主偏極CMアーベル曲面の井草不変量が満たす類多項式について

高島　克幸
三菱電機 情報技術総合研究所

at JANT 3rd　1/27/2001

位数計算

位数計算アルゴリズムは, 代数曲線を用いた離散対数型暗号には, 必須.

- 楕円曲線
  - SEA (Schoof) アルゴリズム
  - 佐藤アルゴリズム

  } ランダムな曲線の位数計算を実用的計算時間で行う

- 超楕円曲線の場合の取り組み
  - Gaudry,Harley … Schoof の種数 2 バージョンだが, 暗号応用のためには, まだ実用的とは言い難い
  - Buhler,Koblitz
  - Gaudry,Hess,Smart (Weil descent を応用）
  - 趙,松尾,川白,辻井 [CMKT] (CMアルゴリズムの改良)

  } ランダムではないが位数のわかった曲線を, 実用的計算時間で得ることができる.

今回の取り組み

・CM アルゴリズムの改良
　[CMKT]とはアプローチが少し違う.)

　・今回の取り組みと[CMKT]の共通点
　　… CMアルゴリズム中, 一番計算量的困難を伴う ‘類多項式計算 ”をできるだけ高速に行うことを目指す.

　・今回の取り組みと[CMKT]の相違点
　　… [CMKT]では, 級数計算（近似計算）を経ないで類多項式を得ようという試みがなされている.
　　今回の取り組みは,級数計算（近似計算）を用いた場合の計算時間削減をアルゴリズム的工夫によって, 行おうという試みである.

共に, ‘類多項式 ”の持つ数論的性質をアルゴリズム改善に反映させたい！という試み だと思う.

全体の流れ

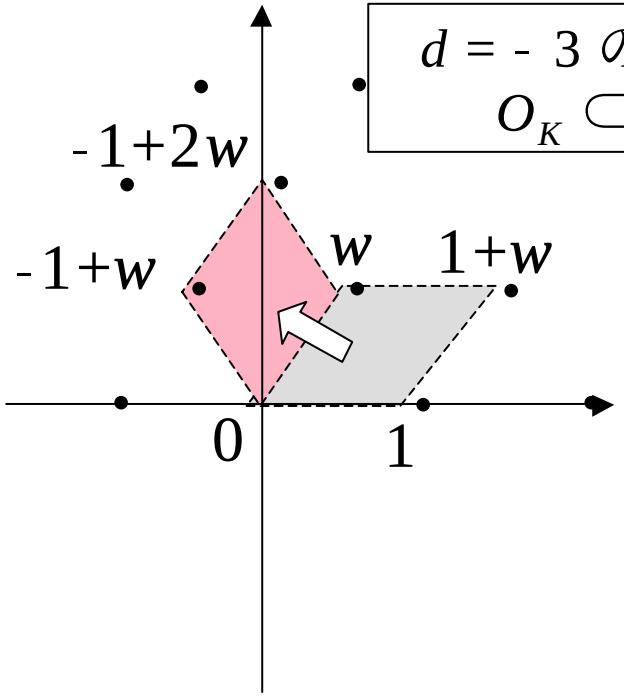
- 楕円曲線CMアルゴリズム (Ⅰ, Ⅱ)
- CMアルゴリズム(Ⅰ, Ⅱ)
- CM体
- 主偏極アーベル曲面
  - CM主偏極アーベル曲面
  - 周期行列の類集合(Ⅰ, Ⅱ)
  - 周期行列の構成(Ⅰ, Ⅱ, Ⅲ)
- 井草類多項式

- 類多項式構成の改良
  - 分母推定アルゴリズム(Ⅰ, Ⅱ)
  - $K_0^*[X]$内可約性による類多項式正当性判定法
  - 定数項分子の相関関係を利用した定数項決定法
  - $c_{4,1}$を利用した$\overline{M}_0$決定法
  - K_0^*の判別式の偶奇性を利用した類多項式構成に適したCM体の選別法
- 実装結果とその効果
- まとめと今後の課題

