Genus 5 hyper-elliptic curves and their coefficient manifolds

難波完爾 (Kanji Namba)

463-3 Kitamizote Sojya Okayama 719-1117

tel/fax. 0866-90-1886

2013. 01. 16

この論文では、種数 5 までの超楕円曲線

$$E:\ y^2 = f(x),\ \deg(f(x)) \le 12$$

について論ずる。

1. 諸概念

超楕円曲線

$$E:\ y^2 = f(x)$$

の定義に現れる多項式 f(x) のチルンハウス変換 (Tschirnhaus transform)、つまり、f(x) と monic な多項式との終結式 (resultant) を、次数に応じて

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

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

のように記す。ここに、(一般の積の) 記号 ⓧ, ⓨ, … は終結式の記号で

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

の (ここだけの) 省略記号であり、(ここだけの呼称であるが) 消去積 (elimination product) とも呼ぶ。記号の結合力は加減乗除 (+, -, ×, /) より弱いものとする。基本性質としては

$$f(x) \textcircled{x} (g(x)h(x)) = (f(x) \textcircled{x} g(x))(f(x) \textcircled{x} h(x))$$

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

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

$$f(x) \textcircled{x} g(x)^n = (f(x) \textcircled{x} g(x))^n = f(x)^n \textcircled{x} g(x)$$

のような (積) 分配法則、結合法則、単位元 (代入, delta-function)、(冪) 交換法則 (exponential commutative law) などがある。

また、素数 p に関する平方剰余、つまり、ルジャンドル記号 (Legendre Symbol) を (a/p) と記す。p が奇素数のときは

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

である。これは、オイラーの定理と呼ばれているものの一つである。

上記、超楕円曲線の合同ゼータ核(congruence ζ-kernel)、ここでは、終結変換(resultant transform)多項式(ここだけの仮の名称)とも呼ぶ、の係数を、f(x)の次数の偶奇に応じて次のように定義する。

a) f(x)の次数が奇数の場合：

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

b) f(x)の次数が偶数の場合：

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

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

これは、無限遠多様体(manifold at infinity)に対応するもので、周知のものであろうと思うが、私には、この定義に至るまでに長い時間を要した。これらの係数を終結係数(resultant coefficient)と呼ぶ。

多項式 f(x)の合同ゼータ(核)多項式、つまり、終結変換多項式を、例えば、ζf(x), $\underline{f}(x)$などと記す。

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

のような多項式である。超楕円曲線

$$E:\ y^2 = f(x)$$

の種数が g = n, つまり、f(x)の次数が 2n+1, 2(n+1)の場合は $\zeta f(x) = \underline{f}(x)$ の次数は 2n である。谷山・志村理論に従えば、合同ゼータ多項式の根、つまり、終結変換多項式 = 0 の解はすべて絶対値 $\sqrt{p}$ の、一般には実数でない複素数であり、例外的な状況では実数のこともあり得る。(これらは合同ゼータ根、終結(変換)根と略称する)

終結変換多項式は整数係数(従って実数)の多項式であるから根は互いに複素共役(complex conjugate)な種数個の解から成っている。これらの解の実数部分を解とする多項式を係数多項式(coefficient polynomial)と呼ぶ。係数多項式 $\eta f(x) = \bar{f}_p(x)$ は

$$\zeta f(x) \circledast x^2+ux+p$$

の平方根として

$$\eta f(x) = \sqrt{\zeta f(x) \circledast x^2+ux+p}$$

のように定義される。終結式の演算はべき乗根と交換可能であるから、むしろ、例えば

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

のように多項式のべき乗根との終結式の定義とするのが自然である。

この意味では、例えば、単位円を自然境界にもつ無限積

$$\eta(x) = x^{1/24}\,\Pi(1-x^n) = \Sigma\, x^{1/4!(3!n+1)\wedge 2}$$

と、$f(x) = x^3-1/2$ の終結式(単位円のなかにすべての根がある)

$$\eta(x) \circledast x^3-1/2 = x^{1/24}\,\Pi(1-x^n) \circledast x^3-1/2$$

のようなものも、べき乗根と積との結合法則から、自然に考えられる。

無限積同士の終結式で有限確定の定数になる場合の具体的な例は知らないが、多くの既知の定数はこのようなものであろうと想像される。

終結変換多項式 $\underline{f}_p(x) = 0$ の解の絶対値は $\sqrt{p}$ の複素数だから、係数多項式 $\bar{f}_p(x) = 0$、つまり、係数根は絶対値 $2\sqrt{p}$ 以下の実数である。そこで、標準係数多項式を

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

と定義すれば、標準係数多項式は絶対値 2 以下の実数のみを根とする多項式である。

2. 具体例

2.1 訂正を兼ねて

Reports of Institute for Mathematics and Computer Science

22nd Symposium on the History of Mathematics, 2011

Kanji Namba: Hyper-elliptic curves and Hasse's inequality, pp. 137-174

の記事の p.153 に於ける

$$E: y^2 = x^{10}+60x^6-208x^5+850x^2-8000x-4672,\ gal = 10T_8 = 5^2\cdot 8$$

の係数多項式の第 3 次係数 c_p の一部に誤りがあり、その原因となった事項など報告・訂正したいと思う。また、主張の一部を訂正します。

上記論文記載の p.153-154 のデータの最初の部分は

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

[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],

ですが、正しい(と思われる)データは

[2, -1, -2, -4, -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], [307, -11, 516, -190, 121808],
[311, -21, 364, -5116, 48850], [313, -9, -168, 2168, -23162],
[317, -11, 136, -3414, 94988], [331, -3, -8, -1238, -51968],

[337, 1, 30, -2754, -32788], [347, -29, 750, -11490, 221462],
[349, 3, 434, 456, 66116], [353, 47, 1262, 26638, 521050],
[359, -13, 390, -2910, 151750], [367, -25, 384, -7776, 175234],
[373, -23, 394, 7802, -224376], [379, -25, 616, -11824, 245954],
[383, -15, 244, -1040, -80908], [389, -1, -474, 2542, 261358],
[397, -39, 874, -13926, 209584], [401, 9, 370, 4602, 161200],
[409, 21, 166, -2734, -32456], [419, 11, 22, 4686, 124238],
[421, -5, 188, 2410, -44436], [431, 3, 396, 15324, 35186],
[433, 5, 228, -9220, -61792], [439, 35, 492, -372, -112194],
[443, 13, 268, -7812, -27426], [449, -11, 190, 838, -271572],
[457, 43, 716, 6508, 89130], [461, 31, 1006, 25928, 649836],
[463, 15, 874, 12926, 489770], [467, 1, 510, -5394, 210656],
[479, -23, 270, 10042, -221060], [487, -8, 526, -1510, 248543],
[491, -45, 922, -24496, 710424], [499, 13, 916, 16824, 456200],
[503, 23, 149, 7339, 307249], [509, 15, 44, 8624, 349316],
[521, 1, -64, 2580, 117000], [523, -13, 632, -1028, 166396],
[541, -21, 918, -20856, 714726], [547, 1, -24, -3356, -272010],
[557, 23, 810, 22630, 696136]]

です。表の数値が少し長めになったが計算にある程度の時間を要したので p = 557 まで記した。この場合、多項式の次数は 10 で偶数だから、係数は

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

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

とする必要がある。

自分はいつも、形式的な定義に従った計算と、階差法に基づいた高速計算法を用いて計算をしているのですが。最初の形式的な定義では、例えば、

$$f_4(u,v,w,z) = x^{10}+60x^6-208x^5+850x^2-8000x-4672 \otimes x^4+ux^3+vx^2+wx+z$$

$$=$$

$$-101978472448u^{10}+174620672000u^9v-336114892800u^9w$$

$$+\cdots-2837346713600000w+5144168058880000z+476443423277056$$

のような 671 項 18085 文字の式です。p = 557 の場合、この式に対し

$$\sum x,y,z,t\in p\ (f_4(x,y,z,t)/p)$$

のような 4 重和を計算する訳です、回数は

$$p^4 = 557^4 = 96254442001$$

で、約千億回です。階差の方法では

$$s0 = [-4672, 9119, 12682, 119580, 962040, 5235960,$$
$$16478640, 29635200, 30240000, 16329600, 3628800]$$

s1 = [[21827584, -42603968, -59250304, -558677760, -4494650880, -24462405120,
-76988206080, -138455654400, -141281280000, -76291891200, -16953753600],
[76713569, 934398, 63824100, 449022840, 2817970320,
11234148960, 23140296000, 24978038400, 13530182400, 2903040000],
[28143182, -22823380, -67552280, -237902160, -1359604320,
-2710843200, -2116540800, -485856000, 68544000],
[38508540, 11996400, -5083680, 195494400, 303984000, 85824000, -29376000, 0],
[29059320, 14097120, -51940800, -18748800, 24019200, 5990400, 0],
[36075960, 20206560, -20299200, -3600000, 8582400, 2995200],
[43233840, 11390400, -11145600, -2937600, 1036800],
[46569600, 4032000, -2419200, 0], [35078400, 0, 0], [16329600, 0], [3628800]]

のように階数毎に、つまり、

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

に応じて複雑にはなりますが、例えば、

$$\sum x,y,z,t \in p \ (f_4(x,y,z,t)/p)$$

の場合でも、計算の核(computational kernel)、つまり、一番深いループのプログラムは

```
d:=d+t[(d0 mod p)+1]:
d0:=d0+d1:d1:=d1+d2:d2:=d2+d3:d3:=d3+d4:d4:=d4+d5:
d5:=d5+d6:d6:=d6+d7:d7:=d7+d8:d8:=d8+d9:d9:=d9+da:
```

といった、同時処理可能な 12 個の加法と平方剰余表の参照だけです。勿論、例えば、

```
d0:=d0+d1: if d0>p then d0:=d0-p fi:
```

などとして、処理中の数値があまり大きくならないようにすることも(場合によっては)必要です。

パソコンでは無理(でもないか)ですが、ちょっと気の利いた計算機ならば加法の部分の実行時間は同時処理により 1 回の加法時間(addition time ≠

additional time)ですみます。

何れにしても、結果の正確性の保証度の高い、しかし、実行時間のかかる計算と、階差法などの、語長は長いが実行時間の短いプログラムを用いて計算する訳です。

私の場合は、好みもあって、昔のように、正確性の保証度の高いプログラムで小さな素数、例えば、

[2, -1, -2, -4, -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], …

を求めておいて、次に階差法などの結果と照合して、ここが問題なのですが、本格的な計算を実行する訳です。

例の場合は

[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]

です。この場合は5箇所符号が異なっています。

[2, -1, -2, 0, -8], [3, 1, 4, 4, 12],[11, -5, 18, 30, 68],
[13, -3, 4, 2, -46], [19, -5, 16, 40, 142]

の符号です。このようなことが、

G. Malle, B.H.Matzat, Inverse Galois Theory
p.416 Appendix: Example Polynomials degree 10

の $T_1 \sim T_{45}$ の T_{17} のところで起こったのです。残りの場所では、Hasseの不等式は正常に検証されて、志村・谷山の定理の確かさを実感した訳です。

私のような実験屋にとっては、計算の動機付けと意欲は研究の継続の動機の一番大切な要素だと思っていますので、ここの同一性の検証も「機械に」やらせれば、「誤りも少ない」でしょうに、何で(好き好んで、見誤りや考え違いの入りやすい)目と手にたよるのか。という意見は痛い程わかるのです。でも、昔の感覚の“香を聞く”という方を選んでいる訳です。かれこれ50年(=半世紀)ばかり続けていますが、誤りこそ、現実というものを(よいことではありませんが)実感できる瞬間なのです。万葉集巻16の第3歌、竹取の翁の非慮之外偶逢です。

上記の続きですが、毎日の例の如く、上記の二つのデータを

“一瞥して”、“一致している”

と(間違えていますが…)、そのときは判断して計算を継続したのでした。でも、何故このようなことが起こったのでしょうか。予兆はあったのでしょうか。何故 $f_3(u,v,w)$ に関係する係数だったのでしょうか。そういえば…、と連想と回想の糸を辿ってゆくと、あるとき、

f3:=(u,v,w)->

に

$$f(x) \textcircled{x} x^3+ux^2+vx+w$$

を計算した式を貼り付け(paste)して実行キーを押したとき、一時的に画面から式が消えたことがあったことを思い出した。その後のコンパイルの処理は、どうやら正しく実行されているらしくプログラムは正常に、つまり、停止したり巨大な数字を出力したり 0 ばかり続くといったこともなかったのです。

コンパイルの段階や、プログラムの入力のミスは通常、何かのはっきりした異常を呈するものだというような思い込みがあったのであろう。

結果としては、ものごとはハッキリしている。3 度でも 5 度でも繰り返し確かめるべきであった…としかいいようがない。そして f3 なる文字列が control に関するものであることにも注意する必要がある。これを関数名に用いたのである。これが、…恐らくは、

「絶対にやってはいけないこと」

の一つ、つまり、不妄語(不蒙語)、不奇語、不両舌などに相当する行為なのだと思った。

「ほとんど正常に作動するプログラム」

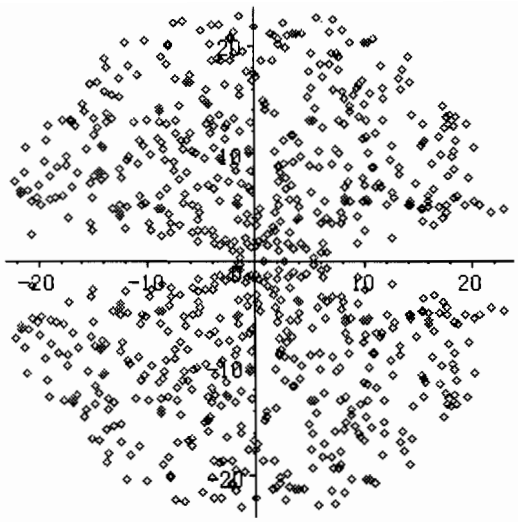
これほど危険なものはない。時々、整数の符号のみ間違える。常に間違えるわけではない。その他のことはみんな正しい。人であれば、このような人が高い地位にいる場合は、社会全体に及ぶような危険な事態を想定しておく必要がある。(バベルの塔の話など思い出す)

