Genus 4 hyper-elliptic curves and Galois groups of their coefficient polynomials

難波　完爾

719-1117 岡山県総社市北溝手 463-3

tel/fax. 0866-90-1886

2009. 12. 27

この論説では、何個かの種数 4 の超楕円曲線の終結変換多項式とその係数多項式のガロア群について述べる。

1. 記号と定義

f(x)を有理係数の 9 次多項式とし、これに対応する種数 4 の超楕円曲線

$$C:\quad y^2 = f(x) = x^9+a_1x^8+a_2x^7+a_3x^6+a_4x^5+a_5x^4+a_6x^3+a_7x^2+a_8x+a_9$$

および次のように終結式で定義された関数

$$f_1(u) = f(x) ⓧ x+u,\ f_2(u,v) = f(x) ⓧ x^2+ux+v,\ f_3(u,v,w) = f(x) ⓧ x^3+ux^2+vx+w,$$

$$f_4(u,v,w,) = f(x) ⓧ x^4+ux^3+vx^2+wx+t$$

を考える。これらは f(x)のチルンハウス変換(Tschirnhaus　transformation)と呼ばれる。ここで、f(x)と g(x)の変数 x に関する終結式(resultant)を、一時的省略記法として、次のように略記する：

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

ただし、記号ⓧの結合力(adhesiveness)は、通常の四則(+, -, ×, /)などより弱いものとする。従って、例えば、次のような交換や結合の法則などが成立する。

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

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

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

$$f(x) = g(x) \mod h(x) \rightarrow f(x) ⓧ h(x) = g(x) ⓧ h(x)$$

$$f(x) ⓧ x-y = f(y)$$

また、(a/p)をルジャンドルの記号とする。つまり、

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

とする。このとき、f(x)のチルンハウス変換のルジャンドル和

$$a_p = \sum x\in p\ (f_1(x)/p),\ b_p = \sum x,y\in p\ (f_2(x,y)/p),\ c_p = \sum x,y,z\in p\ (f_3(x,y,z)/p),$$

$$d_p = \sum_{x,y,z,t \in p} \left(f_4(x,y,z,t)/p \right)$$

を考え、これで定まる 8 次多項式

$$\bar{f}(x) = x^8 + a_p x^7 + b_p x^6 + c_p x^5 + d_p x^4 + p c_p x^3 + p^2 b_p x^2 + p^3 a_p x + p^4$$

を f(x) の終結変換多項式 (*resultant transformation*) といい、$\bar{f}(x) = 0$ を終結変換方程式という。終結変換多項式は各素数に対応した素体 (prime field)

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

に対応して定義される。志村-谷山理論によって終結根 (= 終結方程式の解) の絶対値は $\sqrt{p}$ の複素数であることが知られている。終結根は常に

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

の形の複素数であるから、$|u| \leq 2\sqrt{p}$ の実数が存在して

$$\bar{f}(x) = 0,\ x^2 + ux + p = 0$$

が共通根をもつ。従って、

$$\bar{f}(x) ⓧ x^2 + ux + p = p^4 (u^4 - a_p u^3 + (b_p - 4p) u^2 + (3pa_p - c_p) u + d_p - 2pb_p + 2p^2)^2$$

のように表現できる。この平方根部分

$$\underline{f}(u) = u^4 - a_p u^3 + (b_p - 4p) u^2 + (3pa_p - c_p) u + d_p - 2pb_p + 2p^2$$

を f(x) の係数多項式 (*coefficient polynomial*) という。係数方程式、係数根等は同様とする。係数根は常に実数での絶対値は $2\sqrt{p}$ に等しいか小さい。

$$a = a_p/\sqrt{p}\ ,\ b = b_p/p,\ c = c_p/p\sqrt{p}\ ,\ d = d_p/p^2$$

とおいた多項式

$$\underline{f}(u) = u^4 - au^3 + (b-4) u^2 + (3a-c) u + d - 2b + 2$$

を f(x) の標準係数多項式 (*normalized coefficient polynomial*) という。標準係数方程式の解、つまり、標準係数根の絶対値は 2 以下の実数である。係数方程式は常に種数と同じ次数であり、今の場合は 4 次で常にガロア群が可解 (solvable) な最大の場合である。係数多項式 $\underline{f}(x)$ のガロア群は当然 f(x) の代数的な性質を何らかの意味で引き継いだものとなっているはずである。

ここで、仮称であるが、差商 (difference quotient) の概念にふれる。多項式 f(x) の差商とは差の商

$$(f(x) - f(y)) / (x - y)$$

で定義される対称式である。当然、差商の概念は繰り返すことができる。しかし、これは交代行列の商として表現できる対称式なので、行列式的な表現をする。

$$f|g(x,y) = \begin{vmatrix} f(x) & f(y) \\ g(x) & g(y) \end{vmatrix} \Big/ \begin{vmatrix} 1 & 1 \\ x & y \end{vmatrix}$$

$$f|g|h(x,y,z) = \begin{vmatrix} f(x) & f(y) & f(z) \\ g(x) & g(y) & g(z) \\ h(x) & h(y) & h(z) \end{vmatrix} \Big/ \begin{vmatrix} 1 & 1 & 1 \\ x & y & z \\ x^2 & y^2 & z^2 \end{vmatrix}$$

などと定義する。上記の省略記法を用いれば、$1|f$, $1|x|f$ などである。

例えば f が多項式

$$f(x) = x^4+ax^3+bx^2+cx+d$$

のときには

$$1|f(x,y) = x^3+x^2y+xy^2+y^3+(x^2+xy+y^2)a+(x+y)b+c$$

であり、x,y の 3 次対称式である。これは所謂楕円曲線である。特に、f(x) が(標準)係数多項式のとき、(標準)係数楕円曲線(*coefficient elliptic curve*)という。相異なる係数根を座標とする点は係数楕円曲線上の点である。

また、$x+y = u$, $x-y = v$ とおけば

$$2u^3+3au^2+4bu+2v^2u+av^2+4c = 0$$

あるいは、$x+y = s$, $xy = t$ とおけば、

$$(1|f(x,y) \textcircled{y}\ u-x-y) \textcircled{x} (t-xy \textcircled{y}\ u-x-y) = (u^3+au^2+(b-2v)u+c-va)^2 = 0$$

である。これは、

$$v = (u^3+au^2+bu+c)/(2u+a)$$

を意味している。また、

$$1|x|f(x,y,z) = x^2+y^2+z^2+xy+xz+yz+(x+y+z)a+b$$

は xyz-空間の楕円体面(ellipsoid)になっている。f(x) が係数多項式の場合に係数楕円曲面(*coefficient ellipsoid*)という。相異なる係数根を座標にもつ点は係数楕円曲面上にある。係数楕円曲面 S と立方体 $T = [-2,2]^3$ の関係では S-T、つまり、係数楕円曲面 S の立方体 T の外の部分が連結でない場合もあり得る。

例 1.

$$C:\ y^2 = x^9-3x^8-2x^7-5x^6+4x^5-x^4+3x^3+2x^2-6x-4$$

この例は、p = 11 の場合の表現変換多項式(representation transformation polynomial)

$$\bar{a}_{12} = x^{(p+1)/4} F(7/12,11/12,1,1-x) = x^3$$

$$\bar{a}_{12}(x)[x]x^{10}-1$$

$$=$$

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

の場合の例である。これは、以下の論説にある多項式である：

難波完爾：種数 2 の楕円曲線と $\sin^2$-予想、

津田塾大学 数学・計算機科学研究所報 28,

第 17 回数学史シンポジウム (2006) p.141

この多項式は有理数体 Q 上既約であり、素体 F_{11} では

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

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

のように完全分解している。この場合判別式は

$$\det(f(x))=f(x) ⓧ f'(x)=2^{12}\cdot 17^2\cdot 14389\cdot 60817139$$

以下は終結変換多項式の係数のデータである：

$$[p, a_p, b_p, c_p, d_p]$$

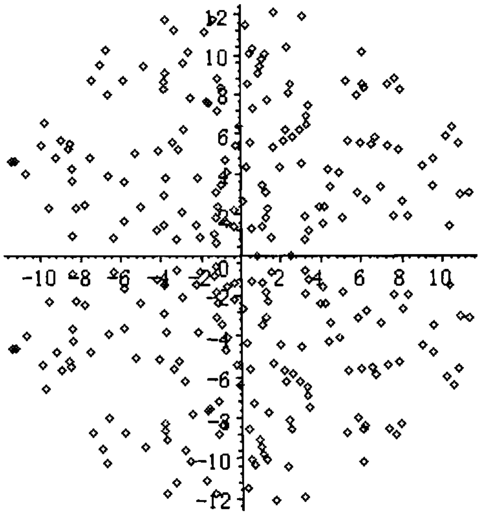
[[2, -1, -1, -3, -6], [3, -1, 1, -2, 12], [5, 5, 17, 43, 99], [7, 4, 20, 58, 186],
[11, 0, -4, 0, -74], [13, -1, 8, -33, 38], [17, -5, 0, 44, 0], [19, 4, 6, -31, -330],
[23, -3, 24, -55, 438], [29, -8, 50, -272, 1474], [31, -3, 33, 94, -148],
[37, 5, 26, 273, 1854], [41, -2, 24, 356, -1228], [43, -1, 39, -251, 2536],
[47, -1, 8, -101, 1290], [53, 5, 144, 705, 9842], [59, -4, 32, -62, 784],
[61, -25, 376, -4218, 37000], [67, 2, 42, 592, 2946], [71, -2, 4, 300, -6880],
[73, -14, 30, 726, -8986], [79, -1, 100, 262, 5702], [83, 8, 85, 498, 3560],
[89, 7, 84, 305, 3054], [97, 13, 191, 2465, 21825], [101, 4, 84, -306, -1800],
[103, -15, 139, -461, -1133], [107, 18, 259, 2994, 36240],

[109, -16, 196, -2996, 34124], [113, 4, 60, -324, 3350], [127, -13, 47, -96, 2312],
[131, 20, 256, 2884, 34990], [137, -12, 36, -733, 16700],
[139, -16, 303, -3778, 54640], [149, 11, 70, -57, -1278], [151, 3, 80, 699, 942]]

下の表は終結根のグラフである：

$$\bar{f}(x) = x^8+a_px^7+b_px^6+c_px^5+d_px^4+pc_px^3+p^2b_px^2+p^3a_px+p^4 = 0$$

$$p = 2 \sim 151$$



終結根の偏角の分布については、f(x)が非可解(non-solvable)のときには

$$\sin^2(\theta)+\sin^2(2\theta)+\sin^2(3\theta)+\sin^2(4\theta)$$

に比例するであろうというのが、種数 4 の超楕円曲線の場合の $\sin^2$-予想である。しかし、種数 1,2,3 の場合には、計算の複雑性の問題もあり、かなり質のよい資料もあって、

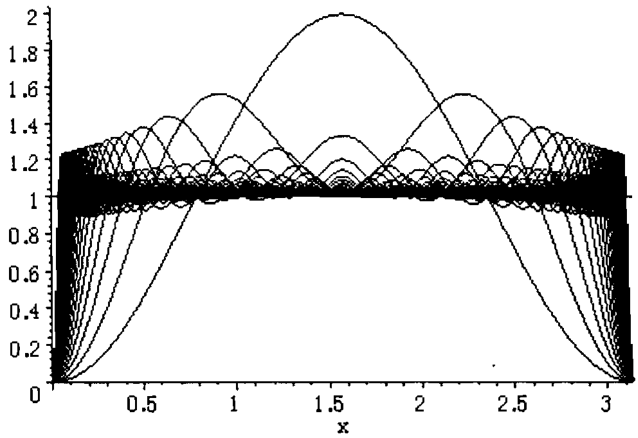
$$\sin^2(\theta)+\sin^2(2\theta),\quad \sin^2(\theta)+\sin^2(2\theta)+\sin^2(3\theta)$$

などに比例するという予想は確かであろうと推定するに十分と感じている。

種数 1,2,3 等では考察する多項式の次数も 3,5,7 と素数になっていることもあり、種数 4 の場合の多項式 f(x)の次数 9 は、当然のことながら、素数ではない。最初の自明でない 3 個の場合から一般の法則を推定することには慎重であるべきだと思う。そのような意味でも種数 4 というのは本質的(critical)な意味がある場合であると思っている。

