

Modulo- p 演算による行列の逆転

三菱電機 中研 下地貞夫

小林健三 大貝佳子

1. まえがき

Modulo- p 演算は、整数の計算において最後の答が整数であれば、中間の値はいくら大きくても、また分数であっても、 p による簡約値の範囲内の整数の計算で、目的の答を得ることが出来る^{1,2)}。これはミニコンのようなシンプルな演算装置を持つ計算機に対して特に有効な方法であると考えられる。

p を計算機の最大ビット数に近い値に選び、いくつかの p についての計算結果を組み合わせることにより、多重精度の計算の中間を単精度で済ませることができ、計算時間を著しく短縮することができる³⁾。

ここでは、高橋・石橋の方法⁴⁾に基づき、実際の問題に適用する目的で、Modulo- p 演算による行列反転プログラムを作成し、その結果が得られたのを報告を行なう。正および負の数を平等に扱ふ必要から絶対最小剰余系を用い、また簡約値を組み合わせて元の数を求めるための連立合同式の解法および

プログラムの検証法をも含めて、この方法を適用するにあたっての考え方を述べる。

2. 簡約値から元の数を求める方法

行列反転の方法は標準の消去法によるアルゴリズムを用いたが、これをModulo- p 演算で行なうこと、および簡約値の形で得られた解から元の数を求めることが問題となる。剰余系の選定との関連から、まず、整数 Y とそれを p で簡約した y との関係を整理しておく。

互に素な p_1 および p_2 を用い、 Y を

$$Y = p_1 X_1 + y_1 = p_2 X_2 + y_2, \quad 0 \leq y_1 < p_1, \quad 0 \leq y_2 < p_2 \quad (1)$$

と書く。既知の p_1, p_2, y_1, y_2 から Y, X_1, X_2 を求めるものとする。一般に、互に素な k 個の p_i から、 Y に対して、

$$Y \equiv y_1 \pmod{p_1}, Y \equiv y_2 \pmod{p_2}, \dots, Y \equiv y_k \pmod{p_k} \quad (2)$$

を連立する。 M_s および M_s^{-1} を次のように定め、

$$p_1 p_2 \cdots p_k = M_s p_s, \quad \text{および} \quad M_s M_s^{-1} \equiv 1 \pmod{p_s} \quad (3)$$

すなわち、 $M_s M_s^{-1}$ を p_s で簡約した時にのみ1で、他の p_i について簡約した時には、すべて0になるようにする。この時

$$Y \equiv M_1 M_1^{-1} y_1 + M_2 M_2^{-1} y_2 + \cdots + M_k M_k^{-1} y_k \pmod{p_1 p_2 \cdots p_k} \quad (4)$$

が、連立合同式(2)の解である⁵⁾。実際は、

$$Y \equiv M_i \cdot M_i^{-1} \cdot y_i \equiv y_i \pmod{p_i} \quad i=1, \dots, k \quad (5)$$

(4)式を用いて Y を計算する場合に、 k 個の k 重精度の乗算、簡約および加算を必要とする。

計算のアルゴリズムとしては、漸化式の形で与えられるものが望ましく、係数 λ_i を求めて行くという方法をとる。すなわち、(2)の解を

$$\left. \begin{aligned} Y_i &= y_i, \quad q_i = y_i \\ q_i &\equiv (p_1 \cdot p_2 \cdots p_{i-1})^{-1} \cdot (y_i - Y_{i-1}) \pmod{p_i} \\ Y_i &= p_1 \cdot p_2 \cdots p_{i-1} \cdot q_i + Y_{i-1} \end{aligned} \right\} \quad (6)$$

によって求める”。この計算は2重、3重、 $\dots$ 、 k 重精度の乗算、簡約および加算を順々に積み重ねて行けば良いから、(4)式を用いる場合に比べて、相当に計算量が減少される。

(6)式は(4)式と同等であり、互に移り変ることが出来る。

$$p_2 \cdot (p_2)^{-1} \pmod{p_1} + p_1 \cdot (p_1)^{-1} \pmod{p_2} = p_1 \cdot p_2 + 1 \quad (7)$$

