

多項式剰余公式の計算アルゴリズム

庄司卓夢

TAKUMU SHOJI

新潟大学自然科学研究科

GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY, NIIGATA UNIVERSITY

田島慎一

SHINICHI TAJIMA

新潟大学工学部情報工学科

FACULTY OF ENGINEERING, NIIGATA UNIVERSITY

Abstract

Hermite 補間積分は、剰余公式として扱うことができる。本研究では、その積分核を代数解析的な手法で解析し、微分型の剰余公式の計算アルゴリズムの導出、および数式処理システムへの実装を行う。

1 剰余公式と Hermite 補間積分

任意の多項式 $\varphi(x)$ を $f(x)$ で割った商を $q(x)$ 、余りを $r(x)$ とすると、

$$\varphi(x) = q(x)f(x) + r(x), \deg r(x) < \deg f(x)$$

と表せる。ここで、 $\varphi(x), f(x) \in K[x]$, $K = \mathbb{Q}$, $Z = \{x \in \mathbb{C} \mid f(x) = 0\}$ とする。この時、剰余 $r(x)$ は、 Z と、 Z における $\varphi(x)$ の値と、 Z における $\varphi(x)$ の導関数の値を用いて表せる。これを、剰余公式と呼ぶことにする。

例 1.1 $f(x) = (x - \alpha)(x - \beta)$ の場合。

$r(x)$ は 1 次以下の多項式であるから、 $r(x) = Ax + B$ とおける。

連立方程式 $\varphi(\alpha) = r(\alpha) = A\alpha + B$, $\varphi(\beta) = r(\beta) = A\beta + B$ を解いて、

$$r(x) = \frac{\varphi(\alpha) - \varphi(\beta)}{\alpha - \beta}x + \frac{\alpha\varphi(\beta) - \beta\varphi(\alpha)}{\alpha - \beta} \text{ と表せる。}$$

例 1.2 $f(x) = (x - \alpha)^2$ の場合。

$\varphi'(x) = q'(x)(x - \alpha)^2 + 2q(x)(x - \alpha) + r'(x)$ を用いて、例 1.1 と同じように連立方程式を解くと、

$$r(x) = \varphi'(\alpha)x + \varphi(\alpha) - \alpha\varphi'(\alpha) \text{ と表せる。}$$

さて、 $\varphi(x)$ に対し、 $r(x)$ を対応させる写像を R とおく。写像

$$R: K[x] \longrightarrow K[x]$$

は線形であり、次のような解析的表示を持つ。

定理 1.3 (Hermite 補間積分)

$$R(\varphi)(x) = r(x) = \frac{1}{2\pi\sqrt{-1}} \oint \frac{f(y) - f(x)}{y - x} \frac{1}{f'(y)} \varphi(y) dy.$$

$f(y) - f(x)$ は $y - x$ を因子に持つから, $\frac{f(y) - f(x)}{y - x}$ が多項式であることがすぐにわかる. そこで, $\frac{f(y) - f(x)}{y - x} = \sum_{i=0}^{m-1} \kappa_i(y) x^i$ とおくと, Hermite 補間は,

$$r(x) = \sum_{i=0}^{\deg f - 1} \left\{ \frac{1}{2\pi\sqrt{-1}} \oint \frac{\kappa_i(y)}{f'(y)} \varphi(y) dy \right\} x^i$$

の形になる.

例 1.4 $f(x) = (x - \alpha)(x - \beta)$ の場合.

