チェビシェフ多項式の 2 変数への拡張と公開鍵暗号（ElGamal 暗号）への応用

Ⅰ.チェビシェフ(Chebyshev)の多項式

$$\cos\theta = \frac{1}{2}(e^{i\theta} + e^{-i\theta})$$

より

$$\cos n\theta = \frac{1}{2}(e^{in\theta} + e^{-in\theta})$$

であるから

$$\cos\theta\cos n\theta = \frac{1}{4}(e^{i\theta} + e^{-i\theta})(e^{in\theta} + e^{-in\theta})$$

$$= \frac{1}{4}(e^{i(n+1)\theta} + e^{-i(n+1)\theta} + e^{i(n-1)\theta} + e^{-i(n-1)\theta})$$

$$= \frac{1}{2}\{\cos(n+1)\theta + \cos(n-1)\theta\}$$

よって

$$\cos(n+1)\theta - 2\cos\theta\cos n\theta + \cos(n-1)\theta = 0$$

ここで

$$a_n = \cos n\theta\,,\quad x = \cos\theta$$

とおくと

$$a_{n+1} - 2x\cdot a_n + a_{n-1} = 0$$

したがって

$$a_{n+2} = 2x\cdot a_{n+1} - a_n$$

が成り立つ。

この漸化式と $a_0 = 1, a_1 = x$ であることより， a_n は x の多項式となることがわかる。

$a_n = T_n(x)$ とおく。これをチェビシェフの多項式という。

ここで

$$\cos(mn\theta) = \cos(m(n\theta))$$

であるから,

$$\cos n\theta = y$$

とおくと,

$$T_{mn}(x) = T_m(y)$$

$$y = T_n(x)$$

であるから

$$T_{mn}(x) = T_m(T_n(x))$$

したがって

$$T_{mn}(x) = T_m(T_n(x)) = T_n(T_m(x))$$

が成り立つ。

上記の議論は， $\cosh\theta = \frac{1}{2}(e^{\theta} + e^{-\theta})$ についても成り立ち,

$-1 \leqq x \leqq 1$ のとき　$T_n(x) = \cos(n\arccos(x))$

$x \geqq 1$ のとき　$T_n(x) = \cosh(n\arccos h(x))$

x≦－1 のとき　　$T_n(x) = (-1)^n \cosh(n \arccos h(-x))$

である。

上記の事柄は，t の 2 次方程式

$$t^2 - 2xt + 1 = 0$$

の 2 解をα, βとすると

$$x = \frac{1}{2}(\alpha + \beta),\quad \alpha\beta = 1$$

となるから

$$a_n = \frac{1}{2}(\alpha^n + \beta^n)$$

とおいても得られる。

Ⅱ.チェビシェフの多項式の任意の体への拡張

次に，任意の体 K で考える。GF(2)では 2＝0 であるので，2 次方程式

$$t^2 - 2xt + 1 = 0$$

では GF(2)の拡大体上で不都合が生じる。2 次方程式を次のように変えて考える。

t の 2 次方程式

$$t^2 - xt + 1 = 0$$

の 2 解をα，βとすると，解と係数の関係により

$\alpha + \beta$ ＝x，α β＝1

ただし，この方程式が K 上に解を持たない場合は，この 2 次方程式による K の拡大体を考える。

$$a_n = \alpha^n + \beta^n$$

とおく。

a_nは，漸化式

$$a_{n+2} - x \cdot a_{n+1} + a_n = 0$$

を満たす。このとき

$$a_0 = \alpha^0 + \beta^0 = 2,\quad a_1 = \alpha + \beta = x$$

逆に

$$a_0 = 2\,,\, a_1 = x$$

$$a_{n+2} = x \cdot a_{n+1} - a_n$$　（n は負でない整数）

でa_nを定めると，特性方程式方程式$t^2 - xt + 1 = 0$の 2 解をα，βとするとき

$$a_n = \alpha^n + \beta^n$$

となる。

ちなみに，$x = 2\cos\theta$とすると，$a_n = 2\cos n\theta$となる。

a_nは次の性質を満たす。

命題　1

$$b_0 = 2$$

$$b_1 = \alpha^n + \beta^n = a_n = y$$

とし，漸化式　$b_{n+2} - y \cdot b_{n+1} + b_n = 0$（n は負でない整数）で$b_n$を定めるとき，

$$b_m = a_{mn}$$

証明

漸化式の特性方程式

$$t^2 - yt + 1 = 0$$

の 2 解をγ，δとするとb_0, b_1の定め方により

$$b_m = \gamma^m + \delta^m$$

また，$\alpha^n + \beta^n = y$，$\alpha^n \beta^n = (\alpha\beta)^n = 1$より$\alpha^n$, β^nはこの特性方程式の解であるから

$$b_m = \gamma^m + \delta^m = (\alpha^n)^m + (\beta^n)^m = \alpha^{mn} + \beta^{mn} = a_{mn}$$

証明終わり

$\{a_n\}$の漸化式とa_0, a_1が x の多項式であることより，a_nは x の多項式となることがわかる。
よって，$a_n = f_n(x)$とおくと，上記の証明から

$$b_m = f_m(y) = f_m(f_n(x))$$

$$b_m = a_{mn} = f_{mn}(x)$$

であるから

$$f_{mn}(x) = f_m(f_n(x)) = f_n(f_m(x))$$

が成り立つことがわかる。

第 n 項の高速計算法

n を任意の自然数とするとき，n を 2 進法で表す。

$$n = (\cdots(((s_0 \cdot 2 + s_1) \cdot 2 + s_2) \cdot 2 + s_3) \cdot 2 + \cdots) + s_p$$

ただし，s_iは 0 か 1 の値をとり，$s_0 \neq 0$である。(バイナリー法)

$$a_0 = 2,\ a_1 = x$$

$$a_{n+2} = x \cdot a_{n+1} - a_n$$　（n は負でない整数）

とする。
a_n, a_{n+1}の組が与えられたとき，a_{2n}, a_{2n+1}の組は次のように求められる。

$$a_{2n} = \alpha^{2n} + \beta^{2n} = (\alpha^n + \beta^n)^2 - 2(\alpha\beta)^n = {a_n}^2 - 2$$

