令和5年度　修士論文

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

2024年1月25日

新潟大学大学院自然科学研究科博士前期課程
数理物質科学専攻

概要

本論文は，著者が学部，修士にて学んだ代数的整数論の知識を基盤とし，Joseph H. Silverman 著の *The Arithmetic of Elliptic Curves* [Sil] を参考にして楕円曲線暗号に関する内容や計算例についてまとめたものである．なお，2023 年 12 月にて [Sil] の日本語訳である [シルヴァーマン] が出版された．代数的整数論については著者が学部からゼミで読んできた [Ono] をはじめ [ノイキルヒ]，[藤崎] も参照してほしい．本論文の特色を 2 つ述べる．1 つ目の特色は楕円曲線の応用の 1 つである楕円曲線暗号を主軸としたことである．楕円曲線上の群法則は不明確なものでないにも関わらず，それを用いることで解くことが困難な楕円曲線離散対数問題 (ECDLP) を作り出すことができた．そのため Diffie-Hellman 鍵交換や ELGamal 公開鍵暗号を楕円曲線暗号として用いることでより解読が困難となる．Shanks の小ステップ-大ステップアルゴリズムと Pollard の ρ 法は任意の ECDLP を解くことができるアルゴリズムであり，さらに Semaev，Satoh，Araki，Smart によるアルゴリズムは $|E(\mathbb{F}_p)| = p$ という特別な条件を満たす楕円曲線に対する ECDLP を容易に解くことができる．2 つ目の特色は，計算機である PARI/GP [PARI, version 2.15.4] を用いた計算例を作成したことである．楕円曲線上の点の計算や群構造の理解，Semaev，Satoh，Araki，Smart によるアルゴリズムを用いた ECDLP の計算例など広い用途で PARI/GP を用いた．また，実行したコマンドを記載しコメントをつけることで，計算例の理解を促し類似の問題に応用できるようにした．

第 1 章では，第 2 章以降の内容の前提となる知識について必要最低限の準備を行った．1.1 節ではアフィン多様体，射影多様体に関する定義や定理について紹介した．1.2 節では因子の性質についてまとめ，リーマン・ロッホの定理や楕円曲線に関係する事実を紹介した．

第 2 章では，2.1 節と 2.2 節にて楕円曲線の定義や群法則についてまとめた．また，楕円曲線論全体の概要については [ST] も参照してほしい．2.3 節では PARI/GP にて楕円曲線を定義する方法や群法則に基づいた計算例，モーデル・ヴェイユ群 $E(\mathbb{Q})$ の生成元の計算例などを紹介した．PARI/GP の使用方法や各コマンドの詳細については [User's Guide] を参照してほしい．

第 3 章では，楕円曲線暗号に用いられる有限体上の楕円曲線についてまとめた．3.1 節では $E(\mathbb{F}_q)$ の位数に関する重要な定理である Hasse の定理を，証明やそれに必要な知識を含めて紹介した．証明は [Sil] を参考にしている．3.2 節では PARI/GP を用いた $E(\mathbb{F}_p)$ の計算例について紹介した．

第 4 章では，楕円曲線暗号や関係するアルゴリズムについて紹介した．暗号理論に関しては [コブリッツ] も参照してほしい．4.1 節では有名な楕円曲線暗号の手順について，4.2 節では楕円曲線暗号の基となっている ECDLP を解くことができるアルゴリズムについて紹介した．4.3 節では特別な場合の ECDLP を解くアルゴリズムと PARI/GP を用いた計算例を紹介した．

謝辞

主指導教員である星明考先生には，学部 4 年生からの 3 年間に渡り，セミナーを通して数学の知識や考え方，教養を教えていただきました．また，本論文をまとめるにあたり，数学の内容に関するものだけでなく，より読みやすく有益な論文となるための様々な助言をいただきました．ここに深く感謝の意を表します．

星研究室の卒業生である金井和貴先輩と博士後期課程の池田愛輝先輩には，学部生の頃からセミナーの発表や数学への向き合い方など様々な面でお世話になり，本論文に関しても助言をいただきました．また，同期の髙橋和暉君とはセミナーにて発表を行うときだけでなく準備段階から議論を交わしたことで，発表の質を向上し数学の理解を深めることができました．後輩の飯田紘明君はセミナーでの私の発表に関する助言をくれました．皆様に深く感謝いたします．

最後に，常に私を支え応援し続けてくださった家族に，心からの感謝を申し上げます．

記号

始めに，本論文で用いる記号や用語について記す.

- $\mathbb{N}$: 自然数全体
- $\mathbb{Z}$: 有理整数環
- $\mathbb{Q}$: 有理数体
- $\mathbb{R}$: 実数体
- $\mathbb{C}$: 複素数体
- $\mathbb{F}_q$: 位数 q の有限体
- $\mathrm{char}(K)$: 体 K の標数
- $R^\times$: 環 R の乗法群
- $K^\times = K\backslash\{0\}$: 体 K の乗法群
- $\mathrm{Gal}\,(L/K)$: 体のガロア拡大 L/K のガロア群
- $[L : K]$: 体の拡大 L/K の拡大次数
- $\overline{K}$: K の代数的閉包 (1 つ固定する)
- $\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (x_1, \ldots, x_n) \mid x_i \in \overline{K}\}$: n 次元アフィン空間
- $\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n \mid x_i \in K\}$: $\mathbb{A}^n$の K 有理点の集合

目次

1　準備

この章では，Silverman [Sil, I, II] の内容を参考に，第 2 章以降で必要となる知識や前提となるものの一部をまとめる．

1.1　代数多様体・代数曲線

K を完全体，$\overline{K}$ を K の代数的閉包とする (完全体とは全ての代数拡大が分離拡大となる体であった．例えば，$\mathbb{Q}, \mathbb{R}$ などの $\mathrm{char}(K) = 0$ となる体 K や，素数 p に対する有限体 $\mathbb{F}_p$ などである)．

定義 1.1. n 変数多項式環 $\overline{K}[X] = \overline{K}[X_1, \ldots, X_n]$ のイデアルを $I \subset \overline{K}[X]$ とする．
各 I ごとに V_Iを以下のように定める：

$$V_I := \{P \in \mathbb{A}^n \mid f(P) = 0, \forall f \in I\} \subset \mathbb{A}^n = \mathbb{A}^n(\overline{K}).$$

この V_I を**アフィン代数的集合** (**affine algebraic set**) という．

定義 1.2. $V \subset \mathbb{A}^n = \mathbb{A}^n(\overline{K})$ をアフィン代数的集合とする．
V に対するイデアル $I(V)$ を以下のように定める：

$$I(V) := \{f \in \overline{K}[X] \mid f(p) = 0, \forall p \in V\} \subset \overline{K}[X].$$

さらに $I(V) = \langle g \rangle (g \in K[X])$ となるとき，V を $\boldsymbol{K}$ **上のアフィン代数的集合**といい $\boldsymbol{V/K}$ と表す．
また V/K のとき，V の K 有理点の集合は $V(K) = V \cap \mathbb{A}^n(K)$ となる．

定義 1.3. $V \subset \mathbb{A}^2 = \{P = (x_1, x_2) \mid x_i \in \overline{\mathbb{Q}}\}$ をアフィン代数的集合とする．

$$V \text{ は}\textbf{アフィン多様体 (affinevariety)} \overset{\text{def}}{\Longleftrightarrow} I(V) \subset \overline{K}[X] \text{ が素イデアル.}$$

定義 1.4. アフィン多様体 V/K に対して，$\boldsymbol{V/K}$ **のアフィン座標環** (**affinecoordinatering**) を次のように定める：

$$K[V] := K[X]/I(V/K).$$

また，$K[V]$ の商体 $K(V)$ を $\boldsymbol{V/K}$ **の関数体** (**functionfield**) という．

定義 1.5. アフィン多様体 V に対して, V の次元を次のように定める：

$$\dim(V) := [\overline{K}(V) : \overline{K}].$$

定義 1.6. V をアフィン多様体, $p \in V, I(V) = (f_1, \ldots, f_n)\,(f_1, \ldots, f_n \in \overline{K}[X])$ とする.

V が点 P で**非特異** $\overset{\text{def}}{\Longleftrightarrow} \left(\dfrac{\partial f_i}{\partial X_j}(P)\right)_{1 \le i \le m,\, 1 \le j \le n}$ のランクが $n - \dim(V)$.

V が**非特異** $\overset{\text{def}}{\Longleftrightarrow} V$ が任意の点で非特異.

また, **非特異** (**nonsingular**) であることを**滑らか** (**smooth**) であるともいう.

注意 1.7. V が定数ではない 1 つの多項式方程式 $f(X_1, \ldots, X_n) = 0$ で与えられているとき, $\dim(V) = n - 1$ であることから次の必要十分条件が成り立つ.

$$P \in V \text{ が特異点} \Leftrightarrow \frac{\partial f}{\partial X_1}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0.$$

定義 1.8. V をアフィン多様体, $P \in V$, $M_P = \{f \in \overline{K}[V] \mid f(P) = 0\}$ とする.

M_P による $\overline{K}[V]$ の局所環を次のように定める：

$$\overline{K}[V]_P := \{F \in \overline{K}(V) \mid F = f/g \text{ であり } f, g \in \overline{K}, g(P) \neq 0\}.$$

$\overline{K}[V]_P$は***V* の *P* における局所環** (**local ring**) ともいう.

アフィン空間を用いて, 次の射影曲線を定める.

定義 1.9. 元 $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} (x_0 = \cdots = x_n = 0$ を除く$)$ に対して, 同値関係 $\sim$ を以下のように定める：

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \overset{\text{def}}{\Longleftrightarrow} 0 \le \forall i \le n, \exists \lambda \in \overline{K}^{\times} \text{s.t.}\, x_i = \lambda y_i.$$

この同値関係 $\sim$ を法として定まる集合 $\mathbb{A}^{n+1}/\sim$ を ***n* 次元射影空間** (**Projective n-space**) といい, $\mathbb{P}^n$ と表す.

この同値関係により定まる同値類 $\{(\lambda x_0, \ldots, \lambda x_n) \mid \lambda \in K^{\times}\}$ を $[x_1, \ldots, x_n]$ と表し各 $x_0, \ldots, x_n$を $(x_0, \ldots, x_n)$ の**斉次座標** (**homogeneous coordinates**) という.

定義 1.10. イデアル $I \in \overline{K}[X]$ を $I = (f)$ (斉次多項式 $f \in \overline{K}[X]$) と表せるとき, I を**斉次イデアル** (**homogeneous ideal**) という.

