数理解析研究所講究録
791巻 1992年 140-149


# 孫子定理の一応用
## －代数方程式の数値的因数分解－

名古屋大学工学部　鳥居達生
〃　　梅井鉄也
〃　　杉浦洋

## 1．はじめに

孫子定理（中国剰余定理ともいう）を関数近似の方法である補間法の立場から解釈し，その結果を1変数多項式の数値的因数分解に応用する．

はじめに記号を定義する．$p(x)$，$q(x)$を任意の多項式とする．

$\deg p$ ； $p(x)$の次数

$(p,q)$ ； $p(x)$と$q(x)$の最大公約因子．とくに$(p,q)=1$ならば，$p$，$q$は互いに素．

$\|p\|$ ： 多項式$p(x)$のノルム．この定義は

$$\|p\| = \max |a_i|,$$

ただし $p(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$．

多項式$p(x)$を，多項式$X(x)$で割ったときの商と余りを，

それぞれ $Q(x)$, $R(x)$ とすれば

$$P(x) = Q(x)X(x) + R(x) \qquad (1.1)$$
$$\deg R < \deg X$$

となる。この表現は一通りである。

$P$ が $X$ で割り切れるとき，すなわち $R=0$ のとき

$$X \mid P$$

と書く。また，二つの多項式 $P_1$, $P_2$ が $X \mid P_1 - P_2$ ならば

$$P_1 \equiv P_2 \pmod{X}$$

と書き，$P_1$ と $P_2$ は，$X$ を法として合同であるという。

多項式の除算 (1.1) において，$R \equiv P \pmod{X}$ があるが余りの一意性より，余り $R$ を

$$R = P(x) \bmod X(x) = P \bmod X$$

と書く。

多項式 $X(x)$ の0点を $x_1, x_2, \cdots, x_m$ とする。重根ならば，重複度だけ並べるとする。除算 (1.1) において，$X(x)$ の0点上で $P(x)$ と $R(x)$ は，次の意味で一致する。点 $x_i$ が $X(x)$ の $\mu \geq 1$ 乗根ならば $R^{(k)}(x_i) = P^{(k)}(x_i)$, $0 \leq k < \mu$.

ただし $P^{(k)}(x)$ は，$P(x)$ の $k$ 階導関数。$R(x)$ の次数は $X(x)$ のそれより小さいことから $R$ は，$P(x)$ の $X(x)$ の0点上における補間多項式である。すなわち，代数演算

$$P \bmod X$$

は，$P(x)$ の $X(x)$ の 0 点上の Hermite 補間法である．

この知見に立てば，最早補近似関数を多項式に限定する必要はない．形式的には，補間法が定義できる関数族ならばよい．$f(x)$ を十分滑らかな関数として，$f, \bmod X$ を $f(x)$ の $X$ の 0 点上における Hermite 補間多項式とする．後に有理式の Hermite 補間を考える．

孫子定理　多項式 $P, Q, R$ が

$$(P, Q) = 1, \quad \deg R < \deg P + \deg Q$$

ならば

$$A(x)P(x) + B(x)Q(x) = R(x)$$

$$\deg A < \deg Q, \quad \deg B < \deg P$$

を満たす多項式 $A(x), B(x)$ は一意に存在する．

孫子定理は，初等整数論で有名な定理であり，古数数学時代によれば，孫子算経は 3 世紀頃の本とある．

これを多項式に拡張し，最も成功した応用例は，FFT であろう．

$A, B$ のもの方は，いろいろある[1]．わかり易さを旨として一例を示す．

$(P, Q) = 1$ であるから Euclid の互除法により

$$A_0 P + B_0 Q = 1$$

$$\deg A_0 < \deg Q, \quad \deg B_0 < \deg P$$

を満たす多項式 $A_0, B_0$ がただ一つ存在する．上式の両辺に $R$ をかけ，$PQ$ を法として合同をとる．

$$RA_0P + RB_0Q = R \quad , \mod PQ$$

ところで

$$\begin{aligned} RA_0P \ , \mod PQ &= (RA_0, \mod Q)\cdot P \\ &= ((R, \mod Q)\cdot A_0, \mod Q)\cdot P \\ &= AP \end{aligned}$$

とおけば $\deg A < \deg Q$ である．

同様にして

$$\begin{aligned} RB_0Q, \mod PQ &= ((R, \mod P)\cdot B_0, \mod P)\cdot Q \\ &= BQ \end{aligned}$$

