数理解析研究所講究録
第 486 巻 1983 年 11-26

3　不定方程式の p進解法　と　その応用

東大・理・情報科学　村尾裕一 (Hirokazu Murao)
都立大・理・数学　古川昭夫 (Akio Furukawa)

1。はじめに

線形 Diophantine 方程式を多項式環上で解くことは，$\mathbb{Z}$ 上の多項式及び有理式を主に扱う現在の数式処理システムにおいては，有用性が高い。つまり，多項式 $F, G, C \in \mathbb{Z}[u_1, \cdots, u_n][x]$ が与えられた時，不定方程式

$$A \cdot F + B \cdot G = C$$

を満たす多項式 $A, B \in \mathbb{Q}[u_1, \cdots, u_n][x]$ をある条件のもとで求めるのである。例えば，部分分数分解[3]は，

$$\deg_x(C) < \deg_x(F) + \deg_x(G),$$

$$\deg_x(A) < \deg_x(G), \quad \deg_x(B) < \deg_x(F)$$

という条件のもとで，上の問題に帰着する。[6]

ところで，x を体 $K = \mathbb{Q}(u_1, \cdots, u_n)$ の上で代数的とし，その代数的拡大体 $K(x)$ について考えよう。$F(X) \in \mathbb{Z}[u_1, \cdots, u_n][X]$ を x の最小多項式とすると，$K(x)$ は $K[X]/(F)$ と K 上同形で

あり，$K(x)$の元は．xの多項式として表わしうる。さらに．係数の分母を通分することがいわゆる有理化である。

例)．　$\omega^2+\omega+1=0$　として．

$$\frac{1}{3\omega+5}=\frac{-9\omega^2-9\omega+4}{13}$$

一般に．REDUCEにおいてそうであるように．多くの数式処理システムでは．有理式の表現が簡潔である（有理式を係数とする多項式などと比べて）ので，$K(x)$の元について．この有理化した形を求めるのが我々の目的である。それには．

最小多項式 $F \in \mathbb{Z}[u_1,\cdots,u_n][X]$　と．

$G \in \mathbb{Z}[u_1,\cdots,u_n][X]$　（但し．$\deg_X(G) < \deg_X(F)$）

とを与えられたとき，

$A\cdot F + B\cdot G = C$　　over $\mathbb{Z}$，

$\deg_X(B) < \deg_X(F)$

を満足する．$A, B \in \mathbb{Z}[u_1,\cdots,u_n][X]$，$C \in \mathbb{Z}[u_1,\cdots,u_n]$が求められればよい。これらより．

$B\cdot G \equiv C \pmod{(F)}$

ゆえ．

$$\frac{1}{G} \equiv \frac{B}{C} \pmod{(F)}$$

となり，$1/G$を有理化したことになる。

問題：

多項式 $F, G \in \mathbb{Z}[u_1, \cdots, u_n][X]$

但し．F は既約，$\deg_X(G) < \deg_X(F)$

が与えられた時，

以下を満たす．$A, B \in \mathbb{Z}[u_1, \cdots, u_n][X]$，$C \in \mathbb{Z}[u_1, \cdots, u_n]$ を求める：

$A \cdot F + B \cdot G = C$ over $\mathbb{Z}$，

$\deg_X(B) < \deg_X(F)$，

$\gcd(C, \text{content}(B, X)) = 1$，

但し．content (B, x) は．X についての多項式 B の係数すべての gcd を表わす．

存在性については．F を既約としたことから．$\gcd(F, G) = 1$ で．このことから明らかであろう。又．上の A, B, C が符号の不定性を除いて一意的であることは容易に示される。

解法としては．gcd の場合と同様に剰余列をつくるか，結果の次数の上限がわかっている（$< \deg_X(F)$）ことから未定係数法が考えられる。しかし、数式処理においては．その表現法が限られていることや，計算量及び式の膨張という観点で．これらをできる限り多項式のまま計算したい。それには、前者の場合剰余列のかわりに、擬剰余列[3]をつくればよい。それでも、最悪の場合には．F と G との終結式を計算することに

