Hyper-elliptic curves and Hasse's inequality

難波完爾 (Kanji Namba)

463-3 Kitamizote Sojya Okayama 719-1117

tel/fax. 0866-90-1886

2012. 02. 12

目的：有眼体上の種数(genus)が g = n の超楕円曲線が

$$E:\ y^2 = x^{2n-1}+a_1x^{2n-2}+\cdots+a_{2n-2}x+a_{2n-1}$$

のように右辺が奇数次の多項式で与えられた場合から、より一般的な表示である偶数次多項式で与えられる

$$E:\ y^2 = x^{2n}+a_1x^{2n-1}+\cdots+a_{2n-1}x+a_{2n}$$

の場合を考察する。この場合、無限遠点、無限遠直線、無限遠平面等を考慮する必要がある。この場合の Hasse の不等式、つまり、係数方程式の解が標準区間[-2,2]に属し、あるいはその区間での密度分布に関する $\sin^2$-予想等について論ずる。

1. 諸概念

超楕円曲線

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

の多項式 f(x)に対し、Tschirnhaus 変換、つまり、monic な多項式との終結式(resultant)

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

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

を考える。ここに、ⓧなどは終結式の省略記号で

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

の(ここだけの)記号法である。終結式は、(ここだけの呼称であるが)消去積(elimination product)とも呼ぶ。尚、記号の結合力(adhesiveness)は加減乗除(+, -, ×, /, √)などより弱いものとする。基本的性質の例としては

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

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

$$f(y) = f(x) \circledast y\text{-}x$$

などであり、有理式や冪根(そして無限積)にも拡張できて、

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

$$f(x) \circledast g(x)^n = f(x)^n \circledast g(x),\ f(x) \circledast \sqrt{g(x)} = \sqrt{f(x)} \circledast g(x)$$

などの性質がある。勿論、無限積にも拡張可能である。

また、pを素数とするとき、ルジャンドル記号(Legendre symbol)あるいは平方剰余記号(quadratic residue symbol)を(n/p)と記す。特に、pが奇素数のときは

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

これは、オイラーの定理と呼ばれているものである。$p = \{0,1,\cdots, p-1\}$と考えての和、つまり、Legendre sumを

$a_p = 1+\sum x\in p\,(f_1(x)/p)$, $b_p = a_p+\sum x,y\in p\,(f_2(x,y)/p)$, $c_p = b_p+\sum x,y,z\in p\,(f_3(x,y,z)/p)$, $\cdots$

とし、多項式

$$\bar{f}_p(x) = x^{2n-2}+a_p x^{2n-3}+b_p x^{2n-4}+\cdots+p^{n-2}b_p x^2+p^{n-1}a_p x^2+p^n$$

を、多項式f(x)の終結変換多項式(resultant transformation polynomial)あるいは合同ゼータ核(congruence zeta kernel)と呼ぶ。

$$a_p = 1+\sum x\in p\,(f_1(x)/p),\ b_p = 1+\sum x\in p\,(f_1(x)/p)_p+\sum x,y\in p\,(f_2(x,y)/p),$$

$$c_p = 1+\sum x\in p\,(f_1(x)/p)_p+\sum x,y\in p\,(f_2(x,y)/p)_p+\sum x,y,z\in p\,(f_3(x,y,z)/p)$$

などは、無限遠多様体(manifold at infinity)を単純に数え上げる(count out)だけであるが、…。

事実としては、この定義に(私は)2011.05.02, 15:30に到達した。この式に至るまでには多くの試行錯誤を要したが、結果は既に良く知られているに違いないと感じられる簡潔な式であった。兎も角、このために、以前は、2g+1次の多項式に帰着できる場合の計算や数値的な実験や検証が中心であった。

注意：現在の定義はf(x)が偶数次の多項式の場合で、f(x)が奇数の場合は、従来の、

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

である。

終結変換方程式

$$\bar{f}_p(x) = 0$$

の解(=根)を、終結(変換)根(resultant transformation root)と呼ぶ。

終結根はすべて絶対値 $\sqrt{p}$ の複素数、つまり、

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

の形の複素数であることが谷山・志村の理論で知られている。終結根の角度の、すべての素数にわたる密度分布が、楕円曲線の場合は、虚数乗法をもたない場合は $\sin^2(\theta)$ であることは、2006 年に R. Taylor によって証明されている。

種数 g が 2 以上の場合は、f(x)のガロア群が非可解(not solvable)のときには、

$$\sin^2(\theta) + \sin^2(2\theta) + \cdots + \sin^2(g\theta)$$

に比例するであろうというのが、$\sin^2$-予想($\sin^2$-conjecture for hyper-elliptic curve)である。現実には、もっと広い範囲の f(x)に対して成立するものと思うが…。以下に、種数 4 の場合、奇数・偶数次の多項式で与えられる場合の $\sin^2$-予想に関する計算結果をガロア群が S(9), S(10)の場合の例について記す。多項式は

G. Malle, B.H.Matzat: Inverse Galois Theory, Springer Monographs in Mathematics, Springer, 1991, p. 415,416 Appendix: Example Ploynomials

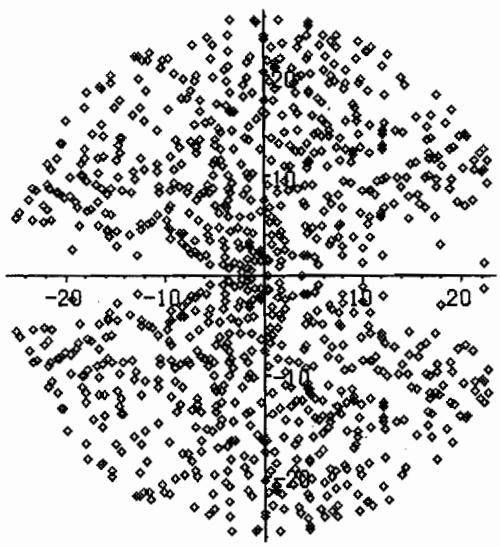
degree 9,10 T_{34}, S_9 ;T_{45} S_{10}

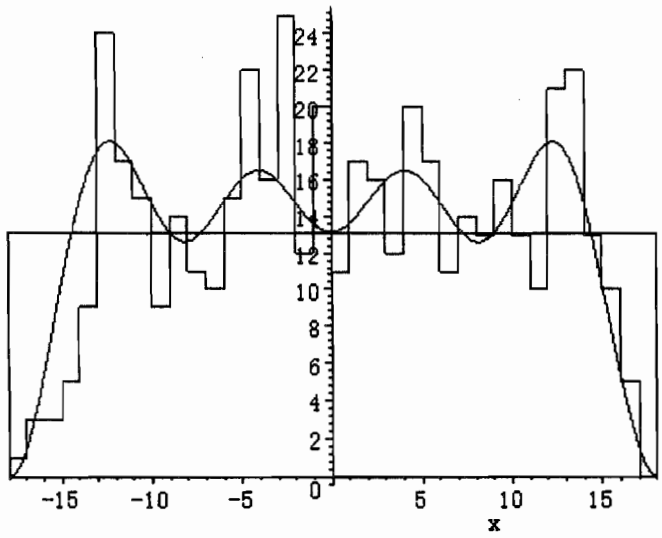
からの引用である。

$$y_2 = f(x) = x^9 - x^6 + 2x^5 + x^4 - 3x^3 + x^2 + x - 1,$$

$$f_p(x) = x^8 + ax^7 + bx^6 + cx^5 + dx^4 + pcx^3 + p^2bx^2 + p^3ax + p^4 = 0$$

$$\mathrm{gal}(f(x)) = S(9),\ p = 2 \sim 659$$





参考、検証のため、基本データの一部を記す：

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

[2, -2, -4, -8, -16], [3, 1, 1, 0, 2], [5, 5, 12, 21, 38], [7, 5, 23, 73, 204],

[11, 3, 15, 59, 211], [13, 9, 34, 42, -62], [17, 7, 37, 211, 977], [19, -1, 7, 6, -6],

[23, -1, 12, -51, 310], [29, 2, 19, -140, -84], [31, 4, -14, -105, -615],

[37, 4, 47, 318, 1140], [41, 4, 47, 52, 936], [43, 14, 116, 814, 5494],

[47, 7, 76, 350, 3792], …

[601, 3, 227, 577, -246513], [613, -5, 297, -10553, 431483],

[617, 25, 266, 7489, 302218], [619, 17, -54, 6194, 485142],

[631, -3, 659, -13227, 525720], [641, -16, 988, -3734, 486276],

[643, -1, 920, -3114, 955876], [647, 21, 197, 2206, -62668],

[653, 9, 1696, 18873, 1366662], [659, 3, 331, 11022, -297242]

次の例は、上記引用例の偶数次の場合で、

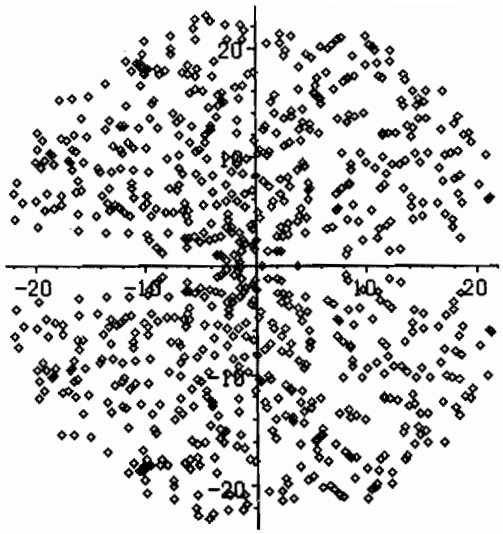
$$E:\ y^2 = f(x) = x^{10}+x^9-x^8-x^7-x^5-2x^4-x^3+2x^1+2x+1$$

$$\det(f(x)) = f(x) \otimes f'(x) = 467 \cdot 514417$$

である。終結根の角分布の図は

$$f_p(x) = x^8+ax^7+bx^6+cx^5+dx^4+pcx^3+p^2bx^2+p^3ax+p^4 = 0$$

$$p = 2 \sim 547$$



のようであり、角分布の期待値は

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

に比例するであろうと予想されている。所謂、$\sin^2$-conjecture である。最大の謎は、

「何故、$\sin^2(nx)$の“等しい”重さの和なのか」

why it should be equal weighted $\sin^2$-sum?

