No. ⑥

Date 1・7・

効率的な超特異性判定アルゴリズムについて　　橋本（東京電機）

＝ supersingular testing

Supersingular testing とは？

ある楕円曲線 E（over $\mathbb{F}_q$, $q = p^n$, p は素数）が与えられたとき，E が ordinary か supersingular かを判定するアルゴリズム．

（イメージの為の補足

［素数判定］…… $x \in \mathbb{N}_{>1}$ が素数かどうかを判定する．）

Supersingularity testing algorithm には，以下の2タイプがある：

- probablistic algorithm → determistic alorithm に比べて，$\tilde{O}(n^2)$ （$n = \log_2 p$）なので効率的だが，supersingular curve であることを示せない．（$\tilde{O}$：poly log は無視する．）
- determistic algorithm → prob. algo. に比べて非効率で $\tilde{O}(n^3)$ の計算量が必要．ただし，結果が数学的に保証される．

Notions.

$p \geq 5$ なる素数に対して $\mathbb{F}_p$ を素体，$\overline{\mathbb{F}_p}$ を $\mathbb{F}_p$ の代数閉包とする．

$\mathbb{F}_{p^2}$：2次拡大体．

Isogeny graph

- vertex：楕円曲線の同型類
- edge：Isogeny

楕円曲線 / $\mathbb{F}_q$.

$\mathbb{F}_q$ 上の種数 1 の 非特異代数曲線 を 楕円曲線 という.

Example

$p \geq 5$ のとき, 任意の楕円曲線は以下のような short Weierstrass model で与えられる.

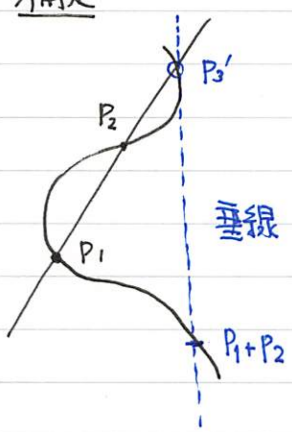
$E : \quad y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_q,\ 4a^3 + 27b^2 \neq 0)$ □

E を以下, $\mathbb{F}_q$ 上の楕円曲線 とする.

$$E(\mathbb{F}_q) := \{ (x, y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + ax + b \} \cup \{ \infty \}$$

ここにアーベル群の構造を入れたものを 有理点群 (Mordell - Weil 群) と呼ばれる.

補足



- 単位元 ∞
- 逆元 : $P = (x, y)$ に対して $-P = (x, -y)$.

E が supersingular $\Leftrightarrow$ $\# E(\mathbb{F}_q) = 1 \mod p$.

Isoginy.

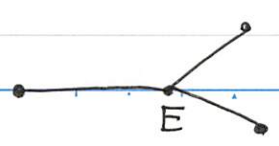
E_1, E_2 : 楕円曲線

群準同型 $\phi : E_1(\mathbb{F}_q) \longrightarrow E_2(\mathbb{F}_q)$ を 同種 (Isogeny) という.
(かつ有理多項式で表せる)

このとき, E_1 と E_2 は Isogenious という.

$p \nmid \ell$ であるような ℓ に対して, $\ker \phi \simeq \mathbb{Z}/\ell\mathbb{Z}$ のとき, ϕ を (separable) ℓ-isogeny という.

(2- isogeny)



n-torsion subgroup

$E[n] = \{ P \in E(\mathbb{F}_q) \mid nP = \infty \}$

このPを torsion point という.

実際に n-isogeny を計算するときは、$P \in E[n]$ の情報が必要である.

Example

$p = 17795587$ として、$E : y^2 = x^3 + x$ に対して, $E[101]$は $\mathbb{F}_p$ の200次拡大に入る.

計算効率化 の point (isogeny) ← 以下の①, ②を効率化するとよい.

① $P \in E[\ell]$ を求める.

② Véluの公式 (または その亜種) を用いる.

$y^2 = x^3 + ax + b$ として, Gを $E(\mathbb{F}_q)$の有限部分群とする.

$G = \{\infty\} \cup G^+ \cup G^-$ ($P \in G^+$ とすれば, $-P \in G^-$ とするように分割する) とする.

