ふわっと理解する!楕円曲線暗号のイメージ

climax

2025 年 6 月 10 日

目次

1 前書き

私たちの生活は、スマートフォンでのメッセージ交換やオンラインショッピングなど、デジタル通信技術によって支えられています。これらの通信の安全性を担保しているのが「暗号」です。その中でも、特に強力かつ効率的で、現代のセキュリティの根幹をなす技術の一つが**楕円曲線暗号 (Elliptic Curve Cryptography, ECC)** です。

この技術は、大学で学ぶような高度な数学に基づいているため、一見すると非常に難解に思えるかもしれません。しかし、その根底にあるアイデアは、高校数学で学ぶ概念を知っていれば仕組みをざっくりと理解することができます。またその過程で関連する定理なども紹介できたらと思います。

この文章の目的は、楕円曲線暗号がどのような数学的な「部品」から組み立てられているのかを、ステップバイステップで解き明かし、その全体像のイメージを掴むことです。最終的には、「なぜ楕円曲線暗号は安全で、効率的なのか」という問いに、自分なりの答えを見つけることを目指します。

この暗号の核心は、**「有限体上の楕円曲線における離散対数問題の困難性」**に基づいています。楕円曲線という特殊な図形の上で行う計算は、ある方向には簡単ですが、その逆方向の計算は極めて困難です。この「一方向性」が、現代のデジタル社会の安全を守る「鍵」となっているのです。またこの文を通じて、有限体上での楕円曲線暗号がなぜ有限体上での離散対数を使用する暗号よりも有効なのかを理解していただけたらと思います。

一応大学数学の予備知識なしで読めるようにはしてありますが、ラグランジェの定理を知らないと結構しんどい内容になっているかもしれません申し訳ないです。

またこのレポートは N・コブリッツ著、櫻井幸一訳の 「数論アルゴリズムと楕円曲線暗号入門」 の内容に自身の補足を加えたものを主軸としています。

2 対称性を記述する言語：群

暗号理論の舞台となる「数の世界」の構造を理解するために、まず**群（ぐん）**という代数構造を導入します。これは、図形の対称性や、数の世界の規則性を記述するための、非常に強力な数学の言葉です。

2.1 群の定義と基本的な概念

定義 2.1 (群 (Group))**.** 集合 G と、その上の二項演算 $\circ$ の組 $(G, \circ)$ が**群**であるとは、以下の 3 つの公理を満たすことをいいます。

1. **結合法則 (Associativity)**: G の任意の元 a, b, c に対して、$(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ。
2. **単位元の存在 (Identity element)**: G のすべての元 a に対して、$e \circ a = a \circ e = a$ を満たす特別な元 $e \in G$ が存在する。この e を**単位元**と呼ぶ。
3. **逆元の存在 (Inverse element)**: G の各元 a に対して、$a \circ a^{-1} = a^{-1} \circ a = e$ を満たす元 $a^{-1} \in G$ が必ず存在する。この a^{-1} を a の**逆元**と呼ぶ。

さらに、任意の元 a, b について交換法則 $a \circ b = b \circ a$ が成り立つとき、この群を**アーベル群** (または可換群) と呼びます。

定義 2.2 (部分群 (Subgroup))**.** 群 $(G, \circ)$ の空でない部分集合 H が、G と同じ演算 $\circ$ によってそれ自身も群となるとき、H を G の**部分群**であるといいます。

例 2.3. 整数のなす群 $(\mathbb{Z}, +)$ を考えます。このとき、偶数全体の集合 $2\mathbb{Z} = \{\dots, -2, 0, 2, 4, \dots\}$ は、足し算について閉じており、単位元 '0' を含み、各元の逆元（偶数の逆元は偶数）も含むため、$(\mathbb{Z}, +)$ の部分群です。

定義 2.4 (生成元と巡回群)**.** ある群 G の中に特別な元 g があり、その g のべき乗 $(g^1, g^2, g^3, \dots)$ を計算していくだけで、G の全ての元を過不足なく生み出せるとき、g を**生成元**と呼びます。生成元を持つ群のことを**巡回群**と呼びます。

例 2.5. 法 5 の乗法群 $\mathbb{F}_5^* = (\{1, 2, 3, 4\}, \times)$ を考えます。元 '2' のべき乗を計算すると、$2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$, $2^4 \equiv 1 \pmod 5$ となり、集合 $\{1, 2, 3, 4\}$ のすべての元を生成できました。したがって、'2' はこの群の生成元であり、この群は巡回群です。

定理 2.6 (巡回群の部分群)**.** 巡回群の部分群は、また巡回群である。

Proof. 巡回群を $G = \langle g \rangle$、H を G の部分群とする。G の位数を n とする $(0 \leq k \leq n-1)$。H の元の中で最も指数が小さい元を g^m とする。H の任意の元は g^k で表せ、$k = qm + r$ $(0 \leq r < m)$ と表せる。群を成すので g^m の逆元も存在し、左から作用させて、$g^{k-qm} = g^r$。g^k, g^{qm} は H の元であるため g^r も H の元であるはずだが、$r > 0$ なら m が最小であることに矛盾。よって $r = 0$。したがって H の任意の元は g^m のべき乗で表せる。よって H は巡回群である。 □

定義 2.7 (位数 (Order))**.** 群には 2 種類の「位数」があります。

1. **群の位数**: その群に含まれる元の総数。$|G|$ と書きます。
2. **元の位数**: ある元 a を何回演算すると、初めて単位元 e に戻るか、という最小の正の整数。

例 2.8. 再び $\mathbb{F}_5^* = (\{1,2,3,4\}, \times)$ を考えます。

- **群の位数**: 元が 4 つなので、群の位数は $|\mathbb{F}_5^*| = 4$ です。
- **元の位数**: 元 '4' の位数を考えます。$4^1 = 4$, $4^2 = 16 \equiv 1 \pmod 5$ なので、'4' の位数は 2 です。一方、生成元 '2' の位数は 4 です。

定義 2.9 (準同型写像・同型写像)**.** 2 つの群 $(G, \circ)$ と $(H, *)$ があるとき、写像 $f : G \to H$ が任意の $a, b \in G$ に対して $f(a \circ b) = f(a) * f(b)$ を満たすとき、**準同型写像**といいます。さらに、準同型写像 f が全単射であるとき、**同型写像**といい、G と H は**同型**であるといいます。同型な群は、元の名前が違うだけで構造は全く同じものです。

例 2.10. n 次正則行列（逆行列を持つ行列）全体のなす群を一般線形群といい、$GL_n(\mathbb{R})$ と書きます。この群から、ゼロでない実数全体のなす乗法群 $(\mathbb{R}^\times, \times)$ への写像 $f(A) = \det(A)$ を考えます。

行列式の性質 $\det(AB) = \det(A)\det(B)$ より、この写像は

$$f(AB) = f(A)f(B)$$

を満たすため、群準同型写像です。この写像の核（単位元 1 に写される元の集合）は、行列式が 1 であるような行列の集合となり、これは特殊線形群 $SL_n(\mathbb{R})$ と呼ばれる重要な部分群をなします。[6]

2.2 ラグランジュの定理

定理 2.11 (ラグランジュの定理)**.** 有限群 G において、その任意の部分群の位数は、必ず G 全体の位数を割り切る。

系 2.12 (系)**.** 有限群の任意の元の位数は、必ず群全体の位数を割り切る。

3 整数論の基礎事項

3.1 合同式とオイラー関数

定義 3.1 (合同式)**.** 整数 a, b と正の整数 m があるとき、$a - b$ が m で割り切れることを、$a \equiv b \pmod m$ と書き、「a と b は m を法として合同である」といいます。

定義 3.2 (オイラーの ϕ 関数)**.** 正の整数 n に対して、1 から n までの整数のうち、n と互いに素なものの個数を $\phi(n)$ と書きます。

系 3.3 (ϕ 関数の乗法性)**.** オイラーの ϕ 関数は乗法的関数である。すなわち、互いに素な正の整数 m, n に対して、

$$\phi(mn) = \phi(m)\phi(n)$$

が成り立つ。

Proof. 0 から $mn-1$ の間で mn と共通の因数を持たない整数の数を数える。その範囲内の各整数 j について、j_1 は j を法 m のもとで最小の非負剰余であるとし（すなわち、$0 \leq j_1 < m$ かつ $j \equiv j_1 \pmod{m}$)、j_2 は j を法 n のもとで最小の非負剰余であるとする（すなわち、$0 \leq j_2 < n$ かつ $j \equiv j_2 \pmod{n}$)。

中国剰余定理より、ペア (j_1, j_2) に対して、0 から $mn-1$ までの間に $j \equiv j_1 \pmod{m}$ かつ $j \equiv j_2 \pmod{n}$ となる j がただ一つだけ存在する。これは、j とペア (j_1, j_2) の間に一対一対応があることを意味する。

ここで、j が mn と共通の因数を持たないことは、「j が m と共通の因数を持たない」ことと、「j が n と共通の因数を持たない」ことが同時に成り立つことと同値である。さらに、「j が m と共通の因数を持たない」ことは「j_1 が m と共通の因数を持たない」（すなわち $\gcd(j_1, m) = 1$）ことと同値であり、「j が n と共通の因数を持たない」ことは「j_2 が n と共通の因数を持たない」（すなわち $\gcd(j_2, n) = 1$）ことと同値である。