各斉次イデアル I に対して,

$$V_I := \{P \in \mathbb{P}^n \mid f(P) = 0, \forall f \in I\} \subset \mathbb{P}^n = \mathbb{P}^n(\overline{K})$$

と定め，V_I を**射影代数的集合** (**projective algebraic set**) という．

さらに，各射影代数的集合 V に対して斉次イデアルを $\boldsymbol{I(V)} \subset \overline{K}[X]$ と表し，$I(V)$ は $\{f \in \overline{K}[X] \mid f : \text{斉次多項式}, f(P) = 0\,(\forall P \in V)\}$ により生成される．

もしイデアル $I(V)$ が $K[X]$ の斉次多項式により生成されるならば，V は $\boldsymbol{K}$ **上で定義されている**といい $\boldsymbol{V/K}$ と表す．

定義 1.11. $\mathbb{P}^n$の K 有理点の集合を次のように定める:

$$\mathbb{P}^n(K) := \{[x_0, \ldots, x_n] \in \mathbb{P}^n \mid x_i \in K\}.$$

また，V/K ならば V の K 有理点は

$$V(K) = V \cap \mathbb{P}^n(K)$$

となり，一般に

$$V(K) = \{P \in V \mid P^\sigma = P, \forall \sigma \in \mathrm{Gal}\,(\overline{K}/K)\}$$

と表せる．

定義 1.12. $V \subset \mathbb{P}^n(\overline{K})$ を射影代数的集合とする．

斉次イデアル $I(V) \subset \overline{K}[X]$ が素イデアルであるとき，V を**射影多様体** (**projective variety**) という．

射影多様体 V の次元や関数体などは，アフィン部分多様体 $V \cap \mathbb{A}^n$ を用いて定める．

定義 1.13. V/K を射影多様体とし，$\mathbb{A}^n \subset \mathbb{P}^n\,(V \cap \mathbb{A}^n \neq \emptyset)$ とする．

$\boldsymbol{V}$ **の次元** (**dimension**) を $\dim\,(V \cap \mathbb{A}^n)$ と定める．

また，$\boldsymbol{V}$ **の関数体** (**function field**) を $K(V) := K(V \cap \mathbb{A}^n)$ と定める．

定義 1.14. V を射影多様体，$P \in V$ とし，$\mathbb{A}^n \subset \mathbb{P}^n\,(P \in \mathbb{A}^n)$ とする．

$$V \text{ が } P \text{ で}\textbf{滑らか}\,(\textbf{smooth}) \overset{\text{def}}{\Longleftrightarrow} V \cap \mathbb{A}^n \text{が } P \text{ で滑らか.}$$

また，$\boldsymbol{V}$ **の** $\boldsymbol{P}$ **における局所環** (**local ring**) は

$$\overline{K}[V]_P := \overline{K}[V \cap \mathbb{A}^n]_P$$

と定める．

射影多様体間の写像として，次が定められる．

定義 1.15. $V_1, V_2 \subset \mathbb{P}^n(\overline{K})$ を射影多様体とする.

$$\begin{array}{rccc} \phi\colon & V_1 & \longrightarrow & V_2 \\ & \cup & & \cup \\ & P & \longmapsto & [f_0(P), \ldots, f_n(P)] \end{array}$$

$(f_0, \ldots, f_n \in \overline{K}(V_1), f_0, \ldots, f_n$は$\forall P \in V_1$において定義されている.$)$

このような ϕ を **V_1から V_2への有理写像** (**rational map**) という.

$V_1/K, V_2/K$ であるとき, $\forall \sigma \in \mathrm{Gal}\,(\overline{K}/K)$ に対して

$$\phi^\sigma(P) = [f_0^\sigma(P), \ldots, f_n^\sigma(P)].$$

また, $\forall P \in V_1$ に対して

$$\phi(P)^\sigma = \phi^\sigma(P^\sigma).$$

さらに, ϕ と K に対して次のように定める.

$$\phi\text{が } \boldsymbol{K} \text{ 上で定義される} \overset{\mathrm{def}}{\Longleftrightarrow} \exists \lambda \in \overline{K}^\times \text{ s.t. } \lambda f_0, \ldots, \lambda f_n \in K(V_1).$$

定義 1.16. $V_1, V_2 \subset \mathbb{P}^n$ を射影多様体とし,

$$\text{有理写像 } \phi\colon \quad \begin{array}{ccc} V_1 & \longrightarrow & V_2 \\ \cup & & \cup \\ P & \longmapsto & [f_0(P), \ldots, f_n(P)] \end{array}$$

$(f_0, \ldots, f_n \in \overline{K}(V_1), f_0, \ldots, f_n$は$\forall P \in V_1$において定義されている.$)$

とする.

次の (1),(2) を満たす関数 $g \in \overline{K}(V_1)$ が存在するとき, ϕ が $P \in V_1$ で**正則** (**regular**) であると定義する.

1. 各 gf_i が P で正則である.
2. $0 \leq \exists i \leq n$ s.t. $(gf_i)(P) \neq 0$.

このような g が存在するとき,

$$\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]$$

と表す. g は V_1 の各点ごとに異なる場合がある.

有理写像 ϕ が $\forall P \in V_1$ で正則であるとき, ϕ を**正則写像** (**regular map**) という.

以下, 曲線とは次元 1 の射影多様体を指すこととする. 曲線に対しても定義 1.10, 定義 1.13, 定義 1.14 のように定められる.

定義 1.17. 滑らかな射影曲線 $C, p \in C$ に対して

$C/K : C$ が K 上で定義されている.

$K(C) : C/K$ の関数体.

$\overline{K}[C]_p : C$ の P における局所環.

命題 1.18 ([Sil, Ⅱ.2, Proposition 2.1, page 19])**.** C を滑らかな射影曲線，$V \subset \mathbb{P}^N$ を多様体，$P \in C$ を滑らかな点，$\phi : C \longrightarrow V$ を有理写像とする．このとき，ϕ は P で正則である．特に C が滑らかならば，ϕ は正則写像となる.

定理 1.19 ([Sil, Ⅱ.2, Theorem 2.3, page 20])**.** $\phi : C_1 \longrightarrow C_2$ を滑らかな射影曲線の正則写像とする．このとき，ϕ は定数または全射となる.

定義 1.20. $C_1/K, C_2/K$ を滑らかな射影曲線とし，$\phi : C_1 \longrightarrow C_2$を K 上で 定義された定数でない有理写像とする.

ϕ により誘導される K を固定する関数体の単射を

$$\begin{array}{rccc} \phi^* : & K(C_2) & \longrightarrow & K(C_1) \\ & \cup & & \cup \\ & f & \longmapsto & f \circ \phi \end{array}$$

と表す.

定義 1.21. $\phi : C_1 \longrightarrow C_2$ を K 上で定義された写像とする.

ϕ が定数であるとき，**ϕ の次数を 0** と定義する.

そうでないとき，ϕ を**有限写像** (**finite map**) といい，その**次数** (**degree**) は

$$\deg \phi := [K(C_1) : \phi^* K(C_2)].$$

体の拡大 $K(C_1)/\phi^* K(C_2)$ が分離的，非分離的，純非分離的であるとき，それぞれ ϕ が**分離的** (**separable**)，**非分離的** (**inseparable**)，**純非分離的** (**purely inseparable**) であるという．体の拡大の**分離次数** (**separable degree**)，**非分離次数** (**inseparable degree**) をそれぞれ $\mathbf{deg}_s\, \boldsymbol{\phi}, \mathbf{deg}_i\, \boldsymbol{\phi}$ と表す.

1.2 因子

定義 1.22. 滑らかな射影曲線 C に対して，次のような形式和

$$D = \sum_{P \in C} n_P(P) \ \ (n_P \in \mathbb{Z}, \text{有限個の } P \in C \text{ を除いて } n_P = 0)$$

を C の**因子 (divisor)** という．$\boldsymbol{D}$ **の位数**は $\deg D := \sum_{P \in C} n_P$ とする．

C の因子全体の集合は自由アーベル群となるため $\boldsymbol{C}$ **の因子群 (divisor group)** といい $\mathbf{Div}(\boldsymbol{C})$ と表す．

さらに位数 0 の因子は $\mathrm{Div}(C)$ の部分群をなし，これを $\mathbf{Div^0}(\boldsymbol{C})$ と表す．

また $\forall \sigma \in \mathrm{Gal}\,(\overline{K}/K)$ に対して $D^\sigma = D$ となるとき，$\boldsymbol{D}$ **は** $\boldsymbol{K}$ **上で定義されている**といい $\boldsymbol{D/K}$ と表す．

K 上で定義された D からなる群を$\mathbf{Div}_{\boldsymbol{K}}(\boldsymbol{C})$ と表し，さらに位数 0 の因子のみで構成されたものを $\mathbf{Div}^{\mathbf{0}}_{\boldsymbol{K}}(\boldsymbol{C})$ と表す．

注意 1.23. $D = n_1(P_1) + \cdots + n_r(P_r)(n_1, \ldots, n_r \neq 0)$ において，D/K であるためには $P_1, \ldots, P_r \in C(K)$ である必要はなく，$P_i^\sigma = P_j (1 \leq i, j \leq r)$ であればよい．

特別な因子である主因子を定めるために準備する．

命題 1.24 ([Sil, II.1, Proposition 1.1, page 17])**.** C を滑らかな射影曲線とし, 点 $P \in C$ で滑らかとする．

このとき，$\overline{K}[C]_P$は離散付値環となる．

$\overline{K}[C]_P$ 上の付値は $\overline{K}[C]_P$の極大イデアルである M_Pを用いて 以下のように定められ, $\overline{K}(C)$ 上に延長できる．

定義 1.25. C を滑らかな射影曲線とし，点 $P \in C$ で滑らかとする．このとき，$\overline{K}[C]_P$ 上の付値は以下のように与えられる．

$$\begin{array}{rccc} \mathrm{ord}_P\colon & \overline{K}[C]_P & \longrightarrow & \{0,1,2,\ldots\} \cup \{\infty\} \\ & \cup & & \cup \\ & f & \longmapsto & \sup\{d \in \mathbb{Z} \mid f \in M_P^d\}. \end{array}$$

さらに, $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$ とすることで, 以下のように ord_P を $\overline{K}(C)$ に拡張できる．

$$\mathrm{ord}_P : \overline{K}(C) \longrightarrow \mathbb{Z} \cup \infty.$$

さらに，$\mathrm{ord}_P(t) = 1$ となる関数 $t \in \overline{K}(C)$ を点 P の C に関する**一意化変数** (**uniformizer**) という．これはイデアル M_P の生成元となっている．

定義 1.26. C を滑らかな射影曲線, $f \in \overline{K}(C)^\times$とする．

f に関する因子を以下のように定める：

$$\mathrm{div}(f) := \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

さらに，各 ord_P が付値であることから

$$\mathrm{div} : \overline{K}(C)^{\times} \longrightarrow \mathrm{Div}(C) \,(\text{アーベル群における準同型写像})$$

となる．

これらを用いて，主因子を定義する．

定義 1.27. $D \in \mathrm{Div}(C)$ とする．このとき

$D = \mathrm{div}\,(f)\,(f \in \overline{K}(C)^{\times})$ となるとき，D を**主因子** (**principal divisor**) という．

また，$D_1, D_2 \in \mathrm{Div}(C)$ に対して $D_1 - D_2$ が主因子となるとき，D_1, D_2 は**線形同値** (**linearly equivalent**) といい，$D_1 \sim D_2$ と表す．

C の**因子類群** (**divisor class group**) または**ピカール群** (**Picard group**) とは $\mathrm{Div}(C)$ の主因子全体からなる部分群 P による

$$\mathrm{Pic}\,(C) := \mathrm{Div}(C)/P$$

のことであり，$\mathrm{Gal}\,(\overline{K}/K)$ により定まる $\mathrm{Pic}\,(C)$ の部分群を $\mathbf{Pic_K(C)}$ と表す．

命題 1.28 ([Sil, Ⅱ.3, Proposition 3.1, page 28])**.** C を滑らかな射影曲線，$f \in \overline{K}(C)^{\times}$ とすると次が成り立つ．

1. $\mathrm{div}\,(f) = 0 \Leftrightarrow f \in \overline{K}^{\times}$.
2. $\deg(\mathrm{div}\,(f)) = 0$.

