アルゴリズム 42－4
（1994．11．18）

一変数多項式を成分に持つ行列の行列式の計算について

鈴木 治郎

信州大学医療技術短期大学部

Fermat の予想の第一の場合，すなわち $x^l + y^l = z^l, (xyz, l) = 1$ は自明でない整数解を持たないという予想に関して，現在，べき指数 $l < 8.858 \times 10^{20}$ については予想の成立することが示されている．この事実の検証のための計算において，成分が単項式である行列の行列式が現われる．それを数式処理システムにおいて標準的なガウス-ジョルダンの掃き出し法にもとづいた計算法を用いた場合，計算量は行列のサイズ n に対して $O(2^{2n})$ と指数関数増大になる．ここではモジュラー算法を用いて一変数多項式に適したアルゴリズムに記述することで，$O(m^3)$ で実行できる計算法を与える．ただし m は多項式としての行列式の次数である．

ON SOME COMPUTATION OF THE DETERMINANT FOR A MATRIX WITH POLYNOMIAL ELEMENTS

SUZUKI Jiro
School of Allied Medical Sciences, Shinshu University

Asahi 3-1-1, Matumoto, Nagano, 390 JAPAN

For the first case of Fermat's last theorem, that is the equation $x^l + y^l = z^l, (xyz, l) = 1$ has non-trivial integer solution for $l \geq 3$, we know the fact that the conjecture is true for $l < 8.858 \times 10^{20}$. In the computation of the fact, we have done the computation of the determinant for some matrices with monomial elements. When we compute the determinant by the Gauss-Jordan method, we need $O(2^{2n})$ computation for the size n of matrix. We show that we can implement a $O(m^3)$ method with modular arithmetic where m is the degree of the determinant, especially suitable for one-variable polynomials.

1 はじめに

以下の問題は整数論における特殊な問題において必要となる計算を効率的に実行するためのアルゴリズムに関する話なので，まず，簡単にもとの問題との関連について触れる．

Fermat の予想の第一の場合，すなわち「方程式

$$x^l + y^l = z^l, \qquad (xyz, l) = 1$$

は $l \geq 3$ ならば自明でない整数解をもたない」という予想に関して現在のところべき指数 l が $l < 8.858 \times 10^{20}$の範囲では予想が正しいことが鈴木 [5] によって得られている．

この事実は次の Pollaczek[4] の定理にもとづく．($\varphi(\cdot)$ はオイラーの関数を表わす)

定理 1 *Fermat* の予想第一の場合が誤り（つまり自明でない解をもつ）としたとき，$1 \leq h \leq (a-1)/2$ の範囲の各 h に関して構成される単項式を成分とする $2\varphi(h) \times \varphi(h)$ 行列の，$\varphi(h) \times \varphi(h)$ 小行列式全体が lを法として共通の零点をもたないならば，

$$k^{l-1} \equiv 1 \pmod{l^2} \qquad (1 < k \leq a) \tag{1}$$

が成り立つ．

この定理が成り立つ場合，すなわち合同式 (1) が成り立つわけだが，l^2を法とする剰余類についての一般論と比較すると，lが小さいときにこの合同式が成り立つことは事実に反する．このため定理の仮定である「自明でない解をもつ」という性質が誤りとなる．上記べき指数に関する結果は合同式と両立できるような lの評価に Coppersmith[1] が与えたものを用いると上記べき指数の範囲が得られる．

以下の節では上記定理の小行列式の性質の証明に現われる計算について述べる．そこでコンピュータ処理にかかる問題として考慮する性質は

- 一変数単項式を成分として与えられる行列の行列式の計算になる
- 行列式として得られる多項式の係数は整数として正確に求める
- 行列式の多項式としての次数は行列のサイズを n としたとき n^2になる．

の 3 点である．このうち 3 番目の性質は以下では用いないが，以下で述べる方法の計算量 $O(nm^3) = O(n^7)$ を導く．

なお，以下の計算量評価においてモジュラー算法で用いる素数の個数に比例する部分は評価に入れていない．これは，たとえば数式処理システム上で直接に計算する方法と比較したことを想定した場合，係数の増大にともなう計算量の増大は両者に効いてくるから，それを無視してもアルゴリズムの比較は可能なためである．

以下の構成は第 2 節において掃き出し法により行列式を求める場合の計算量の評価，第 3 節において我々の実行したアルゴリズムの解説，第 4 節で計算例をあげる．本稿における計算は東京大学計算機センターの HITAC S-820/80 を用いて 1992 年に行われた．

2 掃き出し法による計算量

多項式を成分にもつ n 次正方行列について，それを掃き出し法で計算する場合，1 回の掃き出しのステップごとに得られる多項式の次数は直前のステップで得られた多項式の次数の和，およそ 2 倍に等しい．また，そのステップにおいて各成分の計算は多項式の積だから，直前のステップで得られた多項式の次数の積に計算量は比例する．よって，掃き出し法の計算量 $O(n^3)$ と合わせて $O(n^3 2^{2n})$ を得る．

計算量が指数関数増大になる原因は上記分析にあるように多項式の積の計算の実行にある．実際はさらに多項式の係数増大の問題も生じるため，多倍長数処理にともなう計算時間の増大も起こる．

Granville&Monagan[2] においてはワークステーション上で数式処理システム Maple を用いてのパッケージ（掃き出し法）により計算している．

3 実際の計算法

以下では変数 X についての多項式を成分にもつ n 次正方行列を $M_h(X)$, その行列式を $D_h(X)$ で表わす．

$$D_h(X) = \sum_{i=0}^{m} c_i X^i$$

と表されるとする．これを $\{c_i\}$ を変数と見た関係式とみなし X に適当な整数を代入して得られる連立方程式を解くことで係数 $\{c_i\}$ を求める．