…というような本質的というか末端の事実を離れ、再(々)計算の結果を記す。

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

$$gal = 10T_8 = 5^2 \cdot 8, \text{ resultant transform roots}$$

$$p = 2 \sim 557$$



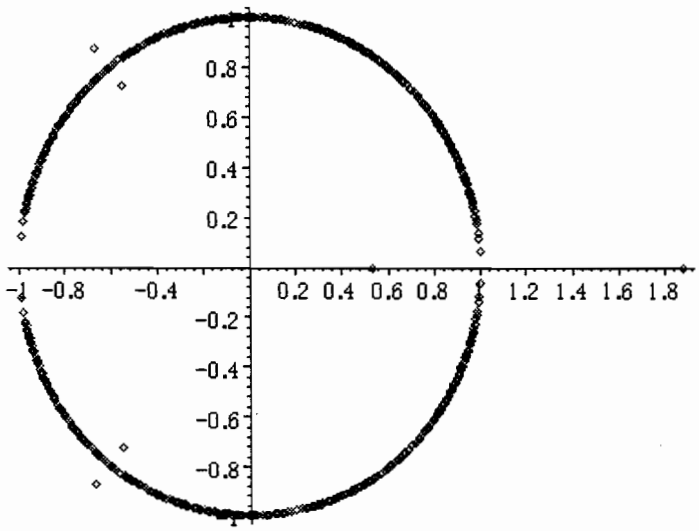
このグラフでは、$\overline{f_p}(x) = \zeta f_p(x) = 0$ の絶対値 $\sqrt{p}$ の根をそのまま plot している。角分布は正規の場合の

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

型であろうと思う。次の図は $\sqrt{p}$ で割った標準終結根(normalized resultant transform(ation) roots)の分布を記す。単位円周上に分布するというのが志村・谷山理論の主張である。

normalized resultant transform roots

p = 2 ~ 557



この場合、単位円周上にない点が存在する。判別式は

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

であり、p = 2, 5, 89, 87723, 7416739 に於いては例外的な挙動をする可能性がある。つまり、その素点(= 素数)では f(x)は重根をもち、種数が退化するからである。しかし、解の絶対値が $\sqrt{p}$ であるという性質は保たれる場合も多い。

p = 2 の場合、標準終結多項式は

$$g(x) = x^8-x^6-3\sqrt{2}/2\cdot x^5-7/2\cdot x^4-3\sqrt{2}/2\cdot x^3-x^2+1$$

であり、その根は

$$-0.9715836924\pm0.2366962794i,\ -0.3164847297\pm0.9485976048i,$$
$$0.08443506237\pm0.9964289840i,\ 0.5337578006,\ 1.873508919$$

である。2 個の実根の絶対値は 1 と異なるが、他の複素根の絶対値は 1 である。しかし、これは近似値によるものでやはり代数的な証明が必要であるが、g(x)の係数が対称、

$$g(x) = x^8g(1/x)$$

つまり、根の逆数を根にもつ方程式が自分自身と一致することは必要である。しかし、十分とはいえない。

実部の 2 倍、つまり、標準係数方程式(= 余弦変換)は

$$x^8-x^6-3\sqrt{2}/2\cdot x^5-7/2\cdot x^4-3\sqrt{2}/2\cdot x^3-x^2+1 \ \textcircled{x}\ x^2+yx+1$$
$$= (y^4-5y^2+3\sqrt{2}/2\cdot y+1/2)^2$$

の平方根の

$$y^4-5y^2+3\sqrt{2}/2\cdot y+1/2$$

であり、この根

$$-2.407266720,\ -0.1688701247,\ 0.6329694595,\ 1.943167385$$

はすべて実数であるが[-2,2]に属さない -2.407266720 がある。

p = 5 の場合、基礎データは

$$[p, a_p, b_p, c_p, d_p] = [5, -1, 0, 0, 0]$$

だから、

$$1+a_p = 1+a_p+b_p = 1+a_p+b_p+c_p = 1+a_p+b_p+c_p+d_p = 0$$

であり、標準終結多項式は

$$x^8+1 = 0$$

で、標準終結根は 1 の原始 16 乗根の全体で、絶対値はすべて 1 の複素数である。

p = 89 の場合、標準終結多項式は

$$g(x) = x^8-\sqrt{89}/89\cdot x^7+39/89\cdot x^6-1175\sqrt{89}/7921\cdot x^5+4607/7921\cdot x^4$$
$$-1175\sqrt{89}/7921\cdot x^3+39/89\cdot x^2-\sqrt{89}/89\cdot x+1$$

であり、解は

$$-0.6671554507\pm0.8741888463i,\ -0.5516861428\pm0.7228868058i,$$
$$0.2869392118\pm0.9579487923i,\ 0.9849022757\pm0.1731112572i$$

であり、それらの絶対値は、順に

$$1.099682924,\ 0.9093530305,\ 1,\ 1$$

だから、標準終結根のうち 4 個の絶対値は 1 ではない。

他の除外素数 p = 87623, 414739 については、現在の実験的手法ではとても処理できる大きさではないから、将来の数学の発展に待つしかないが興味のある問題です。

標準終結多項式を

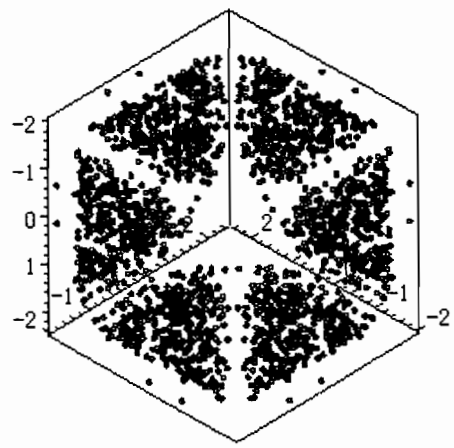
$$x^8+ax^7+bx^6+cx^5+dx^4+cx^3+bx^2+ax+1$$

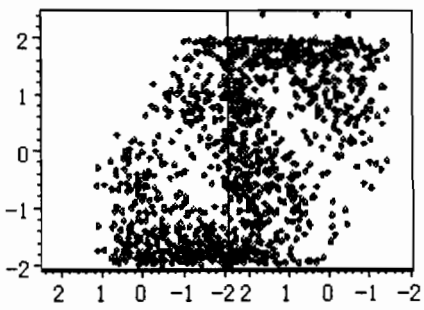
とすると、標準係数多項式は

$$x^8+ax^7+bx^6+cx^5+dx^4+cx^3+bx^2+ax+1 \ ⓧ\ \sqrt{x^2+yx+1}$$
$$= y^4-ay^3+(b-4)y^2+(3a-c)y+d-2b+2$$

です。次の図は異なる 3 個の標準係数根を座標にもつ点を xyz-空間に表示したものの例です。

$$E:\ y^2 = x^{10}+60x^6-208x^5+850x^2-8000x-4672,\ gal = 10T_8 = 5^2\cdot 8$$
$$y^4-ay^3+(b-4)y^2+(3a-c)y+d-2b+2 = 0$$
$$p = 2 \sim 557$$





これらの点のある方向への射影が S 字状の分布をするという性質はここでも見られます。

係数多項式のガロア群は p = 5 の $4T_1 = C(4)$ を除いて、p = 89 も含め、少なくとも p = 557 までは $4T_4 = S(4)$ ですから、一般に $4T_4 = S(4)$ と予想されます。勿論、p = 87623, 414739 については未知です。

2.2 種数 3 の場合の例

$$E: y^2 = x^8+2x^6-5x^4+2x^2+1 = f(x)$$

$$gal = 8T_9 = E(8):2 = D(4)[x]2$$

$$\det(f(x)) = 2^{28}\cdot 7^2$$

この場合はガロア群は非常に高い対称性をもった場合で、終結根の角分布が、一般の種数 3 の超楕円曲線の

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

と異なり、虚数乗法をもたない楕円曲線の場合と同じ

$$\sin^2(x)$$

に比例すると予想される場合です。

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

[2, -2, -3, -6],[3, 3, 9, 11],[5, 1, 13, 5],[7, -1, 6, -6],[11, 3, 29, 55],
[13, 1, 5, -51],[17, -7, 53, -227],[19, 3, 41, 107],[23, -9, 77, -437],
[29, 13, 101, 577],[31, 7, 101, 387],[37, -11, 117, -807],[41, -7, 29, 85],
[43, -13, 173, -1193],[47, 7, 85, 659],[53, -19, 221, -1943],[59, -5, 121, -589],
[61, 9, 109, 461],[67, 11, 221, 1375],[71, -1, 213, -213],[73, 9, 221, 1157],

[79, 7, 101, 1155],[83, 3, 233, 427],[89, -23, 301, -3115],[97, -7, 101, -1619],
[101, 1, 301, 101],[103, 7, 317, 1323],…

少し大きい方では

[2003, 91, 8029, 360431],[2011, 115, 8957, 457479],[2017, -7, 1781, 47101],
[2027, 67, 5725, 269879],[2029, 89, 4973, 267997],[2039, -41, 6157, -169237],
[2053, -35, 5021, -105831],[2063, -49, 6813, -204813],
[2069, 133, 11893, 623465],[2081, -135, 11061, -603075],
[2083, -101, 8525, -425025],[2087, -33, 6293, -139829],
[2089, -23, 29, -79323],[2099, -29, 6265, -123781],[2111, -25, 5205, -106509],
[2113, -23, 1637, 25533],[2129, 41, 5141, 126733],[2131, 51, 6761, 214811],
[2137, -31, 917, 97093],[2141, 169, 14189, 776941],[2143, -89, 8309, -385389],
[2153, -183, 17549, -1016843],[2161, 41, 6053, 152989],
[2179, 59, 4013, 257407],[2203, 11, 5033, 47827]

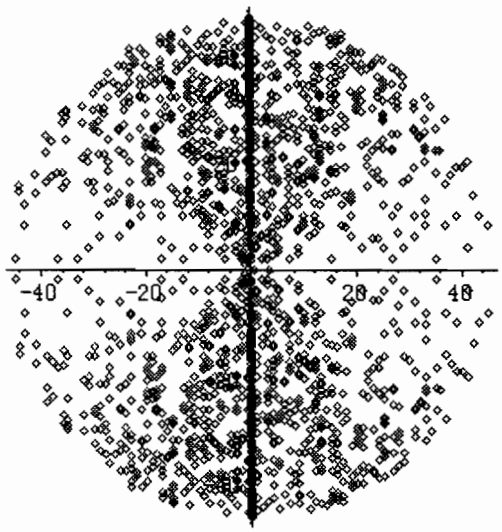
などです。終結根の角分布の様子を記しておきましょう：

$$E: y^2 = x^8+2x^6-5x^4+2x^2+1 = f(x)$$

$$gal = 8T_9 = E(8):2 = D(4)[x]2$$

$$\det(f(x)) = 2^{28}\cdot 7^2$$

$$p = 2 \sim 2203$$

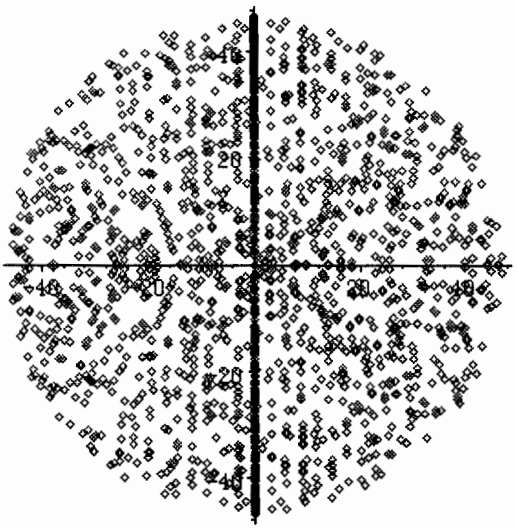


これは、興味深いことに、虚数軸に 1/2、残り半分が $\sin^2(x)$ の分布に従うと予想されます。このような現象は、種数 2 でも起こり得るのでしょうか、これも興味ある問題です。

以下の図は、終結解の(絶対値を保った)3 倍角の点の分布です。純虚数の部分を除くと一様分布のような印象ですが、実軸から 45° までの範囲と残りの部分には規則性の微妙な変化があるような印象です。

$$E: y^2 = x^8+2x^6-5x^4+2x^2+1 = f(x)$$

$$p = 2 \sim 2203$$



これは、p と終結係数

$$a = 1+a_p,\ b = 1+a_p+b_p,\ c = 1+a_p+b_p+c_p$$

から、3 倍角の公式を用いて得られる 6 次方程式

$$x^6p^3+(3p^2c+a^3p^2-3p^2ab)x^5+(3pc^2+3bp^2a^2-3a^2p^3-3cpab+b^3p+3p^4-3p^2b^2)x^4$$
$$+(c^3-3cpb^2+6p^3c-6p^3ab+6ap^2b^2-3cp^2a^2)x^3+(p^2b^3-3cp^2ba+3a^2p^3b+3p^5-3p^3b^2-3p^4a^2+3p^2c^2)x^2$$
$$+(a^3p^4-3p^4ba+3p^4c)x+p^6 = 0$$