また，

$$a_n a_{n+1} = (\alpha^n + \beta^n)(\alpha^{n+1} + \beta^{n+1})$$

$$= (\alpha^{2n+1} + \beta^{2n+1}) + (\alpha\beta)^n(\alpha + \beta)$$

$$= a_{2n+1} + x$$

よって

$$a_{2n+1} = a_n a_{n+1} - x$$

これより，(a_n, a_{n+1}) の組から

$$(a_{2n}, a_{2n+1}) = (a_n{}^2 - 2, a_n a_{n+1} - x)$$

$$(a_{2n+1}, a_{2n+2}) = (a_n a_{n+1} - x, a_{n+1}{}^2 - 2)$$

が求まる。この 2 つを繰り返し用いると，a_n を高速に求めることができる。

Ⅲ.3 次方程式の解への拡張

体 K での t の 3 次方程式

$$t^3 - xt^2 + yt - 1 = 0 \cdots ①\quad \text{ただし} x \neq y$$

の 3 解を α，β，γ とする。

ただし，この方程式が K 上に解を持たない場合は，この 3 次方程式による K の拡大体を考える。

解と係数の関係により

$$\alpha + \beta + \gamma = x\ ,\ \alpha\beta + \beta\gamma + \gamma\alpha = y\ ,\ \alpha\beta\gamma = 1$$

このとき，$y = \dfrac{1}{\alpha} + \dfrac{1}{\beta} + \dfrac{1}{\gamma}$

が成り立つから，①は

$$t^3 - (\alpha + \beta + \gamma)t^2 + \left(\frac{1}{\alpha} + \frac{1}{\beta} + \frac{1}{\gamma}\right)t - 1 = 0$$

となる。

$$a_n = \alpha^n + \beta^n + \gamma^n \quad \text{ただし，n は整数}$$

とおく。n が自然数でなく整数とすることが，ポイントである。

$$a_0 = 3$$

$$a_1 = \alpha + \beta + \gamma = x$$

$$a_2 = \alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = x^2 - 2y$$

a_n は漸化式

$$a_{n+3} - x \cdot a_{n+2} + y \cdot a_{n+1} - a_n = 0 \quad \text{（n は整数）}$$

を満たす。

逆に

$$a_0 = 3\ ,\ a_1 = x\ ,\ a_3 = x^2 - 2y$$

$$a_{n+3} - x \cdot a_{n+2} + y \cdot a_{n+1} - a_n = 0 \quad \text{（n は整数）}$$

で a_n を定めると，特性方程式 $t^3 - xt^2 + yt - 1 = 0$ の 3 解を α，β，γ とするとき

$$a_n = \alpha^n + \beta^n + \gamma^n$$

となる。

a_n は次の性質を満たす。

命題　2

$$z=\alpha^n+\beta^n+\gamma^n=a_n$$

$$w=(\alpha\beta)^n+(\beta\gamma)^n+(\gamma\alpha)^n=\frac{1}{\alpha^n}+\frac{1}{\beta^n}+\frac{1}{\gamma^n}=a_{-n}$$

とする。

$$b_0=3$$

$$b_1=\alpha^n+\beta^n+\gamma^n=a_n=z$$

$$b_2=\alpha^{2n}+\beta^{2n}+\gamma^{2n}=(\alpha^n+\beta^n+\gamma^n)^2-2\{(\alpha\beta)^n+(\beta\gamma)^n+(\gamma\alpha)^n\}=z^2-2w$$

とし，漸化式

$$b_{n+3}-z\cdot b_{n+2}+w\cdot b_{n+1}-b_n=0$$　（n は整数）

でb_nを定めるとき，

$$b_m=a_{mn}$$

証明

漸化式の特性方程式

$$t^3-zt^2+wt-1=0$$

の 3 解をλ,μ,νとすると，b_0,b_1,b_2の定め方により

$$b_m=\lambda^m+\mu^m+\nu^m$$

である。

また，$\alpha^n+\beta^n+\gamma^n=z$，$\alpha^n\beta^n+\beta^n\gamma^n+\gamma^n\alpha^n=\frac{1}{\alpha^n}+\frac{1}{\beta^n}+\frac{1}{\gamma^n}=w$，$\alpha^n\beta^n\gamma^n=(\alpha\beta\gamma)^n=1$ より

$\alpha^n,\beta^n,\gamma^n$はこの方程式の解であるから

$$b_m=\lambda^m+\mu^m+\nu^m=(\alpha^n)^m+(\beta^n)^m+(\gamma^n)^m=\alpha^{mn}+\beta^{mn}+\gamma^{mn}=a_{mn}$$

証明終わり

$\{a_n\}$の漸化式とa_0,a_1,a_2が x,y の多項式であることより，a_nは x,y の多項式となることがわかる。

よって，$a_n=F_n(x,y)$とおくと，上記の証明から

$$b_m=F_m(z,w)=F_m(F_n(x,y),F_{-n}(x,y))$$

$$b_m=a_{mn}=F_{mn}(x,y)$$

であるから

$$F_{mn}(x,y)=F_m(F_n(x,y),F_{-n}(x,y))=F_n(F_m(x,y),F_{-m}(x,y))$$

が成り立つことがわかる。

また，①の両辺をt^3で割ると

$$\left(\frac{1}{t}\right)^3-y\left(\frac{1}{t}\right)^2+x\frac{1}{t}-1=0$$

となり，これを$\frac{1}{t}$の方程式と考えたとき，①と x,y が入れ替わっている。

このことにより，

$$F_{-n}(x,y)=F_n(y,x)$$

が成り立つことがわかる。したがって,

$$F_{mn}(x,y)=F_m(F_n(x,y),F_n(y,x))=F_n(F_m(x,y),F_m(y,x))$$

が成り立つ。具体的に$F_n(x,y)$を求めてみると，次のようになる。

$$F_0(x,y)=3$$

$$F_1(x,y)=x$$

$$F_2(x,y)=x^2-2y$$

$$F_3(x,y)=x^3-3xy+3$$

$$F_4(x,y)=x^4-4x^2y+2y^2+4x$$

$$F_5(x,y)=x^5-5x^3y+5xy^2+5x^2-5y$$

$$F_6(x,y)=x^6-6x^4y+9x^2y^2+6x^3-2y^3-12xy+3$$

第 n 項の高速計算法

高速に

$$a_n=\alpha^n+\beta^n+\gamma^n \quad と \quad a_{-n}=\frac{1}{\alpha^n}+\frac{1}{\beta^n}+\frac{1}{\gamma^n}$$

