数理解析研究所講究録 1420 巻 2005 年 142-149

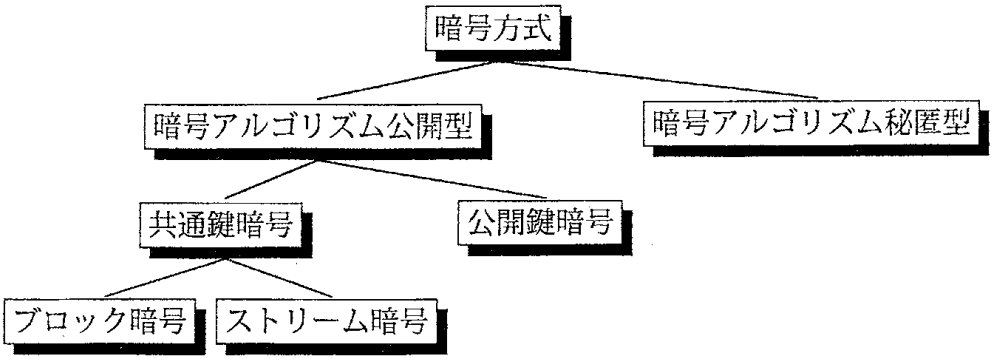


# 円分数, 暗号及び 2 次分割

松田 修三* 平松 豊一†
Shuzo Matsuda Toyokazu Hiramatsu

法政大学工学部
Department of Systems and Control Engineering
Faculty of Engineering, Hosei University

## 1 ストリーム暗号



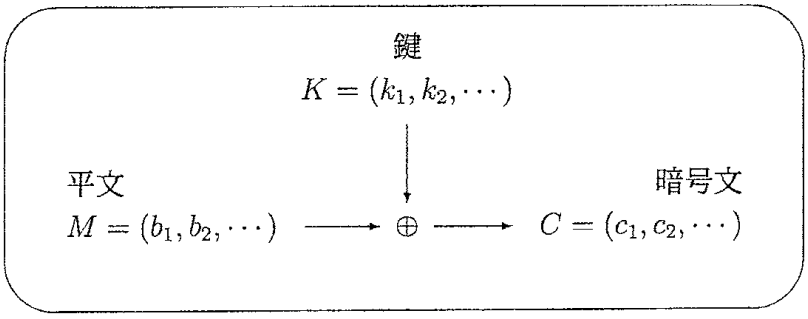

暗号方式の分類

送信者と受信者が同じ鍵 $K$ を秘密に共有する暗号系を共通鍵暗号系という. 共通鍵暗号系のうち, 平文のビット列 $M=(b_1,b_2,\cdots)$ を, 鍵のビット列 $K=(k_1,k_2,\cdots)$ ( 鍵系列 ) を用いて

$$c_1=b_1\oplus k_1,\ c_2=b_2\oplus k_2,\ \cdots$$

*E-mail : matsuda@k.hosei.ac.jp
†E-mail : hiramatu@k.hosei.ac.jp

と暗号化する暗号系をストリーム暗号という．ここで，演算 $\oplus$ は 2 を法とする加算を表す．$C = (c_1, c_2, \cdots)$ が暗号文となる．




ストリーム暗号

ストリーム暗号方式は，高速な暗号処理が実現可能であり，通信ネットワークにおける回線暗号装置等で用いられる．この方式では，鍵系列発生器すなわち擬似乱数発生器でいかに完全乱数に近い乱数を生成できるかが暗号の安全性に対する重要な要因の一つである．代表的な例としては，RC4 ( RSA Security 社 )，MULTI-S01 ( 日立，2000 年 ) 等がある．

