ICOT Technical Report: TR-155

TR-155

ある種の環上の多項式の因数分解について
(Lenstra の方法とその一般化)

横山和弘, 野呂正行, 竹島　卓
(富士通)

February, 1986

©1986, ICOT

ICOT
Mita Kokusai Bldg. 21F
4-28 Mita 1-Chome
Minato-ku Tokyo 108 Japan
(03) 456-3191～5
Telex ICOT J32964

Institute for New Generation Computer Technology

ある種の環上の多項式の因数分解について
(Lenstra の方法とその一般化)

富士通・国際研　横山　和弘
野呂　正行
竹島　卓

§1 はじめに

今日の多項式の因数分解の効率的なアルゴリズムの研究は、E.R. Berlekamp〔1〕が有限体上の一変数多項式の因数分解アルゴリズムを1967年に発表したことに始まる。これを受けて、H. Zassenhause〔15〕が Hensel の補題を利用した整数環上の一変数多項式の因数分解アルゴリズムを1969年に示した。このアルゴリズム (Berlekamp-Zassenhaus) の基本的な枠組みを、現在に至るまでの多くの研究者が踏襲しており、この意味で Berlekamp-Zassenhaus のアルゴリズムは因数分解アルゴリズムの主流をなしている。即ち、1969年以降の多くの因数分解アルゴリズムの研究は上の枠組みの各部分の改良・拡張に向けられていた。詳しくは、以下の通りである。

Berlekamp-Zassenhaus のアルゴリズムの基本枠組み

一変数多項式の因数分解　(整数環上)

(i) mod p での因数分解＝有限体上の因数分解 (Berlekamp)

(ii) Lifting up　(Hensel 構成)

(iii) Finding True Factors　(Lift up された因子の候補から真の因子を捜す。)

(iii) の部分については、旧来 Trial Division と呼ばれる、割れるかどうか実際に割ってみて調べる方法が採られてきた。しかし、この方法では最悪の場合に計算時間が元の多項式の次数に対して指数的 (exponential) になってしまう欠点があった。この問題に対する一つの解答として、A.K. Lenstra, H.W. Lenstra and L. Lovasz〔5〕が1982年に lattice を用いた方法を発表し、計算時間が元の多項式の次数に対して多項式 (polynomial) になることを可能にした。その後、A.K. Lenstra は lattice 論法を使う因数分解アルゴリズムを次々に発表した：

整数環上の多変数多項式の因数分解 (1983年)〔7〕、代数拡大体上の一変数多項式の因数分解 (1983年)〔8〕、代数拡大体上の多変数多項式の因数分解 (1984年)〔10〕、有限体上の多変数多項式の因数分解 (1985年)〔11〕。

注意) A.K. Lenstra はこの他に root approximation を使った一変数多項式の因数分解 (1984年)〔9〕、transcendental evaluation を使った多変数多項式の因

数分解（1985年）〔12〕（M. von der Hulst との共著）等を発表している。

さらに、この一般化として von zur Gathen〔14〕が Lenstra の方法をある種の付値環上の多項式の因数分解に拡張した。（1983年）

そこで今回、この Lenstra の方法の紹介および抽象化・一般化について論じてみることにする。まず§2 で二つの典型的なアルゴリズムを示し、その数学的裏付けを取り出す。次に§3 で拡張を試み、更に§4 で von zur Gathen による一般化を紹介する。

§2 Lenstra の方法

このセクションでは、Lenstra の方法を紹介し、その本質的な部分を抽出する。

2-1 整数環上の一変数多項式の因数分解（A.K. Lenstra et al.〔5〕）

F(X) を $\mathbb{Z}$ 上の monic かつ square free である一変数多項式とする。ここで n = degree F(X) とおく。

(i) mod p 上での因数分解。（ただし、p は素数であり F(X) は mod p 上で square free になるように取る。）

$H_0(X)$: F(X) の mod p 上での既約因子とする。（ℓ = degree $H_0(X)$）

(ii) Lifting up（Hensel 構成）：必要な bound C_0 を予め計算する。

H(X): F(X) の mod p^k 上での既約因子とする。（ただし、$p^k > C_0$）

(iii) Finding a True Factor : $m = \ell, \ell+1, .., n-1$ に対して以下を実行。

(a) Making a lattice Lm

$L_m = \{ G(X) \mid \text{degree } G(X) \leq m$ かつ $H(X) \mid G(X) \bmod p^k \}$ なる lattice を作る。この lattice の Base として、次の M がとれる。

$M = \{ p^k \cdot X^i \mid 0 \leq i < \ell \} \cup \{ H(X) \cdot X^j \mid 0 \leq j \leq m - \ell \}$

ここで、$G(X) = \Sigma G_i X^i$ に対して $\underline{G} = (G_m, G_{m-1}, .., G_0)$ を対応させこれらを同一視する。これにより多項式は lattice の元とみることができる。（lattice には、通常のノルムをいれる。）

(b) Finding a Short Vector in lattice Lm

この M に対して、Basis Reduction Algorithm for $\mathbb{Z}$-lattice を適用して Reduced Base を作る。この Reduced Base を $\underline{B_0}, .., \underline{B_m}$ とする。これらは、$B_0(X), .., B_m(X)$ に対応する。