が求められることを示す。

$$a_n{}^2=(\alpha^n+\beta^n+\gamma^n)^2=\alpha^{2n}+\beta^{2n}+\gamma^{2n}+2\{(\alpha\beta)^n+(\beta\gamma)^n+(\gamma\alpha)^n\}$$

$$=\alpha^{2n}+\beta^{2n}+\gamma^{2n}+2(\frac{1}{\gamma^n}+\frac{1}{\alpha^n}+\frac{1}{\beta^n})$$

$$=a_{2n}+2a_{-n}$$

よって

$$a_{2n}=a_n{}^2-2a_{-n}\cdots②$$

また

$$a_na_{n+1}=(\alpha^n+\beta^n+\gamma^n)(\alpha^{n+1}+\beta^{n+1}+\gamma^{n+1})$$

$$=\alpha^{2n+1}+\beta^{2n+1}+\gamma^{2n+1}+(\alpha+\beta)(\alpha\beta)^n+(\beta+\gamma)(\beta\gamma)^n+(\gamma+\alpha)(\gamma\alpha)^n$$

$$=\alpha^{2n+1}+\beta^{2n+1}+\gamma^{2n+1}+(x-\gamma)\left(\frac{1}{\gamma}\right)^n+(x-\alpha)\left(\frac{1}{\alpha}\right)^n+(x-\beta)\left(\frac{1}{\beta}\right)^n$$

$$=\alpha^{2n+1}+\beta^{2n+1}+\gamma^{2n+1}+\left\{x\left(\frac{1}{\alpha^n}+\frac{1}{\beta^n}+\frac{1}{\gamma^n}\right)-\left(\frac{1}{\alpha^{n-1}}+\frac{1}{\beta^{n-1}}+\frac{1}{\gamma^{n-1}}\right)\right\}$$

$$=a_{2n+1}+(x\cdot a_{-n}-a_{-n+1})$$

より

$$a_{2n+1}=a_na_{n+1}-(x\cdot a_{-n}-a_{-n+1})\cdots③$$

ここで,

$$a_{n+3}-x\cdot a_{n+2}+y\cdot a_{n+1}-a_n=0$$

であるから

$$a_{-n+1}-x\cdot a_{-n}+y\cdot a_{-n-1}-a_{-n-2}=0$$
$$xa_{-n}-a_{-n+1}=y\cdot a_{-n-1}-a_{-n-2}$$

よって

$$a_{2n+1}=a_n a_{n+1}-(y\cdot a_{-n-1}-a_{-n-2})\cdots④$$

②，③，④より次の漸化式が成り立つ。

$$a_{2n}=a_n{}^2-2a_{-n}$$

$$a_{2n+1}=a_n a_{n+1}-y\cdot a_{-n-1}+a_{-n-2}$$

$$a_{2n+2}=a_{n+1}{}^2-2a_{-n-1}$$

$$a_{2n+3}=a_{n+1}a_{n+2}-x\cdot a_{-n-1}+a_{-n}$$

$$a_{-2n}=a_{-n}{}^2-2a_n$$

$$a_{-2n-1}=a_{-n}a_{-n-1}-x\cdot a_{n+1}+a_{n+2}$$

$$a_{-2n-2}=a_{-n-1}{}^2-2a_{n+1}$$

$$a_{-2n-3}=a_{-n-1}a_{-n-2}-y\cdot a_{n+1}+a_n$$

これらを用いると

$a_n,a_{n+1},a_{n+2},a_{-n},a_{-n-1},a_{-n-2}$ の組から

$a_{2n},a_{2n+1},a_{2n+2},a_{-2n},a_{-2n-1},a_{-2n-2}$　または　$a_{2n+1},a_{2n+2},a_{2n+3},a_{-2n-1},a_{-2n-2},a_{-2n-3}$

の組を求めることができ，したがって，a_n を高速に求めることができる。

周期に関する考察

命題　3

α，β，γ は相異なるとき，

異なる (a_n,a_{n+1},a_{n+2}) の個数と，異なる $(\alpha^n,\beta^n,\gamma^n)$ は個数と等しい。

証明

$(a_n,a_{n+1},a_{n+2})=(a_m,a_{m+1},a_{m+2})$ と仮定すると

$$(\alpha^n+\beta^n+\gamma^n,\alpha^{n+1}+\beta^{n+1}+\gamma^{n+1},\alpha^{n+2}+\beta^{n+2}+\gamma^{n+2})$$
$$=(\alpha^m+\beta^m+\gamma^m,\alpha^{m+1}+\beta^{m+1}+\gamma^{m+1},\alpha^{m+2}+\beta^{m+2}+\gamma^{m+2})$$

よって

$$\alpha^n+\beta^n+\gamma^n=\alpha^m+\beta^m+\gamma^m$$
$$\alpha^{n+1}+\beta^{n+1}+\gamma^{n+1}=\alpha^{m+1}+\beta^{m+1}+\gamma^{m+1}$$
$$\alpha^{n+2}+\beta^{n+2}+\gamma^{n+2}=\alpha^{m+2}+\beta^{m+2}+\gamma^{m+2}$$

