楕円曲線暗号入門

（「計算機緒論２」 配布資料）

2010 年 8 月 3 日 (火)

伊豆 哲也

目次

第 1 章

楕円曲線と楕円曲線のなす群

楕円曲線暗号は有限体上で定義される楕円曲線を使用します. 本章では, 有限体 (素体) 上の楕円曲線について説明します.

1.1 有限体

素数 p に対し, 0 から $p-1$ までの整数の集合

$$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$$

を考えます. 整数を p で割った余りは 0 から $p-1$ の整数になるので, この集合の要素同士を加算して得られた値を p で割った結果は, またこの集合の要素となります.

演習 1.1　集合 $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ における加算 $x + y$ の結果を表 1.1 にまとめよ.

集合 $\mathbb{F}_p$ のある要素 x と $x+p$ を p で割った余りは等しいので, $\mathbb{F}_p$ では x と $x+p$ は等しいことになります. よって $x - y = x + p - y$ となり, 集合 $\mathbb{F}_p$ における減算も計算することができます.

演習 1.2　集合 $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ における減算 $x - y$ の結果を表 1.2 にまとめよ.

このように要素同士で加算・減算を計算することができる集合を **加法群 (additive group)** と呼びます.

表 1.1　集合 $\mathbb{F}_7$ における加算の計算結果

x \ y	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

表 1.2　集合 $\mathbb{F}_7$ における減算の計算結果

x \ y	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

コラム　群

集合 G と演算 $\circ$ が (i) G の任意の要素 a, b, c に対し $(a \circ b) \circ c = a \circ (b \circ c)$ となる, (ii) G の任意の要素 a に対し $a \circ e = e \circ a = a$ となる G の要素 e が存在する, (iii) G の任意の要素 a に対し $a \circ a' = a' \circ a = e$ となる G の要素 a' が存在する, という全ての条件が成立するとき, G は演算 $\circ$ に関する群 (group) であると言います. 特に演算が $+$ となるときを加法群と呼んでいます. 演算 $\circ$ は可換 (つまり $x \circ y = y \circ x$) とは限りませんが, 加法群は可換 (つまり $x + y = y + x$) と考えます.

集合 $\mathbb{F}_p$ の要素同士を乗算して得られた値を p で割った結果は, またこの集合の要素となります.

演習 1.3　集合 $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ における乗算 $x \times y$ の結果を表 1.3 にまとめよ.

集合 $\mathbb{F}_p$ では p で割った余りに着目しているので, $x,\ x+p,\ x+2p,\ x+3p, \ldots$ は全て等しいことになります. よって $x \div y = (x+p) \div y = (x+2p) \div y = \cdots$ と考えることができますので, 整数の除算として割り切れた値を用いることで除算を計算可能です. (一般に, 整数 $p,\ x$ に対し, ある整数 $a,\ b$ が $ap + by = 1$ を満たすとき, $by \equiv 1 \pmod{p}$ つまり $b \equiv y^{-1} \pmod{p}$ となり, $x \div y = x \times b$ と変形できます. このような $a,\ b$ は拡張 Euclid の互除法によって効率的に計算可能です.)

演習 1.4　集合 $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ における除算 $x \div y\ (y \neq 0)$ の結果を表 1.4 にまとめよ.

このように, 要素同士で加算・減算・乗算・除算 (ただし 0 による除算は除く) を計算することができる p 個の要素を持つ集合 $\mathbb{F}_p$ を **素体 (prime field)** と呼びます.

素体のように, 有限個の要素を持つ集合で, 要素間の加算・減算・乗算・除算 (ただし 0 による除算は除く) が計算できるとき, その集合を **有限体 (finite field)** と言います. 有限体の要素の個数は, 素数のべきになることが知られています. 素体は有限体の例になっています.

表 1.3　集合 $\mathbb{F}_7$ における乗算の計算結果

x \ y	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

表 1.4　集合 $\mathbb{F}_7$ における除算の計算結果

x \ y	0	1	2	3	4	5	6
0	—						
1	—						
2	—						
3	—						
4	—						
5	—						
6	—						

コラム　体

体は英語で field と言いますが, field という単語には (もともと) 体という意味はありませんでした. これは, ドイツ語の köper (体, からだ) という単語から直接に日本語に訳されたからです. 体では四則演算が自由に計算できるため, 野原のように自由がきくということで, 英語としては field が使用されています.

1.2 楕円曲線の定義方程式

素体 $\mathbb{F}_p$ 上の楕円曲線を以下のように定義します.

定義 1.5 (楕円曲線の定義方程式) 方程式

$$E : y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_p,\ \Delta_E = 4a^3 + 27b^2 \neq 0) \tag{1.1}$$

で定義される曲線を素体 $\mathbb{F}_p$ 上の **楕円曲線 (elliptic curve)** という.

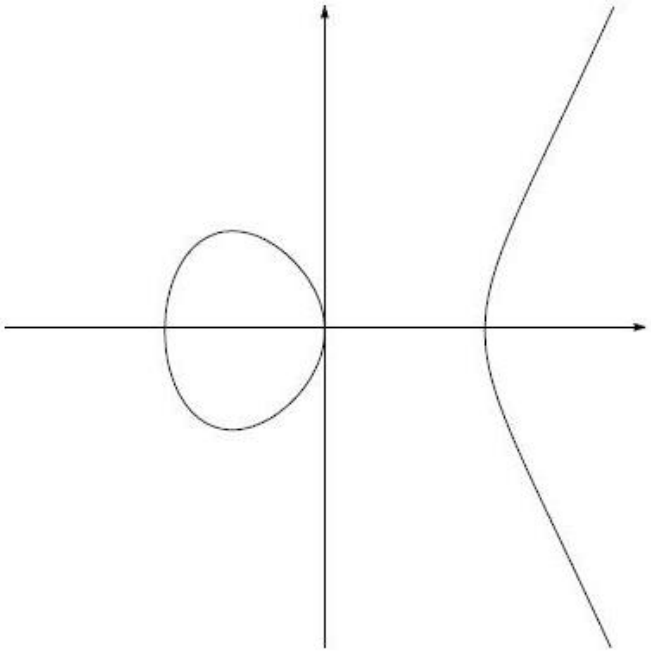
演習 1.6 方程式 $E : y^2 = x^3 + 3x + 4$ は素体 $\mathbb{F}_7$ 上の楕円曲線であることを示せ.

楕円曲線 E 上の点のうち, x, y 座標がともに有限体 $\mathbb{F}_p$ の要素であるような点 (x, y) を **$\mathbb{F}_p$-有理点 ($\mathbb{F}_p$-rational point)** と呼びます. また **無限遠点 (the point at infinity)** と呼ばれる特別な点 $\mathcal{O}$ も有理点として扱います. 無限遠点は (x, y) という表記ができない唯一の点です.

演習 1.7 素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ の 10 個の有理点を表 1.5 に示せ.

表 1.5 楕円曲線 $y^2 = x^3 + 3x + 4$ の $\mathbb{F}_7$-有理点

P_0	$\mathcal{O}$		
P_1	$(0, 2)$	P_9	$(0,\quad)$
P_2	$(1, 1)$	P_8	$(1,\quad)$
P_3	$(2, 2)$	P_7	$(2,\quad)$
P_4	$(5, 2)$	P_6	$(5,\quad)$
P_5			



コラム　判別式

楕円曲線の定義方程式で登場した $\Delta_E = 4a^3 + 27b^2 \neq 0$ という条件は, 式 (1.1) の右辺が重複解を持つ場合を排除するための条件です. この Δ_E を **判別式 (discriminant)** と言います. 2 次の方程式 $F : y = x^2 + Bx + C$ の判別式は $\Delta_F = B^2 - 4C$ であり, $\Delta_F \neq 0$ のときに F は重複解を持たなかったのと同様です.

一般に n 次の方程式 $G : y = A_0x^n + A_1x^{n-1} + \cdots + A_n$ に対する判別式は $\Delta_G = A_0^{2(n-1)}(\alpha_1 - \alpha_2)^2 \times \cdots \times (\alpha_1 - \alpha_n)^2 \times (\alpha_2 - \alpha_3)^2 \times \ldots (\alpha_2 - \alpha_n)^2 \times \cdots \times (\alpha_{n-1} - \alpha_n)^2$ で定義されます. ここで $\alpha_1, \ldots, \alpha_n$ は G の解を表します. 興味がある方は, $n = 3$ の場合の判別式を導出し, 特に楕円曲線の場合に $\Delta_E = 4a^3 + 27b^2$ となることを確認してみて下さい.

1.3 加法公式

楕円曲線の有理点の集合は加法群となる, つまり有理点同士の加算・減算を計算することが可能です. このときの加算の計算ルールはとても特徴的になっています (点同士の x 座標, y 座標を足しあわすわけではありません). まずは幾何的な計算方法を説明し, 次に代数的な計算方法 (加法公式) を示します.

定義 1.8 (加法の計算方法) 素体 $\mathbb{F}_p$ 上の楕円曲線 $E : y^2 = x^3 + ax + b$ 上の 2 点 P, Q $(\neq \mathcal{O})$ の和 $R = P + Q$ を以下のように定める.

1. 2 点 P, Q を通る直線 ($P = Q$ の場合には P を通る接線) ℓ を引く.
2. 楕円曲線 E と直線 ℓ の 3 つ目の交点を R' とする (交点がない場合には $R' = \mathcal{O}$ とする).
3. R' の x 軸に関する対称点を R とする ($R' = \mathcal{O}$ の場合には $R = \mathcal{O}$ とする).

