ICOT Technical Report: TR-365

TR-365

Euclid環上の因数分解及びGCDについて
格子算法の応用

横山和弘、竹島　卓

April, 1988

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

Euclid 環上の因数分解およびＧＣＤについて

格子算法の応用

On factorization and GCD over Euclidean rings :

An Application of algorithm of lattices

横山和弘

富士通㈱国際情報社会科学研究所

竹島卓

富士通㈱国際情報社会科学研究所

ソフトウェア科学会正会員 No. 119-757-1198

Kazuhiro Yokoyama

International Institute for Advanced Study of Social Information Science,

FUJITSU LIMITED.

Taku Takeshima

International Institute for Advanced Study of Social Information Science

FUJITSU LIMITED.

概要

A.K.Lenstra, H.W.Lenstra と L.Lovasz が格子算法を整数環上の一変数多項式の因数分解アルゴリズムに応用し、計算時間が元の多項式の次数に対してその次数の多項式オーダーになることを可能にして以来、格子算法が種々の因数分解アルゴリズムに応用されている。そこで、本論文では、A.K.Lenstra による格子算法の基本的性質を抽出し、Euclid 環上の因数分解およびＧＣＤに格子算法が適用できることを示した。具体的には、Euclid 付値環上の因数分解およびＧＣＤへの応用と、ある種の条件の下での Euclid 環上の因数分解への応用である。

キーワード

因数分解アルゴリズム

ＧＣＤアルゴリズム

格子算法

1 はじめに

数式処理システムを構築する上で、多項式の因数分解は必要不可欠な機能の一つである。効率的な因数分解アルゴリズムの研究は、1967年に 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発表したことに始まる。これを受けて、1969年に H.Zassenhaus〔18〕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示した。この Berlekamp-Zassenhaus のアルゴリズムが、現在の因数分解アルゴリズム研究の基となっている。

この改良として、1982年に A.K.Lenstra と H.W.Lenstra, L.Lovasz〔6〕が格子算法を整数環上の一変数多項式の因数分解アルゴリズムに応用し、計算時間が元の多項式の次数に対してその次数の多項式オーダーになることを可能にした。それ以後、格子算法が種々の因数分解アルゴリズムに応用されている。例として、A.K.Lenstra により、整数環上の多変数多項式の因数分解（1983年）〔8〕、代数拡大体上の一変数多項式の因数分解（1983年）〔9〕、代数拡大体上の多変数多項式の因数分解（1984年）〔11〕、有限体上の多変数多項式の因数分解（1985年）〔12〕等が発表された。更に、この一般化として 1983年に J.von zur Gathen〔17〕が A.K.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。因数分解以外にも、J.von zur Gathen〔16〕は整数のＧＣＤ計算に格子算法が適用できることを示唆した。

そこで、本論文では、A.K.Lenstra による格子算法の基本的性質を抽出し、Euclid 環上の因数分解およびＧＣＤに A.K.Lenstra 流の格子算法が適用できることを示した。具体的には、2節において格子の概念を拡張し、R-module を新たにR-格子と名付け一般的な性質を示した。3節においては、J.von zur Gathen〔16〕の結果を一般化し、Euclid 付値環におけるＧＣＤ計算に格子算法を応用した。4節においては、二つの応用について述べた。第一に、Euclid 付値環においては、ほぼそのままの形で A.K.Lenstra の示したアルゴリズムが適用できること。第二に、Euclid 環において、ある種のノルムの評価関数の存在を仮定することにより、同様の算法が適用できることを示した。即ち、A.K.Lenstra の定理がそのままの形で一般化できるように、必要なノルムの性質・条件を提示し、それを基に A.K.Lenstra の定理を一般化した。5節において、まとめとして本研究の具体的例に言及し、格子算法の展望について述べた。

2 Euclid 環および格子の基本性質

本節では、必要な定義および格子に関する基本的性質を述べる。

記号として、Z、Q、RおよびCで各々整数環、有理数体、実数体および複素数体を表すことにする。また、GF(q) によりq個の元よりなる有限体を表すことにする。

定義 2.1 可換環Rが Euclid 環であるとは、次を満たす写像 d が存在することを言う。この d をRのノルムと言う。

d:R-{0} → Z⁺∪{0} なる写像でR-{0} の任意の二元 a, b に対し次を満たす。

$$d(a\cdot b) \geq d(a) \qquad \text{.....(2.1)}$$

$$a = b\cdot q + r \quad \text{ここで } d(b) > d(r) \text{ かまたは } r = 0 \text{ となる割算が存在。} \qquad \text{.....(2.2)}$$

上記定義によりRが Euclid 環であるならば、Rは単項イデアル環となり、特に素元分解環になる。即ち、Rの元に対して既約因子が定義でき、元の既約分解は可逆元を除いて一意的に定まる。

定義 2.2 可換環Rが Euclid 付値環であるとは、Rが Euclid 環であり、定義 2.1 の条件 (2.1)および (2.2)を満たすノルム d が一般の意味で付値に拡張できる(とう)ことを言う。本論文では、この付値を新たにノルムと呼ぶ。

即ち、d(0) = 0 と定義した上で、Rの任意の元 a 及び b に対して次が成り立つ場合である。

$$d(a) = 0 \text{ ならば } a = 0 \text{ となる。} \qquad \text{.....(2.3)}$$

$$d(a\cdot b) = d(a)\cdot d(b) \qquad \text{.....(2.4)}$$

$$d(a+b) \leq d(a) + d(b) \qquad \text{.....(2.5)}$$

この時、d を Euclid 付値 (Euclidean valuation)と言う。

上の定義により、Rが Euclid 付値環であるならば、(2.2) と (2.4)を合わせて、次を得る。

Rの元 a に対し、d(a) = 1 ならば、a は可逆元である。即ち、Rのある元 b が存在して a·b = 1 となる。逆に、(2.4) により a が可逆元であるならば、d(a) = 1 である。

注意) 一般の Euclid 環に対しても、新たにノルム d' を、

d' = d - d(1) + 1 に取り(移)換えることにより、a が可逆元であるならば、

d(a) =1とすることができる。

定義 2.3 ノルム d が Euclid 付値であり、更に次の条件 (2.6) を満たす時に、d を non-Archimedean と言い、(2.6) を満たさない時を Archimedean と言う。 $d(a+b) \leq \max\{d(a), d(b)\}$ .....(2.6)

Rが Euclid 付値環である時、Rの商体Qに対して、次の様にノルムが定義できる。

定義 2.4 Qの元 c に対して、c = a/b なる a, b をRから取った時に、

$d(c) = d(a)/d(b)$と定義する。 .....(2.7)

定義 2.4 において、c = a/b なる a, b の取り方に依らないことは、以下により言える。

c = a/b = a'/b' ならば a・b' = a'・b となり、

d(a)・d(b') = d(a')・d(b)。即ち、d(a)／d(b) = d(a')／d(b')。

d が Archimedean である時は、次の定理が言えることに注意しておく。

定理 2.1 Rが Euclid 付値環であり、d をRの Euclid 付値とする。更に、d が Archimedean である時RよりCの中への同形σと、ある実数βが存在して、任意のRの元 a に対して $d(a) = |\sigma(a)|^{\beta}$ となる。 .....(2.8)

証明は、藤崎〔4〕定理 6.14 を参照。

以下、Euclid 環Rの上の格子(lattice) について考える。まず最初に普通の意味での格子を定義する。

定義 2.5 n次元 Euclid 空間R^n の部分集合Lが格子であるとは、Lが次の条件を満たすことを言う。また、Lの各元を格子点と言う。

n個のR-線形独立な元 $X_1, X_2, \ldots, X_n$ がLに属し、更にLの任意元は $X_1, X_2, \ldots, X_n$ のZ-結合で表すことができる。この時、$X_1, X_2, \ldots, X_n$ をLの基底と言う。

また、nをLの次元 (またはランク)と言う。

即ち、格子とはZ-module のことである。

定義 2.5 を一般化して、次のR-module をR上の格子として定義する。以下、Rの商体をQとする。

定義 2.6 Q上のn次元線形空間の部分集合LがR-格子であるとは、Lが次の条件を満たすことを言う。また、Lの各元をR-格子点と言う。

n個のQ-線形独立な元 $X_1, X_2, \ldots, X_n$ がLに属し、更にLの任意元は $X_1, X_2, \ldots, X_n$ のR-結合で表すことができる。この時、$X_1, X_2, \ldots, X_n$ をLの基底と言う。