次のグラフは $\sin^2(nx)$ の和の平均を示したものである：

$1/n\cdot(\sin^2(x)+\sin^2(2x)+\cdots+\sin^2(nx))$, $n = 0 \sim 40$



この図からも解るように、種数 g が大きくなったときの $\sin^2$-予想は一様分布に近づく。

以下は、上記超楕円曲線の $p < 100$ の場合の係数多項式の表である：

$[2, (x+1)(x^3-9x+6)]$, $[3, (x+3)(x^3-2x^2-5x+8)]$, $[5, x^4-5x^3-3x^2+32x-21]$,
$[7, x^4-4x^3-8x^2+26x+4]$, $[11, (x^2-4x-16)(x^2+4x-16)]$, $[13, x^4+x^3-44x^2-6x+168]$,
$[17, x^4+5x^3-68x^2-299x+578]$, $[19, x^4-4x^3-70x^2+259x+164]$,
$[23, x^4+3x^3-68x^2-152x+392]$, $[29, x^4+8x^3-66x^2-424x+256]$,
$[31, x^4+3x^3-91x^2-373x-272]$, $[37, x^4-5x^3-122x^2+282x+2668]$,
$[41, x^4+2x^3-140x^2-602x+166]$, $[43, x^4+x^3-133x^2+122x+2880]$,
$[47, x^4+x^3-180x^2-40x+4956]$, $[53, x^4-5x^3-68x^2+90x+196]$,
$[59, x^4+4x^3-204x^2-646x+3970]$, $[61, x^4+25x^3+132x^2-357x-1430]$,
$[67, x^4-2x^3-226x^2-190x+6296]$, $[71, x^4+2x^3-280x^2-726x+2634]$,
$[73, x^4+14x^3-262x^2-3792x-2708]$, $[79, x^4+x^3-216x^2-499x+2384]$,
$[83, x^4-8x^3-247x^2+1494x+3228]$, $[89, x^4-7x^3-272x^2+1564x+3944]$,
$[97, x^4-13x^3-197x^2+1318x+3589]$

上記の表では $p = 2, 3, 11$ のみ既約でなく、他の場合は既約多項式であり、$p \leq 151$ で既約な場合はすべてガロア群は $S(4) = 4!$ である。

平凡かも知れないが、複雑性が係数多項式にも継承されるであろうと云う意味で、次のように予想している：

予想・問題

C: $y^2 = f(x)$, 2n+1 次多項式 $f(x)$ が非可解のとき

その係数多項式 $\underline{f}(x)$ のガロア群は、一般には、S_n である

例外的な場合は何を意味するか。

標準係数多項式の解、つまり、標準係数方程式

$$\underline{f}(u) = u^4 - au^3 + (b-4)u^2 + (3a-c)u + d - 2b + 2 = 0$$

$$a = a_p/\sqrt{p},\ b = b_p/p,\ c = c_p/p\sqrt{p},\ d = d_p/p^2$$

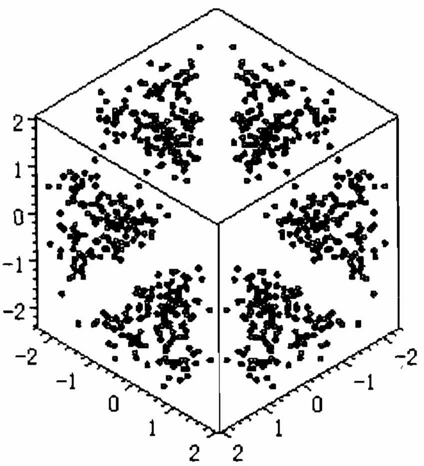
の 4 個の[-2,2]の解のうち、異なる 3 個の解を座標とする xyz-空間の点のグラフは次のようである。4 個の解を表示するには 4 次元の空間が必要であるが、表示が可能な 3 次元の空間への射影でしか表現ができなかったのである。

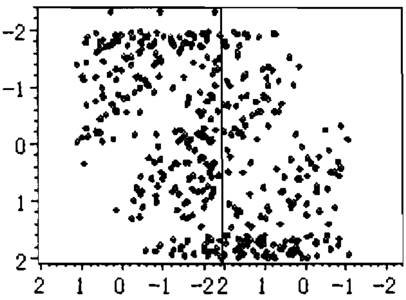
これも、異なる方向から見た図を二つ表示しておく。確かなことは、分布は空間的に一様ではないし、また、点、曲線、曲面など代数的に退化した多様体の上に正の密度で分布しているようでもない。しかし、このような分布多様体の全体像を確定するという「分布多様体問題」は基本的な問題である。

$$C:\quad y^2 = f(x) = x^9 - 3x^8 - 2x^7 - 5x^6 + 4x^5 - x^4 + 3x^3 + 2x^2 - 6x - 4$$

$$\underline{f}(u) = u^4 - au^3 + (b-4)u^2 + (3a-c)u + d - 2b + 2 = 0$$

$$p = 2 \sim 151$$





次は標準楕円曲線についてである。標準係数多項式は

$$\underline{f}(x) = x^4 - ax^3 + (b-4)x^2 + (3a-c)x + d - 2b + 2$$

であるから、標準楕円曲線は

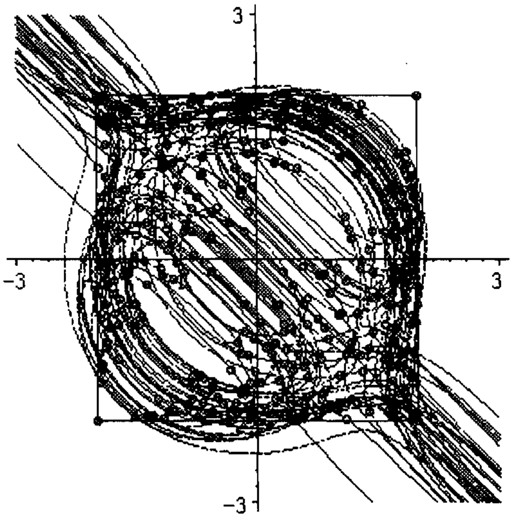
$$1|\underline{f}(x,y) = x^3 + x^2y + xy^2 + y^3 - a(x^2 + xy + y^2) + (b-4)(x+y) + (3a-c)$$

である。退化するものは p ＝ 11 の場合の $(x+y)(11x^2-48+11y^2) = 0$ のみである。$\det(f(x)) = 2^{12}\cdot 17^2\cdot 14389\cdot 60817139$ であるから、11 は判別式の約数ではないが例外的な挙動をしている。

$$C:\quad y^2 = f(x) = x^9 - 3x^8 - 2x^7 - 5x^6 + 4x^5 - x^4 + 3x^3 + 2x^2 - 6x - 4$$

$$1|\underline{f}(x,y) = x^3 + x^2y + xy^2 + y^3 - a(x^2 + xy + y^2) + (b-4)(x+y) + (3a-c)$$

$$p = 3 \sim 151$$



異なる標準根を座標にもつ点はこれらの楕円曲線上に分布しているのである。標準的な楕円曲線といえば、当然、

$$y^2 = \underline{f}(x) = x^4 - ax^3 + (b-4)x^2 + (3a-c)x + d - 2b + 2$$

あるいは

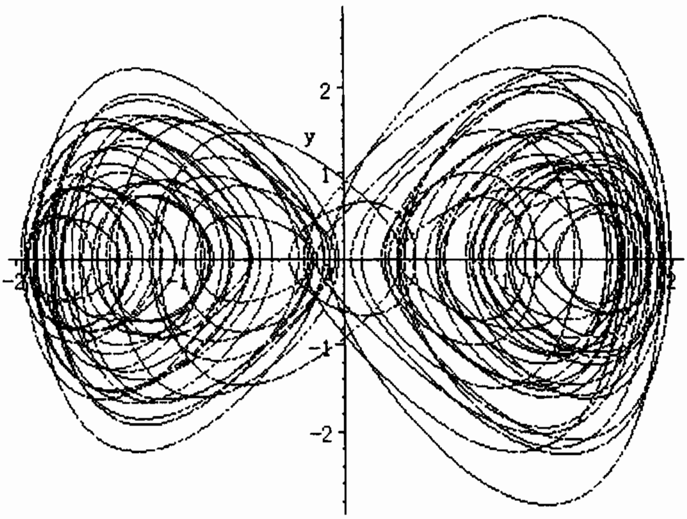
$$E:\quad y^2 = -\underline{f}(x) = -(x^4 - ax^3 + (b-4)x^2 + (3a-c)x + d - 2b + 2)$$

の方が、主役ではないかとの意見があると思う。当然のことである。これら2種類の楕円曲線は既約な場合にはどのように関連しているのであろうか。以下は切断面の x-座標が $[-2,2]$ にはいる $y^2 = -\underline{f}(x)$ の方のグラフを示しておく：

$$C:\quad y^2 = f(x) = x^9 - 3x^8 - 2x^7 - 5x^6 + 4x^5 - x^4 + 3x^3 + 2x^2 - 6x - 4$$

$$y^2 = -\underline{f}(x) = -(x^4 - ax^3 + (b-4)x^2 + (3a-c)x + d - 2b + 2)$$

$$p = 3 \sim 151$$



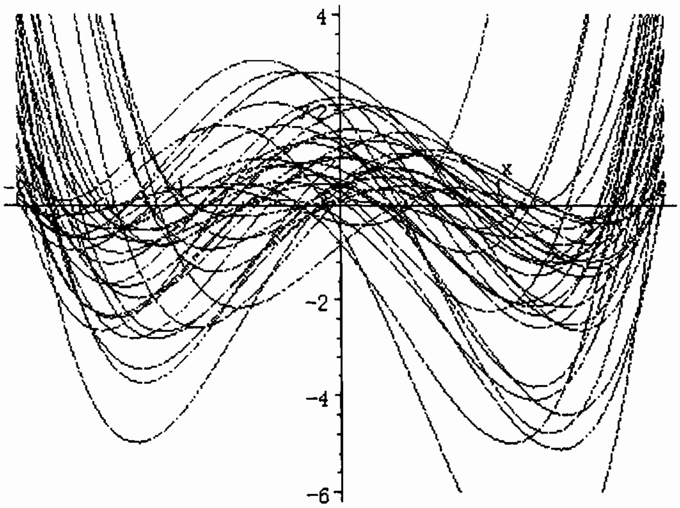
これらのグラフの y の上限には非自明な上限があるのであろうか。ここでは、特徴的な共通の通過点とか包絡線 (envelope) などは見当たらないのであるが…本当にそうなのであろうか。問題としては残しておこう。

もっと素朴に、そもそも、標準係数多項式のグラフについてはどうなのかという疑問も自然である。

$$C:\quad y^2 = f(x) = x^9 - 3x^8 - 2x^7 - 5x^6 + 4x^5 - x^4 + 3x^3 + 2x^2 - 6x - 4$$

$$y = f(x) = x^4 - ax^3 + (b-4)x^2 + (3a-c)x + d - 2b + 2$$

$$p = 3 \sim 151$$



例 2. 岡本多項式の一例

$$C:\quad y^2 = f(x) = x(x^8+8x^6+14x^4-35)$$

この場合 f(x)は既約ではない。$x^8+8x^6+14x^4-35$ は既約で、そのガロア群は [2^4]S(4)で位数は $384 = 2^7\cdot 3$ であり、判別式は

$$\det(f(x)) = f(x) ⓧ f'(x) = -2^{40}\cdot 5^5\cdot 7^7$$

この多項式は、

数学の風景 野海正俊・日比孝之(編), 野海正俊著、

パンルヴェ方程式-対称性からの入門、朝倉書店、p.72. 表 4. R_3

からの引用である。

以下は終結変換多項式の p < 100 の係数のデータである：

$$C:\quad y^2 = f(x) = x(x^8+8x^6+14x^4-35)$$

$$[p, a_p, b_p, c_p, d_p]$$

$$p = 2 \sim 97$$

[2, 0, -1, -2, -4], [3, 0, -1, 0, -8], [5, 0, -6, 0, 25], [7, 0, 7, 0, 0],
[11, 0, 10, 0, -6], [13, 4, 20, 92, 298], [17, -4, 12, -76, 582], [19, 0, 44, 0, 1192],
[23, 0, 31, 0, 1168], [29, -2, -11, -42, 1572], [31, 0, 0, 0, 0],
[37, 4, 10, 156, 594], [41, 6, 45, 108, 648], [43, 0, 39, 0, 456],
[47, 0, 20, 0, -602], [53, -12, 56, 148, -2416], [59, 0, 8, 0, -6000],
[61, -10, 25, -56, 2128], [67, 0, 27, 0, 3352], [71, 0, 92, 0, 3046],
[73, 20, 116, -740, -14822], [79, 0, 20, 0, 4602], [83, 0, 103, 0, 3720],
[89, -10, 45, 308, -3432], [97, -30, 546, -7590, 85058]

