Hyper-elliptic curves over finite fields and Tschebysheff-shift

by Kanji Namba

463-3 Kitamizote Sojya Okayama 719-1117

tel/fax. 0866-90-1886

2015. 01. 05

key words

hyper-elliptic curve, finite field, Tschebysheff polynomial, Legendre polynomial, Taniyama-Shimura theory, resultant transform, congruence zeta, coefficient transform, cyclic involution, $\sin^2$-conjecture (for hyper-elliptic curves), Lissajous curve elliptic involution property, Vandermonde transform, Mordell-Weil group

1. introduction, definition and notions

ここでは、有限体上の、超楕円曲線(hyper-elliptic curve)

$$C:\ y^2 = x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n = f(x)$$

とその終結変換多項式(≒ resultant transform polynomial, ζ-polynomial)について考える。

先ず、有限(素)体

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

を考え、平方剰余の記号(= Legendre symbol)を(odd prime)

$$(a/p) = \#\{x\in p : x^2 = a \text{ in } F_p\}-1\ \ (= a^{(p-1)/2} \bmod p)\ \ \in \{-1,0,1\}$$

と記す。

1.1 終結式

終結式(resultant)の省略記号として変数を○で囲んだ記号、気持ちとしては変数を隠す(conceal)あるいは消す(eliminate)作用素を、(ここだけの省略記号)として用いる。例えば、

$$f(x)\textcircled{x}\, g(x) = \text{resultant}(f(x),g(x),x)$$

のように記し、消去積(elimination product)とも呼ぶ。

$$f(x)\textcircled{x}\,(x-y) = f(y)$$

$$f(x) ⓧ g(x) = (-1)^{nm} g(x) ⓧ f(x)$$

$$f(x) ⓧ (g(x)h(x)) = (f(x) ⓧ g(x))(f(x) ⓧ h(x))$$

$$f(x) ⓧ (g(x)/h(x)) = (f(x) ⓧ g(x))/(f(x) ⓧ h(x))$$

$$f(x) ⓧ g(x)^n = f(x)^n ⓧ g(x)$$

$$f(x) ⓧ (g(x,y) ⓨ h(y)) = (f(x) ⓧ g(x,y)) ⓨ h(y)$$

などの性質がある。上記 3 式は帰納的な定義と考えてもよい。消去積は何重にも重ねて用いられることが多いのでこのような記法を用いた。

例えば、代数的整数、虚数単位 $i = \sqrt{-1}$, 黄金比 $\omega (= (1+\sqrt{5})/2$, golden ratio), 2 の立方根 $(= \sqrt[3]{2})$ の和、差、積で表現できる式、$\sqrt[3]{2} + i\omega$、が代数的整数であることは、それぞれの (monic) 定義方程式

$$t-(x+yz) = 0,\ x^3-2 = 0,\ y^2+1 = 0,\ z^2-z-1 = 0$$

の終結式

$$(((t-(x+yz)) ⓧ x^3-2) ⓨ y^2+1) ⓩ z^2-z-1 =$$

$$t^{12}+9t^{10}-8t^9+30t^8+69t^6-12t^5-78t^4+4t^3+237t^2+228t+89$$

が (monic な多項式の終結式が monic だから)、monic であることが (計算しなくても) 解る。

一般終結式 (general resultant) は

$$ⓧ(f_1(x), \cdots, f_n(x))$$

のように記す。内容は $f_1(x), \cdots, f_n(x)$ が「互いに素」(relatively prime) であることを意味しており、多項式

$$g_i(x) = f_1(x) \cdots f_n(x)/f_i(x)$$

の係数を $f_i(x)$ の次数だけずらしながら記した $f_1(x) \cdots f_n(x)$ の次数の正方行列 (あるいは行列式) である。特に、各因子が一次式 $f_i(x) = x-a_i$ の場合は Vandermonde's matrix (determinant) である。例えば

$$ⓧ(x^3-2, x^2+1, x^2-x-1) = -125 = -5^3$$

$$\begin{vmatrix} 1, -1, 0, -1, -1, 0, 0 \\ 0, 1, -1, 0, -1, -1, 0 \\ 0, 0, 1, -1, 0, -1, -1 \\ 1, -1, -1, -2, 2, 2, 0 \\ 0, 1, -1, -1, -2, 2, 2 \\ 1, 0, 1, -2, 0, -2, 0 \\ 0, 1, 0, 1, -2, 0, -2 \end{vmatrix}$$

1.2　終結係数(resultant coefficient)

代数拡大での曲線上の点の個数の計算のためには

$$f_n(u_1,\cdots,u_m) = f(x) \otimes x^m+u_1x^{m-1}+\cdots+u_{m-1}x+u_m$$

として、(⊗の結合力は+, -, ×, /より弱い)Legendre 和(pは省略して)

$$a_n = \sum u_1,\cdots,u_m \in p\ (f_n(u_1,\cdots,u_m)/p)$$

と定義し、終結変換多項式(resultant transform = ζ-polynomial)を

a)　f(x)の次数 n が奇数の場合

$$\zeta f(x) = x^{2n}+a_1x^{2n-1}+\cdots+a_nx^{n-1}+pa_{n-1}x^{n-2}+\cdots+p^{n-1}a_1x+p^n$$

b)　f(x)の次数 n が偶数の場合

$$b_m = 1+a_1+\cdots+a_m$$

$$\zeta f(x) = x^{2n}+b_1x^{2n-1}+\cdots+b_nx^{n-1}+pb_{n-1}x^{n-2}+\cdots+p^{n-1}b_1x+p^n$$

と定義する。

次に係数多項式(coefficient polynomial = η-polynomial)を

$$\eta f(t) = \sqrt{\zeta f(x) \otimes t^2+tx+p}$$

とする。($\zeta f(x) \otimes t^2+tx+p$ は完全平方なので)

定義の説明として、谷山・志村理論(Simura-Taniyama　theory)によると、$\zeta f(x) = 0$ の根 α は

$$\alpha = \sqrt{p}\, e^{i\theta} = \sqrt{p}\,(\cos\theta+i\sin\theta)$$

の形の複素数であるから

$$t^2-(2\sqrt{p}\cos\theta)\,t+p = (t-\alpha)\,(t-\bar{\alpha}) = 0$$

を満足している。言い換えると、ζf(x)は実係数であるから、

$$\zeta f(x) \otimes t^2+tx+p$$

は完全平方式で $\zeta f(x) = 0$ の実部(real part)、つまり、$x = 2\sqrt{p}\cos\theta$ を t^2+tx+p に代入したものの積になっている。つまり、Taniyama-Shimura property は

$$\eta f(t) = 0$$

の根はすべて Hasse 区間$[-2\sqrt{p}, 2\sqrt{p}]$に属する実数であるということである。標準係数多項式(normalized coefficient polynomial = ξ-polynomial)は、標準区間[-2,2]に写したもので

$$\xi f(t) = \eta f(\sqrt{p}t) = \sqrt{\zeta f(x) \otimes t^2+\sqrt{p}tx+p}$$

で定義される。これは、ζf(x)の測度$(dx/\sqrt{4-x^2})$での直交展開、つまり、Tschebysheff 多項式展開(Tschebysheff expansion)に他ならない。

Tschebysheff 多項式は $x = 2\cos(\theta)$ としたときの $2\cos(n\theta)$ を x の多項式と

して表現したもので余弦の n 倍公式である。つまり、

$$t_n(x) = \sqrt{s^{2n}+1} \circledS\ sx\text{-}s^2\text{-}1$$

である。結果は、よく知られているとおり

$[1, x], [2, x^2-2], [3, x^3-3x], [4, x^4-4x^2+2], [5, x^5-5x^3+5x], [6, x^6-6x^4+9x^2-2],$

$[7, x^7-7x^5+14x^3-7x], [8, x^8-8x^6+20x^4-16x^2+2], [9, x^9-9x^7+27x^5-30x^3+9x],$

$[10, x^{10}-10x^8+35x^6-50x^4+25x^2-2], [11, x^{11}-11x^9+44x^7-77x^5+55x^3-11x],$

$[12, x^{12}-12x^{10}+54x^8-112x^6+105x^4-36x^2+2],$

$[13, x^{13}-13x^{11}+65x^9-156x^7+182x^5-91x^3+13x],$

$[14, x^{14}-14x^{12}+77x^{10}-210x^8+294x^6-196x^4+49x^2-2],$

$[15, x^{15}-15x^{13}+90x^{11}-275x^9+450x^7-378x^5+140x^3-15x],$

$[16, x^{16}-16x^{14}+104x^{12}-352x^{10}+660x^8-672x^6+336x^4-64x^2+2],$

$[17, x^{17}-17x^{15}+119x^{13}-442x^{11}+935x^9-1122x^7+714x^5-204x^4+17x],$

$[18, x^{18}-18x^{16}+135x^{14}-546x^{12}+1287x^{10}-1782x^8+1386x^6-540x^4+81x^2-2],$

$[19, x^{19}-19x^{17}+152x^{15}-665x^{13}+1729x^{11}-2717x^9+2508x^7-1254x^5+285x^3-19x],$

$[20, x^{20}-20x^{18}+170x^{16}-800x^{14}+2275x^{12}-4004x^{10}+4290x^8-2640x^6+825x^4-100x^2+2]$

などである。終結変換多項式

$$\zeta f(x) = x^{2n}+a_1x^{2n-1}+\cdots+a_nx^{n-1}+pa_{n-1}x^{n-2}+\cdots+p^{n-1}a_1x+p^n$$

が

$$\zeta f(s) = s^{2n}+p^n+a_1s\,(s^{2(n-1)}+p^{n-1})+\cdots+a_{n-2}s^{n-2}\,(s^2+p)+a_ns^{n-1}$$

の形であるから、各部分と $s^2+\sqrt{p}sx+p$ の$\circledS$終結式を計算することにより、Tschebysheff 多項式展開

$$\xi f(x) = t_n(x)+a_1t_{n-1}(x)+\cdots+a_{n-1}x+a_n$$

が得られるのである。だから、a_i は Tschebysheff 係数、あるいは Tschebysheff 変換(transform)と表現するのが適当かも知れない。Hasse-Taniyama-Shimura property は Tschebysheff transform の実根条件なのである。

例 1.

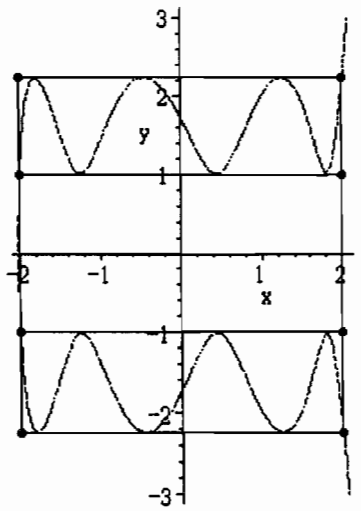
$$y^2 = x^7-7x^5+14x^3-7x+3$$

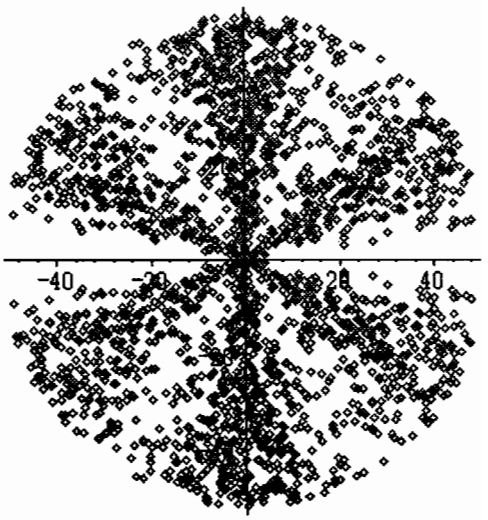
この超楕円曲線の種数(genus)は 3 である。つまり、7 次 Tschebysheff 多項式の種数 3 だけの shift、Tschebysheff-shift 多項式(仮の名称)である。

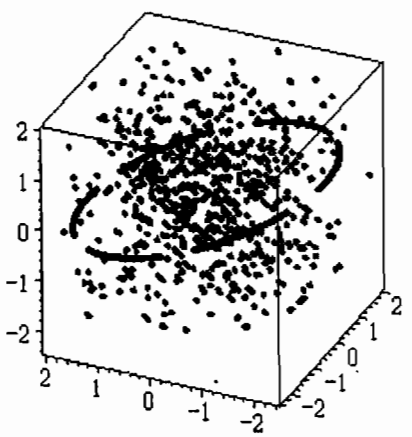
以下の図は標準 ζ-根の xyz-空間$[-2,2]^3$での像です：

$$\xi f(x) = t_3(x)+a_1t_2(x)+a_2x+a_3 = 0$$

$$[x,y,z]: \xi f(x) = \xi f(y) = \xi f(z) = 0,\ p = 3 \sim 2671$$


3
2
y
1
-2
-1
1
2
x
-1
-2
-3


-40
40


2
1
0
-1
-2
2
1
0
-1
-2
2
1
0
-1
-2

基本データの一部は、$[p, a_p, b_p, c_p]$について：

[3, 0, 0, 0],[5, 0, 0, 1],[7, 0, 0, 0],[11, 0, 0, 44],[13, 1, 9, -17],[17, 0, 0, -66],
[19, 0, 0, -130],[23, 0, 0, 82],[29, -1, 57, -99],[31, 0, 0, -8],[37, 0, 0, 254],
[41, 24, 315, 2480],[43, 4, 125, 336],[47, 0, 0, 192],[53, 0, 0, -144],
[59, 0, 0, -70],[61, 0, 0, 680],[67, 0, 0, 752],[71, 7, 227, 1001],[73, 0, 0, 986],
[79, 0, 0, -28],[83, -15, 317, -2587],[89, 0, 0, 140],[97, 21, 347, 3493],
[101, 0, 0, -762],[103, 0, 0, 24],[107, 0, 0, 462],[109, 0, 0, 1078],
[113, -26, 499, -6108],[127, 6, 365, 1532],[131, 0, 0, 1546],[137, 0, 0, -1104],
[139, -22, 401, -6108],[149, 0, 0, -1790],[151, 0, 0, 212],[157, 0, 0, 794],
[163, 0, 0, 1186],[167, -57, 1577, -25771],[173, 0, 0, -2142],[179, 0, 0, 2244],
[181, -2, 479, -828],[191, 0, 0, 2536],[193, 0, 0, 1988],[197, 32, 699, 11592],
[199, 0, 0, 722],[211, -33, 219, 1613],[223, 19, 759, 8503],[227, 0, 0, -2604]

