構造の数理 (講義ノート)

桔梗宏孝

暗号や符号では有限の代数構造が重要になっている。整数や多項式をもとに組織的に代数構造が構成される様子を味わってほしい。

1　整数

1.1　合同式

普通の時計において，12 時から針を 3 時間進めても 15 時間進めても 3 時を指している。また，9 時間逆にまわしても 3 時である。一般に，12 時から x 時間 (x は整数で，正でも負でもよい) 進めると，x を 12 で割った余りの時間を指している。ただし，余り 0 の場合は 12 である。現在よく使われている暗号や符号では，この「余りの世界」が使われている。

定理 1.1.1（割り算の原理） 任意の整数 x に対し，

$$x = 12q + r, \quad 0 \leq r < 12$$

となる q と r がちょうど 1 組存在する。

さらに一般に，$N > 0$ とすると

$$x = Nq + r, \quad 0 \leq r < N$$

となる q と r がちょうど 1 組存在する。

q を x/N の商，r を余りと呼ぶ。r を $x \bmod N$ とも書く。

たとえば，$15 \bmod 12 = 3$, $3 \bmod 12 = 3$, $-9 \bmod 12 = 3$ である。

定義 1.1.2（法 N の合同） $N \neq 0$ を整数とする。整数 x, y に対し，$x - y$ が N の整数倍のとき $x \equiv y \pmod{N}$ と書き，x と y は**法 N で合同**，あるいは mod N で合同という。

mod N の合同という関係についての基本的な性質をまとめておく。

命題 1.1.3 N, x, y は整数で，$N > 0$ とする。

(1) $x \equiv x \pmod{N}$
(2) $x \equiv y \pmod{N}$ ならば $y \equiv x \pmod{N}$
(3) $x \equiv y \pmod{N}$, $y \equiv z \pmod{N}$ ならば $x \equiv z \pmod{N}$

証明. (3) だけ示す。$x \equiv y \pmod{N}$, $y \equiv z \pmod{N}$ と仮定する。すると，$x-y$ と $y-z$ は共に N の整数倍である。すると，$x-z = (x-y)+(y-z)$ より，$x - z$ も N の整数倍である。 □

命題 1.1.4 N, x, y, m は整数で，$N > 0$ とする。

(1) $x \equiv y \pmod{N} \iff x \bmod N = y \bmod N$
(2) $x \equiv y \pmod{N} \Rightarrow mx \equiv my \pmod{N}$
(3) $m \neq 0$ のとき，$x \equiv y \pmod{N} \iff mx \equiv my \pmod{mN}$
(4) $x \equiv y \pmod{mN} \Rightarrow x \equiv y \pmod{N}$

証明. (1) $x \equiv y \pmod{N}$ と仮定する。$x = q_1N + r_1$, $y = q_2N + r_2$ とする。$r_1 \geq r_2$ と仮定してよい。そうでなければ，$x-y = (q_1-q_2)N+(r_1-r_2)$. $x-y$ が N の整数倍なので，r_1-r_2 も N の整数倍。しかし，$0 \leq r_1-r_2 < N$ なので，$r_1 - r_2 = 0$. よって，$x \bmod N = r_1 = r_2 = y \bmod N$.

(2) $x - y$ が N の整数倍ならば，$mx - my = m(x - y)$ も N の整数倍。

(3) ($\Rightarrow$) $x \equiv y \pmod N$ と仮定する。すると，$x - y = qN$ (q:整数) と書ける。すると，$m(x-y) = mqN$．よって，$mx - my$ は mN の整数倍。

($\Leftarrow$) $mx \equiv my \pmod{mN}$ と仮定する。すると，$mx - my = qmN$ (q:整数) と書ける。すると，$m(x-y) = mqN$．$m \neq 0$ なので，$x - y = qN$．よって，$x - y$ は N の整数倍。

(4) mN の整数倍は N の整数倍になっている。 □

mod N で合同という概念は整数の足し算とかけ算との相性がよい。

命題 1.1.5 $x \equiv x' \pmod N$ かつ $y \equiv y' \pmod N$ ならば,

$$x + y \equiv x' + y' \pmod N, \quad xy \equiv x'y' \pmod N$$

証明. $x \equiv x' \pmod N$ かつ $y \equiv y' \pmod N$ と仮定する。すると，$x - x'$ と $y - y'$ は共に N の整数倍である。

$$(x + y) - (x' + y') = (x - x') + (y - y')$$

より，これも N の整数倍。よって，$x + y \equiv x' + y' \pmod N$.

また,

$$xy - x'y' = xy - x'y + x'y - x'y' = (x - x')y + x'(y - y')$$

より，これも N の整数倍。よって，$xy \equiv x'y' \pmod N$. □

1.2 最大公約数とユークリッドの互除法

定義 1.2.1（約数，公約数） 整数 m, d に対し，m が d の整数倍のとき，d を m の**約数**と呼ぶ。d が m の約数かつ d が n の約数のとき，d を m と n の**公約数**と呼ぶ。m と n の公約数のうち最大のものを $\gcd(m, n)$ と書き，m と n の**最大公約数**と呼ぶ。

定理 1.2.2（ユークリッドの互除法） $m, n > 0$ が整数で，

$$m = qn + r$$

とすると

(1) $r = 0$ のとき，$\gcd(m, n) = n$
(2) $r \neq 0$ のとき，$\gcd(m, n) = \gcd(n, r)$

証明. (1) $n > 0$ なので，n の約数の最大値は n．一方，$r = 0$ より，n の約数は m の約数でもある。したがって，$\gcd(m, n) = n$.

(2) d を任意の整数とする。d が m と n を同時に割り切ることと d が n と r を同時に割り切ることが同値なことがすぐにわかる。

したがって，m と n の公約数の集合と n と r の公約数の集合は一致する。よって，その最大値も一致する。 □

正の整数 m と n の最大公約数は次のようにして求まる。

(1) $r := m \bmod n$ を計算。$(0 \leq r < n$ である$)$
(2) $r = 0$ の場合は，n が最大公約数。
(3) $r > 0$ の場合は，n と r の最大公約数が求めるもの。
すなわち，$m := n$; $n := r$ として，(1) へもどる。

例 1.2.3 2109 と 1653 の最大公約数を求める。

引けるだけ引いた残りが余りであることに注意。

$$\begin{array}{rcrcr} 2109 & - & 1653 & = & 456 \\ 1653 & - & 456 \times 3 & = & 285 \\ 456 & - & 285 & = & 171 \\ 285 & - & 171 & = & 114 \\ 171 & - & 114 & = & 57 \\ 114 & - & 57 \times 2 & = & 0 \end{array}$$

57 が求める最大公約数。

$$\begin{aligned} & \gcd(2109, 1653) = \gcd(1653, 456) = \gcd(456, 285) \\ = \quad & \gcd(285, 171) = \gcd(171, 114) = \gcd(114, 57) = 57 \end{aligned}$$

問 1.2.4　次の問に答えよ。

1. 2257 mod 1073 を計算せよ (2257 ÷ 1073 の余り)。
2. 2257 と 1073 の最大公約数を求めよ。

上の例 1.2.3 で，2 番目の式の左辺の 456 を 1 番目の式の左辺で置き換えると

$$1653 - (2109 - 1653) \times 3 = 285$$

すなわち，

$$1653 \times 4 - 2109 \times 3 = 285$$

$$456 - 285 = 171$$

の 456 と 285 を 2109 と 1653 の整数倍の和で置き換えると，171 も 2109 と 1653 の整数倍の和になることがわかる。

同様に，114 も 2109 と 1653 の整数倍の和になり，57 も 2109 と 1653 の整数倍の和になる。

このことを一般に議論すれば，次の命題を得る。

命題 1.2.5　$m, n \neq 0$ を整数とすると

$$mx + ny = \gcd(m, n)$$

となる整数 x, y が存在する。

この命題は次のような等式を考え，右辺に対してユークリッドの互除法を適用することでも示せる。x, y も 1 組求まる。

$$
\begin{array}{llllll}
(1) & 2109 \cdot 1 & +1653 \cdot 0 & = & 2109 & \text{当然の式} \\
(2) & 2109 \cdot 0 & +1653 \cdot 1 & = & 1653 & \text{当然の式} \\
(3) & 2109 \cdot 1 & +1653 \cdot (-1) & = & 456 & (1) - (2) \\
(4) & 2109 \cdot (-3) & +1653 \cdot 4 & = & 285 & (2) - (3) \times 3 \\
(5) & 2109 \cdot 4 & +1653 \cdot (-5) & = & 171 & (3) - (4) \\
(6) & 2109 \cdot (-7) & +1653 \cdot 9 & = & 114 & (4) - (5) \\
(7) & 2109 \cdot 11 & +1653 \cdot (-14) & = & 57 & (5) - (6)
\end{array}
$$

$\gcd(m, n) = 1$ となるときが重要である。

定義 1.2.6　$m, n \neq 0$ とする。$\gcd(m, n) = 1$ のとき，m と n は**互いに素**であるという。

命題 1.2.7　$m, n > 0$ を整数とすると次の条件は同値である。

(1)　m と n は互いに素。
(2)　$mx + ny = 1$ となる整数 x, y が存在する。
(3)　$mx \equiv 1 \pmod{n}$ となる整数 x が存在する。
(4)　$nx \equiv 1 \pmod{m}$ となる整数 x が存在する。

証明.　(1) $\Rightarrow$ (2) は命題 1.2.5 による。

(2) $\Rightarrow$ (1). $d = \gcd(m, n)$ とする。(2) を仮定すると d は m, n を割り切るから $mx + ny$，すなわち 1 を割り切る。$d > 0$ より，$d = 1$.

(2) $\Rightarrow$ (3). $mx + ny = 1$ とする。$ny \equiv 0 \pmod{n}$ より，$mx \equiv 1 \pmod{n}$.

(3) $\Rightarrow$ (2). $mx \equiv 1 \pmod{n}$ とする。すると，$mx - 1 = qn$ となる整数 q がある。すなわち，$mx + n(-q) = 1$.

(2) と (4) の同値性も同様である。　□

定義 1.2.8　$N > 0$ を整数とする。整数 m に対し，$mx \equiv 1 \pmod{N}$ となる整数 x を **mod N の m の逆元** (あるいは**逆数**) と呼ぶ。正確には，**乗法の逆元**と呼ぶ。このとき，とくに $x \bmod N$ (x を N で割った余り，$0 \leq (x \bmod N) < N$) を $m^{-1} \bmod N$ と書く。

上の命題から m が $\bmod N$ の逆元をもつことの必要十分条件は m と N が互いに素であることである。$\bmod N$ の逆元も (あれば) ユークリッドの互除法で求められる。

例 1.2.9　$\bmod 97$ で 23 の逆元を求める。

$23x \equiv 1 \pmod{97}$ を解くのだが，常に正しい式 $97x \equiv 0 \pmod{97}$ も利用する。

2 つの式からユークリッドの互除法で x の係数を小さくしていく。最初の 2 つの係数が互いに素なら最後は $x \equiv a \pmod{N}$ の形の式になる。

$$
\begin{array}{llrll}
(1) & 97x & \equiv & 0 \pmod{97} & \text{あたりまえの式} \\
(2) & 23x & \equiv & 1 \pmod{97} & \text{解く式} \\
(3) & 5x & \equiv & -4 \pmod{97} & (1) - (2) \times 4 \\
(4) & 3x & \equiv & 17 \pmod{97} & (2) - (3) \times 4 \\
(5) & 2x & \equiv & -21 \pmod{97} & (3) - (4) \\
(6) & x & \equiv & 38 \pmod{97} & (4) - (5)
\end{array}
$$

$23 \times 38 = 874 = 97 \times 9 + 1 \equiv 1 \pmod{97}$

さらに，$(23 \times 38 - 1)/97 = 9$ より，

$$23 \times 38 + 97 \times (-9) = 1$$

がわかる。

上の例のように，$Nx \equiv 0 \pmod{N}$ と $mx \equiv 1 \pmod{N}$ に対して，x の係数にユークリッドの互除法を施して，$x \equiv a \pmod{N}$ の形が出たら，a は必ず $\bmod N$ での m の逆元になる。これは，すでに存在がわかっているからである。

この方法で，m と n が互いに素のとき，$mx + ny = 1$ となる整数 x, y も計算できる。

問 1.2.10　mod 97 で 22 の逆元を求めよ。$97x + 22y = 1$ となる整数 x, y を一組求めよ。1 から 96 までの数を適当に選んで，mod 97 での逆元を求めよ。

問 1.2.11　容積 3 リットルのバケツと 5 リットルのバケツがある。これを利用して 1 リットルの水を作る方法を述べよ。

容積 1600cc の容器と 1300cc の容器がある。これを利用して 100cc の水を作る方法を述べよ。

1.3　中国剰余定理

次のようなパズルがある。

> 1 から 100 までの数を思い浮かべてください。その数を 3, 5, 7 で割って，余りを教えてください。その数を当ててみせます。

思い浮かべた数を x とすると，

$$x \equiv a \pmod 3, \quad x \equiv b \pmod 5, \quad x \equiv c \pmod 7$$

という連立方程式を解くことになる。結論からいうと，

$$x = (70a + 21b + 15c) \bmod 105$$

となる。

これは次の定理からわかる。

定理 1.3.1　m と n が互いに素で，a, b は整数とする。すると，$mu + nv = 1$

となる整数 u, v がある。このとき，

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

の必要十分条件は

$$x \equiv nva + mub \pmod{mn}.$$

とくに，上の連立方程式の解は 1 から mn (0 から $mn-1$) の間にちょうど 1 つ存在する。

証明. $x \equiv a \pmod{m}$ かつ $x \equiv b \pmod{n}$ と仮定する。すると，$nx \equiv na \pmod{mn}$ かつ $mx \equiv mb \pmod{mn}$ である。さらに，$nvx \equiv nva \pmod{mn}$ かつ $mux \equiv mub \pmod{mn}$ となり，両辺をそれぞれ加えると，$(nv+mu)x \equiv nva + mub \pmod{mn}$. ここで，$nv + mu = 1$ なので，$x \equiv nva + mub \pmod{mn}$.

