Genus 3 hyper-elliptic curves and 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

2008.12.31

1. 超幾何級数と対合

例えば、Weierstrass の標準形

$$C:\quad y^2 = f(x) = x^3+ax+b$$

で表示された有限体

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

上の楕円曲線で決定される群（Poincaré-Mordell group）の位数は、Legendre 記号 (x/p) を用いて

$$n_p = 1+ a_p+p$$

$$a_p = \sum x\in p\,(f(x)/p)$$

の形に表現されることはよく知られている。楕円曲線の所謂、j-invariant（の定数倍）

$$x = j = -27b^2/4a^3$$

を変数として、ルジャンドルの多項式あるいはフックスの関数を用いて

$$a(x) = x^{(p-1)/4}P_{[p/6]}(\sqrt{x})$$

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

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

のように記すことができる。ルジャンドルの多項式（Legendre polynomial）は

$$1,\ x,\ 1/2\cdot(3x^2-1),\ 1/2\cdot x(5x^2-3),\ 1/8\cdot(35x^4-30x^2+3),\ 1/8\cdot x(63x^4-70x^2+15),\ \cdots$$

のような多項式である。p = 19 を例にとると、

$$[p/4] = [19/4] = 4,\ [p/6] = 3$$

であるから、求める a(x) は $P_2(x) = 1/2\cdot(3x^2-1)$, 7/12 = -1, 11/12 = 8 などに着目して

$$a(x) = x^{18/4}\cdot 1/2\cdot\sqrt{x}\,(5x-3) = 1/2\cdot x^5(5x-3) = (-7x+8)\,x^5$$

である。フックスの関数の方では 7/12 = -1 であるから、次の項から先は消

えて

$$F(7/12,11/12,1,1-x) = 1+7/12 \cdot 11/12 \cdot (1-x) + \cdots = 1+7(1-x) = 8x-7$$

となるので、$(p+1)/4 = 5$ から、結果は同一の関数を与えている。

このように、体の標数が有限のときは、標数 0 の有理数体、実数体、複素数体と異なって、無限級数ではなく、素数に従属するが、多項式、つまり、擬多項式(pseudo-polynomial)とでも呼ぶべきものになっていることが本質的な点である。

$$a(x) = x^5(-7x+8)$$

$p = 19$ での原始根(primitive root)の全体は

[2, 3, 10, 13, 14, 15]

である。

$a(x)$の $p = \{0,1,2,\cdots,p-1\}$ での、絶対値最小剰余(least absolute value residue, lavr)列は

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

であり、Hasse の限界は $2\sqrt{p} = 2\sqrt{19} = 8.717797888\cdots$ であるから、勿論、この条件を満たしている。

$a(x)$の原始根 b に対応する表現変換多項式(representation transformation polynomial)とは、

$$\underline{a}(x) = \sum n \in p\text{-}1\ a(b^n)\, x^n$$

のことである。つまり、x^n の係数を $a(b^n)$にした多項式で、添字(index)は

$$p-1 = \{0,1,2,\cdots,p-2\}$$

の範囲としたものである。例えば、最小の原始根 $b = 2$ の場合は $b^n \bmod p$ の表が

[1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10]

であるから、

$$\underline{a}(x) = 1-2x+2x^2-6x^3+2x^4-3x^5+5x^6-7x^7-6x^8+4x^9-x^{10}-4x^{11}-8x^{12}-5x^{13}+x^{14}+4x^{16}+4x^{17}$$

である。x^{15} がないのは、$2^{15} = 12$ で $a(12) = 0$ となっているからである。

$p = 19$ の場合の $F_p = GF(p) = p = \{0,1,2,\cdots,p-1\}$の円分多項式(cyclotomic polynomial)は

$$x^{19}-x = x(x-1)(x+1)(x^2-x+1)(x^2+x+1)(x^6-x^3+1)(x^6+x^3+1)$$

である。

二つの多項式

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

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

（退行）終結行列（resultant matrix）は

$$\begin{pmatrix}
0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n \\
0 & \cdots & a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 \\
 & \cdots & & & & \cdots & & \\
a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\
0 & \cdots & 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m \\
0 & \cdots & b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 \\
 & \cdots & & & & \cdots & & \\
b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0
\end{pmatrix}$$

を、行に関する変形、つまり、$x^{m-i}f(x)$の$g(x)$による剰余のx^j の係数c_{ij} を成分とする$g(x)$の次数を次数とする正方行列を考え、それを

$$f(x)\,[x]\,g(x) = (c_{ij})$$

と記する。上の行列の表示を用いれば

$$\left(\begin{array}{ccc|ccc}
\hline
c_{11} & c_{12}\cdots & c_{1m} & 0 & 0\cdots & 0 \\
c_{21} & c_{22}\cdots & c_{2m} & 0 & 0\cdots & 0 \\
 & \cdots & & & \cdots & \\
c_{m1} & c_{m2}\cdots & c_{mm} & 0 & 0\cdots & 0 \\
\hline
\multicolumn{6}{c}{0 \ \cdots \ 0 \ b_0 \ b_1 \ \cdots \ b_{m-1} \ b_m} \\
\multicolumn{6}{c}{0 \ \cdots \ b_0 \ b_1 \ \cdots \ b_{m-1} \ b_m \ 0} \\
\multicolumn{6}{c}{\cdots \qquad\qquad \cdots} \\
\multicolumn{6}{c}{b_0 \ b_1 \ \cdots \ b_{m-1} \ b_m \ 0 \ \cdots \ 0}
\end{array}\right)$$

である。このような退行型の行列を考えたのは、$g(x)$が円分多項式のような場合

$$f(x)\,[x]\,g(x)$$

の固有値が実数になり易いであろうと考えたからである。

先ず、表現変換多項式

$$\underline{a}(x) = 1-2x+2x^2-6x^3+2x^4-3x^5+5x^6-7x^7-6x^8+4x^9-x^{10}-4x^{11}-8x^{12}-5x^{13}+x^{14}+4x^{16}+4x^{17}$$

と、F_{19}の特性多項式の因子$x^{18}-1$の終結行列を考える。

終結行列演算子（resultant matrix operator）$[x]$の結合力は加減乗除よりも弱いものとする。

$$\underline{a}(x)\,[x]\,x^{18}-1$$

$$=$$

$$\begin{pmatrix}
4, 8, -9, -6, 1, -3, 3, 3, 4, 2, 3, 7, -4, 6, 0, 1, -2, 1 \\
8, -9, -6, 1, -3, 3, 3, 4, 2, 3, 7, -4, 6, 0, 1, -2, 1, 4 \\
-9, -6, 1, -3, 3, 3, 4, 2, 3, 7, -4, 6, 0, 1, -2, 1, 4, 8 \\
-6, 1, -3, 3, 3, 4, 2, 3, 7, -4, 6, 0, 1, -2, 1, 4, 8, -9 \\
1, -3, 3, 3, 4, 2, 3, 7, -4, 6, 0, 1, -2, 1, 4, 8, -9, -6 \\
-3, 3, 3, 4, 2, 3, 7, -4, 6, 0, 1, -2, 1, 4, 8, -9, -6, 1 \\
3, 3, 4, 2, 3, 7, -4, 6, 0, 1, -2, 1, 4, 8, -9, -6, 1, -3 \\
3, 4, 2, 3, 7, -4, 6, 0, 1, -2, 1, 4, 8, -9, -6, 1, -3, 3 \\
4, 2, 3, 7, -4, 6, 0, 1, -2, 1, 4, 8, -9, -6, 1, -3, 3, 3 \\
2, 3, 7, -4, 6, 0, 1, -2, 1, 4, 8, -9, -6, 1, -3, 3, 3, 4 \\
3, 7, -4, 6, 0, 1, -2, 1, 4, 8, -9, -6, 1, -3, 3, 3, 4, 2 \\
7, -4, 6, 0, 1, -2, 1, 4, 8, -9, -6, 1, -3, 3, 3, 4, 2, 3 \\
-4, 6, 0, 1, -2, 1, 4, 8, -9, -6, 1, -3, 3, 3, 4, 2, 3, 7 \\
6, 0, 1, -2, 1, 4, 8, -9, -6, 1, -3, 3, 3, 4, 2, 3, 7, -4 \\
0, 1, -2, 1, 4, 8, -9, -6, 1, -3, 3, 3, 4, 2, 3, 7, -4, 6 \\
1, -2, 1, 4, 8, -9, -6, 1, -3, 3, 3, 4, 2, 3, 7, -4, 6, 0 \\
-2, 1, 4, 8, -9, -6, 1, -3, 3, 3, 4, 2, 3, 7, -4, 6, 0, 1 \\
1, 4, 8, -9, -6, 1, -3, 3, 3, 4, 2, 3, 7, -4, 6, 0, 1, -2
\end{pmatrix}$$

では、固有多項式は $(x-19)^9(x+19)^9$ であり最小多項式は $(x-19)(x+19)$ である。つまり、

$$A = 1/p\cdot\underline{a}(x)\,[x]\,x^{18}-1$$

は巡回対合(cyclic involution)である。

尚、表現多項式

$$\underline{a}(x) = 1-2x+2x^2-6x^3+2x^4-3x^5+5x^6-7x^7-6x^8+4x^9-x^{10}-4x^{11}-8x^{12}-5x^{13}+x^{14}+4x^{16}+4x^{17}$$

$$= 4(x+1)(x+2)(x+3)(x+4)(x+5)(x+6)^2(x+7)(x+9)(x+10)$$

$$(x+11)(x+12)(x+13)(x+14)(x+15)(x+17)(x+18)$$

は、有理数体上の既約多項式であるけれども、有限体 F_p 上ではかなりの因子は一次因子で $\underline{a}(x)$ を $x^{p-1}-1$ で割った既約分数表示

$$\underline{a}(x)/(x^{p-1}-1) = b(x)/c(x)$$

の分母の次数は常に

$$[p/12]+1$$

であろうと予想している。また、$b(x)$が$[p/12]$次の F_p 上で既約な多項式になるような原始根が存在するのではないかと思っている。任意の既約成分に応じた直和対合分解が可能である。例えば、$\underline{a}(x)[x]x^2+x+1$ の場合、

$$A = 1/\sqrt{p}\cdot\underline{a}(x)[x]x^2+x+1$$

が対合になっている。残りの因子の場合は $1/p$ を乗じたものが対合、つまり、

$$A^2 = E$$

という性質をもつ。言い換えると、もとに戻す作用である。つまり、A の信号を発して A で受信すれば、もとのものでない部分が影響を受けた部分であることが解る。

例えば、

$$A = 1/19\cdot\underline{a}(x)[x]x^{18}-1$$

のような巡回対合であれば、その列の信号列を発信して、A を掛け(受信す)れば、どれだけの遅延の後にどれだけの強さの信号が返って来たか解る。乱数列でも同様なことは当然考えられるが、$\sqrt{p}$ 程度の長さ p の列では、自分自身の長さの自乗 p^2 と $(\sqrt{p})^2 = p$ 程度の大きさの“雑音”(noise)を考慮しておかなければならない。巡回対合の場合は自身の長さの自乗 p^2 であるが、ずらした列との内積は常に 0 である。

問題(予想)

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

$$a(x) = x^{[p/4]}P_{[p/6]}(\sqrt{x})$$

$\underline{a}(x)$は $a(x)$の表現変換、$f(x)\mid(x^{p-1}-1)$ で $x^{12}-1$ と互いに素ならば、

$$A = 1/p\cdot\underline{a}(x)[x]f(x)$$

は常に対合である。$f(x) = x^2+1,\ x^2-x+1,\ x^2+x+1$ のとき

$$A = 1/\sqrt{p}\cdot\underline{a}(x)[x]f(x),$$

$$A = 1/p\cdot\underline{a}(x)[x]f(x)$$

の何れかが対合である。

$p = 19$ の場合 $A = 1/\sqrt{19}\cdot\underline{a}(x)[x]x^2+x+1$ が対合になっている。

現実の場合、楕円曲線の族に応じて Fuchs の関数が対応している。

normal form	name of family	multiplier	parameter	degree
$y^2 = x(x-1)(x-q)$	Legendre family			
$a_2(z)$	$F(1/2,1/2,1,z)$	1	$z = q$	$d = [p/2]$
$y^2 = x^3+(3qx+4)^2$	Hessian family			
$a_3(z)$	$F(1/3,2/3,1,z)$	1	$z = 1/q^3$	$d = [p/3]$
$y^2 = x(x^2+px+q)$	Euler family			
$a_4(z)$	$F(1/4,3/4,1,z)$	1	$z = 4p/q^3$	$d = [p/4]$
$y^2 = x^3+px^2+q$				
$a_6(z)$	$F(1/6,5/6,1,z)$	1	$z = -27p/q^3$	$d = [p/6]$
$y^2 = ?$	(2-fold) Euler family			
				$d = [p/8]$
$p=8n+1$, $a_8(z)$	$F(1/8,5/8,1,1-z)$	z^{3n}	$(z/p) = 1$	
		$z^{3n}/\sqrt{-2}$	$(z/p) = -1$	
$p=8n+3$, $a_8(z)$	$F(3/8,7/8,1,1-z)$	z^{3n+1}	$(z/p) = 1$	
		$z^{3n+1}/\sqrt{-2}$	$(z/p) = -1$	
$p=8n+5$, $a_8(z)$	$F(1/8,5/8,1,1-z)$	1	$\langle z/p\rangle = z^{2n+1} = 1$	
		$\sqrt{-1}$	$\langle z/p\rangle = -1$	
		$\sqrt{\langle z/p\rangle/2}$	$(z/p) = -1$	
$p=8n+7$, $a_8(z)$	$F(3/8,7/8,1,1-z)$	z^n	$(z/p) = 1$	
		$z^n/\sqrt{2}$	$(z/p) = -1$	
$y^2 = x^3+px+q$	Weierstrass family			
$p=4n+1$, $a_{12}(z)$	$F(1/12,5/12,1,1-z)$	z^n	$z = -27p^2/4q^3$	$d = [p/12]$
$p=4n-1$, $a_{12}(z)$	$F(7/12,11/12,1,1-z)$	z^n		