なるし、途中で簡約化を行ったとしても、最終的にBとCとが大きなgcdをもつことも考えられる。このことは、未定係数法によっても基本的に同じである。

そこで考えられるのが、gcd計算[8]との類似性から、構成法を用いることである。P.S.Wangは、一変数有理式の部分分数分解の場合についてその方法を示した[16]が、我々はその方法をもとに、多変数の場合に拡張することを試た。

2。解法の全体像

一般に、多項式に対する構成的解法は、以下の四段階からなる：

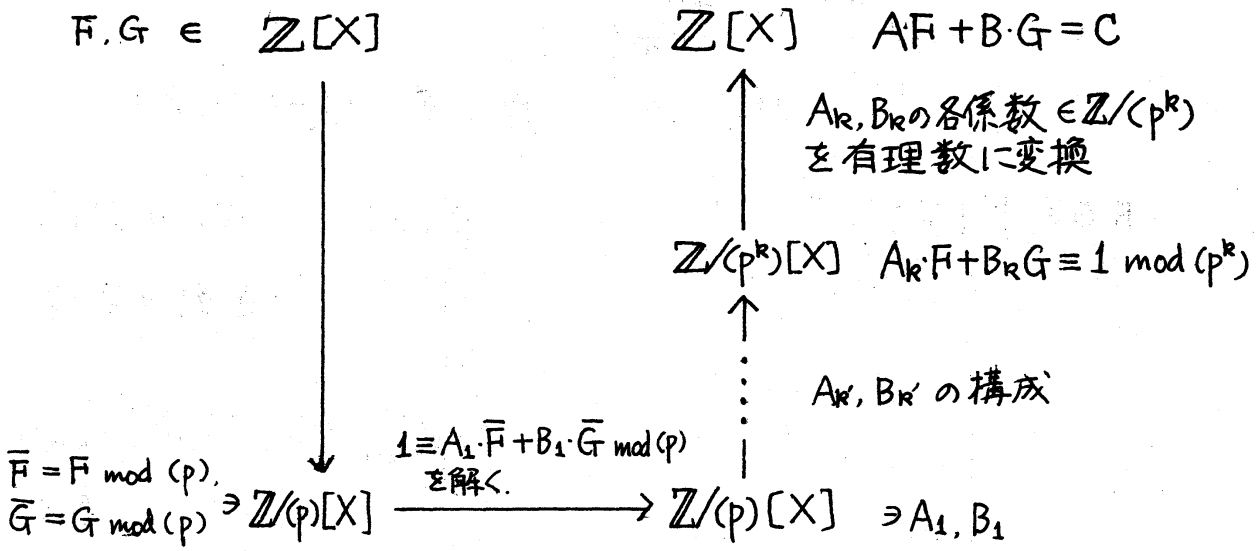
1) 適当な法を選び、その剰余環への準同型写像により多項式の像をつくる（各係数について行えばよい），
2) それらの像に対して、与えられた問題をとく，
3) 構成法により、逐次法をあげていく，
4) もし可能なら（解が存在するなら）ば，元の多項式環へと変換する。

1)の法として，$\mathbb{Z}$上では，一変数の場合素数p（のつくるイデアル(p)），多変数$(u_1,\cdots,u_n)$の場合$(u_1-b_1,\cdots,u_n-b_n)$（但し、$b_i\in\mathbb{Z}$）ととればよい。2)においては、より小さな係数域（上記では体）において解くため，アルゴリズム自体は

同じでも，係数の膨張は押さえられる。3)の段階は，p-進展開あるいは，一般化したTaylor展開の高次の項を求めていくことに他ならない。

2-1　一変数の場合.

基本的に，P.S.Wangのアルゴリズム"に同じであるので，以後詳細は省略する。



上図で，pとしては次の条件を満たす素数を選ぶ：

- $p \nmid lc_x(F)$，$p \nmid lc_x(G)$，
- $\gcd(\bar{F}, \bar{G})$ over $\mathbb{Z}/(p) = 1$.