楕円曲線 CM アルゴリズム（I）

$K = \mathbf{Q}(\sqrt{d}\,)$ ($d < 0$, d : 非平方整数) を虚 2 次体とする.
その 整数環 O_K は, $\mathbf{Z} + \mathbf{Z}w$ ($\mathrm{Im}(w) > 0$) と書ける.

$$w = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \mod 4 \\ (1+\sqrt{d}\,)/2 & \text{if } d \equiv 1 \mod 4 \end{cases}$$



$d = -3$ の時の
$O_K \subset \mathbf{C}$

$w\,O_K \subset O_K$

($d = -3$ の時には,
$w\,w = -1 + w$
$w\,(1+w) = -1 + 2w$)

w は, 楕円曲線 $E = \mathbf{C}/O_K$ の自己準同型を定める. 実際, E の自己準同型全体は, O_K と一致する.

即ち, $O_K \cong \mathrm{End}(E)$.

楕円曲線 CM アルゴリズム（I）

では, $O_K \cong \mathrm{End}(E)$ となる楕円曲線（の同型類）E は, $\mathbf{C}/O_K$ 以外にどれだけあるか？

- O_K のイデアル類群 Cl_K の代表系を, $\boldsymbol{a}_i\ (i = 1, \ldots, h)$ とする.
  O_K と同様に, $\boldsymbol{a}_i\ (\subset \mathbf{C})$ も格子になっている.
  $\mathbf{C}/\boldsymbol{a}_i\ (i = 1, \ldots, h)$ が上記 E 全体を与える.

- $\boldsymbol{a}_i\ (i = 1, \ldots, h)$ から複素上半平面の点 $w_i\ (i = 1, \ldots, h)$ を定める.

- $j(w)$: j 不変量（複素上半平面上の複素数値関数）を用いた以下の多項式が CM 楕円曲線の場合の類多項式.

$$H(X) := \prod_{i=1}^{h} (X - j(w_i)) \qquad \in \mathbf{Z}[X]$$

- $H(X)$ を有限体 $\mathbf{F}$ に還元した方程式を解くことで、有理点位数のわかった $\tilde{E}$ / $\mathbf{F}$ を得る.

CMアルゴリズム（I）

- 楕円曲線 CM アルゴリズム と種数 2 の場合の主な相違点（本発表に関係するもの）
  - j 不変量に対応する井草不変量があり, その類多項式（モニック）も定義されるが, その係数は一般には $\mathbf{Q} \setminus \mathbf{Z}$ の元である.

    ⬇

    有効な近似計算に必要な有効桁数が増え, 計算時間も多くなる.
  - 種数 2 曲線のヤコビアンを考える場合, そのアーベル多様体としての同型類を考えるだけでは不十分で, 主偏極という付加データも必要になる.
  - 種数 2 の場合, $H(X)$ にあたるもの（後に定義する $H_i(X)$ とは異なる）は必ずしも $\mathbf{Q}$ 上既約でない.

CMアルゴリズム（II）

入力: CM 体 K のオーダーO

出力: 有限体 $\mathbf{F}$, 準同型環O のヤコビアンを持つ $\mathbf{F}$上の種数2超楕円曲線$\widetilde{C}$

1. K 内のヴェイユ数の計算から, 適当な有限体 $\mathbf{F}$ と,出力として得られる$\mathbf{F}$上定義された超楕円曲線のヤコビアンの $\mathbf{F}$ 有理点の位数を得る
2. K のイデアル類群,単数群の計算から, 類多項式構成に必要な準同型環 O の主偏極アーベル曲面/ $\overline{\mathbf{Q}}$の周期行列を計算する.
3. テータ零値を用いて各々の周期行列に対応する井草不変量を計算し, $\mathbf{Q}$係数の類多項式を構成する.
4. 類多項式の $\mathbf{F}$ への還元から, 2.のアーベル曲面の $\mathbf{F}$ への還元をヤコビアンに持つ$\mathbf{F}$上の超楕円曲線$\widetilde{C}$ の係数を求める.

CM体 ([K:Q]=4)

- 実2次体 K_0 の総虚2次拡大体 K

  e.g. $K = \mathbf{Q}\left(\sqrt{-(n+\sqrt{m})}\right)$,

  $(m,n \in \mathbf{Z}_{>0}$, m:非平方数, $n^2-m > 0)$

  以後, この CM 体を(m,n)で表す.