を用いると、

$$\begin{aligned} Y_2 &\equiv p_1 \cdot [(p_1)^{-1} \cdot (y_2 - y_1)] \pmod{p_2} + y_1 \\ &\equiv p_1 \cdot (p_1)^{-1} \pmod{p_2} \cdot y_2 + [1 - p_1 \cdot (p_1)^{-1} \pmod{p_2}] \cdot y_1 \\ &\equiv p_2 \cdot (p_2)^{-1} \pmod{p_2} \cdot y_1 + p_1 \cdot (p_1)^{-1} \pmod{p_2} \cdot y_2 \pmod{p_1 p_2} \end{aligned}$$

となる。 Y_3 については、(4)式を変形して

$$Y_3 \equiv p_3 \cdot (p_3)^{-1} \pmod{p_1 p_2} \cdot Y_2 + p_1 p_2 [(p_1 p_2)^{-1}] \pmod{p_3} \cdot y_3 \quad (8)$$

と書き、(8)式を3個の p に拡張した、

$$\begin{aligned}
 & P_2 P_3 (P_2 P_3)^{-1} (\text{mod } p_1) + P_1 P_3 (P_1 P_3)^{-1} (\text{mod } p_2) + P_1 P_2 (P_1 P_2)^{-1} (\text{mod } p_3) \\
 & = P_1 P_2 P_3 + 1
 \end{aligned} \tag{9}$$

を用いることにより同様に計算される。

完全剰余系としては、(1)式に見えるように、非負の最小剰余系を選ぶと、 Y が負の場合に(4)式および(6)式のいずれも $\text{mod } p_1 p_2 \cdots p_k$ として、 $p_1 p_2 \cdots p_k$ について Y の補数が与えられる。そこで、負の数も同様に扱うためには、絶対最小剰余系、 $-(p_1-1)/2, \dots, -1, 0, 1, \dots, (p_1-1)/2$ などを用い、 $|Y| \leq (p_1 p_2 \cdots p_k - 1)/2$ の範囲を表現することにした。

また、 P は計算の途中で分数が現われても、割算を行ないそのまま計算を進めうるように素数とし、15ビットのミニコンを用いたので、その範囲で大きいものを選んだ。 $2^{15} = 32768$ に近い $p_1 = 32749, p_2 = 32719, \dots, p_{10} = 32633$ であり、最大のものから10個用意した。これで、ほぼ $\pm 5 \times 10^{44}$ の範囲の数を扱うことができる。

3. 計算法について

行列反転をModule- p 演算で行なうには、次のような演算が必要である。

(1) 簡約

割算の命令を使って、商と余りに分け、余りの部分だけを取り出す。ここでは、数値を次の区間、

$$-(P-1)/2 \leq y \leq (P-1)/2 \quad (10)$$

に簡約を行なうので、余りが $(P-1)/2$ を越えていれば、 P を引いて簡約値とする。

(2) 逆数

文献1に従って、フェルマの小定理に基づく方法を用いた。すなわち、 P を法として a の逆数は、

$$a^{-1} \equiv a^{P-2} \pmod{P} \quad (11)$$

となるので、 P を2進数で表わしておくと、

$$a^{P-2} = a^{\sum_{i=0}^{s-1} d_i \cdot 2^i} = a^{d_0} \cdot a^{d_1 \cdot 2} \cdot \dots \cdot a^{d_{s-1} \cdot 2^{s-1}} \quad (12)$$

によって、速やかに計算される。 d_i は1または0である。

(3) 行列反転

順々に消去を行ない、 $\{a_{ij}\}$ をストアした場所には、最後に逆行列 $\{a_{ij}\}^{-1}$ がストアされるという標準の方法を用いた。 $\{a_{ij}\}$ の要素が整数であれば、行列式 $|a_{ij}|$ および a_{ij} の余因子 D_{ij} は共に整数であり、計算スラッパの最後で求められる $|a_{ij}|$ および $\{a_{ij}\}^{-1}$ を用いて、 $D_{ij} = \{a_{ij}\}^{-1} \cdot |a_{ij}|$ が得られる。

一般に分数の分母と分子を共に未知として、 $\text{mod } P$ での値から、元の数を求める方法は存在しないが、一方が別に計算される場合には、このように他方を得ることは出来る。

(4) 簡約値から元の数を求める計算

$p_1, p_2, \dots, p_k$ は素数であり、順に $p_1, p_1 \cdot p_2, p_1 \cdot p_2 \cdot p_3$ を法とする完全剰余系における Y を求めていくので、 $|Y| \leq (p_1 \cdot p_2 \cdots p_k - 1)/2$ となれば、そこから先の Y の簡約値は Y 自身に等しくすべて同じ値になる。たとえば、 $Y \leq (p_1 \cdot p_2 - 1)/2, (p_2 \cdot p_3 - 1)/2, (p_1 \cdot p_3 - 1)/2$ であれば、それぞれの完全剰余系における Y の簡約値は同じ値で Y に等しい。