逆に，$x \equiv nva + mub \pmod{mn}$ と仮定する。

m は mn の約数なので，$x \equiv nva + mub \pmod{m}$ である。$mu \equiv 0 \pmod{m}$ と $mu+nv = 1$ より，$nv \equiv 1 \pmod{m}$ である。これと，$mub \equiv 0 \pmod{m}$ より，$nva + mub \equiv a \pmod{m}$ である。

同様に，$nva + mub \equiv b \pmod{n}$ である。 □

例 1.3.2　次の連立合同式を考える。

$$x \equiv a \pmod{3}, \quad x \equiv b \pmod{5}$$

$3 \times 2 - 5 = 1$ なので，これは

$$x \equiv 6b - 5a \pmod{15}$$

と同値。一方，

$$x \equiv c \pmod{7}, \quad x \equiv d \pmod{15}$$

を考えると，$7 \times (-2) + 15 = 1$ より，これは

$$x \equiv 15c - 14d \pmod{105}$$

と同値。$d = 6b - 5a$ を代入すると

$$x \equiv 15c - 14(6b - 5a) \pmod{105}$$

すなわち，

$$x \equiv 70a - 84b + 15c \pmod{105}$$

$-84 \equiv 21 \pmod{105}$ なので，

$$x \equiv 70a + 21b + 15c \pmod{105}$$

これが，

$$x \equiv a \pmod{3}, \quad x \equiv b \pmod{5}, \quad x \equiv c \pmod{7}$$

の必要十分条件である。

1.4　オイラーの定理とフェルマーの小定理

定義 1.4.1　$N > 0$ を整数とする。$\mathbb{Z}_N^* = \{a \in \mathbb{Z} : 0 \leq a < N,\ a \text{ と } N \text{ は互いに素 }\}$ と定義する。$\mathbb{Z}_N^*$ の要素の個数を $\varphi(N)$ と書く。$\varphi(N)$ を**オイラー関数**と呼ぶ。

例 1.4.2　$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$, $\varphi(12) = 4$.
$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$, $\varphi(10) = 4$.
$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, $\varphi(7) = 6$.

補題 1.4.3　$N > 0$ を整数とする。

(1)　a と N が互いに素ならば $a \bmod N \in \mathbb{Z}_N^*$.
(2)　$a \in \mathbb{Z}_N^*$ ならば $a^{-1} \bmod N \in \mathbb{Z}_N^*$.
(3)　$a, b \in \mathbb{Z}_N^*$ ならば $ab \bmod N \in \mathbb{Z}_N^*$.

証明.　(1) a と N が互いに素とすると，命題 1.2.7 より，$ab \equiv 1 \pmod{N}$ となる整数 b がある。$a' = a \bmod N$ とすると $0 \leq a' < N$ かつ $a' \equiv a \pmod{N}$．すると，$a'b \equiv ab \equiv 1 \pmod{N}$．命題 1.2.7 より，$a'$ と N は互いに素。よって，$a \bmod N = a' \in \mathbb{Z}_N^*$.

(2) $a \in \mathbb{Z}_N^*$ とすると，a と N が互いに素なので $b = a^{-1} \bmod N$ が存在する。定義より，$ab \equiv 1 \pmod{N}$ かつ $0 \leq b < N$ である。よって，$b \in \mathbb{Z}_N^*$ である。

(3) $a, b \in \mathbb{Z}_N^*$ とする。すると，$aa' \equiv 1 \pmod{N}$，$bb' \equiv 1 \pmod{N}$ となる整数 a', b' が存在する。$c = ab \bmod N$ とすると，$0 \leq c < N$ で，$c \equiv ab \pmod{N}$．よって，$c(a'b') \equiv ab(a'b') = (aa')(bb') \equiv 1 \pmod{N}$．すなわち，$c \in \mathbb{Z}_N^*$. □

定理 1.4.4（オイラーの定理）　$N > 0$ を整数とする。N と互いに素な任意

の整数 a に対し

$$a^{\varphi(N)} \equiv 1 \pmod{N}$$

証明. $a \in \mathbb{Z}_N^*$ の場合に先ず議論する。

$\mathbb{Z}_N^* = \{a_1, \ldots, a_m\}$，$m = \varphi(N)$ と書ける。補題 1.4.3 より，$i = 1, \ldots, m$ について，$a'_i = aa_i \bmod N$ とすると $a'_i \in \mathbb{Z}_N^*$ である。

主張.

$$\{a'_1, a'_2, \ldots, a'_m\} = \{a_1, a_2, \ldots, a_m\}$$

$i \neq j$ ならば $a'_i \neq a'_j$ を示せばよい。この対偶を示そう。$a'_i = a'_j$ と仮定する。すなわち，$aa_i \bmod N = aa_j \bmod N$．すると，$aa_i \equiv aa_j \pmod{N}$．両辺に $b = a^{-1} \bmod N$ をかけると，$baa_i \equiv baa_j \pmod{N}$．$ba \equiv 1 \pmod{N}$ なので，$1 \cdot a_i \equiv 1 \cdot a_j \pmod{N}$．すなわち，$a_i \equiv a_j \pmod{N}$．$0 \leq a_i, a_j < N$ なので，$a_i = a_j$．これで，主張が示せた。

主張より，左右それぞれの要素をすべて掛け合わせても等しいので，

$$a'_1 a'_2 \cdots a'_m = a_1 a_2 \cdots a_m$$

$a'_i \equiv aa_i \pmod{N}$ より，

$$a^m a_1 a_2 \cdots a_m = (aa_1)(aa_2) \cdots (aa_m) \equiv a_1 a_2 \cdots a_m \pmod{N}$$

すなわち，

$$a^m a_1 a_2 \cdots a_m \equiv a_1 a_2 \cdots a_m \pmod{N}$$

$b_i = a_i^{-1} \bmod N$ とする。この両辺に $b_m \cdots b_2 b_1$ をかけると，

$$a^m (a_1 a_2 \cdots a_m)(b_m \cdots b_2 b_1) \equiv (a_1 a_2 \cdots a_m)(b_m \cdots b_2 b_1) \pmod{N}$$

$a_i b_i \equiv 1 \pmod{N}$ なので，$(a_1 a_2 \cdots a_m)(b_m \cdots b_2 b_1) \equiv 1 \pmod{N}$．よって，

$$a^m \equiv 1 \pmod{N}$$

a を N と互いに素な任意の整数とする。$a' = a \bmod N$ とすると，$a'^{\varphi(N)} \equiv 1 \pmod{N}$ であるが，$a \equiv a' \pmod{N}$ より，$a^{\varphi(N)} \equiv a'^{\varphi(N)} \equiv 1 \pmod{N}$. □

$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$ で上の議論を考えてみる。

$$3 \cdot 1 \equiv 3 \pmod{10} \tag{1}$$
$$3 \cdot 3 \equiv 9 \pmod{10} \tag{2}$$
$$3 \cdot 7 \equiv 1 \pmod{10} \tag{3}$$
$$3 \cdot 9 \equiv 7 \pmod{10} \tag{4}$$

よって，

$$(3 \cdot 1)(3 \cdot 3)(3 \cdot 7)(3 \cdot 9) \equiv 3 \cdot 9 \cdot 1 \cdot 7 \pmod{10}$$

したがって，

$$3^4(1 \cdot 3 \cdot 7 \cdot 9) \equiv 1 \cdot 3 \cdot 7 \cdot 9 \pmod{10}$$

両辺に $9 \cdot 3 \cdot 7$ をかけると，

$$3^4(3 \cdot 7 \cdot 9)(9 \cdot 3 \cdot 7) \equiv (3 \cdot 7 \cdot 9)(9 \cdot 3 \cdot 7) \pmod{10}$$

$(3 \cdot 7 \cdot 9)(9 \cdot 3 \cdot 7) \equiv 1 \pmod{10}$ より，

$$3^4 \equiv 1 \pmod{10}$$

p が素数ならば，$Z_p^* = \{1, 2, \ldots, p-1\}$ である。したがって次の定理を得る。

定理 1.4.5（フェルマーの小定理） p を (正の) 素数とする。整数 a が p で割り切れないならば

$$a^{p-1} \equiv 1 \pmod{p}$$

さらに，任意の整数 a に対し

$$a^p \equiv a \pmod{p}$$

素数 p に対してはもっと強いことが成り立つ。

定理 1.4.6　p が素数のとき，$\mathbb{Z}_p^*$ は 1 つの要素のべき $(\mathrm{mod}\ p)$ で生成される。すなわち，ある $a \in \mathbb{Z}_p^*$ に対し，

$$\mathbb{Z}_p^* = \{a^i \bmod p : i = 1, 2, \ldots, p-1\}$$

a を**生成元**あるいは**原始元**と呼ぶ。

証明は少し長くなるので省略する。

例 1.4.7　$\mathbb{Z}_7^*$ は 3 で生成される。5 も生成元である。

命題 1.4.8　$\mathbb{Z}_p^*$ の生成元はちょうど $\varphi(p-1)$ 個ある。

証明.　a を $\mathbb{Z}_p^*$ の生成元とする。$l > 0$ で l と $p-1$ が互いに素のとき，a^l も生成元になることを示せばよい。

l と $p-1$ が互いに素なので，$lj \equiv 1 \pmod{p-1}$ となる整数 $j > 0$ がある。$lj = 1 + m(p-1)$ $(m \geq 0)$ と書ける。

すると，$(a^l)^j = a^{lj} = a^{1+m(p-1)} = a(a^{p-1})^m \equiv a \cdot 1^m = a \pmod{p}$. よって，$a^l$ の累乗で，$\mathbb{Z}_p^*$ の要素がすべて表せる。　□

この命題を少し一般化して，ちょっとした個数の計算をすると $\mathbb{Z}_p^*$ の生成元の存在が示せる。

1.5　RSA 暗号

コンピュータ上のデータ (テキスト，ファイル) は 0 と 1 の有限列 (2 進列，ビット列) で表現されている (と考えられる)。この節では，内容がわからないようにしてファイルを送信するための暗号の技術の一つを解説する。

ファイルは 2 進列であるが，2 進列は 2 進数と解釈すると整数を表していると考えられる。

例 1.5.1（2 進数） 11010110 を 2 進数として考えると

$$1 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$$

になる。2 進数の足し算では 10 進数のときと同様に一般に繰り上がりが生じる。掛け算も 10 進数のときと同様にできる。

RSA 暗号は公開鍵暗号と呼ばれる暗号である。一般に暗号化と暗号の復号という操作が必要であるが，暗号化と復号に同じ鍵を使う場合を共通鍵暗号と呼び，暗号化の鍵と復号の鍵が異なり，暗号化のための鍵を公開しても問題ないものを公開鍵暗号と呼ぶ。

共通鍵暗号は，情報を共有したいグループごとに固有の鍵が必要である。したがって，鍵がたくさん必要になる。公開鍵暗号の場合は，同じ人に暗号を送るときは，1 つの公開鍵ですむ。

定義 1.5.2（RSA 暗号） p, q を 2 つの異なる大きな素数とする。L を $p-1$ と $q-1$ の (最小) 公倍数とする。e を L と互いに素な数とする。たとえば，$e = 41, 257, 65537$ で試し，それでもだめなら 2 ずつ増やしていって見つける。$N = pq$ とする。

公開鍵: e と N

暗号化法: 平文 $x < N$ に対し，$y = x^e \bmod N$ を暗号とする。

復号法: $d = e^{-1} \bmod L$ とすると，$x = y^d \bmod N$ で復号できる。

定理 1.5.3　RSA の暗号は上記の復号法で復号できる。

証明．　$y = x^e \bmod N$ とする。$ed \equiv 1 \pmod{L}$ より，$ed = 1 + mL$ と書ける。

$y^d \equiv x^{ed} \pmod{N}$.

$N = pq$ より，

$$y^d \equiv x^{ed} \pmod{p}, \quad y^d \equiv x^{ed} \pmod{q}$$

L は $p-1$ の倍数なので,

$$x^{ed} = x^{1+mL} = x(x^{p-1})^{m'}$$

と書ける。x が p の倍数でなければ,

$$x^{ed} = x(x^{p-1})^{m'} \equiv x \cdot 1^{m'} \equiv x \pmod{p}$$

x が p の倍数ならば両辺とも 0 と合同なので，いつでも

$$x^{ed} \equiv x \pmod{p}$$

よって,

$$y^d \equiv x \pmod{p}$$

同様に

$$y^d \equiv x \pmod{q}$$

中国剰余定理より (あるいは $y^d - x$ が p と q で割り切れるから)

$$y^d \equiv x \pmod{pq}$$

$0 < x < N = pq$ なので，$y^d \bmod N = x$. □

原理的には公開鍵 e, N から秘密鍵 d を求めることは可能である。$N = pq$ と因数分解すればあとは簡単であるが，実は p と q の桁が大きいと (例えば 1000 ビット程度)，実際に N の因数を早く見つける方法は今のところ知られていない。もちろん，しらみつぶしに p を生成して N を割ってみればよいのであるが，2^{1000} 個近く調べる必要があり，現在のコンピュータをもってしてもこの方法では相当時間がかかる。他に d を求める方法は知られていない。ただし，早く計算する方法がないことが証明できているわけでもない。ロシアの当局がうまい方法を見つけて公表していないだけかも知れない。

ところで，d の桁も 1000 桁程度あるかも知れないが，その場合は $y^d \bmod N$ を計算するのに 2^{1000} 回程度の掛け算をする必要があるのだろうか。そう

だとしたら暗号の復号は事実上できなくなる。しかし，うまくやるとべきの桁数程度の演算回数で累乗計算ができる。

命題 1.5.4　d の 2 進数表現を α とする。すると $x^d \bmod N$ の計算は α の長さ程度の回数の $\bmod N$ の掛け算でできる。

証明.　2 進数 α に対し，0 を最後につけた $\alpha 0$ は $\alpha \times 2$ を表し，1 を最後につけた $\alpha 1$ は $\alpha \times 2 + 1$ を表す。したがって，$x^\alpha \bmod N = a$ とすると，

$$x^{\alpha 0} \bmod N = a^2 \bmod N, \quad x^{\alpha 1} \bmod N = a^2 x \bmod N$$

これを利用すると，d の 2 進数表現の桁数程度の演算で $x^d \bmod N$ が計算できる。

例えば，$3^{37} \bmod 100$ を計算してみよう。$37 = 100101_2$ である。べきを 2 進数で書く。

$$\begin{aligned}
3^1 &= 3, \\
3^{10} &= 3^2 = 9, \\
3^{100} &= (3^{10})^2 = 81, \\
3^{1001} &= (3^{100})^2 \cdot 3 = 81^2 \cdot 3 \equiv 83 \pmod{100} \\
3^{10010} &= (3^{1001})^2 \equiv 83^2 \equiv 89 \pmod{100} \\
3^{100101} &= (3^{10010})^2 \cdot 3 \equiv 89^2 \cdot 3 \equiv 63 \pmod{100}
\end{aligned}$$

□

1.6　ElGamal 暗号

RSA 暗号は大きな素数の積の素因数分解が難しいことを利用した暗号であるが，ここで紹介する ElGamal 暗号は次の離散対数問題の難しさを利用した暗号である。RSA は整数の性質にかなり依存した暗号であるが，ElGamal 暗号は演算が 1 つ定義されている状況 (いわゆる群) でも同様の暗

