種数2の楕円曲線と $\sin^2$-予想

難波完爾

719-1117 岡山県総社市北溝手 463-3

tel/fax. 0866-90-1886

2006.12.18

1. 楕円曲線の $\sin^2$-予想

楕円曲線の例を挙げながら、その類型について述べる。

楕円曲線(elliptic curve)

$$y^2 = x^3+ax^2+bx+c = f(x)$$

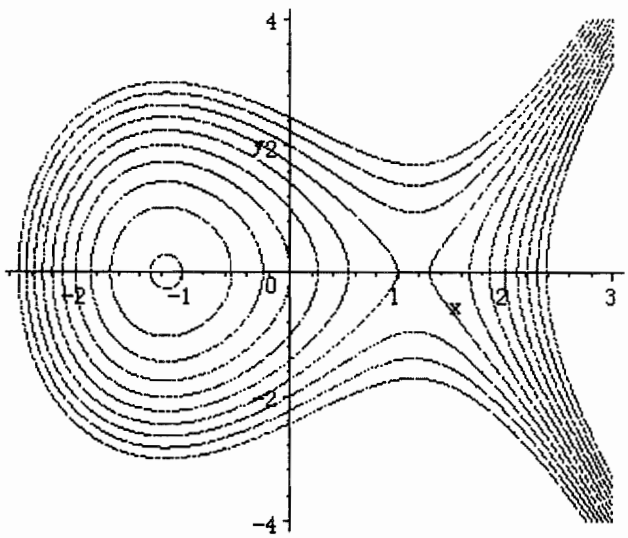
に対して、有限素体

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

上の曲線と考えて、集合

$$E_p = \{(x,y) : y^2 = f(x)\} \cup \{\infty\}$$

に群の構造が入ること(Poincaré-Mordell の群とも呼ばれる)が知られている。∞ は無限遠点で、群の単位元である。実体としては、y-軸に平行な任意の直線である。



群の位数(order)は、各 x に対して、y の2次方程式

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

の $F_p = p = \{0,1, \cdots, p-1\}$ での解の個数

$$\#\{y : y^2 = f(x)\}$$

の総和に、単位元(=無限遠点)の個数 1 を加えたものである。

つまり、f(x)が有限体で 0 でないものの平方ならば 2、0 ならば 1、平方でないならば 0 個である。通常、

$$F_p = Z/pZ = Z/(p)$$

と見なして、平方剰余・非剰余を表すルジャンドルの記号

$$(a/p) = \#\{y : y^2 = a\} - 1 = a^{(p-1)/2} \bmod p$$

によって定める。具体的な計算にあたっては、予めルジャンドルの記号の表を作っておいて参照する方法をとった。勿論、相互律や補充律を用いて計算することもできるが、今の場合は先に表を作る方が計算は易しい。

さて、ルジャンドル記号の和

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

に対して、2 次式

$$x^2 + a_p x + p$$

を考える。x = 1 の値は

$$(a/p) + 1 = \#\{y : y^2 = a\}$$

であることと、無限遠点の 1 を考慮すれば、これが群としての位数である。さて、ここでの問題は、方程式

$$x^2 + a_p x + p = 0$$

の、複素数としての解について考察することである。この方程式は実根をもたないこと、

つまり、ハーセ(Hasse)不等式

$$|a_p| < 2\sqrt{p}$$

が成立することが知られているから、任意の解 α_p の絶対値は $\sqrt{p}$ であり、

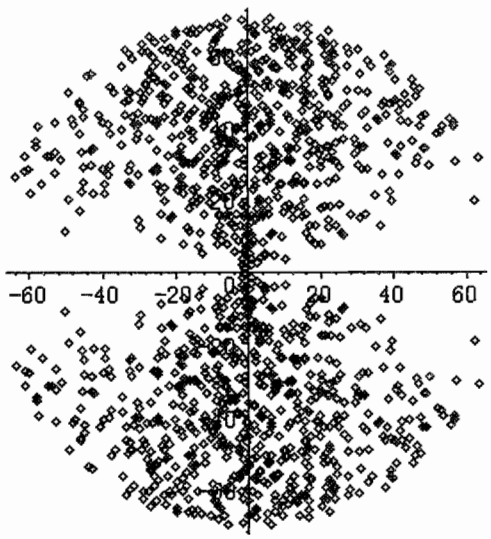
$$\alpha_p = \sqrt{p}\, e^{i\theta} = \sqrt{p}\ (\cos\theta_p + i \sin\theta_p)$$

の形に表現できる。素数 p を変化させたときの θ_p の分布はどんな(密度)関数にしたがうのであろうかと問うた訳である。

予想は、$\sin^2\theta$ の場合と、一様分布と $\theta = \pi/2 = (= 90°)$ が半々の和になっている 2 つの場合があり、後者の場合は楕円曲線が虚数乗法(complex multiplication)をもつ、ということである。

佐藤-テイトの $\sin^2$-予想は、例えば、

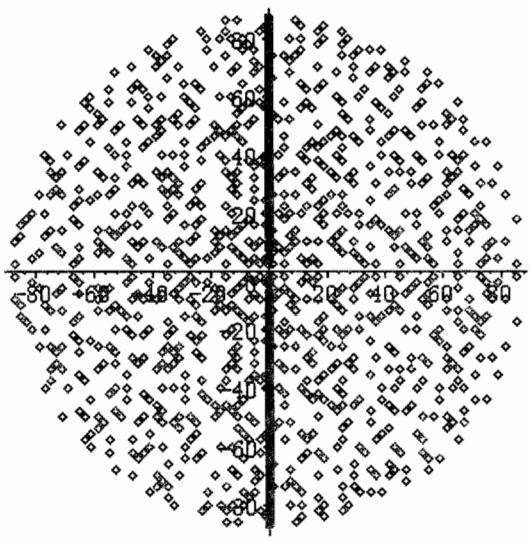
$$y^2 = x^3-x-1$$



$\sin^2\theta$

であり、例えば(虚数乗法をもつ場合で)

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



uniform + ($\theta = \pi/2$)

のように、一様分布と、点分布の和である。

最初は、デデキンドの η 関数

$$\eta(x) = x^{1/24} \prod_{n\in N} (1-x^n) = x^{1/24} \sum_{n\in Z} (-1)^n x^{n(3n+1)/2}$$

の展開を用いて、例えば、

$$E:\ y^2 = x(x^2+x-1)$$

に対応する a_p を、$k=2$ の場合であるが、$y = x^{1/2}$ として

$$\eta(x)^2\eta(5x)^2 = x^{1/2}(1+a_1x+a_2x^2+a_3x^3+\cdots) = y+b_3y^3+b_5y^5+b_7y^7+\cdots$$

$$=$$

$$1-2x-x^2+2x^3+x^4+0x^5+2x^6+2x^7-6x^8-4x^9-\cdots$$

等と計算していった訳である。昭和 38 年 3 月以前のことである。

佐藤先生が、かなりハッキリと、確信に近い感覚で、$\sin^2$ 則(昭和 38 年 5 月 13 日付の手紙)を意識しかけた時期は 4 月 8 日の少し前でしょう。

現在では、2006 年 5 月に R. Taylor によって、楕円曲線の多くの場合、「佐藤-テイト予想」は解決されています。

これは、L. Clozel, M. Harris, N. Shephard-Barron との共同研究に基づくものです。

前回の報告、

Dedekind η 関数と $\sin^2$-予想

津田塾大学　数学・計算機科学研究所報 27(2006)

第 16 回　数学史シンポジウム(2005)

16th Symposium on the History of Mathematics(2005)

pp. 95-167

に載せなかった例を 2 つばかり載せておきます：

$$k = 24/n(m+1),\ y = x^{1/k}$$

$$\eta(x)^n\eta(mx)^n = x^{1/k}(1+a_1x+a_2x^2+a_3x^3+\cdots) = y+b_{k+1}y^{k+1}+b_{2k+1}y^{2k+1}+b_{3k+1}y^{3k+1}+\cdots$$

から、計算したものです。

次の図は

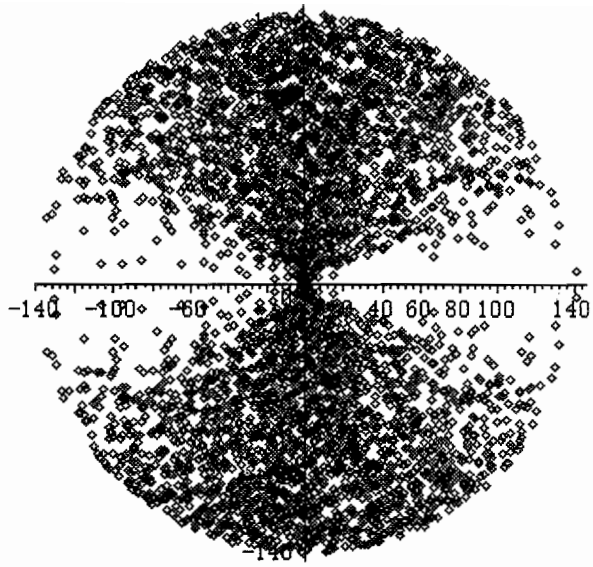
$$\eta(x)^8\eta(2x)^8,\ k = 1 = 24/(3\cdot 8),$$

$$p = 3 \sim 19997$$

の場合で、分布は、勿論

$$\sin^2\theta$$

に比例しています：

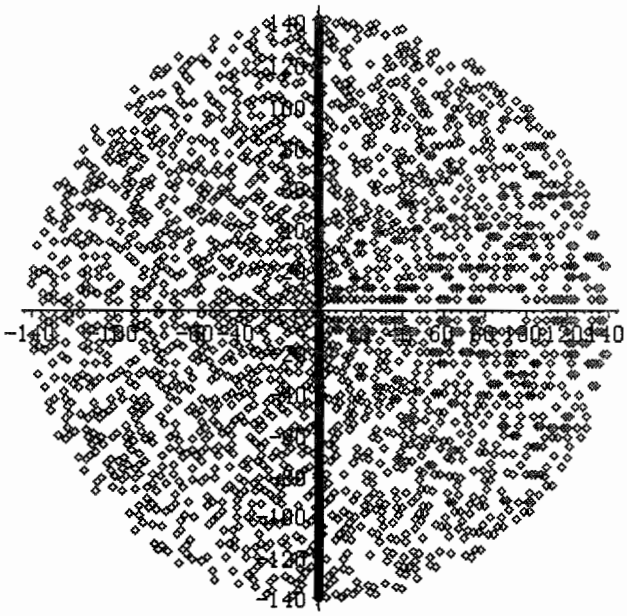


また、

$$\eta(x)^3\eta(7x)^3$$

$$k = 24/8 \cdot 3 = 1,\ p = 3 \sim 19997$$

$$\sqrt{p}x^2 - a_p x + p\sqrt{p} = 0$$



のような角度の分布をしている。解の分布も何か $y = \pm x$ を境に、実軸の正の部分の近くと、第 2･3 象限の様子は、一様分布なのだけれども神秘的な異なる様相をみせています。

実軸上の 80~100 あたりの小さい“穴”は何を意味しているのでしょうか。不思議な現象です。ここに特異点か“何か”があるのでしょう。

一般的なことであろうが、何か新しい真実が姿を現すときには、非常に強い抵抗感を伴うのが普通である。それは、誤字、誤記、脱字、忘却、消去、無意味な記号や反対の意味の記号、二つの意味をもつ記号などの(無意識での)挿入、脱力感、疲労感、眠気、無気力…等、考えられる、あるいはそれ以上のあらゆる形態をとって現れる…というのが私の経験である。

恐らく、それは、認識の座を支えている細胞や細胞のネットワークの集団としての生存をかけた行為なのであろうと思う。つまり、新しい体制が想定されることへの自然な行為なのです。別な表現をすると…何か「新しいかも知れない」ものの認知の査証なのです。

それが、意識に“のぼらない”ように、そっとして欲しいのだが…という希望と、真実という場への世界の地平線の移動の重みの確かな認識の感触なのでしょう。

2. Hasse の不等式

ルジャンドルの多項式 $P_n(x)$ は、次のような多項式である。

$$P_n(x) = 1/(2^n n!) \cdot d^n/dx^n (x^2-1)^n$$

(Rodrigues の公式)

で与えられ漸化式

$$nP_n(x) - (2n-1)xP_{n-1}(x) + (n-1)P_{n-2}(x) = 0$$

をみたす。閉区間[-1,1]での直交多項式系の一つである。母関数は

$$1/\sqrt{1-2tx+t^2} = \sum_{n\in\omega} P_n(x)t^n$$

である。

あるいは、1-2x によって、[-1,1]を[0,1]に変換して

$$P_n^*(x) = P_n(1-2x) = \sum_{r\in\omega} (nCr)(n+rCr)x^r$$

とする。

$$P_n^*(x)$$

$$P_0^*(x) = 1,\ P_1^*(x) = 1-2x,\ P_2^*(x) = 1-6x+6x^2,\ P_3^*(x) = 1-12x+30x^2-20x^3,$$

$$P_4^*(x) = 1-20x+90x^2-140x^3+70x^4,\ P_5^*(x) = 1-30x+210x^2-560x^3+630x^4-252x^5,\ \cdots$$

この場合の係数

$$k(n,r) = (nCr)(n+rCr)$$

についてであるが、

$$nCr = n(n-1)\cdots(\underline{n-r+1})/r!$$

$$n+rCr = (\underline{n+r})(n+r-1)\cdots(n+1)/r!$$

に注意すれば、r-1 から r に変化するとき

$$k(n,0) = 1$$

$$k(n,r) = k(n,r-1)(n+r)(n-r+1)/r^2$$

であることが解る。

下の図は

$$P_n^*(x) = \sum_{r\in\omega} k(n,r)\,x^r$$

の値を、素数 p について、n 次ルジャンドル多項式に対して、有限体 $F_p = GF(p) = p$ で、

$$[P_n^*(x), n]$$

の範囲 $0 \le n, x < p-1$ でのすべての組(ordered pair)を、一例として、$p = 97$ の場合に図示したものです。

$p = 97$ では、有限体 F_{97} に於いて

$$1/6 = 81 = -16,\ 1/4 = 73 = -24,\ 1/3 = 65 = -32,\ 1/2 = 49 = -48$$

であること、及び、Hasse の不等式に表れる

$$2\sqrt{p} = 2\sqrt{97} = 19.69771560\cdots$$

を参照すると、例えば、$[x, 1/6] = [x, 81]$ の $20 \le x \le 77$ の部分が明確なスリットとして除外されていることが解るでしょう。

この性質は、$p = 97$ の限ったことではない。ただし、このようなスリットとして観察できるためには、$4\sqrt{p} < p$、言い換えると

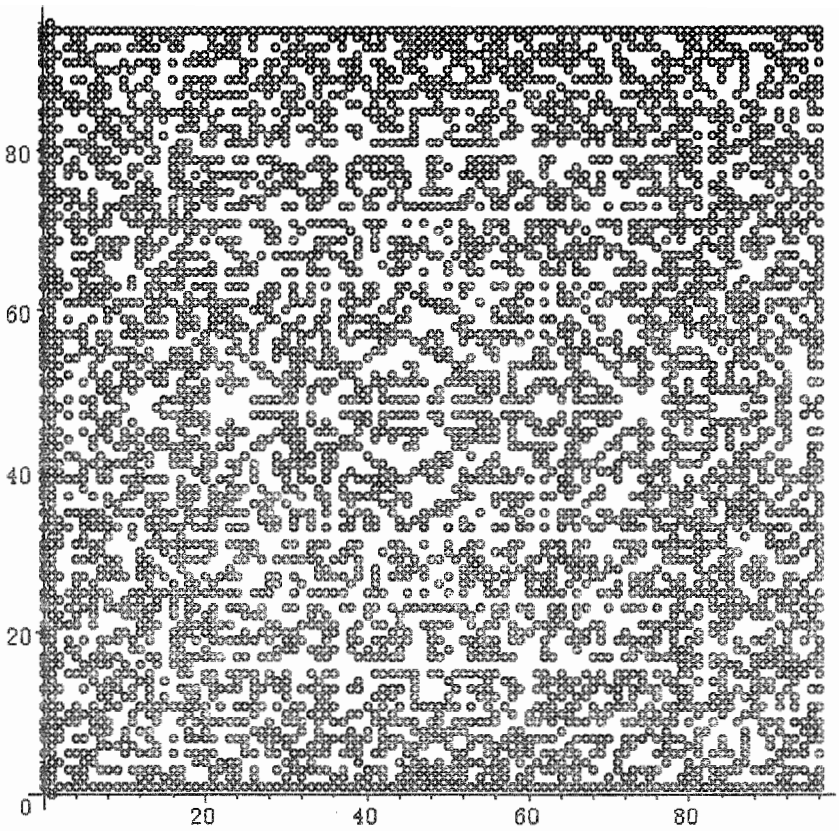
$$17 \le p$$

であることが必要である。

しかも、値は、例えば、$n = 1/2 = 49$ であれば、4 の倍数、$n = 1/3 = 65$ であれば 3 の倍数、$n = 1/4 = 73$ であれば 2 の倍数という具合になっていることが読みとれると思う。

$$p = 97$$

$$[P_n^*(x), n]$$



以前、楕円曲線の族

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

を考えて、(Weierstrass の族ではない。Weierstrass の場合は $y^2 = x^3+ax+b$)の有限体上での解の個数を $p = \{0,1,2,\cdots,p-1\}$ として

$$a_p = \sum_{x\in p}(x^3+ax^2+b)^{(p-1)/2}$$

を計算したとき、

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

であり、これが、$n = 1/6$ の場合のルジャンドル多項式であることを認識していたから、これが Hasse の不等式の意味に違いないと確信した瞬間であった。

現実には、

$$(x^3+ax^2+b)^{(p-1)/2} = c_0+c_1x+c_2x^2+\cdots+c_{p-1}x^{p-1}+\cdots+x^{3(p-1)/2}$$

の形に展開して、x に関する和をとるのであるが、$x \neq 0$ なら p を法として $x^{p-1}= 1$ であるから、

$$\sum_{x\in p} x^{p-1} = p-1 = -1$$

に着目すれば、x^{p-1} の係数を求めて符号を変えればよいことが解る。$p \geq 17$ ならば、絶対値最小剰余(least absolute value residue)として一意的に定まるのである。

具体的計算は、多項定理により、$s = (p-1)/2$ とおくと

$$(x^3+ax^2+b)^{(p-1)/2} = x^{p-1}(x+a+b/x^2)^s$$

であるから、

$$(x+a+b/x^2)^s$$

の定数項を求めればよい。

$$(x+a+b/x^2)^s = \sum s!/((s-3n)!(3n)!)\, a^{s-3n}(x+b/x^2)^{3n}$$

であり、$(x+b/x^2)^{3n}$ の定数項は、

$$(3n)!/(n!(2n)!)\, b^n$$

であるから、積をとって

$$s!/((s-3n)!(3n)!)\,(3n)!/(n!(2n)!) = s!/((s-3n)!n!(2n)!)$$

が係数である。

$$s!/((s-3n)!n!(2n)!) = (-1)^n(-s)(-s+1)\cdots(-s+3n+1)/((2n)!n!)$$

である。

$s = (p-1)/2$ であるから、F_p では、$-s = 1/2$ である。そこで、

$$(a)_n = a(a+1)\cdots(a+n-1)$$

と記すことにすれば、

$$(1/2)_{3n} = (1/6)_n(3/6)_n(5/6)_n 27^n$$

$$(2n)!/2^{2n} = n!(1/2)_n$$

であるから、$3/6 = 1/2$ に注意して、

$$(-1)^n(-s)(-s+1)\cdots(-s+3n+1)/((2n)!n!) = (1/6)_n(5/6)_n/n!^2 \cdot (-27/4)^n$$