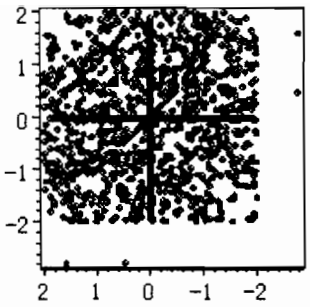
の根として求められます。角度の分布は虚数軸の点分布と一様分布の和であろうと思われます。これも一つの面白い問題でしょう。

次の図は、標準係数方程式の解を座標にもつ xyz-空間の像を平面に射影してものです。

$$E: y^2 = x^8+2x^6-5x^4+2x^2+1 = f(x)$$

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

$$p = 2 \sim 2203$$

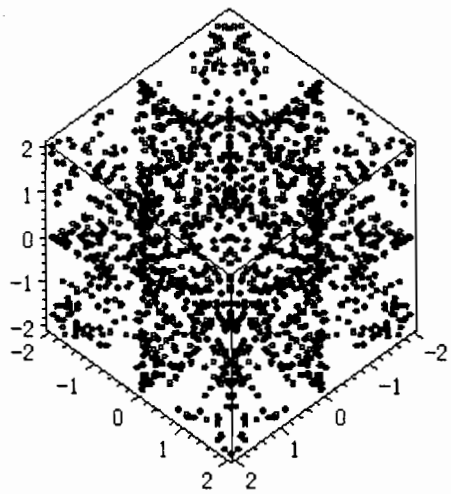


3 倍角の標準係数根の場合は次のようです。異なる方向からの射影です。

$$E: y^2 = x^8+2x^6-5x^4+2x^2+1 = f(x)$$

$$x^3-(a^3+3c-3ba)x^2-(3a^2-3c^2-3ba^2+3b^2-b^3+3abc)x-6b^2a+3ca^2-c^3+3b^2c+2a^3 = 0$$

$$p = 2 \sim 2203$$



例えば、まだ全体像は解りませんが、種数 2 の場合でも整数の二つの助変数 y,z をもつ x の 5 次多項式の族

$$k(x,y,z) = zx^5+(z^2-z-1)x^3-(z-3)x^2+(z-3)x+1+yx^2(x-1)^2$$

に対して

$$E: y^2 = k(x,y,z)$$

終結根の角分布は $\sin^2(x)$ に比例するであろうと予想されています。

$$\det(k(x,y,z)) = k(x,y,z) \textcircled{x} k_x(x,y,z)$$

$$= z^3(4z^5-4z^4+(-24y-40)z^3+(-y^2+34y+91)z^2+(30y^2+14y-4)z+4y^3-y^2)^2$$

であり、平方の中身は

$$4z^5-4z^4+(-24y-40)z^3+(-y^2+34y+91)z^2+(30y^2+14y-4)z+4y^3-y^2$$

$$= 4y^3+(-z^2+30z-1)y^2+(-24z^2+34z+14)zy+(4z^4-4z^3-40z^2+91z-4)z$$

のように、z の 5 次式、y の 3 次式である。また、

$$h(y,z) = 4z^5-4z^4+(-24y-40)z^3+(-y^2+34y+91)z^2+(30y^2+14y-4)z+4y^3-y^2$$

の判別式については

$$\det_z(h(y,z)) = h(y,z) \textcircled{z} h_z(y,z) = -1024(27y^3+55y^2+72y+67)(y^2-35y+25)^5$$

$$\det_y(h(y,z)) = h(y,z) \textcircled{z} h_y(y,z) = -64z(z^2-11z-1)^5$$

など、正 12 面体群を想像させる代数構造をもっているのである。

$$\det(27x^3+55x^2+72x+67) = 3^3 \cdot 31^5,$$

$$\det(x^2-35x+25) = -3^2 \cdot 5^3, \det(x^2-11x-1) = -5^3$$

これに関しての基本的問題の一つは、超楕円曲線

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

の終結根の角分布が $\sin^2(x)$ になる多項式の決定でしょう。例えば、5 次多項式の、上記 2 助変数 y,z をもつ x の 5 次多項式の族 k(x,y,z) と本質的に異なる族は存在するか、あるいは 3 助変数の族が存在するか。また、基本的な問題ですが

予想(問題)

任意の自然数 $n \geq 3$ に対して、超楕円曲線

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

の終結根の角分布が $\sin^2(x)$ になる多項式 f(x) が存在する。

3. 種数 5 の超楕円曲線

種数 5 の超楕円曲線は、11 次または 12 次の多項式 f(x) によって

$$E: \quad y^2 = f(x)$$

の形の式で定義されます。

例えば、f(x) が 11 次多項式の場合ガロア群の構造によって大まかに分類するとしても

$$8T_8 = S_{11}, 8T_7 = A_{11}, 8T_6 = M_{11}, 8T_5 = L_2(11),$$

$$8T_4 = F_{110}\ ,\ 8T_3 = F_{55}\ ,\ 8T_2 = D_{11},\ 8T_1 = 11$$

の 8 種類あります。勿論、同じガロア群をもつ多項式でも終結根の角分布や標準係数多様対(normal coefficient manifold)の構造は異なることがあります。

さらに、f(x)が 12 次多項式の場合ガロア群の構造は 301 種もあります。七小町の通(かよい)小町の中将ではありませんが、99 などの 3 倍程度はあります。

3.1 種数 5 の例

$$E:\quad y^2 = x^{12}+x^{10}+x^8-x^6+x^2-1$$

$$gal = 12T_{137}\ ,\ det = -2^{24}\cdot 53^4$$

この超楕円曲線の種数は 5 で、基本データは

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

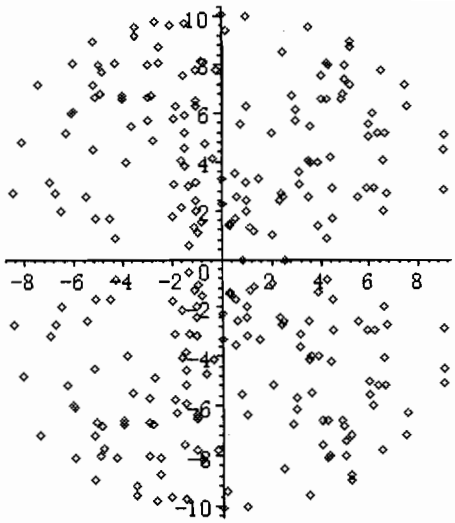
[2, -1, -1, -3, -6, -12], [3, -3, 9, -17, 43, -77], [5, -3, 15, -45, 134, -322],
[7, 5, 29, 93, 346, 794], [11, -3, 41, -119, 810, -2006],
[13, -11, 89, -475, 2233, -8483], [17, 1, 41, -123, 477, -4435],
[19, -11, 33, 87, -677, 1747], [23, -3, 13, -57, 23, 1967],
[29, -11, 57, -11, -695, 5581], [31, -1, 71, -39, 3206, -3174],
[37, -3, 17, -171, 905, 5525], [41, 5, 159, 579, 11290, 29666],
[43, -7, 109, -911, 7970, -49886], [47, -9, -45, 693, 794, -38026],
[53, 5, 45, -63, -93, 111], [59, 3, 47, 77, 3014, 19954],
[61, -11, 223, -2005, 24118, -165762], [67, -21, 275, -2223, 17978, -130882],
[71, 1, 105, -413, 12539, -9889], [73, 9, 135, 719, 14902, 89046],
[79, 1, 81, 1171, 9339, 71015], [83, 5, 257, 871, 35675, 99427],
[89, -3, 55, -493, 4186, -57582], [97, 1, 329, -859, 45949, -189395],
[101, -27, 471, -6845, 82454, -838402], [103, -19, 493, -6281, 99095, -943073],

です。終結根の分布は

$$E:\quad y^2 = x^{12}+x^{10}+x^8-x^6+x^2-1 = f(x)$$

$$\zeta f(x) = 0$$

$$p = 2 \sim 107$$



である。この分布が、p を大きくしていった極限で種数 5 の場合の標準予想分布

$$\sin^2(x)+\sin^2(2x)+\sin^2(3x)+\sin^2(4x)+\sin^2(5x)$$

に近づくでしょうか。この段階ではかなり異なるような印象です。異なるとしたらどんな極限分布なのでしょうか。そもそも、極限となる安定した分布が存在し得るのでしょうか。今は $p = 107$ までですが、この方法では一組の係数を得るためには p^5 に比例する計算を行わねばなりません。2 倍の大きさについて計算するためには $2^5 = 32$ 倍以上の計算量が必要です。仮に 100 まで 1 日で済むとすれば 200 では 1 月、400 では 3 年近くかかります。$100000 = 10^5$ 倍の計算能力であれば 1000 程度の素数までは現実に計算できるでしょう。新しい数学上や情報処理の着想や発見が必須です。

このようなことを記したのは、時代の進歩が計算というものの質的変化をもたらす可能性があること、そして将来、例えば、2012 年には、数学の(一般個人の所有できる)処理機構もこのような段階にあったのかという記録のためです。例えば、13 インチ・フロッピーディスクなど、今でさえ過去の霞のなかです。

係数多項式

$$\eta f(x) = x^5-ax^4+(b-5p)x^3+(4pa-c)x^2+(5p^2+d-3pb)x-2p^2a-e+2pc$$

についてはどうでしょうか。勿論、この場合は偶数(12 次)だから

$$a = 1+a_p,\ b = 1+a_p+b_p,\ c = 1+a_p+b_p+c_p,\ d = 1+a_p+b_p+c_p+d_p,\ e = 1+a_p+b_p+c_p+d_p+e_p$$

としての話です。この因数分解の様子を見ましょう。

$[2, x^5-11x^3+4x^2+16x+6]$, $[3, (x+1)(x^2+x-4)(x^2-5)]$, $[5, x(x+4)(x+2)(x-2)^2]$,
$[7, (x-2)(x-4)(x+2)(x^2-2x-4)]$, $[11, x(x-2)(x+2)(x^2+2x-12)]$,
$[13, (x+5)(x+3)(x+1)(x^2+x-18)]$, $[17, (x^2+7x-6)(x-3)^3]$,
$[19, (x+7)(x^2+3x-20)(x^2-73)]$, $[23, (x+9)(x-3)(x-9)(x^2+5x-8)]$,
$[29, (x+9)(x-3)(x+7)(x^2-3x-74)]$, $[31, (x+4)(x^2-4x-8)(x^2-60)]$,
$[37, (x-3)(x+11)(x-11)(x^2+5x-34)]$, $[41, (x-2)(x+2)(x+6)(x-6)^2]$,
$[43, (x-2)(x^2+8x-44)(x^2-52)]$, $[47, (x+6)(x^2-172)(x^2+2x-128)]$,
$[53, (x-6)(x^4-214x^2+5831)]$, $[59, (x-8)(x+8)(x-14)(x^2+10x-40)]$,
$[61, (x-2)(x+12)(x-8)(x^2+8x-4)]$, $[67, (x+12)(x^2+8x-16)(x^2-160)]$,
$[71, (x-5)(x^2+3x-136)(x^2-97)]$, $[73, (x-12)(x+8)(x-6)(x^2-148)]$,
$[79, (x+5)(x^2-109)(x^2-7x-168)]$, $[83, (x-5)(x^2-x-84)(x^2-73)]$,
$[89, (x+10)(x+18)(x-10)(x^2-16x-4)]$, $[97, (x-7)(x^2+11x-62)(x-3)^2]$,
$[101, x(x+2)(x-12)(x+18)^2]$, $[103, (x+7)(x-7)(x+13)(x^2+5x-56)]$, …

p = 2 の場合は、既約多項式が記してありますが、多項式の定義自体を含め個別に計算検討して下さい。奇素数については、一次、二次の式の積に分解し、完全分解しているものについては重複因子をもっています。これは、

$$f(x) = x^{12}+x^{10}+x^8-x^6+x^2-1$$

のガロア群の対称性の反映の一部でしょう。例えば、

$$f(x) = x^{12}+x^{10}+x^8-x^6+x^2-1$$

に対し、すべての奇素数に応ずる係数多項式

$$\eta f(x) = x^5-ax^4+(b-5p)x^3+(4pa-c)x^2+(5p^2+d-3pb)x-2p^2a-e+2pc$$

は高々 2 次の因数に分解する。

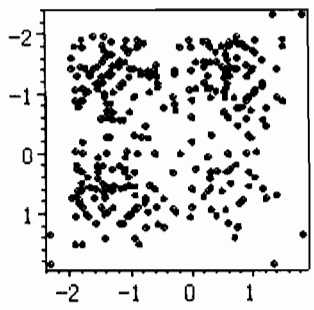
ということの証明が与えられればすばらしいことだと思います。恐らく、一例から類型へと発展させることができるでしょう。

次のものは、標準係数根の対を xy-平面に記したものです。標準係数根は[-2,2]の実数ですから、除外素数 2, 53 を除いて、正方形$[-2,2]^2$ 内の集合として表示されています。

$$E:\ y^2 = x^{12}+x^{10}+x^8-x^6+x^2-1 = f(x)$$

$$\eta f(\sqrt{p}x) = 0$$

$$p = 2 \sim 107$$



この場合もガロア群の対称性を反映して、5 次元立方体$[-2,2]^5$ のなかの退化多様体、つまり、何らかの代数関係を正の比率の素数がもつような状況が期待される。2 次元空間への射影である上図のなかに何個かの直線や曲線を読みとれることがそれを意味しています。このような退化多様体の存在条件、存在比率の決定など将来の問題でしょう。

