中央大学理工学研究所論文集　第6号　2000年
Journal of the Institute of Science and Engineering, Chuo University

Jacobi多様体のCM Typeの計算

Computation of CM Type of Jacobian Varieties

松尾和人[*]　趙 晋輝[†]　辻井重男[‡]　百瀬文之[§]　関口 力[§]

あらまし　近年盛んに研究されているJacobi多様体上の暗号系に於いて，CM体法を用いて暗号系を構成する場合，CM Jacobi多様体のCM type及びreflex CM typeを計算する必要が生ずる．本論文では，Frobenius endomorphismの素イデアル分解を用いた，有限体上のJacobi多様体及び，代数体上のCM Jacobi多様体のCM type，reflex CM typeの計算アルゴリズムを提案する．

キーワード　Jacobi多様体，虚数乗法，CM体，CM Type，Reflex CM Type

1　まえがき

近年公開鍵暗号系の標準的構成と成りつつある楕円曲線暗号を始めとする平面代数曲線のJacobi多様体上の離散対数問題に基づく暗号系において，暗号系の構成上，安全な曲線の生成は必要不可欠である．

安全な曲線は，そのJacobi多様体上の離散対数問題に対する攻撃が位数の指数時間オーダーであることで定義されるが，Jacobi多様体上の離散対数問題への攻撃は，baby-step-giant-step法を始めとする一般の多様体に適用可能な方法と，特殊な多様体に対してより効率的な方法に分類される．

一般の多様体に適用可能な方法は，その時間計算量が，多様体の位数をNとしたとき，$O(\sqrt{N})$であり，Pohlig-Hellman法として知られているbaby-step-giant-step法の改良アルゴリズムは時間計算量が，多様体の位数の最大素因子の指数オーダーである．従って，これらの攻撃法は位数が大きな素因数を持つ多様体に対しては適用不可能である．これらの方法とは別に多様体の特殊性に着目した解法が幾つか考案されている．MOV［32］として知られている楕円曲線に対する攻撃法は，Frey，Rückによって超楕円曲線のJacobi多様体に拡張されているが［15］［54］，楕円曲線の位数が定義体の乗法群の位数を割るときに準指数時間オーダーの計算量である．また，その位数が定義体の標数を割る多様体に対して，多項式時間オーダーの攻撃法が提案されている［46］．

最近になって，Gaudry達によって曲線のgenusが4以上の場合に計算量が$O(\sqrt{N})$より小さくなる，即ちbaby-step-giant-step法より高速な，攻撃法が提案された［16］［12］．この方法は大きな位数の自己同型を持つ多様体に対して現実的な攻撃法である．しかしながら，曲線のgenusが小さくまた大きな位数の自己同型を持たない多様体を用いた暗号系の構成は，暗号系の多様性の面からも，未だに必要であると考えられる．

以上の議論から，Jacobi多様体上で安全な暗号系を構成するためには，その位数を知る必要がある．

楕円曲線においては，有限体上の曲線の位数を計算する方法として知られているSchoof法およびその改良であるSEA法を用いる方法と，有限体上へのreductionの位数が高速に計算できる代数体上のCM楕円曲線を用いる方法が知られている．

[*] 東洋通信機（株），〒253－0192　神奈川県高座郡寒川町小谷2－1－1，Toyo Communication Equipment Co.,Ltd.,2-1-1 Koyato, Samukawa-machi Koza-gun, Kanagawa, 253-0192 Japan
[†] 中央大学理工学部電気電子工学科．中央大学理工学研究所　〒112－8551　東京都文京区春日1－13－27，Department of Electrical and Electronic Engineering, Chuo University. The Institute of Science and Engineering, Chuo University. 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan.
[‡] 中央大学理工学部情報工学科．中央大学理工学研究所　〒112－8551　東京都文京区春日1－13－27，Department of Information and System Engineering, Chuo University. The Institute of Science and Engineering, Chuo University. 1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan.
[§] 中央大学理工学部数学科．中央大学理工学研究所　〒112－8551　東京都文京区春日1－13－27，Department of Mathematics,Chuo Uni-versity.The Institute of Science and Engineering, Chuo Uni-versity.1-13-27 Kasuga, Bunkyo-ku, Tokyo, 112-8551 Japan.