拡大 $K/\mathbf{Q}$ は次のいずれか

拡大1. K /**Q**:ガロアで, $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$

拡大2. K /**Q**:ガロアで, $\mathrm{Gal}(K/\mathbf{Q}) \cong \mathbf{Z}/4\mathbf{Z}$

拡大3. K /**Q**:非ガロアで, そのガロア閉包を L とした時,

$\mathrm{Gal}(L/\mathbf{Q}) \cong D_4$ (位数8の2面体群)

主偏極アーベル曲面

- アーベル曲面 A と主偏極 Y の対 (A, Y) のことを主偏極アーベル曲面という.
- 種数 2 の超楕円曲線 C のヤコビアン Jac$C$ は,主偏極アーベル曲面 $(A, Y) = (\mathrm{Jac}C, \Theta)$ を定める.

$$\mathbf{H}_2 = \left\{ \Omega \in \mathrm{M}_2(\mathbf{C}) \,\middle|\, \begin{array}{c} \Omega = {}^t\Omega \\ \mathrm{Im}(\Omega);\text{正定値} \end{array} \right\}$$

次数 2 のジーゲル上半空間

- (A, Y)の同型類全体と$\mathbf{H}_2$ の間には, 自然な同一視が存在する (以後, $\mathbf{H}_2$ の元を, “周期行列 ”ということにする).

CM主偏極アーベル曲面

・あるCM 体 K のオーダーO (以下では, K の整数環O_K の場合のみ扱う) に対し, $i : O \cong \mathrm{End}(A)$ となる (A, Y) をCM主偏極アーベル曲面 (A, i, Y) という.

・(A, i, Y) に対して, Emb(K, **C**)の元の対Φ が決まる. (K, Φ) を (A, i, Y) のCM タイプという.

・K_0の類数が 1 なら, $(K, \Phi = \{1, j\})$をCM タイプに持ち, $i : O_K \cong \mathrm{End}(A)$ となる (A, i, Y) が存在する. 以下, そのような (K, Φ) を1つ固定する.

・CM タイプ (K, Φ) に対し, その双対 (reflex) CMタイプ (K^*, Φ^*) が一意的に定まる.

・$\Phi = \{1, j\}$ に対し, $\overline{\Phi} = \{1, \overline{j}\}$ とする($\overline{j} := j \circ r$, r は複素共役).

CMアーベル曲面の同型類集合（I）

$\Psi = \Phi, \overline{\Phi}$ に対し,

$$M_\Psi := \left\{ \begin{array}{c} \text{CMタイプ}(K, \Psi),\ i : O_K \cong \text{End}(A) \text{ の} \\ \text{CM主偏極アーベル曲面 } (A, i, Y) \text{ の同型類} \end{array} \right\}$$

とし,

$$M := \left\{ \begin{array}{c} i : O_K \cong \text{End}(A) \text{ の} \\ \text{CM主偏極アーベル曲面}(A, i, Y) \text{ の同型類} \end{array} \right\}$$

とした時, M_Φ, $M_{\overline{\Phi}}$, M の i を込めない(A, Y)のみの同型類集合への射影をそれぞれ, $\overline{M_\Phi}$, $\overline{M_{\overline{\Phi}}}$, $\overline{M}$ とすると, **拡大2** の時, $\overline{M} = \overline{M_\Phi}$ となり, **拡大1,3** の時, $\overline{M} = \overline{M_\Phi} \cup \overline{M_{\overline{\Phi}}}$ となる.

CMアーベル曲面の同型類集合（II）

・$(A_0, Y_0) \in \overline{M}_\Phi$ を1つ固定して,

$\overline{M}_0 :=$ { (A_0, Y_0) と K^* 上共役な 主偏極アーベル曲面(A, Y)の同型類 }

とすると, $\overline{M}_0 \subseteq \overline{M}$ となる.