という点であろうと(私は)思う。

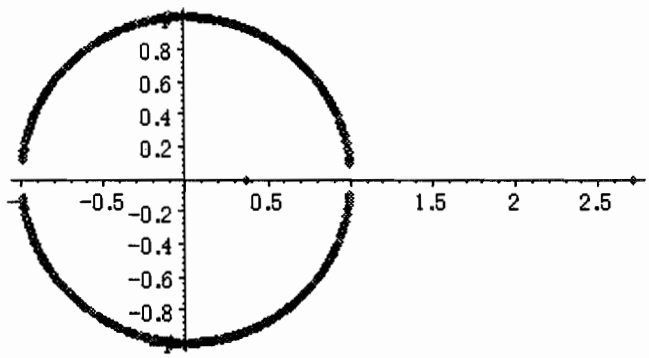
標準終結多項式(normalized resultant transform polynomial)は、解の絶対値が 1 であるように、標準化(normalize)したもので、

$$a = (a_p+1)/\sqrt{p},\ b = (b_p+a_p+1)/p,\ c = (c_p+b_p+a_p+1)/(p\sqrt{p}),\ d = (d_p+c_p+b_p+a_p+1)/p^2$$

$$\bar{f}_p(x) = x^8+ax^7+bx^6+cx^5+dx^4+cx^3+bx^2+ax+1$$

の解である。確認のため、その図も記しておく。

normalized resultant roots: $\bar{f}_p(x) = 0$, $p = 2, 3, \cdots, 547$

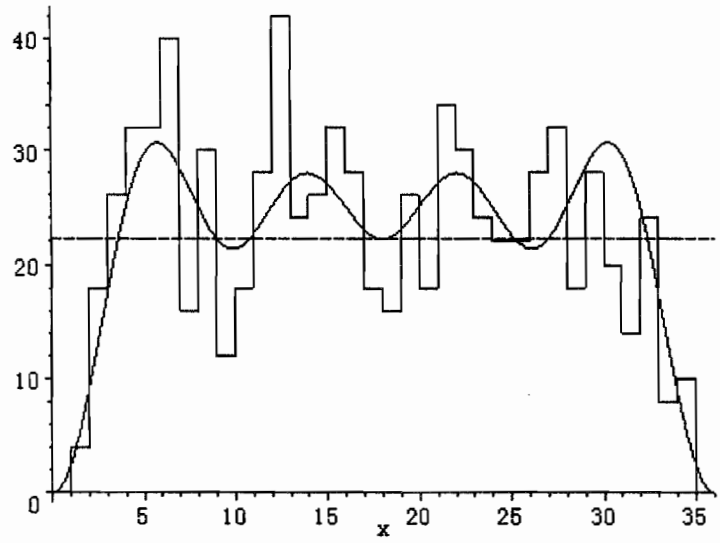


実数軸上に、絶対値 1 でない解が存在するが、これは p = 2 の場合である。

p = 3 ~ 547 には、800 個の解が存在する。以下の図は π/36 = 10° 間隔での統計である。

$$\bar{f}_p(x) = 0,\ p = 3 \sim 547$$

$$100/9\,(\sin^2(x) + \sin^2(2x) + \sin^2(3x) + \sin^2(4x))$$



参考のための基本データは

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

[[2, -2, -4, -8, -16], [3, 3, 5, 7, 12], [5, 1, 3, 0, 2], [7, 5, 9, -10, -58],
[11, 5, 23, 80, 236], [13, 6, 24, 75, 238], [17, -1, 9, -3, 503], [19, 5, 33, 121, 757],
[23, 6, 45, 207, 1171], [29, 7, 35, 27, -163], [31, 6, 30, 186, 1818],

[37, 2, 46, 241, 1560], [41, 2, 16, 258, 1219], [43, 12, 109, 710, 4544],

[47, 12, 158, 1396, 9948], …

[503, -9, 135, 1719, 173589], [509, -18, 582, -10864, 381634],

[521, -10, 188, 7384, -70198], [523, 5, 56, 8316, 174568],

[541, -17, 284, -2758, 144056], [547, -11, 802, -3648, 480332]]

である。ここに記したデータの大きさに差があるのは多項式の次数に従って、現在の(自分の)計算法では、次数×種数の 4 乗(= $d \cdot g^4$)に比例した計算量が必要なためである。$\sin^2$-sum の中央の谷底の点が丁度、平均値に一致していることは、自明であろうけれども、美しい点の一つである。

さて、

$$\bar{f}_p(x) \circledast x^2+ux+p$$

は完全平方式であるから、その平方根

$$\underline{f}_p(x) = \bar{f}_p(x) \circledast \sqrt{x^2+ux+p}$$

を係数多項式(coefficient polynomial)と呼ぶ。また、標準化して、

$$\underline{f}_p(\sqrt{p}x)$$

を標準係数多項式(normalized coefficient polynomial)と呼ぶ。標準係数多項式の根はすべて、多項式 f(x)に、平方因子をもつなどの退化がない場合は、区間[-2,2]の実数である。

注意すべき点としては、f(x)の次数が高い場合は、判別式

$$\det(f(x)) = f(x) \circledast f'(x)$$

の素因子ばかりではなく高次の導関数との終結式も関係する可能性があることである。

標準化した終結変換多項式では

$$\bar{f}_p(\sqrt{p}x) \circledast x^2+ux+1$$

の形の終結式が標準係数多項式であるから、所謂、余弦変換(cosine transformation)にすぎない。$\bar{f}_p(\sqrt{p}x)$は実数係数であるから完全平方になるのである。

2. 諸例

2.1 種数 2 の超楕円曲線

$$E: \quad y^2 = x^6-2x^5+x^4-2x^3+6x^2-4x+1$$

について記す。この曲線は、

Math. J. Okayama Univ. 53 (2011), pp75-82

Torsion of elliptic curves over quadratic cyclotomic fields

Filip Najman

p.81 (13)

による。

最初の試みでは、f(x)の次数が偶数の場合は、終結変換の係数を f(x)が奇数の場合と同様に従来の、

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

としては、うまく行かない、つまり、Hasse の不等式が成立せず、この形で定義した終結根の分布は、例えば、種数 3 の場合に倣って計算し

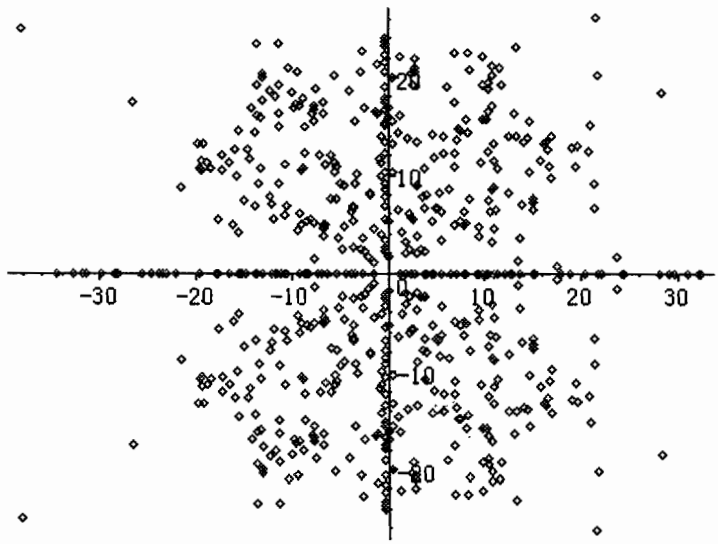
$$[p,\ a_p,\ b_p,\ c_p]$$

[2, -2, -4, -7], [3, 1, -1, 5], [5, -1, -7, 7], [7, -1, 7, -7], [11, -1, 11, -11], [13, 4, 8, -13], [17, -4, -5, -43], [19, 5, 25, 83], [23, -7, 19, -151], [29, 2, -23, 107], [31, -1, -50, 50], [37, -16, 127, -667], [41, 8, 59, 301], [43, 7, 13, 323], [47, -1, -82, 82], [53, 5, 109, 203], [59, -13, 119, -815], [61, 0, -61, 121], [67, -7, 85, -481], [71, -7, 89, -509], [73, -1, -143, 143], [79, -9, 182, -806], [83, -1, 26, -26], [89, 11, 125, 931], [97, -13, 157, -1309], [101, -4, -89, -211], [103, 19, 286, 1754], [107, 5, -77, 713],…

などのデータから

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

$$x^6+a_px^5+b_px^4+c_px^3+pb_px^3+p^2a_px+p^3 = 0,\ p = 2 \sim 587$$

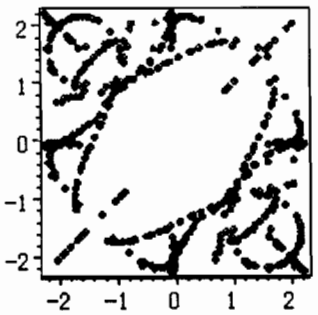


係数多項式は例外なく S(3)である。

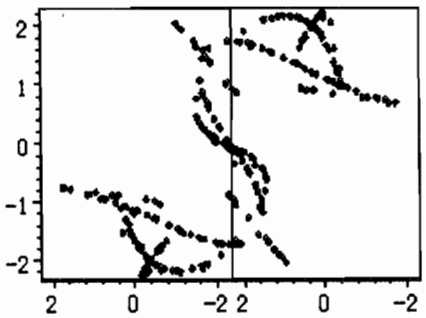
$$x^3-ax^2+(b-3)x+2a-c=0$$

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

の解の xyz-空間表示は



や、別の方向からは



のような図形を眺め、その法則は具体的には記述できるが、何か美しさに欠けるという「強い違和感」をもった、つまり、もっと本質を穿った簡潔な定義があるに違いないと思った訳である。上記では、p = 587 までしか計算してないのは g = 3 に倣って c_p まで、つまり、3 重和(triple sum)を計算しているためである。

以下は、g = 2 で、終結変換係数 (resultant transformation coefficient) を

$$a_p = 1+\sum x\in p\,(f_1(x)/p),$$

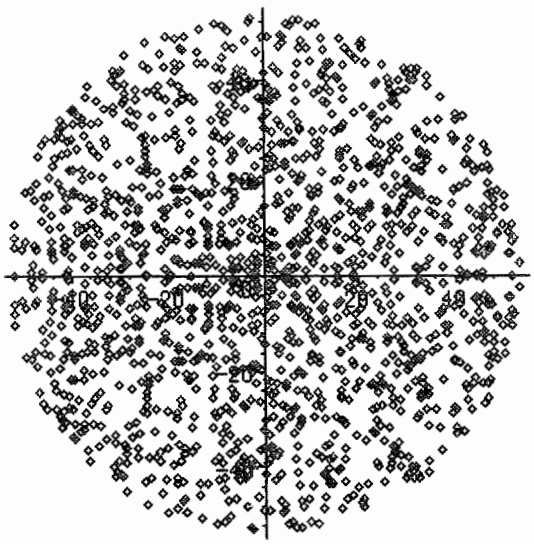
$$b_p = 1+\sum x\in p\,(f_1(x)/p)+\sum x,y\in p\,(f_2(x,y)/p)$$

と定義した場合である：

終結根 (resultant transform root) の分布については次のようである。

$$f(x) = x^4+a_px^3+b_px^2+pa_px+p^2 = 0$$

$$p = 2 \sim 2861$$



この範囲では、実数軸の周辺の分布が“やゝ濃い”感じがあるが、予想としては角分布の極限分布は一様分布であろうと、半分疑いながら、思う。兎も角、確かめる必要があります。