のようです。$p \neq \pm 1 \bmod 7$ に対しては、係数多項式は

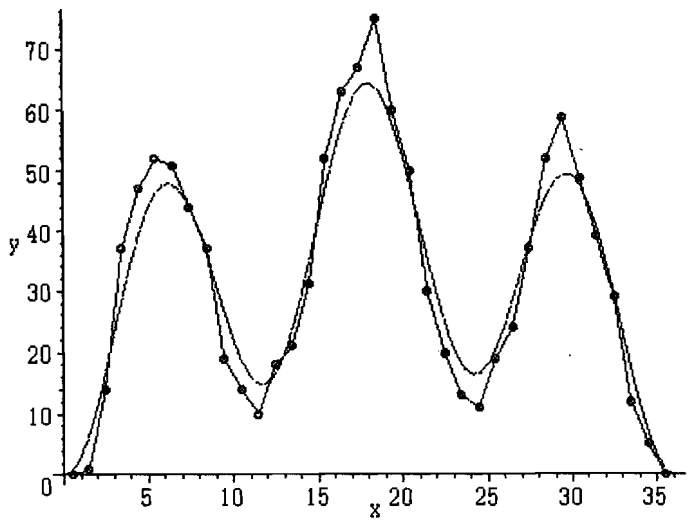
$$t_3(x)+k = x^3-3x+k$$

の形ですから、

$$t_3(x)+k \text{ ⓚ } t_3(y)+k = (y-x)(x^2+yx+y^2-3) = 0$$

から、Lissajous curve として標準正方形$[-2,2]^2$に内接する楕円が得られます。勿論、立体像では立方体に内接する半径$\sqrt{6}$の円です。

尚、$p \neq \pm 1 \bmod 7$, $p = \pm 1 \bmod 7$ となる素数から生ずるζ根、つまり、$\zeta f(x) = 0$ の根は $p = 3 \sim 2671$ の範囲で 780 個と 380 個です。極限の比は 2:1 で、その偏角の分布の図はのようです。



全体の分布の期待値は、標語的表現では

$$2\cdot\sin^2(3x)+1\cdot\sin^2(x)$$

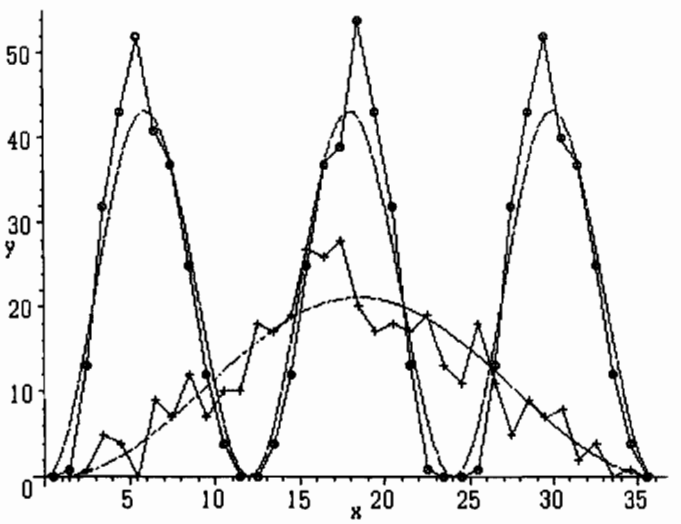
に比例する分布ということでしょう。つまり、$\sin^2(x)$, $\sin^2(3x)$に 1:2 の重さで分布するのでしょう。勿論これは予想(conjecture)です。少なくとも、図から$\sin^2(3x)$に比例する部分には、少し無理があるかも知れません。
更に高次の「何か」があることは確かでしょう。今の、私の計算能力では、pの大きさを 10 倍まで計算してみることはできませんが、何か本質的に新しい概念が登場する可能性のある場面です。成分に分けた表示では

$$y^2 = x^7-7x^5+14x^3-7x+3$$

angular distribution, $p = 3 \sim 2671$

$p \neq \pm1 \bmod 7$, $p = \pm1 \bmod 7$

$\sin^2(3\pi x)$, $\sin^2(\pi x)$

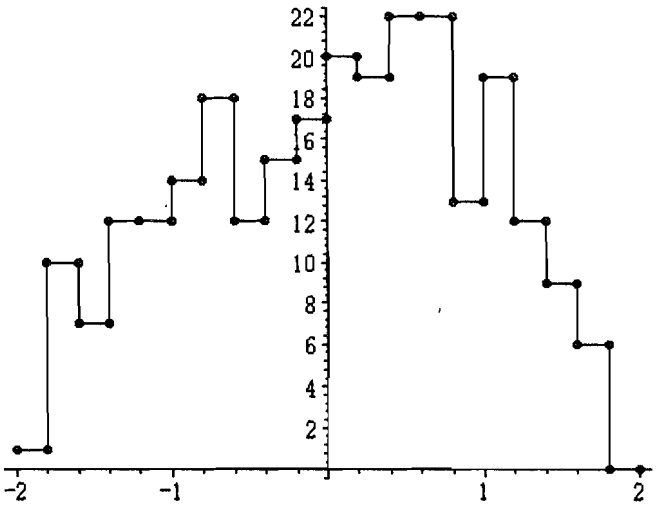


である。因みに、$p \neq \pm1 \bmod 7$に対応する

$$t_3(x)+k = x^3-3x+k,\ k = a_3/p^{3/2}$$

の頻度の図は次のようである。$\sqrt{4-x^2}$(半円)の形であれば $\sin^2(3\pi x)$を意味している。

$p \neq \pm1 \bmod 7$, $p = 3 \sim 2671$



例 2

$$y^2 = x^{11}-11x^9+44x^7-77x^5+55x^3-11x+5$$

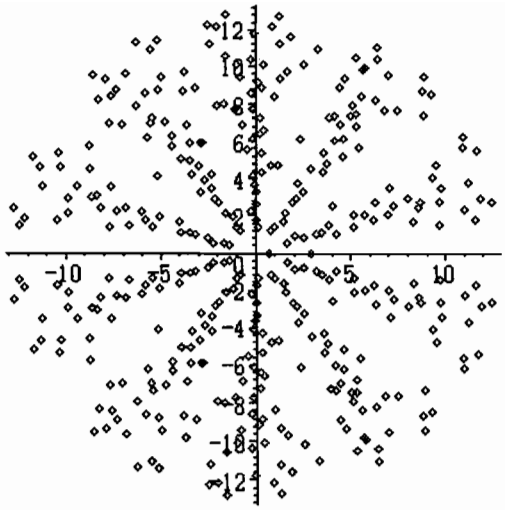
この場合も 11 次の Tschebysheff 多項式の種数 5 だけの shift です。

計算量の関係で p = 3 ~ 167 までのデータですが、基本データは次のようです。[p, a_p, b_p, c_p, d_p, e_p] :

[2, -1, -2, -4, -8, -14], [3, 0, 0, 0, 0, -1], [5, 0, 0, 0, 0, 50], [7, 0, 0, 0, 0, -1], [11, 0, 0, 0, 0, 0], [13, 0, 0, 0, 0, 30], [17, 0, 0, 0, 0, 462], [19, 0, 0, 0, 0, -1284], [23, -2, 55, -160, 1726, -5980], [29, 0, 0, 0, 0, -2406], [31, 0, 0, 0, 0, 3596], [37, 0, 0, 0, 0, 2194], [41, 0, 0, 0, 0, -4350], [43, 16, 247, 2344, 21402, 143792], [47, 0, 0, 0, 0, 14316], [53, 0, 0, 0, 0, -5568], [59, 0, 0, 0, 0, 3544], [61, 0, 0, 0, 0, 37210], [67, -5, 257, -1229, 31263, -116057], [71, 0, 0, 0, 0, -46410], [73, 0, 0, 0, 0, 13970], [79, 0, 0, 0, 0, -21186], [83, 0, 0, 0, 0, -9240], [89, 3, 343, 635, 52835, 67683],[97, 0, 0, 0, 0, -136468], [101, 0, 0, 0, 0, -44352], [103, 0, 0, 0, 0, 102190],[107, 0, 0, 0, 0, 31284], [109, 26, 525, 7800, 107582, 1179004], [113, 0, 0, 0, 0, 181704], [127, 0, 0, 0, 0, -189646], [131, -16, 423, -4632, 82738, -756624], [137, 0, 0, 0, 0, -317594], [139, 0, 0, 0, 0, 12116], [149, 0, 0, 0, 0, -199606], [151, 0, 0, 0, 0, 407002],[157, 0, 0, 0, 0, 519972], [163, 0, 0, 0, 0, -335076], [167, 0, 0, 0, 0, 413694]

$$y^2 = x^{11}-11x^9+44x^7-77x^5+55x^3-11x+5$$

$$\zeta f(x) = 0,\ p = 2 \sim 167$$



この場合も $p \neq \pm 1 \bmod 11$ の場合は、標準係数多項式は

$$\xi f(x) = t_5(x) + k = x^5 - 5x^3 + 5x + k$$

の形です。従って、これらの、実数解の対(x,y)を xy-平面に記したものは、k を消去した

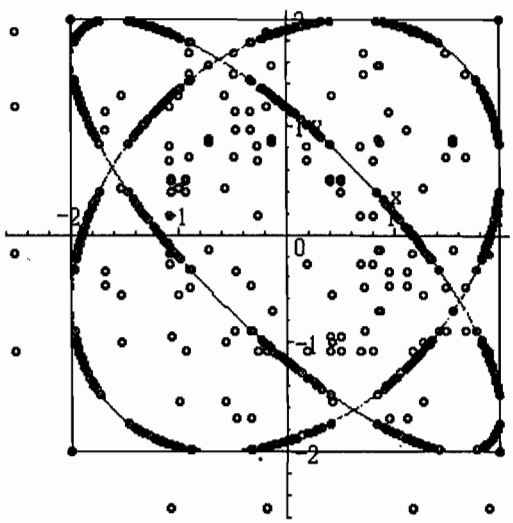
$$x^5 - 5x^3 + 5x + k - (y^5 - 5y^3 + 5y + k) = x^5 - 5x^3 + 5x - (y^5 - 5y^3 + 5y)$$

$$= 1/4 \cdot (y-x)\,(-2x^2 + 5 + \sqrt{5} - xy + xy\sqrt{5} - 2y^2)\,(2x^2 - 5 + \sqrt{5} + xy + xy\sqrt{5} + 2y^2) = 0$$

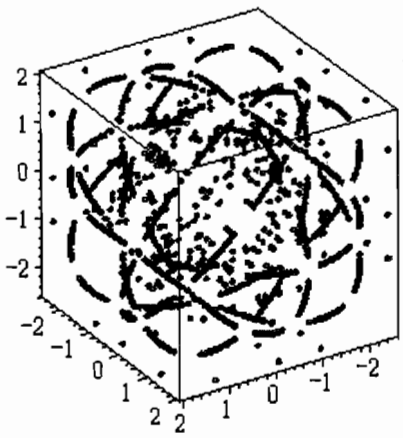
という基本平方形 $[-2,2]^2$ に内接する楕円、つまり、リサージュ楕円(Lissajous ellipse)の上にあります。(2 つの楕円)

$$y^2 = x^{11} - 11x^9 + 44x^7 - 77x^5 + 55x^3 - 11x + 5$$

$$[x,y]: \xi f(x) = \xi f(x) = 0,\ p = 2 \sim 167$$



参考のため、xyz-空間での点分布は、一般の視点からですが、荒い籠(かご)のような図形です。



初めて、この図形に出会ったのは p = 2 ~ 67 の段階で、2012.06.29.17:43 のことで、「わっ！出た」(What d'état)と思ったのです。そこで、

なれれれれ、ひさしきともに、あへるものかな

とよみてながめる。勿論、

$$p \neq \pm 1 \bmod 11,\ p = \pm 1 \bmod 11$$

によって明確に区別されます。それらは、$p \neq \pm 1 \bmod 11$ のもの 32 個と、$p = \pm 1 \bmod 11$ のもの 6 個で、極限は mod 11 の既約剰余の比 4:1 でしょう。

[23, -2, 55, -160, 1726, -5980], [43, 16, 247, 2344, 21402, 143792],

[67, -5, 257, -1229, 31263, -116057], [89, 3, 343, 635, 52835, 67683],

[109, 26, 525, 7800, 107582, 1179004], [131, -16, 423, -4632, 82738, -756624],

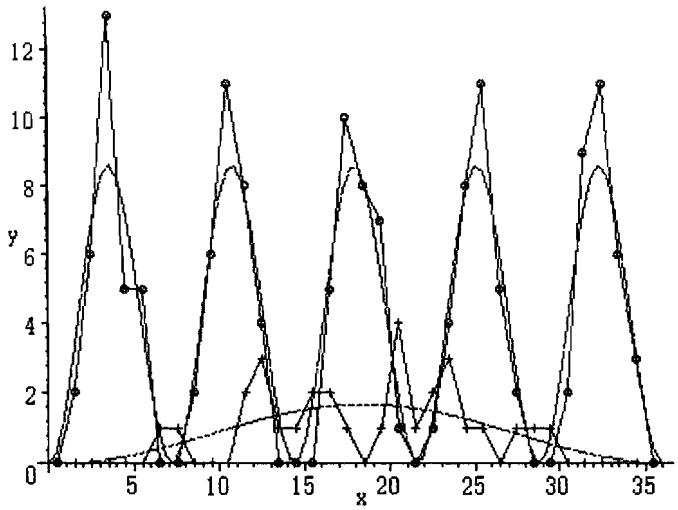
これらに対しても考慮した結果の表は次のようです。

$$y^2 = x^{11}-11x^9+44x^7-77x^5+55x^3-11x+5$$

angular distribution, $p = 3 \sim 167$

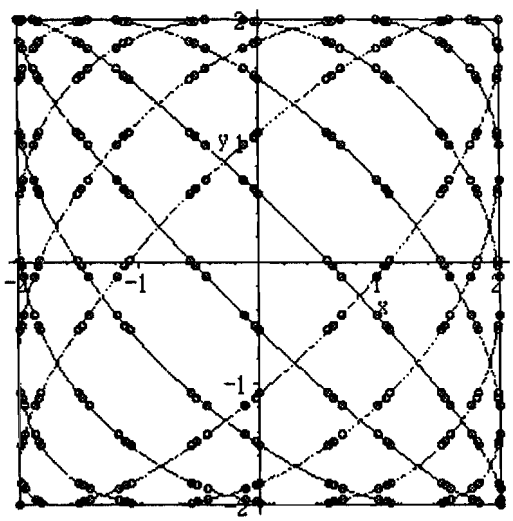
$$p \neq \pm 1 \bmod 11,\ p = \pm 1 \bmod 11$$

$$4\sin^2(5\pi x),\ \sin^2(\pi x)$$



例 3.

$$y^2 = x^{23}-23x^{21}+230x^{19}-1311x^{17}+4692x^{15}-10948x^{13}$$
$$+16744x^{11}-16445x^9+9867x^7-3289x^5+506x^3-23x+11$$
$$\det = 2^{161}\cdot 3^{46}\cdot 23^{23}$$
$$p = 3, 5, 7$$
$$\eta f(x) = x^{11}-11x^9+44x^7-77x^5+55x^3-11x+k$$
$$k = -1/3^{11/2}\ ,\ 3186/5^{11/2}\ ,\ 57140/7^{11/2}$$



上記の種数 11 の場合は p = 11 の場合でさえ、$t_{11}(x)+k = 0$ の形であるとは確かめているのですが k の値は計算できていません。大変興味があります。

何しろ、今の計算方法では、

$$f_n(u_1,\cdots,u_{11}) = f(x) \otimes x^{11}+u_1x^{10}+\cdots+u_{10}x+u_{11}$$

の Legendre 記号を $n = 11^{11} = 285311670611$ 回計算する必要があります。私のパソコンには荷が重いのです。p = 11, 13, …などは現在でも計算可能な範囲でしょう。しかし、p が 100 を越える範囲のデータを得るのは大変な感じです。

$$p = 47$$

$$x^{47}-47x^{45}+1034x^{43}-14147x^{41}+134890x^{39}-951938x^{37}+5154396x^{35}-21906183x^{33}$$
$$+74144004x^{31}-201619660x^{29}+442473416x^{27}-784384692x^{25}+1120549560x^{23}$$
$$-1282801080x^{21}+1166182800x^{19}-830905245x^{17}+455657715x^{15}-187623765x^{13}$$
$$+56071470x^{11}-11593725x^{9}+1545830x^{7}-118910x^{5}+4324x^{3}-47x+23$$