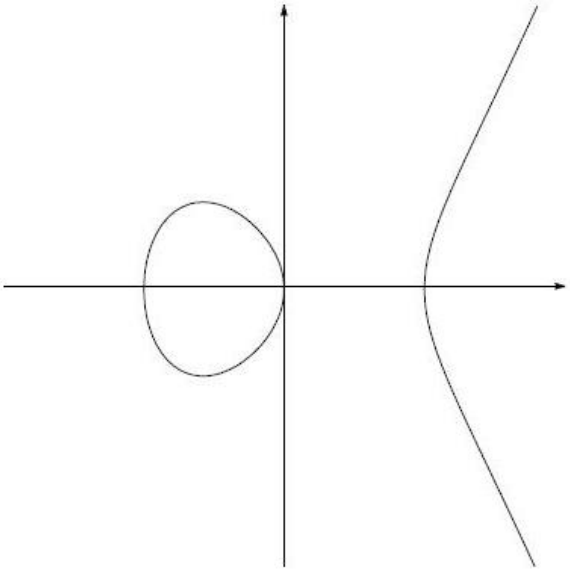
途中で得られた R' を R の逆元と呼び, $R' = -R$ とかくことが多い.

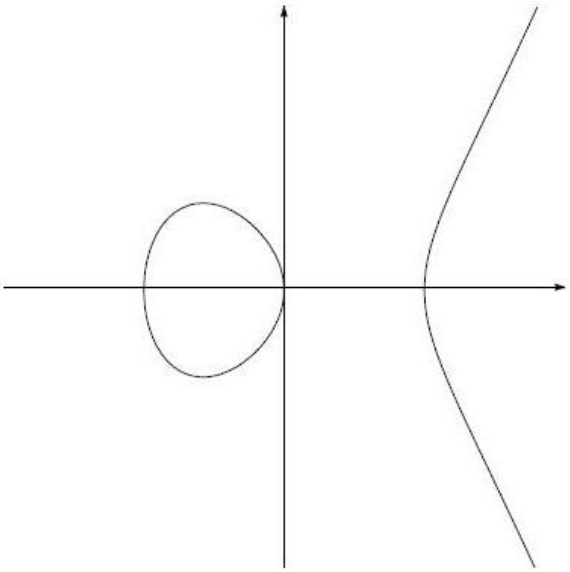
なお無限遠点 $\mathcal{O}$ を有理点に含めたのは, 上の計算手順をわかりやすくするためです.

演習 1.9 演習 1.7 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ において, それぞれの点の逆元を表 1.6 に示せ.

表 1.6 楕円曲線 $y^2 = x^3 + 3x + 4$ の $\mathbb{F}_7$-有理点の逆元

点	座標	逆元の座標	逆元	点	座標	逆元の座標	逆元
P_0	$\mathcal{O}$						
P_1	$(0, 2)$			P_6	$(5, 5)$		
P_2	$(1, 1)$			P_7	$(2, 5)$		
P_3	$(2, 2)$			P_8	$(1, 6)$		
P_4	$(5, 2)$			P_9	$(0, 5)$		
P_5	$(6, 0)$						





コラム　楕円曲線と楕円

楕円曲線 (elliptic curve) と楕円 (ellipse) は異なる曲線です. ところが楕円曲線暗号の省略として「楕円暗号」という単語が用いられるため, 楕円曲線暗号とは楕円を用いた暗号と誤解されることがあります. ある新聞社は「楕円暗号」を公式用語として使用しているため, 今でもこのような誤解が後を絶ちません.

もっとも楕円曲線は, 楕円の弧の長さを計算する際に登場する関数 (の逆関数) として導入されたものです. 従って楕円曲線と楕円は非常に強い結びつきを持っています.

次に楕円曲線の計算方法を数式で表現してみましょう.

定義 1.10 (楕円曲線の加法公式) 素体 $\mathbb{F}_p$ 上の楕円曲線 $E : y^2 = x^3 + ax + b$ 上の 2 点 $P,\ Q$ の和 $R = P + Q$ を以下のように定める.

- $P = \mathcal{O}$ のとき: $R = Q$ とする.
- $Q = \mathcal{O}$ のとき: $R = P$ とする.
- それ以外のとき: $P = (x_P, y_P),\ Q = (x_Q, y_Q)$ とかくとき
  - $y_P = -y_Q$ のとき: $R = \mathcal{O}$ とする (このとき $Q = -P$ となっている).
  - $y_P \neq -y_Q$ のとき: $R = (x_R, y_R)$ とする. ここで $x_R,\ y_R$ は

$$x_R = \lambda^2 - x_P - x_Q, \quad y_R = \lambda(x_P - x_R) - y_P$$

であり, λ は 2 点 $P,\ Q$ を通る直線 (または点 P での接線) の傾き

$$\lambda = \begin{cases} \dfrac{y_P - y_Q}{x_P - x_Q} & x_P \neq x_Q \\ \dfrac{3x_P^2 + a}{2y_P} & x_P = x_Q \end{cases}$$

をあらわす.

演習 1.11 演習 1.7 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ において, $P_2 + P_4,\ 2 \times P_6$ をそれぞれ求めよ.

コラム　接線の傾き

平面上の 2 点 $P=(x_P,y_P)$, $Q=(x_Q,y_Q)$ を通る直線の傾きは $(y_P-y_Q)/(x_P-x_Q)$ です．しかし $x_P=x_Q$ のときには分母が 0 になるため, 特別な扱いが必要になります．そこで P, Q が楕円曲線 $E: y^2=x^3+ax+b$ 上の点であることを利用すると

$$\frac{y_P-y_Q}{x_P-x_Q}=\frac{(y_P-y_Q)(y_P+y_Q)}{(x_P-x_Q)(y_P+y_Q)}=\frac{y_P^2-y_Q^2}{(x_P-x_Q)(y_P+y_Q)}=\frac{(x_P^3+ax_P+b)-(x_Q^3+ax_Q+b)}{(x_P-x_Q)(y_P+y_Q)}$$
$$=\frac{(x_P-x_Q)(x_P^2+x_Px_Q+x_Q^2+a)}{(x_P-x_Q)(y_P+y_Q)}=\frac{x_P^2+x_Px_Q+x_Q^2+a}{y_P+y_Q}$$

という式変形ができますので, $P=Q$ つまり $x_P=x_Q$, $y_P=y_Q$ の場合の傾きは

$$\frac{y_P-y_Q}{x_P-x_Q}=\frac{x_P^2+x_Px_Q+x_Q^2+a}{y_P+y_Q}=\frac{3x_P^2+a}{2y_P}$$

となります.

楕円曲線 $y^2 = x^3 + 3x + 4$ の $\mathbb{F}_7$-有理点の加算結果は表 1.7 のようになります.

表 1.7　楕円曲線 $y^2 = x^3 + 3x + 4$ の $\mathbb{F}_7$-有理点の加算結果

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
P_0	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
P_1	P_1	P_8	P_9	P_6	P_7	P_4	P_5	P_3	P_2	P_0
P_2	P_2	P_9	P_1	P_4	P_6	P_3	P_7	P_5	P_0	P_8
P_3	P_3	P_6	P_4	P_1	P_9	P_2	P_8	P_0	P_5	P_7
P_4	P_4	P_7	P_6	P_9	P_8	P_1	P_0	P_2	P_3	P_5
P_5	P_5	P_4	P_3	P_2	P_1	P_0	P_9	P_8	P_7	P_6
P_6	P_6	P_5	P_7	P_8	P_0	P_9	P_2	P_1	P_4	P_3
P_7	P_7	P_3	P_5	P_0	P_2	P_8	P_1	P_9	P_6	P_4
P_8	P_8	P_2	P_0	P_5	P_3	P_7	P_4	P_6	P_9	P_1
P_9	P_9	P_0	P_8	P_7	P_5	P_6	P_3	P_4	P_1	P_2

演習 1.12　定義 1.8 の加法の計算方法をもとに, 定義 1.10 の加法公式を導出せよ.

コラム **楕円曲線の一般形**

このテキストでは, 楕円曲線の定義方程式として $y^2 = x^3 + ax + b$ という式を用いていますが (定義 1.4), 一般には

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

という定義方程式を用います (Weierstrass の標準形). この式に変数変換を施すことで $y^2 = x^3 + ax + b$ という式が得られます.

1.4 有理点のなす群

前節で説明した通り, 楕円曲線では有理点同士の加算・減算が計算可能です. このように楕円曲線上の有理点のなす加法群を **Mordell-Weil 群 (Mordell-Weil group)** と呼びます.

加法群の要素の個数を **群位数 (group order)** と言います. 楕円曲線上の有理点のなす加法群の位数とは有理点の個数のことに他なりません.

演習 1.13　演習 1.7 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ の群位数 $\#E$ を求めよ.

素体 $\mathbb{F}_p$ 上の楕円曲線の群位数に関しては, 以下の定理が有名です.

定理 1.14 (Hasse-Weil の定理)　素体 $\mathbb{F}_p$ 上の楕円曲線 E の群位数を $\#E$ とかくとき, $\#E$ は

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$$

を満たす.

Hasse-Weil の定理 (定理 1.14) は, 素体 $\mathbb{F}_p$ 上の楕円曲線の有理点のなす群の群位数がおよそ p 個になることを保証しています. 例えば, 素体 $\mathbb{F}_7$ 上の楕円曲線の群位数は表 1.8 のようになっています. このような性質から, 素体上の楕円曲線は暗号や素因数分解など, さまざまな用途に用いられています.