・**拡大1,3** の時, $\overline{M}_{\Phi,0} := \overline{M}_0 \cap \overline{M}_\Phi$, $\overline{M}_{\bar{\Phi},0} := \overline{M}_0 \cap \overline{M}_{\bar{\Phi}}$

$(\overline{M}_0 = \overline{M}_{\Phi,0} \cup \overline{M}_{\bar{\Phi},0})$ とする.

---

1. $\overline{M}_0$ に属する周期行列の具体的な計算法は？

→ “周期行列の構成”

2. $\overline{M}_0 \neq \overline{M}$ かどうか判定する方法は？

→ “K_0^* の判別式の偶奇性を利用した類多項式構成に適したCM体の選別法”

周期行列の構成（I）

K, K^*のガロア閉包をL として, K^* のイデアル $\boldsymbol{a}$ に対し,

$$g(\boldsymbol{a}) := (\boldsymbol{a}^{j^*}\boldsymbol{a}O_L) \cap O_K \qquad (\Phi^* = \{1, j^*\})$$

とする. この g を利用して, K_0 の単数からなる群$U_1 \subseteq U_0 \subseteq U$
を以下のように定め, $d := [U : U_1]$, $d_0 := [U_0 : U_1]$ とする $(d_0 \mid d)$.

- U := {K_0内の総正な単数 }
- $U_1 := \{N_{K/K_0}(e) \mid e : K$ 内の単数 }
- $U_0 := \{m\overline{m}\,\mathrm{N}(\boldsymbol{a})^{-1} \mid \exists \boldsymbol{a}: K^*$のイデアル s.t. $g(\boldsymbol{a})=mO_K$ (単項) }

次にK のイデアル類群 Cl_K の部分群 $Cl'_{K,0} \subseteq Cl'_K \subseteq Cl_K$
を以下のように定義し, $h'_0 := \#\, Cl'_{K,0}$, $h' := \#\, Cl'_K$ とする $(h'_0 \mid h')$.

- Cl'_K := {[$\boldsymbol{b}$] | $\exists \boldsymbol{b}$: Kのイデアル s.t. $\boldsymbol{b}\overline{\boldsymbol{b}} = mO_K, m \in K_0$: 総正 }
- $Cl'_{K,0}$:= { [$g(\boldsymbol{a})$] | $\exists \boldsymbol{a}: K^*$のイデアル }

周期行列の構成（II）[Spallek]

・$\overline{M}_{\Phi} \neq \phi$ なら,
$\#\overline{M}_{\Phi} = d\ h',\ \#\overline{M}_{\Phi,0} = d_0 h'_0 \quad (d_0 h'_0 \mid d\ h')$

・一般には, $d_0 h'_0 < d\ h'$ となり得る. [G.Shimura, “Abelian Varieties with Complex Multiplication and Modular Functions” p.114] では, この場合 ‘類多項式の既約性が成り立たない “と呼んでいる.

$O_{K_0} \cong \mathbf{Z} + \mathbf{Z}w \quad w > 0 \qquad e_0 > 0 :\ K_0$ の基本単数

Cl'_K の代表系を $\mathfrak{a}_i$ $(i = 1, \ldots, h')$ とし, $Cl_K - Cl'_K \neq \phi$ ならその代表系を $\mathfrak{a}'_i$ $(i = 1, \ldots, h')$ とする.

$$\left.\begin{array}{l} \mathfrak{a}_i \cong O_{K_0} + O_{K_0} t_i, \quad \mathrm{Im}(t_i) > 0, \mathrm{Im}(t_i^j) < 0 \\ \mathfrak{a}'_i \cong O_{K_0} + O_{K_0} t'_i, \quad \mathrm{Im}(t'_i) > 0, \mathrm{Im}(t_i'^{\bar{j}}) < 0 \end{array}\right\} \Leftarrow K_0 \text{の類数} = 1$

周期行列の構成 (II) [Spallek]

1. $\overline{M_\Phi} = \{(t_i, j) \mid i = 1, \ldots, h'\}$ if $d = 1$

   $\overline{M_\Phi} = \{(t_i, j), (e_0 t_i, j) \mid i = 1, \ldots, h'\}$ if $d = 2$

   $\overline{M_{\bar{\Phi}}} = \{(e_0 t_i, \bar{j}) \mid i = 1, \ldots, h'\}$ if $N(e_0) = -1$