3.2 例

$$E:\ y^2 = x^{12}-12x^{10}-8x^9+54x^8+72x^7-84x^6-216x^5-63x^4+376x^3+216x^1-480x+208$$

$$gal = 12T_{133},\ det = 2^{84}\cdot 3^{32}$$

この曲線の基本データは

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

$$[2, 0, -1, -2, -4, -8],\ [3, 2, 6, 18, 54, 162],\ [5, 3, 5, 8, 26, 80],$$

$$[7, 1, 15, 10, 96, 80],\ [11, -1, 3, -42, 118, 8],\ [13, 2, 21, -11, 78, -667],$$

$$[17, 9, 55, 159, 398, 638],\ [19, 13, 89, 419, 1599, 6451],$$

$$[23, 0, 37, 177, 410, 6911],\ [29, 11, 85, 290, 118, -2410],$$

$$[31, -10, 75, -377, 1896, -11329],\ [37, 3, 19, -21, -597, -14043],$$

$$[41, 14, 201, 1869, 15766, 104453],\ [43, 7, 87, 244, 498, -2530],$$

$$[47, -2, 67, 115, 2904, 15755],\ \cdots$$

です。先ず、データの数が少ないことが解ります。

$$f_5(u,v,w,z,t) = f(x) \otimes x^5+ux^4+vx^3+wx^2+zx+t$$

を、私的な事情によるのですが、私のパソコンでは「式が大きすぎて処理できない」との答えが返ってきます。しかし、このような事態は一般的な

現象で、次数を上げて行けば、たとえ、“京”のような大型処理装置でもすぐにこのような事態(項数の爆発)に遭遇します。 つまり、

「一般式を先に計算して、後で個別の値を代入するか

先に個別の値を代入して、後で式を計算するか」

の問題です。普通は(経験上)、メモリーが許せば一般式の計算を先行させるのが計算が早いことが多いのです。やむを得ず、後で式を計算するといった方針に従ったという事情によりますが、やはり、実際の数値のデータを見るということは(私にとって)必須の要件です。問題の本質がどのような複雑性をもつのかという感触の体感です。

このような記事の一つの意味は、計算結果などの範囲がその時代で可能であった事柄を反映していることです。それが歴史(= history, histoir、その時代に語られた物語)の意味(= 存在意義)です。

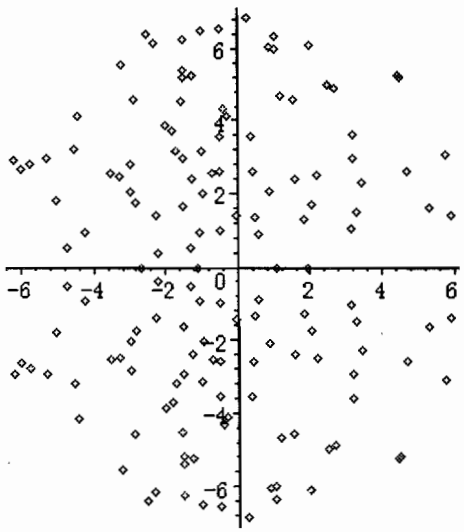
おそらく、最も基本的な複雑性(computational complexity, amount)の問題は、種数 g の超楕円曲線の終結係数(= congruence ζ-function)の計算の計算量が p^g であるかという問題でしょう。

問　題

種数 g の超楕円曲線の終結係数の計算量は p^g か？

(希望的)予想としては、p^g より小さい algorithm が存在すると考えていますが…。

現実には、一日の(私のつたない)計算量ですが、ここは絵だけです。



$$\sin^2(x)+\sin^2(2x)+\sin^2(3x)+\sin^2(4x)+\sin^2(5x)$$

の分布は夢でしょうか。

4. 冪階差(exponential difference)

冪階差とは、べき乗(power)の階差から生ずる数列のことである。例えば、n = 2 の場合は平方数の場合であるが、階差は

$$0 \quad 1 \quad 4 \quad 9$$
$$1 \quad 3 \quad 5$$
$$2 \quad 2$$

のようになり、[0,1,2]が階差(列)である。階差多項式は x(1+2x) あるいは、因子 x を除いた 1+2x という 1 次式である。

例えば、x^3 の列[0,1,8,27]を生成する階差列を考えてみよう。つまり、

$$[a,b,c,d] \rightarrow [a+b,b+c,c+d,d]$$

の初項が順次[0,1,8,27]となるような[a,b,c,d]は何かという問題である。つまり、2 項係数の行列を用いて記せば

$$\begin{pmatrix} 27 \\ 8 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 3 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} d \\ c \\ b \\ a \end{pmatrix}$$

となる行列を求める問題である。このような行列の逆行列は、この行列の checker bord 変換、つまり、(i,j)成分に i+j の偶奇に応じて符号を変えること、つまり、(-1)^(i+j)を乗じて得られることが知られている。従って、この場合だと

$$\begin{pmatrix} 6 \\ 6 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & -3 & 3 & -1 \\ 0 & 1 & -2 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 27 \\ 8 \\ 1 \\ 0 \end{pmatrix}$$

などとして得られる。勿論、これは、直接的な考察からも得られる。行を反転して記せば

$$A = ([i \leq j] (-1)^{i+j} j!/(i!(j-i)!))$$

の形の行列である。このような状況を 5 次式まで記せば、次のようである。従って、多項式の階差成分は右から係数の列ベクトルを乗ずればよいことが解る。

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 120 \\ 0 & 0 & 0 & 0 & 24 & 240 \\ 0 & 0 & 0 & 6 & 36 & 150 \\ 0 & 0 & 2 & 6 & 14 & 30 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -5 & 10 & -10 & 5 & -1 \\ 0 & 1 & -4 & 6 & -4 & 1 \\ 0 & 0 & 1 & -3 & 3 & -1 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 5 & 25 & 125 & 625 & 3125 \\ 1 & 4 & 16 & 64 & 256 & 1024 \\ 1 & 3 & 9 & 27 & 81 & 243 \\ 1 & 2 & 4 & 8 & 16 & 32 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

勿論、左辺はn次の冪階差列であり、右辺の行列は冪の行列である。要は上半2項係数行列が冪階差(exponential difference)の変換行列であるという一点につきる。これは、簡単なことであるが重要な点である。このような、冪階差(変換)行列の固有多項式は常に

$$(x-1)^n$$

であり、最小多項式でもある。最も大切な点は、n次多項式はその表現の複雑さと関係なくn個の(同時計算可能な)加法で順次計算が可能なことである。つまり、単位加法時間(unit addition time)で処理することができる。

以下の表は13次までのx^nの階差列である。

[1], [0, 1], [0, 1, 2], [0, 1, 6, 6], [0, 1, 14, 36, 24], [0, 1, 30, 150, 240, 120],
[0, 1, 62, 540, 1560, 1800, 720], [0, 1, 126, 1806, 8400, 16800, 15120, 5040],
[0, 1, 254, 5796, 40824, 126000, 191520, 141120, 40320],
[0, 1, 510, 18150, 186480, 834120, 1905120, 2328480, 1451520, 362880],
[0, 1, 1022, 55980, 818520, 5103000, 16435440,
29635200, 30240000, 16329600, 3628800],
[0, 1, 2046, 171006, 3498000, 29607600, 129230640,
322494480, 479001600, 419126400, 199584000, 39916800],
[0, 1, 4094, 519156, 14676024, 165528000, 953029440, 3162075840,
6411968640, 8083152000, 6187104000, 2634508800, 479001600,],
[0, 1, 8190, 1569750, 60780720, 901020120, 6711344640, 28805736960,
76592355840, 130456085760, 142702560000,
97037740800, 37362124800, 6227020800]

以下の表はxを除いた階差多項式の表である。

0, 1, $x+2$, x^2+6x+6, $x^3+14x^2+36x+24$, $x^4+30x^3+150x^2+240x+120$,
$x^5+62x^4+540x^3+1560x^2+1800x+720$, $x^6+126x^5+1806x^4+8400x^3+16800x^2+15120x+5040$,
$x^7+254x^6+5796x^5+40824x^4+126000x^3+191520x^2+141120x+40320$,

$x^8+510x^7+18150x^6+186480x^5+834120x^4+1905120x^3+2328480x^2+1451520x+362880,$

$x^9+1022x^8+55980x^7+818520x^6+5103000x^5+16435440x^4$

$+29635200x^3+30240000x^2+16329600x+3628800,$

$x^{10}+2046x^9+171006x^8+3498000x^7+29607600x^6+129230640x^5+322494480x^4$

$+479001600x^3+419126400x^2+199584000x+39916800,$

$x^{11}+4094x^{10}+519156x^9+14676024x^8+165528000x^7+953029440x^6+3162075840x^5$

$+6411968640x^4+8083152000x^3+6187104000x^2+2634508800x+479001600,$

$x^{12}+8190x^{11}+1569750x^{10}+60780720x^9+901020120x^8+6711344640x^7$

$+28805736960x^6+76592355840x^5+130456085760x^4+142702560000x^3$

$+97037740800x^2+37362124800x+6227020800$

興味深いことに、偶数べきに対応する奇数次の多項式は x+2 と既約因子の積であり、偶数次の多項式は既約多項式であろうと思う。

$0, 1, x+2, x^2+6x+6, (x+2)(x^2+12x+12), x^4+30x^3+150x^2+240x+120,$

$(x+2)(x^4+60x^3+420x^2+720x+360),$

$x^6+126x^5+1806x^4+8400x^3+16800x^2+15120x+5040,$

$(x+2)(x^6+252x^5+5292x^4+30240x^3+65520x^2+60480x+20160),$

$x^8+510x^7+18150x^6+186480x^5+834120x^4+1905120x^3+2328480x^2+1451520x+362880,$

$(x+2)(x^8+1020x^7+53940x^6+710640x^5+3681720x^4$

$+9072000x^3+11491200x^2+7257600x+1814400),$

$x^{10}+2046x^9+171006x^8+3498000x^7+29607600x^6+129230640x^5+322494480x^4$

$+479001600x^3+419126400x^2+199584000x+39916800,$

$(x+2)(x^{10}+4092x^9+510972x^8+13654080x^7+138219840x^6+676589760x^5$

$+1808896320x^4+2794176000x^3+2494800000x^2+1197504000x+239500800),$

$x^{12}+8190x^{11}+1569750x^{10}+60780720x^9+901020120x^8+6711344640x^7$

$+28805736960x^6+76592355840x^5+130456085760x^4+142702560000x^3$

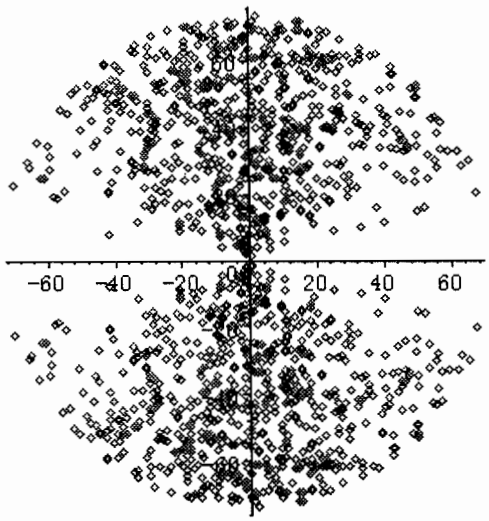
$+97037740800x^2+37362124800x+6227020800$

これらの多項式から生ずる超楕円曲線の終結変換多項式とその根の偏角について検討する。

以下、3 ~ 12 次の場合について順次記す。

$y^2 = x^3+14x^2+36x+24 = (x+2)(x^2+12x+12)$

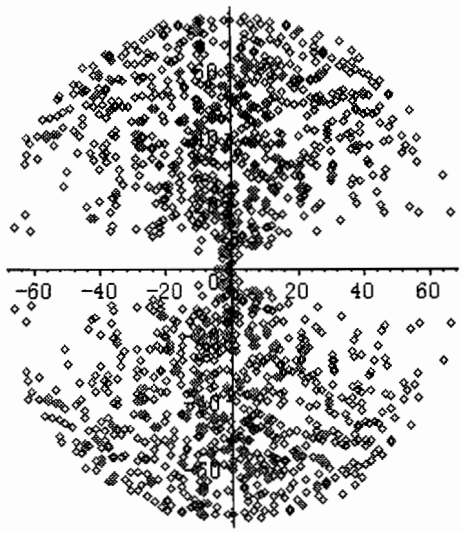
$p = 2 \sim 5313$



この角分布は R. Taylor の定理のように $\sin^2 x$ に比例する。

$$y^2 = x^4+30x^3+150x^2+240x+120$$

$$p = 2 \sim 5659$$



この角分布も、勿論、$\sin^2 x$ に比例する。

次の場合は、種数 2 の超楕円曲線である。

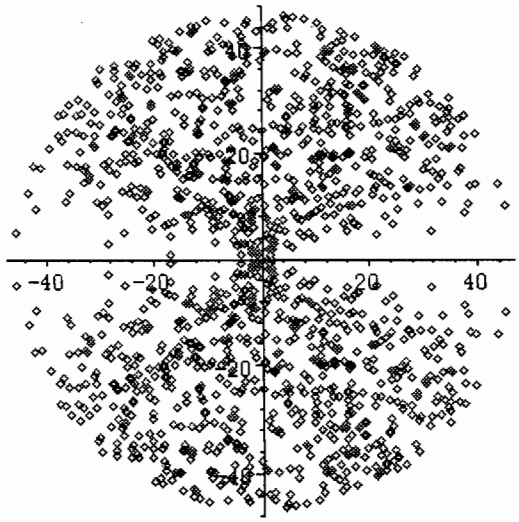
$$y^2 = x^5+62x^4+540x^3+1560x^2+1800x+720 = (x+2)(x^4+60x^3+420x^2+720x+360)$$

$$\det = 2^{20}\cdot 3^8\cdot 5^3\cdot 17^3$$

equivalent to

$$f(x-2) = x(x^4+52x^3+84x^2-272x+136)$$

$$p = 2 \sim 2179$$



この分布型は、標準型の

$$\sin^2 x+\sin^2 2x$$

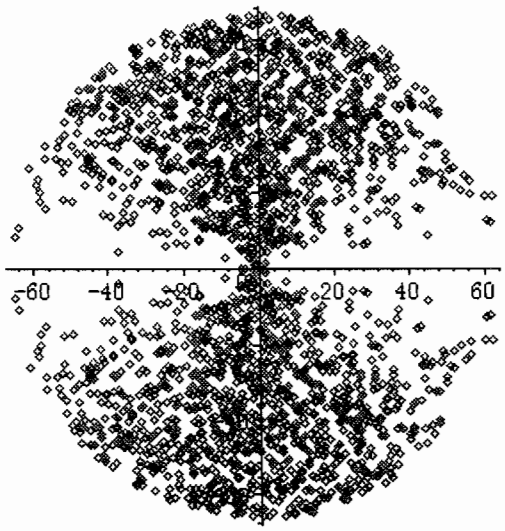
であろうと予想される。

$$y^2 = x^6+126x^5+1806x^4+8400x^3+16800x^2+15120x+5040$$

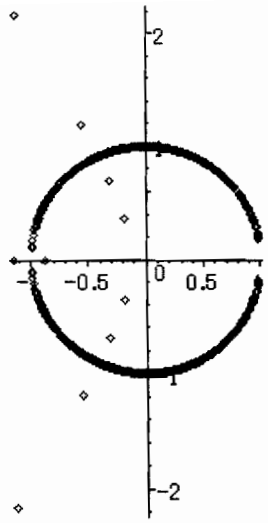
gal = 6T11= 2 wr S(3)=[2^3]S(3)=2S_4(6),