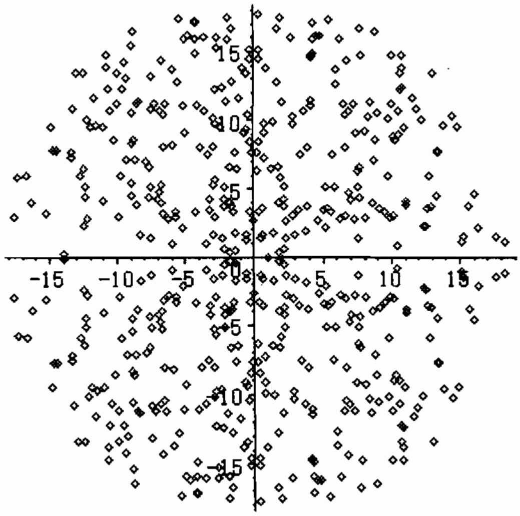
次のものは終結変換方程式の解の分布のグラフである：
分布の型が

$$\sin^2(\theta)+\sin^2(2\theta)+\sin^2(3\theta)+\sin^2(4\theta)$$

なのかどうか現時点では見当がつかない。可解でない場合の分布の類型の列挙という問題は大切であると思う。

$$\bar{f}(x)=x^8+a_px^7+b_px^6+c_px^5+d_px^4+pc_px^3+p^2b_px^2+p^3a_px+p^4=0$$

$$p=2\sim 347$$



また、係数方程式の因数分解の様子は次のようである：

$$C:\quad y^2=f(x)=x(x^8+8x^6+14x^4-35)$$

$$f(x)=x^4-ax^3+(b-4)x^2+(3a-c)x+d-2b+2$$

$$p=2\sim 97$$

$[2,\ x^4-9x^2+2x+8], [3,\ x^4-13x^2+16], [5,\ x^4-26x^2+135], [7,\ x^2(x^2-21)], [11,\ x^4-34x^2+16],$
$[13,\ x^4-4x^3-32x^2+64x+116], [17,\ x^4+4x^3-56x^2-128x+752], [19,\ x^4-32x^2+242],$
$[23,\ x^4-61x^2+800], [29,\ x^4+2x^3-127x^2-132x+3892], [31,\ x^4-124x^2+1922],$
$[37,\ (x-12)(x^3+8x^2-42x-216)], [41,\ x^4-6x^3-119x^2+630x+320], [43,\ x^4-133x^2+800],$
$[47,\ (x^2+16x+44)(x^2-16x+44)], [53,\ x^4+12x^3-156x^2-2056x-2734], [59,\ x^4-228x^2+18],$
$[61,\ x^4+10x^3-219x^2-1774x+6520], [67,\ x^4-241x^2+8712], [71,\ x^4-192x^2+64],$
$[73,\ x^4-20x^3-176x^2+5120x-21100], [79,\ x^4-296x^2+13924], [83,\ x^4-229x^2+400],$
$[89,\ x^4+10x^3-311x^2-2978x+4400], [97,\ x^4+30x^3+158x^2-1140x-2048]$

このように、f(x)の代数的性質が、係数方程式の可約性や既約な場合のガロア群の構造に反映していることが解る。

以下の表は既約な場合のガロア群と素数の表である：

$$p \le 347$$

$$S(4) = 4!$$

[2, 13, 17, 29, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149,
173, 181, 193, 197, 229, 233, 241, 257, 269, 277, 281, 293, 313, 317, 337]

$$D(4) = 2\times4$$

[5, 19, 23, 43, 59, 67, 107, 127, 131, 139, 163, 199, 251, 263, 271, 311, 347]

$$E(4) = 2\times2$$

[3, 11, 71, 79, 83, 103, 151, 167, 191, 211, 223, 227, 239, 283, 307, 331]

$$C(4) = 4$$

[31]

調べた範囲は $p \le 347$ で、この範囲素数が 69 個あり、5 個の可約な場合

[7, $x^2(x^2-21)$], [37, $(x-12)(x^3+8x^2-42x-216)$], [47, $(x^2+16x+44)(x^2-16x+44)$]
[157, $(x^2-30x+136)(x^2+20x-114)$], [179, $(x^2+6x-300)(x^2-6x-300)$],

がある。可約なものが有限個なのか無限個なのかも面白い問題である。全体の個数は

可約	S(4)	A(4)	E(4)	D(4)	C(4)	総数
5	30	0	17	16	1	69

のようである。A(4), C(4) は例外的で、可約なものが有限個であるか無限個なのか予想できない。出現頻度は

$$S(4) = 1/2,\ E(4) = D(4) = 1/4$$

であろうと予想される。また、

予想

A(4), C(4)

は、$p = 31$ の C(4) を除いて出現しない。$p = 31$ では標準係数多項式は

$$x^4-4x^2+2,\ \det = 2^{11}$$

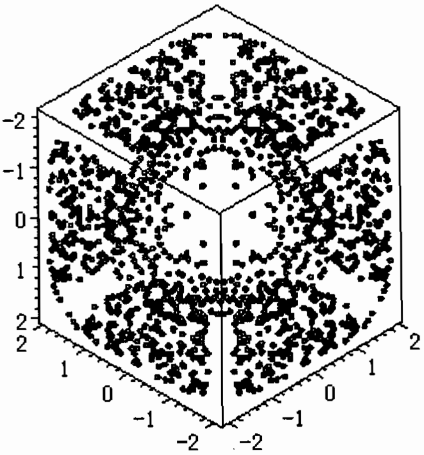
のように極めて特徴的な多項式である。

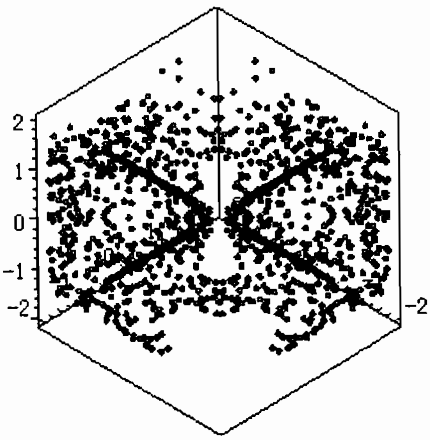
以下に標準係数根の xyz-空間でのグラフを、異なる方向からの図としてあげる。直線に見えるのは平面が退化した方向から見ているからである。正の密度でその上に点が分布していることが解る。

$$C: \quad y^2 = f(x) = x\,(x^8+8x^6+14x^4-35)$$

$$\underline{f}(x) = x^4-ax^3+(b-4)\,x^2+(3a-c)\,x+d-2b+2 = 0$$

$$p = 2 \sim 347$$





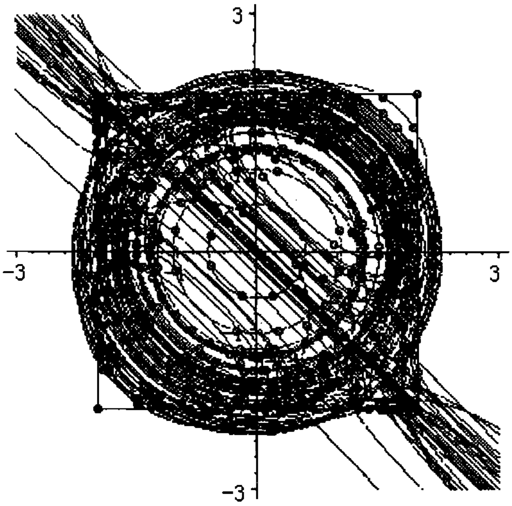
標準楕円曲線についても図示しておく：

今回は、濃い図であるがかなり特徴的な性質が見える。

$$C: \quad y^2 = f(x) = x\,(x^8+8x^6+14x^4-35)$$

$$1|\underline{f}(x,y) = x^3+x^2y+xy^2+y^3-a\,(x^2+xy+y^2)+(b-4)\,(x+y)+(3a-c)$$

$$p = 2 \sim 347$$



形式的な標準係数楕円曲線が退化して直線 x+y ＝ 0 と円に分解する場合が多く存在する。

[3, 5, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, 167, 179, 191, 199, 211, 223, 227, 239, 251, 263, 271, 283, 307, 311, 331, 347]

である。S(4)になる場合は退化せず

D(4)

[5, 19, 23, 43, 59, 67, 107, 127, 131, 139, 163, 199, 251, 263, 271, 311, 347]

E(4)

[3, 11, 71, 79, 83, 103, 151, 167, 191, 211, 223, 227, 239, 283, 307, 331]

の場合は退化している。p = 31 の C(4)の場合は

$$(x+y)(y^2+x^2-4)$$

であり、正方形$[-2,2]^2$に内接している。また、

$$[7,\ x^2(x^2-21)],\ [47,\ (x^2+16x+44)(x^2-16x+44)],$$

$$[179,\ (x^2+6x-300)(x^2-6x-300)]$$

の場合は含まれるが

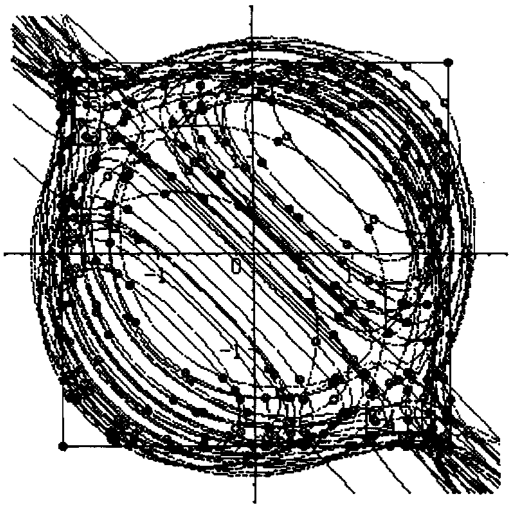
$$[37,\ (x-12)(x^3+8x^2-42x-216)],\ [157,\ (x^2-30x+136)(x^2+20x-114)],$$

の場合は退化しない。

$$C:\ \ y^2 = f(x) = x(x^8+8x^6+14x^4-35)$$

$$1|\underline{f}(x,y) = x^3+x^2y+xy^2+y^3-a(x^2+xy+y^2)+(b-4)(x+y)+(3a-c)$$

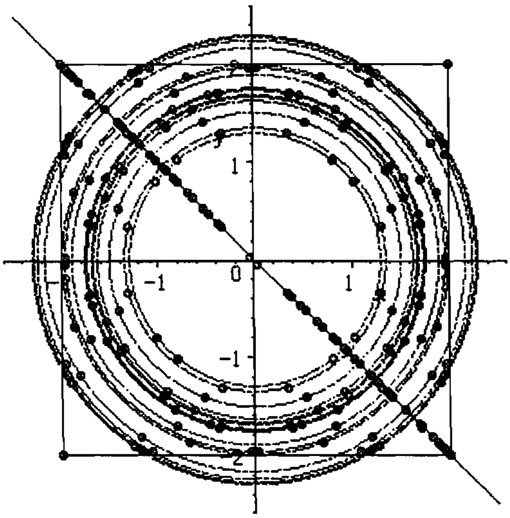
$$p = 2 \sim 347,\ gal = S(4)$$



C: $y^2 = f(x) = x(x^8+8x^6+14x^4-35)$

$1|\underline{f}(x,y) = x^3+x^2y+xy^2+y^3-a(x^2+xy+y^2)+(b-4)(x+y)+(3a-c)$

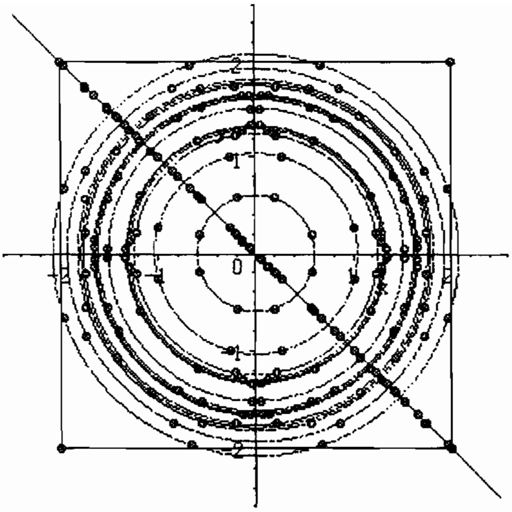
$p = 2 \sim 347$, gal = D(4)



