虚数乗法論を用いた超楕円曲線暗号の構成

松尾和人 (東洋通信機)
趙晋輝 (中央大学)
辻井重男 (中央大学)

CM超楕円曲線

- Jacobi多様体がCMを持つ超楕円曲線

超楕円曲線を用いた
暗号系の構成

安全な位数を持つ超楕円曲線が必要

位数が計算できる曲線が必要

CM超楕円曲線

CM超楕円曲線を用いた暗号系の構成

- CM超楕円曲線の構成
  - Spallek,Wamelen,Murabayashi-Umegaki
  - Liftingによる方法
- 有限体上での位数計算

定義

C : 体F上のHEC

$\mathrm{charF} \neq 2$

$Y^2 = f(\mathrm{X})$

$f \in F[X], \deg f = 2g + 2 or 2g + 1, discf \neq 0$

g : Cのgenus

$\mathbf{J}_c$: CのJacobi多様体

K : $\mathbf{J}$のGalois CM体

d_k : Kのdiscriminant

O_K : Kのmaximal order

π : $\mathbf{J}$の$\mathbf{F}_p$上のFrobenius endo

χ : πの特性多項式

Q上種数2のCM超楕円曲線の生成

1. CM体KとCMtype(K,Φ)を選択;
2. CM体K'で完全分解する素数pを選択;
   ($ordinaly\ reduction$)
3. $\mathbf{F}_p$上の種数2の全超楕円曲線CのCMtypeを計算;
4. $CMtype$が(K,Φ)なる曲線をテーブル化;
5. テーブル内の曲線から$End(\mathbf{J})\cong O_K$なる
   曲線を選択しinvariantを計算;
6. $step1-step4$をいくつかのpに対して行い
   invariantをCRTでliftする

$\mathbf{F}_p$上で与えられたCMtypeを持つ曲線の選択

- Cmtypeからp-Frobenius endomorphismの特性多項式を計算(テーブル作成）
- $\mathbf{F}_p$上の各曲線のJacobi多様体のp-Frobenius endomorphisumの特性多項式を計算
- 特性多項式を比較

テーブル作成

$\mathfrak{p} \supset p : O_{K'}$ の素イデアル

$$(\pi) = \prod_{i=1}^{2} \varphi_i'(\mathfrak{p}) \subset O_K$$

1. pを$O_{K'}$上で素イデアル分解し$\mathfrak{p}$を得る
2. (π)を計算
3. πを計算
4. πの特性多項式$\chi(t)$を計算

$$K = \mathbf{Q}(\alpha), \alpha = \sqrt{-2+\sqrt{2}}.$$

$g(t) = t^4 + 4t^4 + 2 : \alpha$の$Q$上の最小多項式

$$(K, \{\varphi_1, \varphi_2\})$$

$$\varphi_1 : \alpha \mapsto \alpha$$

$$\varphi_2 : \alpha \mapsto -3\alpha - \alpha^3$$

$$(K' = K, \{\varphi_1', \varphi_2'\})$$

$$\varphi_1' : \alpha \mapsto \alpha$$

$$\varphi_2' : \alpha \mapsto 3\alpha + \alpha^3$$

$$g \equiv (t+1)(t+3)(t+4)(t+6) \bmod 7$$

$$p = 7$$

$$(7) = \prod_{\sigma \in Gal(K/\mathbf{Q})} \sigma(\langle 7, 4+\alpha \rangle)$$

$$(\pi_0) = (3 - 2\alpha + \alpha^2 - \alpha^3)$$

$$\chi(t) = t^4 - 4t^3 + 10t^2 - 28t + 49$$

$\mathbf{F}_p$上で与えられたCmtypeを持つ曲線の選択

- *Cmtypeからl-Frobenius endomorphismの特性多項式を計算(テーブル作成）*
- **$\mathbf{F}_p$上の各曲線のJacobi多様体の*p*-Frobenius endomorphisumの特性多項式を計算**
- **特性多項式を比較**