(c) Checking the Candidate

上記の $\underline{B_0}$ に対して $|\underline{B_0}|$ が、$|F(X)|$ 及び C_0 により求まる C より小さければ、GCD(F(X), $B_0(X)$) は non trivial である。

特に、はじめて上記の条件を満たした m に対して $B_0(X)$ は F(X) の既約因子である。またそれがなければ F(X) は既約である。

注意) Basis Reduction Algorithm とは、base が与えられた時にその base より以下に定義する Reduced base を作るアルゴリズムである。

定義 1 (Reduced Base of $\mathbb{Z}$-lattice): $\underline{B_0},\ldots,\underline{B_m}$ が Reduced Base とは、その直交化した base $\underline{B_0}^*,\ldots,\underline{B_m}^*$ が次を満たすことを言う。(E. Kaltofen〔4〕)

(*) $|\underline{B_i}^*|^2 \geq \frac{1}{2}|\underline{B_{i-1}}^*|^2$ for $1 \leq i \leq m$

更にこの時、$\underline{B_0}$ について、次が成り立つ。

(**) $|\underline{B_0}|^2 \leq 2^n |\underline{G}|^2$ for any $\underline{G}$ in L_m

(この意味で $\underline{B_0}$ を short vector と言う。)

注意) ここの論法で求めたいものは、(**) を満たす $\underline{B_0}$ であり、すべての base は必要としない。

次に、もう一つの lattice 論法の典型的例を挙げる。

2-2 有限体上の二変数多項式の因数分解 (A.K. Lenstra〔11〕)

$F(X,Y)$ を有限体 $GF(q)$ 上の二変数多項式とする。更に、$F(X,Y)$ は primitive かつ square free とする。(ここで $q=p^e$, $e \geq 1$ また $n = \mathrm{degree}_X F(X,Y)$)

(i) 適当に選んだ $GF(q)$ 上の一変数多項式 $f(Y)$ に対して、 mod $f(Y)$ での因数分解。($u = \mathrm{degree}_Y f(Y)$) (多くの場合は、$u = 2$ に取れる。)

$H_0(X,Y)$: $F(X,Y)$ の mod $f(Y)$ での既約因子とする。($\ell = \mathrm{degree}_X H_0(X,Y)$)

ここで、 $GF(q)[X,Y]/<f(Y)> \cong (GF(q)[Y]/<f(Y)>)[X]$

$\cong GF(q^u)[X]$

よって、(i) は有限体 $GF(q^u)$ 上の因数分解となる。

(Berlekamp のアルゴリズム〔3〕を適用する。)

(ii) Lifting up (拡張された Hensel 構成) : 必要な bound C_0 を計算。

$H(X,Y)$: $F(X,Y)$ の mod $f(Y)^k$ での既約因子とする。

(iii) Finding a True Factor : $m = \ell, \ell+1,\ldots,n-1$ に対して以下を実行。

(a) Making a lattice L_m

$L_m = \{ G(X,Y) \mid \mathrm{degree}_X G(X,Y) \leq m$ かつ $H(X,Y) \mid G(X,Y) \bmod f(Y)^k \}$ なる lattice を作る。

この lattice の Base として、次の M がとれる。

$M = \{ f(Y)^k \cdot X^i \mid 0 \leq i < \ell \} \cup \{ H(X,Y) \cdot X^j \mid 0 \leq j \leq m-\ell \}$

ここで、$G(X,Y) = \Sigma G_i(Y)X^i$ に対して $\underline{G} = (G_m, G_{m-1},\ldots,G_0)$ を対応させ、これらを同一視する。これにより多項式は $GF(q)(Y)$ 上の lattice の元とみることができる。 lattice には、以下のノルムをいれる。

$GF(q)(Y)$ の元 $G(Y)$ に対して $d(G(Y)) = \mathrm{degree}_Y G(Y)$ と $G(Y)$ のノルムを定義する。$\underline{A} = (A_n(Y), A_{n-1}(Y),\ldots,A_1(Y)) \in (GF(q)(Y))^n$ に対しては、

$d(\underline{A}) = \max \{ d(A_i(Y)) \}$ と定義する。

(b) Finding a Short Vector in lattice L_m

この M に対して、Basis Reduction Algorithm for $GF(q)(X)$-lattice を適用して Reduced Base を作る。この Reduced Base を $\underline{B_0},\ldots,\underline{B_m}$ とする。

(c) Checking the Candidate

上記の $\underline{B_0}$ に対して $d(\underline{B_0})$ が、$\underline{d(F(X,Y))\text{ 及び }C_0\text{ により求まる }C}$ より小さければ、$GCD(F(X,Y),B_0(X,Y))$ は non trivial である。

特に、はじめて上記の条件を満たした m に対して $B_0(X,Y)$ は $F(X,Y)$ の既約因子である。またそれがなければ $F(X)$ は既約である。

定義 2 (Reduced Base of GF(q)(Y)-lattice) : $\underline{B_0},\ldots,\underline{B_m}$ が reduced base とは、 $B = \begin{bmatrix} \underline{B_0} \\ \underline{B_1} \\ \vdots \\ \underline{B_m} \end{bmatrix}$ に対して、列の置換により次の B' が得られる時を言う。

$$(***)\quad B' = \begin{bmatrix} \underline{B'_0} \\ \underline{B'_1} \\ \vdots \\ \underline{B'_m} \end{bmatrix} \text{ such that } \begin{array}{ll} \text{(a) } d(\underline{B'_i}) \leq d(\underline{B'_j}) & \text{for } 0 \leq i < j \leq m \\ \text{(b) } d(B'_{i,i}) \geq d(B'_{i,j}) & \text{for } 0 \leq i < j \leq m \\ \text{(c) } d(B'_{i,i}) > d(B'_{i,j}) & \text{for } 0 \leq j < i \leq m \end{array}$$