なのである。従って、求める係数は

$$a^s \sum_{n<p/6} (1/6)_n(5/6)_n/n!^2 \cdot (-27b/4a^3)^n$$

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

となるのである。

有理数体 Q、実数体 R、複素数体 C など、標数(characteristic number, character) 0 の体では

$$F(1/6,5/6,1,x) = \sum_{n\in N} (1/6)_n(5/6)_n/n!^2\, x^n$$

は無限級数であるけれども、有限体では、任意の 2 でない素数、つまり、奇素数は

$$p = 6n \pm 1$$

の形をしているから、

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

は $n = [p/6]$ 次より高い次数の項は

$$(1/6)_n (5/6)_n = 0$$

となり、$n = [p/6]$ 次の多項式で、上記のルジャンドル多項式 $P_n(x)$ で表現できるのである。

この内容は

Kanji Namba, Legendre polynomial over finite fields and factorization of integers, Int. Symp. in memory of Hua Loo Keng, Beijin. Vol.1 Number theory, Springer-Verlag (1991) pp.209-222

に掲載されているが、結局、3/6 = 1/2 という等式に思い至ったことが key であったと思う。

当時は、東大教養学部の数学教室の事務室では、山崎圭次郎先生、近藤武先生、金子晃さん、などと色々雑談しながら、演習問題で収束半径が 4/27 = $2^2/3^3$ の級数がでてきたとき、3 次式の判別式との関係などと関係して、近藤先生が、そういうのは「超幾何級数なんだ」といったのが印象的であったし、また、“はげみ”になった。

また、当時、斎藤正彦先生のところで、超準解析(non-standard analysis)のセミナーがあり、セミナーの後で、木下素夫先生、杉浦光夫先生と「宇佐」という店で酒を飲むの習慣になっていたが、その時、ガウスのヂスキチオーネス(Disquisitiones Arithmeticae)のドイツ語訳の話など、自分の雲を掴む夢みたいな話をきいてもらったことも大いに励みになったと思う。

上記の話のパラメータである

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

は楕円曲線

$$E: \quad y^2 = x^3 + ax^2 + b$$

の j-不変量(j-invariant)で、これを変数として取り扱うことができるのである。これらから、

Legendre の標準形

$$y^2 = x(x-1)(x-a) \qquad F(1/2,1/2,1,x)$$

Euler の標準形

$$y^2 = x(x^2+ax+1) \qquad F(1/4,3/4,1,x)$$

Hesse の標準形

$$x^3+y^3+3axy$$

そして、今述べた

$$y^2 = x^3+ax^2+b \qquad F(1/6,5/6,1,x)$$

Weierstrass の標準形

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

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

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

などへの変換にはそんなに困難はない。しかし、有理関数の合成に関する交換可能な組合せ、つまり、

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

の、例えば、Tchebycheff の多項式などに対応するような、三角関数や逆三角関数から、例えば

$$T_{2n}(x) = (-1)^n \cos(2n \cos^{-1}(x))$$

$$T_{2n+1}(x) = (-1)^n \sin((2n+1)\sin^{-1}(x))$$

のような族

$$T_0(x) = 1,\ T_1(x) = x,\ T_2(x) = 2x^2-1,\ T_3(x) = 4x^3-3x,\ T_4(x) = 8x^4-8x^2+1,$$

$$T_5(x) = 16x^5-20x^3+5x,\ T_6(x) = 32x^6-48x^4+18x^2-1,\cdots$$

では、例えば、

$$T_6(x) = T_3(T_2(x)) = T_2(T_3(x))$$

つまり、この場合は $T_2(x), T_3(x)$ の交換可能性であるが

$$2(4x^3-3x)^2-1 = 4(2x^2-1)^3-3(2x^2-1) = 32x^6-48x^4+18x^2-1$$

等となっている。

楕円関数の n-倍射 (n-multiple)、つまり、例えば、Weierstrass 標準形で

$$E:\ y^2 = x^3+ax+b$$

で表示されている場合は、E 上の点 (x,y) の n-倍射

$$[n](x,y) = (f_n(x,y), g_n(x,y))$$

を考えると、x-座標の有理関数 $f_n(x,y)$ は y を y^2 の形で含み、従って

$$[n](x) = f_n(x, \pm\sqrt{x^3+ax+b})$$

は有理関数になっている。この有理関数の次数を、既約表示した場合の分母と分子の次数の高い方と定義すると、n^2-次の有理式であることが知られ

ている。

従って、場合によっては、n-次の有理式f(x)が存在して

$$[n](x)=f(f(x))$$

となることも可能であろう。このような関数を合成平方根(compositional square root)という。

勿論、任意のn-倍射に対して合成平方根が存在する訳ではない。合成平方根が存在する場合は、Hilbert-Weberの類多項式の解で記述される係数をもつことが知られている。例えば、

$$D: y^2 = x^3+1$$

について、[2](x)と[3](x)を求めてみよう。

1. [2](x)について

D上の点をp=(u,v)とする。pを通りDに接する直線の方程式は

$$f(x,y)=y^2-(x^3+1) \ =0$$

と考えると、

$$l: \ f_x(u,v)(x-u)+f_y(u,v)(y-v)=-3u^2(x-u)+2v(y-v)=0$$

そこで、h(x)とk(x)のxに関する終結式を、例えば

$$h(x)\,ⓧ\,k(x)=\mathrm{res}(h(x),k(x),x)$$

のように、ここだけの記号として記し、消去積(elimination product)と呼ぶことにする。積、ⓧ, ⓨ,…の結合力は加減乗除(+, −, ×, /)よりも弱いものとする。

Dの接線lとDの交点は、連立方程式

$$y^2-(x^3+1)=0,\ v^2-(u^3+1)=0$$

$$-3u^2(x-u)+2v(y-v)=0$$

を解いて求められる。つまり、xとvの関係は

$$y^2-(x^3+1)\,ⓨ\,-3u^2(x-u)+2v(y-v)\,ⓤ\,v^2-(u^3+1)$$

を計算すればよい。結合法則

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

が成立するから、消去はどの順番に行ってもよい。前から順に行うと、

$$y^2-(x^3+1)\,ⓨ\,-3x^2(u-x)+2y(v-y)\,ⓤ\,v^2-(u^3+1)$$

$$=$$

$$(4u+4ux^3-x^4+8x)^2(-x+u)^4$$

である。つまり

$$u = [2](x) = x(x^3-8)/4(x^3+1)$$

である。これは、確かに $4 = 2^2$ の有理式である。この式は2次の有理式の合成積に因数分解される。

$$x(x^3-8)/4(x^3+1) = x(x+4)/4(x+1) \bullet x(x-2)/(x+1)$$

である。

しかしながら、一般に、nm 次の有理式 f(x)が、n 次有理式 g(x)と m 次有理式 h(x)の合成として

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

の形に分解可能か、或いは係数をどの範囲なら可能かなどの、合成素因数分解(compositional factrization)や合成素(compositional primality)の判定問題、さらに、その複雑性、つまり計算量(complexity, computational amount)などの問題は今後の研究に待つ部分が多いと思う。将来の発展が期待される分野であろうと思う。

勿論、一次変換の群(一次分数変換群)が単数の如く合成分解に作用する。

2. [3](x)について

$$D: y^2 = x^3+1$$

の2倍射(duplication map)のが

$$u = [2](x) = x(x^3-8)/4(x^3+1)$$

あるいは、関係

$$4u+4ux^3-x^4+8x = 0$$

で与えられることは既に述べた。今度は

$$(u,v), (x,y)$$

を通る直線と D との交点(s,t)を求めてみよう。直線の方程式を

$$m: \quad (s-u)(y-v)-(x-u)(t-v) = 0$$

とする。解くべき連立方程式は

$$y^2-(x^3+1) = 0,\ v^2-(u^3+1) = 0,\ t^2-(s^3+1) = 0,$$

$$4u+4ux^3-x^4+8x = 0$$

$$(s-u)(y-v)-(x-u)(t-v) = 0$$

である。変数は x,y,u,v,s,t の6個で、方程式は5個である。これから、x と s の関係を得たいのである。まず、簡単に消去できるのは u である。しかし、u,v を含む式は

$$v^2-(u^3+1) = 0,\ (s-u)(y-v)-(x-u)(t-v) = 0$$

の2個である。従って、次の式では、結合の法則は成立しない：

$$((s-u)(y-v)-(x-u)(t-v)\ⓥ\ v^2-(u^3+1))\ⓤ\ 4u+4ux^3-x^4+8x$$

故に、

$$y^2-(x^3+1)\ⓨ(((s-u)(y-v)-(x-u)(t-v)\ⓥ\ v^2-(u^3+1))\ⓤ\ 4u+4ux^3-x^4+8x)\ⓣ\ t^2-(s^3+1)$$

を計算すればよい。結果は

$$81(4+x^3)^4x^3(72x^5s+9x^8s+144x^2s-x^9+96x^6-48x^3-64)^2(4u+4ux^3-x^4+8x)^4(s-x)^6$$

であり、新しい因子から

$$72x^5s+9x^8s+144x^2s-x^9+96x^6-48x^3-64=0$$

つまり、

$$s=[3](x)=(x^9-96x^6+48x^3-64)/9x^2(x^6+8x^3+16)$$

を得る。これは、確かに $9=3^2$ 次の多項式である。これには、合成平方根

$$[\sqrt{3}](x)=-(x^3+4)/3x^2$$

が存在する。

このことは、その合成平方(compositional square)を計算して確かめることができる。

$$[\sqrt{3}]([\sqrt{3}](x))=(x^9-96x^6+48x^3-64)/9x^2(x^3+4)^2$$

大切な点は、この関数の係数が整数の範囲で求まっていることである。これは、$Z(\sqrt{-3})$ の類数が1であることとも関係している。また、

$$[2](x)=x(x^3-8)/4(x^3+1)$$

とも交換可能である。

$$[2]([\sqrt{3}](x))=[\sqrt{3}]([2](x))=[2\sqrt{3}](x)$$

$$=-\frac{(x^3+4)(x^9+228x^6+48x^3+64)}{12x^2(x^3-8)^2(x^3+1)}$$

これとは独立に、何か非自明な、有理関数の交換可能な“組”をずっと探し続けていた。そして、1993年7月に Marseille, Luminy で Colloquium Takeuchi というのが開かれて、その帰路、Nice に立ち寄り、丘の上から海を見ていたとき

$$27x/(4x-1)^3,\quad 64x(1-x)^3/(8x+1)^3$$

の組が雲のごとく(心に)浮かんできたのであった。

今一つ関数に関する(補助的な、群論では馴染みの内容だが)記号

$$f(x)\Rightarrow g(x)=f(x)\bullet g(x)\bullet f^1(x)=f(g(f^1(x)))$$

を導入しておく。これが「ならば」(imply)に相当することは

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

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

などの指数法則からも解る。

さて、例えば、

$$f(x)=-1/x^3,\ f^{1}(x)=-1/x^{1/3}$$

$$g(x)=[2](x)=x(x^3-8)/4(x^3+1)$$

$$h(x)=[\sqrt{3}](x)=-(x^3+4)/3x^2$$

などを考えてみよう。$f^{1}(x)^3=-1/x$ であるから、

$$g(-1/x^{1/3})=-(-1-8x)/(4x^{1/3}(1-x))$$

であるから

$$f(x)\Rightarrow g(x)=-1/g(-1/x^{1/3})^3=64x(x-1)^3/(8x+1)^3$$

$$f(x)\Rightarrow h(x)=-1/h(-1/x^{1/3})^3=27x/(4x-1)^3$$

等となっている。(合成)交換可能性はこれからの帰結である。

楕円曲線の曲線族とそれを特徴づけるフックス関数を含む交換図式をあげておく：

上半の交換図式は、二つの楕円曲線

$$C:\ x^3+y^3=1$$

$$D:\ y^2=x^3+1$$

の $\sqrt{3}$, 2倍射の交換可能有理関数と関係しており、例えば

$$-x(x-2)^3/(2x-1)^3$$

は

$$1/x,\quad 1-x$$

の両方と交換可能である。つまり、

$$-x(x-2)^3/(2x-1)^3\bullet 1/x=1/x\bullet -x(x-2)^3/(2x-1)^3$$

$$-x(x-2)^3/(2x-1)^3\bullet 1-x=1-x\bullet -x(x-2)^3/(2x-1)^3$$

であり、

$$(1+\omega x)^3/(1+\bar{\omega}x)^3$$

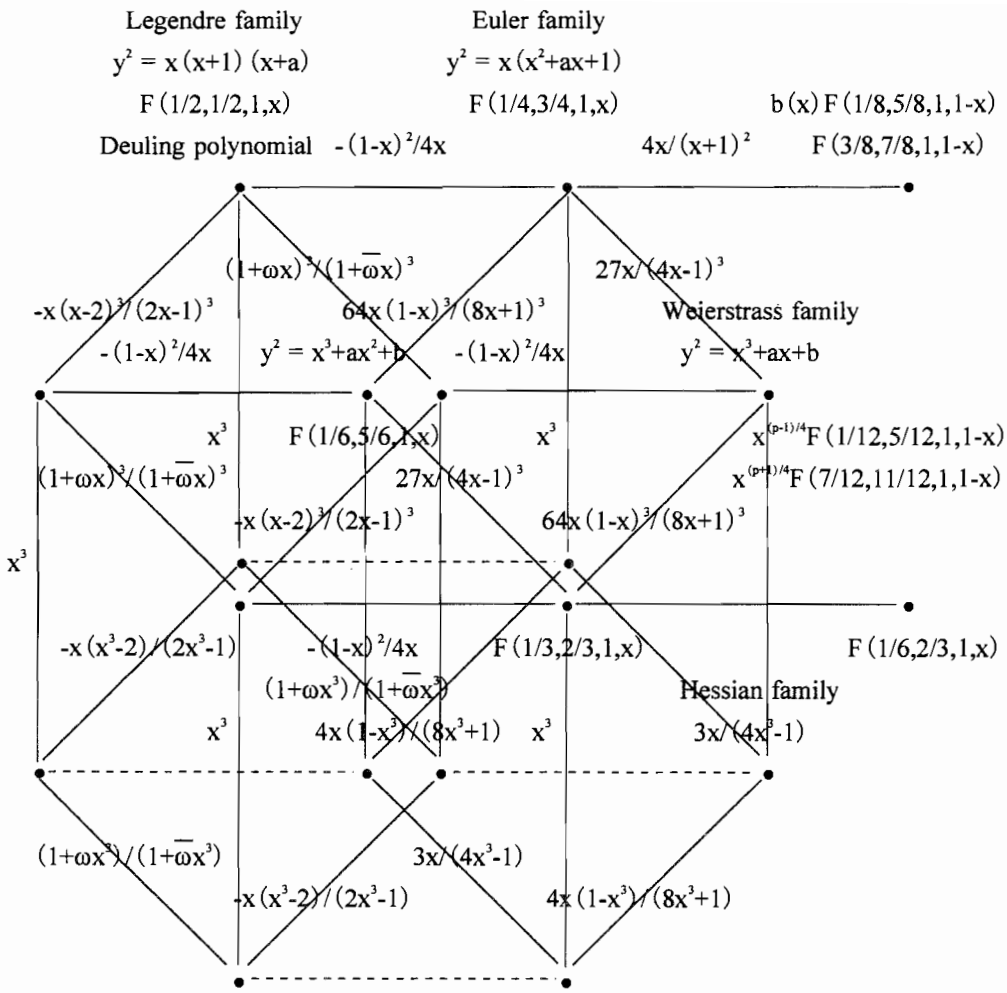
については

$$1/x,\quad 1-x$$

との右からの作用を、ともに左からの $1/x$ に変換する：

$$(1+\omega x)^3/(1+\bar{\omega}x)^3\bullet 1/x=(1+\omega x)^3/(1+\bar{\omega}x)^3\bullet 1-x=1/x\bullet(1+\omega x)^3/(1+\bar{\omega}x)^3$$

といった、簡単ではあるが基本的な性質がある。



この、交換図式は、Weierstrass の標準形を終点にもつという形式をもつが、実質的には、対称群 $S(4) = 4!$ が可解群 (solvable group) であることを、有理関数の合成代数系という言葉で述べたもので、各関数は組成列に対応した有理式である。

当然のことであるが

$$S(3) = \langle 1/x,\ 1-x \rangle = \{x,\ 1/x,\ 1-x,\ 1/(1-x),\ 1-1/x,\ x/(x-1)\}$$

その不変式が

$$27x/(4x-1)^3 \bullet -(1-x)^2/4x \ = -(1-x)^2/4x \ \bullet (1+\omega x)^3/(1+\bar{\omega}x)^3$$
$$= 27(x-1)^2x^2/4(1-x+x^2)^3$$

のように、合成分解するが、

$$-(1-x)^2/4x \ \bullet (1+\omega x)^3/(1+\bar{\omega}x)^3 = -(1-x)^2/4x \ \bullet (1+\bar{\omega}x)^3/(1+\omega x)^3$$

でもある。二つの右因子

$$(1+\omega x)^3/(1+\bar{\omega}x)^3,\ (1+\bar{\omega}x)^3/(1+\omega x)^3$$

は、勿論、左からの 1/x の合成で移り合える関係にある。例えば

$$27(x-1)^2x^2/4(1-x+x^2)^3 = 27x/(4x-1)^3 \bullet -(1-x)^2/4x$$

のような(合成)因数分解から、

$$27(x-1)^2x^2/4(1-x+x^2)^3 = -(1-x)^2/4x \bullet (1+\bar{\omega}x)^3/(1+\omega x)^3$$

のような因子はどのようにすれば形式的に見つけられるのであろうか。これは、例えば

$$-(1-y)^2/4y = 27(x-1)^2x^2/4(1-x+x^2)^3$$

を、有理関数の範囲で、y について解くことである。y については 2 次方程式である。

係数を整理すれば、

$$(x^2-x+1)^3y^2-(x^2+2x-2)(x^2-4x+1)(2x^2-2x-1)y+(x^2-x+1)^3 = 0$$

であり、その判別式は

$$(x^2+2x-2)^2(x^2-4x+1)^2(2x^2-2x-1)^2-4(x^2-x+1)^6 = -27x^2(x-1)^2(x-2)^2(2x-1)^2(x+1)^2$$

となり、$Q(\sqrt{-3})$で一次式の積

$$((1+\omega x)^3y-(1+\bar{\omega}x)^3)((1+\bar{\omega}x)^3y-(1+\omega x)^3) = 0$$

に分解するのである。

任意の S(n)の可解部分群の組成列に応じて、このような有理関数の合成代数系の図式が存在するであろう。その表示は、例えば一次変換の群の自由さなどを除くと、一意的ではないかと考えている。端点は群で、矢印が有理関数の図表なのである。

それは、可解な代数方程式のべき根による解法そのものといってもよいであろう。代数曲線の微分方程式とそのモノドロミーのガロア理論である。

余談. むかし、岩村聯先生との雑談のなかで

$$2^4 = 4^2$$

のように、2, 4 の組は、ベキに於いて交換可能な非自明な唯一の組である。など雑談したことがある。

$$x^y = y^x$$

ならば、勿論

$$x^(1/x) = y^(1/y)$$

であるから、

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

の同じ値に対応するx,yは指数的には交換可能である。

有理数の範囲では無数の解が存在することは常識であろうが、故島内剛一先生等との雑談の“名残”…もあって、(このような話が消えてしまうのも残念なので)少し説明する。今、

$$x = (n/m)^{(m/(n-m))}, y = (n/m)^{(n/(n-m))}$$

の組を考えてみよう。

$$x^y = ((n/m)^{(m/(n-m))})^{((n/m)^{(n/(n-m))})}$$
$$= (n/m)^{((m/(n-m)\cdot(n/m)^{(n/(n-m))})}$$

である。

$$m/(n-m) = (n/(n-m))(m/n)$$

であるから、

$$(m/(n-m)\cdot(n/m)^{(n/(n-m))} = (n/(n-m))(m/n)\cdot(n/m)^{(n/(n-m))}$$
$$= (n/(n-m))\cdot(n/m)^{(n/(n-m)-1)} = (n/(n-m))\cdot(n/m)^{(m/(n-m))}$$