$\chi(t)$の計算

$$\chi(t) = t^4 - s_1 t^3 + s_2 t^2 - s_1 pt + p^2 \ \ where\ s_1, s_2 \in \mathbf{Z}$$

$$1:\ s_1 = \#C(\mathbf{F}_p) - p - 1$$

$$s_2 = \frac{s_1^2 + \#C(\mathbf{F}_{p^2}) - p^2 - 1}{2}$$

$$2:\ s_1 = \frac{\#\mathbf{J}_t(\mathbf{F}_p) - \#\mathbf{J}(\mathbf{F}_p)}{2(l+1)}$$

$$s_2 = -\frac{\#\mathbf{J}_t(\mathbf{F}_p) + \#\mathbf{J}(\mathbf{F}_p)}{2} - p^2 - 1\ (Elkies)$$

$\mathbf{J}_t$: Cの2次ツイストC_tのJacobi多様体

$\chi(t)$のチェック

$$\chi_T(t) = t^4 - S_1 t^3 + S_2 t^2 - S_1 p t + p^2$$

例） $\chi_T(t) = t^4 - 4t^3 + 10t^2 - 28t + 49$

$$\Rightarrow S_1 = 4, S_2 = 10$$

$s_1 = S_1, s_2 = S_2$ならば残す

これを$\mathbf{F}_p$上の全てのCに対して行う

$$Y^2 = a_6 X^6 + a_5 X^5 + a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0$$

$\Rightarrow p^7$回

探索直線数の削減

$p \neq 2,5$のとき

$$Y^2 = X^6 + \{0,1,\gamma_4,\gamma_4^2,\gamma_4^3\}X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$$

$$Y^2 = X^5 + \{0,1,\gamma_2\}X^3 + a_2X^2 + a_1X + a_0$$

$a_i \in \mathbf{F}_p, \gamma_2 \in \mathbf{F}_p$: 平方非剰余数,

$\gamma_4 \in \mathbf{F}_l$: 平方非剰余且つ４乗非剰余数

$\Rightarrow p^4$回

$\gamma_4 \notin \mathbf{F}_p$

$$Y^2 = X^6 + \{0,1,\gamma_2\}X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$$

deg$f$=6の時のチェック

- fが$\mathbf{F}_p$上に根を持つならば終了
  $\gcd(f, X^p - X) \neq 1$
- $\mathbf{F}_p$-有理点を数えてをs_1, s_2を求める
- $s_1 \neq \pm S_1$ならば終了
- $\mathbf{F}_{p^2}$ -有理点を数えてをs_2を求める
- $s_2 = S_2$ならば与えられたCMtypeである

deg$f$=5の時のチェック

$$\#\mathbf{J}(\mathbf{F}_p)=\chi(1), \#\mathbf{J}_t(\mathbf{F}_p)=\chi(-1)$$

$$^\forall D\in\mathbf{J}(\mathbf{F}_p), [\chi(1)]D=0$$

$$^\forall D\in\mathbf{J}_t(\mathbf{F}_p), [\chi(-1)]D=0$$

例） $\chi(t)=t^4-4t^3+10t^2-28t+49$

$$\#\mathbf{J}(\mathbf{F}_7)=\chi(1)=28, \#\mathbf{J}_t(\mathbf{F}_7)=\chi(-1)=92$$

deg$f$=5の時のチェック

1. $D \in \boldsymbol{J}(\mathbf{F}_p)$に対して$[\chi(-1)]D=0$
   $D \in \boldsymbol{J}_t(\mathbf{F}_p)$に対して$[\chi(1)]D=0$をテスト
   - 成立したら$C=Ct$とする
2. $D \in \boldsymbol{J}(\mathbf{F}_p)$に対して$[\chi(1)]D=0$
   $D \in \boldsymbol{J}_t(\mathbf{F}_p)$に対して$[\chi(-1)]D=0$をテスト
   - 成立しなければ終了
   - 数回繰り返す
3. 有理点を数えてをs_1,s_2を求める
   - $s_1=S_{1,}\ s_2= S_2$ならば与えられたCMtypeである