-, 48, {(1 6 4 2 5 3), (1 5) (2 6) (3 4)}

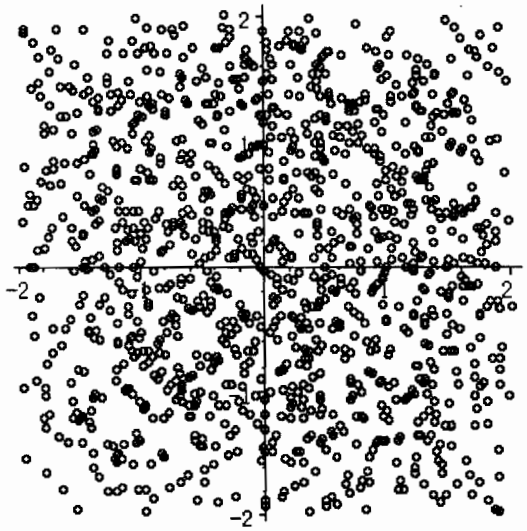
p = 2 ~ 4421



標準終結変換根の分布は次のようである。単位円周上に存在しないものは判別式の約数となる一部の素数の場合である。



以下の図は、標準係数多項式の解を座標にもつ xy-平面グラフである。図形は直線 y = x に関して対称である。



この場合の角分布は $\sin^2 x$ であるのも不思議である。係数多項式も一次因子に分解している。Legendre polynomial の場合もこのような現象がおこった。これには理由があるのだろうか。印象としては、次数 6 の種数 2 の曲線の場合は $\sin^2 x$ になる場合が多いのではないかとの“無意識”の印象があるからである。(意識しているではないか…との反論がありそう)

ついでに、次の階差多項式

$$(x+2)(x^6+252x^5+5292x^4+30240x^3+65520x^2+60480x+20160)$$
$$= x^7+254x^6+5796x^5+40824x^4+126000x^3+191520x^2+141120x+40320$$

の 6 次の因子についても調べておこう。ガロア群も同型である。分布グラフなど極めて似ているのは印象的である。似ているという点では(つまらん！、こんな句は小学生向きで昔からあると思うが…)

ここがいいと、そそとほほえむ、ちちとははは

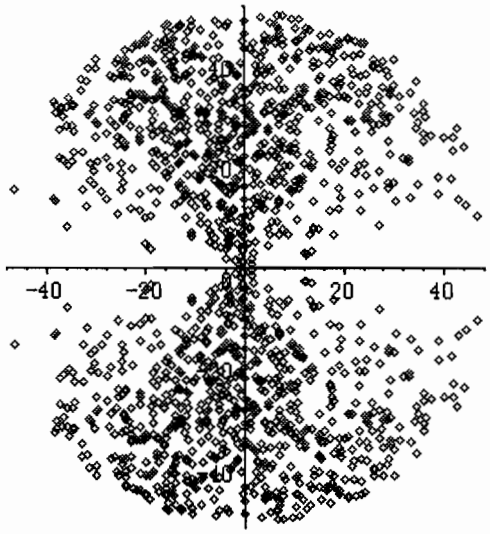
といった関係か…。

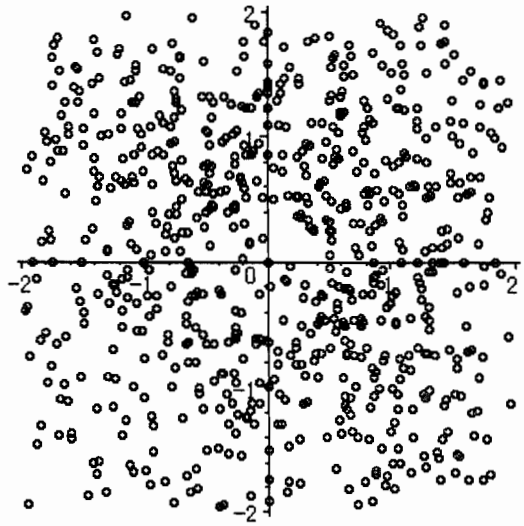
$$y^2 = x^6+252x^5+5292x^4+30240x^3+65520x^2+60480x+20160$$

gal = 6T11= 2 wr S(3)=[2^3]S(3)=2S_4(6),

-, 48, {(1 6 4 2 5 3), (1 5)(2 6)(3 4)}

p = 2 ~ 2579

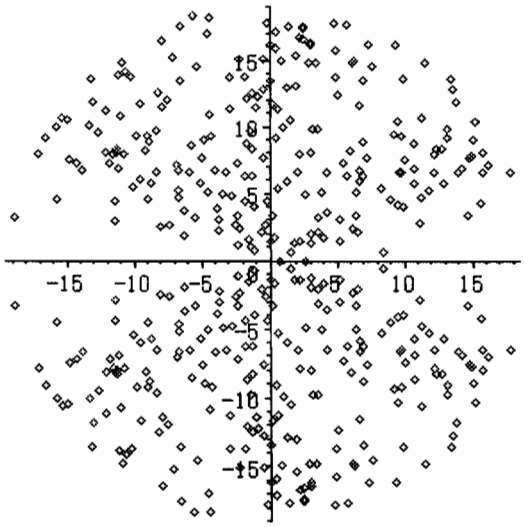


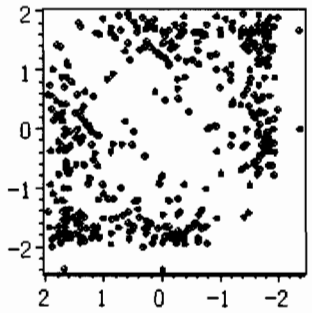


$$y^2 = (x+2)(x^6+252x^5+5292x^4+30240x^3+65520x^2+60480x+20160)$$

$= x^7+254x^6+5796x^5+40824x^4+126000x^3+191520x^2+141120x+40320$

$p = 2 \sim 367$





この分布型は、標準型の

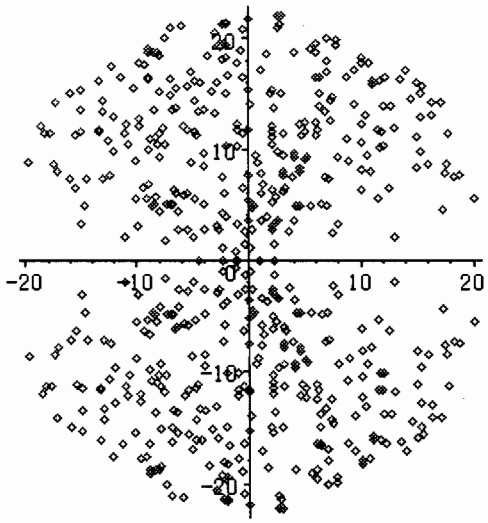
$$\sin^2 x+\sin^2 2x+\sin^2 3x$$

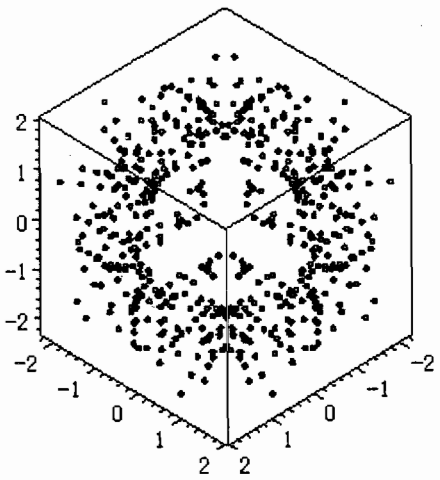
であろうと思われる。

$y^2 = x^8+510x^7+18150x^6+186480x^5+834120x^4+1905120x^3+2328480x^2+1451520x+362880$

gal = 8T44 = [2^4]S(4), -, 384, {(1 2)(3 5 7)(4 6 8), (1 6 4 7 2 5 3 8)}

$p = 2 \sim 499$





分布型は標準形の

$$\sin^2 x+\sin^2 2x+\sin^2 3x$$

であろうと思われる。何かの模様が見えるので更に計算してその正体を見たいものである。

これに関連して、次の次数の

$$(x+2)(x^8+1020x^7+53940x^6+710640x^5+3681720x^4$$
$$+9072000x^3+11491200x^2+7257600x+1814400)$$

の 8 次の因子についても“双子”のような関係にあるのか検討する。x-2 を代入して一次の因子を除くと

$$x^8+1004x^7+39772x^6+148592x^5-472760x^4-17152x^3+831232x^2-707584x+176896$$

である。x に 2x を代入して簡約化すると、

$$2x^8+1004x^7+19886x^6+37148x^5-59095x^4-1072x^3+25976x^2-11056x+1382$$

であり、monic でなくなる。

$$y^2 = x^8+1004x^7+39772x^6+148592x^5-472760x^4-17152x^3+831232x^2-707584x+176896$$

gal = 8T44 = [2^4]S(4), -, 384, {(1 2)(3 5 7)(4 6 8), (1 6 4 7 2 5 3 8)}

$$\det = 2^{61}\cdot 3^{34}\cdot 5^{14}\cdot 7^5\cdot 59^2\cdot 691\cdot 3229^2$$

であり、ガロア群も同一である。p = 691 だけが重複因子でない。これも興味深い数である。勿論、

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

$$1/2-x^2/6-x^4/90-x^6/945-x^8/9450-x^{10}/93555-691x^{12}/638512875-2x^{14}/18243225-\cdots$$

の 12 次の係数の分子である。また、

$$\cot(x) = \cos(x)/\sin(x) = \sin(x)'/\sin(x) = \log(\sin(x))'$$

という対数微分でもあります。対数微分は無限積を根の逆数の冪和(の符号を変えたもの)を係数とする級数(無限和)に変換する作用素です。同じことですが、標準一次分数式(因子)、

$$1/(x-a) = -1/a\cdot(1-x/a) = -1/a\cdot(1+x/a+x^2/a^2+x^3/a^3+\cdots)$$

の形の和(重複因子は n 倍)に表示する作用素です。Hasse の不等式を満足する係数多項式の場合などでは Laurent 級数の方、つまり、根の冪和そのものを係数とする級数の方が有用かもしれませんが…。

例えば、

$$79,\ f(x) = (x^2+2x-217)(x^3-12x^2-163x+1362)$$

は、種数 5 の超楕円曲線

$$y^2 = x^{12}+14x^{10}+65x^8+140x^6+175x^4+350x^2+175$$

の場合の係数多項式ですが、その対数微分の Laurent 級数展開(x= 1/t)は

$$5x+10x^2+908x^3+2200x^4+200052x^5+681020x^6+47988488x^7$$

$$+211381712x^8+12051491332x^9+\cdots$$

のようです。無限和と無限積の自然な対応関係は重要な研究対象です。

兎も角、$\tau = d/dx\bullet\log$ の逆作用素は $\tau^* = \exp\bullet\int dx$ です。冪和級数を無限積に戻すのは指数積分(対数微分に対応する用語としては積分指数か?…)です。

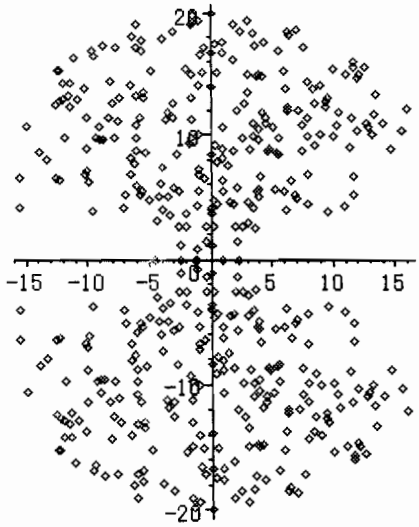
話は戻って、終結変換根(ζ-root)の角度分布型は標準形の

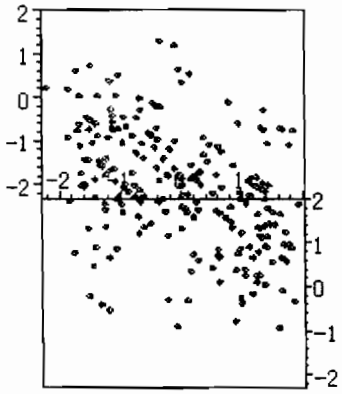
$$\sin^2x+\sin^2 2x+\sin^2 3x$$

であろうか？、この段階では、場合によっては $\sin^2 x+\sin^2 2x$ などという可能性も残っていると思う。是非継続して計算・検討を続けたいところである。

$$y^2 = x^8+1004x^7+39772x^6+148592x^5-472760x^4-17152x^3+831232x^2-707584x+176896$$