標準終結根分布

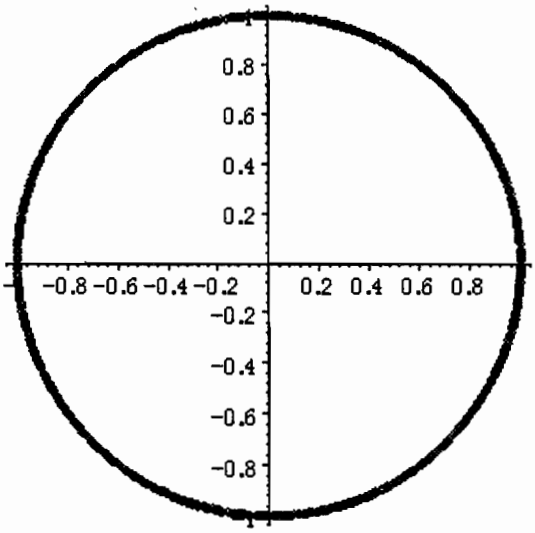
$$a = a_p/\sqrt{p},\quad b = b_p/p$$

$$f(x) = x^4+ax^3+bx^2+ax+1 = 0$$

については、次のようである。

$$f(x) = x^4+ax^3+bx^2+ax+1 = 0$$

$$p = 2 \sim 2861$$

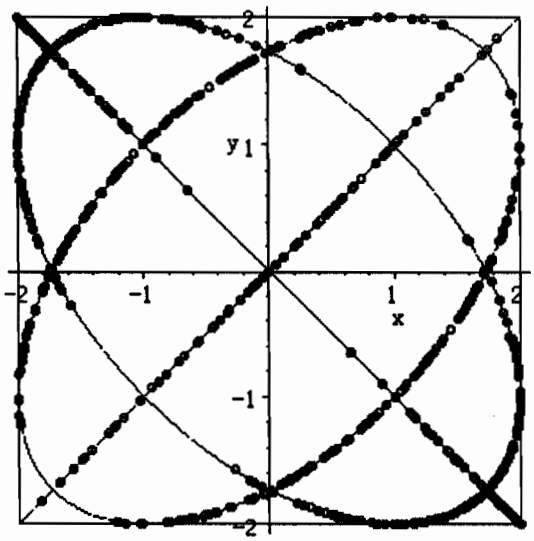


この図のように、標準終結根の絶対値は常に 1 であることが解る。

次のものは、標準係数方程式の根 (= 標準係数根、normalized coefficient root) を図示したものである。

$$\underline{f}(x) = x^2\text{-}ax+b\text{-}2 = 0$$

$$\underline{f}(x) = \underline{f}(y) = 0,\ p = 2 \sim 2861$$



ここに現れる楕円の方程式は

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

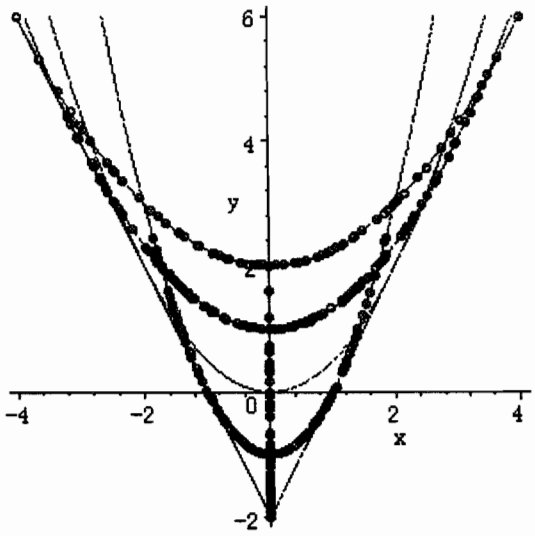
である。

終結係数の分布

$$a = a_p/\sqrt{p},\quad b = b_p/p$$

(a, b)

$p = 2 \sim 2861$

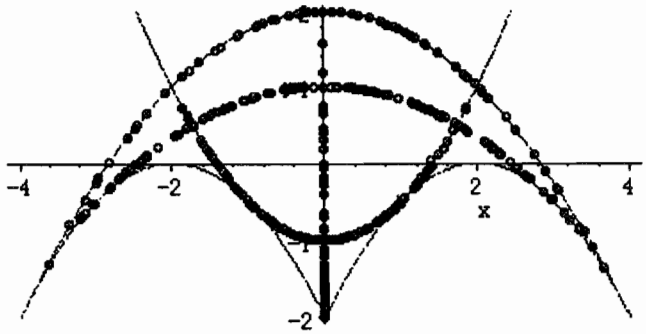


この曲線族は

$$y = x^2/n + (n-1),\ n = 1,2,3,4$$

$$x = 0$$

この曲線族から、y-軸方向に $x^2/2$ を引いたものは次のようである。



これらの、終結係数は

$$k = 26$$

での剰余によって分類され、密度は

n	curve, $x^2/n+(n-1)$	residue class	density
0	$x = 0$	1, 4, 5, 7, 8, 9, 10, 11	2/3
1	$y = x^2-1$	3, 4, 9, 10	1/3
2	$y = x^2/2$	none	0
3	$y = x^2/3+1$	2, 6, 7, 11	1/3
4	$y = x^2/4+2$	1, 12	1/6

これは、私に「こうでなくっちゃ！」と思わせた瞬間であった。そして、このことは、知っている人はとっくの昔から知っているに違いないと確信したときでもある。つまり、自分だけが知らなかった訳である。

知って知る知らざりきとそ知れる恥じらい

2.2 Cartan matrix for the root system E_8

$$\begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

この行列の固有多項式と galois 群は

$$f(x) = x^8-16x^7+105x^6-364x^5+714x^4-784x^3+440x^2-96x+1$$

$$gal(f) = 4[\times]2 = \langle (1,5,4,8)(2,6,3,7), (1,6,4,7)(2,5,3,8) \rangle$$

$$\det(f(x)) = f(x) \circledast f'(x) = 2^8 \cdot 3^4 \cdot 5^6$$

であり、可解群である。従って、終結変換方程式の根の角分布は

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

と異なる可能性はある。寧ろ、種数 2 の場合に対応する

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

かも知れない。

$$[p, \Sigma x \in p(f_1(x)/p), \Sigma x,y \in p(f_2(x,y)/p), \Sigma x,y,z \in p(f_3(x,y,z)/p)]$$

$$[2, -2, -4, -8], [3, 3, 9, 27], [5, 5, 24, 120], [7, 7, 25, 63], [11, -1, 9, -41],$$

$$[13, 1, 13, 37], [17, 9, 65, 265], [19, -1, 17, -17], [23, 7, 73, 271],$$

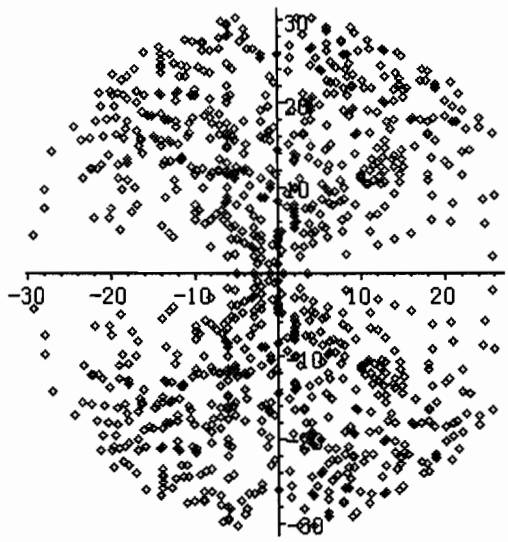
[29, 5, 13, -79], [31, -1, 13, 243], [37, -7, 77, -323], [41, 17, 133, 805],

[43, 3, 49, -13], [47, -1, 41, 295], [53, -11, 121, -883], [59, -5, 69, -89],

[61, -3, 53, -31], [67, -5, 161, -517], [71, -5, 17, -581], [73, -3, 13, 977],

[79, 27, 441, 4435], [83, -21, 305, -3077], [89, 17, 309, 2677], [97, 5, 61, -567], ⋯

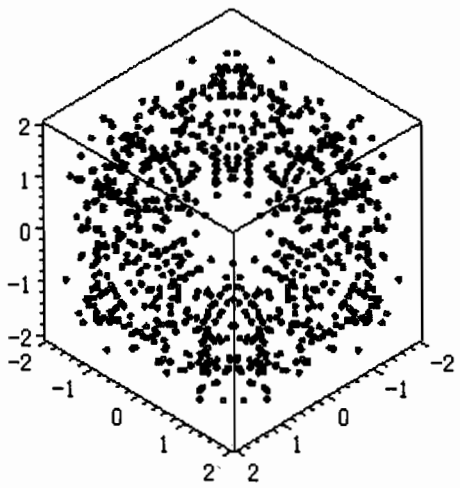
$\bar{f}_p(x) = 0,\ p = 2 \sim 941$



標準係数方程式：

$$\underline{f}_p(x) = \bar{f}_p(x) \otimes \sqrt{x^2+ux+p} \quad = x^3-ax^2+(b-3)x+2a-c$$

$$(x,y,z),\ \underline{f}_p(x) = \underline{f}_p(y) = \underline{f}_p(z) = 0,\ p = 3 \sim 941$$



係数多項式の因数型：

p = 19,29,59,61,67,107,307,419,499,883, ⋯

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

$$p = 13,17,37,53,73,179,229,281,409,601,757,821, \cdots$$

$$(x+a)\,(x+b)\,(x+c)$$

$$\text{other primes} \neq 2, 3, 5$$

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

$Z(\sqrt{p})$で既約なものは存在しない。

2.3 種数 4 の例

種数 4 では、f(x)の次数が偶数の場合は 10 次多項式である。この場合は

$$a_p = 1+\sum x\in p\,(f_1(x)/p),\ b_p = a_p+\sum x,y\in p\,(f_2(x,y)/p),$$

$$c_p = b_p+\sum x,y,z\in p\,(f_3(x,y,z)/p),\ d_p = c_p+\sum x,y,z,t\in p\,(f_4(x,y,z,t)/p)$$

まで必要な場合で、4 重和まで計算が必要で、ある程度の計算量のため大きな素数までのデータを得るには時間を要する。

また、係数方程式

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

に対する 4 重対(x,y,z,t)の 3 次元の xyz-空間への射影は次のようである。

最初の例について、標準係数根などについて記しておく。

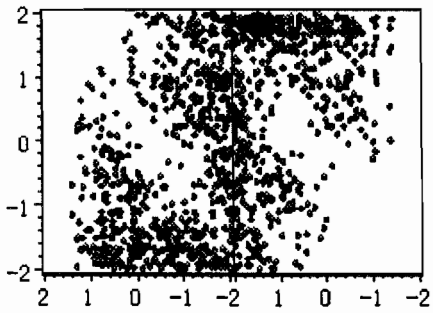
$$E:\ y^2 = f(x)\ = x^{10}+x^9-x^8-x^7-x^5-2x^4-x^3+2x^1+2x+1$$

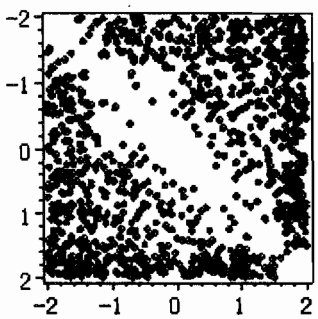
$$\det(f(x)) = f(x)\,\textcircled{x}\,f'(x) = 467\cdot 514417$$

以下の図は標準係数根を座標にもつ点を表示したものである。

$$(x,y,z);\ \underline{f}_p(x) = \underline{f}_p(y) = \underline{f}_p(z) = 0$$

$$p = 2 \sim 547$$





上図の方向への射影では、S 字状の密度の濃い部分と、下図では対角線の付近の密度の低い部分が現れる傾向があるが理由は解らない。空間的に一様な分布ではないけれども、$\sin^2$-予想の分布を、係数解(coefficient roots)の分布から読みとることは、今の自分には、できていない。

これは、比較的、一般的な視点からの表示である。この場合は、明確な退化多様体、つまり、その上に正の確率で分布するような、点、曲線、曲面等は、(私には)見当たらない。恐らく、一般の場合には存在しないのではないかと思っている。p = 3, 7, 11 を除いて、係数多項式は $Z(\sqrt{p})$ で既約のようである。

3. 要検討例

以下の例は、やはり、

G. Malle, B.H.Matzat: Inverse Galois Theory,

p.416 Appendix: Example Ploynomials

degree 10, T_{18} gal $= 5^2 \cdot 8$

からの引用である。問題の曲線は

$$E: \quad y^2 = x^{10}+60x^6-208x^5+850x^2-8000x-4672$$

である。判別式は

$$\det(f(x)) = f(x) \otimes f'(x) = -2^{42} \cdot 5^{10} \cdot 89^2 \cdot 87623^2 \cdot 7414739^2$$

であり、何か、一癖ありそうな、多項式である。

判別式の因数での分解の様子を一応表示しておく。勿論、その因子のところ、つまり、その標数(characteristic number)の素体(prime field)では重複因子になっている。

factor	$x^{10}+60x^6-208x^5+850x^2-8000x-4672$
2	x^{10}
5	$(x^2+2x+3)^5$
89	$(x+71)^2(x^4+18x^3+57x^2+47x+39)(x^4+18x^3+57x^2+47x+22)$
87623	$(x+35826)(x+6060)(x+27188)^2$ $(x^2+37706x+60254)(x^2+43857x+73769)(x^2+85044x+39760)$
7414739	$(x+4448861)^2(x^8+5931756x^7+3560004x^6+3952493x^5$ $+2022082x^4+1472x^3+7399955x^2+2140557x+3676715)$