ここで，ストリーム暗号方式をもう少し一般的に定義しておこう．

次の条件を満たす組 $\{P, C, K, L, F, E, D\}$ をストリーム暗号方式と呼ぶ．

1) $P$ は平文の有限集合；

2) $C$ は暗号文の有限集合；

3) $K$ は鍵の有限集合で，鍵空間という；

4) $L$ は鍵ストリームアルファベットと呼ばれる有限集合；

5) $F = (f_1, f_2, \cdots)$ は鍵ストリーム生成関数である：

$$f_i : K \times P^{i-1} \to L \quad (i \geq 1);$$

6) 各 $z \in L$ に対し，暗号化規則 $e_z \in E$ が一つ存在し，これに対応した復号化規則 $d_z \in D$ が一つ存在する．そして，$e_z : P \to C$ と $d_z : C \to P$ は任意の平文 $x \in P$ に対し，$d_z(e_z(x)) = x$ をみたす．

ブロック暗号はストリーム暗号の鍵ストリームで，すべての $i \geq 1$ に対して $z_i = K$ の場合と考えられる．また，ストリーム暗号は，すべての $i \geq 1$

で $z_{i+d}=z_i$ のとき, 周期 $d$ をもつという. 更に, $P=C=L=\mathbb{F}_2=\{1,0\}$ のとき,

$$\begin{aligned} e_z(x) &= x\oplus z, \\ d_z(y) &= y\oplus z \end{aligned}$$

となる.

## 2 円分数とその原点

### 2.1

$n\geq 2$ とし, $\mathbb{F}_n=\mathbb{Z}/n\mathbb{Z}$, $\mathbb{F}_n^\times=\mathbb{F}_n-\{0\}$ とする. $\{D_0,D_1,\ldots,D_{d-1}\}$ が

$$\begin{aligned} D_i\cap D_j &= \quad (i\neq j), \\ \mathbb{F}_n^\times &= \bigcup_{i=0}^{d-1} D_i \end{aligned}$$

をみたすとき, これを $\mathbb{F}_n^\times$ の分割という. 特に, $D_0$ が $\mathbb{F}_n^\times$ の部分群で, 残りの $D_i=g_iD_0$ $(g_i\in\mathbb{F}_n^\times)$ のとき $D_i$ 達を位数 $d$ の円分類という. また,

$$(i,j)_d=|(D_i+1)\cap D_j| \qquad (i,j=0,1,\ldots,d-1)$$

なる高々 $d^2$ 個の数を位数 $d$ の円分数という. ただし, $\mathbb{F}_n^\times$ の指数 $d$ の部分群 $D_0$ はいくつもありうる. その選び方によって, 異なる円分数が与えられる.

ここで特に, $n=p=df+1$ を奇素数とし, $\theta$ を $\mathbb{F}_p^\times$ の原始元, $D_0$ を $\theta^d$ で生成された部分群とする. このとき, $(i,j)_d$ は次の性質をもつ.

1°. $i\equiv i'$, $j\equiv j'$ $(\mathrm{mod}\ d)$ のとき

$$(i,j)_d=(i',j')_d.$$

2°. $$(i,j)_d=(d-i,j-i)_d=\begin{cases}(j,i)_d, & f:\text{even},\\ (j+\frac{d}{2},i+\frac{d}{2})_d, & f:\text{odd}.\end{cases}$$

3°. $\sum_{j=0}^{d-1}(i,j)_d = f - n_i$, ここで,

$$n_i = \begin{cases} 1, & i \equiv 0 \pmod{d}, \quad f : \text{even}, \\ 1, & i \equiv \frac{d}{2} \pmod{d}, \quad f : \text{odd}, \\ 0, & \text{他}. \end{cases}$$

4°. $\sum_{i=0}^{d-1}(i,j)_d = f - k_j$, ここで,

$$k_j = \begin{cases} 1, & j \equiv 0 \pmod{d}, \\ 0, & \text{他}. \end{cases}$$

5°. $$\sum_{i=0}^{d-1}(i,i+j)_d = \begin{cases} f-1, & j = 0, \\ f, & j \neq 0. \end{cases}$$

6°. $$\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}(i,j)_d = df - 1 = n - 2.$$

7°. $(i,j)_{d'} = (i,j)_d$.
$(i,j)_{d'}$ は, $\theta' \equiv \theta^s \pmod{n}$ なる原始元を base にしたもの. ( 必要なら, $(s, n-1) = 1$ ).