最近になって，genus が 2 以上の平面代数曲線の Jacobi 多様体の構成法が盛んに研究され始めた．Pila によって Schoof 法の拡張が行われ［42］，更に Adleman，Huang によって改良がなされている［2］［19］［3］．Gaudry，Harley はこの方法と λ 法を組み合わせて有限体上の genus 2 の超楕円曲線の Jacobi 多様体の位数計算を実装したが［17］，実際に位数計算可能な Jacobi 多様体の位数は暗号系に用いる為の十分な大きさを持っていない．

これとは別に，Spallek［52］によって theta 関数を用いた CM Jacobi 多様体を持つ genus2 の超楕円曲線の構成法が提案されている．この方法は Wang［61］，Weber［60］，Wamelen［57］［58］等によって様々な拡張，改良がなされてきた．また，著者等は有限体の曲線を代数体に lifting することで，Jacobi 多様体が CM を持つ平面代数曲線を構成する研究を行っている［22］［31］［18］［24］．これらの方法によって代数体上の CM 多様体が構成されると，著者等が提案している暗号系の構成法によって多様体 base の安全な暗号系を効率的に得ることができる［8］［56］．

しかしながら，超楕円曲線を始めとする genus 2 以上の曲線の Jacobi 多様体の CM 理論では，楕円曲線の CM 理論と異なり，CM type，reflex CM type が自明なものでなくなり［29］［49］［50］［51］，著者等が提案している CM 多様体の構成法，CM 多様体を用いた安全な暗号系の構成法に於いても代数体上の Jacobi 多様体の CM type，reflex CM type の計算を必要とする．

そこで，本論文では，まず有限体上の Jacobi 多様体の CM 体の計算アルゴリズムを示し，次にこの多様体の CM type，reflex CM type の計算アルゴリズムを提案する．そして，これらを応用して代数体上の CM 多様体の CM type，reflex CM type の計算アルゴリズムを提案する．最後に，計算例と実装結果を述べる．

2　Jacobi 多様体

k を体とし，$F(X,\ Y)\in k[X,\ Y]$ としたとき，

$$C : F(X,\ Y)=0$$

を平面代数曲線という．

以下，常に C は非特異で既約であるとする．

C の点 P_i の整係数線形結合

$$D=\sum_i m_i P_i\ \ m_i\in\mathbb{Z}$$

を C の因子という．

C の全因子の集合は Abel 群を形成する．これを因子群と呼び，$\mathfrak{D}$ で表わす．因子 D の次数は $\deg D=\Sigma_i m_i$ で定義される．次数 0 の因子の集合は $\mathfrak{D}$ の部分群 $\mathfrak{D}^0$ を形成する．

$h\in k(C)$ に対して与えられる因子

$$(h)=\sum_i P_i-Q_i$$

を主因子という．ここで，P_i と Q_i は各々 h の零点と極を表わす．全ての主因子の集合 $\mathfrak{D}^l$ は $\mathfrak{D}^0$ の部分群になることが知られている．

C の Jacobi 多様体 $\mathfrak{J}(k)$ は

$$\mathfrak{J}(k)=\mathfrak{D}^0/\mathfrak{D}^l.$$

と定義される．Jacobi 多様体は Abel 多様体であることが知られている．

これまでに，Jacobi 多様体上の効率的な加算アルゴリズムが，一般平面代数曲線に関して Volcheck［55］，

C_{ab} 曲線に関して Arita 等［6］，superelliptic curve に関して Galbrath 等［13］，超楕円曲線に関して Cantor［7］によって，各々提案されている．

Jacobi 多様体上の離散対数問題は，与えられた D_1，$D_2\in\ \mathfrak{J}(\mathbb{F}_q)$ に対して，$D_1=mD_2$ が成り立つ $m\in\mathbb{Z}$ を求める問題である．

3　Ordinary Jacobi 多様体の CM 体の計算

ここでは，曲線 C の Jacobi 多様体 $\mathfrak{J}$ の CM 体 K を定義し，K を求めるアルゴリズムを示す．

A を体 k 上の g 次の Abel 多様体とする．$K\cong End A\otimes_{\mathbb{Z}}\mathbb{Q}$ が $\mathbb{Q}$ 上総実拡大の総虚 2 次拡大のとき，K を A の CM 体といい，A は CM を持つという．

以下，同型写像 $\iota: K\to End A\otimes_{\mathbb{Z}}\mathbb{Q}$ によって，$a\in K$ と $\iota(a)\in End A\otimes_{\mathbb{Z}}\mathbb{Q}$ を同一視する．また，$End A$ は k 上で定義されているものとする．

k が有限体であり，$[K:\mathbb{Q}]=2g$ のとき，A は ordinary といい，常に CM を持つ．$A/\mathbb{F}_q$ が ordinary であることと $Z(X)$ が重根を持たないことは同値である［53］．

π を ordinary Abel 多様体 $A/\mathbb{F}_q$ の q-Frobenius endomorphism とすると，A の CM 体は $K=\mathbb{Q}(\pi)$ で与えられる．そこで，C の $\mathbb{F}_{q^i}$- 有理点の数を $i=1..g$ に対して数え上げて A の合同ゼータ関数を計算することによって，q-Frobenius endomorphism の特性多項式 $Z(X)\in\mathbb{Z}[X]$ を得れば，この $Z(X)$ が K の生成多項式となる．

以上により， Jacobi 多様体が ordinary である曲線の CM 体を求めるアルゴリズムが Algorithm 1 で与えられる．

Algorithm 1（CM 体）.
Input：曲線 $C/\mathbb{F}_q$.
Output：C の Jacobi 多様体 $\mathfrak{J}$ の CM 体 K の生成多項式 $Z(X)$．または，$\mathfrak{J}$ が ordinary でないとき，false.