同様に、nをLの次元（またはランク）と言う。

定義 2.6 によれば、定義 2.5 の意味での格子はZ-格子となる。

R-格子Lとその基底Xに対して、次が成り立つ。

補題 2.1 R-格子LのR-基底 $X_1, X_2, \ldots, X_n$ に対して、$X_1, X_2, \ldots, X_n$ を横ベクトルとして考え、これらを縦に並べてできる行列をXと置く。この時、

d(det(X))はR-基底の取り方に依らず、Lにより唯一定まる。

証明：Lの二つのR-基底により定まる行列をX及びX'とする。この時、基底の変換行列Pが存在して、PX = X' かつ$P^{-1}X' = X$となり、しかもP^{-1}はR-行列である。ここで、

$$d(\det(X')) = d(\det(P \cdot X)) = d(\det(P) \cdot \det(X)) \geq d(\det(X))$$

同様に、

$$d(\det(X)) = d(\det(P^{-1} \cdot X')) = d(\det(P^{-1}) \cdot \det(X')) \geq d(\det(X'))$$

この二つの式により、d(det(M)) = d(det(M')) を得る。 #

注意) 補題 2.1 の証明と同様な議論により、Euclid 環の二元が各々、他方の可逆元倍である時、そのノルムは等しいことが判る。

補題 2.1 により、R-格子Lに対して、次が定義される。

定義 2.7 R-格子Lに対して、補題 2.1 により定まる値を、格子Lの行列式（determinant of lattice）または格子Lの基本領域と言い、d(L)で表す。

即ち、d(L) = d(det(X)) である。 .....(2.9)

次に、R-格子Lの各元にノルムを定める。

定義 2.8 R-格子Lに対して、Lに以下のノルムが定義できる。

Lの元 $X = (x_1, \ldots, x_n)$ に対して

$$d_s(X) = (d(x_1)^s + d(x_2)^s + \ldots + d(x_n)^s)^{1/s} \quad .....(2.10)$$

ここで s は自然数とする。s を無限大にした時に得られるノルムを d_∞ とおけば

$$d_\infty(X) = \max \{ d(x_1), \ldots, d(x_n) \} \text{ となる。} \quad .....(2.11)$$

d_2-ノルムに関しては、特に Archimedean の場合は、定理 2.1 により、RはCに埋め込むことができ、ノルムは絶対値と同値であるので、自然な意味で、各格子点の間に次の内積が定義できることに注意しておく。

Lの元 $X=(x_1,\ldots,x_n)$ と $Y=(y_1,\ldots,y_n)$ に対して、内積 (X, Y) は

$(X, Y) = d(x_1 \cdot y_1 + \ldots + x_n \cdot y_n)$ と定義する。 .....(2.12)

この時、$(X, X) = d_2(X)^2$ となる。 .....(2.13)

格子に関して重要な概念の一つに、「小さいノルムを持つ」格子点 (short vecto r) がある。以下「小さいノルムを持つ」格子点について定義する。

定義 2.9 格子Lの元 X が小さいノルムを持つとは、X が以下の条件を満たすことを言う。

Lのノルム d_L およびLの次元により決まるある正の実数 δ が存在し、任意のLの元 Y に対して、 $d_L(X) \leq \delta \cdot d_L(Y)$ となる。 .....(2.14)

特に δ が1に取れる時は、上の X は最小のノルムを持つことになる。

格子Lに対して、小さいノルムを持つ格子点を求める方法がある種の Euclid 付値環に対して提案されている。Z-格子に対しては、d_2-ノルムに関して A.K.Lenstra, H.W.Lenstra と L.Lovasz〔6〕、E.Kaltofen〔5〕等があり、GF(q)〔x〕- 格子に対しては、d_∞-ノルムに関して A.K.Lenstra〔12〕、J.von zur Gathen〔17〕等がある。本論文では、これらの方法が一般の Euclid 付値環に対しても適応可能であることを以下に示す。

最初に、簡約化基底 (reduced base) について定義する。ノルムが non-Archime dean の場合と Archimedean の場合に分けて定義する。

定義 2.10 d が non-Archimedean かつ d_2-ノルムの場合の簡約化基底 :

Lの基底 $B_1,\ldots,B_n$ が簡約化基底であるとは、その直交化した基底 $B_1^*,\ldots,B_n^*$ が次を満たすことを言う。

$$d_2(B_i^*)^2 \geq \tfrac{1}{2} \cdot d_2(B_{i-1}^*)^2 \quad \text{for } 2 \leq i \leq n \qquad .....(2.15)$$

ここで、直交化した基底とは、次をさす。(,) は d による内積を表す。

$$B_i^* = B_i - \sum_{j<i} \mu_{i,j} B_j^* \qquad \mu_{i,j} = (B_i, B_j^*)/(B_j^*, B_j^*) \qquad .....(2.16)$$

上記の簡約化基底に対し、B_1 は次の性質を持つ。

任意のLの元 X に対して、 $d_2(B_1)^2 \leq 2^{n-1} \cdot d_2(X)^2$ .....(2.17)

即ち、B_1 は $\delta = 2^{(n-1)/2}$ とした時の小さいノルムの格子点となる。

定義 2.11 d が Archimedean かつ d_∞-ノルムの場合の簡約化基底 :

Lの基底 $B_1,\ldots,B_n$ が簡約化基底であるとは、$B_1,\ldots,B_n$ が次を満たすことを言う。

$B_1,\ldots,B_n$ を横ベクトルと見た時、

$$B = \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{bmatrix}$$ に対して、列の置換により次のB'が得られることを言う。

$$B' = \begin{bmatrix} B'_1 \\ B'_2 \\ \vdots \\ B'_n \end{bmatrix}$$ ただし、(a) $d_\infty(B'_i) \leq d_\infty(B'_j)$ for $1 \leq i < j \leq n$

(b) $d(B'_{i,i}) \geq d(B'_{i,j})$ for $1 \leq i < j \leq n$

(c) $d(B'_{i,i}) > d(B'_{i,j})$ for $1 \leq j < i \leq n$

.....(2.18)

上記の簡約化基底に対し、B_1 は次の性質を持つ。

任意のLの元 X に対して、 $d_\infty(B_1) \leq d_\infty(X)$ .....(2.19)

即ち、B_1 は$\delta = 1$とした時の小さいノルムの格子点となる。

以上の簡約化基底に対して、その最初の元が小さいノルムの格子点となるので、小さいノルムの格子点を求めることは、与えられた基底に対して、その基底を簡約化することに帰着することができる。この基底を簡約化するアルゴリズムを基底簡約アルゴリズム (Basis Reduction Algorithm)と呼ぶ。

線形空間のノルムに関して、次の補題を挙げておく。

補題 2.2 Rを Euclid 付値環とし、そのノルムを d とする。また、n次元のQ-線形空間Lに対して、d が Archimedean または non-Archimedean に応じて、d_2 または d_∞ をその線形空間のノルム d_L として定める。この時、次が成り立つ。Rのn個の元 $a_1,\ldots,a_n$ に対して、

$d(a_1 \cdot a_2 \cdot \ldots \cdot a_n) = d(a_1) \cdot d(a_2) \cdot \ldots \cdot d(a_n)$ .....(2.20)

Lの元 $X = (x_1,\ldots,x_n)$ に対して、$d_L(X)$ と X の成分 x_i のノルムとの間に

$d_L(X) \geq d(x_i)$ for $1 \leq i \leq n$ .....(2.21)

Lの元を行とする正方行列Mに対して、その各行を $M_1,\ldots,M_n$ とした時、

$d(\det(M)) \leq d_L(M_1) \cdot d_L(M_2) \cdot \ldots \cdot d_L(M_n)$ .....(2.22)