$$\chi(t) = t^4 - 4t^3 + 10t^2 - 28t + 49$$

$$Y^2 = f_i(X)$$

$$f_1 = X^5 + X^2 + X$$

$$f_2 = X^5 + 5X^2 + X + 3$$

$$f_3 = X^5 + X^3 + 6X^2 + X$$

$$f_4 = X^5 + X^3 + 4X^2 + 4X$$

$\mathbf{Q}$上種数2のCM超楕円曲線の生成

1. CM体KとCMtype(K,Φ)を選択;
2. CM体K'で完全分解する素数pを選択;
   $(ordinaly\ reduction)$
3. $\mathbf{F}_p$上の種数2の全超楕円曲線CのCMtypeを計算;
4. $CMtype$が(K,Φ)なる曲線をテーブル化;
5. テーブル内の曲線から$End(\mathbf{J})\cong O_K$なる曲線を選択しinvariantを計算;
6. $step1-step4$をいくつかのpに対して行いinvariantをCRTでliftする

Kohelの方法
End(E)の決定法

$E:\mathbf{F}_l$上のordinary楕円曲線

$K:E$のCM体

$O_K\;:K$のmaximal order

$\pi:$ Eの$\mathbf{F}_l$上のFrobenius endo.

$m:\mathbf{Z}[\pi]$のconductor

$$\mathbf{Z}[\pi]\subseteq End(E)\subseteq O_K$$

$$End(E)=\mathbf{Z}+cO_K$$

なる$c\in\mathbf{Z}$を求める

$$^{\exists}a \in \mathbf{Z} \quad s.t. \quad O_K = \mathbf{Z}\left[\frac{\pi - a}{m}\right]$$

$$^{\forall}n \quad s.t. \quad n \mid m$$

$$E[n] \subseteq \ker(\pi - a) \Leftrightarrow End(E) \supseteq \mathbf{Z}\left[\frac{\pi - a}{n}\right]$$

$$m = l_1^{e_1} l_2^{e_2} \cdots l_i^{e_i} \cdots \quad (l_i : \text{素数})$$

各素数l_iに対し

$$E\left[l_i^{j_i}\right] \subseteq \ker(\pi - a), E\left[l_i^{j_i+1}\right] \not\subset \ker(\pi - a)$$

なるjを求める。(division polynomialを利用)

$$End(E) = \mathbf{Z} + cO_K$$

$$c = \frac{m}{\prod l_i^{j_i}}$$

定義

$C : \mathbf{F}_p$上のordinaryHEC

$v^2 = h(u)$

$= u^{2g+1} + a_1 u^{2g} + \cdots + a_{2g}$

$a_i \in \mathbf{F}_p$

g : Cのgenus

$\mathbf{J}$: CのJacobi多様体

$K : \mathbf{J}$のGalois CM体

$d_k : K$のdiscriminant

$O_K : K$のmaximal order

$\pi : \mathbf{J}$の$\mathbf{F}_p$上のFrobenius endo.

$z : \pi$の特性多項式

End(**J**)の決定

$\mathbf{Z}[\pi] \subseteq O \subseteq O_K, O \cong End(\mathbf{J})$
なるOを求める。

与えられた$End(\mathbf{J})$であるかどうかをチェックする

整数環の整基底

α : 代数的整数

$F = \mathbf{Q}(\alpha), [F : Q] = n$

$g(t) \in \mathbf{Z}[t]$: αのmin.poly.

$d(g)$: gのdiscriminant

O_Fの$\mathbf{Z} - basis$

$[1, \omega_1, \cdots, \omega_{n-1}]$

$$\omega_i = \frac{f_i(\alpha)}{m_i}$$

$f_i \in \mathbf{Z}[t]$, $\deg f_i = i$

$m_i \in \mathbf{Z}$, $m_i \mid m_{i+1}$

$$d(g) = \left(\prod_{i=1}^{n-1} m_i \right)^2 d_K$$

$g(t)$から求まる。

End(J)の決定

O_Kの$\mathbf{Z}-basis$を$\chi(t)$から計算

$$\mathbf{B}_{o_K} = (1, \omega_1, \cdots, \omega_3), \ \omega_i = \frac{g_i(\pi)}{m_i}$$

$$g_i \in \mathbf{Z}[t], \deg g_i = i \ , \ m_i \in \mathbf{Z} \ , \ m_i \mid m_{i+1}$$

$$\mathbf{Z}[\pi] = \mathbf{Z} + \mathbf{Z}m_1\omega_1 + \cdots + \mathbf{Z}m_3\omega_3$$

