楕円曲線暗号とその計算機 (PARI/GP) での計算例について

渡邊崇弘

新潟大学大学院自然科学研究科数理物質科学専攻
博士前期課程 2 年

2024 年 2 月 9 日

修士論文について

修士論文の内容

- 第 1 章：第 2 章以降の準備

  (代数多様体，代数曲線，因子)

- 第 2 章：楕円曲線

  (群法則，整数点に関する計算例)

- 第 3 章：有限体上の楕円曲線

  (Hasse の定理，$E(\mathbb{F}_p)$ の計算例)

- 第 4 章：楕円曲線の暗号への応用

  (楕円曲線暗号，DLP を解くアルゴリズムの概要，
  特別な ECDLP に関する計算例)

発表の流れ

§1 楕円曲線

§2 有限体上の楕円曲線

§3 楕円曲線の暗号への応用

参考文献

[PARI] The PARI Group, PARI/GP version 2.15.4, Univ. Bordeaux, 2023, http://pari.math.u-bordeaux.fr/.

[Sil] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition, Graduate Texts in Mathematics 106, Springer-Verlag, 2009, xx+513 pp.

楕円曲線の定義

定義 (完全体 K 上の楕円曲線 [Sil, Ⅲ.1])

ワイエルシュトラス形式

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$(a_1, a_2, a_3, a_4, a_6 \in K)$$

により定義された滑らかな曲線 ($\Delta_E \neq 0$) を K 上の楕円曲線 E という.

$\mathbb{Q}$ 上の楕円曲線の例 [Sil, Ⅲ.2, Example 2.4]

$E : y^2 = x^3 + 17$
$E : y^2 = x^3 + 5x + 11$

楕円曲線の群法則

定義 (楕円曲線 E の群法則 [Sil, Ⅲ.2, Group Law Algorithm 2.3])

楕円曲線 E，E 上の点 $P=(x_1,y_1)$,$Q=(x_2,y_2)$ に対して，次のように演算 $\oplus$ と $\ominus$ を定める：

- $\ominus P=(x_1,-y_1-a_1x_1-a_3)$.
- $P\oplus Q=(\lambda^2+a_1\lambda-a_2-x_1-x_2,-\lambda x_3-a_1x_3-\nu-a_3)$.

λ と ν は次のように定める：

$x_1\neq x_2$のとき

$$\lambda=\frac{y_2-y_1}{x_2-x_1},\ \nu=\frac{y_1x_2-y_2x_1}{x_2-x_1}$$

$x_1=x_2$のとき

$$\lambda=\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3},$$

$$\nu=\frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}.$$

楕円曲線の群法則

定義 (楕円曲線 E の群法則 [Sil, Ⅲ.2, Group Law Algorithm 2.3])

楕円曲線 E，E 上の点 $P=(x_1,y_1)$,$Q=(x_2,y_2)$ に対して，次のように演算 $\oplus$ と $\ominus$ を定める：

- $\ominus P=(x_1,-y_1-a_1x_1-a_3)$.
- $P\oplus Q=(\lambda^2+a_1\lambda-a_2-x_1-x_2,-\lambda x_3-a_1x_3-\nu-a_3)$.

λ と ν は次のように定める：

$x_1\neq x_2$のとき

$$\lambda=\frac{y_2-y_1}{x_2-x_1},\ \nu=\frac{y_1x_2-y_2x_1}{x_2-x_1}$$

$x_1=x_2$のとき

$$\lambda=\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3},$$

$$\nu=\frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3}.$$

- **楕円曲線上の演算は明確だが複雑である.**

楕円曲線の群法則

定義 ($\oplus$ を用いた表記法 [Sil, Ⅲ.2])

$m \in \mathbb{Z}, P \in E$ に対して

- $[m]P := \underbrace{P \oplus \cdots \oplus P}_{m \text{ 個}} \ (m > 0).$
- $[m]P := \underbrace{\ominus P \ominus \cdots \ominus P}_{|m| \text{ 個}} \ (m < 0).$
- $[m]P := O \ \ (m = 0).$

- 楕円曲線離散対数問題に関係がある.