したがって

$$\begin{pmatrix}1&1&1\\ \alpha&\beta&\gamma\\ \alpha^2&\beta^2&\gamma^2\end{pmatrix}\begin{pmatrix}\alpha^n\\ \beta^n\\ \gamma^n\end{pmatrix}=\begin{pmatrix}1&1&1\\ \alpha&\beta&\gamma\\ \alpha^2&\beta^2&\gamma^2\end{pmatrix}\begin{pmatrix}\alpha^m\\ \beta^m\\ \gamma^m\end{pmatrix}$$

ここで，α，β，γ は相異なるから

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{vmatrix} = (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha) \neq 0$$

したがって,

$$(\alpha^n, \beta^n, \gamma^n) = (\alpha^m, \beta^m, \gamma^m)$$

逆も成り立つ。

ゆえに,

$$(a_n, a_{n+1}, a_{n+2}) = (a_m, a_{m+1}, a_{m+2}) \Leftrightarrow (\alpha^n, \beta^n, \gamma^n) = (\alpha^m, \beta^m, \gamma^m)$$

したがって，この 1 対 1 対応により,

異なる (a_n, a_{n+1}, a_{n+2}) の個数と，異なる $(\alpha^n, \beta^n, \gamma^n)$ の個数は等しい。

証明終わり。

補題

$$\alpha+\beta+\gamma = \delta+\mu+\nu \text{ , } \alpha\beta+\beta\gamma+\gamma\alpha = \delta\mu+\mu\nu+\nu\delta \text{ , } \alpha\beta\gamma = \delta\mu\nu$$

$\Leftrightarrow$集合として，$\{\alpha, \beta, \gamma\} = \{\delta, \mu, \nu\}$

証明

$$\alpha+\beta+\gamma = \delta+\mu+\nu, \alpha\beta+\beta\gamma+\gamma\alpha = \delta\mu+\mu\nu+\nu\delta, \alpha\beta\gamma = \delta\mu\nu$$

とすると

$$\begin{aligned}(x-\alpha)(x-\beta)(x-\gamma) &= x^3-(\alpha+\beta+\gamma)x^2+(\alpha\beta+\beta\gamma+\gamma\alpha)x-\alpha\beta\gamma \\ &= x^3-(\delta+\mu+\nu)x^2+(\delta\mu+\mu\nu+\nu\alpha)x-\delta\mu\nu \\ &= (x-\delta)(x-\mu)(x-\nu)\end{aligned}$$

よって，3 次方程式 $(x-\alpha)(x-\beta)(x-\gamma)=0$ の解と，3 次方程式 $(x-\delta)(x-\mu)(x-\nu)=0$ 解は一致する。

したがって,

$$\{\alpha, \beta, \gamma\} = \{\delta, \mu, \nu\}$$

逆は明らか。

証明終わり

命題　4

異なる (a_n, a_{-n}) の個数と，異なる集合 $\{\alpha^n, \beta^n, \gamma^n\}$ の個数は等しい。

証明

$(a_m, a_{-m}) = (a_n, a_{-n})$ とする。

$a_m = a_n$　より

$$\alpha^m+\beta^m+\gamma^m = \alpha^n+\beta^n+\gamma^n \cdots ①$$

$a_{-m} = a_{-n}$　より

$$\frac{1}{\alpha^m}+\frac{1}{\beta^m}+\frac{1}{\gamma^m} = \frac{1}{\alpha^n}+\frac{1}{\beta^n}+\frac{1}{\gamma^n}$$

ここで，$\alpha\beta\gamma = 1$ を用いると

$$\alpha^m\beta^m+\beta^m\gamma^m+\gamma^m\delta^m = \alpha^n\beta^n+\beta^n\gamma^n+\gamma^n\alpha^n \cdots ②$$

また，$\alpha\beta\gamma = 1$より

$$\alpha^m\beta^m\gamma^m = \alpha^n\beta^n\gamma^n \cdots ③$$

よって，①，②，③と補題により

$$\{\alpha^m, \beta^m, \gamma^m\} = \{\alpha^n, \beta^n, \gamma^n\}$$

逆は明らか。よって，

$$(a_m, a_{-m}) = (a_n, a_{-n}) \quad \Leftrightarrow \quad \{\alpha^m, \beta^m, \gamma^m\} = \{\alpha^n, \beta^n, \gamma^n\}$$

したがって，この 1 対 1 対応により，

異なる(a_n, a_{-n})の個数と，異なる$\{\alpha^n, \beta^n, \gamma^n\}$の個数は等しい。

証明終わり

ここで，

異なる$\{\alpha^n, \beta^n, \gamma^n\}$の個数×3!≧異なる$(\alpha^n, \beta^n, \gamma^n)$の個数

であるから，α，β，γが相異なるとき

異なる(a_n, a_{-n})の個数×6≧異なる$(\alpha^n, \beta^n, \gamma^n)$の個数=異なる$(a_n, a_{n+1}, a_{n+2})$の個数

さらに，

異なる$(\alpha^n, \beta^n, \gamma^n)$の個数＝$\alpha^n, \beta^n, \gamma^n$それぞれの異なる個数の最小公倍数

異なる(a_n, a_{-n})の個数≦(体 K の位数)^2

であるから，α, β, γを体 K とその拡大体にうまく配置できれば，異なる(a_n, a_{n+1}, a_{n+2})の個数を，(体 K の位数)^2 程度まで延長できる可能性がある。

$p \neq 0$として，任意の整数 n について$a_{n+p} = a_n$を満たすとき，p を周期という。

ここでは，正の周期だけを考える。

周期のうち最小なものを，基本周期という。このとき，次の定理が成り立つ。

定理

すべての周期は基本周期の倍数である。

証明

基本周期を T とし，T でないある周期を p とすると，p>T より，整数 m を用いて

$$p = Tm + r \quad (0 \leqq r < T)$$

と表されるから

$$r = p - Tm$$

となる。T,p は共に周期であるから

$$a_{n+r} = a_{n+p-Tm} = a_{n+p} = a_n$$

よって，r>0 とすると r は周期となり，0≦r<T より T が最小の周期であることに反する。

したがって，r=0 となるから，

$$p = Tm$$

ゆえに，p は T の倍数である。

証明終わり

これより，基本周期は任意の周期の約数であるといえる。したがって，1 つの周期が求められれば，その周期を素因数分解することにより，基本周期の候補が見つかる。
異なる (a_n, a_{n+1}, a_{n+2}) の個数は，基本周期である。
体から零元 0 を除けば群をなすから，異なる $(\alpha^n, \beta^n, \gamma^n)$ の個数は（拡大体の位数－1）の約数である。