ただし、上記表に於いて、$\langle z/p\rangle$ は 4 乗剰余、(z/p)は平方剰余（Legendre symbol）、

$$\sqrt{-1}, \sqrt{2}, \sqrt{-2}$$

などは F_p に於ける値で、平方剰余、4 乗剰余だけの自由さがある。そのどれを採用しても Hasse の不等式は満足されると思う。特に、

$$a_8(z) = b_8(z) \cdot F(1/8,5/8,1,1-z)$$

の部分は実験式であって是非検証、あるいは厳密化、そして証明が必要な

“予想”の式である。大きな考え違いなどが含まれている可能性がある部分である。

対合に関して、予想問題として提出した性質

$F_p = GF(p) = p = \{0,1,2,\cdots,p-1\}$
$a(x)$と$x^{p-1}-1$の既約因子$f(x)$に対し
$A = 1/q \cdot a(x)\,[x]\,f(x),\ q = p, \sqrt{p}$
$A^2 = E$

を、$a(x)$の対合性(involution property)と呼ぶことにしよう。

勿論、係数が$1/\sqrt{p}$の場合は、x^2+1の gauss 整数の退化、x^2+x+1, x^2-x+1の Eisenstein 整数の退化に相当している。その外の場合は常に$1/p$であろうと予想されている。

この退化が、$\sin^2$-予想の$\theta = 0$付近に$1/\sqrt{p}$程度の乱れ、所謂、Gibbs の現象を引き起こしているのではないかと思っている。

上述の

$$a(x) = x^{(p-1)/4} P_{[p/6]}(\sqrt{x})$$

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

および、それに、平方剰余$(x/p) = x^{(p-1)/2}$を掛けた関数は、対合性を有することは確かであろうけれども、例えば、

$$F(1/8,5/8,1,1-z)$$

に関係した関数については、Hasse の不等式について(私は)わずかな、つまり、上記の表程度の、実験的な知識をもっているにすぎない。

問　題
$a_2(x),\ a_3(x),\ a_4(x),\ a_6(x),\ a_{12}(x)$
の外の対合性をもつ関数族を決定すること

2. 種数3の超楕円曲線とその係数方程式

この章の目的は、種数3の超楕円曲線

$$C:\quad y^2 = x^7+a_1x^6+a_2x^5+a_3x^4+a_4x^3+a_5x^2+a_6x+a_7 = f(x)$$

の終結変換多項式(resultant transformation polynomial)とその係数多項式(coefficient polynomial)の根の分布の類型に関するものである。

先ず、終結式の省略記号(この場限りの記号・用語法)として

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

のような記号を用い、消去積(elimination product)と呼ぶことにする。記号ⓧ,ⓨなどの結合力は加減乗除などの算法より弱いものとする。消去積の性質には結合法則や積に関する分配律と代入(substitution)に関する性質

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

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

$$f(x) ⓧ x-y = f(y)$$

などがある。チルンハウス(チルナウス W. von Tschirunhaus 1651-1708)変換

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

に対し、平方剰余記号(Legendre symbol)を(x/p)として、それらの有限素体

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

での和を

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

とおく。このとき、

$$\bar{f}(x) = x^6+a_px^5+b_px^4+c_px^3+pb_px^2+p^2a_px+p^3$$

を f(x)の終結変換(resultant transform)多項式、$\bar{f}(x) = 0$ を終結変換方程式と呼ぶ。志村・谷山理論により、終結変換方程式の解はすべて

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

の形に表示できることが知られている。偏角 θ の分布に関する generic な場合、つまり、f(x)が非可解(non-solvable)な場合(この場合は genus 3)は、

$$\sin^2\theta + \sin^2 2\theta + \sin^2 3\theta$$

であろうというのが $\sin^2$-予想である。

例えば、

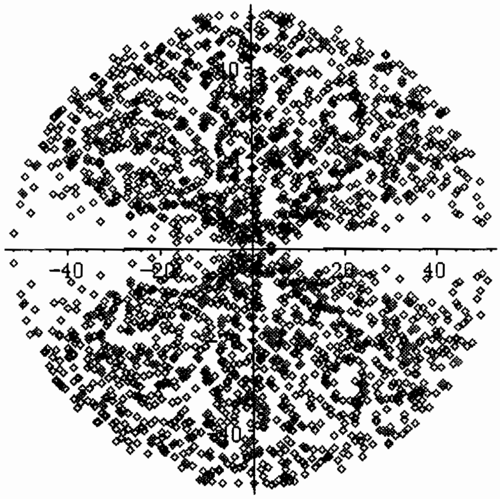
$$f(x) = x^7+x^6-x^5+x^3-x^2-x+1$$

は gal = S(7)で非可解であり、det(f(x)) = f(x) ⓧ f'(x) = 184607 は素数である。次の図は終結変換方程式の根を複素平面上に plot したものである。

$$y^2 = x^7+x^6-x^5+x^3-x^2-x+1$$

$$x^6+ax^5+bx^4+cx^3+bpx^2+ap^2x+p^3 = 0$$

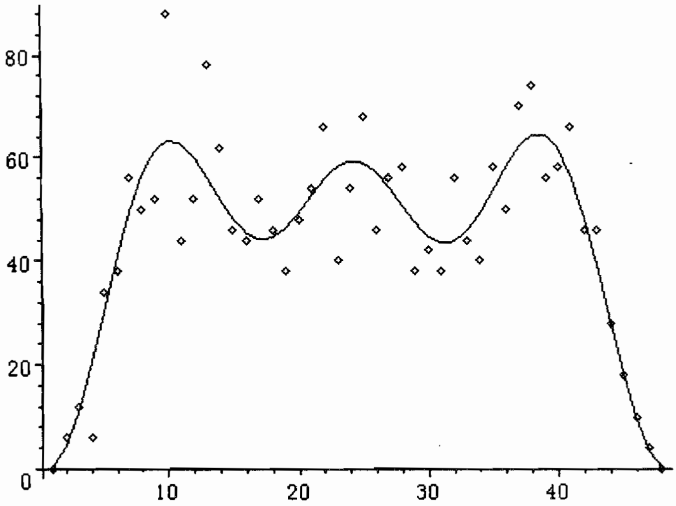
$$p = 3 \sim 2707$$



angular distribution

$\sin^2\theta + \sin^2 2\theta + \sin^2 3\theta$

$p = 3 \sim 2411$ (2136 roots)



終結変換方程式の解の偏角の分布については、可解な場合色々の可能性がある。

さて、解の絶対値が $\sqrt{p}$ であることは

$$\bar{f}(x) = x^6+a_px^5+b_px^4+c_px^3+pb_px^2+p^2a_px+p^3 = (x^2+ux+p)(x^2+vx+p)(x^2+wx+p)$$

$$|u|, |v|, |w| < 2\sqrt{p}$$

のような表示が可能であることを意味している。この実数の係数 u,v,w を

解とする方程式は、終結式(=消去積)を用いて、共通解の存在条件として

$$\bar{f}(x) \otimes x^2+yx+p = p^3(y^3-a_py^2+(b_p-3p)y-c_p+2pa_p)^2$$

と表現できるから

$$y^3-a_py^2+(b_p-3p)y-c_p+2pa_p = (y-u)(y-v)(y-w)$$

である。この多項式を f(x)の係数多項式(coefficient polynomial)という。現実には $a = a_p/\sqrt{p}$, $b = b_p/p$, $c = c_p/p\sqrt{p}$ と標準化して

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

の左辺を標準係数多項式(normalized coefficient polynomial)、この方程式を標準係数方程式(normalized coefficient equation)という。

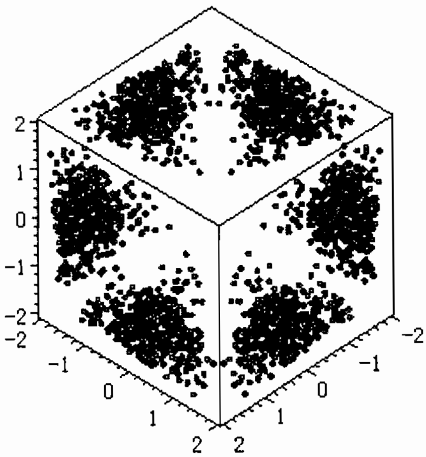
この方程式の解は、勿論、3 根とも[-2,2]の範囲に存在する。この方程式の 3 根を、例えば、(x,y,z)のように xyz-空間の点と考えて、立方体$[-2,2]^3$の内部の点として表示することができる。しかし、一般には、正の密度で分布するような代数曲面、曲線、点などは存在しないようであるけれども、f(x)が可解であるとか、可約な場合には、そのような部分代数多様体(algebraic sub-manifold)が存在する場合がある。

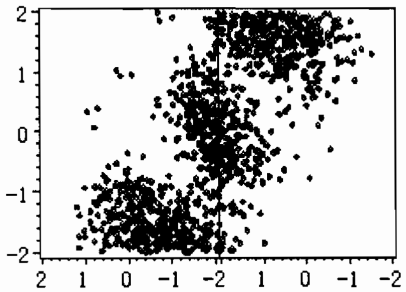
上記の例の場合の標準係数方程式の 3 つの解を x,y,z として、すべての順序で並べた点(x,y,z)の、xyz-空間の立方体$[-2,2]^3$での分布は

$$y^2 = x^7+x^6-x^5+x^3-x^2-x+1$$

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

$$p = 3 \sim 2707$$





のようである。上図は x+y+z = 0 と垂直な方向から見たもの、下図は、例えば、x-軸の方向から y-軸が水平になる方向から見たものである。この図からも、一般に標準係数方程式の解の分布は空間的に一様ではないことが解る。しかし、この場合には次元の退化、つまり、特定の曲面、曲線、点などの上に正の密度で存在するような様子はみられないようである。可解でない場合はどうも *S* の形の集合上に分布するような印象がある。

次の例では、標準係数方程式の解が、例えば、立方体に内接する円周上に正の密度で存在する。

例 1. $f(x) = x(x^6-7x^4+14x^2-7)+3$

この場合は可解で

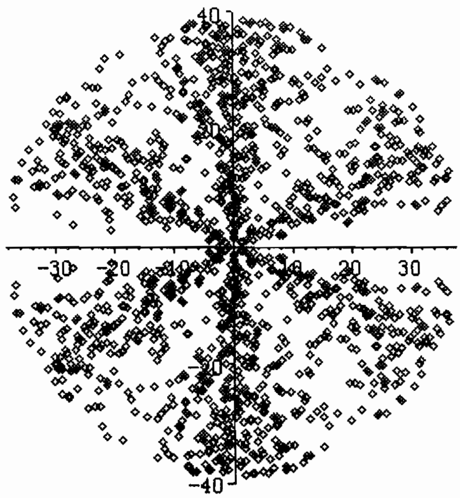
$$\mathrm{gal}(f(x)) = F_{42}(7) = \langle (2\,4\,3\,7\,5\,6), (1\,2\,3\,4\,5\,6\,7) \rangle$$

多項式 $x(x^6-7x^4+14x^2-7)$ は Tchebycheff の多項式を 2 倍に拡大したものである。その 3 だけの shift である。また、判別式は、$\det(f(x)) = f(x) ⓧ f'(x) = 5^3 7^7$ である。

$$C:\ \ f(x) = x(x^6-7x^4+14x^2-7)+3$$

$$\bar{f}(x) = x^6+a_p x^5+b_p x^4+c_p x^3+pb_p x^2+p^2 a_p x+p^3 = 0$$

$$p = 2\sim1489$$



偏角の分布は

$$\sin^2 3\theta$$

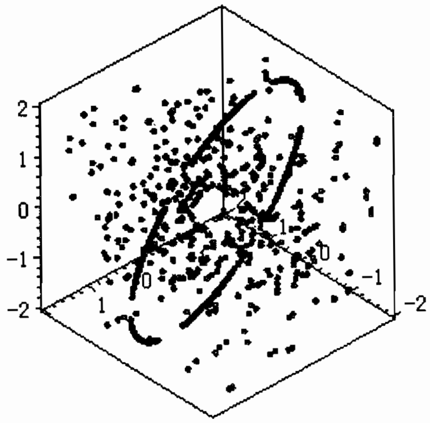
と予想されている。尚、genus 2 の場合も含め、$\sin^2 2\theta$ に比例すると予想される超楕円曲線が存在するかどうかは非常に興味がある問題である。