号が考えられるという意味でより汎用的である。IC カードの情報は楕円曲線と呼ばれる代数曲線上の点同士で定義されるある演算を使った ElGamal 暗号で暗号化されている。

離散対数問題について述べよう。Z_n^* や有限体の乗法群において，b をその要素とするとき，b^x の計算は x が整数のとき高速にできるが，与えられた要素 b' に対し，$b^x = b'$ となる整数 x を求めるのはかなり困難である。このような x を b と b' から求める問題を**離散対数問題**と呼ぶ。離散対数問題は任意の群において考えることができる。また，次の仮定を **Diffie-Hellman の仮定**と呼ぶ。p を大きな素数とする。$\mathbb{Z}_p^*$ の要素 g に対し，$g^a \bmod p$ と $g^b \bmod p$ の値から $g^{ab} \bmod p$ の値を計算するのは困難である。

ElGamal 暗号

大きな素数 q を固定する。$\mathbb{Z}_q^*$ は位数 (大きさ)$q-1$ の巡回群である。

$q :=$ 適度に大きな素数 (擬素数); (q は公開する)
$1 < g < q-1$ なる g を 1 つ選ぶ．(g も公開する)
　g は $\mathbb{Z}_p^*$ の生成元が望ましい。
$1 < a < q-1$ をランダムに選ぶ．(a は秘密鍵)
$h = g^a \bmod q$; (h は公開する)
x の暗号化 ($0 < x < q$):
　$(g^k \bmod q,\ xh^k \bmod q)$
復号:
　暗号 (y, z) に対し，
　　$x = zy^{-a} \bmod q$

この復号の方法でもとに戻ることを示しておく。

$y = g^k \bmod q$ より，$y^a \equiv g^{ka} \pmod q$．$y' = (y^a)^{-1} \bmod q$ とすると，$y'g^{ka} \equiv 1 \pmod q$．すると $z = xh^k \equiv xg^{ak} \pmod q$．したがって，$zy' \equiv x \pmod q$．

2　多項式 (整式)

コンピュータ上ではデータは 2 進列で表されており，RSA 暗号などでは 2 進列を 2 進数と考えて，整数の演算を利用してデータの加工を行なっている。2 進列は 2 進数と考える必要があるわけではない。誤り訂正符号などではある種の多項式と考えた場合の演算を利用している。この節ではこの考え方を説明する。

10 進数 (整数) 1425 は

$$10^3 + 4 \cdot 10^2 + 2 \cdot 10 + 5$$

を表わしていて，これから 10 進数同士の足し算と掛け算の筆算方法が導かれる。

$$\begin{array}{cccccc} & 1 & 4 & 2 & 5 \\ + & & 3_1 & 7_1 & 6 \\ \hline & 1 & 8 & 0 & 1 \end{array} \qquad \begin{array}{cccccc} & & 1 & 4 & 2 & 5 \\ & \times & & 3 & 7 & 6 \\ \hline & & 8 & 5 & 5 & 0 \\ & 9 & 9 & 7 & 5 & \\ 4 & 2 & 7 & 5 & & \\ \hline 5 & 3 & 5 & 8 & 0 & 0 \end{array}$$

次に 1 変数整数係数多項式を考えよう。たとえば，$x^3 + 4x^2 + 2x + 5$ や $3x^2 + 7x + 6$ などがこの例である。これらの和や積は，整数の筆算と似た方法で計算できる。x を省略して，係数だけ並べるだけで計算ができる。多項式の演算は繰り上がりがないのが特徴である。

$$\begin{array}{cccccc} & 1 & 4 & 2 & 5 \\ + & & 3 & 7 & 6 \\ \hline & 1 & 7 & 9 & 11 \end{array} \qquad \begin{array}{cccccc} & & 1 & 4 & 2 & 5 \\ & \times & & 3 & 7 & 6 \\ \hline & & 6 & 24 & 12 & 30 \\ & 7 & 28 & 14 & 35 & \\ 3 & 12 & 6 & 15 & & \\ \hline 3 & 19 & 40 & 53 & 47 & 30 \end{array}$$

結果の列 1 7 9 11 は $x^3+7x^2+9x+11$，3 19 40 53 47 30 は $3x^5+19x^4+40x^3+53x^2+47x+30$ のことである。x を変数とする 1 変数整数係数多項式の全体を $\mathbb{Z}[x]$ と書く。

さらに，多項式の係数を mod 10 で計算することにすると次のようになる。

$$\begin{array}{cccccc} & 1 & 4 & 2 & 5 \\ + & & 3 & 7 & 6 \\ \hline & 1 & 7 & 9 & 1 \end{array} \qquad \begin{array}{cccccc} & & 1 & 4 & 2 & 5 \\ & \times & & 3 & 7 & 6 \\ \hline & & 6 & 4 & 2 & 0 \\ & 7 & 8 & 4 & 5 & \\ 3 & 2 & 6 & 5 & & \\ \hline 3 & 9 & 0 & 3 & 7 & 0 \end{array}$$

これは 10 進数の筆算に非常に近く，実は繰り上がりをすべて無視した演算になる。$\mathbb{Z}_{10}=\{0,1,2,3,4,5,6,7,8,9\}$ とおく。係数を $\mathbb{Z}_{10}$ の要素に限定した変数 x の多項式全体を $\mathbb{Z}_{10}[x]$ と書く。上の演算を $\mathbb{Z}_{10}[x]$ の足し算と掛け算と呼ぶ。

同じことを 2 進列に対して考える。2 進列が与えられたとき，それら (0 と 1) を係数とする 1 変数整数係数多項式と考えて足し算や掛け算を行い，最後に係数を 2 で割った余りで置き換える。$\mathbb{Z}_2=\mathbb{F}_2=\{0,1\}$ とし，$\mathbb{F}_2$ に係数をもつ変数 x の多項式全体を $\mathbb{F}_2[x]$ と書き，この足し算と掛け算を $\mathbb{F}_2[x]$ の足し算と掛け算と呼ぶ。

たとえば 1011 は x^3+x+1 のことと考える。x を表わす 2 進列は 10 である。$x^2=10^2=100$，$x^3=10^3=1000$，... となっている。$\mathbb{F}_2[x]$ の要素として，$1011+111$ と 1011×111 は次のようになる。

$$\begin{array}{cccccc} & 1 & 0 & 1 & 1 \\ + & & 1 & 1 & 1 \\ \hline & 1 & 1 & 0 & 0 \end{array} \qquad \begin{array}{cccccc} & & 1 & 0 & 1 & 1 \\ & \times & & 1 & 1 & 1 \\ \hline & & 1 & 0 & 1 & 1 \\ & 1 & 0 & 1 & 1 & \\ 1 & 0 & 1 & 1 & & \\ \hline 1 & 1 & 0 & 0 & 0 & 1 \end{array}$$

足し算はビットごとの排他的論理和になっている。

2.1 $\mathbb{F}_2[x]$ の割り算の原理

定義 2.1.1 $\mathbb{F}_2[x]$ の要素 (多項式) に対して，係数が 0 でない項の最大次数をその多項式の**次数**と呼ぶ。たとえば，$1011 = x^3 + x + 1$ の次数は 3 次である。一般に，1 から始まる n ビットの列は $\mathbb{F}_2[x]$ の $n-1$ 次多項式を表す。$f \in \mathbb{F}_2[x]$ に対し，f の次数を $\deg f$ と書く。この定義だと 0 の次数は決まらない。0 の次数を $-\infty$ とする流儀もあるが，定数項しかないという考えで，0 の次数も 0 にしておく。

また，$f \in \mathbb{F}_2[x]$ に対し，x に a を代入して $\mathbb{F}_2 = \mathbb{Z}_2$ で計算 (すなわち，mod 2 で計算) した結果を $f(a)$ と書く。$f = 1011 = x^3 + x + 1$ のとき，$f(0) = (0^3 + 0 + 1) \bmod 2 = 1$，$f(1) = (1^3 + 1 + 1) \bmod 2 = 3 \bmod 2 = 1$ である。

定理 2.1.2（割り算の原理） $f \in \mathbb{F}_2[x]$ で $f \neq 0$ とする。任意の $g \in \mathbb{F}_2[x]$ に対し，

$$g = qf + r, \quad 0 \leq \deg r < \deg f$$

となる $q, r \in \mathbb{F}_2[x]$ がちょうど 1 組存在する。

q を g/f の商，r を余りと呼ぶ。r を $g \bmod f$ とも書く。

$\mathbb{F}_2 = \mathbb{Z}_2$ で，$-1 \equiv 1 \pmod 2$ に注意すると，割り算も整数の割り算の筆算と同様にできる。繰り上がりがないので，引き算で「借りる」必要がない。

$$\begin{array}{rcl}
 & 1\ 1 & \\
\hline
1\ 1\ 1 \,)\, 1\ 0\ 1\ 1 & & \\
\quad 1\ 1\ 1 & & \\
\hline
\quad\ \ 1\ 0\ 1 & & \\
\quad\ \ 1\ 1\ 1 & & \\
\hline
\quad\ \ \ 1\ 0 & &
\end{array}
\qquad
\begin{array}{rcl}
 & 1\ 1\ 1 & \\
\times & 1\ 1 & \\
\hline
 & 1\ 1\ 1 & \\
1\ 1\ 1 & & \\
\hline
1\ 0\ 0\ 1 & & \\
+\quad\ \ 1\ 0 & & \\
\hline
1\ 0\ 1\ 1 & &
\end{array}$$

この例は，$1011 = x^3 + x + 1$ を $111 = x^2 + x + 1$ で割る計算で，右側は検算である。$\mathbb{F}_2[x]$ で 0 でない多項式は最高次の係数が 1 である。するとこのような筆算が必ずできることがわかる。したがって，割り算の原理が成り立つ。この割り算の原理を使うと $\mathbb{F}_2[x]$ が整数と同じような性質をたくさんもつことがわかる。

多項式が整数と異なる点は，根の概念である。多項式 $f = f(x) \in \mathbb{F}_2[x]$ に対し，x に $\mathbb{F}_2$ の要素 a を代入して $\mathbb{F}_2$ で計算した値を $f(a)$ と書く。$\mathbb{F}_2 = \{0, 1\}$ なので，$f(0)$ と $f(1)$ しか考えない。$f(a) = 0$ となるとき，a を f の**根**と呼ぶ。

定義 2.1.3　$f, g \in \mathbb{F}_2[x]$ とする。$f = gh$ となる $h \in \mathbb{F}_2[x]$ があるとき，g を f の**因子** (因数) と呼ぶ。g が f の因子であることと $f \bmod g = 0$ が同値である。

定理 2.1.4（因数定理）　$a \in \mathbb{F}_2$ とする。$x - a$ (係数の 2 進表記は $1a$) が $f \in \mathbb{F}_2[x]$ の因子であることと，$f(a) = 0$ (a が f の根) が同値である。

証明.　割り算の原理から，$f(x) = (x - a)q + r$ で，r の次数が 0 次の形で書ける。0 次多項式は $\mathbb{F}_2$ の要素である。すると，$f(a) = r$. よって，余り r が 0 ということと，$f(a) = 0$ が同値になる。　□

定義 2.1.5（法 F の合同）　$F \neq 0$ を $\mathbb{F}_2[x]$ の要素とする。多項式 $f, g \in \mathbb{F}_2[x]$ に対し，$f - g$ が F で割り切れるとき (余りが 0)，$f \equiv g \pmod{F}$ と書き，f と g は**法 F で合同**，あるいは $\bmod F$ で合同という。

$\bmod F$ の合同という関係についての基本的な性質をまとめておく。

命題 2.1.6　$F, f, g, h \in \mathbb{F}_2[x]$ で，$F \neq 0$ とする。

(1)　$f \equiv f \pmod{F}$
(2)　$f \equiv g \pmod{F}$ ならば $g \equiv f \pmod{F}$

(3) $f \equiv g \pmod{F}$, $g \equiv h \pmod{F}$ ならば $f \equiv h \pmod{F}$

命題 2.1.7 F, f, g, h は $\mathbb{F}_2[x]$ の要素とする。

(1) $f \equiv g \pmod{F} \iff f \bmod F = g \bmod F$
(2) $f \equiv g \pmod{F} \Rightarrow hf \equiv hg \pmod{F}$
(3) $h \neq 0$ とする。$f \equiv g \pmod{F} \iff hf \equiv hg \pmod{hF}$
(4) $f \equiv g \pmod{hF} \Rightarrow f \equiv g \pmod{F}$

命題 2.1.8 $f \equiv f' \pmod{F}$ かつ $g \equiv g' \pmod{F}$ ならば,

$$f + g \equiv f' + g' \pmod{F}, \quad fg \equiv f'g' \pmod{F}$$

2.2 最大公約数とユークリッドの互除法

定義 2.2.1（約数，公約数） $\mathbb{F}_2$ 係数 1 変数多項式 f, g, h に対し，$f = gh$ と書けるとき，g(h も) を f の**因子** (因数) と呼ぶ。h が f の因子かつ h が g の因子のとき，h を f と g の**公因子**と呼ぶ。f と g の公因子のうち次数が最大のものを $\gcd(f, g)$ と書き，f と g の**最大公因子**と呼ぶ。

定理 2.2.2（ユークリッドの互除法） f, g が $\mathbb{F}_2$ 係数 1 変数多項式で，$g \neq 0$ のとき,

$$f = qg + r$$

とすると

(1) $r = 0$ のとき，$\gcd(f, g) = g$
(2) $r \neq 0$ のとき，$\gcd(f, g) = \gcd(g, r)$

$\mathbb{F}_2$ 係数多項式 f と $g \neq 0$ の最大公因子は次のようにして求まる。

(1) $r := f \bmod g$ を計算。($\deg g > 0$ ならば $0 \leq \deg r < \deg g$ である)
(2) $r = 0$ の場合は，g が最大公因子。

(3) $r \neq 0$ の場合は，g と r の最大公因子が求めるもの。
すなわち，$f := g$; $g := r$ として，(1) へもどる。

(1) の計算のあと $\deg r = 0$ となると，$r = 1$ あるいは 0 なので，遅くとも次の回で終了する。

例 2.2.3　1111 $(= x^3 + x^2 + x + 1)$ と 1010 $(= x^3 + x)$ の最大公因子を求める。

$$\begin{array}{rcrcr} 1111 & - & 1010 & = & 101 \\ 1010 & - & 101 \times 10 & = & 0 \end{array}$$

101 $(= x^2 + 1)$ が最大公因子。

命題 2.2.4　$f, g \neq 0$, $f, g \in \mathbb{F}_2[x]$ とすると

$$fu + gv = \gcd(f, g)$$

となる $u, v \in \mathbb{F}_2[x]$ が存在する。

$\gcd(m, n) = 1$ となるときが重要である。

定義 2.2.5　$f, g \neq 0$, $f, g \in \mathbb{F}_2[x]$ とする。$\gcd(f, g) = 1$ のとき，f と g は**互いに素**であるという。