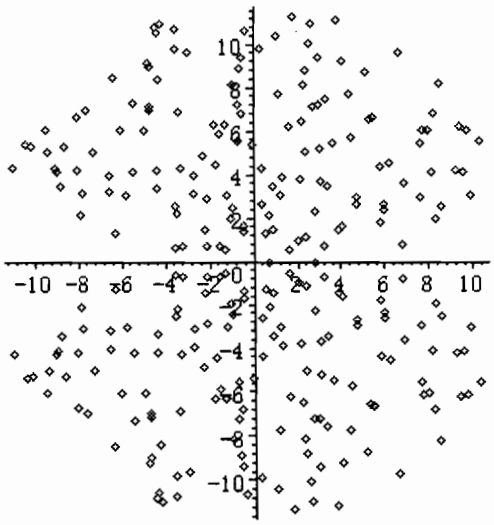
$$p = 2 \sim 401$$

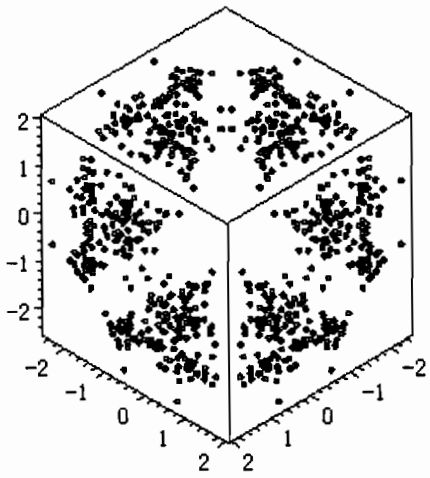




$$y^2 = x^9+1022x^8+55980x^7+818520x^6+5103000x^5+16435440x^4$$
$$+29635200x^3+30240000x^2+16329600x+3628800$$
$$= (x+2)(x^8+1020x^7+53940x^6+710640x^5+3681720x^4$$
$$+9072000x^3+11491200x^2+7257600x+1814400)$$

$$p = 2 \sim 139$$





分布型は標準形の

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

であろう。

$$y^2 = x^{10}+2046x^9+171006x^8+3498000x^7+29607600x^6+129230640x^5$$
$$+322494480x^4+479001600x^3+419126400x^2+199584000x+39916800$$

$$\det = -2^{79}\cdot 3^{36}\cdot 5^{14}\cdot 7^7\cdot 11^9\cdot 13^2\cdot 691\cdot 2177327^2\cdot 333097^2$$

ここでも、素数 p = 691 が単純因子として出現している。

また、p = 691 を法とした因数分解でも

$$(x+2)^2(x^2+654x+654)(x+439)(x+254)(x+438)(x+255)(x^2+2x+2)$$

のような謎に満ちた因数をもっている。

例えば、n = 12 のときの階差多項式

$$x^{12}+8190x^{11}+1569750x^{10}+60780720x^{9}+901020120x^{8}+6711344640x^{7}$$
$$+28805736960x^{6}+76592355840x^{5}+130456085760x^{4}+142702560000x^{3}$$
$$+97037740800x^{2}+37362124800x+6227020800$$

では、判別式は

$$\det = 2^{118}\cdot 3^{53}\cdot 5^{18}\cdot 7^{11}\cdot 11^{9}\cdot 13^{11}\cdot 43\cdot 127\cdot 271^{2}\cdot 491^{2}\cdot 1499^{2}\cdot 7045265011097^{2}$$

で、単純因子は 43·127 で、43 は類数 1 の虚 2 次体を生成し、$127 = 2^{7}-1$ は Mersenne 数です。 ついでに、12 までの階差多項式の判別式を表にまとめておきましょう。

$$0,\ 0,\ 1,\ -2^{2}\cdot 3,\ -2^{11}\cdot 3,\ 2^{11}\cdot 3^{23}\cdot 5^{3}\cdot 7^{2},\ 2^{20}\cdot 3^{8}\cdot 5^{3}\cdot 17^{3},\ -2^{24}\cdot 3^{8}\cdot 5^{3}\cdot 7^{5}\cdot 17\cdot 2381^{2},$$
$$-2^{55}\cdot 3^{14}\cdot 5^{3}\cdot 7^{5}\cdot 31^{3}\cdot 89^{2},\ 2^{55}\cdot 3^{28}\cdot 5^{7}\cdot 7^{5}\cdot 31\cdot 3381769^{2},\ 2^{77}\cdot 3^{34}\cdot 5^{14}\cdot 7^{5}\cdot 59^{2}\cdot 691^{3}\cdot 3229^{2},$$
$$-2^{79}\cdot 3^{36}\cdot 5^{14}\cdot 7^{7}\cdot 11^{9}\cdot 13^{2}\cdot 691\cdot 2177327^{2}\cdot 333097^{2},$$
$$-2^{118}\cdot 3^{53}\cdot 5^{18}\cdot 7^{5}\cdot 11^{9}\cdot 43^{5}\cdot 127^{3}\cdot 149^{2}\cdot 1237^{2}\cdot 23071^{2},$$
$$2^{118}\cdot 3^{53}\cdot 5^{18}\cdot 7^{11}\cdot 11^{9}\cdot 13^{11}\cdot 43\cdot 127\cdot 271^{2}\cdot 491^{2}\cdot 1499^{2}\cdot 7045265011097^{2}$$

これらの数字は、例の双子のような多項式の対を思い起こさせます。ここでは、p = 17, 31, 127, 691 など表情豊かな素数が登場しています。

兎も角、一番大切なことは、これらの計算には、原則として、「加法」(addition)のみが用いられていると云う点です。

例えば、素数 p での平方剰余(= Legendre symbol)の表は

$$[0, -1, -1, \cdots, -1]$$

のような、長さ p の列を、平方数を生成する階差数列

$$[0, 1, 2]$$

から、例えば、p = 7 では、順次加えた、

$$[0, 1, 2]\rightarrow[1, 3, 2]\rightarrow[4, 5, 2]\rightarrow[9=2, 0\ 2]$$
$$\rightarrow[2, 2, 2]\rightarrow[4, 4, 2]\rightarrow[1, 6, 2]\rightarrow[0, 1, 2]$$

のような輪の、始点を除いた場所を[a,b,c]の a 番目を 1 に変えるだけです。(現実には[p/2]回で十分)。このようにして、平方の表

$$u = [0, 1, 1, -1, 1, -1,-1]$$

ができます。

例えば、楕円曲線

$$y^{2} = ax^{3}+bx^{2}+cx+d$$

の場合、3 次の階差列[x,y,z,t]は、任意の 3 次多項式を生成しますから、

$$[x,y,z,t] \to [x+y,y+z,z+t,t] \mod p$$

を計算し、a = 0 から a = a+u[x] mod p のように、この列に u の x+1 番目の元 u[x]を加え合わせるだけです。a は絶対値が最小になるようにし、この操作を p 回行います。$p \geq 17$ ならば、結果は絶対値 $2\sqrt{p}$ より小という Hasse の不等式を満足します。$q = a/(2\sqrt{p})$ は[-1,1]で $\sqrt{1-q^2}$ に比例します。勿論、偏角の方では $\sin^2\theta$ に比例するというのと同値になります。これが R.Taylor 氏によって 2006 年に証明された $\sin^2$-conjecture = Sato-Tate 予想で、今では $\sin^2$-定理です。

超楕円曲線でも階差列の階層は深くなりますが事情は変わりません。例えば、

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

の場合(既約、gal = 5! = S(5)、非可解)では 1,2 段の階差は

$$[-6, 3, 12, 96, 192, 120],$$

$$[[36, -18, -72, -576, -1152, -720], [-11, 5, 82, 276, 120],$$

$$[40, -30, -60, -48], [96, -18, 36], [192, -48], [120]]$$

で、これらが遺伝子の役割をはたします。分布は標準型 $\sin^2x+\sin^2 2x$ です。

ともあれ、加法と表の参照は、数珠のような輪空間の基本性質であり、化学・生物での基本作用です。つまり、我々の身体とか環境のなかで平凡に行われている代謝などの物質の(化学)変化過程(など)に、有限体上の楕円曲線や超楕円曲線の数理が用いられている可能性があるということです。

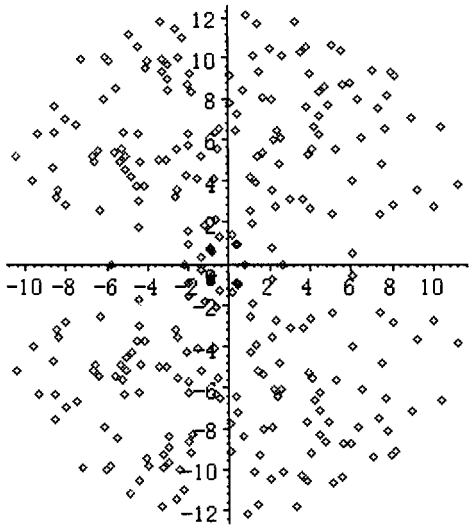
想像できることは、自・他の認識やラベリング、発生の順序などを化学物質や化学反応の順序や分岐の構造として表現し、その制御などのコーディング(coding)の場面などで用いられている、生命活動の一つの基本要素、つまり、経験・学習・記憶などの(化学的, chemical)情報処理の機構に関するものでしょう。

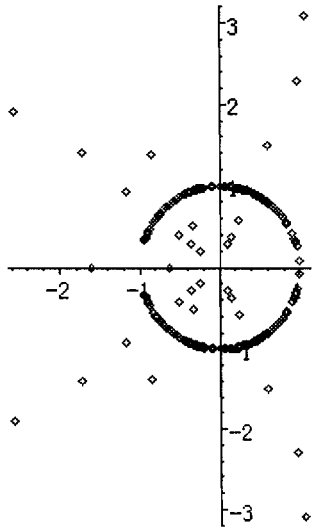
今はまだ、雑多な諸概念の素成分の混濁液ですが、いずれ、何かの簡潔な実体に凝縮したり結晶したりするでしょう。恐らく、生命の歴史や認識の始まりというものはこのような揺籃、濫觴の、永い退屈とも思えるような、時間や時代を経ているものと思います。つまり、後から見れば当然というものですが、先には無限の多様性の大気や海洋に漂うの浮遊物のたまり場です。このような視点からは、認識の時間も輪のように繋がったもの

かも知れません。

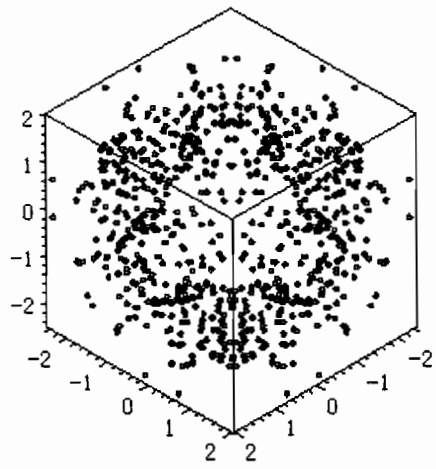
$$y^2 = x^{10}+2046x^9+171006x^8+3498000x^7+29607600x^6+129230640x^5+322494480x^4$$
$$+479001600x^3+419126400x^2+199584000x+39916800$$
$$\det = -2^{79}\cdot 3^{36}\cdot 5^{14}\cdot 7^7\cdot 11^9\cdot 13^2\cdot 691\cdot 2177327^2\cdot 333097^2$$

$p = 2 \sim 151$





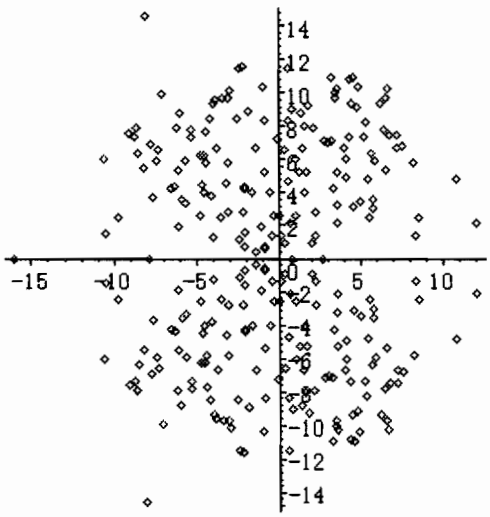
上記の Hasse 図($\alpha/\sqrt{p}$ の図)では絶対値 1 でないものがありますが、これは判別式の約数 2, 3 の場合です。