1. $i=1..g$ に対して C の $\mathbb{F}_{q^i}$- 有理点 N_i を計算する．
2. 各 N_i について $M_i=N_i-q^i-1$ を計算する．
3. 等式
$$\sum\alpha_j^n=M_i$$
から Newton 公式を用いて，α_j の基本対称式 $s_i=\sum\prod^{i}\alpha_j$ を計算する．
4. $Z(X)=X^{2g}-_{s1}X^{2g-1}+_{s2}X^{2g-2}+\cdots+q^{g-1}X+q^g\in\mathbb{Z}[X]$ を計算する．
5. $Z(X)$ が重根を持つ場合，false を出力して終了．
6. $Z(X)$ を出力して終了．

□

Algorithm 1 の時間計算量は $O(q^g)$ であるが，我々の用途では q，g は十分に小さいので，実用的に計算可能である．

これとは別に時間計算量 $O\left(q^{\frac{1}{4}[8g/5]+O_g(1)}\right)$ のアルゴリズムが Elkies によって提案されている［14］．しかし，このアルゴリズムは超楕円曲線の Jacobi 多様体に特化した方法であり，また genus 毎に異なるアルゴリズムを必要とする．

4　Ordinary Jacobi 多様体の CM Type の計算

ここでは，代数体上の Jacobi 多様体の CM type，reflex CM type の計算について述べる．そこで，まず CM type，reflex CM type を定義し，次に，有限体上の Jacobi 多様体の CM type，reflex CM type の計算アルゴ

リズムを示す．そして，これらを用いて代数体上の Jacobi 多様体の CM type，reflex CM type の計算アルゴリズムを構成する．尚，記法は［51］に従う．

ρ を複素共役写像，K を $2g$ 次の CM 体とする．K の $\mathbb{C}$ への埋め込みを $\varphi_1,...,\varphi_g$，$\rho\varphi_1,...,\rho\varphi_g$ と表わしたとき，K の CM type は $\Phi=\{\varphi_1,...,\varphi_g\}$ で与えられる．また，組（K，Φ）を CM type という．

$x\in K$ に対して，type normN_Φ が以下で定義される．

$$N_\Phi(x)=\prod_i x^{\varphi_i}$$

L を K の正規閉包，$G=Gal(L/\mathbb{Q})$ とする．$\tilde{\varphi}_i$ を φ_i の L への延長とし，$\tilde{\Phi}\subset G$ でこれらの集合を表わす．また $H\subset G$ で K の固定群を表わし，

$$S=H\tilde{\Phi},$$
$$S'=\{\sigma^{-1}|\sigma\in S\},$$
$$H'=\{\gamma|\gamma\in G,\ \gamma S'=S'\}$$

とする．このとき，$H'=\{\gamma\in G|S\gamma=S\}$ が成り立つ．

$K'\subset L$ を H' の固定体とし，Ψ を S' の K' への制限によって得られる K' の $\mathbb{C}$ への埋め込みの集合とすると，（K'，Ψ）は CM type になる．この組（K'，Ψ）を（K，Φ）の reflex という．

Algorithm 2 に，与えられた CM type（K，Φ）に対して reflex CM type（K'，Ψ）を計算するアルゴリズムを示す．

Algorithm 2（**Reflex CM Type**）.
Input：CM type（K，Φ）.
Output：reflex CM type（K'，Ψ）.

1. K の正規閉包 L を計算する.
2. $G=Gal(L/\mathbb{Q})$ を計算する.
3. K の固定群 $H\subset G$ を計算する.
4. $S=H\tilde{\Phi}$ を計算する.
5. $H'=\{\gamma\in G|S\gamma=S\}$ を計算する.
6. H' 固定体 $K'\subset L$ と $g':=[K':\mathbb{Q}]/2$ を計算する.
7. $S'=\{\gamma\in G|\gamma^{-1}\in S\}$ を計算する.
8. K' への制限が $\mathbb{C}$ への互いに異なる埋め込みになる，g' 個の S' の元の集合 $\tilde{\Psi}\subset S'$ を計算する.
9. （K'，Ψ）を出力して終了．ここで Ψ は，$\tilde{\Psi}$ の元の K' への制限によって得られる，$\mathbb{C}$ への埋め込みの集合を表わす.

