

1.

逐次代数拡大体上での 1 変数多項式の
GCD について

富士通情報研 野呂 正行

1.1 はじめに

有理数体上の単拡大上での 1 変数多項式の GCD をモジュラ計算法は, [7] により与えられ, [8] により改良された. しかし, 逐次拡大の形で与えられた係数体上での 1 変数多項式の GCD 計算を行なうために逐次拡大を単拡大に変換することは, 定義多項式の次数, 係数の増大を招き, 結果として, GCD 計算に多大な時間, 空間を必要とすることになる. 本稿では, 逐次拡大のまま, GCD のモジュラ計算を行なう方法を述べる.

(発表後, [6] で既に同様のアルゴリズムが発表されていることが判明した. [6] では, 漸近計算量を良くする目的で, [2] による dynamic evaluation を用いたアルゴリズムを提案しているが, 基本とする, 判別式に関する性質は我々と同じものを用いていて, しかも, その性質は, [1] により既に得られていることも判明した.)

1.2 判別式

$K_0 = \mathbb{Q}$, α_i ($i = 1, \dots, n$) を, K_{i-1} 上代数的とし, $K_i = K_{i-1}(\alpha_i)$ とする. $K_i = K_{i-1}[\alpha_i] = \mathbb{Q}[\alpha_i, \dots, \alpha_i]$ である. K_n の整数環を R_n とし, $K = K_n$, $R = R_n$ とする.

有限次代数拡大 K/F に対し, $\beta \in K$ の K/F に関するノルムを $N_{K/F}(\beta)$ と書く.

$K/\mathbb{Q}$ を m 次拡大とすると m 個の共役写像 σ_i による $\alpha \in F$ の像を $\alpha^{(i)}$ と書く.

$\{\beta_1, \dots, \beta_m\} \subset K$ に対し,

$$D(\beta_1, \dots, \beta_m) = \begin{pmatrix} \beta_1^{(1)} & \beta_2^{(1)} & \dots & \beta_m^{(1)} \\ \vdots & \vdots & & \vdots \\ \beta_1^{(m)} & \beta_2^{(m)} & \dots & \beta_m^{(m)} \end{pmatrix}$$

と定義する.

α_i の K_{i-1} 上のモニックな最小多項式を $m_i(x) \in Q[\alpha_{i-1}, \dots, \alpha_1][x]$ とする.

このとき, $m_i(x)$ において, $x \mapsto t_i, \alpha_j \mapsto t_j$ ($j = 1, \dots, i-1$) という置き換えを行ったものを $M_i(t_i, \dots, t_1)$ と書けば,

$$K_i = Q[t_i, \dots, t_1]/I_i$$

$$(I_i = \text{Ideal}(M_i(t_i, \dots, t_1), \dots, M_1(t_1))).$$

以下では, $M_i \in Z[t_i, \dots, t_1]$ なる場合を考える. このとき $m_i(x) \in Z[\alpha_{i-1}, \dots, \alpha_1][x]$ で, モニックな多項式となる.

命題 1 α_i は代数的整数.

Proof $\alpha_1, \dots, \alpha_{i-1}$ が代数的整数ならば, $m_i(x)$ の各係数は $Z[\alpha_{i-1}, \dots, \alpha_1]$ の元だから代数的整数. よって α_i は, 代数的整数を係数とするモニック多項式の根となり, 代数的整数. $\square$

命題 2 $e_i = \deg(m_i(x)), d_i = \text{disc}_{K_i/K_{i-1}}(\alpha_i), D = \prod_{i=1}^n N_{K_{i-1}/Q}(d_i) \prod_{j=i+1}^n e_j$ とおけば, $R \subset \frac{1}{D} Z[\alpha_n, \dots, \alpha_1]$.

Proof $G = \{\prod_{j=1}^n \alpha_j^{n_j} | 0 \leq n_j < e_j\} \subset R$ は K/Q の Q ベクトル空間としての基底より, G を適当に整列したベクトルを $(\gamma_1, \dots, \gamma_m)$ とすると, $\theta \in R$ は, 適当な $c_j \in Q$ により $\theta = \sum_j c_j \gamma_j$ と書ける.