単純に公式に代入すると,

$$\begin{aligned} r(x) &= \frac{1}{2\pi\sqrt{-1}} \oint \frac{(y - \alpha)(y - \beta) - (x - \alpha)(x - \beta)}{y - x} \frac{\varphi(y)}{(y - \alpha)(y - \beta)} dy \\ &= \frac{1}{\alpha - \beta} \frac{1}{2\pi\sqrt{-1}} \oint (x + y - (\alpha - \beta)) \left(\frac{1}{y - \alpha} - \frac{1}{y - \beta} \right) \varphi(y) dy \\ &= \frac{1}{\alpha - \beta} \left\{ \frac{1}{2\pi\sqrt{-1}} \oint \left(\frac{\varphi(y)}{y - \alpha} - \frac{\varphi(y)}{y - \beta} \right) dy x + \frac{1}{2\pi\sqrt{-1}} \oint \left(\frac{(y - (\alpha - \beta))\varphi(y)}{y - \alpha} - \frac{(y - (\alpha - \beta))\varphi(y)}{y - \beta} \right) dy \right\} \\ &= \frac{\varphi(\alpha) - \varphi(\beta)}{\alpha - \beta} x + \frac{\alpha\varphi(\beta) - \beta\varphi(\alpha)}{\alpha - \beta} \end{aligned}$$

となり, 確かに 例 1.1 と答えが一致する.

2 代数的局所コホモロジー

有理関数の特異性に注目した同値類

$$\left[\frac{h(x)}{f^\ell(x)} \right] = \frac{h(x)}{f^\ell(x)} + K[x]$$

を考えると, これは $H_{[Z]}^1(K[x])$ の元とみなせるので, $\left[\frac{h(x)}{f^\ell(x)} \right]$ を有理関数 $\frac{h(x)}{f^\ell(x)}$ の定める代数的局所コホモロジー類と呼ぶ. これを用いれば, Hermite 補間は,

$$r(x) = \sum_{i=0}^{\deg f - 1} \left\{ \frac{1}{2\pi\sqrt{-1}} \oint \left[\frac{\kappa_i(y)}{f'(y)} \right] \varphi(y) dy \right\} x^i$$

となる.

一般に, 次が成り立つ.

補題 2.1

$$\text{Ext}_{K[x]}^1(K[x]/\langle f^\ell(x) \rangle, K[x]) \cong \left\{ \left[\frac{h(x)}{f^\ell(x)} \right] \in H_{[Z]}^1(K[x]) \mid h(x) \in K[x] \right\}.$$

ベクトル空間 $K[x]/\langle f^\ell(x) \rangle$ とベクトル空間 $\left\{ \left[\frac{h(x)}{f^\ell(x)} \right] \in H_{[Z]}^1(K[x]) \mid h(x) \in K[x] \right\}$ の間には留数による自然な pairing が存在する. この pairing は非退化であり, 次の双対定理が成り立つ.

定理 2.2 ベクトル空間 $\left\{ \left[\frac{h(x)}{f^\ell(x)} \right] \in H_{[Z]}^1(K[x]) \mid h(x) \in K[x] \right\}$ は, ベクトル空間 $K[x]/\langle f^\ell(x) \rangle$ の双対ベクトル空間の構造を持つ.

3 双対基底

今, 割る多項式 $f(x)$ が既約であるとする. 積分核 $[\frac{\kappa(x,y)}{f(y)}]$ を x について整理すると, $[\frac{\kappa(x,y)}{f(y)}] = \sum_{i=0}^{\deg f} [\frac{\kappa_i(y)}{f(y)}] x^i$ となるから, $K[x]/\langle f(x) \rangle$ の単項式基底 $\{1, x, x^2, \dots, x^{m-1}\}$ に対する双対基底は,

$$\{[\frac{\kappa_0(x)}{f(x)}], [\frac{\kappa_1(x)}{f(x)}], \dots, [\frac{\kappa_{m-1}(x)}{f(x)}]\}$$

で与えられる. ここで, $a_i(x) = \kappa_i(x) f'(x)^{-1} \bmod f(x)$ とおくと, $[\frac{\kappa_i(y)}{f(y)}] = [\frac{f'(y) f'(y)^{-1} \kappa_i(y)}{f(y)}] = a_i(y) [\frac{f'(y)}{f(y)}]$ となるから,

$$\{a_0(x) [\frac{f'(x)}{f(x)}], a_1(x) [\frac{f'(x)}{f(x)}], \dots, a_{m-1}(x) [\frac{f'(x)}{f(x)}]\}$$

と変形できる.