したがって、数えるべき j の個数（$\phi(mn)$）は、$\gcd(j_1, m) = 1$ を満たす j_1 と、$\gcd(j_2, n) = 1$ を満たす j_2 のペアの個数と等しい。条件を満たす j_1 の個数は $\phi(m)$ であり、j_2 の個数は $\phi(n)$ である。よって、ペアの総数は $\phi(m)\phi(n)$ となる。これで $\phi(mn) = \phi(m)\phi(n)$ が証明された。 □

例 3.4 (ϕ 関数の計算)**.** $\phi(36)$ の値を計算する。$36 = 2^2 \cdot 3^2$ であり、2^2 と 3^2 は互いに素なので、ϕ 関数の乗法性を用いることができる。

$$\phi(36) = \phi(2^2)\phi(3^2)$$

素数のべき乗 p^k に対する公式 $\phi(p^k) = p^k - p^{k-1}$ を用いると、

$$\phi(2^2) = 2^2 - 2^1 = 4 - 2 = 2$$
$$\phi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$$

となる。よって、$\phi(36) = 2 \cdot 6 = 12$ である。

定理 3.5 (オイラーの定理)**.** n を正の整数とし、a を n と互いに素な整数とすると、$a^{\phi(n)} \equiv 1 \pmod{n}$ が成り立つ。

Proof. まず、法が素数のべき乗 $m = p^\alpha$ の場合に数学的帰納法で示す。

$m = p$ のとき、これはフェルマーの小定理 $a^{p-1} \equiv 1 \pmod{p}$ に他ならず、成立する。

$a^{\phi(p^{\alpha-1})} \equiv 1 \pmod{p^{\alpha-1}}$ の成立を仮定する。このとき、$a^{\phi(p^{\alpha-1})} = 1 + bp^{\alpha-1}$ となる整数 b が存在する。この両辺を p 乗すると、

$$(a^{\phi(p^{\alpha-1})})^p = (1 + bp^{\alpha-1})^p$$

右辺を二項展開すると、$p \geq 2$ より

$$(1 + bp^{\alpha-1})^p = 1 + p(bp^{\alpha-1}) + \binom{p}{2}(bp^{\alpha-1})^2 + \cdots \equiv 1 \pmod{p^\alpha}$$

となる。一方、左辺の指数は $\phi(p^{\alpha-1}) \cdot p = (p^{\alpha-1} - p^{\alpha-2})p = p^\alpha - p^{\alpha-1} = \phi(p^\alpha)$ である。したがって、$a^{\phi(p^\alpha)} \equiv 1 \pmod{p^\alpha}$ が示された。

次に、一般の $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ の場合を考える。a と n が互いに素なので、a は各 $p_i^{\alpha_i}$ とも互いに素である。上記より、$a^{\phi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$ が成り立つ。ϕ 関数の乗法性より、$\phi(n) = \phi(p_1^{\alpha_1}) \dots \phi(p_k^{\alpha_k})$ であり、$\phi(p_i^{\alpha_i})$ は $\phi(n)$ の因数である。よって、$a^{\phi(n)} = (a^{\phi(p_i^{\alpha_i})})^k \equiv 1^k \equiv 1 \pmod{p_i^{\alpha_i}}$ が、すべての i について成立する。これは、$a^{\phi(n)} - 1$ が、互いに素なすべての $p_i^{\alpha_i}$ で割り切れることを意味する。したがって、中国剰余定理の考え方から、$a^{\phi(n)} - 1$ はその積である n でも割り切れ、$a^{\phi(n)} \equiv 1 \pmod{n}$ が結論付けられる。 □

系 3.6 (フェルマーの小定理)**.** p を素数とし、a を p で割り切れない整数とすると、$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ。

3.2 拡張ユークリッドの互除法と乗法逆元

合同式の世界で「割り算」を実現するためには、乗法逆元を求める必要があります。

命題 3.7. a が法 m に関して乗法逆元を持つための必要十分条件は、a と m が互いに素であること、すなわち $\gcd(a, m) = 1$ である。

この乗法逆元は、**拡張ユークリッドの互除法**を用いて効率的に計算することができます。

アルゴリズムの概要

ユークリッドの互除法は、2 つの整数 a, m の最大公約数 $\gcd(a, m)$ を求めるアルゴリズムです。これは、a を m で割った余りを r としたとき、$\gcd(a, m) = \gcd(m, r)$ となる性質を繰り返し利用します。

拡張ユークリッドの互除法は、この計算過程を逆順にたどることで、$\gcd(a, m)$ だけでなく、ベズーの等式として知られる

$$ax + my = \gcd(a, m)$$

を満たす整数 x, y の組を見つけ出します。

$\gcd(a, m) = 1$ の場合、この式は $ax + my = 1$ となります。これを法 m で考えると、my の項は 0 になるため、$ax \equiv 1 \pmod{m}$ となります。このとき得られる x が、まさしく a の法 m における乗法逆元です。

ユークリッドの互除法は、2 回の操作でビット長が半分程度になるため、操作回数は $O(\log N)$、全体の計算量は $O(\log^2 N)$ となります。

3.3 繰り返し二乗法

$x^n \pmod{m}$ のような、巨大なべき乗の剰余を高速に計算するためのアルゴリズムです。単純に x を $n-1$ 回掛けるのではなく、指数 n を 2 進数的に分解することで計算を効率化します。この方法は、以下の関係を再帰的に利用します。

$$x^n = \begin{cases} (x^{n/2})^2 & (n \text{ が偶数のとき}) \\ x \cdot (x^{(n-1)/2})^2 & (n \text{ が奇数のとき}) \end{cases}$$

n は最大で $\log_2 n$ ビットで表現できるので、乗算の回数は $O(\log n)$ 回となります。1 回あたりの乗算コストは $O((\log m)^2)$ なので、全体の計算量は $O((\log n)(\log^2 m))$ となります。

3.4 中国剰余定理

これは、複数の異なる「法」に関する連立合同式を解くための強力な道具です。

定理 3.8 (中国剰余定理)**.** $n_1, n_2, \ldots, n_k$ をどの 2 つも互いに素な正の整数とする。このとき、任意の整数 $a_1, a_2, \ldots, a_k$ に対して、連立合同式

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

を満たす解 x が、$0 \le x < N = n_1 n_2 \ldots n_k$ の範囲にただ一つだけ存在する。

Proof. $N = n_1 n_2 \dots n_k$ とおく。各 $i = 1, \dots, k$ に対して、$N_i = N/n_i$ とすると、n_i と N_i は互いに素である。したがって、拡張ユークリッドの互除法により、$N_i y_i \equiv 1 \pmod{n_i}$ となる乗法逆元 y_i が存在する。このとき、

$$x = a_1 N_1 y_1 + a_2 N_2 y_2 + \cdots + a_k N_k y_k$$

とすると、この x が求める解の一つである。$j \neq i$ のとき、N_j は n_i の倍数なので、$N_j \equiv 0 \pmod{n_i}$ である。したがって、

$$x \equiv a_i N_i y_i \pmod{n_i}$$

となり、$N_i y_i \equiv 1 \pmod{n_i}$ であったから、$x \equiv a_i \pmod{n_i}$ が成り立つ。解の一意性は、もし x と x' という 2 つの解が存在すると仮定すると、$x - x'$ は全ての n_i で割り切れるため、N の倍数となり、$0 \leq x, x' < N$ の範囲では $x = x'$ となることから示される。 □

例 3.9. 連立合同式

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

を解く。$N = 3 \cdot 5 \cdot 7 = 105$。$N_1 = 35, N_2 = 21, N_3 = 15$。それぞれの逆元は、$35y_1 \equiv 2y_1 \equiv 1 \pmod{3} \Rightarrow y_1 = 2$、$21y_2 \equiv y_2 \equiv 1 \pmod{5} \Rightarrow y_2 = 1$、$15y_3 \equiv y_3 \equiv 1 \pmod{7} \Rightarrow y_3 = 1$。よって、$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233$。$233 \equiv 23 \pmod{105}$。よって解は $x = 23$ である。

命題 3.10. 任意の正の整数 n について、そのすべての正の約数 d に対する $\phi(d)$ の和は n に等しい。

$$\sum_{d|n} \phi(d) = n$$

Proof. まず、関数 $f(n) = \sum_{d|n} \phi(d)$ が乗法的であることを示す。m, n を互いに素な正の整数とする。mn の任意の約数 d は、m の約数 d_1 と n の約数 d_2 を用いて、

$d = d_1 d_2$ と一意に表すことができる。このとき、d_1 と d_2 も互いに素である。

$$\begin{aligned} f(mn) &= \sum_{d|mn} \phi(d) \\ &= \sum_{d_1|m} \sum_{d_2|n} \phi(d_1 d_2) && \text{（約数のペアに分解）} \\ &= \sum_{d_1|m} \sum_{d_2|n} \phi(d_1)\phi(d_2) && \text{（}\phi\text{ の乗法性より）} \\ &= \left(\sum_{d_1|m} \phi(d_1) \right) \left(\sum_{d_2|n} \phi(d_2) \right) && \text{（和の分離）} \\ &= f(m) f(n) \end{aligned}$$

よって、$f(n)$ は乗法的関数である。

次に、n が素数のべき乗 p^α の場合について $f(p^\alpha)$ を計算する。

$$\begin{aligned} f(p^\alpha) &= \sum_{i=0}^{\alpha} \phi(p^i) \\ &= \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^\alpha) \\ &= 1 + (p-1) + (p^2 - p) + \cdots + (p^\alpha - p^{\alpha-1}) \end{aligned}$$