C: $y^2 = f(x) = x(x^8+8x^6+14x^4-35)$

$1|\underline{f}(x,y) = x^3+x^2y+xy^2+y^3-a(x^2+xy+y^2)+(b-4)(x+y)+(3a-c)$

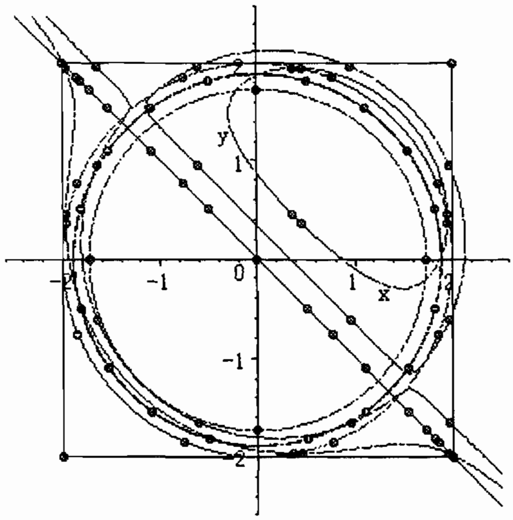
$p = 2 \sim 347$, gal = E(4)



$$C:\quad y^2 = f(x) = x(x^8+8x^6+14x^4-35)$$

$$l|\underline{f}(x,y) = x^3+x^2y+xy^2+y^3-a(x^2+xy+y^2)+(b-4)(x+y)+(3a-c)$$

$$p = 7, 31, 37, 47, 157, 179$$

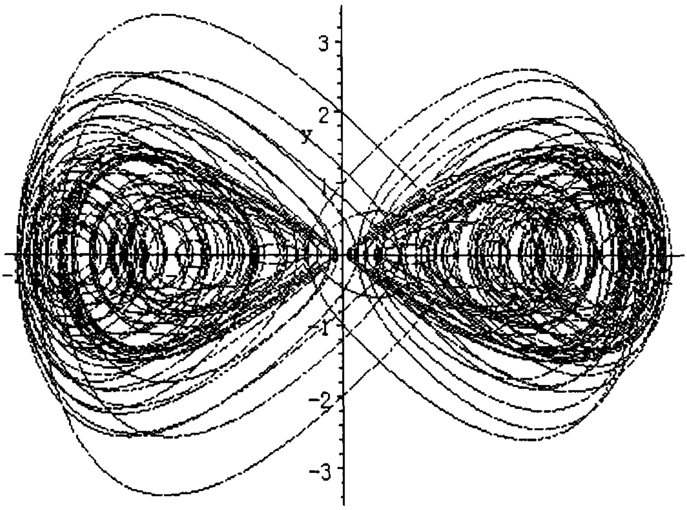


以下の図は、$y^2 = -\underline{f}(x)$の形の標準楕円曲線である：

$$C:\quad y^2 = f(x) = x(x^8+8x^6+14x^4-35)$$

$$y^2 = -\underline{f}(x) = -(x^4-ax^3+(b-4)x^2+(3a-c)x+d-2b+2)$$

$$p = 2 \sim 347$$



例 3.

$$C: \quad y^2 = x(x^2-1)(x^6+1)$$

$$\det = -2^{12} \cdot 3^6$$

この例は、可約なもので終結方程式の根(= 終結根)が純虚数や実数になる確率が正のものである。

$[p, a_p, b_p, c_p, d_p]$

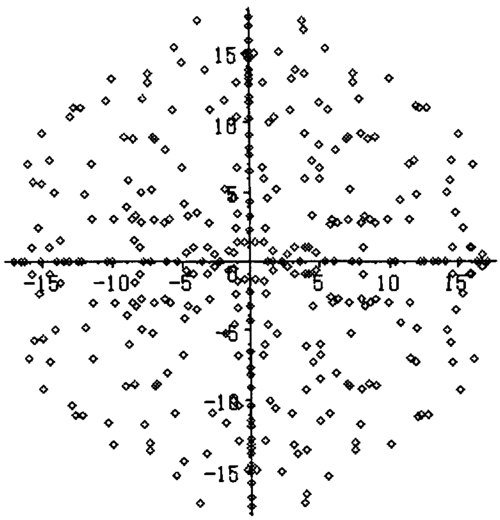
[[2, 0, 0, -2, -3], [3, 0, -2, 0, 9], [5, 0, 0, 0, -50], [7, 0, -4, 0, -26],
[11, 0, 4, 0, -154], [13, 4, 4, -52, -442], [17, -4, -24, -12, 910],
[19, 0, 4, 0, -570], [23, 0, -4, 0, -730], [29, 16, 64, -464, -5394],
[31, 0, 28, 0, 966], [37, -4, 4, 148, -3034], [41, -4, -56, -44, 4590],
[43, 0, 36, 0, -602], [47, 0, 28, 0, -1274], [53, -16, 64, 848, -12402],
[59, 0, 36, 0, -2714], [61, -20, 100, 1220, -19642], [67, 0, 4, 0, -8442],
[71, 0, -68, 0, 5350], [73, 16, 60, 1136, 20006], [79, 0, -164, 0, 18054],
[83, 0, 36, 0, -7802], [89, -4, -216, 84, 28654], [97, 16, 92, 1776, 31430],
[101, -16, 64, 1616, -33330], [103, 0, 252, 0, 31846], [107, 0, 36, 0, -15194],
[109, 4, 4, -436, -24634], [113, 28, 520, 7700, 96078], [127, 0, 284, 0, 46150],
[131, 0, 324, 0, 50566], [137, -36, 712, -11916, 163950], [139, 0, 36, 0, -28634],
[149, -32, 256, 4768, -120690], [151, 0, 188, 0, 48166],
[157, -20, 100, 3140, -80698], [163, 0, 324, 0, 52486], [167, 0, 92, 0, -23002],
[173, 0, 0, 0, -59858], [179, 0, 196, 0, 6086], [181, -12, 36, 2172, -78554],
[191, 0, 764, 0, 218886], [193, 8, -516, -584, 151430],

[197, -16, 64, 3152, -102834], [199, 0, 508, 0, 133350], [211, 0, 4, 0, -87354],
[223, 0, 668, 0, 198598], [227, 0, 100, 0, -57658], [229, 20, 100, -4580, -150682],
[233, -68, 2344, -56236, 1000110], [239, 0, -196, 0, -3130],
[241, -16, -164, -2032, 160006], [251, 0, 4, 0, -123994],
[257, -4, -888, 756, 333070], [263, 0, 92, 0, 10406],
[269, -48, 576, 12912, -454610], [271, 0, 92, 0, 139654],
[277, 52, 676, -14404, -527962], [281, -4, -984, 852, 404206],
[283, 0, 484, 0, 113766], [293, -16, 64, 4688, -209202],
[307, 0, 196, 0, -68154], [311, 0, 284, 0, 34406]]

$$C:\quad y^2 = x(x^2-1)(x^6+1)$$

$$\bar{f}(x) = x^8+a_px^7+b_px^6+c_px^5+d_px^4+pc_px^3+p^2b_px^2+p^3a_px+p^4 = 0$$

$$p = 2 \sim 311$$



この場合、係数方程式の可約性や既約な場合のガロア群については次のようである。

[2, (x-1)(x³+x²-7x-5)], [3, x⁴-14x²+39], [5, x²(x²-20)], [7, x⁴-32x²+128],
[11, x²(x²-40)], [13, (x²-52)(x-2)²], [17, (x+8)²(x-6)²], [19, x²(x²-72)],
[23, x⁴-96x²+512], [29, (x²-116)(x-8)²], [31, x⁴-96x²+1152],
[37, (x²-148)(x+2)²], [41, (x²+2x-112)²], [43, x²(x²-136)], [47, x⁴-160x²+512],
[53, (x²-212)(x+8)²], [59, x²(x²-200)], [61, (x²-244)(x+10)²], [67, x²(x²-264)],
[71, x⁴-352x²+25088], [73, (x²-8x-148)²], [79, x⁴-480x²+56448], [83, x²(x²-296)],
[89, (x+18)²(x-16)²], [97, (x+10)²(x-18)²], [101, (x²-404)(x+8)²],

[103, x^4-160x^2+1152], [107, $x^2(x^2-392)$], [109, $(x^2-436)(x-2)^2$],
[113, $(x^2-14x-64)^2$], [127, x^4-224x^2+6272], [131, $x^2(x^2-200)$],
[137, $(x^2+18x-80)^2$], [139, $x^2(x^2-520)$], [149, $(x^2-596)(x+16)^2$],
[151, $x^4-416x^2+36992$], [157, $(x^2-628)(x+10)^2$], [163, $x^2(x^2-328)$],
[167, x^4-576x^2+2048], [173, $x^2(x^2-692)$], [179, $x^2(x^2-520)$],
[181, $(x^2-724)(x+6)^2$], [191, x^4], [193, $(x^2-4x-652)^2$], [197, $(x^2-788)(x+8)^2$],
[199, $x^4-288x^2+10368$], [211, $x^2(x^2-840)$], [223, x^4-224x^2+128], [227, $x^2(x^2-808)$],
[229, $(x^2-916)(x-10)^2$], [233, $(x^2+34x+128)^2$], [239, $x^4-1152x^2+204800$],
[241, $(x^2+8x-596)^2$], [251, $x^2(x^2-1000)$], [257, $(x+32)^2(x-30)^2$],
[263, $x^4-960x^2+100352$], [269, $(x^2-1076)(x+24)^2$], [271, $x^4-992x^2+236672$],
[277, $(x^2-1108)(x-26)^2$], [281, $(x^2+2x-1056)^2$], [283, $x^2(x^2-648)$],
[293, $(x^2-1172)(x+8)^2$],[307, $x^2(x^2-1032)$],[311, $x^4-960x^2+51200$]

などである。

可約なものは $x^2(x^2-a)$, $(x+a)^2(x^2-b)$, $(x^2+ax+b)^2$ の形に分類される。以下はその型と対応する素数の表である。

$x^2(x^2-a)$

[5, 11, 19, 43, 59, 67, 83, 107, 139, 163, 173, 179, 191, 211, 227, 251, 283, 307]

$(x+a)^2(x^2-b)$

[13, 29, 37, 53, 61, 101, 109, 149, 157, 181, 197, 229, 269, 277, 293]

$(x^2+ax+b)^2$

[17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 281]

既約なもののガロア群は

D(4):8

[3, 23, 47, 71, 103, 167, 223, 239, 363, 271, 311]

C(4):4

[7,31,79,127,151,199]

で、E(4),A(4),S(4)は登場しない。D(4),C(4)の出現頻度の比は 2:1 であろうか。A(4)はここでも登場していない。

型	$x^2(x^2-a)$	$(x+a)^2(x^2-b)$	$(x^2+ax+b)^2$	S(4)	A(4)	E(4)	D(4)	C(4)
個数	18	15	11	0	0	0	11	6