演習 1.15　演習 1.7 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ の群位数は Hasse-Weil の定理 (定理 1.14) を満たしていることを示せ.

表 1.8　素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + ax + b$ の群位数

		b						
		0	1	2	3	4	5	6
a	0	–	12	9	13	3	7	4
	1	8	5	–	6	10	–	11
	2	8	5	–	6	10	–	11
	3	8	12	9	6	10	7	4
	4	8	5	–	6	10	–	11
	5	8	12	9	6	10	7	4
	6	8	12	9	6	10	7	4

コラム　Deuring の定理

Hasse-Weil の定理 (定理 1.14) は, 素体上の楕円曲線の群位数の範囲を示しています. ではその範囲内のある自然数を選んだとき, 群位数がその自然数となるような楕円曲線は存在するでしょうか？ Deuring の定理はこの疑問を肯定的に答えてくれます. つまり Deuring の定理は, 係数 a, b を変化させることで, Hasse-Weil の定理の範囲内の自然数を群位数に持つ楕円曲線が必ず存在することを保証してくれます. 興味がある方は素体 $\mathbb{F}_7$ 上の楕円曲線の場合 (表 1.8) で確認してみて下さい.

1.5 スカラー倍算

素体 $\mathbb{F}_p$ 上の楕円曲線 E 上の点 P を選びます (この点を **ベースポイント (base point)** と呼びます). 適当な整数 d に対し, ベースポイント P を d 倍した点

$$d \times P = \underbrace{P + \cdots + P}_{d \text{ 個}}$$

を求める計算を **スカラー倍算 (scalar multiplication)** と呼びます.

実際にスカラー倍算を計算するには, 加法公式を繰り返して適用していきます.

演習 1.16 演習 1.7 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ において, 点 P_1 をベースポイントとしたときの以下のスカラー倍算を計算しなさい.

$2 \times P_1 =$
$3 \times P_1 =$
$4 \times P_1 =$
$5 \times P_1 =$
$6 \times P_1 =$
$7 \times P_1 =$

このように, ベースポイントを 2 倍, 3 倍, ... していくと, かならず途中で計算結果が無限遠点 $\mathcal{O}$ に等しくなります. そのときのスカラーの値をベースポイントの **点位数 (point order)** と言います. 別の言い方をすると, ベースポイント P の点位数とは $d \times P = \mathcal{O}$ となる最小の自然数のことです.

なお, 楕円曲線上のどの点をベースポイントに選んでも, その点の点位数は群位数の約数になることが知られています.

演習 1.17 演習 1.7 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ において, 点 P_1 の点位数を求めよ.

コラム **べき乗算とスカラー倍算**

整数 x の指数 d 乗 x^d を求める演算をべき乗算と言い, (この値を mod N したものが) RSA 暗号の暗号化・復号で必要となります. 同様に, スカラー倍算 $d \times P$ は, 本テキストの目標である楕円曲線暗号において, 必要となります.

スカラー倍算 $d \times P$ を計算する場合, 加法公式を $d-1$ 回適用すれば計算することができます. 例えば,

$$8 \times P = P + P + P + P + P + P + P + P$$

は加法公式を 7 回適用することによって計算可能です. しかし,

$$8 \times P = 2 \times (2 \times (2 \times P))$$

と表せることを利用すれば, 3 回の加法公式で計算可能です. この考え方を発展させると, 効率的にスカラー倍算を計算することができます. ただしスカラー d の 2 進数展開を

$$\begin{aligned} d &= 2^{n-1} + d_{n-2} \cdot 2^{n-2} + \cdots + d_1 \cdot 2 + d_0 \quad (d_i \in \{0,1\}) \\ &= (1, d_{n-2}, \ldots, d_1, d_0)_2 \end{aligned}$$

とします.

アルゴリズム 1.1　スカラー倍算の計算アルゴリズム

入力: ベースポイント P, スカラー $d = (1, d_{n-2}, \ldots, d_1, d_0)_2$
出力: スカラー倍点 $d \times P$

1. $Q \leftarrow P$
2. $i = n-2, \ldots, 1, 0$ に対し以下を処理する:
   2.1 $Q \leftarrow 2 \times Q$
   2.2 $d_i = 1$ ならば $Q \leftarrow Q + P$
3. Q を出力する.

このアルゴリズムを用いると, スカラー倍算 $d \times P$ を計算するのに必要な加法公式の回数は (平均で) $1.5 \log_2 d$ 回程度となり, 素朴に加法公式を適用した場合の $d-1$ 回に比べて効率的であることがわかります.

演習 1.18　上のスカラー倍算計算アルゴリズムにおいて, スカラーが $d = 3045 = (1,0,1,1,1,1,1,0,0,1,0,1)_2$ の場合に, 下表を用いて変数 Q の変化を調べよ. また, 加算公式の使用回数を求めよ.

i	10	9	8	7	6	5	4	3	2	1	0
d_i	0	1	1	1	1	1	0	0	1	0	1
2.1 処理前											
2.1 処理後											
2.2 処理後											

コラム **有限体上の楕円曲線の群構造**

有限体 $\mathbb{F}_q$ 上の楕円曲線 E の Mordell-Weil 群を $E(\mathbb{F}_q)$ とかくとき, $E(\mathbb{F}_q)$ は 2 つの巡回群 $C_1,\ C_2$ の直積になる, つまり

$$E(\mathbb{F}_q) \simeq C_1 \times C_2 \quad (\#C_1 | \#C_2,\ \#C_1 | (q-1))$$

となることが知られています. なお楕円曲線暗号では, $E(\mathbb{F}_q)$ が素数位数の巡回群になる (つまり $E(\mathbb{F}_q) \simeq C_1$) となるような楕円曲線を使用することが多いです.

1.6 スカラー倍算の高速化 (1) 〜 射影座標

楕円曲線暗号を処理するプログラムでは, スカラー倍算の計算時間が支配的になります. そこで, いくつかのスカラー倍算の高速化手法を紹介していきます.

素体 $\mathbb{F}_p$ では, 加算・減算の計算時間に比べて乗算の計算時間は長く, 除算の計算時間はさらに長い (乗算の 10〜50 倍) のが普通です. しかし楕円曲線の加法公式 (定義 1.10) は除算の計算を必要とするため, その計算も長い時間を必要とします. そこでこの除算計算を回避するために, **射影座標 (projective coordinates)** という新しい座標を導入します.

射影座標では, 平面上の点の座標は 3 つの要素の組 $(X : Y : Z)$ によって表されます. ただし, 2 点 $(X : Y : Z)$, $(X' : Y' : Z')$ の間に

$$X' = cX, \quad Y' = cY, \quad Z' = cZ$$

となるような定数 $c \in \mathbb{F}_p$ が存在するとき, この 2 点は等しいと考えます. したがって

$$(X : Y : Z) = (2X : 2Y : 2Z) = \cdots = (X/Z : Y/Z : 1)$$

となります. そこで, ある点の通常の座標 (アフィン座標) における座標値 (x, y) と, 射影座標における座標値 $(x : y : 1)$ を同一視します. このとき, 射影座標における点 $(X : Y : Z)$ はアフィン座標における点 $(X/Z, Y/Z)$ と同一視できることになります.

コラム **Jacobian 射影座標**

射影座標において, 2 点が等しいかどうかの判定ルールを

$$X' = c^2X, \quad Y' = c^3Y, \quad Z' = cZ$$

と変更した場合の射影座標を **Jacobian 射影座標 (Jacobian projective coordinate)** と言います. このように判定ルールを変更させることで, さまざまな射影座標を得ることができます.

射影座標における楕円曲線の定義方程式は

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \quad (a, b \in \mathbb{F}_p,\ \Delta_E = 4a^3 + 27b^2 \neq 0)$$

となります. これは, アファイン座標における楕円曲線の定義方程式 $y^2 = x^3+ax+b$ に $x = X/Z$, $y = Y/Z$ を代入することで得られます. また射影座標では, 無限遠点は X 座標値と Z 座標値が 0 の点と定義します.

同様にして, 射影座標における加法公式を得ることもできます. 射影座標では無限遠点も座標表記できるため, 場合分けが不要となり, 表記がシンプルになっています.

定義 1.19 (射影座標における楕円曲線の加法公式) 射影座標における素体 $\mathbb{F}_p$ 上の楕円曲線

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

上の 2 点 $P = (X_P : Y_P : Z_P)$, $Q = (X_Q : Y_Q : Z_Q)$ の和 $R = P + Q = (X_R : Y_R : Z_R)$ を以下のように定める.

- $P \neq Q$ のとき

$$\begin{aligned} X_R &= vA \\ Y_R &= u(v^2X_PZ_Q - A) - v^3Y_PZ_Q \\ Z_R &= v^3Z_PZ_Q \end{aligned}$$

  ただし $u = Y_QZ_P - Y_PZ_Q$, $v = X_QZ_P - X_PZ_Q$, $A = u^2Z_PZ_Q - v^3 - 2v^2X_PZ_Q$

- $P = Q$ のとき

$$\begin{aligned} X_R &= 2hs \\ Y_R &= w(4B - h) - 8Y_P^2s^2 \\ Z_R &= 8s^3 \end{aligned}$$

  ただし $w = aZ_P^2 + 3X_P^2$, $s = Y_PZ_P$, $B = sX_PY_P$, $h = w^2 - 8B$

演習 1.20 射影座標における楕円曲線の加法公式を計算するのに必要な乗算の回数を求めよ.