楕円曲線の群法則

定義 ($\oplus$ を用いた表記法 [Sil, Ⅲ.2])

$m \in \mathbb{Z}, P \in E$ に対して

- $[m]P := \underbrace{P \oplus \cdots \oplus P}_{m \text{ 個}} \ (m > 0).$
- $[m]P := \underbrace{\ominus P \ominus \cdots \ominus P}_{|m| \text{ 個}} \ (m < 0).$
- $[m]P := O \ \ (m = 0).$

- 楕円曲線離散対数問題に関係がある.

定義 (モーデル・ヴェイユ群 [Sil, Ⅷ, page 207])

K 上の楕円曲線 E の K 有理点全体と無限遠点 O からなる集合

$$E(K) := \{(x, y) \in E \mid x, y \in K\} \cup \{O\}$$

をモーデル・ヴェイユ群という.

楕円曲線の群法則

定理 (楕円曲線 E, モーデル・ヴェイユ群 $E(K)$ の群構造 [Sil, Ⅲ.2, Proposition 2.2])

(1) E は加法 $\oplus$ により，単位元を無限遠点 O，P の逆元を $\ominus P$ とするアーベル群である．

(2) $E(K)$ は E の部分群である．

$E(\mathbb{Q})$ の例 [Sil, Ⅲ.2, Example 2.4]

(1) $\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 + 17$ において
$\langle (-2, 3), (2, 5) \rangle = E(\mathbb{Q}) = \langle (-2, 3), (-1, 4) \rangle$

(2) $\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 + 5x + 11$ において
$E(\mathbb{Q}) = \{O\}$

- これらは計算機 (PARI/GP) にて確認できる．

計算機 (PARI/GP) による $E(\mathbb{Q})$ に関する計算例

$\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 + 17$ に関する計算例 [Sil, II I.2, Example 2.4]

$E(\mathbb{Q})$ に含まれる整数点は，
$(-2, \pm 3), (-1, \pm 4), (2, \pm 5), (4, \pm 9), (8, \pm 23), (43, \pm 282),$
$(52, \pm 375), (5234, \pm 378661)$ の 16 個のみであり，
$\langle (-2, 3), (2, 5) \rangle = E(\mathbb{Q}) = \langle (-2, 3), (-1, 4) \rangle$ である．

- 整数点が上記の 16 個であることは Nagell が証明．
- 16 個の整数点は PARI/GP により得ることもできる．

```
gp > E=ellinit([0,17]); \\ E を定義
gp > for(a=-100000000,100000000,\
b=ellordinate(E,a);if(b,c=[a,b[1]];print(c)))
```

出力は `[-2, 3]`, `[-1, 4]`, `[2, 5]`, `[4, 9]`, `[8, 23]`, `[43, 282]`, `[52, 375]`, `[5234, 378661]`.

計算機 (PARI/GP) による $E(\mathbb{Q})$ に関する計算例

- [Sil, Ⅲ.2, Example 2.4] にて $E(\mathbb{Q}) = \langle (-2, 3), (2, 5) \rangle \simeq \mathbb{Z}^2$ が紹介されている.
- PARI/GP により $E(\mathbb{Q}) = \langle (-2, 3), (-1, 4) \rangle \simeq \mathbb{Z}^2$ が分かる.

```
gp > ellgenerators(E) \\ E(Q) の生成元を計算
[[-2, 3], [-1, 4]]
```

計算機 (PARI/GP) による $E(\mathbb{Q})$ に関する計算例

- [Sil, Ⅲ.2, Example 2.4] にて $E(\mathbb{Q}) = \langle (-2,3),(2,5) \rangle \simeq \mathbb{Z}^2$ が紹介されている.
- PARI/GP により $E(\mathbb{Q}) = \langle (-2,3),(-1,4) \rangle \simeq \mathbb{Z}^2$ が分かる.

`gp > ellgenerators(E)` \\ $E(\mathbb{Q})$ の生成元を計算

```
[[-2, 3], [-1, 4]]
```

- $P_1 = (-2,3), P_2 = (-1.4), P_3 = (2,5), P_6 = (43,282),$ $P_8 = (5234, 378661)$ と定義すると PARI/GP での計算により,
  $[-2]P_1 \oplus P_3 = P_2,$
  $[-1]P_1 \oplus [2]P_3 = P_6 = [3]P_1 \oplus [2]P_2,$
  $[-4]P_1 \oplus [3]P_3 = P_8 = [2]P_1 \oplus [3]P_2.$
- [Sil] に紹介の無かった点 P_2, P_6, P_8 の表し方についても上のように確認できた.