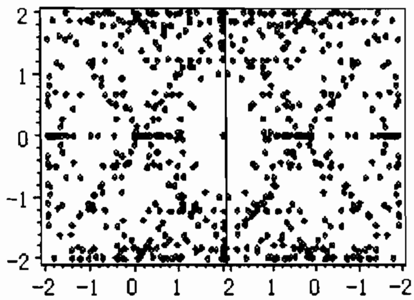
以下は係数根(= 標準係数方程式の解)の分布図である。3 次元空間に射影

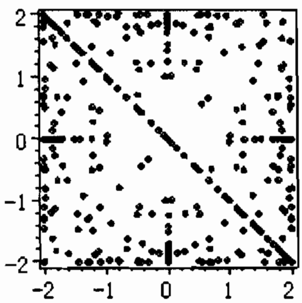
したものを、視点を変えて2例示しておく。

$$C:\quad y^2 = x(x^2-1)(x^6+1)$$

$$x^4-ax^3+(b-4)x^2+(3-c)x+2+d-2b = 0$$

$$p = 2 \sim 311$$

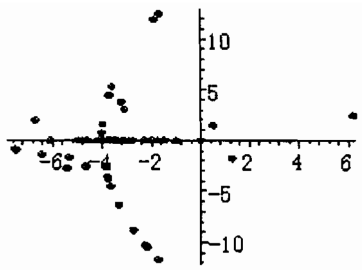




また、次の図は、標準係数多項式の係数[-a,b-4,3a-c]を 3 次元空間内の点集合として表示したものである。

$$[-a, b-4, 3a-c]$$

$$p = 2 \sim 311$$



明かな曲線群が見られる。しかし、すべての点が何個かの曲面や曲線上に分布しているというところまでは詰められてはいない。

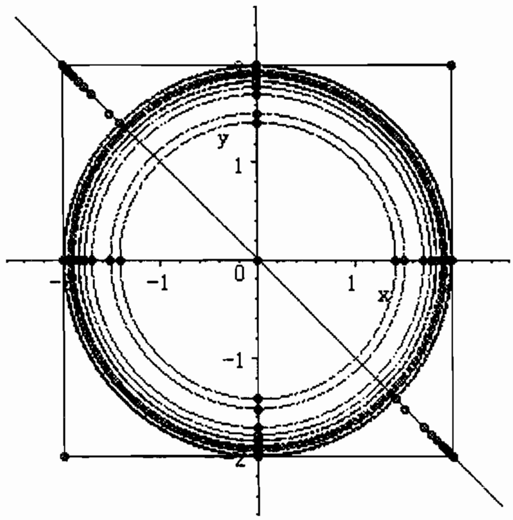
さて、形式的標準楕円曲線については次のようである：

$$x^2(x^2-a)$$

$$1|\underline{f}(x,y)=x^3+x^2y+xy^2+y^3-a(x^2+xy+y^2)+(b-4)(x+y)+(3a-c)$$

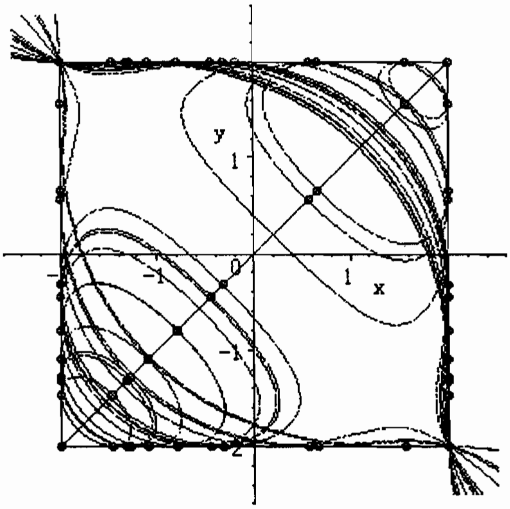
$$=k(x+y)(x^2+y^2-h)=0$$

[5, 11, 19, 43, 59, 67, 83, 107, 139, 163, 173, 179, 191, 211, 227, 251, 283, 307]



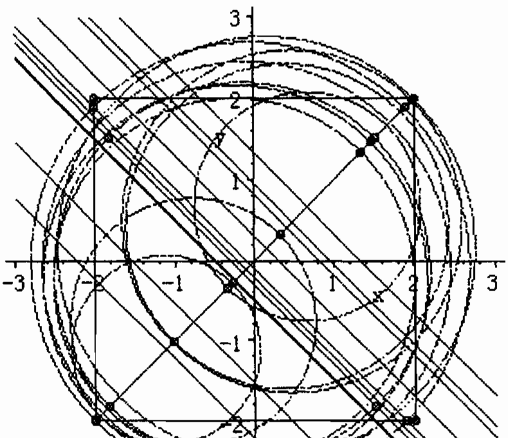
$$(x+a)^2(x^2-b)$$

[13, 29, 37, 53, 61, 101, 109, 149, 157, 181, 197, 229, 269, 277, 293]



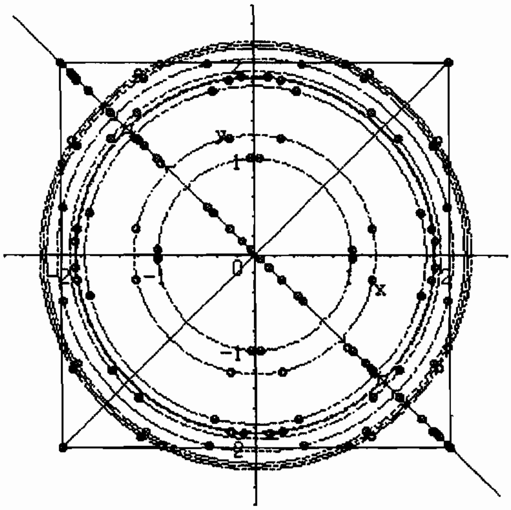
$(x^2+ax+b)^2$

[17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 281]



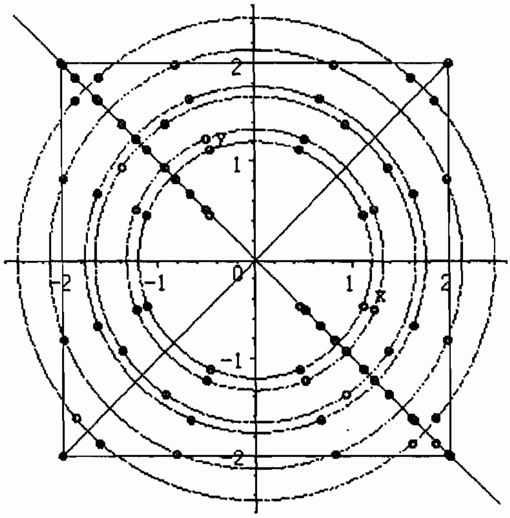
D(4):8

[3, 23, 47, 71, 103, 167, 223, 239, 363, 271, 311]



C(4):4

[7,31,79,127,151,199]



以下の考察は、標準係数多項式に関する 4 次の曲線ついてである。最も簡単なものは f(x)の和

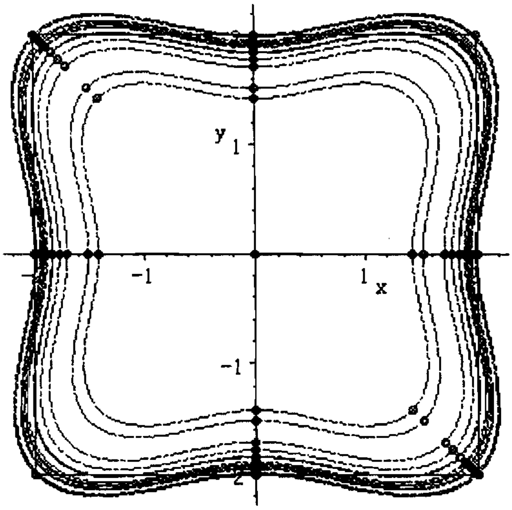
$$f(x)+f(y)$$

である。このような簡潔な対称式から何が導かれるのか疑問に思うのであるがなかなか美しい世界を見せてくれるのである。

$$x^2(x^2-a)$$

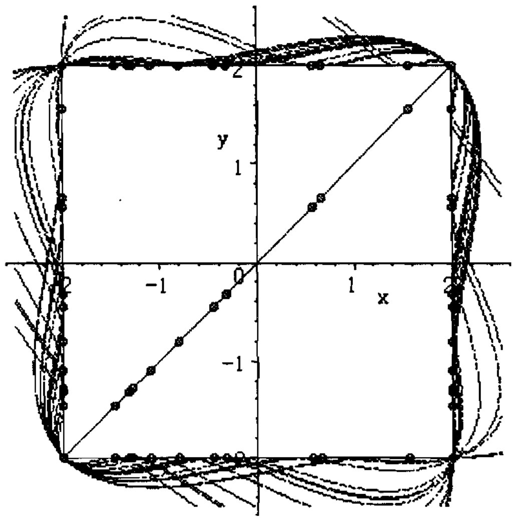
$$f(x)+f(y)=(x^4+y^4)-a(x^3+y^3)+(b-4)(x^2+y^2)+(3-c)(x+y)+2(2+d-2b)=0$$

[5, 11, 19, 43, 59, 67, 83, 107, 139, 163, 173, 179, 191, 211, 227, 251, 283, 307]



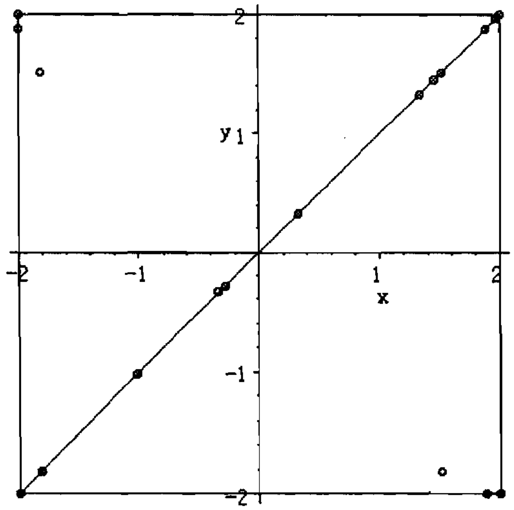
(x+a)²(x²-b)

[13, 29, 37, 53, 61, 101, 109, 149, 157, 181, 197, 229, 269, 277, 293]



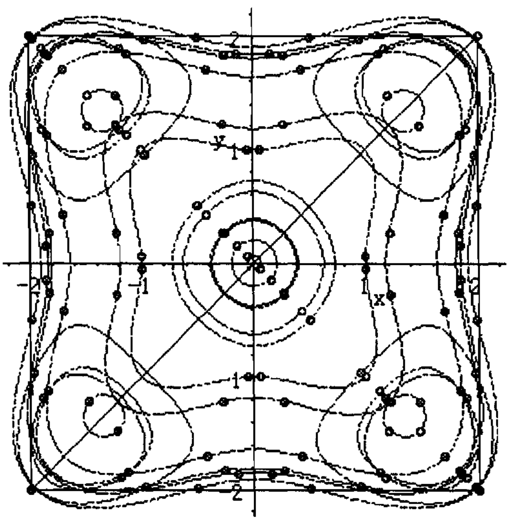
(x²+ax+b)²

[17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 281]



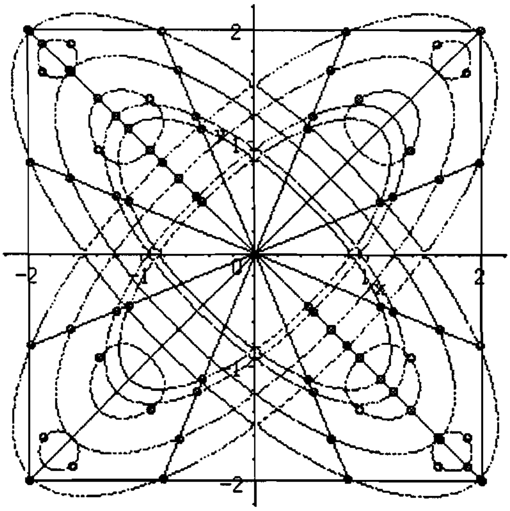
D(4):8

[3, 23, 47, 71, 103, 167, 223, 239, 363, 271, 311]



C(4):4

[7,31,79,127,151,199]