となり $\deg B < \deg P$ である．この多項式 $A, B$ は，定理の条件を満たす．

ここで次の問題を考える．

問題　有理式 $P/Q$ と多項式 $X$ を与える．$(Q, X) = 1$ として $P/Q, \mod X$ を求めよ．

解法．$\deg P, \deg Q < \deg X$ として一般性を失なわない．

$(Q, X) = 1$ であるから，孫子定理より

$$SQ + TX = P \quad , \deg S < \deg X, \ \deg T < \deg Q$$

を満たす多項式 $S, T$ を求める．明らかに

$$S = P/Q, \mod X$$

である．これが有理式 $P/Q$ の $X$ の0点の補間多項式である．

解法では，$X$ の0点を陽に必要としないことに注意．

以後簡単のためこれを $X$ 上の補間式という．

とくに $X(x) = x^N - 1$，$N = 2^n$ ならば，$S(x)$ は，次のように FFT によって高速に求まる．

$P(x)$，$Q(x)$ に逆 FFT を $N$ 項 適用し，$x^N - 1$ の0点上で，それらを標本化する．標本点上で，$N$ 回の除算 $P(x_i)/Q(x_i)$ $(x_i^N - 1 = 0)$ を行なう．こうして得られた標本に $N$ 項 FFT を適用すれば $S(x)$ が得られる．すなわち，たたみこみ演算と同じ手間である．

ついでに $SQ + T\cdot(x^N - 1) = P$ の $T$ を求める．両辺 $x^N + 1$ と合同をとれば，$x^N - 1$，$\mathrm{mod}\ x^N + 1 = 2$ に注意すれば

$$T = \frac{1}{2}(SQ - P),\ \mathrm{mod}\ x^N + 1$$

$$= \frac{1}{2}(SQ,\ \mathrm{mod}(x^N + 1) - P)$$

となる．したがって中点公式に基づく $N$ 項 FFT を3回使えばよいことになる．実際の手間としては項数 $N$ の循環型たたみこみ演算を用いてある．

## 2. Bairstow 法の拡張

周知のように，Bairstow 法は，実係数多項式の2次因子をとり出す方法である．まず Bairstow 法に対し，独自の解

就をうえよう．$f(x)$をうえられた多項式とする．$X(x)$を試みの2次因子とし $f$ を $X$ で割ったときの商と余りを $Q, R$ とすれば $f = QX + R$ となる．$Q$を補助関数とし，有理式 $f/Q$ を $X$ 上で補間し，それを $S(x)$ とおけば

$$S(x) = \frac{f}{Q}, \mod X = \frac{R}{Q}, \mod X$$

となる．ただし $(Q, X) = 1$ を仮定した．$X+S$ を新しい2次因子 $X$ と考え，同様な操作を繰り返す．これがBairstow法である．$\varepsilon > 0$ を十分小とする．$\|R\| < \varepsilon$ ならば，これが2次収束であることも次によって簡単にわかる．

$(Q, X) = 1$ であるから $SQ + TX = R$ において $\|S\|$, $\|T\|$ は，ともに $O(\varepsilon)$ である．

一方，$f = QX + R = QX + SQ + TX = Q(X+S) + TX$ において，$f, \mod (X+S)$ を評価すれば

$$f \equiv TX \equiv -TS, \mod (X+S)$$

したがって，$\|TS\| \leq \|T\|\|S\| = O(\varepsilon^2)$.

以上において，試みの因子 $X(x)$ の次数2は，本質的な制限ではない．$X$ の次数は任意であってよい．とくに $\deg X = [\deg f/2]$ にとったとき，これは分割統治法とよばれる算法となる．Freeman は，$X(x)$ の係数に関する非線形方程式を Newton 法で解いている[1]．著者らの上述の算法も，

結果的には同じであるが記述が簡単である.

再び元の問題に立ち返る. 試みの因子 $X$ の次数を適当に大きくとり $f = QX + R$ と表わしたとき, $\deg Q$, $\deg R$ は, ともに $\deg X$ より小さくできる. このとき $QX + R = 0$ を $X$ に関する1次式とみなす. ($Q$ と $R$ の次数の制限はなくてもよい).

すなわち多項式 $f(x)$ の因数分解は, 一般性を失うことなく1次式

$$QX + R = 0 \overbrace{\pmod f}, \quad \deg Q,\ \deg R < \deg X \qquad (2.1)$$

を解くことに帰着できる.

孫子定理をくり返し使い多項式列 $S_k$, $T_k$, $Q_k$ をつくる.