これは伸縮級数（テレスコープ和）となり、途中の項がすべて打ち消し合うため、$f(p^\alpha) = p^\alpha$ となる。

任意の正の整数 n は $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ と素因数分解できる。$f(n)$ は乗法的であるため、

$$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots f(p_k^{\alpha_k}) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = n$$

となり、題意は示された。 □

4 暗号の舞台：有限体

この章では、暗号理論の計算の舞台となる有限体について、その基本的な定義と性質を解説する。

4.1 基礎的な定義と性質

定義 4.1 (体 (Field))**.** 集合 F に加法 ‘+‘ と乗法 ‘・‘ の 2 つの演算が定義されており、加法と乗算において結合則と可換則、そして分配則が成立する。また、加法単位元 (0) と乗法単位元 (1)、加法逆元が存在し、0 を除くすべての元に対して乗法逆元

が存在するような代数構造を**体**という。代表的な例としては、有理数からなる体 $\mathbb{Q}$、実数からなる体 $\mathbb{R}$、複素数からなる体 $\mathbb{C}$、そして素数 p を法とする整数からなる体 $\mathbb{Z}/p\mathbb{Z}$ がある。

定義 4.2 (ベクトル空間 (Vector Space))**.** ベクトル空間は、これまで実数上で扱ってきたのと同様に任意の体 F 上で定義できる。すべてのベクトル空間は基底をもち、基底の元の数を次元と呼ぶ。

定義 4.3 (体の拡大 (Field Extension))**.** 体 F がより大きな体 K に含まれているとき、K は F の**拡大体**であるという。このとき、K は自動的に F 上のベクトル空間となる。そのベクトル空間が有限次元ならば、それを有限次拡大という。有限拡大の次数とは、そのベクトル空間としての次元のことである。拡大体を得る 1 つの共通した方法は、F にある要素を加えることである。体 K が要素 α と体 F の要素によって構成されるすべての有理式からなるとき、$K = F(\alpha)$ と書く。

4.2 本章で用いる記号と用語

この章を読み進めるにあたり、いくつか重要な記号と用語の意味を先に確認しておきましょう。

$\mathbb{F}_p$ p を素数とするとき、$\mathbb{F}_p$ は p 個の元からなる**有限体**を表します。具体的には、集合 $\{0, 1, \ldots, p-1\}$ に対して、足し算と掛け算をすべて「p で割った余り」で考える世界（$\mathbb{Z}/p\mathbb{Z}$ と同じもの）のことです。

モニック多項式 (Monic Polynomial) 多項式の中で、最も次数の高い項の係数が 1 であるもののことです。例えば、$x^2 + 2x + 3$ はモニックですが、$2x^2 + x + 1$ はモニックではありません。多項式の因数分解を考える際に、代表として扱いやすい形です。

既約多項式 (Irreducible Polynomial) 整数の世界における**素数**の、多項式版だと考えてください。素数が「1 と自分自身以外では割り切れない整数」であるように、既約多項式は「定数でない 2 つの多項式の積で表すことができない多項式」を指します。例えば、$\mathbb{F}_2$ 上の多項式 $x^2 + x + 1$ は、$\mathbb{F}_2$ の元を係数とする 1 次の多項式（x や $x + 1$）の積では表せないため、既約多項式です。

定義 4.4 (多項式環 (Polynomial Ring))**.** 体 F 上で定義される多項式環とは、F の要素を係数としてもつ X のべき乗の有限和からなり、実数上の多項式のときと同様に加算と乗算を行うことができる。これを $F[X]$ と表記する。多項式環は唯一の因数分解をもつ。すなわち、すべてのモニック多項式は（因数の並べ順を除けば）モニック

既約多項式の積としてただ 1 通りにかける。

定義 4.5 (代数的元と最小多項式)**.** F を含む拡大体 K の元 α は、もしそれが F の元を係数としてもつ多項式の根となるならば、F 上の**代数的元**であるという。このような場合、α を根とする $F[X]$ のモニック既約多項式が唯一つ存在する。このモニック既約多項式が次数 d をもつとすると、$F(\alpha)$ の任意の元（すなわち α のべき乗と F の元をふくむ任意の有理式）は、実際にはベキ乗 $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ の線形結合で表される。従って、これらの α のべき乗は F 上の $F(\alpha)$ の基底を形成し、α を添加して得られた拡大の次数は α のモニック既約多項式の次数と同じになる。

定義 4.6 (標数 (Characteristic))**.** もし乗法の単位元 1 を F において何回足し合わせても 0 にならないとき、F が標数 0 をもつという。このような場合、F は有理数体と同形な体を含む。そうでないならば、$1 + 1 + \cdots + 1$ (p 回足す) が 0 になるような素数 p が存在し、p は体 F の標数という。このとき、F は素体 $\mathbb{Z}/p\mathbb{Z}$ と同形な体を含む。

4.3 有限体の構造

定義 4.7 (有限体)**.** 有限体とは、元の個数が有限である体のことである。

定理 4.8 (有限体の位数)**.** 任意の有限体 $\mathbb{F}_q$ の元の数（位数）q は、ある素数 p と正の整数 f を用いて $q = p^f$ の形に表せる。

証明の概略. 有限体の標数は素数 p となる。このとき有限体は、素体 $\mathbb{F}_p$ を部分体として含み、$\mathbb{F}_p$ 上のベクトル空間とみなせる。その次元を f とすると、元の総数は p^f 個となるためである。 □

定理 4.9. 全ての有限体 $\mathbb{F}_q$ の乗法群 $\mathbb{F}_q^*$ （0 を除いた元の集まり）は、位数 $q-1$ の**巡回群**である。

この定理は、有限体には必ず「生成元」が存在することを保証しており、離散対数暗号の基礎となります。

4.4 有限体の詳細な構造

ここでは、有限体が持つ重要な性質について、いくつかの命題と例を通して詳しく見ていきます。

命題 4.10 (元の位数)**.** 有限体 $\mathbb{F}_q$ の乗法群 $\mathbb{F}_q^*$ の任意の元の位数は、$q-1$ の約数で

ある。

Proof. 乗法群 $\mathbb{F}_q^*$ の位数（元の総数）は $q-1$ である。ある元 $a \in \mathbb{F}_q^*$ と、その位数を k とする。元 a が生成する巡回部分群 $\{a, a^2, \ldots, a^k = 1\}$ の位数は k である。ラグランジュの定理によれば、部分群の位数は群全体の位数を割り切る。したがって、k は $q-1$ の約数でなければならない。 □

例 4.11 (有限体上の多項式演算)**.** $\mathbb{F}_5$ 上の多項式環 $\mathbb{F}_5[X]$ での計算を考える。係数の計算はすべて法 5 で行う。例えば、2 つの多項式 $(x+4)$ と $(2x+3)$ の和を計算すると、

$$(x+4)+(2x+3) = 3x+7$$

となる。ここで、係数 7 は法 5 で 2 と合同であるため、

$$3x+7 \equiv 3x+2 \pmod 5$$

となる。

命題 4.12 (有限体の元の特徴付け)**.** $q = p^f$ とする。$\mathbb{F}_q$ の元は、多項式 $x^q - x = 0$ の解全体と一致する。逆に、任意の素数のべき乗 q に対して、多項式 $x^q - x$ の $\mathbb{F}_p$ 上の分解体は、ちょうど q 個の元からなる体である。

Proof. まず、$\mathbb{F}_q$ の元が $x^q = x$ を満たすことを示す。$a = 0$ の場合は自明である。$a \in \mathbb{F}_q^*$ の場合、乗法群 $\mathbb{F}_q^*$ の位数は $q-1$ なので、ラグランジュの定理（またはその系）より $a^{q-1} = 1$ が成り立つ。この両辺に a を掛けると $a^q = a$ を得る。

次に、多項式 $f(x) = x^q - x$ の根が q 個の元からなる体を成すことを示す。$f(x)$ の導関数は $f'(x) = qx^{q-1} - 1$ である。標数 p の体では $q = p^f$ は 0 となるため、$f'(x) = -1$ となる。導関数が 0 にならないため $f(x)$ は重根を持たず、したがって q 個の異なる根を持つ。これらの根が体を成すか確認する。a, b を $f(x)$ の根、すなわち $a^q = a, b^q = b$ を満たす元とする。

- 乗法について: $(ab)^q = a^q b^q = ab$。よって積 ab も根である。
- 加法について: 後述の補題より、標数 p の体では $(a+b)^p = a^p + b^p$ が成り立つ。これを繰り返し適用すると、$(a+b)^{p^f} = a^{p^f} + b^{p^f}$、すなわち $(a+b)^q = a^q + b^q = a+b$ となる。よって和 $a+b$ も根である。

逆元や単位元も同様に根の集合に含まれるため、この集合は体を成す。これは $x^q - x$ の根をすべて含む最小の体、すなわち分解体である。 □

補題 4.13 (フロベニウス自己準同型)**.** 標数 p の体において、等式 $(a+b)^p = a^p + b^p$ が成り立つ。

Proof. 二項定理より $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k}b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k}b^k$ である。ここで、二項係数 $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ を考える。p は素数であり、$1 \leq k \leq p-1$ の範囲では分母の $k!$ も $(p-k)!$ も p で割り切れない。したがって、分子の p は約分されずに残るため、$\binom{p}{k}$ は p の倍数となる。標数 p の体では p の倍数は 0 とみなせるため、中間の項はすべて消え、$(a+b)^p = a^p + b^p$ が得られる。 □