さらに，異なる (a_n, a_{n+1}, a_{n+2}) の個数は，異なる $(\alpha^n, \beta^n, \gamma^n)$ の個数と等しいから，

基本周期は（拡大体の位数－1）の約数

である。

実装例　$GF(2)$ の既約多項式 $x^{127}+x^{63}+1$ を用いて体を構成する。$2^{127}-1$ はメルセンヌ素数である。この体上で公開鍵暗号を作成するとき，この体の位数は 2^{127} であるから，

（ｉ）体が拡大されず，位数が 2^{127} のとき

（体の位数－1）＝ $2^{127}-1$

（ii）拡大体の位数が $(2^{127})^2$ のとき

（拡大体の位数－1）＝ $(2^{127})^2-1=(2^{127}-1)(2^{127}+1)$

$2^{127}+1$=3×5671372782015641057722910123862803524 3

（iii）拡大体の位数が $(2^{127})^3$ のとき

（拡大体の位数－1）＝ $(2^{127})^3-1=(2^{127}-1)\{(2^{127})^2+2^{127}+1\}$

$(2^{127})^2+2^{127}+1$ ＝7×2287×15241×349759
×339212878596211796110770323541353281494127285320354524672773903

t の 3 次方程式 $t^3-xt^2+yt-1=0$ で，100000 個の x,y の乱数の組で実験したところ，

周期が $(2^{127})^2-1$ の約数であるものは　66647 個　あり，その内

周期が $2^{127}-1$ であるものは　16765 個

周期が $2^{127}+1$ の約数であるものは　0 個

周期が $(2^{127})^2+2^{127}+1$ の約数であるものは　33353 個　あり，その内

周期が $(2^{127})^2+2^{127}+1$ であるものは　28486 個

あった。

周期が $(2^{127})^2+2^{127}+1$ である x，y を用いるのが良いと思われる。

チェビシェフ多項式との関係

t の 3 次方程式

$$t^3-xt^2+yt-1=0$$

において，y=x とおくと

$$t^3-xt^2+xt-1=0$$

この方程式は $t=1$ を解に持ち，因数分解すると

$$(t-1)\{t^2-(x-1)t+1\}=0$$

となるから，

2 次方程式 $t^2-xt+1=0$ から作られる多項式を $f_n(x)$ とし，この 3 次方程式から作られる多項式を $g_n(x)$ とすると

$$g_n(x)=f_n(x-1)+1$$

となる。この式と

$$f_{mn}(x) = f_m(f_n(x))$$

より

$$g_{mn}(x) = f_{mn}(x-1)+1 = f_m(f_n(x-1))+1 = f_m(g_n(x)-1)+1 = g_m(g_n(x))$$

と示されるので，新たな多項式が求まった訳ではない。

Ⅳ 公開鍵暗号の作成

3 次方程式の解の場合で示す。2 次方程式の解の場合も同様である。

暗号文受信者の初期設定

1.乱数$m \in N$および体 K 上の乱数 x,y を生成する。ただし，乱数 x,y は周期が最大となるようにとり，m は周期以下の数とする。

2.初期条件$a_0 = 3, a_1 = x, a_2 = x^2 - 2y$で，高速計算法により$z = a_m, w = a_{-m}$を計算する。

3.x, y, z, wを公開する。

m が秘密鍵であり，x, y, z, wが公開鍵である。

$GF(2)$の既約多項式による拡大体上では，$a_0 = 1, a_1 = x, a_2 = x^2$であり，他の式も$2 \equiv 0$に注意して変形する。

暗号文送信者の作業

1.乱数$n \in N$および体 K 上の乱数 u,v を生成する。ただし，乱数 u,v は周期が最大となるようにとり，n は周期以下の数とする。

2.初期条件$a_0 = 3, a_1 = u, a_2 = u^2 - 2v$で，高速計算法により$s = a_n, t = a_{-n}$を計算する。

3.初期条件$a_0 = 3, a_1 = z, a_2 = z^2 - 2w$で，高速計算法により$p = a_n, q = a_{-n}$を計算する。

4.平文を M とし，p,q をブロック暗号の秘密鍵として M をブロック暗号化したものと，s,t を送信する。

暗号文受信者の復号処理

1.初期条件$a_0 = 3, a_1 = s, a_2 = s^2 - 2t$で，高速計算法により$p = a_m, q = a_{-m}$を計算する。

2.p,q をブロック暗号の秘密鍵として暗号文を復号し M を得る。

Ⅴ　デジタル署名

2 次方程式の解のとき

αが 2 次方程式$t^2 - xt + 1 = 0$の解のとき

$$a_n = \alpha^n + \alpha^{-n} \quad \text{より}$$

$$a_{-n} = a_n$$

$$a_n{}^2 = (\alpha^n + \alpha^{-n})^2 = \alpha^{2n} + \alpha^{-2n} + 2 = a_{2n} + 2$$

よって

$$a_{2n} = {a_n}^2 - 2$$

また

$$a_m a_n = (\alpha^m + \alpha^{-m})(\alpha^n + \alpha^{-n}) = \alpha^{m+n} + \alpha^{-(m+n)} + \alpha^{m-n} + \alpha^{-(m-n)} = a_{m+n} + a_{m-n}$$