命題 2.2.6　$f, g \neq 0$, $f, g \in \mathbb{F}_2[x]$ とすると次の条件は同値である。

(1)　f と g は互いに素。
(2)　$fu + gv = 1$ となる u, $v \in \mathbb{F}_2[x]$ が存在する。
(3)　$fu \equiv 1 \pmod{g}$ となる $u \in \mathbb{F}_2[x]$ が存在する。
(4)　$gv \equiv 1 \pmod{f}$ となる $v \in \mathbb{F}_2[x]$ が存在する。

整数における素数に対応する概念が既約多項式である。

定義 2.2.7　$f \in \mathbb{F}_2[x]$ で，$\deg f \geq 1$ とする。$\deg g < \deg f$ なる任意の

$g \in \mathbb{F}_2[x]$ に対し，$g \neq 0$ ならば g と f が互いに素になるとき，f を**既約**と呼ぶ。f が既約であることと，f が $\mathbb{F}_2[x]$ において 1 次以上 $\deg f$ 未満の因子をもたないことが同値である。

整数において，p が素数のとき，$\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ とすると，これは $\bmod p$ の掛け算で閉じていて，$\mathbb{Z}_p^*$ のどの要素も乗法の逆元を $\mathbb{Z}_p^*$ にもっていた。さらに，$\mathbb{Z}_p^*$ は 1 つの要素の ($\bmod p$ での) 累乗で生成されていた。

これと同じような状況が既約多項式で割った余りの集合で起きる。

2.3 $\mathbb{F}_2[x]$ の既約多項式

$\mathbb{F}_2[x]$ における既約多項式をいくつか調べてみよう。例によって，係数を並べたビット列で表記する。左が高次の係数である。一般に，$\mathbb{F}_2[x]$ の要素が 1 次の因子をもたないためには定数項 (一番右) が 1 で，1 の個数が奇数である必要がある。たとえば，$f = 101$ とすると，$f(1) = 1^2 + 1 = 0$ なので 101 は既約でない。また，m 次式と n 次式を掛けるとちょうど $(m+n)$ 次式になる。よって，因子をもてば，半分以下の次数の (既約) 因子をもつ。たとえば，7 次式が 4 次の因子をもつとすると，4 次 $\times$3 次の形の因数分解ができる。すなわち，3 次の因子をもつ。さらに分解できれば，もっと低い次数の既約因子をもつ。

1 次式　10, 11 (1 次式はすべて既約)

2 次式　111

1 次の因子をもたない条件，最高次 (一番左) が 1 で，定数項が 1 で，1 の個数が奇数個を満たすのはこれしかない。2 次式は因子をもてば 1 次の因子をもつので，111 は既約。

3 次式　1011, 1101

1 次の因子をもたないのはこの 2 つ。3 次式が因数分解できたら 1 次の因子をもつはずなので，これらは既約である。

4 次式　10011, 11001, 11111

1 次の因子をもたないのはこれらと 10101．4 次式が因数分解できるとすると，1 次式または 2 次式の既約因子をもつ。したがって，111 で割り切れないことだけ調べればよい。上の 3 つは 111 で割ると余りが 0 でない。一方，$10101 = 111^2$ である。

問 2.3.1　$\mathbb{F}_2[x]$ の 8 次多項式 110000111 が $\mathbb{F}_2[x]$ で既約であることを示せ。(ヒント．8 次式が既約でなければ，4 次以下の既約因子をもつ。)

実は次が成り立つ。

定理 2.3.2　自然数 $n \geq 1$ に対し，$\mathbb{F}_2[x]$ には n 次の既約多項式がある。

実数係数の 1 変数既約多項式は高々 2 次で，複素数係数の 1 変数既約多項式は 1 次のものしかない。有理数係数の場合も，$n \geq 1$ ならば n 次の既約多項式がある。

2.4　2^n 元体

$\mathbb{F}_2[x]$ の 2 次以下の要素は，$\{0, 1, 10, 11\}$ である。この集合は $\mathbb{F}_2[x]$(多項式) の和で閉じている。f, g をこの 2 次以下の多項式とするとき，f と g の積を $fg \bmod 111$ (多項式として掛けて，111 で割った余りを演算結果とする) で定義する。このように和と積を考えたとき，

$$\mathbb{F}_4 = \{0, 1, 10, 11\}$$

と定義する。$\mathbb{F}_4$ はこの和と積について，$\mathbb{F}_2[x]$ や整数とほぼ同様の性質を満たし，さらに，0 でない要素は積について逆元をもつ。実際，$10 \times 11 = 110 \equiv 1 \pmod{111}$．すなわち，$a \neq 0$ ならば $ax = 1$ となる x がとれる。このような性質をもつものを**体**と呼ぶ。0 でないものについて (余りのない) 割り算ができるので，有理数や実数などと同じである。$\mathbb{F}_4$ は 4 つの要素か

らなる体なので，4 元体と呼ばれる。一般に，q 個の要素からなる体を q 元体と呼ぶ。

定理 2.4.1（2^n 元体の存在） F を $\mathbb{F}_2[x]$ の n 次の既約多項式とする。$q = 2^n$ に対し，

$$\mathbb{F}_q = \mathbb{F}_2[x] \text{ の } n-1 \text{ 次以下の多項式全体}$$

とし，和を $\mathbb{F}_2[x]$ における和，$f, g \in \mathbb{F}_q$ に対し，積 fg を f と g の多項式としての積を F で割った余りと定義する。すると，$\mathbb{F}_q$ は体になる。

$\mathbb{F}_q$ の要素の個数はちょうど q である。$n-1$ 次以下の多項式の係数は $n-1$ 次，$n-2$ 次，...，1 次，0 次の n 個の係数を並べて表現でき，それぞれ値は 0 または 1 の 2 通りずつある。したがって，2^n 通りある。

証明. 体の正確な定義をしていないが，ほとんどの性質は $\mathbb{F}_2[x]$ の演算から受け継がれる。0 でないものが積について逆元をもつことを示せばよい。$f \in \mathbb{F}_q$ とすると，F が既約なので，$\mathbb{F}_2[x]$ の要素として F と f の最大公因子は 1 である。命題 2.2.6 より，$fu + Fv = 1$ となる $u, v \in \mathbb{F}_2[x]$ がある。$g = u \bmod F$ とすると g は $n-1$ 次以下で，$fg \equiv 1 \pmod{F}$ である。すなわち，$\mathbb{F}_q$ の演算で，$fg = 1$ である。 □

3 次以上の既約多項式は複数あるので，$\mathbb{F}_q$ という表現は不適切に見える。しかし，q 個の元からなる体は本質的に一つしかないことが知られているので単に $\mathbb{F}_q$ と書くのである。しかし，この「本質的に一つ」という意味は少し難しい概念なので省略する。積の定義に使う既約多項式が異なれば，同じ表現の要素でも，積の値が異なることがある。以下，使う既約多項式はそのつど固定されているものとする。

さて，$\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ の要素は積について逆元をもっていたが，もっと強く，ある 1 つの要素のべきで生成できることが知られている。

定理 2.4.2（原始元の存在） q 元体 $\mathbb{F}_q$ に対し，ある $\alpha \in \mathbb{F}_q^*$ をうまくとると

$$\mathbb{F}_q^* = \{\alpha^i : i = 1, 2, \cdots, q-1\}$$

と書ける。特に，$\alpha^{q-1} = 1$ である。α を $\mathbb{F}_q$ の**原始元**と呼ぶ。

オイラーの定理の証明と同様に，$x \in \mathbb{F}_q^*$ ならば $x^{q-1} = 1$ がわかる。上の定理は，$\mathbb{F}_q[y](\mathbb{F}_q$ 係数多項式) の理論を使って証明されるが，少し長くなるので省略する。

具体的なものについては，実際に確認できる。

例 2.4.3 $\mathbb{F}_2[x]$ において mod 1011 で積を計算する $\mathbb{F}_8$ を考える $(8 = 2^3)$。すると，10 が原始元である。実際，$\alpha = 10$ とすると，

$\alpha = 10$,
$\alpha^2 = 100$,
$\alpha^3 = 1000 \equiv 11 \pmod{1011}$,
$\alpha^4 = 110$,
$\alpha^5 = 1100 \equiv 111 \pmod{1011}$,
$\alpha^6 = 1110 \equiv 101 \pmod{1011}$,
$\alpha^7 = 1010 \equiv 1 \pmod{1011}$.

既約多項式 f に対し，mod f で考えた体の原始元として $10 = x$ が選べるとき，f を**原始既約多項式**と呼ぶ。

問 2.4.4 $\mathbb{F}_2[x]$ の要素 10011, 11001 は原始既約多項式であることを示せ。11111 は原始既約多項式ではない。mod 11111 の原始元を 1 つ求めよ (11 がそう)。

2.5　体係数多項式

$\mathbb{F}_{2^n}$，$\mathbb{Z}/p\mathbb{Z}$ (p は素数) のような集合をその足し算とかけ算の演算をこめて体と呼ぶ。要素の個数が q の体を q **元体**と呼び，$\mathbb{F}_q$ と書く。要素の個数が q の体は本質的に 1 つしかないことが知られているので，$\mathbb{F}_q$ という 1 通りの記法で書かれる。$GF(q)$ と書くこともある。

p が素数のとき，$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ で，$+$ は整数として加えてから p で割った余りをとる演算，$\cdot$ は整数としてかけてから p で割った余りをとる演算である。

$n \geq 2$ に対し，$\mathbb{F}_p[x]$ の n 次既約多項式 f が存在する。$\mathbb{F}_p[x]/(f)$ は集合としては $\mathbb{F}_p$ 係数 $n-1$ 次以下の 1 変数多項式で，$+$ は多項式としての足し算 (係数ごとの足し算)，$\cdot$ は $\mathbb{F}_p$ 係数多項式としてかけ算をしてから f で割った余りをとる演算である。$\mathbb{F}_p[x]/(f)$ は体になる (0 でない要素はかけ算についての逆元をもつ)。$\mathbb{F}_p[x]/(f)$ の要素は n 個の係数が $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ のどれかということで決まるので，要素の個数は p^n 個である。有限体はこのパターンで構成されるものしかないことが知られている。$\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(f)$，($f$ は n 次の 1 変数既約多項式) である。

有限体 $\mathbb{F}_q$ に対し，その要素を係数とする 1 変数多項式が再び考えられる。それを $\mathbb{F}_q[y]$ とする。係数を最高次から順に左から右に並べた表記も使う。たとえば，$a_0y^3 + a_1y^2 + a_2y + a_3 = (a_0, a_1, a_2, a_3)$ である。この係数の並び，すなわち $\mathbb{F}_q$ の要素の列を**係数ベクトル**と呼ぶのが一般的である。

定義 2.5.1　$\mathbb{F}_q$ の要素を m 個並べた $(a_0, a_1, a_2, \ldots, a_{m-1})$ $(a_i \in \mathbb{F}_q)$ の形の並び (ベクトル) の全体を $\mathbb{F}_q^m$ と書く。$\mathbb{F}_q^m$ の要素は $(m-1)$ 次以下の 1 変数多項式 (の係数ベクトル) と考えられる。

次の表記も標準的ではないが，ある意味ですっきりした記法と考えられる。

定義 2.5.2　$f = (a_0, a_1, \ldots, a_{m-2}, a_{m-1}) \in \mathbb{F}_q^m$ と $\mathbb{F}_q$ の要素 y，あるいは変数 y に対し，

$$f(y) = a_0 y^{m-1} + a_1 y^{m-2} + \cdots + a_{m-2} y + a_{m-1}$$

と定義する。

$f = (1, 2, 3) \in \mathbb{R}^3$ とすると，$f(y) = y^2 + 2y + 3$ で，$f(1) = 6$ である。$f = (1, 0, 0, 0)$ とすると $f(y) = y^3$ である。

$\mathbb{F}_q[y]$ に対しても $\mathbb{F}_2[x]$ のときと似た割り算の原理が成り立つ。実際，この割り算の原理は係数が体ということだけで成り立つ。

定理 2.5.3（割り算の原理）　K を体とする。$f \in K[y]$ で $\deg f > 0$ とする。任意の $g \in K[y]$ に対し，

$$g = qf + r, \quad 0 \leq \deg r < \deg f$$

となる $q, r \in K[y]$ がちょうど 1 組存在する。

q を g/f の商，r を**余り**あるいは**剰余**と呼ぶ。r を $g \bmod f$ とも書く。

例で説明しよう。$K = \mathbb{F}_4 = \mathbb{F}_2[x]/(111)$ (111 は $x^2 + x + 1$ のこと) を考える。多項式は係数をカンマで区切って並べて表記することにする。$\mathbb{F}_4 = \{0, 1, 10, 11\}$ で，$10^2 = 11$, $11^2 = 10$, $10 \times 11 = 1$ である。

$f = (11, 1, 10) = 11y^2 + y + 10$, $g = (1, 11, 10, 1, 0, 1) = y^5 + 11y^4 + 10y^3 + y^2 + 1$ とする。

$$
\begin{array}{rrrl}
 & & & 10\quad 10\quad 1\quad 1 \\
\cline{4-4}
11 & 1 & 10 &)\ 1\quad 11\quad 10\quad 1\quad 0\quad 1 \\
 & & & \ \ 1\quad 10\quad 11 \\
 & & & \cline{4-6}
 & & & \quad\ 1\quad 1\quad 1 \\
 & & & \quad\ 1\quad 10\quad 11 \\
 & & & \cline{4-6}
 & & & \quad\quad 11\quad 10\quad 0 \\
 & & & \quad\quad 11\quad 1\quad 10 \\
 & & & \cline{4-6}
 & & & \quad\quad\quad 11\quad 10\quad 1 \\
 & & & \quad\quad\quad 11\quad 1\quad 10 \\
 & & & \cline{4-6}
 & & & \quad\quad\quad\quad 11\quad 11
\end{array}
$$

割る多項式の最高次の係数 11 に逆元 $11^{-1} = 10$ があることが本質的である。体に係数をもつ多項式ならばこれはいつも成り立つ。

定義 2.5.4（合同） 整数や $\mathbb{F}_2[x]$ の場合と同様に，$f, g, F \in K[y]$ に対し，$f - g \bmod F = 0$ のとき，$f \equiv g \pmod{F}$ と書く。