$\mathbf{Z}[\pi] \subseteq O \subseteq O_K$なる$O$を全て求める

$$\chi(t) = t^4 - 4t^3 + 10t^2 - 28t + 49$$

O_Kの$\mathbf{Z}-basis$を$\chi(t)$から計算

$$\mathbf{B}_{O_K} = \begin{pmatrix} 1 & \omega_1 & \cdots & \omega_3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \pi & \dfrac{\pi^2+1}{2} & \dfrac{\pi^3+3\pi^2-11\pi+7}{28} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \pi & \pi^2 & \pi^3 \end{pmatrix} \begin{pmatrix} 1 & 0 & \dfrac{1}{2} & \dfrac{7}{28} \\ 0 & 1 & \dfrac{1}{2} & -\dfrac{11}{28} \\ 0 & 0 & 0 & \dfrac{3}{28} \\ 0 & 0 & 0 & \dfrac{1}{28} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathbf{Z}[\pi] = \mathbf{Z} + \mathbf{Z}m_1\omega_1 + \cdots + \mathbf{Z}m_3\omega_3$$

$$\mathbf{B}_{\mathbf{Z}[\pi]} = \begin{pmatrix} 1 & \pi & \pi - 1 & \pi^3 + 3\pi^2 - 11\pi + 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \pi & \pi^2 & \pi^3 \end{pmatrix} \begin{pmatrix} 1 & 0 & \frac{1}{2} & \frac{7}{28} \\ 0 & 1 & \frac{1}{2} & -\frac{11}{28} \\ 0 & 0 & 0 & \frac{3}{28} \\ 0 & 0 & 0 & \frac{1}{28} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 28 \end{pmatrix}$$

$$\mathbf{Z}[\pi] \subseteq O \subseteq O_K$$

$$\mathbf{B}_{\mathbf{Z}[\pi]} : (a_{ij}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 28 \end{pmatrix} \Rightarrow \mathbf{B}_O : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \{1,2\} & \{0,1\} \\ 0 & 0 & 0 & \{1,2,4,7,14,28\} \end{pmatrix}$$

$$\mathbf{B}_O : \begin{pmatrix} b_{11} \mid a_{11} & 0 \le b_{12} < b_{11} & b_{13} & b_{14} \\ 0 & b_{22} \mid a_{22} & 0 \le b_{23} < b_{22} & b_{24} \\ 0 & 0 & b_{33} \mid a_{33} & 0 \le b_{34} < b_{33} \\ 0 & 0 & 0 & b_{44} \mid a_{44} \end{pmatrix}$$

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&1\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&2\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&0\\0&0&0&2\end{pmatrix}$$

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&4\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&0\\0&0&0&4\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&7\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&0\\0&0&0&7\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&14\end{pmatrix}$$

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&0\\0&0&0&14\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&28\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&2&0\\0&0&0&28\end{pmatrix}$$

$\mathbf{Z}[\pi] \subset O' \subset O_K$

O'の$\mathbf{Z}-basis$に対応する写像が$End(\mathbf{J})$に存在するならば

$O' \subseteq O \cong End(\mathbf{J})$

O'を替えて繰り返せば$O \cong End(\mathbf{J})$が求まる。

$\underline{O \cong End(\mathbf{J})\text{となる曲線を求める}}$

Oの$\mathbf{Z}-basis$に対応する写像が$End(\mathbf{J})$に存在し、

$O' \supset O$の$\mathbf{Z}-basis$に対応する写像が

$End(\mathbf{J})$に存在しない曲線を求める。

$$\mathbf{B}_o = (1, \omega_1, \cdots, \omega_3),\ \omega_i = \frac{g_i(\pi)}{m_i}$$