標準係数多項式の解の分布は

$$C:\quad f(x) = x(x^6-7x^4+14x^2-7)+3$$

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

$$p = 2\sim1213$$



である。立方体 $[-2,2]^3$ の表面に内接する半径 $\sqrt{6}$ の円の部分が見えるが、これは、標準係数多項式が

$$x^3-ax^2+(b-3)x-c+2a = x^3-3x+k$$

の形のもので、$p = 2\sim1213$ の素数 198 個のうち 134 個存在し、比率は $67/99 \fallingdotseq 2/3$ である。この場合円が、正の確率でその上に分布する退化した部分多様体である。

当然のことであるが、$x+y+z = 0$, $xy+yz+zx = -3$ のときは

$$x^2+y^2+z^2 = (x+y+z)^2-2(xy+yz+zx) = 0-2(-3) = 6$$

となるからである。この場合 k は円周上の位置を指示しているが。興味深いことに、図に見られるとおり、円の一部が欠けている。

多項式 $x^7-7x^5+14x^3-7x$ は本質的にはチェビシェフ多項式（Tchebycheff polynomial）$T_7(x)$ であり、二つの方程式

$$x = t+1/t,\ y = t^7+1/t^7$$

から t を消去したもの

$$t^{14}- yt^7+1 \textcircled{t}\ t^2- xt+1 = (y-(x^7-7x^5+14x^3-7x))^2$$

ということもできる。ここでの多項式はそれを 3 だけ shift したものである。ここでの定数は特殊な値で、何故 3 のとき、終結変換方程式の解の分布が $\sin^2 3\theta$ になるのか理由は（今の私には）解らない。

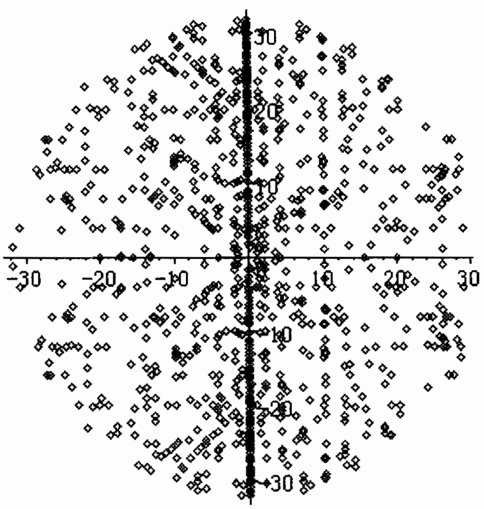
例 2. $f(x) = x(x^2+1)(x^4+1)$

これは、勿論、可約な奇関数の場合である。

$$C:\quad f(x) = x(x^2+1)(x^4+1)$$

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

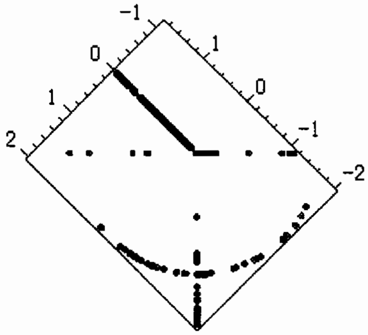
$$p = 2\sim1019$$



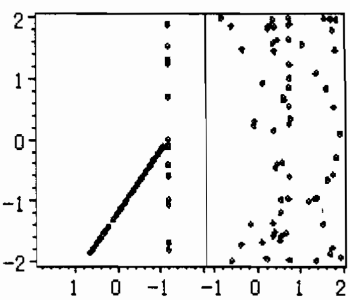
偏角の分布は、純虚数のものが正の確率で存在する。

$$C:\quad f(x)=x(x^2+1)(x^4+1)$$

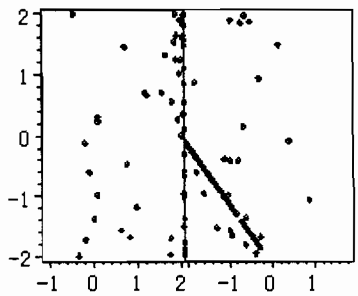
$$x^3-ax^2+(b-3)x+2a-c=0,\ p=2\sim1019$$



これは、標準係数方程式の解を、3 次方程式の標準的解法に従って計算した順序に従って対[x,y,z]を作り、それを xyz-空間に表示したものを、原点を含む平面が直線に退化する方向から見たものである。この場合は、すべての解が、原点を通る二つの垂直な平面、その交線を中心線とする半円筒面、原点に、解の曲面との角度 30° で入射する半直線、の 4 個の既約な代数部分多様体の上に分布している。立体角 30° については、斜辺が $\sqrt{2}$ で、他の辺が $1/\sqrt{2}$ の直角三角形の小さい方の角という意味である。



は、同じ図を、やはり、原点を含む平面が直線に退化する直角の方向からみたものである。円筒面の包絡面がかすかに点線として認識できる。同様にもう一方の直角の方向から見たものは



であるが、円筒の包絡面は半円筒のこの部分での分布密度は恐らくは 0 であるために明確には見えない。立方体の中心と稜の中点を結ぶ線分は、標準方程式が完全立方になる場合であり、二つの稜を含む長方形の面になるのは、重根をもつ場合、つまり、

$$(x-h)(x-k)^2$$

の形の場合である。また、この面と垂直な平面は、

$$(x-h)(x^2-k)$$

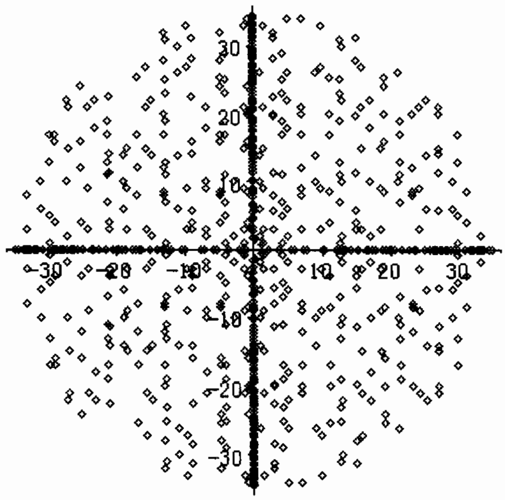
の形の場合、つまり、2 根が絶対値が等しく符号が反対のときである。もう一つの因子はその平面上の高さを意味している。半円筒面は 2 次の既約因子に関係している。勿論、この円筒面は立方体 $[-2,2]^3$ に表面上の直線で接している。

例 3. $f(x)=(x^2+1)(x^4+6x^2+1)=x(x^6+7x^4+7x^2+1)$

$$C:\ f(x)=x(x^6+7x^4+7x^2+1)$$

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

$$p=2\sim1213$$



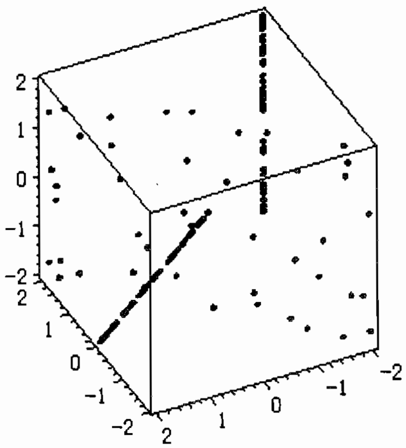
偏角の分布は一様分布と、実軸、虚軸、そして(恐らくは)一様分布の和である。

標準係数方程式の解の分布は、一つの半直線と、立方体の稜、原点を通る平面の3個である。

$$C:\quad f(x)=x(x^6+7x^4+7x^2+1)$$

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

$$p=2\sim1213$$



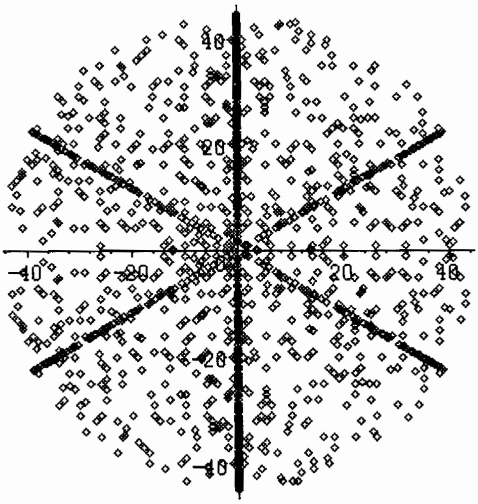
図では、平面に退化する方向からは見てないが対角面の上に分布している様子や位置の関係は想像できると思う。

例 4. $f(x)=x(x^6+6)$

$$C:\quad f(x) = x(x^6+6)$$

$$\bar{f}(x) = x^6+a_p x^5+b_p x^4+c_p x^3+pb_p x^2+p^2 a_p x+p^3 = 0$$

$$p = 2\sim2011$$



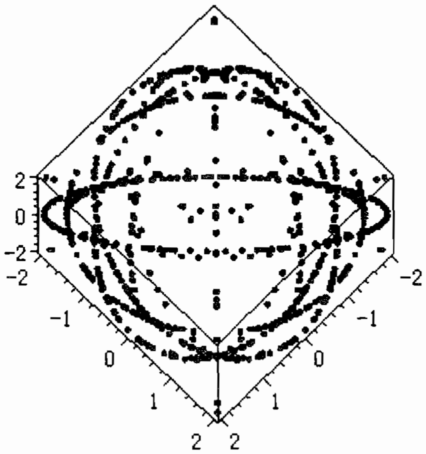
偏角の分布は、実軸、そして60°の直線、そして一様分布である。

標準係数方程式の解の分布は、何個かの互いに入れ子の楕円と直線と、残りの部分である。

$$C:\quad f(x) = x(x^6+6)$$

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

$$p = 2\sim2011$$



偶然の図形であるが、capped　lady と(私は)呼んでいる。倍角の係数方程式

は・

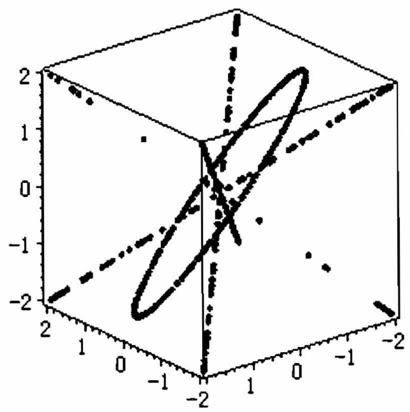
$$x^3-ax^2+(b-3)x-c+2a \otimes y+2-x^2 = y^3+(-a^3+2b)y^2+(-3+2b-2ac+b^3)y+2-4b-c^2+2b^2$$

であり、その解の分布は

$$C:\ \ f(x) = x(x^6+6)$$

$$x^3+(-a^3+2b)x^2+(-3+2b-2ac+b^3)x+2-4b-c^2+2b^2 = 0$$

$$p = 2\sim 2011$$



のような、一つの円と互いに斜めに貫通する 3 本の直線、円を含む平面と直交して中心を通る直線である。

次の図は、標準係数方程式

$$g(x) = x^3-ax^2+(b-3)x-c+2a = 0$$

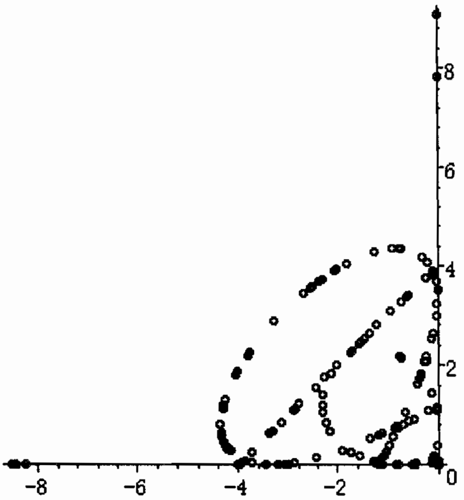
の二つの極値、極大値は正で極小値は負であるが、その対の $[g(u),g(v)]$ を xy-平面に plot したものの分布を描いたものである。当然、第 2 象限の図形である。

$$C:\ \ f(x) = x(x^6+6)$$

$$g(x) = x^3-ax^2+(b-3)x-c+2a = 0$$

$$[g(u),g(v)],\ g'(u) = g'(v) = 0,\ u < v$$

$$p = 2\sim 2011$$



綺麗な、曲線上に分布している様子がわかる。これは互いに接する、2 次曲線なのだろうか。微妙に異なるようにも見える…が。何れ、この曲線自体は明確になると思うが、曲線の正体が判明するのはずっと後になるかも知ない。軸の上の点は、極大か極小が 0 の点だから、勿論、重根をもつ場合である。