- $P \neq Q$ のとき:
- $P \neq Q$ のとき:

射影座標を用いてスカラー倍算を計算するには, 射影座標における点 $P = (x : y : 1)$ のスカラー倍算 $d \times P = (X : Y : Z)$ を求め, その結果をアフィン座標 $(X/Z, Y/Z)$ に変換することになります. アフィン座標におけるスカラー倍算では加法公式を使うたびに除算が必要だったのに対し, 射影座標におけるスカラー倍算では除算が 1 回しか必要ありませんので, 高速化の効果は絶大です.

コラム **座標の比較**

アフィン座標, 射影座標, Jacobian 射影座標において, 加法公式を計算するのに必要な乗算の回数は以下のようになります.

	$P \neq Q$ のとき	$P = Q$ のとき
アフィン座標	乗算 3 回, 除算 1 回	乗算 4 回, 除算 1 回
射影座標	乗算 14 回	乗算 12 回
Jacobian 射影座標	乗算 16 回	乗算 10 回

アルゴリズム 1.1 で紹介したスカラー倍算の計算アルゴリズムを用いる場合, スカラー d の各ビット d_i に対し, $P = Q$ の場合の加法公式を必ず計算し, $P \neq Q$ の場合の加法公式を 1/2 の確率で計算するので, $P = Q$ の場合の加法公式の計算が高速な Jacobian 射影座標が好まれます.

1.7 スカラー倍算の高速化 (2) 〜 ウィンドウ法

アルゴリズム 1.1 のスカラー倍算の計算アルゴリズムはスカラー d の 2 進展開を利用していました. 同様に, スカラー d の m 進展開を利用することも可能です. 例えば $m = 8$ の場合のアルゴリズムは以下のようになります (簡単のため n は 3 の倍数であると仮定します).

アルゴリズム 1.2　スカラー倍算の計算アルゴリズム (8 進展開の利用)

入力: ベースポイント P, スカラー $d = (d_{n-1}, d_{n-2}, \ldots, d_1, d_0)_2$
出力: スカラー倍点 $d \times P$

0. $i = 0, 1, \ldots, 7$ に対し以下を処理する:
  0.1 $P_i \leftarrow i \times P$
1. $Q \leftarrow P_{4d_{n-1}+2d_{n-2}+d_{n-3}}$
2. $i = n-4, n-7, \ldots, 2$ に対し以下を処理する:
  2.1 $Q \leftarrow 8 \times Q$
  2.2 $Q \leftarrow Q + P_{4d_i+2_{i-1}+d_{i-2}}$
3. Q を出力する.

アルゴリズム 1.2 は, ステップ 0. で P_0, P_1, $\ldots$, P_7 というテーブルをあらかじめ計算しておき, ステップ 1. やステップ 2.2 でその値を参照しています. アルゴリズム 1.1 に比べ, 全体の処理が 3 ビットごとにまとめられていることに注意して下さい. このようなスカラー倍算の高速化手法を **ウィンドウ法 (window method)** と呼びます.

演習 1.21　上のスカラー倍算計算アルゴリズムにおいて, スカラーが $d = 3045 = (1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1)_2$ の場合に, 下表を用いて変数 Q の変化を調べよ. また, 加算公式の使用回数を求めよ.

i	8	5	2
$d_i d_{i-1} d_{i-2}$	111	100	101
2.1 処理前			
2.1 処理後			
2.2 処理後			

アルゴリズム 1.1 と比べると, アルゴリズム 1.2 のステップ 2.1 の計算回数は 1/3 になっていますが, $8 \times P$ を計算するのに 3 回の加法公式を必要とするため, ステップ 2.1 に関する加法公式の使用回数はほぼ n 回です. また, ステップ 2.2 の計算回数も 1/3 になっているため, ステップ 2.2 に関する加法公式の使用回数はほぼ $n/3$ 回です. アルゴリズム 1.1 ではステップ 2.2 を確率 1/2 で実行したため, ステップ 2.2 に関する加法公式の使用回数はほぼ $n/2$ 回だったことを考えると, 高速化できていることがわかります. しかしアルゴリズム 1.2 はステップ 0.1 でテーブルを作成する際に加法公式を使用しているので, その分を差し引く必要があります.

コラム **適切なウィンドウサイズ**

スカラー d が 160 ビットの場合, $m = 2^4$ または 2^5 に設定した場合に加法公式の使用回数が最小になることが知られています.

1.8 スカラー倍算の高速化 (3) 〜 符号付き 2 進展開法

楕円曲線では, ある点 P のマイナスの点 $-P$ を簡単に求めることができます (アフィン座標なら $(x, -y)$, 射影座標なら $(X : -Y : Z)$). 従って, スカラー d の符号付き 2 進数展開

$$\begin{aligned} d &= 2^{n-1} + d_{n-2} \cdot 2^{n-2} + \cdots + d_1 \cdot 2 + d_0 \quad (d_i \in \{-1, 0, 1\}) \\ &= (1, d_{n-2}, \ldots, d_1, d_0)_2 \end{aligned}$$

がわかっていれば, 次のようなスカラー倍算アルゴリズムを用いることができます.

アルゴリズム 1.3　スカラー倍算の計算アルゴリズム (符号付き 2 進展開の利用)

入力: ベースポイント P, スカラー $d = (d_{n-1}, d_{n-2}, \ldots, d_1, d_0)_2$
出力: スカラー倍点 $d \times P$

---

1. $Q \leftarrow P$
2. $i = n-2, \ldots, 1, 0$ に対し以下を処理する:
   2.1 $Q \leftarrow 2 \times Q$
   2.2 $d_i = 1$ ならば $Q \leftarrow Q + P$
   2.3 $d_i = -1$ ならば $Q \leftarrow Q - P$
3. Q を出力する.

スカラー d の符号付き 2 進展開による表し方は何通りも考えられますが, **NAF (non-adjacent form, 非隣接形式)** と呼ばれる表し方が有名です. スカラー d に対し, まず $3d$ の (符号なし) 2 進展開を $(e_{n+1}, e_n, \ldots, e_0)_2$ と d の (符号なし) 2 進展開を $(f_{n+1}, f_n, \ldots, f_0)_2$ を求めます. $d = (3d - d)/2$ なので, $3d$ の 2 進展開から d の 2 進展開を引いた結果を 2 で割れば, d の符号付き 2 進展開を得ることができます (つまり $d_i = e_{i+1} - f_{i+1}$). NAF においては, その名の通り, 1 または -1 というビット値が連続しないため, スカラー d における ± 1 の個数は平均的に $\log_2 d/3$ 個となります. よってアルゴリズム 1.3 で NAF を使用すると, 加法公式の使用回数は平均で $1.33 \log_2 n$ 回となります.

コラム **べき乗と符号付き 2 進展開**

べき乗計算に符号付き 2 進展開を用いると, $d_i = -1$ のときに除算が必要となり, 逆に計算時間の増大を招いてしまいます.

本章のまとめ

- 素体とは p 個の要素からなる集合で, 要素間の加算・減算・乗算・除算を計算することができる.
- 楕円曲線とは, 方程式 $y^2 = x^3 + ax + b$ で表される曲線である.
- 楕円曲線では, 加法公式によって点同士の加算・減算を計算することができる.
- 楕円曲線暗号ではスカラー倍算が重要であり, さまざまな高速化手法が考案されている.

[**おまけコラム**]

本章では楕円曲線上の有理点が加法群になることを説明しましたが, この加法群を用いた暗号系が楕円曲線暗号となります. 群は現代数学における基本的な概念で, 他のさまざまな場面でも繰り返し登場するのですが, だからといって全ての群から暗号系を構成できるとは限りません. 暗号を構成するには, 一方向性関数が存在し, その関数が効率的に計算できる必要があります. 楕円曲線の場合, スカラー倍の逆問題 ($d \times P$ から d を求める問題) が一方向性関数であり, 加法公式によって効率的な計算が可能となっています. このように楕円曲線では困難性と効率性の微妙なバランスが成立しているため, 実用的な暗号が構築できるのです. 新しい暗号を構築する目的で, 新しい群, あるいは新しい一方向性関数の探索は続いているのですが, 楕円曲線のように優れた性質を持つものは見つけられていません.

第 2 章

離散対数問題と解法アルゴリズム

本章では, 楕円曲線離散対数問題を解くいくつかのアルゴリズムを紹介します.

2.1 楕円曲線離散対数問題 (ECDLP)

素体 $\mathbb{F}_p$ 上の楕円曲線 E において, ベースポイント P と整数 d から点 $Q = d \times P$ 計算するのは簡単でした (この計算をスカラー倍算と呼ぶのでした). 逆に, 点 P, Q から $Q = d \times P$ となる整数 d ($1 \leq d \leq \ell$, ℓ はベースポイント P の点位数) を求める問題を **楕円曲線離散対数問題 (elliptic curve discrete logarithm problem, ECDLP)** と言います.

演習 2.1 演習 1.7 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ において, $P = P_1$, $Q = P_2$ とするとき, $Q = d \times P$ となる整数 d を求めよ.

演習 2.1 のように, 点位数が小さい場合の楕円曲線離散対数問題は簡単に解くことができます. しかし点位数が大きい場合, 楕円曲線離散対数問題を解くことは非常に困難です. 次節から, 楕円曲線離散対数問題のいくつかの解法を紹介していきます.