$$\begin{aligned}\omega_i \in O \cong End(\mathbf{J}) &\Leftrightarrow \mathbf{J}[m_i] \subseteq \ker(g_i(\pi)) \\ &\Leftrightarrow \mathbf{J}\left[l_j^{e_j}\right] \subseteq \ker(g_i(\pi)),\ {}^{\forall} l_j^{e_j}\ s.t\ m_i = \prod l_j^{e_j}\end{aligned}$$

$${}^{\forall} i, \omega_i \in O \Leftrightarrow O \subseteq End(\mathbf{J})$$

$$\mathbf{B}_{O_K} = \begin{pmatrix} 1 & \pi & \dfrac{\pi^2+1}{2} & \dfrac{\pi^3+3\pi^2-11\pi+7}{28} \end{pmatrix}$$

従って

$$End(\mathbf{J}) \cong O_K \Leftrightarrow \begin{cases} \mathbf{J}[2] \subseteq \ker(\pi^2-1) = \mathbf{J}(\mathbf{F}_{7^2}) \\ \mathbf{J}[4] \subseteq \ker(\pi^3+3\pi^2+\pi+3) \\ \mathbf{J}[7] \subseteq \ker(\pi^3+3\pi^2+3\pi) \end{cases}$$

$\mathbf{J}[l^e] \subset \ker(g(\pi))$のチェック

$step1 : D \in \mathbf{J}\left[q^e\right]$を選ぶ;

$step2 : g(\pi)D = 0$を確かめる;

step1 - step2を繰り返し

$\exists D \; s.t. \; g(\pi)D \neq 0 \Rightarrow \mathbf{J}\left[l^e\right] \not\subset \ker(g(\pi))$

$\nexists D \; s.t. \; g(\pi)D \neq 0 \Rightarrow \mathbf{J}\left[l^e\right] \subseteq \ker(g(\pi))$

Dは$\mathbf{J}\left[l^e\right]$の基底から選べば十分

$D \in \mathbf{J}[l^e]$の選択

- Division polynomial の利用
  - Cantor, Kanayama
  - genus 2
- 探索的方法
  - $\chi(t)$から拡大体上の位数を知ることができる
  - memory必要

$D \in \mathbf{J}[l^e]$の探索

$step\,1: \chi(t)$を用いて$l^e \mid \#\mathbf{J}\left(\mathbf{F}_{p^n}\right)$となる$n$を決定する;

$step\ 2: e_s$ s.t. $l^{e_s} \parallel \#\mathbf{J}\left(\mathbf{F}_{p^n}\right)$を求める;

$step\,3:$ Baby-step giant-step法を用いて

$\mathbf{J}\left[l^{e_s}\right] \cap \mathbf{J}\left(\mathbf{F}_{p^n}\right)$の群構造と生成系を求める;

$step\ 4: \mathbf{J}\left[l^{e}\right] \cap \mathbf{J}\left(\mathbf{F}_{p^n}\right)$の生成系を求める;

$\mathbf{J}[l^e] \cap \mathbf{J}(\mathbf{F}_{p^n})$ の群構造決定

$step\,1 : O_r = {}^{\#\mathbf{J}\left(\mathbf{F}_{p^n}\right)}\!\big/_{l^{e_s}}$ を求める;

$step\,2 : D_i \in \mathbf{J}\left(\mathbf{F}_{p^n}\right)$をランダムに選ぶ;

$step\,3 : D_i = O_r D_i;$

$$step4 : \mathbf{0} = \mathbf{A}\begin{pmatrix} D_1 \\ \vdots \\ D_i \end{pmatrix}; \mathbf{A} : i \times i\ matrix$$

$step5 : \mathbf{A}$のSNF $\mathbf{S}$を求める。

$step6 : \mathbf{S}$の対角要素の積がl^{e_s}でなければ$step\,2$へ;

