楕円位数多項式の有限フーリエ変換と対称巡回対合

難波完爾（Kanji Namba）

463-3 Kitamizote Sojya Okayama 719-1117

tel/fax. 0866-90-1886

key words

finite Fourier transformation（fFt = Vandermonte tr. = coefficient tr.），

elliptic order polynomial（= elop），Legendre Fuchs polynomial, p-property,

fast finite Fourier transformation（= ffFt），finite fields, Poincaré-Mordell-Weil group,

residual matrix, involution property, Fourier property

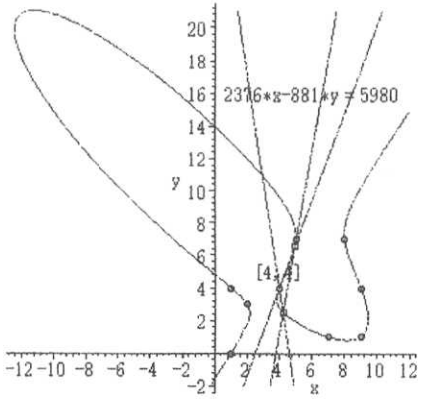
ここでの主題は有限体上の楕円曲線および位数多項式とそのフーリエ変換です。

1. 楕円曲線の話

楕円曲線とは、一つの見方ですが、x,y の 3 次関係式のことです。

$$1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3$$

の連比で定まります。つまり、9 個の独立な関係式があれば楕円曲線はきまります。下の図は $\sqrt{2017}$ に関するものです：



例．$\sqrt{2017}$ = 44.91102314577123948 78 … の桁から生ずる 9 個の点

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

を通る x,y の 3 次曲線は

$$f(x, y) =$$

$$197820-240108x+72197y+44664x^2+29229xy-32635y^2-2376x^3-2850x^2y+423xy^2+1892y^3$$

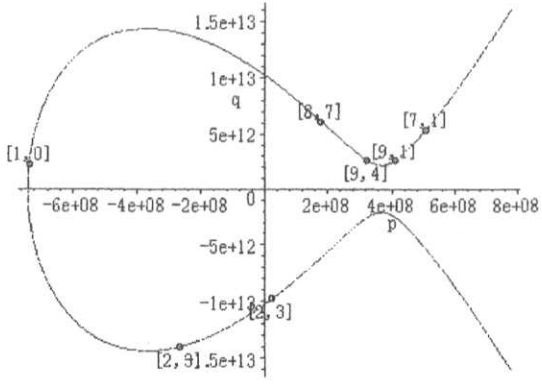
これは、双有理変換（bi-rational transformation, Cremona tr.）

$$x = 2(644172608475q+513672399785278138892730 3-8410787332383p-18756578p^2)/(260119259670q+136387259290117454597289+3860271656512896p-9378289p^2),$$

$$y = 4(192880161902389097608830 9-3003947794609764p+427240369650q-9378289p^2)/(260119259670q+136387259290117454597289+3860271656512896p-9378289p^2),$$

で Weierstrass の標準形

$$q^2 = p^3-408026433083562027p-104779260287362322220001446$$



に変形できます。図には最初の 9 点のうち 7 点の像が記してあります。これは 1, p, q , p^2 の有理式です。逆関数は

$$p = 3(235436216809y-167273034984x-718309020580)/(-2376x+881y+5980),$$

$$q = 142560(-81196610217624x^2+1337436873200676x+56841317172501yx-1052990854572940-1210907099373349y+585347779991 00y^2)/(-2376x+881y+5980)^2$$

です。係数の大きさは別にして構造は思いの外簡潔です。少し一般的な状況を考えるとこの程度の複雑性をもった式が登場するのは当たり前なのです。上記では p, q は変数（variable）ですが、変数を x, y などに変更して

$$y^2 = f(x) = x^3-408026433083562027x-104779260287362322220001446$$

を考えます。右辺の多項式の判別式は

$$\det(f(x)) = f(x) \otimes f'(x) = 2^{25}\cdot 3^{14}\cdot 5^{7}\cdot 11^{2}\cdot 10624127\cdot 153259622647529756768495 9$$

例えば、判別式の因数でない素数 p = 2017 を素体(prime field)と考えて法 p の(剰余, residue, modulus)を考えてみましょう。簡約(reduction)などの用語が用いられます。mod p では(正の剰余の形で)、曲線や変換は

$$t^2 = s^3+1470s+1325,$$

$$154+1932x+1602y+290x^2+991yx+1654y^2+1658x^3+1184x^2y+423xy^2+1892y^3 = 0,$$

$$x = 2(1507t+1982+1717s+495s^2)/(827t+823+596s+1256s^2),$$

$$y = 4(1204+942s+1256s^2+1556t)/(827t+823+596s+1256s^3),$$

$$s = 3(1880y+199x+1696)/(1658x+881y+1946),$$

$$t = 1370(733x^3+1816x+243yx+1357+1999y+1137y^3)/(1658x+881y+1946)^3$$

が得られます。

例えば、

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

とすると、その判別式は

$$x^3+ax+b \otimes 3x^2+a = 4a^3+27b^2$$

(この場合は 2 項式)です。有限体上では、C 上の点の全体と単位元(= 無限遠点, point at infinity)を加えたものが可換群(Poincaré-Mordell-Weil group)の構造をもち、その位数(order) n_p は $p = \{0, 1, \cdots, p-1\}$ として

$$n_p = 1+a_p+p,\quad a_p = \sum_{x<p}(x^3+ax+b/p),$$

$$(k/p) = \#\{x\in p : x^2 = k\}-1 = (x^3+ax+b)^{(p-1)/2} \bmod p \in \{-1,0,1\},\ \text{if } p > 2$$

で与えられ、これは、例えば

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

の多項式です。ここだけの仮の名称ですが、楕円位数多項式(elliptic order polynomial, elop)と呼びます。現実には Legendre の多項式です。これは、

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

の展開の x^{p-1} の係数の絶対値最小剰余(least absolute value residue, lavr)です。

例えば、Weierstrass の標準形

$$y^2 = x^3+ax+b,\quad z = j = -27b^2/4a^3$$

の場合、$p \geq 17$ ですが

$$P_n(1-2z) = F(-n, n+1, 1, z)$$

$$a_p(z) = (\text{lavr})$$

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

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

$$|a_p(z)| \leq 2\sqrt{p}\ ,\ \text{Hasse's inequality}$$

などが成立します。有限体の定義多項式

$$x-x^p = x(1-x^{p-1}),\ \delta(x) = 1-x^{p-1}$$

を考えると、p = 37 の場合

$$y-(x^3+14x+17)^{18} \otimes x(1-x^{p-1})\ \bmod 37 =$$

$$y^{17}-2y^{36}-16y^{35}-3y^{34}+8y^{33}-13y^{32}+11y^{31}-9y^{30}-2y^{29}+13y^{28}+3y^{27}+18y^{26}+9y^{25}+y^{24}-5y^{23}+9y^{22}+15y^{21}$$

$$-2y^{20}+2y^{18}-15y^{17}-9y^{16}+5y^{15}-y^{14}-9y^{13}-18y^{12}-3y^{11}-13y^{10}+2y^9+9y^8-11y^7+13y^6-8y^5+3y^4+16y^3+2y^2-y$$

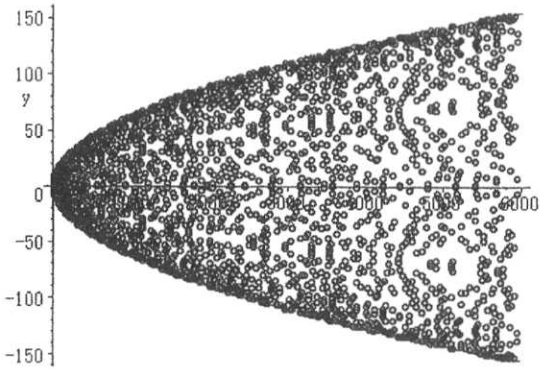
であり、この多項式の trace、つまり、p-1 = 36 次の係数 -2 が求めるものです。現実的には、先ず平方剰余(= Legendre symbol)の表を作り、$x^3+14x+17$ mod p の値を表で求め和をとるなどするのは一つの能率的な方法です。

以下の図は p = 6n+1 のとき

$$(x^3+k)^{(p-1)/2} = (x^3+k)^{3n},\ x^{p-1} = x^{6n} = (x^3)^{2n}$$

の係数

$$a_p = k^n(3n)!/(n!(2n)!)\ \bmod p,\ (\text{lavr}),\ p = 6n+1,\ n = 1 \sim 1000$$

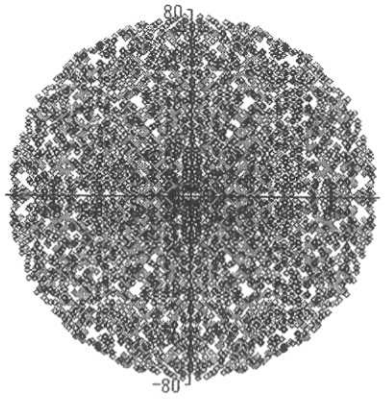


を記したものである。k^n は $x^6-1 = 0$ の解である。

$$p = (n+1)^3-n^3 = 3n^2+3n+1 = (3(1+2n)^2+1)/4$$

では、Poincaré-Mordell-Weil 群の位数は加法群の位数 p と確率 1/6 で一致する。

$$x^2+a_px+p = 0,\ p = 6n+1,\ n = 1 \sim 1000$$



これは $p = (a^2+3b^2)/4$ と表現したとき $a = \pm 1$、つまり、$(4p-1)/3 = b^2$ となる整数 $b = 2n+1$ が存在するような p である。要するに Eisenstein の整数の表なのです。偏角の分布は一様分布です。

$$y^2 = x^4+k$$

の場合はどうでしょうか。この場合は $p = 4n+1$ とすると $(p-1)/2 = 2n$ ですから

$$(x^4+k)^{(p-1)/2} = x^{2(p-1)}+\cdots+(2n)!/n!^2\cdot x^{p-1}+\cdots+k^{(p-1)/2}$$

となります。$x^{2(p-1)}$, x^{p-1} を除いて、x での和をとると、mod p で -1 になります。つまり

$$\delta(x) = 1-x^{p-1}$$

が $x = 0$ の表現関数、言い換えると、$x = 0$ のみで 1 となる関数であるということです。$x^{2(p-1)}$ からの 1 が加わるのです。だから、