演習 2.2 素体 $\mathbb{F}_p$ では加算・減算が自由に計算できるので, 適当な要素 P, $Q \in \mathbb{F}_p$ に対して $Q = d \times P$ となる要素 d を求める問題を考えることができる. この問題を解くことは簡単か？難しいか？を考察せよ.

コラム **対数と離散対数**

$P,\ Q = P^d$ が実数の場合, $P,\ Q$ から d を求める問題を (対数問題) はとても簡単に解くことができて, 対数 $\log_P Q$ を計算すれば良いのでした. これは対数関数 $y = \log_P Q$ が連続性や単調増加性というありがたい性質を持っているからです.

これに対して $Q = d \times P$ から d を求める問題 (楕円曲線離散対数問題) を解くのは困難です. その理由の一つには, スカラー倍算の結果が離散的に変化するという性質が挙げられます.

2.2 総当り法

楕円曲線上の 2 点 P, Q から $Q = d \times P$ となる整数 d ($1 \leq d \leq \ell$, ℓ は P の点位数) を求める問題 (楕円曲線離散対数問題) を解くのに, $2 \times P$, $3 \times P, \ldots, \ell \times P$ を順番に計算していく方法を **総当たり法 (brute force method)** と言います.

演習 2.3 周波数が 4 GHz の計算機は, 1 秒間に 4×2^{30} 個の命令を実行することができる. 1 回のスカラー倍算を計算するのに 1 個の命令が必要だと仮定した場合, 2^{160} 回のスカラー倍算を計算するのに必要な時間を予想せよ. またその時間を算出せよ. なお 1 年は約 3×10^7 秒である.

コラム **数式処理ソフト**

2^{160} という値を計算しようと思っても, 暗算や筆算では太刀打ちできませんし, 計算できる電卓もなかなか見あたりません (ちなみに $2^{160} = 1461501637330902918203684832716283019655932542976$ です). 数式処理ソフトは, 計算機上でこのような計算を実現してくれるソフトであり, 暗号の研究をする上では欠かせないツールです. Mathematica や Maple は有名な数式処理ソフトですが, 値段が高価であるため, なかなか個人で購入するわけにはいきません. これに対して Risa/Asir はフリーの数式処理ソフトですが, 個人でいろいろ実験するには十分の機能を持っています.

2.3 Baby-step Giant-step 法

楕円曲線離散対数問題を解くのに, **Baby-step Giant-step 法 (Baby-step Giant-step method)** という総当たり法よりも優れたアルゴリズムがあります.

楕円曲線離散対数問題 $Q = d \times P$ に対し, ベースポイント P の点位数 ℓ を用いて $m = \lfloor \sqrt{\ell} \rfloor$ と定めます ($\lfloor x \rfloor$ は x の小数点以下を切り捨てた整数を表します). このとき $d = sm + t$ $(0 \leq s,\ t < m)$ と表すことができますので, $s,\ t$ が求めれば d を求められます. ではどうやって $s,\ t$ を求めればよいでしょうか.

さらに $R = m \times P$ とおくと,

$$Q = d \times P = (sm + t) \times P = s \times (m \times P) + t \times P = s \times R + t \times P$$

となりますので, $s,\ t$ は

$$Q - t \times P = s \times R \tag{2.1}$$

という関係式を満たしているはずです. そこで 2 種類のデータベースとして

$$Q,\ Q - P,\ Q - 2 \times P,\ Q - 3 \times P, \ldots,\ Q - (m-1) \times P$$

と

$$\mathcal{O},\ R,\ 2 \times R,\ 3 \times R, \ldots,\ (m-1) \times R$$

を計算し, それぞれを x 座標の小さい順に並べておきます. もしも 2 つのデータベースに同じ点が見つかった場合, 対応する値が $s,\ t$ として得られ, 目標の d を求められることになります.

それぞれのデータベースを作るには m 回ずつのスカラー倍算を必要としますので, 全体では $2m$ 回, つまり $2\sqrt{\ell}$ 回程度のスカラー倍算が必要です.

演習 2.4 Baby-step Giant-step 法を用いると, ℓ が 160 ビットの場合の楕円曲線離散対数問題を解くのに必要なスカラー倍算の回数は 2^{81} 回程度となる. 演習 2.3 と同性能の計算機を使用した場合, 2^{81} 回のスカラー倍算を計算するのに必要な時間を予想するとともに, その時間を算出せよ. なお 1 年は約 3×10^7 秒である. さらに, Baby-step Giant-step 法が使用するデータベースの大きさを予想し, そのサイズを算出せよ.

コラム　計算の限界値

暗号の研究では,「2° 回」という値の計算可能性がよく話題になります. 以下は個人的な感覚ですが, 個人の計算の限界は $2^{30} \sim 2^{35}$ 回, 大学や会社などの組織による計算の限界値は $2^{40} \sim 2^{45}$ 回, インターネットを利用した計算の限界値は $2^{50} \sim 2^{55}$ 回といったところです.

2.4 ρ 法

楕円曲線離散対数問題を解くのに, **ρ 法 (ρ method)** という, Baby-step Giant-step 法よりも優れた解法があります.

楕円曲線離散対数問題 $Q = d \times P$ に対し, 何らかの方法で

$$s \times P + t \times Q = s' \times P + t' \times Q$$

となる整数 $s,\ t,\ s',\ t'$ $(s \neq s',\ t \neq t')$ が見つかったとします. このとき

$$(t - t') \times Q = (s' - s) \times P$$

つまり

$$Q = \frac{s' - s}{t - t'} \times P$$

となるので, この分数 $(s' - s)/(t - t')$ から楕円曲線離散対数問題の解 d を求めることができます. なお分数は $\bmod \ell$ での演算であることに注意して下さい (ℓ はベースポイント P の点位数).

例 2.5 素体 $\mathbb{F}_{229}$ 上の楕円曲線 $E : y^2 = x^3 + x + 44$ において, $P = (5, 116)$, $Q = (155, 166)$ に関する楕円曲線離散対数問題 $Q = d \times P$ を考えます. ここで点 P の点位数は $\ell = 239$ です.

このとき

$$26 \times P + 108 \times Q = 47 \times P + 188 \times Q = (9, 18)$$

となるので,

$$Q = \frac{47 - 26}{108 - 188} \times P = \frac{21}{-80} \times P = 176 \times P$$

より楕円曲線離散対数問題の解 $d = 176$ を得られます.

$R_i = s_i \times P + t_i \times Q$ と書くことにすると, ρ 法の目標は, $R_i = R_j$ となる点のペア $R_i,\ R_j$ を見つけることです. このような点のペアをコリジョンペアと呼びます.

コラム　誕生日の逆理 (バースデーパラドックス)

クラスの中から誕生日が同じである 2 人を見つけるには, 何人が必要でしょうか. 予想してみて下さい.

簡単な計算により, (365 の平方根程度の) 23 人いれば確率 1/2 で誕生日が同じである 2 人を見つけられることが証明できます. この人数はおそらくみなさんの予想よりも少なかったのではないでしょうか. 直感的な結論と理論的な結論に差が生じるような議論を逆理と呼ぶため, この誕生日に関する逆理を誕生日の逆理と呼びます. ρ 法の計算時間解析では, 誕生日の逆理が用いられています.

ρ 法は, 楕円曲線上の点をランダムに選んでいき, それらの中からコリジョンペアを探索するという戦略をとります. 楕円曲線上の点 R をもとにランダムな点を効率的に求めるために, 次のような関数 (Random Walk 関数) f を利用します.

$$f(R) = \begin{cases} R + M_0 & \text{if } x(R) \equiv 0 \pmod 4 \\ R + M_1 & \text{if } x(R) \equiv 1 \pmod 4 \\ R + M_2 & \text{if } x(R) \equiv 2 \pmod 4 \\ R + M_3 & \text{if } x(R) \equiv 3 \pmod 4 \end{cases}$$

ここで $x(R)$ は点 R の x 座標値を表します. ただし $M_i = u_i \times P + v_i \times Q$ は楕円曲線上からランダムに選ばれた点です.

例 2.6 例 2.5 の続きとして, 点 $R_0 = (39, 159) = 54 \times P + 175 \times Q$ に関数 f を繰り返し適用させると, 以下のような点が得られます. このとき R_9 と R_{21} がコリジョンペアになっています. ただし

$$M_0 = (135, 117) = 79 \times P + 163 \times Q \quad M_1 = (96, 97) = 206 \times P + 19 \times Q$$
$$M_2 = (84, 62) = 87 \times P + 109 \times Q \quad M_3 = (72, 134) = 219 \times P + 68 \times Q$$

です.

i	R_i	s_i	t_i	$x(R_i) \bmod 4$	i	R_i	s_i	t_i	$x(R_i) \bmod 4$
0	$(39, 159)$	54	175	3	16	$(197, 92)$	193	0	1
1	$(160, 9)$	34	4	0	17	$(211, 47)$	160	19	3
2	$(130, 182)$	113	167	2	18	$(194, 145)$	140	87	2
3	$(27, 17)$	200	37	3	19	$(0, 68)$	227	196	0
4	$(36, 97)$	180	105	0	20	$(223, 153)$	67	120	3
5	$(119, 180)$	20	29	3	21	$(9, 18)$	47	188	1
6	$(108, 89)$	0	97	0	22	$(167, 57)$	14	207	3
7	$(81, 168)$	79	21	1	23	$(75, 136)$	233	36	3
8	$(223, 153)$	46	40	3	24	$(57, 105)$	213	104	1
9	$(9, 18)$	26	108	1	25	$(159, 4)$	180	123	3
10	$(167, 57)$	232	127	3	26	$(185, 227)$	160	191	1
11	$(75, 136)$	212	195	3	27	$(158, 26)$	127	210	2
12	$(57, 105)$	192	24	1	28	$(197, 92)$	214	80	1
13	$(159, 4)$	159	43	3	29	$(211, 47)$	181	99	3
14	$(185, 227)$	139	111	1	30	$(194, 145)$	161	167	2
15	$(158, 26)$	106	130	2	31	$(0, 68)$	9	37	0

コラム　分割数

左で紹介した Random walk 関数 f は, ランダム性を向上させるために, 4 個に分割されていました. このパラメータを分割数と言います. ρ 法により大規模な離散対数問題を解く際には, 分割数が 20 程度の関数が使用されます.