算法1. 初期値 $Q_0 = Q$

$$S_k Q_k + T_k X = R$$

$$Q_{k+1} = Q + T_k$$

$$k = 0, 1, 2, \cdots$$

孫子定理より $(Q_k, X) = 1$ ならば, 上の漸化式は支障なく進行する.

いま, $X_{k+1} = X + S_k$ をおく.

定理. $X_k$, $Q_k$ が, それぞれ $X_\infty$, $Q_\infty$ に収束したとすれば $QX + R = Q_\infty X_\infty$ が成り立つ. すなわち $X_\infty$ は1次式 (2.1) の解である.

証明．帰納法を用いて

$$QX+R = QX+S_k Q_k + T_k X$$
$$= (Q+T_k)X + S_k Q_k$$
$$= Q_{k+1}X + S_k Q_k$$

$Q_k, X_k$ の収束を仮定したので $S_k$ の極限を $S_\infty$ とすれば上式の右辺は $Q_\infty(X+S_\infty) = Q_\infty X_\infty$ に収束する．

（証明終）

次は，収束次数の問題である．それに必要な補題から述べる．

補題1．算法1における $S_k Q_k + T_k X = R$, $k=0,1,2,\cdots$ において $\|R\| < \varepsilon$, $\|X\| = O(1)$, $\|Q_0\| = O(1)$ のとき

$$\|S_k\| = O(\varepsilon), \quad \|T_k\| = O(\varepsilon)$$
$$\|T_k - T_{k-1}\| = O(\varepsilon^k), \quad \|S_k - S_{k-1}\| = O(\varepsilon^k)$$

となる．ただし $\varepsilon > 0$ は十分小とする．

証明　$S_{k+1}Q_{k+1} + T_{k+1}X = R$ と $k$ を1減じた式を辺々差引けば

$$(T_{k+1}-T_k)X + S_{k+1}(Q+T_k) - S_k(Q+T_{k-1}) = 0$$
$$(T_{k+1}-T_k)X + (S_{k+1}-S_k)Q_k = -S_k(T_k - T_{k-1}).$$

$k=0$ のとき（$\|R\| < \varepsilon$ と）$(Q_0, X) = 1$ より $\|S_0\| = O(\varepsilon)$, $\|T_0\| = O(\varepsilon)$ となる．また，各 $k$ において，$(Q_k, X) = 1$ を仮定したので $\|S_k\| = O(\varepsilon)$, $\|T_k\| = O(\varepsilon)$．よって $T_k - T_{k-1}$ に関する漸

化式において $T_{-1}=0$ と考え，帰納法により，$\|T_k - T_{k-1}\| = O(\varepsilon^k)$，
$\|S_k - S_{k-1}\| = O(\varepsilon^k)$ を証明できる．　（証明終）

定理　多項式列 $X_k$ の収束次数は1である．

証明．　$f = QX+R$ を $\bmod X_k$ の意味で評価する．

$$QX+R = QX + S_k Q_k + T_k X$$

$X_{k+1} = X + S_k$ であるから

$$QX+R, \bmod X_{k+1} = Q_{k+1}(-S_k) + S_k Q_k$$
$$= -S_k (T_k - T_{k-1})$$

したがって，補題1より

$$\|QX+R, \bmod X_k\| \le \|S_k\| \|T_k - T_{k-1}\|$$
$$= O(\varepsilon) \cdot O(\varepsilon^k) = O(\varepsilon^{k+1})$$

が得られる．　（証明終）

1次収束する方法をリスタート方式で使えば，高次収束となる．すなわち　$X_0 = X$ とおき　$X_k = X + S_{k-1}$，$k=1,2,\cdots,m$ をつくる．$X_m$ をあらためて $X_0$ とおき，これを反復すれば $m+1$ 次収束となる．

$X$ を1次因子とするとき，$m=1,2,3$ に対応する算法は Newton 法，Halley 法，Kiss 法となる．

FFT を使い高速算法となるのは $X$ が円周等分多項式でその次数が2のべきの場合である．数値実験は，これからの予定．

分割統治法の著者らの実験例は，文献 2) による．

## 参考文献

1) Freeman, T. L ; A divide and conquer method for polynomial zeros , J. Comput. Appl. Math . 30 , pp. 71~79 (1990)

2) 園田信吾，猪井鉄也，杉浦洋，鳥元基生；分割統治法による多項式の数値的因数分解，日本応用数理学会論文誌，Vol. 1 , No. 4 , pp. 277~290 (1991)．