命題 4.14 (フロベニウス写像)**.** $\sigma(a) = a^p$ で定義される写像 $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ は、$\mathbb{F}_q$ の自己同型写像である。この写像で不変な元（$a^p = a$ を満たす元）は、素体 $\mathbb{F}_p$ の元に他ならない。また、σ^f は恒等写像である（ただし $q = p^f$）。

Proof. 前述の補題より $\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$ であり、また明らかに $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$ なので、σ は準同型写像である。有限体上の単射な準同型写像は全射でもあるため、これは自己同型写像となる。元 a が不変である条件は $a^p - a = 0$ だが、これはまさに素体 $\mathbb{F}_p$ の元が満たすべき方程式である。また、$q = p^f$ なので、任意の元 $a \in \mathbb{F}_q$ に対して $a^q = a$ が成り立つ。写像の言葉で言えば、$a^{p^f} = \sigma^f(a) = a$ となり、σ^f は恒等写像である。 □

例 4.15 ($\mathbb{F}_9$ の構成)**.** $\mathbb{F}_{3^2} = \mathbb{F}_9$ を構成する。まず、$\mathbb{F}_3$ 上で既約なモニック 2 次多項式が必要である。例えば x^2+1, x^2-x-1, x^2+x-1 などがそれに当たる。ここで $f(x) = x^2 - x - 1$ を選び、その根の一つを α とすると、$\mathbb{F}_9$ の元は $a + b\alpha$ $(a, b \in \mathbb{F}_3)$ の形で表せる。α は $f(x) = 0$ の根なので $\alpha^2 = \alpha + 1$ である。この α のべき乗を計算していくと、$\alpha^1 = \alpha$, $\alpha^2 = \alpha + 1$, $\alpha^3 = \alpha^2 + \alpha = (\alpha+1) + \alpha = 2\alpha + 1$, $\alpha^4 = 2\alpha^2 + \alpha = 2(\alpha+1) + \alpha = 3\alpha + 2 \equiv 2 \pmod 3$, ..., $\alpha^8 = 1$ となり、α は位数 8、すなわち乗法群 $\mathbb{F}_9^*$ の生成元であることがわかる。このような生成元を与える既約多項式は**原始多項式**と呼ばれる。

命題 4.16 (部分体の構造)**.** $q = p^f$ とする。$\mathbb{F}_q$ の部分体は、f の正の約数 d に対して $\mathbb{F}_{p^d}$ の形のものだけが、それぞれちょうど一つずつ存在する。

Proof. まず、d が f の約数であるとき、$\mathbb{F}_{p^d}$ が $\mathbb{F}_{p^f}$ の部分体であることを示す。$f = dk$ となる整数 k が存在する。$\mathbb{F}_{p^d}$ の任意の元 α は $\alpha^{p^d} = \alpha$ を満たす。この式の両辺に p^d 乗を繰り返し適用すると、

$$\alpha^{p^f} = \alpha^{(p^d)^k} = (\dots((\alpha^{p^d})^{p^d})\dots)^{p^d} = \alpha$$

となり、α は $x^{p^f} - x = 0$ の根でもある。したがって $\alpha \in \mathbb{F}_{p^f}$ であり、$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^f}$ である。

逆に、$\mathbb{F}_{p^f}$ の任意の部分体を K とする。K はある素体 $\mathbb{F}_p$ 上のベクトル空間なので、その元の数は p^d の形をしているはずである。K は $\mathbb{F}_{p^f}$ の部分集合なので、ラグ

ランジュの定理より、加法群としての位数 p^d は p^f の約数でなければならず、乗法群としての位数 $p^d - 1$ は $p^f - 1$ の約数でなければならない。これらの条件から、d は f の約数であることが示される。 □

命題 4.17 ($x^q - x$ の因数分解)**.** $q = p^f$ とする。多項式 $x^q - x$ は、$\mathbb{F}_p[X]$ において、次数が f の約数 d となるような全てのモニック既約多項式の積として（重複なく）因数分解される。

Proof. $g(x)$ を次数が d であるような $\mathbb{F}_p$ 上のモニック既約多項式とし、d は f の約数であるとする。$g(x) = 0$ の根 α を添加して得られる体は $\mathbb{F}_{p^d}$ である。前命題より $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^f}$ であるため、α は $\mathbb{F}_{p^f}$ の元でもある。したがって α は $x^{p^f} - x = 0$ の根であり、$g(x)$ は $x^{p^f} - x$ を割り切る。

逆に、$x^{p^f} - x$ を割り切る任意のモニック既約多項式を $h(x)$ とし、その次数を d とする。$h(x) = 0$ の根 β は $x^{p^f} - x = 0$ を満たすので $\beta \in \mathbb{F}_{p^f}$ である。β が生成する体 $\mathbb{F}_{p^d}$ は $\mathbb{F}_{p^f}$ の部分体となるため、前命題より d は f の約数でなければならない。

$x^{p^f} - x$ は重根を持たないため、上記の条件を満たすすべてのモニック既約多項式の積に因数分解される。 □

例 4.18 (多項式の最大公約数)**.** $\mathbb{F}_2[X]$ において、$f(x) = x^4 + x^2 + 1$, $g(x) = x^3 + 1$ の最大公約数 (GCD) をユークリッドの互除法を用いて計算する。

$$f(x) = (x) \cdot g(x) + (x^2 + x + 1)$$
$$g(x) = (x + 1) \cdot (x^2 + x + 1) + 0$$

最後のゼロでない余りが GCD であるから、$\mathrm{GCD}(f, g) = x^2 + x + 1$ となる。

5 離散対数問題に基づく公開鍵暗号

5.1 公開鍵暗号とは

これまでに紹介した暗号技術は、暗号化と復号に同じ鍵を使う「共通鍵暗号方式」でした。この方式は、事前に安全な方法で鍵を共有しなければならないという「鍵配送問題」を抱えています。

この問題を解決したのが**公開鍵暗号方式**です。この方式の画期的な点は、暗号化と復号に**異なる 2 つの鍵**、すなわち**公開鍵**と**秘密鍵**のペアを用いる点にあります。

- **公開鍵 (Public Key)**: その名の通り、誰にでも公開して良い鍵です。

- **秘密鍵 (Private Key)**: 自分だけが秘密に保管し、誰にも教えてはいけない鍵です。

この仕組みはよく**南京錠と鍵**のセットに例えられます。公開鍵は「開いた南京錠」のようなもので、誰にでも配ることができます。メッセージを送りたい人は、その南京錠を使って箱を施錠（暗号化）します。しかし、施錠された箱を開ける（復号する）ことができるのは、その南京錠に対応する唯一の「鍵」（秘密鍵）を持っているあなただけです。

この公開鍵暗号の技術は、主に以下の 3 つの目的で利用されます。

5.1.1 1. 鍵交換 (Key Exchange)

目的: 通信内容を盗聴される可能性のあるインターネット上で、安全に**共通鍵を共有する**こと。公開鍵暗号の計算は比較的速度が遅いため、通信のすべてを公開鍵暗号で行うのは非効率です。そこで、安全性を確保したい最初の段階でだけ公開鍵暗号を使い、高速な共通鍵暗号で使うための「共通鍵」を安全に生成・共有します。このレポートで後述する**Diffie-Hellman 鍵交換**が代表例です。

5.1.2 2. 電子署名 (Digital Signature)

目的: メッセージの**認証**（誰が作成したか）と**完全性**（改ざんされていないか）を保証すること。暗号化とは逆に、送信者が自身の**秘密鍵**で情報に「署名」します。受信者や第三者は、送信者の**公開鍵**を使って、その署名が本物であるかを検証できます。秘密鍵を持つ本人しか署名を作成できないため、なりすましや改ざんを防ぐことができます。このレポートで後述する**デジタル署名基準 (DSS)**が代表例です。

5.1.3 3. (狭義の) 公開鍵暗号

目的: メッセージの**秘匿**（内容を秘密にする）こと。送信者は、受信者の**公開鍵**を使ってメッセージを暗号化します。暗号化されたメッセージは、対応する**秘密鍵**を持つ受信者本人にしか復号できません。これにより、第三者による盗聴を防ぎます。このレポートで後述する**ElGamal 暗号**が代表例です。

これらの仕組みを実現する数学的な困難性の一つが、次に紹介する「離散対数問題」です。

5.2 離散対数問題 (DLP)

離散対数とは、連続的な場合から有限群を区別し特徴づけるものです。

定義 5.1 (離散対数問題)**.** 有限巡回群 G とその生成元 b, 元 $y \in G$ が与えられたとき、$b^x = y$ となる整数 x を求める問題を、離散対数問題と呼びます。

この離散対数を求める難しさを利用した暗号やプロトコルが存在します。

5.3 Diffie-Hellman 鍵交換システム

$G = \mathbb{F}_p^*$ とし、g と p は公開する。(なお、g が生成元だと望ましい) A さん、B さんがそれぞれ $a, b \in \mathbb{Z}$ を決める (まだ公開しない)。その後、g^a, g^b をそれぞれ計算して互いに送受信する。その後互いに受け取った数を、最初に決めた数のべき乗する。その際に $g^{ab} \pmod p$ が両者で共有できるということである。通信経路上に流れる情報は g, p, g^a, g^b のみであることに注意したい。