以下に基本データを記す。

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

[2, -1, -2, 0, -8], [3, 1, 4, -4, 12], [5, -1, 0, 0, 0], [7, 1, 1, 9, 81], [11, -5, 18, 30, 68],
[13, -3, 4, 2, -46], [17, 3, 18, 50, 186], [19, -5, 16, 40, 142], [23, -7, 35, -115, 105],
[29, -7, 4, 32, 726], [31, 1, 21, 173, 609], [37, -3, 10, 126, -536],
[41, -3, -30, 6, 1676], [43, -9, 50, 294, 946], [47, -9, 74, -386, 3170],
[53, -5, 84, 334, 4876], [59, 3, 20, -66, 1650], [61, -5, 56, 422, 4588],
[67, 7, 66, -828, 7558], [71, 7, 116, 312, 6258], [73, -2, 34, -24, -2029],
[79, 9, -11, -75, 2461], [83, -1, 60, -20, 482], [89, -2, 40, -1214, 5782],
[97, -1, 62, 110, 5082], [101, 7, 100, -764, -828], [103, -5, 20, -100, 3762],

[107, -7, 192, 1468, 19174], [109, 3, -156, 216, 18552], [113, 1, 90, 282, 16740],
[127, -15, 142, -2094, 40016], [131, 11, 202, -2468, 35696], [137, -3, 74, 186, 1084],
[139, -7, 116, 1790, 35874], [149, -1, 198, -1218, 19716], [151, 9, 42, 1106, 13984],
[157, -11, 202, 2236, 55090], [163, -23, 396, 7156, 101216], [167, 7, 151, 615, -5831],
[173, 21, 186, 1488, -48548], [179, 17, 200, -440, -12784], [181, 27, 332, -426, -21546],
[191, -7, 259, -1863, 67829], [193, -5, 416, -3556, 94902], [197, 7, -64, 212, 18408],
[199, -17, 328, -3144, 37070], [211, 19, 334, -3792, 74050], [223, 5, 186, -3762, 1740],
[227, 3, 174, -1454, 99782], [229, -11, 102, 1820, 33172], [233, 13, -177, -1155, 36973],
[239, -18, 294, -4914, 123409], [241, 25, 354, 3386, 24752], [251, -21, -28, -66, 67210],
[257, 1, 16, -1880, -5940], [263, -21, 84, 2212, -45366], [269, -1, -148, 338, 96316],
[271, -17, 564, -8596, 227126], [277, -19, 140, 958, 19108],
[281, -3, -180, -1268, 46904], [283, -13, 218, 1030, -38804],
[293, -27, 638, 11614, 194882]

終結変換多項式(合同ゼータ核, resultant transformation polynomial, congruence zeta kernel)については、偶数次のときの式

$$a = (a_p+1)/\sqrt{p},\ b = (b_p+a_p+1)/p,\ c = (c_p+b_p+a_p+1)/(p\sqrt{p}),\ d = (d_p+c_p+b_p+a_p+1)/p^2$$

$$\bar{f}_p(x) = x^8+ax^7+bx^6+cx^5+dx^4+cx^3+bx^2+ax+1$$

など、無限遠点を考慮した式を用いた。しかし、ここでは、多くの、Hasseの不等式を満足しない素数が存在する。

$$E:\ y^2 = x^{10}+60x^6-208x^5+850x^2-8000x-4672$$

$$f_p(x) = x^8+ax^7+bx^6+cx^5+dx^4+pcx^3+p^2bx^2+p^3ax+p^4 = 0$$

$$p = 2 \sim 293$$

について、mod 8で、±1, ±3の組に対して異なる振る舞いをするのである。±1の組は$\sqrt{p}$ の $\sin^2$-sum 分布に添うが、±3の組の素数に対しては、特異な振る舞いをするのである。

これは、定義式の未完成を意味するのか、それとも、何か、新しい本質的な現象の発露なのか、はたまた(多くの場合そうであるが…)、既に良く知られた現象なのか、注意深い検討が必要である。

標準終結根については、mod 8で{1,7}のものについては

$$p \bmod 8 = 1,7,\ p = 2 \sim 293$$

[79,167,191,233,503]

[79, $x^{10}+60x^6+29x^5+60x^2+58x+68$],

[167, $x^{10}+60x^6+126x^5+15x^2+16x+4$],

[191, $x^{10}+60x^6+174x^5+86x^2+22x+103$],

[233, $x^{10}+60x^6+25x^5+151x^2+155x+221$],

[7,23,31]

[7, $(x^5+x+3)(x^5+3x+6)$],

[23, $(x^5+9x+14)(x^5+5x+8)$],

[31, $(x^5+21x+29)(x^5+8x+11)$],

[73,239]

[73, $(x^5+44x+11)(x+44)x(x+29)(x+53)(x+20)$],

[239, $(x^5+13x+27)(x+11)(x+213)(x+114)(x+220)(x+159)$],

[103,137,137,241,263,271]

[103, $(x+71)(x+48)(x^2+14x+12)(x^2+7x+54)(x^2+41x+70)(x^2+25x+74)$],

[137, $(x+65)(x+82)(x^2+53x+107)(x^2+115x+124)(x^2+2x+72)(x^2+94x+4)$],

[241, $(x+179)(x+224)(x^2+134x+118)(x^2+169x+119)(x^2+93x+18)(x^2+165x+109)$],

[263, $(x+57)(x+28)(x^2+140x+216)(x^2+95x+155)(x^2+21x+86)(x^2+185x+67)$],

[271, $(x+112)(x+166)(x^2+253x+75)(x^2+270x+230)(x^2+123x+156)(x^2+160x+8)$],

ここに挙げた、多項式の法 8 での剰余で分類された素体での因数分解の類型と終結根の絶対値の分布には明確な関連性は指摘できるが、その精密な構造については、(今の私には)ほとんど解らない、というのが実状である。

ガロア群が特殊な個々の多項式 f(x)で決定される超楕円曲線に対しては、興味ある本質的な現象が多く存在するであろう。今後の研究が強く期待される部分である。

以下に、部分的であるが、偶数次多項式で決定される超楕円曲線のガロア群を代表する多項式と終結根の Hasse 不等式(=谷山・志村性)について記す。表は

G. Malle, B.H.Matzat: Inverse Galois Theory,

p. 416 Appendix: Example Ploynomials degree 10

の部分に対して、偶数次の場合の式を適用した場合の除外素数(一部)の表である。各場合について p = 3 ~ 151 までは確かめたものであるが、大きい素数で判別式の約数になっているものについては疑問符を記しておいた。

$[293, (x^2+156x+290)(x^8+137x^7+20x^6+221x^5+218x^4+142x^3+184x^2+143x+190)]$

谷山・志村関係をみたさないものは

$[5, 13, 37, 59, 83, 101, 149, 179, 197, 251, 269, 277, 283]$

$[5, (x^2+2x+3)^5]$,

$[13, (x^2+4x+9)(x^8+9x^7+7x^6+8x^5+4x^4+3x^3+4x^2+9x+11)]$

$[37, (x^2+x+10)(x^8+36x^7+28x^6+19x^5+20x^4+26x^3+33x^2+3x+36)]$,

$[59, (x^2+4x+13)(x^8+55x^7+3x^6+40x^5+38x^4+5x^3+17x^2+44x+40)]$,

$[83, (x^2+37x+35)(x^8+46x^7+6x^6+77x^5+72x^4+77x^3+26x^2+78x+42)]$,

$[101, (x^2+9x+55)(x^8+92x^7+26x^6+59x^5+18x^4+21x^3+33x^2+63x+84)]$,

$[149, (x^2+127x+16)(x^8+22x^7+21x^6+110x^5+58x^4+53x^3+89x^2+67x+6)]$,

$[179, (x^2+98x+133)(x^8+81x^7+163x^6+103x^5+149x^4+131x^3+102x^2+147x+86)]$,

$[197, (x^2+91)(x^8+106x^6+67x^4+186x^3+10x^2+16x+137)]$,

$[251, (x^2+74x+58)(x^8+177x^7+147x^6+191x^5+241x^4+247x^3+123x^2+166x+6)]$,

$[269, (x^2+261x+250)(x^8+8x^7+83x^6+9x^5+95x^4+185x^3+57x^2+205x+76)]$,

$[277, (x^2+201x+110)(x^8+76x^7+126x^6+108x^5+225x^4+26x^3+217x^2+59x+23)]$,

$[283, (x^2+76x+36)(x^8+207x^7+80x^6+52x^5+20x^4+79x^3+68x^2+195x+279)]$,

である。因数の形に於いて区別はないようである。

以下のものは、p mod 8 = 1,7 の場合の類型である。

$[41,47,71,89,97,113,127,151,193,199,223,257,281]$

$[41, (x+19)(x+12)(x^4+22x^3+33x^2+29x+15)(x^4+29x^3+21x^2+35x+17)]$,

$[47, (x+12)(x+32)(x^4+15x^3+37x^2+38x+1)(x^4+35x^3+3x^2+11x+27)]$,

$[71, (x+45)(x+64)(x^4+7x^3+49x^2+59x+6)(x^4+26x^3+37x^2+39x+61)]$,

$[89, (x+71)^2(x^4+18x^3+57x^2+47x+39)(x^4+18x^3+57x^2+47x+22)]$,

$[97, (x+43)(x+92)(x^4+5x^3+25x^2+28x+46)(x^4+54x^3+6x^2+33x+93)]$,

$[113, (x+104)(x+23)(x^4+90x^3+77x^2+37x+112)(x^4+9x^3+81x^2+51x+8)]$,

$[127, (x+101)(x+72)(x^4+26x^3+41x^2+50x+107)(x^4+55x^3+104x^2+5x+4)]$,

$[151, (x+119)(x+114)(x^4+37x^3+10x^2+68x+51)(x^4+32x^3+118x^2+x+141)]$,

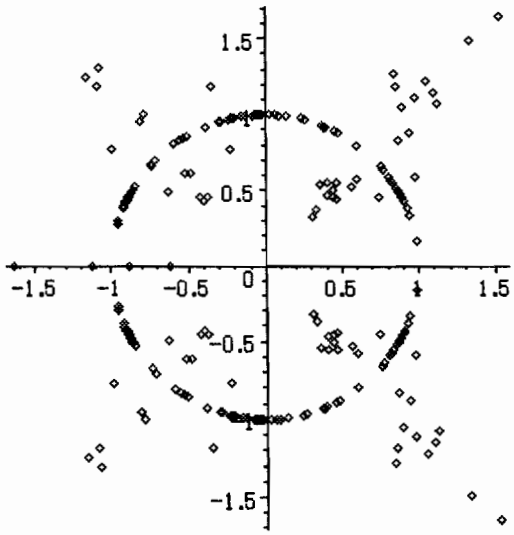
$[193, (x+2)(x+185)(x^4+191x^3+4x^2+185x+113)(x^4+8x^3+64x^2+126x+6)]$,

$[199, (x+179)(x+183)(x^4+20x^3+2x^2+40x+133)(x^4+16x^3+57x^2+116x+195)]$,

$[223, (x+185)(x+76)(x^4+38x^3+106x^2+14x+191)(x^4+147x^3+201x^2+111x+216)]$,

$[257, (x+199)(x+218)(x^4+58x^3+23x^2+49x+88)(x^4+39x^3+236x^2+209x+171)]$,

$[281, (x+188)(x+241)(x^4+93x^3+219x^2+135x+123)(x^4+40x^3+195x^2+213x+218)]$,



p mod 8 = 3,5 の場合の因数分解について、谷山・志村関係をみたすもの

[3,11,19,29,43,53,61,67,89,107,109,131,139,157,163,173,181,211,227,229,293]