計算機 (PARI/GP) による $E(\mathbb{Q})$ に関する計算例

$\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 + 5x + 11$ に関する計算例

$E(\mathbb{Q}) = \{O\}$ である.

```
gp > E=ellinit([5,11]); \\ E を定義
gp > for(a=-100000000,100000000,\
b=ellordinate(E,a);if(b,c=[a,b[1]];print(c)))
gp >
```

計算機 (PARI/GP) による $E(\mathbb{Q})$ に関する計算例

$\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 + 5x + 11$ に関する計算例

$E(\mathbb{Q}) = \{O\}$ である.

```
gp > E=ellinit([5,11]); \\ E を定義
gp > for(a=-100000000,100000000,\
b=ellordinate(E,a);if(b,c=[a,b[1]];print(c)))
gp >
```

- 上記の入力から $-100000000 \leq x \leq 100000000$ において $(x, y) \in E$ となる整数点が存在しないと分かる.
  $E(\mathbb{Q})$ の生成元を計算してみる.

```
gp > E=ellinit([5,11]); \\ E を定義
gp > ellgenerators(E) \\ E(Q) の生成元を計算
[]
```

- ここから $E(\mathbb{Q}) = \{O\}$ であるので，整数点どころか有理点すら 1 つも存在しないと分かる.

Hasse の定理

- 楕円曲線暗号を作成する際は，有限体上の楕円曲線を用いる．
- 有限体上の楕円曲線に対する重要な定理として，次の定理がある．

定理 (Hasse の定理 [Sil, V.1, Theorem 1.1])

$\mathbb{F}_q$ 上の楕円曲線 E，$\mathrm{char}(\mathbb{F}_q) = p$ に対して

$$\left| |E(\mathbb{F}_q)| - q - 1 \right| \leq 2\sqrt{q}$$

が成り立つ．

Hasse の定理

- 楕円曲線暗号を作成する際は，有限体上の楕円曲線を用いる．
- 有限体上の楕円曲線に対する重要な定理として，次の定理がある．

定理 (Hasse の定理 [Sil, V.1, Theorem 1.1])

$\mathbb{F}_q$ 上の楕円曲線 E，$\mathrm{char}(\mathbb{F}_q) = p$ に対して

$$\left| |E(\mathbb{F}_q)| - q - 1 \right| \leq 2\sqrt{q}$$

が成り立つ．

- Hasse の定理から分かる重要な内容は，$E(\mathbb{F}_q)$ に含まれる点がほとんど $q+1$ 個であり，誤差の範囲は $\pm 2\sqrt{q}$ 個であるということ．

計算機 (PARI/GP) による $E(\mathbb{F}_p)$ に関する計算例

- PARI/GP を用いることで，$E(\mathbb{F}_q)$ の位数，構造，生成元について計算することができる．

$\mathbb{F}_{17}$ 上の楕円曲線 $E : y^2 = x^3 + 8$ に関する計算例

$|E(\mathbb{F}_{17})| = 18$，$E(\mathbb{F}_{17}) \simeq \mathbb{Z}/18\mathbb{Z}$，$E(\mathbb{F}_{17}) = \langle (1,3) \rangle$ である．

```
gp > E=ellinit([0,8],D=17); \\ E を定義
gp > E.no \\ E(F_17) の位数を計算
18
gp > E.cyc \\ E(F_17) の構造を計算
[18]
gp > E.gen \\ E(F_17) の生成元を計算
[[Mod(1, 17), Mod(3, 17)]]
```

計算機 (PARI/GP) による $E(\mathbb{F}_p)$ に関する計算例

実際に，PARI/GP にて計算をすると
$[1](1,3) = (1,3), [2](1,3) = (11,9),$
$[3](1,3) = (4,2), [4](1,3) = (14,7),$
$[5](1,3) = (3,16), [6](1,3) = (0,12),$
$[7](1,3) = (12,11), [8](1,3) = (2,4),$
$[9](1,3) = (15,0), [10](1,3) = (2,13),$
$[11](1,3) = (12,6), [12](1,3) = (0,5),$
$[13](1,3) = (3,1), [14](1,3) = (14,10),$
$[15](1,3) = (4,15), [16](1,3) = (11,8),$
$[17](1,3) = (1,14), [18](1,3) = O,$
となり，$[1](1,3), \ldots, [18](1,3)$ が $E(\mathbb{F}_{17})$ に含まれる 18 個の点である．