例 1. チェビシェフ多項式

$$C: \quad y^2 = x(x^2-3)(x^6-6x^4+9x^2-3)$$

$$\det = 2^8 \cdot 3^{18}$$

この例では、係数多項式はすべて可約である。

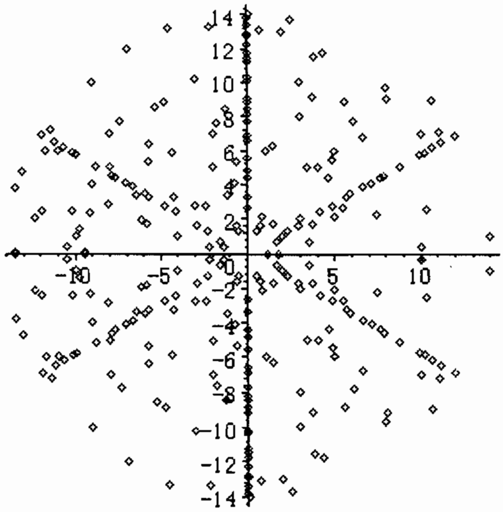
$[p, a_p, b_p, c_p, d_p]$

[[2, 0, -1, -1, -4], [3, 0, 0, 0, 0], [5, -4, 5, 20, -80], [7, 0, 7, 0, 0],
[11, 0, 11, 0, 0], [13, -6, 13, -78, 468], [17, 8, 20, -40, -410],
[19, 0, 76, 0, 2166], [23, 0, 23, 0, 0], [29, 4, 29, -116, -464], [31, 0, 31, 0, 0],
[37, -8, 28, 232, -2378], [41, -8, 41, 328, -2624], [43, 0, 43, 0, 0],
[47, 0, 47, 0, 0], [53, 16, 164, 1072, 7414], [59, 0, 59, 0, 0],
[61, -10, 61, -610, 6100], [67, 0, 67, 0, 0], [71, 0, 284, 0, 30246],
[73, 24, 364, 4200, 39750], [79, 0, 79, 0, 0], [83, 0, 83, 0, 0],
[89, 40, 596, 3832, 17542], [97, 18, 97, 1746, 31428],
[101, 20, 101, -2020, -40400], [103, 0, 103, 0, 0], [107, 0, 428, 0, 68694],
[109, 24, 220, 3336, 52566], [113, 16, 113, -1808, -28928],
[127, 0, 508, 0, 96774], [131, 0, 131, 0, 0], [139, 0, 139, 0, 0],
[149, -20, 149, 2980, -59600], [151, 0, 151, 0, 0], [157, 22, 157, 3454, 75988],
[163, 0, 652, 0, 159414], [167, 0, 167, 0, 0], [173, -4, 173, 692, -2768],
[179, 0, 716, 0, 192246], [181, 72, 2524, 56664, 896118], [191, 0, 191, 0, 0],
[193, 14, 193, 2702, 37828], [197, 8, 20, -2056, -67946],
[199, 0, 796, 0, 237606]]

$$C: \quad y^2 = x(x^2-3)(x^6-6x^4+9x^2-3)$$

$$\bar{f}(x) = x^8+a_px^7+b_px^6+c_px^5+d_px^4+pc_px^3+p^2b_px^2+p^3a_px+p^4 = 0$$

$$p = 2 \sim 199$$



この場合、係数方程式の因数分解は次のようである。

[[2, x^4-9x^2+x+12], [3, x^4-12x^2+18], [5, $x^4+4x^3-15x^2-80x-280$], [7, x^4-21x^2-588], [11, x^4-33x^2-2420], [13, $x^4+6x^3-39x^2-156x-3588$], [17, $x^4-8x^3-48x^2+448x-11392$], [19, $(x^2-228)(x^2+228)$], [23, $x^4-69x^2-23276$], [29, $x^4-4x^3-87x^2+464x-47560$], [31, $x^4-93x^2-57660$], [37, $x^4+8x^3-120x^2-1120x-76304$], [41, $x^4+8x^3-123x^2-1312x-137104$], [43, $x^4-129x^2-155316$], [47, $x^4-141x^2-203228$], [53, $x^4-16x^3-48x^2+1472x-908320$], [59, $x^4-177x^2-403796$], [61, $x^4+10x^3-183x^2-1220x-440420$], [67, $x^4-201x^2-592548$], [71, $x^4-2822960$], [73, $x^4-24x^3+72x^2+1056x-3829104$], [79, $x^4-237x^2-973596$], [83, $x^4-249x^2-1129796$], [89, $x^4-40x^3+240x^2+6848x-9408448$], [97, $x^4-18x^3-291x^2+3492x-1775100$], [101, $x^4-20x^3-303x^2+8080x-2080600$], [103, $x^4-309x^2-2164236$], [107, $x^4-9708752$], [109, $x^4-24x^3-216x^2+4512x-5151312$], [113, $x^4-16x^3-339x^2+7232x-2889184$], [127, $x^4-16258032$], [131, $x^4-393x^2-4461860$], [139, $x^4-417x^2-5332596$], [149, $x^4+20x^3-447x^2-11920x-6631096$], [151, $x^4-453x^2-6840300$], [157, $x^4-22x^3-471x^2+6908x-7614500$], [163, $(x^2-5868)(x^2+5868)$], [167, $x^4-501x^2-9259148$], [173, $x^4+4x^3-519x^2-2768x-10298344$], [179, $x^4-45626384$], [181, $x^4-72x^3+1800x^2-17568x-164415888$], [191, $x^4-573x^2-13862780$], [193, $x^4-14x^3-579x^2+5404x-14265788$], [197, x^4-8x^3-768x^2+6784x-1542688], [199, x^4-62727984]]

可約なもの

[19, 163]

[19, (x^2-228) (x^2+228)], [163, (x^2-5868) (x^2+5868)]

既約なもののガロア群は

S(4)

[2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97,
101, 109, 113, 149, 157, 173, 181, 193, 197]

D(4)

[7, 11, 23, 31, 43, 47, 59, 67, 71, 79, 83,
103, 107, 127, 131, 139, 151, 167, 179, 191, 199]

C(4)

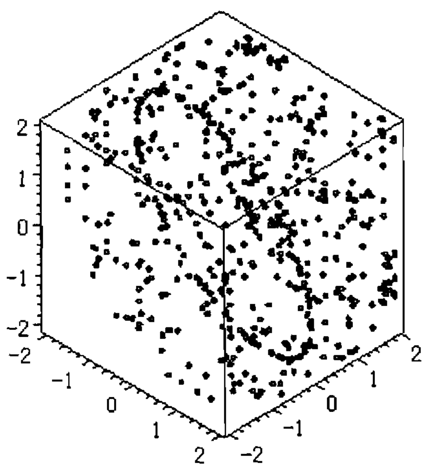
[3]

以下は係数根(= 標準係数方程式の解)の分布図である。3 次元空間に射影したものを例示しておく。

$$C: \quad y^2 = x(x^2-3)(x^6-6x^4+9x^2-3)$$

$$x^4-ax^3+(b-4)x^2+(3-c)x+2+d-2b = 0$$

$$p = 2 \sim 199$$



標準係数根が立方体に内接する円周上に正の確率で分布している様子が解る。

さて、形式的標準楕円曲線については次のようである：

[19, $(x^2-228)(x^2+228)$], [163, $(x^2-5868)(x^2+5868)$]

$$1|\underline{f}(x,y) = x^3+x^2y+xy^2+y^3-a(x^2+xy+y^2)+(b-4)(x+y)+(3a-c)$$

この場合は形式楕円曲線は

$$(y+x)(x^2+y^2) = 0$$

と、原点と直線に縮退してしまう。

S(4)

$$1|\underline{f}(x,y) = x^3+x^2y+xy^2+y^3-a(x^2+xy+y^2)+(b-4)(x+y)+(3a-c)$$

[2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97,
101, 109, 113, 149, 157, 173, 181, 193, 197]

しかし、このなかには[2,-2]を通らないものが幾つかある。

[5, 29, 41, 101, 113, 149, 173],

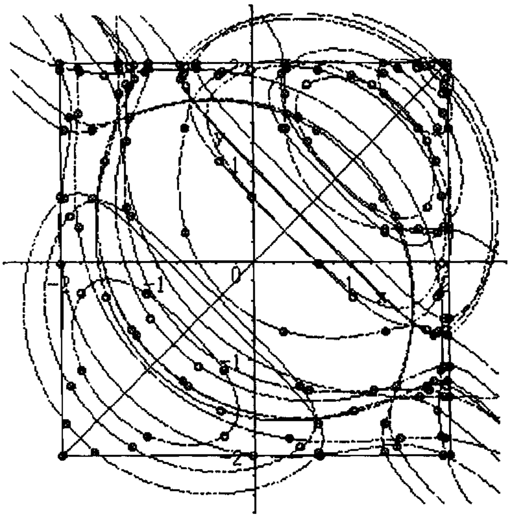
[13, 17, 37, 53, 61, 73, 89, 97, 109, 157, 181, 193, 197]

の二つに分かれる。

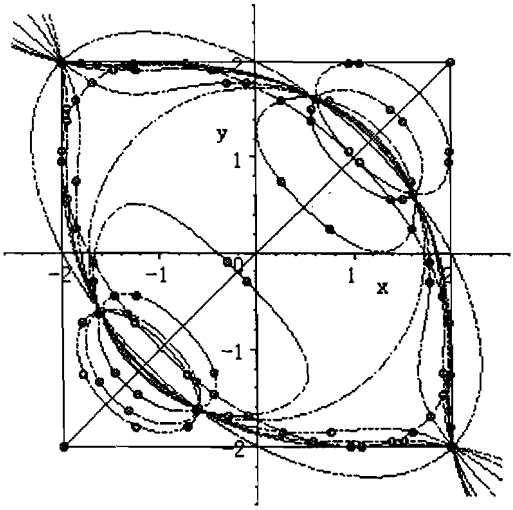
S(4)

$$1|\underline{f}(x,y) = x^3+x^2y+xy^2+y^3-a(x^2+xy+y^2)+(b-4)(x+y)+(3a-c)$$

[13, 17, 37, 53, 61, 73, 89, 97, 109, 157, 181, 193, 197]



[5, 29, 41, 101, 113, 149, 173]



これらの楕円曲線はすべて

$$x^2+xy+y^2=4,\ x^2+y^2=3$$

の4交点を共有する。また、これらの交点を通り $[-2,2]^2$ に内接する楕円

$$x^2+xy+y^2=3$$

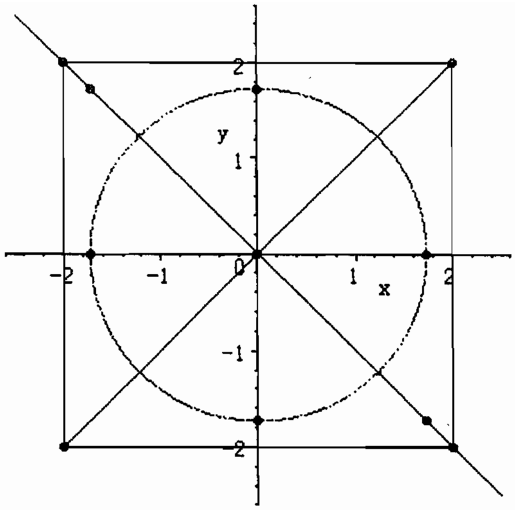
上に標準係数根の対を座標にもつ点が分布している。これが、最初の係数根のグラフに立方体に内接する円として“ぼんやり”見えていたものの一つの正体であろう。

D(4)

$$1|\underline{f}(x,y)=x^3+x^2y+xy^2+y^3-a(x^2+xy+y^2)+(b-4)(x+y)+(3a-c)$$

$$=(y+x)(x^2+y^2-3)$$

[7, 11, 23, 31, 43, 47, 59, 67, 71, 79, 83,
103, 107, 127, 131, 139, 151, 167, 179, 191, 199]



[71, 107, 127, 179, 199]

の場合は原点に縮退している。

4 次の対称曲線には商差 x|f もある。これについては、例はあげなかったが当然検討すべき対象である。これらの差商の曲線が、ガロア群の構造の反映としての図形に品位ある形をもって湧出してきたことに驚く。多様でありながら簡潔という感覚である。しかし、説明はできない…。

2. 指数の交換法則追記

このノートでは、第 17 回数学史シンポジウム(2006) p.117 余談のところで述べた、指数の交換法則

$$a\hat{}b = b\hat{}a$$

のときに出会った関数についての続きである。その関数は

$$f(x) = e^x(x/(e^x-1))+\log(x/(e^x-1))$$

という、偶関数である。ここに、

$$x/(e^x-1)$$

はベルヌーイ数の生成関数(=母関数)である。f(x)が偶関数であることは

$$e^x(x/(e^x-1))+\log(x/(e^x-1)) = -e^{-x}(x/(e^{-x}-1))+\log(-x/(e^{-x}-1))$$

である。この条件は

$$e^x(x/(e^x-1))+e^{-x}(x/(e^{-x}-1)) = \log(-x/(e^{-x}-1))-\log(x/(e^x-1))$$

と同値である。この、指数と対数で記述された共通の関数は何であろうか。左辺は

$$e^x(x/(e^x-1))+e^{-x}(x/(e^{-x}-1))=e^x(x/(e^x-1))-x/(e^x-1)=x(e^x-1)/(e^x-1)=x$$