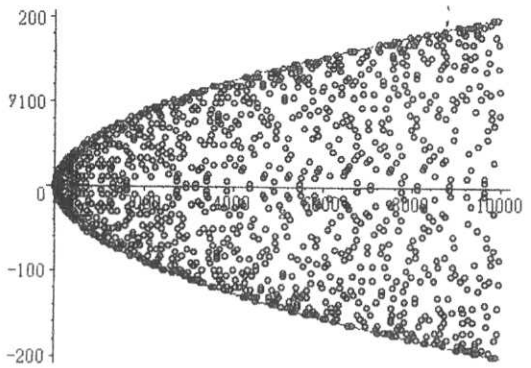
$$x^2+(1+(2n)!/n!^2)x+p$$

が合同 ζ-核となるのです。この多項式の 1 での値が p(= 加法群の位数)に一致することは

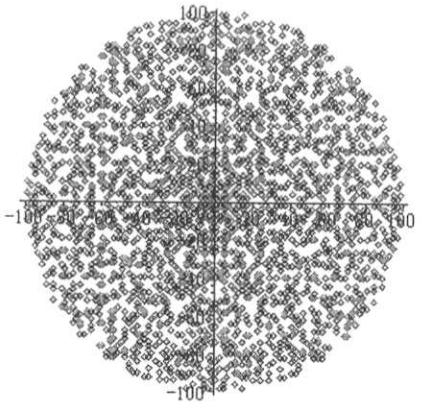
$$2+(2n)!/n!^2 = 0$$

を意味します。この場合も ζ-多項式は Gauss 整数に分解することが知られています。

$$a_p = k^{2n}(1+(2n)!/n!^2) \mod p,\ (\text{lavr}),\ p = 4n+1,\ n = 1 \sim 2500$$



下の図は $x^2+(1+(2n)!/n!^2)x+p$ の複素数根の図ですが、これは、Gauss 整数の図そのものです。



$$p = a^2+b^2 = (a+bi)(a-bi)$$

ですから、a, b のうち一つの絶対値 1 であることを意味しますから、$p = n^2+1$ の形の整数です。

$$y^2 = x^4+k$$

の楕円曲線をもちいて、p を因数にもつ整数(p は未知として)の確率 1/2 の多項式時間計算法と関係していると思います。一般に

$$y^2 = x^4+ax^2+bx+c$$

は、双有理変換

$$s = 2y+2x^2+a/3,\ t = 4xy+4x^3+2xa+b$$

$$x = -3/2\cdot(b-t)/(3s+2a),\ y = -1/12\cdot(-54s^3-54s^2a+27t^2-54tb+27b^2+8a^3)/(3s+2a)^2$$

によって、

$$t^2 = s^3+(-9a^2-108c)/27\cdot s+2a^3/27-8ca/3+b^2$$

に写されますから、今の場合は

$$y^2 = x^3+4kx$$

が対応する曲線です。だから、この曲線から出発してもよかった訳です。

確率多項式時間可能素因数(probabilistic polynomial time computable prime factor, pptc-prime)と関連して、少なくとも2系列

name	prime	family	provability
Eisenstein	$p = 3n^2+3n+1$	$y^2 = x^3+k$	1/3
Gauss	$p = n^2+1$	$y^2 = x^4+k$	1/2

があることが解ります。$p = n^2+1$, $3n^2+3n+1$ 型の素数が無限個存在(当然肯定的)するかどうかは有名な未解決の古典的問題です。

2. 終結式の話

終結式(resultant)は次のような規則をもつ多項式(有理式)の間の積である。終結積の記号ⓧ, ⓨ, ⓩ, …は変数を○で囲んで消去したもので、

$$f(x)\,⓪\,g(x) = \mathrm{resultant}(f(x), g(x), x)$$

である。消去積(elimination product)と呼び、ここだけの記号として用いる。記号の結合力は加減乗除(+, −, ×, ÷ = /, …)などより弱い。

$$f(x)\,⓪\,x\text{-}y = f(y),\ y\text{-}x\,⓪\,f(x) = f(y)$$

$$f(x)\,⓪\,g(x)h(x) = (f(x)\,⓪\,g(x))(f(x)\,⓪\,h(x))$$

$$f(x)g(x)\,⓪\,h(x) = (f(x)\,⓪\,h(x))(g(x)\,⓪\,h(x))$$

$$f(x)\,⓪\,(g(x)/h(x)) = (f(x)\,⓪\,g(x))/(f(x)\,⓪\,h(x))$$

$$f(x)/g(x)\,⓪\,h(x) = (f(x)\,⓪\,h(x))/(g(x)\,⓪\,h(x))$$

$$f(x)\,⓪\,(g(x,y)\,ⓨ\,h(y)) = (f(x)\,⓪\,(g(x,y)\,ⓨ\,h(y)$$

また、合成関数に関しては、例えば

$$f^t(h(x))\,⓪\,g(h(x)) = f^t(y)\,⓪\,g(y)^k = f^t(y)^k\,⓪\,g(y)$$

$$k = \deg(h(x))$$

などの性質がある。

例えば、

$$f(x) = x^3+2xy+3,\ g(x) = x^2+y+2,\ h(x) = x^3-2xy^2$$

の場合、

$$f(h(x)) = x^9-6x^7y^2+12x^5y^4-8x^3y^6+2x^3y-4xy^3+3$$

$$g(h(x)) = x^6-4x^4y^2+4x^2y^4+y+2$$

です。また

$$f(x)\,⓪\,g(x) = y^3-2y^2-4y+17$$

$$f(h(x))\,⓪\,g(h(x)) = (y^3-2y^2-4y+17)^3 = f(x)\,⓪\,g(x)^3$$

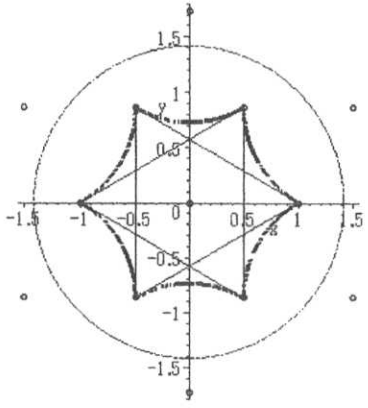
従って、f(x), g(x)がyを含まない場合はh(x)がyの複雑な式を含む場合でも

$$f(h(x))\,⓪\,g(h(x))$$

はyを含まない。

例. 双曲幾何の正多角形

種数1の曲面の基本領域の、特殊なもので、一つは長方形ですが、双曲幾何学の観点かみれば、Poincaré circleの半径が∞の場合です。種数2の、つまり二つ穴のcompact曲面の基本領域があります。これは双曲幾何の正6角形です。内角の和が $2\pi = 360°$ の正多角形



を描いているとき、たまたま、何個かの新聞に箸墓古墳の航空写真が掲載されていた。

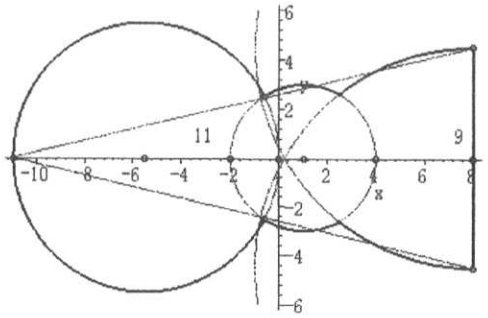
奈良県桜井市の箸墓古墳は、邪馬台国の有力候補地とされる纒向遺跡の

なかの全長約 280 ㍍の古墳で、墳丘部分は、第七代孝霊天皇の皇女の陵墓として、宮内庁が管理している。(記事より引用)

朝日新聞の記事(2016.07)の写真の 4 倍の拡大画面上では、後円部の直径は約 5.5cm、最長部の長さ約 9.5~9.7cm、最前部の長さ約 4.5cm で、くびれ部分の長さ約 2.5cm である。この写真自体は古墳を真上から写したものではないが、かなり垂直の方向から写したもので、後円部は円形に近いので形の近似の試案を試みる。この古墳は前方後円墳というには前方部は方形をなしていなくて、むしろ、何個かの円周部分から構成されている印象である。

偶然であろうが、上記の各部分の数字は半整数(= 整数の半分)なので2倍したものは整数に近い。兎も角、古墳は古代の人の残した巨大な絵文字である。説文解字ではないが意味をもっている。

以下の図は、円形部の直径 11、対称軸の長さ 8、最前部の直線部分 9、中間の小円の直径 3 としたものである。

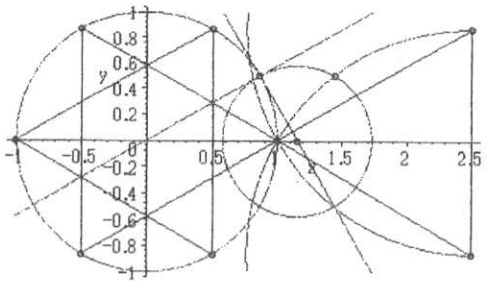


図では、対称軸を x-軸にとり、円周部と対称軸の交点が原点である。半径 3 の円の中心は(1, 0)である。大小の二つの円と直線を含む部分は、太陽・月と例えば金星(venus)、あるいは時空の舟、彗星(commet)であろうか。

いにしえの こころはしずか ひとかたの
おかにのぞみて いけるほしそら

図は航空写真、それも、垂直な視点からではないので、近似的なものである。もとの設計者はチャントした図形を想定していたに違いない。最初

に感じたのは円とそれに内接する正三角形が接し円の半径のところに交点をもつ図形である。

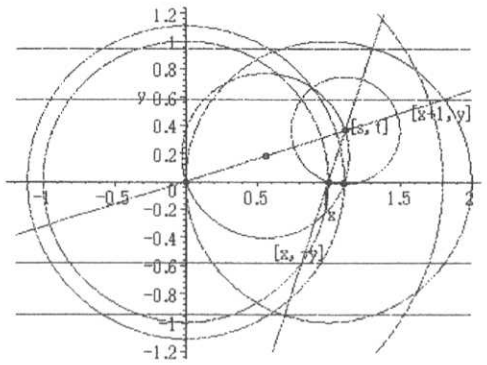


これが古代の人の意図したものであるかどうかは知るよしもない。現実のレーダによる反射波の実測では、墳丘の前方部は、鏡の取手のように直線で構成されている。しかし、端点にこのような数値が用いられているかどうかは検討に値することだと思っている。少なくとも当時の鏡のデザインには用いられている。当時の人々の概念世界のなかでの数の位置を知る確かな物証である(と思う)。

みずのもに かがみてうつす すがたみの
かがみにうつる いけるひととき

こうしてみると量子状態で「すべて」の可能性があり「どれか」を選択するのは「エネルギー」を要するように思える。古墳時代とは(私感であるが)鏡(=鑑)の「ひも(紐)がうてな(台)」にとって代わる時代だったのかも知れないと思う。