これより,

$$\theta^{(1)} = \sum_j c_j \gamma_j^{(1)}$$

...

$$\theta^{(m)} = \sum_j c_j \gamma_j^{(m)}$$

これを, $(c_1, \dots, c_m)$ に関する方程式と見て解くと,

$$c_j = \Delta_j / \Delta = \Delta \Delta_j / \Delta^2.$$

ここで,

$$\Delta_j = \det(D(\gamma_1, \dots, \gamma_{j-1}, \theta, \gamma_{j+1}, \dots, \gamma_m)),$$

$$\Delta = \det(D(\gamma_1, \dots, \gamma_m)).$$

一般に $\beta_1, \dots, \beta_m \in R$ ならば, $\det(D(\beta_1, \dots, \beta_m))^2 \in Z$ より $\Delta^2 \in Z$. よって, $\Delta \Delta_j = \Delta^2 c_j \in Q$ かつ Δ, Δ_j は代数的整数だから, $\Delta \Delta_j \in Z$. よって, $c_j \in \frac{1}{\Delta^2} Z$. θ は任意だから $R \subset \frac{1}{\Delta^2} Z[\alpha_n, \dots, \alpha_1]$. $\{\prod_{j=1}^{n-1} \alpha_j^{n_j} | 0 \leq n_j < e_j\} \subset R$ を適当に整列したものを改めて $\Gamma = (\gamma_1, \dots, \gamma_l)$ (l は K_{n-1}/Q の拡大次数) とする. 見やすくするため, α_n を α, e_n を e, K_{n-1} を $F, m_n(x)$ を $m(x)$ と書く.

$$\Delta = \det(D(\Gamma, \alpha \Gamma, \alpha^2 \Gamma, \dots, \alpha^{e-1} \Gamma))$$

σ を K/Q の共役写像とすれば, $\sigma|_F$ は F/Q の共役写像より, その個数は l 個. そのそれぞれに対し, K への拡張が e 個ずつある.

$\sigma(\Gamma) = \Gamma^{(t)}$ なる e 個の σ による α の像を α_{ts} ($s = 1, \dots, e$) とする. この時, $m(x) = \sum_i c_i(\Gamma)x^i$ とすれば, $\{\alpha_{ts} | (s = 1, \dots, e)\}$ は $m^{(t)}(x) = \sum_i c_i(\Gamma^{(t)})x^i$ の根全体となる.

$$D(\Gamma, \alpha\Gamma, \alpha^2\Gamma, \dots, \alpha^{e-1}\Gamma) = \begin{pmatrix} G_1 \\ G_2 \\ \vdots \\ G_l \end{pmatrix}$$

ただし,

$$G_k = \begin{pmatrix} \Gamma^{(k)} & \Gamma^{(k)}\alpha_{k1} & \dots & \Gamma^{(k)}\alpha_{k1}^{e-1} \\ \vdots & \vdots & & \vdots \\ \Gamma^{(k)} & \Gamma^{(k)}\alpha_{ke} & \dots & \Gamma^{(k)}\alpha_{ke}^{e-1} \end{pmatrix}$$

Δ を計算する際, 各 G_k に対し, $\Gamma^{(k)}$ を係数と見なして, vandermonde 行列に対するのと同様な掃き出しを行なうことができる. すなわち行に対する基本変形により, G_k は次の行列 $\delta_k H_k$ に変形できる.

ただし,

$$H_k = \begin{pmatrix} \Gamma^{(k)} & * & * & * \\ 0 & \Gamma^{(k)} & * & * \\ \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \Gamma^{(k)} \end{pmatrix}$$

$$\delta_k = \begin{vmatrix} 1 & \alpha_{k1} & \dots & \alpha_{k1}^{e-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_{ke} & \dots & \alpha_{ke}^{e-1} \end{vmatrix}$$

よって,

$$\Delta = \prod_k \delta_k \begin{vmatrix} H_1 \\ H_2 \\ \vdots \\ H_l \end{vmatrix} = \pm \prod_k \delta_k \det(D(\Gamma))^e$$

既に述べたことより, $\{\alpha_{ks} | (s = 1, \dots, e)\}$ は $m^{(k)}(x)$ の根全体だから,

$$\begin{aligned}
\delta_k^2 &= \text{disc}_{K/F} m^{(k)}(x) \\
&= \text{resultant}_x(m^{(k)}(x), \frac{d}{dx} m^{(k)}(x)) \\
&= (\text{disc}_{K/F} m(x))^{(k)}
\end{aligned}$$

よって,

$$\Delta^2 = N_{F/Q}(\text{disc}_{K/F} m(x)) \det(D(\Gamma))^{2e}$$

よって帰納法により

$$\Delta^2 = \prod_{i=1}^n N_{K_{i-1}/Q}(\text{disc}_{K_i/K_{i-1}} m_i(x)) \prod_{j=i+1}^n \epsilon_j \quad \square$$

補題 3/3/

$f \in \frac{1}{a}R[x]$, $a \in Z$, $f = gh$, f, g, h : モニックならば, $g, h \in \frac{1}{a}R[x]$.