命題 1.28 から主因子が $\mathrm{Div}^0(C)$ の部分群をなすと分かるので，次のように定義できる．

定義 1.29. C を滑らかな射影曲線，P を主因子からなる$\mathrm{Div}^0(C)$ の部分群とする．

C の次数が 0 となる因子からなる因子類群は

$$\mathrm{Pic}^0(C) := \mathrm{Div}^0(C)/P$$

となる．定義 1.27 と同様に，$\mathrm{Gal}\,(\overline{K}/K)$ により定まる $\mathrm{Pic}^0(C)$ の部分群を $\mathrm{Pic}^0_K(C)$ と表す．

命題 1.28，定義 1.29 より $\mathrm{Ker}\,(\mathrm{div}) = \overline{K}^{\times}, \mathrm{Coker}\,(\mathrm{div}) = \mathrm{Pic}^0(C)$ なので以下の完全列が成り立つ．

$$1 \longrightarrow \overline{K}^{\times} \longrightarrow \overline{K}(C)^{\times} \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \longrightarrow \mathrm{Pic}^0(C) \longrightarrow 0 \quad (\text{exact}).$$

これは，これまで学んできた代数的整数論における分数イデアル $\mathfrak{a}$ に関する完全列と類似している．

$$1 \longrightarrow \mathfrak{o}_K^{\times} \longrightarrow K^{\times} \longrightarrow I_K \longrightarrow H_K \longrightarrow 1 \quad (\text{exact}).$$

ここから，曲線に関する代数幾何学において基本的な定理であるリーマン・ロッホの定理のための準備をする．

定義 1.30. C を滑らかな射影曲線とする．

$\forall p \in C$ に対して $n_P \geq 0$ となるとき，$D = \sum_{P \in C} n_P(P)$ が正の数であるといい，$D \geq 0$ と表す．さらに，$\forall D_1, D_2 \in \mathrm{Div}(C)$ に対して $D_1 - D_2 \geq 0$ であるとき $D_1 \geq D_2$ と定める．これは，$\mathrm{Div}(C)$ 上の半順序となる．

定義 1.31. C を滑らかな射影曲線，$D \in \mathrm{Div}(C)$ とする．

次のように有限次元 $\overline{K}$ ベクトル空間を定める：

$$\mathfrak{L}(D) := \{f \in \overline{K}(C)^{\times} \mid \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

次元は $l(D) = \dim_{\overline{K}} \mathfrak{L}(D)$ と表す．

命題 1.32 ([Sil, Ⅱ.4, Proposition 4.2 (a), page 30])**.** C を滑らかな射影曲線とする．このとき，Ω_C は 1 次元 $\overline{K}(C)$ ベクトル空間である．

注意 1.33 ([Sil, Ⅱ.4, Remark 4.4, page 32])**.** $\omega_1, \omega_2 \in \Omega_C$ を 0 でない微分形式とする．このとき命題 1.32 より

$$\exists f \in \overline{K}(C)^{\times} \text{ s.t. } \omega_1 = f\omega_2$$

となるので

$$\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2)$$

である．

注意 1.33 より，滑らかな射影曲線 C での標準因子は定義 1.34 のように定められる．

定義 1.34. C を滑らかな射影曲線，Ω_C を C における微分形式の集合とする．

このとき $\forall\omega \in \Omega_C \backslash \{0\}$ に対して，$\mathrm{div}\,(\omega)$ の $\mathrm{Pic}\,(C)$ における像を C 上の**標準因子類** (**canonical divisor class**) といい，この因子類に含まれる任意の因子を**標準因子** (**canonical divisor**) という．

定理 1.35 (**リーマン・ロッホの定理**，**Riemann-Roch theorem**)**.** C を滑らかな射影曲線，K_Cを C 上の標準因子とする．このとき，$\forall D \in \mathrm{Div}(C)$ に対して

$$l(D) - l(K_C - D) = \deg D - g + 1$$

となる $g \geq 0\,(g \in \mathbb{Z})$ が存在する．この g を C の**種数** (**genus**) という．

リーマン・ロッホの定理を用いることで，因子 D と種数 g に関する性質を証明できる．

系 1.36 ([Sil, Ⅱ.5, Corollary 5.5, page 35])**.** C を滑らかな射影曲線，K_Cを C 上の標準因子，g を C の種数 とする．

このとき，次の (1)〜(3) が成り立つ．

1. $l(K_C) = g$.
2. $K_C = 2g - 2$.
3. $\deg D > 2g - 2 \Rightarrow l(D) = \deg D - g + 1$.

これらの性質は，次の章で定義する楕円曲線に関する事実を証明する際に用いられるものである．[Sil, Ⅲ.3, pages 58–66] を参照.

2　楕円曲線

この章では，2.1 節と 2.2 節にて Silverman [Sil, Ⅲ] の内容を参考に，楕円曲線の定義や群法則についてまとめる．さらに，2.3 節にて PARI/GP [PARI, version 2.15.4] を用いてモーデル・ヴェイユ群での計算や整数点に関する計算例を紹介する．PARI/GP の使用方法や各種コマンドについては [User's Guide] を参照．また，Magma や Sage 等の様々な計算機の使用を軸とした楕円曲線の計算に関しては [横山 1] を，特に Magma を用いる際の文法やプログラムに関しては [横山 2] を参照.

2.1　楕円曲線の定義

定義 2.1. 種数 1 の滑らかな射影曲線 E , 点 $O \in E$ に対して

組 (E, O) を**楕円曲線** (**elliptic curve**) という.

また, E の定義方程式の全ての係数が K の元かつ $O \in E(K)$ であるとき

E は $\boldsymbol{K}$ **上で定義されている**といい $\boldsymbol{E/K}$ と表す.

このとき, E は $\boldsymbol{K}$ **上の楕円曲線である**ともいう.

K 上の楕円曲線 (E, O) は

$$\phi\colon E \longrightarrow \mathbb{P}^2,\ \phi = [x, y, 1]\ (\phi(O) = [0, 1, 0])$$

という写像により, 次の滑らかな射影曲線 C と同型となる.

$$C\colon Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

$$(a_1, \ldots, a_6 \in \overline{K}).$$

この方程式を**ワイエルシュトラス形式** (**Weierstrass form**) という.

$x = \frac{X}{Z}, y = \frac{Y}{Z}$ とすることで方程式 (2.1) は次のように簡略化できる.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2}$$

$\mathrm{char}\,(\overline{K}) \neq 2$ ならば，方程式 (2.2) に次の代入

$$y \longmapsto \frac{1}{2}(y - a_1x - a_3)$$

を行うことで，次のように項を減らすことができる.

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{2.3}$$

$$(b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6).$$

さらに $\mathrm{char}\,(\overline{K}) \neq 2, 3$ ならば，方程式 (2.3) に次の代入

$$(x, y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

を行うことで，次のようにより項を減らすことができる．

$$y^2 = x^3 - 27c_4x - 54c_6$$

$$(c_4 = b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2b_4 - 216b_6).$$

ここから，どのようなワイエルシュトラス形式で与えられた射影曲線が非特異かどうかに着目する．

ワイエルシュトラス形式で与えられた E に対して

$$\Delta_E := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

を定め，***E* の判別式**という．

また，c_4, c_6を用いて表すと $1728\Delta_E = c_4^3 - c_6^2$ となる．

命題 2.2 ([Sil, Ⅲ.1, Proposition 1.4, pages 45–47])**.** ワイエルシュトラス形式で与えられた E に対して，次が成り立つ．

1. E は非特異である $\Leftrightarrow \Delta_E \neq 0$.
2. E は節点を持つ $\Leftrightarrow \Delta_E = 0, c_4 \neq 0$.
3. E は尖点を持つ $\Leftrightarrow \Delta_E = c_4 = 0$.

このことから，

$$\text{ワイエルシュトラス形式で与えられた } E \text{ が楕円曲線} \Leftrightarrow \Delta_E \neq 0$$

となる．

例 2.3. K 上の射影曲線である

$$E_A : y^2 + Axy = x^3$$

において，$b_2 = A^2, b_4 = 0, b_6 = 0, b_8 = 0$ なので $\Delta_{E_A} = 0$ となるから E_A は楕円曲線でない．さらに $c_4 = A^4$ なので $A = 0$ のとき尖点を持ち，$A \neq 0$ のとき節点を持つと分かる．

例 2.4. K 上の射影曲線である

$$E_B : y^2 + By = x^3$$

において, $b_2 = 0, b_4 = 0, b_6 = B^2, b_8 = 0$ なので $\Delta_{E_A} = -3^3B^4$ となるから $\mathrm{char}(K) \neq 3$ かつ $B \neq 0$ ならば，E_B は楕円曲線である.

2.2 群法則

この節では楕円曲線 E に演算 $\oplus$ を導入して群構造を定める．この $\oplus$ を幾何的に説明すると，以下のようになる.

$E : K$ 上の楕円曲線, $P, Q \in E$,

$L_1 : P, Q$ を通る直線 ($P = Q$ ならば P の接線), $R \in E : E$ と L_1の交点.

これらに対して L_2を R と O を通る直線とすると，L_2と E の 3 つ目の交点は $P \oplus Q$ である．さらに $(P \oplus Q) \oplus R = O$ である.

次に，以下のように E 上の演算として定めることができる.

定義 2.5. K 上の楕円曲線 $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

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 は以下のように定める：

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

$$x_1 = x_2\text{のとき，}\ \lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},\ \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

このとき E は加法 $\oplus$ により，単位元を無限遠点 O, P の逆元を $\ominus P$ とし結合法則と交換法則を満たすアーベル群となる[Sil, Ⅲ.2, Proposition 2.2, pages 51–52].

さらに，E 上の有理点全体の集合である $E(K)$ もアーベル群なので, $E(K)$ は E の部分群である[Sil, Ⅲ.2, Proposition 2.2, pages 51–52].

この $E(K)$ は以下のように呼ばれている.

定義 2.6. K 上の楕円曲線 E に対して

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

を**モーデル・ヴェイユ群 (Mordell-Weil group)** という.

また, $\oplus$を用いた次の表記法を定める.

定義 2.7. $m \in \mathbb{Z}, P \in E$ に対して

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

補題 2.8 ([Sil, Ⅲ.2, Group Law Algorithm 2.3, pages 53–54], [Sil, Ⅲ, Exercise 3.25, page 110])**.** $P = (x, y) \in E$ に対して, $[2]P$ の x 座標 $x([2]P)$, y 座標 $y([2]P)$ はそれぞれ

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

$$y([2]P) = \frac{2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + b_2b_8x - b_4b_6x + b_4b_8 - b_6^2}{(2y + a_1x + a_3)^3},$$

となる.

2.3 計算機 (PARI/GP) を用いた整数点に関する計算例

この節では, 計算機 PARI/GP [PARI, version 2.15.4] を用いた楕円曲線の整数点や演算 $\oplus$ に関する計算例を紹介する. 各種コマンドについては [User's Guide, 3.15 Elliptic curves, pages 506–558] を参照.

まず, PARI/GP にて $\mathbb{Q}$ 上の楕円曲線 $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ を定義するには `E=ellinit([`a_1, a_2, a_3, a_4, a_6`],D=1);` と入力する. $D = 1$ は E が $\mathbb{Q}$ 上で定義されていることを表している.

また, $a_1 = a_2 = a_3 = 0$ ならば `ellinit([`a_4, a_6`],D=1);` のみ入力すればよく, $\mathbb{F}_p$上 (p : 素数) で定義する場合は $D = p$ とする. さらに $\mathbb{Q}$ 上で定義する場合は `E=ellinit([`a_1, a_2, a_3, a_4, a_6`]);`, `E=ellinit([`a_4, a_6`]);` のように $D = 1$ を省略できる.

例 2.9. $\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 + 8$ を用いて, PARI/GP での計算方法を紹介する. E は以下のように入力して定義できる.

```
gp > E=ellinit([0,8]); \\ E を定義
gp > E.disc \\ E の判別式を計算
-27648
```

E を定めた後は, E に関する値を求められる．上記では E の判別式は -27648 であることを示している．

次に，E 上の整数点や演算 $\oplus$ に関する計算を行ってみる．

```
gp > for(a=-100000000,100000000,\
b=ellordinate(E,a);if(b,c=[a,b[1]];print(c)))
[1, 3]
[2, 4]
[46, 312]
```

これは $-100000000 \leq x \leq 100000000$, $0 \leq y$ において $(x, y) \in E$ となる整数点を示しており，楕円曲線を表す式において y^2 であることを考慮すると，
$(1, \pm 3), (2, \pm 4), (46, \pm 312) \in E$ が E 上の整数点であると分かる．

```
gp > for(a=-5,5,b=ellmul(E,[1,3],a);print(b))
[-4519919/6651241, -47556428853/17153550539]
[31073/2704, -5491823/140608]
[433/121, 9765/1331]
[-7/4, 13/8]
[1, -3]
[0]
[1, 3]
[-7/4, -13/8]
[433/121, -9765/1331]
[31073/2704, 5491823/140608]
[-4519919/6651241, 47556428853/17153550539]
```

これは，上から $[-5](1, 3), \ldots, [5](1, 3)$ の値が出力されている．

```
gp > elladd(E,[1,-3],[46,312]) \\ (1,-3)⊕(46,312) を計算
[2, -4]
gp > ellsub(E,[1,-3],[46,312]) \\ (1,-3)⊖(46,312) を計算
[34/225, -9548/3375]
```

これは $\oplus$と$\ominus$ による計算を行っており
$(1,-3) \oplus (46,312) = (2,-4)$ と $(1,-3) \ominus (46,312) = \left(\frac{34}{225}, \frac{-9548}{3375}\right)$ が分かる.