従って, 剰余公式は,

$$\begin{aligned} r(x) &= \sum_{i=0}^{\deg f-1} \left\{ \frac{1}{2\pi\sqrt{-1}} \oint a_i(y) [\frac{f'(y)}{f(y)}] \varphi(y) dy \right\} x^i \\ &= \sum_{i=0}^{\deg f-1} \sum_{\alpha \in Z} a_i(\alpha) \varphi(\alpha) x^i \end{aligned}$$

となる.

4 Noether 作用素表示

既約多項式 $f(x)$ が与えられたとし, 割る多項式として $f^\ell(x)$ を考える. Hermite 補間は,

$$r(x) = \frac{1}{2\pi\sqrt{-1}} \oint \frac{f^\ell(y) - f^\ell(x)}{y - x} \frac{1}{f^\ell(y)} \varphi(y) dy$$

となるが, このままでは計算が困難である. そこで次の定理を利用する.

定理 4.1 (Noether 作用素表示) 代数的局所コホモロジー類 $[\frac{h(x)}{f^\ell(x)}]$ は, $\ell-1$ 階の微分作用素 L を用いて,

$$[\frac{h(x)}{f^\ell(x)}] = L[\frac{f'(x)}{f(x)}], \quad L = \sum_{i=0}^{\ell-1} \left(-\frac{d}{dx}\right)^{\ell-1-i} a_i(x), \quad a_i(x) \in K[x]/\langle f(x) \rangle.$$

と表せる. この微分作用素を Noether 作用素と呼ぶ.

Noether 作用素の具体的な計算法については [1, 2, 3] を参照. さて, この定理を用いて, 部分積分を行いながら式変形をしていくと,

$$\begin{aligned} \frac{1}{2\pi\sqrt{-1}} \oint \frac{h(y)}{f^\ell(y)} \varphi(y) dy &= \frac{1}{2\pi\sqrt{-1}} \oint L[\frac{f'(y)}{f(y)}] \varphi(y) dy \\ &= \frac{1}{2\pi\sqrt{-1}} \oint \frac{f'(y)}{f(y)} \sum_{i=0}^{\ell-1} a_{\ell-1-i}(y) \frac{d^i \varphi}{dy^i}(y) dy \\ &= \sum_{i=0}^{\ell-1} \sum_{\alpha \in Z} a_{\ell-1-i}(\alpha) \varphi^{(i)}(\alpha) \end{aligned}$$

となるから, $\frac{f^\ell(y)-f^\ell(x)}{y-x} = \sum_{i=0}^{(\deg f)\ell-1} \kappa_i(y)x^i$ とおけば,

$$\begin{aligned} r(x) &= \sum_{i=0}^{(\deg f)\ell-1} \left\{ \frac{1}{2\pi\sqrt{-1}} \oint \frac{\kappa_i(y)}{f^\ell(y)} \varphi(y) dy \right\} x^i \\ &= \sum_{i=0}^{(\deg f)\ell-1} \sum_{j=0}^{\ell-1} \sum_{\alpha \in Z} a_{i,\ell-1-j}(\alpha) \varphi^{(j)}(\alpha) x^i \end{aligned} \quad (1)$$

となる.

また, 別のやり方として,

$$\frac{f^\ell(y)-f^\ell(x)}{y-x} \frac{1}{f^\ell(y)} = \frac{f(y)-f(x)}{y-x} \left(\frac{f^{\ell-1}(x)}{f^\ell(y)} + \cdots + \frac{f(x)}{f^2(y)} + \frac{1}{f(y)} \right)$$

と変形し, $h(x,y) = \frac{f(y)-f(x)}{y-x}$ とおけば,

$$\begin{aligned} r(x) &= \sum_{i=0}^{\ell-1} \left\{ \frac{1}{2\pi\sqrt{-1}} \oint \frac{h(x,y)}{f^{i+1}(y)} \varphi(y) dy \right\} f^i(x) \\ &= \sum_{i=0}^{\ell-1} \left\{ \frac{1}{2\pi\sqrt{-1}} \oint L_i \left[\frac{f'(y)}{f(y)} \right] \varphi(y) dy \right\} f^i(x) \\ &= \sum_{i=0}^{\ell-1} \left\{ \sum_{j=0}^{\deg f-1} \sum_{\alpha \in Z} (L_i \varphi)(\alpha) x^j \right\} f^i(x) \end{aligned} \quad (2)$$

となり, f -adic 展開された剰余公式を得ることもできる.