□

次に，有限体上の Jacobi 多様体の CM type を計算するアルゴリズムについて述べる．

A を標数 0 の体 k 上で定義された CM 体 K を持つ g 次元 Abel 多様体とすると，A は複素 torus と同型であり，g 次元の解析座標を用いて，$EndA\otimes_{\mathbb{Z}}\mathbb{Q}$ の解析座標による表現 M を得る．$\varphi_1,...,\varphi_{2g}$ を K の $\mathbb{C}$ への埋め込みの全てとすると，M は g 個の互いに異なる埋め込み $\varphi_1,...,\varphi_g$ の直積と同値になる．$\Phi=\{\varphi_1,...,\varphi_g\}$ とすると，（K，Φ）は CM type であり，A は type（K，Φ）であるという．A の定義体 k は reflex CM 体 K' を含むことが知られている．

また，A の CM type（K，Φ）に関して与えられる H，S に対して，$H=\{\gamma|\gamma\in G,\ \gamma S=S\}$ ならばそのときに限って，A は simple であることが知られている．

以降，A は simple であると仮定する．

K'_0を，reflex type $\{\phi_1,...,\phi_{g'}\}$ が K'_0の $\mathbb{C}$ への互いに異なる埋め込みになる，K' の総実部分体とする．p を K'_0

で不分岐な素数とする．また，$\mathfrak{p}$ を（p）の上にある K' の素イデアルとし，$\mathfrak{P}$ を $\mathfrak{p}$ の上にある k の素イデアルとする．$\pi \in K$ を $\tilde{A} = A \bmod \mathfrak{P}$ の $N\mathfrak{P}$-Frobenius endomorphism とすると，Frobenius endomorphism の素イデアル分解

$$(\pi) = (N_{\Psi}(\mathfrak{p}))^{f(\mathfrak{P}/\mathfrak{p})}$$

を得る．ここで，f（$\mathfrak{P}/\mathfrak{p}$）は $\mathfrak{P}/\mathfrak{p}$ の惰性次数を表わすが，k が与えられていないとき，この値を直接計算することはできない．しかし，$\tilde{A}$ が $\mathbb{F}_q$ 上定義されていて，即ち $N(\mathfrak{P}) = q$ であり，$f(\mathfrak{p}/(p))$ が与えられた場合，$q = p^n$ とすると，

$$n = f(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{p}/(p))$$

から $f(\mathfrak{P}/\mathfrak{p})$ を計算することが出来る．また，$\mathfrak{p}$ の下にある K_0 の素イデアルを $\mathfrak{a}$ とすると，多様体が ordinary のとき $f(\mathfrak{p}/\mathfrak{a}) = 1$ であることが知られている．従って，

$$f(\mathfrak{P}/\mathfrak{p}) = n/f(\mathfrak{a}/(p))$$

で $f(\mathfrak{P}/\mathfrak{p})$ を計算可能である．

Algorithm 3 に有限体上の曲線の Jacobi 多様体の CM type（K，Φ）を計算するアルゴリズムを示す．

Algorithm 3（CM Type）.
Input：曲線 $C/\mathbb{F}_q$.
Output：C の Jacobi 多様体 $\mathfrak{J}$ の CM type（K，Φ）と reflex CM type（K'，Ψ）．または，$\mathfrak{J}$ が ordinary でないとき，false.

1. $q = p^n$ となる素数 p と整数 n を計算する．
2. Algorithm 1 を用いて CM 体 K とその生成多項式 $Z(X)$ を計算する．Algorithm 1 が false を返した場合，false を出力し終了．
3. K の正規閉包 L を計算する．
4. $G = Gal(L/\mathbb{Q})$ を計算する．
5. K の固定群 $H \subset G$ を計算する．
6. 互いに複素共役で無い元からなる G の位数 g の部分群の族 $T = \{\tilde{\Phi}_i\}$ を求める．
7. 任意の $\tilde{\Phi}_i$ に対し，以下を行う：
   7.1. $\tilde{\Phi} = \tilde{\Phi}_i$ とする．
   7.2.（K，Φ）を CM type として，Algorithm 2 を用いて reflex CM type（K'，Ψ）を計算する．
   7.3. K' の g' 次総実部分体 K'_0 で，Ψ が K'_0 から $\mathbb{C}$ への埋め込みの K' への延長の集合となっているものを計算する．
   7.4. K'_0 で（p）の素イデアル分解を行い，$(p) = \prod \mathfrak{a}_i^{e_i}$ を得る．
   7.5. 任意の $\mathfrak{a}_i$ に対し，以下を行う：
      7.5.1. $\mathfrak{a} = \mathfrak{a}_i$ とする．
      7.5.2. $\mathfrak{a}/(p)$ の惰性次数 f を計算する．
      7.5.3. $f \nmid n$ ならば 7.5.7. へ．
      7.5.4. K' で $\mathfrak{a}$ の素イデアル分解を行い，完全分解 $\mathfrak{a} = \prod \mathfrak{p}\mathfrak{p}'$ をチェックする．完全分解していない場合，7.5.7. へ．

7.5.5. $\mathfrak{Q}=(N_{\Psi'}\mathfrak{p})^{n/f}$ を計算する.