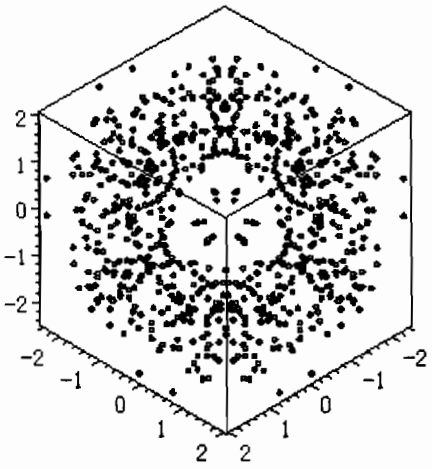


$$y^2 = x^{10}+4092x^9+510972x^8+13654080x^7+138219840x^6+676589760x^5$$
$$+1808896320x^4+2794176000x^3+2494800000x^2+1197504000x+239500800$$

$$\det = -2^{96}\cdot 3^{53}\cdot 5^{18}\cdot 7^5\cdot 11^9\cdot 43^3\cdot 127\cdot 149^2\cdot 1237^2\cdot 23071^2$$

$$p = 2 \sim 149$$

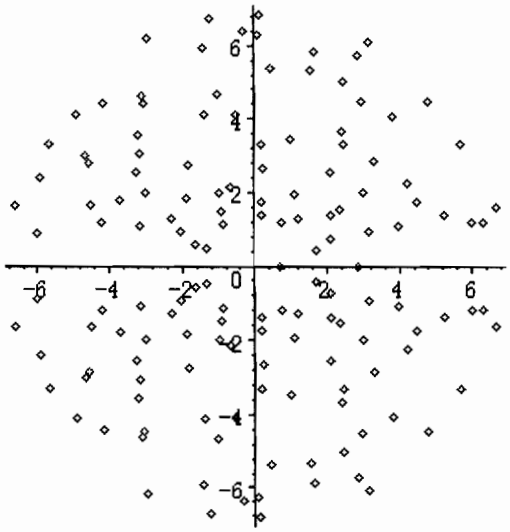


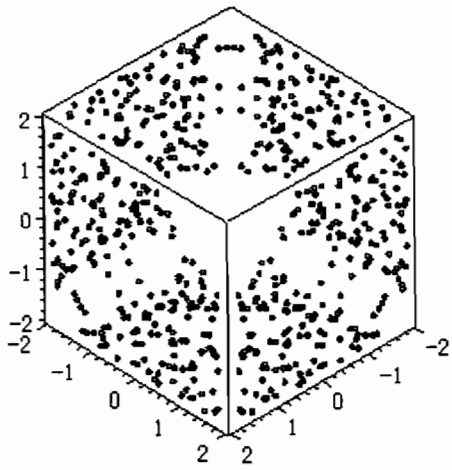


中程のグラフは Hasse のグラフで、単位円周上にない点は、判別式の約数 2,3 の場合です。

$$y^2 = x^{11}+4094x^{10}+519156x^9+14676024x^8+165528000x^7+953029440x^6+3162075840x^5$$
$$+6411968640x^4+8083152000x^3+6187104000x^2+2634508800x+479001600$$

$$p = 2 \sim 47$$





係数多項式(coefficient　polynomial,ξf(x))は次のようである。因数分解を明示してないものは既約でガロア群は(この表の範囲では)すべて 5! = S(5)である。

$[2, x^5+x^4-12x^3-4x^2+24x+8]$, $[3, x^5+x^4-15x^3-12x^2+45x+18]$,

$[5, (x-2)(x^4+x^3-20x^2-15x+50)]$, $[7, x^5+x^4-37x^3-30x^2+336x+175]$,

$[11, x^5+x^4-55x^3-44x^2+605x+242]$, $[13, (x+6)(x+2)^2(x-6)^2]$,

$[17, x^5-2x^4-91x^3+166x^2+1821x-1890]$, $[19, x^5-6x^4-74x^3+364x^2+1292x-4608]$,

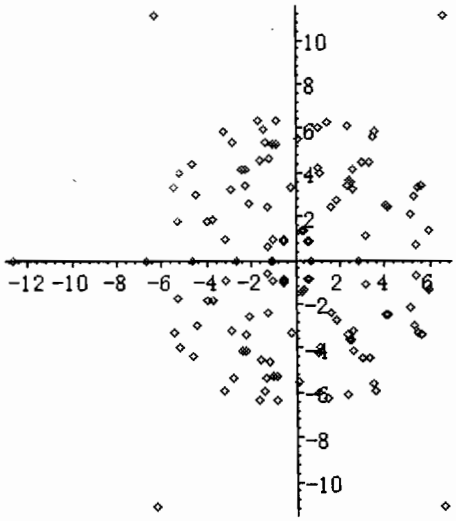
$[23, x^5-139x^3+108x^2+4701x-8796]$, $[29, x^5+2x^4-131x^3-150x^2+3437x+3118]$,

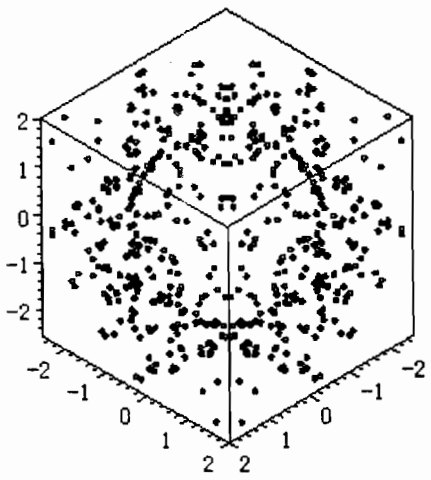
$[31, x^5-109x^3-160x^2+2636x+6784]$, $[37, x^5-8x^4-156x^3+1216x^2+1872x-11424]$,

$[41, x^5-4x^4-206x^3+700x^2+7984x-5008]$, $[43, x^5+10x^4-124x^3-1280x^2-555x-430]$,

$[47, x^5-2x^4-216x^3+448x^2+6848x-16128]$

$$y^2 = x^{12}+8190x^{11}+1569750x^{10}+60780720x^9+901020120x^8+6711344640x^7$$
$$+28805736960x^6+76592355840x^5+130456085760x^4+142702560000x^3$$
$$+97037740800x^2+37362124800x+6227020800$$
$$\det = 2^{118}\cdot 3^{53}\cdot 5^{18}\cdot 7^{11}\cdot 11^9\cdot 13^{11}\cdot 43\cdot 127\cdot 271^2\cdot 491^2\cdot 1499^2\cdot 7045265011097^2$$
$$p = 2 \sim 43$$





係数多項式は

[2, $x^5-12x^3+6x^2+18x+6$], [3, $x^5-3x^4-6x^3+9x^2+45x-135$], [5, $x^5-5x^4-25x^2+375x-2125$],

[7, $x^5-7x^4+14x^3-147x^2+1617x-12691$], [11, $x^5-x^4-55x^3+44x^2+605x-242$],

[13, $x^5-13x^4+104x^3-1521x^2+22815x-318565$], [17, $(x^2-21)(x^3-43x-86)$],

[19, $(x^2-x-29)(x^3-x^2-45x-80)$], [23, $(x^2+5x-26)(x^3+x^2-48x+96)$],

[29, $(x-2)(x+6)(x-9)(x^2+9x-18)$], [31, $(x^2+7x+2)(x^3-3x^2-108x+296)$],

[37, $(x+2)(x^2+9x-34)(x^2+5x-60)$], [41, $(x^2-8x-32)(x^3-104x+168)$]

[43, $x^5+9x^4-117x^3-1070x^2+711x+12678$]

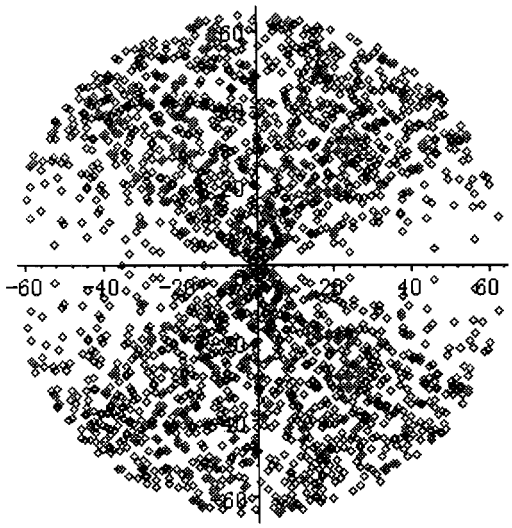
この段階では、係数多項式の素因数分解については、判別式 det の約数、p = 2,3,5,7,11,13,43 については既約でガロア群は 5! = S(5)であること、判別式

と互いに素、(p, det)= 1 な素数については可約なこと程度のことしか解っていない。例えば、上記の p = 43 に対応する超楕円曲線にいついては

$$y^2 = x^5+9x^4-117x^3-1070x^2+711x+12678$$

$$\det = 3^4 \cdot 5 \cdot 491 \cdot 1577879 \cdot 29062193$$

$$\mathrm{gal} = 5! = S(5),\ p = 2 \sim 4139$$



のように、p = 3 ~ 17, 43 など(すべては確かめていないが)、分布は標準型である。判別式の因子 491 は、もとの 12 次の冪差多項式と共通である。

恐らく、無意識には認識していて(主張の内容が強いので)、明示しては記してこなかった問題であるが…、

例えば、$\sin^2 x+\sin^2 2x$ 型の曲線について

素数分割問題

素数の全体 P を等確率の Q, R に分けて
Q 上では、$\sin^2 x$
R 上では、$\sin^2 2x$
の角分布をもつようにできるか。

といった類の問題を考えたい。あるいは、素数分割問題が肯定的なような超楕円曲線を定義する多項式は何か。勿論、これは、高い種数の曲線にもあてはまる問題でもある。

例として、当研究所、第 18 回数学史シンポジウム(2011)報告集の

種数 3 の超楕円曲線 $\sin^2$-予想

pp.179 でも取りあげた(種数は 2 ですが…)

$$y^2 = x^5-5x^3+5x-11$$

について記す。これは、5 次の Tschebycheff 多項式

$$(x^5-5x^3+4x)^2 = t^{10}-xt^5+1 \ ⓣ \ t^2-xt+1$$

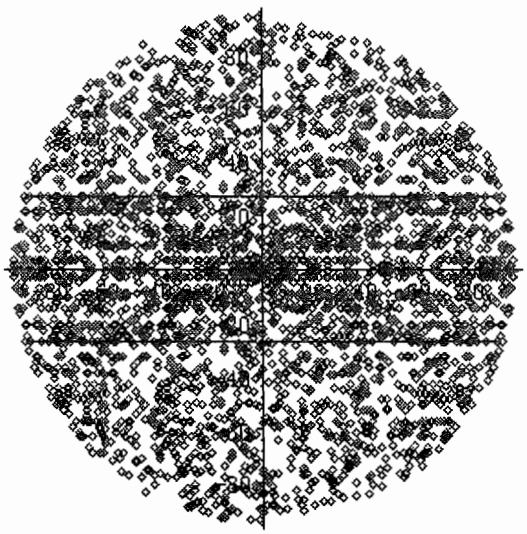
や Painlevé 方程式関連の岡本多項式 $x^6+5x^4+5x^2+5$ など思い出させる。

以下に記すものがその(現在までの計算の)データである。

$$y^2 = x^5-5x^3+5x-11 = (x-1)(x^4+x^3+6x^2+6x+11)$$

$$\det = 5^{11}$$

$$p = 2 \sim 9001$$

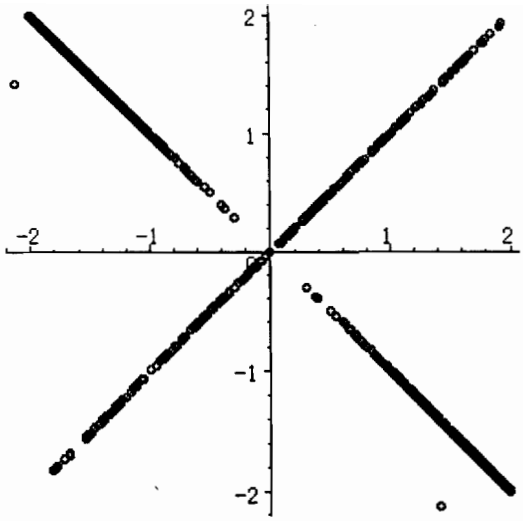


終結根の偏角の分布は、一様分布に収束するのではないかと思っているが、$y = \pm 27$ のあたりに(理由は解らないが)密度の変化の線があるのではとの感覚がある。このような帯が何故現れるのかなどは興味ある現象です。

標準係数解のグラフは、係数多項式が

$$[2, (x+3)(x-2)],[3, x^2-8],[5, x^2-10],[7, x^2-24],[11, x^2],[13, x^2-48],$$
$$[17, x^2-32],[19, (x-4)^2],[23, x^2-56],[29, (x-6)^2],[31, (x+4)^2],$$
$$[37, (x-12)(x+12)],[41, (x+6)^2],[43, x^2-72],[47, x^2-152],[53, x^2-176],$$
$$[59, (x+12)^2],[61, (x+2)^2],[67, x^2-264],[71, (x+12)^2],[73, x^2-288],$$
$$[79, (x+8)^2],[83, x^2-296],[89, (x+6)^2],[97, x^2-384],\cdots$$

のような形、つまり、x^2-a, $(x+a)^2$ のような形をしていることから、



のようである。y = x と y = -x では分布密度が明らかに異なります。具体的な分布密度も興味があります。

例えば、p = 37 では

$$(x-12)(x+12) = x^2-12^2$$

で x^2-a の a が平方の場合、p = 11 の x^2 は $(x-a)^2$ の a = 0 の場合である。

係数多項式が (x-a) (x+a) の形になる素数は p = 9001 までの範囲で

[11, 37, 131, 157, 251, 491, 599, 673, 1439, 1933, 2833,
2917, 3037, 3371, 4357, 5639, 5879, 6971, 7079, 8039, 8291]