系 4 $f \in \frac{1}{a}Z[\alpha_n, \dots, \alpha_1][x]$, $a \in Z$, $f = gh$, f, g, h : モニックならば, $g, h \in \frac{1}{aD}Z[\alpha_n, \dots, \alpha_1][x]$.

系 5 $f_1 \in \frac{1}{a}Z[\alpha_n, \dots, \alpha_1][x]$, $f_2 \in \frac{1}{b}Z[\alpha_n, \dots, \alpha_1][x]$, $a, b \in Z$, $g = \text{GCD}(f_1, f_2)$, f_1, f_2, g : モニックならば,

$$g \in \frac{1}{\text{GCD}(a, b)D}Z[\alpha_n, \dots, \alpha_1][x].$$

1.3 モジュラ計算

補題 6 α_i の Q 上の最小多項式を $h(x)$ とすれば, $N_{K_i/Q}(x - \alpha_i)$ は $h(x)$ の冪となる.

Proof 既約多項式のノルムが, 既約多項式の冪になることからわかる. $\square$

$p \in Z$ を素数とする.

$$S = Z[t_n, \dots, t_1],$$

$$\bar{S} = Z_p[t_n, \dots, t_1],$$

S から $\bar{S}$ への標準的射影による f の像を $\bar{f}$ と書く.

$$I_Q = \text{Ideal}(M_n(t_n, \dots, t_1), \dots, M_1(t_1)) \subset Q[t_n, \dots, t_1],$$

$$I = \text{Ideal}(M_n(t_n, \dots, t_1), \dots, M_1(t_1)) \subset S,$$

$$\bar{I} = \text{Ideal}(\bar{M}_n(t_n, \dots, t_1), \dots, \bar{M}_1(t_1)) \subset \bar{S}$$

$$\phi: \bar{S}[x] \rightarrow (\bar{S}/\bar{I})[x] \text{ (標準的射影)}$$

とおく.

補題 7 α_i の Q 上の最小多項式を $h_i(x) \in Z[x]$ とすれば, $h_i(t_i) \in I$.

Proof $h_i(\alpha_i) = 0$ で, I は極大イデアルだから $h_i(t_i) \in I_Q$. M_i は I_Q の, $t_n > \dots > t_1$ なる辞書式順序に関するグレブナ基底となっていて, $h_i(t_i)$ の 0 への正規化を考えれば, M_i の頭項が 1 で, 整数

係数であることより正規化に現れる係数は全て整数. よって $h_i(t_i) \in I$. $\square$

命題 8 $p \nmid \text{disc}(h_i(x)) (i = 1, \dots, n)$ ならば, $\bar{I}$ は極大イデアルの交わり. 特に $\bar{I}$ は radical.

Proof $h_i(t_i) \in I$ より $\bar{h}_i(t_i) \in \bar{I}$. $\text{disc}(\bar{h}_i(x)) = \text{disc}(h_i(x)) \bmod p \neq 0$ より, 各 t_i に対し, 無平方な t_i の 1 変数多項式が $\bar{I}$ の中に存在する. $\bar{I}$ は 0 次元だから, Seidenberg の補題 92 [4] により $\bar{I}$ は極大イデアルの交わりとなる. $\square$

補題 9 $\bar{I} = \cap J_k$ (J_k は相異なる極大イデアル) とし, $f_1, f_2 \in (\bar{S}/\bar{I})[x]$ かつ $lc(f_1), lc(f_2)$ は単元とする. この時次の性質を満たす g が $\bar{S}/\bar{I}$ の単元倍を除いて一意的に存在する. この g を $GCD(f_1, f_2)$ と定義する.