↑ ただし, $P \in G^+ \Leftrightarrow -P \in G^-$

$P = (x_P, y_P) \in G^+$ に対して

$$g_P^x := 3x_P^2 + a, \quad g_P^y := -2y_P$$

$$v_P := 2g_P^x \quad u_P := (g_P^y)^2$$

$$v = \sum_{P \in G^+} v_P \quad w = \sum_{P \in G^+} (u_P + x_P v_P)$$

このとき, E/G と f_g は次のように表せる.

$$E/G : y^2 = x^3 + (a - 5v)x + (b - 7w)$$

$$f_g(x, y) = \left(x + \sum_{P \in G^+} \frac{v_P}{x - x_P} - \frac{u_P}{(x - x_P)^2},\ y - \sum_{P \in G^+} \frac{2u_P y}{(x - x_P)^3} - v_P \frac{y - y_P - g_P^x g_P^y}{(x - x_P)^2} \right)$$

$f_g : E \to E/G$ で $\ker f_g \simeq G$.

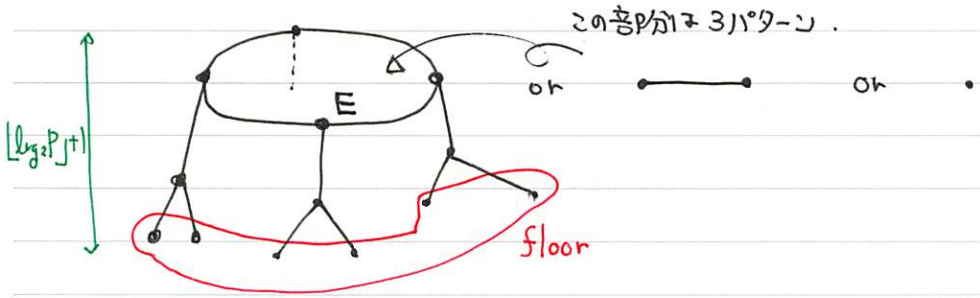
Isogeny graph を用いる方法.

ordinary と supersingular と isogeny graph の構造が異なる.

ordinary curve / $\mathbb{F}_{p^2}$	super curve / $\mathbb{F}_{p^2}$
volcano graph	Ramanujan graph

graph が volcano か Ramanujan かを調べれば, supersingular かどうかがわかる.

Volcano graph ($\ell=2$)



Eの j-invariant は以下のように定義される.

$$j_E = 1728 \frac{4a^3}{4a^3+27b^2}$$

このとき, E_1 と E_2 が 同型 ($/\overline{\mathbb{F}}_q$) と $j_{E_1} = j_{E_2}$ が 同値である.
(as ellipic curve)

Sutherland は モジュラー多項式を使うことにより ℓ-isogeny を計算してグラフを描く.

Modular polynomial. $\Phi_\ell(X,Y)$

Eを固定して, $(j_E, j_1), (j_E, j_2), \cdots, (j_E, j_{\ell+1})$ を根にもつ $\mathbb{Z}$-係数の多項式を $\Phi_\ell(X,Y)$ でかく.
ここで, $j_1, \cdots, j_{\ell+1}$ は E と ℓ-isogenious な j-invariant である.

- ordinary case

  j on Volcano graph $\Longrightarrow$ $j \in \mathbb{F}_q$ ($q=p^2$)
  Otherwise $\Longrightarrow$ $j \notin \mathbb{F}_q$ ($q=p^2$)
  ← このような j をみつけるのがポイント

- supersingular case

  すべての頂点に対して $j \in \mathbb{F}_{p^2}$.

Isogeny graph を用いた supersingularity testing

$\mathbb{F}_{p^2}$ 上の 演算

支配的

R : square or forth root
m : multiplication
i : inverse
c : const. multi

	1step 当たりのコスト
Sutherland	$3R + 9m + 15c$
H.-Takashima	$3R + 3m$
H.-Nuida	$\frac{3}{2}R + \frac{3}{2}i + 6m + \frac{3}{2}c$

そこまで変化はない

変化は大きい.