などではどうでしょうか。しばらくは夢でしょうね。

Tschebysheff 多項式に定数を加えた多項式(Tschebysheff shift)については、例えば、次数 5 種数 2 の場合などでは

$$p \neq \pm 1 \bmod 5,\ p = \pm 1 \bmod 5$$

によって、分布が

$$\sin^2(2\pi x),\ \sin^2(\pi x)$$

に分解されることはよく認識されていました。例えば、

$$y^2 = x^5-5x^3+5x+1 = (x+1)(x^4-x^3-4x^2+4x+1)$$

での基本データは

$$[p,\ a_p,\ b_p]$$

[3, 0, 1], [5, 0, 0], [7, 0, 6], [11, 2, 18], [13, 0, -12], [17, 0, 20], [19, 2, 34], [23, 0, 38], [29, -8, 54], [31, 4, 46], [37, 0, 12], [41, 12, 98], [43, 0, 50], [47, 0, -34], [53, 0, 48], [59, -12, 134], [61, 4, 126], [67, 0, 42], [71, -6, 106], [73, 0, 24], [79, -6, 122], [83, 0, 50], [89, 8, 174], [97, 0, 0], [101, 16, 246], [103, 0, -130], [107, 0, -150], [109, 16, 262], [113, 0, 68], [127, 0, -90], [131, 18, 298], [137, 0, -108], [139, -14, 282], [149, 28, 414], [151, -8, -2], [157, 0, 60], [163, 0, -142], [167, 0, 62], [173, 0, -40], [179, -16, 342], [181, 8, 198], [191, 30, 562], [193, 0, 8], [197, 0, 200], [199, 2, 394]

のようです。$p \neq \pm 1 \bmod 5$ のときは、$a_p = 0$ であること、つまり、標準係数多項式が

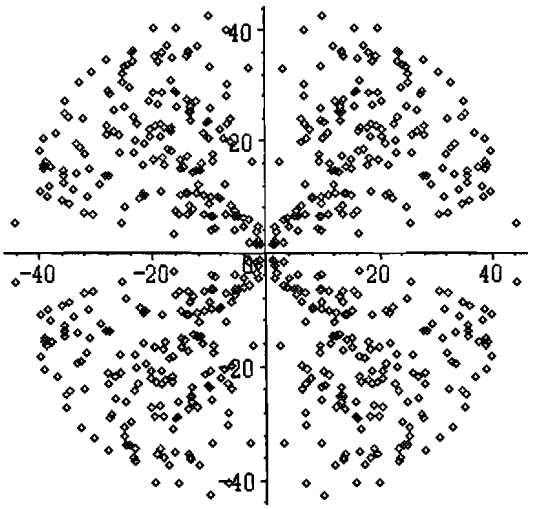
$$t_3(x)+b_p/p = x^3-3x+k,\ k = b_p/p$$

であることが解ります。角分布の様子は

$$y^2 = x^5-5x^3+5x+1$$

$$p \neq \pm 1 \bmod 5,\ p = 3 \sim 2099$$

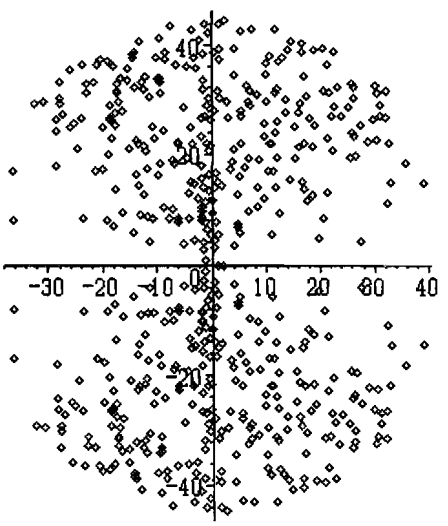
$$\sin^2(2\pi x)$$



$$y^2 = x^5-5x^3+5x+1$$

$$p = \pm 1 \bmod 5,\ p = 3 \sim 2099$$

$$\sin^2(\pi x)$$



上記のような例から、Tschebysheff多項式の次数が q = 3, 5, 7, 11, (23)などのとき

$$p \neq \pm 1 \bmod q,\ p = \pm 1 \bmod q$$

によって、種数 g = (q-1)/2 に対し、g-1:1 の比の分解

$$\sin^2(gx),\ \sin^2(x)$$

が可能かも知れないとの問題意識があります。例えば、類数 1 の虚 2 次体

$$q = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

との関連も興味があります。q = 19 の場合は

$$y^2 = x^{19}-19x^{17}+152x^{15}-665x^{13}+1729x^{11}-2717x^9+2508x^7-1254x^5+285x^3-19x+9$$

$$[3,0,0,0,0,0,0,0,0,0],\ [5,0,0,0,0,0,0,0,0,262],\ [7,0,0,-3,0,0,3,0,0,-1]$$

のように p = 7 で $p \neq \pm 1 \bmod 19$ にも関わらず、標準係数多項式が

$$x^9-9x^7+27x^5-30x^3+9x+k$$

の形ではありません。q としては p = 2q+1 型の素数列と関係しているのかななどと興味がそそられる。1, 3, 7 や 2, 5, 11, 23, 47 など、兎も角、実例に当たって見たいのです。

2. 楕円曲線と標準対合分解

先ず、Legendre の多項式

$$P^*_n(x) = \sum r \in n\ (n+r)!/((n-r)!r!^2)\cdot(-x)^r$$

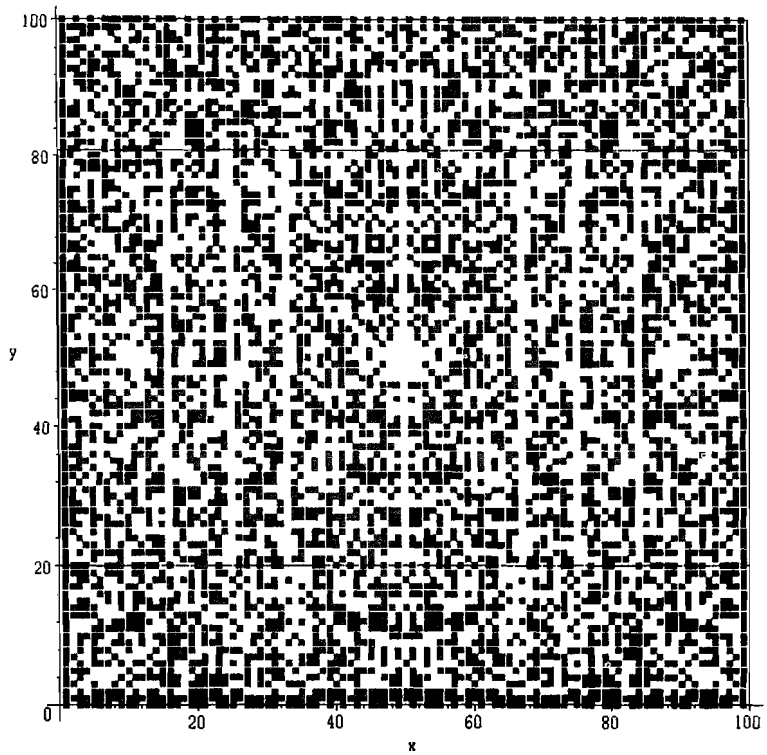
$$= \sum r \in n\ (-n)_r(n+1)_r/r!^2\cdot(-x)^r = F(-n, n+1, 1, x)$$

の話から始めましょう。

以下の図は、Legendre 多項式 F(-n, n+1, 1, x)の有限体 F_{101} で計算したものの表です。縦軸が次数 n で m = F(-n, n+1, 1, x)となっていれば、(n, m)の点は黒点で示してあります。空白は値が現れないことを意味しています。

Example 1. p = 101

$$[n, P_n(x)],\ n, x \in p,\ p = 101$$



横線は Hasse の限界、つまり、

$$2\sqrt{p} = 2\sqrt{101} = 20.09975124$$

です。p = 101 に対し

16 = -5/6, 25 = -1/4, 33 = -2/3, 50 = -1/2, 67 = -1/3, 75 = -3/4, 84 = -1/6

の場所に縦線の空白の線が見てとれます。

有限体 $F_p = \{0,1,\cdots,p-1\} = p$ での Fuchs 多項式です。

$$F(1/6,5/6,1,x),\ F(1/4,3/4,1,x),\ F(1/3,2/3,1,x),\ F(1/2,1/2,1,x)$$

の値は

$$2|F(1/4,3/4,1,x),\ 3|F(1/3,2/3,1,x),\ 4|F(1/2,1/2,1,x)$$

のような約数をもち Hessian range $[-2\sqrt{p}, 2\sqrt{p}]$ の範囲にあります。これらは、それぞれ楕円曲線の族

$F(1/6,5/6,1,x)$ $y^2 = x^3+ax^2+b$ (Whock-family 仮称)

$F(1/4,3/4,1,x)$ $y^2 = x(x^2+ax+b)$ Euler-family

$F(1/3,2/3,1,x)$ $y^3+x^3+axy+b = 0$ Hesse-family

$F(1/2,1/2,1,x)$ $y^2 = x(x-1)(x-a)$ Legendre-Family

に対応しています。ワイエルシュトラス族(Weierstrass-family)

$$y^2 = x^3+ax+b$$

に対しては

$$x^{(p-1)/4}\, F(1/12,5/12,1,1-x) \quad \text{if } p = 1 \bmod 4$$

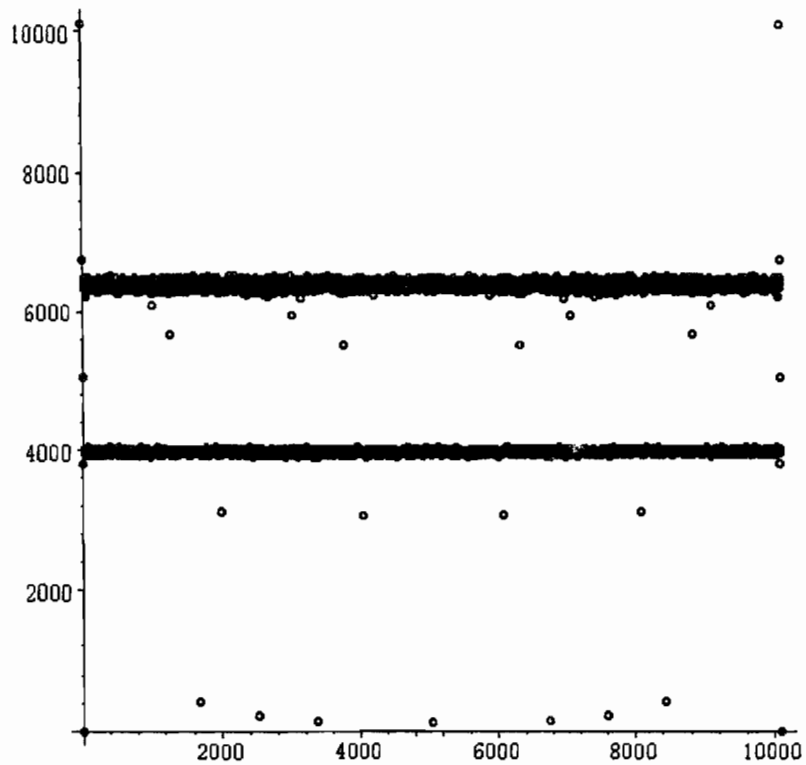
$$x^{(p+1)/4}\, F(7/12,11/12,1,1-x) \quad \text{if } p = -1 \bmod 4$$

が対応しているのです。ですから、$p \geq 17$ に対しては、絶対値最小剰余(least absolute value residue, lavr)として値が一意的に定まります。

2.1 Example p = 10111

次の図は、少し大きい素数の場合の F(-n, n+1, 1, x)の値の個数についての図です。

$[n, \#\{P_n(x) : x \in p\}]$, p = 10111



勿論、最小の group のものは

$$F(1/6,5/6,1,x),\ F(1/4,3/4,1,x),\ F(1/3,2/3,1,x),\ F(1/2,1/2,1,x)$$

で、次の group は

$$F(1/5,4/5,1,x),\ F(2/5,3/5,1,x)$$

です。偶関数と奇関数の平均の間の領域には

$$F(1/8,7/8,1,x),\ F(3/8,5/8,1,x)$$
$$F(1/10,9/10,1,x),\ F(3/10,7/10,1,x)$$

などがあります。ほとんどの場合が random であるとすれば、何らかの規則性があることは明確なのですが、(私は)現段階では少なくとも代数的に簡潔な特性は知りません。非常に興味ある研究対象であることは明確です。

2.2 係数変換多項式(coefficient transform polynomial, ctp)

有限体

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

で考える。多項式

$$f(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n$$

係数変換多項式を、法 p での原始根(primitive root) r に対し、

$$n' = n+1 = \{0,1,..,n\}$$

として、(別にこんな記法は必要ありませんが)

$$f[r](x) = \sum k\in n' f(r^k)x^k$$
$$= (1-x^{p-1})(a_0/(1-x)+a_1/(1-rx)+a_2/(1-r^2x)+\cdots+a_n/(1-r^nx))$$

と定義する。任意の n に関して F_p では

$$(1-x^{p-1})/(1-r^nx)$$

は p-2 次の多項式であるから、結果は p-2 次の多項式である。

このとき

$$(cf)[r](x) = c(f[r](x))$$
$$(f+g)[r](x) = f[r](x)+g[r](x)$$
$$f[r](sx) = f[rs](x)$$

などの性質がある。つまり、左からは加法的(left-additive)右からは乗法的(right-productive)である。

原始根 r に対する係数変換作用素(coefficient transform operator, cto)[r]は、有限体上の 1 変数の p-2 次以下の多項式の成す p-1 次 vector 空間

$$W = F_p^{p-1}[x] = [1, x,\cdots, x^{p-2}]$$

の Vandermonde 行列

$$V = (r^{(i-1)(j-1)})$$

による線形変換

$$[r]: F_p^{p-1}[x] \rightarrow F_p^{p-1}[x]$$

です。従って、ファンデルモンド変換(Vandermonde transformation)という名称がふさわしいと思いますが。まあ、(私は)後で気付いたので、差し当たり、両方の名称を使います。

Vandermonde 行列 $V = (r^{(i-1)(j-1)})$ は正則行列ですから、係数逆変換が存在します。また、この変換は、有限フーリエ変換(finite Fourier transform, fFt)でもあります。$F^4 = id$ という($x^4 = 1$, $x = i = \sqrt{-1}$ に対応)Fourier 変換の基本性質が成立するのです。

これは、簡単な性質ですが、後半の多項式に気付くまでに時間を要したのです。

いもしらで　ひたりなれにし　こころねを
おもいそめきと　おもほへるかな

これの説明であるが…

いしきせず　つかいさえした　ていぎしき
きづかざりきと　きづくはかなさ

といったところでしょう。

説明の方は、ほわ〜っと感(= who how what feeling)が足りませんね。

例. $p = 71$, $f(x) = F(1/6,5/6,1,x)$

この場合、次数は$[71/6] = 11$ である。

$$F(1/6,5/6,1,x) = 1-61x+30x^2-65x^3+26x^4-54x^5+11x^6-26x^7+22x^8-61x^9+10x^{10}-47x^{11}$$