注意 5.2 (Diffie-Hellman 予想)**.** g, p, g^a, g^b だけしか分からない場合、g^{ab} を求めるのは困難という予想。現状では多項式時間で解くアルゴリズムは発見されていない。Diffie-Hellman 鍵交換で使用されているアルゴリズムの計算困難性は、離散対数問題の困難性と比較して同等かそれ以下である。しかしまだ未解決問題である。

例 5.3. $p = 53, g = 2, a = 29, b = 19$ の場合

- $2^{29} \equiv 21 \pmod{53}$
- $2^{19} \equiv 12 \pmod{53}$
- $21^{19} \equiv 45 \pmod{53}$
- $12^{29} \equiv 45 \pmod{53}$

しかしこの場合だと 52 通りのブルートフォース攻撃をしかけることで簡単に解読できる。

5.4 Massey-Omura 暗号系

全ユーザーが同意した $\mathbb{F}_q$ を固定し公開しているとする。各ユーザーは $\gcd(e, q-1) = 1$ を満たす乱数 e を生成し、拡張ユークリッドの互除法を用いて $d = e^{-1} \pmod{q-1}$ を計算することができる。ユーザー A, B の乱数を e_A, d_A, e_B, d_B とし、メッセージを $P \in \mathbb{F}_q$ とする。しかしこれは B が偽物の場合でも B は問題なく受け取ることができることに注意。

1. A は $C_1 = P^{e_A}$ を計算し、B に送信する。
2. B は $C_2 = (C_1)^{e_B} = P^{e_A e_B}$ を計算し、A に返信する。

3. A は $C_3 = (C_2)^{d_A} = P^{e_A e_B d_A} = P^{e_B}$ を計算し、B に送信する。
4. B は $C_4 = (C_3)^{d_B} = P^{e_B d_B} = P$ を計算し、平文を復元する。

注意 5.4 (補足)**.**

- $\gcd(e, q-1) = 1$ なのはなぜか。　ラグランジュの定理より、G の元の位数は $|G|$ の約数である。0 を除いた乗法群 $\mathbb{F}_q^*$ の位数は $q-1$ であり、元 g の指数は法 $q-1$ で考えることができる。e と d で暗号化・復号を行うには、$ed \equiv 1 \pmod{q-1}$ である必要があり、そのためには e が法 $q-1$ での乗法逆元を持つこと、すなわち $\gcd(e, q-1) = 1$ が必要となる。
- また B が偽物だった場合に備え署名が必要である。また離散対数問題を解くことが出来る場合、P と P^{e_A} から e_A を求めることができるため、それ以降のメッセージは全て盗み見える。

5.5 ElGamal 暗号

大きな素数 p を決め、$g \in \mathbb{F}_p$ を定める（g は生成元)。正の整数 a を $\{1, \ldots, p-2\}$ からランダムに決定し、$y = g^a \pmod{p}$ とおく。公開鍵は (p, g, y)、秘密鍵は a である。メッセージ P を他のユーザーに送る際は、ランダムな乱数 k を生成し、$(g^k \pmod{p}, Py^k \pmod{p})$ の組を送る。受信側は a を知っているので組の 1 つ目を a 乗して 2 つ目を割ることで P が出せる。

注意 5.5 (安全性)**.** DH 問題には素数 p、生成元 g、$g^a \pmod{p}, g^b \pmod{p}$ が与えられているが、ElGamal 暗号が解けると仮定する。$u = g^b$ は乱数とみなせ $(1 \leq k \leq p-1)$、$v = m \cdot y^k$ より $m = v \cdot (u^a)^{-1}$ である。B 君（攻撃者）が平文 m を計算できるなら、$v \cdot m^{-1} = u^a = (g^b)^a = g^{ab}$ がわかり、DH 問題が解けてしまう。

5.6 デジタル署名基準 (Digital Signature Standard)

デジタル署名基準（DSS）は、コンピューターの世界の書類の正当性を示すものです。デジタル署名を行うには公開鍵暗号が必要であり、手順としては以下の 3 つのステップがあります。

5.6.1 Step 1: 鍵生成

1. 160 ビット程度の素数 q を生成する。
2. $p \equiv 1 \pmod{q}$ を満たす 512 ビット程度の素数 p を生成する。
3. 位数が q であるような $\mathbb{F}_p^*$ の唯一の巡回部分群が存在するので、その生成元 g

を選ぶ。このとき、$g = h^{(p-1)/q} \pmod{p}$ とし、$g \neq 1$ となるような h を選ぶ。

4. 秘密鍵となる整数 x を $0 < x < q$ の範囲でランダムに選ぶ。
5. 公開鍵 $y = g^x \pmod{p}$ を計算する。

この結果、公開パラメータは (p, q, g)、個人の公開鍵は y、秘密鍵は x となります。

5.6.2 Step 2: 署名生成

1. メッセージ m にハッシュ関数を適用し、$H(m)$ を得る。
2. 乱数 k を $0 < k < q$ の範囲でランダムに選択する。
3. $r = (g^k \pmod{p}) \pmod{q}$ を計算する。$(r \neq 0)$
4. $s = k^{-1}(H(m) + xr) \pmod{q}$ を満たす s を求める。

この (r, s) のペアが署名となります。署名はメッセージの内容とその際に生成される乱数により変化します。

5.6.3 Step 3: 署名検証

検証には公開されている変数 (p, q, g, y) と署名 (r, s) を使います。

1. $w = s^{-1} \pmod{q}$ を計算する。
2. $u_1 = H(m) \cdot w \pmod{q}$ を計算する。
3. $u_2 = r \cdot w \pmod{q}$ を計算する。
4. $v = (g^{u_1} y^{u_2} \pmod{p}) \pmod{q}$ を計算する。

$v = r$ と一致するかで検証できます。

5.6.4 公開鍵暗号との関係と認証局

一般的な公開鍵暗号は受信者側のみがメッセージを見れることを目的としていますが、デジタル署名は、送られてきたメッセージが本人のものかを公開鍵で検証することに注意されたい。つまり、暗号化で用いる「公開 $\rightarrow$ 秘密」という鍵の使い方の順番が、署名では「秘密 $\rightarrow$ 公開」の逆になっています。

また、この公開鍵が本人のものか（攻撃者の偽装でないか）を保証するのが**認証局 (CA)**です。公開鍵のデジタル証明書を CA のデジタル署名付きで発行します。x は g に対する y の離散対数なのでシステムの安全性は、$\mathbb{F}_p^*$ の離散対数問題に依存すると考えられています。

5.7 Pohlig-Hellman のアルゴリズム

まず、$q-1$ の素因数はすべて小さいものと仮定する。この場合、$q-1$ はスムーズ (smooth) であると呼ぶこともある。この仮定のもとでは、$\mathbb{F}_q^*$ における b の離散対数を効率よく計算するアルゴリズムが存在する。簡単のため b は $\mathbb{F}_q^*$ の生成元とする。ここでは Silver, Pohlig, Hellman らによって提案されたアルゴリズムを紹介する。

まず $q-1$ の各素因数 p_i に対し、p_i 乗根 $r_{p_i,j} = b^{j(q-1)/p_i}$ $(j = 0, 1, \ldots, p_i - 1)$ を計算（繰返し二乗法）し、テーブルを作成する。このテーブルを用いて $y \in \mathbb{F}_q^*$ の離散対数を計算する準備が整った。今回の目的は y を固定した際に、$b^x = y$ となるような $x \pmod{q-1}$ を見つけることである。$q-1 = \prod p_i^{a_i}$ より、$x \pmod{p_i^{a_i}}$ を見つけられれば十分である。なぜならば、中国剰余定理より x は一意に定まるからだ。よって $q-1$ の素因数を固定し、$x \pmod{p^a}$ を求める方法を示す。

$0 \leq x < p^a$ として、$x = \sum_{k=0}^{a-1} x_k p^k$ と表した場合を考える。

1. x_0 **を求める:** $\quad y^{(q-1)/p} = (b^x)^{(q-1)/p} = b^{x(q-1)/p} = b^{(\sum_{k=0}^{a-1} x_k p^k)(q-1)/p}$

   指数のうち $\sum_{k=1}^{a-1} x_k p^k$ の部分は p の倍数なので、b にかかる指数を法 $q-1$ で考えると、この部分は $b^{m(q-1)} = 1$ となり消える。よって、

   $$y^{(q-1)/p} \equiv b^{x_0(q-1)/p} \pmod{p}$$

   ここで $r_{p,x_0} = b^{x_0(q-1)/p}$ であったから、あらかじめ計算したテーブルと比較して $y^{(q-1)/p} = r_{p,x_0}$ となる x_0 を見つける。

2. x_1 **を求める:**

   $y_1 = y \cdot b^{-x_0}$ を計算する。すると $y_1 = b^{x-x_0} = b^{(\sum_{k=1}^{a-1} x_k p^k)}$ となる。 両辺を $(q-1)/p^2$ 乗すると、

   $$y_1^{(q-1)/p^2} = b^{(x-x_0)(q-1)/p^2} = b^{(\sum_{k=1}^{a-1} x_k p^{k-1})(q-1)/p}$$