さて、もとに戻って、双曲正多角形、つまり、境界円(Poincaré circle)と直交する円で囲まれた内角和 360° の図形について考える。次の図は、正 10 角形の作図を意図したものである。要するに、多角形の辺を構成する円の中心がその上にあるような円の半径を知りたいのである。図であるが、着目する点に文字(変数)を記したものである。



縦の線は単位円周上の正 10 角形の y 座標で Tschebychev 多項式

$$x^2-2yx+1 \text{ ⓧ } x^{10}+1 = 4y^2(5-20y^2+16y^4)^2$$

の解直線

$$y(5-20y^2+16y^4)=0$$

で 5 本の直線から成っている。例えば、(x,y)を y が正の最小解とすると、2 本の直線は

$$t = as,\ t = b(s-1)$$

の形の直線で、それぞれ

$$[[0, 0],[1+x, y]],\ [[1, 0],[x, -y]]$$

を通るものである。

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

これら 2 直線の交点[s,t]を中心とする円で[1,0]を通るものを C とすると、必然的に[x,y]も通る。この円と[0,0],[s,t]を直径とする円の交点を[h,k]とすると、[0,0],[s,t],[h,k]は直角三角形の頂点なので

$$r = s^2+t^2-(s-1)^2-t^2 = 2s-1$$

が求める Poincaré円の半径の自乗である。従って、解くべき方程式系は

$$[r = 2s-1,\ t = as,\ t = b(s-1),\ y = a(x+1),\ -y = b(x-1),\ x^2+y^2 = 1,\ 5-20y^2+16y^4 = 0]$$

である。 先ず

$$s = (r+1)/2,\ a = y/(x+1),\ b = -y/(x-1)$$

が得られる。t-as, t-b(s-1)に代入すると、分子として

$$2tx-2t+yr-y,\ -2tx-2t+yr+y$$

だから、x, y について解くと、

$$x = 1/r,\ y = 2t/r$$

ここまで来れば明らかで、

$$x^2+y^2-1 \text{ ⓨ } 5-20y^2+16y^4$$

の解の逆数が求める半径の自乗 r である。両辺とも y^2 の関数だから、

$$x^2+y^2-1 \text{ ⓨ } 5-20y^2+16y^4 = (x^2+y-1 \text{ ⓨ } 5-20y+16y^2)^2$$

である。要するに $5-20y+16y^2$ に $y = 1-x^2$ を代入したものである。

Tschebychev 多項式を

$$x^2-2yx+1 \text{ ⓧ } x^{10}+1 = 4y^2(5-20y^2+16y^4)^2$$

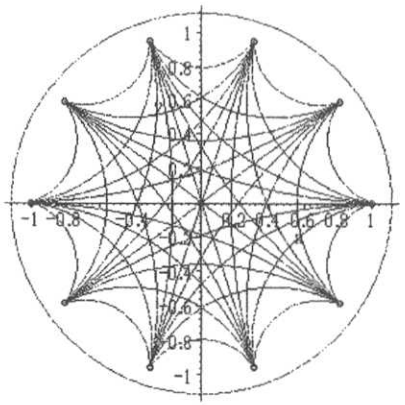
としたのが、むしろ、不自然なのであって、係数を 1 として x = 2/r

$$x^2+y^2 = 4,\ x^2-yx+1 \text{ ⓧ } x^{10}+1 = (y^4-5y^2+5)^2y^2$$

を考えるべきだったのである。結果は、$y = 4-x^2$ を代入した、

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

であり、逆数の方も(この場合は)同じ、黄金分割 $(=(\sqrt{5}\pm1)/2$, golden ratio)の方程式を得るのである。半径は正であるから、$r = \sqrt{5}\pm1$ が得られる。$(r = 2/x)$



$$x^2+y^2-4 \text{ ⓨ } z^2-yz+1 \text{ ⓩ } z^{2n}+1$$

の計算であるが、終結式は結合的であるから、

$$x^2+y^2-4 \text{ ⓨ } z^2-yz+1 = z^4+(x^2-2)z^2+1$$

$$z^4+(x^2-2)z^2+1 \text{ ⓩ } z^{2n}+1 = (z^2+(x^2-2)z+1 \text{ ⓩ } z^n+1)^2$$

を得る。つまり、

$$f_n(x) = z^2 + (x^2-2)z + 1 \ ⓩ \ z^n + 1$$

が r = 2/x の方程式である。

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

$[5, -(x-2)(x+2)(x^2+x-1)^2(x^2-x-1)^2]$, $[6, (x^2-2)^2(x^4-4x^2+1)^2]$,

$[7, -(x-2)(x+2)(x^3+x^2-2x-1)^2(x^3-x^2-2x+1)^2]$, $[8, (x^8-8x^6+20x^4-16x^2+2)^2]$,

$[9, -(x-2)(x+2)(x-1)^2(x+1)^2(x^3-3x-1)^2(x^3-3x+1)^2]$,

$[10, (x^2-2)^2(x^8-8x^6+19x^4-12x^2+1)^2]$,

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

$[12, (x^4-4x^2+2)^2(x^8-8x^6+20x^4-16x^2+1)^2]$,

$[13, -(x-2)(x+2)(x^6+x^5-5x^4-4x^3+6x^2+3x-1)^2(x^6-x^5-5x^4+4x^3+6x^2-3x-1)^2]$,

$[14, (x^2-2)^2(x^{12}-12x^{10}+53x^8-104x^6+86x^4-24x^2+1)^2]$,

$[15, -(x-2)(x+2)(x-1)^2(x+1)^2(x^2-x-1)^2(x^2+x-1)^2(x^4-x^3-4x^2+4x+1)^2(x^4+x^3-4x^2-4x+1)^2]$,

$[16, (x^{16}-16x^{14}+104x^{12}-352x^{10}+660x^8-672x^6+336x^4-64x^2+2)^2]$,

$[17, -(x-2)(x+2)(x^8-x^7-7x^6+6x^5+15x^4-10x^3-10x^2+4x+1)^2$

$(x^8+x^7-7x^6-6x^5+15x^4+10x^3-10x^2-4x+1)^2]$,

$[18, (x^2-2)^2(x^4-4x^2+1)^2(x^{12}-12x^{10}+54x^8-112x^6+105x^4-36x^2+1)^2]$,

$[19, -(x-2)(x+2)(x^9+x^8-8x^7-7x^6+21x^5+15x^4-20x^3-10x^2+5x+1)^2$

$(x^9-x^8-8x^7+7x^6+21x^5-15x^4-20x^3+10x^2+5x-1)^2]$,

$[20, (x^4-4x^2+2)^2(x^{10}-16x^{14}+104x^{12}-352x^{10}+659x^8-664x^6+316x^4-48x^2+1)^2]$

これらの多項式は n が偶数なら完全平方、奇数なら $4-x^2$ を除いた因子が完全平方である。また、奇素数なら、平方根は既約 n $=(p-1)/2$ 次の既約多項式の積で、そのガロア群は C(n)、つまり、加法群 $n = \{0, 1, \cdots, n-1\}$ であり、その判別式は $g(x)ⓧ g'(x) = p^n$ である。

$[3, (x-1)(x+1)]$

$[5, (x^2+x-1)(x^2-x-1)]$

$[7, (x^3+x^2-2x-1)(x^3-x^2-2x+1)]$

$[9, (x-1)(x+1)(x^3-3x-1)(x^3-3x+1)]$

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

$[13, (x^6+x^5-5x^4-4x^3+6x^2+3x-1)(x^6-x^5-5x^4+4x^3+6x^2-3x-1)]$

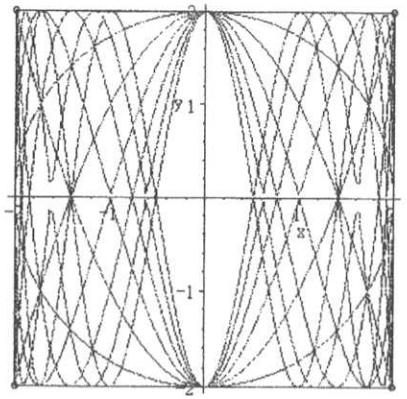
$[15, (x-1)(x+1)(x^2-x-1)(x^2+x-1)(x^4-x^3-4x^2+4x+1)(x^4+x^3-4x^2-4x+1)]$

$[17, (x^8-x^7-7x^6+6x^5+15x^4-10x^3-10x^2+4x+1)(x^8+x^7-7x^6-6x^5+15x^4+10x^3-10x^2-4x+1)]$

$[19, (x^9+x^8-8x^7-7x^6+21x^5+15x^4-20x^3-10x^2+5x+1)(x^9-x^8-8x^7+7x^6+21x^5-15x^4-20x^3+10x^2+5x-1)]$

これらの多項式は sin の加法公式みたいなもので、第 2 種の Tschebychev 多項式とでもいうものです。

$$y^2 = z^2 + (x^2-2)z + 1 \ ⓩ \ z^n + 1, \ n = 1 \sim 6$$

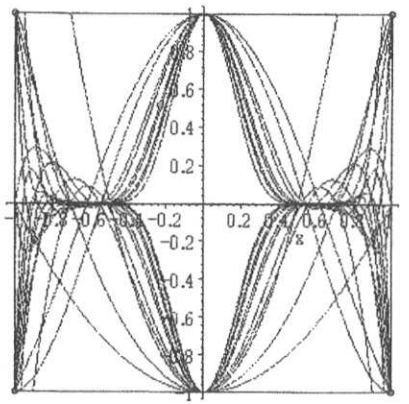


解がすべて実根で、[-2,2]に入るので、係数の順序を反転した多項式の解の絶対値は 1/2 より大きい。以下のものは[-2,2]の範囲で記したものである。最初に(自分が)見たものはこれであった。

あんりやまあ　いともかしこき　あやのはし

ともののこころね　においそめにき

といって驚き。後で「当たり前じゃん」と云って(一部)失望する。



しかし、例えば、p = 29 では

$$x^{14}-x^{13}-13x^{12}+12x^{11}+66x^{10}-55x^{9}-165x^{8}+120x^{7}+210x^{6}-126x^{5}-126x^{4}+56x^{3}+28x^{2}-7x-1$$