右辺は

$$\log(-x/(e^{-x}-1))-\log(x/(e^x-1))=\log((-x/(e^{-x}-1))/(x/(e^x-1)))$$

$$=\log(-(e^x-1)/(e^{-x}-1))=\log(e^x)=x$$

であり、両辺ともに恒等関数 x になっている。

元の着想に戻って、この等式が如何にして導かれたのかの道筋を辿る。

$$x^y=y^x$$

に於いて、y = ax と仮定する。最初の条件から、

$$x^y = x\hat{}(ax) = (ax)\hat{}x = y^x$$

であり、従って、対数をとって、

$$ax\cdot\log(x)=\log(ax)\cdot x$$

であるが、$x\neq 0$ であるから、

$$a\cdot\log(x)=\log(a)+\log(x)$$

となり、従って

$$(a-1)\log(x)=\log(a)$$

である。log(a) = u とおくと、$a=e^u$ である。つまり、

$$\log(x)=\log(a)/(a-1)=u/(e^u-1)$$

となる。ここに、既に、u の代わりに x と記すが、ベルヌーイ数の母関数

$$x/(e^x-1)$$

が登場するのである。これは、本質的には $x\cdot\cot(\pi ix)$ なのである。

ともあれ、

$$\log(x)=\log(a)/(a-1)$$

から、

$$x=a\hat{}(1/(a-1)),\ y=ax=a\cdot a\hat{}(1/(a-1))=a\hat{}(a/(a-1))$$

である。また、当然のことながら、

$$x\hat{}y=a\hat{}(1/(a-1))\hat{}(a\hat{}(a/(a-1)))=a\hat{}(1/(a-1)\cdot a\hat{}(a/(a-1)))$$

$$=a\hat{}(a\hat{}(a/(a-1))/(a-1))$$

$$y\hat{}x=a\hat{}(a/(a-1))\hat{}(a\hat{}(1/(a-1)))=a\hat{}(a/(a-1)\cdot a\hat{}(1/(a-1)))$$

$$=a\hat{}(a\hat{}(a/(a-1))/(a-1))$$

から、指数交換法則 x^y = y^x となっている。関数、

$$f(x)=x\hat{}(x\hat{}(x/(x-1))/(x-1))$$

は、関数等式

$$f(x)=f(1/x)$$

を満足するのである。それには、$\log(f(x))$について示せばよいであろう。

$$\log(f(x))=(x^{\wedge}(x/(x-1))/(x-1)\cdot\log(x)$$

それは、

$$\log(f(1/x))=x^{\wedge}((-1/x)/(1/x-1))/(1/x-1)\cdot-\log(x)$$

$$=x^{\wedge}(1/(x-1))/((1-x)/x)\cdot-\log(x)$$

$$=x^{\wedge}(x/(x-1))/(1-x)\cdot-\log(x)=(x^{\wedge}(x/(x-1))/(x-1)\cdot\log(x)$$

によっても解る。また、

$$\log(\log(f(x)))=x\cdot\log(x)/(x-1)+\log(\log(x)/(x-1))$$

でもある。従って、$\log(x)/(x-1)$の代わりに、ベルヌーイ数の母関数$x/(e^x-1)$に関する表現と思うと

$$\log(\log(f(e^x)))=xe^x/(e^x-1)+\log(x/(e^x-1))$$

が、偶関数であるという性質になるのである。

さて、最初の性質

$$x^y=y^x \rightarrow x^{1/x}=y^{1/y}$$

から決まる関数は

$$x=a^{\wedge}(1/(a-1)),\ y=a^{\wedge}(a/(a-1))$$

のときどんな関数であろうか。

$$x^{1/x}=(a^{\wedge}(1/(a-1)))^{\wedge}(a^{\wedge}(-1/(a-1)))=a^{\wedge}(1/(a-1)\cdot a^{\wedge}(-1/(a-1)))$$

$$=a^{\wedge}(a^{\wedge}(-1/(a-1))/(a-1))$$

$$y^{1/y}=(a^{\wedge}(a/(a-1)))^{\wedge}(a^{\wedge}(-a/(a-1)))=a^{\wedge}(a/(a-1)\cdot a^{\wedge}(-a/(a-1)))$$

$$=a^{\wedge}(a^{\wedge}(-1/(a-1))/(a-1))$$

これらの式は当然等しい。

$$g(x)=x^{\wedge}(x^{\wedge}(-1/(x-1))/(x-1))$$

とおくと

$$\log(g(x))=x^{\wedge}(-1/(x-1))/(x-1)\cdot\log(x)$$

$$\log(\log(g(x)))=-\log(x)/(x-1)+\log(\log(x)/(x-1))$$

である。この場合、も$\log(x)/(x-1)$の代わりに、ベルヌーイ数の母関数$x/(e^x-1)$を代入すると、

$$-\log(x)/(x-1)+\log(\log(x)/(x-1))=-x/(e^x-1)+\log(x/(e^x-1))$$

である。最初の関数と次の関数は

$$\log(\log(f(e^x)))=xe^x/(e^x-1)+\log(x/(e^x-1))$$

$$\log(\log(g(e^x))) = -x/(e^x-1)+\log(x/(e^x-1))$$

である。

$$\log(\log(f(e^x)))-\log(\log(g(e^x))) = x(e^x+1)/(e^x-1)$$

左辺の関数も偶関数

$$x(e^x+1)/(e^x-1) = -x(e^{-x}+1)/(e^{-x}-1)$$

であるから、$\log(\log(g(e^x)))$も偶関数である。直接にも

$$x/(e^{-x}-1)+\log(-x/(e^{-x}-1)) = -e^x x/(e^x-1)+\log(e^x x/(e^x-1))$$

$$= -e^x x/(e^x-1)+x+\log(x/(e^x-1)) = -x/(e^x-1)+\log(x/(e^x-1))$$

として確かめられる。

$$x/(e^{-x}-1)+\log(-x/(e^{-x}-1)) = -x/(e^x-1)+\log(x/(e^x-1))$$

なる式からは、

$$x/(e^{-x}-1)+x/(e^x-1) = \log(-x/(e^{-x}-1))-\log(x/(e^x-1))$$

が得られる。この場合も

$$x/(e^{-x}-1)+x/(e^x-1) = -e^x x/(e^x-1)+x/(e^x-1) = -x$$

$$\log(-x/(e^{-x}-1))-\log(x/(e^x-1)) = \log(e^{-x}) = -x$$

である。

$$e^x x/(e^x-1)-x/(e^x-1) = x(e^x-1)/(e^x-1) \quad = x$$

$$(-x/(e^{-x}-1))/(x/(e^x-1)) = e^{-x}$$

など、自明な関係であるが大切な関係である。

$$\log(x) = \log(a)/(a-1),$$

$$\log(y) = \log(x)+\log(a) = \log(a)/(a-1)+\log(a)$$

$$= \log(a)(1+1/(a-1)) = a\cdot\log(a)/(a-1) = a\cdot\log(x)$$

従って、x,y の組は

$$y = ax, \quad \log(y) = a\cdot\log(x)$$

を同時に満足する。つまり、行列式

$$\begin{vmatrix} x & y \\ \log(x) & \log(y) \end{vmatrix}$$

は0である。このようにして、結合法則から、交換可能性

$$x\cdot\log(y) = xa\cdot\log(x) = y\cdot\log(x)$$

が導かれる。

$$\log(x) \ = \log(a)/(a-1), \log(y) \ = a\cdot\log(a)/(a-1)$$

次の二つの関数はともに偶関数であるから、

$$\log(\log(f(e^x)))=xe^x/(e^x-1)+\log(x/(e^x-1))$$
$$\log(\log(g(e^x)))=-x/(e^x-1)+\log(x/(e^x-1))$$

これらの和も偶関数である。

$$\log(\log(f(e^x)))+\log(\log(g(e^x)))=x+2\cdot\log(x/(e^x-1))$$

これは、直接に

$$-x+2\cdot\log(-x/(e^{-x}-1))=-x+2\cdot\log(xe^x/(e^x-1))=-x+2(x+\log(x/(e^x-1))$$
$$=x+2\cdot\log(x/(e^x-1))$$

からも確かめられる。つまり、

$$x/2+\log(x/(e^x-1))=\log(xe^{x/2}/(e^x-1))=\log(x/2\cdot(1/(e^{x/2}+1)+1/(e^{x/2}-1))$$

が偶関数であるということにすぎない。この関数の微分は奇関数である。

具体的には

$$(x/(e^x-1))'=((e^x-1)-xe^x)/(e^x-1)^2$$

であるから、

$$\log(x/(e^x-1))'=((e^x-1)-xe^x)/(e^x-1)^2\cdot(e^x-1)/x=((e^x-1)-xe^x)/(x(e^x-1))$$
$$=1/x-e^x/(e^x-1)$$

により、

$$1/2+\log(x/(e^x-1))'=1/x+((e^x-1)/2-e^x)/(e^x-1)=1/x-1/2\cdot(e^x+1)/(e^x-1)$$
$$=1/x-1/2\cdot\coth(x/2)=1/x-1/2\cdot(e^{x/2}+e^{-x/2})/(e^{x/2}-e^{-x/2})$$

また、

$$x/2+\log(x/(e^x-1))=\log(xe^{x/2}/(e^x-1))=\log(x/(e^{x/2}-e^{-x/2}))$$

であるから、

$$-x/(e^{-x/2}-e^{x/2})=x/(e^{x/2}-e^{-x/2})=x/\sinh(x/2)$$

が偶関数であることも明かである。

$$xe^{x/2}/(e^x-1)=x/2\cdot(1/(e^{x/2}+1)+1/(e^{x/2}-1))$$
$$-xe^{-x/2}/(e^{-x}-1)=-x/2\cdot(1/(e^{-x/2}+1)+1/(e^{-x/2}-1))=-x/2\cdot(e^{x/2}/(e^{x/2}+1)-e^{x/2}/(e^{x/2}-1))$$
$$=-x/2\cdot(-1/(e^{x/2}+1)-1/(e^{x/2}-1))=x/2\cdot(1/(e^{x/2}+1)+1/(e^{x/2}-1))$$

これも、

$$(x/2)/(e^{x/2}+1)+(x/2)/(e^{x/2}-1))$$

のように表示してみると、やはり、本質的にはベルヌーイ数の母関数なのである。最初の関数について、

$$-x/(e^x-1)+\log(x/(e^x-1))=-x/(e^x-1)-x/2+\log(xe^{x/2}/(e^x-1))$$
$$=-x/2((e^x-1)+2)/(e^x-1)+\log(xe^{x/2}/(e^x-1))$$

$$= -x/2\cdot(e^{x/2}+e^{-x/2})/(e^{x/2}-e^{-x/2})+\log(x/(e^{x/2}-e^{-x/2}))$$

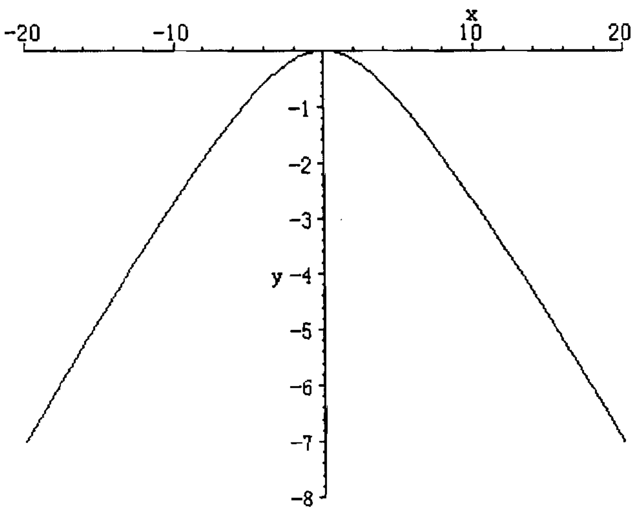
は偶関数であることの直接的な表現である。

次の関数についても

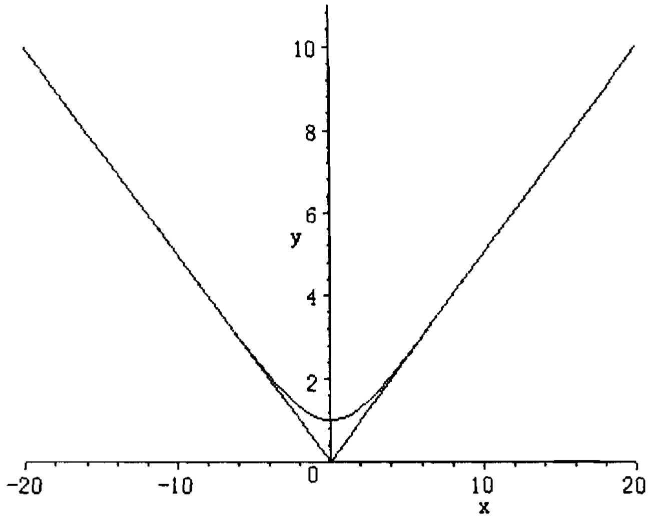
$$xe^x/(e^x-1)+\log(x/(e^x-1)) = xe^x/(e^x-1)-x/2+\log(xe^{x/2}/(e^x-1))$$
$$= x/2(2e^x-(e^x-1))/(e^x-1)+\log(xe^{x/2}/(e^x-1))$$
$$= x/2\cdot(e^{x/2}+e^{-x/2})/(e^{x/2}-e^{-x/2})+\log(xe^{x/2}/(e^x-1))$$