   (この時, $d = 1$, $Cl_K = Cl'_K$)

   $\overline{M_{\bar{\Phi}}} = \phi$ if $N(e_0) = 1$ & $Cl_K = Cl'_K$

   $\overline{M_{\bar{\Phi}}} = \{(t_i', \bar{j}) \mid i = 1, \ldots, h'\}$ if $d = 1$ & $Cl_K \neq Cl'_K$

   $\overline{M_{\bar{\Phi}}} = \{(t_i', \bar{j}), (e_0 t_i', \bar{j}) \mid i = 1, \ldots, h'\}$ if $d = 2$ & $Cl_K \neq Cl'_K$

2. 1.の $(h, y) \in K \times \mathrm{Emb}(K, \mathbf{C})$は, 次の周期行列 Ω を表す.

$$\Omega = \frac{1}{w - w^s} \begin{pmatrix} w^2 h - w^{y^2} h^y & wh - w^y h^y \\ wh - w^y h^y & h - h^y \end{pmatrix}$$

3. Ω を $\mathrm{Sp}(2, \mathbf{Z})$で変換して, ジーゲルの基本領域内に移す.

井草類多項式

- $a,b\in\frac{1}{2}\mathbf{Z}^2\big/\mathbf{Z}^2, a^t b\equiv 0 \bmod 2, \Omega$: 周期行列に対して, テータ零値を

$$q\begin{bmatrix}a\\ b\end{bmatrix}(\Omega):=\sum_{n\in\mathbf{Z}^2}\exp(p\,i^{\,t}(n+a)\Omega(n+a)+2p\,i^{\,t}(n+a)b)$$

で定義する.

- $J_i(\Omega)$ $(i=2,4,6,10)$ をテータ零値の適当な多項式で定義する.

- $j_1:=\frac{J_2^5}{J_{10}}, j_2:=\frac{J_2^3 J_4}{J_{10}}, j_3:=\frac{J_2^2 J_6}{J_{10}}, j_4:=\frac{J_4 J_6}{J_{10}}, j_5:=\frac{J_4^5}{J_{10}^2}, j_6:=\frac{J_6^5}{J_{10}^3}$

- $H_i(X):=\prod_{\Omega\in\bar{M}_0}(X-j_i(\Omega))=\sum_{k=0}^{s}c_{i,k}X^{s-k}\in\mathbf{Q}[X]$ $(i=1,\ldots,6)$

・以降, $c_{i,k}$ の分母, 分子をそれぞれ $d_{i,k}$, $e_{i,k}$ と表す.

類多項式構成の改良

- 分母推定アルゴリズム
- $K_0^*[X]$内可約性による類多項式正当性判定法
- 定数項分子の相関関係を利用した定数項決定法
- $c_{4,1}$を利用した$\overline{M_0}$決定法
- K_0^*の判別式の偶奇性を利用した類多項式構成に適したCM体の選別法