（但し．$lc_x(F)$は．Xの多項式Fの主係数，即ち0でないXの最高次の係数を表す.）又，$\mathbb{Z}/(p)$としては$\{-\lceil p/2 \rceil, \cdots, 0, \cdots, \lceil p/2 \rceil\}$ととる。構成回数の上限を与えるkとしては．A, B, Cの係数の最大値をdとして．$p^j > 2d^2$を満たす最小のjをとればよい。dを正確に求めることは，問題をとくことに

他ならず，理論値は一般に大き過ぎるので，インプリメントの際にはF,Gや多倍長とのかね合いで充分に大きくとればよい（後述）。

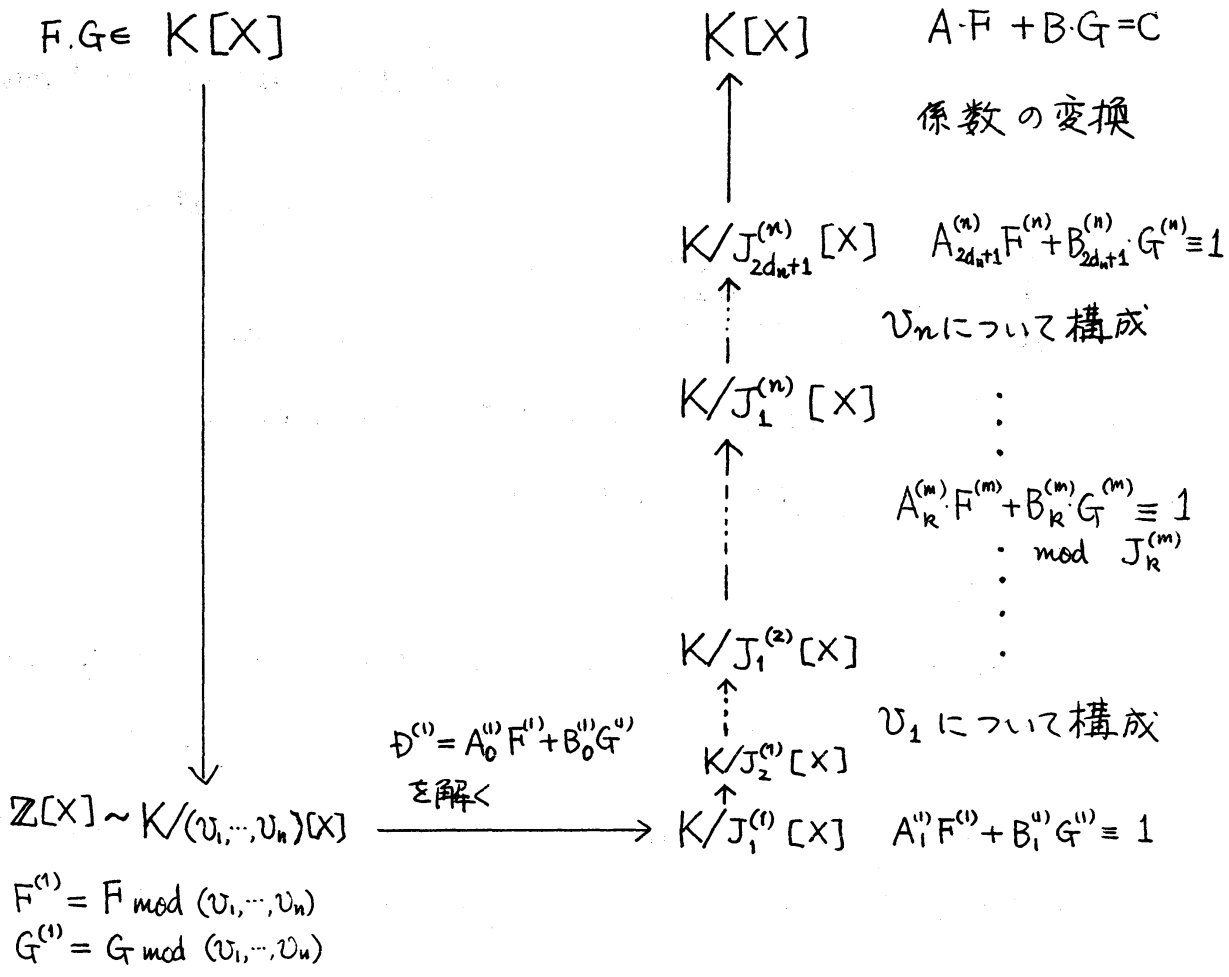
2-2 多変数の場合

notation: $K = \mathbb{Z}[u_1, \cdots, u_n]$,

$$J_k^{(m)} = (q,\ v_1^{2d_1+1}, \cdots, v_{m-1}^{2d_{m-1}+1},\ v_m^k,\ v_{m+1}, \cdots, v_n)$$

$$J_1^{(m+1)} = J_{2d_m+1}^{(m)}$$

$$v_i = u_i - b_i \quad , \quad b_i \in \mathbb{Z} \quad (i=1, \cdots, n)$$



法 $(u_1-b_1, \cdots, u_n-b_n)$ については、一変数の場合と同様に、次の条件が必要である：

- $lc_x(F)$, $lc_x(G) \not\equiv 0 \mod (u_1-b_1, \cdots, u_n-b_n)$