証明: (2.20)は (2.4)によりただちに言える。また、(2.21)は定義とZの性質により直ちに求まる。

(2.22)は Hadamard の不等式と呼ばれるもので、一般にC上の正方行列に対して成り立つ。よって、定理 2.1 により d が Archimedean である時は成り立つ。

d が non-Archimedean である場合は、$M_i = (m_{i,j})$ とおけば、

$det(M) = \Sigma\ sign(s) \cdot m_{1,s(1)} \cdot \ldots \cdot m_{n,s(n)}$ （ここで、Σはすべての置換 s を動く。）である。よって、

$$d(det(M)) = d(\Sigma\ sign(s) \cdot m_{1,s(1)} \cdot \ldots \cdot m_{n,s(n)})$$

$$\leq \max \{ d(m_{1,s(1)} \cdot \ldots \cdot m_{n,s(n)}) \}$$

(2.21)により、各 i に対して、$d(m_{i,j}) \leq d_L(M_i)$ であるので、

$$\leq d_L(M_1) \cdot d_L(M_2) \cdot \ldots \cdot d_L(M_n)$$

以上により補題は証明された。 ∎

本節の最後に基底簡約アルゴリズムについて例を挙げる

例 2.1 R = Z かつ d が絶対値 | | であり、Lのノルムが d_2-ノルムの場合:

定義 2.10 において、簡約化基底を (2.15) を満たすものとしたが、実際のアルゴリズムでの簡約基底の構成では以下の様に行う。

$B_1,\ldots,B_n$ を格子の基底とする。そして、その直交化した基底を

$B^*_1,\ldots,B^*_n$ とする。記号を (2.15) 及び (2.16) と同じにとる。

この時に、$B_1,\ldots,B_n$ が簡約基底になるために、次の条件を課す。

$$| \mu_{i,j} | \leq \frac{1}{2} \quad \text{for } 0 \leq j < i \leq m \qquad \ldots\ldots(2.22)$$

$$| B^*_i + \mu_{i,i-1} B^*_{i-1} |^2 \geq 3/4 \cdot | B^*_{i-1} |^2 \quad \text{for } 1 < i \leq n \qquad \ldots\ldots(2.23)$$

この条件を満たすように、基底を換える。

注意) もともと、A.K.Lenstra et al〔6〕の論文では上の条件 (2.22) および (2.23)が簡約化基底の定義であった。(2.15)の定義は、E.Kaltofen〔5〕による改良された基底簡約アルゴリズムでの簡約化基底の定義を一般化したものである。

例 2.2 R = GF(q) [Y] かつ d がRの元 F(X) に対して、

$d(F(X)) = 2^{degree\ F(X)}$ の場合

基本的には Euclid の互除法を用いて簡約化基底を作る。この加法的なタイプに対して、J.von zur Gathen〔17〕が改良・一般化したアルゴリズムを発表している。ここでは、von zur Gathen によるアルゴリズムの簡約化基底を紹介する。(この定義でも B_1 は最小ノルムの格子点になる。)

定義 2.12 （ von zur Gathen による簡約化基底 ）

定義 2.11 の B' の条件 (2.18) の (b)、(c) を次のように変える。

$$(b)'\quad d(B'_{i,i}) > d(B'_{i,j}) \quad \text{for } i \neq j \qquad \ldots\ldots(2.24)$$

3 ＧＣＤへの応用

以下Ｒを Euclid 付値環として、Ｒの元の間のＧＣＤの計算への格子の応用を述べる。即ち、ＲにおけるＧＣＤの計算が格子の小さいノルムを求めることに帰着されることを示す。

与えられたＲ及びＲ-格子Ｌに対して、各々のノルムを d 及び d_L と置く。次を仮定する。

仮定 3.1 Ｒ-格子Ｌに対して、Ｌの小さいノルムの格子点を求めるアルゴリズムが存在する。即ち、Ｌの基底および定数 δ が与えられた時、次を満たす X を求めるアルゴリズムが存在する。

Ｌの任意の格子点 Y に対して、

$$d_L(X) \leqq \delta \cdot d_L(Y) \qquad .....(3.1)$$

Ｒは素元分解環であるので、Ｒの複数の元に対して最大公約因子ＧＣＤが存在し、ＧＣＤは可逆元を除いて唯一定まることが言える。

注意）Ｒの元 a の因子と言う場合は、可逆元は入らないことに注意しておく。

仮定 3.2 Ｒの任意の元 a に対して、次を満たす a' を求めるアルゴリズムが存在する。

$$d(a') \geqq \delta \cdot d(a) + 1 \qquad .....(3.2)$$

Ｒの異なる二つの元 a, b が与えられた時、ＧＣＤ(a, b)を求めるアルゴリズムを示す。

a, b に対して、次のベクトル U, V を定義する。

$$U = (b \cdot a', 1),\ V = (a \cdot a', 0) \qquad .....(3.3)$$

U, V を基底とする２次元のＲ-格子Ｌを作る。このＬに対して仮定 3.1 のアルゴリズムを起動して、小さいノルムの格子点 $X = (x_1, x_2)$ を算出する。

この時、次の定理が言える。

定理 3.1 上記の a, b 及び X に対して、

$x_1 = 0$ かつ $x_2 = k \cdot a / GCD(a, b)$ となる。ここで、$d(k) \leqq \delta$ である。

証明: $g = GCD(a, b)$ とし、$Z = (-b/g) \cdot V + (a/g) \cdot U$ に取れば、$Z = (0, a/g)$ である。Ｌの小さいノルムの格子点 $X = (x_1, x_2)$ に対して、$X = s \cdot V + t \cdot U$, ここで s, t はＲの元, の形であることに注意しておく。また、$t = x_2$ である。

X は小さいノルムの格子点であることより、

$d_L(X) \leq \delta \cdot d_L(Z) = \delta \cdot d(a/g) = \delta \cdot d(a) / d(g)$

一方、$x_1 = (s \cdot a + t \cdot b) \cdot a'$であるので、

$d(x_1) = d((s \cdot a + t \cdot b) \cdot a') = d(a') \cdot d(s \cdot a + t \cdot b)$

よって(3.2) により、

$$(\delta \cdot d(a) + 1) \cdot d(s \cdot a + t \cdot b) \leq d(x_1)$$
$$\leq d_L(X) \leq \delta \cdot d_L(Z) = \delta \cdot d(a) / d(g)$$

このことは、$d(s \cdot a + t \cdot b) = 0$を意味する。即ち、$s \cdot a + t \cdot b = 0$となる。これより、$x_1 = 0$を得、$x_2 = t = k \cdot (a/g)$ となることが判る。ここで k はあるRの元であり、$d(x_2) \leq d_L(X) \leq \delta \cdot d_L(Z) = \delta \cdot d(a) / d(g)$ より、$d(k) \leq \delta$を得る。 #

定理 3.1 は、J.von zur Gathen (16) の結果を一般化したものである。

特にδが1である時は、上の定理によりGCD(a, b) = a / x_2 となることが言える。一般に、$N = \{ c \mid 2 \leq d(c) \leq \delta \}$ が有限集合でNの元全体が判っていれば、次の方法でGCDを求めることが出来る。

アルゴリズム 3.1

(i) Rの異なる二元 a, b に対して、ベクトル U, V を (3.3)により定義する。

(ii) U, V をR-基底とするR-格子Lに対して、その小さいノルムの格子点を求め、それを X とする。

(iii) X の第2成分 x_2 に対して、次を行う。

Nの元をノルムに番号を付け、それらを $n_1, \ldots, n_t$ とする。

(ここで、t = #N である。)

$S = \{ n_i \mid n_i \mid x_2$ かつ $a \cdot n_i \mid x_2 \cdot b \}$ を求める。

s をSの中で d(s) が最大になるものとする。(一つとは限らない)

この時、GCD(a, b) = $(a \cdot s) / x_2$ となる。

アルゴリズム 3.1 の正当性を以下で示す。

補題 3.1 アルゴリズム 3.1 は正しいGCDを計算する。

証明: g = GCD(a, b) とおけば、$x_2 = k \cdot (a/g)$ であることより、

$s \mid x_2$ かつ $a \cdot s \mid x_2 \cdot b$ ならば、$s \mid k \cdot (a/g)$ かつ $s \mid k \cdot (b/g)$ となる。

.....(3.4)

よって、$s \mid k$ を示せば、k はSの元であることより、$d(s) = d(k)$ が言え、$s = k \cdot r$ となる。ここで、r はRの可逆元である。即ち、アルゴリズム 3.1 は正しいことが言える。よって以下、$s \mid k$ を示す。$s \nmid k$ であるとして矛盾を導く。