定義 2.5.5（因子，公因子） K を体とする。K 係数 1 変数多項式 f, g, h に対し，$f = gh$ と書けるとき，g と h を f の**因子** (因数, factor, divisor) と呼ぶ。g が f の因子であるための必要十分条件は $f \equiv 0 \pmod{g}$ である。h が f の因子かつ h が g の因子のとき，h を f と g の**公因子**と呼ぶ。f と g の公因子のうち次数が最大で，最大次の係数が 1 のものを $\gcd(f, g)$ と書き，f と g の**最大公因子**と呼ぶ。

定理 2.5.6（因数定理） K を体，$a \in K$ とする。$y - a$ が $f \in K[y]$ の因子であることと，$f(a) = 0$ が同値である。

$f(a) = 0$ となる a を f の根 (こん) あるいは零点と呼ぶ。

証明. 割り算の原理から，$f(y) = (y - a)q + r$ で，r の次数が 0 次の形で書ける。0 次多項式は K の要素である。すると，$f(a) = r$. よって，余り r が 0 ということと，$f(a) = 0$ が同値になる。 □

定理 2.5.7　K を体，$f(y) \in K[y]$ を n 次多項式とする。すると，$f(y)$ の K における根 ($f(y) = 0$ の解) の個数は高々 n 個である。

証明．　$a_1 \in K$ で $f(a_1) = 0$ とすると，因数定理より，$f(y) = (y - a_1)f_2(y)$ と因数分解する。$a_2 \in K$ で $f(a_1) = 0$，$a_2 \neq a_1$ とすると，$f(a_2) = (a_2 - a_1)f_2(a_2) = 0$．$(a_2 - a_1)^{-1}$ を右側の $=$ の両辺にかけると，$f_2(a_2) = 0$．したがって，$f_2(y) = (y - a_2)f_3(y)$ と因数分解できる。すると，$f(y) = (y - a_1)(y - a_2)f_3(y)$．$a_3 \in K$ で $f(a_3) = 0$，$a_3 \neq a_1, a_2$ とすると，$f(a_3) = (a_3 - a_1)(a_3 - a_2)f_3(a_3) = 0$．$a_3 - a_1 \neq 0$，$a_3 - a_2 \neq 0$ でこれらが K の要素であることからそれぞれ逆元をもつので $f_3(a_3) = 0$．因数定理より，$f_3(y) = (y - a_3)f_4(y)$ と因数分解できる。

根の個数だけ 1 次の因数が出てくるので，それが n 個を越えると n 次より高次の式になるので矛盾する。　□

定理 2.5.8（ユークリッドの互除法）　$f, g \in K[y]$ で，$g \neq 0$ とする。

$$f = qg + r, \quad q, r \in K[y]$$

とすると

(1)　$r = 0$ のとき，$\gcd(f, g) = a^{-1}g$ (a は g の最高次係数)
(2)　$r \neq 0$ のとき，$\gcd(f, g) = \gcd(g, r)$

K 係数多項式 f と $g \neq 0$ の最大公因子は次のようにして求まる。

(1) $r := f \bmod g$ を計算。($\deg g > 0$ ならば $0 \leq \deg r < \deg g$ であり，$\deg g = 0$ ならば，$g \in K$ で $g^{-1} \in K$ がある。)
(2) $r = 0$ の場合は，$a^{-1}g$ が最大公因子。ここで，a は g の最高次の係数。
(3) $r \neq 0$ の場合は，g と r の最大公因子が求めるもの。
すなわち，$f := g$; $g := r$ として，(1) へもどる。

(1) の計算のあと $\deg r = 0$ なら $r \in K$ あるいは 0 なので，遅くとも次の回で終了する。

3 Reed-Solomon 符号

3.1 Reed-Solomon 符号の定義

ここまでの知識で，Reed-Solomon 符号と呼ばれる誤り訂正符号が説明できる。一般に有限体 $\mathbb{F}_q$ に対し，誤り訂正能力 t の Reed-Solomon 符号 $RS(q,t)$ が定義される。($2t+1$ が符号の「最小距離」なので，$RS(q,2t+1)$ と表記されることが多い。) Reed-Solomon 符号は CD，DVD，放送，バーコード，宇宙探査機などで広く使われている。

$\mathbb{F}_q$ 上の Reed-Solomon 符号は，$\mathbb{F}_q$ の要素を $(q-1)$ 個並べた列 (ベクトル) である。これは $\mathbb{F}_q[y]$ の要素 (多項式) として $(q-2)$ 次多項式と考える。1 つの係数を**符号語 (codeword)** と呼ぶ。$(q-1)$ 個の係数 (符号語) のうち t 個が何らかの理由で壊れて別のものになっても，正しい符号 (多項式) に復元できるようになっている。q の値が大きければ，誤り訂正能力 t は大きくしたり，小さくしたりできる。

$q = 2^8$ のときの $\mathbb{F}_q = \mathbb{F}_2[x]/(f)$ ($f \in \mathbb{F}_2[x]$ は 8 次の既約多項式，例えば $f = 110000111 = x^8 + x^7 + x^2 + x + 1$) がよく使われるが，$\mathbb{F}_{929} = \{0, 1, 2, \cdots, 928\}$ を使った 2 次元バーコード (PDF417) もある。

定義 3.1.1（Reed-Solomon 符号） $\mathbb{F}_q$ の原始元 α を 1 つ決める。また「誤り訂正能力」t を 1 つ決める。

$$g(y) = (y-\alpha)(y-\alpha^2)\cdots(y-\alpha^{2t-1})(y-\alpha^{2t})$$

とする。

$$\begin{aligned} RS(q,t) &= \{f \in \mathbb{F}_q^{q-1} : \mathbb{F}_q[y] \text{ の要素として } f(y) \equiv 0 \pmod{g(y)}\} \\ &= \{f \in \mathbb{F}_q^{q-1} : \mathbb{F}_q \text{ において } f(\alpha^i) = 0 \ (i = 1, 2, \ldots, 2t)\} \end{aligned}$$

を **Reed-Solomon 符号** (の集合) と呼ぶ。$g(y)$ を $RS(q,t)$ の**生成多項式**と呼ぶ。

$RS(q,t)$ の要素はデータに対する符号の空間として用意されたものである。与えられたデータを $RS(q,t)$ の要素に変換する方法はいくつかあるが，次の方法がよく使われる。

定義 3.1.2（Reed-Solomon 符号への符号化） $RS(q,t)$ の生成多項式を g とする。$\mathbb{F}_q^{q-2t-1}$ の要素は次の方法で，$RS(q,t)$ の要素に変換される。

$f = (a_0, \ldots, a_{q-2t-2}) \in \mathbb{F}_q^{q-2t-1}$ に対し，次のように順に計算して，$\tilde{f}$ を求める。

$$
\begin{aligned}
f_1 &:= f \cdot y^{2t} = (a_0, \ldots, a_{q-2t-2}, \underbrace{0, \ldots, 0}_{2t \text{ 個}}) \\
r &:= f_1 \bmod g \\
\tilde{f} &:= f_1 + (-r) = (a_0, \ldots, a_{q-2t-2}, \underbrace{*, \ldots, *}_{-r})
\end{aligned}
$$

すると，$\tilde{f} \bmod g = 0$，すなわち $\tilde{f} \in RS(q,t)$ となる。

$\tilde{f}$ は f の係数ベクトルと $-r$ の係数ベクトルをつないだものになっている。

$-r$ という余分な情報をつけてデータを大きくすることにより，データの破損に対して強くしていることになる。

例 3.1.3 $RS(8,2)$ を考える。$\mathbb{F}_8 = \mathbb{F}_2[x]/(1011)$ と書ける。$\alpha = 10 = x$ とする。α のべきを計算すると次の表になる。

α	α^2	α^3	α^4	α^5	α^6	α^7
10	100	11	110	111	101	1

$$\alpha^3 = 10^3 \bmod 1011 = 1000 \bmod 1011 = 11,$$
$$\alpha^5 = (110 \times 10) \bmod 1011 = 111,$$
$$\alpha^6 = (111 \times 10) \bmod 1011 = 101,$$
$$\alpha^7 = (101 \times 10) \bmod 1011 = 1$$

となる。$RS(8,2)$ の生成多項式は

$$\begin{aligned} g(y) &= (y-\alpha)(y-\alpha^2)(y-\alpha^3)(y-\alpha^4) \\ &= (y+\alpha)(y+\alpha^2)(y+\alpha^3)(y+\alpha^4) \\ &= (y^2+\alpha^4 y+\alpha^3)(y^2+\alpha^6 y+1) \\ &= y^4+\alpha^3 y^3+y^2+\alpha y+\alpha^3 \end{aligned}$$

係数ベクトルは

$$\begin{aligned} g &= (1,\alpha^3,1,\alpha,\alpha^3) \\ &= (1,11,1,10,11) \end{aligned}$$

$RS(8,2)$ の要素は $g(y)$ を因数にもつ高々 6 次の多項式全体である。係数ベクトルの長さは 7(以下) である。

$\mathbb{F}_8^3$ の要素は次のように $RS(8,2)$ の要素に変換できる。

$\mathbb{F}_8$ の要素をすべて長さ 3 の 2 進列で表現することにすると $\mathbb{F}_8^3$ の要素は長さ 9 の 2 進列と考えられる。

$f = 010111101 = (010,111,101) = (\alpha,\alpha^5,\alpha^6)$ に対し,

$$\begin{aligned} f_1 &= f \cdot y^4 = (\alpha,\alpha^5,\alpha^6,0,0,0,0) \\ f_1 \bmod g &= (\alpha,0,0,\alpha^5) \\ \tilde{f} &= (\alpha,\alpha^5,\alpha^6,\alpha,0,0,\alpha^5) \\ &= 010\ 111\ 101\ 010\ 000\ 000\ 111 \end{aligned}$$

$f_1 \bmod g$ の計算は次の通りである。

$$
\begin{array}{rcccc|ccccc}
 & & & & & \alpha & 1 & \alpha^2 & & & \\
\hline
1 & \alpha^3 & 1 & \alpha & \alpha^3 & \alpha & \alpha^5 & \alpha^6 & 0 & 0 & 0 & 0 \\
 & & & & & \alpha & \alpha^4 & \alpha & \alpha^2 & \alpha^4 & & \\
\hline
 & & & & & & 1 & \alpha^5 & \alpha^2 & \alpha^4 & & \\
 & & & & & & 1 & \alpha^3 & 1 & \alpha & \alpha^3 & \\
\hline
 & & & & & & & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^3 & \\
 & & & & & & & \alpha^2 & \alpha^5 & \alpha^2 & \alpha^3 & \alpha^5 \\
\hline
 & & & & & & & & \alpha & 0 & 0 & \alpha^5
\end{array}
$$

命題 3.1.4　定義 3.1.2 の符号化法は，$\mathbb{F}_q^{q-2t-1}$ と $RS(q,t)$ の間の 1 対 1 対応を与えている。したがって，$RS(q,t)$ の要素数は q^{q-2t-1} である。

証明.　$\mathbb{F}_q^{q-1}$ に属するベクトルを多項式と見るとき，上位 $q-2t-1$ 個の係数を任意に決めても，下位の $2t$ 個の係数を調整すれば $RS(q,t)$ の要素にできることがこの符号化からわかる。

逆に 2 つの多項式 $f_1, f_2 \in R(q,t)$ の上位 $q-2t-1$ 個の係数が一致するならば，$f_1 - f_2$ は $2t-1$ 次以下の多項式になる。一方，$f_1 \equiv 0 \pmod{g}$，$f_2 \equiv 0 \pmod{g}$ より，$f_1 - f_2 \equiv 0 \pmod{g}$ となる。g が $2t$ 次で $f_1 - f_2$ が $2t-1$ 次以下なので，$(f_1 - f_2) \bmod g = f_1 - f_2$ となり，$f_1 = f_2$ である。□

3.2　Reed-Solomon 符号の誤り訂正能力

定義 3.2.1（Hamming 距離）　$f_1 = (a_0, a_1, \ldots, a_{m-1})$，$f_2 = (b_0, b_1, \ldots, b_{m-1})$ を $\mathbb{F}_q^m$ の要素とするとき，$\{i : a_i \neq b_i\}$ の要素の個数を f_1 と f_2 の $\mathbb{F}_q$ 上の **Hamming 距離**と呼ぶ。

$f_1, f_2 \in RS(q,t)$，$f_1 \neq f_2$ のとき，f_1 と f_2 の $\mathbb{F}_q$ 上の Hamming 距離が $2t+1$ 以上であることを示す。これがわかれば，$f \in RS(q,t)$ に対し，f の係数のいくつかが変更を受けて $f_1 \in \mathbb{F}_q^{q-1}$ となったとき，その変更を受けた係数の個数が t 以下のとき，f_1 と Hamming 距離が t 以下の $RS(q,t)$ の要

素はもとの f しかない。したがって，原理的には誤りを修正できる。

定義 3.2.2　α を $\mathbb{F}_q$ の原始元とする。$\Phi_\alpha : \mathbb{F}_q^{q-2t-1} \to \mathbb{F}_q^{q-1}$ を次のように定義する。$f \in \mathbb{F}_q^{q-2t-1}$ を 1 変数多項式 $f(y)$ と考えて，

$$\Phi_\alpha(f) = (f(\alpha^{q-2}), f(\alpha^{q-3}), \ldots, f(\alpha), f(1))$$

と定義する。変換 Φ を**離散的 Fourier 変換**と呼ぶ。

任意の $\mathbb{F}_q$ 係数多項式 f に対し，この $\Phi_\alpha(f)$ の定義は意味をもつ。

命題 3.2.3　次が成り立つ。

(1) $\{\Phi_\alpha(f) : f \in \mathbb{F}_q^{q-2t-1}\}$ の異なる要素の $\mathbb{F}_q$ 上の Hamming 距離は $2t+1$ 以上。
(2) Φ_α は 1 対 1 写像である。
(3) $RS(q,t) = \{\Phi_\alpha(f) : f \in \mathbb{F}_q^{q-2t-1}\}$.
(4) $RS(q,t)$ の異なる要素の $\mathbb{F}_q$ 上の Hamming 距離は $2t+1$ 以上。

証明. 以下，演算は $\mathbb{F}_q$ 上の多項式としての演算とする。また，Φ_α を単に Φ と書く。

(1) $f_1, f_2 \in \mathbb{F}_q^{q-2t-1}$ とすると，定義から $\Phi(f_1) - \Phi(f_2) = \Phi(f_1 - f_2)$ である。$\Phi(f_1) \neq \Phi(f_2)$ のとき，$f_3 = f_1 - f_2$ とすれば，$\Phi(f_1) - \Phi(f_2) = \Phi(f_3)$ で，$f_3 \neq 0$ である。

$$\Phi(f_3) = (f_3(\alpha^{q-2}), f_3(\alpha^{q-3}), \ldots, f_3(\alpha), f_3(1))$$