7.5.6. $Z(X)$ の K 上の任意の根 π に対して，条件 $\pi\in\mathfrak{Q}$をチェックする．条件を満足する π が存在する場合，(K, Φ)，(K', Ψ) を各々CM type，reflex CM type として出力し終了.

7.5.7. 可能なら $\mathfrak{a}_i\neq\mathfrak{a}$を選び 7.5.1. へ.

7.6. 可能なら $\tilde{\Phi}_i\neq\tilde{\Phi}$ を選び，7.1. へ.

□

以上の結果を用いて，以下で代数体上の CM Jacobi 多様体の CM type，reflex CM type を計算するアルゴリズムを構成する.

A の定義体 k を代数体，即に$\mathbb{Q}$の有限次代数拡大とする．k の素イデアル$\mathfrak{P}$に対して $\tilde{A}=A \bmod \mathfrak{P}$とすると，$\mathfrak{P}$の下にある K_0'の素イデアル$\mathfrak{a}$が K' で完全分解するとき，$\tilde{A}$ は ordinary であることが知られている．この状況は高い確率で起こると期待できる．従って，k を非常に小さな有限体に reduction して，Algorithm 3 を用いて CM type を計算することが可能である.

以下に，代数体上の CM Jacobi 多様体の CM type，reflex CM type の計算アルゴリズムを示す.

Algorithm 4（代数体上の多様体の CM Type）.
Input：Jacobi 多様体 $\mathfrak{J}$が CM を持つ曲線 C/k.
Output：$\mathfrak{J}$ の CM type（K，Φ）と reflex CM type（K'，Ψ）.

1. 小さな有限体 $\mathbb{F}_q$ を選ぶ.
2. C の $\mathbb{F}_q$ への reduction $\tilde{C}$ に対して，Algorithm 3 を用いて，CM type（K，Φ）と reflex CM type（K'，Ψ）を計算する．Algorithm 3 が false を返した場合，1. へ.
3. (K, Φ)，(K', Ψ) を各々CM type，reflex CM type として出力し終了.

□

Algorithm 4 とは別に，CM 多様体の位数計算法として示された［56］，Frobenius endomorphism の素イデアル分解をランダムサーチを用いて行うアルゴリズムが考えられる．このアルゴリズムは，K' の類数が小さいとき Algorithm 4 より高速に計算可能である.

ランダムサーチを用いたアルゴリズムを以下に示す.

Algorithm 5（代数体上の多様体の CM Type）.
Input：Jacobi 多様体 $\mathfrak{J}$が CM を持つ曲線 C/k.
Output：$\mathfrak{J}$ の CM type（K，Φ）と reflex CM type（K'，Ψ）.

1. 小さな有限体 $\mathbb{F}_q$ を選ぶ.
2. Algorithm 1 を用いて C の $\mathbb{F}_q$ への reduction $\tilde{C}$ の CM 体 K を計算する．Algorithm 1 が false を返した場合，1. へ.
3. Algorithm 3 と同様に L，G，H，T を計算する.
4. 任意の $\tilde{\Phi}_i\in T$ に対し，以下を行う：
   4.1. $\tilde{\Phi}=\tilde{\Phi}_i$ とする.
   4.2. (K, Φ) を CM type として，Algorithm 2 を用いて reflex CM type（K'，Ψ）を計算する.
   4.3. K' の g' 次総実部分体 K_0'で，Ψ が K_0'から$\mathbb{C}$への埋め込みの K' への延長の集合となっているものを計算する.
   4.4. 絶対ノルム $N\omega$ が小さな素数 p である $\omega\in K'$ を探す.
   4.5. p の上にある k の素イデアル$\mathfrak{p}$に対して，情性次数 $f=\mathfrak{p}/(p)$ を計算する.
   4.6. $\mathbb{F}_{p^f}$-Frobenius endomorphism の特性多項式 $Z(X)$ を Algorithm 1 を用いて計算する.
   4.7. $\pi=(N_{\Psi'}(\omega))^f$を計算する.
   4.8. π の特性多項式 $Z'(X)$ を計算する.
   4.9. $Z'(X)=Z(X)$ ならば (K, Φ)，(K', Ψ) を各々CM type，reflex CM type として出力し，終了.

4.10. 可能なら $\tilde{\Phi}_i \neq \tilde{\Phi}$ を選び，4. 1. へ.

□

5 実装結果

5.1 CM 体の計算例（Algorithm 1）

Algorithm 1 により

$$C/\mathbb{F}_5 : Y^2 = X^7 + 4X^6 + 3X^5 + 3X^4 + X^3 + X + 4$$

の Jacobi 多様体 $\mathfrak{J}$ の Frobenius endomorphism π の特性多項式 $Z(X)$ が,

$$Z(X) = X^6 + 8X^4 - 4X^3 + 40X^2 + 125$$

と計算される.