である。要点は

$$n/(n-m) = m/(n-m)+1$$

という一点である。こうして、指数部分のnとmが入れ代わったから、

$$y^x = ((n/m)^{(n/(n-m))})^{((n/m)^{(m/(n-m))})}$$
$$= (n/m)^{((n/(n-m)\cdot(n/m)^{(m/(n-m))})}$$

によって、

$$x^y = y^x$$

なる、指数交換する対

$$(x,y) = ((n/m)^{(m/(n-m))}, (n/m)^{(n/(n-m))})$$

が助変数表示された。

では、これはどのようにして見つけられたのであろうか。

$y = ax$ とおいてみよう。$x^y = y^x$ ならば、

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

故に、

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

$x \neq 0$ として、xで割って、

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

従って、

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

故に、y = ax, 1/(a-1)+1= a/(a-1)より、

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

である。これは、

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

を意味している。aを変数xに置き換えた関数

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

は、何か奇妙な関数であるが、x = 0, 1を特異点にもつ。

さて、

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

のいくつかの例を見よう。

a) a = 2のとき、

$$x = a\hat{}(1/(a-1)) = 2\hat{}1 = 2, y = 2\hat{}2 = 4$$

で、これは、話のネタになった数である。

b) a = 3のとき、

$$x = 3\hat{}(1/2) = \sqrt{3}, y = 3\hat{}(3/2) = 3\sqrt{3}$$

従って、

$$\sqrt{3}\hat{}(3\sqrt{3}) = (3\sqrt{3})\hat{}\sqrt{3}.$$

c) 2 = 1/(a-1)のとき、つまり、a = 3/2のとき、

$$x = (3/2)\hat{}2 = 9/4, \quad y = (3/2)\hat{}3 = 27/8$$

従って、

$$(9/4)\hat{}(27/8) = (27/8)\hat{}(9/4)$$

である。勿論、結果は無理数である。

$$(9/4)\hat{}(27/8) = (3/2)\hat{}(27/4) = (27/8)\hat{}(9/4) = 15.43888736\cdots$$

d) n = 1/(a-1)のとき、a = 1+1/n = (n+1)/nであるから、

$$x = (n+1)^n/n^n, \quad y = (n+1)^{n+1}/n^{n+1}$$

であり、これは、自然対数の底eの定義に現れそうな

$$x = (1+1/n)^n, \quad y = (1+1/n)^{n+1}$$

である。この様にして、両方ともeに収束するような有理数の無限個の対は得られる。両者ともに有理数となる組はこれだけなのであろうか。

$$e\hat{}e = e^e = 15.15426223\cdots$$

が何やら意味をもちそうな雰囲気がでてきた。

先ず、関数

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

の関数等式

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

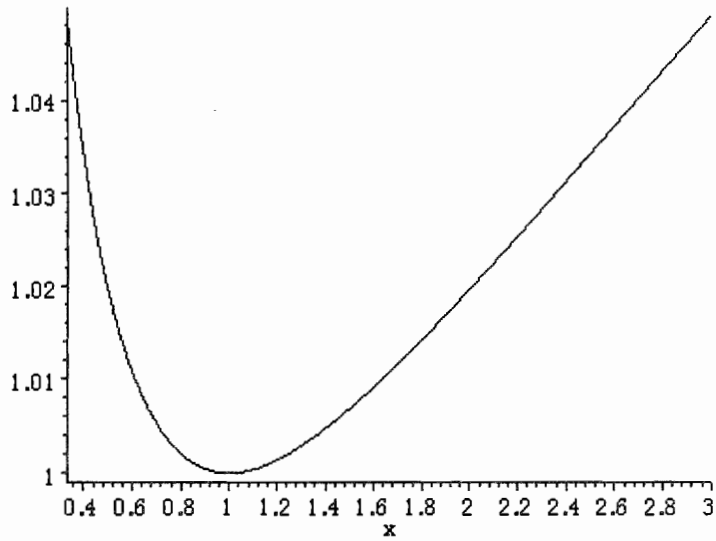
を示しておく。この関数の対数をとると、

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

更に対数をとると、

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

が得られる。



また、

$$h(1+x) = (x+1)\cdot\log(1+x)/x + \log(\log(1+x)/x)$$

$$= 1+x^2/24-x^3/24+107x^4/2880-47x^5/1440+10447x^6/362880-3097x^7/120960+\cdots$$

であり、1が極小であることも解る。更にh(1+x)の対数をとると

$$k(x) = \log(h(1+x)) = x^2/24-x^3/24+209x^4/5760-89x^5/2880+3193x^6/1209606-51x^7/2240+\cdots$$

などとなっている。この級数の x^n の係数の分母は常に n+1 までの素数しか含まない。

例えば、n = 28 のときは

$$\frac{102460937\cdot 515057277109\cdot 407917312151770709}{2^{43}\cdot 3^{17}\cdot 5^8\cdot 7^4\cdot 11^2\cdot 13^2\cdot 17\cdot 19\cdot 23\cdot 29}$$

関数等式の証明は

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

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

である。また、

$$(1+\omega x)^3/(1+\bar{\omega}x)^3$$

は、1-x も 1/x も 1/x に変換する。つまり、

$$(1+\omega x)^3/(1+\bar{\omega}x)^3 \bullet 1/x = (1+\omega x)^3/(1+\bar{\omega}x)^3 \bullet 1\text{-}x = 1/x \bullet (1+\omega x)^3/(1+\bar{\omega}x)^3$$

であるから、この関数との合成を g(x) とすると

$$g(x) = h((1+\omega x)^3/(1+\bar{\omega}x)^3)$$

は、絶対不変式

$$y = 27(x-1)^2x^2/4(1-x+x^2)^3$$

の関数となっている。この関数はまだ未知の性質をもっていると思うが、今のところ単に提示ということだけである。この関数の歴史には興味がある。

3. 表現変換式と対合

例えば、Weierstrass の標準形での楕円曲線

$$C:\ y^2 = x^3+ax+b$$

に対し、所謂、j-invariant

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

を変数として、ルジャンドル記号、つまり、素体 $F_p = GF(p) = p$ での平方・非平方に応じて ±1 を対応させる関数

$$(u/p) = \#\{y\in p: y^2 = u \bmod p\} - 1 = u^{(p-1)/2} \bmod p$$

の x^3+ax+b の値の $p = \{0,1,2,\cdots, p-1\}$ での総和

$$a_p = \sum x\in p\ (x^3+ax+b/p)$$

は、z の関数として定まることが知られている。それは ± の符号の自由さはあるかも知れないが、$p = \pm 1 \bmod 4$ に応じて

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

で与えられることが知られている。ルジャンドル多項式に平方根を代入した多項式

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

としてもよい。

$P_{[p/6]}(\sqrt{x})$ のように表現の上では $\sqrt{x}$ が現れるが、ルジャンドルの多項式は奇数次あるいは偶数次の項のみ現れるので、最初の $x^{[p/4]}$ にも吸収されて、

結果はxの多項式になるのである。

また、$a_{12}(x)$の添字(suffix)の$_{12}$であるが、これは、

$$F(1/12,5/12,1,1-x) = x^{(1\pm1)/4}P_{[p/6]}(\sqrt{x})$$

がn = [p/12]次の多項式なので、このように「仮に」つけた。

この関数を素体F_pで、絶対値最小剰余(least absolute value residue, lavr)として計算する。Hasseの不等式

$$|a_p| < 2\sqrt{p}$$

との関連から、$p \geq 17$では一意的に値が定まる。

この数は、あまり大きくはないとはいえ、手計算の時代にはp = 2, 3, 5, 7, 11, 13,…など、小さい素数で実験して一般の法則や式を導く、あるいは、発見するというのは自然なことであったと思われるので、17が最小の一般的な場合であるというので、あまり注意を惹かなかったのかも知れない。

例えば、p = 17は、4を法にして1であるから

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

の方のフックス関数であるが、ルジャンドルの関数としては、[17/6]= 2であるから、$P_2(x)$である。

先ず、p = 17 = 12+5であるから、0 = 1+5/12、故に5/12 = -1である。5・7 = 35 = 2・17+1であるから、1/12 = -7 = 10である。故に、一次の係数は

$$(1/12)(5/12)/1 = 7$$

である。2次の係数は-1, -7に1づつ加えた0, -6を掛けて$2^2 = 4$で割るのであるが、すでに0がでているので、

$$(-1)(0)(-7)(-6)/(1^2\cdot2^2) = 0$$

2次以降の項は消えて、結果は1次式

$$F(1/12,5/12,1,1-x) = 1+7(1-x) = 8-7x = 8+10x$$

である。これが[17/12]= 1の意味である。[17/4]= 4であるから、

$$a_{12}(x) = x^{(p-1)/4}F(1/12,5/12,1,1-x) = x^4(8+10x)$$

である。ルジャンドル多項式の方から見ると、[17/6]= 2であるから、

$$P_2(x) = 3x^2/2-1/2$$

である。2・8+1 =17であるから、-1/2 = 8、従って -3/2 = 24 = 7である。つまり、3/2 = 10である。xに$\sqrt{x}$ を代入、つまり、x^2をxに代えると

$$x^4P_2(\sqrt{x}) = 3x/2-1/2 = 8+10x$$

のように 勿論、同じ多項式を得る。

次の表はその値の絶対値最小剰余(lavr)である：

$$[a_{12}(x) : x = 0 \sim 16]$$

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

勿論、Hasseの不等式は

$$|a_{12}(x)| < 2\sqrt{17} = 8.246211252$$

であり、p = 17での絶対値最小剰余は8以下であるから、この場合は特別で、常に成立するが…。上の表では8は存在せず、7が一個存在する。角度の方で

$$\sin^2\theta$$

に比例するということは、[-1,1]の区間で標準化すれば、単位円の内部、つまり

$$\sqrt{1-x^2}$$

に比例することである。両端の近くでは、分布はこの関数に比例して疎になっているのである。

さて、ここから、表現(変換)多項式(representation transform polynomial)の定義を与えようと思う。

$$f(x)$$

を、体 $F_p = p = \{0,1,2,\cdots, p-1\}$ の乗法群、つまり、0でない元の全体

$$F_p^{\times} = p-1 = \{1,2,\cdots, p-1\} = (p-1)'$$

で定義された関数とするとき、多項式

$$\bar{f}(x) = \sum n \in p-1\ f(r^n)\, x^n$$

を f(x)の(原始根 r に応ずる)表現変換多項式(rep. polynomial)という。当然、原始根の個数だけ存在する。

今の場合、つまり、p = 17での原始根の全体は

$$[3, 5, 6, 7, 10, 11, 12, 14]$$

の8個である。さしあたり、最小の r = 3を考えよう。その冪の表は

$$[3^n : n = 0 \sim 15]$$

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

である。この順に $a_{12}(r^n) = a_{12}(3^n)$ を書き出したものが、次の表である。

$$[\ a_{12}(3^n) : n = 0 \sim 15]$$

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

以下に、同じ内容の一覧表を挙げておく。

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$a_{12}(n)$	0	1	6	1	-3	6	0	6	-3	4	7	-4	-2	2	3	-5	-2
3^n	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
$a_{12}(3^n)$	1	1	4	7	2	6	-5	-4	-2	3	-3	6	-3	-2	6	0	-

従って、表現変換多項式は、r = 3 の場合であるが、

$$\bar{a}_{12}(x) = 1+x+4x^2+7x^3+2x^4+6x^5-5x^6-4x^7-2x^8+3x^9-3x^{10}+6x^{11}-3x^{12}-2x^{13}+6x^{14}+0x^{15}$$

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

である。x^{15} が消えているのは、$3^{15} = 6$ で $a_{12}(6) = 0$ となるからである。

原始根として、逆元をとれば、定数のところを除いて逆の順になる。例えば、r = 1/3 = 6 ならば

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

となり、今度は x の項が消え、x^{15} の係数は 1 となっている。

3.1 終結行列 (resultant matrix)

二つの多項式

$$f(x) = a_0x^n+a_1x^{n-1}+\cdots+a_n = a_0(x-c_1)(x-c_2)\cdots(x-c_n)$$

$$g(x) = b_0x^m+b_1x^{m-1}+\cdots+b_n = b_0(x-d_1)(x-d_2)\cdots(x-d_m)$$

の(シルベスターの)終結行列(resultant matrix)とは

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & \cdots & 0 \\ & & \cdots & & & \cdots & \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_m & \cdots & 0 \\ & & \cdots & & & \cdots & \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{pmatrix}$$

の形の行列のことである。下の n 行は多項式環で g(x) で生成される主イデアルを意味している。これらを上の m 行に何倍かして加えて、つまり、行変形で

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} & 0 & \cdots & 0 \end{pmatrix}$$

$$\begin{pmatrix} c_{21} & c_{12} & \cdots & c_{2n} & 0 & \cdots & 0 \\ & \cdots & & & \cdots & & \\ c_{n1} & c_{n2} & \cdots & c_{nn} & 0 & \cdots & 0 \\ b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_m & \cdots & 0 \\ & \cdots & & & \cdots & & \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{pmatrix}$$

上方主対角行列あるいは

$$\begin{pmatrix} 0 & \cdots & 0 & d_{11} & d_{12} & \cdots & d_{1n} \\ 0 & \cdots & 0 & d_{21} & d_{22} & \cdots & d_{2n} \\ & \cdots & & & \cdots & & \\ 0 & \cdots & 0 & d_{n1} & d_{n2} & \cdots & d_{nn} \\ b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_m & \cdots & 0 \\ & \cdots & & & \cdots & & \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \end{pmatrix}$$

の形に表現する。前者を高次係数消去型あるいは主対角型、後者を剰余型と呼ぶ。

例えば、剰余型は、剰余を rem と記せば

$$\mathrm{rem}\,(x^k f(x), g(x), x)$$

の係数を順に並べたものであり、前者の剰余消去型あるいは主対角型

$$x^k f(x)$$

の m 次以上の項を g(x)で生成されるイデアルで消去したもので、係数反転多項式

$$\underline{f}(x) = x^n f(1/x), \; g(x) = x^m g(1/x)$$

について、剰余を、逆の順序であるが、順に書いたものである。

次に、終結行列を反対方向にした行列を考える。

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

$$\begin{pmatrix} 0 & \cdots & b_0 & b_1 & \cdots & b_m & 0 \\ & \cdots & & & \cdots & & \\ b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \end{pmatrix}$$

これを、逆行型終結行列(anti-resultant matrix)と呼ぶ。これに関しても

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} & 0 & \cdots & 0 \\ c_{21} & c_{12} & \cdots & c_{2n} & 0 & \cdots & 0 \\ & \cdots & & & \cdots & & \\ c_{n1} & c_{n2} & \cdots & c_{nn} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \\ 0 & \cdots & b_0 & b_1 & \cdots & b_m & 0 \\ & \cdots & & & \cdots & & \\ b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \end{pmatrix}$$

及び

$$\begin{pmatrix} 0 & \cdots & 0 & d_{11} & d_{12} & \cdots & d_{1n} \\ 0 & \cdots & 0 & d_{21} & d_{22} & \cdots & d_{2n} \\ & \cdots & & & \cdots & & \\ 0 & \cdots & 0 & d_{n1} & d_{n2} & \cdots & d_{nn} \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_m \\ 0 & \cdots & b_0 & b_1 & \cdots & b_m & 0 \\ & \cdots & & & \cdots & & \\ b_0 & b_1 & \cdots & b_m & 0 & \cdots & 0 \end{pmatrix}$$

の形の高次係数消去型あるいは主対角型と剰余型との行列が考えられる。剰余型と高次係数消去型は係数の順序を反転させた場合の剰余に帰着できるので、今は、剰余型をもってf(x)とg(x)の終結行列とする。

つまり、剰余型n-次正方行列を

$$f(x) \circledast g(x)$$

と記し、順行型終結行列(この場合、単に終結行列という)とよび、逆行行列についても剰余型n-次正方行列を

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

と記し、順行型終結行列(anti-resultant)と呼ぶ。行列の次数は、左の関数の次数であるから、例えば、

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

の次数は g(x) の次数 m である。

逆行型の終結行列を考えた理由は逆行巡回行列は対称行列で固有値が実数になるからである。

3.2 表現変換多項式と $x^p-x=0$ での値

先ず、f(x) の例として、p = 17 での表現多項式

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

をとり、もう一つの多項式としては、体 F_p の定義多項式

$$x^{17}-x=x(x-1)(x+1)(1+x^2)(1+x^4)(1+x^8)$$

の一つの因子

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

を考える。

$$\mathrm{rem}(f(x),g(x))=-4x^7-11x^6+8x^5+5x^4+x^3+7x^2-2x+3$$

である。従って、係数の列は

$$[-4,\ -11,\ 8,\ 5,\ 1,\ 7,\ -2,\ 3]$$

であり、f(x) に x を乗ずる毎に、剰余は定数項に最高次 x^7 の係数の符号を変えたものを補うことになるから、(逆行)終結行列は

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

$$=$$

$$\begin{pmatrix} -4, & -11, & 8, & 5, & 1, & 7, & -2, & 3 \\ -11, & 8, & 5, & 1, & 7, & -2, & 3, & 4 \\ 8, & 5, & 1, & 7, & -2, & 3, & 4, & 11 \\ 5, & 1, & 7, & -2, & 3, & 4, & 11, & -8 \\ 1, & 7, & -2, & 3, & 4, & 11, & -8, & -5 \\ 7, & -2, & 3, & 4, & 11, & -8, & -5, & -1 \\ -2, & 3, & 4, & 11, & -8, & -5, & -1, & -7 \\ 3, & 4, & 11, & -8, & -5, & -1, & -7, & 2 \end{pmatrix}$$

である。この行列を A と記せば、これは対称行列であるから、固有値は実数である。具体的には、固有多項式

$$\mathrm{ch}(A,x)=(x-17)^2(x+17)^2$$

で最小多項式は

$$x^2-17^2=(x-17)(x+17)$$

である。つまり、

は対合(involution)、つまり、Eを単位行列とすれば

$$X^2 = E$$

であり、トレースは 0 である。つまり、±1 がそれぞれ 4 重の固有値になっている。

一般に、任意の素数 p に対し、

$$g(x) | x^{p-1}-1,\ (x^{12}-1, g(x)) = 1$$

つまり、$x^{p-1}-1$ の(既約と限らない)因子 $g(x)$ で $x^{12}-1$ と互いに素ならば

$$A = 1/p \cdot \bar{a}_{12}(x)\,[x]\,g(x)$$

は常に対であることが予想される。

予想

$g(x) | x^{p-1}-1,\ ((x^2+1)(x^2+x+1), g(x)) = 1$ のとき

$$A = 1/p \cdot \bar{a}_{12}(x)\,[x]\,g(x)$$

は常に対合であり、$g(x) = x^2+1,\ x^2+x+1$ のとき

$$A = 1/\sqrt{p} \cdot \bar{a}_{12}(x)\,[x]\,g(x)$$

は対合である。

上記では、原始根として、r = 3 をとったが、一般の、例えば他の原始根をとっても同様である。例えば、3 の次の原始根 r = 5 の場合は

$$f(x) = \bar{a}_{12}(x) = 1+6x-3x^2+2x^4+3x^5+6x^6+7x^7-2x^8-2x^9+4x^{10}-4x^{11}-3x^{12}+x^{13}-5x^{14}+6x^{15}$$

で終結行列は

$$\bar{a}_{12}(x)\,[x]\,x^8+1$$

=

$$\begin{pmatrix}
-4, & -11, & 8, & 5, & 1, & 7, & -2, & 3 \\
-11, & 8, & 5, & 1, & 7, & -2, & 3, & 4 \\
8, & 5, & 1, & 7, & -2, & 3, & 4, & 11 \\
5, & 1, & 7, & -2, & 3, & 4, & 11, & -8 \\
1, & 7, & -2, & 3, & 4, & 11, & -8, & -5 \\
7, & -2, & 3, & 4, & 11, & -8, & -5, & -1 \\
-2, & 3, & 4, & 11, & -8, & -5, & -1, & -7 \\
3, & 4, & 11, & -8, & -5, & -1, & -7, & 2
\end{pmatrix}$$