計算機 (PARI/GP) による $E(\mathbb{F}_p)$ に関する計算例

$\mathbb{F}_{31}$ 上の楕円曲線 $E : y^2 = x^3 + 5x + 11$ に関する計算例

$|E(\mathbb{F}_{31})| = 36$, $E(\mathbb{F}_{31}) \simeq \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$,
$E(\mathbb{F}_{31}) = \langle (8, 25), (20, 19) \rangle$ である.

```
gp > E=ellinit([5,11],D=31); \\ E を定義
gp > E.no \\ E(F_31) の位数を計算
36
gp > E.cyc \\ E(F_31) の構造を計算
[12, 3]
gp > E.gen \\ E(F_31) の生成元を計算
[[Mod(8, 31), Mod(25, 31)],
 [Mod(20, 31), Mod(19, 31)]]
```

楕円曲線暗号

- 元々，Diffie-Hellman 鍵交換や ELGamal 公開鍵暗号などは次の離散対数問題を基にして作られた．

定義 (離散対数問題 (DLP) [Sil, XI.4, page 376])

G を群，$x, y \in G$ $(y \in \langle x \rangle)$ とする．

$$x^m = y$$

を満たす $m \geq 1$ を決定する問題を離散対数問題という．また，DLP と表される．

DLP の例

$G = \mathbb{F}_{5^3}^{\times}$ において $11^m = 16$ を満たす $m \geq 1$ を求める．

楕円曲線暗号

- より難しい暗号にするために，楕円曲線を用いて作られた DLP が次の楕円曲線離散対数問題である．

定義 (楕円曲線離散対数問題 (ECDLP) [Sil, XI.4, Example 4.1(c)])

$\mathbb{F}_q$ 上の楕円曲線 E，$P, Q \in E(\mathbb{F}_q)$ $(Q \in \langle P \rangle)$ とする．

$$[m]P = Q$$

を満たす $m \geq 1$ を決定する問題を楕円曲線離散対数問題という．また，ECDLP と表される．

ECDLP の例

$\mathbb{F}_{17}$ 上の楕円曲線 $E : y^2 = x^3 + 8$，$G = E(\mathbb{F}_{17})$ において $[m](1, 3) = (3, 1)$ を満たす $m \geq 1$ を求める．

特別な ECDLP に関する計算例

- 現在，任意の ECDLP を解くアルゴリズムとして有効なものは Shanks の小ステップ-大ステップアルゴリズム，Pollard の ρ 法である．
- この 2 つのアルゴリズムは任意の群 G に対する DLP を解くアルゴリズムであり，任意の ECDLP に対して有効なアルゴリズムは見つかっていない．
- しかし，特別な仮定を満たす ECDLP に対して有効なアルゴリズムは次のように存在する．

特別な ECDLP に関する計算例

- 現在，任意の ECDLP を解くアルゴリズムとして有効なものは Shanks の小ステップ-大ステップアルゴリズム，Pollard の ρ 法である．
- この 2 つのアルゴリズムは任意の群 G に対する DLP を解くアルゴリズムであり，任意の ECDLP に対して有効なアルゴリズムは見つかっていない．
- しかし，特別な仮定を満たす ECDLP に対して有効なアルゴリズムは次のように存在する．

特別な ECDLP に関する計算例

- 現在，任意の ECDLP を解くアルゴリズムとして有効なものは Shanks の小ステップ-大ステップアルゴリズム，Pollard の ρ 法である．
- この 2 つのアルゴリズムは任意の群 G に対する DLP を解くアルゴリズムであり，任意の ECDLP に対して有効なアルゴリズムは見つかっていない．
- しかし，特別な仮定を満たす ECDLP に対して有効なアルゴリズムは次のように存在する．