すなわち

$$a_m a_n = a_{m+n} + a_{m-n}$$

これより

$$a_m a_n a_{m+n} = {a_{m+n}}^2 + a_{m-n} a_{m+n}$$

$$= {a_{m+n}}^2 + a_{(m-n)+(m+n)} + a_{(m-n)-(m+n)}$$

$$= {a_{m+n}}^2 + a_{2m} + a_{2n}$$

$$= {a_{m+n}}^2 + {a_m}^2 + {a_n}^2 - 4$$

よって

$$a_m a_n a_{m+n} - {a_{m+n}}^2 - {a_m}^2 - {a_n}^2 + 4 = 0$$

この恒等式は，三角関数では

$$2\cos\alpha\cos\beta\cos(\alpha+\beta) - \cos^2\alpha - \cos^2\beta - \cos^2(\alpha+\beta) + 1 = 0$$

に対応する。この三角関数の恒等式を使う方法は，石井雅治氏の電子署名についての論文[1]より得た。

$a_n = f_n(x)$ とおくと

$$f_m(x) f_n(x) f_{m+n}(x) - \{f_m(x)\}^2 - \{f_n(x)\}^2 - \{f_{m+n}(x)\}^2 + 4 = 0$$

$$f_{mn}(x) = f_m(f_n(x))$$

が成り立つ。

Schnorr 署名の変形

(1) x , $z = f_n(x)$ を送信者の公開鍵とする。n が送信者の秘密鍵である。

(2) 送信者は，文書 M に対して秘密の乱数 k を選び，次の γ ，文書 M と γ を合わせた文書のハッシュ値 e および δ を計算する。ただし， δ の計算は整数の四則演算で行う。

$$\gamma = f_k(x)$$

$$e = h(M, \gamma)$$

$$\delta \equiv ne + k \mod \text{(周期)}$$

(γ , δ)が M の署名である。

このとき,

$$f_k(x) f_{ne}(x) f_{ne+k}(x) - \{f_k(x)\}^2 - \{f_{ne}(x)\}^2 - \{f_{ne+k}(x)\}^2 + 4 = 0$$

より

$$f_k(x)f_e(f_n(x))f_{ne+k}(x) - \{f_k(x)\}^2 - \{f_e(f_n(x))\}^2 - \{f_{ne+k}(x)\}^2 + 4 = 0$$

すなわち

$$\gamma \cdot f_e(z) \cdot f_\delta(x) - \gamma^2 - \{f_e(z)\}^2 - \{f_\delta(x)\}^2 + 4 = 0 \cdots ①$$

が成り立つ。

(3) 送信者は，受信者に文書 M とその署名(γ , δ) を送る。

(4) 受信者は，ハッシュ e=h(M, γ)および $f_e(z), f_\delta(x)$ を求め，そして①の左辺を計算し，それが 0 に等しければ文書 M の署名が確認され，受信者は M が送信者のもの確信する。

ElGamal 署名の変形

(1) x , $z = f_n(x)$ を送信者の公開鍵とする。n が送信者の秘密鍵である。

(2) 送信者は，文書 M に対して周期と互いに素な秘密の乱数 k を選び，次の γ ，文書 M と γ を合わせた文書のハッシュ値 h(M, γ) ， δ を計算する。ただし， δ の計算は整数の四則演算で行う。また， k^{-1} はユークリッドの互除法で計算できる

$$\gamma = f_k(x)$$

e=h(M, γ)

$$\delta \equiv (e - n\gamma) \cdot k^{-1} \mod \text{(周期)}$$

(γ , δ) が M の署名である。

このとき $k\delta + n\gamma \equiv e$ であるから

このとき,

$$f_{k\delta}(x)f_{n\gamma}(x)f_{k\delta+n\gamma}(x) - \{f_{k\delta}(x)\}^2 - \{f_{n\gamma}(x)\}^2 - \{f_{k\delta+n\gamma}(x)\}^2 + 4 = 0$$

より

$$f_\delta(f_k(x))f_\gamma(f_n(x))f_{k\delta+n\gamma}(x) - \{f_\delta(f_k(x))\}^2 - \{f_\gamma(f_n(x))\}^2 - \{f_{k\delta+n\gamma}(x)\}^2 + 4 = 0$$

すなわち

$$f_\delta(\gamma) \cdot f_\gamma(z) \cdot f_e(x) - \{f_\delta(\gamma)\}^2 - \{f_\gamma(z)\}^2 - \{f_e(x)\}^2 + 4 = 0 \cdots ②$$

が成り立つ。

(3) 送信者は，受信者に文書 M とその署名(γ , δ) を送る。

(4) 受信者は，ハッシュ e=h(M, γ)および $f_\delta(\gamma), f_\gamma(z), f_e(x)$ を求め，そして②の左辺を計算し，それが 0 に等しければ文書 M の署名が確認され，受信者は M が送信者のものと確信する。

Schnorr 署名の変形の方が，ElGamal 署名の変形より，送信者側は互除法による逆元の計算がなく，受信者側は指数の計算が少ないため，効率が良い。

3 次方程式の解への拡張

α， β， γ が 3 次方程式 $t^3 - xt^2 + yt - 1 = 0$ の解のとき

$$\alpha^m = s, \beta^m = t, \gamma^m = u, \alpha^n = x, \beta^n = y, \gamma^n = z$$

とおくと

$$a_m a_n a_{m+n} = (\alpha^m + \beta^m + \gamma^m)(\alpha^n + \beta^n + \gamma^n)(\alpha^{m+n} + \beta^{m+n} + \gamma^{m+n})$$

$$= (s+t+u)(x+y+z)(sx+ty+uz)$$
$$= (sx+ty+uz+sy+tx+tz+uy+ux+sz)(sx+ty+uz)$$
$$= (sx+ty+uz)^2 + (sy+tx+tz+uy+ux+sz)(sx+ty+uz)$$
$$= (sx+ty+uz)^2 + \{s^2(zx+xy) + t^2(xy+yz) + u^2(yz+zx)\} + \{x^2(us+st) + y^2(st+tu) + z^2(tu+ts)\}$$
$$+ (st+tu+us)(xy+yz+zx) - (stxy+tuyz+uszx)$$
$$= (sx+ty+uz)^2 + (s^2+t^2+u^2)(xy+yz+zx) + (st+tu+us)(x^2+y^2+z^2)$$
$$- (s^2yz+t^2zx+u^2xy) - (tux^2+usy^2+stz^2)$$
$$+ (st+tu+us)(xy+yz+zx) - (stxy+tuyz+uszx)$$