特にこの時 $\underline{B_0}$ は the shortest vector になることがわかる。

即ち、$\underline{B_0},\ldots,\underline{B_m}$ が reduced base $\Rightarrow$ $\underline{B_0}$ は the shortest vector

注意) 2-1 と同様に、ここの論法で欲しいのは、the shortest vector であり、reduced base 全体は必要とはしない。

2-3 lattice 論法の key lemma

上記のアルゴリズムの正当性を保証する定理を示す。

以下 K で、$\mathbb{Z}$ または GF(q) [Y] を、α で ideal $< p >$ または $< f(Y) >$ を表すものとする。

K [X] の元 F(X) をとる。F(X) は square free かつ primitive かつ monic と仮定する。($n = \text{degree}_X F(X)$)

更に、F(X) に対して次の仮定が成り立つとする。

(仮定 1): Hensel 構成

F(X) は (K/α^k) [X] において因子 H(X) を持ち、H(X) は次を満たす。($k \geq 1$)

(1) $\ell c(H(X)) = 1$ (ℓc は最高次の係数を表す。)

(2) $H(X) \mid F(X) \mod \alpha^k$

(3) $H(X) \equiv H_1(X) \mod \alpha$

(4) $H_1(X) \nmid F(X) \mod \alpha$

ここで、$H_1(X)$ は (K/α) [X] における F(X) の既約因子とする。

定理 1 (Existence and Uniqueness Theorem)

F(X) は $H(X) \mid G_0(X) \bmod \alpha^k$ なる K上の既約因子 $G_0(X)$ を持つ。またこのような $G_0(X)$ は unit 倍をのぞいて唯一である。

更に F(X) の因子 G(X) に対して、次の三条件は同値である。

(1) $H(X) \mid G(X) \bmod \alpha$

(2) $H(X) \mid G(X) \bmod \alpha^k$

(3) $G_0(X) \mid G(X)$

特に $H(X) \mid G_0(X) \bmod \alpha$ である。

定理 1 により、$L_n = \{ G(X) \mid \text{degree } G(X) \leqq n$ かつ $H(X) \mid G(X) \bmod \alpha^k \}$ の中に F(X) の既約因子が必ず存在することが言え、その因子の次数を m とすれば、L_m の中にあることも言える。よって、L_m の中から抜き出すことをすればよいことがわかる。

次に K におけるノルムを d とおく。即ち、K が $\mathbb{Z}$ の時には $d = |\ |$ であり、K が GF(q)[Y] の時には $d = \text{degree}_Y$ である。

更に K-module に対して、そのノルム d を次のように決める。

$\underline{M} = (M_n, M_{n-1}, \ldots, M_0)$ に対し $d(\underline{M}) = \Sigma d(M_i)$ for $K = \mathbb{Z}$

$d(\underline{M}) = \max \{ d(M_i) \}$ for $K = GF(q)(Y)$

(仮定 2): d の性質について

K のノルム d は次を満たす。

(イ) t 個の元の積に対して、ある関数 $C_{0,t}$ が存在して次を満たす。

$d(\prod M_i) \geqq C_{0,t}(d(M_1), \ldots, d(M_t))$

ここで $C_{0,t} : \mathbb{Z}^t \to \mathbb{Z}^+$ 単調増加で、変数について対称である。

(ロ) 行列 M に対して、その各行を $\underline{M_1}, \ldots, \underline{M_m}$ とした時に、ある関数 $C_{1,m}$ が存在して次を満たす。

$d(\det M) \leqq C_{1,m}(d(\underline{M_1}), \ldots, d(\underline{M_m}))$

ここで $C_{1,m} : \mathbb{Z}^m \to \mathbb{Z}^+$ 単調増加で、変数について対称である。

(仮定 3): Basis Reduction Algorithm for K について

K-module L の base M が与えられた時に、Basis Reduction Algorithm が存在して、'short vector' $\underline{B}$ を計算する。ここで、m は Lのランクとする。

$\underline{B}$ が 'short vector' であるとは、次を満たすものを言う。

(ハ) 任意の L の元 $\underline{B'}$ に対して、ある関数 C_2 が存在して、

$d(\underline{B}) \leqq C_2(m) \cdot d(\underline{B'})$ となる。

ここで $C_2 : \mathbb{Z} \to \mathbb{Z}^+$ 単調増加の関数

注意) K = $\mathbb{Z}$ について、上の (イ),(ロ),(ハ) は次のようにとれる。

(イ) $C_{0,t}(|M_1|, \ldots, |M_t|) = \prod |M_i|$

(ロ) $C_{1,m}(|\underline{M_1}|,\ldots,|\underline{M_m}|) = \Pi\,|\underline{M_i}|$

(ハ) $C_2(m) = 2^{m-1/2}$

$K = GF(q)[Y]$ について、上の (イ),(ロ),(ハ) は次のようとれる。

(イ) $C_{0,t}(d(M_1),..,d(M_t)) = \Sigma\, d(M_i)$

(ロ) $C_{1,m}(d(\underline{M_1}),\ldots,d(\underline{M_m})) = \Sigma\, d(\underline{M_i})$