が q = ±1 mod p の素数に限り、つまり、

$$f_n(x) = z^2+(x^2-2)z+1 \ ⓩ \ z^n+1$$

が mod q で完全分解するなど、興味深い性質がある。

$$f_n(x) = z^2+(x^2-2)z+1 \ ⓩ \ z^n+1 = (x^2-4)^p \bmod p$$

3. 有限体上の Fourier 変換

複素数の範囲の Fourier 行列 ($A^4 = E$) としては

$$A = \begin{pmatrix} 1/2 & 1/2 & 1/2 & 1/2 & 0 \\ 1/2 & i/2 & -1/2 & -i/2 & 0 \\ 1/2 & -1/2 & 1/2 & -1/2 & 0 \\ 1/2 & -i/2 & -1/2 & i/2 & 0 \\ a+b+c & a & b & c & -1 \end{pmatrix}$$

があります。固有多項式は

$$|xE-A| = (x+1)^2(x-1)^2(x-i)$$

ですから、固有値 $-i$ に応ずる固有空間はありません。

eigen value	m	eigen vectors	
-1	2	[-1, 1, 1, 1, 0]	[0, 0, 0, 0, 1]
1	2	[1, 0, 1, 0, (a+c)/2+b]	[2, 1, 0, 1, 3(a+c)/2+b]
i	1	[0, (-1-i)/(c-a), 0, (1+i)/(c-a), 1]	

eigen value	m	eigen vectors	
-1	2	[-1, 1, 1, 1, 0]	[0, 0, 0, 0, 1]
1	2	[1, 0, 1, 0, a+b]	[2, 1, 0, 1, 3a/2+b]
i	1	[0, -1, 0, 1, 0]	

-1 に応ずる固有空間が、助変数 a,b,c に関係しないことも興味があります。

有限素体 (finite prime field) は素数 p 個の元から成る体で

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

などと色々な記法 (notion) がある。

有限体 F_p 上の高々 p-1 次の多項式の成す p 次線形空間を

$$F_p^p[x] = \{a_0+a_1x+a_2x^2+\cdots+a_{p-1}x^{p-1} : a_i \in p\} = p \text{ to } p = p2p$$

などと記す。ものとしては p の元の p 個の列の全体

$$p^p = \{f : f: p \to p\} = p\hat{}p$$

である。有限 (素) 体の定義多項式 (defining polynomial) は

$$x-x^p = x(1-x^{p-1}),\ \delta(x) = 1-x^{p-1} = \langle x=0 \rangle$$

で、デルタ関数 δ(x) は x = 0 の表現関数 (representing function, characteristic polynomial) である。

q を法 p での原始根 (primitive root) とするとき、有限フーリエ変換 (finite Fourier transform, fFt)

$$[q] : F_p^{p-1}[x] \to F_p^{p-1}[x] = p\hat{}(p-1)$$

を次のように定義する。

$$f(x) = \sum_{i<p-1} a_i x^i = a_0+a_1x+a_2x^2+\cdots+a_{p-2}x^{p-2}$$

に対し

$$f(x)[q](x) = (1-x^{p-1})\sum_{i<p-1} a_i/(1-q^ix) = \sum_{i<p-1} f(q^i)x^i$$

と定義する。この部分を不変部分空間として含む。

p^p = p2p の場合は

$$[q] : F_p^p[x] \to F_p^p[x] = p\hat{}p = p2p$$

を考えるのは自然である。この場合、

$$f(x) = \sum_{i<p} a_i x^i = a_0+a_1x+a_2x^2+\cdots+a_{p-2}x^{p-2}+a_{p-1}x^{p-1}$$

に対し

$$f(x)[q](x) = (1-x^{p-1})\left(\sum_{i<p-1} a_i/(1-q^ix)+a_{p-1}\right)$$

と定義する。

$\delta(x) = 1-x^{p-1}$ は周期 p-1 の無限級数の最初の p-1 個を取り出す作用素で、「一度だけよ」作用素 (once only operator, ichidodakeyo operator, ichop) と「ここだけで」呼ぶ。x^i の係数が $f(q^i)$ の級数に変換するという意味から、係数変換 (coefficient transform) とも、また、数列の変換行列が Vandermonde 行列 (q^{ij}) であることから、Vandermonde 変換 (Vandermonde transform) とも呼ばれる。

フーリエ変換 F の一番基本的な特性は $F^4 = I$、つまり、4 回作用させると元に戻るという特性である。それ故、フーリエ変換は認識や行動の概念、例えば、受識想行 (sense, memory, imagine, action = smia, 受想行識と少し順番が異なる) と深く関係しているのである。変換 [q] の逆変換は逆元 q^{-1} による

変換[q^{-1}]の原点対称 -[q^{-1}]である。

一般に、原始根の積は原始根とはならないが原始根の逆元は原始根である。

例　p = 37, q = 2

$$[2]: p\hat{}(p-1) \to p\hat{}(p-1)$$

この場合、例えば、πの10進法展開の36桁の変換を考えてみよう。

[3, 1, 4, 1, 5, 9, 2, 6, 5, 3, 5, 8, 9, 7, 9, 3, 2, 3,

8, 4, 6, 2, 6, 4, 3, 3, 8, 3, 2, 7, 9, 5, 0, 2, 8, 8]

対応する多項式は、

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

である。このフーリエ変換[2]は f(2^n) mod p（絶対値最小剰余, lavr)は列表示で

[-12, 10, 10, -12, 0, 8, 6, -3, -5, 6, -9, -5, 16, 16, -5, 17, -5, 1,

15, -3, 14, -13, -6, 11, -8, -3, 16, -17, -4, 9, 2, 13, 9, -5, 16, -9]

更に、$[2]^2$の結果は

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

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

$[2]^3$の結果は

[12, 9, -16, 5, -9, -13, -2, -9, 4, 17, -16, 3, 8, -11, 6, 13, -14, 3,

-15, -1, 5, -17, 5, -16, -16, 5, 9, -6, 5, 3, -6, -8, 0, 12, -10, -10]

$[2]^4$の結果は、勿論、元の数列が再生されて、

[3, 1, 4, 1, 5, 9, 2, 6, 5, 3, 5, 8, 9, 7, 9, 3, 2, 3,

8, 4, 6, 2, 6, 4, 3, 3, 8, 3, 2, 7, 9, 5, 0, 2, 8, 8]

である。

従って、例の $x^4-1=0$ のスペクトル分解で、

$$x^4-1 = (x-1)(x+1)(x-i)(x+i)$$

例えば、

$$(x-1)(x+1)(x+i) = (x^4-1)/(x-i)$$

のように現実に割り算を実行すれば多項式になるが、そのまま記せば、x = [2]のとき

$$(x-1)(x+1)(x-i)(x+i) = x^4-1 = 0$$

だから、例えば、固有値 i に関しては(x-i)のところで分配法則を用いると

$$x(x-1)(x+1)(x+i) = i(x-1)(x+1)(x+i)$$

となるから、$(x-1)(x+1)(x+i) = (x^4-1)/(x-i)$ が固有値 i に応ずる射影子(projection) P_i です。勿論、射影子、つまり、対合(involution)であることは、

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

ですが、$(x^4-1)' = 4x^3$ ですから、1の分解(partition of unitty)は

$$1 = ((x+1)(x-i)(x+i) - (x-1)(x-i)(x+i) + i(x-1)(x+1)(x+i) - i(x-1)(x+1)(x-i))/4$$
$$= (x^4-1)(1/(x-i) + (-1)/(x+1) + i/(x-i) + (-i)/(x+i))/4$$

から導かれます。例えば、1に対応する射影子は、所謂、トレース(trace)で

$$(1+[2]+[2]^2+[2]^3)/4$$

です。上記、p = 37 の場合では

[0, 3, 16, -2, -1, 9, -10, 6, -18, 15, -7, 10, -11, 2, 1, 17, -15, 10,

0, -10, 15, -17, -1, -2, 11, -10, 7, -15, 18, -6, 10, -9, 1, 2, -16, -3]

これらの成分は、あくまでも仮にであるが、次のようである：

value	1	i	-1	$-i$
projector	$(1+x+x^2+x^3)/4$	$(1+ix-x^2-ix^3)/4$	$(1-x+x^2-x^3)/4$	$(1-ix-x^2+ix^3)/4$
sort	act, fact	feel, sense	note, know	hope, will

例．楕円位数多項式

有限体上の楕円曲線で決まる可換群 Poincaré-Mordell-Weil 群の位数を表現する多項式(elop)が知られている。

family of curves	form	polynomial	case
(Whock)	$y^2 = x^3+qx^2+r$	F(1/6,5/6,1,x)	
Euler	$y^2 = x(x^2+qx+r)$	F(1/4,3/4,1,x)	
Hesse	$y^3+x^3+qxy+r = 0$	F(1/3,2/3,1,x)	
Legendre	$y^2 = x(x-1)(x-q)$	F(1/2,1/2,1,x)	
Weierstrass	$y^2 = x^3+qx+r$	$x^{(p-1)/4} \cdot$ F(1/12,5/12,1,1-x)	p = 4n+1
		$x^{(p+1)/4} \cdot$ F(7/12,11/12,1,1-x)	p = 4n-1

これらの多項式では、絶対値最小剰余が意味をもっている。Hasse の不等式から $p \geq 17$ では一意的に値が定まる。

例　Weierstrass family p = 199

原始根の一部は

[3, 6, 15, 22, 30, 34, 38, 39, 41, 44, 48, 54, 68, 69, 71, 73, 75, 77, 84, 87, 95, 97, 99, …]

ここでは、理由はないが(何でも良いが)9がらみで q = 99 を用いる。

p = -1 mod 4 であるから、

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

$$x^{50} \cdot (188x^{16}+22x^{15}+42x^{14}+21x^{13}+145x^{12}+193x^{11}+124x^{10}+80x^{9}$$

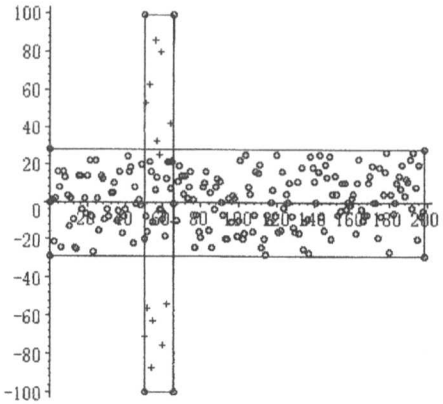
$$+25x^{8}+32x^{7}+86x^{6}+136x^{5}+112x^{4}+63x^{3}+143x^{2}+53x+128)$$