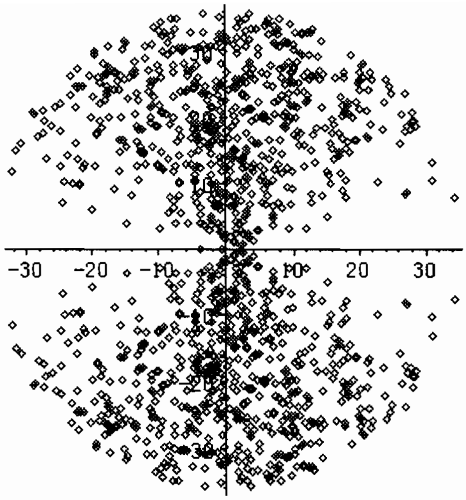
一般的な問題として、恐らくは、種数 3 の超楕円曲面の変形理論に於ける、退化曲面の類型などと関連しても興味ある問題であろうと思う。

問　題
正の密度でその上に分布するすべての部分多様体を決定すること

例 5.

$$C: y^2 = x^7+3x^6+2x^5-x^4-2x^3-2x^2-x-1$$

$$gal = D(7)\ ,\ det = 71^3,\ p = 2\sim1283$$



その角分布は $\sin^2\theta$ であろうと予想されている。特に、興味ある問題は、種数2の超楕円曲線を含め

$$\sin^2 2\theta$$

の分布密度をもつ超楕円曲線が存在するかという問題である。勿論、

$$\sin^2\theta + \sin^2 2\theta,\ \sin^2\theta + \sin^2 3\theta,\ \sin^2 2\theta + \sin^2 3\theta$$

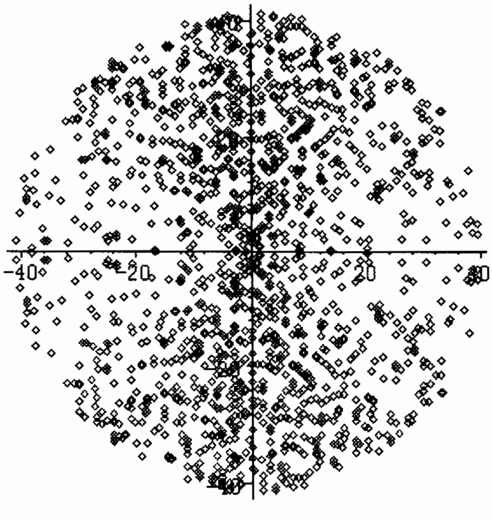
などの角分布をもつ曲線の存在も興味ある問題である。

例 6. $y^2 = x(x^6+ax^3+b)$ の形のもの

$$y^2 = x(x^3-4)(2x^3-9)$$

$$x^6+ax^5+bx^4+cx^3+bpx^2+ap^2x+p^3 = 0,$$

$$p = 2 \sim 1699$$

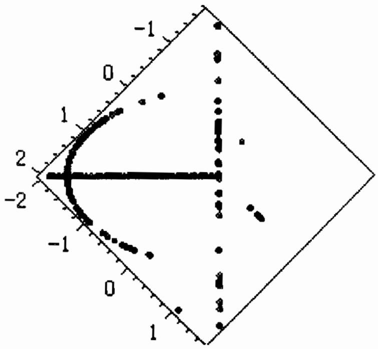


$$y^2 = x(x^3-4)(2x^3-9)$$

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

$$a = a_p/\sqrt{p},\ a = b_p/p,\ c = c_p/(p\sqrt{p})$$

$$p = 2 \sim 1699$$



この場合は3平面と半楕円筒面である。斜めの点線も恐らくは平面上の一直線上には位置していない。

この例は、数学セミナーの塩田徹治先生の記事[私の愛する等式]

立方と平方の差は X^3-Y^2 は？

の記事のなかの

$$f = t^4-4t,\quad g = t^6-6t^3+6,\quad h = 8t^3-36$$

(日本評論社、数学セミナー vol.45 no.2 /533. p.31. 2006.2.

[特集]美しき等式の世界)

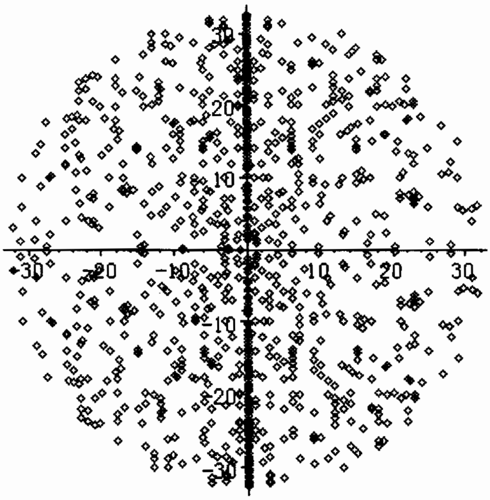
を参考にした。これらの式の背景には K3 曲面や E_8 のルートなどの対称性の関係が存在するという。

例 7.

$$y^2 = x(x^3-4)(x^3-8)$$

$$x^6+ax^5+bx^4+cx^3+bpx^2+ap^2x+p^3=0,$$

$$p = 2 \sim 1087$$



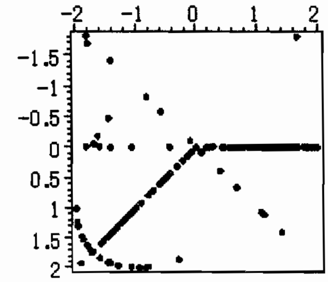
以下の図は、この超楕円曲線の標準係数多項式の 3 次方程式の標準的解法に従って求めた解の順に 3 重対(triple)として xyz-空間に表示したものである。各軸の方向への射影した形で示す。要点は、例 6 より更に微細な構造が見えることである。

$$y^2 = x(x^3-4)(x^3-8)$$

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

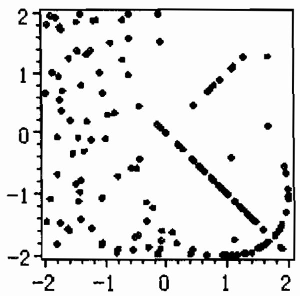
$$a = a_p/\sqrt{p},\ a = b_p/p,\ c = c_p/(p\sqrt{p})$$

$$p = 2 \sim 1087$$

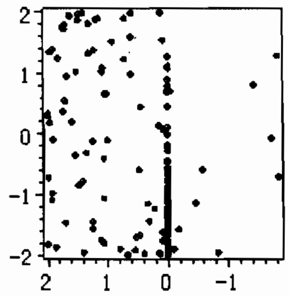


半楕円筒面の一部、対角線、稜の中点を結ぶ線分等はすべて、平面や曲面を線状に見える位置から見たものである。この図形を水平の中心線に従っ

て、90° 回転したものが次の図である。



従って、右半平面に現れた楕円の一部は、平面内の曲線で、上の図では直線に退化している。この図形を縦の中心線を中心に 90° 回転したものが次の図である。

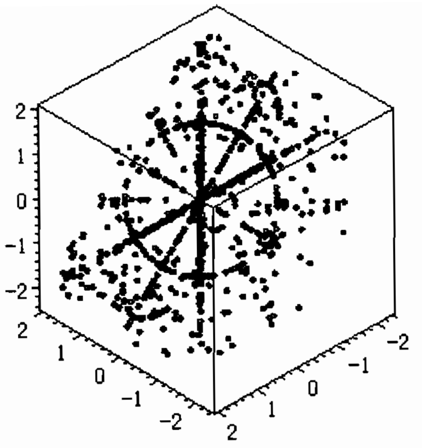


この図には、縦の中心線の外の明確な曲線は、今の私には、見えてない。

さて、3 根 x,y,z を順序を無視して、6 個の点

(x,y,z), (x,z,y), (y,x,z), (y,z,x), (z,x,y), (z,y,x)

として表示したものを、例えば、x+y-z と垂直な方向から見たものが次のものである。



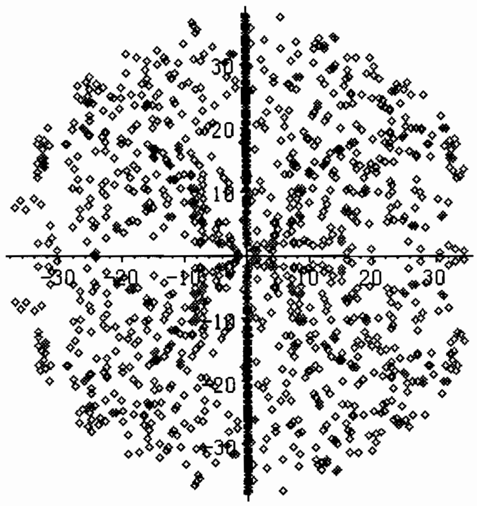
これは、図形が、半径 $\sqrt{2}$ の円筒面上にも、正の密度で分布していることを意味する。平面上の楕円を円筒の平面による切断面として見ていたのである。

例 8.　$y^2 = x(x^6+ax^4+bx^2+c)$、奇関数の例

$$y^2 = x(x^2-1)(x^2-4)(x^2-9)$$

$$x^6+ax^5+bx^4+cx^3+bpx^2+ap^2x+p^3 = 0$$

$$p = 2 \sim 1433$$

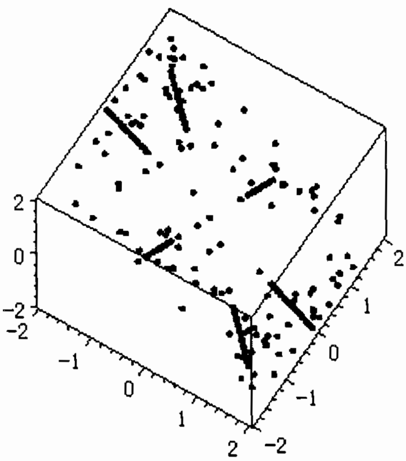


$$y^2 = x(x^2-1)(x^2-4)(x^2-9)$$

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

$$a = a_p/\sqrt{p},\ a = b_p/p,\ c = c_p/(p\sqrt{p})$$

$p = 2 \sim 1087$



この例では、平面上にある 3 本の互いに 60° の角度で交わる直線の一部となっている。

3. 係数方程式の判別式

種数 3 の超楕円曲線の係数多項式

$$x^3-ax^2+(b-3)x+2a-c$$

の判別式は、平行移動で不変だから、

$$\det(x^3-ax^2+(b-3)x+2a-c) =$$

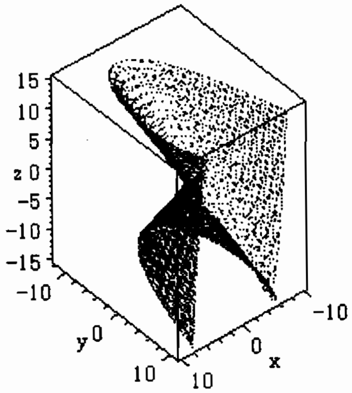
$$\det(x^3+(b-3-a^2/3)x-2a^3/27+a-c+b/3) =$$

$$27(c-(a+ab/3-2a^3/27))^2+4(b-(a^2/3+3))^3=$$

$$27c^2+(-18ab-54a+4a^3)c-9a^2-a^2b^2+42a^2b-108+108b-8a^4+4b^3-36b^2$$

で与えられる。判別式 = 0、つまり、係数方程式は標準係数方程式が重根をもつための必要十分条件である。これを表す曲面は、

$$27(z-(x+xy/3-2x^3/27))^2+4(y-(x^2/3+3))^3=0$$



のような、二つの放物面がくっついたような奇妙な曲面である。この曲面の特異点は

$$z-(x+xy/3-2x^3/27)=0,\quad y-(x^2/3+3)=0$$

で与えられ、

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

$$z=x+xy/3-2x^3/27=2x+x^3/27$$

なる助変数表示された曲線が特異多様体である。元の変数にもどり、例えば、変数 y に項 $x^2/3+3$ を代入する作用素(operator)、つまり、代入子(substitutor)と考えれば

$$x^3-ax^2+(b-3)x+2a-c\,[b=a^2/3+3,\ c=2a+a^3/27]=1/27\,(3x-a)^3$$

である。つまり、これは、標準係数多項式が完全立方となるための条件でもあった。

例 9. $y^2=x(x^6-33x^4-33x^2+1)$

この方程式で定まる超楕円曲線

$$C:\quad y^2=x(x^6-33x^4-33x^2+1)$$

の終結変換係数

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

について記す。この多項式は、正 12 面体に関係する多項式である。先ず、

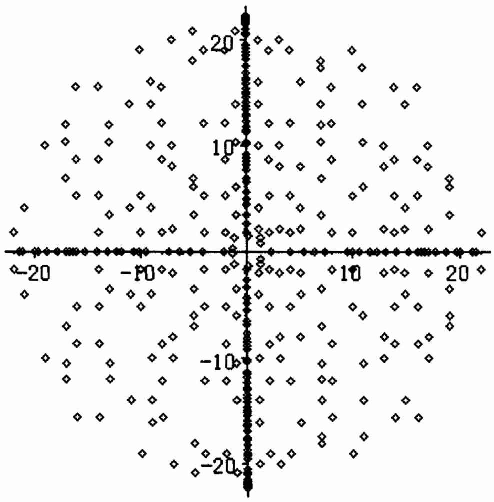
$$y^2=x(x^6-33x^4-33x^2+1)=x(x^2+1)(x^2-6x+1)(x^2+6x+1)$$