例 2.10 ([Sil, Ⅲ.2, Example 2.4, page 55]). まず, $E : y^2 = x^3 + 17$ と

$$\begin{aligned} P_1 &= (-2,3) \\ P_2 &= (-1.4) \\ P_3 &= (2,5) \\ P_4 &= (4,9) \\ P_5 &= (8,23) \\ P_6 &= (43,282) \\ P_7 &= (52,375) \\ P_8 &= (5234,378661) \end{aligned}$$

を定義する.

```
gp > E=ellinit([0,17]); \\ E を定義
gp > P1=[-2,3]; \\ P1 を定義
gp > P2=[-1,4]; \\ P2 を定義
gp > P3=[2,5]; \\ P3 を定義
gp > P4=[4,9]; \\ P4 を定義
gp > P5=[8,23]; \\ P5 を定義
gp > P6=[43,282]; \\ P6 を定義
gp > P7=[52,375]; \\ P7 を定義
gp > P8=[5234,378661]; \\ P8 を定義
```

次に, 整数点 $(x,y) \in E$ を計算してみる.

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

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

[Sil, Ⅲ.2, Example 2.4] にて整数点が $\pm P_1, \pm P_2, \pm P_3, \pm P_4, \pm P_5, \pm P_6, \pm P_7, \pm P_8$ の 16 個のみであると知られているので，全ての整数点を得ることができた．さらに [Sil, ⅡI.2, Example 2.4] において，任意の $P \in E(\mathbb{Q})$ は，ある $m, n \in \mathbb{Z}$ により

$$P = [m]P_1 \oplus [n]P_3$$

と表せること，つまり

$$E(\mathbb{Q}) = \langle P_1, P_3 \rangle \simeq \mathbb{Z}^2$$

であることを紹介している．P_4, P_5, P_7 については [Sil, Ⅲ.2, Example 2.4] でも紹介されているが，P_2, P_6, P_8 についても次のように表すことができる．

$$\begin{aligned}
P_1 &= P_1, \\
P_2 &= [-2]P_1 \oplus P_3, \\
P_3 &= P_3, \\
P_4 &= [1]P_1 \oplus [-1]P_3, \\
P_5 &= [-2]P_1, \\
P_6 &= [-1]P_1 \oplus [2]P_3, \\
P_7 &= [3]P_1 \oplus [-1]P_3, \\
P_8 &= [-4]P_1 \oplus [3]P_3.
\end{aligned}$$

さらに，PARI/GP を用いてこれらが正しいことを以下のように確認できる (PARI/GP では==を用いることで，等しいか確認でき，true ならば 1，false ならば 0 が出力される)．

`gp > P1==elladd(E,ellmul(E,P1,1),ellmul(E,P3,0))` \\ P_1 **と** $[1]P_1 \oplus [0]P_3$ **が等しいか確認**

```
1
gp > P2==elladd(E,ellmul(E,P1,-2),ellmul(E,P3,1)) \\ P_2 と [-2]P_1 ⊕ [1]P_3 が等しいか確認
1
gp > P3==elladd(E,ellmul(E,P1,0),ellmul(E,P3,1)) \\ P_3 と [0]P_1 ⊕ [1]P_3 が等しいか確認
1
gp > P4==elladd(E,ellmul(E,P1,1),ellmul(E,P3,-1)) \\ P_4 と [1]P_1 ⊕ [-1]P_3 が等しいか確認
1
gp > P5==elladd(E,ellmul(E,P1,-2),ellmul(E,P3,0)) \\ P_5 と [-2]P_1 ⊕ [0]P_3 が等しいか確認
1
gp > P6==elladd(E,ellmul(E,P1,-1),ellmul(E,P3,2)) \\ P_6 と [-1]P_1 ⊕ [2]P_3 が等しいか確認
1
gp > P7==elladd(E,ellmul(E,P1,3),ellmul(E,P3,-1)) \\ P_7 と [3]P_1 ⊕ [-1]P_3 が等しいか確認
1
gp > P8==elladd(E,ellmul(E,P1,-4),ellmul(E,P3,3)) \\ P_8 と [-4]P_1 ⊕ [3]P_3 が等しいか確認
1
```

ここで，PARI/GP にてモーデル・ヴェイユ群 $E(\mathbb{Q})$ の生成元を計算してみる．

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

上記の出力から

$$E(\mathbb{Q}) = \langle P_1, P_2 \rangle \simeq \mathbb{Z}^2$$

と表せることが分かる．さらに，既に

$$P_3 = [2]P_1 \oplus P_2,$$
$$P_2 = [-2]P_1 \oplus P_3$$

であることが分かっているので，$P_1, \ldots, P_8$ は次のように P_1 と P_2 でかける．

$$P_1 = P_1,$$
$$P_2 = P_2,$$
$$P_3 = [2]P_1 \oplus P_2,$$
$$P_4 = [-1]P_1 \oplus [-1]P_2,$$
$$P_5 = [-2]P_1,$$
$$P_6 = [3]P_1 \oplus [2]P_2,$$
$$P_7 = P_1 \oplus [-1]P_2,$$
$$P_8 = [2]P_1 \oplus [3]P_2.$$

最後に，PARI/GP を用いてこれらが正しいことを確認してみる．

```
gp > P1==elladd(E,ellmul(E,P1,1),ellmul(E,P2,0)) \\ P1 と [1]P1 ⊕ [0]P2 が等しいか確認
1
gp > P2==elladd(E,ellmul(E,P1,0),ellmul(E,P2,1)) \\ P2 と [0]P1 ⊕ [1]P2 が等しいか確認
1
gp > P3==elladd(E,ellmul(E,P1,2),ellmul(E,P2,1)) \\ P3 と [2]P1 ⊕ [1]P2 が等しいか確認
1
gp > P4==elladd(E,ellmul(E,P1,-1),ellmul(E,P2,-1)) \\ P4 と [-1]P1 ⊕ [-1]P2 が等しいか確認
1
gp > P5==elladd(E,ellmul(E,P1,-2),ellmul(E,P2,0)) \\ P5 と [-2]P1 ⊕ [0]P2 が等しいか確認
1
gp > P6==elladd(E,ellmul(E,P1,3),ellmul(E,P2,2)) \\ P6 と [3]P1 ⊕ [2]P2 が等しいか確認
```

```
1
gp > P7==elladd(E,ellmul(E,P1,1),ellmul(E,P2,-1)) \\ P_7 と [1]P_1 ⊕ [−1]P_2 が等しいか確認
1
gp > P8==elladd(E,ellmul(E,P1,2),ellmul(E,P2,3)) \\ P_8 と [2]P_1 ⊕ [3]P_2 が等しいか確認
1
```

例 2.11. $E : y^2 = x^3 + 5x + 11$ に対して，整数点 $(x, y) \in E$ を計算してみる．

```
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 >
```

上記の例では，$-100000000 \leq x \leq 100000000$ において $(x, y) \in E$ となる整数点が存在しない．実際，$E(\mathbb{Q}) = \{O\}$ であることが以下のように確かめられる．

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

3　有限体上の楕円曲線

この章では，3.1 節にて Silverman [Sil, Ⅲ, V] の内容を参考に，有限体上の楕円曲線 $E/\mathbb{F}_q$ における $E(\mathbb{F}_q)$ の位数に関する重要な定理である Hasse の定理 (定理 3.9) を紹介する．3,2 節では $E(\mathbb{F}_p)$ の構造を理解することを目的とした計算機 (PARI/GP) の活用例について紹介する．また，Hasse の定理は E. Artin が自身の学位論文にて予想し，H. Hasse が 1933 年に証明したものである．

3.1　Hasse の定理

Hasse の定理の証明を紹介する前に，必要な定義や定理を記載する．

系 3.1 ([Sil, Ⅲ.5, Corollary 5.5, page 79])**.** $E/\mathbb{F}_q\,(q=p^k, k\in\mathbb{N}), \phi_q$を q 乗フロベニウス写像, $m,n\in\mathbb{Z}$ とする．このとき

$$\begin{array}{rccc} f\colon & E & \longrightarrow & E \\ & \cup & & \cup \\ & P & \longmapsto & [m]P+[n]P \end{array} \quad \text{が分離的である} \Leftrightarrow p\nmid m.$$

特に $m=1, n=-1$ のとき，つまり $\mathrm{id}-\phi_q$ は分離的である．

定義 3.2. E_1, E_2 を楕円曲線とする．

ϕ が E_1から E_2への**同種写像** (**Isogeny**) $\overset{\text{def}}{\Longleftrightarrow}$ 正則写像 $\phi: E_1 \longrightarrow E_2\,(\phi(O)=O)$.

E_1と E_2が**同種** (**Isogenous**) $\overset{\text{def}}{\Longleftrightarrow}$ 同種写像 $\phi: E_1 \longrightarrow E_2\,(\phi(E_1)\neq\{O\})$ が存在する．

定理 1.19 より同種写像 ϕ は定数または全射となると分かり，$\phi(O)=O$ より

同種写像ϕはゼロ写像または全射

となる．このことから，ゼロ写像以外の任意の同種写像は曲線間の有限写像である．さらに定義 1.21 と同様に，ゼロ写像でない同種写像 $\phi: E_1 \longrightarrow E_2$から

$$\phi^*: \overline{K}(E_2) \longrightarrow \overline{K}(E_1)$$

を得る．**ϕ の次数** (**degree**) を

$$\deg\phi := [\overline{K}(E_1) : \phi^*\overline{K}(E_2)]$$

と表し, 体の拡大 $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$ が分離的, 非分離的, 純非分離的であるとき, それぞれ ϕ が**分離的** (**separable**), **非分離的** (**inseparable**), **純非分離的** (**purely inseparable**) であるといい, 体の拡大の**分離次数** (**separable degree**), **非分離次数** (**inseparable degree**) をそれぞれ $\boldsymbol{\deg_s \phi, \deg_i \phi}$ と表す.

定理 3.3 ([Sil, Ⅲ.4, Theorem 4.10, page 72])**.** $\phi : E_1 \longrightarrow E_2$ をゼロ写像でない同種写像とする. このとき,

$$\phi \text{が分離的} \Rightarrow \phi \text{は不分岐}, \ |\mathrm{Ker}\,\phi| = \deg\phi, \ \overline{K}(E_1)/\phi^*\overline{K}(E_2) \text{がガロア拡大.}$$

定理 3.4 ([Sil, Ⅲ.3, Theorem 3.6, page 64])**.** E/K を楕円曲線とする.
E 上の演算である $\oplus : E \times E \longrightarrow E, \ominus : E \longrightarrow E$ は正則写像となる.

楕円曲線 E_1から E_2への 同種写像全体を

$$\mathrm{Hom}(E_1, E_2) := \{f \mid f : E_1 \longrightarrow E_2, \text{同種写像}\}$$

と表す.

楕円曲線はアーベル群なのでそれらの間の写像も群を作り, 2 つの同種写像 $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ の和は

$$(\phi + \psi)(P) = \phi(P) \oplus \psi(P)$$

と定義され, 定理 3.4 より $\phi + \psi$ は正則写像であり

$$(\phi + \psi)(O) = \phi(O) \oplus \psi(O) = O$$

より $\phi + \psi$ は同種写像となるから, この加法により $\boldsymbol{\mathrm{Hom}(E_1, E_2)}$ **は群**となる.

さらに, $E_1 = E_2$ ならば同種写像の合成を行えるため,

$$(\phi\psi)(P) = \phi(\psi(P))$$

を乗法とする環である.

定義 3.5. E を楕円曲線とする.

$\boldsymbol{E}$ **の自己準同型環** (**endomorphism ring**) を

$$\mathrm{End}(E) := \mathrm{Hom}(E, E) = \{f \mid f : E \longrightarrow E, \text{同種写像}\}$$

と表す. また, $\mathrm{End}(E)$ の単元は $\boldsymbol{E}$ **の自己同型群** (**automorphism group**) をなし, $\boldsymbol{\mathrm{Aut}(E)}$ と表す.