であるが，$f_3(y)$ は $q-2t-2$ 次以下の 0 でない多項式だったので，その根 ($f_3(y) = 0$ となる y の個数) は高々 $q-2t-2$ 個である。すなわち，$\Phi(f_3)$ の成分 (係数) のうち，0 となるものは高々 $q-2t-2$ 個となり，残りの成分は 0 でない。$(q-1) - (q-2t-2) = 2t+1$ なので，$\Phi(f_3)$ の $2t+1$ 個以上の成分は 0 でない。これは，$\Phi(f_1)$ と $\Phi(f_2)$ の Hamming 距離が $2t+1$ 以上であることを意味する。

(2) $f_1 \neq f_2$ とする。$\Phi(f_1) \neq \Phi(f_2)$ を示せばよい。$f_3 = f_1 - f_2$ とすると $f_3 \neq 0$ である。(1) の議論から，$\Phi(f_1) - \Phi(f_2) = \Phi(f_3) \neq 0$ である。したがって，$\Phi(f_1) \neq \Phi(f_2)$ である。

(3) 定義より，$f_1, f_2 \in \mathbb{F}_q^{q-2t-1}$ に対し，$\Phi(f_1 + f_2) = \Phi(f_1) + \Phi(f_2)$ で，さらに，$c \in \mathbb{F}_q$ とすると $\Phi(cf_1) = c\Phi(f_1)$ である。$f \in \mathbb{F}_q^{q-2t-1}$ は

$$f(y) = c_0 y^{q-2t-2} + c_1 y^{q-2t-3} + \cdots + c_{q-2t-3} y + c_{q-2t-2}$$

と書けるので，$f(y) = y^j$ $(j = 0, 1, \ldots, q-2t-2)$ のときに，$\Phi(f) \in RS(q, d)$ を示せばよい ($RS(q, t)$ が多項式の和と $\mathbb{F}_q$ の要素倍の演算で閉じていることも定義からすぐにわかる)。$h = \Phi(f)$ とすると，

$$\begin{aligned} h = \Phi(f) &= ((\alpha^{q-2})^j, (\alpha^{q-3})^j, \ldots, \alpha^j, 1^j) \\ &= ((\alpha^j)^{q-2}, (\alpha^j)^{q-3}, \ldots, \alpha^j, 1). \end{aligned}$$

h を y の関数の形で書くと

$$\begin{aligned} h(y) &= (\alpha^j)^{q-2} y^{q-2} + (\alpha^j)^{q-3} y^{q-3} + \cdots + \alpha^j y + 1 \\ &= (\alpha^j y)^{q-2} + (\alpha^j y)^{q-3} + \cdots + \alpha^j y + 1. \end{aligned}$$

主張 1　$h(\alpha) = h(\alpha^2) = \cdots = h(\alpha^{2t}) = 0.$

$h(y) = y^j$ で，j は $0, 1, \ldots, q - 2t - 2$ のどれかである。$1 \leq k \leq 2t$ とすると，$1 \leq j + k \leq q - 2$ である。

$$\begin{aligned} h(\alpha^k) &= (\alpha^j \alpha^k)^{q-2} + (\alpha^j \alpha^k)^{q-3} + \cdots + \alpha^j \alpha^k + 1 \\ &= (\alpha^{j+k})^{q-2} + (\alpha^{j+k})^{q-3} + \cdots + \alpha^{j+k} + 1. \end{aligned}$$

さて，$\alpha^{q-1} = 1$ だったので，$(\alpha^{q-1})^{j+k} = 1$ である。よって，$(\alpha^{j+k})^{q-1} = 1$ となる。$\beta = \alpha^{j+k}$ とすると，α の位数が $q-1$ であることと $1 \leq j+k \leq q-2$ より，$\beta \neq 1$ かつ $\beta^{q-1} - 1 = 0$ である。

$$(\beta - 1)(\beta^{q-2} + \beta^{q-3} + \cdots \beta + 1) = \beta^{q-1} - 1 = 0$$

と $\beta - 1 \neq 0$ より，

$$\beta^{q-2} + \beta^{q-3} + \cdots \beta + 1 = 0$$

となる。すなわち， $h(\alpha^k) = 0$ である。

Φ が単射だったので，$\{\Phi(f) : f \in \mathbb{F}_q^{q-2t-1}\}$ の要素の個数は q^{q-2t-1} である。一方，命題 3.1.4 より，$RS(q,t)$ の要素の個数も q^{q-2t-1} である。$\{\Phi(f) : f \in \mathbb{F}_q^{q-2t-1}\} \subset RS(q,t)$ なので，この 2 つの集合は一致する。 □

例 3.2.4　例 3.1.3 の $RS(8,2)$ を考える。$\mathbb{F}_8 = \mathbb{F}_2[x]/(1011)$ で，$\alpha = 10$ である。例 3.1.3 より，

$$(\alpha, \alpha^5, \alpha^6, \alpha, 0, 0, \alpha^5) \in RS(8,2)$$

であった。

$$h = (\alpha^3, 1, \alpha^6) \quad (h(y) = \alpha^3 y^2 + y + \alpha^6)$$

とすると

$$\Phi_\alpha(h) = (\alpha, \alpha^5, \alpha^6, \alpha, 0, 0, \alpha^5)$$

である。実は $c = (\alpha, \alpha^5, \alpha^6, \alpha, 0, 0, \alpha^5)$ とすると

$$\Phi_{\alpha^{-1}}(c) = h$$

である。

一般に，$\mathbb{F}_q$ の原始元 α と $f \in \mathbb{F}_q^{q-1}$ に対し，

$$-\Phi_{\alpha^{-1}}(\Phi_\alpha(f)) = f, \quad -\Phi_\alpha(\Phi_{\alpha^{-1}}(f)) = f$$

である。$\mathbb{F}_2$ がベースの場合は $-1 = 1$ なので，符号の $-$ は必要ない。

3.3 Reed-Solomon 符号の誤り訂正

$RS(q,t)$ のデータに t 箇所以下の誤りが生じたとき (送信中に雑音がはいる，CD にきずがつく，バーコードがかすれる，読取で少し失敗する等)，それを復元する方法を述べる。この方法はいくつも提案されているが，ここではユークリッドの互除法を使う方法を紹介する。

ここでは，添字の付け方を多項式の次数にあわせる。

$f = (c_{q-2}, c_{q-3}, \ldots, c_1, c_0) \in RS(q,t)$ に誤りが生じて f_1 になったとする。変更を受けた係数の位置 (次数) の集合を I とすると $f_1(y) = f(y) + \sum_{i \in I} e_i y^i$ $(e_i \in \mathbb{F}_q)$ となる。$e(y) = \sum_{i \in I} e_i y^i$ を**誤り多項式**と呼ぶ。誤り多項式が求まればもとのデータが復元できる。

最初に方法を述べ，なぜ求まるかはあとで説明する。

誤り多項式の求め方

$f(y) \in RS(q,t)$，$\alpha \in \mathbb{F}_q$ を $RS(q,t)$ で使う原始元とする。$f_1(y) = f(y) + e(y)$ で，$e(y)$ の 0 でない係数をもつ次数の集合を I とすると，

$$e(y) = \sum_{i \in I} e_i y^i$$

である。$|I| \leq t$ のとき，誤り位置の集合 I と係数 e_i を求めるのが目標となる。

$S := (f_1(\alpha^{2t}), f_1(\alpha^{2t-1}), \ldots, f_1(\alpha))$ とする。

S を多項式と考える。すると，$2t-1$ 次以下の多項式になる。もし，誤りがなければ (すなわち $e(y) = 0$ ならば) $RS(q,t)$ の定義より，$S(y) = 0$ である。以下，$S(y) \neq 0$，すなわち誤りがあったとする。

$S = S(y)$ をシンドローム多項式と呼ぶ。

次に，

$$y^{2t} \equiv 0 \cdot S(y) \pmod{y^{2t}} \tag{1}$$

$$S(y) \equiv 1 \cdot S(y) \pmod{y^{2t}} \tag{2}$$

の左辺に対してユークリッドの互除法を適用して，

$$\Omega(y) \equiv \Lambda(y) \cdot S(y) \pmod{y^{2t}} \tag{3}$$

となる互いに素な多項式 $\Omega(y)$ と $\Lambda(y)$ を

$$\deg \Lambda(y) \leq t, \quad \deg \Omega(y) < \deg \Lambda(y)$$

となるように求める。この方程式は**鍵方程式** (key equation) と呼ばれる。$|I| \leq t$ のとき，ユークリッドの互除法により解が必ず求まることが知られている。さらに，$\Lambda(0)^{-1}$($\mathbb{F}_q$ における乗法の逆元) を (3) の両辺にかけ，$\Lambda(y)$ の定数項が 1 になるようにしておく。

$\Lambda(y) = 0$ の $\mathbb{F}_q$ における解をすべて求める。実は，

$$\Lambda(y) = \prod_{i \in I} (1 - \alpha^i y) \quad (I \text{ は誤りの位置})$$

となっており，$\Lambda(y) = 0$ の根は丁度 $\{\alpha^{-i} : i \in I\}$ である。よって，

$$i \in I \iff \Lambda(\alpha^{-i}) = 0$$

である。これで，誤り位置 I がわかる。$\Lambda(y)$ を誤り位置検出多項式 (error locator polynomial) と呼ぶ。

さらに，$i \in I$ に対し，$e(y)$ の y^i の係数 e_i は，

$$\Omega(\alpha^{-i}) = e_i \alpha^i \chi_i(\alpha^{-i}), \quad \chi_i(y) = \prod_{j \in I, j \neq i} (1 - \alpha^j y)$$

により求まる。

例 3.3.1　$f = (\alpha, \alpha^5, \alpha^6, \alpha, 0, 0, \alpha^5)$ に誤りが生じて，$f_1 = (\alpha, \alpha^5, \alpha^4, \alpha, 0, \alpha^2, \alpha^5)$ になったとする。わかっているの f_1 でけである。誤り多項式は

$e(y) = \alpha^3 y^4 + \alpha^2 y$ であるが，これはまだわからない。まず，

$$S = (f_1(\alpha^4), f_1(\alpha^3), f_1(\alpha^2), f_1(\alpha)) = (\alpha, \alpha^6, 0, \alpha)$$

である。

$$y^4 \equiv 0 \cdot S(y) \pmod{y^4} \tag{1}$$

$$\alpha y^3 + \alpha^6 y^2 + \alpha \equiv 1 \cdot S(y) \pmod{y^4} \tag{2}$$

の左辺に着目してユークリッドの互除法の計算を行う。

$$\begin{array}{cccc} & & \alpha^6 & \alpha^4 \\ \alpha & \alpha^6 \quad 0 \quad \alpha &) \, 1 & 0 \quad 0 \quad 0 \quad 0 \\ & & 1 & \alpha^5 \quad 0 \quad 1 \\ \hline & & & \alpha^5 \quad 0 \quad 1 \\ & & & \alpha^5 \quad \alpha^3 \quad 0 \quad \alpha^5 \\ \hline & & & \alpha^3 \quad 1 \quad \alpha^5 \end{array}$$

を使って，$(1) - (2) \times (\alpha^6 y + \alpha^4)$ (両辺の演算) を考えると

$$\alpha^3 y^2 + y + \alpha^5 \equiv (\alpha^6 y + \alpha^4) \cdot S(y) \pmod{y^4} \tag{3}$$

次に

$$\begin{array}{cccc} & & \alpha^5 & \alpha^5 \\ \alpha^3 & 1 \quad \alpha^5 &) \, \alpha & \alpha^6 \quad 0 \quad \alpha \\ & & \alpha & \alpha^5 \quad \alpha^3 \\ \hline & & & \alpha \quad \alpha^3 \quad \alpha \\ & & & \alpha \quad \alpha^5 \quad \alpha^3 \\ \hline & & & \alpha^2 \quad 1 \end{array}$$

を使って，$(2) - (3) \times (\alpha^5 y + \alpha^5)$ を考えると

$$\alpha^2 y + 1 \equiv (\alpha^4 y^2 + \alpha y + \alpha^6) \cdot S(y) \pmod{y^4} \tag{4}$$

となる。左辺の次数が右辺の S の係数の次数より低くなったので，鍵方程式の解が得られた。(実は，左辺と右辺の S の係数が互いに素という条件は自動的に満たされている。) α^6 の逆元である α を (4) の両辺にかけると，

$$\alpha^3 y + \alpha \equiv (\alpha^5 y^2 + \alpha^2 y + 1) \cdot S(y) \pmod{y^4}$$

次に誤り位置検出多項式 $\Lambda(y) = \alpha^5 y^2 + \alpha^2 y + 1$ の根を求める。$y = \alpha, \alpha^2, \ldots$ について調べると，$y = \alpha^3$ のとき，$\Lambda(y) = 0$ となる。$(\alpha^3)^{-1} = \alpha^4$ なので，4 次の係数が誤りの 1 つである。$\alpha^4 y - 1$ で $\Lambda(y)$ は割り切れ，$\Lambda(y) = (\alpha y - 1)(\alpha^4 y - 1)$ となる。

すなわち，誤りが 1 次と 4 次の係数であることがわかった。誤り多項式を

$$e(y) = e_4 y^4 + e_1 y$$

と置くと，

$$\alpha^3 y + \alpha = e_1 \alpha(\alpha^4 y + 1) + e_4 \alpha^4(\alpha y + 1)$$

となる (理由は次節)。$y = \alpha^{-1}$ を代入すると，$\alpha^2 + \alpha = e_1 \alpha(\alpha^3 + 1)$ となり，$e_1 = \alpha^2$ が得られる。

$y = \alpha^{-4}$ を代入すると，$\alpha^{-1} + \alpha = e_4 \alpha^4(\alpha^{-3} + 1)$ となり，$e_4 = \alpha^3$ が得られる。

これで，誤り多項式

$$e(y) = \alpha^3 y^4 + \alpha^2 y$$

が求まる。

誤り多項式が求まる理由

上の「誤り多項式の求め方」を詳しく分析する。鍵方程式の解の存在と一意性がポイントとなる。

以下，$f(y) \in RS(q,t)$，$\alpha \in \mathbb{F}_q$ を $RS(q,t)$ で使う原始元とする。$f_1(y) = f(y) + e(y)$ で，$e(y) = \sum_{i \in I} e_i y^i$，$i \in I$ ならば $e_i \neq 0$ とする。さらに，$|I| \leq t$ とする。

定理 3.3.2　$S := (f_1(\alpha^{2t}), f_1(\alpha^{2t-1}), \ldots, f_1(\alpha))$ とする。鍵方程式

$$\begin{aligned}
&\Omega(y) \equiv \Lambda(y) \cdot S(y) \pmod{y^{2t}} \\
&\deg \Lambda(y) \leq t, \quad \deg \Omega(y) < \deg \Lambda(y) \\
&\Omega(y) \text{ と } \Lambda(y) \text{ は互いに素}
\end{aligned}$$