- $\gcd(F^{(1)}, G^{(1)})$ over $\mathbb{Z} = 1$.

$D^{(1)} = A_0^{(1)} F^{(1)} + B_0^{(1)} G^{(1)}$ を解くには、前記の一変数の場合を用いればよい。数係数についても法 (q) をとるのは、除算の際に有理数となるのを防ぐためであり、同様に、A, B, Cの数係数より十分大きくとればよい。後で示すように、$A_1^{(1)} F^{(1)} + B_1^{(1)} G^{(1)} \equiv 1 \mod (q)$ が一度求まればよいので、一変数の構成に用いた p^k でよい（十分大きければ）。

構成法は、EEZアルゴリズム[5]のように、各変数毎に行っていく。変数 v_m については、後に示す構成法を繰返して、$v_m^{2d_m}$ までの近似を求める。ここで d_m は、A, B, C中の変数 v_m についての最大の次数で、これは、A, B, Cの行列式表現[4]から、簡単な計算によりその上限が求められる。そこまで変数 v_m について構成した時点で、

$$A_0^{(m+1)} \cdot F + B_0^{(m+1)} \cdot G \equiv D^{(m+1)} \mod (v_{m+1}, \cdots, v_n)$$

を満たす $A_0^{(m+1)}$, $B_0^{(m+1)}$, $D^{(m+1)}$ を求める。これは、$A_0^{(m+2)}$, $B_0^{(m+2)}$, $D^{(m+2)}$ を有理式変換アルゴリズムで求める際に、単位元の不定性を除くのに用い、これにより、$\mathbb{Z}$ 上のA, B, Cへと最終的に変換される。