定義 3.6. A をアーベル群 とする．次の (1), (2) を満たす $d : A \longrightarrow \mathbb{R}$ を**二次形式** (**quadratic form**) という．

1. $\forall \alpha \in A\,,\, d(\alpha) = d(-\alpha)$.
2. ペアリング $\begin{array}{ccc} A \times A & \longrightarrow & \mathbb{R} \\ \cup & & \cup \\ (\alpha, \beta) & \longmapsto & d(\alpha+\beta) - d(\alpha) - d(\beta) \end{array}$ が双線形である．

さらに，次の (3), (4) を満たす二次形式 d を**正定値** (**positive definite**) という．

3. $\forall \alpha \in A\,,\, d(\alpha) \geq 0$.
4. $d(\alpha) = 0 \Leftrightarrow \alpha = 0$.

系 3.7 ([Sil, Ⅲ.6, Corollary 6.3, page 85])**.** E_1, E_2 を楕円曲線とする．このとき

$$\text{次数写像 deg}: \quad \begin{array}{ccc} \mathrm{Hom}(E_1, E_2) & \longrightarrow & \mathbb{Z} \\ \cup & & \cup \\ \phi & \longmapsto & [\overline{K}(C_1) \colon \phi^* \overline{K}(C_2)] \end{array}$$

は正定値二次形式である．

補題 3.8 ([Sil, V.1, Lemma 1.2, page 138])**.** A : アーベル群, $d : A \longrightarrow \mathbb{Z}$: 正定値二次形式 とする．このとき

$\forall \psi, \phi \in A$ に対して

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi) d(\psi)}$$

となる．

これらを用いることで，Hasse の定理は以下のように証明できる．

定理 3.9 (Hasse)**.** 楕円曲線 $E/\mathbb{F}_q$，$\mathrm{char}(\mathbb{F}_q) = p$ に対して，次が成り立つ．

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

証明. ϕ_q を q 乗フロベニウス写像とする．

このとき，$\forall P \in E(\overline{\mathbb{F}}_q)$ に対して

$$P \in E(\mathbb{F}_q) \Leftrightarrow \phi_q(P) = P$$

となるので，$E(\mathbb{F}_q) = \mathrm{Ker}\,(\mathrm{id} - \phi)$ となる．

ここで，$\mathrm{id} - \phi_q$ は系 3.1 より分離的である．さらに定理 3.3 より

$$|E(\mathbb{F}_q)| = |\mathrm{Ker}\,(\mathrm{id} - \phi)| = \deg(\mathrm{id} - \phi).$$

系 3.7 より $\mathrm{End}(E)$ 上の次数関数は正定値二次形式であり $\deg\phi = q$ なので，補題 3.8 より

$$\big||E(\mathbb{F}_q)| - q - 1\big| = |\deg(\mathrm{id} - \phi_q) - \deg(\phi_q) - \deg(\mathrm{id})| \leq 2\sqrt{d(\phi_q)d(\mathrm{id})} = 2\sqrt{q}.$$

□

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** ということである．また，$E(\mathbb{F}_q)$ を計算するアルゴリズムとして **Schoof のアルゴリズム** (**Schoof's Algorithm**) があり，$E(\mathbb{F}_q)$ の値を $O\left((\log q)^8\right)$ ステップ (定義 4.12) で計算する．[Sil, XI.3, Schoof's Algorithm 3.1, pages 373–375] を参照．さらに，Schoof のアルゴリズムの計算コストを下げたアルゴリズムの詳細と PARI/GP への実装に関しては [安田 2] を参照.

3.2 計算機 (PARI/GP) を用いた $E(\mathbb{F}_p)$ の計算例

$E(\mathbb{F}_p)$ を計算する方法の 1 つとして，計算機 PARI/GP による方法を紹介する．以下，`E.no`, `E.cyc`, `E.gen` というコマンドを用いて具体例を示しながら紹介する.

例 3.10. 例 2.9 での楕円曲線 $E : y^2 = x^3 + 8$ を $\mathbb{F}_{17}$ 上で考える.

```
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)]]
```

`E.no` に対する出力から $|E(\mathbb{F}_{17})| = 18$，`E.cyc` に対する出力から $E(\mathbb{F}_{17}) \simeq \mathbb{Z}/18\mathbb{Z}$, `E.gen` に対する出力から $E(\mathbb{F}_{17}) = \langle(1,3)\rangle$ であると分かる.

実際に $[1](1,3), \ldots, [18](1,3)$ を計算すると以下のようになる.

```
for(a=1,18,b=ellmul(E,[1,3],a);print(b)) \\ [1](1,3),...,[18](1,3) の計算
[Mod(1, 17), Mod(3, 17)]
```

```
[Mod(11, 17), Mod(9, 17)]
[Mod(4, 17), Mod(2, 17)]
[Mod(14, 17), Mod(7, 17)]
[Mod(3, 17), Mod(16, 17)]
[Mod(0, 17), Mod(12, 17)]
[Mod(12, 17), Mod(11, 17)]
[Mod(2, 17), Mod(4, 17)]
[Mod(15, 17), Mod(0, 17)]
[Mod(2, 17), Mod(13, 17)]
[Mod(12, 17), Mod(6, 17)]
[Mod(0, 17), Mod(5, 17)]
[Mod(3, 17), Mod(1, 17)]
[Mod(14, 17), Mod(10, 17)]
[Mod(4, 17), Mod(15, 17)]
[Mod(11, 17), Mod(8, 17)]
[Mod(1, 17), Mod(14, 17)]
[0]
```

例 3.11. 例 2.11 での楕円曲線 $E : y^2 = x^3 + 5x + 11$ を $\mathbb{F}_{31}$ 上で考える.

```
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)]]
```

これらより, $|E(\mathbb{F}_{31})| = 36$, $E(\mathbb{F}_{31}) \simeq \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $E(\mathbb{F}_{31}) = \langle (8, 25), (20, 19) \rangle$ であると分かる.

4　楕円曲線の暗号への応用

この章では Silverman [Sil, XI] の内容を参考に，4.1 節では ECDLP により暗号を生成するアルゴリズムを，4.2 節では DLP を解くためのアルゴリズムの概要を紹介している．さらに，4.3 節では特別な場合の ECDLP を解くアルゴリズムの概要を紹介し，[PARI, ver 2.15.4] を用いた計算例を示している．

4.1　有限体上の楕円曲線を用いた暗号

1976 年に Diffie と Hellman により公開鍵暗号というアイデアが発明され，そこに数学を応用することで次のような実用的な暗号が発明された．

有名なものとして，まず **RSA 暗号** (**RSA cryptosystem**) が存在する．これは 1977 年に Rivest, Shamir, Adleman により公開されたものであり，大きな数の因数分解の難しさを利用した暗号である．次により解読が困難 (つまり難しい問題を基にした) な暗号として，Diffie と Hellman による **Diffie-Hellman 鍵交換** (**Diffie-Hellman Key Exchange**) (アルゴリズム 4.5) や ELGamal による **ELGamal 公開鍵暗号** (**ELGamal Public Key cryptosystem**) (アルゴリズム 4.9) が発明された．これらは元々, $\mathbb{F}_q^\times$ ($q = p^k, k \in \mathbb{Z}$) における DLP (定義 4.1) を基にした暗号であった．しかし，Koblitz と Miller が基にする問題を ECDLP (定義 4.2) 置き換えたことで，**楕円曲線暗号** (**elliptic curve cryptography**) が作り出された．

定義 4.1 (離散対数問題 (DLP))**.** 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** (**Discrete Logarithm Problem**) という．また，**DLP** と表される．

定義 4.2 (楕円曲線離散対数問題 (ECDLP))**.** $E/\mathbb{F}_q$ を楕円曲線, $P, Q \in E(\mathbb{F}_q)$ ($Q \in \langle P \rangle$) 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** (**Elliptic Curve Discrete Logarithm Problem**) という．また，**ECDLP** と表される．

定義 4.3. 関数 $f(n), g(n) > 0\,(\forall n \in \mathbb{N})$ に対して，$f(n) < Cg(n)$ となる定数 C が存在するとき，$f(n) = O(g(n))$ と表す.

任意の群 G に対する DLP を解くことができるアルゴリズムとして **Shanks の小ステップ-大ステップアルゴリズム** (**Shanks's Babystep-Giantstep Algorithm**)(アルゴリズム 4.14)，**Pollard の ρ 法** (**Pollard's ρ algorithm**)(アルゴリズム 4.16) が存在し, これらにより $O(\sqrt{q})$ ステップで解くことができる. しかし用いられている群によってより短時間で解ける場合がある．次の 3 つの例が有名なものである.

例 4.4 ([Sil, XI.4, Example 4.1, page 377])**.** $q = p^k$ $(k \in \mathbb{Z})$ とする.

1. $G = \mathbb{F}_q^+$
   DLP は $xm = y (x, y \in \mathbb{F}_q)$ の解 m を求めることになる.
   $\mathbb{F}_q$における x の逆元 を求めれば解け，ユークリッドの互除法を用いることで $O(\log(q))$ ステップで解くことができる.
2. $G = \mathbb{F}_q^\times$
   DLP は $x^m = y (x, y \in \mathbb{F}_q^\times)$ の解 m を求めることになる.
   指数解析法を用いることで $\exp\left(c\sqrt{\left(\log(q)\right)\left(\log(\log(q))\right)^2}\right)$ (c は小さい絶対定数) ステップで解くことができる.
3. $G = E(\mathbb{F}_q)$
   DLP は定義 4.2 での ECDLP となる.
   一般的に最短の解法が Shanks の小ステップ-大ステップアルゴリズム (アルゴリズム 4.14)，Pollard の ρ 法 (アルゴリズム 4.16) であり，解くことが難しい問題となる.
   $E/\mathbb{F}_p$ (p は素数, $p \geq 3$) において $|E(\mathbb{F}_p)| = p$ となる場合は特別な解法があり,4.3 節で紹介する.

次の 2 つのアルゴリズムは任意の群 G に対して用いることができるが，$E(\mathbb{F}_q)$ を用いた楕円曲線暗号の場合を紹介する．例 4.4 でも触れたように，ECDLP を用いた暗号は解読の困難性が高い．また，暗号の概要に現れるアリスとボブとは，一般的に暗号の送信者と受信者として用いられる人名である.

アルゴリズム 4.5 (Diffie-Hellman 鍵交換, [Sil, XI.4, Diffie-Hellman Key Exchange 4.2, page 378])**.** 以下の手順により，アリスとボブは楕円曲線上のある点を，事前にその点を知らずに安全に交換できる.

1. アリスとボブの間で，有限体 $\mathbb{F}_q$，楕円曲線 $E/\mathbb{F}_q$，点 $P \in E(\mathbb{F}_q)$ を一致させる．
2. アリスは秘密にする $a \in \mathbb{Z}$ を選び，点 $A = [a]P \in E(\mathbb{F}_q)$ を計算する．
3. ボブは秘密にする $b \in \mathbb{Z}$ を選び，点 $B = [b]P \in E(\mathbb{F}_q)$ を計算する．
4. アリスとボブは安全とは限らない通信回路で A と B を交換する．
5. アリスは $[a]B = [ab]P$，ボブは $[b]A = [ab]P$ を計算する．

以上により，アリスとボブは値 $[ab]P$ を共有できる．

Diffie-Hellman 鍵交換 (アルゴリズム 4.5) の安全性に関係する点として，注意 4.6，注意 4.7 を挙げられる．

注意 4.6 ([Sil, XI.4, Remark 4.3.2, page 378])．アリスとボブで一致させる $P \in E(\mathbb{F}_q)$ は，P の位数が大きな素数で割り切れることが重要である．その理由の 1 つとして，Pohlig と Hellman による中国式剰余定理を用いたアルゴリズム (Pohlig-Hellman アルゴリズム) により，ECDLP を解く時間は P の位数を割り切る最大の素数にのみ依存するという事実がある．

注意 4.7 ([Sil, XI.4, Remark 4.3.4, page 378])．アリスとボブの通信を盗聴し値 $[ab]P$ を得たい人物イヴについて考える．イヴは有限体 $\mathbb{F}_q$，楕円曲線 $E/\mathbb{F}_q$，点 $P \in E(\mathbb{F}_q)$，$A \in E(\mathbb{F}_q)$，$B \in E(\mathbb{F}_q)$ を知ることができる．ここから $[ab]P$ を得る方法として次の 2 つが考えられる．

1. $A = [a]P$, $B = [b]P$ を ECDLP として解き，値 a, b を得て，$[ab]P$ を計算する．
2. 点 P, $A = [a]P$, $B = [b]P$ から直接 $[ab]P$ を求める (定義 4.8 での問題に帰着する)．