(ハ) $C_2(m) = 1$

(上記の (ロ) については、Hadamard の定理による。)

上記の $\mathbb{Z}$ の場合の d を乗法的と呼び、GF(q) [Y] の場合の d を加法的と呼ぶことにする。

定義 3 (Notation) : 以下のように C_0, C_1 を定義する。

$$C_0(t,D) \equiv C_{0,t}(D,..,D)$$

$$C_1(i,D_1,m-i,D_2) \equiv C_{i,m}(\underbrace{D_1,..,D_1}_{i},\underbrace{D_2,..,D_2}_{m-i})$$

定理 2 仮定 1・2・3 が成り立つとする。

$L_m = \{ G(X) \mid \text{degree } G(X) \leq m \text{ かつ } H(X) \mid G(X) \bmod \alpha^k \}$

に対して、L_m の元 B が次の条件を満たすとする。

(D1) $C_1(m,d(F),n,d(B)) < C_0(\ell,d(\alpha^k))$

この時、$G_0(X) \mid B(X)$ である。特に、GCD(F(X),B(X)) は non-trivial。

上の条件 (D) は真の因子であるための必要条件であるので、逆の十分条件を示す必要がある。

(仮定 4): Bounds of Coefficients

F(X) の任意の因子 $G_0(X)$ に対して、ある関数 C_3 が存在して次がなりたつ。

(ニ) $d(G_0(X)) \leq C_3(n,d(F(X)))$

ここで、$C_3 : \mathbb{Z}^2 \to \mathbb{Z}^+$ なる関数

この (ニ) を直接 (D1) の d(B) に代入することで、次の定理を得る。

定理 3 仮定 1・2・3・4 のもとで仮定 1 の α^k の k を次を満たすようにとる。

(D2) $C_1(n,d(F),n,C_2(n+1)\cdot C_3(n,d(F))) < C_0(\ell,d(\alpha^k))$

この時 $m = \ell,..,n-1$ に対して L_m を作り、更に Basis Reduction Algorithm により 'short vector' B(X) を作る。この B(X) がはじめて定理 2 の条件 (D1) を満たす m に対して、B(X) は F(X) の既約因子になる。

注意) 上の (ニ) は次のようにとることができる。

$C_3(n,d(F(X))) = ({}_{2n}C_n)^{1/2}\,|F(X)|$ for $K = \mathbb{Z}$

$C_3(n,d(F(X))) = d(F(X))$ for GF(q) [Y]

上記の定理により、Lenstra のアルゴリズムは二番目のステップ（ 即ち Hensel 構成 ）において、(D2) を満たすような k を計算し、α^k まで持ち上げ、三番目のステップで得られる 'short vector' について、(D1) の条件を調べればよいことがわかる。

2-4 Basis Reduction Algorithm について

Basis Reduction Aigorithm について補足する。

(A) K = $\mathbb{Z}$ の場合

定義 1 において、Reduced Base を (*) を満たすものとしたが、実際のアルゴリズムでの Reduced Base の構成では以下の様に行う。

$B_0,\ldots,B_m$ を lattice の base とする。そして、その直交化した base を $B^*_0,..,B^*_m$ とする。即ち次のようになる。(,) は内積を表す。

$$B^*_i = B_i - \Sigma \mu_{i,j} B^*_j \qquad \mu_{i,j} = (B_i, B^*_j)/(B^*_j , B^*_j)$$

この時に、$B_0,\ldots,B_m$ が Reduced Base になるために、次の条件を課す。

(*') (a) $|\mu_{i,j}| \leqq 1/2$ for $0 \leqq j < i \leqq m$

(b) $|B^*_i + \mu_{i,i-1}B^*_{i-1}|^2 \geqq 3/4 \cdot |B^*_{i-1}|^2$ for $0 < i \leqq m$

この条件を満たすように、base を変えていく。

注意) もともと、A.K. Lenstra et al〔5〕の論文では上の条件 (*') が Reduced Base の定義であった。しかし、E. Kaltofen〔4〕による改良された Basis Reduction Algorithm では Reduced Base の定義として (*) を使っており、ここでは E. Kaltofen のアルゴリズムを採ることにする。

(B) K = GF(q) [Y] の場合

基本的には Euclid の互除法を用いて Reduced Base を作る。この加法的なタイプに対して、 J. von zur Gathen〔14〕が改良・一般化したアルゴリズムを発表している。von zur Gathen のアルゴリズムについては、後で紹介する。

ここでは、von zur Gathen によるアルゴリズムの Reduced Base を紹介する。

(当然、この定義でも B_0 は the shortest vector になる。)

定義 2' (von zur Gathen による Reduced Base)

定義 2 の B' の条件 (***) (b)、(c) を次のように変える。

(b)' $d(B'_{i,i}) > d(B'_{i,j})$ for $i \neq j$

§3 Euclid 環およびある種の付値環上の多項式の因数分解

このセクションでは Lenstra 流の lattice 論法の拡張を考える。

3-1 Euclid 環の上の多項式の因数分解 (direct な適用)