が求める Fuchs-Legendre polynomial である。Hasse の不等式から、

$$|f(x)| < 2\sqrt{p} = 28.21347196$$

下の図は、係数(+印)値は • で記した。値の方は Hasse の不等式を満たしている。

$$[x, f(x)], x \in p \ \& \ \text{coeff}(f(x))$$

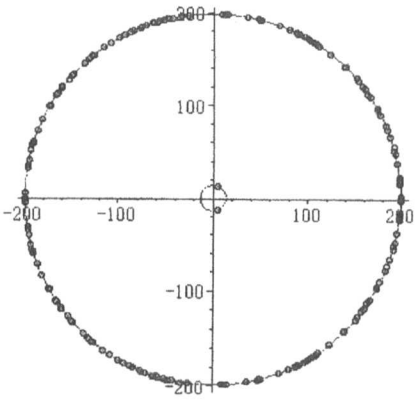


フーリエ変換 f(x)[q](x)の 1 の p-1 乗根での値の絶対値は常に p, $\sqrt{p}$, 1 の何れかである。

$$g(z) = y^2+pzy+p^2 \ ⓨ \ y\text{-}f(x)[q](x) \ ⓧ \ x^{p-1}-1$$

は f(x)の値の絶対値が p のときには、その実部、つまり、$p \cdot \cos(\theta)$ として[-2,2]の範囲の実根をもつ。

$$f(x)[q](e^{2\pi ik/(p-1)}), k \in p-1$$



上記の図で、絶対値 $\sqrt{p} = 14.10673598$ の二つの複素数は

$$f(x)[q]((-1\pm i\sqrt{3})/2) = (11\pm 15i\sqrt{3})/2$$

である。$x^{p-1}-1$ は因数として、$x^{11}-1$ をもつが、この剰余行列(residue matrix)

$$A = 1/p \cdot f(x)[q|x]x^{11}-1 = 1/p \cdot$$

$$\begin{pmatrix}
-38, -21, 46, -6, 70, 112, 20, 32, -108, 66, 26 \\
-21, 46, -6, 70, 112, 20, 32, -108, 66, 26, -38 \\
46, -6, 70, 112, 20, 32, -108, 66, 26, -38, -21 \\
-6, 70, 112, 20, 32, -108, 66, 26, -38, -21, 46 \\
70, 112, 20, 32, -108, 66, 26, -38, -21, 46, -6 \\
112, 20, 32, -108, 66, 26, -38, -21, 46, -6, 70 \\
20, 32, -108, 66, 26, -38, -21, 46, -6, 70, 112 \\
32, -108, 66, 26, -38, -21, 46, -6, 70, 112, 20 \\
-108, 66, 26, -38, -21, 46, -6, 70, 112, 20, 32 \\
66, 26, -38, -21, 46, -6, 70, 112, 20, 32, -108 \\
26, -38, -21, 46, -6, 70, 112, 20, 32, -108, 66
\end{pmatrix}$$

は巡回対称対合(cyclic simmetric involution, sci)である。$A^2 = E$

次数 5 の対称巡回対合(sci)に関しては、p = 1 mod 5 に対して常に 2 個

$$1/p \cdot F(1/3,2/3,1,x)[q|x][x^5-1], 1/p \cdot F(1/4,3/4,1,x)[q|x][x^5-1]$$

のみであろうと予想されている。また、7 に関しては p = 1 mod 7 に対して、本質的に、常に 5 個

$$1/p \cdot F(1/3,2/3,1,x)[q|x][x^7-1] \approx 1/p \cdot F(1/4,3/4,1,x)[q|x][x^7-1]$$

$$1/p\cdot F(1/6,5/6,1,x)\,[q|x]\,[x^7-1]\approx$$

$$1/p\cdot x^{(p-1)/4}\cdot F(1/12,5/12,1,1-x),\ x^{(p+1)/4}\cdot F(7/12,11/12,1,1-x)$$

の2個と、これらで記述できない2種類と、

$$[p\text{-}3\ (a+b),a,a,b,a,b,b]$$

の型の5種類に限ると予想されている。(7-sci problem, 7-sci conjecture)

p = 11, 13 などの素数に対しても、q = 1 mod p の素数に関しては

p sci は一定個数 sci(p)

個になるような関数 sci(p)が存在すると、今の段階では、予想している。

sci(5) = 2, sci(7) = 5, sci(11) = ?

4. 諸算法と有限フーリエ変換

先ず乗法との関連の例は一種の積である「たたみこみ」あるは合成積(convolution)と呼ばれる概念について述べる。

例. 次のものはπの10進表示の桁の50桁を記したものである。

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

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

これは多項式の係数表示(coefficient form)で多項式表示(polynomial form)は

$$f(x) = x^{39}+5x^{38}+7x^{37}+3x^{36}+9x^{35}+9x^{34}+3x^{33}+9x^{32}+6x^{31}+x^{40}+7x^{39}+9x^{38}+x^{37}+4x^{36}+8x^{35}$$
$$+8x^{34}+2x^{33}+5x^{31}+9x^{30}+7x^{29}+2x^{28}+3x^{27}+8x^{26}+3x^{25}+3x^{24}+4x^{23}+6x^{22}+2x^{21}+6x^{20}+4x^{19}+8x^{18}$$
$$+3x^{17}+2x^{16}+3x^{15}+9x^{14}+7x^{13}+9x^{12}+8x^{11}+5x^{10}+3x^{9}+5x^{8}+6x^{7}+2x^{6}+9x^{5}+5x^{4}+x^{3}+4x^{2}+x+3$$

である。積f(x)g(x)の係数表示は

fg =

[0, 15, 29, 34, 39, 68, 117, 147, 132, 166, 239, 204, 287, 354, 335, 348, 422, 415, 392,
506, 484, 496, 501, 499, 598, 525, 536, 569, 617, 617, 697, 738, 721, 672, 775, 822,
937, 853, 850, 883, 924, 939, 1063, 1084, 992, 957, 1135, 1094, 1054, 1038, 1207,
1107, 1061, 1080, 1106, 989, 958, 865, 970, 919, 968, 832, 756, 811, 837, 635, 738,
759, 714, 681, 625, 603, 698, 617, 537, 612, 623, 492, 491, 470, 371, 329, 348, 334,
346, 281, 226, 284, 215, 137, 214, 177, 113, 181, 126, 73, 86, 46, 8, 0, 0]

各次数の係数が所謂たたみこみ(コンボリューション, convolution)である。

この場合各桁の最大は9で項数の最大は50であるからfgの項の最大は

81×50 = 4050である。上の例では1135が最大である。100項までは必要である。1の101乗根を用いるとして、

$$p = 101n+1 > 4050$$

の形の素数は、

4243, 5051, 5657, 6263, 6869, 7879, 8081, 9091, 9293, 9697,…

のように無限に存在する。今はp = 4243とし、素体F_p = pを考える。pでは$x^{101}-1 = 0$は完全分解し、それらの101個の解は

1, 31, 85, 90, 210, 228, 265, 316, 327, 459, 486,…

1でない解はすべて$x^{101}-1$の原始根(primitive root with respect to $x^{101}-1$)である。念のため記すとmod pでの原始根ではない。q = 31として Fourier 変換[31]を考える。

f[31] = f(x)[31](x) =

[247, 1170, 3381, 3934, 2783, 1903, 709, 3451, 3522, 931, 0, 2264, 1584, 932, 711,
3900, 727, 1984, 2158, 3941, 3956, 1559, 2993, 3438, 382, 324, 1627, 208, 1510,
1931, 1465, 2591, 634, 3131, 2397, 1130, 2903, 378, 3167, 561, 1083, 395, 2098,
2111, 3886, 2802, 1152, 3240, 1296, 3564, 1681, 125, 1031, 1258, 1278, 2375, 929,
3963, 2520, 188, 38, 1881, 503, 17, 1639, 2114, 3207, 3882, 1347, 2594, 2832, 677,
4233, 1183, 319, 3124, 3628, 1779, 1322, 1725, 2224, 1430, 1823, 231, 3906, 572,
2194, 646, 1590, 966, 2949, 2424, 76, 1663, 1330, 824, 384, 2890, 3904, 1625, 1808]

g[31] = g(x)[31](x) =

[225, 608, 1983, 2602, 3936, 2921, 2675, 1697, 416, 772, 2853, 4192, 82, 2496, 2142,
2255, 343, 3095, 2404, 3572, 1005, 287, 1790, 3768, 857, 3289, 2028, 3160, 694, 3883,
503, 2498, 2809, 1501, 2115, 3597, 1146, 920, 3375, 2598, 4033, 3760, 2970, 2017,
582, 3707, 2546, 2321, 4006, 2842, 1735, 892, 272, 1632, 2922, 573, 935, 3967, 3751,
3368, 1227, 994, 3760, 2471, 2955, 289, 3221, 2889, 879, 4040, 281, 746, 3542, 1314,
2336, 847, 1809, 912, 3666, 1531, 687, 2533, 2055, 2234, 347, 2707, 4236, 3242,
1461, 3554, 3235, 3466, 845, 4146, 2087, 3468, 2907, 812, 2850, 3824, 2551]

であり、項別の積はmod pで

f•g =

[416, 2779, 583, 2152, 2705, 333, 4197, 1007, 1317, 1665, 0, 3340, 2598, 1108, 3968,
3004, 3267, 859, 2886, 3221, 89, 1918, 2804, 505, 663, 643, 2745, 3858, 4162, 692,
2856, 1743, 3089, 2630, 3513, 4059, 326, 4077, 508, 2129, 1692, 150, 2336, 2158, 133,

150, 1079, 1444, 2587, 847, 1594, 1182, 394, 3687, 476, 3115, 3043, 906, 3359, 977,
4196, 2794, 3145, 3820, 1982, 4197, 2285, 849, 216, 3793, 2351, 125, 2767, 1524,
2659, 2639, 3374, 1622, 946, 1829, 408, 2911, 3939, 2651, 1865, 3952, 1614, 2533,
2069, 577, 1751, 444, 575, 4166, 788, 2093, 379, 301, 1254, 2248, 67]

である。[31]の逆変換は、-1/101 mod p = 42, 1/31 mod p = 1095 により

-1/101[1/31] = 46[1095]

である。従って

46 f•g(x)[1095](x) =

[0, 15, 29, 34, 39, 68, 117, 147, 132, 166, 239, 204, 287, 354, 335, 348, 422, 415, 392,
506, 484, 496, 501, 499, 598, 525, 536, 569, 617, 617, 697, 738, 721, 672, 775, 822,
937, 853, 850, 883, 924, 939, 1063, 1084, 992, 957, 1135, 1094, 1054, 1038, 1207,
1107, 1061, 1080, 1106, 989, 958, 865, 970, 919, 968, 832, 756, 811, 837, 635, 738,
759, 714, 681, 625, 603, 698, 617, 537, 612, 623, 492, 491, 470, 371, 329, 348, 334,
346, 281, 226, 284, 215, 137, 214, 177, 113, 181, 126, 73, 86, 46, 8, 0, 0]