しかし，楕円曲線 Diffie-Hellman 問題 (定義 4.8) を解く方法として現在知られているものは，$A = [a]P$, $B = [b]P$ を解いて値 a, b を得る方法のみなのでイヴは値 a, b を知る必要がある．つまり (1) の方法を行うしかない．

定義 4.8 (楕円曲線 Diffie-Hellman 問題)．$E(\mathbb{F}_q)$ 上で 3 つの点 P, $[a]P$, $[b]P$ が与えられる．点 $[ab]P$ を計算せよ．

ELGamal 公開鍵暗号 (アルゴリズム 4.9) にて用いられる平文，暗号文とは，それぞれ送りたいメッセージ，安全に送るためにメッセージを一時的に変換したもののことである．

アルゴリズム 4.9 (ELGamal 公開鍵暗号, [Sil, XI.4, ELGamal Public Key Cryptosystem 4.4, page 379])**.**

1. アリスとボブの間で，有限体 $\mathbb{F}_q$，楕円曲線 $E/\mathbb{F}_q$，点 $P \in E(\mathbb{F}_q)$ を一致させる．
2. ボブは秘密にする $b \in \mathbb{Z}$ を選び，点 $B = [b]P \in E(\mathbb{F}_q)$ を計算する．
3. 点 B を公開し，ボブの公開鍵とする．また，b を秘密鍵とする．
4. アリスは平文 $M \in E(\mathbb{F}_q)$ と乱数 $k \in \mathbb{Z}$ を選び，$A_1 = [k]P, A_2 = M + [k]B$ $(A_1, A_2 \in E(\mathbb{F}_q))$ を計算する．
5. アリスは暗号文 (A_1, A_2) を安全とは限らない通信回路でボブに送信する．
6. ボブは秘密鍵 b を用いて $M = A_2 - [b]A_1 \in E(\mathbb{F}_q)$ を計算する．

アルゴリズム 4.9 (6) にて $M = A_2 - [b]A_1$ とあるが，これは次のように導出できる．

$$\begin{aligned} A_2 - [b]A_1 &= (M + [k]B) - [b][k]P \\ &= M + [k][b]P - [b][k]P \\ &= M. \end{aligned}$$

上記の式から，ボブは乱数 k を知らずとも平文 M を得ることができると分かる．

注意 4.10 ([Sil, XI.4, Remark 4.3.4, page 378])**.** 注意 4.7 と同様に，アリスとボブの通信を盗聴し平文 M を得たい人物イヴについて考える．イヴは有限体 $\mathbb{F}_q$，楕円曲線 $E/\mathbb{F}_q$，点 $P \in E(\mathbb{F}_q)$, $A_1 \in E(\mathbb{F}_q)$, $A_2 \in E(\mathbb{F}_q)$ を知ることができるので，$M = A_2 - [k]B$ を得るためには $[k]B = [kb]P$ が必要となる．ここから $[k]B = [kb]P$ を得る方法として次の 2 つが考えられる．

1. $A_1 = [k]P$, $B = [b]P$ を ECDLP として解き，値 k, b を得て，$[kb]P$ を計算する．
2. 点 P, $A_1 = [k]P$, $B = [b]P$ から直接 $[kb]P$ を求める (定義 4.8 での問題に帰着する)．

しかし注意 4.7 で述べた通り，イヴは値 k, b を知る必要があるため，(1) の方法を行うしかない．

Diffie-Hellman 鍵交換 (アルゴリズム 4.5) や ELGamal 公開鍵暗号 (アルゴリズム 4.9) はアリスとボブが情報を交換できるようにするアルゴリズムであったが，次の楕円曲線電子署名アルゴリズム (ECDSA) (アルゴリズム 4.11) は電子著名の正当性を検証できるようにするものである．

アルゴリズム 4.11 (楕円曲線電子署名アルゴリズム (ECDSA), [Sil, XI.4, Elliptic Curve Digital Signature Algorithm (ECDSA) 4.6, pages 380–381])**.**

1. アリスとボブの間で，有限体 $\mathbb{F}_p$，楕円曲線 $E/\mathbb{F}_p$，素数位数 N の点 $P \in E(\mathbb{F}_p)$ を一致させる．
2. アリスは秘密にする $a \in \mathbb{Z}$ を選び，点 $A = [a]P \in E(\mathbb{F}_p)$ を計算する．
3. 点 A を公開し，アリスの署名検証鍵 (公開鍵) とする．また，a はアリスの署名生成鍵 (秘密鍵) となる．
4. アリスは著名する電子文書 $d \pmod N$ と乱数 $k \pmod N$ を選び，$[k]P$ を計算し s_1, s_2 を
$$\begin{aligned} s_1 &\equiv x([k]P) \pmod N \\ s_2 &\equiv (d + as_1)k^{-1} \pmod N \end{aligned} \tag{4.1}$$
とおく ($[k]P$ の x 座標 $x([k]P) \in \mathbb{F}_p$，完全代表系 $\mathbb{F}_p = \{1, \ldots, p-1\}$)．さらに文書 d の署名として (s_1, s_2) を公開する．
5. ボブは
$$v_1 \equiv ds_2^{-1} \pmod N \tag{4.2}$$
$$v_2 \equiv s_1 s_2^{-1} \pmod N \tag{4.3}$$
を計算する．次に $[v_1]P + [v_2]A \in E(\mathbb{F}_p)$ を計算し
$$x([v_1]P + [v_2]A) \equiv s_1 \pmod N$$
となることを検証する．

実際，楕円曲線電子署名アルゴリズム (アルゴリズム 4.11) にて (1)〜(4) を行うと，ボブは次のように (5) の検証を行える．

$$\begin{aligned} [v_1]P + [v_2]A &\equiv [ds_2^{-1}]P + [s_1 s_2^{-1}][a]P \pmod N && (\because \text{合同式 (4.2), (4.3)}) \\ &= [s_2^{-1}(d + as_1)]P \\ &\equiv [k]P \pmod N && (\because \text{合同式 (4.1)}). \end{aligned}$$

4.2 DLP を解くアルゴリズム

ここから，任意の群 G に対する DLP を解くためのアルゴリズムである Shanks の小ステップ-大ステップアルゴリズム (アルゴリズム 4.14)，Pollard の ρ 法 (アルゴリズム 4.16) を紹介する．また，この節では DLP を定義 4.1 での問題として考える．

これらのアルゴリズムの複雑性を説明する際に，定義 4.12 の**ステップ** (**steps**)，**記憶領域** (**storage**) を判断基準として用いる．

定義 4.12. 平均値で見た際，アルゴリズムが T 回の群演算を必要とし，群の S 個の元の値を保存する必要があるとき，アルゴリズムが $\boldsymbol{T}$ **ステップかかり** $\boldsymbol{S}$ **領域を要する**という．

注意 4.13. アルゴリズムを実行している際に行う元のリストの整列や比較などに要する時間は，一般に群の演算にかかる時間と比べると少ないため，定義 4.12 での判断基準では無視している．

アルゴリズム 4.14，アルゴリズム 4.16 は DLP を解くために，2 つの集合に共通な元である**衝突する元** (**collisions**) を求めるため**衝突アルゴリズム** (**collision algorithm**) とよばれる．

アルゴリズム 4.14 (Shanks の小ステップ-大ステップアルゴリズム, [Sil, XI.5, Proposition 5.2, page 382])**.** G を群，$x, y \in G$，$\mathrm{ord}\,(x) = n$ とする．以下のアルゴリズムは，DLP を $O(\sqrt{n})$ ステップかつ $O(\sqrt{n})$ 領域で解く．

1. $N = \lceil \sqrt{n} \rceil$ (N を $\sqrt{n}$ 以上の最小の整数) とする．
2. G の元のリスト (小ステップ)
$$x, x^2, x^3, \ldots, x^N$$
を作成する．
3. $z = x^{-N}$ とおき，G の元のリスト (大ステップ)
$$yz, yz^2, yz^3, \ldots, yz^N$$
を作成する．
4. 小ステップ，大ステップの間で一致する元を探す．一致するものがあれば $x^i = yz^j = yx^{-jN}$ となるので $y = x^{i+jN}$ となる．一致するものがなければ，y は x のべき乗でないと分かる．

$n = \mathrm{ord}(x) \geq 1$ より $N \geq 2$ であるから，アルゴリズム 4.14 は x を x^1 倍し続ける小ステップと，yx^{-N} を x^{-N} $(N \geq 2)$ 倍し続ける大ステップを用いて衝突する元を探すアルゴリズムである．

次に，アルゴリズム 4.16 と強く関係のある衝突定理を紹介する．

定理 4.15 ([Sil, XI.5, Theorem 5.3, page 382])**.** S を N 個の元をもつ有限集合，$f : S \longrightarrow S$ を関数とする．初期値 $x_0 \in S$ から始まる点列 $x_0, x_1, x_2, \ldots$ を

$$x_i = f(x_{i-1}) = \underbrace{f \circ f \circ \cdots \circ f}_{i \text{ 回}}(x_0)$$

により定義する．さらに，

> T を数列 $(x_i)_{i \geq 0}$において x_{T-1}が一度だけ現れるような最大の整数，
> L を $x_{T+L} = x_T$となる最小の整数

と定義する．このとき，以下の (1), (2) が成り立つ．

1. $T \leq \exists i \leq T + L - 1$ s.t. $x_{2i} = x_i$
2. $f : S \longrightarrow S$ の繰り返しによる S のかき混ぜが十分にランダムならば，最初の一致である x_{T+L} が見つかるまでのステップ数の期待値は $\sqrt{\dfrac{\pi N}{2}}$ である．

定理 4.15 は，数列 $x_0, x_1, x_2, \ldots$ において $x_2 i = x_i$ を満たす項を $O(\sqrt{n})$ ステップかかることを表している．アルゴリズム 4.16 はこのことを利用したものであるためステップ数はアルゴリズム 4.14 と同じ $O(\sqrt{n})$ ステップである．しかし実質的に記憶領域を必要としないという特徴がある．また，アルゴリズム 4.16 は 1978 年に Pollard によって提案されたアルゴリズムである．

アルゴリズム 4.16 (Pollard の ρ 法, [Sil, XI.5, Algorithm 5.4, pages 384–386])**.** G を群，$x, y \in G$, $\mathrm{ord}(x) = n$ とする．群 G をおよそ同じサイズの 3 つの集合 A, B, C を用いて

$$G = A \cup B \cup C$$

と分割し，かき混ぜが十分にランダムである

$$f(z) = \begin{cases} xz & (z \in A) \\ z^2 & (z \in B) \\ yz & (z \in C) \end{cases}$$

を用いる．この関数 f を用いて，初期値 $z_0 = 1$ に繰り返し f を適用すると

$$z_i = \underbrace{f \circ f \circ \cdots \circ f}_{i \text{ 回}}(z_0) = x^{\alpha_i} y^{\beta_i} \ (\alpha_i, \beta_i \in \mathbb{Z})$$

と表せる．$\alpha_0 = \beta_0 = 0$ とすると，関数 f の定義と α, β がそれぞれ x, y の乗数であることより

$$\alpha_{i+1} = \begin{cases} \alpha_i + 1 & (z_i \in A) \\ 2\alpha_i & (z_i \in B) \\ \alpha_i & (z_i \in C) \end{cases} \quad \beta_{i+1} = \begin{cases} \beta_i & (z_i \in A) \\ 2\beta_i & (z_i \in B) \\ \beta_i + 1 & (z_i \in C) \end{cases}$$

となる．さらに，初期値を $\omega_0 = 1$ とした点列 $\omega_{i+1} = f(f(\omega_i))$ を用いる．このとき，

$$\begin{aligned} &\omega_0 = 1 = z_0 \\ &\omega_1 = f(f(\omega_0)) = f(f(z_0)) = z_2 \\ &\omega_2 = f(f(\omega_1)) = f(f(z_1)) = z_4 \\ &\vdots \end{aligned}$$

より

$$\omega_i = z_{2i} = x^{\gamma_i} y^{\delta_i} \quad (\gamma_i = \alpha_{2i},\ \delta_i = \beta_{2i})$$