誕生日の逆理によると, コリジョンペアを見つけるためには $\sqrt{\ell}$ 個の点を計算・保存する必要があります. そこで保存領域を節約するために, 点 R_i を保存するのは **特徴点 (distinguished point)** となる場合に限定することにします. ここで特徴点とは「その点の x 座標がある値 θ で割りきれる点」のことです. 特徴点を用いることで, 記憶すべき点の個数を $1/\theta$ に削減することができるのです.

特徴点だけを保存していく場合, コリジョンペアも特徴点同士で探索します. なお $R_i = R_j$ ならば

$$f(R_i) = f(R_j),\ f(f(R_i)) = f(f(R_j)),\ f(f(f(R_i))) = f(f(f(R_j))), \ldots$$

となりますので, 特徴点以外の点でコリジョンペアが存在すれば, 特徴点同士でもコリジョンペアが存在することがわかります.

例 2.7 例 2.6 において, 特徴点の定義を「x 座標の下 1 桁が 0 になっている」(つまり $\theta = 10$) とすると, $R_1 = (160, 9)$, $R_2 = (130, 182)$, $R_{19} = (0, 68)$, $R_{31} = (0, 68)$ が特徴点になっています.

このとき R_{19} と R_{31} がコリジョンペアになっているので,

$$R_{19} = 227 \times P + 196 \times Q = 9 \times P + 37 \times Q = R_{31}$$

という関係式から楕円曲線離散対数問題の解 $d = 176$ を求めることができます.

ρ 法は, $\sqrt{\ell}$ 回のスカラー倍算を必要とするため, Baby-step Giant-step 法と同程度の計算時間を必要とします. しかし保存すべき点の個数は $\sqrt{\ell}/\theta$ となり, Baby-step Giant-step 法よりも少なくて済むというメリットがあります.

なお楕円曲線離散対数問題に対しては, ρ 法が最も優れていることが経験的に知られていますが, もっと優れた解法が登場することが否定されているわけではありません. 実際, 量子計算機と呼ばれる計算機が実現された場合, 楕円曲線離散対数問題に対する効率的な解法が既に知られています.

コラム **Certicom**

Certicom 社とはカナダの Waterloo 大学の Scott Vanstone が 1985 年に設立した暗号のベンチャー会社で, 楕円曲線暗号の草分けとして有名です (最近, やはり Waterloo 大学発のベンチャー会社である RIM 社に買収されました). Certicom 社は古くから楕円曲線暗号の標準化を積極的に推進し, 利用分野の拡大に貢献してきています.

2.5 楕円曲線離散対数問題の最前線

これまでに解かれた楕円曲線離散対数問題の記録を以下にまとめます. これら記録は, 全て ρ 法によって達成されています. (Certicom Challenge については右ページのコラムを参照して下さい.)

成功日	問題のサイズ	備考
1997 年 12 月	79 ビット	Certicom Challenge
1998 年 01 月	89 ビット	Certicom Challenge
1998 年 03 月	97 ビット	Certicom Challenge
2002 年 10 月	109 ビット	Certicom Challenge
2009 年 07 月	112 ビット	

2009 年 7 月に解かれた 112 ビット楕円曲線離散対数問題の具体的なパラメータは以下の通りです.

$$
\begin{aligned}
p &= (2^{128} - 3)/(11 \cdot 6949) \\
a &= 4451685225093714772084598273548424 \\
b &= 2061118396808653202902996166388514 \\
\#E &= 4451685225093714776491891542548933 \\
x_P &= 188281465057972534892223778713752 \\
y_P &= 341987549103317082716786189608268 8 \\
\ell &= 4451685225093714776491891542548933 \\
x_Q &= 1415926535897932384626433832795028 \\
y_Q &= 3846759606494706724286139623885544 \\
d &= 3125216360147724771617673518566 99
\end{aligned}
$$

なお点 Q の x 座標値は $\lfloor (\pi - 3) \times 10^{34} \rfloor$ となっており, 解かれた楕円曲線離散対数問題のパラメータが恣意的でないことを保証しています.

112 ビットの楕円曲線離散対数問題の解読では, ソニー・コンピュータエンタテインメント社の PlayStation 3 というゲーム機が 200 台以上使用されたことが話題になりました. 実際の計算は, 2009 年の 1 月から 7 月までの約半年が必要だったとのことです.

コラム **Certicom Challenge**

Certicom 社は, 楕円曲線離散対数問題の何問かの懸賞問題をインターネットで公開しており, サイズに応じて賞金も大金になっています. このうち難問かは既に解かれていますが, 残りについては現在もチャレンジが行われています. ちなみに最も難しい 359 ビットのパラメータを解いた場合の賞金は 100,000 ドルで, 驚くほどの大金ではありませんが, この問題が解けた場合に得られる名声はお金に代えられませんので, 賞金自体にはあまり意味はないと考えるべきなのでしょう.

2.6 特別な楕円曲線離散対数問題の解法

一般的な楕円曲線離散対数問題に対しては, ρ 法が最も優れていることは説明しました. しかし特殊な楕円曲線離散対数問題に対しては, もっと優れた解法が知られています.

2.6.1 Menezes-Okamoto-Vanstone による解法

カナダの Waterloo 大学の Alfred Menezes, Scott Vanstone と NTT の Tatsuaki Okamoto は, 素体 $\mathbb{F}_p$ 上の楕円曲線の群位数が $p+1$ になる場合 (Supersingular 曲線), その曲線上での楕円曲線離散対数問題が簡単に解けることを示しました.

演習 2.8 表 1.8 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線のうち, Supersingular 曲線を全て示せ. また, (この場合の) Supersingluar 曲線の係数に共通する特徴を指摘せよ.

2.6.2 Semaev-Smart-Satoh-Araki による解法

ロシアの Igor Semaev, イギリスの Bristol 大学の Nigel Smart, 東工大の Takakazu Satoh と Kiyomichi Araki は, 素体 $\mathbb{F}_p$ 上の楕円曲線の群位数が p になる場合 (Anomalous 曲線), その曲線上での楕円曲線離散対数問題が簡単に解けることを独立に示しました.

例 2.9 表 1.8 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線のうち, Anomalous 曲線を全て示せ.

コラム **ペアリング**

Menezes-Okamoto-Vanstone による楕円曲線離散対数問題の解法では, 楕円曲線上の点を別の乗法群の要素に変換し, 乗法群での離散対数問題を解くことで, もとの楕円曲線離散対数問題を解くという手法をとります. 変換は **ペアリング (pairing)** という写像によって実現されます.

ペアリングとは, 楕円曲線上の 2 点から乗法群への写像 $e : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \to G$ であって, 楕円曲線上の点 $P,\ P',\ Q,\ Q'$ に対し, $e(P + P', Q) = e(P, Q) \cdot e(P', Q)$, $e(P, Q + Q') = e(P, Q) \cdot e(P, Q')$ という性質が成り立ちます. このため, ペアリングを **双線型写像 (bilinear map)** と呼ぶこともあります.

暗号分野では, ペアリングはこのように楕円曲線離散対数問題を解くためのツールとして使用されていましたが, 近年になって, ID ベース暗号などの新しい暗号を構成するためのツールとしても広く使用されるようになっています.

この章のまとめ

- 楕円曲線離散対数問題とは, 与えられた楕円曲線上の点 P, Q から $Q = d \times P$ となるスカラー d を求める問題である.
- 楕円曲線離散対数問題の解法として, 総当たり法, Baby-step Giant-step 法, ρ 法がある. このうち最も優れているのは ρ 法である.

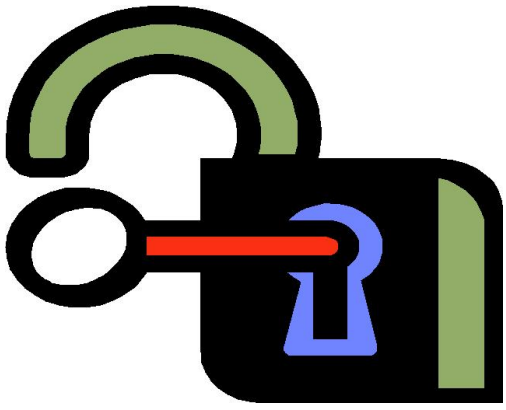
[おまけコラム]

楕円曲線暗号の研究は世界的にさまざまな研究者によって進められていますが, 日本の場合, その研究者の多くが企業に所属しているという特徴があります. これは, 楕円曲線暗号が数学的な性質と工学的な性質を兼ね備えており, 企業の研究所のような広く浅くの研究スタイルがこの性質に合致していたのが原因でしょう. しかし近年では研究に必要となる知識が深くなっているため, 大学でも盛んに研究されるようになっています.