分母推定アルゴリズム（I）

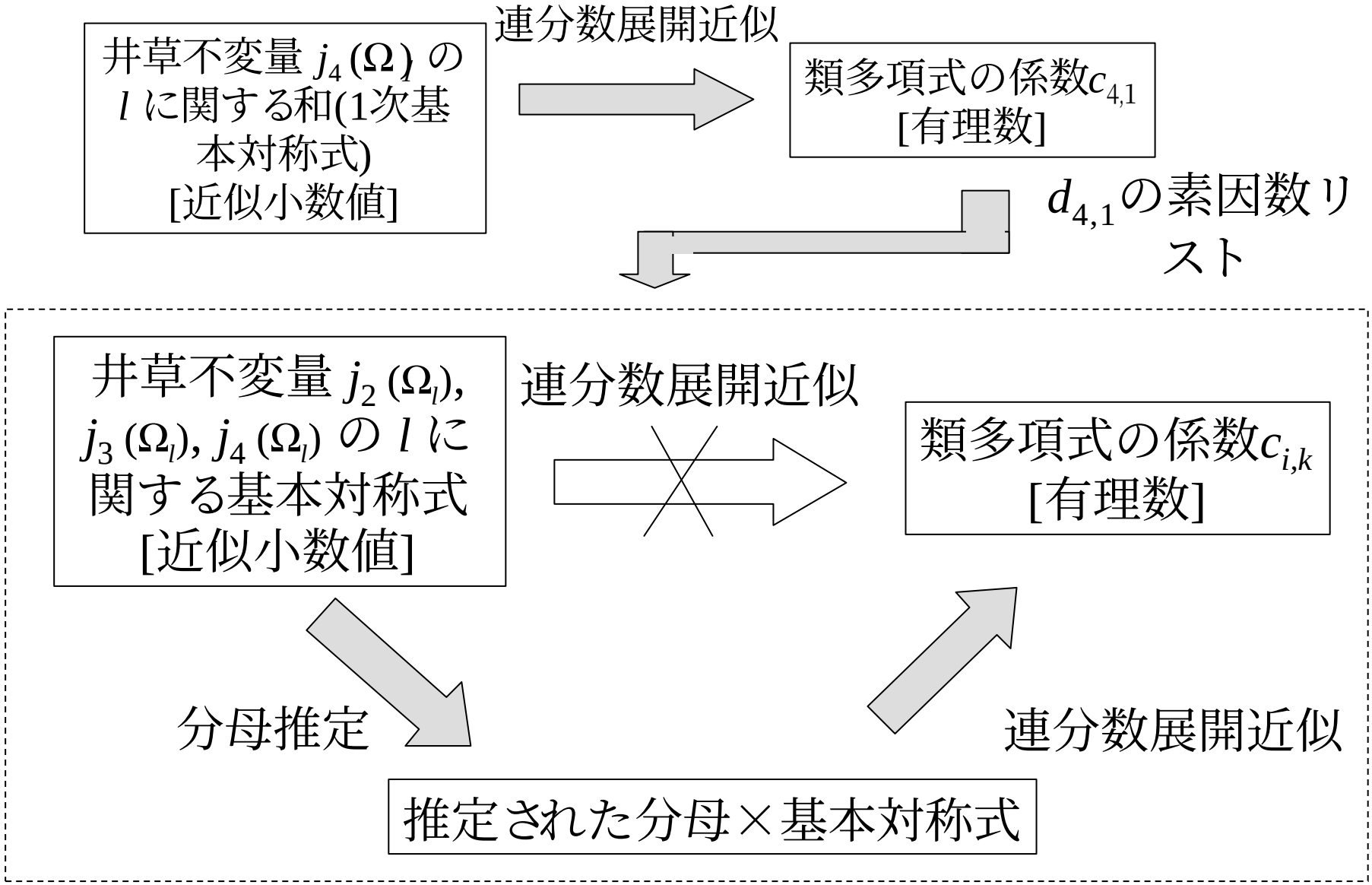
$(m, n) = (3, 8)$, $H_i(X)$の係数の分母 $d_{i,k}$ ：

$k \diagdown i$	2	3	4
1	$3^7 5^6 19^8$	$3^8 5^6 19^8$	$3^2 19^4$
2	$3^{14} 5^{12} 19^{16}$	$3^{16} 5^{11} 19^{16}$	$3^4 19^8$
3	$3^{14} 5^{18} 19^{24}$	$3^{16} 5^{17} 19^{24}$	$3^4 19^{12}$
…			
最大値 $(1 \leqq k \leqq 10)$	$3^{14} 5^{30} 19^{24}$	$3^{16} 5^{30} 19^{24}$	$3^4 19^{12}$

見て取れること：

- 全ての $d_{i,k}$ に現れる素因数は小素因数のみで共通 (3,5,19)
- $c_{4,1}$ の分母 $d_{4,1}$が絶対値最小
- $(\max_{1 \leq k \leq 10} d_{i,k}$の各素因数の指数$) / (d_{i,1}$の各素因数の指数$)$ は
  それほど大きくならない.