   先ほどと同様に $k \geq 2$ の項は消えるため、

   $$y_1^{(q-1)/p^2} \equiv b^{x_1(q-1)/p} \pmod{p}$$

   これにより $y_1^{(q-1)/p^2} = r_{p,x_1}$ となる x_1 を見つける。

3. x_i **を求める（帰納的ステップ）:**

   $x_0, \ldots, x_{i-1}$ が求まったとし、$y_i = y/b^{\sum_{k=0}^{i-1} x_k p^k} = b^{\sum_{k=i}^{a-1} x_k p^k}$ を計算する。両辺を $(q-1)/p^{i+1}$ 乗すると、

   $$y_i^{(q-1)/p^{i+1}} \equiv b^{x_i(q-1)/p} \pmod{p}$$

となる。従って、$y_i^{(q-1)/p^{i+1}} = r_{p,x_i}$ となる x_i を見つける。

この結果、$x \equiv \sum x_k p^k \pmod{p^a}$ を得ることができる。$q-1$ の各素因数べきに対しこれを実行すると、最終的に中国剰余定理を用いて全体の x を求める。このアルゴリズムは、$q-1$ の素因数がすべて小さい場合に有効である。

5.8 指標計算アルゴリズム (Index-Calculus Algorithm)

5.8.1 イデアルと剰余環について

指標計算法で用いられる体の構造を理解するために、イデアルと剰余環の概念を補足する。

定義 5.6 (イデアル (Ideal))**.** R を環、$I \subset R$ とする。I について、

1. I は加法について部分群である。
2. $\forall r \in R, \forall x \in I$ に対し、積 $rx \in I$ が成立する時、左イデアルという。
3. $\forall r \in R, \forall x \in I$ に対し、積 $xr \in I$ が成立する時、右イデアルという。

上記が全て成立する時、両側イデアルという。R が可換環の時、単にイデアルと言われる。

定義 5.7 (剰余環 (Quotient Ring))**.** R を環、$I \subset R$ を両側イデアルとする。このとき、剰余類の集合

$$R/I = \{x + I \mid x \in R\}$$

は和と積の演算

$$(x+I)+(y+I) = (x+y)+I$$

$$(x+I)(y+I) = xy+I$$

によって環になる。これを**剰余環** (factor ring) という。

例 5.8. $R = \mathbb{Z}$ を整数の環、$I = m\mathbb{Z}$ を m の倍数の集合とする。$m\mathbb{Z}$ はイデアルである。よって $\mathbb{Z}/m\mathbb{Z}$ は剰余環であり、その元は $\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ である。

例 5.9. $\mathbb{R}[x]$ を実数係数 1 変数多項式環とすると、$\langle x \rangle$ は x で生成されるイデアルである。$\mathbb{R}[x]/\langle x \rangle$ は剰余環であり、$\mathbb{R}[x]/\langle x \rangle \cong \mathbb{R}$ である。

Pohlig-Hellman 法は、$q-1$ が小さな素因数を持つ場合に有効でした。ここでは、$q-1$ が大きな素因数を持つ場合にも適用できる、より強力な準指数時間アルゴリズム

である**指標計算アルゴリズム**を紹介します。このアルゴリズムは、素体 $\mathbb{F}_p$ だけでなく、拡大体 $\mathbb{F}_q = \mathbb{F}_{p^n}$ での離散対数問題にも有効です。

5.8.2 アルゴリズムの舞台設定

まず、$q = p^n$ はかなり大きな数で、b は $\mathbb{F}_q^*$ の生成元であるとします。このアルゴリズムは、体 $\mathbb{F}_q$ を、多項式環 $\mathbb{F}_p[X]$ を用いて $\mathbb{F}_q \cong \mathbb{F}_p[X]/\langle f(X)\rangle$ と表現できることを利用します。ここで $f(X)$ は $\mathbb{F}_p$ 上の n 次の既約多項式です。

この集合 $\mathbb{F}_p[X]/\langle f(X)\rangle$ とは一体何でしょうか？これは、「係数が $\mathbb{F}_p$ の元である多項式を、$f(X)$ で割った余りの世界」と考えることができます。整数の世界で ‘mod 12‘ を考えると、どんな整数も 0 から 11 までの余りで表現されるのと似ています。同様に、この世界ではどんな多項式も $f(X)$ で割った余り、すなわち次数が $n-1$ 以下の多項式として一意に表すことができます。この集合の元は $p^n = q$ 個あり、体をなします。

アルゴリズムの基本戦略

このアルゴリズムのアイデアは、整数における素因数分解のアナロジーを多項式の世界で実行することです。整数の世界で「$1365 = 3 \cdot 5 \cdot 7 \cdot 13$」のように素因数分解できるように、多項式の世界でも「$x^4 + 1 = (x^2 + x + 1)(x^2 - x + 1)$」のように**既約多項式**の積に分解できます。

指標計算アルゴリズムは、この多項式の「素因数分解」を利用します。まず、比較的小さな「素数」（低次の既約多項式）をたくさん集めた集合を用意します。これを**因子基底 (Factor Base)** と呼びます。そして、離散対数を求めたい元と因子基底との関係式を多数集め、連立一次方程式を解くことで問題を解決します。

因子基底とは

因子基底 B は、アルゴリズムの効率を左右する非常に重要な要素です。

- **集合の定義**: 因子基底 B は、ある次数 m を定め、次数が m 以下の $\mathbb{F}_p$ 上のモニックな既約多項式全体の集合として定義されます。
- **次数 m の選び方**: m の値はトレードオフの関係にあります。
  - m が小さすぎると、因子基底の要素数が少なくなり、ランダムに選んだ多項式が都合よく基底の元の積に分解できる確率が非常に低くなります。
  - m が大きすぎると、因子基底の要素数が膨大になり、解くべき連立一次方程式のサイズが大きくなりすぎて計算が困難になります。

  そのため、アルゴリズム全体の計算量が最小になるように、最適な m を選択する必要があります。

5.8.3 アルゴリズムの手順

このアルゴリズムは“予備計算”と“個別計算”の 2 段階からなります。

1. **予備計算段階**: 因子基底 B に含まれるすべての多項式の離散対数を計算し、データベース化する。
   (a) 小さな次数 m 以下の既約多項式からなる集合（**因子基底 B**）を選ぶ。
   (b) 乱数 t を選び、$c(X) \equiv b(X)^t \pmod{f(X)}$ を計算する。
   (c) $c(X)$ が因子基底 B の元の積に**因数分解**できるか試す。

$$c(X) = c_0 \prod_{a_i \in B} a_i(X)^{\alpha_i}$$

   (d) 分解できたら、両辺の対数をとり、法 $q-1$ の合同式を得る。

$$t \equiv \mathrm{ind}(c_0) + \sum \alpha_i \mathrm{ind}(a_i(X)) \pmod{q-1}$$

   (e) 因子基底の数だけ独立な合同式が集まるまでこれを繰り返し、連立一次方程式を解いて各因子基底の離散対数 $\mathrm{ind}(a_i(X))$ のデータベースを作成する。
2. **個別計算段階**: 予備計算で作ったデータベースを利用して、任意の元の離散対数を計算する。
   (a) 対数を求めたい元 $y(X)$ に対し、乱数 s を選び、$y_s(X) \equiv y(X)b(X)^s \pmod{f(X)}$ を計算する。
   (b) $y_s(X)$ が因子基底 B の元の積に**因数分解**できるか試す。（成功するまで s を変えて繰り返す）

$$y_s(X) = y_0 \prod_{a_i \in B} a_i(X)^{\beta_i}$$

   (c) 分解できたら、両辺の対数をとる。

$$\mathrm{ind}(y_s(X)) = \mathrm{ind}(y(X)) + s \equiv \mathrm{ind}(y_0) + \sum \beta_i \mathrm{ind}(a_i(X)) \pmod{q-1}$$

   (d) この式の右辺は、定数の対数とデータベースの値なので全て既知である。したがって、移項するだけで未知の $\mathrm{ind}(y(X))$ を計算できる。

指標計算アルゴリズムは準指数時間で動作するため、有限体上の離散対数問題の安全性を評価する上で非常に重要です。この攻撃法の存在が、より高い安全性を持つ楕円曲線暗号への移行を促す一因となりました。

（補足）今回は拡大体の場合のみ示したが、素体の場合でもほぼアルゴリズムの流れは変化しない。因子基底が次数が m 以下のモニック多項式の集合から、ある数以下の素数の集合に変化するだけである。

6 主役の登場：楕円曲線

6.1 楕円曲線の定義と群構造

定義 6.1 (楕円曲線)**.** あらゆる体への適用が可能な楕円の方程式の一般形 $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ が存在し、

- 標数 $K \neq 2,3$ の時、$y^2 = x^3 + Ax + B$ に変形される。
- 標数 $K = 2$ の時、$y^2 + cy = x^3 + ax + b$ または $y^2 + xy = x^3 + Ax^2 + b$ のような形に変形できる。

注意 6.2 (非特異性)**.** $F(x, y) = y^2 - x^3 - Ax - B$ とする。この時 2 つの偏微分 $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ のうち少なくとも 1 つがゼロでない曲線上の点を非特異 (Smooth) という。ここで、式の右辺の 3 次多項式が多重根を持たないことが、曲線上のすべての点が非特異であるということと同値である。

この曲線上の点の集合には、幾何学的な操作によって**加法**を定義することができ、無限遠点 O を単位元とする**アーベル群**をなします。

- **逆元**: 点 $P = (x, y)$ の逆元は $-P = (x, -y)$ です。
- **和** $P + Q$: P と Q を通る直線が曲線と交わる 3 点目の点を R' とすると、$P + Q = -R'$ となります。
- **2 倍算** $2P$: 点 P における接線が曲線と交わるもう 1 つの点を S' とすると、$2P = -S'$ となります。