に対しても、1/p = 1/17 を乗じたものは対合である。登場する数値は順序が変更されているだけである。

原始根 3 の場合に他の既約な因子から生ずる(逆行)終結行列についても具体的に行列表示を与えておく。

因子 x^4+1 の場合、

$$\bar{a}_{12}(x)\,[x]\,x^4+1$$

$$=$$

$$\begin{pmatrix} 17, & 0, & 0, & 0 \\ 0, & 0, & 0, & -17 \\ 0, & 0, & -17, & 0 \\ 0, & -17, & 0, & 0 \end{pmatrix}$$

固有多項式は $(x-17)^2(x+17)^2$ で対合である。

因子 x^2+1 の場合、これは $x^{12}-1$ の因子で、ガウス整数の退化がおこる場合である。

$$\bar{a}_{12}(x)\,[x]\,x^2+1$$

$$=$$

$$\begin{pmatrix} -1, & -4 \\ -4, & 1 \end{pmatrix}$$

この場合、固有多項式は x^2-17 であり、$1/\sqrt{p}\cdot A$ が対合である。

因子 x+1 の場合、

$$\bar{a}_{12}(x)\,[x]\,x+1$$

$$=$$

$$[-17]$$

この場合、固有多項式は x+17 であり、$1/p\cdot A$ が対合である。

因子 x-1 の場合、

$$\bar{a}_{12}(x)\,[x]\,x+1$$

$$=$$

$$[17]$$

この場合、固有多項式は x-17 であり、$1/p\cdot A$ が対合である。

例 2. p = 37 の場合、原始根は

$$[2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, \underline{35}]$$

であり、

$$a_{12}(x) = x^{(p-1)/4} F(1/12,5/12,1,1-x) = x^9(26x^3+15x^2+32x+2)$$

である。r＝2とすると、表現変換多項式は

$$\bar{a}_{12}(x) = 2x^{35}+6x^{34}-x^{33}+2x^{31}+3x^{30}+3x^{29}+3x^{28}-10x^{27}-10x^{26}+7x^{25}-2x^{24}+4x^{23}+10x^{22}+8x^{21}+4x^{20}-2x^{19}$$
$$+4x^{18}+7x^{17}-2x^{16}+5x^{15}+6x^{14}-7x^{13}+11x^{12}-4x^{11}+8x^{10}-2x^9+5x^8-8x^7-9x^6-6x^5-2x^4+8x^3+x^2-6x+1$$

この場合 $x^{p-1}-1$ は多くの既約因子の積に分解される。

$$x^{p-1}-1 = x^{36}-1 = (x-1)(x+1)(x^2+x+1)(1-x+x^2)(x^2+1)(x^4-x^2+1)(x^6+x^3+1)(1-x^3+x^6)$$
$$(x^{12}-x^6+1)$$

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

である。次数の高い順に対合かどうか判定する。

a) $x^{12}-x^6+1$ の場合

$$\bar{a}_{12}(x)\,[x]\,x^{12}-x^6+1$$

$$=$$

$$\begin{pmatrix}
-2, -3, 14, 21, -24, 1, -15, -4, -6, -9, 5, -11 \\
-3, 14, 21, -24, 1, -17, -4, -6, -9, 5, -11, 2 \\
14, 21, -24, 1, -17, -7, -6, -9, 5, -11, 2, 3 \\
21, -24, 1, -17, -7, 8, -9, 5, -11, 2, 3, -14 \\
-24, 1, -17, -7, 8, 12, 5, -11, 2, 3, -14, -21 \\
1, -17, -7, 8, 12, -19, -11, 2, 3, -14, -21, 24 \\
-17, -7, 8, 12, -19, -10, 2, 3, -14, -21, 24, -1 \\
-7, 8, 12, -19, -10, -15, 3, -14, -21, 24, -1, 17 \\
8, 12, -19, -10, -15, -4, -14, -21, 24, -1, 17, 7 \\
12, -19, -10, -15, -4, -6, -21, 24, -1, 17, 7, -8 \\
-19, -10, -15, -4, -6, -9, 24, -1, 17, 7, -8, -12 \\
-10, -15, -4, -6, -9, 5, -1, 17, 7, -8, -12, 19
\end{pmatrix}$$

この行列は対称行列ではない。しかし、固有多項式は

$$(x-37)^6(x+37)^6$$

であり、最小多項式は

$$x^2-37^2 = (x-37)(x+37)$$

となり、1/p･A は対合である。固有値は 6 重である。固有空間を生成する簡潔な直交系を与えることは一つの課題であろう。

b) x^6+x^3+1 の場合

$$\bar{a}_{12}(x)\,[x]\,x^6+x^3+1$$

=

$$\begin{pmatrix} 0, & 0, & 37, & 0, & 0, & 0 \\ 0, & 37, & 0, & 0, & 0, & 0 \\ 37, & 0, & 0, & 0, & 0, & 0 \\ 0, & 0, & -37, & 0, & 0, & -37 \\ 0, & -37, & 0, & 0, & -37, & 0 \\ -37, & 0, & 0, & -37, & 0, & 0 \end{pmatrix}$$

固有多項式は

$$(x-37)^3(x+37)^3$$

であり、最小多項式は

$$x^2-37^2 = (x-37)(x+37)$$

となり、1/p･A は対合である。

c)　x^6+x^3+1 の場合

$$\bar{a}_{12}(x)[x]x^6-x^3+1$$

=

$$\begin{pmatrix} -22, & 8, & -13, & 20, & -14, & 32 \\ 8, & -13, & -2, & -14, & 32, & 22 \\ -13, & -2, & -6, & 32, & 22, & -8 \\ -2, & -6, & 19, & 22, & -8, & 13 \\ -6, & 19, & 20, & -8, & 13, & 2 \\ 19, & 20, & -14, & 13, & 2, & 6 \end{pmatrix}$$

固有多項式と最小多項式の対は

$$(x-37)^3(x+37)^3,\ (x-37)(x+37)$$

であり、何か固有値の重複度の等しい対合という概念は必要になりそうである。以下では、調和対合(baranced involution)と呼ぶことにする。

d)　x^4-x^2+1 の場合

$$\bar{a}_{12}(x)[x]x^4-x^2+1$$

=

$$\begin{pmatrix} 0, & -37, & 0, & 37 \\ -37, & 0, & 37, & 0 \\ 0, & 0, & 0, & 37 \\ 0, & 0, & 37, & 0 \end{pmatrix}$$

この場合も 1/p･A は調和対合である。

e)　$1-x+x^2$ の場合

$$\bar{a}_{12}(x)\,[x]\,1-x+x^2$$

$$=$$

$$\begin{pmatrix} -37, & 0 \\ -37, & 37 \end{pmatrix}$$

この場合 1/p･A は調和対合である。

f)　x^2+x+1, x^2+1 の場合

$$\bar{a}_{12}(x)\,[x]\,x^2+x+1 \qquad \bar{a}_{12}(x)\,[x]\,x^2+1$$

$$= \qquad =$$

$$\begin{pmatrix} -3, & 4 \\ 7, & 3 \end{pmatrix} \qquad \begin{pmatrix} 6, & -1 \\ -1, & -6 \end{pmatrix}$$

この場合は $1/\sqrt{p}$･A は調和対合である。

g)　$x+1$, $x-1$ の場合

$$\bar{a}_{12}(x)\,[x]\,x+1 \qquad \bar{a}_{12}(x)\,[x]\,x-1$$

$$= \qquad =$$

$$(37) \qquad (37)$$

である。x^2-1 のように積に関する終結行列をとると、勿論、固有多項式の積であるが、

$$\bar{a}_{12}(x)\,[x]\,x^2-1$$

$$=$$

$$\begin{pmatrix} 0, & 37 \\ 37, & 0 \end{pmatrix}$$

のように 1/p･A は正則対合である。

なお、巡回対合に関しては、今の場合 x^2+1, x^2+x+1 を因子に含まないような $x^{36}-1$ の因子で x^n-1 の形のものは存在しない。x^n+1 では(既約ではないが) x^3+1, x^9+1 の 2 個が存在する。

h)　x^9+1 の場合

$$\bar{a}_{12}(x)\,[x]\,x^9+1$$

$$=$$

$$\begin{pmatrix} -14, & -5, & -15, & -8, & 13, & 2, & 6, & -19, & 17 \\ -5, & -15, & -8, & 13, & 2, & 6, & -19, & 17, & 14 \end{pmatrix}$$

$$\begin{pmatrix} -15, -8, 13, 2, 6, -19, 17, 14, 5 \\ -8, 13, 2, 6, -19, 17, 14, 5, 15 \\ 13, 2, 6, -19, 17, 14, 5, 15, 8 \\ 2, 6, -19, 17, 14, 5, 15, 8, -13 \\ 6, -19, 17, 14, 5, 15, 8, -13, -2 \\ -19, 17, 14, 5, 15, 8, -13, -2, -6 \\ 17, 14, 5, 15, 8, -13, -2, -6, 19 \end{pmatrix}$$

この場合は固有多項式は

$$(x+37)^4(x-37)^5$$

であり、最小多項式は

$$(x+37)(x-37)$$

となり、1/p·A は対合であるが、重複度は異なるので調和対合ではない。因子 x+1 の影響である。勿論、この場合は tr(1/p·A)= 1 である。

x^n+1 のような場合は、終結行列は巡回行列ではない。先頭の数が後ろに入るとき符号が変わる。このような行列を準巡回行列(pseudo-cyclic matrix)と呼ぶことにする。

i) x^3+1 の場合

$$\bar{a}_{12}(x)\,[x]\,x^3+1$$

$$=$$

$$\begin{pmatrix} 0, & -37, & 0 \\ -37, & 0, & 0 \\ 0, & 0, & 37 \end{pmatrix}$$

この場合も固有多項式は

$$(x+37)(x-37)^2$$

であり、最小多項式は

$$(x+37)(x-37)$$

となり、1/p·A は対合であるが、重複度は異なるので調和対合ではない。因子 x+1 の影響である。勿論、この場合も tr(1/p·A)= 1 である。

例 3. p = 47 の場合、p = 2·23+1 で、p-1 は素数 q = 23 の 2 倍である。

原始根は

[5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45]

であり、

$$a_{12}(x) = x^{(p+1)/4} F(7/12,11/12,1,1-x) = x^{12}(18x^3+36x^2+5x+36)$$

である。r＝5とすると、表現変換多項式は

$$\bar{a}_{12}(x) = 3x^{45}-9x^{44}+10x^{42}-6x^{41}-6x^{40}-2x^{39}-x^{38}-8x^{37}-4x^{36}+13x^{35}-8x^{34}-6x^{32}-4x^{31}+9x^{30}$$
$$-7x^{29}-8x^{28}-11x^{27}-3x^{26}+3x^{25}+9x^{24}+2x^{23}-12x^{22}+7x^{21}-8x^{20}-3x^{19}-12x^{18}-x^{17}+4x^{16}$$
$$+10x^{15}-5x^{14}+8x^{13}+2x^{12}+3x^{10}+12x^9+6x^8+8x^7-7x^6-6x^5-4x^4-6x^3+2x^2-12x+1$$

この場合 $x^{p-1}-1$ は既約因子の積への分解は次のようである：

$$x^{p-1}-1 = x^{46}-1 = (x-1)(x+1)$$
$$(x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1)$$
$$(1-x+x^2-x^3+x^4-x^5+x^6-x^7+x^8-x^9+x^{10}-x^{11}+x^{12}-x^{13}+x^{14}-x^{15}+x^{16}-x^{17}+x^{18}-x^{19}+x^{20}-x^{21}+x^{22})$$

である。次数の高い順に対合かどうか判定する。

a)　$x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$ の場合

$\bar{a}_{12}(x)\,[x]\,x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$

=

7, 1, 16, -9, 2, 11, 18, -4, 13, 24, 1, 12, 15, 11, 26, -5, -5, -6, 0, 14, 6, 12

-6, 9, -16, -5, 4, 11, -11, 6, 17, -6, 5, 8, 4, 19, -12, -12, -13, -7, 7, -1, 5, -7

15, -10, 1, 10, 17, -5, 12, 23, 0, 11, 14, 10, 25, -6, -6, -7, -1, 13, 5, 11, -1, 6

-25, -14, -5, 2, -20, -3, 8, -15, -4, -1, -5, 10, -21, -21, -22, -16, -2, -10, -4, -16, -9, -15

11, 20, 27, 5, 22, 33, 10, 21, 24, 20, 35, 4, 4, 3, 9, 23, 15, 21, 9, 16, 10, 25

9, 16, -6, 11, 22, -1, 10, 13, 9, 24, -7, -7, -8, -2, 12, 4, 10, -2, 5, -1, 14, -11

7, -15, 2, 13, -10, 1, 4, 0, 15, -16, -16, -17, -11, 3, -5, 1, -11, -4, -10, 5, -20, -9

-22, -5, 6, -17, -6, -3, -7, 8, -23, -23, -24, -18, -4, -12, -6, -18, -11, -17, -2, -27, -16, -7

17, 28, 5, 16, 19, 15, 30, -1, -1, -2, 4, 18, 10, 16, 4, 11, 5, 20, -5, 6, 15, 22

11, -12, -1, 2, -2, 13, -18, -18, -19, -13, 1, -7, -1, -13, -6, -12, 3, -22, -11, -2, 5, -17

-23, -12, -9, -13, 2, -29, -29, -30, -24, -10, -18, -12, -24, -17, -23, -8, -33, -22, -13, -6, -28,-11

11, 14, 10, 25, -6, -6, -7, -1, 13, 5, 11, -1, 6, 0, 15, -10, 1, 10, 17, -5, 12, 23

3, -1, 14, -17, -17, -18, -12, 2, -6, 0, -12, -5, -11, 4, -21, -10, -1, 6, -16, 1, 12, -11

-4, 11, -20, -20, -21, -15, -1, -9, -3, -15, -8, -14, 1, -24, -13, -4, 3, -19, -2, 9, -14, -3

15, -16, -16, -17, -11, 3, -5, 1, -11, -4, -10, 5, -20, -9, 0, 7, -15, 2, 13, -10, 1, 4

-31, -31, -32, -26, -12, -20, -14, -26, -19, -25, -10, -35, -24,-15, -8, -30,-13, -2,-25,-14,-11,-15

0, -1, 5, 19, 11, 17, 5, 12, 6, 21, -4, 7, 16, 23, 1, 18, 29, 6, 17, 20, 16, 31

-1, 5, 19, 11, 17, 5, 12, 6, 21, -4, 7, 16, 23, 1, 18, 29, 6, 17, 20, 16, 31, 0

6, 20, 12, 18, 6, 13, 7, 22, -3, 8, 17, 24, 2, 19, 30, 7, 18, 21, 17, 32, 1, 1

14, 6, 12, 0, 7, 1, 16, -9, 2, 11, 18, -4, 13, 24, 1, 12, 15, 11, 26, -5, -5, -6

-8, -2, -14, -7, -13, 2, -23, -12, -3, 4, -18, -1, 10, -13, -2, 1, -3, 12, -19, -19, -20, -14

6, -6, 1, -5, 10, -15, -4, 5, 12, -10, 7, 18, -5, 6, 9, 5, 20, -11, -11, -12, -6, 8

この場合、符号などの関係で行の記号列としての長さにアンバランスがある。しかし、1/p･A は調和対合である。

b) $1-x+x^2-x^3+x^4-x^5+x^6-x^7+x^8-x^9+x^{10}-x^{11}+x^{12}-x^{13}+x^{14}-x^{15}+x^{16}-x^{17}+x^{18}-x^{19}+x^{20}-x^{21}+x^{22}$ の場合

$\bar{a}_{12}(x)\,[x]\,1-x+x^2-x^3+x^4-x^5+x^6-x^7+x^8-x^9+x^{10}-x^{11}+x^{12}-x^{13}+x^{14}-x^{15}+x^{16}-x^{17}+x^{18}-x^{19}+x^{20}-x^{21}+x^{22}$

=

1, 7, -28, 9, -10, 21, -4, 18, -3, 4, -7, 18, 3, 25, -16, 15, -13, 22, -18, 14, -36, 14

8, -29, 10, -11, 22, -5, 19, -4, 5, -8, 19, 2, 26, -17, 16, -14, 23, -19, 15, -37, 15, -1

-21, 2, -3, 14, 3, 11, 4, -3, 0, 11, 10, 18, -9, 8, -6, 15, -11, 7, -29, 7, 7, -8

-19, 18, -7, 24, -10, 25, -24, 21, -10, 31, -3, 12, -13, 15, -6, 10, -14, -8, -14, 28, -29, 21

-1, 12, 5, 9, 6, -5, 2, 9, 12, 16, -7, 6, -4, 13, -9, 5, -27, 5, 9, -10, 2, 19

11, 6, 8, 7, -6, 3, 8, 13, 15, -6, 5, -3, 12, -8, 4, -26, 4, 10, -11, 3, 18, 1

17, -3, 18, -17, 14, -3, 24, 4, 5, -6, 8, 1, 3, -7, -15, -7, 21, -22, 14, 7, 12, -11

14, 1, 0, -3, 14, 7, 21, -12, 11, -9, 18, -14, 10, -32, 10, 4, -5, -3, 24, -5, 6, -17

15, -14, 11, 0, 21, 7, 2, -3, 5, 4, 0, -4, -18, -4, 18, -19, 11, 10, 9, -8, -3, -14

1, -4, 15, 6, 22, -13, 12, -10, 19, -15, 11, -33, 11, 3, -4, -4, 25, -6, 7, -18, 1, -15

-3, 14, 7, 21, -12, 11, -9, 18, -14, 10, -32, 10, 4, -5, -3, 24, -5, 6, -17, 0, -14, -1

11, 10, 18, -9, 8, -6, 15, -11, 7, -29, 7, 7, -8, 0, 21, -2, 3, -14, -3, -11, -4, 3

21, 7, 2, -3, 5, 4, 0, -4, -18, -4, 18, -19, 11, 10, 9, -8, -3, -14, 0, -15, 14, -11

28, -19, 18, -16, 25, -21, 17, -39, 17, -3, 2, -10, 31, -12, 13, -24, 7, -21, 6, -7, 10, -21

9, -10, 12, -3, 7, -11, -11, -11, 25, -26, 18, 3, 16, -15, 4, -21, 7, -22, 21, -18, 7, -28

-1, 3, 6, -2, -2, -20, -2, 16, -17, 9, 12, 7, -6, -5, -12, -2, -13, 12, -9, -2, -19, -9

2, 7, -3, -1, -21, -1, 15, -16, 8, 13, 6, -5, -6, -11, -3, -12, 11, -8, -3, -18, -10, 1

9, -5, 1, -23, 1, 13, -14, 6, 15, 4, -3, -8, -9, -5, -10, 9, -6, -5, -16, -12, 3, -2

4, -8, -14, -8, 22, -23, 15, 6, 13, -12, 1, -18, 4, -19, 18, -15, 4, -25, -3, -6, 7, -9

-4, -18, -4, 18, -19, 11, 10, 9, -8, -3, -14, 0, -15, 14, -11, 0, -21, -7, -2, 3, -5, -4

-22, 0, 14, -15, 7, 14, 5, -4, -7, -10, -4, -11, 10, -7, -4, -17, -11, 2, -1, -1, -8, 4

-22, 36, -37, 29, -8, 27, -26, 15, -32, 18, -33, 32, -29, 18, -39, 11, -20, 21, -23, 14, -18, 22

この場合も 1/p･A は調和対合である。

c)　x+1, x-1 の場合

$$\bar{a}_{12}(x)[x]_{x+1} = (-47) \qquad \bar{a}_{12}(x)[x]_{x-1} = (-47)$$

この場合も符号は同調している。

恐らくは、応用の広いと思われる巡回対合(cyclic involution)の場合について述べる。

d)　$x^{23}-1$ の場合

$$\bar{a}_{12}(x)[x]_{x^{23}-1} =$$

-9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3
-2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9
-8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2
7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8
-18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7
-7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18
2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7
9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2
-13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9
4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13
15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4
-8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15
3, 6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8
6, 2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3
2, 17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6
17, -14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2
-14, -14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17
-14, -15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14
-15, -9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14
-9, 5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15
5, -3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9
-3, 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5

$$\lfloor\ 3, -9, -2, -8, 7, -18, -7, 2, 9, -13, 4, 15, -8, 3, 6, 2, 17, -14, -14, -15, -9, 5, -3\ \rfloor$$