K を Euclid 環とし、そのノルムを d とする。即ち、K、d は次を満たす。

定義 4 (Euclid 環): K が Euclid 環であるとは、ある d が存在して次を満たす。

$d : K \to \mathbb{Z}^+ \cup \{0\}$ なる写像で Kの任意の二元 a、b に対し次を満たす。

(a) $d(a \cdot b) \geq d(a)$

(b) $a = b \cdot q + r \qquad d(b) > d(r)$

なる '割算' が存在。

注意) K が Euclid 環ならば、K は単項イデアル環となり、特に素元分解環 (U.F.D) となる。

以下 Euclid 環の上での一変数多項式の因数分解を示す。

K の任意の ideal α に対して、K のある元 a が存在して $\alpha = \langle a \rangle$ と表すことができることに注意しておく。

(仮定 0): mod α での因数分解と Euclid 算法

K に対して次が成り立つ。

(ホ) 定義 4 (b) の割算が計算可能。

(ヘ) K の prime ideal α に対して、K/α 上の因数分解アルゴリズムが知られている。

以下仮定 0 が成り立つとする。この時、次の Hensel の補題が成り立つ。

定理 4 (Hensel の補題)

K 上の一変数多項式 F(X), H(X) 及び G(X) が次の条件を満たすとする。

(a) $F(X) \equiv G(X) \cdot H(X) \mod \alpha$ (α は K の prime ideal)

(b) H(X) は monic である。

(c) H(X) と G(X) は mod α 上互いに素である。

この時、任意の正整数 k に対して、以下を満たす $H_k(X)$, $G_k(X)$ を構成することができる。

(1) $F(X) \equiv G_k(X) \cdot H_k(X) \mod \alpha^k$

(2) $H_k(X) \equiv H(X)$, $G_k(X) \equiv G(X) \mod \alpha$

(3) degree $H_k(X)$ = degree H(X)

F(X)を K上の monic な一変数多項式とし、F(X) を因数分解することを考える。

(A) F(X) の K/α 上での既約因子の中で F(X) が重複して持たないものがある時。

その内のひとつを取り出して $H_0(X)$ とおく。

($H_0(X) \mid F(X)$ in K/α [X] かつ $H_0(X)^2 \nmid F(X)$ in K/α [X])

この時には Hensel 構成より仮定 1 を満たす H(X) を作ることができる。

そこで、仮定 2・3・4 のもとで次の因数分解アルゴリズムが考えられる。

アルゴリズム 1 (仮定 0・2・3・4・(A))

(i) mod α での因数分解

(ii) Hensel 構成

ここで定理 3 の条件 (D2) を満たすように k をとる。

(iii) Finding a True Factor

Basis Reduction Algorithm for K-lattice を用いる。

'short vector' に対する判定条件は、定理 2 の (D1)

(B) 重複因子を持つ場合

F(X) に対して次の discriminant をみる。

R = Resultant (F(X),F'(X)) (ここで F'(X) は F(X) の導関数)

(1) R が α に属さない時

この時 F(X) は mod α で square-free 即ち重複因子を持たない。

(2) $R \neq 0$ かつ R は α に属する時

$\alpha' = < p' >$: prime ideal such that $p' \nmid R$ なる α' に取替れば、F(X) は mod α' で square-free となる。

(3) R = 0 の時

F'(X) ≠ 0 の時には、GCD(F(X),F'(X)) が non-trivial であり、GCD(F(X),F'(X)) の因数分解に帰着させる。

F'(X) = 0 の時、char K = s ≠ 0 である。(s は素数である)

そして $F(X) = G(X^s)$ なる G(X) がとれる。よって G(X) の因数分解に帰着させる。

更に G(X) が既約の場合には、$G(X^s)$ は既約であるか、もしくは、ある多項式 $G_0(X)$ の s 乗となる。 即ち $G(X^s) = (G_0(X))^s$

この場合 $G(X) = \Sigma G_i X^i$、$G_0(X) = \Sigma G_{0,i} X^i$ とおくと $G_i = (G_{0,i})^s$ である。よって K の元に対しその s 乗根を求めるアルゴリズムがあれば、この場合にも既約因子を求めることができる。

上記の操作をまとめて、square-free 化の操作と呼ぶことにする。

以上をまとめて、次の形のアルゴリズムをえる。

アルゴリズム 2 (仮定 0・2・3・4)

(i) square-free 化の操作

(ii) mod α での因数分解

(iii) Hensel 構成

ここで定理 3 の条件 (D2) を満たすように k をとる。

(iv) Finding a True Factor

Basis Reduction Algorithm for K-lattice を用いる。

'short vector' に対する判定条件は、定理 2 の (D1)

(v) square-free 化の操作の逆操作

(char K ≠ 0 の時は、 s 乗根を求めるアルゴリズムがあれば、既約因子をさせる。)

3 2 d への制限

上記の d について以下の場合を考える。

定義 5 : (valuation ; Euclidean valuation)

d が Euclidean valuation であるとは、定義 4 の (a)、(b) を満たし、更に一般の意味で valuation になる時に言う。即ち、次が成り立つ。

(1) $d(a) \geq 0$ for a in K ; $d(a) = 0$ ならば $a = 0$

(2) $d(a \cdot b) = d(a) \cdot d(b)$ for a, b in K

(3) $d(a + b) \leq d(a) + d(b)$ for a, b in K

注意) K が $\mathbb{Z}$ の時の $|\ |$ は上の条件を満たす。また、K が GF(q) [Y] の時の d に対しては、$w = 2^d$ とおくことで上の条件を満たす。