(1) $g|f_1, g|f_2$

(2) $h|f_1, h|f_2$ ならば $h|g$

Proof $j \neq k$ ならば $J_j + J_k = \bar{S}$ より, 中国剰余定理により $\psi : \bar{S}/\bar{I} \simeq \oplus_k \bar{S}/J_k$. よって, $\psi : (\bar{S}/\bar{I})[x] \simeq \oplus_k (\bar{S}/J_k)[x]$.

$\psi_k : (\bar{S}/\bar{I})[x] \rightarrow (\bar{S}/J_k)[x]$ を標準的射影とする. $f \in (\bar{S}/\bar{I})[x]$ に対し, $f = 0 \Leftrightarrow \forall k \psi_k(f) = 0$ が成り立つ.

$lc(f_1), lc(f_2)$ は単元より, $\psi_k(f_1), \psi_k(f_2) \neq 0$. よって, $(\bar{S}/J_k)[x]$ は体上の多項式環より, $(\bar{S}/J_k)[x]$ における f_1, f_2 の モニックな GCD が一意的に存在する. それを g_k とおき, $g = \psi^{-1}(g_1, \dots, g_k, \dots)$ と定義する. この時 g が (1), (2) を満たすことを示す.

(1) : $\exists h_k \in (\bar{S}/J_k)[x]$ s.t. $\psi_k(f_1) = \psi_k(g)h_k$. $h = \psi^{-1}(h_1, \dots, h_k, \dots)$ とすれば, $f_1 = gh$ より $g|f_1$. 同様に $g|f_2$.

(2) : $\psi_k(h)|\psi_k(g)$ が $(\bar{S}/J_k)[x]$ における GCD の存在と一意性によりいえるから, (1) と同様に $h|g$ となる.

一意性 : g_1 が (1) を満たすとする, $g|g_1$ かつ $g_1|g$. これより $\psi_k(g)|\psi_k(g_1)$ かつ $\psi_k(g_1)|\psi_k(g)$. よって, $\exists c_k \in \bar{S}/J_k \setminus \{0\}$ s.t. $\psi_k(g_1) = c_k \psi_k(g)$. よって, $c = \psi^{-1}(c_1, \dots, c_k, \dots)$ とおけば, c は $\bar{S}/\bar{I}$ の単元で, $g_1 = cg$. $\square$

$f_1 \in \frac{1}{a}Z[\alpha_n, \dots, \alpha_1][x]$, $f_2 \in \frac{1}{b}Z[\alpha_n, \dots, \alpha_1][x]$, $a, b \in Z$, $g = GCD(f_1, f_2)$, f_1, f_2, g : モニックとする.

$f_1 = gh_1$ なる h_1 をとれば, $g, h_1 \in \frac{1}{aD}Z[\alpha_n, \dots, \alpha_1][x]$. これより

$F_1 = (aD)^2 f_1$, $G_1 = aDg$, $H_1 = aDh_1$ とおけば, $F_1, G_1, H_1 \in Z[\alpha_n, \dots, \alpha_1][x]$ で, $F_1 = G_1 H_1$.

この等式を $Q[t_n, \dots, t_1][x]$ 上で見れば, 両辺が $\bmod I_Q$ で等しいことを意味するが, 正規化操作を考えれば $\bmod I$ で等しいことがわかる. よって,

$$\phi(\bar{F}_1) = \phi(\bar{G}_1)\phi(\bar{H}_1).$$

同様に, $F_2 = (bD)^2 f_2$, $G_2 = bDg$, $H_2 = bDh_2$ とおけば, $F_2, G_2, H_2 \in Z[\alpha_n, \dots, \alpha_1][x]$ で,

$$\phi(\bar{F}_2) = \phi(\bar{G}_2)\phi(\bar{H}_2).$$

仮定 10 素数 p が, $p \nmid a, p \nmid b, p \nmid \text{disc}(h_i(x)) (i = 1, \dots, n)$ を満たす.

補題 11 素数 p が, $p \nmid \text{disc}(h_i(x)) (i = 1, \dots, n)$ ならば $p \nmid D$

Proof $D_i = N_{K_i/K_{i-1}}(\text{disc}_{K_i/K_{i-1}}(\alpha_i))$ は α_i の共役の差の重複度付きの積である. α_i は $h_i(x)$ の根より α_i の共役は全て $h_i(x)$ の根. $\text{disc}(h_i(x))$ は, α_i の共役すべての差積の 2 乗だから, 自然数 E が存在して, 代数的整数として $D_i | \text{disc}(h_i(x))^E$. 両辺は有理整数だから, 有理整数として $D_i | \text{disc}(h_i(x))^E$. よって D の素因子はいずれかの $\text{disc}(h_i(x))$ の素因子となる. $\square$

この補題により, p が仮定 10 を満たせば, D が $\text{mod } p$ で単元であることがいえる.