## 2.2

円分数の原点は Gauss にある ( : Disquisitiones Arithmeticae, 1801). $p = df + 1$ を素数とし, $\theta = e^{\frac{2\pi i}{p}}$, $g$ を $\mathbb{F}_p^\times$ の原始元, $\lambda$ を整数とする. このとき,

$$(f;\lambda) = \sum_{j=0}^{f-1} \theta^{\lambda g^{dj}}$$

を Gauss は周期と呼んだ. そして, $D_0$ を $g^d$ で生成された $\mathbb{F}_p^\times$ の部分群, $D_i = g^i D_0$ ( $0 \leq i \leq d-1$ ) とする.

$$(f;g^i) = \sum_{r \in D_i} \theta^r$$

が成立する. この等式の右辺は, 円分方程式 $x^p-1=0$ の根の和を表すから, 周期 $(f;\lambda)$ は $g$ の選び方によらない. また, $\{D_0, D_1, \ldots, D_{d-1}\}$ は $\mathbb{F}_p^\times$ の分割を与える故,

$$\sum_{i=0}^{d-1}(f;g^i)=-1$$

となる. この周期を使って, .

**Theorem 2.1 (Gauss)** $4p=a^2+27b^2$, $a\equiv 1 \pmod 3$ とする. このとき,

$$x^3-y^3\equiv 1 \pmod p$$

の解 $(x,y)$ の個数 $N$ は, $N=p+a-2$ で与えられる.

**Proof** $p=3f+1$ とし, 2つの周期 $(f;\lambda)$, $(f;\mu)$ を考え,

$$(f;\mu)=\theta^{\mu_1}+\cdots+\theta^{\mu_f}$$

とおく. このとき,

$$(f;\lambda)(f;\mu)=\sum_{j=1}^{f}(f;\lambda+\mu_j) \qquad (*)$$

が成立する. そこで, Gauss は, $i,j\in\{0,1,2\}$ に対し, 円分数 $(i,j)$ を $0\le m,n\le f-1$ で

$$1+g^{3m+i}\equiv g^{3n+j} \pmod p$$

をみたす組 $(m,n)$ の個数として定義する. $(i,j)=(j,i)_3$ である. このとき, $(*)$ 等により

$$\begin{aligned} N&=9\cdot(0,0)+6,\\ \alpha&=(1,2)=(2,1)=(0,0)+1,\\ a&=9\alpha-p-1 \end{aligned}$$

と計算でき, $a=N-p+2$ を得る. ■

## 3 円分数と暗号化生成関数

$\{G,+\}$ をアーベル群とし, $|G|=d$ とおく. 暗号化生成関数を $f(x)$ とし, $g_i \in G$ に対し,

$$C_i = \{x \in \mathbb{F}_n : f(x) = g_i\}$$

とおくとき, $\{C_0, C_1, \ldots, C_{d-1}\}$ を特性類という. $\mathbb{F}_n^{\times}$ の任意の分割 $\{D_0, D_1, \ldots, D_{d-1}\}$ に対し, これを特性類とする暗号化生成関数 $f(x)$ がある. この $f(x)$ を構成する. $n=p=df+1$ を奇素数とし,

$$G = \{g_0, g_1, \ldots, g_{d-1}\}$$

とする. このとき,

$$f(x) : \mathbb{F}_p \to G$$

なる関数 $f(x)$ の構成は次のようである. $\{D_0, D_1, \ldots, D_{d-1}\}$ を円分類とし,

$$C_0 = D_0 \cup \{0\}, \quad C_i = D_i \quad (i = 1, 2, \ldots, d-1)$$

とおく. このとき, $x \in C_i$ に対し

$$f(x) = g_i$$

とする. 暗号の安全性のために大切な $f(x)$ の非線形性が円分数によって決定されることが知られている.