[3, $(x^8+2x^6+x^4+2x^3+2x^2+x+2)(x^2+1)$], [11, $(x^8+6x^6+8x^4+x^3+4x^2+6x+5)(x^2+5)$],

[19, $(x^2+14x+9)(x^8+5x^7+16x^6+16x^5+15x^4+8x^2+4x+15)$],

[29, $(x^2+4x+2)(x^8+25x^7+14x^6+10x^5+21x^4+7x^3+17x^2+5x+13)$],

[43, $(x^2+x+34)(x^8+42x^7+10x^6+24x^5+40x^4+11x^3+5x^2+8x+27)$],

[53, $(x^2+27x+5)(x^8+26x^7+35x^6+38x^5+25x^4+40x^3+14x^2+5x+9)$],

[61, $(x^2+48x+35)(x^8+13x^7+12x^6+6x^5+23x^4+3x^3+27x^2+2x+53)$],

[67, $(x^2+10x+65)(x^8+57x^7+35x^6+32x^5+11x^4+14x^3+16x^2+2x+58)$],

[89, $(x^4+18x^3+57x^2+47x+39)(x+71)^2(x^4+18x^3+57x^2+47x+22)$],

[107, $(x^2+68x+68)(x^8+39x^7+62x^6+87x^5+93x^4+71x^3+83x^2+14x+32)$],

[109, $(x^2+32x+46)(x^8+77x^7+106x^6+42x^5+53x^4+88x^3+87x^2+35x+88)$],

[131, $(x^2+35x+20)(x^8+96x^7+26x^6+52x^5+78x^4+83x^3+120x^2+35x+107)$],

[139, $(x^2+4x+83)(x^8+135x^7+72x^6+44x^5+24x^4+75x^3+71x^2+24x+4)$],

[157, $(x^2+99x+51)(x^8+58x^7+16x^6+11x^5+39x^4+80x^3+139x^2+57x+50)$],

[163, $(x^2+5x+28)(x^88+158x^7+160x^6+155x^5+21x^4+74x^3+20x^2+110x+66)$],

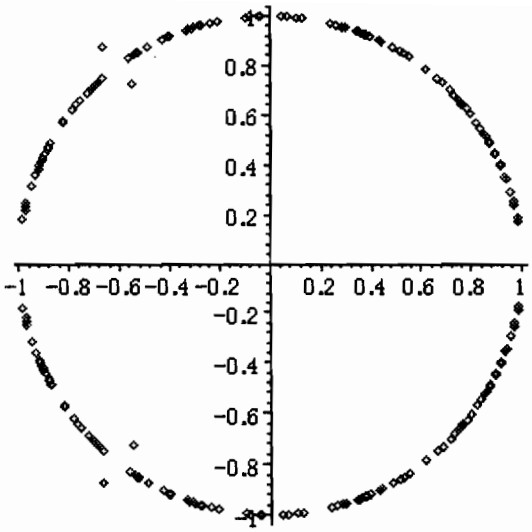
[173, $(x^2+143x+35)(x^8+30x^7+161x^5+46x^4+35x^3+132x^2+140x+84)$],

[181, $(x^2+152x+53)(x^8+29x^7+64x^6+138x^5+127x^4+143x^3+131x^2+21x+127)$],

[211, $(x^2+15x+68)(x^8+196x^7+157x^6+142x^5+125x^4+77x^3+51x^2+118x+43)$],

[227, $(x^2+66x+36)(x^8+161x^7+7x^6+98x^5+150x^4+211x^3+196x^2+125x+72)$],

[229, $(x^2+145x+44)(x^8+84x^7+142x^6+217x^5+132x^4+187x^3+53x^2+117x+102)$],



のようである。上の図で、標準終結根の絶対値が 1 でないものは、p = 89 の場合で、これは f(x)の判別式の約数となる場合で、f(x)が平方因子を含み、所謂、退化した場合である。

以下の場合は、8 を法として ±3 = 3, 5 の素数の場合で、Hasse の不等式、あるいは、谷山・志村の関係式、つまり、終結根(resultant transformation roots)の絶対値が $\sqrt{p}$ でない可能性のある場合である。

現実には p = 3 ~ 293 の素数のうち

3,11,19,29,43,53,61,67,89,107,109,131,139,157,163,173,181,211,227,229,293

のとき、$\sqrt{p}$ でない絶対値の終結根をもつ。mod 8 の ±3 の素数で、この列に現れないもの、つまり、谷山・志村関係をみたすものは、

5, 13, 37, 59, 83, 101, 149, 179, 197, 251, 269, 277, 283

である。ここまでの個数の比は 21/13 = 1.615384615 である。極限の比がどうなるかは未知である。

p mod 8 = 3,5, p = 2 ~ 293

	gal	$y^2 = f(x)$	det	$\neq\sqrt{p}$
T_1	10	$x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$	11^9	11
T_1	D_5	$x^{10}-2x^8+7x^6+41x^4+103x^2+47$	$2^{10}\cdot 5^4\cdot 11^8\cdot 43^4\cdot 47^5$	47
T_3	D_{10}	$x^{10}-2x^9+2x^8-2x^7+2x^6-x^5+3x^4-4x^3+x^2+1$	$3^5\cdot 11^2\cdot 47^4$	3
T_4	$5\cdot 4$	$x^{10}+22x^5-4$	$-2^{18}\cdot 5^{25}$	5
T_5	$2\times 5\cdot 4$	$x^{10}-2x^8-x^6+5x^4-5x^2+3$	$2^{10}\cdot 3^5\cdot 17^6$	3
T_6	$5 \wr 2$	$x^{10}-x^9+3x^7-3x^6+x^5+5x^4-x^3+2x^2+3x+1$	$7^5\cdot 11^4\cdot 53^2$	7,11,53
T_7	A_5	$x^{10}-x^8-4x^7-5x^6-8x^5-3x^4+4x^3+4x^2+4$	$-2^{30}\cdot 17^8$	-
T_8	$2^4\cdot 5$	$x^{10}-4x^8+2x^6+5x^4-2x^2-1$	$-2^{10}\cdot 11^8$	-
T_9	$5^2\cdot 2^2$	$x^{10}-x^9-5x^8+11x^6+4x^5-10x^4+25x^2+5x-5$	$-3^9\cdot 5^8\cdot 7^5\cdot 29^2\cdot 43^2$	3,7,29
T_{10}	$5^2\cdot 4$	$x^{10}+36x^5-176$	$-2^{36}\cdot 5^{25}\cdot 11^4$	5,11
T_{11}	$A_5\times 2$	$x^{10}+x^8-4x^2+4$	$2^{36}\cdot 17^4$	17
T_{12}	S_5/A_4	$x^{10}+2x^9+3x^8-x^6-2x^5-x^4+3x^3+2x+1$	$2^{27}\cdot 13^4$	-
T_{13}	S_5/D_6	$x^{10}-x^9-x^8+3x^6-x^5-2x^4+3x^3-x^2-x+1$	-1609^3	?
T_{14}	$2 \wr 5$	$x^{10}-x^9-9x^7+2x^6+29x^5-27x^4-4x^3+1x^2-4x+1$	$11^8\cdot 89^2\cdot 131\cdot 241^2$	89,131
T_{15}	$2^4\cdot 5\cdot 2$	$x^{10}-x^6-2x^4-2x^2-1$	$-2^{10}\cdot 47^4$	-
T_{16}	-	$x^{10}+7x^8+17x^6-31x^4-40x^2+127$	$2^{10}\cdot 3^{12}\cdot 5^{16}\cdot 127^5$	3,127
T_{17}	-	$x^{10}+2x^5-7$	$-2^{25}\cdot 5^{10}\cdot 7^4$	-
T_{18}	$5^2\cdot 8$	$x^{10}+60x^6-208x^5+850x^2-8000x-4672$	$-2^{42}\cdot 5^{10}\cdot 89^2\cdot 87623^2\cdot 7414739^2$	89,? ±3 (8)
T_{19}	$5^2\cdot D_4$	$x^{10}-10x^8+35x^6-2x^5-50x^4+10x^3+25x^2-10x+2$	$2^{14}\cdot 5^{12}$	-
T_{20}	$5^2\cdot Q_4$	$x^{10}+20x^8+70x^6+42x^5-425x^4+420x^3+275x^2-630x+436$	$-2^{10}\cdot 3^{10}\cdot 5^{15}\cdot 7^6\cdot 479^2\cdot 141461^2$	5 ?
T_{21}	$D_5 \wr 2$	$x^{10}+x^6-2x^5-x^4+3x^2-2x+1$	$2^{10}\cdot 3^2\cdot 29^2\cdot 761^2$	?
T_{22}	$S_5\times 2$	$x^{10}-x^9+2x^8-x^7+2x^6-2x^5-2x^3+x^2+1$	$3^5\cdot 1609^2$	3, ?
T_{23}	$2 \wr (5\cdot 2)$	$x^{10}-2x^8-x^7+3x^6+2x^5-2x^4-2x^3+2x^2+3x+1$	$47^4\cdot 191$	?
T_{24}	$2^4\cdot 5\cdot 2$	$x^{10}-2x^8-4x^6+8x^2-4$	$-2^{28}\cdot 13^6$	-
T_{25}	-	$x^{10}-2x^9-2x^7+4x^5+2x^4+10x^3+2x^2+8x+2$	$-2^{12}\cdot 13^7\cdot 389^2$	-
T_{26}	$L_2(9)$	$x^{10}-4x^9+12x^7-12x^6+12x^4-48x^3+64x+32$	$-2^{48}\cdot 3^{24}$	67
T_{27}	-	$x^{10}+3x^6-2x^5+x^2+2x+1$	$2^{10}\cdot 3^4\cdot 5^5\cdot 349^2$	5
T_{28}	-	$x^{10}-10x^7+10x^6+36x^5+50x^4-10x^3-1$	$-2^{10}\cdot 3^6\cdot 5^{10}\cdot$	5, ?

			$29^2 \cdot 26693^2$	
T_{29}	$2 \wr (5 \cdot 4)$	$x^{10}+x^9-x^8-2x^7-x^6-x^5+3x^4+2x^3+x^7-3x+1$	$2^{18} \cdot 3^5 \cdot 7^2 \cdot 37^2$	3
T_{30}	$PGL_2(9)$	$x^{10}-2x^9+9x^8-7x^2+14x-7$	$2^{32} \cdot 7^7 \cdot 19^6$	-
T_{31}	M_{10}	$x^{10}-2x^9+9x^8+2916x^2-5832x+2916$	$2^{43} \cdot 3^{60} \cdot 5^3$	-
T_{32}	S_6	$x^{10}-2x^9+x^8-9x^2+2x-1$	$-2^{38} \cdot 7^3 \cdot 13^3$	-
T_{33}	$(5 \cdot 4) \wr 2$	$x^{10}-2x^9+6x^8-8x^7+12x^6+24x^4+68x^2-24x+40$	$2^{46} \cdot 3^2 \cdot 5^3 \cdot 73^2 \cdot 433^2$	73, ?
T_{34}	$2^4 \cdot A_5$	$x^{10}+2x^6-4x^4-3x^2-4$	$-2^{36} \cdot 17^4$	3,17,131
T_{35}	$P\Gamma L_2(9)$	$x^{10}-2x^9+9x^8+2916x^2-5832x+2916$	$2^{43} \cdot 3^{60} \cdot 5^3$	-
T_{36}	$2 \wr A_5$	$x^{10}+3x^8-2x^7+7x^6-2x^5+7x^4-2x^3+3x^2+1$	$2^{18} \cdot 7 \cdot 29^4$	-
T_{37}	$2^4 \cdot S_5$	$x^{10}-4x^6+3x^4+2x^2-1$	$-2^{10} \cdot 35983^2$	-
T_{38}	-	$x^{10}+x^9-x^8-2x^7-3x^6+x^5+3x^4-2x^3+x^2+x-1$	$-2^8 \cdot 3^8 \cdot 53^3$	5,53
T_{39}	$2 \wr S_5$	$x^{10}+x^8-x^7-x^5-x^3+x^2+1$	$7 \cdot 53^2 \cdot 139^2$	7,53
T_{40}	$A_5 \wr 2$	$x^{10}+x^9-x^8-x^7-2x^6+2x^3+3x^2+x+1$	$-5^5 \cdot 17^2 \cdot 1459^2$	5,17,?
T_{41}	-	$x^{10}+x^9-x^8-2x^7-x^6-x^5+3x^4+2x^3+x^2-3x+1$	$2^{18} \cdot 3^5 \cdot 7^2 \cdot 37^2$	3
T_{42}	-	$x^{10}+10x^6-8x^5-25x^2+40x-16$	$-2^{52} \cdot 5^{10}$	-
T_{43}	$S_5 \wr 2$	$x^{10}-x^8-x^5+2x^4+2x^3-2x^2-x+1$	$3^5 \cdot 5^2 \cdot 11^2 \cdot 7369$	3,5,11,?
T_{44}	A_{10}	$x^{10}-2x^7-x^5+x^4-x^3+x^2-x+1$	$-3^2 \cdot 67^2 \cdot 641^2$	-
T_{45}	S_5	$x^{10}+x^9-x^8-x^7-x^5-2x^4-x^3+2x^7+2x+1$	$467 \cdot 514417$	-