5.2 CM Type 及び Reflex CM Type の計算例（Algorithm2, 3）

上で得られた CM 体 $K = \mathbb{Q}(\pi)$ の正規閉包 L が,

$$L = \mathbb{Q}(\alpha),$$
$$\alpha^{12} + 40\alpha^{10} + 70\alpha^9 + 473\alpha^8 + 130\alpha^7 + 1140\alpha^6 - 1930\alpha^5 + 3121\alpha^4 - 320\alpha^3 + 11840\alpha^2 + 7000\alpha + 2500 = 0$$

と計算され，また $\sigma_i \in G = Gal(L/\mathbb{Q})$ が

$$\sigma_i : \alpha \mapsto \beta_i$$

と計算される．但し，$\beta_i \in L$ は基底

$$[1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5,\ \alpha^6,\ \alpha^7,\ \alpha^8,\ \alpha^9,\ \alpha^{10},\ \alpha^{11}]$$

を用いて，以下の通り表される.
（スペースの都合上略記する.）

β_1 = [0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0],
β_2 = [2616193934740536517100, . . . , 656426790570060893] /44079546759333438820 0,
β_3 = [201845838860895008500, . . . , 351401409778066759] /44079546759333438820 0,
β_4 = [−569589533078828300, . . . , 351401409778066759] /975211211489677850,
β_5 = [−1132133549739108090700, . . . , −641225904222685309] /44079546759333438820 0,
β_6 = [−1428451754910693043300, . . . , −369577002476958779] /44079546759333438820 0,
β_7 = [227700187725596296500, . . . , 54517175209915571] /88159093518666877640,
β_8 = [92837286578722300, . . . , 378314604862821] /445698147212673800,
β_9 = [−187591664257510043800, . . . , −42520408396493604] /11019886689833597050,
β_{10} = [3882690408690415100, . . . , −2891966176429239] /4952758062846453800,
β_{11} = [−1318421992476154389500, . . . , −392328736908221989] /44079546759333438820 0,
β_{12} = [123228047019602445900, . . . , 43264084984372713] /11019886686898333597050.

また，複素共役写像$\rho=\sigma_4$である．

以上を用いて，$\mathfrak{J}$のCM type（K，Φ），reflex CM type（K'，Ψ）が，

$$
\begin{aligned}
&K=\mathbb{Q}(\pi),\\
&\quad \pi^6+8\pi^4-4\pi^3+40\pi^2+125=0,\\
&\Phi=\{\sigma_1,\ \sigma_2,\ \sigma_3\},\\
&K'=\mathbb{Q}(\xi),\\
&\quad \xi^6+26\xi^5+223\xi^4+654\xi^3-54\xi^2-3100\xi+2500=0,\\
&\Psi=\{\sigma_1,\ \sigma_5,\ \sigma_6\},
\end{aligned}
$$

と計算される．

5.3　CM Type 及び Reflex CM Type の計算時間

有限体$\mathbb{F}_p$上のgenus 2の超楕円曲線のJacobi多様体のCM type，reflex CM typeの計算をAlgorithm 3を用いて行ったときの，計算に要した時間を**図1**に示す．

図1において，横軸は$\mathbb{F}_p$の位数p，縦軸はCM type，reflex CM typeの計算に要した時間を表す．また，点Aは，$[L:\mathbb{Q}]=4$の場合，点Bは，$[L:\mathbb{Q}]=8$の場合を各々表す．

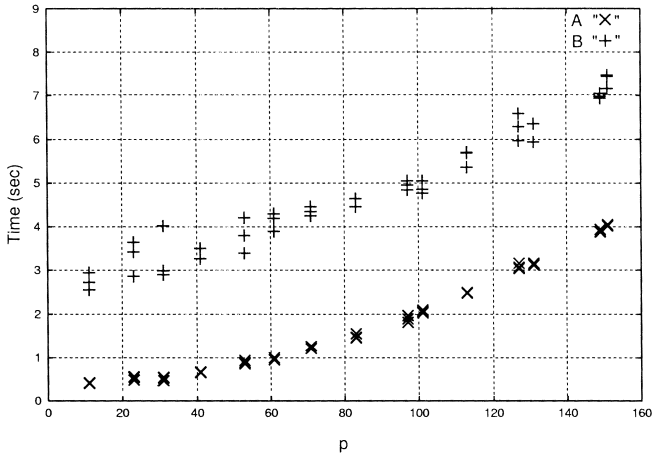

図1：CM Type, Reflex CM Type の計算時間

尚，計算はKASH/KANT［9］を用いて，UltraSPARC-IIi301MHz上で行った．

参考文献

［1］ L. M. Adleman, “A subexponential algorithm for the discrete logarithm problem with applications,” Proc. 20th Ann. IEEE Symp. on Foundations of Computer Science, pp. 55-60, 1979.

［2］ L. M. Adleman, M. D. A. Huang：“Primality Testing and Abelian Varieties Over Finite Fields,” Springer-Verlag, 1992.

［3］ L. M. Adleman, M. D. A. Huang：“Counting rational points on curves and abelian varieties over finite fields,” Proc. of ANTS-2, Springer-Verlag, 1996.