であり、$F_p = F_{71}$ では高々 2 次の因子に分解されている。(Deuling property)

$$24(x^2+70x+63)(x+18)(x+43)(x+37)(x+38)(x+52)(35+x)(x+32)(x+27)(x+33)$$

勿論、Hasse の不等式は

$$|F(1/6,5/6,1,x)| < 2\sqrt{71} = 16.85229955$$

です。$p = 71$ の原始根(primitive root)の一つは $r = 7$ で、このときの Vandermonde 変換[7]を考えてみましょう。定義から、

$$F(1/6,5/6,1,x)[7](x) =$$
$$(1-x^{70})(1/(1-x)-61/(1-7x)+30/(1-7^2x)-65/(1-7^3x)+26/(1-7^4x)-54/(1-7^5x)$$
$$+11/(1-7^6x)-26/(1-7^7x)+22/(1-7^8x)-61/(1-7^9x)+10/(1-7^{10}x)-47/(1-7^{11}x))$$

です。具体的に計算すると、

$$f(x)[7](x) = \sum n<p-1\ f(7^n)x^n =$$
$$-3x^{69}-12x^{68}-9x^{67}+5x^{66}+2x^{63}-6x^{62}+16x^{61}+6x^{60}+11x^{59}-4x^{58}-14x^{56}+3x^{54}+8x^{53}-8x^{52}-2x^{51}+7x^{50}$$
$$-11x^{49}+12x^{48}-12x^{47}+x^{46}-5x^{45}-7x^{44}-3x^{42}-8x^{41}+2x^{40}-9x^{39}-5x^{38}+6x^{37}-13x^{36}-12x^{35}+8x^{34}-6x^{33}$$

$$-2x^{32}+3x^{31}-x^{30}-10x^{29}+12x^{28}+3x^{27}+8x^{26}+8x^{25}-2x^{24}+5x^{21}+10x^{20}+2x^{19}+13x^{18}-8x^{17}-12x^{15}$$
$$+4x^{14}-16x^{12}-8x^{11}+15x^{10}+14x^{9}-15x^{8}-14x^{7}+12x^{6}-3x^{5}+14x^{4}+9x^{3}+12x^{2}+9x-1$$

です。x^{13}, x^{16}, x^{22}, x^{23}, x^{43}, x^{55}, x^{57}, x^{64}, x^{65} などの項は係数が 0 です。Hasse の不等式から係数はすべて絶対値 16 以下であることが確認できます。

係数を k として、$x = k/(2\sqrt{p})$ の分布は $\sqrt{1-x^2}$ に比例するという、係数の $\sin^2$-予想は証明されていると思いますが、私は、詳しいことは知りません。(証明方法、歴史、未解決の部分など良い解説を与えることは非常に意義ある重要なことだと思います)

楕円係数変換多項式については、有理数体 Q 上既約(予想、問題、定理?)で、F_p 上では、一次以外の因子の次数の和は、例えば、F(1/6,5/6,1,x)[7](x) の項の数、この場合は[p/6]、を越えないことが Vandermonde 変換の性質から解ります。

$$f(x)[7](x)=$$
$$68(x+30)(x+14)(x+17)(x+8)(x+51)(x+48)(x+34)(x+66)(x+60)(x+47)$$
$$(x+49)(x+55)(x+36)(x+37)(x+54)(x+33)(x+67)(x+58)(x+56)(x+43)$$
$$(x+4)(x+13)(x+25)(x+19)(x+38)(x+68)(x+18)(x+64)(x+9)(x+44)$$
$$(x+27)(x+7)(x+1)(x+22)(x+24)(x+2)(x+26)(x+20)(x+57)(x+59)$$
$$(x+50)(x+65)(x+69)(x+29)(x+15)(x+12)(x+31)(x+45)(x+39)(x+62)$$
$$(x+46)(x+52)(x+53)(x+23)(x+61)(x+40)(x+63)$$
$$(x+28)^2(x^2+2x+44)(x^8+53x^7+41x^6+34x^5+29x^3+13x^2+36x+21)$$

です。重複因子も irregular 因子と数えれば

$$(x+28)(x^2+2x+44)(x^8+53x^7+41x^6+34x^5+29x^3+13x^2+36x+21)$$

が問題の因子で、次数の和は 1+2+8 = 11 です。しかし、これは

$$(1/(1-x)-61/(1-7x)+30/(1-7^2x)-65/(1-7^3x)+26/(1-7^4x)-54/(1-7^5x)$$
$$+11/(1-7^6x)-26/(1-7^7x)+22/(1-7^8x)-61/(1-7^9x)+10/(1-7^{10}x)-47/(1-7^{11}x))$$
$$=$$
$$68(x+28)(x^2+2x+44)(x^8+53x^7+41x^6+34x^5+29x^3+13x^2+36x+21)/$$
$$(x+70)(x+6)(x+32)(x+42)(x+16)(x+10)$$
$$(x+5)(x+3)(x+35)(x+11)(x+21)(x+41)$$

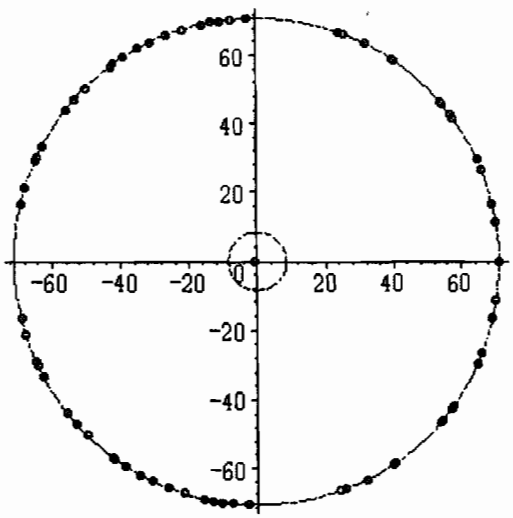
の分子から来ているので当然です。

係数変換多項式の一番の特徴は 1 の p-1 乗根 $x = e^{i(2\pi k/(p-1))}$ を代入した値の絶対値が

$$(x-1)(x+1)(x^2+1)(x^2+x+1)=0$$

の根、つまり、Gauss, Eisenstein の整数の場合を除いて、絶対値 p になることです。勿論、上記の根での値は 1, $\sqrt{p}$, p の何れかです。値が p のときは正常(normal)、または非退化(non-degenerate)と呼び、1, $\sqrt{p}$ のとき退化(degenerate)とよぶ。

$$F(1/6,5/6,1,x)[7](e^{i(2\pi k/(p-1))}),\ k=0\sim p-2$$



この場合は Gauss, Eisenstein の退化はない。また、±1 に対しては

$$F(1/6,5/6,1,x)[7](1)=-1,\ F(1/6,5/6,1,x)[7](-1)=p$$

である。従って p = 71, F(1/6,5/6,1,x)[7](x)の場合は 1 のみ退化する。

2.3 終結積(resultant product)

二つの多項式の終結積行列(resultant product matrix, rpm)、剰余行列(residual matrix)は、f(x), g(x)に対し、d = degree(g(x))として

$$f(x)[x]g(x)=[\mathrm{coeff}(\mathrm{rem}(x^{i-1}f(x),g(x),x),x,d-j)]$$

つまり、(i,j)元が $x^{i-1}f(x)$ の g(x)での剰余の x^{d-j} の係数とした、g(x)の次数の正方行列のことです。

終結行列は

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$$

$$g(x)=b_0x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m$$

に対し、係数を順次並べて

$$\begin{pmatrix} 0 & 0 & \cdots & a_0 & a_1 & \cdots & a_{n-1} & a_n \end{pmatrix}$$

$$\left(\begin{array}{cccccccc} 0 & \cdots & a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 \\ & & \cdots & & & \cdots & & \\ a_0 & a_1 & \cdots & a_{n-1} & a_n & \cdots & 0 & 0 \\ \hline 0 & 0 & \cdots & b_0 & b_1 & \cdots & b_{m-1} & b_m \\ 0 & \cdots & b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 \\ & & \cdots & & & \cdots & & \\ b_0 & b_1 & \cdots & b_{m-1} & b_m & \cdots & 0 & 0 \end{array}\right)$$

の形の行列とする。この行列を

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

の形に表示する。この場合、B, C は g(x), f(x) の次数 m, n の正方行列で C は正則行列です。E を m 次単位行列として (m, m+n) 型の行列

$$(E\ -AC^{-1})$$

を左から乗じて

$$(E\ -AC^{-1})\begin{pmatrix} A & B \\ C & D \end{pmatrix} = (A-AC^{-1}C \quad B-AC^{-1}D) = (O \quad B-AC^{-1}D)$$

の形の行列に導く。

$$f(x)\,[x]\,g(x) = B-AC^{-1}D$$

が定義です。

と、表現は少し硬いですが、詰まるところは、例えば、

$$g(x) = x^m+b_1x^{m-1}+\cdots+b_{m-1}x+b_m$$

の場合ですと、剰余の方では g(x) = 0、つまり、等式

$$x^m = -b_1x^{m-1}-\cdots-b_{m-1}x-b_m$$

を f(x) の g(x) による剰余

$$f(x) = q(x)\,g(x)+r(x)$$

$$r(x) = c_{11}x^{m-1}+c_{12}x^{m-2}+\cdots+c_{1m-1}x+c_{1m}$$

の係数を降冪の順 (descending order) においた行 (row)

$$(c_{11}\ c_{12}\cdots c_{1m-1}\ c_{1m})$$

を第 1 行とし、それに x を乗じて、つまり、1 つづつ前にずらし、溢れた

$$c_{11}x^m = c_{11}(-b_1x^{m-1}-\cdots-b_{m-1}x-b_m)$$

の係数を加える。すなわち

$$(c_{12}-c_{11}b_1 \quad \cdots \quad c_{1m}-c_{11}b_{m-1}\ 0-c_{11}b_m)$$

を次の行とする。これを m-1 回繰り返した m 次正方行列が f(x)[x]g(x)の定義です。

2.4 標準対合分解(normal involution resolution)

さて、p ≥ 17 の場合を考えましょう。楕円曲線の j-不変量を変数 x とした関数、例えば

$$F(1/6,5/6,1,x),\ F(1/4,3/4,1,x),\ F(1/3,2/3,1,x),\ F(1/2,1/2,1,x)$$

$$x^{(p-1)/4}F(1/12,5/12,1,1-x)\quad \text{if } p = 1 \bmod 4$$

$$x^{(p+1)/4}F(7/12,11/12,1,1-x)\quad \text{if } p = -1 \bmod 4$$

の一つを a(x)としましょう。a(x)の絶対値最小剰余(least absolute value residue, lavr)を考えると p ≥ 17 の場合は Hasse の不等式によって値が定まります。

$$|a(x)| \le 2\sqrt{p}$$

ですから、そこで、a(x)、例えば、a(x)= F(1/6,5/6,1,x)を楕円係数多項式(elliptic coefficient polynomial, ecp)と仮に呼ぶことにします。楕円係数多項式の係数変換多項式

$$a(x)[r](x) = \sum n \in p\text{-}1\ a(r^n)x^n$$

のすべての係数の絶対値は Hasse の限界内、つまり、$2\sqrt{p}$ 以下です。

ここでの主張は、円分因子、つまり、有理整数 Z の範囲での因数(factor)

$$q(x) \mid (x^{p-1}-1)$$

とその終結積行列、つまり、次のような略記法[r|x]を導入し

$$B = a(x)[r|x]q(x) = a(x)[r](x)[x]q(x)$$

を考える。特に、q(x)が既約多項式である場合は

$$A = 1/s \cdot B = 1/s \cdot a(x)[r|x]q(x)$$

が対合(involution)、つまり、

$$A^2 = E$$

となる s は 1, $\sqrt{p}$, p の何れかである。この s を対合因子(involution factor)と呼ぶ。対合因子が 1, $\sqrt{p}$ とき退化因子(degenerate factor)といい、そうでないとき正常因子(normal factor)という。退化因子は

$$q(x) = x+1,\ x-1,\ x^2+1,\ x^2-x+1$$

の場合に限られる。特に

$$x^2+1,\ x^2-x+1$$

の場合の退化は Gauss, Eisenstein 整数の退化がおこる場合である。q(x)の任意の既約因子が正常因子であるとき q(x)は正常因子という。

有限楕円対合分解(定理？)
(elliptic involution property of finite field, eipf)
q(x)を x^{p-1}-1 の正常因子とするとき
楕円係数変換多項式 a(x)[r](x)と q(x)の終結積行列
A = a(x)[r|x]q(x)= 1/p·a(x)[r](x)[x]q(x)
は対合(involution)である。

この性質の色々の観点からの証明(あるいは反例, proof or counter-example)を期待している。

例 p = 11, $x^{(p+1)/4}$F(7/12,11/12,1,1-x)

この場合は、例の、花月、の少年の、

月はとも、はなに四かあり、春は花、夏は瓜、秋は果、冬は火

のように、簡単だけれどすべての要素を含んでいるのです。

F(7/12,11/12,1,1-x)は楕円曲線のワイヤストラス標準形(Weierstrass normal form)に対応する Fuchs 多項式で次数は[p/12]= 0 です。p = 11 の場合は定数 1 です。また、$x^{(p+1)/4} = x^3$ です。11 での原始根の一つが 2 であることは

$$2^5 = 32 = -1 \bmod 11$$

から解ります。従って、係数変換多項式、つまり、Vandermonde 変換多項式は、例えば、最小剰余の表示で

$$x^3[2](x) = (1-x^{10})/(1-8x) = 1-3x-2x^2-5x^3+4x^4-x^5+3x^6+2x^7+5x^8-4x^9$$

です。Hasse の限界は $2\sqrt{p} = 6.633249580$ ですから、$-5 = 6 \bmod p$ の可能性があります。可能な多項式は

$$1-3x-2x^2-5x^3+4x^4-x^5+3x^6+2x^7+5x^8-4x^9 = -(x-1)(x^4+x^3+x^2+x+1)(4x^4-5x^3-2x^2-3x+1)$$

$$1-3x-2x^2+6x^3+4x^4-x^5+3x^6+2x^7-6x^8-4x^9 =$$

$$-(x-1)(2x-1)(x+1)(2x^2+2x-1)(x^4+x^3+x^2+x+1)$$

$$1-3x-2x^2+6x^3+4x^4-x^5+3x^6+2x^7+5x^8-4x^9$$

$$1-3x-2x^2-5x^3+4x^4-x^5+3x^6+2x^7-6x^8-4x^9$$

の 4 種で、有理数体で既約なものは最後の二つです。有限体 F_{11} では完全分解する。

$$1/11\cdot x^3[2|x]x^{10}-1$$

$$1/11\cdot(1-3x-2x^2+6x^3+4x^4-x^5+3x^6+2x^7+5x^8-4x^9[x]x^{10}-1)$$

$$= 1/11\cdot$$

$$\begin{pmatrix}
-4 & 5 & 2 & 3 & -1 & 4 & 6 & -2 & -3 & 1 \\
5 & 2 & 3 & -1 & 4 & 6 & -2 & -3 & 1 & -4 \\
2 & 3 & -1 & 4 & 6 & -2 & -3 & 1 & -4 & 5 \\
3 & -1 & 4 & 6 & -2 & -3 & 1 & -4 & 5 & 2 \\
-1 & 4 & 6 & -2 & -3 & 1 & -4 & 5 & 2 & 3 \\
4 & 6 & -2 & -3 & 1 & -4 & 5 & 2 & 3 & -1 \\
6 & -2 & -3 & 1 & -4 & 5 & 2 & 3 & -1 & 4 \\
-2 & -3 & 1 & -4 & 5 & 2 & 3 & -1 & 4 & 6 \\
-3 & 1 & -4 & 5 & 2 & 3 & -1 & 4 & 6 & -2 \\
1 & -4 & 5 & 2 & 3 & -1 & 4 & 6 & -2 & -3
\end{pmatrix}$$

$$1/11\cdot -x^3[2|x]x^5-1 = 1/11\cdot$$

$$\begin{pmatrix}
8 & -1 & -4 & 6 & 2 \\
-1 & -4 & 6 & 2 & 8 \\
-4 & 6 & 2 & 8 & -1 \\
6 & 2 & 8 & -1 & -4 \\
2 & 8 & -1 & -4 & 6
\end{pmatrix}$$