Example

$$Y^2 = f_i(X)$$

$$f_1 = X^5 + X^2 + X$$

$$f_2 = X^5 + 5X^2 + X + 3$$

$$f_3 = X^5 + X^3 + 6X^2 + X$$

$$f_4 = X^5 + X^3 + 4X^2 + 4X$$

$$End(\mathbf{J}) \cong O_K \Leftrightarrow \begin{cases} \mathbf{J}[2] \subseteq \ker(\pi^2 - 1) = \mathbf{J}(\mathbf{F}_{7^2}) \\ \mathbf{J}[4] \subseteq \ker(\pi^3 + 3\pi^2 + \pi + 3) \\ \mathbf{J}[7] \subseteq \ker(\pi^3 + 3\pi^2 + 3\pi) \end{cases}$$

J[2]$\subset$ker(π^2-1)のチェック

各 f_i に対して

$$X^{49} - X = 0 \bmod f_i$$

をチェック

$$X^{49} - X \begin{cases} = 0 \bmod f_i & ;\mathrm{i} = 2,4 \\ \neq 0 \bmod f_i & ;\mathrm{i} = 1,3 \end{cases}$$

$$f_2 = u^5 + 5u^2 + u + 3$$

$$f_4 = u^5 + u^3 + 4u^2 + 4u$$

$\mathbf{J}[2] \subseteq \ker(\pi^2 - 1) = \mathbf{J}(\mathbf{F}_{7^2})$のチェック

各iに対して

$$u^{49} - u = 0 \bmod h_i$$

をチェック

$$u^{49} - u \begin{cases} = 0 \bmod h_i \ ;\mathrm{i} = 2,4 \\ \neq 0 \bmod h_i \ ;\mathrm{i} = 1,3 \end{cases}$$

$$h_2 = u^5 + 5u^2 + u + 3$$

$$h_4 = u^5 + u^3 + 4u^2 + 4u$$

$\mathbf{J}[m] \subset \ker(g(\pi))$のチェック

$step0 : d \in \mathbf{J}[n]$を含む$\mathbf{F}_p$の拡大$\mathbf{F}_{p^l}$を決定;

$step1 : nd = 0$なるdivisor $d \in \mathbf{J}(\mathbf{F}_{p^l})$をランダムに選択;

$step2 : f(\pi)d = 0$をチェック;

step1 - step2を繰り返し

$\exists d \ s.t. f(\pi)d \neq 0 \Rightarrow \mathbf{J}[n] \not\subset \ker(f(\pi))$

$\nexists d \ s.t. f(\pi)d \neq 0 \Rightarrow \mathbf{J}[n] \subseteq \ker(f(\pi))$

$d \in \mathbf{J}[n]$を含む拡大次数の探索

$step0 : i := 1;$

$step1 : \#\mathbf{J}\left(\mathbf{F}_{p^i}\right)$を計算;

$step2 : n \nmid \#\mathbf{J}\left(\mathbf{F}_{p^i}\right)$ならば$i := i + 1;$ goto $step1;$

$step3 :$ iを出力;

$d \in \mathbf{J}[n]$の探索

$step0 :\#\mathbf{J}\left(\mathbf{F}_{p^l}\right) = q^{e_1} s$を計算$\left(q : prime \mid n = q^e\right)$;

$step\,1 : d_0 \in \mathbf{J}\left(\mathbf{F}_{p^l}\right)$をランダムに選択;

$step2 : d_1 := sd_0$を計算;

$step\,3 : \mathrm{i} := 2;$

$step4 : d_i := qd_{i-1}$を計算;

$step\,5 : d_i \neq 0$ならば$\mathrm{i} := \mathrm{i} + 1;\ \mathrm{goto}\ step4;$

$step\,6 : d_{i-e}$を出力;

Example

CM体$K := \mathbf{Q}\left(\sqrt{-2+\sqrt{2}}\right)$

$d_K = 2048$

$c_K = 1$

$End(\mathbf{J}) \cong O_K$なる曲線を$\mathbf{F}_7$上で求める

$v^2 = u^5 - 140u^3 - 240u^2 + 3810u + 6928$ (Spallek curve)