(3.4) により、$s_1 = GCD(s, k)$、$s_2 = s/s_1$ とおくと、

$s_2 \mid (a/g)$ かつ $s_2 \mid (b/g)$ となる。これは、$s_2 \mid GCD((a/g), (b/g))$ を意味する。しかし、$GCD((a/g), (b/g))$は1であるので、s_2 は可逆元でしかない。これは、$s \nmid k$ に反する。　　#

次に δ が1の場合に対して、上の定理の拡張として三つ以上の元のGCDの計算について述べる。その前に無平方を定義しておく。

定義 3.1　Rの元 a が無平方 (square-free)であるとは、a の任意の因子 b に対して、b^2 は a の因子にならないことを言う。

Rの異なるn個の元 $a_1,\ldots,a_n$ に対して、そのGCDを g とする。但し、a_1 は無平方であると仮定する。即ち、a_1 はRの元の二乗では割れないとする。

次のn個のQ-線形独立なベクトルを考える。

$$U_1 = (a_2 \cdot a_1', a_3 \cdot a_1', \ldots, a_n \cdot a_1', 1)$$
$$U_2 = (-(a_1 \cdot a_1'), 0, \ldots, 0)$$
$$\vdots$$
$$U_n = (0, \ldots, -(a_1 \cdot a_1'), 0) \qquad \ldots\ldots(3.5)$$

ここで、a_1' は仮定 3.2 により得られるRの元。即ち、次を満たす。

$$d(a_1') \geq d(a_1) + 1 \qquad \ldots\ldots(3.6)$$

L を $U_1,\ldots,U_n$ により生成されるR格子とする。基底簡約アルゴリズムを起動して最小ノルムの格子点を求め、それを $X = (x_1,\ldots,x_n)$ とする。この時、次の定理が成り立つ。

定理 3.2 上記の X に対して、次が成り立つ。

$x_1 = x_2 = \ldots = x_{n-1} = 0$ かつ $x_n = k \cdot a_1/g$ となる。ここで、k は可逆元である。

証明: $Z = (a_1/g) \cdot U_1 + (a_2/g) \cdot U_2 + \ldots + (a_n/g) \cdot U_n$ とおく。

この時、$Z = (0, \ldots, a_1/g)$ である。よって、$d_L(Z) = d(a_1/g) \leq d(a_1)$。

X はLの最小ノルムの格子点であるので、$d_L(X) \leq d_L(Z) \leq d(a_1/g)$。

特に、$d(x_i) \leq d_L(X) \leq d(a_1/g) \leq d(a_1)$である。　.....(3.7)

さて、X はLの元であるので、あるRの元 $s_1,\ldots,s_n$ が存在して、

$X = s_1 \cdot U_1 + \ldots + s_n \cdot U_n$ と書ける。よって、i成分に対して（$1 \leqq i \leqq n-1$）

$x_i = s_1 \cdot a_1' \cdot a_{i+1} - s_{i-1} \cdot a_i' \cdot a_i = (s_1 \cdot a_{i+1} - s_{i-1} \cdot a_i) \cdot a_1'$ となる。

また、$x_n = s_1$ である。ゆえに、n未満のiに対して、次が成り立つ。

$$d(x_i) = d((s_1 \cdot a_{i+1} - s_{i-1} \cdot a_i) \cdot a_1')$$
$$= d(s_1 \cdot a_{i+1} - s_{i-1} \cdot a_i) \cdot d(a_1')$$
$$\leqq d(a_1) \qquad \ldots\ldots(3.8)$$

（3.6）と（3.8）により、

$d(s_1 \cdot a_{i+1} - s_{i-1} \cdot a_i) = 0$ 即ち、$s_1 \cdot a_{i+1} - s_{i-1} \cdot a_i = 0$ を得る。

よって、n未満のiに対して、$x_i = 0$ である。

また、$1 \leqq i < n$に対し、$x_n = s_1 = a_1 \cdot k_{i+1} / GCD(a_1, a_{i+1})$ かつ

$s_i = a_{i+1} \cdot k_{i+1} / GCD(a_1, a_{i+1})$ の形になる。 $\ldots\ldots(3.9)$

ここで、k_{i+1} はRの元。以上をまとめると、

$s_1 = a_1 \cdot k_2 / GCD(a_1, a_2) = \ldots = a_1 \cdot k_n / GCD(a_1, a_n)$ となり、

$GCD(a_1, a_i) = g_i \cdot g$ と置けば、

$s_1 = (a_1 \cdot k_2) / (g_2 \cdot g) = \ldots = (a_1 \cdot k_n) / (g_n . g)$ となる。

$\ldots\ldots(3.10)$

もし、g_2 が1、即ち可逆元であるとすると、

$d(s_1) = d(x_n) \leqq d(a_1/g)$ より、これは、$d(k_2) = 1$、即ち k_2 は可逆元であることを意味し、定理は成り立つ。

よって、$d(g_2) \geqq 2$ と仮定してよい。同様の議論により、すべてのiに対して $d(g_i) \geqq 2$ と仮定できる。（3.10）に g を乗じれば、

$g \cdot s_1 = (a_1/g_2) \cdot k_2 = \ldots = (a_1/g_n) \cdot k_n$ となる。 $\ldots\ldots(3.11)$

まず、$g_2 \mid k_2$ の場合を考える。この時、$g_i \mid k_i$（$2 \leqq i \leqq n$）となる。

$s_1 = (a_1/g) \cdot (k_2/g_2)$ であり、$k = k_2/g_2$ と置けば、$d(k) \leqq 1$ となり、定理を得る。よって、最後に残る場合は、$g_i \nmid k_i$（$2 \leqq i \leqq n$）の場合である。

以下、$g_i \nmid k_i$ の場合を考える。$g^0_i = GCD(g_i, k_i)$、$g^1_i = g_i/g^0_i$ とおく。g^1_i は可逆元ではないことに注意しておく。

g 及び g_i の定義により、あるiが存在して、$g^1_z \nmid g_i$ となる。よって、$g^1_z \mid a_1$ であることより、$GCD(g^1_z, a_1/g_i)$ は可逆元ではない。よって、（3.11）か

らＧＣＤ(g'_2, $g \cdot s_1$) は可逆元ではないことが判る。従って、g'_2 の定義により、ＧＣＤ(g'_2, a_1/g'_2) は可逆元ではない。これは、a_1 が無平方であることに反する。以上により定理は証明された。　　#

定理 3.2 により、$a_1,\ldots,a_n$ に対して、そのＧＣＤ g は基底簡約アルゴリズムにより得られる X の第ｎ成分 x_n を取り、a_1 を x_n で割ることにより求めることが出来る。

例 3.1 R = Z かつ d が絶対値の時 (J.von zur Gathen [16] を参照)

2節の例 2.1 により、$\delta = 2$ と取れる。よって、仮定 3.2 に対しては、

$a' = 2 \cdot |a| + 1$とすれば良い。　　.....(3.12)

この時、Ｚの異なる二元 a, b に対して、そのＧＣＤを g とする。

$V = (a \cdot (|a| + 1), 0)$, $U = (b \cdot (|a| + 1), 1)$と置く。.....(3.13)

U 及び Vにより生成されるＺ-格子Ｌを考える。Ｌに対して、基底簡約アルゴリズムを起動して、小さいノルムの格子点 X を求める。この時、第２成分 x_2 に対し

$x_2 = k \cdot a/g$ であり、$|k| = 1$ または 2 となる。

注意) この場合の基底簡約アルゴリズムは、実際は Euclid の互除法を行っているに過ぎない。

例 3.2 R = GF(q) [x] かつ $d = 2^{degree}$ の時 (例 2.2 参照)

2節の例 2.2 により、$\delta = 1$ と取れる。よって、仮定 3.2 に対しては、

$a_1'(x) = a_1(x) \cdot x$ とすれば良い。　　.....(3.14)

定理 3.2 により、$a_1(x)$ が無平方であるならば、三つ以上の異なるＲの元 $a_1(x),\ldots,a_n(x)$ に対して

$U_1 = (a_2(x) \cdot a_1(x) \cdot x , a_3(x) \cdot a_1(x) \cdot x ,\ldots, a_n \cdot a_1(x) \cdot x , 1)$

$U_2 = (-(a_1(x))^2 \cdot x , 0 ,\ldots, 0)$

$\vdots$

$U_n = (0 ,\ldots, -(a_1(x))^2 \cdot x , 0)$　　.....(3.15)