定義 6 : (non-Archimedean valuation and Archimedean valuation)

上の条件 (3) を次の条件に置き換えた時に d を non-Archimedean と言い、それが成立しない時を Archimedean と言う。

(3)' $d(a + b) \leq \max \{ d(a), d(b) \}$ for a, b in K

(A) d が non-Archimedean Euclidean valuation の時

仮定 3・4 の条件について、以下のようにとれる。

(イ) $C_{0,t}(d(M_1),\ldots,d(M_t)) = \prod d(M_i)$

(ロ) $C_{1,m}(d(\underline{M_1}),\ldots,d(\underline{M_m})) = \prod d(\underline{M_i})$

(ハ) $C_2(m) = 1$

(ニ) $C_3(n, d(F(X))) = d(F(X))$

また、Basis Reduction Algorithm に対しては、GF(q) [Y] の時と同様なアルゴリズムが存在する。(または、von zur Gathen のアルゴリズム)

(B) d が Archimedean Euclidean valuation の時

この場合は、K の商体が複素数体の部分体と同形となるので、Mignotte の評価 (M. Mignotte [13]) が使え、仮定 3・4 の条件について、以下のようにとれる。

(イ) $C_{0,t}(d(M_1),\ldots,d(M_t)) = \prod d(M_i)$

(ロ) $C_{1,m}(d(\underline{M_1}),\ldots,d(\underline{M_m})) = \prod d(\underline{M_i})$

(ハ) $C_2(m) = 2^{m-1/2}$

(ニ) $C_3(n, d(F(X))) = ({}_{2n}C_n)^{1/2}\, d(F(X))$

また、Basis Reduction Algorithm に対しては、$\mathbb{Z}$ の時と同様なアルゴリズムでよい。

以上により次の定理を得る。

定理 5 (Euclidean valuation を持つ環上の多項式の因数分解)

K を Euclid 環とし、d を Euclidean valuation とする。この時仮定 0 が成り立つならば、アルゴリズム 1 及び 2 が存在する。

§4 von zur Gathen による拡張　(J. von zur Gathen〔14〕)

このセクションでは von zur Gathen による Lenstra の方法の拡張を紹介する。von zur Gathen は以下に定義する a ring with sufficient valuations に対して Lenstra の方法を拡張した。

定義 7 : (Hensel ring)

K を valiation v を持った環とする。この時 K が Hensel ring であるとは、以下の条件を満たす時に言う。

(a) 任意の K の元 a に対して $v(a) \leq 1$

(b) 任意の K の元 a, b と任意の正の数 ε に対して、ある K の元 c が存在して次を満たす。

$$v(a) \leq v(b) \Rightarrow v(a - b \cdot c) \leq \varepsilon$$

更にこの v を Hensel valuation と言う。

(Hensel ring は Henselian ring とは異なることに注意!)

ここで更に上の (b) について a, b が与えられた時に c を計算できることを仮定しておく。

次に Euclidean valuation を新しく定義しなおす。

定義 8 : (Euclidean valuation)

K の non-trivial valuation w が Euclidean valuation であるとは、ある β ($0 < \beta < 1$) が存在して次を満たす。

(a) 任意の K の元 a に対して $a \neq 0 \Rightarrow w(a) \geq 1$

(b) 任意の K の元 a, b に対して、ある K の元 c が存在して次を満たす。

$$b \neq 0 \Rightarrow w(a - c \cdot b) \leq \beta w(b)$$

更にこの時 K を Euclidean valuation Ring と言う。

定義 9 : (inverse bound)

V = a set of valuations of K とし、w をそれ以外のある valuation とする。また、B_u、B を実数 ($u \in V$) とする。この時 ((B_u), B) が inverse bound であるとは、以下の条件を満たす時に言う。

K の元 a に対して　$w(a) < B$ かつ任意の $u \in V$ に対し $u(a) \leq B_u$

$$\Rightarrow \quad a = 0$$

定義 10 : (a ring with sufficient valuations)

K を Hensel かつ Euclidean valuation ring とする。V = a set of non-trivial Hensel valuations of K とし、w を Euclidean valuation とする。

この時 K が a ring with sufficient valuations とは以下の条件を満たす時に言う。

(い) Modular factorization : $v \in V$ に対し v により決まる maximal ideal

$m_v = \{ a \in K \mid v(a) < 1 \}$ を考える。この時、$(K/m_v)[X]$ 上の因数分解アルゴリズムが存在する。また、ある p_v が存在して $m_v = p_v K$ となる。

(ろ) Inverse bounds : 任意の K の元 b に対して、$v(b) = 1$ なる V の元 v を見つけることができる。この時、$\tau = v(p_v)$ とおく。
更に、任意の正の実数 B に対して以下を満たす整数 N を計算できる。

$$B_u = \begin{cases} \tau^N & \text{if } u = v \\ 1 & \text{if } u \in V - \{ v \} \end{cases}$$

とおけば、$((B_u), B)$ が inverse bound となる。

(は) Gauss lemma : Q を K の商体とする。任意の Q [X] の元 F(X) に対して、次を満たす K の元 a を計算できる。
F(X) を Q 上で割る任意の monic な多項式 G(X) に対して、$a \cdot G(x) \in K[X]$

