{n+1}|$$

がわかった。$|b_n| < |b_{n+1}|$ なので、

$$|y/x - (-a_n/b_n)| < 1/|b_n b_{n+1}| < 1/|b_n|^2$$

レポート問題 3.1. すなわち、y/x は既約分数 $-a_n/b_n$ で近似され、その誤差は分母の自乗すなわち $1/|b_n|^2$ 未満である。「b_n と b_{n+1} の符号が逆」「$|b_n| < |b_{n+1}|$」などの事実に証明を与えることで、上の議論を完成させよ。

これによりたとえば、円周率 π の $355/113 = 3.1415929208$ による近似誤差は 113^{-2} 以下であることがわかる。

4 Berlekamp Massey法

この節については、読んで理解することを必ずしも期待しない。が、2300年のときを経て、なお互除法が現代の暗号理論に大きな役割を果たしていることに触れてもらうために用意した。現代的な点は、「整数・実数」がその類似物である「多項式環・形式冪級数体」に置き換わっても互除法が働くことにある。

次のような状況を考える。$\mathbb{F}_2 = \{0, 1\}$ を2元体とし、

$$\chi := (x_0, x_1, \ldots) \in \mathbb{F}_2^{\mathbb{N}}$$

を $\mathbb{F}_2$ 成分の数列とする。χ が（N 階）線形漸化式を満たすとは、ある定数 $a_0, \ldots, a_N \in \mathbb{F}_2$, $a_N \neq 0$ に対して

$$\sum_{i=0}^{N} a_i x_{i+j} = 0 \quad (j = 0, 1, 2, \ldots)$$

が成立することである。

暗号解読や符号の設計、擬似乱数発生法の設計の際に、次のような問題がしばしば発生する。

問題 4.1. 数列 χ が与えられている。χ はある線形漸化式を満たすことがわかっている。この線形漸化式を求めよ。

より実際的には、「線形漸化式の階数は M 以下であることがわかっている。数列は、$x_0, x_1, \ldots, x_{2M-1}$ の $2M$ 個を求めてある。このときに線形漸化式を求めよ。」という状況設定である。

Berlekamp-Massey 法は、互除法を用いた次のようなアルゴリズムである。χ の生成母関数を

$$\chi(t) := \sum_{i=0}^{\infty} x_i t^{-i-1} \in \mathbb{F}_2[[t^{-1}]]$$

とし、形式冪級数体

$$\mathbb{F}_2((t^{-1})) := \{ \sum_{i=-n_0}^{\infty} b_i t^{-i} | b_i \in \mathbb{F}_2,\ n_0 \in \mathbb{Z} \}$$

を考える。

$$\sum_{i=-n_0}^{\infty} b_i t^{-i} \quad (b_{-n_0} \neq 0)$$

の次数を n_0 で定義する。

1 と $\chi(t)$ の間の互除法を、係数環を $\mathbb{F}_2[t]$ として行う。すなわち、$x, y \in \mathbb{F}_2((t^{-1}))$ に対し、

$$y = q_1 x + r_1, \quad q_1 \in \mathbb{F}_2[t], \ \ \deg(r_1) < \deg(x)$$

となるような q_1, r_1 を求めることを繰り返して、互除法を行う。

通常の実数に対する互除法と同じことが言えて、

$$\chi(t) = g(t)/f(t)$$

$g(t), f(t) \in \mathbb{F}_2[t]$:互いに素、とあらわせているときにはこの方法で $g(t), f(t)$ が求まる。

ここで

$$f(t) = \sum_{i=0}^{N} b_i t^i$$

とおくと、

$$f(t)\chi(t) = \sum_{i=1}^{N}\sum_{j=0}^{\infty} b_i x_j t^{i-j-1} = \sum_{k=-N}^{\infty}(\sum_{i=0}^{N} b_i x_{k+i-1})t^{-k} = g(t)$$

だから t^{-k} の係数は $k \geq 1$ で 0 となり、$a_i = b_i$ $(i = 0, \ldots, N)$ とおくとこれは χ が満たす線形漸化式の係数を与え、目的は達せられる。