などは対称巡回対合(symmetric cyclic involution, sci)である。これなど、2が11での原始根の一つであることをよく示しています。

例 p = 13, $x^{(p-1)/4}F(1/12,5/12,1,1-x)$

Fuchs多項式で次数は[p/12]です。p = 13の場合は1次式です。また、$x^{(p-1)/4} = x^3$ です。13での原始根の一つが2であることは

$$2^6 = 64 = -1 \bmod 13$$

から解ります。1/12 = -1, 5/12 = -5 は 12 = -1 mod p から

$$F(1/12,5/12,1,1-x) = 1+(-1)(-5)/1^2\cdot(1-x) = 1+5(1-x) = 6-5x$$

です。

$$x^{(p-1)/4}F(1/12,5/12,1,1-x) = 6x^3-5x^4$$

から、

$$6x^3-5x^4[2](x) = (1-x^{12})(6/(1-8x)-5/(1-16x))$$

$$= 1-6x+x^2-x^3+4x^4+3x^5+2x^6+2x^7+4x^9+5x^{10}-2x^{11}$$

$$= -(x+1)(x^2-x+1)(2x^4-5x^3-2x^2-7x-1)(x^4-x^2+1)$$

と絶対値最小剰余(lavr)の形に記しました。この場合は有理数体上可約です。Hasse の限界は

$$2\sqrt{13} = 7.211102550$$

ですから、6+7 = p の可能性があります。つまり、

$$1+7x+x^2-x^3+4x^4+3x^5+2x^6+2x^7+4x^9+5x^{10}-2x^{11}$$

も可能な表現です。x^8 の係数は 0 です。こちらは有理数体上既約ですが、有限体 F_{13} では(一次因子に)完全分解します。

F_{13} の特性多項式 $x^p-x = x(x^{p-1}-1)$ の円分既約分解(cyclotomic factorization)は

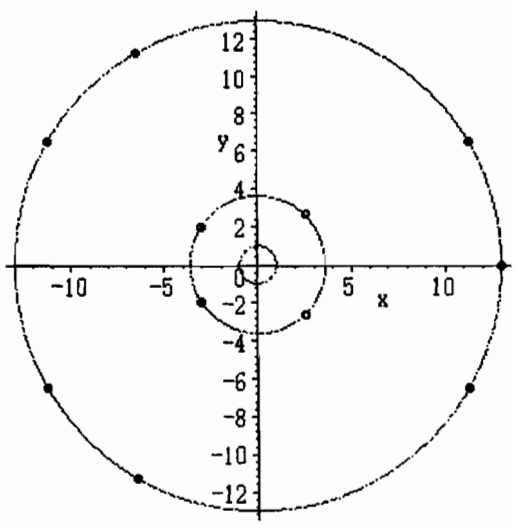
$$x^{12}-1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^2+1)(x^4-x^2+1)$$

と虚数単位 $i = \sqrt{-1}$ (x^2+1, Gauss integer)や 1 の原始立方根 $\omega = (-1\pm\sqrt{-3})/2$ (x^2+x+1, Eisenstein integer)などの因子をもっています。1 年 12 月余りと奇妙な符合(意味の巡り合わせ)です。さて、これらの因子の

$$6x^3-5x^4[2](x) = 1+7x+x^2-x^3+4x^4+3x^5+2x^6+2x^7+4x^9+5x^{10}-2x^{11}$$

に円分多項式の根、つまり、1 の p-1 乗根を代入したものの絶対値は 1, $\sqrt{p}$, p に限る。つまり、対合因子(involution factor)である。

$$6x^3-5x^4[2](e^{2\pi ik/12})$$



因子が 1 のものは存在せず、$\sqrt{p}$ のものは $\pm i, \omega, \bar{\omega}$ に限る。つまり、$(x^2+x+1)(x^2+1)$ である。

対合因子は、終結積(= 消去積, resultant, elimination product)により、

$$(py-(6x^3-5x^4[2](x)))\textcircled{x}[x-1, x+1, x^2+1, x^2+x+1, x^2-x+1, x^4-x^2+1]$$

$$= [y-1, y-1, 13y^2+6y+1, 13y^2-5y+1, y^2+y+1, y^4-y^2+1]$$

が得られる。このようにして正常因子に対しては再び $x^{p-1}-1 = 0$ の根が再生されている。退化因子に対しては

$$(y-(6x^3-5x^4[2](x)))\circledast[x^2+1, x^2+x+1] = [y^2+6y+13, y^2-5y+13]$$

である。一応、円分対合分解(cyclotomic involution resolution)の成分を記す。

$$1/p\cdot 6x^3-5x^4[2|x]x-1 = (1)$$

$$1/p\cdot 6x^3-5x^4[2|x]x+1 = (1)$$

$$1/\sqrt{p}\cdot 6x^3-5x^4[2|x][x^2+1, x^2+x+1] = 1/\sqrt{p}\cdot$$

$$\begin{pmatrix} 2 & -3 \\ -3 & -2 \end{pmatrix} \quad \begin{pmatrix} 3 & 4 \\ 1 & -3 \end{pmatrix}$$

$$1/p\cdot 6x^3-5x^4[2|x]x^2-x+1 =$$

$$\begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$$

$$1/p\cdot 6x^3-5x^4[2|x]x^4-x^2+1 =$$

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$$

対称巡回対合(sci)に関しては

$$1/p\cdot -6x^3-5x^4[2|x]x^3-1 =$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

であり、13 が分解するのは Gauss, Eisenstein 整数のみである。因みに 13 での原始根は

$$[2, 2^5, 2^7, 2^{11}] \bmod 13 = [2, 6, 11, 7]$$

です。業平の視点では、七段は

いとゞしく　過ぎゆくかたの　恋しきに　うら山しくも　かへる浪かな

十一段は

忘るなよ　ほどは雲ゐに　なりぬとも　空ゆく月の　めぐり逢ふまで

とあります。7, 11 は 12 での既約剰余(irreducible residue)、13 での原始根(primitive root)でもあります。12 と 13 は古今集の在原元方の「こぞことし」

にも聞くところです。兎も角、時(年月≒ 12)には未知の道があると思います。

例. p = 71, r = 7

$$F(1/6,5/6,1,x)[7](x) = \sum n<p-1\ f(7^n)\,x^n =$$

$$-3x^{69}-12x^{68}-9x^{67}+5x^{66}+2x^{63}-6x^{62}+16x^{61}+6x^{60}+11x^{59}-4x^{58}-14x^{56}+3x^{54}+8x^{53}-8x^{52}-2x^{51}+7x^{50}$$

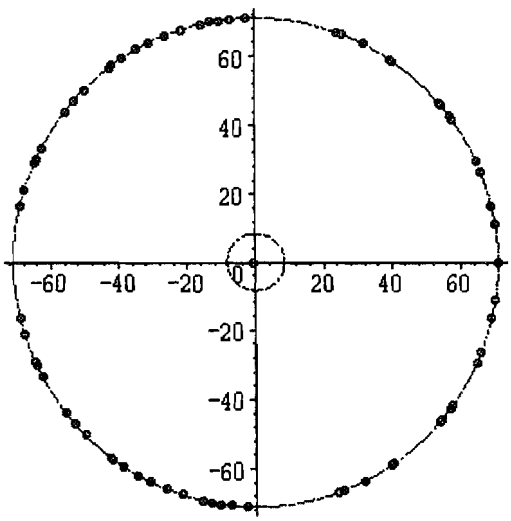
$$-11x^{49}+12x^{48}-12x^{47}+x^{46}-5x^{45}-7x^{44}-3x^{42}-8x^{41}+2x^{40}-9x^{39}-5x^{38}+6x^{37}-13x^{36}-12x^{35}+8x^{34}-6x^{33}$$

$$-2x^{32}+3x^{31}-x^{30}-10x^{29}+12x^{28}+3x^{27}+8x^{26}+8x^{25}-2x^{24}+5x^{21}+10x^{20}+2x^{19}+13x^{18}-8x^{17}-12x^{15}$$

$$+4x^{14}-16x^{12}-8x^{11}+15x^{10}+14x^9-15x^8-14x^7+12x^6-3x^5+14x^4+9x^3+12x^2+9x-1$$

の続き。

$$F(1/6,5/6,1,x)[7](e^{2\pi i k/70})$$



円分多項式 $x^{p-1}-1$ の有理数体上の分解は

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

$$(x-1)(x+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)$$

$$(x^6+x^5+x^4+x^3+x^2+x+1)(x^6-x^5+x^4-x^3+x^2-x+1)$$

$$(x^{24}-x^{23}+x^{19}-x^{18}+x^{17}-x^{16}+x^{14}-x^{13}+x^{12}-x^{11}+x^{10}-x^8+x^7-x^6+x^5-x+1)$$

$$(x^{24}+x^{23}-x^{19}-x^{18}-x^{17}-x^{16}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}-x^8-x^7-x^6-x^5+x+1)$$

である。今の場合は x-1 のみが退化因子である。

$$F(1/6,5/6,1,x)[7|x]x-1 = (-1)$$

$$1/p\cdot F(1/6,5/6,1,x)[7|x]x+1 = (1)$$

この例のように x-1 のみ退化し、退化係数は 1 である。また、以下の行列はすべて対合である：

$$A = 1/p \cdot F(1/6,5/6,1,x)\,[7|x]\,x^4+x^3+x^2+x+1$$

$$=$$

$$\begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$B = 1/p \cdot F(1/6,5/6,1,x)\,[7|x]\,x^4-x^3+x^2-x+1$$

$$= 1/71 \cdot$$

$$\begin{pmatrix} 38 & -15 & 42 & 36 \\ 23 & 4 & 74 & -38 \\ 27 & 51 & -15 & -23 \\ 78 & -42 & 4 & -27 \end{pmatrix}$$

$$C = 1/p \cdot F(1/6,5/6,1,x)\,[7|x]\,x^6+x^5+x^4+x^3+x^2+x+1$$

$$= 1/71 \cdot$$

$$\begin{pmatrix} -46 & -6 & -13 & -10 & -62 & -60 \\ 40 & 33 & 36 & -16 & -14 & 46 \\ -7 & -4 & -56 & -54 & 6 & -40 \\ 3 & -49 & -47 & 13 & -33 & 7 \\ -52 & -50 & 10 & -36 & 4 & -3 \\ 2 & 62 & 16 & 56 & 49 & 52 \end{pmatrix}$$

$$D = 1/p \cdot F(1/6,5/6,1,x)\,[7|x]\,x^6-x^5+x^4-x^3+x^2-x+1$$

$$= 1/71 \cdot$$

$$\begin{pmatrix} 56 & -2 & 49 & -62 & 52 & -16 \\ 54 & -7 & -6 & -4 & 40 & -56 \\ 47 & -60 & 50 & -14 & -2 & -54 \\ -13 & 3 & 33 & -49 & -7 & -47 \\ -10 & 46 & -62 & 6 & -60 & 13 \\ 36 & -52 & -4 & -50 & 3 & 10 \end{pmatrix}$$

例えば、上記の 4 個の行列は対合(involution)である。大きさの関係で 24 次正方行列の第 1 行のみしか記さないがこれらの行列も対合である。

$$1/p \cdot F(1/6,5/6,1,x)\,[7|x]\,x^{24}-x^{23}+x^{19}-x^{18}+x^{17}-x^{16}+x^{14}-x^{13}+x^{12}-x^{11}+x^{10}-x^8+x^7-x^6+x^5-x+1$$

$$= 1/71 \cdot$$

$$[57, 18, -65, -12, -20, 67, -17, 17, -12, -64, 50,$$
$$-45, -3, -16, 25, 38, -66, 0, -43, 8, 38, 44, 7, -87]$$
$$1/p\cdot F(1/6,5/6,1,x)\,[7|x]\,x^{24}+x^{23}-x^{19}-x^{18}-x^{17}-x^{16}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}-x^{8}-x^{7}-x^{6}-x^{5}+x+1$$
$$= 1/71\cdot$$
$$[49, 10, 27, 28, -24, -39, -33, -41, -38, 22, 16,$$
$$39, 33, 62, 49, -42, -38, -6, -57, -4, 18, -2, 47, 47]$$

これらの分解を円分対合分解(cyclic involution resolution, cir)という。

$$x^5+1,\ x^7+1,\ x^{35}+1$$

は $x^{70}-1$ の正常(= 非退化)因子である。

$$1/p\cdot F(1/6,5/6,1,x)\,[7|x]\,x^5+1$$
$$=$$
$$\begin{pmatrix} 26 & 12 & 11 & 16 & 62 \\ 12 & 11 & 16 & 62 & -26 \\ 11 & 16 & 62 & -26 & -12 \\ 16 & 62 & -26 & -12 & -11 \\ 62 & -26 & -12 & -11 & -16 \end{pmatrix}$$

この行列も勿論対合である。しかし、巡回成分の最後の元を挿入するときに符号が変わっている。従って F(1/6,5/6,1,x) の x に-x を代入し、x^5+1 に-x を代入して x^5-1 を考慮して

$$1/p\cdot F(1/6,5/6,1,-x)\,[7|x]\,x^5-1$$
$$=$$
$$\begin{pmatrix} 26 & -12 & 11 & -16 & 62 \\ -12 & 11 & -16 & 62 & 26 \\ 11 & -16 & 62 & 26 & -12 \\ -16 & 62 & 26 & -12 & 11 \\ 62 & 26 & -12 & 11 & -16 \end{pmatrix}$$

$$1/p\cdot F(1/6,5/6,1,-x)\,[7|x]\,x^7-1$$
$$=$$
$$\begin{pmatrix} 44 & -12 & 42 & -5 & -18 & -8 & 28 \\ -12 & 42 & -5 & -18 & -8 & 28 & 44 \\ 42 & -5 & -18 & -8 & 28 & 44 & -12 \\ -5 & -18 & -8 & 28 & 44 & -12 & 42 \end{pmatrix}$$

$$\begin{pmatrix} -18 & -8 & 28 & 44 & -12 & 42 & -5 \\ -8 & 28 & 44 & -12 & 42 & -5 & -18 \\ 28 & 44 & -12 & 42 & -5 & -18 & -8 \end{pmatrix}$$

$$1/p \cdot F(1/6,5/6,1,-x)\,[7|x]\,x^{35}-1$$

$$=$$

[11, -6, 7, 2, -1, 10, 10, -9, -8, -2, -13, -4, 0, -19, 10, 1, 5, 0,
2, 19, 15, 12, -4, 9, 20, -21, -15, 11, 20, 5, 23, -14, 6, -22, 11]