ここで

$$-(s^2yz+t^2zx+u^2xy) = (st+tu+us)(xy+yz+zx) - (s+t+u)(syz+tzx+uxy)$$
$$- (stxy+tuyz+uszx)$$
$$-(tux^2+usy^2+stz^2) = (st+tu+us)(xy+yz+zx) - (xtu+yus+zst)(x+y+z)$$
$$- (stxy+tuyz+uszx)$$

であるから

$$(s+t+u)(x+y+z)(sx+ty+uz)$$
$$= (sx+ty+uz)^2 + (s^2+t^2+u^2)(xy+yz+zx) + (st+tu+us)(x^2+y^2+z^2)$$
$$+ (st+tu+us)(xy+yz+zx) - (s+t+u)(syz+tzx+uxy) - (stxy+tuyz+uszx)$$
$$+ (st+tu+us)(xy+yz+zx) - (xtu+yus+zst)(x+y+z) - (stxy+tuyz+uszx)$$
$$+ (st+tu+us)(xy+yz+zx) - (stxy+tuyz+uszx)$$
$$= (sx+ty+uz)^2 + (s^2+t^2+u^2)(xy+yz+zx) + (st+tu+us)(x^2+y^2+z^2)$$
$$- (s+t+u)(syz+tzx+uxy) - (xtu+yus+zst)(x+y+z)$$
$$+ 3(st+tu+us)(xy+yz+zx) - 3(stxy+tuyz+uszx)$$
$$= (sx+ty+uz)^2 + (s+t+u)^2(xy+yz+zx) + (st+tu+us)(x+y+z)^2$$
$$- (s+t+u)(syz+tzx+uxy) - (tux+usy+stz)(x+y+z)$$
$$- (st+tu+us)(xy+yz+zx) - 3(stxy+tuyz+uszx)$$

$\alpha\beta\gamma = 1$ より $stu = 1, xyz = 1$ であるから

$$(s+t+u)(x+y+z)(sx+ty+uz)$$
$$= (sx+ty+uz)^2 + (s+t+u)^2\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right) + \left(\frac{1}{s}+\frac{1}{t}+\frac{1}{u}\right)(x+y+z)^2$$
$$- (s+t+u)\left(\frac{s}{x}+\frac{t}{y}+\frac{u}{z}\right) - \left(\frac{x}{s}+\frac{y}{t}+\frac{z}{u}\right)(x+y+z)$$
$$- \left(\frac{1}{s}+\frac{1}{t}+\frac{1}{u}\right)\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right) - 3\left(\frac{1}{sx}+\frac{1}{ty}+\frac{1}{uz}\right)$$

を得る。よって

$$a_m a_n a_{m+n} = {a_{m+n}}^2 + {a_m}^2 a_{-n} + a_{-m} {a_n}^2 - a_m a_{m-n} - a_{-m+n} a_n - a_{-m} a_{-n} - 3a_{-m-n} \cdots ①$$

①は任意の整数 m，n について成り立つから，①の m に-m を，n に-n を代入すれば

$$a_{-m} a_{-n} a_{-m-n} = {a_{-m-n}}^2 + {a_{-m}}^2 a_n + a_m {a_{-n}}^2 - a_{-m} a_{-m+n} - a_{m-n} a_{-n} - a_m a_n - 3a_{m+n} \cdots ②$$

①の m に-m を代入すれば

$$a_{-m} a_n a_{-m+n} = {a_{-m+n}}^2 + {a_{-m}}^2 a_{-n} + a_m {a_n}^2 - a_{-m} a_{-m-n} - a_{m+n} a_n - a_m a_{-n} - 3a_{m-n} \cdots ③$$

①の n に-n を代入すれば

$$a_m a_{-n} a_{m-n} = {a_{m-n}}^2 + {a_m}^2 a_n + a_{-m} {a_{-n}}^2 - a_m a_{m+n} - a_{-m-n} a_{-n} - a_{-m} a_n - 3a_{-m+n} \cdots ④$$

①，②より

$$a_m a_{m-n} + a_n a_{-m+n} = -a_m a_n a_{m+n} + {a_{m+n}}^2 + {a_m}^2 a_{-n} + a_{-m} {a_n}^2 - a_{-m} a_{-n} - 3a_{-m-n} \cdots ⑤$$

$$a_{-n} a_{m-n} + a_{-m} a_{-m+n} = -a_{-m} a_{-n} a_{-m-n} + {a_{-m-n}}^2 + {a_{-m}}^2 a_n + a_m {a_{-n}}^2 - a_m a_n - 3a_{m+n} \cdots ⑥$$

したがって，$a_m a_{-m} - a_n a_{-n} \neq 0$ のとき⑤，⑥より a_{m-n}, a_{-m+n} が $a_m, a_n, a_{-m}, a_{-n}, a_{m+n}, a_{-m-n}$ で表されるから，これを③，④に代入すれば，$a_m, a_n, a_{-m}, a_{-n}, a_{m+n}, a_{-m-n}$ についての恒等式が得られる。

Schnorr 署名の変形

(1) $x, y, z = F_n(x,y), w = F_{-n}(x,y)$ を送信者の公開鍵とする。n が送信者の秘密鍵である。

(2) 送信者は，文書 M に対して秘密の乱数 k を選び，次の γ, λ および γ, λ と文書 M とを合わせた文書のハッシュ値 e および δ を計算する。ただし，δ の計算は整数の四則演算で行う。

$\gamma = F_k(x,y)$

$\lambda = F_{-k}(x,y)$

e=h(M, γ , λ)

$\delta = ne + k \mod$ (周期)