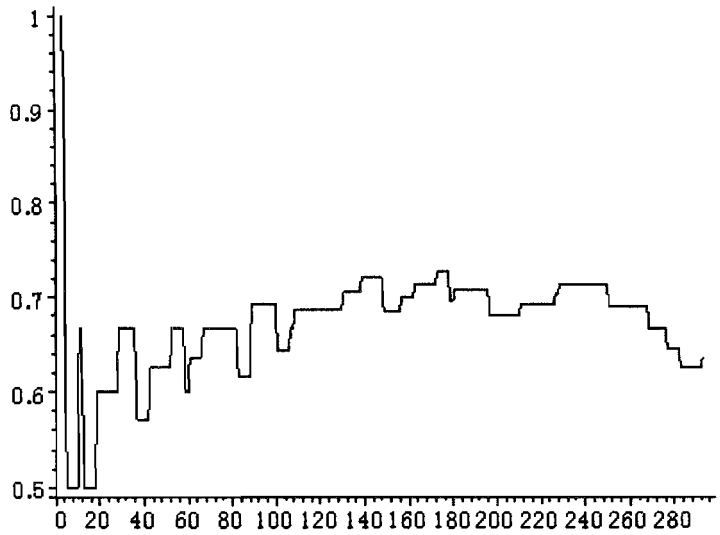
この表の示すところは、(計算に誤りがなければ…)

$$y^2 = x^{10}+60x^6-208x^5+850x^2-8000x-4672$$

$$gal = 5^2 \cdot 8,\ p = \pm 3 \bmod 8 \text{ の一部}$$

を除いて、Hasse の不等式、つまり、標準終結根の絶対値は 1 であった。勿論、この全体が正の確率をもつか、あるいは、多いけれども有限個か、などなかなか興味深い。

少ないデータから極限の状態を想像することは難しい…が、取りあえず、n までの $p = \pm 3 \bmod 8$ の素数のうちで、標準終結根で 1 でないものが存在する素数の割合を $p = 293$ までの範囲でグラフに記す。ちょっと…先行きの解らない雰囲気である。まあ気楽に考えて下さいとのことでしょう。



ゴキブリ(=蜚蠊, cockroach)、に関する諺ではないが、「1 匹いれば、30 匹はいる」(これが正しければ、銀河系はすぐにこの虫で満たされるか、体が小さくなる…が、ゴキブリであり続けるにはある程度の素粒子は必要。従って、正しくは正しくないが…)、上記のような、新しい系列は多く存在するものと思う。また、判別式と互いに素な素数で、標準終結根の絶対値が 1 でない場合も散見される。このような個別の条件の研究も大切なものと考える。新しい未知の洞窟への入り口の可能性がある。

3. 楕円関数の係数変換多項式と 5 次巡回対合

有限素体

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

上の楕円曲線の族、例えば、Weierstrass family, Euler family, Hessian family, Legendre family などに応じて、楕円曲線の j-不変量(j-invariant)を変数とした多項式、例えば、

$$a_{12}(x) = x^{(p\pm1)/4} P_{[p/6]}(x)$$

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

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

$$a_4(x) = F(1/4,3/4,1,x)$$

$$a_3(x) = F(1/3,2/3,1,x)$$

$$a_2(x) = F(1/2,1/2,1,x)$$

あるいは、それに、平方剰余記号(= Legendre symbol) $x^{(p-1)/2}$ を乗じたものが知られている。$a_6(x)$に関する族の popular な名前は知らないが

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

に対応するものである。

これも余談であるが、ワイヤストラスとかオイラーなど自分に関する呼称を思い起こさせる。…わがよたれそつねならむ…などから、たれそ(=誰そ= Who could knew)に因んで、仮に Whock-family とでも呼んでおくか…。

一般に、$p \geq 17$ では、Hasse の不等式から、絶対値最小剰余(least absolute value residue, lavr)として一意的に定まる。勿論、$p < 17$ に於いても、僅かの多様性を除いて決定でき代数的な意味をもっている。

例. $p = 31, a_{12}(x)$

例によって、初めから解説すると、

$$7/12 = 29 = -2 \bmod 31, \quad 11/12 = 19 \bmod 31$$

であるから、

$$F(7/12, 11/12,1,1-x) = 1+(-2)\,19/1\cdot x+(-2)(-1)\,19\cdot 20/4\cdot x^2 = 1+24x+4x^2$$

である。$p = 31 = -1 \bmod 4$ であるから、

$$(31+1)/4 = 8$$

より、

$$a_{12}(x) = x^8(1+24(1-x)+4(1-x)^2) = x^8(-2-x+4x^2)$$

である。また、$p = 31$ の場合の原始根(primitive root)は

$$[3, 11, 12, 13, 17, 21, 22, 24]$$

である。今の場合は 3 を考えることにする。

係数変換多項式(coefficient transformation polynomial)は、$a_{12}(x)$に原始根のべき乗を代入したもの、例えば、この場合 3^n を代入した列、の絶対値最小剰余

$$[a_{12}(3^n) \ : n = 0, 1, \cdots, p-2] =$$

$[1, 0, -9, 8, 4, 2, -6, 6, 5, 4, -4, 8, -1, -5, 7, 3, -4, -1, -8, 5, 0, -2, -2, -10, 3, -2, 4, 7, 10, 8]$

を x^n の係数とした多項式

$$\underline{a_{12}}(x) =$$

$$8x^{29}+10x^{28}+7x^{27}+4x^{26}-2x^{25}+3x^{24}-10x^{23}-2x^{22}-2x^{21}+5x^{19}-8x^{18}-x^{17}-4x^{16}+3x^{15}$$

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

である。上記多項式で x, x^{20} の項が抜けているのは $a_{12}(3) = a_{12}(3^{20}) = 0$ を意味

している。勿論、これらの係数は Hasse の不等式

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

つまり、今の場合は $2\sqrt{31} = 11.13552873$ で、11 はないが ±10 は現れている。係数変換多項式は、原始根の選び方によって異なることには注意が必要である。

剰余行列（residue matrix）とは

$$A_{ji} = g(x)\, x^{k-j-1} \bmod f(x) \text{ の } x^{k-i-1} \text{ の係数}$$

を成分とする行列のことで、

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

と記す。今は f(x) としては、有限素体 F_p の定義方程式

$$x^p-x$$

の約数となる多項式を考える。例えば、p = 31 の場合であれば、

$$x^p-x =$$

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

$$(1-x+x^3-x^4+x^5-x^7+x^8)(1+x-x^3-x^4-x^5+x^7+x^8)$$

のように既約因子は 1,2,4,8 次のものが各々 2 個づつ存在する。勿論、x を除いて、所謂、円分多項式（cyclotomic polynomial）である。

楕円曲線の族、例えば、Weierstrass family には

$$\underline{a}_{12}(x) = x^{(p\pm1)/4} P_{[p/6]}(x)$$

が対応しており、その係数変換多項式、つまり、b を原始根として x^n の係数を $f(b^n)$ とした p-2 次の多項式

$$\underline{f}(x) = \sum_{n=0}^{p-2} f(b^n)\, x^n$$

を f(x) の係数変換多項式として、既約円分多項式 g(x) との剰余行列（residue matrix）

$$A = \underline{a}_{12}(x)\,[x]\,g(x)$$

を作れば、

$$1/\sqrt{p}\cdot A\ ,\ 1/p\cdot A$$

の何れかは、対合（involution）、つまり、自乗が単位行列、$B^2 = E$ となる。掛けるべき定数が $1/\sqrt{p}$ になるのは、Gauss の整数あるいは Eisenstein の整数の場合に限る。つまり、

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

の約数

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

などに限る。通常は

$$1/p \cdot A$$

が対合になっている。これから、円分既約分解による対合分解(involution resolution)ができる。

以下に、$p = 31$, $a_{12}(x)$の場合、つまり、Weierstrass involution resolution、つまり、$a_{12}(x)$による分解を記す。

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

$$(1-x+x^3-x^4+x^5-x^7+x^8)\,(1+x-x^3-x^4-x^5+x^7+x^8)$$

が既約円分分解である。

$$f(x) = \underline{a}_{12}(x)$$

と略記すれば、x^2+x+1に対応する対合は

$$1/\sqrt{31} \cdot f(x)\,[x]\,x^2+x+1 = 1/\sqrt{31} \cdot \begin{pmatrix} 6 & 1 \\ -5 & -6 \end{pmatrix}$$

であり、勿論、Eisenstein latticeに対応している。以下、省略して記す

$$f(x)\,[x]\,x^2-x+1 = \begin{pmatrix} 0, & -31 \\ -31, & 0 \end{pmatrix}$$

この場合は$1/p = 1/31$が標準化因子(normalizer)である。

$$f(x)\,[x]\,x^4+x^3+x^2+x+1$$

$$\begin{pmatrix} 0, & 0, & 31, & 0 \\ 0, & 31, & 0, & 0 \\ 31, & 0, & 0, & 0 \\ -31, & -31, & -31, & -31 \end{pmatrix}$$

$$f(x)\,[x]\,x^4-x^3+x^2-x+1$$

$$\begin{pmatrix} 12, & 26, & -9, & 6 \\ 38, & -21, & 18, & -12 \\ 17, & -20, & 26, & -38 \\ -3, & 9, & -21, & -17 \end{pmatrix}$$

$$f(x)\,[x]\,x^8-x^7+x^5-x^4+x^3-x+1$$

$$\begin{pmatrix} 5, & 2, & -22, & 30, & 6, & 1, & 20, & -8 \\ 7, & -22, & 25, & 11, & -4, & 20, & -3, & -5 \\ -15, & 25, & 4, & 3, & 13, & -3, & 2, & -7 \end{pmatrix}$$

$$\begin{pmatrix} 10, 4, 18, -2, 12, 2, -22, 15 \\ 14, 18, -12, 22, -8, -22, 25, -10 \\ 32, -12, 8, 6, -36, 25, 4, -14 \\ 20, 8, -26, -4, -7, 4, 18, -32 \\ 28, -26, -24, 13, -16, 18, -12, -20 \end{pmatrix}$$

$$f(x)\,[x]\,x^8+x^7-x^5-x^4-x^3+x+1$$

$$\begin{pmatrix} -31, 0, 0, 0, 0, 31, 0, 0 \\ 31, 0, -31, -31, 0, 0, 31, 31 \\ -31, -31, 0, 31, 31, 31, 0, -31 \\ 0, 0, 0, 0, 0, 0, 0, 31 \\ 0, 0, 0, 0, 0, 0, 31, 0 \\ 0, 0, 0, 0, 0, 31, 0, 0 \\ 0, 0, 0, 0, 31, 0, 0, 0 \\ 0, 0, 0, 31, 0, 0, 0, 0 \end{pmatrix}$$