6.2 点の加算公式

幾何学的な加法定義は、代数的な座標計算式に落とし込むことができます。$y^2 = x^3 + Ax + B$ の曲線上の 2 点 $P = (x_1, y_1), Q = (x_2, y_2)$ の和を $P + Q = (x_3, y_3)$ とすると、その座標は以下のように計算できます。

1. $P \neq Q$ **の場合** $(x_1 \neq x_2)$ 直線 PQ の傾きを $\alpha = \frac{y_2-y_1}{x_2-x_1}$ とすると、

$$x_3 = \alpha^2 - x_1 - x_2$$
$$y_3 = \alpha(x_1 - x_3) - y_1$$

2. $P = Q$ **の場合** $(y_1 \neq 0)$ 点 P での接線の傾きを $\alpha = \frac{3x_1^2+A}{2y_1}$ とすると、

$$x_3 = \alpha^2 - 2x_1$$
$$y_3 = \alpha(x_1 - x_3) - y_1$$

例 6.3. 曲線 $y^2 = x^3 + 1$ 上の点 $P = (2, 3)$ の位数を求めます。$A = 0, B = 1$ です。まず $2P$ を計算します。$P = Q$ の場合の公式を使い、$x_1 = 2, y_1 = 3$ なので、

$$\alpha = \frac{3(2^2) + 0}{2(3)} = \frac{12}{6} = 2$$

$$x_3 = 2^2 - 2(2) = 0$$

$$y_3 = 2(2 - 0) - 3 = 1$$

よって $2P = (0, 1)$ です。次に $4P = 2P + 2P$ を計算します。$x_1 = 0, y_1 = 1$ として、

$$\alpha = \frac{3(0^2) + 0}{2(1)} = 0$$

$$x_3 = 0^2 - 2(0) = 0$$

$$y_3 = 0(0 - 0) - 1 = -1$$

よって $4P = (0, -1)$ です。$2P = (0, 1)$ なので、$4P = -2P$ であり、$6P = O$ となります。$2P \neq O$ かつ $3P \neq O$ (計算すると $(-1, 0)$ ではない) なので、P の位数は 6 です。

6.3 有限体上の楕円曲線

暗号で実際に使われるのは、実数体ではなく有限体 $\mathbb{F}_q$ 上の楕円曲線です。$\mathbb{F}_q$ の元は有限個しかないため、その上の楕円曲線上の点の数も当然有限になります。この点の個数を N とすると、自明な上限として $N \leq 2q + 1$ (各 $x \in \mathbb{F}_q$ に対して y が 2 つ、および無限遠点) が考えられます。

より正確に点の個数を見積もるために、ルジャンドル記号（より一般には指標）$\chi(u)$ を用います。これは、u が $\mathbb{F}_q$ で平方根を持つかどうかに応じて $+1, -1, 0$ の値を取る関数です。ある x に対して方程式 $y^2 = u = x^3 + Ax + B$ の解の個数は $1 + \chi(u)$ となります。これを全ての x について合計し、無限遠点を加えることで、総数 N は

$$N = 1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(x^3 + Ax + B)) = q + 1 + \sum_{x \in \mathbb{F}_q} \chi(x^3 + Ax + B)$$

と表せます。

ハッセの定理とランダムウォーク

上記の式の誤差項 $\sum \chi(\dots)$ の大きさを評価することが重要になります。ここで、和の中の $\chi(x^3 + Ax + B)$ の値は $+1$ と -1 をほぼ同じ割合で取ることが期待されます。

この和を計算することは、コインを q 回投げて、表なら右に 1 歩、裏なら左に 1 歩進む**「ランダムウォーク」**に非常によく似ています。確率論によれば、q ステップのランダムウォークの後にいる地点の原点からの距離は、平均的には $\sqrt{q}$ のオーダーになります。

この直感的な類推を、数学的に厳密かつ強力に保証するのが次のハッセの定理です。

定理 6.4 (ハッセの定理)**.** $\mathbb{F}_q$ 上で定義された楕円曲線上の点の個数を N とすると、N は以下の不等式を満たす。

$$|N - (q+1)| \leq 2\sqrt{q}$$

この定理は、点の個数 N が期待値である $q+1$ から大きくはずれず、その誤差が $2\sqrt{q}$ の範囲に収まることを保証しています。これにより、暗号として利用するのに十分な大きさの群が得られることの理論的な裏付けとなります。

また、この点の集合がなすアーベル群は、必ずしも巡回群であるとは限りませんが、高々 2 つの巡回群の直積 $Z_{n_1} \times Z_{n_2}$ の形になることが知られています。

6.4 楕円曲線上のスカラー倍算

楕円曲線暗号の根幹をなす計算は、点 P と整数 k から $kP = P + P + \cdots + P$ を求める**スカラー倍算**です。これをナイーブに $k-1$ 回の足し算で行うのは非効率ですが、べき乗剰余を計算する「繰り返し二乗法」と同様の考え方で、高速に計算できます。

この方法は**ダブル・アンド・アッド法**と呼ばれます。例えば $100P$ を計算したい場合、100 を 2 進数で表現すると $100 = 64 + 32 + 4 = 2^6 + 2^5 + 2^2$ となります。

$$100P = (2^6 + 2^5 + 2^2)P = 2^6P + 2^5P + 2^2P$$

P から始めて、自分自身を繰り返し 2 倍（ダブル）していき $(2P, 4P, 8P, \dots, 64P)$、必要な項だけを足し合わせる（アッド）ことで計算できます。

命題 6.5. 与えられた点 $P \in E(\mathbb{F}_q)$ に対して、kP の座標は $O(\log k \cdot (\log q)^2)$ 程度のビット演算で計算可能である。

この計算は高速に行える一方、その逆問題、すなわち「点 P と点 $Q = kP$ が与えられたときに、整数 k を求める」問題は**楕円曲線離散対数問題 (ECDLP)** と呼ばれ、非常に困難です。この計算の非対称性が、楕円曲線暗号の安全性の根拠となっています。

7 楕円曲線暗号

この章の目的は、$\mathbb{F}_q$ で定義される楕円曲線 E のなす有限アーベル群を使って、これまでの章で見てきたような公開鍵暗号系を構成することです。

7.1 楕円曲線離散対数問題 (ECDLP)

有限体の乗法群における乗算が楕円曲線上の点の加算に対応し、べき乗がスカラー倍算に対応します。このアナロジーに基づき、楕円曲線上の離散対数問題を定義します。

定義 7.1 (ECDLP)**.** E を $\mathbb{F}_q$ 上の楕円曲線とし、B を E 上の点とする。与えられた点 $P \in E$ について、$kB = P$ となる整数 $k \in \mathbb{Z}$ が存在するとき、その k を求める問題を**楕円曲線離散対数問題 (Elliptic Curve Discrete Logarithm Problem)** と呼ぶ。

スカラー倍算 kP の計算はダブル・アンド・アッド法により効率的に行える一方、その逆問題である ECDLP を解くのは非常に困難であると信じられています。この計算の非対称性が、楕円曲線暗号の安全性の中核をなします。

注意 7.2 (楕円曲線暗号が優れている理由)**.** 有限体における離散対数問題には、指標計算アルゴリズムのような準指数時間で問題を解く強力な攻撃手法が存在します。しかし、一般的な楕円曲線に対しては、このような特殊な構造を利用した攻撃が（現在のところ）知られておらず、より小さい鍵長で同等の安全性を実現できます。これが、多くの現代的な暗号システムで楕円曲線が採用されている理由です。

7.2 平文の埋め込み

暗号化を行う前に、平文メッセージ m を楕円曲線 E 上の点 P_m として符号化（埋め込み）する必要があります。この方法は単純かつ系統的であることが望ましいです。

ここでは確率的な方法を一つ紹介します。平文 m から、ある決まった手順で $\mathbb{F}_q$ の元 x を生成します。そして、$x^3 + Ax + B$ の値を計算し、これが $\mathbb{F}_q$ の中で平方根 y

を持つかどうかを判定します。もし平方根が存在すれば、点 $P_m = (x, y)$ を得ます。もし存在しなければ、m から別の x を生成する、といった試行を繰り返します。$\mathbb{F}_q$ の元の約半分は平方剰余であるため、この方法は比較的少ない試行回数で成功することが期待できます。

7.3 楕円曲線暗号プロトコル

ECDLP の困難性を利用して、既存の公開鍵暗号と同様のプロトコルを構成できます。

7.3.1 Diffie-Hellman 鍵交換の類似

A さんと B さんが、第三者に知られることなく共通鍵を共有するためのプロトコルです。

1. 事前準備として、楕円曲線 E とその上の点 B を公開情報とする。
2. A さんは秘密の整数 a を選び、$P_A = aB$ を計算して B さんに送る。
3. B さんも秘密の整数 b を選び、$P_B = bB$ を計算して A さんに送る。
4. A さんは、受け取った P_B と自身の秘密 a を使って、$aP_B = a(bB) = (ab)B$ を計算する。
5. B さんは、受け取った P_A と自身の秘密 b を使って、$bP_A = b(aB) = (ab)B$ を計算する。

これにより、両者は共通の点 $K = (ab)B$ を共有できます。通信経路上で E, B, P_A, P_B が盗聴されても、ECDLP が困難なため、秘密の a, b や共通鍵 K を計算することは困難です。

7.3.2 Massey-Omura 暗号の類似

これはメッセージ（点）P_m を転送するための公開鍵暗号ですが、第三者だけでなく、通信相手にさえもメッセージの内容を一時的に読めなくする点が特徴です。事前の準備として、曲線上の点の総数 N が計算されていると仮定します。