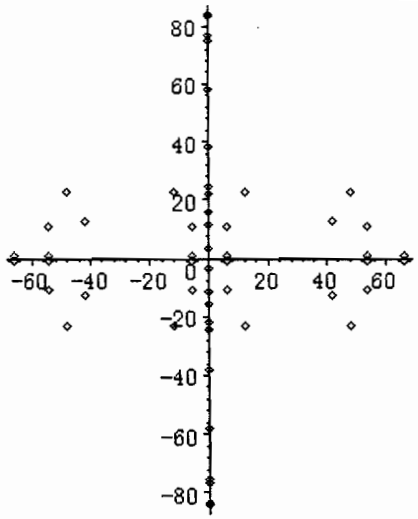
の 21 個で x^2 のものは

[11, 131, 251, 491, 599, 1439, 3371, 5639, 5879, 6971, 7079, 8039, 8291]

の 13 個です。勿論、恐らく無限に存在するのでしょう。これらの比が例特定の定数になるとか、2:1 であるとかは興味ある問題です。

しかしながら、これらの素数に対応する終結根は次の図のような分布ですので偏角の態勢に大きな変化はあたえないというのが印象です。また、存在範囲には特徴(例えば y 座標の範囲、つまり、虚数部の絶対値の上限)がありそうです。これも一つの謎です。

resultant transform roots for (x-a) (x+a)



素数の全体を、係数多項式

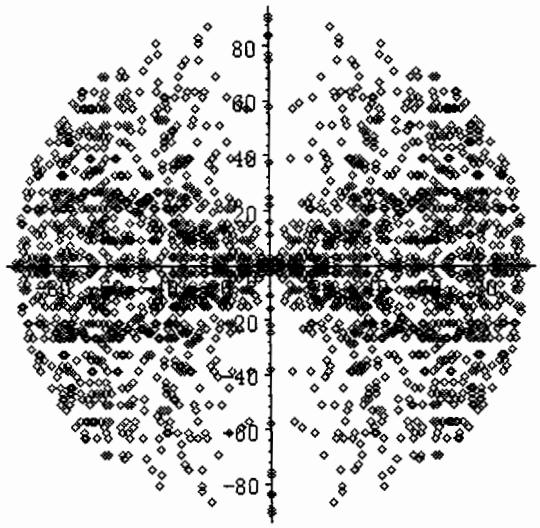
$$x^2-ax+b-2p$$

の係数によって分類することができます。

total primes	$a = 0$ (x^2-a)	$a \neq 0$ $(x-a)^2$
1108	577	531

resultant transform roots for x^2-a

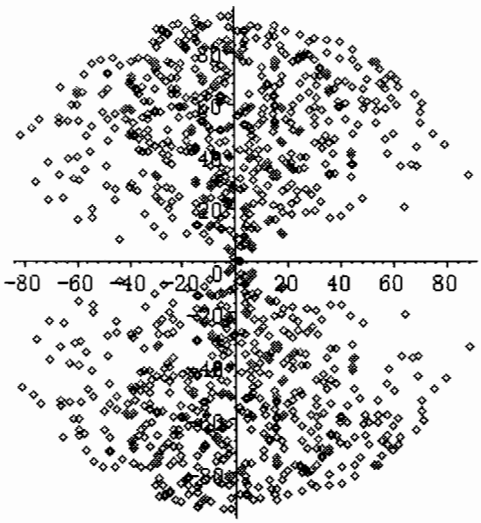
577 primes in p = 3 ~ 8893



この場合の偏角の分布は、全く新しい、$\cos^2 x$ 型であろうと思われます。

resultant transform roots for $(x-a)^2$

531 primes in p = 3 ~ 8893



後半の方の偏角分布は $\sin^2 x$ でしょう。何れにしても非常に興味ある研究対象です。このような奇妙な特徴をもつ曲線の発見と規則性の記述は、超楕円曲線の、現在は未知ですが、将来発見されるであろう一般の変形の特異点などとして現れるのではないかという観点から、個々の固有性豊かな例は、深い発見的な意味をもっていると思っています。

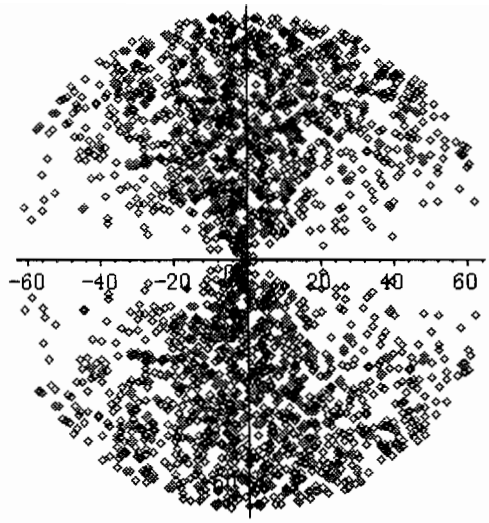
話のついでに種数 2 の岡本超楕円曲線にもふれておきます。

$$y^2 = x^6+5x^4+5x^2+5$$

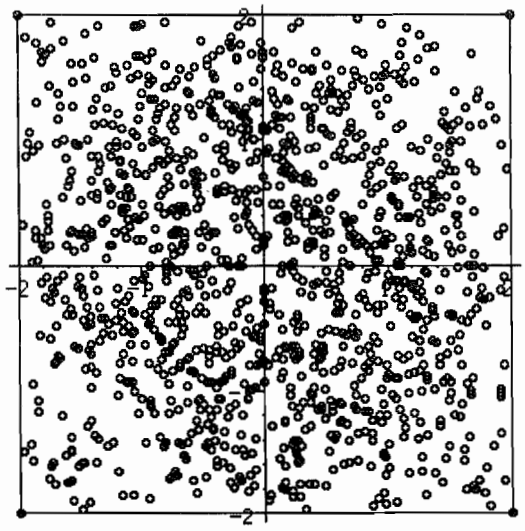
gal = 6T11 = [2^3]S(3) = 2 wr S(3) = 2S_4(6),

-, 48, {(1 5)(2 6)(3 4), (1 6 4 2 5 3)}, det = $2^{16}\cdot 5^5$

p = 2 ~ 4637



ガロア群は 6 次冪階差多項式の場合と同じです。偏角の分布も $\sin^2 x$ 型でしょう。係数多項式は常に 1 次因子に完全分解し、異なる標準係数根を座標にもつ点の分布は



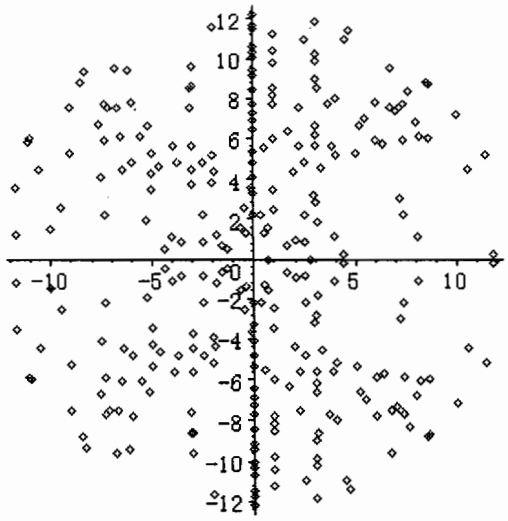
のように、標準偏角分布 $\sin^2 x+\sin^2 2x$ の一つの典型である y = x を避けるようには分布せず、中心付近にも一様に分布している。

種数 4 の例ですが、

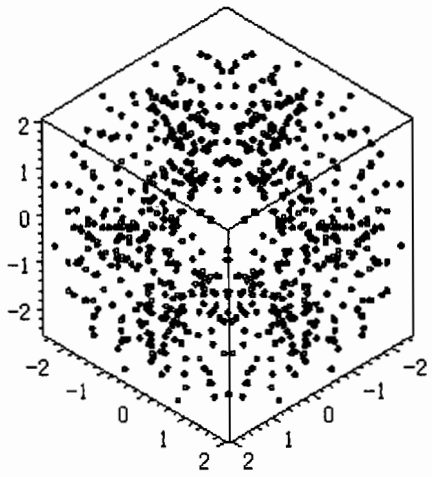
$$y^2 = x^9+24x^6-320 = (x^3+4)(x^6+20x^3-80)$$

$$\det = -2^{48}\cdot 3^{27}\cdot 5^5$$

$$p = 2 \sim 157$$



のように、虚数軸の上にも分布している特徴的なものです。標準係数解を座標にもつ点の3次元像の(ある方向への)射影像は



です。係数多項式も、判別式の約数でない場合は2次と一次式の二つの積あるいは3次と一次の積か何れかで既約なものはないようです。既約3次因子をもつ場合の素数は

$$p = 19, 31, 61, 73, 103, 109, 127, 139, 151, 157, \cdots$$

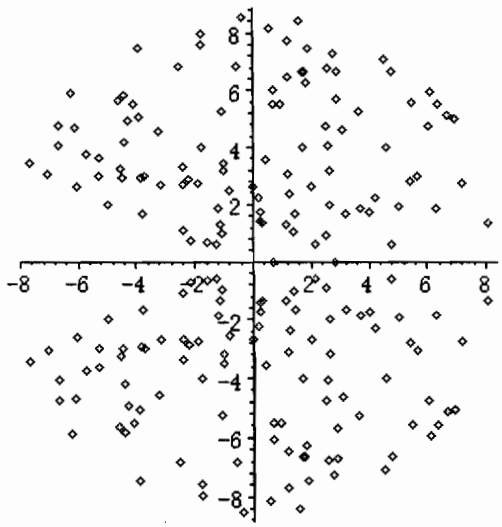
で、密度は解りませんが正の密度でしょう。

また、本論文の主題の種数5の超楕円曲線となる場合の岡本曲線

$$y^2 = x^{12}+14x^{10}+65x^8+140x^6+175x^4+350x^2+175$$

$$\det = 2^{74}\cdot 5^{20}\cdot 7^7$$

p = 2 ~ 79

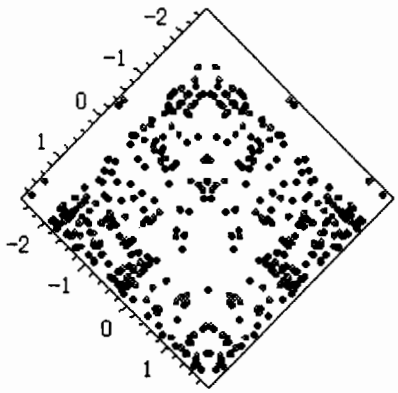


以下の図は標準係数多項式 ・

$$x^5-ax^4+(b-5)x^3+(-c+4a)x^2+(5-3b+d)x+2c-e-2a$$

の異なる 2 根を座標にもつ点のグラフです。5 個の[-2,2]の解をうまく図示できる方法があればよいのですが…

normalized coefficient roots pair, p = 2 ~ 79



図形の点分布は何かの規則性を暗示していますが、今はまだ明確な規則性は知られていない。係数多項式は、判別式の約数 2,3,7 を除いて、少なくとも 2,3 次の多項式の積に分解している。

$[2, x^5-12x^3+6x^2+18x+6]$, $[3, (x^2-5)(x^3-9x-4)]$, $[5, x^5+x^4-25x^3-20x^2+125x+50]$,

$[7, x(x^4+x^3-28x^2-21x+98)]$, $[11, (x+4)(x-2)(x^3+4x^2-16x-48)]$,
$[13, (x-2)(x^2-4x-4)(x^2+2x-28)]$, $[17, (x^3-5x^2-55x+270)(x^2-x-33)]$,
$[19, (x+8)(x^2-12)^2]$, $[23, (x^2+x-63)(x^3+7x^2-63x-372)]$,
$[29, (x-9)(x-10)(x+5)(x^2+8x-21)]$, $[31, (x^2-5x-9)(x^3-x^2-61x-104)]$,
$[37, (x^2+2x-95)(x^3-99x-134)]$, $[41, (x^2-2x-46)(x^3+8x^2-114x-868)]$,
$[43, (x^2+4x-108)(x^3-6x^2-64x-104)]$, $[47, (x^2-8x-40)(x^3-6x^2-22x+32)]$,
$[53, (x^2-4x-48)(x^3-8x^2-36x+256)]$, $[59, (x^2-2x-170)(x^3+6x^2-166x-664)]$,
$[61, (x^2+2x-20)(x^3-152x-344)]$, $[67, (x^2+6x-34)(x^3+4x^2-212x-256)]$,
$[71, (x^2-2x-206)(x^3+14x^2-54x-896)]$, $[73, (x^2+13x-11)(x^3+3x^2-153x-482)]$
$[79, (x^2+2x-217)(x^3-12x^2-163x+1362)]$

これらに関連しては、種数 g の一つの超楕円曲線から生ずる(素数に対応する)一連の係数多項式で定まる(種数[g/2]の)超楕円曲線の族に関する研究も興味ある対象です。現在はまだ博物史の段階でしょうが、いずれ、特定の族からその本質が明かされて、多様性の意味の記述ができるような時が来ることを期待している訳です。兎も角、対象物は具体的に眼前に存在し手でさわる感触を味わうことができるのです。(自分自身を)振り返ってみると、例えば、$f_i(u) = f(x) \otimes x+u$ を考えるという、一見、無駄なような定義式こそ時間の結晶だったのです。

References

[1] 野海正俊著 パンルヴェ方程式 -対称性からの入門-, 4 数学の風景、朝倉書店

[2] Kanji Namba; Hyper-elliptic curves and Hasse's inequality, 第 22 回数学史シンプジウム(2011)報告集、津田塾大学 数学・計算機科学研究所報 33, pp.137-174

[3] Kanji Namba; Hyper-elliptic curves over finite fields and their projective manifolds, 2012 年度応用数学合同研究集会報告集、龍谷大学瀬田、pp.30-36