［4］ L. M. Adleman, J. D. Marrais, M. D. Huang: “A Subexponential Algorithms for Discrete Logarithms over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields,” Proc. of ANTS95, Springer, 1995.

［5］ S. Arita, “Public key cryptosystems with C_{ab} curve 2),” IEICE, Proc. of SCIS’98, 7. 1-B, 1998.

［6］ S. Arita, A. Yoshikawa, H. Miyauch, “A software implementation of discrete-log-based cryptosystems with C_{ab} curve,” IEEE Japan Proc. of SCIS’99, T3-1. 3, 1999.

［7］ D. Cantor：“Computing in the jacobian of hyperelliptic curve,” Math. Comp. , vol. 48, p. 95-101, 1987.

［8］ J. Chao, N. Matsuda, S, Tsujii “Efficient construction of secure hyperelliptic discrete logarithm problems” Springer-Verlag Lecture Notes on Computer Science, Vol. 1334, pp. 292-301, 1997.

［9］ M. Daberkow, C. Fieker, J. Klners, M. Pohst, K. Roegner, M. Schrnig, K. Wildanger：“KANT V4,” J. Symb. Comp. , Vol. 24, No3, pp267-283, 1997.

［10］ H. Cohen “A course in computational algebraic number theory” Springer, GTM-138, 1995.

［11］ J. DeJong, R. Noot, “Jacobians with complex multiplication,” Arithmetic Algebraic Geometry, Birkhäuser PM89, pp. 177-192, 1991.

［12］ I. Duursma, P. Gaudry, F. Morain, “Speeding up the discrete log computation on curves with automorphisms,” LIX/RR/99/03, Ecole Polytech. , 1999.

［13］ S. D. Galbrath, S. Paulus, N. P. Smart：“Arithmetic on superelliptic curves,” preprint.

［14］ N. D. Elkies, “Elliptic and modular curves over finite fields and related computational issues,” Computational Perspective on Number Theory in honor of A. O. L. Atkin, 1995.

［15］ G. Frey, H. G. Rück：“A remark concerning m-divisibility and the discrete logarihm in the divisor class group of curves,” Mathematics of Computation, 62, 865-874, 1994.

［16］ P. Gaudry “A variant of the Adelman-DeMarrais-Huang algorithm and its application to small genera” Preliminary version, June 1999.

［17］ P. Gaudry, R. Harley, “Counting Points on Hyperelliptic Curves over Finite Fields,” ANTS-IV, Springer, LNCS1838, pp. 297-312, 2000.

［18］ T. Haga, K. Matsuo, J. Chao, S. Tsujii：“Construction of CM Hyperelliptic Curve using Ordinary Liftings”, IEICE, Japan, Proc. of SCIS2000, C51, 2000.

［19］ M. D. Huang, D. Ierardi：“Counting Rational Point on Curves over Finite Fields,” Proc. 32nd IEEE Symp. on the Foundations of Computers Science, 1993.

［20］ T. Honda：“Isogeny classes of abelian varieties over finite fields,” J. Math. Soc. Japan, vol. 20, No. 1-2, p. 83-95, 1968.

［21］ J. Igusa：“Arithmetic variety of moduli for genus two,” Ann. of Math. , vol. 72, No. 3, p. 612-649, 1960.

［22］ H. Kawashiro, O. Nakamura, J. Chao, S. Tsujii：“Construction of CM hyperelliptic curves using RM family,” IEICE ISEC97-72, pp. 43-49, 1998.

［23］ J. Klüners, M. Pohst：“On Computing Subfields,” J. Symbolic Computation, 11, 1996.

［24］ H. Kuboyama, K. Kamio, K. Matsuo, J. Chao, S. Tsujii：“Construction of Superelliptic Curve Cryptosystem”, IEICE, Japan, Proc. of SCIS2000, C52, 2000.

［25］ N. Koblitz：“Elliptic Curve Cryptosystems,” Math. Comp. , vol. 48, p. 203-209, 1987.

［26］ N. Koblitz：“Hyperelliptic cryptosystems,” J. of Cryptology, vol. 1, p, 139-150, 1989.

［27］ N. Koblitz, “A very easy way to generate curves over prime field for hyperelliptic cryptosystem,” CRYPTO’97, Ramp session, 1997.

［28］ S. Lang：“Abelian Varieties”, Interscience, New York 1959.

［29］ S. Lang：“Complex multiplication” Springer-Verlag, 1983.

［30］ H. W. Lenstra：“Algorithms in Algebraic Number Theory,” Bulletin of The Amer. Math. Soc. , 2, vol. 26, pp. 211-244, 1992.

［31］ K. Matsuo, J. Chao, S. Tsujii：“On lifting of CM hyperelliptic curves,” IEICE Proc. SCIS’99, 1999.