偶然に、 Y が p_i の多数の積に等しい時は、(7)式の初めのステップで Y と異なったもので、互に等しい値が現われるが、それは別に検算して、発見することができる。

(5) 多重精度計算

いま p は単精度一杯に近くとってあるが、答がそれを越えるときは、多重精度の計算が必要である。(7)式の計算を行なうために、多重精度データの加算および多重精度データと単精度データの乗・除算が必要である。

ここでは、多重精度データを構成する各ワードのサインビットは、最上位のもののみを有効として、符号の判定や大小の比較、オーバーフローの検出などに用い、中2位以下のものには常に0をセツトして有効扱いとした。1ワード毎に区切ったものを普通の演算回路の方式に倣って処理し、加・減算および乗・除算を行なった。

4 演算性

Modulo-p 演算においては、計算の中間のステップで大きな値が現われてオーバーフローしたり、丸めのために桁落ちして精度を損うことはなく、厳密な結果が得られる¹⁾。

Ill-behavior なものの例として、ロトキンの行列 $\{L_{ij}\}$ ⁶⁾

$$\left. \begin{aligned} L_{ij} &= 1 & i=1 \\ &= 1/(i+j-1) & i \geq 2 \end{aligned} \right\} \quad (13)$$

を選び、反転した結果を示す。各要素の分母の最小公倍数を掛け、4行4列の L_4 については、次のような結果になる。

$p_1 = 32749$ による簡約値は

$$\{420 \cdot L_4\}^{-1} = \frac{1}{12169} \cdot \begin{Bmatrix} 196 & -5880 & -9229 & 12169 \\ -1470 & -3349 & -1304 & -7516 \\ 2840 & -11351 & -15186 & -9306 \\ -1715 & -12169 & -4563 & 4653 \end{Bmatrix} \quad (14)$$

$p_2 = 32719$ による簡約値は

$$\{420 \cdot L_4\}^{-1} = \frac{1}{12139} \cdot \begin{Bmatrix} 196 & -5880 & -9199 & 12139 \\ -1470 & -3319 & -1424 & -7796 \\ 2940 & -11381 & 15366 & -9486 \\ -1715 & -12139 & -4743 & -4743 \end{Bmatrix} \quad (15)$$

$p_3 = 32714$ による簡約値は

$$\{420 \cdot L_4\}^{-1} = \frac{1}{12137} \cdot \begin{Bmatrix} 196 & -5880 & -9199 & 12137 \\ -1470 & -3319 & -1432 & -7388 \\ 2940 & -11383 & 15373 & -9498 \\ -1715 & -12837 & -4749 & -4749 \end{Bmatrix} \quad (16)$$

簡約値に対する元の数は

$$\{420 \cdot L_4\}^{-1} = \frac{-1}{20580} \cdot \begin{Bmatrix} 196 & -5880 & 23520 & -20580 \\ -1470 & 29400 & -132300 & 123480 \\ 2940 & -44100 & 211680 & -205800 \\ -1715 & 20580 & -102900 & 102900 \end{Bmatrix} \quad (17)$$

となり，これから直ちに $\{L_4\}^{-1}$ が得られる。

計算速度を，16ビットのミニコンで Extended アセンブラによる浮動小数点演算を行なった場合と比較すると次のようになる。(6)式の計算は p を3つ用いると，要素当り，整数型の加・減算を7回，乗・除算を6回，必要とする。この計算にはあまり時間を必要としないので，全体として約4倍の計算速度を得ることが出来る。

最後に，御指導下さった京大・一松教授に謝意を表す。

参考文献

- 1) 高橋・石橋：情報処理，vol. 1, p. 78 (1960)
- 2) 高橋・石橋：J. Inform. Proc. Soc. Japan 1 (1961)
- 3) Merrill : IEEE. Trans. EC-13 No.2 (1964)
- 4) 一松：数値計算，至文堂 (昭38)
- 5) 三瓶・中山訳：整数論入門，共立全書 (昭34)
- 6) 大原・石原：情報処理，vol. 14, p. 135 (1973)