ただし $\{c_i\}$ は比較的大きな整数になるので，適当な素数の組 $\{p\}$ に関する合同式を解いて $\{c_i \bmod p\}$ を求めた後，中国式剰余定理によって $\{c_i\}$ を構成する．以下にその詳細を述べる．

1. 行列式で与えられる多項式の次数 m を定める．もちろん実際の問題に応じて定め方も異なる．

2. 行列式の各項の係数の上限 B を定める．理論的に次の Hadamard の不等式型の評価ができる．

   補題 1 (Goldstein-Graham[3]) (i,j) 成分 $a_{i,j}$ が次数 $n_{i,j}$ の多項式 $a_{i,j} = \sum_{k=0}^{n_{i,j}} a_{i,j,k} X^k$ で与えられている行列 $(a_{i,j})_{i,j=1,n}$ について，その行列式として得られる多項式の係数の上限 B は

   $$B = \sqrt{\prod_{i=1}^{n} \sum_{j=1}^{n} ||a_{i,j}||^2}$$

   で与えられる．ただし $||a_{i,j}|| = \sum_{k=0}^{n_{i,j}} |a_{i,j,k}|$ である．

3. モジュラー算法で用いる素数の組 $\{p_k\}$ を，上限 Bに対して不等式

$$\prod_k p_k > 2B$$

を満たすように定める．この不等式の条件を満たすときに Bより絶対値が小さい整数は p_kを法とした剰余類から中国式剰余定理を用いて一意に構成できる．なお各 p_k はそれを法とした整数計算が，実際に用いるコンピュータの単精度整数計算に収まる大きさの素数とすると実行効率が高い．

4. $M_h(X)$ を $s = 0, 1, \ldots, m$ で評価する．すなわち $M_h(s)$ を求める．なお，$M_h(X)$ の各成分は多項式であるが $X = s$ で評価する際には多項式評価の標準的な方法である Horner 法によらずに $\{s^i \mid i = 0, 1, \ldots, m\}$ をメモリにおいてから計算したほうが効率的であり，それは，スーパーコンピュータのような内積計算に向いたコンピュータにおいて顕著に差が出る．津田 [7] に書いてあるように「スーパーコンピュータにおいては必ずしも従来良いとされてきたアルゴリズムが良いとは限らない」の一例である．

5. $M_h(s)$ から行列式 $D_h(s)$ を計算する．掃き出し法でよい．計算量は $O(n^3)$ である．

6. 各 p_kについて合同式

$$\begin{pmatrix} 0^0 & 0^1 & \cdots & 0^m \\ 1^0 & 1^1 & \cdots & 1^m \\ \vdots & \vdots & \ddots & \vdots \\ m^0 & m^1 & \cdots & m^m \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_m \end{pmatrix} \equiv \begin{pmatrix} D_h(0) \\ D_h(1) \\ \vdots \\ D_h(m) \end{pmatrix} \pmod{p_k} \qquad (2)$$

を解く．左辺の正方行列の行列式は van der Monde の行列式，すなわち$\prod_{0 \le i < j \le m}(j-i)$ であるから，法として用いる素数が条件 $m < p_k$を満たせば必ず一意に解を持つ．計算量は $O(m^3)$ になる．

7. 中国式剰余定理により $\{c_i \bmod p_k\}$ から $\{c_i\}$ を構成する．

と，以上で計算がすべて実行される．

4 計算例

$h = 8$ の場合，鈴木 [5] で計算した $M_8(X)$ の一つは次のようになる．

$$\begin{pmatrix} X & X & X & X \\ X^2 & X^3 & X & X^3 \\ X^2 & X & X^5 & X^4 \\ X & X^3 & X^5 & X^7 \end{pmatrix}$$

また，それに対する行列式は

$$D_8(X) = X^4(X-1)^4(X+1)^2(X^6+X^5+3X^4+X^3+3X^2+X+1)$$

になる．係数は鈴木 [5] における最大の例でおよそ 200 桁，上限 B はおよそ 900 桁になった．「およそ」としてあるのは実際は第 1 節で述べた小行列式を 5 つ同時に計算させているために評価を緩くしてあることによる．なお，$h = 53$ の場合の計算時間は 120 秒 ($m = 532$) であった．

参考文献

[1] Coppersmith,D. *Fermat's last theorem (case 1) and the Wieferich criterion.* Math. Comp. **54** (1990).

[2] Granville,A. Monagan,B. *The first case of Fermat's last theorem is true for all prime exponents up to 714,591,416,091,389.* Trans. Amer. Math. Soc. **306** (1987) 329–359.

[3] Goldstein,A.J. Graham,R.L. *A Hadamard-type bound on the coefficients of a determinant of polynomials.* SIAM Rev. **16** (1974) 394–395.

[4] Pollaczek,F. *Über den grössen Fermat'schen Satz.* Wien. Berichte. Abt. IIa **126** (1917) 45–59.

[5] Suzuki,J. *On the generalized Wieferich criteria.* Proc. Japan Acad. Ser.A. **70-7** 230–234.

[6] 中澤・上野・加藤. スーパーコンピュータ HITAC S-820 の効率的使用法 (1)-(3). 東京大学大型計算機センター センターニュース **21** No.7–11.

[7] 津田孝夫. 数値処理プログラミング (岩波講座ソフトウェア科学 **9**). 岩波書店 (1988).