であり、多項式としての積 fg(x) = f(x)g(x)が f(x),g(x)の有限 Fourier 変換(= fFt)の項別積の有限 Fourier 変換(inverse finite fourier transformation, ifFt)に等しいというよく知られた性質を示している。計算量(computational complexity, computational amount)については高速有限 Fourier 変換(fast finite fourier transformation, ffFt)との関係は特に重要である。

例. 合成関数の場合

係数は適当に選んだ次の多項式

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

の合成平方(compositinal square) f(f(x))を考えてみよう。

(100 次)係数表示では

f(f(x)) =

$$x^{81}+9x^{80}+27x^{79}+3x^{78}-153x^{77}-225x^{76}+\cdots+343x^5-123x^4+47x^3-17x^2+7x-4$$

=

[-4, 7, -17, 47, -123, 343, -827, 1720, -3170, 5188, -7713, 10619, -13557, 16013, -17421,
17372, -16041, 14003, -11297, 7957, -4915, 3177, -3639, 4746, -3741, 2830, -4186, 5935,
-5757, -37, 4241, 2658, -5599, -734, 4763, -5566, -7561, 15169, 12309, -15538, -15027,
8752, 2105, -7053, 23246, 23449, -39231, -50546, 27339, 60002, 525, -32379, -10585,
-16544, -18567, 47228, 71343, -34418, -108899, -9697, 106265, 51593, -70004, -66174,

27193, 54116, 1161, -31181, -10477, 12517, 8687, -2809, -4219, -162, 1341, 423, -225,
-153, 3, 27, 9, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

である。合成関数の係数の範囲の計算はなかなか難しい問題ですが、今の場合は、最大最小は-108899, 106265 です。例えば f(f(f(x)))では

-539624124407348535546332468834898758353683344716052,
528145208990995545028840896487860192178972363186417

で、f(f(f(f(x))))の場合は計算していませんが…。

以前同様、例えば $x^{101}-1$ を用い(少し余裕をもって)300000 > 108899+106265 程度の素数を考える。この範囲の 101n+1 型の素数は

300779, 301183, 301789, 301991, 302597, 305021, 307243, 308051, 309667, …

などです。今は p-1 = 300778 = 2·101·1489 を考えましょう。$x^{101}-1$ mod p の解は

1, 6068, 7296, 7910, …, 295155, 295389, 296626

です。1 でない数は $x^{101}-1$ mod p での原始根です。例えば q = 7296 としましょう。F_p = 300779 で

f[q](x) =

$$53141x^{100}+241070x^{99}+63492x^{98}+\cdots+256015x^3+257440x^2+116459x+2 =$$

[2, 116459, 257440, 256015, 185408, 227172, 12569, 160332, 24566, 61735, 149907,
261867, 71399, 31181, 157968, 222111, 228109, 161685, 261757, 204663, 79092,
146789, 220704, 63227, 161076, 196710, 297867, 273388, 263644, 194277, 110259,
266487, 10216, 253504, 75336, 166035, 73234, 73385, 190790, 97906, 168475,
93579, 94799, 202872, 123191, 228031, 63969, 11988, 258292, 192946, 1090,
210447, 280636, 200921, 52762, 102173, 111131, 80580, 159489, 4962, 210674,
136389, 212205, 214447, 91047, 114034, 293300, 98609, 169733, 201055, 280319,
35714, 184034, 13552, 270410, 256420, 161859, 45282, 296914, 269807, 181060,
285307, 189835, 274960, 263465, 254930, 168608, 110633, 94286, 235501, 186414,
169545, 3763, 276075, 55291, 19762, 149593, 200047, 63492, 241070, 53141]

従って、係数毎に f(x) mod p を計算したものは、例えば f(2) = 629 で、

f0f =

[629, 121379, 28203, 227555, 51419, 145308, 167481, 8463, 66199, 250010, 247307,
269381, 271193, 271725, 149881, 229415, 283356, 38059, 127086, 283132, 173824, 63368,
160003, 169912, 243316, 44629, 204164, 176720, 288391, 262908, 23187, 98814, 171510,

285534, 224929, 192807, 182929, 156636, 62830, 44445, 45406, 237700, 205958, 275073,
164313, 48557, 268711, 87719, 275280, 289567, 147942, 203887, 16587, 281008, 36782,
171555, 220166, 300478, 261245, 87391, 290264, 237711, 241754, 220920, 120023, 16717,
97262, 126298, 269180, 216917, 241115, 210685, 267123, 44874, 144231, 78777, 182137,
59731, 65130, 298618, 277344, 251605, 73688, 205905, 236409, 257642, 147026, 58970,
136377, 207226, 238257, 83027, 331, 64243, 186010, 291342, 211095, 48723, 25423,
126397, 193351]

です。また、-1/101 mod p = 2978, 1/7296 mod p = 144989 により

-1/101[1/7296] = 2978[144989]

だから、絶対値最小剰余(= lavr)として

-2978f◎f[144989] = f(f(x)) =

[-4, 7, -17, 47, -123, 343, -827, 1720, -3170, 5188, -7713, 10619, -13557, 16013, -17421,
17372, -16041, 14003, -11297, 7957, -4915, 3177, -3639, 4746, -3741, 2830, -4186, 5935,
-5757, -37, 4241, 2658, -5599, -734, 4763, -5566, -7561, 15169, 12309, -15538, -15027,
8752, 2105, -7053, 23246, 23449, -39231, -50546, 27339, 60002, 525, -32379, -10585,
-16544, -18567, 47228, 71343, -34418, -108899, -9697, 106265, 51593, -70004, -66174,
27193, 54116, 1161, -31181, -10477, 12517, 8687, -2809, -4219, -162, 1341, 423, -225,
-153, 3, 27, 9, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

であることが確認される。

例. 楕円曲線 $y^2 = x^3+47x+78$, p = 101 の場合。

$$f(x) = (x^3+47x+78)^{(p-1)/2} = (x^3+47x+78)^{50}$$

を mod p で計算する問題を考える。直接計算の結果は

$$f(x) \mod p =$$

$$x^{150}+27x^{148}+62x^{147}+33x^{146}+73x^{145}+\cdots$$

$$+7x^{100}+33x^{99}+25x^{98}+63x^{97}+85x^{96}+33x^{95}+99x^{94}+5x^{93}+49x^{92}+34x^{91}+35x^{90}+\cdots$$

$$+13x^5+14x^4+89x^3+14x^2+12x+1$$

であり、素体 $F_p = p = 101$ の特性多項式 $x(x^{100}-1)$ での剰余 mod p は

$$f_p(x) = \mathrm{rem}(f(x), x(x^{100}-1), x) \mod p =$$

$$7x^{100}+33x^{99}+25x^{98}+63x^{97}+85x^{96}+33x^{95}+\cdots+90x^6+64x^5+48x^4+74x^3+98x^2+24x+1 =$$

[1, 24, -3, 74, 48, -37, -11, 9, -27, -50, 20, 43, -14, 14, 59, -20, 18, 12, -3, 6,
-43, -1, 34, 33, -39, -22, -15, -50, -8, 9, 35, 4, -20, 17, -20, -18, 72, 42, -8, 76,
53, -22, 9, 27, 11, -26, -6, -2, -49, -7, -8, 11, -26, -33, -50, -34, 34, -23, -43, 19,

-26, -20, -21, 43, -37, 24, 50, 38, -28, -17, 9, -3, 21, 11, -14, 18, -26, -30, -24, -34,
-42, -5, 16, -34, -21, 42, 37, -3, 8, 30, 35, 34, 49, 5, -2, 33, -16, -38, 25, 33, 7]

である。大切な事は、p = {0, 1, …, p-1} = 101 の各点では $f_p(x) = f(x)$ となること(pointwise equal)ということです。勿論、$f_p(x)$ は 100 次、f(x) は 150 次多項式ですから形式(多項式として)は異なる(formaly different)。

有限体 p の特性多項式(生成多項式, characteristic, generating polynomial)は p のすべての点で 0 となる(多項式としては 0 でない)多項式で、この多項式での商空間(剰余, residue polynomial)が $f_p(x)$ です。Fourier 変換は実・相の「かけはし」なのです。要するに生成多項式は真空(vacuum space)を意味し、これを ideal の生成元(generator)と考えた剰余環(residue ring)を考えている訳です。

$$\delta(x) = 1-x^{p-1}$$

についても、$x-x^p = x\,d(1-x^{p-1}) = x\delta(x)$ であり、$x-x^p$ を space polynomial と呼んで、その一つの因数と考えることもできる。狭義有限 Fourier 変換は δ(x) 上の変換なのである。

p = 101 の原始根 q = 2 による変換は

$$x^3+47x+78[2](x) =$$

$$-12x^{99}+44x^{98}-26x^{97}-48x^{96}+31x^{95}+\cdots+22x^7+4x^6+10x^5-23x^4-44x^3+27x^2-22x+25 =$$

[25, -22, 27, -44, -23, 10, 4, 22, -5, 43, 46, 15, -40, 7, 44, -35, -3, -35, 42, 11,
-16, 8, -27, 47, 34, 33, 29, 5, 31, -32, 33, -26, -40, -44, 39, 24, -40, -36, 18, -11,
47, -20, -2, 38, 49, 24, 2, -20, 11, -34, 30, -24, 28, -2, -23, 45, -50, 33, -41, 12,
9, 40, -6, 48, 11, -11, -43, -11, 13, 44, -30, 47, -19, 8, 21, 22, 26, 50, 24, -14,
22, -20, -6, -2, 16, 31, -6, -10, 37, -35, 8, -26, -44, 17, 6, 31, -48, -26, 44, -12]

であり 3 次式を計算したものの表です。個別に (p-1)/2 = 50 乗すると平方剰余(Legendre symbol)の列

$$f(x)[2](x) = (x^3+47x+78)^{(p-1)/2}[2](x) =$$

$$-x^{99}-x^{98}-x^{97}-x^{96}+x^{95}+x^{94}+\cdots+x^9+x^8+x^7+x^6-x^5+x^4-x^3-x^2+x+1 =$$

[1, 1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, -1, -1, -1, -1, -1, -1, -1, 1, -1, -1, 1, -1,
1, -1, 1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, -1, -1, -1, 1, 1, -1, -1, 1, 1, -1, 1, -1, -1,
1, 1, -1, -1, 1, 1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, 1, 1, -1, 1,
1, -1, -1, 1, 1, 1, 1, 1, -1, 1, 1, 1, -1, 1, -1, -1, -1, -1, 1, 1, 1, -1, -1, -1, -1]