(γ , λ , δ)が M の署名である。

ただし，$\gamma\lambda - F_{ne}(x,y) F_{-ne}(x,y) \neq 0$ となるように k をとる。

(3) 送信者は，受信者に文書 M とその署名(γ , λ , δ)を送る。

(4) 受信者は，ハッシュ値 e=h(M, γ , λ)を求める。そして

$A = F_e(z,w)$， $B = F_{-e}(z,w)$

$G = F_\delta(x,y)$， $H = F_{-\delta}(x,y)$

を求め，さらに

$P = G(G - \gamma A) + \gamma^2 B + \lambda(A^2 - B) - 3H$

$Q = H(H - \lambda B) + \lambda^2 A + \gamma(B^2 - A) - 3G$

$D = \gamma\lambda - AB \quad (D \neq 0)$

$Z = \lambda P - AQ$

$W = -BP + \gamma Q$

を求める。このとき次の等式が成り立てば，文書 M の署名が確認され，受信者は M が送信者のものと確信する。

$$(Z-D\gamma B)Z+D^2\{\gamma^2 A+\lambda(B^2-A)-\gamma G-HB\}-3DW=0$$
$$(W-D\lambda A)W+D^2\{\lambda^2 B+\gamma(A^2-B)-\lambda H-GA\}-3DZ=0$$

上記の恒等式の証明

$$a_m a_n a_{m+n}={a_{m+n}}^2+{a_m}^2 a_{-n}+a_{-m}{a_n}^2-a_m a_{m-n}-a_{-m+n}a_n-a_{-m}a_{-n}-3a_{-m-n}$$

より

$$F_k(x,y)F_{ne}(x,y)F_{k+ne}(x,y)=\{F_{k+ne}(x,y)\}^2+\{F_k(x)\}^2F_{-ne}(x,y)+F_{-k}(x,y)\{F_{ne}(x,y)\}^2$$
$$-F_k(x,y)F_{k-ne}(x,y)-F_{-k+ne}(x,y)F_{ne}(x,y)-F_{-k}(x,y)F_{-ne}(x,y)-3F_{-k-ne}(x,y)$$

したがって

$$\gamma F_{ne}(x,y)F_\delta(x,y)=$$
$$\{F_\delta(x,y)\}^2+\gamma^2F_{-ne}(x,y)+\lambda\{F_{ne}(x,y)\}^2-\gamma F_{k-ne}(x,y)-F_{-k+ne}(x,y)F_{ne}(x,y)-\lambda F_{-ne}(x,y)-3F_{-\delta}(x,y)$$

このとき

$$F_{ne}(x,y)=F_e(z,w)$$
$$F_{-ne}(x,y)=F_{-e}(z,w)$$

が成り立つから

$$\gamma F_e(z,w)F_\delta(x,y)=$$
$$\{F_\delta(x,y)\}^2+\gamma^2F_{-e}(z,w)+\lambda\{F_e(z,w)\}^2-\gamma F_{k-ne}(x,y)-F_{-k+ne}(x,y)F_e(z,w)-\lambda F_{-e}(z,w)-3F_{-\delta}(x,y)$$

ここで,

$$X=F_{k-ne}(x,y),\quad Y=F_{-k+ne}(x,y)$$

とおき，さらに

$$A=F_e(z,w),\quad B=F_{-e}(z,w)$$
$$G=F_\delta(x,y),\quad H=F_{-\delta}(x,y)$$

とおくと

$$\gamma AG=G^2+\gamma^2B+\lambda A^2-\gamma X-YA-\lambda B-3H\cdots①$$

同様にして

$$\lambda BH=H^2+\lambda^2A+\gamma B^2-\lambda Y-XB-\gamma A-3G\cdots②$$

また

$$\gamma BX=X^2+\gamma^2A+\lambda B^2-\gamma G-HB-\lambda A-3Y\cdots③$$
$$\lambda AY=Y^2+\lambda^2B+\gamma A^2-\lambda H-GA-\gamma B-3X\cdots④$$

①，②より

$$\gamma X+AY=G(G-\gamma A)+\gamma^2B+\lambda(A^2-B)-3H\cdots⑤$$
$$BX+\lambda Y=H(H-\lambda B)+\lambda^2A+\gamma(B^2-A)-3G\cdots⑥$$

が成り立つから,

$$D=\gamma\lambda-AB\quad(D\neq0)$$

とおき，⑤，⑥の右辺をそれぞれ P，Q とすると

$$DX=\lambda P-AQ$$

$$DY = -BP + \gamma Q$$

また，③，④の両辺に D^2 をかけて

$$(DX - D\gamma B)DX + D^2\{\gamma^2 A + \lambda(B^2 - A) - \gamma G - HB\} - 3D(DY) = 0$$

$$(DY - D\lambda A)DY + D^2\{\lambda^2 B + \gamma(A^2 - B) - \lambda H - GA\} - 3D(DX) = 0$$

となるから，$Z = DX, W = DY$ とおけば，恒等式が得られる。

ElGamal 署名の変形も，2 次方程式の場合と同様に設計できる。

Ⅵ　今後の課題

1. α，β や γ が有限体 K の拡大体にあるとき，x,y がどのような条件を満たせば周期が最大になるか不明である。体 K およびその拡大体の位数から，考えられる周期をすべて求め，最大周期未満の周期になる x,y を除外するのがよいであろう。
2. 2 次方程式 $t^2 - xt + 1 = 0$ や 3 次方程式 $t^3 - xt^2 + yt - 1 = 0$ が解かれて，α，β や γ が求められると，離散対数問題に帰着する。2 次方程式や 3 次方程式が指数時間でしか解けない体 K が望ましい。$GF(2)$ の既約多項式による拡大体上では，2 次式の平方完成ができないため，解の公式は適用できない。
3. 通常の離散対数問題では，準指数時間の解読法が存在するようだが，この方法に準指数時間の攻撃法が存在すれば，この方法は暗号化・復号化に時間がかかるため，この方法は無意味である。この辺りは不明である。

参考文献

[1] 石井雅治，2 冪剰余環上の Chebyshev 多項式の周期性と電子署名，日本応用数理学会論文誌 Vol.18,No.2, (2008),257-265