と置き、これらにより生成される GF(q) [x] -格子Ｌを考える。Ｌに対して、基底簡約アルゴリズムを起動して、最小ノルムの格子点 X を求める。この時、第ｎ成分 $x_n = k \cdot a_1(x)/ＧＣＤ(a_1(x),\ldots,a_n(x))$ となり、k は GF(q) の元である。よって、$a_1(x)/x_n$ によりＧＣＤ($a_1(x),\ldots,a_n(x)$) が求まる。

4 因数分解への応用

以下Rを Euclid 付値環とし、Rを係数環とする一変数多項式の因数分解への格子の応用を述べる。A.K.Lenstra の定理が一般の Euclid 付値環に対し、ほぼそのままの形で成り立つこと、更には、Euclid 環においてもその定理に必要であるいくつかの性質および評価式をノルムが満たせば、やはり定理が成り立つことを示す。このことにより、因数分解アルゴリズムに格子算法が適用できる。

ここでは、節3の記号をそのまま使うことにする。

αをRの素イデアルとする。Rは単項イデアル環であるので、αは極大イデアルである。更に、R／αは体になる。

以下R〔X〕における因数分解を考える。

まず、R〔X〕の元 F(X) に関して必要な定義をする。

定義 4.1 F(X) が無平方（ square-free ）であるとは、F(X) が重複する因子を持たないことを言う。（ 定義 3.1 参照 ）

定義 4.2 F(X) がモニック（ monic ）であるとは、F(X) の最大次数の係数が1であることを言う。

定義 4.3 F(X) が原始的（ primitive ）であるとは、F(X)のｉ次の係数 F_i に対して、$F_0,\ldots,F_n$ のＧＣＤが1であることを言う。ここで、F(X) の次数をｎとする。

注意）モニックであれば、原始的である。

F(X) が原始的でない場合は、その係数のＧＣＤを括りだすことにより、F(X) の因数分解がその原始的な部分の因数分解に帰着される。

更に、F(X) がモニックでない時、F(X) の次数をｎとし、ｎ次の係数を F_n とする。

この時、$F_0(X) = (F_n)^{n-1} \cdot F(X/F_n)$ とおけば、　　.....(4.1)

$F_0(X)$ はモニックとなる。F(X) の因数分解は $F_0(X)$ の因数分解に帰着されることは次の関係により判る。

E(X) は F(X) の因子　⟺　$E_0(X)$ は $F_0(X)$ の因子

ここで、$E_0(X) = (E_m)^{m-1} \cdot E(X/E_m)$、degree E(X) = ｍとする。

.....(4.2)

よって、以下、無平方かつモニックである F(X) の因数分解を考える。ここで、F(X) の次数をｎとする。

まずRに関して次を仮定する。

仮定 4.1 Rに対して次が成り立つ。

Rの任意の素イデアルαに対して、R／α上の因数分解アルゴリズムが知られている。

仮定 4.2 任意のR-格子Lに対して、Lの小さいノルムの格子点を求めるアルゴリズムが存在する。

以下仮定 4.1 および仮定 4.2 が成り立つとする。この時、次の Hensel の補題が成り立つ。

定理 4.1 (Hensel の補題)

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

$K(X) \equiv G(X) \cdot H(X) \mod \alpha$ .....(4.3)

H(X) は monic である。 .....(4.4)

H(X) と G(X) は $\mod \alpha$ で互いに素である。 .....(4.5)

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。

$K(X) \equiv G_k(X) \cdot H_k(X) \mod \alpha^k$ .....(4.6)

$H_k(X) \equiv H(X)$, $G_k(X) \equiv G(X) \mod \alpha$ .....(4.7)

degree $H_k(X)$ = degree H(X) .....(4.8)

証明は、あるRの元 a が存在して$\alpha = \langle a \rangle$ と書けることにより、R = Z における証明と同様である。 (佐々木 [15] 補題 2.2 参照。)

仮定 4.1 により、F(X)を (R／α) [X] において因数分解し、その既約因子を一つ取り $H_1(X)$ とする。ここで、$\alpha = \langle a \rangle$ とし、degree $H_1(X)$ = h とする。

更に $H_1(X)^2 \nmid F(X) \mod \alpha$ と仮定する。

この時、定理 4.1 の Hensel の補題より、次が成り立つ。

F(X) は (R／α^k) [X] において、既約因子 H(X) を持ち、更に次を満たす。

H(X) はモニック .....(4.9)

$H(X) \mid F(X) \mod \alpha^k$ .....(4.10)

$H(X) \equiv H_1(X) \mod \alpha$ .....(4.11)

$H_1(X)^2 \nmid F(X) \mod \alpha$ .....(4.12)

ここで、kは正の整数とする。

次の定理を示す。

定理 4.2 (Existence and Uniqueness Theorem)

上記の仮定の下で、F(X) は $H(X) \mid G_0(X) \bmod \alpha^k$ なるR上の既約因子 $G_0(X)$ を持つ。またこのような $G_0(X)$ は可逆元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。

$H(X) \mid G(X) \bmod \alpha$ .....(4.13)

$H(X) \mid G(X) \bmod \alpha^k$ .....(4.14)

$G_0(X) \mid G(X)$ .....(4.15)

特に $H(X) \mid G_0(X) \bmod \alpha$ である。 .....(4.16)

証明: $G_0(X)$ の存在は明らかであり、唯一性は、F(X) が無平方であり、かつモニックであることにより、言える。以下、三条件が同値であることを示す。

(4.14)ならば (4.13) 、(4.15)ならば (4.13) は明らか。

よって、(4.13)ならば (4.14) および (4.15) が成り立つことを言えばよい。

そこで (4.13) を仮定する。

この時、(4.12)により、$H(X) \nmid (F(X)/G(X)) \bmod \alpha$ である。

従って、$H(X) \nmid (F(X)/G(X)) \bmod \alpha$ となり、このことは、$G_0(X) \mid G(X)$を意味する。即ち、(4.15)が言えた。

次に (4.14) を言う。

(4.12)により、H(X) と F(X)/G(X)は (R／α) 〔X〕 において互いに素である。よって、あるR 〔X〕 の元 $\lambda(X)$ および $\mu(X)$ が存在して、

$\lambda(X) \cdot H(X) + \mu(X) \cdot (F(X)/G(X)) \equiv 1 \bmod \alpha$ となる。

よって、あるα 〔X〕 の元 $\nu(X)$ が存在して、

$\lambda(X) \cdot H(X) + \mu(X) \cdot (F(X)/G(X)) = 1 - \nu(X)$ となる。 .....(4.17)

(4.17)の両辺に $(1 + \nu(X) + \ldots + \nu(X)^{k-1}) \cdot G(X)$をかけて、

$$\lambda(X) \cdot (1 + \nu(X) + \ldots + \nu(X)^{k-1}) \cdot G(X) \cdot H(X)$$
$$+ \mu(X) \cdot (1 + \nu(X) + \ldots + \nu(X)^{k-1}) \cdot F(X)$$
$$= (1 - \nu(X)) \cdot (1 + \nu(X) + \ldots + \nu(X)^{k-1}) \cdot G(X)$$
$$= (1 - \nu(X)^k) \cdot G(X) \equiv G(X) \bmod \alpha^k$$ を得る。 .....(4.18)

(4.18)により、あるR 〔X〕 の元 $\lambda'(X)$および $\mu'(X)$が存在して、

$\lambda'(X) \cdot H(X) + \mu'(X) \cdot F(X) \equiv G(X) \bmod \alpha^k$ を得る。 .....(4.19)

(4.10)により、(4.19)は次を意味する。

$H(X) \mid \lambda'(X) \cdot H(X) + \mu'(X) \cdot F(X) \bmod \alpha^k$

即ち、$H(X) \mid G(X) \bmod \alpha^k$ となり、(4.14)が言えた。 ∎

さてここで、R-格子$L_{m,k}$ を次の様に定義する。

$L_{m,k} = \{ E(X) \mid \text{degree } E(X) \leq m \text{ かつ } H(X) \mid E(X) \bmod \alpha^k \}$ .....(4.20)

定理 4.2 により、$L_{n,k}$ 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、$L_{s,k}$ の中にあることも言える。よって、$L_{s,k}$ の中から抜き出すことをすればよいことが判る。