が得られます。1/2 mod p = -50 = 51 ですから逆変換 -[51]を施すと

$$-(x^3+47x+78)^{(p-1)/2}[2][51](x) =$$

$$33x^{99}+25x^{98}-38x^{97}-16x^{96}+33x^{95}-2x^{94}+\cdots-11x^6-37x^5+48x^4-27x^3-3x^2+24x+8 =$$

[8, 24, -3, -27, 48, -37, -11, 9, -27, -50, 20, 43, -14, 14, -42, -20, 18, 12, -3, 6,
-43, -1, 34, 33, -39, -22, -15, -50, -8, 9, 35, 4, -20, 17, -20, -18, -29, 42, -8, -25,
-48, -22, 9, 27, 11, -26, -6, -2, -49, -7, -8, 11, -26, -33, -50, -34, 34, -23, -43, 19,
-26, -20, -21, 43, -37, 24, 50, 38, -28, -17, 9, -3, 21, 11, -14, 18, -26, -30, -24, -34,
-42, -5, 16, -34, -21, 42, 37, -3, 8, 30, 35, 34, 49, 5, -2, 33, -16, -38, 25, 33]

が得られる。

$$f_p(x) = \mathrm{rem}(f(x), x(x^{100}-1), x) \mod p =$$

$$7x^{100}+33x^{99}+25x^{98}+63x^{97}+85x^{96}+33x^{95}+\cdots+90x^5+64x^4+48x^3+74x^2+24x+1 =$$

[1, 24, -3, 74, 48, -37, -11, 9, -27, -50, 20, 43, -14, 14, 59, -20, 18, 12, -3, 6,
-43, -1, 34, 33, -39, -22, -15, -50, -8, 9, 35, 4, -20, 17, -20, -18, 72, 42, -8, 76,
53, -22, 9, 27, 11, -26, -6, -2, -49, -7, -8, 11, -26, -33, -50, -34, 34, -23, -43, 19,
-26, -20, -21, 43, -37, 24, 50, 38, -28, -17, 9, -3, 21, 11, -14, 18, -26, -30, -24, -34,
-42, -5, 16, -34, -21, 42, 37, -3, 8, 30, 35, 34, 49, 5, -2, 33, -16, -38, 25, 33, 7]

と比較すると、上の式は 99 次式で下の式は 100 次の式です。100 次の項 7 が定数項に加算されています。この 7 こそ Poincaré-Mordell-Weil 群、あるいは合同ゼータ核 (congruent ζ-kernel) の trace の項 a_p なのです。

$$x^2-a_px+1,\ a_p = 7$$

つまり、$-(x^3+47x+78)^{(p-1)/2}[2][51](x)$ は p-2 次なので p-1 次の $\delta(x) = 1-x^{p-1}$ での「割算」、つまり、商・剰余分解 (quotient-residue resolution)

$$(x^3+47x+78)^{(p-1)/2} = q(x)\delta(x)+r(x)$$

$$r(x) = -(x^3+47x+78)^{(p-1)/2}[2][51](x)$$

の商 (quotient) 部分

$$(x^3+47x+78)^{(p-1)/2}/\delta(x)$$

の定数項は重要な役割をもっている。ρ を 1 の原始 p-1 乗根とすると微分は $F_p = p$ では

$$dx(1-x^{p-1})/dx =$$

$$(1-x^{p-1})+x(1-x^{p-1})/(1-\rho^0x)+\rho^1x(1-x^{p-1})/(1-\rho^1x)+\cdots+\rho^{p-2}x(x^{p-1}-1)/(1-\rho^{p-2}x)$$

である。一般 Vandermonde の行列 (generalized Vandermonde matrix) は、定数による微分記号はないが、仮に、

$$dx(x^{p-1}-1)/dk = x(1-x^{p-1})/(1-kx)$$

と記すとき、

$$x(1-x^{p-1})/(1-\rho^0x)$$

$$x(1-x^{p-1})/(1-\rho^1x)$$

$$\cdots$$

$$x(1-x^{p-1})/(1-\rho^{p-2}x)$$

$$1-x^{p-1}$$

の x の係数を昇冪の順に並べた p 次正方行列

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 0 \\ 1 & \rho & \rho^2 & \cdots & \rho^{p-2} & 0 \\ 1 & \rho^2 & \rho^4 & \cdots & \rho^{2(p-2)} & 0 \\ & \cdots & & \cdots & & \\ 1 & \rho^{p-2} & \rho^{2(p-2)} & \cdots & \rho^{(p-2)(p-2)} & 0 \\ 1 & 0 & 0 & \cdots & 0 & -1 \end{pmatrix}$$

による p 上の p-1 次多項式の p 次元空間

$$F_p^p[x] = \{a_0+a_1x+\cdots+a_{p-1}x^{p-1} : a_j \in p\} = p^p = p \text{ to } p = p2p$$

の線形変換で

$$f(x) = a_0+a_1x+\cdots+a_{p-2}x^{p-2}$$

とするとき、q = ρ として、指数 p-1 は特別扱いで

$$a_0+a_1x+\cdots+a_{p-1}x^{p-1}\ [q](x) =$$

$$(1-x^{p-1})(a_0/(1-x)+a_1/(1-qx)+\cdots+a_{p-2}/(1-q^{p-2}x)+a_{p-1})$$

$$= f(1)+f(p)x+\cdots+f(p^{p-2})x^{p-2}+a_{p-1}(1-x^{p-1})$$

というものです。つまり、x^{p-1} の項は定数項とのみ $\delta(x) = 1-x^{p-1}$ の交渉関係をもち、p-2 多項式の空間は (通常) の Vandermonde 変換 (ここでは有限 Fourier 変換と呼んでいますが) 不変空間 (invariant space) となっているのです。Fourier 性 (Fourier property)、つまり、$F^4 = E$ (4 回作用させると元に戻る) が成立することは一般 Fourier 変換でも同様です。差は $a_{p-1}(1-x^{p-1})$ のみです。この差が楕円曲線の場合には特性数なのです。

$$\delta(x) = 1-x^{p-1} = 1 \text{ iff } x = 0$$

の意味は「x (= I,私) は 0 である」(= x is 0) ということです。

例. 割り算の場合

互いに素 (relatively prime) な多項式

$$f(x) = a_0+a_1x+\cdots+a_{p-2}x^{p-2}$$

$$g(x) = b_0+b_1x+\cdots+b_{p-2}x^{p-2}$$

に対し、商

$$h(x) = g(x)/f(x) = c_0+c_1x+\cdots+c_{p-2}x^{p-2}$$

が定まるのはどのような場合でしょうか。答は勿論 $a_0 \neq 0$ で $f(x)$ が F_p で重複のない1次因子に完全分解すること、つまり、$1-x^{p-1}$ は完全分解しますから、$f(x)$ は $1-x^{p-1}$ の因数で

$$1-x^{p-1} = f(x)\,k(x)$$

となる多項式が存在することです。従って、

$$h(x) = g(x)/f(x) = g(x)\,k(x) \mod 1-x^{p-1}$$

が求めるものです。有限 Fourier 変換との関連では、反対に

$$f(x)[q](x) = f(1)+f(p)x+\cdots+f(p^{p-2})x^{p-2}$$

の各係数が $f(p^i) \neq 0$ ということです。これは $f(x)$ と $1-x^{p-1}$ は共通因子をもたないことです。この場合、$s(p^i) = g(p^i)/f(p^i)$ を計算して

$$s(x) = s(1)+s(p)x+\cdots+s(p^{p-2})x^{p-2}$$

として、逆 Fourier 変換 $[q]^{-1}$ を考えることができます:

$$s(x)[q]^{-1}(x)$$

上に記したような、異なる二つの性質

$f(x)$ は $1-x^{p-1}$ の因子 ($f(x)$ is a factor of $1-x^{p-1}$)

$f(x)$ と $1-x^{p-1}$ は互いに素 ($f(x)$ and $1-x^{p-1}$ are relatively prime)

と多項式の商 (quotient of polynomials) の関係は興味ある研究対象です。

例. $p = 101$, $q = 99$, $f(x) = x^{(p-1)/4}F(1/12,5/12,1,1-x)$, $f(x)/(19+f(x))$

この赤穂式は有限体上の楕円曲線の Weierstrass 標準形に対応する楕円位数多項式 (= elop) です。今の場合 $p = 101$ で原始根 (primitive root) は

2, 3, 7, 8, 11, 12, 15, 18, 26, 27, 28, 29, 34, 35, 38, 40, 42, 46, 48, 50,

51, 53, 55, 59, 61, 63, 66, 67, 72, 73, 74, 75, 83, 86, 89, 90, 93, 94, 98, 99

の 40 個ありますが、例えば $q = 99$ を考えましょう。

$$(p-1)/4 = 25,\ F(1/12,5/12,1,x) = -31x^8+27x^7+31x^6-50x^5+25x^4+15x^3-31x^2+33x+1$$

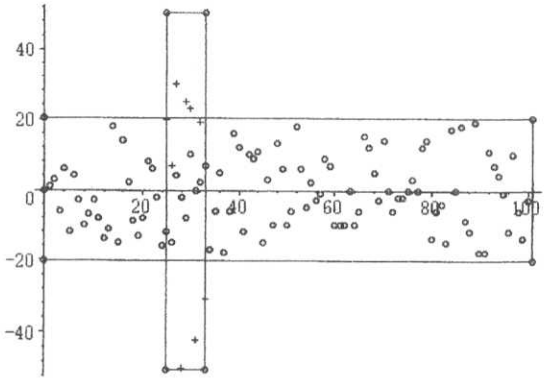
ですから、

$$f(x) = x^{(p-1)/4}F(1/12,5/12,1,1-x) = x^{25}(70x^8+19x^7+59x^6+23x^5+25x^4+51x^3+30x^2+7x+20)$$