$$p = 7;$$

$$z(\pi) = \pi^4 - 4\pi^3 + 10\pi^2 - 28\pi + 49$$

$$v^2 = h_i(u)$$

$$h_1 = u^5 + u^2 + u$$

$$h_2 = u^5 + 5u^2 + u + 3$$

$$h_3 = u^5 + u^3 + 6u^2 + u$$

$$h_4 = u^5 + u^3 + 4u^2 + 4u$$

$$d(z) = (2^3 \cdot 17)^2 d_K$$

O_K の $\mathbf{Z}$-*basis*

$$\left[1, \pi, \frac{\pi^2+1}{2}, \frac{\pi^3+3\pi^2+17\pi+35}{28}\right]$$

$\Rightarrow$

$$\left[1, \pi, \frac{\pi^2-1}{2}, \frac{\pi^3+3\pi^2+17\pi+35}{28}\right]$$

従って

$$End(\mathbf{J}) \cong O_K \Leftrightarrow \begin{cases} \mathbf{J}[2] \subseteq \ker(\pi^2-1) = \mathbf{J}(\mathbf{F}_{7^2}) \\ \mathbf{J}[4] \subseteq \ker(\pi^3+3\pi^2+17\pi+35) \\ \mathbf{J}[7] \subseteq \ker(\pi^3+3\pi^2+17\pi+35) \end{cases}$$

$\mathbf{J}[7] \subseteq \ker(\pi^3 + 3\pi^2 + 17\pi + 35)$のチェック

全ての候補は

$$\mathbf{J}[7] \subseteq \ker(\pi^3 + 3\pi^2 + 17\pi + 35)$$

を満足する。

$\mathbf{J}[2] \subseteq \ker(\pi^2 - 1) = \mathbf{J}(\mathbf{F}_{7^2})$のチェック

各iに対して

$$u^{49} - u = 0 \bmod h_i$$

をチェック

$$u^{49} - u \begin{cases} = 0 \bmod h_i & ;\mathrm{i} = 2,4 \\ \neq 0 \bmod h_i & ;\mathrm{i} = 1,3 \end{cases}$$

$$h_2 = u^5 + 5u^2 + u + 3$$

$$h_4 = u^5 + u^3 + 4u^2 + 4u$$

$\mathbf{J}[4] \subseteq \ker(\pi^3 + 3\pi^2 + 17\pi + 35)$のチェック

$\mathbf{J}[4]$を含む$\mathbf{F}_7$の拡大体上で

$4d = 0$

なるdivisor dをランダムに選び

$(\pi^3 + 3\pi^2 + \pi + 3)d = 0$

をチェック

$^{\exists} d \in \mathbf{J}[4]\ s.t.\ (\pi^3 + 3\pi^2 + \pi + 3)d \neq 0$

$\Rightarrow$

$\mathbf{J}[4] \not\subset \ker(\pi^3 + 3\pi^2 + 17\pi + 35)$

$\mathbf{F}_{7^4}$上で

$\#\mathbf{J}\left(\mathbf{F}_{7^4}\right) = 2^{11} \cdot 2737$

$step\,1 : d_0 \in \mathbf{J}\left(\mathbf{F}_{7^4}\right)$をランダムに選択;

$step2 : d_1 := 2737 d_0$を計算;

$step\,3 : \mathrm{i} := 2;$

$step4 : d_i := 2 d_{i-1}$を計算;

$step\,5 : d_i \neq 0$ならば$\mathrm{i} := \mathrm{i} + 1;$ goto $step4;$

$step\,6 : \left(\pi^3 + 3\pi^2 + 17\pi + 35\right) d_{i-e} = 0$ならばgoto $step1;$

$step\,7 :$ $false$を出力;

$$h_2 \Rightarrow \mathbf{J}[4] \subseteq \ker\left(\pi^3 + 3\pi^2 + 17\pi + 35\right)$$
$$h_4 \Rightarrow \mathbf{J}[4] \not\subset \ker\left(\pi^3 + 3\pi^2 + 17\pi + 35\right)$$

従って

$End(\mathbf{J}) \cong O_K$

なる曲線は

$v^2 = u^5 + 5u^2 + u + 3$

(Igusa invariantがSpallek curveと同じ)

まとめと今後の課題

- 有限体上のordinary超楕円曲線のEnd(**J**)の決定法を検討した。
- 本手法を用いてCM超楕円曲線を生成する。