例 4.2 $f(x) = (x^3 - x - 1)^2$ による剰余公式を求めよ.

(1) x で整理した型

```
[176] hermite_rem(x^3-x-1,2,z,1);
[(3/23*z^2-4/23)*x^5+(-1/23*z+3/23)*x^4+(-7/23*z^2+3/23*z+8/23)*x^3+(-3/23*z^2+1/23*z+1/23)*x^2+(4/23*z^2-2/23*z-7/23)*x+4/23*z^2-3/23*z-4/23, (162/529*z^2-174/529*z-108/529)*x^5+(-105/529*z^2+54/529*z+70/529)*x^4+(-270/529*z^2+290/529*z+180/529)*x^3+(-195/529*z^2+327/529*z+130/529)*x^2+(420/529*z^2-216/529*z-280/529)*x+200/529*z^2-254/529*z+43/529]
```

$Z = \{x | f(x) = 0\}$ とおくと, 答えは,

$$r(x) = \sum_{z \in Z} \left\{ \left(\frac{3z^2-4}{23} \varphi'(z) + \frac{162z^2-174z-108}{23^2} \varphi(z) \right) x^5 + \cdots \right\}$$

となる.

(2) f -adic 型

```
[177] hermite_rem(x^3-x-1,2,z,2);
[[ (3/23*z^2-4/23)*x^2+(-1/23*z+3/23)*x-4/23*z^2+3/23*z+4/23, (162/529*z^2-174/529*z-108/529)*x^2+(-105/529*z^2+54/529*z+70/529)*x-108/529*z^2+116/529*z+72/529 ], [ (-6/23*z^2+9/23*z+4/23)*x^2+(9/23*z^2-2/23*z-6/23)*x+4/23*z^2-6/23*z+5/23 ]]
```

$r(x) = r_1(x)f(x) + r_0(x)$ とおくと,

$$\begin{aligned} r_1(x) &= \sum_{z \in \mathbb{Z}} \left\{ \left(\frac{3z^2 - 4}{23} \varphi'(z) + \frac{-162z^2 - 174z - 108}{23^2} \varphi(z) \right) x^2 + \left(\frac{-z + 3}{23} \varphi'(z) + \frac{-105z^2 + 54z + 70}{23^2} \varphi(z) \right) x \right. \\ &\quad \left. + \frac{-4z^2 + 3z + 4}{23} \varphi'(z) + \frac{-108z^2 + 116z + 72}{23^2} \varphi(z) \right\}, \\ r_0(x) &= \sum_{z \in \mathbb{Z}} \left\{ \frac{-6z^2 + 9z + 4}{23} \varphi(z) x^2 + \frac{9z^2 - 2z - 6}{23} \varphi(z) x + \frac{4z^2 - 6z + 5}{23} \varphi(z) \right\} \end{aligned}$$

となる.

5 一般化

割る多項式 $f(x)$ が $f(x) = f_1^{\ell_1}(x)f_2^{\ell_2}(x) \cdots f_m^{\ell_m}(x)$ で与えられる場合を考える. ここで, $f_1(x), \dots, f_m(x)$ は既約であるとする.

因子が多い場合には, 剰余公式を求める方法として, 中国剰余定理を用いる方法が考えられるが, 本稿では, Hermite 補間を用いる方法について解説する.