となる．

ここから，

$$x^{\alpha_i} y^{\beta_i} = z_i = \omega_i = z_{2i} = x^{\gamma_i} y^{\delta_i}$$

となる z_i, ω_i が見つかるまで計算を続ける．そのような z_i, ω_i の存在は定理 4.15(1) で示されている．さらに z_i, ω_i はそれぞれ直前の項 z_{i-1}, ω_{i-1} から個別に計算することができるのでそれ以前の項を記憶しておく必要がない．これが実質的に記憶領域を必要としない理由である．

A, B, C が G の元をかき混ぜるのに十分であると仮定すると，定理 4.15(2) より

$$x^{\alpha_i} y^{\beta_i} = z_i = \omega_i = z_{2i} = x^{\gamma_i} y^{\delta_i}$$

の一致を求めるのに $O(\sqrt{n})$ ステップ必要であると分かる．一致を求めた後

$$x^{\alpha_i - \gamma_i} = y^{\delta_i - \beta_i}$$

と表す．ここで，$\gcd(\delta_i - \beta_i, n) = 1$ を仮定する ($d = \gcd(\delta_i - \beta_i, n) > 1$ である場合については注意 4.17 にて述べる)．このとき y は x のべき乗として表せ，$x^m = y$ を満たす m が

$$m \equiv (\alpha_i - \gamma_i)(\delta_i - \beta_i)^{-1} \pmod{n}$$

となるので $x^m = y$ が解ける．

注意 4.17 ([Sil, XI.5, Algorithm 5.4, Pollard's ρ algorithm, pages 384–386])**.** $d = \gcd(\delta_i - \beta_i, n) > 1$ となる場合は，y^d を x のべき乗で表せるので

$$x^e = y^d$$

と表す．さらに $\mathrm{ord}(x) = n$ より

$$x^{(e+nu)/d} = y \ \ (0 \leq u \leq d)$$

と表せる．d が大きすぎなければ u を全て確認することで DLP を解くことができる．d が大きすぎる場合はアルゴリズム 4.16 にて得た関係式

$$x^{\alpha_i - \gamma_i} = y^{\delta_i - \beta_i}$$

を用いて解く．

注意 4.6 にて ECDLP では P の位数が大きな素数で割り切れることが重要であったように，DLP でも $\gcd(\delta_i - \beta_i, n) = 1$ を仮定することが多い．

アルゴリズム 4.18 (単純アルゴリズム, [Sil, XI.5, Example 5.1, page 381])**.** G を群，$x, y \in G$, $\mathrm{ord}(x) = n$ とする．y と等しいものが見つかるまで $x_1, x_2, x_3, \ldots$ と計算していく．これを**単純アルゴリズム** (**naive algorithm**) という．このアルゴリズムでは $O(n)$ ステップと $O(1)$ 領域を必要とする．

注意 4.19. 衝突アルゴリズムであるアルゴリズム 4.14，アルゴリズム 4.16 と単純アルゴリズム (アルゴリズム 4.18) を比較すると，衝突アルゴリズムがより少ないステップ数で済むことが分かる．これは衝突する元を求めることが，ある集合の特定の元を求めることよりも容易であることに由来している．

注意 4.20. アルゴリズム 4.16 や次節で紹介するアルゴリズム 4.24 を ECDLP に用いる具体的な方法は [安田 1, 3 ECDLP に対する攻撃, pages 76–80] を参照．また，[安田 1, 4 楕円曲線暗号の安全性, pages 80] では各アルゴリズム (攻撃法) がどのような ECDLP に有効であるかを表としてまとめている．

4.3 特別な ECDLP へのアルゴリズムと計算機 (PARI/GP) での計算例

まず，特別な ECDLP へのアルゴリズムについて考えるために必要な定義を紹介する．

定義 4.21. E を楕円曲線とし，$m \in \mathbb{Z}$ $(m \geq 1)$ とする．

E の m ねじれ部分群 $E[m]$ (m-torsion subgroup) とは E の位数 m の点全体の集合であり，次のように定める：

$$E[m] := \{P \in E \mid [m]P = O\}.$$

E のねじれ部分群 E_{tors} (torsion subgroup) とは E の有限位数の点全体の集合であり，次のように定める：

$$E_{\mathrm{tors}} := \bigcup_{m=1}^{\infty} E[m].$$

定義 4.22. μ_m を 1 の m 乗根全体からなる群とし，$T \in E[m]$，$f \in \overline{K}(E)$ $(\mathrm{div}(f) = m(T) - m(O))$，$T' \in E$ $([m]T' = T)$，$g \in \overline{K}(E)$ $\left(\mathrm{div}(g) = \sum_{R \in E[m]} \Big((T' \oplus R) - (R)\Big)\right)$ とする．

ヴェイユ $\mathbf{e}_m$ ペアリング (Weil $\mathbf{e}_m$ -pairing) を次のように定める：

$$\begin{array}{rccc} e_m\colon & E[m] \times E[m] & \longrightarrow & \mu_m \\ & \cup\!| & & \cup\!| \\ & (S, T) & \longmapsto & \dfrac{g(X \oplus S)}{g(X)} \end{array}$$

($X \in E$ は $g(X \oplus S), g(X)$ がともに定義され $g(X \oplus S) \neq 0, g(X) \neq 0$ となる任意の点)

定義 4.23. $N \geq 1$ $(N \in \mathbb{Z})$ とし，μ_N を 1 の N 乗根全体からなる群とする．**N の $\mathbb{F}_q$ への埋め込み次数 d (embedding degree)** を次のように定める：

$$d := \min\{m \in \mathbb{N} \mid \mu_N \subset \mathbb{F}_{q^m}^{\times}\}.$$

さらに，$|\mathbb{F}_{q^d}^{\times}| = q^d - 1$ より

$$d = \min\{m \in \mathbb{N} \mid \mu_N \subset \mathbb{F}_{q^m}^{\times}\} \Leftrightarrow d = \min\{m \in \mathbb{N} \mid q^m \equiv 1 \pmod{N}\}.$$

次の **MOV アルゴリズム (MOV algorithm)** (アルゴリズム 4.24) は 1990 年に Menezes, 岡本, Vanstone により提案されたアルゴリズムであり，ヴェイユ e_m ペアリング (定義 4.22) を用いて ECDLP を有限体上の乗法群における DLP に還元できることを表している．埋め込み次数と深い関係を持っており，注意 4.25 にて紹介する．また，MOV アルゴリズムの名前の由来は 3 名の提案者の頭文字である．

アルゴリズム 4.24 (MOV アルゴリズム, [Sil, XI.6, Proposition 6.1, page 387])**.** $E/\mathbb{F}_q$ を楕円曲線，$P, Q \in E(\mathbb{F}_q)$ を素数位数 N の点，d を N の $\mathbb{F}_q$ への埋め込み次数，

$gcd(q-1, N) = 1$, $T \in E[N](\overline{\mathbb{F}}_q)$ (P と T で $E[N]$ を生成する) とする．このとき，$E(\mathbb{F}_q)$ における ECDLP

$$Q = [m]P$$

を，$\mathbb{F}_{q^d}^{\times}$ における DLP

$$\mathrm{e}_N(Q, T) = \mathrm{e}_N(P, T)^m$$

に還元する多項式時間アルゴリズムが存在する．

注意 4.25. アルゴリズム 4.24 において，埋め込み次数 d が大きいほど解くことが難しい $\mathbb{F}_{q^d}^{\times}$ における DLP に還元でき，埋め込み次数 d が十分小さいならば容易な DLP に還元できる．

ここから，$E/\mathbb{F}_p$ (p は素数, $p \geq 3$) において $|E(\mathbb{F}_p)| = p$ となる楕円曲線に対する ECDLP を解くために用いることができるアルゴリズム 4.38 を紹介するための準備を行う．

定義 4.26. R を環，べき級数 $F(X, Y) \in R[[X, Y]]$ とする．

以下の (1)〜(5) を満たす $F(X, Y)$ を (**1 変数の可換な**)$\boldsymbol{R}$ **上で定められた形式群** $\boldsymbol{\mathcal{F}}$ (**formal group**) という．また，R 上で定められていることを $\boldsymbol{\mathcal{F}/R}$ と表す．

1. $F(X, Y) = X + Y +$ (次数 2 以上の項)
2. $F(X, F(Y, Z)) = F(F(X, Y), Z)$　(結合法則)
3. $F(X, Y) = F(Y, X)$　(交換法則)
4. $\exists!\ i(T) \in R[[T]]$ s.t. $i(T) = 0$, $F(T, i(T)) = 0$　(逆元)
5. $F(X, 0) = X$, $F(0, Y) = Y$

このとき，$F(X, Y)$ のことを $\mathcal{F}$ **の形式群法則** (**formal group law**) という．形式群法則として $F(X, Y)$ をもつ形式群は $\boldsymbol{(\mathcal{F}, F)}$ と表す．

定義 4.27. ($\mathcal{F}$,F), ($\mathcal{G}$,G) を R 上で定められた形式群とする．$\mathcal{F}$ から $\mathcal{G}$ への $\boldsymbol{R}$ **上で定められた準同型** (**homomorphism**) とは,

$$f(F(X, Y)) = G(f(X), f(Y))$$

を満たす定数項を持たないべき級数 $f \in R[[T]]$ のことである．形式群 $\mathcal{F}, \mathcal{G}$ が $\boldsymbol{R}$ **上で同型** (**isomorphic**) であるとは，R 上で定められた準同型 $f : \mathcal{F} \longrightarrow \mathcal{G}$, $g : \mathcal{G} \longrightarrow \mathcal{F}$ にお

いて

$$f(g(T)) = g(f(T)) = T$$

となるものが存在することをいう.

例 4.28 ([Sil, XI, Example 2.2.1, page 121])**. 形式的加法群** (**formal additive group**) を

$$F(X, Y) = X + Y$$

により定め，$\widehat{\mathbb{G}}_a$ と表す.

例 4.29 ([Sil, XI, Example 2.2.2, page 121])**. 形式的乗法群** (**formal multiplicative group**) を

$$F(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1$$

により定め，$\widehat{\mathbb{G}}_m$ と表す.

例 4.30 ([Sil, XI, Example 2.2.3, page 121])**.** R を環，E を R の元を係数としてもつワイエルシュトラス形式により与えられた楕円曲線とする．このとき，E 上の演算 $\oplus$ により導かれるべき級数 $F(z_1, z_2)$ により定められる $\boldsymbol{E}$ **に関する形式群**を $\widehat{\boldsymbol{E}}$ と表す.

定義 4.31. R を完備局所環，$\mathcal{M}$ を R の極大イデアル，$k = R/\mathcal{M}$，$(\mathcal{F}, F)$ を R 上で定めれらた形式群とする.

$\boldsymbol{\mathcal{F}/R}$ **に対応する群**を $\boldsymbol{\mathcal{F}(\mathcal{M})}$ と表し，$\mathcal{M}$ は群の作用

$$\begin{aligned} x \oplus_{\mathcal{F}} y &= F(x, y) \quad (\text{加法}) \quad (x, y \in \mathcal{M}) \\ \ominus_{\mathcal{F}} x &= i(x) \quad (\text{逆元}) \quad (x \in \mathcal{M}) \end{aligned}$$

をもつ．同様に，$n \geq 1$ に対して $\boldsymbol{\mathcal{F}(\mathcal{M}^n)}$ を上記の群の作用をもつ $\mathcal{M}^n$ からなる $\mathcal{F}(\mathcal{M})$ の部分群として定める.