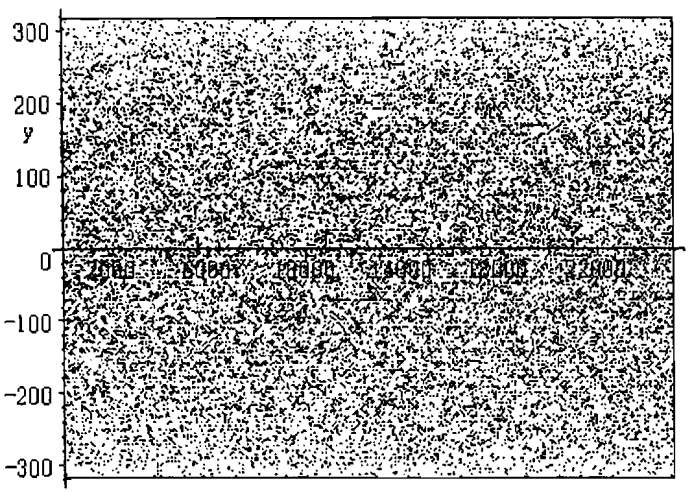
である。これらの場合は、対称巡回対合(symmetric cyclic involution, sci)である。

例えば、(地球や身体の音波あるいは振動での計測など想像しながら…) p = 25127 では、p-1 = 25126 次の sci.が定義されます。仮に 4000m/sec 位の音速で 10Hz 程度の音波(振動)を用いると分解精度は 400m 程度です。1 周期に 2513 秒≒ 42 分、つまり、小 1 時間が必要です。受信者はもとの波形を知っているのですから内積をとるだけで時間のずれ、つまり、経路の長さが分かります。あるいは、音波写真(sonic photo)、超音波顕微鏡(supersonic microscope)などが考えられます。…現実はもっと進んでいるかも知れませんが…。

$$\zeta f(x) = x^{((p+1)/4)} F(7/12,11/12,1,1-x)$$

$$f^*(n) = \zeta f(r^n) = \text{lavr mod } p,\ r = 5\ (= \text{primitive root mod } p)$$

$$p = 25127,\quad |2\sqrt{p}| = 317.0299670$$



これらの対称巡回対合(= 直交系, sci)の計算は、例えば、$p = 10^{10}$ 程度でも

そんなに複雑ではありません。

認識論との関連では、対合 $A^2 = E$ (= identity) は射影 (= 自己認識) と反射 (= 投影) の和

$$A = (A+E)/2+(A-E)/2$$

$$(A\pm E)(A\pm E) = A^2 \pm 2A+E = 2(E\pm A)$$

$$(A+E)(A-E) = A^2-E = O$$

です。

3. 5 次対称巡回対合 (5-sci)

5 次対称巡回対合は、例えば、p = 11 の場合は

$$\begin{pmatrix} 2 & -1 & 6 & 8 & -4 \\ -1 & 6 & 8 & -4 & 2 \\ 6 & 8 & -4 & 2 & -1 \\ 8 & -4 & 2 & -1 & 6 \\ -4 & 2 & -1 & 6 & 8 \end{pmatrix} \quad \begin{pmatrix} 6 & 3 & 6 & -6 & 2 \\ 3 & 6 & -6 & 2 & 6 \\ 6 & -6 & 2 & 6 & 3 \\ -6 & 2 & 6 & 3 & 6 \\ 2 & 6 & 3 & 6 & -6 \end{pmatrix}$$

の 1/11 のような 5 個の数が輪になった行列です。現実には p = 10n+1 の形の素数 (r 原始根) については本質的には 2 種類あって

$$1/p\cdot F(1/3,2/3,1,-x)[r]x^5-1$$

$$1/p\cdot F(1/4,3/4,1,-x)[r]x^5-1$$

で尽くされます (これは予想です)。原始根 r の選び方に多様性があり、要素の順番が異なりますが集合としては一致しています。このような 2 種類の構成要素からなる体系 (system) は化学的な物質の世界にも、例えば、性差のような、対応物があるのではないかと想像できます。3 次元空間の正 5 角形 (等辺等角図形) は平面図形 (pentagon, pentagram の 2 種) であることが知られています。

例. p = 11, r = 2, -1/4 = 8, -3/4 = 2

この場合、$2\cdot 8 = 16/1 = 5$, $5\cdot 7/4 = 1/2 = 6$ であるから、

$$F(1/4,3/4,1,x) = 1+5x+6x^2$$

$$F(1/4,3/4,1,x)[2](x) = (1-x^{10})(1/(1-x)+5/(1-2x)+6/(1-4x^2))$$

$$= 1+2x-4x^2-4x^3+2x^5+2x^6+4x^8-6x^9$$

従って、

$$1/11\cdot F(1/4,3/4,1,-x)[2|x]x^5-1 = 1/11\cdot$$

$$\begin{pmatrix} 6 & 8 & -4 & 2 & -1 \\ 8 & -4 & 2 & -1 & 6 \\ -4 & 2 & -1 & 6 & 8 \\ 2 & -1 & 6 & 8 & -4 \\ -1 & 6 & 8 & -4 & 2 \end{pmatrix}$$

例. $p = 11, r = 2, -1/3 = 7, -2/3 = 3$

この場合、$3.7/1 = -1, -6\cdot 2/4 = -3, -3\cdot 5/9 = -5/3 = 2$ であるから

$$F(1/3,2/3,1,x) = 1-x-3x^2+2x^3$$

$$F(1/3,2/3,1,x)[2](x) = (1-x^{10})(1/(1-x)-1/(1-2x)-3/(1-4x)+2/(1-8x))$$

$$= -1+3x+6x^4-3x^5-3x^6-6x^7+3x^8$$

従って、

$$1/11\cdot F(1/3,2/3,1,-x)[2|x]x^5-1 = 1/11\cdot$$

$$\begin{pmatrix} 6 & 3 & 6 & -6 & 2 \\ 3 & 6 & -6 & 2 & 6 \\ 6 & -6 & 2 & 6 & 3 \\ -6 & 2 & 6 & 3 & 6 \\ 2 & 6 & 3 & 6 & -6 \end{pmatrix}$$

が得られますが、Hasse の限界が $2\sqrt{11} = 6.63324958$ ですから、5, 6 の選択には自由度があります。

例. $p = 10000000061, r = 2, n = [p/10] = 1000000006$ である。

$$2^{1000000006} \bmod p = 7811723043$$

$F(1/4,3/4,1,x)$ は $[p/4] = 2500000015$ 次の多項式である。

$$F(1/4,3/4,1,x)[2|x]x^5+1$$

を計算したい訳であるが、$x^5+1 = 0$ の根は 1 の原始 10 乗根であるから、

$$x^5+1 = (x-2^n)(x-2^{3n})(x-2^{5n})(x-2^{7n})(x-2^{9n})$$

である。このうち、$F(1/4,3/4,1,x)$ の項として現れ得るのは

$n \le p/4$ のみである ($p/4 < 3n, 5n, 7n, 9n$ であるから)。$n \ne m \le p/4$ とすると、Vandermonde 変換の項、つまり、p-2 次の F_p の多項式

$$(1-x^{p-1})/(1-2^m x)$$

は x^5+1 で割り切れる。この点は簡単なことであるが本質的である。従って、終結行列の計算に関与するのは唯一項

$$(1/4)_n(3/4)_n/n!^2\cdot(1-x^{p-1})/(1-2^n x)$$

のみである。

$$(1-x^{p-1})/(1-2^n x) = 1+2^n x+2^{2n}x^2+\cdots+2^{n(10n-1)}x^{10n-1}$$

ここで、x の代わりに-x を代入すると、p-1 は偶数だから、

$$(1-x^{p-1})/(1+2^n x) = 1-2^n x+2^{2n}x^2-\cdots-2^{n(10n-1)}x^{10n-1}$$

である。このように x の符号をかえると

$$F(1/4,3/4,1,-x)[2](x) \mod x^5-1$$

は、剰余定理より $x^5 = 1$ を代入すれば得られる。同一の 4 次式が (p-1)/5 回繰り返されるのであるから。

$$F(1/4,3/4,1,-x)[2|x]x^5-1$$

の第 1 行は F_p では

$$(p-1)/5\cdot(1-2^n x+2^{2n}x^2-2^{3n}x^3+2^{4n}x^4) = -1/5\cdot(x^5+1)/(1-2^n x)$$

である。

さて、具体的には

$$(1/4)_n(3/4)_n/n!^2 = 1174225286$$

$$1174225286/5 = 8234845106$$

ですから、

$$8234845106(1+x^5)/(1-7811723043x)$$

$$= 8958711391x^4+548622171x^3+1028237186x^2+7673171451x+8234845106$$

$$= -1041288670x^4-9451377890x^3+1028237186x^2-2326828610x-1765154955$$

です。剰余のなかには絶対値最小剰余 (lavr) ではないものがあります。

$$\begin{pmatrix} -1041288670, 9451377890, 1028237186, 2326828610, -1765154955 \\ 9451377890, 1028237186, 2326828610, -1765154955, -1041288670 \\ 1028237186, 2326828610, -1765154955, -1041288670, 9451377890 \\ 2326828610, -1765154955, -1041288670, 9451377890, 1028237186 \\ -1765154955, -1041288670, 9451377890, 1028237186, 2326828610 \end{pmatrix}$$

から、5-sci が定まります。

要するに mod p での $\tau = r^{2n}$ は $x^5-1 = 0$ の根で $r^5 = -1$ であるから

$$(1/4)_n(3/4)_n/(n!^2\cdot 5)x^5-1[x]x-\tau^3 =$$

$$\begin{pmatrix} r^{4n} & r^{8n} & r^{2n} & r^{6n} & 1 \\ r^{8n} & r^{2n} & r^{6n} & 1 & r^{4n} \\ r^{2n} & r^{6n} & 1 & r^{4n} & r^{8n} \\ r^{6n} & 1 & r^{4n} & r^{8n} & r^{2n} \end{pmatrix}$$

$$\begin{pmatrix} 1 & r^{4n} & r^{8n} & r^{2n} & r^{6n} \end{pmatrix}$$

だったのである。何か、ちょっと「あれっ!」(ありゃ!あり得ん≒ a rear alien) という虚無感のある表示である。複素数の範囲では

$$A = x^5\text{-}1[x]x\text{-}\tau$$

は$|A| = 0$であり A は対合にはなり得ない。また、有限体

$$F_p = \{0,1,\cdots,p\text{-}1\} = p$$

では、p は 0, ∞ とどのように解釈されるのか興味あります。1/p(= infinity?) の一つの解釈の可能性を与えるという意味はあると思います。

例. $p = 10000000061$, $F(1/3,2/3,1,x)$

$$(1/3)_n(2/3)_n/n!^2 = 5178641491$$

$$(1/3)_{3n}(2/3)_{3n}/(3n)!^2 = 6527490806$$

である。この場合は

$$1/5\cdot(1+x^5)(5178641491/(1\text{-}7811723043x)+6527490806/(1\text{-}3127117921x))$$

が求める多項式で、mod p で

$$1067878781x^4+9921658781x^3+7312793501x^2+6800239997x+8341226496$$

$$=$$

$$\text{-}8932121280x^4\text{-}78341280x^3\text{-}2687206560x^2\text{-}3199760064x\text{-}1658773565$$

の方が 5 対称巡回対合(5-sci)

$$\begin{pmatrix} 8932121280, -78341280, 2687206560, -3199760064, 1658773565 \\ -78341280, 2687206560, -3199760064, 1658773565, 8932121280 \\ 2687206560, -3199760064, 1658773565, 8932121280, -78341280 \\ -3199760064, 1658773565, 8932121280, -78341280, 2687206560 \\ 1658773565, 8932121280, -78341280, 2687206560, -3199760064 \end{pmatrix}$$

を与える。以上 2 つの例では

$$(1/4)_n(3/4)_n/n!^2,\ (1/3)_n(2/3)_n/n!^2,\ (1/3)_{3n}(2/3)_{3n}/(3n)!^2$$

などの計算量が問題だったのです。今の方法では順次計算する方法を(私は)用いていますので p に比例する計算量が必要です。効率的計算法の開発・発見が期待されます。例えば、$p = 1 \bmod 10$ の素数

$$p = p\pi(4) = 31415926535897932384626433832795028841$$

での 2 つの 5-sci の計算などは興味ある問題です。また、π の最初の何桁かで素数になる数(存在も含めて)

$$p\pi(1) = 3,\ p\pi(2) = 31,\ p\pi(3) = 314159,\ \cdots$$

の pπ(5)なども興味があります(試算では 5000 桁は越えそうです)。

4. 位数 5 の対称巡回対合曲面(5-sci surface)

対称巡回対合(sci)は、対称巡回行列

$$A = \begin{pmatrix} a & b & c & d & e \\ b & c & d & e & a \\ c & d & e & a & b \\ d & e & a & b & c \\ e & a & b & c & d \end{pmatrix}$$

について、$A^2 = E$(単位行列)となることである。この条件は

$$a+b+c+d+e = 1,\ ae+ba+cb+dc+ed = 0,\ ad+be+ca+db+ec = 0$$

の 3 条件で表現されます。標準化された 3 次元空間の図形

$$[a+b+c+d+e-1,\ ae+ba+cb+dc+ed,\ ad+be+ca+db+ec]$$

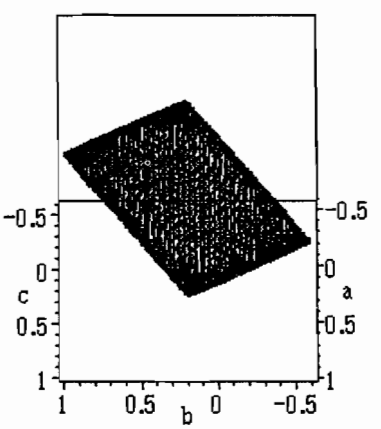
(ideal basis)の 1, 3 式から

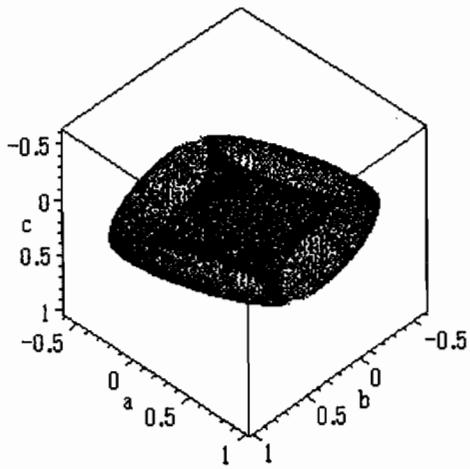
$$e = -(a^2+2ba-a+b^2+cb-b)/(a-c),\ d = (ba+2cb+c^2+b^2-b-c)/(a-c)$$