この行列の固有多項式は

$$(x-47)^{11}(x+47)^{12}$$

で最小多項式は

$$(x-47)^{1}(x+47)$$

であり、自己共役(逆行)巡回行列である。表現として長さが変わらないのは同じ数値が頭から後ろに移動するだけだからである。勿論、1/p・A は対合である。

実は、p = 12n+11 の形の素数では

$$1/p\cdot\bar{a}_{12}(x)\,[x]\,x^{p-1}-1$$

は常に巡回対合である。例えば、p = 11 でも勿論その通りなのであるが、11 < 17 で、形式的には $\bar{a}_{12}(x)$ は絶対値最小剰余としては一意的には決定できない可能性がある。

しかし、その自由さは少なく、期待される一般的な性質から、少ない可能性のうちに絞られるのである。一意性が保証されないということは、自然が基本的な部分で多様性と多義性をもつことを意味する。

その、多様性と多義性こそ、自然が見せてくれる最高の風景ではないだろうか。

例 4.　p = 13 の場合。この場合は 17 より小さい最大の場合である。

原始根は

$$[2, 6, 7, 11]$$

であり、

$$a_{12}(x) = x^{(p-1)/4}F(1/12,5/12,1,1-x) = x^3(8x+6)$$

その値は

$$[0, 1, -6, 4, 1, 4, 3, -2, -1, 0, 5, 2, 2]$$

である。Hasse の限界は

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

であるから、-6 = 7 のみが、可能性のある他の選択である。

1. -6 の場合

r = 2 とすると、表現変換多項式は

$$\bar{a}_{12}(x) = -2x^{11}+5x^{10}+4x^9+2x^7+2x^6+3x^5+4x^4-x^3+x^2-\underline{6}x+1$$

であり、この式は既約である。mod 13 では完全分解して、

$$11\,(1+x)\,(x+9)\,(x+7)\,(x+12)\,(x+5)\,(x+2)\,(x+10)\,(x+3)^2\,(x+11)\,(x+6)$$

これも、何か、真のものであることを感じさせる。

この場合 $x^{p-1}-1$ の既約因子分解は

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

である。

a) x^4-x^2+1 の場合

$$\bar{a}_{12}(x)\,[x]\,x^4-x^2+1$$

$$=$$

$$\begin{pmatrix} 0, & 0, & -13, & 0 \\ 0, & -13, & 0, & 0 \\ -13, & 0, & 0, & 0 \\ 0, & -13, & 0, & 13 \end{pmatrix}$$

であり、$1/p\cdot A$ は調和対合で -6 は先ずこの期待される性質をもっているので真と思われる。b) $1-x+x^2$ の場合

$$\bar{a}_{12}(x)\,[x]\,1-x+x^2$$

$$=$$

$$\begin{pmatrix} -13, & 0 \\ -13, & 13 \end{pmatrix}$$

以下、特に、$1/p\cdot A$, $1/\sqrt{p}\cdot A$ が対合である場合には、行列を提示するだけに止める。

c) x^2+x+1 の場合

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

d) x^2+1 の場合

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

e) $x+1$, $x-1$ の場合、それぞれ

$$(13) \qquad (13)$$

2. $-6 = 7$ を採用したとき、

$$\bar{a}_{12}(x) = -2x^{11}+5x^{10}+4x^9+2x^7+2x^6+3x^5+4x^4-x^3+x^2+\underline{7}x+1$$

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

mod 13 で完全分解することは、-6 = 7 のどちらを採用しても不変である。

a)　x^4-x^2+1 の場合

$$\bar{a}_{12}(x)\,[x]\,x^4-x^2+1$$

$$=$$

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

と、完全に退化してしまう。

b)　$1-x+x^2$ の場合

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

c)　x^2+x+1 の場合

$$\begin{pmatrix} 16, & 4 \\ -12, & -16 \end{pmatrix}$$

固有多項式は x^2-208, $208 = 2^4 \cdot 13$ である。1/13・A は対合ではない。後は、もう調べないが 7 は不自然であると思う。

原始根として r = 6 の場合も

$$\bar{a}_{12}(x)\,[x]\,x^4-x^2+1$$

$$=$$

$$\begin{pmatrix} -13, & 0, & 13, & 0 \\ 0, & 0, & 0, & 13 \\ 0, & 0, & 13, & 0 \\ 0, & 13, & 0, & 0 \end{pmatrix}$$

などと基本の構造は変わらない。

例 5.　　p = 11 の場合。原始根は

$$[2, 6, 7, 8]$$

である。

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

により r = 2 のとき、$2\sqrt{13} = 6.633249580\cdots$

$$\bar{a}_{12}(x) = -4x^9+\underline{5}x^8+2x^7+3x^6-x^5+4x^4-\underline{5}x^3-2x^2-3x+1$$

に於いて 5 = -6 が可能性がある。この場合 2 個そのような場所がある。

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

$$-4x^9-6x^8+2x^7+3x^6-x^5+4x^4-5x^3-2x^2-3x+1= \text{irred.}$$

$$-4x^9+5x^8+2x^7+3x^6-x^5+4x^4+6x^3-2x^2-3x+1= \text{irred.}$$

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

であり、円分多項式分解は

$$x^{p-1}-1 = x^{10}-1 = (x-1)(x+1)(x^4+x^3+x^2+x+1)(x^4-x^3+x^2-x+1)$$

である。5 を-6 に 1 個だけ換えたものは 2 式あり共に既約である。(従って、互いに素)

a) $\bar{a}_{12}(x) = -4x^9-6x^8+2x^7+3x^6-x^5+4x^4-5x^3-2x^2-3x+1$ の場合

a1) $x^4+x^3+x^2+x+1$ の場合

$$\bar{a}_{12}(x)\,[x]\,x^4+x^3+x^2+x+1$$

$$=$$

$$\begin{pmatrix} -11, & 0, & 0, & 0 \\ 11, & 11, & 11, & 11 \\ 0, & 0, & 0, & -11 \\ 0, & 0, & -11, & 0 \end{pmatrix}$$

であり、1/p･A は調和対合である。

a2) $x^4-x^3+x^2-x+1$ の場合

$$\begin{pmatrix} 9, & -12, & 2, & -6 \\ -3, & -7, & 3, & -9 \\ -10, & 6, & -12, & 3 \\ -4, & -2, & -7, & 10 \end{pmatrix}$$

これも、1/p･A は調和対合である。

a3) x+1, x-1 の場合、それぞれ

(11)　　(-11)

である。この場合は符号が異なっている。事実、

$$\bar{a}_{12}(x)\,[x]\,x^2-1$$

$$=$$

$$\begin{pmatrix} -11, & 0 \\ 0, & -11 \end{pmatrix}$$

は調和、つまり、固有値の和が 0 ではない。

a4) x^5-1 の場合、巡回対合の場合

$$\bar{a}_{12}(x)\,[x]\,x^5-1$$

$$=$$

$$\begin{pmatrix} 0, & -11, & 0, & 0, & 0 \\ -11, & 0, & 0, & 0, & 0 \\ 0, & 0, & 0, & 0, & -11 \\ 0, & 0, & 0, & -11, & 0 \\ 0, & 0, & -11, & 0, & 0 \end{pmatrix}$$

で、確かに、1/p･A は巡回対合であるが、面白みのないものである。

a5)　$x^{10}-1$ の場合

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

$$=$$

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

この場合も 1/p･A は調和巡回対称対合である。小さな数を一度だけ用いて見事に織り上げられていると思う。このような作品が(自然のなかに)存在していたのである。

b)　$-4x^9+5x^8+2x^7+3x^6-x^5+4x^4+6x^3-2x^2-3x+1$ の場合

b1)　$x^4+x^3+x^2+x+1$ の場合

$$\bar{a}_{12}(x)\,[x]\,x^4+x^3+x^2+x+1$$

$$=$$

$$\begin{pmatrix} 11, & 0, & 0, & 0 \\ -11, & -11, & -11, & -11 \\ 0, & 0, & 0, & 11 \\ 0, & 0, & 11, & 0 \end{pmatrix}$$

b2)

$$\begin{pmatrix} 9, & -12, & 2, & -6 \\ -3, & -7, & 3, & -9 \\ -10, & 6, & -12, & 3 \\ -4, & -2, & -7, & 10 \end{pmatrix}$$

など同じような複雑さである。巡回対合も同一である。

c)　x^{10}-1 の場合も

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

$$=$$

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

であり、初めの場合と符号と順序が変わっている。内部構造の微妙なねじれまでは今は言及できない。

例えば、p＝23 では

$$\begin{pmatrix} -3, -8, -5, 1, 8, 4, 0, 2, -2, 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1 \\ -8, -5, 1, 8, 4, 0, 2, -2, 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1, -3 \\ -5, 1, 8, 4, 0, 2, -2, 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1, -3, -8 \\ 1, 8, 4, 0, 2, -2, 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1, -3, -8, -5 \\ 8, 4, 0, 2, -2, 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1, -3, -8, -5, 1 \\ 4, 0, 2, -2, 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1, -3, -8, -5, 1, 8 \\ 0, 2, -2, 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1, -3, -8, -5, 1, 8, 4 \\ 2, -2, 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1, -3, -8, -5, 1, 8, 4, 0 \\ -2, 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1, -3, -8, -5, 1, 8, 4, 0, 2 \\ 3, -4, -6, 4, -7, 9, -1, -6, -6, 3, -6, -4, 1, -3, -8, -5, 1, 8, 4, 0, 2, -2 \end{pmatrix}$$

$$\left\{\begin{array}{l}
-4,\ -6,\ 4,\ -7,\ 9,\ -1,\ -6,\ -6,\ 3,\ -6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3 \\
-6,\ 4,\ -7,\ 9,\ -1,\ -6,\ -6,\ 3,\ -6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4 \\
4,\ -7,\ 9,\ -1,\ -6,\ -6,\ 3,\ -6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6 \\
-7,\ 9,\ -1,\ -6,\ -6,\ 3,\ -6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6,\ 4 \\
9,\ -1,\ -6,\ -6,\ 3,\ -6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6,\ 4,\ -7 \\
-1,\ -6,\ -6,\ 3,\ -6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6,\ 4,\ -7,\ 9 \\
-6,\ -6,\ 3,\ -6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6,\ 4,\ -7,\ 9,\ -1 \\
-6,\ 3,\ -6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6,\ 4,\ -7,\ 9,\ -1,\ -6 \\
3,\ -6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6,\ 4,\ -7,\ 9,\ -1,\ -6,\ -6 \\
-6,\ -4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6,\ 4,\ -7,\ 9,\ -1,\ -6,\ -6,\ 3 \\
-4,\ 1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6,\ 4,\ -7,\ 9,\ -1,\ -6,\ -6,\ 3,\ -6 \\
1,\ -3,\ -8,\ -5,\ 1,\ 8,\ 4,\ 0,\ 2,\ -2,\ 3,\ -4,\ -6,\ 4,\ -7,\ 9,\ -1,\ -6,\ -6,\ 3,\ -6,\ -4
\end{array}\right\}$$

が存在するが、11 の場合の方により美しさを感ずるのは自分だけであろうか。

例 6.　p = 7 の場合。原始根は[3, 5]である。

$$a_{12}(x) = x^{(p-1)/4} F(7/12,11/12,1,1-x) = x^2$$

により r = 3 のとき、$2\sqrt{7} = 5.291502622\cdots$

$$\bar{a}_{12}(x) = -3x^5+2x^4+x^3-3x^2+2x+1$$

である。この範囲で-3 = 4, 2 = -5 と変化し得る。このような場所は 4 個存在するから、$2^4 = 16$ 個の式を検討する必要がある。一般的に既約なものを探せばよいであろうと思う。

$$-3x^5+2x^4+x^3-3x^2-5x+1,\quad -3x^5+2x^4+x^3+4x^2+2x+1,\quad -3x^5-5x^4+x^3+4x^2-5x+1$$
$$-3x^5-5x^4+x^3-3x^2+2x+1,\quad 4x^5+2x^4+x^3-3x^2+2x+1,\quad 4x^5+2x^4+x^3+4x^2-5x+1$$
$$4x^5-5x^4+x^3-3x^2-5x+1$$

の 7 個は既約である。

また、円分分解は

$$x^6-1 = (x+1)(x-1)(x^2+x+1)(x^2-x+1)$$

である。x^2+x+1 からは、対合が生ずるということ等に注意して確かめる。

$$1/7\cdot\bar{a}_{12}(x)\ [x]\ x^2+x+1$$

すべて対合になる。また、x^2-x+1 の場合

$$-3x^5+2x^4+x^3-3x^2-5x+1,\quad -3x^5-5x^4+x^3-3x^2+2x+1$$
$$\bar{a}_{12}(x)\ [x]\ x^2-x+1$$

=

$$\begin{pmatrix} 3, & 8 \\ 5, & -3 \end{pmatrix}$$

であり、1/p･A が対合になっている。

また、x^3-1 との関連では

$$-3x^5+2x^4+x^3-3x^2-5x+1,\quad -3x^5-5x^4+x^3-3x^2+2x+1$$

ともに

$$\bar{a}_{12}(x)\,[x]\,x^3-1$$

=

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

であり、1/p･A が巡回対合になる。さらに、x^3+1 との関連では

$$\begin{pmatrix} 0, & 7, & 0 \\ 7, & 0, & 0 \\ 0, & 0, & -7 \end{pmatrix}$$

1/p･A が準巡回対合になる。従って x^3-1 との関連では

$$\bar{a}_{12}(x)\,[x]\,x^6-1$$

=

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

は 1/p･A が巡回対合になる。これらの行列は極小性という意味で固有の美しさを備えているのであろう。

一般には x^2-x+1 では、$1/\sqrt{p}$･A が対合になるのが普通である。

$$-3x^5+2x^4+x^3+4x^2+2x+1$$

$$4x^5+2x^4+x^3-3x^2+2x+1$$

$$\bar{a}_{12}(x)\,[x]\,x^2-x+1$$

=

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

の特性方程式は x^2-7 であり、期待されるように $1/\sqrt{p}\cdot A$ が対合になる。これら、二組の異なる性質をもつ対の登場は興味のあることである。

例 7.　$p=5$ の場合。原始根は[2, 3]である。

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

により $r=2$ のときを考える。$2\sqrt{5} = 5.291502622\cdots$

$$\bar{a}_{12}(x) = -2x^3-x^2+2x+1$$

である。$0 = 5 = -5,\ 1 = -4,\ 2 = -3$ などであるから、$3\times 2^4 = 48$ 通りも考えられる。

これらの式で

$$\bar{a}_{12}(x)\,[x]\,x^2+1,\quad \bar{a}_{12}(x)\,[x]\,x^2-1$$

の $1/p,\ 1/\sqrt{p}$ が対合になるものは、それぞれ 2 個づつ

$$-5x^4-2x^3-x^2+2x+1, \qquad -2x^3-x^2+2x-4$$

$$-2x^3+4x^2+2x+1 \qquad 5x^4-2x^3+4x^2+2x-4$$

$$\bar{a}_{12}(x)\,[x]\,x^2+1 \qquad \bar{a}_{12}(x)\,[x]\,x^2-1$$

$$= \qquad =$$

$$\begin{pmatrix} 4, & -3 \\ -3, & -4 \end{pmatrix} \qquad \begin{pmatrix} 0, & -5 \\ -5, & 0 \end{pmatrix}$$

$$\begin{pmatrix} 4, & -3 \\ -3, & -4 \end{pmatrix} \qquad \begin{pmatrix} 0, & 5 \\ 5, & 0 \end{pmatrix}$$

$$5x^4+3x^3-x^2+2x-4, \qquad 3x^3-x^2+2x+1$$

$$-2x^3-x^2-3x+1, \qquad 5x^4-2x^3-x^2-3x-4$$

$$\bar{a}_{12}(x)\,[x]\,x^2+1 \qquad \bar{a}_{12}(x)\,[x]\,x^2-1$$

$$= \qquad =$$

$$\begin{pmatrix} -1, & 2 \\ 2, & 1 \end{pmatrix} \qquad \begin{pmatrix} 5, & 0 \\ 0, & 5 \end{pmatrix}$$

$$\begin{pmatrix} -1, & 2 \\ 2, & 1 \end{pmatrix} \qquad \begin{pmatrix} -5, & 0 \\ 0, & -5 \end{pmatrix}$$

が対応している。x^4-1 についても巡回行列

$$\bar{a}_{12}(x)\,[x]\,x^4-1$$

$$=$$

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

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

などが得られる。大きな素数の一般的な性質から小さい素数に移ってゆくとき、どのような多様性が現れるか見たかったのである。

例 7.　p = 3 の場合。原始根は[2]である。

これは、もう、F(1/12,5/12,1,1-x)，F(7/12,11/12,1,1-x)の系列には属さない。

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

r = 2 である。また、$2\sqrt{3} = 3.464101616\cdots$ である。

$$\bar{a}_{12}(x) = -x+1$$

この係数の範囲では、-3 = 0 = 3, -2 = 1, -1 = 2 などの可能性がある。それらの多項式から生ずる

$$\bar{a}_{12}(x)\,[x]\,x^2-1$$

の固有多項式の因子が x^2-3, $x\pm3$, $x\pm1$ のものは

$$-3x^2-x+1, \quad -x-2$$

$$\begin{pmatrix} -1, & -2 \\ -2, & -1 \end{pmatrix} (x+3)(x-1)$$

$$3x^2+2x-2, \quad 2x+1$$

$$\begin{pmatrix} 2, & 1 \\ 1, & 2 \end{pmatrix} (x-1)(x-3)$$

の 2 個づつの 2 組で、もう、固有方程式が x^2-3 のものも(x+3)(x-3)，$(x\pm3)^2$ のものも存在しない世界であった。

任意の自然数は高々 4 個の整数の自乗の和であるというラグランジュの定理も p = 3 の世界では通用しないのである。

一般法則を拠り所に,、小さい素数へと追求していって到達した点は「概念」の消滅であった。逆に歴史を“遡れば”概念の登場のクロノグラフということができるであろうか…。歴史の原義は *historia* = narrative history, *histor* = learned, wise man などであるという。

4. 対合と終結変換

終結変換と対合について考えてみる。ことの本質は、絶対値を不変にする変換ということである。

例を p = 11 の場合の

$$f(x) = \bar{a}_{12}(x) = -4x^9-6x^8+2x^7+3x^6-x^5+4x^4-5x^3-2x^2-3x+1$$

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

にとって見よう。

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

であるから、g(x)= 0 の解を a とすれば、a は 1 の原始 5 乗根の冪である。終結式

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

は、勿論、y の 4 次式で、g(x)= 0 の解を f(x)に代入したものを根にもつ多項式である。

具体的には

$$y-f(x) \textcircled{x} g(x) = y^4+y^3-209y^2+121y+14641$$

である。14641= 11^4 であるから、すべての解の絶対値が 11 であるというのと矛盾はしないが、まだその証明というのには十分でない。しかし、

$$y^4+y^3-209y^2+121y+14641 = (y^2+(1+19\sqrt{5})/2\cdot y+121)(y^2+(1-19\sqrt{5})/2\cdot y+121)$$

であり、両因数が実根をもたないことが解れば、解の絶対値がすべて絶対値 11 であることは了解するであろう。

ここでの方法はもっと直接的である。行列としての終結行列

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

$$=$$

$$\begin{pmatrix} 9, & -12, & 2, & -6 \\ -3, & -7, & 3, & -9 \\ -10, & 6, & -12, & 3 \\ -4, & -2, & -7, & 10 \end{pmatrix}$$

の意味は、例えば、第一行は f(x)を g(x)で割った 3 次の剰余

$$f(x) = (-4x^5-10x^4-4x^3+5x^2+2x+7),\quad g(x) = 9x^3-12x^2+2x-6$$

の係数を順に記したものであり、次の行は xf(x)の g(x)による剰余と順に x を掛けたものの剰余であることに注意する。式

$$x^n f(x) = h_n(x)\,g(x)+r_n(x)$$

に於いて、

$$g(x)=0 \rightarrow |x|=1$$

であるから、$g(x)=0$ ならば

$$|f(x)|=|x^n f(x)|=|r_n(x)|$$

なのである。1/11・A が対合であるということは

$$A^2=11^2E$$

でもあり、A の固有値が ±11 であることを意味している。x に関する終結行列としては、y は定数として扱うから、

$$\det(yE-f(x)\textcircled{x}g(x))=y-f(x)\textcircled{x}g(x)=y^4+y^3-209y^2+121y+14641$$

である。しかし、今の場合は

$$A=f(x)[x]g(x)$$

であり、この場合は

$$\det(yE-f(x)[x]g(x))=(y-11)^2(y+11)^2$$

となり、解の絶対値は等しいが、既約性等に於いては著しい差があるのである。

また、行列式の意味に立ち戻れば、例えば、S を反対角行列として

$$|Sy-A|$$

$$=$$

$$\begin{vmatrix} -9 & 12 & -2 & y-6 \\ 3 & 7 & y-3 & 9 \\ 10 & y-6 & 12 & -3 \\ y-4 & 2 & 7 & -10 \end{vmatrix} = \begin{vmatrix} -9 & 12 & -2 & y-f(x) \\ 3 & 7 & y-3 & x(y-f(x)) \\ 10 & y-6 & 12 & x^2(y-f(x)) \\ y-4 & 2 & 7 & x^3(y-f(x)) \end{vmatrix}$$

$$x^3 \quad x^2 \quad x \quad 1$$

のように共通因数として、$g(x)=0$ のときには、$y-f(x)$ を括り出すことができるのである。また、勿論、

$$f(x)\textcircled{x}g(x)=S(f(x)[x]g(x))$$

である。

ユニタリー変換 S で、固有値の絶対値が不変であることは知られているが、この場合に即した偏角の変換の具体的な公式は(今の私は)知らないが、恐らく、ほとんど常識に属する良く知られた公式であろうが、計算の複雑性などと関係して非常に興味なある研究課題であろうと思う。

Donald E. Knuth, *The art of computer programming.* Vol.2 Seminumerical Algorithms.