さて、以下 K を a ring with sufficient valuations と仮定する。この時に K [X] の元に対し次を定義しておく。

定義 11 : (L_q-norm)
v を valuation とする。この時、次の v_q、v_∞ が定義される。

$v_q : K^m \to R$
$\underline{A} \in K^m \to (\Sigma v(A_i)^q)^{1/q}$ ここで、$\underline{A} = (A_1, A_2, .., A_m)$
$v_\infty : K^m \to R$
$\underline{A} \in K^m \to \max \{ v(A_i) \}$ ここで、$\underline{A} = (A_1, A_2, .., A_m)$

以下で von zur Gathen による a ring with sufficient valuations 上の多項式の因数分解アルゴリズムを示す。

Algorithm Factor (von zur Gathen)
Input : K 上の多項式 F(X) ; (V, w) は sufficient valuations
Output : F(X) が可約の時に (E(X), a) を出力。ここで、E(X) は $a^2 \cdot F(X)$ の proper な因子。
(1) F(X) に対して定義 10 (は) の a を計算する。
n = degree F(X) とした時、

$$C = \begin{cases} w(2^n) \cdot w_2(F(X)) & \text{if } w \text{ is Archimedean,} \\ w_\infty(F(X)) & \text{otherwise,} \end{cases}$$

$$\tau(n) = \begin{cases} 2^{n-1/2} & \text{if } w \text{ is Archimedean,} \\ 1 & \text{otherwise,} \end{cases}$$

$B = (C^2 \cdot w(a) \cdot \tau(2n))^n + 1$ とおく。
(2) $b = a \cdot$ discriminant of F(X) とおく。この時以下の v, τ, N, B_u for $u \in V$ を求める。(注意) b = 0 については、§3 3-1 (B) を参照)
v は定義 10 (い) を満たす。また定義 10 (ろ) を満たすようにする。
($v(b) - 1$、$\tau = v(p)$、$B_v = \tau^N$ ここで $m_v = pK$)
(3) F(X) を mod m_v で因数分解する。即ち、$F(X) = f_0(X) \cdot f_1(X)$

ここで、$f_1(X)$ は monic かつ既約であるとする。(k = degree $f_1(X)$)

(4) Lifting up (Hensel ring の上の Hensel 構成 (定理 6))

$F(X) \equiv F_0(X) \cdot F_1(X) \bmod m_v^N$

$F_i(X) \equiv f_i(X) \bmod m_v$ ($i = 0$ or 1) かつ $F_1(X)$ は monic

(5) Finding a True Factor : $m = k, \ldots, n-1$ に対して以下を行う。

(a) Making a module Lm

$M = \{ p^N \cdot X^i \mid 0 \leq i < k \} \cup \{ F_1(X) \cdot X^i \mid 0 \leq i < m + n - k \}$

を base とする module Lm を作る。

(b) Finding a Short Vector in module Lm

M に Basis Reduction Algorithm for Hensel ring module を適用して、short vector G(X) を求める。

(c) Checking the Candidates

$E_1(X) = GCD(F(X), G(X))$ を計算する。(Q上)

If $E_1(X) \neq 1$ かつ degree $E_1(X) < n$ ならば、$E(X) = a \cdot E_1(X)$ とおいて、($E(X)$, a) を出力する。Stop

(6) 'F(X) is irreducible' を出力する。

定理 6 (Hensel ring の上の Hensel 構成)

K を Hensel ring とする。v をその valuation とする。$F(X)$、$F_0(X)$、$F_1(X)$、$S_0(X)$、$S_1(X)$ を K 上の多項式とし、z を K のある元、α、δ、τ を実数とする。この時以下を仮定する。(z としては 1 を取ることが期待される。)

(H1) $v(F(X) - F_0(X) \cdot F_1(X)) \geqq \tau < 1$

(H2) $v(S_1(X) \cdot F_0(X) + S_0(X) \cdot F_1(X) - z) \geqq \delta < 1$

(H3) $F_1(X)$ は monic、degree $F_0(X) \cdot F_1(X) \leqq$ degree $F(X)$、
degree $S_i(X) \leqq$ degree $F_i(X)$ ($i = 0$ or 1)
$\alpha \cdot \delta \leqq 1$、$\alpha^2 \cdot \tau \leqq 1$、かつ $1 \leqq \alpha \cdot v(z)$

この時 K 内の計算で、次を満たす $F_0^*(X)$、$F_1^*(X)$ が作れる。

(H*) $\alpha^* = \alpha$、$\tau^* = \alpha \cdot \tau \cdot \max \{ \delta, \alpha \cdot \tau \}$、$\delta^* < 1/\alpha^*$
とおく。また、$F^*(X) = F(X)$、$S_i^*(X) = S_i(X)$ とおく。
この時、(H1)、(H2)、(H3) がすべて * 付に変えて成立する。

(H*4) $v(F^*_i(X) - F_i(X)) \leqq \alpha \cdot \tau$
$v(S^*_i(X) - S_i(X)) \leqq \alpha \cdot \max \{ \delta, \alpha \cdot \tau \}$

次に Basis Reduction Algorithm for Hensel ring module について説明する。w を K の Euclidean valuation とする。この時 K 上の module L と、その base M に対して、w が non-Archimedean ならば定義 2' により Reduced Base を定義する。(特に w_q に対し $q = \infty$) また w が Archimedean ならば定義 1 により Reduced Base を定義する。(特に w_q に対し $q = 2$) この時 Reduced Base を M より生成するアルゴリズムは存在する。