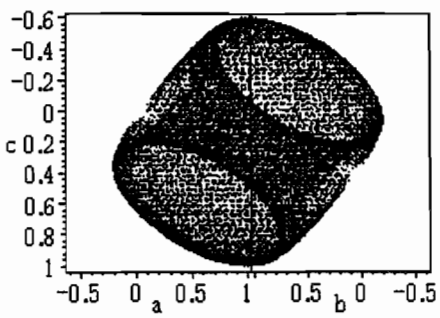
得られる。これを 2 式に代入すると、$1/(a-c)^2$ を除いて

$$b^2-a^3+a^4-c^3+c^4+b^4-2b^3-2bac+ba^2c+3ab^2c+ac^2b-3ba^2-4b^2a-4b^2c$$
$$-3c^2b-a^3c+2ba^3+4b^2a^2+2c^3b-c^3a+4b^2c^2+a^2c^2+3b^3a+3b^3c+ba+cb+ca$$

を得る。この xyz-空間での曲面は次のようである。





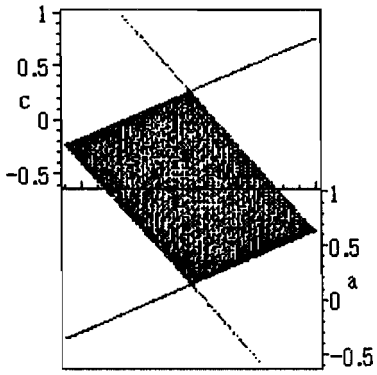


この曲面はトーラス(tolus)を想像させるが…異なる。ある方向からは平行四辺形に見えるのでこれらの綾線を軸に取ることは自然なことである。軸は極値、あるいは、停留値の形で表現される。結論は平行な2平面の組

$$b+1+2/\sqrt{5}-(1/2+\sqrt{5}/2)(a+c),\ b+1-2/\sqrt{5}-(1/2-\sqrt{5}/2)(a+c),$$

$$b-1-(1/2-\sqrt{5}/2)(a+c),\ b-1-(1/2+\sqrt{5}/2)(a+c)$$

と接している。



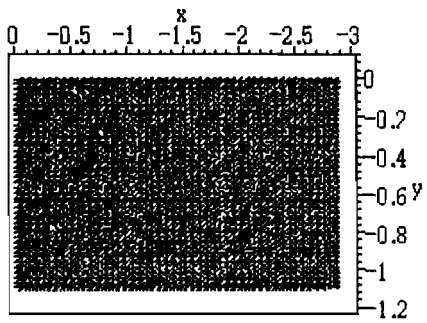
これは、今ひとつ整理して表現するとどのようになるであろうか。

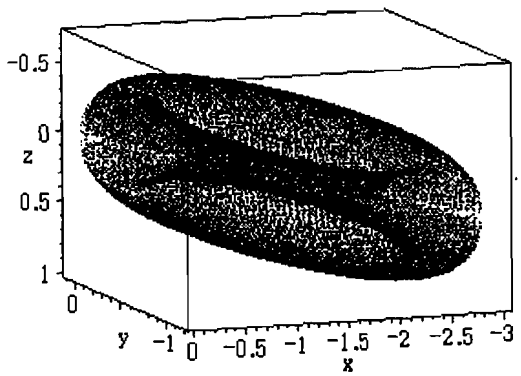
$$z = a,\ x = b\text{-}1\text{-}(1/2+\sqrt{5}/2)(a+c),\ y = b\text{-}1\text{-}(1/2-\sqrt{5}/2)(a+c)$$

言い換えると

$$a = z,\ b = y/2+1-\sqrt{5}/10x+\sqrt{5}/10y+x/2,\ c = -1/\sqrt{5}(x-y+\sqrt{5}z)$$

とおくと、





のようである。しかし、まだ軸は傾いている。

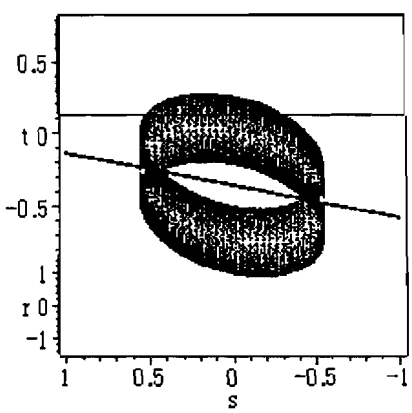
$$z = t+1/5,\ x = r-1-1/\sqrt{5},\ y = s-1+1/\sqrt{5}$$

$$s = y+1-1/\sqrt{5},\ r = x+1+1/\sqrt{5},\ t = z-1/5$$

では、平面

$$s-2\sqrt{5}t-r$$

を描くと



のように分割している。この図形は何か、植物の葉の気孔(pore)や人の唇(lip)や瞼(まぶた，eyelid，lid)を思いおこさせる。開閉などの行為と関係するのであろう。さて、

$$t = q+\sqrt{5}/10\,(s-r)$$

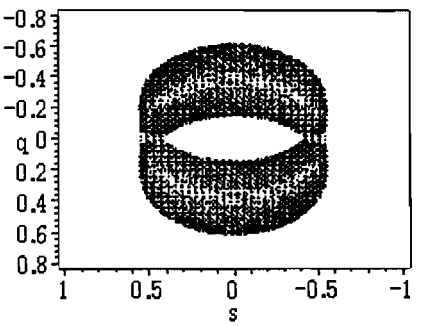
とおき、

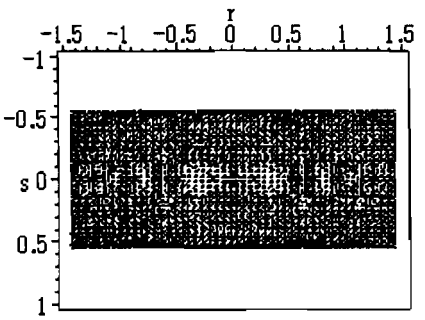
$$s = y+1-1/\sqrt{5},\ q = z-\sqrt{5}/10y+\sqrt{5}/10x,\ r = x+1+1/\sqrt{5}$$
$$y = s-1+1/\sqrt{5},\ x = r-1-1/\sqrt{5},\ z = q+\sqrt{5}/10s+1/5-\sqrt{5}/10r$$

とすると

$$-10\sqrt{5}q^2r^2-5\sqrt{5}/2r^4+2/5-2s^2-2r^2+45/8s^4-\sqrt{5}s^2+\sqrt{5}r^2+45/8r^4$$
$$+50q^4+25q^2s^2+25q^2r^2-5/4s^2r^2-20q^2+10\sqrt{5}q^2s^2+5\sqrt{5}/2s^4$$

なる対称式が得られる。





のような素直な図形である。これは、二つの楕円を楕円に沿って平行移動させて生成される曲面で自己交叉の線をもつ。従って、トーラス面とは異

なるが、円周の 2 つの直積という意味で、似た曲面である。(4,5 次元空間では torus と同型)

さて、対称 4 次式

$$-10\sqrt{5}q^2r^2-5\sqrt{5}/2r^4+2/5-2s^2-2r^2+45/8s^4-\sqrt{5}s^2+\sqrt{5}r^2+45/8r^4$$
$$+50q^4+25q^2s^2+25q^2r^2-5/4s^2r^2-20q^2+10\sqrt{5}q^2s^2+5\sqrt{5}/2s^4$$

の構造を見るため、

$$q^2 = x,\ s^2 = y,\ r^2 = z$$

とおいて 2 次形式と見るときの構造はどのようになっているでしょうか。

$$50x^2+((-10\sqrt{5}+25)z+(10\sqrt{5}+25)y-20)x+(45/8-5\sqrt{5}/2)z^2$$
$$+(-2-5/4y+\sqrt{5})z+(5\sqrt{5}/2+45/8)y^2+(-\sqrt{5}-2)y+2/5$$

の Hessian は

$$\begin{pmatrix} 100, & 10\sqrt{5}+25, & -10\sqrt{5}+25 \\ 10\sqrt{5}+25, & 5\sqrt{5}+45/4, & -5/4 \\ -10\sqrt{5}+25, & -5/4, & 45/4-5\sqrt{5} \end{pmatrix}$$

であり、

$$5\sqrt{5}+45/4 = (5/2+\sqrt{5})^2,\ -5\sqrt{5}+45/4 = (5/2-\sqrt{5})^2$$

ですから、

$$u = 10x,\ v = (5/2+\sqrt{5})y,\ w = (5/2-\sqrt{5})z$$

とおけば、係数が揃いそうです。結果は(2 倍していますが)

$$u^2+2uw+2uv-4u+w^2+4/\sqrt{5}w-2wv+v^2-4/\sqrt{5}v+4/5$$

のように比較的に簡単です。w, v の係数には $\sqrt{5}$ を含む項がありますが u にはありません。その意味で u には特別の意味があります。u について解いてみますと

$$u = -w-v+2+2/5\cdot\sqrt{(25wv-25w-25v+20-5\sqrt{5}w+5\sqrt{5}v)}$$

であり、根号の中身は

$$(5v-\sqrt{5}-5)(5w-5+\sqrt{5})$$

です。

$$u = 10x = 10q^2,\ v = (5/2+\sqrt{5})y = (5/2+\sqrt{5})s^2,\ w = (5/2-\sqrt{5})z = (5/2-\sqrt{5})r^2$$

を代入すると、

$$(5v-\sqrt{5}-5)(5w-5+\sqrt{5}) =$$
$$1/20(5r+5+\sqrt{5})(-5r+5+\sqrt{5})(-5s-5+\sqrt{5})(5s-5+\sqrt{5})$$
$$= 5/4(5r^2-6-2\sqrt{5})(5s^2-6+2\sqrt{5})$$

これから、例えば、

$$h^2 - \sqrt{5}/2\,(5r^2-6-2\sqrt{5}) = 0$$

のような2次曲線の助変数表示を通じて、元の式の2変数の助変数表示が得られる可能性がでてきた。

以下は、部分的なもので、理路は行き止まりであったが(最初、途中まではそう思った)、まあ、辿った道を記しておく。

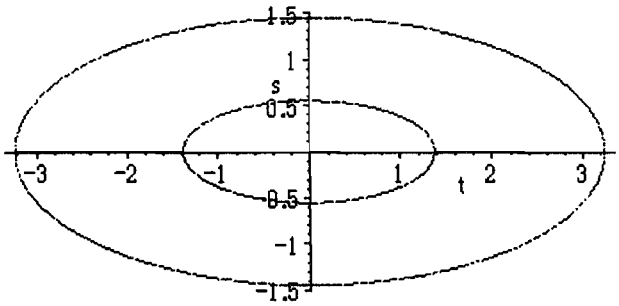
$$1/20\,(5r+5+\sqrt{5})\,(-5r+5+\sqrt{5})\,(-5s-5+\sqrt{5})\,(5s-5+\sqrt{5})$$

を二つの部分(非対称だが)に分けて

$$t^2-1/4\,(5r+5+\sqrt{5})\,(-5r+5+\sqrt{5})$$

$$t^2-1/5\,(-5s-5+\sqrt{5})\,(5s-5+\sqrt{5})$$

とおいてみる。これらは楕円である。



例えば、r = s = 0において、簡潔な解があれば、例の勾配法で助変数表示が可能であろうとの目論見である。現実に

$$t = \pm(5/2-\sqrt{5}/2),\ t = \pm(1+\sqrt{5})$$

であるから、直線

$$t-5/2+\sqrt{5}/2+hs,\quad t-1-\sqrt{5}+kr$$

などを考えると

$$t^2-1/5\,(-5s-5+\sqrt{5})\,(5s-5+\sqrt{5})\,\textcircled{t}\,t-5/2+\sqrt{5}/2+hs = s/4\,(25s-20h+4\sqrt{5}h+4h^2s)$$

$$t^2-1/4\,(5r+5+\sqrt{5})\,(-5r+5+\sqrt{5})\,\textcircled{t}\,t-1-\sqrt{5}+kr = r\,(5r-2k-2\sqrt{5}k+k^2r)$$

であるから、非自明因子から

$$25s-20h+4\sqrt{5}h+4h^2s,\ 5r-2k-2\sqrt{5}k+k^2r$$

を解いて

$$r = 2k(1+\sqrt{5})/(5+k^2),\ s = -4h(-5+\sqrt{5})/(25+4h^2)$$

を得る。

$$v = (5/2+\sqrt{5})s^2,\ w = (5/2-\sqrt{5})r^2$$

に代入すると、

$$v = 80(5+\sqrt{5})h^2/(25+4h^2)^2,\ w = -4(-5+s^2)k^2/((5+k^2)^2$$

が得られる。

$$u^2+2uw+2uv-4u+w^2+4/\sqrt{5}w-2wv+v^2-4/\sqrt{5}v+4/5$$

に代入すると、

$$-1/25$$
$$(-80uk^4h^4-1000uk^4h^2-3125uk^4-800uh^4k^2-10000uk^2h^2-31250uk^2-2000uh^4-25000uh^2$$
$$-78125u+160h^4k^4+64\sqrt{5}h^4k^4-400\sqrt{5}h^2k^4+6250k^4-2500\sqrt{5}k^4+320\sqrt{5}h^4k^2-20000h^2k^2$$
$$+12500\sqrt{5}k^2+4000h^4-1600\sqrt{5}h^4-10000\sqrt{5}h^2+156250+62500\sqrt{5})$$
$$(78125u+80uk^4h^4-160h^4k^4+64\sqrt{5}h^4k^4+2000uh^4+400\sqrt{5}h^2k^4+25000uh^2-12500\sqrt{5}k^2$$
$$-4000h^4-1600\sqrt{5}h^4-6250k^4-2500\sqrt{5}k^4-156250+62500\sqrt{5}+10000uk^2h^2+3125uk^4$$
$$+10000\sqrt{5}h^2+20000h^2k^2+800uh^4k^2+1000uk^4h^2-320\sqrt{5}h^4k^2+31250uk^2)$$
$$/((5+k^2)^4(25+4h^2)^4)$$

のように因数分解する。あるいは、

$$u = -w-v+2\pm 2/5\sqrt{(25wv-25w-25v+20-5w\sqrt{5}+5\sqrt{5}v)}$$

に着目して、根号の中身として

$$2\sqrt{5}(k+\sqrt{5})(-k+\sqrt{5})(2h+5)(2h-5)/((5+k^2)(25+4h^2))$$

を得る。

$$-w-v+2 = 4(-5+\sqrt{5})k^2/(5+k^2)^2-80(5+\sqrt{5})h^2/(25+4h^2)^2+2$$

に注意すると、

$$u = 4(-5+\sqrt{5})k^2/(5+k^2)^2-80(5+\sqrt{5})h^2/(25+4h^2)^2+2$$
$$\pm 2/5(2\sqrt{5}(k+\sqrt{5})(-k+\sqrt{5})(2h+5)(2h-5)/((5+k^2)(25+4h^2)))$$

である。+の場合は

$$u =$$
$$-2/5(2\sqrt{5}-5)(-4h^2k^2+50k^2+25\sqrt{5}k^2-40h^2-20\sqrt{5}h^2+125)^2/((5+k^2)^2(25+4h^2)^2)$$
$$2/5(2\sqrt{5}+5)(-4h^2k^2-50k^2+25\sqrt{5}k^2+40h^2-20\sqrt{5}h^2+125)^2/((5+k^2)^2(25+4h^2)^2)$$