であり、終結変換方程式の根の分布と、係数方程式の根の様子を記す。

$$C:\quad y^2=x(x^6-33x^4-33x^2+1)$$

$$x^6+a_px^5+b_px^4+c_px^3+pb_px^2+p^2a_px+p^3 = 0$$

$$p = 2\sim659$$

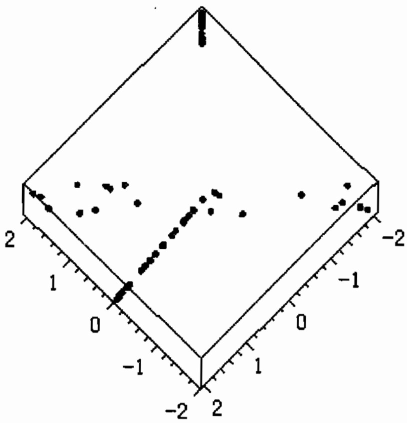


$$C: \quad y^2 = x\,(x^6-33x^4-33x^2+1)$$

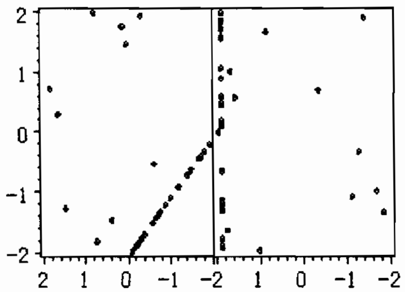
$$x^3-ax^2+(b-3)\,x-c+2a$$

$$a = a_p/\sqrt{p}\ ,\ b = b_p/p\ ,\ c = c_p/(p\sqrt{p})$$

$$p = 2\sim509$$



である。係数方程式の根は、1平面と原点と稜の中点を結ぶ線分、そして平面と平行な1稜の2直線からなっている。図では対角面が直線に見えないように少し傾けて表示している。



これは、係数方程式の解の2直線が原点を通る方向から見たものである。
以下が数値的なデータである。

$$C: \ y^2 = x(x^6-33x^4-33x^2+1)$$

$[p, a_p, b_p, c_p]$

$p = 2 \sim 509$

[[2, 0, -1, -2], [3, 0, 3, 0], [5, 2, -5, -20], [7, 0, 5, 0], [11, 0, 33, 0], [13, 2, 19, 76],
[17, 2, -17, -68], [19, 0, -7, 0], [23, 0, 69, 0], [29, 10, -29, -580], [31, 0, 77, 0],
[37, -22, 251, -1828], [41, 10, -41, -820], [43, 0, 65, 0], [47, 0, 141, 0],
[53, -14, -53, 1484], [59, 0, 177, 0], [61, 18, 99, 236], [67, 0, -55, 0], [71, 0, 213, 0],
[73, -14, 199, -1444], [79, 0, 221, 0], [83, 0, 249, 0], [89, 10, -89, -1780],
[97, 10, -17, -1588], [101, 2, -101, -404], [103, 0, -91, 0], [107, 0, 321, 0],
[109, 2, 307, 460], [113, -14, -113, 3164], [127, 0, -19, 0], [131, 0, 393, 0],
[137, -22, -137, 6028], [139, 0, 161, 0], [149, -14, -149, 4172], [151, 0, 437, 0],
[157, 50, 1283, 20012], [163, 0, 425, 0], [167, 0, 501, 0], [173, 26, -173, -8996],
[179, 0, 537, 0], [181, -70, 2155, -37508], [191, 0, 573, 0], [193, 10, 527, 3916],
[197, 2, -197, -788], [199, 0, -187, 0], [211, 0, 377, 0], [223, 0, -115, 0],
[227, 0, 681, 0], [229, 74, 2491, 48412], [233, 26, -233, -12116], [239, 0, 717, 0],
[241, 58, 1759, 33836], [251, 0, 753, 0], [257, 2, -257, -1028], [263, 0, 789, 0],
[269, 26, -269, -13988], [271, 0, 29, 0], [277, -70, 2443, -50948], [281, 10, -281, -5620],
[283, 0, -175, 0], [293, 34, -293, -19924], [307, 0, 665, 0], [311, 0, 933, 0],
[313, 18, 279, -1316], [317, -22, -317, 13948], [331, 0, -31, 0], [337, -86, 3391, -78772],

[347, 0, 1041, 0], [349, 18, 963, 10604], [353, 34, -353, -24004], [359, 0, 1077, 0],
[367, 0, 1085, 0], [373, 90, 3627, 87356], [379, 0, 1073, 0], [383, 0, 1149, 0],
[389, 34, -389, -26452], [397, -30, -237, 20108], [401, 2, -401, -1604],
[409, 82, 3127, 75740], [419, 0, 1257, 0], [421, 74, 3067, 76828], [431, 0, 1293, 0],
[433, -38, 1439, -33044], [439, 0, 533, 0], [443, 0, 1329, 0], [449, -14, -449, 12572],
[457, -62, 2311, -60868], [461, -38, -461, 35036], [463, 0, 989, 0], [467, 0, 1401, 0],
[479, 0, 1437, 0], [487, 0, -475, 0], [491, 0, 1473, 0], [499, 0, 473, 0], [503, 0, 1509, 0],
[509, 10, -509, -10180]]

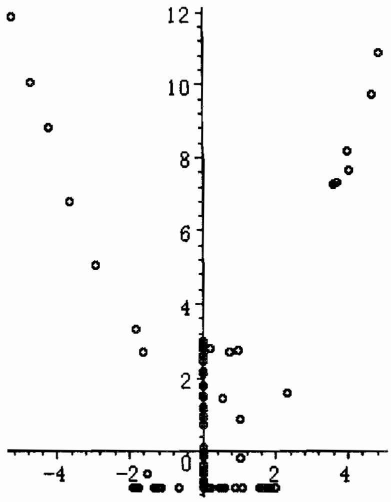
先ず、標準係数 (normalized coefficient)

$$a = a_p/\sqrt{p}\ ,\ b = b_p/p\ ,\ c = c_p/(p\sqrt{p})$$

の最初の関係[a,b]の対を xy-平面に図示してみる。結果は、

$$C: \quad y^2 = x(x^6-33x^4-33x^2+1)$$

$$[a_p, b_p],\ p = 2 \sim 509$$



である。特徴的なのは、線分 y = -1 の[-2,2]の部分と、x = 0 の[-1,3]の部分である。この線分の上端は[0,3]で、p = 509 までの 97 個の素数のうち 26 個が[0,3]である。26/97 ≒ 1/4 であろうか。また、y = -1 の上に分布するものも 24 個であり、これも、24/97 ≒ 1/4 であろう。従って、半数の素数では

$$b_p = -p,\ 3p$$

である。

第一の場合は $a = a_p/\sqrt{p} = 0$ の場合で、

[[2, 0, -1, -2], [3, 0, 3, 0], [7, 0, 5, 0], [11, 0, 33, 0], [19, 0, -7, 0], [23, 0, 69, 0],

[31, 0, 77, 0], [43, 0, 65, 0], [47, 0, 141, 0], [59, 0, 177, 0], [67, 0, -55, 0],
[71, 0, 213, 0], [79, 0, 221, 0], [83, 0, 249, 0], [103, 0, -91, 0], [107, 0, 321, 0],
[127, 0, -19, 0], [131, 0, 393, 0], [139, 0, 161, 0], [151, 0, 437, 0], [163, 0, 425, 0],
[167, 0, 501, 0], [179, 0, 537, 0], [191, 0, 573, 0], [199, 0, -187, 0], [211, 0, 377, 0],
[223, 0, -115, 0], [227, 0, 681, 0], [239, 0, 717, 0], [251, 0, 753, 0], [263, 0, 789, 0],
[271, 0, 29, 0], [283, 0, -175, 0], [307, 0, 665, 0], [311, 0, 933, 0], [331, 0, -31, 0],
[347, 0, 1041, 0], [359, 0, 1077, 0], [367, 0, 1085, 0], [379, 0, 1073, 0], [383, 0, 1149, 0],
[419, 0, 1257, 0], [431, 0, 1293, 0], [439, 0, 533, 0], [443, 0, 1329, 0], [463, 0, 989, 0],
[467, 0, 1401, 0], [479, 0, 1437, 0], [487, 0, -475, 0], [491, 0, 1473, 0], [499, 0, 473, 0],
[503, 0, 1509, 0]]

全部で 52/97 であり約半数である。グラフは原点と稜の中点を結ぶ直線である。係数方程式の形は

$$x^3-x^2a+(b-3)x+2a-c = (x^2-k)x、\ k \geq 0$$

の形で、k = 0 は[p, 0, 3p, 0]場合で 1/4 の割合で像は原点、つまり、方程式は $x^3 = 0$ である。

次の場合は

[[5, 2, -5, -20], [17, 2, -17, -68], [29, 10, -29, -580], [41, 10, -41, -820],
[53, -14, -53, 1484], [89, 10, -89, -1780], [101, 2, -101, -404], [113, -14, -113, 3164],
[137, -22, -137, 6028], [149, -14, -149, 4172], [173, 26, -173, -8996], [197, 2, -197, -788],
[233, 26, -233, -12116], [257, 2, -257, -1028], [269, 26, -269, -13988],
[281, 10, -281, -5620], [293, 34, -293, -19924], [317, -22, -317, 13948],
[353, 34, -353, -24004], [389, 34, -389, -26452], [401, 2, -401, -1604],
[449, -14, -449, 12572], [461, -38, -461, 35036], [509, 10, -509, -10180]]

この場合は立方体の稜で、方程式は

$$(x^2-4)(\sqrt{p}x-k)$$

の形をしている。

最後の場合は、上記のいずれの場合でもない場合で、

[[13, 2, 19, 76], [37, -22, 251, -1828], [61, 18, 99, 236], [73, -14, 199, -1444],
[97, 10, -17, -1588], [109, 2, 307, 460], [157, 50, 1283, 20012], [181, -70, 2155, -37508],
[193, 10, 527, 3916], [229, 74, 2491, 48412], [241, 58, 1759, 33836],
[277, -70, 2443, -50948], [313, 18, 279, -1316], [337, -86, 3391, -78772],
[349, 18, 963, 10604], [373, 90, 3627, 87356], [397, -30, -237, 20108],

$$[409, 82, 3127, 75740], [421, 74, 3067, 76828], [433, -38, 1439, -33044],$$

$$[457, -62, 2311, -60868]]$$

などの場合で、係数方程式は重根をもっている。方程式は

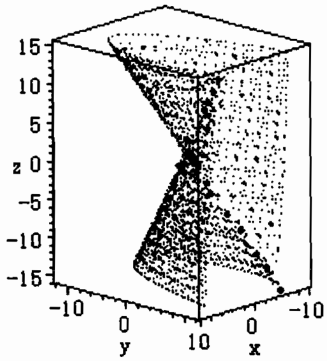
$$(\sqrt{p}x+k)(\sqrt{p}x+h)^2$$

の形で、判別式は当然ながら 0 である。

$$\det(x^3-ax^2+(b-3)x+2a-c) =$$

$$27c^2+(-18ab-54a+4a^3)c-9a^2-a^2b^2+42a^2b-108+108b-8a^4+4b^3-36b^2=0$$

この曲面上に点は分布している。



現実には、この曲面の上にはあるが、稜の上にはなくて、少し差がある。先ず、稜の方程式を求める。

$$f(x,y,z) = -9x^2-54xz+42x^2y+27z^2-18zxy-x^2y^2-8x^4+4x^3z-108+108y-36y^2+4y^3$$

の特異点の集合を求める

$$\partial f/\partial x(x,y,z) = -18x-54z+84xy-18zy-2xy^2-32x^3+12x^2z$$

$$\partial f/\partial y(x,y,z) = 42x^2-18xz-2x^2y+108-72y+12y^2$$

$$\partial f/\partial z(x,y,z) = -54x+54z-18xy+4x^3$$

である。$\partial f/\partial z(x,y,z)=0$ から、z は簡単に求まって

$$z = x+xy/3-2x^3/27$$

となる。これを代入すると

$$\partial f/\partial x(x,y,z) = -18x-54z+84xy-18zy-2xy^2-32x^3+12x^2z = -8/9\cdot x(3y-9-x^2)^2$$

$$\partial f/\partial y(x,y,z) = 42x^2-18xz-2x^2y+108-72y+12y^2 = 4/3(3y-9-x^2)^2$$