特別な ECDLP に関する計算例

アルゴリズム (Semaev, Satoh, Araki, Smart [SIl, XI.6, Proposition 6.5])

p を素数，$p \geq 3$，$\mathbb{F}_p$ 上の楕円曲線 E，$|E(\mathbb{F}_p)| = p$ とする．

1. $P, Q \in E(\mathbb{F}_p)$ は $Q = [m]P$ を満たす O でない点とする．ただし，$m \in \mathbb{Z}$ は未知とする．
2. $\mathbb{Q}_p$ 上の楕円曲線 E' を，p を法とした還元が $\mathbb{F}_p$ 上の E となるように選ぶ．
3. ヘンゼルの補題を用いて点 P, Q を 点 $P', Q' \in E'(\mathbb{Q}_p)$ に持ち上げる．
4. 点 $[p]P', [p]Q'$ は形式群 $E'_1(\mathbb{Q}_p)$ に属する．
   $\log_E : E'_1(\mathbb{Q}_p) \longrightarrow \widehat{\mathbb{G}}_a(p\mathbb{Z}_p) \simeq p\mathbb{Z}_p^+$
   を形式対数写像とし
   $pa = \log_E([p]P') \in p\mathbb{Z}_p, \quad pb = \log_E([p]Q') \in p\mathbb{Z}_p$
   を計算する．
5. 4 での a, b により $m \equiv a^{-1}b \pmod{p}$ が成り立つ．

特別な ECDLP に関する計算例

- $E(\mathbb{F}_p)$ での点を $E(\mathbb{Q}_p)$ の点に持ち上げているが，アルゴリズムの証明から p^2 を法とした点の持ち上げを行えばよいと分かる．
- p^2 を法とした点の持ち上げにおいて，体 $\mathbb{F}_p$ 上の楕円曲線の点を環 $\mathbb{Z}/p^2\mathbb{Z}$ 上の楕円曲線の点に持ち上げることになる．環 $\mathbb{Z}/p^2\mathbb{Z}$ 上の楕円曲線での計算は，$\mathbb{Q}$ 上の楕円曲線における $\oplus, \ominus$ での計算を p^2 を法として行うものである．そのため，分母が非可逆元になる場合があり，それを避ける工夫が必要となる．

特別な ECDLP に関する計算例

- $E(\mathbb{F}_p)$ での点を $E(\mathbb{Q}_p)$ の点に持ち上げているが，アルゴリズムの証明から p^2 を法とした点の持ち上げを行えばよいと分かる．
- p^2 を法とした点の持ち上げにおいて，体 $\mathbb{F}_p$ 上の楕円曲線の点を環 $\mathbb{Z}/p^2\mathbb{Z}$ 上の楕円曲線の点に持ち上げることになる．環 $\mathbb{Z}/p^2\mathbb{Z}$ 上の楕円曲線での計算は，$\mathbb{Q}$ 上の楕円曲線における $\oplus, \ominus$ での計算を p^2 を法として行うものである．そのため，分母が非可逆元になる場合があり，それを避ける工夫が必要となる．

特別な ECDLP に関する計算例

- PARI/GP では $'$ を定義に用いることができないので，E', P', Q' を E_2, P_2, Q_2 と表す．

特別な ECDLP に関する計算例 1 [Sil, XI.6, Example 6.7]

$\mathbb{F}_{127}$ 上の楕円曲線 $E : y^2 = x^3 + 19x + 112$，
点 $P = (106, 72) \in E(\mathbb{F}_{127}), Q = (12, 121) \in E(\mathbb{F}_{127})$
において，$Q = [m]P$ を満たす $m \geq 1$ を求める．

```
gp > E=ellinit([19,112],D=127); \\ E を定義
gp > E2=ellinit([19,112]); \\ E_2 を定義
gp > P=[106,72]; \\ P を定義
gp > Q=[12,121]; \\ Q を定義
```

- PARI/GP での計算のために E_2 は $\mathbb{Q}$ 上で定義する．

特別な ECDLP に関する計算例

- $|E(\mathbb{F}_{127})| = 127$ であることを確認する．

gp > E.no \\ $|E(\mathbb{F}_{127})|$ を計算
127

- ヘンゼルの補題を用いて点 P, Q を点 $P_2, Q_2 \in E_2(\mathbb{Z}/127^2\mathbb{Z})$ に持ち上げる．このとき P_2 は

$$y_1 \equiv 72 \pmod{127}$$
$$y_1^2 - (106^3 + 19 \cdot 106 + 112) \equiv 0 \pmod{127^2}$$

を満たす y_1 により $P_2 = (106, y_1)$ となり，Q_2 は

$$y_2 \equiv 121 \pmod{127}$$
$$y_2^2 - (12^3 + 19 \cdot 12 + 112) \equiv 0 \pmod{127^2}$$