に対し，次が成り立つ。

(1)　この方程式の 1 つの解は

$$\Lambda(y) = \prod_{j \in I}(1 - \alpha^j y), \quad \Omega(y) = \sum_{i \in I} e_i \alpha^i \chi_i(y)$$

$$\text{ここで,} \quad \chi_i(y) = \prod_{j \in I, j \neq i}(1 - \alpha^j y) = \frac{\Lambda(y)}{1 - \alpha^i y}$$

であり，解はこれだけである。

(2)　この方程式は,

$$\begin{aligned}
y^{2t} &\equiv 0 \cdot S(y) \pmod{y^{2t}} \\
S(y) &\equiv 1 \cdot S(y) \pmod{y^{2t}}
\end{aligned}$$

の左辺に着目して y^{2t} と $S(y)$ の最大公約数 (公因子) をユークリッドの互除法で求めようとすると途中で鍵方程式の解を得る。$y^{2t}/S(y)$ の商を $q_2(y)$，余りを $r_2(y)$ とすると

$$y^{2t} = q_2(y) \cdot S(y) + r_2(y)$$

となるが，上の連立方程式は

$$\begin{aligned}
S(y) &\equiv 1 \cdot S(y) \pmod{y^{2t}} \\
r_2(y) &\equiv -q_2(y) \cdot S(y) \pmod{y^{2t}}
\end{aligned}$$

と同値となる。この操作を次数の条件が満たされるまで繰り返すと解が得られる。

証明. (1) $1 \leq j \leq 2t$ のとき, $f(\alpha^j) = 0$ なので, $f_1(\alpha^j) = f(\alpha^j) + e(\alpha^j) = e(\alpha^j)$ である。成分毎に考えると

$$S = (e(\alpha^{2t}), e(\alpha^{2t-1}), \ldots, e(\alpha))$$

である。$i \in I$ に対し,

$$S_i = (e_i \cdot (\alpha^{2t})^i, e_i \cdot (\alpha^{2t-1})^i, \ldots, e_i \cdot \alpha^i)$$

とすると

$$S = \sum_{i \in I} S_i$$

である。各 i について $S_i(y)$ は等比級数になっており，その和は簡単な形である。高校で習うのは実数の場合であるが，同じ議論がこの場合もできる。

$$S_i(y) = e_i \alpha^i ((\alpha^i y)^{2t-1} + (\alpha^i y)^{2t-2} + \ldots + \alpha^i y + 1)$$

であるが

$$\alpha^i y S_i(y) = e_i \alpha^i ((\alpha^i y)^{2t} + (\alpha^i y)^{2t-1} + \ldots + (\alpha^i y)^2 + \alpha^i y)$$

として両辺を引くと

$$(1 - \alpha^i y) S_i(y) = e_i \alpha^i (1 - (\alpha^i y)^{2t})$$

となり,

$$(1 - \alpha^i y) S_i(y) \equiv e_i \alpha^i \pmod{y^{2t}}$$

である。

以下の議論は $1/(1 - \alpha^i y)$ の $i \in I$ に関する和を念頭に行なう。通分の操作から次の $\chi_i(y)$ を考えるのが自然である。

$\chi_i(y) = \prod_{j \in I, j \neq i} (1 - \alpha^j y)$ に対し $\chi_i(y)(1 - \alpha^i y) = \prod_{j \in I} (1 - \alpha^j y)$ なので，上の両辺に $\chi_i(y)$ をかけると

$$\left(\prod_{j \in I} (1 - \alpha^j y) \right) S_i(y) \equiv e_i \alpha^i \chi_i(y) \pmod{y^{2t}}$$

である。$i \in I$ すべてについて両辺の和をとると

$$\left(\prod_{j\in I}(1-\alpha^j y)\right) S(y) \equiv \sum_{i\in I} e_i \alpha^i \chi_i(y) \pmod{y^{2t}}$$

ここで，$\prod_{j\in I}(1-\alpha^j y)$ は $|I|$ 次式 ($|I| \leq t$) で，$\sum_{i\in I} e_i\alpha^i\chi_i(y)$ は $|I|-1$ 次以下の式である。

また，$\prod_{j\in I}(1-\alpha^j y)$ の因数は 1 次式 $1-\alpha^j y$ $(j \in I)$ のみであるが，$\sum_{i\in I} e_i\alpha^i\chi_i(y)$ に α^{-j} $(j \in I)$ を代入すると，

$$\sum_{i\in I} e_i\alpha^i\chi_i(\alpha^{-j}) = e_j\alpha^j\chi_j(\alpha^{-j}) \neq 0$$

である。したがって，因数定理より，$\prod_{j\in I}(1-\alpha^j y)$ と $\sum_{i\in I} e_i\alpha^i\chi_i(y)$ は互いに素であることがわかる。

以上より，

$$\Lambda(y) = \prod_{j\in I}(1-\alpha^j y), \quad \Omega(y) = \sum_{i\in I} e_i\alpha^i\chi_i(y)$$

が鍵方程式の 1 つの解であることがわかる。

主張 1　鍵方程式の解は定数倍を除いて 1 組しかない。すなわち，

$$\Omega_1(y) \equiv \Lambda_1(y)\cdot S(y) \pmod{y^{2t}}$$
$$\Omega_2(y) \equiv \Lambda_2(y)\cdot S(y) \pmod{y^{2t}}$$

でどちらも鍵方程式の条件を満たすならば，

$$\Omega_2(y) = c\Omega_1(y), \quad \Lambda_2(y) = c\Lambda_1(y)$$

となる $c \in \mathbb{F}_q$ が存在する。

鍵方程式の解として $\Lambda(y) = \Lambda_1(y)$，$\Omega(y) = \Omega_1(y)$ と $\Lambda(y) = \Lambda_2(y)$，$\Omega(y) = \Omega_2(y)$ があったとする。すると，

$$\Omega_1(y) \equiv \Lambda_1(y) \cdot S(y) \pmod{y^{2t}} \quad \text{(a)}$$
$$\Omega_2(y) \equiv \Lambda_2(y) \cdot S(y) \pmod{y^{2t}} \quad \text{(b)}$$

であるが，(a) の両辺に $\Lambda_2(y)$ をかけ，(b) の両辺に $\Lambda_1(y)$ をかけると

$$\Lambda_2(y)\Omega_1(y) \equiv \Lambda_2(y)\Lambda_1(y) \cdot S(y) \pmod{y^{2t}}$$
$$\Lambda_1(y)\Omega_2(y) \equiv \Lambda_1(y)\Lambda_2(y) \cdot S(y) \pmod{y^{2t}}$$

となる。両辺同士を引くと

$$\Lambda_2(y)\Omega_1(y) - \Lambda_1(y)\Omega_2(y) \equiv 0 \pmod{y^{2t}}.$$

この左辺は $2t-1$ 次以下の多項式なので，多項式として

$$\Lambda_2(y)\Omega_1(y) - \Lambda_1(y)\Omega_2(y) = 0.$$

すなわち，

$$\Lambda_2(y)\Omega_1(y) = \Lambda_1(y)\Omega_2(y).$$

体係数の 1 変数多項式については，既約因子分解の一意性が定数倍 (係数体の要素倍) を除いて成り立つことが知られている (証明は，整数の素因数分解の一意性の証明と同様で，割り算の原理が本質的である)。$\Omega_1(y)$ と $\Lambda_1(y)$ が互いに素なので $\Omega_1(y)$ は $\Omega_2(y)$ を割り切る。また，$\Omega_2(y)$ と $\Lambda_2(y)$ も互いに素なので，$\Omega_2(y)$ は $\Omega_1(y)$ を割り切る。したがって，次数を考えると，$\Omega_2(y)$ は $\Omega_1(y)$ の定数倍である。同様に，$\Lambda_2(y)$ も $\Lambda_1(y)$ の定数倍である。$\Omega_2(y) = c\Omega_1(y)$，$\Lambda_2(y) = c'\Lambda_1(y)$ $(c, c' \in \mathbb{F}_q - \{0\})$ とすると

$$c'\Lambda_1(y)\Omega_1(y) = c\Lambda_1(y)\Omega_1(y)$$

となり，$c = c'$ がわかる。

(2) 証明の概略だけ述べる。連立合同式ではなく，次の連立方程式で考える。

$$y^{2t} = 1 \cdot y^{2t} + 0 \cdot S(y) \quad \text{(a)}$$
$$S(y) = 0 \cdot y^{2t} + 1 \cdot S(y) \quad \text{(b)}$$

この左辺に着目してユークリッドの互除法を繰り返す。すなわち，上の式を

$$r_0(y) = a_0(y) \cdot y^{2t} + b_0(y) \cdot S(y) \quad \text{(a)}$$
$$r_1(y) = a_1(y) \cdot y^{2t} + b_1(y) \cdot S(y) \quad \text{(b)}$$

と考え，

$$r_{i-1}(y) = a_{i-1}(y) \cdot y^{2t} + b_{i-1}(y) \cdot S(y)$$
$$r_i(y) = a_i(y) \cdot y^{2t} + b_i(y) \cdot S(y)$$

が得られているとき，$r_{i-1}(y) = q_i(y)r_i(y) + r_{i+1}(y)$, $\deg r_{i+1} < \deg r_i$ となるように割り算で分解し，$a_{i+1}(y) = a_{i-1}(y) - q_i(y)a_i(y)$，$b_{i+1}(y) = b_{i-1}(y) - q_i(y)b_i(y)$ として，

$$r_{i+1}(y) = a_{i+1}(y) \cdot y^{2t} + b_{i+1}(y) \cdot S(y)$$

を導く。すると，数学的帰納法により次の主張 2 と主張 3 が証明できる。

主張 2　$i \geq 1$ のとき，

$$\deg b_{i+1}(y) = \deg r_0(y) - \deg r_i(y) = 2t - \deg r_i(y),$$
$$\deg b_{i+1}(y) > \deg b_i(y), \quad \deg r_{i+1}(y) < r_i(y).$$

主張 3

$$\begin{cases} y^{2t} = 1 \cdot y^{2t} + 0 \cdot S(y) \\ S(y) = 0 \cdot y^{2t} + 1 \cdot S(y) \end{cases}$$

$$\Longleftrightarrow$$

$$\begin{cases} r_i(y) = a_i(y) \cdot y^{2t} + b_i(y) \cdot S(y) \\ r_{i+1}(y) = a_{i+1}(y) \cdot y^{2t} + b_{i+1}(y) \cdot S(y) \end{cases}$$

である。しかも，各等式の両辺を多項式倍して，辺々を加えることにより，どちらの方向も導ける。

$r_i(y)$ の次数は i が大きくなるほど下がっていき，$r_i(y)$ が y^{2t} と $S(y)$ の最大公約数になったあと 0 になって終わる。

$r_i(y) = 0$ のとき，$\deg b_i(y) > 1$ である。よって，$\deg r_i(y) < \deg b_i(y)$ となる最小の i がとれる。それを i_0 としよう。取り方より，$\deg r_{i_0-1}(y) \geq \deg b_{i_0-1}(y)$ である。

主張 4

$$R(y) = A(y) \cdot y^{2t} + B(y) \cdot S(y), \quad \deg R(y) < \deg B(y)$$

とすると，

$$\deg b_{i_0}(y) \leq \deg B(y).$$

主張 3 により，

$$r_{i_0-1}(y) = a_{i_0-1}(y) \cdot y^{2t} + b_{i_0-1}(y) \cdot S(y)$$
$$r_{i_0}(y) = a_{i_0}(y) \cdot y^{2t} + b_{i_0}(y) \cdot S(y)$$

に対し，ある多項式 $u_0(y)$ と $v_0(y)$ が存在して，

$$\begin{array}{rrcrcr} & u_0(y)r_{i_0-1}(y) & = & u_0(y)a_{i_0-1}(y) \cdot y^{2t} & + & u_0(y)b_{i_0-1}(y) \cdot S(y) \\ +) & v_0(y)r_{i_0}(y) & = & v_0(y)a_{i_0}(y) \cdot y^{2t} & + & v_0(y)b_{i_0}(y) \cdot S(y) \\ \hline & y^{2t} & = & 1 \cdot y^{2t} & + & 0 \cdot S(y) \end{array}$$

さらにある多項式 $u_1(y)$ と $v_1(y)$ が存在して，

$$\begin{array}{rrrrrr} u_1(y)r_{i_0-1}(y) & = & u_1(y)a_{i_0-1}(y)\cdot y^{2t} & + & u_1(y)b_{i_0-1}(y)\cdot S(y) \\ +) \quad v_1(y)r_{i_0}(y) & = & v_1(y)a_{i_0}(y)\cdot y^{2t} & + & v_1(y)b_{i_0}(y)\cdot S(y) \\ \hline y^{2t} & = & 0\cdot y^{2t} & + & 1\cdot S(y) \end{array}$$

よって，ある多項式 $u(y)$ と $v(y)$ が存在して，

$$\begin{array}{rrrrrr} u(y)r_{i_0-1}(y) & = & u(y)a_{i_0-1}(y)\cdot y^{2t} & + & u(y)b_{i_0-1}(y)\cdot S(y) \\ +) \quad v(y)r_{i_0}(y) & = & v(y)a_{i_0}(y)\cdot y^{2t} & + & v(y)b_{i_0}(y)\cdot S(y) \\ \hline R(y) & = & A(y)\cdot y^{2t} & + & B(y)\cdot S(y) \end{array}$$

$\deg B < \deg b_{i_0}$ とすると，$v(y)b_{i_0}(y)$ と $u(y)b_{i_0-1}(y)$ の次数が同じでなければ和の次数はさがらない。主張 2 より，$\deg b_{i_0}(y) > \deg b_{i_0-1}(y)$ なので，$\deg u(y) > \deg v(y)$ かつ $\deg u(y) \geq \deg b_{i_0}(y) - \deg b_{i_0-1}(y)$ である。よって，

$$\deg u(y) + \deg r_{i_0-1}(y) \geq \deg u(y) + \deg b_{i_0-1}(y) \geq \deg b_{i_0}(y).$$

一方，$\deg u(y)r_{i_0-1}(y) > \deg v(y)r_{i_0}(y)$ なので，$\deg R(y) = \deg u(y)r_{i_0-1}(y) = \deg u(y) + \deg r_{i_0-1}(y)$.

