数理解析研究所講究録
第215巻 1974年 47-54

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后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できる[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[1)]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，好結果が得られたので報告を行なう。正および負の数を平等に扱う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. 簡約値からもとの数を求める方法

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もと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こう。

互に素なp_1およびp_2を用い，Yを

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

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，

$$Y \equiv y_1 \ (\mathrm{mod}\ p_1),\ Y \equiv y_2 \ (\mathrm{mod}\ p_2),\ \cdots,\ Y \equiv y_k \ (\mathrm{mod}\ p_k) \qquad (2)$$

を連立する。M_sおよびM_s^{-1}を次のように定め，

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

すなわち，$M_s \cdot M_s^{-1}$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

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

が，連立合同式(2)の解である[5]。実際に，

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

(4)式を用いてYを計算する場合には，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X_iを求めて行くという方法をとる。すなわち，(2)の解を

$$\left.\begin{aligned} &Y_1 = y_1, \quad q_1 = y_1 \\ &q_i \equiv (p_1 \cdot p_2 \cdots p_{i-1})^{-1} \cdot (y_i - Y_{i-1}) \pmod{p_i} \\ &Y_i = p_1 \cdot p_2 \cdots p_{i-1} \cdot q_i + Y_{i-1} \end{aligned}\right\} \tag{6}$$

によって求める"。この計算は2重，3重，…，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，相当に計算量が減小される。

(6)式は(4)式と同等であり，互に移り変ることができる。

$$p_2 \cdot (p_2)^{-1} (\mathrm{mod}\ p_1) + p_1 \cdot (p_1)^{-1} (\mathrm{mod}\ p_2) = n p_1 \cdot p_2 + 1 \tag{7}$$

を用いると，

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

となる。Y_3については，(4)式を変形して

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

と書き，(8)式を3個のpに拡張した，

$$p_2 \cdot p_3 \cdot (p_2 \cdot p_3)^{-1} (\mathrm{mod}\ p_1) + p_1 \cdot p_3 \cdot (p_1 \cdot p_3)^{-1} (\mathrm{mod}\ p_2) + p_1 \cdot p_2 \cdot (p_1 \cdot p_2)^{-1} (\mathrm{mod}\ p_3)$$
$$= p_1 \cdot p_2 \cdot p_3 + 1 \tag{9}$$

を用いることによって　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 $\mathrm{mod}\ p_1 \cdot p_2 \cdots p_k$ として，$p_1 \cdot p_2 \cdot \cdots \cdot p_k$ についての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，絶対最小剰余系，$-(p_1-1)/2, \cdots, -1, 0, 1, \cdots, (p_1-1)/2$ などを用い，$|Y| \leq (p_1 \cdot p_2 \cdot \cdots \cdot p_k - 1)/2$ 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，16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。$2^{15} = 32768$ に対して，$p_1 = 32749$, $p_2 = 32719$, --，$p_{10} = 32633$ 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Modulo-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，

$$-(p-1)/2 \le y \le (p-1)/2 \qquad (10)$$

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，

$$a^{-1} \equiv a^{p-2} \pmod{p} \qquad (11)$$

となるので，p を2進数で表わしておくと，

$$a^{p-2} = a^{\sum_{i=0}^{s-1} d_i \cdot 2^i} = a^{d_0} \times a^{d_1 \times 2} \times \cdots \cdot a^{d_{s-1} \cdot 2^{s-1}} \qquad (12)$$

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，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，計算ステップの最後で求められる $|a_{ij}|$ および $\{a_{ij}\}^{-1}$ を用いて，$D_{ij} = \{a_{ij}\}^{-1} \times |a_{ij}|$ が得られる[1]。

一般に分数の分母と分子を共に未知として，mod p での値から，元の数を求める方法は未だないが，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, …, p_kは素であり，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，オーバフローの検出などに用い，第2位以下のものには常に0をセットして無効扱いとした。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-behabior なものの例として，ロトキンの行列 $\{L_{ij}\}$[6]

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

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

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

$P_2 = 32719$ による簡約値は

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

$P_3 = 32714$ による簡約値は

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

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できる。

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）