分母推定アルゴリズム（II）



$K_0^*[X]$内可約性による類多項式正当性判定法

- $\overline{M}_{\Phi,0}, \overline{M}_{\bar{\Phi},0}$に対応する類多項式の因子多項式は, K_0^*係数になっている.
- $H_i(X) = H_i^{(\Phi)}(X) H_i^{(\bar{\Phi})}(X)$
- $H_i^{(\Phi)}(X) := \prod_{\Omega \in \overline{M}_{\Phi,0}} (X - j_i(\Omega)),\ H_i^{(\bar{\Phi})}(X) := \prod_{\Omega \in \overline{M}_{\bar{\Phi},0}} (X - j_i(\Omega))$

$$\in K_0^*[X] \qquad (i = 1, \ldots, 6)$$

- ”分母推定 ”で得られた係数候補から, 正しい類多項式の係数を決定することができる.

定数項分子の相関関係を利用した定数項決定法（I）

- $(m,n) = (3,4)$ の時, $H_i(X)$ $(i = 2,3,4)$ の定数項の分子 $e_{i,s}$ $(s = d_0 h_0')$ は以下の通り,

$e_{2,s} = 2^4 \cdot \mathbf{5}^{\mathbf{2}} \cdot \mathbf{131} \cdot \mathbf{64219219}^{3}$

$e_{3,s} = 2^8 \cdot \mathbf{4931} \cdot \mathbf{64219219}^{2} \cdot \mathbf{80007223}$

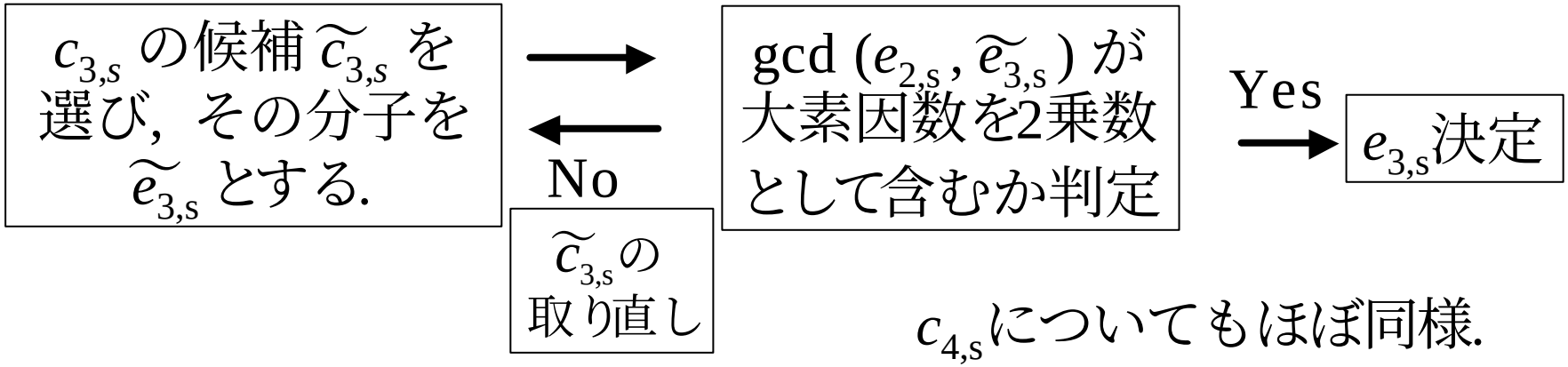
$e_{4,s} = -1 \cdot 2^{16} \cdot 3^2 \cdot \mathbf{5}^{\mathbf{2}} \cdot \mathbf{131} \cdot \mathbf{4931} \cdot \mathbf{80007223}$

← $j_2 = \dfrac{\boldsymbol{J_2}^3 \boldsymbol{J_4}}{J_{10}}$, $j_3 = \dfrac{\boldsymbol{J_2}^2 \boldsymbol{J_6}}{J_{10}}$, $j_4 = \dfrac{\boldsymbol{J_4}\,\boldsymbol{J_6}}{J_{10}}$

- $e_{i,s}$ $(i = 2,3,4)$ は, j_i $(i = 2,3,4)$ の $\boldsymbol{J_2}$, $\boldsymbol{J_4}$, $\boldsymbol{J_6}$, J_{10} による分解に従って, 大素因数を共有する.