$\deg R(y) < \deg B(y) < \deg b_{i_0}$ より，$\deg u(y) + \deg r_{i_0-1}(y) < \deg b_{i_0}$. これは矛盾である。

主張 4 が示された。

鍵方程式で次数の条件を満たしているものがあるので，$\deg b_{i_0}(y) \leq t$ である。したがって，主張 2 より，$\deg r_{i_0-1}(y) \geq t$ である。

今度は，鍵方程式の解があるとすると，それは，ある $u(y)$ と $v(y)$ を使って次のように得られる。

$$\begin{array}{rrrrrr} u(y)r_{i_0-1}(y) & = & u(y)a_{i_0-1}(y)\cdot y^{2t} & + & u(y)b_{i_0-1}(y)\cdot S(y) \\ +) \quad v(y)r_{i_0}(y) & = & v(y)a_{i_0}(y)\cdot y^{2t} & + & v(y)b_{i_0}(y)\cdot S(y) \\ \hline R(y) & = & A(y)\cdot y^{2t} & + & B(y)\cdot S(y) \end{array}$$

このとき，$u(y) \neq 0$ とすると，$\deg R(y) < t$ なので，$\deg v(y)r_{i_0}(y) = \deg u(y)r_{i_0-1}(y)$ である必要がある。

$\deg r_{i_0}(y) < \deg r_{i_0-1}(y)$ なので，$\deg v(y) > \deg u(y)$ である。さらに，

$\deg v(y) + \deg r_{i_0}(y) = \deg u(y)r_{i_0-1}(y) \geq t.$

$\deg b_{i_0}(y) > \deg b_{i_0-1}(y)$ と $\deg v(y) > \deg u(y)$ より，

$$\begin{aligned}\deg B(y) &= \deg(u(y)b_{i_0-1}(y) + v(y)b_{i_0}(y)) \\ &= \deg v(y)b_{i_0}(y) \\ &= \deg v(y) + \deg b_{i_0}(y) \\ &> \deg v(y) + \deg r_{i_0}(y) \\ &\geq t.\end{aligned}$$

これは，$B(y)$ が鍵方程式の解の一部で $\deg B(y) \leq t$ であることに反する。

従って，左辺が $r_{i_0}(y)$ の式の多項式倍で，鍵方程式の解が得られるはずである。もし，$r_{i_0}(y)$ と $b_{i_0}(y)$ が互いに素でないとすると，鍵方程式の解も互いに素でないことになり矛盾する。したがって，$r_{i_0}(y)$ と $b_{i_0}(y)$ は互いに素であり，鍵方程式の定数倍を除いて一意になる解であることがわかる。 □

例

q 元体 $\mathbb{F}_q$ の原始元 α をとり，$RS(q,2)$ を考える。すなわち，誤り訂正能力 2 の場合を考える。

$$f \in RS(q,2) \iff f(\alpha) = f(\alpha^2) = f(\alpha^3) = f(\alpha^4) = 0$$

である。

Reed-Solomon 符号 f に対し誤り E が加わって，f_1 になったとする。

シンドローム多項式 $S(y)$ は次の通りである。

$$\begin{aligned}S(y) &= f_1(\alpha^4)y^3 + f_1(\alpha^3)y^2 + f_1(\alpha^2)y + f_1(\alpha) \\ &= E(\alpha^4)y^3 + E(\alpha^3)y^2 + E(\alpha^2)y + E(\alpha).\end{aligned}$$

誤り位置が 2 箇所以内の誤り訂正には，次の**鍵方程式**の解 $\Omega(y)$，$\Lambda(y)$ を求めればよい。

$\Omega(y) \equiv \Lambda(y)S(y) \pmod{y^4}$
$\deg \Omega(y) < \deg \Lambda(y) \leq 2$
$\Omega(y)$ と $\Lambda(y)$ は互いに素

誤り箇所が誤り訂正能力以下の場合は，この鍵方程式の解は定数倍を除いて一意的である。

さて，$E(y)$ の y^a の係数が $e_a \neq 0$ だったとする。

$S_a(y) = e_a\alpha^a(1 + \alpha^a y + \alpha^{2a}y^2 + \alpha^{3a}y^3)$
とおいて両辺を $\alpha^a y$ 倍すると
$\alpha^a y S_a(y) = e_a\alpha^a(\alpha^a y + \alpha^{2a}y^2 + \alpha^{3a}y^3 + \alpha^{4a}y^4)$
両辺をそれぞれ引くと
$(1 - \alpha^a y)S_a(y) = e_a\alpha^a(1 - \alpha^{4a}y^4)$
となるので
$e_a\alpha^a \equiv (1 - \alpha^a y)S_a(y) \pmod{y^4}$.

(i) 誤り箇所が 1 つの場合，$E(y) = e_a y^a$，$S(y) = S_a(y)$ と書けるので，鍵方程式の解は定数倍を除いて

$e_a\alpha^a \equiv (1 - \alpha^a y)S(y) \pmod{y^4}$

だけである。

事実 1.

誤り箇所が 2 つ以内で，

$C \equiv (1 - Ay)S(y) \pmod{y^4}$ $(A, C \in \mathbb{F}_q)$

が成り立つとき，

$E(y) = e_a y^a$ (誤り箇所は 1 つ)，
$C = e_a\alpha^a$，$A = \alpha^a$ と書ける。

(ii) 誤り箇所が 2 つの場合，$E(y) = e_a y^a + e_b y^b$，
$S(y) = S_a(y) + S_b(y)$ と書ける。

$e_a\alpha^a \equiv (1 - \alpha^a y)S_a(y) \pmod{y^4}$,

$e_b\alpha^b \equiv (1-\alpha^b y)S_b(y) \pmod{y^4}$

より，

$e_a\alpha^a(1-\alpha^b y) + e_b\alpha^b(1-\alpha^a y)$

$\equiv (1-\alpha^a y)(1-\alpha^b y)S(y) \pmod{y^4}$

鍵方程式の解は定数倍を除いてこれだけである。

事実 2.

誤り箇所が 2 つ以内で，

$Cy + D \equiv (Ay^2 + By + 1)S(y) \pmod{y^4}$

$A, B, C, D \in \mathbb{F}_8$，$Cy + D$ と $Ay^2 + By + 1$ は互いに素

が成り立つとき，

$E(y) = e_a y^a + e_b y^b$ (誤り箇所は 2 つ)，

$Ay^2 + By + 1 = (1-\alpha^a y)(1-\alpha^b y)$,

$Cy + D = e_a\alpha^a(1-\alpha^b y) + e_b\alpha^b(1-\alpha^a y)$.

と書ける。

例 1. $\mathbb{F}_q = \mathbb{F}_8 = \mathbb{F}_2[x]/(1011) = \{0, 1, 10, 11, 100, 101, 110, 111\}$

で考える。1011 は $x^3 + x + 1$ のこと (係数ベクトル) である。$\mathbb{F}_8$ の要素は係数ベクトルで表現された 2 次以下の $\mathbb{F}_2$ 係数多項式である。和 $+$ は $\mathbb{F}_2$ 係数多項式としての和 (桁ごとの　mod 2 の和) で，積 $\cdot$ は $\mathbb{F}_2$ 係数多項式としてかけた後に 1011 で割った余りをとる演算とする。$\alpha = 10$ とすると，α のべきは次の表で表される。下の段が上の式の値である。

α	α^2	α^3	α^4	α^5	α^6	α^7
10	100	11	110	111	101	1

さて，$RS(8, 2)$ の Reed-Solomon 符号を受信したところ，

$f_1 = (\alpha, \alpha, \alpha^6, \alpha, 0, 0, \alpha^5)$

であったとする。シンドローム多項式の係数を計算すると

$$
\begin{aligned}
f_1(\alpha) &= \alpha \cdot \alpha^6 + \alpha \cdot \alpha^5 + \alpha^6 \cdot \alpha^4 + \alpha \cdot \alpha^3 + \alpha^5 \\
&= 1 + \alpha^6 + \alpha^3 + \alpha^4 + \alpha^5 \\
&= 1 + 101 + 11 + 110 + 111 \\
&= \alpha^4, \\
f_1(\alpha^2) &= \alpha^2, \\
f_1(\alpha^3) &= 1, \\
f_1(\alpha^4) &= \alpha^5
\end{aligned}
$$

となる。ユークリッドの互除法により，鍵方程式の解を求める。

(1) $y^4 \equiv 0 \cdot S(y) \pmod{y^4}$

(2) $\alpha^5 y^3 + y^2 + \alpha^2 y + \alpha^4 \equiv 1 \cdot S(y) \pmod{y^4}$

(3) $\alpha \equiv (\alpha^2 y + \alpha^4) \cdot S(y) \pmod{y^4}$

(3) は (1) − (2) × 多項式 で得られる。

$(\alpha^4)^{-1}$ を (3) の両辺にかけると

$\alpha^4 \equiv (\alpha^5 y + 1) S(y) \pmod{y^4}$

事実 1 より，誤り多項式は $E(y) = e_a y^a$ と書け，$a = 5$ である。

また，事実 1 より，$\alpha^4 = e_a \alpha^a$ なので，$e_a = \alpha^6$ である。したがって，もとの符号 f は

$f = (\alpha, \alpha^5, \alpha^6, \alpha, 0, 0, \alpha^5)$

と推測される。

再び Reed-Solomon 符号を受信したところ，

$f_1 = (\alpha, 1, \alpha^6, 0, 0, 0, \alpha^5)$

であった。シンドローム多項式の係数を計算すると

$f_1(\alpha) = \alpha$，$f_1(\alpha^2) = 0$，$f_1(\alpha^3) = \alpha^2$，$f_1(\alpha^4) = \alpha^4$ である。

ユークリッドの互除法により，鍵方程式の解を求める。

(1) $y^4 \equiv 0 \cdot S(y) \pmod{y^4}$

(2) $\alpha^4 y^3 + \alpha^2 y^2 + \alpha \equiv 1 \cdot S(y) \pmod{y^4}$

(3) $\alpha^3\, y^2 + \alpha^4\, y + \alpha^2 \equiv (\alpha^3 y + \alpha) \cdot S(y) \pmod{y^4}$

((3) は (1) − (2) × 多項式 による)

(4) $\alpha^6 y + \alpha^4 \equiv (\alpha^4 y^2 + \alpha^5 y + \alpha^3) \cdot S(y) \pmod{y^4}$

((4) は (2) − (3) × 多項式 による)

$\left(\alpha^3\right)^{-1}$ を (4) の両辺にかけると

$\alpha^3 y + \alpha \equiv (\alpha y^2 + \alpha^2 y + 1) S(y) \pmod{y^4}$

を得る。$y = \alpha^2$ とすると，$\alpha y^2 + \alpha^2 y + 1 = 0$ である。

よって，

$\alpha y^2 + \alpha^2 y + 1 = (\alpha^5 y + 1)(\alpha^3 y + 1)$

事実 2 より，$E(y) = e_a y^a + e_b y^b$，$a = 5$，$b = 3$，

($a = 3, b = 5$ でもよい)

$\alpha^3 y + \alpha = e_a \alpha^a (\alpha^b y + 1) + e_b \alpha^b (\alpha^a y + 1)$

と書ける。よって，

$E(y) = \alpha^4 y^5 + \alpha y^3$

であり，もとの符号は

$f = (\alpha, \alpha^5, \alpha^6, \alpha, 0, 0, \alpha^5)$

と推測される。

例 2. $\mathbb{F}_q = \mathbb{F}_7 = \mathbb{Z}/(7) = \{0, 1, 2, 3, 4, 5, 6\}$

で考える。3 が 1 つの原始元である。標数が 2 でないので，符号に注意が必要。

3	3^2	3^3	3^4	3^5	3^6
3	2	6	4	5	1

さて，$RS(7, 2)$ の Reed-Solomon 符号を受信したところ，

$f_1 = (2, 4, 3, 1, 6, 3)$

であったとする。シンドローム多項式の係数を計算 (mod 7 の計算) すると

$$f_1(3) = 2 \cdot 3^5 + 4 \cdot 3^4 + 3 \cdot 3^3 + 3^2 + 6 \cdot 3 + 3 = 4$$

$$f_1(3^2) = 3, \quad f_1(3^3) = 4, \ f_1(3^4) = 3.$$

ユークリッドの互除法により，鍵方程式の解を求める。

$$(1) \quad y^4 \equiv 0 \cdot S(y) \pmod{y^4}$$

$$(2) \quad 3y^3 + 4y^2 + 3y + 4 \equiv 1 \cdot S(y) \pmod{y^4}$$

$$(3) \quad 1 \equiv -(5y + 5) \cdot S(y) \pmod{y^4}$$

$$\equiv (2y + 2) \cdot S(y) \pmod{y^4}$$

(3) は (1) − (2) × 多項式 で得られる。

$2^{-1} = 4$ (in $\mathbb{F}_7$) を (3) の両辺にかけると

$$4 \equiv (y + 1)S(y) \pmod{y^4}$$

係数は $\mathbb{F}_7$ なので，$1 + y = 1 - 6y = 1 - 3^3 y$.

よって，誤り位置は，y^3(3 次) の係数。

$$4 = e_3 \cdot 3^3.$$

$3^3 = 6 = -1$ より，$e_3 = 4 \cdot (-1)^{-1} = -4 = 3$.

よって，元の符号は $f_1(y) - 3y^3$ で

$$(2, 4, 0, 1, 6, 3).$$

と推測される。

再び Reed-Solomon 符号を受信したところ，

$$f_1 = (2, 5, 0, 0, 6, 3)$$

であった。シンドローム多項式の係数を計算すると

$f_1(3) = 2$，$f_1(3^2) = 5$，$f_1(3^3) = 0$，$f_1(3^4) = 2$ である。

ユークリッドの互除法により，鍵方程式の解を求める。

(1) $y^4 \equiv 0 \cdot S(y) \pmod{y^4}$

(2) $2y^3 + 5y + 2 \equiv 1 \cdot S(y) \pmod{y^4}$

(3) $y^2 + 6y \equiv -4y \cdot S(y) \pmod{y^4}$

((3) は (1) − (2) × 多項式 による)

(4) $2 \equiv (y^2 + y + 1) \cdot S(y) \pmod{y^4}$

((4) は (2) − (3) × 多項式 による)

$y = 2$ とすると、mod 7 で、$2^2+2+1 = 0$. $2^{-1} = 4$ なので、$1-4y(= 1+3y)$ を因数にもつ。よって,

$$y^2 + y + 1 = (1 - 4y)(1 - 2y) = (1 - 3^4 y)(1 - 3^2 y)$$

事実 2 より，誤り多項式は $E(y) = e_a y^4 + e_b y^2$ で,

$2 = e_4 \cdot 3^4(1 - 3^2 y) + e_2 3^2(1 - 3^4 y)$

と書ける。よって，$y = 4, y = 2$ と代入してみることにより,

$$E(y) = y^4 + 6y^2 = y^4 - y^2$$

であり，もとの符号は $f_1(y) - E(y)$ で,

$(2, 4, 0, 1, 6, 3)$

と推測される。