この場合のように、約半数は、自明な(trivial)対合になっている。尚、一次の因子についても記しておく。

$$f(x)\,[x]\,x = (1),\ f(x)\,[x]\,x-1 = (31),\ f(x)\,[x]\,x+1 = (-31)$$

である。

ここでの、本題は、このような、既約因子ではなくて、寧ろ、巡回行列になる円分因子、例えば、$x^3\pm1$ のような場合で、その既約因子の対合が退化、つまり、normalizer が $1, 1/\sqrt{p}$ とならない場合の

$$\underline{a}_{12}(x),\ (x/p)\,a_{12}(x) = x^{(p-1)/2}\underline{a}_{12}(x)$$

などで決定される巡回対合(cycilc involution)である。

$$f(x)\,[x]\,x^2-1 = \begin{pmatrix} 31, 0 \\ 0, 31 \end{pmatrix}$$

この場合は対合であるが、成分が $\pm p$ という意味で、自明である。

上記の場合は x^2+x+1 が退化因子であったから、$x^3-1=(x-1)(x^2+x+1)$ からは対合は得られない。

$$f(x)\,[x]\,x^3+1$$

$$\begin{pmatrix} 0, 0, -31 \\ 0, -31, 0 \\ -31, 0, 0 \end{pmatrix}$$

は巡回対合であるが成分にpを含む。以下、行列を成分表記する。

$$f(x)\,[x]\,x^5-1$$

$$=$$

$$[[0, 0, 0, 31, 0], [0, 0, 31, 0, 0], [0, 31, 0, 0, 0], [31, 0, 0, 0, 0], [0, 0, 0, 0, 31]]$$

$$f(x)\,[x]\,x^5+1$$

$$\begin{pmatrix} -12, 24, 14, 3, -6 \\ 24, 14, 3, -6, 12 \\ 14, 3, -6, 12, -24 \\ 3, -6, 12, -24, -14 \\ -6, 12, -24, -14, -3 \end{pmatrix}$$

この行列は、成分が後ろに挿入される度に符号が変わっている。従って、所謂、巡回行列(cyclic matrix)ではない。しかし、次数が奇数であるから、平方剰余、あるいは、同じことであるが、Legendre symbol を掛けて、つまり、行列の(i,j)成分 a_{ij} に対して、$(-1)^{i*j}a_{ij}$ を(i,j)成分とする行列を考えればよい。あるいは、$a_{12}(x)$に Legendre symbol、平方剰余記号を掛けた

$$(x/p)\,a_{12}(x) = (-x)^{(p-1)/2}\,a_{12}(x)$$

の係数変換多項式を考えればよい。係数変換多項式に平方剰余を掛けたものではないことに注意する。それは、巡回行列である。以下それを*を付けて記す。

$$f^*(x)\,[x]\,x^5-1$$

$$\begin{pmatrix} -12, -24, 14, -3, -6 \\ -24, 14, -3, -6, -12 \\ 14, -3, -6, -12, -24 \\ -3, -6, -12, -24, 14 \\ -6, -12, -24, 14, -3 \end{pmatrix}$$

このようにして期待通りの巡回対合を得る。

さて、ここでの主題は、5次の巡回対合である。5次の非自明な巡回対合の全体像はどの様なものか少し眺めていたときの感想から始めよう。

以下の note はそのときの感想である：

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

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

に 1/11 を乗じたような、5 次の整数係数巡回直交行列についてである。

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

が直交行列であるための条件は

$$^tAA = aE$$

の形の対角行列になることであるが、この行列の成分は、意外なことに(勿論、当然であるが)、次の 3 式からなる。

$$a^2+b^2+c^2+d^2+e^2,\ ac+bd+ce+da+eb,\ ab+bc+cd+de+ea$$

だから、対角成分は別にすれば

$$ac+bd+ce+da+eb = 0,\ ab+bc+cd+de+ea = 0$$

で特徴付けられる。従って、例えば、a, b, c を与えれば、d, e は決定してしまう。

計算例

以下のものは、$k^2 = a^2+b^2+c^2+d^2+e^2$ となる既約な直交行列の“類型”の表である。部分的な計算結果、つまり、$a \leq 200$ のため、大きめの k に対しては、この範囲の解にとどまっている。

[[5, [[2, 2, 2, 2, -3]]],

[11, [[4, -2, 1, -6, -8], [6, -3, -2, -6, -6]]],

[31, [[12, 6, 3, -14, 24], [18, -9, -6, 22, 6]]],

[41, [[12, -9, 4, -36, -12], [22, -14, -6, -26, -17]]],

[5·11, [[8, -7, 8, -12, -52], [18, -12, 8, -42, -27]]],

[61, [[18, -6, 2, -21, -54], [24, -16, 3, -48, -24]]],

[71, [[16, -11, 12, -26, -62], [26, 18, 6, -33, 54]]],

[101, [[36, 36, 12, -52, 69], [43, -24, 4, -68, -56]]],

[11^2, [[26, -21, 14, -112, -28], [36, 12, 4, -39, 108], [57, -32, 24, -24, 96],

[60, -40, -10, -85, -46]]],

[131, [[54, -18, -6, -59, -102], [64, -26, -14, -68, -87]]],

[151, [[54, -34, 18, -111, -78], [69, -48, -6, -114, -52]]],

[5·31, [[47, 32, 2, -58, 132], [48, -32, 28, -107, -92]]],

[181, [[48, -36, 27, -156, -64], [84, -28, -21, -84, -132]]],

[191, [[48, -38, 46, -116, -131], [78, 74, 66, -114, 87]]],

[5·41, [[48, -12, 3, -52, -192], [98, -37, -22, -102, -142]]],

…

などである。素数5は別として、非自明なもので素数のものは $p = 1 \bmod 10$ のものに限られ、それらは、符号や順序といった、簡単な操作で移りあえるものは、どうも、常に、2種類しか存在しないのではないかとの印象をもった。

$p = 11$

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

が、その2つの類型の例である。左のものは1つを除いて3の倍数、右のものは1つを除いて偶数である。

$p = 31$

$$\begin{pmatrix} 22, & 18, & -6, & 6, & -9 \\ 18, & -6, & 6, & -9, & 22 \\ -6, & 6, & -9, & 22, & 18 \\ 6, & -9, & 22, & 18, & -6 \\ -9, & 22, & 18, & -6, & 6 \end{pmatrix} \quad \begin{pmatrix} 24, & 12, & 6, & 3, & -14 \\ 12, & 6, & 3, & -14, & 24 \\ 6, & 3, & -14, & 24, & 12 \\ 3, & -14, & 24, & 12, & 6 \\ -14, & 24, & 12, & 6, & 3 \end{pmatrix}$$

$p = 41$

$$\begin{pmatrix} 26, & 14, & 17, & 6, & -22 \\ 14, & 17, & 6, & -22, & 26 \\ 17, & 6, & -22, & 26, & 14 \\ 6, & -22, & 26, & 14, & 17 \\ -22, & 26, & 14, & 17, & 6 \end{pmatrix} \quad \begin{pmatrix} 36, & 12, & -12, & 9, & -4 \\ 12, & -12, & 9, & -4, & 36 \\ -12, & 9, & -4, & 36, & 12 \\ 9, & -4, & 36, & 12, & -12 \\ -4, & 36, & 12, & -12, & 9 \end{pmatrix}$$

$n = 55 = 11 \cdot 5$

$$\begin{pmatrix} 52, & 12, & -8, & 7, & -8 \end{pmatrix} \quad \begin{pmatrix} 42, & 27, & -18, & 12, & -8 \end{pmatrix}$$

$$\begin{pmatrix} 12, -8, 7, -8, 52 \\ -8, 7, -8, 52, 12 \\ 7, -8, 52, 12, -8 \\ -8, 52, 12, -8, 7 \end{pmatrix} \qquad \begin{pmatrix} 27, -18, 12, -8, 42 \\ -18, 12, -8, 42, 27 \\ 12, -8, 42, 27, -18 \\ -8, 42, 27, -18, 12 \end{pmatrix}$$

この場合はn = 55は素数ではないが、二組の既約な解が存在する。

p = 61

$$\begin{pmatrix} 48, 24, -24, 16, -3 \\ 24, -24, 16, -3, 48 \\ -24, 16, -3, 48, 24 \\ 16, -3, 48, 24, -24 \\ -3, 48, 24, -24, 16 \end{pmatrix} \qquad \begin{pmatrix} 54, 21, -2, 6, -18 \\ 21, -2, 6, -18, 54 \\ -2, 6, -18, 54, 21 \\ 6, -18, 54, 21, -2 \\ -18, 54, 21, -2, 6 \end{pmatrix}$$

この場合も確かに、本質的には、この2つのみから成っている。

p = 71

$$\begin{pmatrix} 54, 26, 18, 6, -33 \\ 26, 18, 6, -33, 54 \\ 18, 6, -33, 54, 26 \\ 6, -33, 54, 26, 18 \\ -33, 54, 26, 18, 6 \end{pmatrix} \qquad \begin{pmatrix} 62, 26, -12, 11, -16 \\ 26, -12, 11, -16, 62 \\ -12, 11, -16, 62, 26 \\ 11, -16, 62, 26, -12 \\ -16, 62, 26, -12, 11 \end{pmatrix}$$

少なくとも、ここまでは、p = 10n+1型の素数について、丁度2組、しかも、それだけの解が存在している。

以下の表は、既約構成要素の絶対値の表である。例えば、

[5, [[3, -2, -2, -2, -2]]]

に対しては、[5, [[2, 3]]と省略して記し、

[11, [[6, -6, -6, -2, -3], [6, -6, -3, -6, -2], [6, -6, 2, 6, 3], [6, -6, 3, 2, 6],
[6, -3, -2, -6, -6], [6, -2, -6, -3, -6], [6, 2, -6, 6, 3], [6, 2, 3, -6, 6],
[6, 3, 6, -6, 2], [6, 3, 6, 2, -6], [6, 6, -6, 3, 2], [6, 6, 2, 3, -6],
[8, -4, 2, -1, 6], [8, -1, -4, 6, 2], [8, 2, 6, -4, -1], [8, 6, -1, 2, -4]]]

に対しては、2つの組があり、[11, [[1, 8, 4, 6, 2], [6, 2, 3]]]と記した。

[[5, [[2, 3]]], [10, [[2, 3]]], [11, [[1, 8, 4, 6, 2], [6, 2, 3]]], [15, [[3, 2]]],
[20, [[3, 2]]], [22, [[6, 2, 3], [8, 6, 4, 2, 1]]], [25, [[3, 2]]], [30, [[3, 2]]],
[31, [[24, 14, 12, 6, 3], [22, 18, 9, 6]]], [33, [[6, 3, 2], [8, 6, 4, 2, 1]]],
[35, [[3, 2]]],[40, [[3, 2]]], [41, [[26, 22, 17, 14, 6], [36, 12, 9, 4]]],