## 4 2 次分割の整数論

円分数は暗号の鍵系列生成をデザインするのに有用であった. その円分数と 2 次分割の関係は Gauss に始まる. 位数 3 の円分数は, $4p = x^2 + 27y^2$, $x \equiv 1 \pmod 3$ の解 $(x,y)$ によって決まり, 位数 9 の円分数は, $4p = x^2 + 27y^2$, $x \equiv 7 \pmod 9$ の解 $(x,y)$ によって決まる. 実は殆どの円分数は, 素数 $p$ の表現 $p = x^2 + ny^2$ によって決まることが知られている. その 2 次分割について, 整数 $n$ $(\neq 0)$, 奇素数 $p$ $(p \nmid n)$ に対し

$$p \mid (x^2 + ny^2),\ (x,y) = 1 \Longleftrightarrow \left(\frac{-n}{p}\right) = 1$$

が成立する. ここで, $\left(\frac{*}{p}\right)$ は $p$ を法とする Legendre 記号を表す. そこで, 次の 2 つのアプローチが考えられる :

アプローチ 1 $p = x^2 + ny^2$ と表される大きな素数 $p$ をみつけよ. ここで, $n$ は暗号のためにデザインされたパラメータを表す. そして必要ならばこの 2 次分割を得るためのアルゴリズムをみつけよ.

アプローチ 2 与えられた暗号化パラメータ $n$ に対し, 集合 $B(n) = \{x^2 + ny^2 : x, y \in \mathbb{Z}\}$ から大きな素数をさがせ.

更に, これらのアプローチを分けて考える. アプローチ 1 については,

問 **1.A** 与えられた $n$ に対し, どの素数 $p$ が $p = x^2 + ny^2$ と表されるか?

これについては次の結果がある :

**Theorem 4.1** $n$ を $n \not\equiv 3 \pmod 4$ で squarefree な正整数とする. そのとき, monic で次数 $h(-4n)$ の整係数既約多項式 $f_n(x)$ があって, 奇素数 $p$ で $p \nmid n$, $p \nmid D_{f_n}$ ( $D_{f_n}$ は $f_n$ の判別式 ) に対し

$$p = x^2 + ny^2 \Longleftrightarrow \left(\frac{-n}{p}\right) = 1 \text{ で } f_n(x) \equiv 0 \pmod p \text{ が整数解をもつ}$$

が成立する. ここで, $h(-4n)$ は判別式 $-4n$ の正定値原始 2 次形式の類数を表す. 更に, $K(\alpha)$ ( $\alpha$ は実代数的整数 ) が虚 2 次体 $K = \mathbb{Q}(\sqrt{-n})$ 上のヒルベルト類体のとき, $f_n(x)$ は $\alpha$ の最小多項式である.

問 **1.B** もしそうなら, $p = x^2 + ny^2$ となる解 $(x, y)$ は何個あるか ? また, 解 $(x, y)$ をみつけるアルゴリズムはあるか ?

この問 1.B の後半については, Cornacchia のアルゴリズムがある. 前半は open problem である.

アプローチ 2 については,

問 **2.A** どんな $n$ に対し, $B(n)$ は無限個の素数を含むか ?

これについては,

**Theorem 4.2** $ax^2 + bxy + cy^2$ を判別式 $D$ $(< 0)$ の正定値原始 2 次形式とし, これが表す素数の集合を $PB(a, b, c)$ とするとき, Dirichlet 密度は

$$\delta(PB(a, b, c)) = \frac{1}{h(D)} \text{ または } \frac{1}{2h(D)}$$

で与えられる. 特に, $ax^2 + bxy + cy^2$ は無限個の素数を表現する.

問 **2.B** そのような $n$ に対し, $B(n)$ から大きな素数をいかにみつけるか?

この問 2.B は open problem である.

## 参考文献

[1] D. A. Cox ; Primes of the Form $x^2 + ny^2$, John Wiley and Sons, Inc., 1989.

[2] T. W. Cusick, C. Ding and A. Renvall ; Stream Ciphers and Number Theory (Revised Edition), North-Holland, 2004.

[3] C. Ding and T. Helleseth ; New generalized cyclotomy and its applications, Finite Fields and their Applications, **4** (1998), 140-166.