Third ed.1998,

Henri Cohen, *A Course in computational algebraic number theory*. Grad, Texts in Math. 138. Springer-Verlag. 1993

などでも、FFT などの概念は登場するものの反転の問題は深入りしていない。しかし、私は、この問題は非常に本質的な問題で、我々の空間の時間の方向が定まっていることも関係してると思っている。つまり、時系列を反転するためには非常に高い次元の空間とそのなかの組織化された実体が必要であることを意味しているのかも知れない。

時系列の反転の問題は、歴史的には、高速フーリエ変換のところでもしばしば本質的問題となった部分である。

話は戻って、

$$|Sy-A| = |S||Ey - SA|$$

であるが、S は対称な対合であるから、平方根

$$\sqrt{S}$$

をもつ。$\sqrt{S}$ の例の一つは、

$$\sqrt{S} = (1+i)/2 \cdot E + (1-i)/2 \cdot S$$

$$\begin{pmatrix} (1+i)/2, & 0, & 0, & (1-i)/2 \\ 0, & (1+i)/2, & (1-i)/2, & 0 \\ 0, & (1-i)/2, & (1+i)/2, & 0 \\ (1-i)/2, & 0, & 0, & (1+i)/2 \end{pmatrix}$$

のような形の行列である。奇数次の場合、中心の元は 1 である。

今までのことを総合して書けば、予想として、

$y-f(x)\,[x]\,x^{p-1}-1$

p mod 12	$y-f(x)\,[x]\,x^{p-1}-1$	最小多項式
1	$(x^2-p)^2(x-p)^{(p-7)/2}\ (x-p)^{(p-3)/2}$	$(x^2-p)(x^2-p^2)$
5	$(x^2-p)(x^2-p^2)^{(p-3)/2}$	$(x^2-p)(x^2-p^2)$
7	$(x^2-p)(x^2-p^2)^{(p-3)/2}$	$(x^2-p)(x^2-p^2)$
11	$(x^2-p^2)^{(p-1)/2}$	x^2-p^2

$y-f(x)\,\textcircled{x}\,x^{p-1}-1$

p mod 12	1	5	7	11
x^p-1	$(x^2+1)(x^2+x+1)$	x^2+1	x^2+x+1	-

$y\text{-}f(x)$ ⊛ $x^{p-1}\text{-}1$　　$(x^2\text{-}p)^2$　　$x^2\text{-}p$　　$x^2\text{-}p$　　-

のような表を得る。x^2+1 はガウス整数の退化、x^2+x+1 はアイゼンスタインの整数による退化である。

この退化によって、例えば、$\sin^2$-予想でも、偏角 0 の付近に Gibbs の現象に近い影響を与えると思う。より高い種数の超楕円曲線の $\sin^2$-予想でも、π の種数以下の等分点の近くでこのような、標本数の平方根程度の“ゆらぎ”として観測されるであろう。

反転の概念と聞くと、先ず一番に思い出すのは、恐らくは、フーリエ(Fourier)の行列、つまり、1 の原始 n 乗根で生成されるファンデルモンドの行列

$$F = 1/\sqrt{n}\cdot\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a & a^2 & \cdots & a^{n-1} \\ 1 & a^2 & a^4 & \cdots & a^{n-2} \\ & \cdots & & \cdots & \\ 1 & a^{n-1} & a^{n-2} & \cdots & a \end{pmatrix}$$

であろう。その自乗は、0 を除く n-1 個の元の順序の反転

$$F^2 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ & \cdots & & \cdots & \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$$

であり、F の逆元 F^{-1} は a の逆元 a^{-1} で生成されるフーリエ行列

$$F^{-1} = 1/\sqrt{n}\cdot\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a^{-1} & a^{-2} & \cdots & a \\ 1 & a^{-2} & a^{-4} & \cdots & a^2 \\ & \cdots & & \cdots & \\ 1 & a & a^2 & \cdots & a^{-1} \end{pmatrix}$$

である。勿論、$F^4 = E$ であって、丁度、1 の原始 4 乗根、つまり、虚数単位 $i = \sqrt{-1}$ に相当する役割をもっている。我々の場合ぼ反転行列 S は p-1 次の行列であり、表現多項式は原始根の冪、つまり、体

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

の 0 でない元の全体の値をを対象とした多項式であったから、0 での値は

無視している。恐らく、自然な真の記述の一つでは、0 での値も考慮に入れた(複素数体などの)原始 p 乗根を本質的に用いるものであろう。

事実、p-1 次順行型巡回行列を含む、次のような p 次正方行列

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

の固有多項式は $x^p-x = x(x^{p-1}-1)$ である。

p-1 個の元の巡回置換は、適当な一つの元を固定した形で p の置換とみなされる。原始根の冪乗の順序に項

$$f(b^n)$$

を並べることは、$b^n \neq 0$ であるから、f(0)は固定(無視)して、ということを言外に含んでいる。このような巡回行列が、フーリエ行列 F を通じて、1 の原始 p-1 乗根の冪乗を対角線上にもつ対角行列 T と

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \cdots & & \cdots & \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix} = F^3 \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & a & 0 & \cdots & 0 \\ & & \cdots & & \\ 0 & 0 & 0 & \cdots & a^{-1} \end{pmatrix} F$$

の形で結ばれており、

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

順送り行列と F^2 の積が、列の順序反転になっている。つまり、

$$F^3TFF^2 = F^3TF^3 = S$$

である。$F^3 = F^{-1}$ であり、それ自身は a^{-1} で生成されるフーリエ行列であるから、T から

$$T = FSF$$

といっても同じである。要は、これらの変換が

$$A \rightarrow P^{-1}AP$$

の変換でなくて、

$$A \rightarrow {}^tPAP$$

の形の変換、つまり、所謂、符号数(signature)と絶対値を不変量としていたことであった。対応する微分方程式は

$$X' = AX-XA$$

及び

$$X' = AX+XA$$

の形の方程式で、両者は'PAP の形の変換で結びついていたのである。

5. 円分多項式の既約分解と係数

円分多項式、例えば、p = 19 のとき

$$x^{19}-x = x(x^{18}-1) = x(x-1)(x+1)(x^2+x+1)(x^2-x+1)(x^6+x^3+1)(x^6-x^3+1)$$

のような既約因数分解をもつ。この場合、任意の既約因子、例えば、

$$x^6+x^3+1$$

の係数の集合は、常に 0 または ±1、つまり

$$\{-1,0,1\}$$

である。小さな数で確かめてみると確かにそうである。しかし、これは一般的なことであろうか…と思うのは自然なことであろう。

そして、すぐに、一般には、そうとは限らないことが解る。でも、最低限、無限にそのようなものが存在するとか、正の割合で存在するとか、ほとんどそうでないというようなことが解るのであろうか。

以下のグラフは、$x^n-x = x(x^{n-1}-1)$の因数の係数の集合を記したものである。例えば、

$$[106, [-2, -1, 0, 1]], [211, [-2, -1, 0, 1, 2]]$$

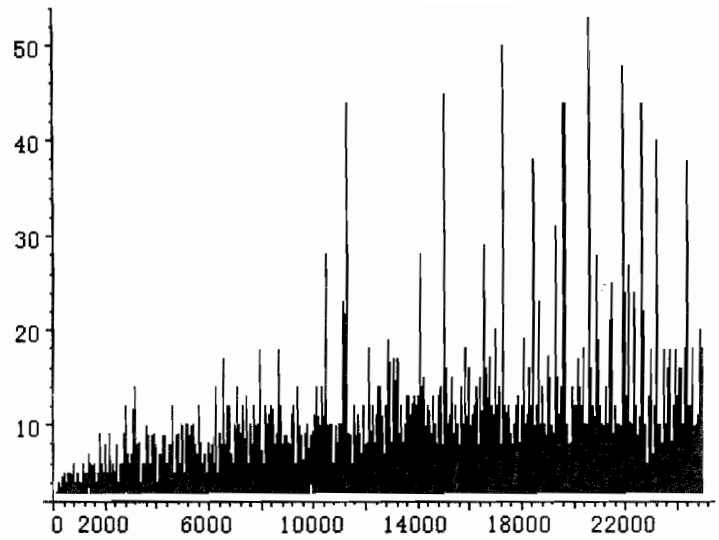
$$[7736, [-7, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5]$$

の場合のように、n = 106 = 2·53 は絶対値 2 のものが最初に現れる数でこの場合、最小と最大の差は 3 である。

n = 211 では最大から最小を引いたものは 4 である。n = 7736 は係数の全体が整数の区間をなさない最小数で差は 12 である。

グラフは n ≤ 25000 での、n と最小と最大の差 s の対を plot したものである。

$$[n,s], n \le 25000$$



具体的には、例えば n = 106 の場合の $x^{106}-x = x(x^{105}-1)$ について、

$$x^{105}-1 =$$

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

$$(x^{12}-x^{11}+x^9-x^8+x^6-x^4+x^3-x+1)(x^{24}-x^{23}+x^{19}-x^{18}+x^{17}-x^{16}+x^{14}-x^{13}+x^{12}-x^{11}+x^{10}-x^8+x^7-x^6+x^5-x+1)$$

$$(x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-2x^{41}-x^{40}-x^{39}+x^{36}+x^{35}+x^{34}+x^{33}+x^{32}+x^{31}-x^{28}$$

$$-x^{26}-x^{24}-x^{22}-x^{20}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}-x^9-x^8-2x^7-x^6-x^5+x^2+x+1)$$

であり、最大次数の既約因子のなかに、0, ±1 でない係数が $-2x^{41}$, $-2x^7$ の形で出ている。

また、例えば、中央付近の高いピークは n = 11306 = 2・5653 で、係数として現れる数字は

[-21, -20, -19, -18, -17, -16, -15, -14, -13, -12, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1,

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 23]

であり、22 は現れていない。当然の予想であるが、任意の長さの整数の区間を、円分多項式の既約因子の係数の集合として含むものが存在するであろうし、また、係数の集合が多数の区間の和になるものもあるであろう。

次のグラフは、$n \le 25000$ での、係数の集合が {-1,0,1} と“ならない”もの、つまり、係数に絶対値 1 より大きいものを含む n の個数 k(n) との比

$$r(n) = k(n)/n$$

について、n は対数をとって、対

$$[\log(n), k(n)/n]$$

の点を表示したものである。例えば、n = 25000 の所では、5175 個で、比率

は

$$5175/25000 = 0.207, \quad \log(25000) = 10.12663110 \cdots$$

である。これが、右上の端の点

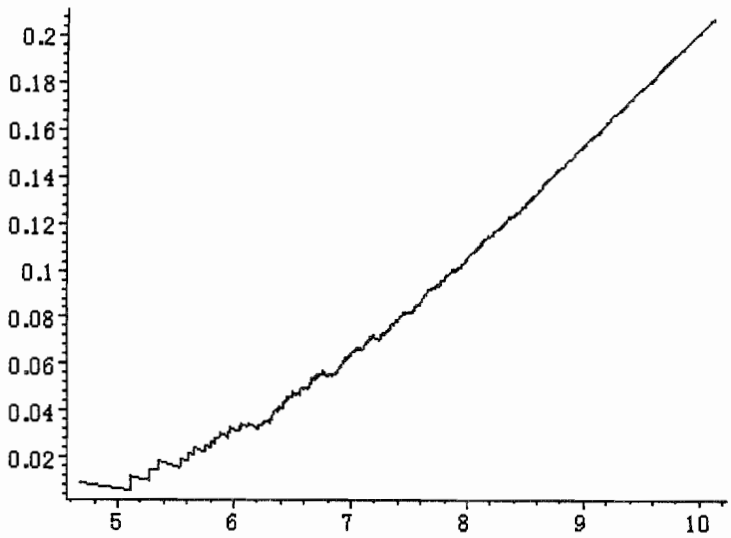
$$[10.126 \cdots, 0.207]$$

である。

これは、比率のグラフであるから、この程度のデータから直線の近似をしたら、とんでもない間違いを犯すことは明白である。n を大きくしても決して比は 1 を越えることはないからである。この極限が 1 であるか、それより小さいかは問題である。絶対値が 1 で収まるものは無限個であろうけれども、その比は任意に小さくなるであろう、つまり、

$$\lim k(n)/n = 1$$

というのを一応の予想としておこう。皆さんはどのように予想するであろうか。



6. 種数2の超楕円曲線と $\sin^2$-θ 予想

先ず、楕円曲線の場合のことですが、

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

について、有限素体

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

上の群（Poincaré-Mordell の群）としての位数が、本質的には、j 不変量（j-invariant）

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

を通じて

$$a_{12}(x) = \begin{cases} x^{(p-1)/4} F(1/12,5/12,1,1-x) & \text{if } p = 1 \bmod 4 \\ x^{(p+1)/4} F(7/12,11/12,1,1-x) & \text{if } p = -1 \bmod 4 \end{cases}$$
$$= x^{[p/4]} P_{[p/6]}(\sqrt{x})$$

などと書けると云いましたが、勿論、何か“怪しさ”を感じられたのではないでしょうか。

先ず、有理数体 Q、実数体 R、複素数体 C などの標数 0（characteristic 0）の体では、

$$F(1/12,5/12,1,1-x)$$

等については、そもそも、無限級数で収束半径など、まして、その正確な値を計算することの複雑さなど“煩わしさ”が頭をかすめるのが常識だろうと思う。…少なくとも私はそうである。

そして、その値を mod p で計算するといっても、大体、求めようとする群の位数は

$$n_p = 1+a_p+p$$
$$|a_p| < 2\sqrt{p}$$

であって、p での剰余の類と「相性」が…“どうも、教養のないものは…兎も角…話にならん”と感ずるのが正常であろうと思う。それに、

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

のなかの、$x^{(p-1)/4}$ と 1-x の位置も…何やら怪しい（= 怪しからん = 怪しくあるらん = 怪しいものだなあ（口語訳））と感ずるのが正常です。

そこです！、つまり、（裏に何か、今は説明できないけれど…）“ある”と思うことのできる「現実」の現象を探すことです。

これが、存在の認識の萌芽なのです。やり方は、現実に存在するものを、

一つづつ、これは(求めている「それ」では)“ない”と否定してゆくことです。それでも、否定しきれないものがやがてでてくるかも知れません。それこそ“問うて”いるものの候補です。大切に“残して”おきましょう。やがて光を発するときがあるかも知れません。どんなものも見なければ、観えてこないのです。十牛図の尋ねて…跡を見るでしょうか。

つまり、“何か”から“何が”に変わる瞬間を見ることでしょうか。兎も角、これは夢ですが…何かありそうな(…と私が(も？、かつて)感じた)話なのです。

さて、ここでの話は、超楕円曲線ですから、5次式の場合で

$$y^2 = x^5+ax^4+bx^3+cx^2+dx+e$$

の解の個数を、有限体 $F_p = GF(p)$ の代数拡大(algebraic extension)で考えようというのです。今の場合は2次の拡大であるが…。

まず、整数は、最高の次数の係数が1の2次方程式

$$x^2+ux+v = 0$$

で特徴付けられる。だから、

$$K = F_p[x]/(x^2+ux+v)$$

と考えるのが自然でしょう。x^2+ux+v が既約ならば、この体は p^2 の個数の元をもっている。さて、この体で

$$x^2+ux+v = 0$$

を満足する元 x に対して

$$y^2 = f(x) = x^5+ax^4+bx^3+cx^2+dx+e$$

の解の個数を数えるのである。答は

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

のルジャンドル記号に1を加えたものである。つまり、(a/p)を Legendre 記号として、

$$(f_2(u,v)/p)+1$$

である。

$$x^2+ux+v = 0$$

の解 x に対して、フロベニウス写像

$$\bar{x} = x^p : K \to K$$

を考えれば、$\bar{x}$ は体の同型写像であり、F_p の元は固定されているから、同一方程式

$$\bar{x}^2+u\bar{x}+v = 0$$

の解である。そして、

$$\bar{x} = x^p = x$$

ならば、F_pの定義から、$x \in F_p$となってx^2+ux+vの既約性に反する。従って、

$$z^2+uz+v = (z-x)(z-\bar{x})$$

であり、終結式(resultant)の定義から、

$$f(x) \otimes x^2+ux+v = f(z) \textcircled{z} (z-x)(z-\bar{x}) = (f(z) \textcircled{z} (z-x))(f(z) \textcircled{z} (z-\bar{x})) = f(x) f(\bar{x})$$

となる。もし、

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

に0でない解が存在すれば、

$$\bar{y}^2 = f(\bar{x})$$

であり、

$$(y\bar{y})^2 = f_2(u,v) = f(x) \otimes x^2+ux+v$$

でもある。従って、Kの平方に対応する式は、F_pの元として平方なのである。現実には、Kでの原始根をzとすれば、奇素数pについては

$$z^{p\hat{}2-1}-1 = (z^{(p\hat{}2-1)/2}-1)(z^{(p\hat{}2-1)/2}+1)$$

と因数分解でき、

$$(p^2-1)/2 = (p+1)\cdot(p-1)/2$$

であるから、$z^{(p\hat{}2-1)/2}+1 = 0$に対応する半数のものは、

$$z^{(p\hat{}2-1)/2} = (z^{p+1})^{(p-1)/2} = (z\bar{z})^{(p-1)/2}$$

であるから、F_pの元であるzのフロベニウス・ノルム(Frobenius norm)

$$|z|^2 = z\bar{z}$$

のルジャンドル記号

$$(z\bar{z}/p) = \pm 1$$

が平方剰余・非剰余を定めているのである。フロベニウス写像は対合、つまり、2度作用させると元に戻る写像、つまり、$y^{p\hat{}2} = y$であるから、$y\bar{y} = y^{p+1}$は常にF_pの元である。