を満たす y_2 により $Q_2 = (12, y_2)$ となる．PARI/GP を次のように用いることで計算できる．

特別な ECDLP に関する計算例

```
gp > f(x,y)=y^2-x^3-19*x-112; \\ f(x,y) を定義
gp > for(a=1,100000000,\
b=[Mod(a,127),Mod(f(P[1],a),127^2)];\
if(b==[Mod(72,127),Mod(0,127^2)],print(a);break))
13026
gp > P2=[106,13026]; \\ P_2 を定義
```

- 上記では $1 \leq a \leq 100000000$ にて

$$a \equiv 72 \pmod{127}, \quad f(P[1], a) \equiv 0 \pmod{127^2}$$

を満たす最小の a は 13026 であることを示している．
ここから $P_2 = (106, 13026)$ と分かる．

特別な ECDLP に関する計算例

```
gp > for(a=1,100000000,\
b=[Mod(a,127),Mod(f(Q[1],a),127^2)];\
if(b==[Mod(121,127),Mod(0,127^2)],print(a);break))
5201
gp > Q2=[12,5201]; \\ Q_2 を定義
```

- 上記では $1 \leq a \leq 100000000$ にて

$$a \equiv 121 \pmod{127}, \quad f(Q[1], a) \equiv 0 \pmod{127^2}$$

を満たす最小の a は 5201 であることを示している．
ここから $Q_2 = (12, 5201)$ と分かる．

特別な ECDLP に関する計算例

- $[127]P_2, [127]Q_2$ を計算する．準備として，
  $\mathbb{Q}$ 上の楕円曲線での $[127]P_2, [127]Q_2$ をそれぞれ
  $M127P_2, M127Q_2$ と定義する．

```
gp > M127P2=ellmul(E2,P2,127); \\ M127P2 を定義
gp > M127Q2=ellmul(E2,Q2,127); \\ M127Q2 を定義
```

- $M127P_2, M127Q_2$ を 127^2 を法として計算すると，
  分母が非可逆元となることにより計算ができず，
  次のようにエラーメッセージが表れる．

特別な ECDLP に関する計算例

- $[127]P_2, [127]Q_2$ を計算する．準備として，$\mathbb{Q}$ 上の楕円曲線での $[127]P_2, [127]Q_2$ をそれぞれ $M127P_2, M127Q_2$ と定義する．

```
gp > M127P2=ellmul(E2,P2,127); \\ M127P2 を定義
gp > M127Q2=ellmul(E2,Q2,127); \\ M127Q2 を定義
```

- $M127P_2, M127Q_2$ を 127^2 を法として計算すると，分母が非可逆元となることにより計算ができず，次のようにエラーメッセージが表れる．

```
gp > Mod(M127P2,127^2)
  ***   at top-level: Mod(M127P2,127^2)
  ***                 ^-----------------
  *** Mod: impossible inverse in Fl_inv: Mod(0, 16129).
gp > Mod(M127Q2,127^2)
  ***   at top-level: Mod(M127Q2,127^2)
  ***                 ^-----------------
  *** Mod: impossible inverse in Fl_inv: Mod(0, 16129).
```

特別な ECDLP に関する計算例

- そのため，**変数変換**

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}$$

を行うことで，分母が非可逆元とならないように計算する．**この変数変換は E_2 の原点 O を $(z, w) = (0, 0)$ へ移す．**

特別な ECDLP に関する計算例

- そのため，変数変換

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}$$

を行うことで，分母が非可逆元とならないように計算する．この変数変換は E_2 の原点 O を $(z, w) = (0, 0)$ へ移す．

- $M127P_2, M127Q_2$ を変数変換したものをそれぞれ $CM127P_2, CM127Q_2$ と定義する．

```
gp > CM127P2=[-M127P2[1]/M127P2[2],-1/M127P2[2]];
```
\\ $CM127P_2$ を定義

```
gp > CM127Q2=[-M127Q2[1]/M127Q2[2],-1/M127Q2[2]];
```
\\ $CM127Q_2$ を定義

特別な ECDLP に関する計算例

- $CM127P_2, CM127Q_2$ を 127^2 を法として計算したものを $M127P_2E_2, M127Q_2E_2$ と定義する.

```
gp > M127P2E2=Mod(CM127P2,127^2)
```
\\ $M127P_2E_2 \equiv CM127P_2 \pmod{127^2}$
```
[Mod(12319, 16129), Mod(0, 16129)]
gp > M127Q2E2=Mod(CM127Q2,127^2)
```
\\ $M127Q_2E_2 \equiv CM127Q_2 \pmod{127^2}$
```
[Mod(2159, 16129), Mod(0, 16129)]
```

- これらより，$[127]P_2 = (12319, 0), [127]Q_2 = (2159, 0)$ と分かる.