定数項分子の相関関係を利用した定数項決定法（II）

例：$H_2(X)$の定数項 $c_{2,s}$ (の分子 $e_{2,s}$)が決定されていて, $H_3(X)$, $H_4(X)$の定数項が未決定の時,



$c_{4,s}$についてもほぼ同様.

利点:

- ”$K_0^*[X]$内可約性判定 ”と異なり, 定数項以外の係数を必要としない.
- 定数項は他係数と比べて, より多くの有効桁数を必要とする場合が多いので, この方法を適用することで, 全体の必要有効桁数を少なくできる.

$c_{4,1}$を利用した$\overline{M}_0$決定法

$s = 2d_0h'_0 \neq 2dh'$ (K_0の類数 1, **拡大3**, $\overline{M}_\Phi \neq \phi$) の時,

- $h'_0 \neq h'$の場合には, $\overline{M}$ の$2dh'$個の井草不変量の内で, どの $2d_0h'_0$個の井草不変量が $\overline{M}_0$ に入るものか不変量計算前に, 確定できるが, $d_0 \neq d$の場合には,確定できない.
- 有理数への変換に必要な有効桁数が一番少ない係数$c_{4,1}$を利用して確定する.

  $j_4(\Omega_l)$ ($l = 1, \ldots, 2dh'$)の$2d_0h'_0$個の組み合わせに対し, その和を計算して, その分母が小素因数から構成されているかどうか判定して, $\overline{M}_0$ の元を確定する.

問題点:

- $\overline{M}_0$ の候補は, $\overline{M}$ の元の$2h'$ ($= s$) 個の組み合わせで, $2^{2h'}$ 個存在し,本方法の計算量は, h' が大きくなると, かなり負荷が増すので, より工夫を施した方法が望まれる.

K_0^*の判別式の偶奇性を利用した類多項式構成に適したCM体の選別法

	(m, n)	$disc_0^*$	d	d_0	h'	h'_0	dh'	$d_0 h'_0$
I	(3, 4)	奇数	2	1	1	1	2	1
	(7, 6)	奇数	2	1	4	4	8	4
II	(3, 6)	奇数	2	2	2	1	4	2
	(5, 11)	奇数	1	1	6	3	6	3
III	(5, 9)	偶数	1	1	6	6	6	6
	(6, 14)	偶数	2	2	6	6	12	12

$disc_0^*$:= K_0^*の判別式

K_0の類数 1
拡大3.
$\overline{M_\Phi} \neq \Phi$
の時に専ら適用

I : $disc_0^*$ 奇数 & $d \neq d_0$
II : $disc_0^*$ 奇数 & $h' \neq h'_0$

III : $disc_0^*$ 偶数 & $d\,h' = d_0\,h'_0$

・$disc_0^*$が奇数の CM体を選択的に用いることで, 効率的に類多項式を構成することができる.

実装結果とその効果

	分母推定なし	分母推定あり
初期データ精度	231	183
テータ級数の項数	841	625
類多項式の次数$(2d_0h_0')$	10	10
不変量計算数$(2dh')$	20	20
不変量計算	20.58 s	12.20 s
$\overline{M}_0$決定	3.04 s	2.90 s
類多項式構成	0.24 s	1.81 s
$K_0^*[X]$内可約性判定	1.86 s	1.86 s
総計時間	25.72 s	18.77 s

- 分母推定法の効果は現在計算したほとんど類多項式で確認された.
- $\overline{M}_0$ 決定を効率的に行う必要がある. ($2^{2h'}$個の可能性)
- $K_0^*[X]$内可約性判定も効率的に行う必要がある.
- テータ級数の主要項の選別法も改良の余地あり.

まとめと今後の課題

- 種数 2 の超楕円曲線構成に対する CM アルゴリズムで最も計算困難性を伴う類多項式構成ステップに対していくつかの改良法を提案した.
- 実装結果についても報告した.

- ”分母素因数閾値 ”B などアルゴリズムに含まれるパラメータの最適化を行えるようにする.
- 計算間違い, バグがなければ）”K_0^* の判別式の偶奇性の利用によるCM体の選別法 ”での現象を理解して, 更なる改良の可能性を探る.