さて、上の計算では $\chi(t)$ という無限の冪級数が必要となったが、実は $\chi(t) \mod t^{-2N-1}$（すなわち、t^{-2N} までの係数）が求まれば、それに対する互除法で $g(t), f(t)$ が求まる。

前の節のような記法を用いれば $x = 1$, $y = \chi(t)$ であり

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a_{n+1} & b_{n+1} \\ a_n & b_n \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

$a_n, b_n \in \mathbb{F}_2[t]$ とできる。$x_n = 0$ となったときが互除法の停止点であり、このとき

$$y = y/x = -a_{n+1}/b_{n+1}$$

であり $\deg(b_{n+1}) = N$ (厳密には、線形漸化式の中で階数最小のものが N 階となる)。

しかるに、y に誤差があるので困るのだが、誤差の次数が $\deg \leq -2N-1$ であれば a_{n+1}, b_{n+1} を求めるまでは同じ連分数展開が行われることをみる。

y に誤差 $\delta(t)$ があったとき、連分数展開が最初に狂ってくるところを a_{m+1}, b_{m+1} とすると、

$$\begin{pmatrix} x'_m \\ y'_m \end{pmatrix} = \begin{pmatrix} a_{m+1} & b_{m+1} \\ a_m & b_m \end{pmatrix} \begin{pmatrix} x \\ y + \delta(t) \end{pmatrix}$$

とおいたときに

$$\deg(x'_m) < \deg(y'_m)$$

が不成立になるということになる。$m \leq n$ であれば、$\deg(b_m), \deg(b_{m+1}) \leq \deg(b_{n+1}) = N$ により

$$\begin{pmatrix} x'_m - x_m \\ y'_m - y_m \end{pmatrix} = \begin{pmatrix} a_{m+1} & b_{m+1} \\ a_m & b_m \end{pmatrix} \begin{pmatrix} 0 \\ \delta(t) \end{pmatrix}$$

のそれぞれの次数は $N + \deg(\delta(t))$ 以下であるから、$\deg \delta(t) \leq -2N - 1$ であれば $x_m - x'_m, y_m - y'_m$ の次数は $-N - 1$ 以下。一方、x_m, y_m は 1 と y の $\mathbb{F}_2[t]$ 係数線形結合であり、$y_m \neq 0$ であるから $\deg(y_m) \geq -N$ ($y_m b_{n+1} \in \mathbb{F}_2[t]$ により、y_m の次数はマイナス「b_{n+1} の次数」以上である。) よって、$\deg(y'_m) \geq -N$ であり、$\deg(y_m) = \deg(y'_m)$。また、$\deg(x'_m) \leq \max\{\deg(x_m), \deg(x_m - x'_m)\}$ より $\leq \deg(y_m) = \deg(y'_m)$。これにより、$m \leq n$ では互除法の係数は $\deg \leq -2N - 1$ の誤差が y にあっても変わらない。

したがって、この程度の誤差なら互除法の途中で

$$y = -a_{n+1}/b_{n+1}$$

となっている。つまり、どこかで「正解」がもとまる。問題は n があらかじめわかっていない、つまりいつ正解が求まったかがわからないことだが、$M \geq N$ に対して y を $2M$ 桁まで計算しておれば $\deg(b_{m+1}) = N$ となった瞬間が $m = n$ であり、y は正確にもとまり $x_n = 0$、したがって $x'_n = b_{n+1}\delta(t)$ で次数は $N - 2M - 1 \leq -M - 1$ となる。一方、y'_n の次数は $\geq -N$ なので、y'_n を x'_n で割った商 q'_n は $\geq -N + M + 1$ 次式となり、$\deg(b_{n+2}) = \deg(q'_n) + \deg(b_{n+1}) \geq M + 1$ となる。すなわち、b_j の次数が初めて M を超えたとき、その直前が求めるべきもの、すなわち $m + 1 = j - 1$ である。これにより $m = n$ は $j - 2$ として求まる。