特別な ECDLP に関する計算例

- $\log_E([127]P_2)$, $\log_E([127]Q_2)$ を計算するにあたり，$y^2 = x^3 + Ax + B$ に対する楕円対数は $\log_E(-\frac{x}{y}) = -\frac{x}{y} + \frac{2}{5}A(-\frac{x}{y})^5 + \cdots$ となり，127^2 を法として計算するため，$|E(\mathbb{F}_{127})| = 127$ より $[127]P_2 = [127]P = (0,0)$, $[127]Q_2 = [127]Q = (0,0)$ となるので

$$\log_E(z) = \log_E\left(-\frac{x}{y}\right) \approx -\frac{x}{y} = z$$

を用いれば十分である．

- $\log_E([127]P_2) \equiv 12319 \equiv 127 \cdot 97 \pmod{127^2}$
$\log_E([127]Q_2) \equiv 2159 \equiv 127 \cdot 17 \pmod{127^2}$
となるため，a, b は

$$a = 97,\ b = 17$$

となる．

特別な ECDLP に関する計算例

- $\log_E([127]P_2)$, $\log_E([127]Q_2)$ を計算するにあたり，$y^2 = x^3 + Ax + B$ に対する楕円対数は $\log_E(-\frac{x}{y}) = -\frac{x}{y} + \frac{2}{5}A(-\frac{x}{y})^5 + \cdots$ となり，127^2 を法として計算するため，$|E(\mathbb{F}_{127})| = 127$ より $[127]P_2 = [127]P = (0,0)$, $[127]Q_2 = [127]Q = (0,0)$ となるので

$$\log_E(z) = \log_E\left(-\frac{x}{y}\right) \approx -\frac{x}{y} = z$$

を用いれば十分である．

- $\log_E([127]P_2) \equiv 12319 \equiv 127 \cdot 97 \pmod{127^2}$
$\log_E([127]Q_2) \equiv 2159 \equiv 127 \cdot 17 \pmod{127^2}$
となるため，a, b は

$$a = 97,\ b = 17$$

となる．

特別な ECDLP に関する計算例

- 求める m は次のように計算される.

```
gp > a=97; \\ a を定義
gp > b=17; \\ b を定義
gp > m=Mod(a^-1*b,127) \\ m ≡ a^{-1}b (mod 127)
Mod(46, 127)
```

- よって，$m \equiv 97^{-1} \cdot 17 \equiv 46 \pmod{127}$ である.

- $[46]P = Q$ であることを以下のように検算してみる. また，ellmul を用いるために m を $\mathbb{Z}$ の元として再定義する.

```
gp > m=46; \\ m を再定義
gp > ellmul(E,P,m)==Q \\ [m]P と Q が等しいか確認
1
```

- $[46]P = Q$ が確かめられた.

特別な ECDLP に関する計算例

- 次の ECDLP においても，同様の手順により m を求めることができる．

特別な ECDLP に関する計算例 2 [Sil, XI, Exercise 11.15]

$\mathbb{F}_{137}$ 上の楕円曲線 $E : y^2 = x^3 + 86x + 98$，
点 $P = (56, 85) \in E(\mathbb{F}_{137}), Q = (54, 86) \in E(\mathbb{F}_{137})$
において，$Q = [m]P$ を満たす $m \geq 1$ を求める．

```
gp > E=ellinit([86,98],D=137); \\ E を定義
gp > E2=ellinit([86,98]); \\ E_2 を定義
gp > P=[56,85]; \\ P を定義
gp > Q=[54,86]; \\ Q を定義
gp > E.no \\ |E(F_137)| を計算
137
```