であり、差は $\pm x/2\cdot(e^{x/2}+e^{-x/2})/(e^{x/2}-e^{-x/2})$ に於ける符号のみである。

$$\log(xe^{x/2}/(e^x-1)) = \log(x/(e^{x/2}-e^{-x/2}))$$



$|x/2|,\quad x/2\cdot(e^{x/2}+e^{-x/2})/(e^{x/2}-e^{-x/2})$



この関数は、$|x/2|$の非常によい近似を与えている。

3. 白石の問題

次のものは白石潤一氏が Apéritif として、数学セミナー 2009.3, vol.48.no.3.570 の巻頭言の「雪を見て思うこと」に記載された一文による。

ここに述べられた結果は既に多くの人が独立に得ていると思うが、問題の全体像は未知の可能性を含んでいるのでこの場を借りて紹介する。

それは、2 重対数(double logarithm)、$\log^2(x) = \log(\log(x))$ の関係

$$x \cdot \log(x) \cdot \log(\log(x))' = 1$$

あるいは

$$\int dx/(x \cdot \log(x)) = \log(\log(x))$$

が現実の例として登場するという意味でも興味深いと思ったからである。この関係はオイラーの関係式

$$0 = 1+e^{\wedge}(\pi \times i)$$

の美しさを思い起こさせるものを含んでいると感じた訳である。

白石潤一氏の

“階乗和の平方因子問題”

(square prime factor of factorial sum problem)

は

$$S(n) = 0!+1!+2!+\cdots+n!$$

が奇数の平方因子をもつかどうかを問う問題である。例えば、

$$2^2 | S(2) = 4$$

であるが、これは偶数である。2009.02.13.10:50 に

$$54503^2 | S(26540)$$

が見つかったので、少なくとも一つは存在することは判明したが。現在は、無限個存在するのではないかと予想している。しかし、それは、

$$\log(\log(n))$$

つまり、n 番目の解は $\exp^2(n) = e^{\wedge}(e^{\wedge}n)$ の整数部分

2, 15, 1618, 528491311, 5148435562634572131 82265,

2851123567946151060558103865798280598385364881793944495341 7128836

といった order の(自然数の)分布であろうという予測である。だから、早晩、第 2 の白石数(Shiraishi number)が見つかるだろうと期待している。この数がどのような姿でこの世に登場するか楽しみである。(一般法則：予想はしばしば偽である)

計算の指針としては、$s(n)=S(n) \bmod p$ を

$$a = 1: s = 2: \text{for } n \text{ from } 2 \text{ to } p\text{-}1: a := a \times n \bmod p: s := s + a \bmod p$$

によって計算し

$$S = \{[p,n] : n \le p,\ p|s(n)\}$$

とおく。そして、S の元に対して $p^2|s(n)$ かどうか check するという方針をとった。

下の図は n = 2 ~ 6000000 について 1000 個毎にその区間に属する素数に対する S の総数

$$\#S = \#\{[p,n] : k \cdot 10^3 < p < (k+1) \cdot 10^3,\ p|s(n)\}$$

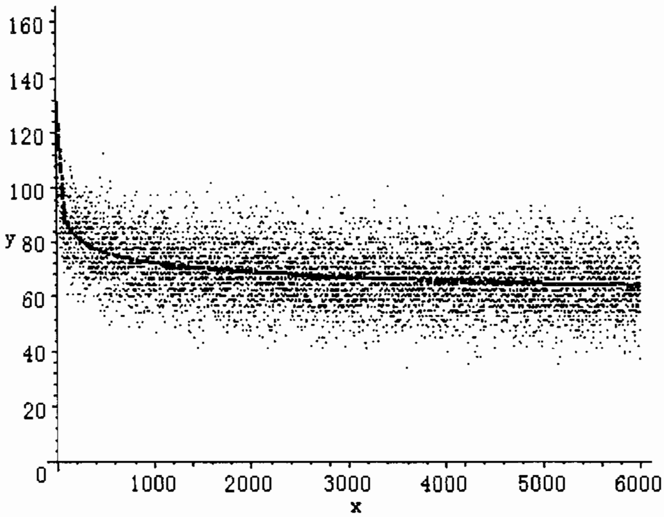
の表である。線のグラフで表示されているのは

$$y = 10^3/\log(k \cdot 10^3),\ k = 1 \sim 6000$$

である。これは、$s(n)= s_p(n)= S(n) \bmod p$ が $1/\log(p)$ の密度に比例すると仮定したときの S の期待される個数である。この図から概ね比例していることは了解できると思う。

$$\#S = \#\{[p,n] : k \cdot 10^3 < p < (k+1) \cdot 10^3,\ p|s(n)\}$$

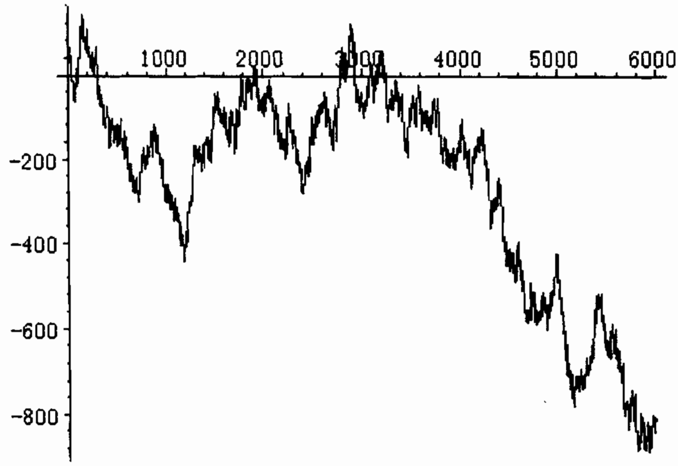
$$y = 10^3/\log(k \cdot 10^3),\ k = 1 \sim 6000$$



素数に関する密度と S の密度の関数が共に、荒く見積もって

$$1/\log(x)$$

であることから、素数と S の n までの累積頻度がどのようであるか興味がある。次のグラフは、1000 ごとの素数の数と S の元の個数について素数の個数から S の個数を引いたものである。



傾向としては#(Pr-S)は負になるような感じもするが、3000000 辺りで符号が変化した経緯もあるから早急な結論は避けるべきでしょう。

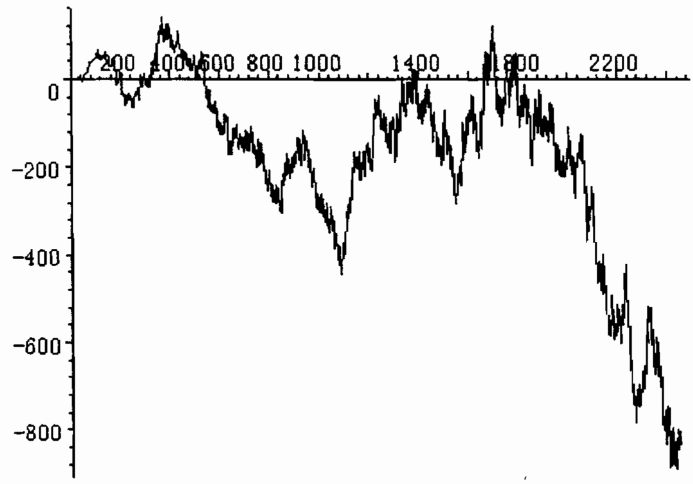
(予想)問題

「#(Pr-S)は無限回符号を変える」

を提出しておきましょう。この方向の結論の方が好みだからという理由である。同じ内容のグラフを、n の代わりに $\sqrt{n}$ に変えて

$(\sqrt{n}, \#(pr\text{-}S)[n])$

として表示したものが次のものである。



以下の表は S(p)の元に対して x mod p^2 が符号を除いて 1 桁になるものを 6000000 まで調べたものである。

[[2, 0], [5, 2], [7, 1], [11, 3], [17, 2],
[19, 8], [19, 4], [19, 5], [23, -8], [31, -8],
[37, 5], [41, -6], [211, 2], [233, 6], [313, 8],
[379, -2], [397, 4], [467, 4], [487, 4], [743, -4],
[839, 9], [2213, -1], [2957, 2], [3359, 2], [3919, 4],
[7547, 1], [12511, 3], [13913, -6], [23117, 2], [34267, -1],
[49999, 6], [54503, 0], [79657, -7], [94613, 9], [189491, -8],
[191353, 8], [204557, 2], [288359, -9], [1330997, 3], [2018957, 2],
[2103083, 3], [2646983, -7], [3892379, -4]]

全体で 43 個存在する。-9 ~ 9 は 19 個の元から成るから、random と仮定すると、0 の出現する可能性は

$$43/19 = 2.263157895$$

であり、現実に、p = 2, 54503 の 2 個が見つかっている。以下のものは出現の順に記したものである：

[0, 2, 1, 3, 2, 8, 4, 5, -8, -8, 5, -6, 2, 6, 8, -2, 4, 4, 4, -4, 9, -1,
2, 2, 4, 1, 3, -6, 2, -1, 6, 0, -7, 9, -8, 8, 2, -9, 3, 2, 3, -7, -4]

次のものはそれを sort したものである。

[-9, -8, -8, -8, -7, -7, -6, -6, -4, -4, -2, -1, -1, 0, 0, 1, 1, 2, 2, 2, 2, 2,
2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 4, 4, 5, 5, 6, 6, 8, 8, 8, 9, 9]

まとめた、頻度表は

±n	0	1	2	3	4	5	6	7	8	9
+	2	2	8	4	5	2	2	0	3	2
-		2	1	0	2	0	2	2	2	1

である。2 が 8 度も登場している。数字に特に高い出現率をもつものがあるのだろうか。調査したものは、値の絶対値が 1000 未満のものであるが、

[[1, 713], [2, 298], [3, 94], [4, 24], [5, 3], [6, 0], [7, 1], [8, 1], [9, 0]]

がその表である。回数の大きいものについて整理すると

[4, [-855, -681, -563, -525, -423, -302, -61, -52, -38, -32,
3, 15, 28, 41, 54, 68, 112, 115, 135, 152, 175, 194, 385, 464]],
[5, [-29, 4, 264]], [6, []], [7, [-51]], [8, [2]], [9, []]

のようである。この範囲でも 2 は 8 度、-51 は 7 度出現している。6 度のものは存在せず、5 度のものが[-29, 4, 264]のように 3 個存在する。

問題

2, -51 は特に高い出現比率をもつのであろうか。

参考文献

［1］ 難波完爾；種数 3 の超楕円曲線と $\sin^2$-予想, 津田塾大学 数学・計算機科学研究所報 29 第 18 回数学史シンポジウム (2007), 2008 pp.157-194

［2］ Kanji Namba; genus 3 hyper-elliptic curves and their coefficient polynomials 2008 年度応用数学合同研究集会報告集 Ryukoku Univ. 2008. pp.9-14

［3］ Kanji Namba; genus 3 hyper-elliptic curves and their coefficient polynomials, 津田塾大学 数学・計算機科学研究所報 30, 第 19 回数学史シンポジウム (2008), 2009. pp.251-296

［4］ Kanji Namba; genus 4 hyper-elliptic curves and Galois group of their coefficient polynomials 2009 年度応用数学合同研究集会報告集 Ryukoku Univ. 2009. pp.95-100