第 3 章

楕円曲線暗号

本章では, 楕円曲線暗号のいくつかの具体的なアルゴリズムを紹介します. どのアルゴリズムでも楕円曲線離散対数問題の困難性が暗号の安全性の根拠となっています.



3.1 **楕円曲線暗号** (ECC)

前章で紹介した通り, 楕円曲線離散対数問題は一般には解くことが難しい問題として知られています. このような楕円曲線離散対数問題の難しさを利用した公開鍵暗号の総称を **楕円曲線暗号 (elliptic curve cryptosystems, ECC)** と呼びます. 楕円曲線離散対数問題の困難性は楕円曲線暗号の安全性の根拠となっています.

楕円曲線暗号にはさまざまなアルゴリズムが知られています. 機能で分類したときの具体的な方式例を表 3.1 にまとめます (これで全てというわけではありません).

楕円曲線暗号の特徴として, 使用する鍵のサイズが他の暗号に比べて小さいことが挙げられます. 例えば公開鍵暗号の標準として RSA 暗号が知られていますが, 現在の標準的な RSA 暗号は 1024 ビットの鍵を使用します. この RSA 暗号と同じ安全性を確保する場合, 楕円曲線暗号の鍵 (つまりスカラー d) のサイズは 160 ビットで良いことが知られています. 従って楕円曲線暗号は, 組み込みデバイスのように計算資源が制限されている環境に向いています.

例 3.1 楕円曲線暗号のパラメータ例を以下に示します. ここで楕円曲線は素体 $\mathbb{F}_p$ 上で定義され, 定義方程式は $E : y^2 = x^3 + ax + b$ で与えられているとします. またベースポイントを $P = (x_P, y_P)$ とし, その点位数を ℓ としています. なおこのパラメータは実際の楕円曲線暗号で使用されています.

$$
\begin{aligned}
p &= 2^{160} - 2^{31} - 1 \\
&= 1461501637330902918203684832716283019653785059327 \\
a &= -3 \\
&= 1461501637330902918203684832716283019653785059324 \\
b &= 163235791306168110546604919403271579530548345413 \\
\#E &= 1461501637330902918203687197606826779884643492439 \\
x_P &= 425826231723888350446541592701409065913635568770 \\
y_P &= 203520114162904107873991457957346892027982641970 \\
\ell &= 1461501637330902918203687197606826779884643492439
\end{aligned}
$$

表 3.1　楕円曲線暗号の具体的な方式の例

機能	方式名
鍵交換	楕円曲線 Diffie-Hellman 鍵交換 (ECDH)
	楕円曲線 Menezes-Qu-Vanstone 鍵交換 (ECMQV)
暗号	楕円曲線 ElGamal 暗号 (ECElGamal)
署名	楕円曲線 DSA 署名 (ECDSA)

コラム　暗号と暗号

暗号という単語には, スクランブルをかけるという意味の「暗号」(encryption) と, スクランブル・鍵交換・署名などのアルゴリズムを総称した「暗号」(cryptsystem) という 2 つの意味があります. 楕円曲線暗号という単語は後者の意味で使われていますが, 誤解されたり誤用されたりしている場面も多いです. そこで後者の意味 (cryptsystem の意味) で使いたい場合には, 「暗号系」という単語を使用します.

3.2 ECDH 鍵交換

インターネット上で相手と共通鍵暗号によって暗号化通信をする場合, 使用する暗号鍵を事前に交換 (共有) する必要があります. 本節では, 楕円曲線を用いた鍵交換法として, 楕円曲線 Diffie-Hellman 鍵交換 (ECDH 鍵交換) を紹介します.

方式 3.2 (ECDH 鍵交換) Alice と Bob は, 素体 $\mathbb{F}_p$ 上の楕円曲線 E と曲線上のベースポイント P を共通のパラメータとして知っているとする. 以下のように Alice と Bob がやりとりすることで, 2 人は共通の鍵 $K_A = K_B$ を共有する.

1. Alice は乱数 d_A を生成し, スカラー倍点 $P_A = d_A \times P$ を Bob に送る.
2. Bob は乱数 d_B を生成し, スカラー倍点 $P_B = d_B \times P$ を Alice に送る.
3. 点 P_B を受け取った Alice は点 $K_A = d_A \times P_B$ を計算し, 暗号鍵として用いる.
4. 点 P_A を受け取った Bob は点 $K_B = d_B \times P_A$ を計算し, 暗号鍵として用いる.

演習 3.3 演習 1.7 で調べた素体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ において $P = P_1$ とするとき, $d_A = 2$, $d_B = 3$ としたときの次の値を求めよ.

$$P_A = \qquad K_B =$$
$$P_B = \qquad K_A =$$

演習 3.4 ECDH 鍵交換において, Alice の鍵 K_A と Bob の鍵 K_B が等しくなっていることを証明せよ.

ECDH 鍵交換への攻撃方法を考えてみましょう. 攻撃者 Carol は, Alice と Bob が ECDH 鍵交換を用いていること, その共通のパラメータ $\mathbb{F}_p$, E, P を知っているとします. また Alice と Bob のやりとりから P_A, P_B も入手できているものとします. このとき P_A, P から d_A を, あるいは P_B, P から d_B を求める問題は楕円曲線離散対数問題そのものであり, Carol は d_A, d_B を求めることができません. このようにして ECDH 鍵交換の安全性は楕円曲線離散対数問題の困難性に基づいていることがわかります.

コラム **楕円曲線 Diffie-Hellman 問題 (ECDH 問題)**

$P_A = d_A \times P$, $P_B = d_B \times P$ であるとき, P_A, P_B, P から $K = d_A \times d_B \times P$ を求める問題を楕円曲線 Diffie-Hellman 問題 (ECDH 問題) と言います.

ECDH 問題は楕円曲線離散対数問題よりも簡単な問題です. というのも, 楕円曲線離散対数問題を解くことができる攻撃者は P_A, P から d_A を求め, $K = d_A \times P_B$ を計算することで, ECDH 問題を解くことができるからです. しかし ECDH 問題を解くことができる攻撃者がいたとしても, d_A, d_B を求めずに K を求めた可能性もありますから, 楕円曲線離散対数問題を解けることには直結しません.

このように ECDH 鍵交換の安全性は, 楕円曲線離散対数問題の困難性だけでなく, ECDH 問題の困難性にも依存しています.

3.3 ECElGamal 暗号

ECDH 鍵交換を拡張すると, ECElGamal 暗号という公開鍵暗号方式を実現することができます.

方式 3.5 (ECElGamal 暗号) Alice と Bob は, 素体 $\mathbb{F}_p$ 上の楕円曲線 E と曲線上のベースポイント P を共通のパラメータとして知っているとする. 以下のように Alice が Bob に暗号文を送信することで, Bob はメッセージ M を受信することができる.

1. あらかじめ Bob は乱数 d_B を生成し, スカラー倍 $P_B = d_B \times P$ を計算する. そして P_B は公開鍵として公開し, d_B は秘密鍵として保管する.
2. Alice による暗号化
   (a) 乱数 r を生成し, スカラー倍 $P_A = r \times P$ を計算する.
   (b) Bob の公開鍵 P_B を入手し, スカラー倍 $K = r \times P_B$ を計算する.
   (c) 楕円曲線上の点として表されたメッセージ M に対し, $C = M + K$ を計算する.
   (d) Bob に暗号文 C と点 P_A を送る.
3. Bob によるメッセージの復号
   (a) 点 P_A と秘密鍵 d_B から, スカラー倍 $K = d_B \times P_A$ を計算する.
   (b) $M = C - K$ を計算し, メッセージ M を入手する.

演習 3.6 ECElGamal 暗号では, Alice が計算したスカラー倍点 K と Bob が計算したスカラー倍点 K は等しくなる. この理由を考察せよ.

コラム　楕円曲線暗号の発明者

楕円曲線暗号は, 1985 年頃に米 IBM の Victor Miller と米 Washington 大学の Neal Koblitz によって独立に提案されました. このように暗号の世界では, 同時期に同じアイディアが考案されるというケースが良く見られます.

3.4 ECDSA 署名

楕円曲線上の署名方式の例として, ECDSA 署名を紹介します.

方式 3.7 (ECDSA 署名) Alice と Bob は, 素体 $\mathbb{F}_p$ 上の楕円曲線 E と曲線上のベースポイント P とその点位数 ℓ を共通のパラメータとして知っているとする. 以下のように Alice が Bob に署名を送ることで, Bob はメッセージ m の内容が改竄されていないことを検証できる.

1. あらかじめ Alice は乱数 d_A $(1 \leq d_A \leq \ell)$ を生成し, スカラー倍 $P_A = d_A \times P$ を計算する. そして P_A は公開鍵として公開し, d_A は秘密鍵として保管する.
2. Alice による署名生成
   (a) 乱数 r を生成し, スカラー倍 $U = r \times P = (x_U, y_U)$ を計算する.
   (b) メッセージ m のハッシュ値 $H(m)$ を計算する.
   (c) $u = x_U \bmod \ell,\ v = (H(m) + u \times d_A)/r \mod \ell$ を計算する.
   (d) Bob に署名 (u, v) を送る.
3. Bob による署名検証
   (a) Alice の公開鍵 P_A をもとに, $d = 1/v \bmod \ell$ と点 $V = d \times H(m) \times P + d \times u \times P_A = (x_V, y_V)$ を計算する.
   (b) $u = x_V \bmod \ell$ ならば署名を受理する.