この時、次が言える。

補題 4.1 $L_{m,k}$ はR-格子になる。

証明: $L'_m = \{ E(X) \in Q[X] \mid \text{degree } E(X) \leq m \}$ とおく。この時、

L'_m の元 E(X) に対して、$E(X) = \sum_{i=0}^{m} E_i \cdot X^i$ と書ける。

そこで、E(X) に $(E_0, E_1, \ldots, E_m)$ を対応させることにより、L'_m はQ-線形空間となり、$L_{m,k}$ はその部分集合である。

$L_{m,k}$ のR-基底として、次が取れることを示せばよい。

$$B_0 = a^k,\ B_1 = a^k \cdot X,\ \ldots,\ B_{h-1} = a^k \cdot X^{h-1}$$

$$B_h = H(X),\ B_{h+1} = H(X) \cdot X,\ \ldots,\ B_m = H(X) \cdot X^{m-h} \qquad \ldots..(4.21)$$

明らかに、上の $B_0,\ldots,B_m$ はQ-線形独立である。また、任意の$L_{m,k}$ の元 E(X) に対して、$H(X) \mid E(X) \bmod \alpha^k$ より、$E(X) - H(X) \cdot D(X) \equiv 0 \bmod \alpha^k$ なる D(X) が存在する。このことは、E(X) が $B_0,\ldots,B_m$ のR-結合で表すことができることを意味する。よって、$B_0,\ldots,B_m$ は$L_{m,k}$ のR-基底である。以上により、$L_{m,k}$ はR-格子になる。 ∎

R-格子$L_{m,k}$ に対して、ノルム d_L を d が Archimedean か non-Archimedean かに応じて、d_Z または d_∞ として定義する。

このR-格子$L_{m,k}$ に対して、次の定理を述べる。

定理 4.3 R-格子$L_{m,k}$ の元 Z(X) が次の条件を満たすとする。

$$d_L(F(X))^m \cdot d_L(Z(X))^n < d(\mathfrak{a})^{kh} \qquad \ldots..(4.22)$$

この時、定理 4.2 の $G_0(X)$ は Z(X) の因子である。

ここで、$\mathfrak{a} = \alpha$である。また h = degree H(X) である。

証明は A.K.Lenstra [12] の証明がそのまま利用できる。

証明: E(X) =ＧＣＤ(F(X), Z(X))とおく。この時、定理 4.2 により、

H(X) | E(X) mod α を言えばよい。そこで、H(X)∤E(X) mod α として矛盾を導く。

ここで、degree Z(X) = z、degree E(X) = e とおく。

H(X) は (R／α) 〔X〕 において既約であるので、H(X) と E(X) は (R／α) 〔X〕 において互いに素である。よって、あるR 〔X〕 の元 λ(X), μ(X) および ν(X) が存在して、λ(X)・H(X) + μ(X)・E(X) = 1 - ν(X) となる。　　.....(4.23)

さて、F(X) と Z(X) により次のR-格子L' を作る。

L' = { A(X)・F(X) + C(X)・Z(X) | A(X), C(X) ∈ R 〔X〕 かつ

degree A(X) < z - e かつ degree C(X) < n - e }

.....(4.24)

L' がR-格子であることは、R-基底Mが次の様に取れることにより判る。特に、L' の次元は n + z - 2・e である。

M = { X^i・F(X) | 0 ≦ i < z - e } ∪ { X^i・Z(X) | 0 ≦ i < n - e }

.....(4.25)

Mが L' を張ることは定義より明らかである。Mの元が線形独立であることを言うには、A(X)・F(X) + C(X)・Z(X) = 0 ならば A(X) = C(X) = 0 を言えばよい。

ここで、degree A(X) < z - e かつ degree C(X) < n - e とする。

実際、A(X)・F(X) + C(X)・Z(X) = 0 ならば

A(X)・(F(X)/E(X)) = -C(X)・(Z(X)/E(X)) となる。　　.....(4.26)

しかし、ＧＣＤ(F(X)/E(X), Z(X)/E(X)) = 1 により、(4.26)は

F(X)/E(X) | C(X) を意味する。degree C(X) < n - e = degree (F(X)/E(X)) より、これは A(X) = C(X) = 0 を意味する。

この L' に対して、ノルム $d_{L'}$ を $L_{n,k}$ 同様に定めれば、補題 2.1 により、Lの行列式 d(L') は次の様になる。

d(L') = d(det(M)) = $d_{L'}$(F(X))$^{z-e}$・$d_{L'}$(Z(X))$^{n-e}$

≦ $d_{L'}$(F(X))^{z}・$d_{L'}$(Z(X))^{n}　となる。　　.....(4.27)

ここで、$d_{L'}$(F(X)) = $d_{L'}$(F(X)・X^i) に注意しておく。

しかも、$d_{L'}$(F(X)) = d_{L}(F(X)) かつ $d_{L'}$ (Z(X)) = d_{L}(Z(X)) より

d(L') ≦ d_{L}(F(X))^{z}・d_{L}(Z(X))^{n}　を得る。　　.....(4.28)

L' の次元が n + z - 2・e であり、L' の元の最大次数が n + z - e - 1 かつ

L' の元の最小次数が e であることにより、L' の基底を次の様に取り代えることができる。

$M' = \{ B_e(X), B_{e-1}(X), \ldots, B_{n+z-e-1}(X) \}$ .....(4.29)

ここで、degree $B_i(X) = i$ である。

この時、$d(L') = d(\det(M'))$

$= d(lc(B_e(X)) \cdot d(lc(B_{e-1}(X)) \cdot \ldots \cdot d(lc(B_{n+z-e-1}(X))$

となる。 .....(4.30)

ここで、lc は最高次の係数 (leading coefficient) を表す。

さて、L' の元 V(X) に対して、degree V(X) < e + h ならば V(X) は α 〔X〕 に属することを示す。

定義より、E(X) | V(X) である。(4.23) の両辺に

(V(X)/E(X)) ・(1 + ν (X) +...+ ν^{k-1}) をかけることにより、次が言える。

ある R 〔X〕 の元 $\lambda'(X)$ と $\mu'(X)$ が存在して、

$\lambda'(X) \cdot H(X) + \mu'(X) \cdot E(X) \equiv V(X)/E(X) \bmod \alpha^k$ となる。.....(4.31)

Z(X) は Lm,k の元であるので、特に H(X) | Z(X) mod α^k である。もともと、

H(X) | F(X) mod α^k であるので、H(X) | GCD(F(X), Z(X)) mod α^k 即ち、

H(X) | E(X) mod α^k となる。よって、H(X) | (V(X)/E(X)) mod α^k である。

しかし、degree (V(X)/E(X)) < h + e - e = h より、H(X) | (V(X)/E(X)) mod α^k は V(X)/E(X) ≡ 0 mod α^k を意味する。 即ち、V(X) ≡ 0 mod α^k を得る。

よって、特に $d(lc(V(X))) \geq d(a)^k$ である。 .....(4.32)

(4.32) により、(4.30) は次の様に評価される。

$d(L') = d(\det(M')) \geq d(a)^{kh}$ .....(4.33)

(4.27) と (4.33) を併せ、z ≦ m であることに注意すれば、

$d_L(F)^n \cdot d_L(Z)^n \geq d(a)^{kh}$ となり矛盾である。

以上により、定理は言えた。 #

定理 4.3 を満たすようなノルムの小さい格子点が存在するように k の値を決める。

この R-格子 Ln,k に対して、仮定 4.2 を用いて、小さいノルムの格子点を求めるのである。そこで、k の値の決め方について述べる。

まず係数の評価 (bound of coefficients) について述べておく必要がある。

定義 4.4 R 〔X〕 の元 F(X) に対して、b(F(X)) を次の様に定める。

$b(F(X)) = \max\{ d(e) \mid E(X) \mid F(X)$ かつ e は $E(X)$ の係数 $\}$ .....(4.34)

定義 4.5 n次以下の多項式 $E(X)$ の係数 $E_0,\ldots,E_n$ によって決まる0または正の整数を取る関数 $c(E(X))$ が係数の評価を与えるとは、

$c(E(X)) \geq b(E(X))$ なる時に言う。 .....(4.35)

ここで必要であるのは、係数の評価を与える関数 c である。

具体的には、c は次の様に取れる。

補題 4.2 上記の係数の評価を与える関数 c として、次が取れる。

(1) d が Archimedean の時

$$c(E(X)) = ({}_nC_n)^{1/2} \cdot (d(E_0)^2 + \ldots + d(E_n)^2)^{1/2} \quad .....(4.36)$$

