# 楕円曲線と巡回対合

難波完爾(Kanji NAMBA)
719-1117岡山県総社市北溝手463-3
tel/fax. 0866-90-1886

対合(involution)というのは、例えば複素数の共役(conjugate)のように、作用$p$の自乗が恒等写像(identity)になるものである。巡回行列(cyclic matrix)でこのような性質をもつものを巡回対合(cyclic involution)という。勿論、Euclid空間の距離を保つ線形変換で巡回的なもの、つまり、巡回直交行列(cyclic orthogonal matrix)というのと同じである。最小多項式(minimal polynomial)が$x^2-1=(x+1)(x-1)$である巡回行列、あるいは固有値(eigen-value)が±1の巡回行列ということもできる。

対合$p$の社会に於ける意味であるが、それは実体としての存在(例えば、1 点)を空間の広い場所に分散して置く(記憶など)とき、時間の経緯、衝撃や雑音などによって変化を受けても$p$によって、局所的な破壊から、元の状態を或程度、復元が可能であるとか、或いは$p$によって何が作用したかを計ることが可能である。これは、純粋数学の内部の問題としてだけではなく社会や認識科学との一つの重要な接点でもある。

ここでは特に、楕円曲線、つまり、$xy$-平面上の3次曲線

$$C:\ y^2 = x^3+ax+b$$

に関係した巡回対合について述べる。

上記のような楕円曲線のワイエルストラス標準形(Weierstraß normal form)を有限体(finite-field)

$$F_p = GF(p) = p = \{0,1,2,\cdots, p-1\}$$

で考えると、$C$は可換群(abelian group)の構造をもつことが知られている。
楕円曲線の$j$-不変量($j$-invariant)、$j = z = -27b^2/4a^3$ を助変数(parameter)として、この群の位数(order)、つまり元の個数は$d = [p/12]$次の多項式

$$a_{12}(z)= \begin{cases} z^{(p-1)/4}\cdot F(1/12,5/12,1,1-z) & \text{if } p = 1 \bmod 4 \\ z^{(p+1)/4}\cdot F(7/12,11/12,1,1-z) & \text{if } p = -1 \bmod 4 \end{cases}$$

の$p \geq 17$では、最小絶対値で与えられる。

例えば、$p = 17$のときは、

$$a_{12}(x)= x^4(10x+8)$$

である。17での原始根は

$$[3,\ 5,\ 6,\ 7,\ 10,\ 11,\ 12,\ 14]$$

なので、例えば、最小の$q = 3$をとる。

$$[a_{12}(q^{i-1}), i = 0\cdots p-2]$$

の表、つまり、$a_{12}(x)$を原始根のべき乗の順に並べた表は

$$[1, 1, 4, 7, 2, 6, -5, -4, -2, 3, -3, 6, -3, -2, 6, 0]$$

である。それを$x$のべきの係数とする多項式

$$f(x)= 1+x+4x^2+7x^3+2x^4+6x^5-5x^6-4x^7-2x^8+3x^9-3x^{10}+6x^{11}-3x^{12}-2x^{13}+6x^{14}$$

を$a_{12}(x)$表現多項式という。

一般的に表現多項式(representing polynomial)を

$$a_{12}(x)= \Sigma_{n\in p-1}\ a_{12}(q^{n-1})x^{n-1}$$

と定義する。係数の絶対値はHasseの不等式から、

$$|a_{12}(x)| < 2\sqrt{p}$$

であり、1の$p$-1乗根、つまり

$$x^{p-1}-1 = 0$$

言い換えると

$$\{\cos(2\pi k/(p-1))+i\cdot\sin(2\pi k/(p-1)):\ k = 0\cdots p-2\}$$

上での$a_{12}(x)$の値は、$p = 1, 5, -5, -1 \bmod 12$に応じて、各々4, 2, 2, 0個が絶対値$\sqrt{p}$ であり他のものは絶対値$p$であることが予想される。

ここでは、一例として、$p = 23$の場合の周期$11 = (p-1)/2$の場合の例を挙げる：

$$p = 23,\ q = 5$$

$$A = 1/23\cdot$$

$$[-1, -8, 5, -6, -2, 7, 10, -12, -4, -9, -3]$$
$$[-8, 5, -6, -2, 7, 10, -12, -4, -9, -3, -1]$$
$$[5, -6, -2, 7, 10, -12, -4, -9, -3, -1, -8]$$
$$[-6, -2, 7, 10, -12, -4, -9, -3, -1, -8, 5]$$
$$[-2, 7, 10, -12, -4, -9, -3, -1, -8, 5, -6]$$
$$[7, 10, -12, -4, -9, -3, -1, -8, 5, -6, -2]$$
$$[10, -12, -4, -9, -3, -1, -8, 5, -6, -2, 7]$$
$$[-12, -4, -9, -3, -1, -8, 5, -6, -2, 7, 10]$$
$$[-4, -9, -3, -1, -8, 5, -6, -2, 7, 10, -12]$$
$$[-9, -3, -1, -8, 5, -6, -2, 7, 10, -12, -4]$$
$$[-3, -1, -8, 5, -6, -2, 7, 10, -12, -4, -9]$$

このような巡回対合は、例えば素数11であれば$p = 11n+1$の形の任意の任意の素数に対して、表現多項式と$x^p-x = x(x^{p-1}-1)$の因数との退行型終結行列(Sylvester matrix, resultant)

$$a_{12}(x)[x]x^r-1$$

として表現できる。

また、例えば、楕円曲線族

$$C:\ y^2 = x^3+ax^2+b$$

に応ずる$d = [p/6]$次の超幾何級数(多項式)

$$a_6(x)= (x/p)F(1/6,5/6,1,x)$$

やその他の楕円曲線族に応ずる

$$a_4(x)= F(1/4,3/4,1,x),\ a_3(x)= F(1/3,2/3,1,x),\ a_2(x)= F(1/2,1/2,1,x)$$

からも巡回対合が終結行列として構成可能である。但し、$a_2(x)$については問題がある。佐藤$\sin^2$-予想との関連については、Dedekind $\eta$関数と佐藤$\sin^2$-予想、津田塾大学数学・計算機科学研究所報、第15回数学史シンポジウム(2005)に掲載予定。