ここでハッシュ関数という関数が登場しますが, これはメッセージの特徴を計算する関数であり, 特徴からメッセージが復元できないという性質を持っています.

演習 3.8 ECDSA 署名の署名検証で, 正しく検証できる理由を考察せよ.

コラム **DTCP**

テレビ送信のディジタル化にあわせ, テレビや録画機のディジタル化が急速に進んでいます. これらディジタル機器での映像コンテンツの無尽蔵な複製を防ぐため, DTCP (Digital Transmission Content Protection) という技術によって, 機器やコンテンツの管理を行っています. DTCP では, 鍵交換部分に ECDH が, 機器認証やコンテンツ認証部分に ECDSA が使用されています.

3.5 安全な楕円曲線暗号のパラメータ

楕円曲線暗号を使用するには, 楕円曲線の係数などのパラメータを設定する必要がありますが, 楕円曲線離散対数問題が解けないようなパラメータを使用する必要があります.

第 2 章で紹介した総当たり法, Baby-step Giant-step 法, ρ 法の攻撃時間はベースポイントの点位数 ℓ によって定まります. そこで ℓ を大きく設定することで, これらの解法を回避することが可能です.

具体的には, 以下のようにして安全な楕円曲線暗号のパラメータを生成します.

方式 3.9 (安全な楕円曲線パラメータの生成) 以下のようにして素体 $\mathbb{F}_p$ 上の安全な楕円曲線 E とベースポイント P が得られる.

1. 素数 p のサイズを決定し, p を求める.
2. ランダムに $a,\ b \in \mathbb{F}_p$ を生成し, 楕円曲線 $E(a,b) : y^2 = x^3 + ax + b$ の群位数を求める. (Hasse-Weil の定理により, この群位数は $p+1-2\sqrt{p} \leq \#E(a,b) \leq p+1+2\sqrt{p}$ を満たす).
3. $\#E(a,b)$ が素数でなければ 2. へ戻る.
4. $\#E(a,b) = p$ ならば 2. へ戻る (Anomalous 曲線の排除).
5. 楕円曲線 $E(a,b)$ 上のベースポイント P をランダムに選ぶ.

演習 3.10 上のアルゴリズムでは Supersingular 曲線に関するチェックをしていない. その理由を考察せよ.

演習 3.11 上のアルゴリズムの 3. では, 群位数が素数でない楕円曲線を排除している. その理由を考察せよ.

コラム **NIST 曲線**

本節では安全な楕円曲線パラメータの生成法を紹介しましたが, 現在の楕円曲線暗号では, 標準的な楕円曲線暗号パラメータは既に定められており, ユーザがいちいち生成する必要はありません. 中でも NIST 曲線は有名な楕円曲線暗号パラメータとして知られています.

この章のまとめ

- 楕円曲線暗号 (ECC) とは楕円曲線離散対数問題を利用したアルゴリズムの総称で, 鍵交換・暗号 (スクランブル)・鍵交換・署名などの機能を持っている.

[おまけコラム]

本章で説明した楕円曲線暗号アルゴリズムが実際に電子機器などに組み込まれて使用されるには, どのようなアルゴリズムをどのような場面で使用するべきかを議論され, 誰がプログラムを組んでも必ず同じになるようなレベルまで詳細に記述した文書を用意する必要があります. このようなプロセスは通常, 標準化と呼ばれます. 楕円曲線暗号の場合, ANSI (米国規格協会), IEEE (電気電子学会), ISO (国際標準化機構), NIST (米国標準技術局), CRYPTREC (電子政府向け推奨暗号策定プロジェクト) などの機関による標準化が進められています. このため, われわれの気づかないような場面で楕円曲線暗号が使用されるようになっています.

参考文献

参考までに, 楕円曲線暗号に関する文献を紹介します. 高校生でも理解できるような入門書から研究者が読むような専門書まで集めてありますが, 必要に応じて選択して下さい.

数学

公開鍵暗号や楕円曲線暗号を深く知るには, 群や体に関する理論 (代数学) を知る必要があります. 以下の 2 冊は代数学への良い入門書であり, シリーズ名の通り現代数学への良き入門書にもなっています.

- 上野 健爾, 代数入門 (現代数学への入門), 岩波書店, 2004 年 5 月.
- 山本 芳彦, 数論入門 (現代数学への入門), 岩波書店, 2003 年 11 月.

実際の公開鍵暗号や楕円曲線暗号を考察するには, 数学的な定理をどのようにして計算機上でプログラムすれば良いかという視点が必要になります. 以下の 3 冊は代数学の教科書ですが, 常に計算機的な視点が意識されています. 特に 3 冊目は, 計算機数学と呼ばれる分野の入門書として有名であり, 著者は暗号の研究者としても活躍しています.

- 木田 祐司, 初等整数論, 朝倉書店, 2001 年 11 月.
- Joseph Silverman, “A Friendly Introduction to Number Theory (3rd edition)”, Pearson Prentice Hall, 2006
  [鈴木 治郎, はじめての数論 (原著第 3 版), ピアソン・エデュケーション, 2007 年]
- Victor Shoup, “A Computational Introduction to Number Theory and Algebra (1st edition)”
  [著者のウェブページから PDF 版のダウンロード可能です: `http://shoup.net/ntb/`]

また以下は暗号学習のために必要な数学を簡潔にまとめています.

- Jeffrey Hoffstein, Jill Pipher, Joseph Silverman, “An Introduction to Mathematical Cryptography”, Springer-Verlag, 2008

暗号

暗号は情報セキュリティを支える基礎技術ですが, その機能や応用は想像もできない位に広がっており, 全貌が見えにくい状況になっています. 以下の 3 冊はその様子をなるべく専門用語を用いずに紹介しており, 一通りの内容を知るには良い入門書となっています.

- 伊藤 正史, 図解雑学 暗号理論, ナツメ社, 2003 年 3 月
- 岡本 龍明, 図解 暗号と情報セキュリティ, 日経 BP 社, 1998 年 7 月
- 今井 秀樹 (編), トコトンやさしい暗号の本, ナツメ社, 2010 年 4 月

現在の暗号学を系統的に学習するには, 次の 2 冊が良いと思います (暗号学は比較的進展の早い分野ですので, 新しい教科書の方が一般的には良いと言えるでしょう).

- 結城 浩, 新版 暗号技術入門 〜 秘密の国のアリス, ソフトバンクパブリッシング, 2008 年 11 月
- 黒澤 馨, 尾形 わかは, 現代暗号の基礎数理, コロナ社, 2004 年 3 月

以下は楕円曲線暗号の教科書です. 2 冊目は楕円曲線理論から暗号まで広い内容が網羅させています. 3 冊目は楕円曲線暗号の実装面を丁寧に説明しており, 楕円曲線暗号の現実を知るには最適なテキストです. 4 冊目は楕円曲線暗号以外のトピックも扱っていますが, 楕円曲線暗号の記述がコンパクトにまとめられています.

- Neal Koblitz, “A Course in Number Theory and Cryptography (2nd edition)”, Springer-Verlag, 1994
  [櫻井 幸一訳, 数論アルゴリズムと楕円暗号理論入門 (原著第 2 版), シュプリンガー・フェアラーク東京, 1997 年 8 月]
- Ian Blake, Gadiel Seroussi, Nigel Smart, “Elliptic Curves in Cryptography”, Cambridge University Press, 2000
  [鈴木 治郎, 楕円曲線暗号, ピアソン・エデュケーション, 2001 年]
- Darrel Hankerson, Alfred Menezes, Scott Vanstone, “Guide to Elliptic Curve Cryptography”, Springer, 2002
- 辻井 重男, 笠原 正雄 (編, 著), “暗号理論と楕円曲線”, 森北出版, 2008 年 8 月

楕円曲線暗号上で定義されるペアリングという写像を用いると, 新しい機能を持った暗号 (例: ID ベース暗号) を構成できることが知られています. 以下のテキストは ID ベース暗号に焦点を絞った入門書です.

- Luther Martin, “Introduction to Identity-Based Encryption”, Artech House, 2008

最新の研究成果を知るには

楕円曲線暗号はとても活発に研究が進められているため, 最新の成果を知るには, 学会で発表される論文のチェックが必要になります.

国内の場合, 本資料が扱ったような楕円曲線暗号に関する研究は, 以下の研究会で多く報告されています.

- 電子情報通信学会 情報セキュリティ (ISEC) 研究会 [2 ヶ月に 1 回 の頻度で開催]
- 応用数理学会 数論アルゴリズム (JANT) 研究会 [3 ヶ月に 1 回 の頻度で開催]

また, ISEC 研究会が主催する以下のシンポジウムでは, 毎回 300 件以上の研究成果が報告されています.

- 暗号と情報セキュリティシンポジウム (SCIS) [年に 1 回の頻度で開催]

海外では, 国際暗号研究学会 (IACR) が開催する以下の国際会議で楕円曲線暗号に関する研究成果が報告されています

- CRYPTO
- EUROCRYPTO
- ASIACRYPTO
- PKC

また以下のような, 楕円曲線暗号に焦点を絞ったワークショップも毎年開催されています.

- Workshop on Elliptic Curve Cryptography (ECC)