である。従って、最初の 3 個の方程式は独立ではなかったのである。共通

の因数 $3y-9-x^2$ から、$y=x^2/3+3$ が求まり、結局、

$$z = x+xy/3-2x^3/27 = 2x+x^3/27$$

となる。これから、$[x, x^2/3+3, 2x+x^3/27]$、あるいは、代入子 (substitutor)

$$[y = x^2/3+3,\ z = 2x+x^3/27]$$

が求まる。事実、

$$f(x, x^2/3+3, 2x+x^3/27) = 0$$

が、恒等的に成り立つことが解る。これが、特異点の助変数表示である。

現実の点は、この曲面上に存在し特異点の近くには位置するが、この特異点集合には属していない。つまり、完全立方にはなっていない。

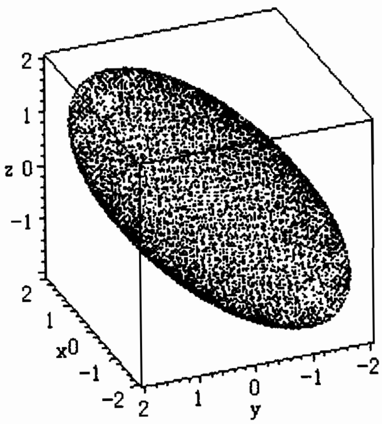
4. 立方体に内接する超楕円体について

ここでは、xyz-空間の立方体 $[-2,2]^3$ に内接する超楕円曲曲面、例えば、基本対称式

$$x+y+z,\quad xy+yz+zx$$

で記述できる次の内接曲面を考える：

$$3(x^2+y^2+z^2)-2(xy+yz+zx) = 8$$



先ず、求める方程式を

$$f(x,y,z) = 1+a(x+y+z)^2+b(xy+yz+zx) = 0$$

として、平面 $z=2$ に接する条件を求めてみよう。

$$\mathrm{grad}(f(x,y,2),[x,y]) = [\partial f/\partial x(x,y,2),\ \partial f/\partial y(x,y,2)]$$

$$= [2a(x+y+2)+b(y+2),\ 2a(x+y+2)+b(x+2)]$$

接平面が z＝2 と一致するための条件として、

$$2a(x+y+2)+b(y+2)=0$$

$$2a(x+y+2)+b(x+2)=0$$

を得る。これを x,y について解くと、

$$x=-2(2a+b)/(4a+b),\ y=-2(2a+b)/(4a+b)$$

であり、これを、f(x,y,2) に代入すると

$$-(-4a+12ab+4b^2-b)/(4a+b)=0$$

を得る。これを a について解くと

$$a=-1/4\cdot b(4b-1)/(-1+3b)$$

となり、f(x,y,z) の係数に代入すると、

$$1-1/4\cdot b(4b-1)(x+y+z)^2/(-1+3b)+b(xy+yz+zx)$$

あるいは、分母を払って

$$4(3b-1)-b(4b-1)(x+y+z)^2+4b(3b-1)(xy+yz+zx)=0$$

を得る。例えば、b＝1 とすると、

$$8-3(x+y+z)^2+8(xy+yz+zx)=8-3(x^2+y^2+z^2)+2(xy+yz+zx)=0$$

で、最初の例に与えたものである。

さて、種数 3 の超楕円曲線は、7 次多項式 f(x) を用いて

$$y^2=f(x)$$

に記することができ、その終結変換多項式は

$$x^6+a_px^5+b_px^4+c_px^3+pb_px^2+p^2a_px+p^3$$

その標準係数方程式は

$$x^3-ax^2+(b-3)x-c+2a$$

$$a=a_p/\sqrt{p},\ b=b_p/p,\ c=c_p/(p\sqrt{p})$$

で得られる。従って、

$$a=x+y+z,\ b-3=xy+yz+zx$$

であるから、

$$4(3t-1)-t(4t-1)a^2/p+4t(3t-1)(b-3)/p=0$$

であり、これを t について整理すると

$$(4a^2-12b+36p)t^2+(-24p-a^2+4b)t+4p=0$$

を得る。あるいは逆数 x＝1/t の方程式として

$$4px^2+(-24p-a^2+4b)x+(4a^2-12b+36p)=0$$

の方が適当であろうか。

例 10. 超楕円曲線

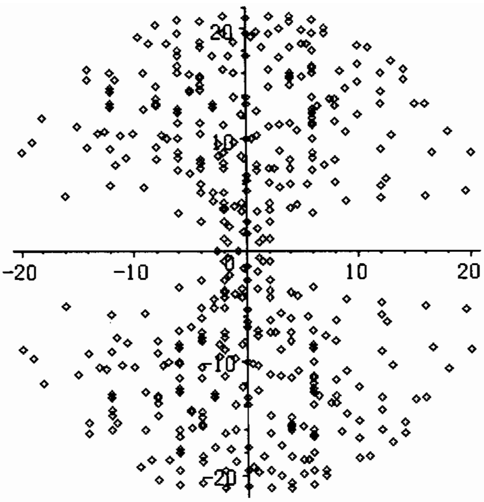
$$C:\quad y^2 = -x(x^3-2)(2x^3-1)$$

の場合。

[[2, -1, -2, -4], [3, -1, 0, 0], [5, 2, -1, -12], [7, -6, 30, -84], [11, 4, 17, 24],
[13, 0, 36, 2], [17, -2, 35, -36], [19, -6, 66, -232], [23, -8, 53, -240], [29, -6, 87, -348],
[31, 0, 45, 128], [37, 12, 84, 402], [41, 6, 123, 492], [43, -12, 129, -776], [47, 0, -3, 0],
[53, 2, 95, 84], [59, 4, 161, 408], [61, 12, 228, 1514], [67, 18, 234, 1928],
[71, 8, 149, 624], [73, -12, 240, -1762], [79, -18, 342, -3044], [83, -4, 185, -408],
[89, 6, 123, 204], [97, -12, 336, -2378], [101, 18, 303, 3636], [103, 18, 342, 3724],
[107, -12, 177, -840], [109, 30, 579, 6932], [113, -18, 195, -1476], [127, 0, 333, -128],
[131, -4, 137, -24], [137, 6, 267, 780], [139, 6, 282, 696], [149, -14, 383, -3276],
[151, -18, 486, -5452], [157, 6, 483, 1892], [163, -18, 354, -3168], [167, 24, 357, 4560],
[173, -6, 519, -2076], [179, 12, -39, -2616], [181, -48, 1236, -20022], [191, 0, 429, 0],
[193, -48, 1200, -19586], [197, 18, 447, 4500], [199, 66, 2022, 36268], [211, 6, 282, -848],
[223, 0, 621, -128], [227, 12, 105, -1464], [229, -42, 1227, -21436], [233, -10, 443, -2100],
[239, -16, 653, -6624], [241, 12, 408, 1734], [251, 20, 497, 4920], [257, -2, 707, -900],
[263, -8, 725, -3696], [269, 10, 791, 5220], [271, -42, 1038, -17764], [277, 6, 411, 5924],
[281, -26, -181, 12012], [283, -60, 2001, -41128], [293, 18, 735, 7956],
[307, 12, 921, 7368], [311, -24, 789, -11472], [313, 0, 912, 54], [317, -6, 375, -348],
[331, 54, 1962, 41528], [337, -12, 912, -8250], [347, -12, 465, -1416],
[349, 36, 156, -7542], [353, -2, 995, -1284], [359, -24, 933, -13776],
[367, -54, 1998, -43868], [373, 12, 1140, 8962], [379, 42, 1698, 34256],
[383, 0, 1149, 0], [389, 2, 1151, 1524], [397, -42, 1779, -36092],
[401, 30, 627, 6780], [409, 84, 3216, 77838], [419, 12, 1113, 8328],
[421, -24, 1212, -17318], [431, 32, 509, 2496], [433, 42, 1887, 39116],
[439, 72, 2613, 63216], [443, 20, 1265, 16440], [449, 14, 1331, 12348],
[457, -54, 1143, -17588], [461, 26, 599, 3588], [463, -30, 1446, -24892],
[467, -36, 1257, -28440], [479, -16, -163, 10272]]

$$C:\quad y^2 = -x(x^3-2)(2x^3-1)$$

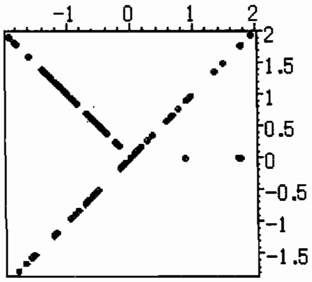
$$p = 2 \sim 487$$



C: $y^2 = -x(x^3-2)(2x^3-1)$

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

$p = 2 \sim 487$



このデータ[p,a,b,c]に対して

$$px^2+(b-6p-a^2/4)x+(a^2-3b+9p) = 0$$

を因数分解した結果は

$[1/4 \cdot (8x-25)(x-4)]$, $[3x^2-73x/4+28]$, $[5x^2-32x+52]$, $[7x^2-21x+9]$, $[11x^2-53x+64]$,
$[(13x-3)(x-3)]$, $[17x^2-68x+52]$, $[19x^2-57x+9]$, $[23x^2-101x+112]$, $[29x^2-96x+36]$,
$[(31x-48)(x-3)]$, $[37x^2-174x+225]$, $[41x^2-132x+36]$, $[43x^2-165x+144]$, $[(x-3)(47x-144)]$,
$[53x^2-224x+196]$, $[59x^2-197x+64]$, $[61x^2-174x+9]$, $[67x^2-249x+225]$, $[71x^2-293x+256]$,

$[73x^2-234x+81]$, $[79x^2-213x+9]$, $[83x^2-317x+208]$, $[89x^2-420x+468]$, $[97x^2-282x+9]$

などである。

既約でないものは $p = 2$ の場合を除いて、つまり、すべての奇素数に対して、可約ならば、この範囲では、因数 $x-3$ を含む。

$$[(13x-3)(x-3),\ (31x-48)(x-3),\ (x-3)(47x-144),\ (127x-48)(x-3),$$
$$(191x-144)(x-3),\ (223x-48)(x-3),\ (313x-27)(x-3),\ 383x(x-3)$$

しかし、x で割れるものもかなり存在する。$p = 383$ は共通の $x(x-3)$ である。

$$[x(157x-468),\ 383x(x-3),\ x(397x-1044),\ x(433x-1152)]$$

もとの方程式は

$$4(3t-1)-t(4t-1)(x+y+z)^2+4t(3t-1)(xy+yz+zx) = 0$$

であり、$x = 1/t$ とおいた（この場合は x は重複しているが別の変数）ので

$$x = 3,\ x = 0$$

は $t = 1/3, \infty$ に相当している。$t = 1/3$ のときは、$3t-1 = 0$ であるから、

$$4(3t-1)-t(4t-1)(x+y+z)^2+4t(3t-1)(xy+yz+zx) = -(x+y+z)^2/9 = 0$$

であり、

$$a = a_p/\sqrt{p} = x+y+z = 0$$

に相当している。事実、

$$[13, 0, 36, 2],\ [31, 0, 45, 128],\ [47, 0, -3, 0],\ [127, 0, 333, -128],\ \cdots$$

である。係数方程式の因数分解は

$$(\sqrt{13}x-2)(\sqrt{13}x+1)^2,\ (-\sqrt{31}x+8)(\sqrt{31}x+4)^2,\ x(47x^2-144),\ (\sqrt{127}x+8)(\sqrt{127}x-4)^2,$$
$$x(191^2-144),\ (\sqrt{223}x+8)(\sqrt{223}x-4)^2,\ (\sqrt{313}x-6)(\sqrt{313}x+3)^2,\ x^3$$

となっている。勿論、重複因子をもつことの必要条件にはなっていない。

$t = \infty$ であれば、t^2 の係数の比と考えて

$$(x+y+z)^2-3(xy+yz+zx) = x^2+y^2+z^2-(xy+yz+zx) = 1/2\cdot((x-y)^2+(y-z)^2+(z-x)^2) = 0$$

であり、これは $x = y = z$、つまり、3 重根でのみ許される。対応する場合は

$$x(157x-468),\ 383x(x-3),\ x(397x-1044),\ x(433x-1152)$$

であるが、係数方程式 $x^3-ax^2+(b-3)x-c+2a$ の因数分解の様子は

$$(157x-2\sqrt{157})^3,\ x^3,\ (397x+14\sqrt{397})^3,\ (433x-14\sqrt{433})^3$$

の 3 重根の場合である。

さて、超楕円曲面方程式（hyper-elliptic rsolution equation）

$$px^2+(b-6p-a^2/4)x+(a^2-3b+9p) = 0$$

の解は実数とは限らない。

[2, 25/8, 4], [3, $73/24\pm\sqrt{47}/24\cdot i$], [5, $16/5\pm2/5\cdot i$], [7, $3/2\pm3\sqrt{21}/14$)], [11, $53/22\pm\sqrt{7}/22\cdot i$],
[13, 3/13, 3], [17, $2\pm4/\sqrt{17}$], [19, $3/2\pm3\sqrt{285}/38$], [23, $101/46\pm\sqrt{103}/46\cdot i$],
[29, $48/29\pm6\sqrt{35}/29$], [31, 48/31, 3], [37, $87/37\pm6\sqrt{21}/37$], [41, $66/41\pm24\sqrt{5}/41$],
[43, $165/86\pm3\sqrt{273}/86$], [47, 3, 144/47], [53, $112/53\pm14\sqrt{11}/53$], [59, $197/118\pm\sqrt{23705}/118$],
[61, $87/61\pm6\sqrt{195}/61$], [67, $249/134\pm9\sqrt{21}/134$], [71, $293/142\pm\sqrt{13145}/142$],
[73, $117/73\pm36\sqrt{6}/73$], [79, $213/158\pm45\sqrt{21}/158$], [83, $317/166\pm43\sqrt{17}/166$],
[89, $210/89\pm12\sqrt{17}/89$)], [97, $141/97\pm24\sqrt{33}/97$]