補題 12 p が仮定 10 を満たす時, $g_0 = \text{GCD}(\phi(\bar{F}_1), \phi(\bar{F}_2))$ が存在して $\phi(\bar{G}_1) | g_0$ かつ $\deg(g_0) \geq \deg(g)$.

Proof $\phi(\bar{F}_k)$ の主係数が単元だから, 補題 9 より GCD が一意的に存在する. $\phi(\bar{G}_1), \phi(\bar{G}_2)$ は同伴より $\phi(\bar{G}_1) | g_0$ が言えるが, $\phi(\bar{G}_1)$ の主係数が単元より $\deg(g_0) \geq \deg(\phi(\bar{G}_1)) = \deg(g)$. $\square$

補題 13 仮定 10 の元で, $\deg(g) = \deg(g_0)$ ならば $\phi(\bar{G}_1)$ と g_0 は同伴.

Proof $\deg(g_0) = \text{MAX}(\deg(g_{0k}) \ (g_{0k} = \psi_k(g_0) = \text{GCD}(\psi_k(\phi(\bar{F}_1)), \psi_k(\phi(\bar{F}_2))))$ より, $\deg(g) = \deg(g_0)$ ならば, $\forall k \deg(g_{0k}) \leq \deg(g)$. 一方で, $\psi_k(\phi(\bar{G}_1)) | g_{0k}$ より $\deg(g) \leq \deg(g_{0k})$. よって $\forall k \deg(g_{0k}) = \deg(g)$. よって g_{0k} の主係数は単元となり g_0 の主係数も単元. $g_0 = \phi(\bar{G}_1)h_0$ とすれば, h_0 は単元. $\square$

$f_1, f_2 \in S[x]$ に対し, p が仮定 10 を満たすとする.

$$J_Q = \text{Ideal}(f_1, f_2, M_n, \dots, M_1) \subset Q[t_n, \dots, t_1][x]$$

$$J = \text{Ideal}(f_1, f_2, M_n, \dots, M_1) \subset S[x]$$

$$\bar{J} = \text{Ideal}(\bar{f}_1, \bar{f}_2, \bar{M}_n, \dots, \bar{M}_1) \subset \bar{S}[x]$$

とおく.

補題 14 $\exists g(x, t_n, \dots, t_1) \in S[x], l_{c_x}(g) \in Z \text{ s.t. } \text{GB}(J_Q) = \{g, M_n, \dots, M_1\}$. $g(x, \alpha_n, \dots, \alpha_1) = \text{GCD}(f_1(x, \alpha_n, \dots, \alpha_1), f_2(x, \alpha_n, \dots, \alpha_1))$.

補題 15 $\exists g \in \bar{S}[x] \text{ s.t. } \bar{J} = \text{Ideal}(g, \bar{M}_n, \dots, \bar{M}_1)$ ならば, $\phi(g) = \text{GCD}(\phi(\bar{f}_1), \phi(\bar{f}_2))$ 即ち $\phi(\bar{f}_1), \phi(\bar{f}_2)$ に対し, 補題 9 の (1), (2) を満たす.

Proof $\bar{J} = \text{Ideal}(g, \bar{M}_n, \dots, \bar{M}_1)$ より, $\exists h_1, \exists h_2, \bar{f}_1 \equiv gh_1 \pmod{\bar{I}}, \bar{f}_2 \equiv gh_2 \pmod{\bar{I}}$ より (1) は OK. また, $\exists a_1, \exists a_2, g \equiv a_1\bar{f}_1 + a_2\bar{f}_2 \pmod{\bar{I}}$ より (2) も OK. $\square$

補題 16 g を補題 14 の g とすると, 有限個の p を除いて $\text{GB}(\bar{J}) = \{\bar{g}, \bar{M}_n, \dots, \bar{M}_1\}$.

以上により次の定理が成立する.