［32］ A. Menezes, S. Vanstone, T. Okamoto：“Reducing Elliptic Curve Logarithms to Logarithms in a Finite Fields,” Proc. of STOC, p. 80-89, 1991.

[33] A. Menezes：“Elliptic Curve Public Key Cryptosystems”, Kluwer Academic, 1993.
[34] V. S. Miller：“Use of Elliptic Curves in Cryptography,” Advances in Cryptology Proceedings of Crypto'85, Lecture Notes in. Computer Science, 218, Springer-Verlag, p. 417-426, 1986.
[35] D. Mumford：“Abelian varieties”, Tata Studies in Mathematics, Oxford , Bobay, 1970.
[36] D. Mumford：“Tata Lectures on Theta Ⅰ”, Birkhäuser, Boston, 1983.
[37] D. Mumford：“Tata Lectures on Theta Ⅱ”, Birkhäuser, Boston, 1984.
[38] V. Müller, A. Stein, C. Thiel：“Computing discrete logarithms in real quadratic congruence function fields of large genus” Preprint, Nov. 13, 1997.
[39] K. Nagao, “Construction of the Jacobians of Curves $Y^2=X^5+k/\mathbb{F}_p$ with Prime Order,” Manuscript, 1998.
[40] F. Oort, T, Sekiguchi：“The canonical lifting of an ordinary jacobian variety need not be a jacobian variety,” J. Math. Soc. Japan, Vol. 38, no. 3, 1986.
[41] S. Paulus：“Ein Algorithmus zur Berechunung der Klassengruppe quadratischer Ordnungen,” über Hauptidealringen, GH Essen, Dr. Thesis, 1996.
[42] J. Pila：“Frobenius maps of abelian varieties and finding roots of unity in finite fields,” Math. Comp. , vol. 55, p. 745-763, 1990.
[43] B. Poonen：“Computational aspects of curves of genus at least 2,” H. Cohen（Ed）“Algorithmic number theory” Lecture Notes in Computer Science, 1122, Second International Symposium, ANTS-Ⅱ, Proceedings, pp. 283-306. 1996.
[44] M. Pohst, H. Zassenhaus：“Algorithmic Algebraic Number Theory,” Cambridge, 1989.
[45] M. Pohst：“Computational Algebraic Number Theory,” DMV21, Birkhäuser, 1993.
[46] H. G. Rück：“on the discrete logarithm problem in the divisor class group of curves” Preprint, 1997.
[47] R. Schoof：“Elliptic curves over finite fields and the computation of square roots mod p,” Math. Comp. , vol. 44, p. 483-494, 1985.
[48] J. P. Serre, J. Tate：“Good reduction of abelian varieties,” Ann. of Math.（2）, 88 1968, page 492-517.
[49] G. Shimura：“Introduction to arithmetic theory of automorphic function,” Iwanami-Shoten and Princeton, 1971.
[50] G. Shimura, Y. Taniyama：“Complex multiplication of abelian varieties and its application to number theory,” Pub. Math. Soc. Jap. no. 6, 1961.
[51] G. Shimura：“Abelian Varieties with Complex Multiplication and Modular Functions,” Princeton Univ. Press, 1998.
[52] A-M. Spallek：“Kurven vom Geschlecht 2 und ihre An-wendung in Public-Key-Kryptosystemen”, Dissertation, preprint, No. 18, 1994.
[53] J. Tate：“Endomorphisms of Abelian varieties over finite fields”, Invent. Math. 2, p. 134-144, 1966.
[54] S. Uchiyama, T. Saitoh：“A Note on The Discrete Logarithm Problem on Elliptic Curves of Trace Two,” IEICE Japan Tech. Rep. ISEC98-27, pp. 51-57, 1998.
[55] E. J. Volcheck：“Computing in the Jacobian of a plane algebraic curve”, Proc. of ANT-1, p. 221-233, LNCS-877, 1994.
[56] T. Wakabayashi, T. Nakamizo, K. Matsuo, J. Chao, S. Tsujii：“Computation of Weil Number of CM Varieties and Design of Jacobian Cryptosystems”, IEICE, Japan, Proc. of SCIS2000, C50, 2000.
[57] P. V. Wamelen：“Examples of genus two CM curves defined over the rationals,” Math. Comp. , 68 (225), pp. 308-320, 1999.
[58] P. V. Wamelen：“PROVING THAT A GENUS 2 CURVE HAS COMPLEX MULTIPLICATION”, Math. Comp. , vol. 68,（1999）pp, 1663-1677.

［59］ W. C. Waterhouse：“Abelian varieties over finite fields” Ann. scient. EC. Norm. Sup. 4°t. 2, 1969, p. 521-560

［60］ H. J. Weber：“Hyperelliptic Simple Factor of J_0（N）with Dimension at Least 3”, Experimental Math. , vol6, 1997.

［61］ X. Wang：“2-dimensional simple factors of $J_0(N)$”, manuscripta math. , 87, pp. 179-197, 1995.