である。実根のものは

2, 7, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 127, 131, 137, 139, 149, 151, 163, 173, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 283, 293, 307, 311, 313, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 409, 419, 421, 433, 443, 449, 463, 467, …

であり、虚根のものは

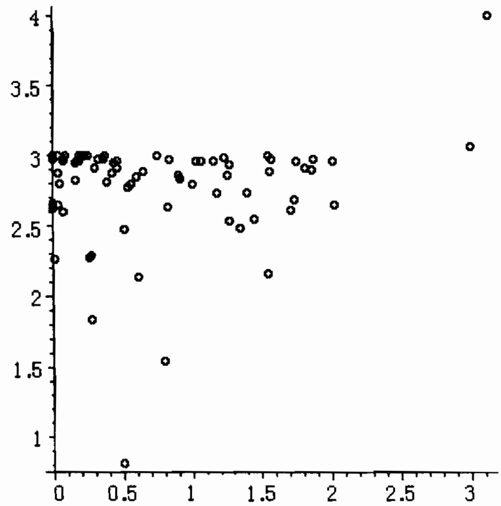
3, 5, 23, 37, 113, 167, 179, 227, 271, 281, 349, 401, 409, 431, 439, 457, 461, 479, …

と、数は比較的少ないけれどかなり存在する。

下の図は、分解方程式が実根をもつ場合の 2 根をその大きさの順の対として xy-平面に図示したものである。

$$C:\quad y^2 = -x(x^3-2)(2x^3-1)$$

$$px^2 + (b-6p-a^2/4)x + (a^2-3b+9p) = 0,\ p = 2 \sim 487$$



特に注目する点は見えないようである。

例 7′. $y^2 = x(x^3-4)(x^3-8)$

これは、既に例7として考察したものであるが、他の観点から検討する。

$$y^2 = x(x^3-4)(x^3-8)$$

[[2, -1, -2, -4], [3, 0, 3, 0], [5, 2, 11, 12], [7, -3, 9, -42], [11, 0, -3, 0],
[13, -9, 27, -54], [17, -2, 47, -60], [19, 3, 9, 114], [23, 0, 33, 0], [29, 10, 23, -60],
[31, 0, 93, 0], [37, 9, 63, 542], [41, -10, 59, -180], [43, -24, 273, -2064], [47, 0, 105, 0],
[53, -14, 143, -1260], [59, 0, 141, 0], [61, 9, -9, -722], [67, 3, 9, 402], [71, 0, 69, 0],
[73, -9, 135, -1278], [79, -9, 81, -1422], [83, 0, 105, 0], [89, -10, 167, -780],
[97, -9, -81, 2034], [101, 2, 47, -108], [103, -15, 225, -3090], [107, 0, 285, 0],
[109, -18, 435, -4140], [113, 14, 143, 420], [127, -24, 525, -6096], [131, 0, 393, 0],
[137, 22, 215, 1716], [139, 21, 441, 5838], [149, -14, 431, -3948], [151, 3, 9, 906],
[157, 6, 51, -2428], [163, -3, 9, -978], [167, 0, 177, 0], [173, 26, 455, 7332],
[179, 0, 393, 0],[181, 27, 243, 1458], [191, 0, 537, 0], [193, 9, -45, -4282],
[197, 2, 587, 780],[199, -15, 225, -5970], [211, -15, 225, -6330], [223, -48, 1245, -21408],
[227, 0, 537, 0],[229, -18, 363, -9324], [233, -26, 635, -10452], [239, 0, 573, 0],
[241, 27, -81, -8406],[251, 0, 753, 0], [257, -2, 371, -228], [263, 0, 645, 0],
[269, 26, 707, 11388],[271, 15, 225, 8130], [277, 54, 1803, 35748], [281, -10, 779, -4980],
[283, 24, 993, 13584],[293, 34, 875, 19788], [307, 24, 1065, 14736], [311, 0, 609, 0],
[313, -27, 27, 7486],[317, -22, 935, -13596], [331, -3, 9, -1986], [337, -9, -81, 10674],
[347, 0, 897, 0],[349, 9, -9, -4178], [353, -34, 659, -10404], [359, 0, 753, 0],
[367, -3, 9, -2202],[373, 9, 207, 14974], [379, 27, 729, 20466], [383, 0, 1149, 0],
[389, 34, 11, -12852],[397, -42, 1347, -33500], [401, -2, 803, -804], [409, 27, 567, 17370],
[419, 0, 357, 0],[421, -45, 675, -6750], [431, 0, 393, 0], [433, -30, 1167, -26116],
[439, 0, 1317, 0],[443, 0, 1185, 0], [449, 14, 863, 5796], [457, 18, -249, -21348],
[461, -38, 1379, -34884],[463, -15, 225, -13890], [467, 0, 1365, 0], [479, 0, 1293, 0],
[487, -15, 225, -14610],[491, 0, -291, 0], [499, 48, 2073, 47904], [503, 0, -255, 0],
[509, 10, 1427, 9180],[521, 22, 1367, 18612], [523, -9, 81, -9414], [541, 27, -405, -29502],
[547, 9, 81, 9846],[557, -38, 1667, -42180], [563, 0, 1113, 0], [569, -26, -409, 25428],
[571, 3, 9, 3426],[577, 9, 99, 13606], [587, 0, 1437, 0], [593, 46, 995, 18492],
[599, 0, 1221, 0],[601, 42, 1959, 43724], [607, -3, 9, -3642], [613, 45, 495, -3242],
[617, 38, 1847, 46740],[619, -9, 81, -11142], [631, 27, 729, 34074],
[641, -50, 1907, -63300],[643, -72, 3225, -92592], [647, 0, 1365, 0],

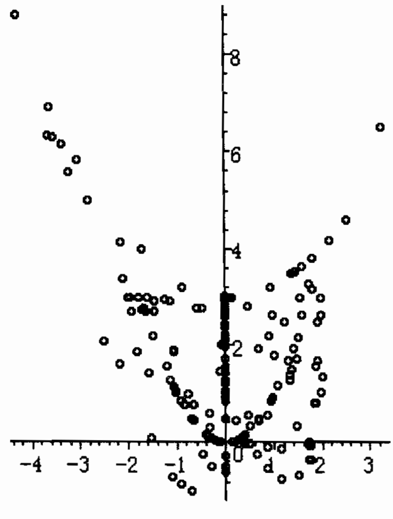
[653, 26, 1175, 13572], [659, 0, 1833, 0],[661, 45, -225, -38410], [673, 45, -45, -32258],
[677, 2, 2027, 2700], [683, 0, 1473, 0],[691, 24, 2217, 33168], [701, 10, -13, -7140],
[709, -81, 4131, -129078], [719, 0, 861, 0],[727, 48, 2757, 69792], [733, -18, 579, -43884],
[739, -24, 2361, -35472], [743, 0, 2193, 0],[751, -45, 2025, -67590],
[757, -9, 243, -41382], [761, 38, 1127, 13908],[769, -99, 4851, -156962],
[773, 34, 1919, 38964], [787, 27, 729, 42498],[797, -22, 791, 132], [809, -10, 491, 3180],
[811, 72, 3729, 116784], [821, 50, -37, -42900],[823, -9, 81, -14814], [827, 0, 2445, 0],
[829, -9, -405, 10026], [839, 0, 1221, 0],[853, -99, 5247, -180394],
[857, -58, 2555, -98484], [859, -27, 729, -46386], [863, 0, 825, 0],[877, 45, -585, -63866],
[881, -50, 2447, -78300], [883, 9, 81, 15894], [887, 0, 1365, 0],[907, 39, 1521, 70746],
[911, 0, 429, 0], [919, 48, 3333, 88224], [929, 46, 2003, 49404],[937, 45, 315, -20626],
[941, 58, 2339, 81084], [947, 0, 2517, 0], [953, -26, 743, 5460],[967, -33, 1089, -63822],
[971, 0, 2877, 0], [977, 62, 995, 1116], [983, 0, 2913, 0],[991, 21, 441, 41622],
[997, -114, 6891, -269228], [1009, 27, -81, -36054],[1013, -46, 2939, -88596],
[1019, 0, 1761, 0], [1021, -138, 8979, -355804],[1031, 0, 3057, 0], [1033, 27, 567, 39834],
[1039, -27, 729, -56106]]

以下は、これらの分布を平面の方向に射影したものである。

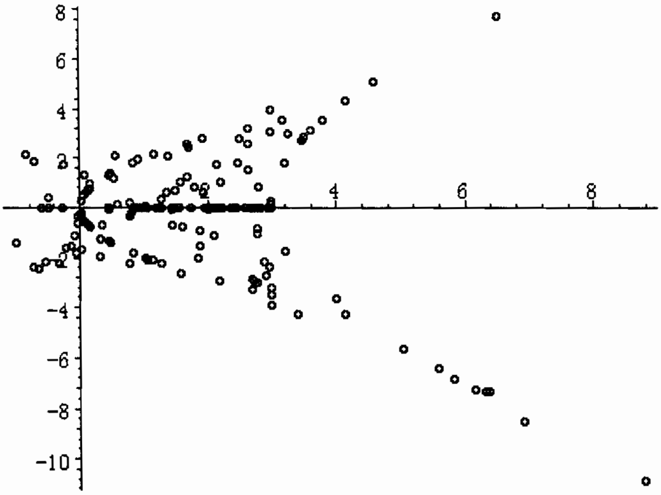
C: $y^2 = x(x^3-4)(x^3-8)$

[a,b]

p = 2 ~ 1039



[b,c]



以下のものは、上記の $[p, a_p, b_p, c_p]$ の表から

$$(-4+12t)p-t(4t-1)a_p^2+4t(-1+3t)(b_p-3p)$$

を求めたものを素因数分解したものの表である。

$[2, -8+105t/2-86t^2]$, $[3, -4(-1+3t)(8t-3)]$, $[5, -4/5(14t-5)^2]$, $[7, -28+1149t/7-1692t^2/7]$,

$[11, -4/11(366t-121)(-1+3t)]$, $[13, -52+4029t/13-468t^2]$, $[17, -68+6752t/17-9856t^2/17]$,

$[19, -76+8637t/19-12924t^2/19]$, $[23, -4/23(-1+3t)(1554t-529)]$,

$[29, -116+20192t/29-30400t^2/29]$, $[31, -4(-1+3t)(90t-31)]$, $[37, -148+32685/37t-48852t^2/37]$,

$[41, -164+40208t/41-60208t^2/41]$, $[43, -172+1020t-65592t^2/43]$,

$[47, -4/47(-1+3t)(6522t-2209)]$, $[53, -212+67040t/53-100192t^2/53]$,

$[59, -4/59(-1+3t)(10302t-3481)]$, $[61, -244+89421t/61-134388t^2/61]$,

$[67, -268+107709t/67t-161532t^2/67]$, $[71, -4/71(-1+3t)(15054t-5041)]$,

$[73, -292+127437t/73-190548t^2/73]$, $[79, -316+149541t/79-224028t^2/79]$,

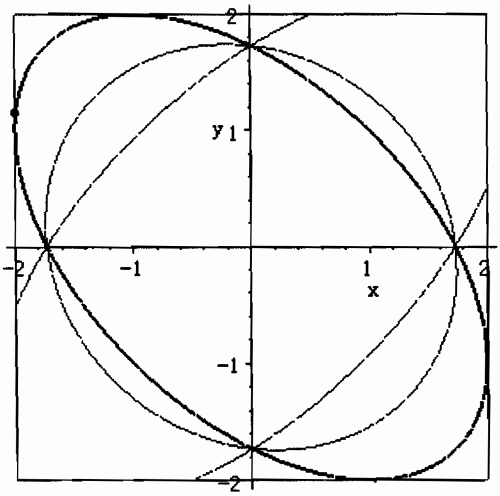
$[83, -4/83(-1+3t)(20562t-6889)]$, $[89, -356+189536t/89-283552t^2/89]$,