(J. von zur Gathen [14] §4 及び E. Kaltofen [4] を参照)

Reduced Base の最初の元を $\underline{B_0}$ とおくと、$\underline{B_0}$ は次を満たす。

任意の L の元 $\underline{A}$ に対して、

$$w_q(\underline{B_0}) \leqq \tau(m) \cdot w_q(\underline{A}) \quad (\text{L のランクを m とする})$$

この意味で、$\underline{B_0}$ を short vector と言う。

最後に上のアルゴリズムの数学的根拠を示す。

定理 7 (定理 2 に対応)

F(X)、G(X)、H(X) を K上の多項式とし、各々の degree を n、m、k とおく。更に、ある S(X)、T(X) が存在して、次を満たすとする。

$v(F(X) - H(X) \cdot S(X)) \leqq \tau$ かつ $v(G(X) - H(X) \cdot T(X)) \leqq \tau$

$((B_u), B)$ を inverse image とし、次を仮定する。

$B_u = 1$ for $u \neq v$、$\tau \leqq B_v < 1$ かつ $w_q(F(X))^n \cdot w_q(G(X))^n < B$

この時 F(X) と G(X) は K 上 non-trivial な共通因子を持つ。

さて上のアルゴリズムの正当性を考えてみる。

§3 3-2 (A) および (B) と同様にして、$a^2 \cdot F(X)$ の任意の因子 $G_i(X)$ に対して次が成り立つ。(Bound of Coefficients)

$w_q(G_i(X)) \leqq w(a) \cdot C$ ここで $q = 2$ または ∞

そこで、$G_1(X)$ として、アルゴリズムのステップ 3・4 の $f_1(X)$ に対して、$f_1(X) \mid G_1(X) \bmod m_v$ となるように取る。ここで $m = \text{degree } G_1(X)$ とおく。

この時、アルゴリズムのステップ 5 (B) で得た short vector G(X) in Lm に対して、次が成り立つ。

$$w_q(G(X)) \leqq \tau(n + m) \cdot w_q(G_1(X)) \leqq w(a) \cdot C$$

そこで次を得る。

$$w_q(F(X))^m \cdot w_q(G(X))^n < w_q(F(X))^n \cdot (w(a) \cdot \tau(2n) \cdot C)^n < B$$

よって定理 7 により次がいえる。

定理 8 (定理 3 に対応)

F(X) が可約である時、Algorithm Factor は $a^2 \cdot F(X)$の proper な因子 E(X) を計算する。

本研究は第五世代コンピュータの研究の一環として、ＩＣＯＴの委託により行ったものである。

Reference

〔1〕 E.R. Berlekamp,"Factoring Polynomials over Finite Fields," Bell System Tech. J. 46 (1967),1853-1859.

〔2〕 E.R. Berlekamp, Algebraic Coding Theory, Chap. 6, McGraw-Hill, New York, 1968.

〔3〕 E.R. Berlekamp,"Factoring Polynomials over Large Finite Fields," Math. Comp. 24 (1970), 713-735.

〔4〕 E. Kaltofen,"On the Complexity of Finding Short Vectors in Integer Lattices," Lecture Note in Computer Science 162 (1983),236-244.

〔5〕 A.K. Lenstra, H.W. Lenstra and L. Lovasz,"Factoring Polynomials with Rational Coefficients," Math. Ann. 261 (1982), 515-534.

〔6〕 A.K. Lenstra,"Lattice and Factorization of Polynomials over Algebraic Number Fields," Lecture Note in Computer Science 144 (1982),32-39.

〔7〕 A.K. Lenstra,"Factoring Multivariate Integral Polynomials," Lecture Note in Computer Science 154 (1983), 458-465.

〔8〕 A.K. Lenstra,"Factoring Polynomials over Algebraic Number Fields," Lecture Note in Computer Science 162 (1983),245-254.

〔9〕 A.K. Lenstra,"Polynomial Factorization by Root Approximation," Lecture Note in Computer Science 174 (1984),272-244.

〔10〕 A.K. Lenstra,"Factoring Multivariate Polynomials over Algebraic Number Fields," Lecture Note in Computer Science 176 (1984),389-396.

〔11〕 A.K. Lenstra,"Factoring Multivariate Polynomials over Finite Fields," J. Computer and System Science 30 (1985),235-248.

〔12〕 A.K. Lenstra and M. van der Hulst,"Factorization of Polynomials by Transcendental Evaluation," Lecture Note in Computer Science 204 (1985), 138-145.

〔13〕 M. Mignotte,"An Inequalties About Univariate Polynomials," Math. Comp. 28 (1974), 1153-1157.

〔14〕 J. von zur Gathen,"Hensel and Newton Methods in Valuation Rings," Math. Comp. 42 (1984), 637-661.

〔15〕 H. Zassenhaus,"On Hensel Factorization. I," J. Number Theory 1 (1969), 291-311.

日本語で紹介したものとして、次を挙げておく。

〔16〕 古川昭夫 :ＬＡＴＴＩＣＥを用いた因数分解法　―因数分解の歴史と到達点―　統計数理研究所創立40周年シンポジウム「数式処理と統計解析の接点」, 49-55.