3。構成法 —— 一変数

$F, G \in \mathbb{Z}[X]$

法を $J_k = (p^k)$ と書き，$J_k \to J_{k+1}$ の構成の一段階を示す。

$$A_k \cdot F + B_k \cdot G \equiv 1 \mod J_k,$$

$$\deg_X(A_k) < \deg_X(G),\ \deg_X(B_k) < \deg_X(F)$$

なる $A_k, B_k \in \mathbb{Z}/J_k[X]$ は既知とする。

$$1 - A_k \cdot F - B_k G \in J_k$$

ゆえ．

$$p^k \cdot C_k = (1 - A_k F - B_k G \mod J_{k+1}),$$

$$C_k \in \mathbb{Z}/(p)[X]$$

と書くことができる。ここで $\deg_X(C_k) < \deg_X(F) + \deg_X(G)$ ゆえ，

$$\alpha_k = \text{remainder}(C_k \cdot A_1,\ G \bmod (p)),$$

$$\beta_k = \text{remainder}(C_k \cdot B_1,\ F \bmod (p))$$

とおけば．

$$C_k \equiv \alpha_k \cdot F + \beta_k \cdot G \mod (p)$$

を満たす。この α_k, β_k が各々 A_k, B_k の補正項となる。即ち．

$$A_{k+1} = A_k + p^k \cdot \alpha_k,$$

$$B_{k+1} = B_k + p^k \cdot \beta_k.$$

$\because$ $A_{k+1} F + B_{k+1} G \equiv (A_k \cdot F + B_k \cdot G) + p^k(\alpha_k F + \beta_k G)$

$\equiv (1 - p^k \cdot C_k) + p^k \cdot C_k$

$\equiv 1 \mod J_{k+1}$ //

4。有理数への変換 (P.S.Wang)[6,7]

このアルゴリズムは P.S.Wang による。詳細は文献を参照のこと。

整数 C, q が与えられた時,

$a/b \equiv C \mod (q)$,

$|a|, |b| < \sqrt{q/2}$

なる a, b を求める:

```
U := (1, 0, q);   V := (0, 1, C);
while √(q/2) ≤ V[3] do
  { Q := ⌈U[3]/V[3]⌉;
    R := U − Q·V;
    U := V;
    V := R }
if |V[3]| ≥ √(q/2) then error
return (V[3], V[2])
        ⋮      ⋮
        a      b
```

例: $C = -2460$, $q = 6561 = 3^8$

U, V の列:
(1, 0, 6561)
(0, 1, -2460)
(1, 2, 1641)
(1, 3, -819)
(3, 8, 3)

$\rightarrow \quad -2460 \equiv \frac{3}{8} \mod 3^8$

(注) この例のように, C が零因子でも構わない。

5。構成法 —— 多変数

$$F, G \in \mathbb{Z}[u_1, \cdots, u_n][X]$$

notation は 2-2 に従う。

$$F^{(m)} = F \mod J_1^{(m+1)}$$

$$G^{(m)} = G \mod J_1^{(m+1)}$$

$J_k^{(m)} \to J_{k+1}^{(m)}$ の構成の一段階を示す。つまり，変数 $u_{m+1}, \cdots, u_n$ は含まず，$u_1, \cdots, u_{m-1}$ は十分に構成され，変数 u_m について k 次の項を求めるステップである。ここで，b_i の選び方から，$lc_X(F^{(m)})$，$lc_X(G^{(m)})$ は定数項を持ち，従って $\mathbb{Z}[u_1, \cdots, u_n]/J_1^{(m+1)}$ で逆元を持つことに注意する。つまり，$F^{(m)}$ $G^{(m)}$ を除数とする除算が可能である。

さて，

$$A_k^{(m)} \cdot F^{(m)} + B_k^{(m)} \cdot G^{(m)} \equiv 1 \mod J_k^{(m)},$$

$$\deg_X(A_k^{(m)}) < \deg_X(G^{(m)}), \quad \deg_X(B_k^{(m)}) < \deg_X(F^{(m)}),$$

なる $A_k^{(m)}, B_k^{(m)} \in K/J_k^{(m)}[X]$ は既知とする。

$$1 - A_k^{(m)} \cdot F^{(m)} - B_k^{(m)} \cdot G^{(m)} \in J_k^{(m)}$$

ゆえ，

$$u_m^k \cdot C_k^{(m)} = (1 - A_k^{(m)} \cdot F^{(m)} - B_k^{(m)} \cdot G^{(m)} \mod J_{k+1}^{(m)})$$

なる $C_k^{(m)} \in K/J_1^{(m)}[X]$ を定義できる。ここで，

$$\deg_X(C_k^{(m)}) < \deg_X(F^{(m)}) + \deg_X(G^{(m)})$$

である。

これより.

$$\alpha_k^{(m)} = \text{remainder}\left(C_k^{(m)} A_1^{(m)},\ G^{(m-1)}\right)$$
$$\beta_k^{(m)} = \text{remainder}\left(C_k^{(m)} B_1^{(m)},\ F^{(m-1)}\right) \quad \in K/J_1^{(m)}[X]$$