$[97, -388+226221t/97-340020t^2/97]$

標準係数方程式の解が明確な、代数曲面、代数曲線を示しているにもかかわらず式にはうまく表現できていない。

そこで、初心に帰って、平面の図形から検討する。正方形 $[-2,2]^2$ に内接する楕円について考える。楕円の代表的なもの〻一つは

$$x^2+xy+y^2-3=0$$



である。図の点は $y^2 = x(x^3-4)(x^3-8)$ の $p = 13$ での一つの因数

$$f(x) = 13x^2+3x\sqrt{13}-30$$

の 2 根

$$-1.991070934,\ 1.159020640$$

を x,y 座標として xy-平面に plot したもので、確かに、$x^2+xy+y^2-3 = 0$ 上にあることが解る。 このことは、終結式を用いて

$$f(x) ⓧ\ x^2+xy+y^2-3\ ⓨ\ f(y) = 0$$

によって示すこともできる。例えば、余談であるが、

$$f(x) ⓧ\ x^2+txy+y^2-3\ ⓨ\ f(y) = 231344100(100t^2+101t-29)(t-1)^2 = 0$$

は $t = 1$ を重根にもつ、他の 2 根

$$t = -101/200 \pm 13\sqrt{129}/200 = 0.2332580850,\ -1.243258085$$

に応ずる楕円も記しておいたが、これは直接には関係のないものである。

さて、もとに戻って、正方形 $[-2,2]^2$ に内接する楕円の助変数表示を求めておこう。

$$f(x,y) = 1+a(x+y)^2+bxy$$

は x,y の 2 次以下の偶数次の基本対称式の一次結合である。直線 $y = 2$ に接する条件として、連立方程式

$$f(x,2) = 1+a(x+2)^2+2bx = 0$$

$$f'(x,2) = \partial f/\partial x(x,2) = 2a(x+2)+2b = 0$$

を得る。これから、x を消去すると、

$$1+a(x+2)^2+2bx\ ⓧ\ 2a(x+2)+2b = -4a(-a+4ab+b^2) = 0$$

である。$a \neq 0$ ならば、

$$-a+4ab+b^2 = 0$$

であるから、a について解いて $a = -b^2/(4b-1)$ を得る。これを $f(x,y)$ に代入して分母を払い、b を別の変数 t に変えると

$$4t-1-t^2(x+y)^2+t(4t-1)xy = 0$$

を得る。

ここで、奇妙なことがおこる。図形の対称性から、上記の表記で y を -y に置き換えた表示

$$4s-1-s^2(x-y)^2-s(4s-1)xy = 0$$

もまた、正方形に内接する楕円の表示である。後者は、定数の比を除いて、前者の別の助変数表示になっているのであろうか。これを確かめる為、例えば、x^2 の係数を消去すると、

$$s^2(4t-1-t^2(x+y)^2+t(4t-1)xy)-t^2(4s-1-s^2(x-y)^2-s(4s-1)xy) = (t-s)(s+t-4st+stxy)$$

となり、xy の項の係数の st が一般には残り、これらの表示はそれぞれ正方形に内接する楕円形のすべてを表示している訳ではないことが解る。少なくとも、裏返しで等価な表示ではなかったことが解る。

では、一般的を想定しながら、如何にして、「非対称性」が入り込んできたのであろうか。推論の仮定の部分、つまり、最初の出発点に問題があるとしか思えない。つまり、対称式(symmetric form)を意識して、

$$f(x,y) = 1+a(x+y)^2+bxy$$

を考えた時点で、交代式(alternating form)

$$f(x,y) = 1+a(x-y)^2+bxy$$

を、(自分は)無意識に、除外していたのである。勿論、

$$1+a(x-y)^2-bxy = 1+a(x+y)^2-(b+4a)xy$$

である。

例えば、$f(x) = 13x^2+3x\sqrt{13}-30$ の場合で、

$$f(x)\ ⓧ\ 4t-1-t^2(x+y)^2+t(4t-1)xy\ ⓨ\ f(y) = 28561(16t^2-455t+169)(43t-13)^2(3t-1)^2$$

$$f(x)\ ⓧ\ 4s-1-s^2(x-y)^2-s(4s-1)xy\ ⓨ\ f(y) = 28561(900s^2-897s+169)(s-1)^2(9s-13)^2(4s-1)^2$$

などと因数の個数も異なる。

$$4t-1-t^2(x+y)^2+t(4t-1)xy\,[t = 1/3]$$
$$= -1/9\cdot(x^2+xy+y^2-3)$$

であるが、

$$4s-1-s^2(x-y)^2-s(4s-1)xy[s=1] = -(x^2+xy+y^2-3)$$

$$4s-1-s^2(x-y)^2-s(4s-1)xy[s=1/4] = -1/16\cdot(x-y)^2$$

のように代入した結果もことなる。

ついでながら、Tchebysheff 多項式

$$x^2-2,\ x(x^2-3),\ x^4-4x^2+2,\ x(x^4-5x^2+5),\ x^6-6x^4+9x^2-2,\ x(x^6-7x^4+14x^2-7),$$

$$x^8-8x^6+20x^4-16x^2+2,\ x(x^8-9x^6+27x^4-30x^2+9),\ \cdots$$

との関連して述べておく。

$$x^2+xy+y^2-3[x=x^2-2,\ y=x^2-2] = (x^2+xy+y^2-3)(x^2-xy+y^2-3)$$

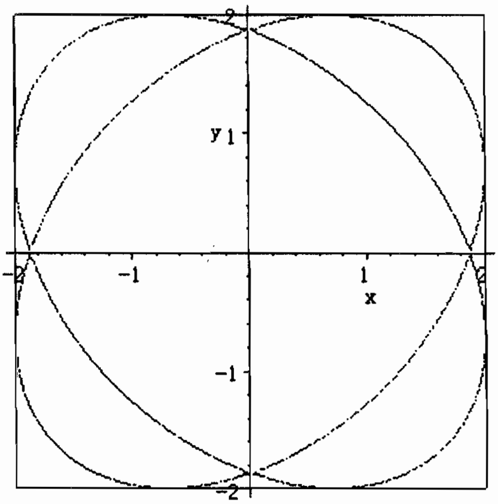
である。内接する 2 つの楕円、つまり、自分自身とその鏡像の積である。

例えば、t = 2 では

$$4t-1-t^2(x+y)^2+t(4t-1)xy[x=x^2-2,\ y=y^2-2,\ t=2]$$

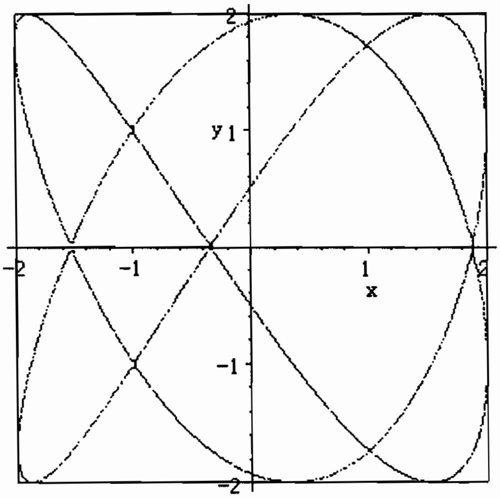
$$=$$

$$-4x^4+28x^2-49-6x^2y^2+28y^2-4y^4$$



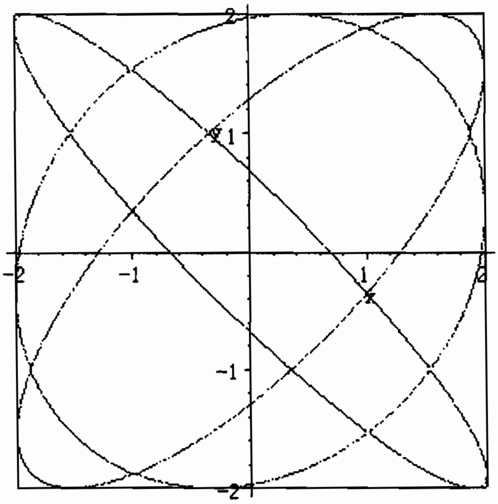
は有理数体上では既約であるけれども、正方形に内接する二つの楕円に分解する。

$$x^2+xy+y^2-3[x=x(x^2-3),\ y=y^2-2]$$



は、所謂、リサージュ曲線の一つである。3次 Tchebysheff 多項式同士では、三個の正方形に接する楕円形が生じる。

$$x^2+xy+y^2-3\,[x = x(x^2-3),\ y = y(y^2-3)]$$



以下のものは、

$$((-x^2+2xy-y^2)t^2+(4-xy)t-1)((-x^2-2xy-y^2)t^2+(4+xy)t-1)$$

$$=$$

$$(y^4-2x^2y^2+x^4)t^4+(4x^2y^2-8x^2-8y^2)t^3+(2x^2+16-x^2y^2+2y^2)t^2-8t+1$$

などに関する、

$$f(x) = x^3-ax^2+(b-3p)x+(c-2ap)$$

の消去積

$$f(x) \otimes ((-x^2-2xy-y^2)t^2+(4+xy)t-1) \circledcirc f(y)$$

の

$$y^2 = x(x^3-4)(x^3-8)$$

[[2, -1, -2, -4], [3, 0, 3, 0], [5, 2, 11, 12], [7, -3, 9, -42], [11, 0, -3, 0],…

での、高々、二次式の有理数解に制限した因数に関する表である。

[[2, {1/4}], [3, {1/2, 1/4}], [5, {1/4, 5/16, 5/4}], [7, {1, 1/4, 7/9}],
[11, {1/4, 11/36, 11/8}], [13, {13/9, 1, 1/4, 13/36}], [17, {1/4, 17/64, 17/4}],
[19, {1, 1/4, 19/9}], [23, {1/4, 23/36, 23/56}], [29, {1/4, 29/100, 29/64, 29/52}],
[31, {1/4}], [37, {1, 1/4, 37/4, 37/49}], [41, {1/2, 1/4, 41/162, 41/2, 41/64, 41/100}],
[43, {43/144, 1/4}], [47, {1/4, 47/36, 47/152}],
[53, {1/2, 1/4, 53/16, 53/50, 53/162, 53/196}], [59, {1/4, 59/36, 59/200}],
[61, {61, 1, 1/4, 61/100, 61/169, 61/196}], [67, {1, 1/4, 67/9}],
[71, {1/4, 71/144, 71/140}], [73, {1, 1/4, 73/36, 73/225}], [79, {79/81, 1, 1/4}],
[83, {1/4, 83/144, 83/188}], [89, {1/4, 89/100, 89/256}], [97, {1, 1/4, 97/81}],
[101, {1/4, 101/4, 101/148}], [103, {103/225, 1, 1/4}], [107, {1/4, 107/392, 107/36}],
[109, {1/4, 109/36}], [113, {1/4, 113/196, 113/256}]]

これらは、最初の 30 個の表である。$p = 61$ では根に 61 が入っているのも、理由は知らないが、印象的である。かなり多くのものは、p/n^2 の形の数であるが、

1/2, 11/8, 23/56, 29/52, 41/162, 41/2, 47/152 …

等はそうではない。

すべての素数に対して、

1, 1/2, 1/4

の何れかが入っている。これらは順に、交叉する直線(分)、半径 2 の円、そして、楕円

$$-1/16(x-y)^2,\ -1/4(x^2+y^2-4),\ -(x^2+xy+y^2-3)$$

である。因数に 1/2 が現れる、つまり、半径 2 の円周上にあるのは、意外なことに、$p = 1039$ までに

$$p = 3, 41, 53$$

の 3 個だけである。最初は、無限個存在するのかと思ったが、有限個かも知れないし、この 3 個だけかも知れない。

因数に 1 が現れる場合、つまり、楕円 $x^2+xy+y^2 = 3$ 上に点が存在するのは、

同範囲の素数 175 個のなか

[7, 13, 19, 37, 61, 67, 73, 79, 97, 103, 139, 151, 163, 181, 193,
199, 211, 241, 271, 313, 331, 337, 349, 367, 373, 379, 409, 421, 463, 487,
523, 541, 547, 571, 577, 607, 613, 619, 631, 661, 673, 709, 751, 757, 769,
787, 823, 829, 853, 859, 877, 883, 907, 937, 967, 991, 1009, 1033, 1039]

の 59 個で、出現率は

$$59/175 = 0.3371428571 \fallingdotseq 1/3$$

であり、恐らくは、1/3 の確率であろう。

ここに見た例は、3 次対称式で記述された係数方程式が、例えば、因数分解するなどの事情で退化した、つまり、可約などの状況の下での性質である。より一般的条件の例や性質の研究が期待される。

参考文献

[1] Kanji Namba; genus 2 hyper-elliptic curves and resultant transformation 2006 年度応用数学合同研究集会報告集 Ryukoku Univ. 2006. pp.57-62

[2] 難波完爾; 種数 2 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 28, 第 17 回数学史シンポジウム (2006), pp.101-174.

[3] Kanji Namba; genus 3 hyper-elliptic curves and resultant transformation 2007 年度応用数学合同研究集会報告集 Ryukoku Univ. 2007. pp.102-107

[4] 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.156-193

[5] 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