1. 各ユーザーは、$\gcd(e, N) = 1$ を満たす秘密の整数 e を選び、その逆元 $d = e^{-1} \pmod N$ を計算しておく。A さんの鍵ペアを (e_A, d_A)、B さんの鍵ペアを (e_B, d_B) とする。
2. A さんは B さんにメッセージ P_m を送るため、まず $C_1 = e_A P_m$ を計算し、B さんに送る。
3. B さんは C_1 を受け取り、$C_2 = e_B C_1 = e_B e_A P_m$ を計算し、A さんに送り

返す。

4. A さんは C_2 を受け取り、自身の秘密鍵 d_A を使って $C_3 = d_A C_2 = d_A e_B e_A P_m = e_B P_m$ を計算し、B さんに送る。
5. B さんは C_3 を受け取り、自身の秘密鍵 d_B を使って $d_B C_3 = d_B e_B P_m = P_m$ を計算し、元のメッセージを復元する。

この方式では、途中の通信 C_1, C_2, C_3 からは ECDLP が困難な限り P_m を知ることはできません。

7.3.3 ElGamal 暗号の類似

メッセージを暗号化して送信するためのプロトコルです。

- **鍵生成**: 各ユーザーは秘密の整数 a を選び、公開鍵 $P_A = aB$ を計算して公開する。
- **暗号化**: 送信者は、受信者 A の公開鍵 P_A を使ってメッセージ（点）P_m を暗号化する。
  1. ランダムな整数 k を選ぶ。
  2. 2 つの点 $C_1 = kB$ と $C_2 = P_m + kP_A$ を計算する。
  3. 暗号文として、点のペア (C_1, C_2) を送信する。
- **復号**: 受信者 A は、自身の秘密鍵 a を使って暗号文 (C_1, C_2) を復号する。

$$P_m = C_2 - aC_1 = (P_m + kP_A) - a(kB) = P_m + k(aB) - a(kB) = P_m$$

これにより、秘密鍵 a を持つ A さんだけが元のメッセージ P_m を復元できます。

7.4 暗号パラメータ (E,B) の選び方

安全な楕円曲線暗号システムを構築するには、その土台となる楕円曲線 E とベースポイント B を慎重に選ぶ必要がある。その選び方には、大きく分けて 2 つのアプローチがある。

7.4.1 ランダムなパラメータの選択

一つは、パラメータをランダムに生成する方法である。まず、大きな有限体 $\mathbb{F}_q$ を固定する。次に、曲線の係数となる $a \in \mathbb{F}_q$ と、ベースポイントの x 座標となる $x_0 \in \mathbb{F}_q$ をランダムに選ぶ。そして、$y_0^2 = x_0^3 + ax_0 + b$ を満たすように係数 b を定める。これにより、点 $B = (x_0, y_0)$ が必ず乗るような楕円曲線 $E : y^2 = x^3 + ax + b$ が得られる。

ただし、こうして生成した曲線が暗号として安全であるかは別問題である。例えば、

Pohlig-Hellman 法のような攻撃を防ぐためには、曲線上の点の総数 N が大きな素因数を持つ（理想的には N 自身が素数であるか、素数に小さな整数をかけたものである）必要がある。そのため、生成した曲線の点の数 N を計算し（Schoof のアルゴリズムなどが知られる)、安全な位数を持つことが確認できるまでこのプロセスを繰り返す必要がある。

7.4.2 CM 法や還元を用いる方法

もう一つは、より高度な数学理論を用いる方法である。例えば、有理数体 $\mathbb{Q}$ のような「大きな」体の上で特定の性質を持つ楕円曲線を考え、それを大きな素数 p を法として「還元」することで、$\mathbb{F}_p$ 上の性質の良い楕円曲線を得るというアプローチがある。

7.4.3 標準化された曲線の利用

理論的には上記の方法で安全な曲線を生成できるが、現実のシステムでは、各々が独自に曲線を生成することは稀である。その理由は、安全なパラメータを生成するには高度な専門知識が必要であり、誤りが許されないためである。

そこで、実際には NIST（アメリカ国立標準技術研究所）や Certicom 社などが専門家によって検証し、安全であることが保証された**標準化された曲線（推奨曲線）**を用いるのが一般的である。これにより、異なるシステム間での相互運用性も確保される。

代表的な標準曲線には、以下のようなものがある。

- **NIST P-256**: Web の TLS/SSL 通信などで広く利用されている標準曲線。
- **secp256k1**: ビットコインやイーサリアムなどのブロックチェーン技術で採用されていることで有名な曲線。

これらの標準化された曲線とベースポイントを用いることで、開発者はパラメータ選択の複雑さを回避しつつ、安全な暗号システムを構築することができる。

8 未来の脅威への備え：耐量子計算機暗号

これまで解説してきた公開鍵暗号は、現在のコンピュータ（古典コンピュータ）では非常に長い時間をかけても解くことが困難な数学的問題を安全性の根拠としています。しかし、1994 年に数学者ピーター・ショアが発表した**ショアのアルゴリズム**により、この前提は将来的に覆される可能性が出てきました。

このアルゴリズムは、もし十分に大規模な**量子コンピュータ**が実現すれば、素因数分解問題や離散対数問題を効率的（多項式時間）に解けることを理論的に示しま

した。これは、現在広く使われている RSA 暗号や楕円曲線暗号 (ECC) が、原理的に破られてしまう未来を意味します。

この「量子の脅威」に対抗するため、世界中の暗号研究者が次世代の暗号技術の開発を進めています。それが**耐量子計算機暗号 (Post-Quantum Cryptography, PQC)** です。

8.1 耐量子計算機暗号とは

耐量子計算機暗号（PQC）とは、現在のコンピュータでも効率的に実行でき、かつ将来登場するであろう量子コンピュータを使っても（既知の量子アルゴリズムでは）効率的に解読することが困難であると信じられている暗号方式のことです [3]。

PQC は量子コンピュータ上で動作するのではなく、あくまで古典コンピュータ上で動作するアルゴリズムであり、その安全性が量子コンピュータによる攻撃にも耐えうるように設計されています。その安全性は、ショアのアルゴリズムでは効率的に解けないとされている、**格子暗号**や**符号理論に基づく暗号**といった、新しい数学的問題に基づいています。

8.2 NIST による PQC 標準化プロセス

この来るべき時代に備え、米国立標準技術研究所（NIST）は 2016 年から PQC の標準化プロジェクトを進めてきました。世界中から提案された暗号方式を、数ラウンドにわたって安全性や性能を評価・選別し、2022 年についに最初の標準化対象アルゴリズムを発表しました [3]。

現在、これらの新しい暗号への移行が世界的に始まっており、当面は既存の暗号（RSA や ECC）と PQC を併用する「ハイブリッド方式」が取られると考えられています。

9 おわりに

この文章では、群論から始まり、整数論、有限体、そして楕円曲線へと、数学的な概念を一つずつ積み上げることで、楕円曲線暗号の仕組みのイメージを掴むことを目指しました。有限体上での離散対数問題では準指数時間アルゴリズムである指標計算法 (index-caluculus-Algolism) が存在するため、点の集合が群を成す楕円曲線上での離散対数問題では一般的には因数分解ができないので指標計算法が使えないというのが今回の肝です。また一般的な (特別な条件を持たない) 楕円曲線上での離散対数問題を解く最良のアルゴリズムでもほとんど指数時間オーダーです。以下が比較表になり

ます。

表 1　暗号方式の鍵長とセキュリティレベルの比較 [2]

セキュリティレベル (ビット)	RSA / 有限体 DLP 鍵長 (ビット)	楕円曲線暗号 (ECC) 鍵長 (ビット)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

10　おまけ

本文では、一般的な楕円曲線暗号には指標計算法が適用できないと述べました。しかし例外として、拡大体上の特定の曲線に対しては、Generalized Weil descent と呼ばれる攻撃法が知られています。[4] これは、拡大体が素体上のベクトル空間と見なせる構造を悪用し、指標計算法の枠組みを楕円曲線上に適用するものです。現在標準として使われる NIST P-256 や secp256k1 は、いずれも素体上の楕円曲線であるため、この攻撃の対象外です。この他にも、ペアリングを用いて楕円曲線上の問題を有限体の離散対数問題に変換（帰着）する攻撃法も存在しますが、[4][5] 現在の標準曲線はこれらの高度な攻撃にも耐えうるように設計されています。

参考文献

[1] N. コブリッツ (著), 櫻井 幸一 (訳), 『数論アルゴリズムと楕円曲線暗号入門』, シュプリンガー・フェアラーク東京, 1997.

[2] National Institute of Standards and Technology (NIST), *Special Publication 800-57 Part 1, Revision 5: Recommendation for Key Management*, U.S. Department of Commerce, May 2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[3] National Institute of Standards and Technology (NIST), *NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, U.S. Department of Commerce, March 2022. https://doi.org/10.6028/NIST.IR.8413

[4] あんこ, “楕円曲線暗号を実装して有名な攻撃を試してみる”, *Zenn*, 2021 年 12 月 25 日公開. https://zenn.dev/anko/articles/ctf-crypto-ellipticcurve

[5] シニアエンジニアの庵, “ペアリング写像”, ペアリング写像. https://sehermitage.web.fc2.com/cmath/pairing.html

[6] 数学の景色, “準同型写像と同型写像の定義・基本的な性質”, 数学の景色, 2022 年 8 月 21 日更新. https://mathlandscape.com/homomorphism/