定理 17 p が仮定 10 を満たすとき, $\text{GB}(\bar{J}) = \{g_0, \bar{M}_n, \dots, \bar{M}_1\}$ ならば,

$$\deg(g_0) \geq \deg(\text{GCD}(f_1, f_2)).$$

$g(x, t_n, \dots, t_1) \in S[x]$ を $g(x, \alpha_n, \dots, \alpha_1) = \text{GCD}(f_1, f_2)$ かつ $l_{c_x}(g) \in Z, p \nmid l_{c_x}(g)$ なる多項式とすると, 仮定 10 を満たす p のうち有限個を除いて $\text{GB}(\bar{J}) = \{g_0, \bar{M}_n, \dots, \bar{M}_1\}$ かつ $\bar{g}$ と g_0 は同伴で, $\deg(g_0) = \deg(\text{GCD}(f_1, f_2))$.

この定理により, 仮定 10 を満たす素数 p を十分多く用意すればそれらは全て, $\text{GCD}(f_1, f_2)$ の正しいモジュライメージになっている. よって, これらを中国剰余定理により合成して, 有理数上に係数を引き戻し, 試し割りを行なうことにより $\text{GCD}(f_1, f_2)$ を得る.

1.4 タイミングデータ

最小分解体の計算に現れる, 2 根以上添加された体上での GCD 計算を例にとる.

$$f = x^6 + 10x^5 + 55x^4 + 140x^3 + 175x^2 - 3019x + 25$$

$$\alpha_1 = \text{a root of } m_1(x) = f(x)$$

$$\alpha_2 = \text{a root of } m_2(x) = m_1(x)/(x - \alpha_1)$$

$$\alpha_3 = \text{a root of } m_3(x) = m_2(x)/(x - \alpha_2)$$

$$K_2 = Q(\alpha_2, \alpha_1), K_3 = Q(\alpha_3, \alpha_2, \alpha_1)$$

例	係数体	$\deg(f_1)$	$\deg(f_2)$	$\deg(g)$
1	K_2	12	11	6
2	K_2	20	6	4
3	K_3	3	2	1
4	K_2	8	7	0
5	K_2	10	8	4
6	K_3	4	2	1

計算機: Sony NEWS5000 (R4000/50MHz)

単位: 秒

旧: グレブナ基底による GCD 計算

mod: モジュラ+中国剰余定理版

候補: モジュラにおいて, GCD 候補生成にかかった時間

check: 試し割り

段数: 使った素数の個数 (素数は 8 桁の素数を用いている)

単拡大: 原始元により単拡大に変換の後, モジュラで計算 (変換時間は除く; K_3 に対する単拡大表現が求まらなかったため, 例 3, 例 6 は略)

例	旧	mod	候補	check	段数	単拡大	段数
1	173	7.3	6.9	0.36	2	28.7	20
2	624	16.2	11.6	4.5	3	78.7	21
3	23.3	9.8	7.7	2.2	2	—	—
4	222	2.4	2.4	0	1	0.27	1
5	2062	14.1	12.5	1.5	3	45.6	21
6	183	27.6	24.5	3.1	2	—	—

参考文献

- [1]Abbott, J. A., Factorization of Polynomials Over Algebraic Number Fields. PhD thesis, University of Bath(1989).
- [2]Duval, D., Diverse questions relatives au CALCUL FORMEL AVEC DES NOMBRES ALGÈBRIQUES. PhD thesis, L'université scientifique, technologique, et médicale de Grenoble(1987).
- [3]Weinberger, P. J., Rothschild, L. P., Factoring polynomials over algebraic number fields. ACM Trans. Math. Softw, 2/4(1976), 335-350.
- [4]Seidenberg, A., Constructions in algebra. Trans. Amer. Math. Soc. 197 (1974), 272-313.
- [5]Langemyr, L., Algorithms for a Multiple Algebraic Extension. MEGA-90(1990), 235-248.
- [6]Langemyr, L., Algorithms for a Multiple Algebraic Extension II. AAECC-9(1991), 224-233.
- [7]Langemyr, L., MacCallum, S., The computation of polynomial greatest common divisors over an algebraic number field. J. Symb. Comp. 8(1989), 429-448.
- [8]Encarnacion, M., J., On a Modular Algorithm for Computing GCDs of Polynomials Over Algebraic Number Fields. Proc. ISSAC'94(1994), 58-65.