注意するべきことは、この場合、$z\bar{z} = (y^{(p+1)/2})^2$は$K= F_p(x)$の元の平方となる$F_p$の元ではあるが、$F_p$の元の平方とは必ずしもなっていないことである。

6.1 ヤコビ多様体

ここでは、深入りせず、例を挙げるに止める。

例 1. 超楕円曲線

$$C:\ y^2 = f(x) = x^5-x^3-2x^2-2x-1$$

この曲線上の2次の“有理点”(rational point)について考えてみよう。対象は

$$(ax+b)/(x^2+ux+v)$$

あるいは、xの2次式と、y = ax+bの対、あるいは、因子(factor)の形で書いて

$$(x^2+ux+v,\ y-(ax+b))$$

であって、$x^2+ux+b = 0$の解 s, t のところで

$$y^2 = f(x),\ y = ax+b$$

が同時に満足されるもの。言い換えると

$$x^2+ux+v = 0 \rightarrow y^2 = f(x) \wedge y = ax+b$$

を満たすものである。式では、

$$x^2+ux+v \mid (ax+b)^2-f(x)$$

である。

$$H = \{(ax+b)/(x^2+ux+v) : x^2+ux+v \mid (ax+b)^2-f(x)\}$$

少し確かめると、すぐに

$$[\pm(3x-5),\ x^2-2x+2],\ [\pm x,\ x^2+x+1],\ [\pm(x-1),\ x^2+2x+2],\ [\pm 1,\ x^2+1]\cdots$$

など、無限に解が存在することが解る。これらの因子には可換群(commutative group, abelean group)の構造が入ることが知られている。この場合、種数 g = 2 の2倍の自由さ、つまり、4個の自由度をもつ、xの3次式

$$y = g(x) = ax^3+bx^2+cx+d$$

などを通じて、加法が定義できる。例えば、和

$$[3x-5,\ x^2-2x+2]+[x-1,\ x^2+2x+2]$$

を定義してみよう。先ず、

$$x^2-2x+2 = 0 \rightarrow g(x) = 3x-5$$

$$x^2+2x+2 = 0 \rightarrow g(x) = x-1$$

となる g(x) を求めると、

$$g(x) = 1/2\cdot x^3+1/2\cdot x^2+x-2 = 1/2\cdot(x-1)(x^2+2x+4)$$

であることが解る。二つの因子の共通の表現を得た訳である。

$$g(x)^2-f(x)$$

は、一般には6次の式で、

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

で割り切れる。従って、新しい2次の因子が求まるはずである。具体的には

$$g(x)^2-f(x)=1/4\cdot(x^2-2x+2)(x^2+2x+2)(x^2-2x+5)$$

であって、 $g(x)$を新しい因子 x^2-2x+5 で割った剰余

$$\mathrm{rem}(g(x),\ x^2-2x+5)=(3x-19)/2$$

の「符号」を変えたものと定義する。つまり、

$$[3x-5,\ x^2-2x+2]+[x-1,\ x^2+2x+2]=[(-3x+19)/2,\ x^2-2x+5]$$

あるいは、

$$[3x-5,\ x^2-2x+2]+[x-1,\ x^2+2x+2]+[(3x-19)/2,\ x^2-2x+5]=0$$

と定義する。単位元0に相当するものはy 軸に平行な任意の直線である。言い換えると、共通の因子の上の互いに符号が反対の点はを逆元と定義するのである。

$$[(-3x+19)/2,\ x^2-2x+5]+[(3x-19)/2,\ x^2-2x+5]=0$$

例2. 超楕円曲線

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

右辺の5次式は1次の因子と2次の因子に分解している。簡単に得られる因子としては

$$[0,\ x(x-1)],\ [0,\ x^2-3],\ [0,\ (x-1)(x+1)],\ [0,\ x(x+1)],$$

$$[\pm1,\ x^2+x-1],\ [\pm2(x+1),\ x^2-x-4],\ [\pm2(x+1),\ x^2+1],$$

$$[\pm3(x+1),\ (x+1)(x-3)],\ [\pm4x,\ x(x-3)],\ [\pm6(x-1),\ (x-1)(x-3)]],\cdots$$

などがある。

勿論、第二成分が1次因子に分解しているところでは、解は通常の解の組である。

$$(x,y)=(-1,\ 0),\ (0,\ 0),\ (1,\ 0),\ (3,\ \pm12)\cdots$$

例えば、$[6(x-1),\ (x-1)(x-3)]$は、$(x-1)(x-3)=0$ の解$\{1,3\}$のところで、それぞれ

$$6(x-1)[x=1]=0,\quad 6(x-1)[x=3]=12$$

を意味している。既約な因子 x^2-x-4 などでは拡大体 K の元での解となっている。例えば、

$$[2(x+1),\ x^2+1]+[2(x+1),\ x^2+1]=2[2(x+1),\ x^2+1]$$

を計算してみよう。この点で2重の接触をしている

$$y = g(x) = ax^3+bx^2+cx+d$$

を求めることである。先ず、与えられた点を通ることは

$$g(x)-2(x+1) = 0 \bmod x^2+1$$

であり、x^2+1 で接していることは、

$$2yu = f'(x),\ u = g'(x),\ y = 2(x+1)$$

から、u,y を消去した x の多項式が x^2+1 で割り切れることである。つまり、

$$4(x+1)g'(x) = f'(x) \mod x^2+1$$

である。これらの係数から、連立(1 次)方程式

$$-2+c-a = 0,\ -2+d-b = 0,\ c+2b-3a = 0,\ -5+c-3a-2b = 0$$

が導かれ、それを解いて

$$g(x) = -1/4\cdot(x^3+5x^2-7x-3)$$

を得る。これから、

$$g(x)^2-f(x) = 1/16\cdot(x-3)^2(x^2+1)^2$$

である。$(x^2+1)^2$ は当然の因子であるから、新し 2 次因子 $(x-3)^2$ が得られる。従って、例えば、h(x)を x の多項式として k(x)で割ったときの剰余を

$$h(x)\boxtimes k(x) = \mathrm{rem}(h(x),k(x),x)$$

等と、(この場限りの記法で、結合力は最弱として)記すると

$$g(x)\boxtimes(x-3)^2 = 1/2\cdot(51-25x)$$

が得られる。最初の目的の 2 倍元は、

$$2[2(x+1),x^2+1] = [1/2\cdot(25x-51),(x-3)^2]$$

と定める。第一の成分 $1/2\cdot(25x-51)$ は剰余 $1/2\cdot(51-25x)$ の符号を変えたものである。この符号を変える操作を“決して”忘れてはならない。(自分はこれを忘れて何度も“彷徨った”。自慢できないが大切な経験である)

重複した因子での剰余については注意が必要であろう。現実には

$$1/2^2\cdot(25x-51)^2-f(x)\boxtimes(x-3)^2 = 0$$

と、ちゃんと 2 次の接線になっているのである。

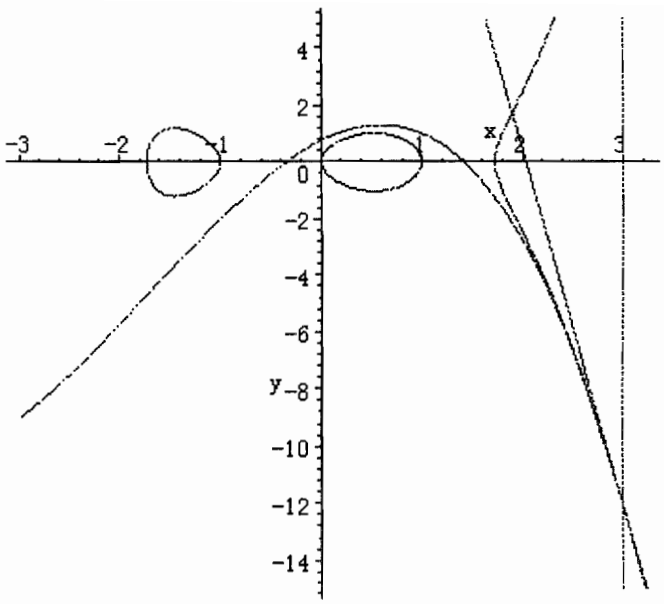
記号についての注意であるが、演算記号 $\boxtimes$ の「結合力」(adhesiveness)が最弱と云った意味は

$$(1/2^2\cdot(25x-51)^2-f(x))\boxtimes(x-3)^2 = 0$$

の括弧を省略するという意味である。$\boxtimes$ の結合力が弱く

$$1/2^2\cdot(25x-51)^2-(f(x)\boxtimes(x-3)^2)$$

のようには結合できないのである。



この図では、$x=3$ に於いてのみ $y=g(x)$ と交わっているが、$x^2+1=0$ の解、つまり、$\pm i$ の所では $y^2=f(x)$ と接しているのである。

これらの概念は、要するに、例えば、イデアルの積の方程式

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

の解を具体的な標準形

$$X=[y^2-f(x),\ y-(ax+b),\ x^2+ux+v]$$

の形で計算しようという問題なのである。

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

の解は、この場合は、互いに素だから

$$a(x)\ (x^2+1)+b(x)\,x(x-3)=1$$

から、

$$g(x)=a(x)\,4x\,(x^2+1)+b(x)\,2\,(x+1)\,x\,(x-3)$$

の形で求めるのである。

6.2 終結変換多項式

このようにして、所謂、チルナウス変換（W. von Tschirnhaus, 1651-1708）

$$f_1(u)=f(x)\circledast x+u$$

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

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

…

のルジャンドル記号の和

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

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

$$c_p = \sum x,y,z \in p \ (f_3(x,y,z)/p)$$

$$\cdots$$

を通じて、例えば、f(x)が 5 次の場合は、全体の因子の個数が、f(x)の終結変換(resultant transform)多項式

$$\underline{f}_p(x) = x^4 + a_p x^3 + b_p x^2 + p a_p x + p^2$$

の 1 での値として関係づけられるのである。以下、f(x)が 2n+1 に場合にはf(x)の終結変換は

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

などと定義される。

志村-谷山の理論によって、終結変換方程式

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

の解は、各素数 p ごとに、絶対値 $\sqrt{p}$ の複素数、つまり

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

の形の複素数であることが知られている。

あるいは、同じことであるが、非実根をもつ因子

$$\underline{f}_p(x) = (x^2 + u_1 x + p) \cdots (x^2 + u_n x + p)$$

の積に分解される。

先ず、極端な例を挙げよう。

例 2.

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

この場合は x^2+1 を除いて、一次の因数に分解している。

プログラムの核の部分は

$$f_1(u) = f(x) \otimes x + u = (u^4 - 1)\, u$$

$$f_2(u,v) = f(x) \otimes x^2 + ux + v = -vu^4 + 4v^2u^2 + v(1-v^2)^2$$

である。直接計算してもよいが、例えば、階差を用いるならば、階差の生成行列

$$\begin{pmatrix} 1, & 0, & 0, & 0, & 0, & 0 \\ 0, & 1, & 1, & 1, & 1, & 1 \\ 0, & 0, & 2, & 6, & 14, & 30 \end{pmatrix}$$

$$\begin{pmatrix} 0, & 0, & 0, & 6, & 36, & 150 \\ 0, & 0, & 0, & 0, & 24, & 240 \\ 0, & 0, & 0, & 0, & 0, & 120 \end{pmatrix}$$

との積をとった

$$[(n^2-1)^2 n,\ (4n-1)n,\ (8n-14)n,\ -36n,\ -24n,\ 0]$$

を[a0, a1, a2, a3, a4, a5]として

```
b:=b+r[1+(a0 mod p)]:
a0:=a0+a1:a1:=a1+a2:a2:=a2+a3:a3:=a3+a4:a4:=a4+a5:
```

などのループを用いて計算すればよい。

実際の Maple のプログラム例を挙げておく。勿論、改良の余地は十分ある。

```
f:=u->(u^4-1)*u: g:=(u,v)->-v*u^4+4*v^2*u^2+v*(1-2*v^2+v^4):
t:=[]: for p from 3 to 10000 do: if isprime(p) then r:=[]: for n from 0 to p-1 do:
s:=n^((p-1)/2) mod p: if s > p/2 then s:=s-p fi: r:=[op(r), s]: od:
a:=0: for m from 0 to p-1 do: a:=a+r[1+(f(m) mod p)]: od:
b:=0: for n from 0 to p-1 do: a0:=(1-2*n^2+n^4)*n mod p: a1:=4*n^2-n mod p:
a2:=8*n^2-14*n mod p: a3:= -36*n mod p: a4:= -24*n mod p: a5:=0 mod p:
for m from 0 to p-1 do: b:=b+r[1+(a0 mod p)]:
a0:=a0+a1:a1:=a1+a2:a2:=a2+a3:a3:=a3+a4:a4:=a4+a5:
od:od: print([p,a,b]); t:=[op(t),[p,a,b]]: fi:od:
```

兎に角、計算をすると、

$$[3, 0, -2],[5, 0, -10],[7, 0, 14],[11, 0, 14],[13, 0, -26],$$
$$[17, 12, 70],[19, 0, -34],[23, 0, 46],[29, 0, -58],[31, 0, 62],\cdots$$

といったデータが得られる。対応する終結変換多項式

$$\underline{f}_p(x) = x^4+a_p x^3+b_p x^2+pa_p x+p^2$$

は、因数分解した形で記すると

$$[3, x^4-2x^2+9],[5, (x^2-5)^2],[7, (x^2+7)^2],[11, x^4+14x^2+121],[13, (x^2-13)^2],$$
$$[17, (x^2+6x+17)^2],[19, x^4-34x^2+361],[23, (x^2+23)^2],[29, (x^2-29)^2],[31, (x^2+31)^2],$$
$$[37, (x^2-37)^2],[41, (x^2+6x+41)^2],[43, x^4+14x^2+1849],[47, (x^2+47)^2], \cdots$$

等である。これらの因数分解の形は 8 を法として

p mod 8	
1	$(x^2+ax+p)^2$

3　　$(x^2-p)^2=(x+\sqrt{p})^2(x-\sqrt{p})^2$

5　　$(x^2+p)^2=(x+\sqrt{-p})^2(x-\sqrt{-p})^2$

7　　$x^4+ax^2+p^2$

であって、1,7 の剰余では、一様分布、3 では実数の符号の異なる重根、5 では符号の異なる純虚根をもっている。

歴史的には、当研究所報、第 14 回数学史シンポジウム(2003)2004 の p.121

(3) f(x) 5次式. x^5-1, x^5-x, $\binom{x}{5}$. 等.

$p<1000$ くらいで. (a_p, b_p-2p) をおめる. table

と、当時、もし種数 2 の場合が計算できるとしたら計算してみましょうと記載されているものです。現実には、私の関心は、むしろ、代数的には特殊性をもたない、一般の(generic)な方に向いていたのかも知れないと(今にしては)思う。

例えば、[π/4;3π/4:1/4]は角度 π/4 と 3π/4 の点分布、確率 1/4 づつ、[1:1/2]は一様分布、確率 1/2 という内容の略記である。

curve	angular distribution type
$y^2=x^5-1$	[π/2:1/2],[π/4;3π/4:1/4],[1:1/4]
$y^2=x^5-x$	[π:1/4],[π/2:1/4],[1:1/2]
$y^2=x(x-1)(x-2)(x-3)(x-4)$	[1:1]

従って、これらは一様分布の部分は含むものの本質的な連続分布は含んでいない。

6.2　終結変換方程式の解の分布型

種数 2 の超楕円曲線

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

(f(x)は 5 次多項式)の終結変換方程式

$$\underline{f}_p(x)=x^4+a_p x^3+b_p x^2+pa_p x+p^2$$

解の分布型について述べる。現在、私の知っている分布型は 6 種類であるが、この類型がすべての場合をつくしているかどうか問題である。新しい類型の登場を楽しみにしている。

分布型	f(x)の Galios group	ex. etc
$\sin^2\theta+\sin^2 2\theta$	S(5), A(5)	$x^5+5x+5,\cdots$

$\sin^2\theta$	C(5), D(5)	$x^5-x^3-2x^2-2x-1,\cdots$
unif.	reducible	$x(x+2)(x^3-2x^2-16x-8),\cdots$
unif + $\pi/2$, $\pi/4$, $3\pi/4$	F(5)	$x^5-2,\cdots$
unif + $\pi/2$, π	reducible	$x^5-x,\cdots$
$(1-\sin^4\theta)/(1-\sin\theta)$?	reducible	$x(x^2-1)(x^2-2),\cdots$

最後の行の空白は新しい分布型の登場のための枠である。現在 $\sin^2 2\theta$ の型のものは、存在しないのではないかと予想しているが、それは特に論拠があってのことではない。探しているが(今のところ、私には)見つけることができないのである。

1. $\sin^2\theta+\sin^2 2\theta$ (generic case)

この型は、所謂、一般型である。ガロア群が非可解群のものはすべてこの型に属すると予想される。特に、代数的な意味はないのだけれども、

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

の例を挙げる。それは、この例から、

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

という分布に思い至ったことと、それが、形式的にも内容的にも、楕円曲線の $\sin^2\theta$ -予想の“心”を最も素直に継承した形式と内容をもっていたからである。

当然のことであるが、最初は $\sin^2\theta$ と云わないで、実部をとって $\sqrt{1-x^2}$ 分布と云ってもよかったのであろうが、θ に着目した“視点”こそ、この予想の深い点なのではないだろうか。つまり、一般の種数 g を見通した視点であったと(結果としてではあるが…)云えるであろう。

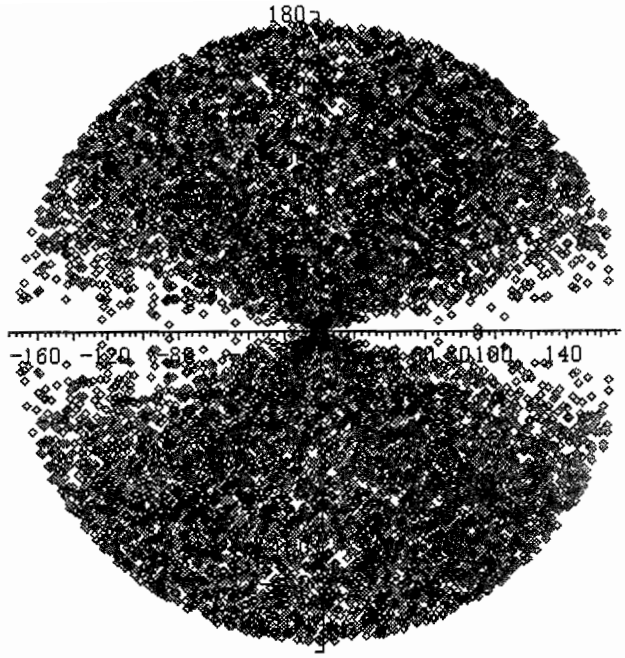
次のものが、そのグラフである:

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

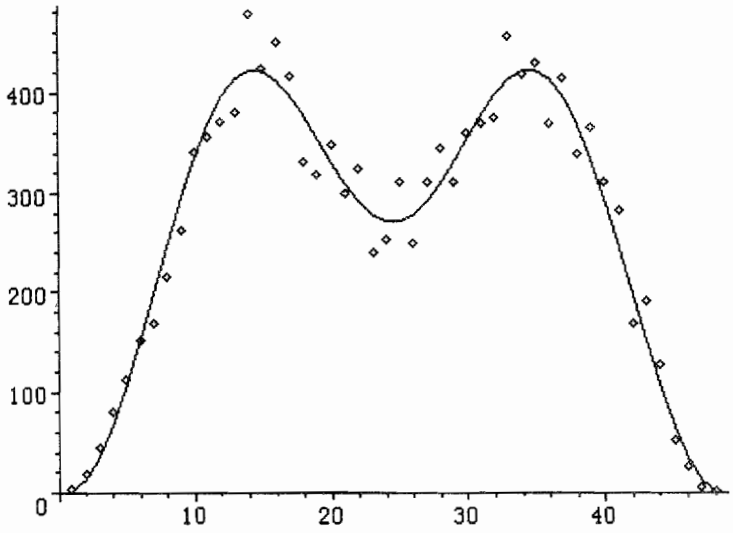
$$\mathrm{gal} = S(5),\ \det = 5^5\cdot 881$$

$$x^4-a_p x^3+b_p x^2-a_p px+p^2 = 0$$

$$p = 3 \sim 30047\ (12992\ \text{roots})$$



angular distribution



つまり、A(5), S(5)はこれに属する、可解群である場合、F(5),D(5),C(5)の場合でもほとんどこの類型に属する。可約な場合の多くもこの類型に属する。例えば、