Hermite 補間は,

$$r(x) = \frac{1}{2\pi\sqrt{-1}} \oint \frac{f_1^{\ell_1}(y)f_2^{\ell_2}(y) \cdots f_m^{\ell_m}(y) - f_1^{\ell_1}(x)f_2^{\ell_2}(x) \cdots f_m^{\ell_m}(x)}{y-x} \frac{1}{f_1^{\ell_1}(y)f_2^{\ell_2}(y) \cdots f_m^{\ell_m}(y)} \varphi(y) dy$$

となるが, $\kappa_f(x, y) = \frac{f_1^{\ell_1}(y)f_2^{\ell_2}(y) \cdots f_m^{\ell_m}(y) - f_1^{\ell_1}(x)f_2^{\ell_2}(x) \cdots f_m^{\ell_m}(x)}{y-x}$ とおき,

$$r(x) = \frac{1}{2\pi\sqrt{-1}} \oint \kappa_f(x, y) \left[\frac{1}{f_1^{\ell_1}(y)f_2^{\ell_2}(y) \cdots f_m^{\ell_m}(y)} \right] \varphi(y) dy$$

として考える.

この積分式から, 剰余公式を求める方法として 3 通りの方法が考えられる.

方法 1

$\frac{\kappa_f(x, y)}{f_1^{\ell_1}(y)f_2^{\ell_2}(y) \cdots f_m^{\ell_m}(y)}$ を部分分数分解すれば, 4 節での計算に帰着される.

方法 2

$Z = \{x | f(x) = 0\}$ に台を持つ代数的局所コホモロジー類 $[\frac{1}{f(x)}]$ を直和分解し,

$$[\frac{1}{f(x)}] = \sigma_{f_1} + \sigma_{f_2} + \cdots + \sigma_{f_m}$$

とおく. ただし, $\sigma_{f_i} \in H_{[Z_{f_i}]}^1(K[x])$ は $Z_{f_i} = \{x | f_i(x) = 0\}$ に台を持つ代数的局所コホモロジー類である.

$\sigma_{f_i} = S_{f_i}[\frac{f_i'(x)}{f_i(x)}]$ となる微分作用素 S に対し, $T_{f_i} = \kappa_f(x, y)S_{f_i}$ とおくと,

$$r(x) = \sum_{i=1}^m \frac{1}{2\pi\sqrt{-1}} \oint T_{f_i} \left[\frac{f_i'(y)}{f_i(y)} \right] \varphi(y) dy$$

を得るので部分積分することで剰余公式が作れる. このような微分作用素 T_{f_i} を求めれば剰余公式が求まる. 微分作用素を用いると, 有理関数の部分分数分解を求めずに T_{f_i} を直接構成できる.

方法 3

まず, 2 因子 $f(x) = f_1(x)f_2(x)$ の場合で考える.

$$\begin{aligned}\kappa_f(x, y) &= \frac{f_1(y)f_2(y) - f_1(x)f_2(x)}{y - x} \\ &= \frac{f_1(y)f_2(y) - f_1(y)f_2(x) + f_1(y)f_2(x) - f_1(x)f_2(x)}{y - x} \\ &= \frac{f_2(y) - f_2(x)}{y - x} f_1(y) + \frac{f_1(y) - f_1(x)}{y - x} f_2(x)\end{aligned}$$

と式変形すると, 積分核は, $[\frac{\kappa_f(x, y)}{f(y)}] = [\frac{\kappa_{f_2}(x, y)}{f_2(y)}] + [\frac{\kappa_{f_1}(x, y)}{f_1(y)f_2(y)}]f_2(x)$ となる.

$\frac{1}{f_1(y)f_2(y)} = \frac{c_{f_1}(y)}{f_1(y)} + \frac{c_{f_2}(y)}{f_2(y)}$ と部分分数分解すれば, Hermite 補間は,

$$\begin{aligned}r(x) &= \frac{1}{2\pi\sqrt{-1}} \oint [\frac{\kappa_{f_2}(x, y)}{f_2(y)}] \varphi(y) dy \\ &\quad + \{ \frac{1}{2\pi\sqrt{-1}} \oint [\frac{c_{f_1}(y)\kappa_{f_1}(x, y)}{f_1(y)}] \varphi(y) dy + \frac{1}{2\pi\sqrt{-1}} \oint [\frac{c_{f_2}(y)\kappa_{f_1}(x, y)}{f_2(y)}] \varphi(y) dy \} f_2(x) \\ &= \sum_{i=0}^{\deg f_2-1} a_{i, \kappa_{f_2}}(\alpha) \varphi(\alpha) x^i + \{ \sum_{i=0}^{\deg f_1-1} a_{i, c_{f_1}\kappa_{f_1}}(\alpha) \varphi(\alpha) x^i + \sum_{i=0}^{\deg f_1-1} a_{i, c_{f_2}\kappa_{f_1}}(\alpha) \varphi(\alpha) x^i \} f_2(x)\end{aligned}$$

となる. m 因子についても同様に計算できる.