即ち、$L_{n,k}$ の元 $E(X)$ に対しては、

$$c(E(X)) = ({}_nC_n)^{1/2} \cdot d_L(E(X)) \quad .....(4.37)$$

(2) d が non-Archimedean の時

$$c(E(X)) = \max\{ d(E_0),\ldots, d(E_n) \} \quad .....(4.38)$$

即ち、$L_{n,k}$ の元 $E(X)$ に対しては、

$$c(E(X)) = d_L(E(X)) \quad .....(4.39)$$

証明: d が Archimedean の時は、定理 2.1 によりRはCに埋め込むことができ、更には d はCでの絶対値と同値である。従って、R = Cの時の議論が使えM.Mignotte [14] により、(1) は言える。

d が non-Archimedean の時は、以下の様にして証明される。

$M = \max\{ d(E_0),\ldots, d(E_n) \}$ とおく。

$E(X)$ の任意の因子 $D(X)$ に対して、そのコファクターを $D'(X)$ とする。即ち、$E(X) = D(X) \cdot D'(X)$ とする。ここで、degree $D(X) = m$とする。

この時、$M \geq d(D_i)$ を言えばよい。

$d(D_i)$ が最大になる i のうち最大なものを i' とおく。

また、$d(D'_j)$ が最大になる j のうち最小なものを j' とおく。

$$E_{i'+j'} = \Sigma D_i \cdot D'_j = D_{i'} \cdot D'_{j'} + \Sigma' D_i \cdot D'_j$$

ここで、Σは $i+j = i'+j'$ なる i, j を動き、Σ' は $i+j = i'+j'$ かつ $(i, j) \neq (i', j')$ なる i, j を動く。

この時、$i < i'$ または $j > j'$ ならば、$d(D_i \cdot D'_j) < d(D_{i'}) \cdot d(D'_{j'})$

よって、$d(\Sigma' D_i \cdot D'_j) < d(D_{i'}) \cdot d(D'_{j'})$ である。

このことより、$d(D_{i'}\cdot D'_{j'}) \leqq \max\{d(E_{i'-j'}), d(\Sigma' D_i\cdot D'_j)\}$

よって、これは、$d(E_{i'-j'}) \geqq d(D_{i'}\cdot D'_{j'})$を意味し、特に

$M \geqq d(E_{i'-j'}) \geqq d(D_{i'})$ となり、(2) を得る。 #

上記で得た、係数の評価を与える関数 c を用いて、$L_{m,k}$ のkを次の様に定める。

$$d(a)^{hk} > d_L(F(X))^n\cdot(\delta\cdot c(F(X)))^n \quad .....(4.40)$$

ここで、δは$L_{m,k}$ により決まるδ_m の最大値とする。($h\leqq m\leqq n$)

この時、次の定理が言える。

定理 4.4 $L_{n,k}$ に対して、小さいノルムの格子点 Z(X) は定理 4.3 の仮定 (4.22)を満たす。よって、$G_0(X)$ は Z(X) の因子である。

更に、$h\leqq m\leqq n$なるmに対して、$L_{m,k}$ より得られた小さいノルムの格子点 $Z_m(X)$ に対し、$Z_m(X)$ が初めて (4.22) を満たすmをsとする。

この時、$s = \text{degree } G_0(X)$であり、$Z_s(X) = r\cdot G_0(X)$ となる。 .....(4.41)

ここで、r はRの元である。

証明: 最初に$L_{n,k}$ の小さいノルムの格子点 Z(X) が定理 4.3 の仮定 (4.22) を満たすことを言う。

$G_0(X)$ は$L_{n,k}$ の元であるので、

$$d_L(Z(X)) \leqq \delta\cdot d_L(G_0(X)) \quad .....(4.42)$$

よって、(4.40) 及び (4.42) と係数の評価関数を用いて、

$$d_L(F(X))^n\cdot d_L(Z(X))^n \leqq d_L(F(X))^n\cdot(\delta\cdot d_L(G_0(X)))^n$$
$$\leqq d_L(F(X))^n\cdot(\delta\cdot c(F(X)))^n < d(a)^{hk} \quad .....(4.43)$$

即ち、Z(X) は (4.22) を満たす。

次に $Z_m(X)$ を考える。もし、$L_{m,k}$ に $G_0(X)$ が属するならば、小さいノルムの格子点 $Z_m(X)$ は (4.42) を満たす。即ち、$G_0(X)$ は $Z_m(X)$ の因子となる。

しかし、$Z_{s-1}(X)$ は (4.22) を満たさないことより、$G_0(X)$ は$L_{s-1,k}$ には属さず、$L_{s,k}$ に属することになる。これは、$G_0(X)$ の次数がsに等しいことを意味し、(4.41) を得る。 #

以上により、F(X) が無平方の場合の因数分解法が示された。まとめると以下の様になる。

アルゴリズム 4.1 (仮定 4.1, 4.2)

(i) mod α での因数分解

（必要あらば、αを取り替えて、mod αでの重複因子にならない因子を取る）

(ii) Hensel 構成

ここで（4.39）を満たすようにkをとる。

(iii) Finding a True Factor

R-格子$L_{m,k}$を作り、その小さいノルムの格子点を求める。

小さいノルムの格子点に対して、（4.22）を満たすかどうか調べる。

最初に満たすmに対して、その小さいノルムの格子点の原始的部分が求めるR上の既約因子となる。

さて、F(X) が重複因子を持つ場合についての因数分解法を述べる。

F(X) に対して次の判別式（discriminant）を考える。

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

f がαに属さない時

この時 F(X) は mod α で無平方、即ち重複因子を持たない。

$f \neq 0$ かつ f がαに属する時

$\alpha' = \langle a' \rangle$ 素イデアルで $a' \mid R$ なる α' に取替れば、

f(X) は mod α' で無平方となる。

$f = 0$ の時

F'(X) $\neq 0$ 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 R = $s \neq 0$ 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 $G(X) = \sum_{i \geq 0} G_i X^i$、$G_0(X) = \sum_{i \geq 0} G_{0,i} X^i$ とおくと $G_i = (G_{0,i})^s$

である。よってR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、無平方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得る。

アルゴリズム 4.2（仮定 4.1, 4.2）

（i）無平方化の操作

（ii）mod α での因数分解

（iii）Hensel 構成

ここで（4.39）を満たすようにkをとる。

(iv) Finding a True Factor

R-格子$L_{m,k}$を作り、その小さいノルムの格子点を求める。

小さいノルムの格子点に対して、（4.22）を満たすかどうか調べる。

最初に満たすmに対して、その小さいノルムの格子点の原始的部分が求めるR上の既約因子となる。

（v）無平方化の操作の逆操作

（char R $\neq$ 0 の時は、s 乗根を求めるアルゴリズムがあれば、既約因子を出すことができる）

以上で Euclid 付値環上の一変数多項式の因数分解アルゴリズムへの格子論法の応用を示したが、一般の Euclid 環に対しては、次の仮定の下で可能となる。

仮定 4.3 d の性質について:（補題 2.1 に対応）

Rのノルム d は次を満たす。

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。

$$d(\prod_{i=1}^{m} m_i) \geq C_{0,t}(d(m_1),..,d(m_t)) \qquad .....(4.44)$$

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

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

$$d(\det M) \leq C_{1,m}(d(M_1),...,d(M_m)) \qquad .....(4.45)$$

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

仮定 4.2' 小さいノルムの格子点を求めるアルゴリズムについて:

R-格子Lの基底Mが与えられた時に、小さいノルムの格子点を求めるアルゴリズムが存在して、小さいノルムの格子点 Z を計算する。ここで、mはLの次元とする。更に、任意のLの元 Z' に対して、ある関数 C_2 が存在して、

$$d_L(Z) \leq C_2(m) \cdot d_L(Z') \text{ となる。} \qquad .....(4.46)$$

ここで $C_2 : Z \rightarrow Z^+$ 単調増加の関数

仮定 4.4 係数の評価について:（補題 4.2 に対応）

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。

ここで、n は F(X) の次数であり、d_L は（4.20）の様に定義した格子のノルムとする。

$$d_L(G_0(X)) \leq C_3(n, d_L(F(X))) \qquad .....(4.47)$$

ここで、$C_3 : Z^2 \to Z^+$ なる単調増加関数

例 4.1 R が Archimedean である時、$C_{0,t}$ 及び $C_{1,m}$, C_2, C_3 は次のようにとれる。（補題 2.2 参照）

$$C_{0,t}(d(m_1),\ldots,d(m_t)) = \prod_{i=1}^{t} d(m_i) \qquad .....(4.48)$$

$$C_{1,m}(d(M_1),\ldots,d(M_m)) = \prod_{i=1}^{t} d(M_i) \qquad .....(4.49)$$

$$C_2(m) = 2^{(m-1)/2} \qquad .....(4.50)$$

$$C_3(n, f) = ({}_{2n}C_n)^{1/2} \cdot f \qquad .....(4.51)$$

例 4.2 R が non-Archimedean である時、$C_{0,t}$ 及び $C_{1,m}$ 上は、それぞれ（4.48）と（4.49）に同じで、C_2, C_3 は次のようにとれる。

（補題 2.2 及び補題 4.2 参照）

$$C_2(m) = 1 \qquad .....(4.52)$$

$$C_3(n, f) = f \qquad .....(4.53)$$

定義 4.6 以下のように C_0, C_1 を定義する。

$$C_0(t, D) \equiv C_{0,t}(D,\ldots, D) \qquad .....(4.54)$$

$$C_1(i, D_1, m-i, D_2) \equiv C_{1,m}(\underbrace{D_1,\ldots, D_1}_{i}, \underbrace{D_2,\ldots, D_2}_{m-i}) \qquad .....(4.55)$$

以上の仮定 4.1, 4.2', 4.3, 4.4 の下で、Euclid 環に対して次が言える。

定理 4.5 Euclid 環上の一変数多項式に対して Hensel 構成ができる。

証明は定理 4.1 の場合と同じで省略する。

そこで、F(X) を R 上のモニックかつ無平方である一変数多項式とし、R/α 上での F(X) の既約因子で、重複因子でないものを一つ取り、それを $H_1(X)$ とおく。

ここで、degree F(X) = n かつ degree $H_1(X)$ = h とおく。

この時、定理 4.2, 4.3, 4.4 及び補題 4.1 に対応して次が言える。証明は全く同様である。

定理 4.6 定理 4.2 が Euclid 環に対して、言える。

ここで、記号は定理 4.2 のものを使うことにする。

補題 4.3 $L_{m,k} = \{ E(X) \mid \text{degree } E(X) \leq m$ かつ $H(X) \mid E(X) \bmod \alpha^k \}$ はR-格子である。(補題 4.1 に対応)

定理 4.7 $L_{m,k}$ に対して、$L_{m,k}$ の元 $Z(X)$ が次の条件を満たすとする。

$$C_1(m, d(F(X)), n, d(Z(X))) < C_0(h, d(\alpha^k)) \quad .....(4.56)$$

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

(定理 4.3 に対応)

定理 4.8 α^k の k を次を満たすようにとる。

$$C_1(n, d(F(X)), n, C_2(n + 1) \cdot C_3(n, d(F(X))) < C_0(h, d(\alpha^k)) \quad .....(4.57)$$

この時 $m = h,..,n-1$ に対して$L_{m,k}$ を作り、小さいノルムの格子点 $Z_m(X)$ を求める。この $Z_m(X)$ がはじめて定理 4.7 の (4.56) を満たすmに対して、$Z_m(X)$ は $F(X)$ の既約因子 $G_0(X)$ の定数 (即ちRの元)倍になる。(定理 4.4 に対応)

定理 4.7 および定理 4.8 の証明については、定理 4.3 および定理 4.4 の証明中の不等式に上記の評価関数を代入することにより得られる。

以上の定理により、仮定 4.1, 4.2', 4.3, 4.4 の下でアルゴリズム 4.1 及びアルゴリズム 4.2 と同様なアルゴリズムが存在することが判る。

例 4.3 RがZまたは GF(q) [x] である時、仮定 4.1 および仮定 4.2 を満たすことが判る。仮定 4.1 は有限体上の一変数多項式の因数分解アルゴリズムの存在により言え、仮定 4.2 は例 2.1 及び例 2.2 により言える。これらは、A.K.Lenstra によるアルゴリズムに他ならない。

5 具体的応用について

Euclid 付値環の具体的な例として、先の節で挙げた整数環Zや GF(q)上の一変数多項式環以外には次が挙げられる。

(1) 一般の体上の一変数多項式環 (non-Archimedean Euclid 付値環)

(2) 二次体 (Archimedean Euclid 付値環)

(1) に関しては、体が有限体の場合は、計算の途中での係数膨張がないので格子算法は有利であるが、一般に無限体の場合には、係数膨張がおこり得るので格子算法における係数膨張を調べる必要がある。特にＧＣＤにおいては、格子の基底簡約アルゴリズムは本質的には Euclid の互助法に他ならないことから、この係数膨張はかなり起こり得ることが予想される。

(2) に関しては、二次体を計算する上で、その環上の演算をどの様に計算機用に定義するかが問題である。更に、一般的な Euclid 環においても、同様である。

最後に、因数分解における格子算法の位置付けについて述べておく。ここで述べた格子算法は、Berlekamp-Zassenhaus 流のアルゴリズムの中の、真の因子の算出のみに応用されている。(E.R.Berlekamp〔3〕及び H.Zassenhaus〔18〕参照)

多くの格子算法に関する研究はこの位置付けの下でなされている。しかし、因数分解そのものに、直接的に格子を利用した方法が A.K.Lenstra〔10〕および A.K.Lenstra と van der Hulst〔11〕により研究されている。よって、格子についての応用研究は今後より広範囲でなされることが予想される。

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。

参考文献

〔1〕 Berlekamp, E.R. : Factoring Polynomials over Finite Fields, Bell Syst. Tech. J., Vol. 46 (1967), pp. 1853-1859.

〔2〕 Berlekamp, E.R. : Algebraic Coding Theory, McGraw-Hill, 1968.

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

〔4〕 藤崎源二郎：体と Galois 理論Ⅲ，岩波講座 基礎数学，岩波書店，1978.

〔5〕 Kaltofen, E. : On the Complexity of Finding Short Vectors in Integer Lattices, Lecture Note in Comp. Sci., Vol. 162 (1983), pp. 236-244.

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

〔7〕 Lenstra, A.K. : Lattice and Factorization of Polynomials over Algebraic Number Fields, Lecture Note in Comp. Sci., Vol. 144 (1982), pp. 32-39

〔8〕 Lenstra, A.K. : Factoring Multivariate Integral Polynomials, Lecture Note in Comp. Sci., Vol. 154 (1983), pp. 458-465.

〔9〕 Lenstra, A.K. : Factoring Polynomials over Algebraic Number Fields, Lecture Note in Comp. Sci., Vol. 162 (1983), pp. 245-254.

〔10〕 Lenstra, A.K. : Polynomial Factorization by Root Approximation, Lecture Note in Comp. Sci., Vol. 174 (1984), pp. 272-244.

〔11〕 Lenstra, A.K. : Factoring Multivariate Polynomials over Algebraic Number Fields, Lecture Note in Comp. Sci., Vol. 176 (1984), pp. 389-396.

〔12〕 Lenstra, A.K. : Factoring Multivariate Polynomials over Finite Fields, J. Comput. and Syst. Sci., Vol. 30 (1985), pp. 235-248.

〔13〕 Lenstra, A.K. and van der Hulst, M. : Factorization of Polynomials by Transcendental Evaluation, Lecture Note in Comp. Sci., Vol. 204 (1985), pp. 138-145.

〔14〕 Mignotte, M. : An Inequalities About Univariate Polynomials, Math. Comp., Vol. 28 (1974), pp. 1153-1157.

〔15〕 佐々木建昭 : 数式処理，情報処理叢書7，情報処理学会，1981.

(16) von zur Gathen, J. : Parallel Algorithm for Algebraic Problems, SIAM J. Comput., Vol. 13 (1984), pp. 802-824.

(17) von zur Gathen, J. : Hensel and Newton Methods in Valuation Rings, Math. Comp., Vol. 42 (1984), pp. 637-661.

(18) Zassenhaus, H. : On Hensel Factorization. I, J. Number Theory, Vol. 1 (1963), pp. 291-311.