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

などもこの系列に属する。

2. $\sin^2\theta$ の分布の場合

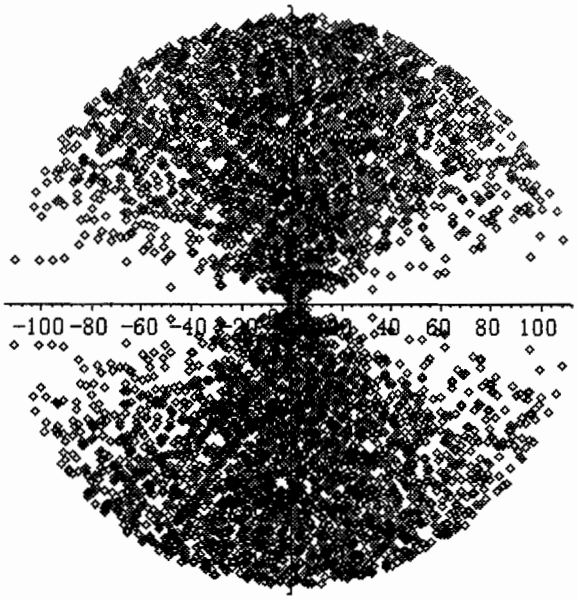
この場合は、既約な多項式 f(x) で、そのガロア群は可解で、C(5), D(5) の何れかであろうと思う。位数 20 の F(5)= M_{20} でこの分布になるものは(現在私は)知らない。

次の例は、Z($\sqrt{-47}$) の Hilbert-Weber の多項式の簡約形に対応するものである。

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

$$\det(f(x)) = f(x) \otimes f'(x) = 47^2 \quad gal = D(5)$$

$$p = 3 \sim 12541$$



この類には、y,z を助変数とする 2-parameter family の

$$f(x) = zx^5+(z^2-z-1)x^3+(3-z)x^2+(z-3)x+1+y(x(x-1))^2$$

が存在する。勿論、

$$f(bx+c)$$

などもこれに属するが、ガロア群が C(5),D(5) であっても $\sin^2\theta$ 型ではなくて、通常は一般型、つまり

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

になっている。

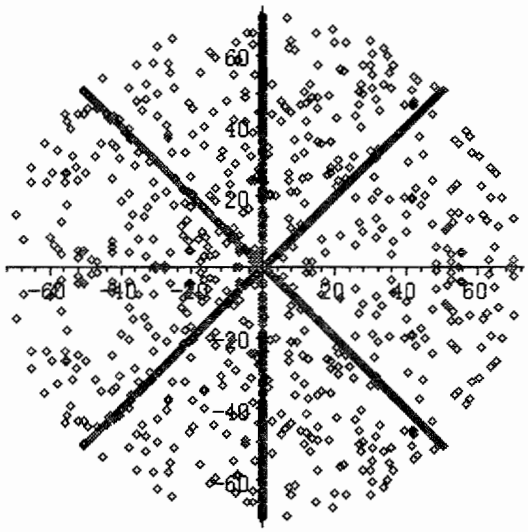
3. 一様分布と純虚数と実数および実部と虚部が等しい分布になる場合

f(x) が既約で、可解な F(5) で、この分布をもつものとして

$$f(x) = x^5-2$$

$$gal = F(5)\ (= M_{20})$$

$$p = 3 \sim 5087$$

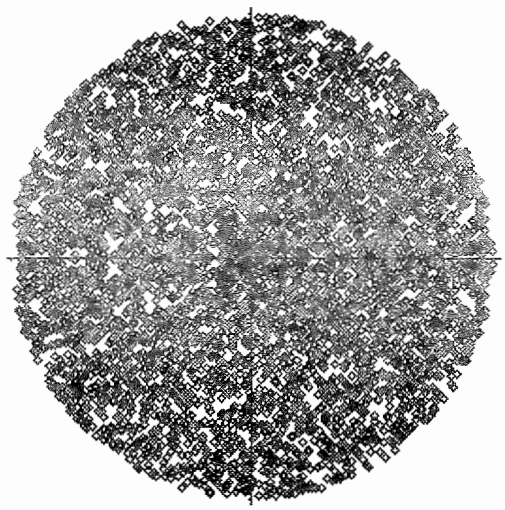


などがある。

4. 可約で、一様分布になる場合、例えば

$$f(x) = x(x+2)(x^3-2x^2-16x-8)$$

$$p = 2 \sim 13313$$



この場合は、1つの助変数nをもつ族が知られている：

$$y^2 = f(x) = x^5-20x^3-40x^2-16x+nx^2(x+2)^2$$

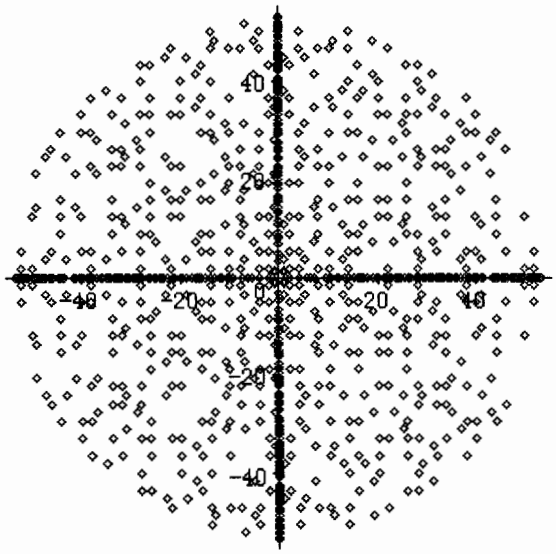
$$\det(f(x)) = f(x) \otimes f'(x) = 2^{16} \cdot (n^2-10n+52)^2$$

5. 一様分布と純虚数と実数になる場合

(special case of 4 with n = 5)

$$f(x) = x(x-2)(x+1)(x+2)(x+4)$$

$$p = 2 \sim 14447$$

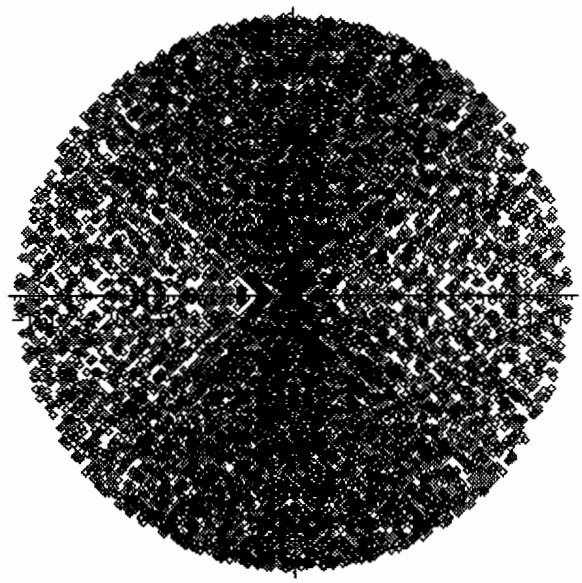


この場合は、変数の shift により

$$x(x^2-1)(x^2-9)$$

と同じ族になる。

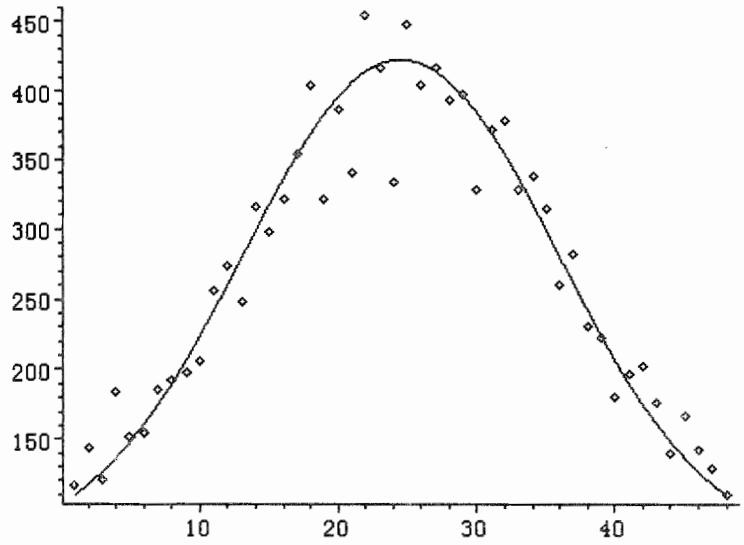
6. 連続分布であるが、$\sin^2\theta$ 型でも $\sin^2\theta+\sin^2 2\theta$ でもない場合



$$f(x) = x(x^n-1)(x^n-2)$$

$$p = 3 \sim 30011$$

などが、これに属す。



この分布は $\theta=0$ で 1/4 であろうと思われる。現在、(深い理由なしに)

$$1+\sin\theta+\sin^2\theta+\sin^3\theta = (1-\sin^4\theta)/(1-\sin\theta)$$

が、その分布に比例するであろうと予想しているものである。

だから、連続な分布であれば

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

の何れかであろうということはできないことは明白である。しかし、これは既約でない場合である。

種数 2 の $\sin^2\theta$-予想

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

1. ガロア群が、S(5), A(5)、つまり、非可解ならば、

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

2. 分布型が $\sin^2\theta$ ならば可解でガロア群は C(5), D(5) である

一般の種数 g の超楕円曲線に関する $\sin^2\theta$-予想

C: $y^2 = f(x)$, irreducible

$$\sin^2\theta+\cdots+\sin^2 h\theta \quad (h \le g)$$

問題

1. 分布が $\sin^2 2\theta$ になるものは存在しない？

2. ガロア群が、$F(5)=M_{20}$ ならば、
一様分布と純虚数と実数および実部と虚部が等しい分布になる？

3 上記6類型でないものが存在する？

7. 5次多項式と2次体の類数に関する一つの予想

問題の多項式は、種数2の超楕円曲線

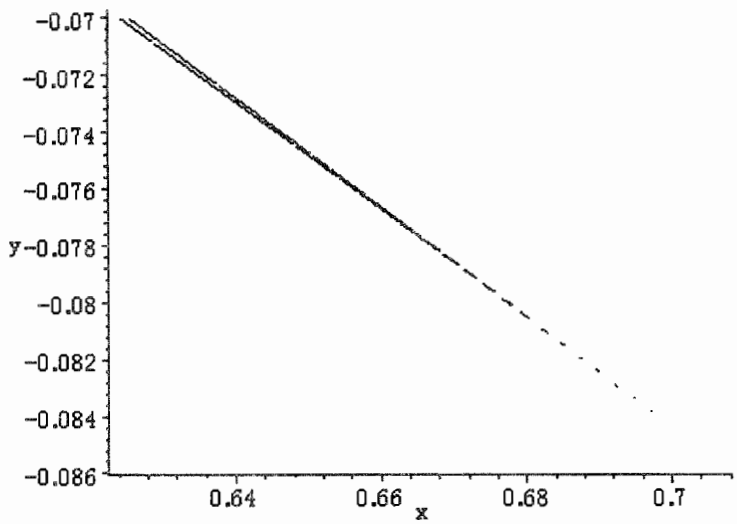
$$C:\ y^2=f(x)$$

の終結変換方程式(resultant transform equation)の解の偏角の分布が、$\sin^2\theta$ の分布の場合、つまり、既約な多項式f(x)で、そのガロア群は可解で、C(5),D(5)であって、有理数y,zを2つの助変数とする多項式

$$f(x)=$$

$$4y^3+(-z^2+30z-1)y^2-2z(3z+1)(4z-7)y+z(4z^4-4z^3-40z^2+91z-4)=$$

$$4z^5-4z^4+(-40-24y)z^3+(91+34y-y^2)z^2+(14y+30y^2-4)z+4y^3-y^2=0$$



に関するものである。

この多項式の判別式は

$$f(x)\circledast f'(x):$$

$$z^3(4y^3+(-z^2+30z-1)y^2-2z(3z+1)(4z-7)y+z(4z^4-4z^3-40z^2+91z-4))^2$$

である。この式の完全平方部分(の平方根)

$$k(y,z) = 4y^3+(-z^2+30z-1)y^2-2z(3z+1)(4z-7)y+z(4z^4-4z^3-40z^2+91z-4)$$

についての問題である。

問題(予想 2006.09.17)

$$|k(n,m)| > 5,\ \text{square free} \rightarrow 5 \mid h(Z(\sqrt{-k(n,m)}))$$

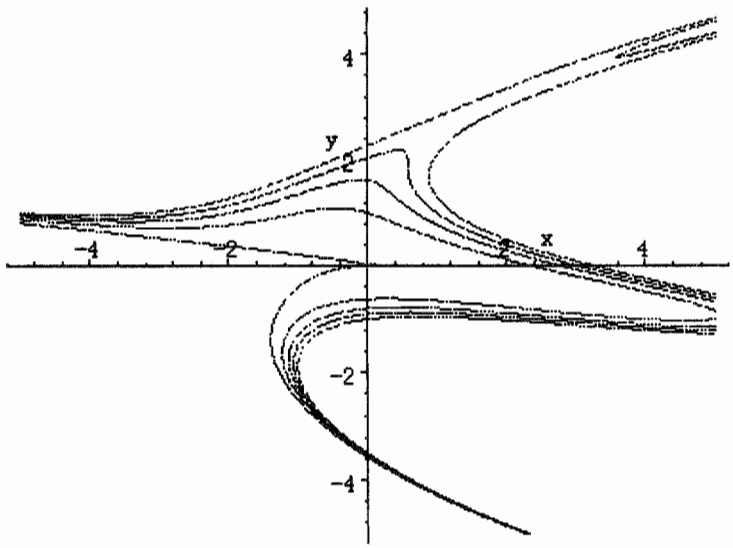
というものである。つまり、任意の正数の対 n, m に対して k(n,m)の絶対値が 5 より大きく平方因子をもたまければ、

$$\sqrt{-k(n,m)}$$

で定まる 2 次体の整数環 $Z(\sqrt{-k(n,m)})$の類数は 5 の倍数であろう、という予想である。

以下の図は、類数 5 の虚 2 次体に対応するグラフである。

$$k(x,y) = 0, 47, 79, 103, 127$$



また、以下の数の表は、例えば **47**(1;5)は、47 が k(n,m)の値として現れ、虚 2 次体の整数環 $Z(\sqrt{-47})$の類数は 5 で、実 2 次体の整数環 $Z(\sqrt{47})$の類数は 1 であることを意味している。また、**401**(5;20)は、-401 が k(n,m)の値として現れ、実 2 次体の整数環 $Z(\sqrt{401})$の類数が 5 で、虚 2 次体の整数環 $Z(\sqrt{-401})$の類数は 20 であることを意味している。

k(n,m)

[3(1), **47**(1;5), **79**(3;5), **103**(1,5), *119*(2;10),
127(1;5), **131**(1;5), *143*(2;10), *159*(2;10), **179**(1;5),
227(1;5), 239(1;15), *303*(2;10), *319*(2;10), **347**(1;5),
439(5;15), 443(3;5), 455(4;20), 479(1;25), **523**(1;5),
571(1;5), 599(1;25), *611*(2;10), 615(4;20), **619**(1;5),
635(2;10), 671(2;30), **691**(1;5), *699*(2;10), **739**(1;5),
751(1;15), **787**(1;5), 803(2;10), 815(2;30), *851*(2;10),
923(2;10), 971(1;15), 1007(2;30), *1115*(2;10), **1123**(1;5),

-k(n,m)

[5(1;2), **401**(5;20), **817**(5;12), **1093**(5;10), **1393**(5;16),
1641(5;44), **1897**(5;27), **2081**(5;60), **2153**(5;32), **3121**(5;40),
3129(10;48), **3181**(5;54), **3253**(5;34), *4097*(10;32), *4321*(10;32),
4889(5;88), *5777*(10;48), **6157**(5;24), *6945*(10;56), **6949**(5;70),
7221(10;56), **7513**(5;36), *7705*(10;56), **8049**(5;100), *8321*(10;144),
8501(5;150), *9321*(10;56), *9553*(10;40)]

この表は、k(n,m)の値の表であるが、そのすべてではないと思う。絶対値の小さい数でこの表に現れていない(平方因子をもたない数)もあると思う。

これらの値の意味することは、想像であるが、

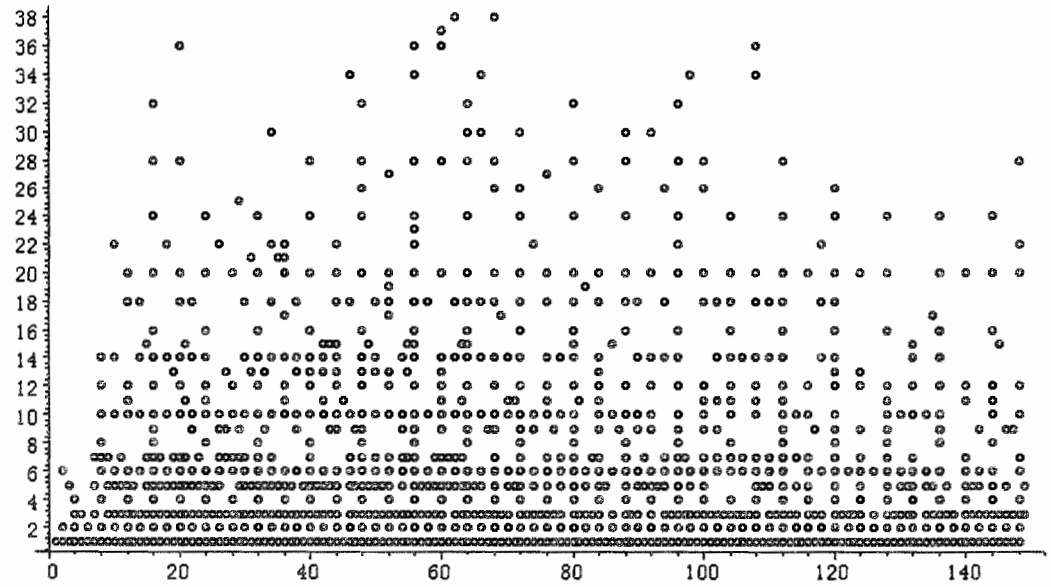
$$\sin^2\theta$$

の分布の場合、f(x)のガロア群が、イデアル類群の構造と本質的に結びついていることを意味していると思う。その構造が明らかになれば、何故

$$\sin^2\theta$$

でなければならなかったのか、などの理由も、例えば、交叉形式などと関連して明白になるであろう。

実虚２次体類数相関表



この表は、$Z(\sqrt{n})$ と $Z(\sqrt{-n})$ の類数を

横軸(=実２次体の類数)、縦軸(=虚２次体の類数)

として記したものです。$n \leq 20000$ 程度ですから、勿論、完全なものではありません。それでも、虚２次体での類数が 2, 4, 8 などの場合は実に次体でも類数はそれらの倍数になっていることが解ります。

references

[1] 難波完爾: Dedekind η 関数と佐藤 $\sin^2$-予想、第 16 回数学史シンポジウム(2005)津田塾大学 数学・計算機科学研究所報 27, 2006. pp. 95-167

[2] Kanji Namba: genus 2 hyper-elliptic curves and resultant transformation, 2006 年度応用数学合同研究集会報告集、龍谷大学瀬田キャンパス 1 号館、Dec. 2006. pp.57-62

[3] 黒川信重: 佐藤-テイト予想研究集会配布パンフレット、2007. 01. 24-26 於、東京工業大学(大岡山キャンパス)本館 213 号室