である。これは意外なことであった。つまり、

$$u = 10q^2$$

であるから、q が h, k の有理式で表現できることを意味している。

$$q =$$

$$\pm 1/5\cdot\sqrt{5}\,(-2\sqrt{5}+5)\,(-4h^2k^2+50k^2+25\sqrt{5}k^2-40h^2-20\sqrt{5}h^2+125)/((5+k^2)\,(25+4h^2))$$

$$\pm 1/5\cdot\sqrt{5}\,(2\sqrt{5}+5)\,(-4h^2k^2-50k^2+25\sqrt{5}k^2+40h^2-20\sqrt{5}h^2+125)/((5+k^2)\,(25+4h^2))$$

これから、検算にかかる。

$$r = 2k\,(1+\sqrt{5})/(5+k^2),\ s = -4h\,(-5+\sqrt{5})/(25+4h^2)$$

$$q = -1/5\cdot\sqrt{5}\,(-2\sqrt{5}+5)\,(-4h^2k^2+50k^2+25\sqrt{5}k^2-40h^2-20\sqrt{5}h^2+125)/((5+k^2)\,(25+4h^2))$$

を

$$x = r-1-1/\sqrt{5},\ y = s-1+1/\sqrt{5},\ z = q+\sqrt{5}/10s+1/5-\sqrt{5}/10r$$

に代入すると、少し複雑であるが

$$x = -1/5\,(\sqrt{5}+5)\,(-\sqrt{5}+k)^2/(5+k^2),$$

$$y = 1/5\,(-5+\sqrt{5})\,(-5+2h)^2/(25+4h^2),$$

$$z = -1/10\,(-1+\sqrt{(-2\sqrt{5}+5)})$$

$$(175k^2-60h^2+250\sqrt{5}+8h^2k^2-20\sqrt{5}h^2+75\sqrt{5}k^2-375k+150h-60h^2k+30k^2h+500\sqrt{(-2\sqrt{5}+5)}$$
$$+50\sqrt{(-2\sqrt{5}+5)}\,h\sqrt{5}-175\sqrt{(-2\sqrt{5}+5)}\,k\sqrt{5}-60\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5}h^2-28\sqrt{5}kh^2+30\sqrt{(-2\sqrt{5}+5)}\,k^2h$$
$$+125\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5}k^2+10\sqrt{5}hk^2-60\sqrt{(-2\sqrt{5}+5)}\,h^2k+250-175\sqrt{5}k+10\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5}hk^2$$
$$-28\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5}kh^2+50h\sqrt{5}-140\sqrt{(-2\sqrt{5}+5)}\,h^2+275\sqrt{(-2\sqrt{5}+5)}\,k^2+150\sqrt{(-2\sqrt{5}+5)}\,h$$
$$-375\sqrt{(-2\sqrt{5}+5)}\,k+250\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5})$$
$$/((5+k^2)\,(25+4h^2))$$

を得る。この式を

$$a = z,\ b = y/2+1-\sqrt{5}/10x+\sqrt{5}/10y+x/2,\ c = -1/5\,(x-y+\sqrt{5}z)\,\sqrt{5}$$

に代入すると

$$a = -1/10\cdot(-1+\sqrt{(-2\sqrt{5}+5)})$$

$$(175k^2-60h^2+250\sqrt{5}+8h^2k^2-20\sqrt{5}h^2+75\sqrt{5}k^2-375k+150h-60h^2k+30k^2h+500\sqrt{(-2\sqrt{5}+5)}$$
$$+50\sqrt{(-2\sqrt{5}+5)}\,h\sqrt{5}-175\sqrt{(-2\sqrt{5}+5)}\,k\sqrt{5}-60\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5}h\text{^}2-28\sqrt{5}kh^2+30\sqrt{(-2\sqrt{5}+5)}\,k^2h$$
$$+125\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5}k^2+10\sqrt{5}hk^2-60\sqrt{(-2\sqrt{5}+5)}\,h^2k+250-175k\sqrt{5}+10\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5}hk^2$$
$$-28\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5}kh^2+50h\sqrt{5}-140\sqrt{(-2\sqrt{5}+5)}\,h^2+275\sqrt{(-2\sqrt{5}+5)}\,k^2+150\sqrt{(-2\sqrt{5}+5)}\,h$$
$$-375\sqrt{(-2\sqrt{5}+5)}\,k+250\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5})/((5+k^2)\,(25+4h^2)),$$

$$b = 1/5\,(20h^2+200h+40k^2h+4h^2k^2+100k\sqrt{5}+16\sqrt{5}kh^2+125+25k^2)/((5+k^2)\,(25+4h^2)),$$

$$c = 1/10\,(\sqrt{(-2\sqrt{5}+5)}+1)$$

$$(175k^2-60h^2+250\sqrt{5}+8h^2k^2-20\sqrt{5}h^2+75\sqrt{5}k^2-375k+150h-60h^2k+30k^2h-500\sqrt{(-2\sqrt{5}+5)}$$
$$-50\sqrt{(-2\sqrt{5}+5)}\,h\sqrt{5}+175\sqrt{(-2\sqrt{5}+5)}\,k\sqrt{5}+60\sqrt{(-2\sqrt{5}+5)}\,\sqrt{5}h^2-28\sqrt{5}kh^2-30\sqrt{(-2\sqrt{5}+5)}\,k^2h$$

$$-125\sqrt{(-2\sqrt{5}+5)}\sqrt{5}k^2+10\sqrt{5}hk^2+60\sqrt{(-2\sqrt{5}+5)}h^2k+250-175k\sqrt{5}-10\sqrt{(-2\sqrt{5}+5)}\sqrt{5}hk^2$$
$$+28\sqrt{(-2\sqrt{5}+5)}\sqrt{5}kh^2+50h\sqrt{5}+140\sqrt{(-2\sqrt{5}+5)}h^2-275\sqrt{(-2\sqrt{5}+5)}k^2-150\sqrt{(-2\sqrt{5}+5)}h$$
$$+375\sqrt{(-2\sqrt{5}+5)}k-250\sqrt{(-2\sqrt{5}+5)}\sqrt{5})/((5+k^2)(25+4h^2))$$

が得られる。さらに、

$$e = -(a^2+2ba-a+b^2+cb-b)/(a-c),\ d = (ba+2cb+c^2+b^2-b-c)/(a-c)$$

に代入すると、

$$d = 1/10(1+\sqrt{(-2\sqrt{5}+5)}\sqrt{5}+2\sqrt{(-2\sqrt{5}+5)})$$
$$(175k^2-60h^2-250\sqrt{5}+8h^2k^2+20\sqrt{5}h^2-75\sqrt{5}k^2+375k+150h+60h^2k+30k^2h+250\sqrt{(-2\sqrt{5}+5)}$$
$$-50\sqrt{(-2\sqrt{5}+5)}h\sqrt{5}-25\sqrt{(-2\sqrt{5}+5)}k\sqrt{5}+20\sqrt{(-2\sqrt{5}+5)}\sqrt{5}h^2-28\sqrt{5}kh^2-10\sqrt{(-2\sqrt{5}+5)}k^2h$$
$$-25\sqrt{(-2\sqrt{5}+5)}\sqrt{5}k^2-10\sqrt{5}hk^2+20\sqrt{(-2\sqrt{5}+5)}h^2k+250-175k\sqrt{5}-10\sqrt{(-2\sqrt{5}+5)}\sqrt{5}hk^2$$
$$-4\sqrt{(-2\sqrt{5}+5)}\sqrt{5}kh^2-50h\sqrt{5}-20\sqrt{(-2\sqrt{5}+5)}h^2+75\sqrt{(-2\sqrt{5}+5)}k^2-50\sqrt{(-2\sqrt{5}+5)}h$$
$$+125\sqrt{(-2\sqrt{5}+5)}k)/((5+k^2)(25+4h^2)),$$
$$e = -1/10(-1+\sqrt{(-2\sqrt{5}+5)}\sqrt{5}+2\sqrt{(-2\sqrt{5}+5)})$$
$$(175k^2-60h^2-250\sqrt{5}+8h^2k^2+20\sqrt{5}h^2-75\sqrt{5}k^2+375k+150h+60h^2k+30k^2h-250\sqrt{(-2\sqrt{5}+5)}$$
$$+50\sqrt{(-2\sqrt{5}+5)}h\sqrt{5}+25\sqrt{(-2\sqrt{5}+5)}k\sqrt{5}-20\sqrt{(-2\sqrt{5}+5)}\sqrt{5}h^2-28\sqrt{5}kh^2+10\sqrt{(-2\sqrt{5}+5)}k^2h$$
$$+25\sqrt{(-2\sqrt{5}+5)}\sqrt{5}k^2-10\sqrt{5}hk^2-20\sqrt{(-2\sqrt{5}+5)}h^2k+250-175k\sqrt{5}+10\sqrt{(-2\sqrt{5}+5)}\sqrt{5}hk^2$$
$$+4\sqrt{(-2\sqrt{5}+5)}\sqrt{5}kh^2-50h\sqrt{5}+20\sqrt{(-2\sqrt{5}+5)}h^2-75\sqrt{(-2\sqrt{5}+5)}k^2+50\sqrt{(-2\sqrt{5}+5)}h$$
$$-125\sqrt{(-2\sqrt{5}+5)}k)/((5+k^2)(25+4h^2))$$

が得られる。これらにより

$$[a+b+c+d+e-1,\ ae+ba+cb+dc+ed,\ ad+be+ca+db+ec]$$

を計算すれば、Maple V では、確かに[0,0,0]が得られるので、(これはやはり他人の目での check が必要である)、一応の信用をしてもよいと思う。

2014.07.15.11.04

感想を述べれば、この計算では、途中でこの計算は行き止まりになると感じていたのであるが…一応の式は求まったことに驚いている。結果の式は、簡潔とは言い難いかも知れないが、自分には驚きであった。

むかし をとこ まどろみて 夢に ひらひらするものあり、見ればてふなり、はねは楕円 紋も楕円、よりて

ひらくとじる このはのまどか くちびるか
まぶたをとじて はなのかをきく

とよみていねけり。

その後 感じたことは、出てきた結果があまり「きれい」ではないこと

である。もっと、簡潔な方法があるのであろうか。

$$100x^2+(20\sqrt{5}y+50y+50z-40-20\sqrt{5}z)x$$
$$+45/4y^2+5\sqrt{5}y^2-5/2yz-2\sqrt{5}y-4z+45/4z^2-5\sqrt{5}z^2+4/5+2\sqrt{5}z-4y$$

そこで、

$$x = t/10-\sqrt{5}/10y-y/4-z/4+1/5+\sqrt{5}/10z$$

とおくと

$$t^2-16/5-2\sqrt{5}z-5yz+2\sqrt{5}y+6y+6z = t^2-1/5\,(-6+2\sqrt{5}+5y)\,(-5z+2\sqrt{5}+6)$$

である。従って、例えば、

$$1/5\,(-6+2\sqrt{5}+5y) = h^2,\ (-5z+2\sqrt{5}+6) = k^2$$

これから、

$$z = -k^2/5+2/\sqrt{5}+6/5,\ y = -h^2+6/5-2/\sqrt{5}\ ,\ t = \pm hk$$

を得る。今、$t = hk$ の場合を考えてみると、

$$x = (5+2\sqrt{5})/500\,(-5k-5h+2\sqrt{5}k)^2$$

である。

$$q^2 = x,\ s^2 = y,\ r^2 = z$$

のようにすべて平方になるようにしたい。方程式は

$$r^2 = -k^2/5+2/\sqrt{5}+6/5,\ s^2 = -h^2+6/5-2/\sqrt{5}$$

であり、これらは楕円である。例えば、$r, s = 0$ とおくと、

$$h = -1+1/\sqrt{5},\ k = -1-\sqrt{5},$$
$$k = 1+\sqrt{5},\ h = -1+1/\sqrt{5},$$
$$h = 1-1/\sqrt{5},\ k = -1-\sqrt{5},$$
$$k = 1+\sqrt{5},\ h = 1-1/\sqrt{5}$$

の4組の解が得られる。従って、例えば、

$$r = u\,(k+1+\sqrt{5})\,,\ s = v\,(h+1-1/\sqrt{5})$$

が得られる。これから、

$$k-1-\sqrt{5}+5u^2k+5u^2+5\sqrt{5}u^2,\ -5v^2h-5v^2+v^2\sqrt{5}-5h+5-\sqrt{5}$$

を解くと、

$$k = 1/5\,(1+\sqrt{5})\,(5u+\sqrt{5})\,(-5u+\sqrt{5})/(5u^2+1)\,,\ h = 1/5\,(-5+\sqrt{5})\,(v-1)\,(1+v)/(1+v^2)$$

が得られる。これを代入すると

$$s^2 = -8/5v^2\,(-3+\sqrt{5})/(1+v^2)^2,\ r^2 = 8u^2\,(3+\sqrt{5})/(5u^2+1)^2,$$
$$q^2 = 1/25\,(5+2\sqrt{5})\,(1+2v^2-10u^2-5u^2v^2-v^2\sqrt{5}+5\sqrt{5}u^2)^2/((5u^2+1)^2(1+v^2)^2)$$

が得られる。これらは、定数部分を除くと平方式である。こうして(符号

のとり方に自由さはあるが)

$$r = (2+2\sqrt{5})u/(5u^2+1),\ s = (2-2/\sqrt{5}v/(1+v^2),$$

$$q = 1/5\sqrt{(5+2\sqrt{5})}\,(1+2v^2-10u^2-5u^2v^2-v^2\sqrt{5}+5u^2\sqrt{5})/((5u^2+1)(1+v^2))$$

を得る。この場合も2重根号

$$\sqrt{(5+2\sqrt{5})}$$

が登場する。恐らくこれは必然なのである。この値を根とする多項式は

$$x^4-10x^2+5 = 0$$

である。

5-sci の存在については、上記のような理路とは関係なく、$p = 1 \bmod 10$ の素数に対し、連立 Diophantine 方程式

$$a+b+c+d+e = p,\ ae+ba+cb+dc+ed = 0,\ ad+be+ca+db+ec = 0$$

の(本質的には2通り?)整数解を与える(効率的)な方法の研究は、計算量(computational amount)や計算の複雑性(computationl complexity)の観点からも興味深いものです。

参考文献

[1] 難波完爾 Dedekind η 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 27, 第16回数学史シンポジウム(2005), 2006, pp. 95-167

[2] 難波完爾 Hyper-elliptic curve and Hasse's inequality, 津田塾大学 数学・計算機科学研究所報 33, 第22回数学史シンポジウム(2011), 2012, pp. 137-174

[3] 難波完爾 Genus 5 hyper-elliptic curves and their coefficient manifolds, 津田塾大学 数学・計算機科学研究所報 34, 第 23 回数学史シンポジウム(2012), 2013, pp. 277-325

[4] 難波完爾 数学と論理, 講座 数学の考え方 23, 朝倉書店 2011

[5] Kanji Namba: Elliptic involution property of finite fields, 2014年度応用数学合同研究集会予稿集, 主催:日本数学会応用数学分科会、協賛:日本応用数理学会、龍谷大学理工学部、龍谷大学瀬田キャンパス, 2014, pp.94-99

[6] 堀内秀晃・秋山虔 校注、竹取物語 伊勢物語、新日本古典文学大系17、岩波書店2005, p. 86, 91