例 5.1 $f(x) = (x^2 + 1)^2(x^3 - x - 1)$ による剰余公式を求めよ.

```
[442] hermite_rem_g([[x^2+1, 2, z1], [x^3-x-1, 1, z2]], 11);
((-1/10*p1z1+21/100*p0z1)*z1+22/575*p0z2*z2^2+59/575*p0z2*z2+1/20*p1z1+11/50*p0z
1-99/575*p0z2)*x^6+((1/20*p1z1+3/25*p0z1)*z1+59/575*p0z2*z2^2-77/575*p0z2*z2+1/1
0*p1z1-4/25*p0z1+22/575*p0z2)*x^5+(1/10*p0z1*z1-11/115*p0z2*z2^2+28/115*p0z2*z2+
1/5*p0z1-8/115*p0z2)*x^4+((1/10*p1z1-1/100*p0z1)*z1+118/575*p0z2*z2^2-154/575*p0
z2*z2-1/20*p1z1-8/25*p0z1+44/575*p0z2)*x^3+((1/20*p1z1-43/100*p0z1)*z1-176/575*p
0z2*z2^2+103/575*p0z2*z2-3/20*p1z1-13/50*p0z1+217/575*p0z2)*x^2+((1/20*p1z1-63/1
00*p0z1)*z1+59/575*p0z2*z2^2-77/575*p0z2*z2-3/20*p1z1-4/25*p0z1+22/575*p0z2)*x+
(-1/20*p1z1-8/25*p0z1)*z1-99/575*p0z2*z2^2+22/575*p0z2*z2-1/10*p1z1+13/50*p0z1+15
8/575*p0z2
```

$Z_1 = \{x|x^2 + 1 = 0\}$, $Z_2 = \{x|x^3 - x - 1 = 0\}$ とおくと, 答えは,

$$\begin{aligned}r(x) &= \sum_{z_1 \in Z_1} \{((-1/10)\varphi'(z_1) + \frac{21}{100}\varphi(z_1))z_1 + \frac{1}{20}\varphi'(z_1) + \frac{11}{50}\varphi(z_1))x^6 + \dots\} \\ &\quad + \sum_{z_2 \in Z_2} \{(\frac{22}{575}\varphi(z_2)z_2^2 + \frac{59}{575}\varphi(z_2)z_2 - \frac{99}{575}\varphi(z_2))x^6 + \dots\}\end{aligned}$$

となる.

6 まとめ

Hermite 補間積分は積分型の剰余公式であり, 極の位数が高い場合は複雑な式変形が必要となるため従来
の方法ではアルゴリズムの構成ができなかった. しかし, 本研究により, 微分作用素を用いると微分型の剰
余公式に書き換えることが明らかになった. その結果, アルゴリズムの構成が可能になり, 計算機への実装
も可能となった.

参 考 文 献

- [1] 庄司卓夢, 田島慎一: 高速留数計算アルゴリズム,
京都大学数理解析研究所講究録 1456 「Computer Algebra-Design of Algorithms, Implementations and
Applications」(2005), 133-143.
- [2] 加藤涼香, 田島慎一: 有理関数のローラン展開アルゴリズムと代数的局所コホモロジー,
京都大学数理解析研究所講究録 1395 「Computer Algebra-Design of Algorithms, Implementations and
Applications」(2004), 50-56.
- [3] 田島慎一: Holonomic な定数係数線形偏微分方程式系と Grothendieck duality,
京都大学数理解析研究所講究録「積分核の代数解析的研究」掲載予定.