[44, [[8, 6, 4, 2, 1], [6, 3, 2]]],[45, [[3, 2]]], [50, [[2, 3]]],
[55, [[8, 4, 2, 1, 6], [12, 8, 7, 52], [27, 18, 12, 8, 42], [3, 2], [3, 2, 6]]],
[60, [[3, 2]]], [61, [[24, 16, 3, 48], [54, 21, 18, 6, 2]]],
[62, [[14, 12, 6, 3, 24], [18, 9, 6, 22]]], [65, [[3, 2]]],
[66, [[6, 3, 2], [6, 4, 2, 1, 8]]],[70, [[2, 3]]],
[71, [[62, 26, 16, 11, 12], [54, 33, 26, 18, 6]]], [75, [[2, 3]]],
[77, [[8, 4, 2, 1, 6], [3, 2, 6]]], [80, [[2, 3]]],
[82, [[36, 12, 9, 4], [17, 14, 6, 26, 22]]],
[85, [[2, 3]]], [88, [[8, 4, 2, 1, 6], [3, 2, 6]]], [90, [[3, 2]]],
[93, [[24, 12, 6, 3, 14], [18, 22, 9, 6]]]]

この表からも 55 = 11·5 では新しい既約解が存在していることが解る。

例 p = 331 の場合

[331, [[144, -52, -18, -159, -246], [146, -66, -3, -186, -222]]]

のように 2 通りの解がある。この係数に応じて

$f(x) = 144x^4-52x^3-18x^4-159x-246 = 144(x+8)(x+181)(x+330)(x+207) \mod 331$

$g(x) = 146x^4-66x^3-3x^2-186x-222 = 146(x+116)(x+267)(x+330)(x+207) \mod 331$

である。これから想像されることは、330 は p で ±1 であること、一次因数に完全に分解していること。また、

$$x^5-1 = (x+8)(x+267)(x+181)(x+330)(x+207)$$

であり、f(x), g(x)の因数は、奇妙なことに x+116 を除いて、このなかから採用されている。(x+330)(x+207)は共通因数である。従って

$$(x+8)(x+181)(x+330)(x+207) \otimes x^5-1 =$$

$$2^5\cdot 3^2\cdot 7\cdot 11\cdot 13^2\cdot 71\cdot 281\cdot 331^4\cdot 3224731\cdot 5520271\cdot 592621$$

$$(x+116)(x+267)(x+330)(x+207) \otimes x^5-1 =$$

$$2^6\cdot 3^2\cdot 11\cdot 13^2\cdot 31\cdot 67\cdot 71\cdot 101\cdot 281\cdot 331^3\cdot 5520271\cdot 151451\cdot 526441\cdot 592621$$

であり、こちらの方は、当然ながら、331 のベキは 3 である。因数の 116 はどのようにして決定したのであろうか。

例えば、p = 31 の場合

[[22, -9, 6, -6, 18], [22, -6, -9, 18, 6], [22, 6, 18, -9, -6], [22, 18, -6, 6, -9],
[24, -14, 3, 6, 12], [24, 3, 12, -14, 6], [24, 6, -14, 12, 3], [24, 12, 6, 3, -14]]

の 2 種類、最高次の係数を正の最大値として、計 8 個が存在する。これらから、例えば、

$$22x^4-9x^3+6x^2-6x+18 = 22\,(x+29)\,(x+30)\,(x+27)\,(x+8)$$

のように mod 31 で分解すると、完全に一次の因子に分解される。

p = 10n+1 型の素数については

$$a_m(x),\ m = 2,3,4,6,12$$

の係数変換多項式の x^5-1 での剰余

$$a_m(b^n)\,x^n \bmod x^5-1$$

から、既約な解が得られるであろうと予想されているから、これら、5 組の解は二組に縮約するものと考えられるが、現実にはどうであろうか。

p = 31

$$a_6(x) = F(1/6,\ 5/6,1,x) = 1+x+24x^2+29x^3+10x^4+27x^5$$

の場合。

$$[a_6(3^n) : n = 0 \sim p-2] =$$

[-1, 4, 7, 4, 0, 4, 0, 8, -3, -4, 2, 0, -1, 1, -5, 9, 4, 5, -4, 3, -4, -8, -6, 10, -9, -4, 6, -7, -2, -10]

で、その表現多項式、つまり、係数変換多項式は

$$\underline{a_6}(x) =$$

$$-10x^{29}-2x^{28}-7x^{27}+6x^{26}-4x^{25}-9x^{24}+10x^{23}-6x^{22}-8x^{21}-4x^{20}+3x^{19}-4x^{18}+5x^{17}$$

$$+4x^{16}+9x^{15}-5x^{14}+x^{13}-x^{12}+2x^{10}-4x^9-3x^8+8x^7+4x^5+4x^3+7x^2+4x-1$$

である。

$$B_6 = \underline{a_6}(x)\,[x]\,x^5+1 =$$

[[12, 14, 6, -24, 3]

[14, 6, -24, 3, -12]

[6, -24, 3, -12, -14]

[-24, 3, -12, -14, -6]

[3, -12, -14, -6, 24]]

は巡回対合ではないが。従って、$(-1)^{i+j}$ を掛けて、つまり、checker bord 変換をすると

$$B_6 = \underline{a_6}^*(x)\,[x]\,x^5-1$$

[12, -14, 6, -24, 3]

[-14, 6, -24, 3, 12]

[6, -24, 3, 12, -14]

[-24, 3, 12, -14, 6]

[3, 12, -14, 6, -24]

のような巡回対合を得る。これは、$a_{12}(x)$から得られた［12, 6, 3, -14, 24］と同伴(conjugate)のもので本質的に新しいものではない。

p = 31

$$a_4(x) = F(1/4,3/4,1,x) = 1+6x+12x^2+16x^3+18x^4+15x^5+15x^6+9x^7$$

の場合。

$$[a_4(3^n) : n = 0 \sim p-2] =$$

[-1, 10, -4, -4, 8, 2, 0, -2, 8, -10, 0, -8, -4, 4, 4, 0, 8, -4, -8, -8, 4, 2, -8, -6, 0, -2, 8, 4, 0, 6]

であり、従って、

$$\underline{a_4}(x) =$$

$$6x^{29}+4x^{27}+8x^{26}-2x^{25}-6x^{23}-8x^{22}+2x^{21}+4x^{20}-8x^{19}-8x^{18}-4x^{17}+8x^{16}$$

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

である。剰余行列は

$$B_4 = \underline{a_4}(x)\,[x]\,x^5+1 =$$

[[-3, 12, 14, 6, -24]

[12, 14, 6, -24, 3]

[14, 6, -24, 3, -12]

[6, -24, 3, -12, -14]

[-24, 3, -12, -14, -6]

である。checker bord 変換で巡回対合が得られる。この場合も得られる対合は[12, 6, 3, -14, 24]と同伴で、新しい類型ではない。

p = 31

$$a_3(x) = F(1/3,2/3,1,x) = 1+14x+25x^2+28x^3+30x^4+16x^5+23x^6+13x^7+21x^8+20x^9+27x^{10}$$

の場合。

$$[a_3(3^n) : n = 0 \sim p-2] =$$

[1, -4, 5, -4, 8, 8, -4, -4, -1, -4, 2, 8, 5, 5, -7, 5,

-4, -7, -4, -1, -4, -4, -10, 2, 5, 8, -10, 5, 2, 2]

であり、

$$\underline{a_3}(x) =$$

$$2x^{29}+2x^{28}+5x^{27}-10x^{26}+8x^{25}+5x^{24}+2x^{23}-10x^{22}-4x^{21}-4x^{20}-x^{19}-4x^{18}-7x^{17}-4x^{16}$$

$$+5x^{15}-7x^{14}+5x^{13}+5x^{12}+8x^{11}+2x^{10}-4x^9-x^8-4x^7-4x^6+8x^5+8x^4-4x^3+5x^2-4x+1$$

である。

$$B_3 = \underline{a_3}(x)\,[x]\,x^5+1 =$$

[[22, -18, -6, -6, -9]

[-18, -6, -6, -9, -22]

[-6, -6, -9, -22, 18]

[-6, -9, -22, 18, 6]

[-9, -22, 18, 6, 6]]

からは、checker boad 変換で新しい巡回対合の類型

[18, -9, -6, 22, 6]

を得ることができる。

p = 31

$$a_2(x) = F(1/2,1/2,1,x) =$$

$$1+8x+20x^2+7x^3+x^4+16x^5+10x^6+14x^7+14x^8+10x^9+16x^{10}+x^{11}+7x^{12}+20x^{13}+8x^{14}+x^{15}$$

の場合

$$[a_2(3^n) : n = 0 \sim p-2] =$$

[-1, 4, -8, -8, 0, 4, 0, -4, 0, -4, 8, 0, 8, -8, -8, 0, -8, 8, 8, 0, 8, 4, 0, 4, 0, -4, 0, 8, -8, -4]

であり、

$$\underline{a_2}(x) =$$

$$4x^{29}+8x^{28}-8x^{27}+4x^{25}-4x^{23}-4x^{21}-8x^{20}-8x^{18}-8x^{17}+8x^{16}+8x^{14}+8x^{13}-8x^{12}-8x^{10}+4x^9+4x^7-4x^5+8x^3+8x^2-4x+1$$

である。

$$B_3 = \underline{a_2}(x)[x]x^5-1 =$$

[-15, 0, -12, 12, 16]

[0, -12, 12, 16, -15]

[-12, 12, 16, -15, 0]

[12, 16, -15, 0, -12]

[16, -15, 0, -12, 12]

$$B'_3 = \underline{a_2}(x)[x]x^5+1$$

[15, 16, -12, -12, 0]

[16, -12, -12, 0, -15]

[-12, -12, 0, -15, -16]

[-12, 0, -15, -16, 12]

[0, -15, -16, 12, 12]]

は共に、checker boad 変換をしても、巡回対合を生成しない。

結論めいたものを述べれば、外のかなり多くの素数についても調べて、

[12, 6, 3, -14, 24]は $a_{12}(x)$, $a_6(x)$, $a_4(x)$に符号変換したものから生成でき、

[18, -9, -6, 22, 6]は $a_3(x)$に符号変換したものから生成できる。

また、$a_2(x)$からは、どちらも生成できない。

そこで、目的の問題であるが、

> 問題 (well-known?)
> $p = 1 \bmod 10$ の素数に対しては
> 非自明な巡回対合の類型は
> $\underline{a_4}^*(x)[x]x^5-1$, $\underline{a_3}^*(x)[x]x^5-1$
> の2つのみか

勿論、主要な眼点は、

$$\text{Euler family} \quad a_4^*(x) = (x/p)\,a_4(x) = x^{(p-1)/2}\cdot F(1/4,3/4,1,x)$$

$$\text{Hessian family} \quad a_3^*(x) = (x/p)\,a_3(x) = x^{(p-1)/2}\cdot F(1/3,2/3,1,x)$$

の係数変換多項式と x^5-1 の剰余行列

$$\underline{a_4}^*(x)[x]x^5-1,\ \underline{a_3}^*(x)[x]x^5-1$$

で類型が「尽くされる」か…ということである。

何故、このような、問題意識をもったかについてであるが、近時、5を周期とする基本的対称性が、化学、鉱物学、物理学、生物学などの分野で話題にもなり、また、古代から、易、孫子、書経等でも、桜、ほのかな香りの梅、異臭を放つラフレシアまで5に関係している。

$$5^2 = 4^2+3^2 = 3^2+2^2+2^2+2^2+2^2$$

を別格として、$p = 10n+1$ の素数に応じて、各々4個の同値類から成る2組、一方は偶数(Euler, Gauss的, feminine?)、他方は3の倍数(Hesse, Eisenstein的, manly?)を基調としている。

自然の言語は「5の言語」(quintics)も用いているのではないか

という“夢”である。数の世界には、有限体上の楕円曲線のなかに「対応物」の候補があるということを述べたかったのである。

references

[1] Kanji Namba: *Hyper-elliptic curves over finite fields and manifolds at infinity*, Reports of 2011 symp. on applied math., Ryukoku Univ. pp.26-31.