- $|E(\mathbb{F}_{137})| = 137$ と分かる．

特別な ECDLP に関する計算例

- ヘンゼルの補題を用いて点 P, Q を点 $P_2, Q_2 \in E_2(\mathbb{Z}/137^2\mathbb{Z})$ に持ち上げる.

```
gp > f(x,y)=y^2-x^3-86*x-98; \\ f(x,y) を定義
gp > for(a=1,100000000,\
b=[Mod(a,137),Mod(f(P[1],a),137^2)];\
if(b==[Mod(85,137),Mod(0,137^2)],print(a);break))
11593
gp > P2=[56,11593]; \\ P_2 を定義
gp > for(a=1,100000000,\
b=[Mod(a,137),Mod(f(Q[1],a),137^2)];\
if(b==[Mod(86,137),Mod(0,137^2)],print(a);break))
12553
gp > Q2=[54,12553]; \\ Q_2 を定義
```

- $P_2 = (56, 11593), Q_2 = (54, 12553)$ と分かったので，それらを定義する.

特別な ECDLP に関する計算例

- $\mathbb{Q}$ 上の楕円曲線での $[137]P_2, [137]Q_2$ をそれぞれ $M137P_2, M137Q_2$ と定義する.

```
gp > M137P2=ellmul(E2,P2,137); \\ M137P2 を定義
gp > M137Q2=ellmul(E2,Q2,137); \\ M137Q2 を定義
```

- 変数変換

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}$$

を $M137P_2, M137Q_2$ に行ったものをそれぞれ $CM137P_2, CM137Q_2$ と定義する.

```
gp >
CM137P2=[-M137P2[1]/M137P2[2],-1/M137P2[2]];
\\ CM137P2 を定義
gp >
CM137Q2=[-M137Q2[1]/M137Q2[2],-1/M137Q2[2]];
\\ CM137Q2 を定義
```

特別な ECDLP に関する計算例

- $CM137P_2, CM137Q_2$ を 137^2 を法として計算したものを $M137P_2E_2, M137Q_2E_2$ と定義する.

```
gp > M137P2E2=Mod(CM137P2,137^2)
```
\\ $M137P_2E_2 \equiv CM137P_2 \pmod{137^2}$
```
[Mod(15207, 18769), Mod(0, 18769)]
gp > M137Q2E2=Mod(CM137Q2,137^2)
```
\\ $M137Q_2E_2 \equiv CM137Q_2 \pmod{137^2}$
```
[Mod(8905, 18769), Mod(0, 18769)]
```

- これらより，$[137]P_2 = (15207, 0), [137]Q_2 = (8905, 0)$ と分かる.

特別な ECDLP に関する計算例

- $\log_E([137]P_2)$, $\log_E([137]Q_2)$ を計算するにあたり，$y^2 = x^3 + Ax + B$ に対する楕円対数は $\log_E(-\frac{x}{y}) = -\frac{x}{y} + \frac{2}{5}A(-\frac{x}{y})^5 + \cdots$ となり，137^2 を法として計算するため，$|E(\mathbb{F}_{137})| = 137$ より $[137]P_2 = [137]P = (0,0)$, $[137]Q_2 = [137]Q = (0,0)$ となるので

$$\log_E(z) = \log_E\left(-\frac{x}{y}\right) \approx -\frac{x}{y} = z$$

を用いれば十分である．

- $\log_E([137]P_2) \equiv 15207 \equiv 137 \cdot 111 \pmod{137^2}$
$\log_E([137]Q_2) \equiv 8905 \equiv 137 \cdot 65 \pmod{137^2}$
となるため，a, b は

$$a = 111,\ b = 65$$

となる．

特別な ECDLP に関する計算例

- 求める m は次のように計算される．

```
gp > a=111; \\ a を定義
gp > b=65; \\ b を定義
gp > m=Mod(a^-1*b,137) \\ m ≡ a^{-1}b (mod 137)
Mod(66, 137)
```

- よって，$m \equiv 111^{-1} \cdot 65 \equiv 66 \pmod{137}$ である．

- $[66]P = Q$ であることを以下のように検算してみる．また，ellmul を用いるために m を $\mathbb{Z}$ の元として再定義する．

```
gp > m=66; \\ m を再定義
gp > ellmul(E,P,m)==Q \\ [m]P と Q が等しいか確認
1
```

- $[66]P = Q$ が確かめられた．

特別な ECDLP に関する計算例

今後の課題

- 計算機における様々なアルゴリズムの実行
- 既存のアルゴリズムへの工夫
- 耐量子暗号