は.

$$\alpha_k^{(m)} \cdot F_k^{(m)} + \beta_k^{(m)} \cdot G_k^{(m)} \equiv C_k^{(m)} \mod J_k^{(m)}$$

を満たし, この $\alpha_k^{(m)}$, $\beta_k^{(m)}$ が $A_k^{(m)}$, $B_k^{(m)}$ の補正項となる:

$$A_{k+1}^{(m)} = A_k^{(m)} + v_m^k \cdot \alpha_k^{(m)}$$
$$B_{k+1}^{(m)} = B_k^{(m)} + v_m^k \cdot \beta_k^{(m)}.$$

$\because$ $A_{k+1}^{(m)} F^{(m)} + B_{k+1}^{(m)} \cdot G^{(m)}$

$\equiv (A_k^{(m)} F^{(m)} + B_k^{(m)} G^{(m)}) + v_m^k (\alpha_k^{(m)} F^{(m)} + \beta_k^{(m)} G^{(m)})$

$\equiv (1 - v_m^k \cdot C_k^{(m)}) + v_m^k \cdot C_k^{(m)}$

$\equiv 1 \mod J_{k+1}^{(m)}$ //

$\alpha_k^{(m)}$, $\beta_k^{(m)}$ の計算は, 効率の面から.

$$X^i \equiv Q_i^{(m)} \cdot F^{(m)} + R_i^{(m)} \cdot G^{(m)} \mod J_1^{(m)}$$
$$(i = 0, \cdots, \deg_X(FG) - 1)$$

なる $Q_i^{(m)}$, $R_i^{(m)}$ を一度だけ計算しておき (上記の剰余として), $Q_i^{(m)}$, $R_i^{(m)}$ の $C_k^{(m)}$ の X^i についての係数による線形結合をつくればよい。前後するが, あらかじめ F, G には変数変換 $u_i \to v_i$ を施しておき, $K/J_1^{(m)}$ における係数の除算は, 級数計算と同様に行えばよい。

変数 v_m について充分構成した後, v_{m+1} についての構成に

うつる際の $A_1^{(m+1)}$, $B_1^{(m+1)}$ は.

$$A_1^{(m+1)} = A_{2d_m+1}^{(m)},$$
$$B_1^{(m+1)} = B_{2d_m+1}^{(m)}$$

で与えられる。

6。有理式への変換

前節の構成法を変数 v_m について充分行った後, $A_{2d_m+1}^{(m)}, B_{2d_m+1}^{(m)}$ の X の中乗の各係数多項式 (v_m) について, 有理式を構成する。それには, 当初の問題と同様に, v_m の多項式を d として, $(m = v_m^{2d_m+1})$

$$c \cdot m + b \cdot d = a$$

なる $a, b, (c) \in \mathbb{Z}[v_1, \cdots, v_n]/J_1^{(m+1)}$ を求めればよい。この時.

$$\deg_{v_m}(a),\ \deg_{v_m}(b) \leq d_m$$

という条件をつけることにより, a, b は, もし存在すれば. a又は b の係数 $(\in \mathbb{Z}[v_1, \cdots, v_n]/J_1^{(m)})$ の1つを決めれば一意的に定められる。この係数は.

$$D^{(m)} = b \mod (v_m), \text{ あるいは.}$$
$$B_0^{(m)} = a \mod (v_m),$$

より与えられる。ここで, $D^{(n+1)} = C$ は gcd が1であるという条件より定数項をもち. その結果, $D^{(m)}$ 及び b には零因

子は含まれない。

v_m の多項式 $m = v_m^{2d_m+1}$, $d \in \mathbb{Z}[v_1,\cdots,v_n]/J_1^{(m+1)}$,
$D^{(m)} \in \mathbb{Z}[v_1,\cdots,v_n]/J_1^{(m)}$ が与えられたとき,

$$a/b \equiv d \mod m,$$
$$\deg_{v_m}(a),\ \deg_{v_m}(b) \le d_m,$$
$$b \equiv D^{(m)} \mod (v_m)$$