定義 4.32. R 上で定められた形式群 $(\mathcal{F}, F)$ の**不変微分** (**invariant differential**) を

$$\omega \circ F(T, S) = \omega(T)$$

を満たす微分形式

$$\omega(T) = P(T)\, dt \in R[[\, T \,]]\, dt$$

と定められる．

$$P\big(F(T,S)\big)F_X(T,S) = P(T)$$

を満たすとき，$\omega(T) = P(T)\,dt$ は不変微分である．

さらに $P(0) = 1$ のとき，不変微分は**正規化されている** (**normalized**) という．

定義 4.33. R をねじれのない環，$K = R \otimes Q$，$\mathcal{F}/R$ を形式群，

$$\omega(T) = (1 + c_1T + c_2T^2 + c_3T^3 + \cdots)\,dt$$

を $\mathcal{F}/R$ 上の正規化不変微分とする．

***$\mathcal{F}/R$* の形式対数** (**formal logarithm**) とは，

$$\text{べき級数 } \log_{\mathcal{F}}(T) = \int \omega(T) = T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \cdots \in K[[\,T\,]]$$

のことをいい，***$\mathcal{F}/R$* の形式指数** (**formal exponential**) とは，一意に定まるべき級数であり，

$$\log_{\mathcal{F}} \circ \exp_{\mathcal{F}}(T) = \exp_{\mathcal{F}} \circ \log_{\mathcal{F}}(T) = T$$

を満たす $\exp_{\mathcal{F}}(T) \in K[[\,T\,]]$ のことである．

定理 4.34 ([Sil, Ⅳ.6, Theorem 6.4, page 132])**.** K を $\mathrm{char}(K) = 0$ であり正規化された離散付値 ν ($\nu(K^\times) = \mathbb{Z}$) に関して完備な体とする．$R$ を K の付値環，$\mathcal{M}$ を R の極大イデアル，p を $\nu(p) > 0$ をみたす素数とする．

1. 形式対数は，準同型

   $$\log_{\mathcal{F}} : \mathcal{F}(\mathcal{M}) \longrightarrow K$$

   を誘導し，K 上での群法則は加法となる．
2. $r > \frac{\nu(p)}{p-1}$ を整数とする．このとき，形式対数は同型

   $$\log_{\mathcal{F}} : \mathcal{F}(\mathcal{M}^r) \xrightarrow{\simeq} \widehat{\mathbb{G}}_a(\mathcal{M}^r)$$

   を誘導する．

定義 4.35. K を離散付値 ν に関して完備な局所体，$R = \{x \in K \mid \nu(x) \geq 0\}$ を K の整数環，E/K を

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

により与えられる楕円曲線とする．

E を与えるワイエルシュトラス形式において，$a_1, a_2, a_3, a_4, a_6 \in R$ であるものの中で $\nu(\Delta_E)$ が最小値となるものを**極小 (ワイエルシュトラス) 形式** (**minimal** (**Weierstrass**) **form**) という．さらに $\nu(\Delta_E)$ の最小値は $\boldsymbol{\nu}$ **における** $\boldsymbol{E}$ **の最小判別式の付値**という．

定義 4.36. K を離散付値 ν に関して完備な局所体，R を K の整数環，π を R に対する一意化変数, $\tilde{}$を π を法とした還元，E/K を極小ワイエルシュトラス形式により与えられた楕円曲線，$P \in E(K)$ とする．

次の $E(K)$ の部分集合を定める：

$$E_1(K) = \{P \in E(K) \mid \widetilde{P} = \widetilde{O}\}.$$

命題 4.37 ([Sil, VII.2, Proposition 2.2, page 191])**.** K を離散付値 ν に関して完備な局所体，R を K の整数環，E/K を極小ワイエルシュトラス形式により与えられた楕円曲線,

$$w(z) = z^3(1 + A_1 z + A_2 z^2 + \cdots) \in R[[z]]$$

とする．このとき，写像

$$\begin{array}{ccc} \widehat{E}(\mathcal{M}) & \longrightarrow & E_1(K) \\ \cup & & \cup \\ z & \longmapsto & \left(\dfrac{z}{w(z)}, -\dfrac{1}{w(z)}\right) \end{array}$$

から群の同型 $\widehat{E}(\mathcal{M}) \simeq E_1(K)$ を得る．

アルゴリズム 4.38 (Semaev, Satoh, Araki, Smart, [Sil, XI.6, Proposition 6.5, page 389])**.** p を素数，$p \geq 3$，$E/\mathbb{F}_p$ を楕円曲線，$|E(\mathbb{F}_p)| = p$ とする．このとき，以下のアルゴリズムにより $E(\mathbb{F}_p)$ に対する ECDLP を $\mathbb{F}_p$ に対する DLP に還元できる．

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. 楕円曲線 $E'/\mathbb{Q}_p$ を，p を法とした還元が $E/\mathbb{F}_p$ 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．

注意 4.39 ([Sil, XI.6, Remark 6.6, page 389])**.** アルゴリズム 4.38 において，$E(\mathbb{F}_p)$ での点を $E(\mathbb{Q}_p)$ の点に持ち上げているが，実際には p^2 を法とした点の持ち上げと $\widehat{\mathbb{G}}_a(p\mathbb{Z}_p)/\widehat{\mathbb{G}}_a(p^2\mathbb{Z}_p) \simeq p\mathbb{Z}_p/p^2\mathbb{Z}_p$ での形式対数の計算のみが必要となることが証明から分かる．証明については [Sil, XI.6, Proposition 6.5, Proof, page 389] を参照.

注意 4.40. 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 [Sil, XI.6, Example 6.7, page 390].

ここから，PARI/GP により計算を行いながらアルゴリズム 4.38 を実行してみる．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.

例 4.41 ([Sil, XI.6, Example 6.7, page 390])**.** 楕円曲線 $E : y^2 = x^3 + 19x + 112$，点 $P = (106, 72) \in E(\mathbb{F}_{127}), Q = (12, 121) \in E(\mathbb{F}_{127})$ とする．アルゴリズム 4.38 を用いて $Q = [m]P$ を満たす $m \in \mathbb{Z}$ を求める.

まず，PARI/GP に楕円曲線や点を定義する．方程式 $E : y^2 = x^3 + 19x + 112$ を E から $\mathbb{Z}/127^2\mathbb{Z}$ へ持ち上げたものは E_2 とする．しかし，注意 4.40 より PARI/GP での計算のために E_2 は $\mathbb{Q}$ 上で定義する.

```
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
```

アルゴリズム 4.38 を用いるため $|E(\mathbb{F}_{127})| = 127$ であることを確認する.

```
gp > E.no \\ |E(F_127)| を計算
127
```

次に，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

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

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

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

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．

```
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．

```
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．

次に，$[127]P_2, [127]Q_2$ 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).
```

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．また，この変数変換は $E2$ 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 $CM127P_2, CM127Q_2$ と定義し，それらを 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 > CM127P2=[-M127P2[1]/M127P2[2],-1/M127P2[2]]; \\ CM127P2 を定義
gp > M127P2E2=Mod(CM127P2,127^2) \\ M127P2E2 ≡ CM127P2 (mod 127^2)
[Mod(12319, 16129), Mod(0, 16129)]
gp > CM127Q2=[-M127Q2[1]/M127Q2[2],-1/M127Q2[2]]; \\ CM127Q2 を定義
gp > M127Q2E2=Mod(CM127Q2,127^2) \\ M127Q2E2 ≡ CM127Q2 (mod 127^2)
[Mod(2159, 16129), Mod(0, 16129)]
```

$y^2 = x^3 + Ax + B$ 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,

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

を用いれば十分である．このことから

$$\log_E(M127P_2E_2) \equiv 12319 \equiv 127 \cdot 97 \pmod{127^2}$$
$$\log_E(M127Q_2E_2) \equiv 2159 \equiv 127 \cdot 17 \pmod{127^2}$$

となるため，アルゴリズム 4.38 (4) での a, b は

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

となる．これらより，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．最後に $[46]P = Q$ であることを以下のように確認する．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
```

以上より $[46]P = Q$ が確かめられた.

例 4.42 ([Sil, XI, Exercise 11.15, page 407])**.** 楕円曲線 $E : y^2 = x^3 + 86x + 98$，点 $P = (56, 85) \in E(\mathbb{F}_{137}), Q = (54, 86) \in E(\mathbb{F}_{137})$ とする．アルゴリズム 4.38 を用いて $Q = [m]P$ を満たす $m \in \mathbb{Z}$ を求める.

例 4.41 と同様の手順により解くことができる.

```
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
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
gp > M137P2=ellmul(E2,P2,137); \\ M137P_2 を定義
gp > M137Q2=ellmul(E2,Q2,137); \\ M137Q_2 を定義
gp > CM137P2=[-M137P2[1]/M137P2[2],-1/M137P2[2]]; \\ CM137P_2 を定義
gp > M137P2E2=Mod(CM137P2,137^2) \\ M137P_2E_2 ≡ CM137P_2 (mod 137^2)
[Mod(15207, 18769), Mod(0, 18769)]
gp > CM137Q2=[-M137Q2[1]/M137Q2[2],-1/M137Q2[2]]; \\ CM137Q_2 を定義
gp > M137Q2E2=Mod(CM137Q2,137^2) \\ M137Q_2E_2 ≡ CM137Q_2 (mod 137^2)
[Mod(8905, 18769), Mod(0, 18769)]
```

例 4.41 と同様に

$$\log_E(z) \approx z$$

を用いれば十分なので,

$$\log_E(M137P_2E_2) \equiv 15207 \equiv 137 \cdot 111 \pmod{137^2}$$
$$\log_E(M137Q_2E_2) \equiv 8905 \equiv 137 \cdot 65 \pmod{137^2}$$

となるため，アルゴリズム 4.38 (4) での a, b は

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

となる．これらより，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．最後に $[66]P = Q$ であることを以下のように確認する．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
```

以上より $[66]P = Q$ が確かめられた．

今後の課題の 1 つとして，アルゴリズム 4.14 やアルゴリズム 4.16 など様々なアルゴリズムを計算機にて用いられるようになり，[安田 2] のように既存のアルゴリズムに工夫を施せるようになることが挙げられる．量子コンピューターに対抗することを目的とした耐量子暗号が盛んに研究されているように，日々多くの暗号とそれを解読するアルゴリズムが生み出されている．日常生活においても数学の存在を意識できるようになることを目指しながら，最新の暗号やアルゴリズムの用途，構造を理解し，研究を展開していきたい．

参考文献

[コブリッツ] N. コブリッツ（櫻井 幸一 訳）, 数論アルゴリズムと楕円暗号理論入門, シュプリンガー・フェアラーク東京, 1997, 369 ページ.

[シルヴァーマン] J. H. シルヴァーマン（鈴木 治郎 訳）, 楕円曲線の数論 基礎概念からアルゴリズムまで, 共立出版, 2023, 614 ページ.

[ノイキルヒ] J. ノイキルヒ（足立 恒雄 監修, 梅垣 敦紀 訳）, 代数的整数論, 丸善出版, 2012, 600 ページ.

[藤崎] 藤崎 源二郎, 体とガロア理論, 岩波基礎数学選書, 岩波書店, 1991, 502 ページ.

[安田 1] 安田 雅哉, 楕円曲線暗号の攻撃とその安全性 (*Computer Algebra : Design of Algorithms, Implementations and Applications*), 京都大学数理解析研究所講究録 1814, Computer Algebra : Design of Algorithms, Implementations and Applications, 2012, 74–84, `http://hdl.handle.net/2433/194549`.

[安田 2] 安田 雅哉, 有限体上の楕円曲線に関連した計算問題, 第 25 回整数論サマースクール報告集 「楕円曲線とモジュラー形式の計算」, 2017, 43–68, `https://toyama.repo.nii.ac.jp/records/16635`.

[横山 1] 横山 俊一, 楕円曲線の計算にみる数論システムの進展状況 (数式処理 : その研究と目指すもの), 京都大学数理解析研究所講究録 1785, 数式処理 : その研究と目指すもの, 2012, 57–66, `http://hdl.handle.net/2433/172739`.

[横山 2] 横山 俊一, 楕円曲線の計算法入門：実践編, 第 25 回整数論サマースクール報告集 「楕円曲線とモジュラー形式の計算」, 2017, 81–103, `https://toyama.repo.nii.ac.jp/records/16635`.

[Ono] Takashi Ono, *An Introduction to Algebraic Number Theory*, The University Series in Mathematics, Plenum Press, 1990, xii+223 pp.

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

[User's Guide] The PARI Group, *User's Guide to PARI/GP* (*version 2.15.4*), Univ. Bordeaux, 2023, `https://pari.math.u-bordeaux.fr/pub/pari/manuals/2.15.4/users.pdf`.

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

[ST] Joseph H. Silverman, John T. Tate, *Rational Points on Elliptic Curves*, Second Edition, Undergraduate Texts in Mathematics, Springer-Verlag, 2015, xxii+332 pp.