なる $a, b \in K/J_1^{(m)}[v_m]$ を求める:

```
U := (1, 0, m); V := (0, 1, d);
while dm < deg_vm(V[3]) do
  { Q := quotient(U[3], V[3], v_m)
    R := U − Q·V;
    U := V;
    V := R }
if deg_vm(V[2]) > d then error
return (V[3]·D^(m)/(b mod (v_m)), V[2])
```

上のアルゴリズム中では, 常に

$$U[1]\cdot m + U[2]\cdot d = U[3],$$
$$V[1]\cdot m + V[2]\cdot d = V[3]$$

が成り立っている。つまり, これは元の問題の剰余列を作る

解法を行っていることと同等である。但し、この場合、係数域が $\mathbb{Z}(v_1,\cdots,v_{m-1})/(v_1^{2d_1+1},\cdots,v_{m-1}^{2d_{m-1}+1})$ であるため、整級数環と同様の演算が行われ、それらの元は多項式として表現される。このため、係数の不要な膨張は防げる。但し、体ではないため、上記アルゴリズム中の Q の計算では除算ができないことがありうる。このことは、$lc_{v_m}(d)$ が単位元であっても取り除くことはできない。同様に、$q=p^k$ ととったときも、数係数について起こりうることで、注意が必要である。

7。インプリメント上の注意及び結論

以上述べた方法は、すべて選んだ法が'ラッキー'であった場合に適用されるものである。その意味で、ここで述べた構成的解法は、確率的アルゴリズムの域を出ない。この問題点は、EZGCD アルゴリズム等の構成的アルゴリズムには共通のものであり[2]、法として何が'ラッキー'であるかを正確に把握するには結局元の問題を正確に解いてしまうしかない。我々の問題において、有理数(式)における"error"というのは、法はラッキーであったとして、構成の回数が足りないかどうかを check する必要がある。前述のように、構成の回数の上限は、正確には与えようがないためである。また、前節で述べた零因子の問題は、$lc_{v_m}(d)$ をまず単位元になるように法をとるこ

とで確率を低くすることができる。それには、いくつかの法 (b_i) に対して $A_1^{(1)}$, $B_1^{(1)}$ を計算し、できるだけ X^j の係数を0としないものを選ぶことである。もし、それでも除算不能となった場合には(変数 v_m で)、b_i $(i=1,\cdots,m-1)$ をその時点で変えればよい。

いずれにしても、A,B,Cに対する行列式表現からわかるように、係数域を十分に大きくとれば、上記の問題が起こる確率はかなり低くなる。(反例:1) ただし、インプリメントの際には、これらの問題点には注意が必要であり、2節に示したように4つの段階に完全に切り離すことはできない。

現在、一変数の場合についてインプリメントした限りでは、Fが高次の場合、我々の方法が有効であることが確かめられている。

[参考文献]

1) J.H. Davenport, B.M. Trager; "Factorization over Finitely Generated Fields", Proc. SYMSAC '81

2) 村尾裕一, 修士論文, 東京大学・理学部情報科学科, 1981

3) 佐々木建昭, 「数式処理」, 情報処理叢書

4) T. Sasaki, "Extended Euclidean Algorithm and Determinants" (in preparation)

5) P.S. Wang, "The EEZ-GCD Algorithm", SIGSAM bul., no. 54 (1980) pp. 50-60,

6) P.S. Wang, "A p-adic Algorithm for Univariate Partial Fractions", Proc. SYMSAC '81

7) P.S. Wang, M.J.T. Guy, J.H. Davenport, "P-adic Reconstruction of Rational numbers", SIGSAM bul., no. 62 (1982) pp. 2-3

8) D.Y.Y. Yun, "The Hensel lemma in Algebraic Manipulation", Ph.D. Thesis, Dept. of Math., M.I.T., 1973