です。Hasse の不等式から

$$|f(x)| < 2\sqrt{101} = 20.09975124\cdots$$

以下の図は $f(x)$ と $f(x)[99](x)$ の係数を表示したものです。



勿論、有限 Fourier 変換の係数は $f(x)$ の値です。いまの場合は

$$[-18, \cdots, 19]$$

の範囲のすべての整数で、Hasse の範囲でこれに属さないものは -20, -19, 20 の 3 個です。従って、例えば

$$(19+f(x))[99](x)$$

の係数はすべて 0 ではありませんから逆元が存在します。勿論、

$$f(x)[99](x)+19$$

とは異なります。

$$f(x)[99](x) =$$

$$-10x^{99}+3x^{98}-13x^{96}-12x^{95}+10x^{94}+18x^{93}+9x^{92}-6x^{91}-6x^{90}-9x^{89}+11x^{88}+2x^{87}-2x^{86}+16x^{85}-6x^{83}+7x^{82}$$

$$-17x^{81}+17x^{80}+7x^{79}+8x^{78}+12x^{77}-6x^{76}-3x^{75}-12x^{74}+6x^{73}-16x^{72}+19x^{71}+4x^{70}-6x^{69}+18x^{68}-11x^{66}+11x^{65}$$

$$+14x^{64}-8x^{63}-15x^{62}-2x^{61}-9x^{60}-3x^{59}-10x^{58}+4x^{57}-18x^{56}+2x^{55}-10x^{53}+10x^{52}+3x^{51}-3x^{50}-6x^{49}-12x^{48}-6x^{47}$$

$$-4x^{46}-10x^{45}-15x^{43}+9x^{42}-8x^{41}+5x^{40}-15x^{39}-7x^{38}+3x^{37}+12x^{36}-10x^{35}+14x^{34}+15x^{33}+5x^{32}+12x^{31}+2x^{30}$$

$$+10x^{29}-14x^{28}-10x^{27}-8x^{26}-18x^{25}-12x^{24}+13x^{23}-14x^{21}-x^{20}-6x^{19}+6x^{18}-15x^{17}-12x^{16}-x^{15}+6x^{14}-18x^{13}-3x^{12}$$

$$-2x^{11}+18x^{10}+4x^9-5x^8-2x^7-10x^6-3x^5+14x^4+7x^3+6x^2-14x+1$$

であり、この場合は x^{21}, x^{44}, x^{54}, x^{67}, x^{84}, x^{97} などの係数は 0 ですから逆元は存在しません。しかし、$(19+f(x))[99](x)$ の場合は係数にすべて 19 が加わりますから、係数は、最小剰余 (lavr) の形で記しますが

$$h(x) = (19+f(x))[99](x) =$$

$$9x^{99}+22x^{98}+19x^{97}+6x^{96}+7x^{95}+\cdots+16x^5+33x^4+26x^3+25x^2+5x+20 =$$

$$[20, 5, 25, 26, 33, 16, 9, 17, 14, 23, 37, 17, 16, 1, 25, 18, 7, 4, 25, 13,$$

18, 5, 19, 32, 7, 1, 11, 9, 5, 29, 21, 31, 24, 34, 33, 9, 31, 22, 12, 4,
24, 11, 28, 4, 19, 9, 15, 13, 7, 13, 16, 22, 29, 9, 19, 21, 1, 23, 9, 16,
10, 17, 4, 11, 33, 30, 8, 19, 37, 13, 23, 38, 3, 25, 7, 16, 13, 31, 27, 26,
36, 2, 26, 13, 19, 35, 17, 21, 30, 10, 13, 13, 28, 37, 29, 7, 6, 19, 22, 9]

です。項の mod p での逆元の列は

[-5, -20, -4, 35, 49, 19, 45, 6, -36, 22, -30, 6, 19, 1, -4, -28, 29, -25, -4, -31,
-28, -20, 16, -41, 29, 1, 46, 45, -20, 7, -24, -13, -21, 3, 49, 45, -13, 23, -42, -25,
-21, 46, -18, -25, 16, 45, 27, -31, 29, -31, 19, 23, 7, 45, 16, -24, 1, 22, 45, 19, -10,
6, -25, 46, 49, -37, 38, 16, -30, -31, 22, 8, 34, -4, 29, 19, -31, -13, 15, 35, -14,
-50, 35, -31, 16, 26, 6, -24, -37, -10, -31, -31, -18, -30, 7, 29, 17, 16, 23, 45]

であり、この fourier 逆変換 $[99]^{-1} = -[1/99] = -[50]$ 列は

$$m(x) = -(19+f(x))[99][50](x) =$$

[-48, 44, -3, 23, 9, 42, -43, -40, 16, 4, -23, 4, -46, 34, 25, 17, -41, -35, 11, 39,
-34, 32, 49, -21, -2, -44, -23, -28, -10, -8, -49, -18, -14, 13, 10, -25, -5, 36, -50,
-42, 46, -35, 2, -48, -28, -50, -7, -47, 30, -4, 19, -41, -11, -31, -19, -20, 1, 3,
-27, -14, -37, -1, 47, -34, -37, 15, 50, 13, -13, 48, 28, 3, -26, -37, 10, 29, -1, 19,
11, 12, 6, 50, 17, -23, -10, -39, 23, -31, -16, 43, -1, 36, 38, 40, 41, 11, -11, 12, -49, -19]

と、係数列表示(coefficient sequence representation)される。現実には

$$19+f(x) = 19+x^{25}(70x^8+19x^7+59x^6+23x^5+25x^4+51x^3+30x^2+7x+20) =$$
$$70x^{33}+19x^{32}+59x^{31}+23x^{30}+25x^{29}+51x^{28}+30x^{27}+7x^{26}+20x^{25}+19$$

であり、

$$s(x) =$$
$$-17x^{32}+47x^{31}-32x^{29}-30x^{28}+7x^{27}-6x^{26}-22x^{25}+38x^{24}-5x^{23}-22x^{22}-2x^{21}+40x^{20}-34x^{19}-7x^{18}-42x^{17}-29x^{16}$$
$$-20x^{15}+30x^{14}-40x^{13}-35x^{12}+25x^{11}+33x^{10}+25x^9-x^8-48x^7+9x^6+10x^5+31x^4-33x^3-44x^2-28x+4$$

として、最大公約数(gcd)の等式

$$m(x)(19+f(x))-s(x)(x^{p-1}-1) = 1$$

を得ている。

これらの概念を少し一般化して 0 でない係数の逆元を採用した場合は、例えば、上記の

$$f(x) = F(1/12,5/12,1,x) = -31x^8+27x^7+31x^6-50x^5+25x^4+15x^3-31x^2+33x+1 =$$
$$70(x+30)(x+62)(x+70)(x+74)(x+76)(x+84)(x^2+56x+49)$$

ですから、$x^{p-1}-1$ と互いに素な因子

$$f(x)/\gcd(x^{p-1}-1,f(x)) = x^2+56x+49$$

を考えると、その有限体 $F_p = p$ での値は常に 0 でなく逆元が存在する。今同様に p = 101 とし、原始根として、q = 8 をとると、逆変換は

$$[8]^{-1} = -[1/8] = -[38]$$

である。• を項の逆数の変換とし Fourier 変換を計算すると

$$h(x) = -(x^3+56x+49[8]\bullet[38](x)) =$$
$$50x^{89}-36x^{88}-30x^{87}+10x^{86}+x^{85}-41x^{84}+25x^{83}+3x^{82}+21x^{81}-10x^{80}+36x^{89}-11x^{88}-37x^{87}-15x^{86}$$
$$+27x^{85}+31x^{84}-29x^{83}+4x^{82}-15x^{81}+38x^{80}+21x^{79}-8x^{78}+25x^{77}+2x^{76}-24x^{75}+34x^{74}-21x^{73}+15x^{72}$$
$$-13x^{71}-7x^{70}+19x^{69}-14x^{68}-46x^{67}+30x^{66}-32x^{65}+19x^{64}-x^{63}+34x^{62}-37x^{61}+2x^{60}-16x^{59}-10x^{58}+31x^{57}$$
$$-34x^{56}-19x^{55}+3x^{54}-45x^{53}+50x^{52}+11x^{51}-36x^{50}-38x^{49}-47x^{48}+50x^{47}+8x^{46}+31x^{45}-7x^{44}-16x^{43}$$
$$+27x^{42}-21x^{41}-46x^{40}-31x^{39}-50x^{38}-24x^{37}-44x^{36}+4x^{35}+13x^{34}-15x^{33}+x^{32}-28x^{31}+4x^{30}+37x^{29}-46x^{28}$$
$$-45x^{27}+27x^{26}-14x^{25}-34x^{24}-36x^{23}+46x^{22}-4x^{21}-10x^{20}+49x^{19}-32x^{18}-3x^{17}+19x^{16}-8x^{15}+22x^{14}$$
$$-32x^{13}+7x^{12}-36x^{11}-44x^{10}-14x^9+11x^8-31x^7-15x^6+36x^5+32x^4-21x^3+12x^2-47x+24$$

が得られる。これは

$$h(x)(x^2+56x+49) = (50x+37)(x^{100}-1)+1$$

を意味している。つまり、法 $x^{100}-1$ で h(x)は $x^2+56x+49$ の逆元である。大切な点は同じ結果に至る複数の道があることで、恐らくそこには複雑さの差がある可能性がある。

勿論、通常の級数展開

$$1/(49+56x+x^2) =$$
$$1/49-8/343\cdot x+9/343\cdot x^2-496/16807\cdot x^3+3905/117649\cdot x^4$$
$$-4392/117649\cdot x^5+242047/5764801\cdot x^6-1905632/40353607\cdot x^7+\cdots$$

を有限体 $F_p = p = 101$ で計算した

$$\cdots -22x^{102}-33x^{100}+30x^{99}+38x^{98}+38x^{97}+50x^{96}-16x^{95}-39x^{94}+39x^{93}+30x^{92}+45x^{91}+50x^{90}+$$
$$\cdots -3x^{10}-x^{29}+x^8-7x^7+40x^6+22x^5+40x^4+15x^3+28x^2+20x+33$$

の x^{99} 項以下の多項式とは異なる。

5. 有限高速 Fourier 変換(finite fast Fourier transform, ffFt)

先ず、例から始めよう。整数の素因数分解、Vandermonde 行列の分解定理(factorization theorem of Vandermonde matrix, ftVm)の話である。Vandermonde 行列は $V = (x^n)$ の形の行列である。

例えば、$12 = 2^2\cdot 3$ の場合、$x^{12}-1 = 0$ の解 x に対し次のような疎行列(sparse

matrix) A, B, C を考える。

$$A = \begin{pmatrix}
1,0,0,0,0,0,1,0,0,0,0,0\\
0,1,0,0,0,0,0,x,0,0,0,0\\
0,0,1,0,0,0,0,0,x^2,0,0,0\\
0,0,0,1,0,0,0,0,0,x^3,0,0\\
0,0,0,0,1,0,0,0,0,0,x^4,0\\
0,0,0,0,0,1,0,0,0,0,0,x^5\\
1,0,0,0,0,0,x^6,0,0,0,0,0\\
0,1,0,0,0,0,0,x^7,0,0,0,0\\
0,0,1,0,0,0,0,0,x^8,0,0,0\\
0,0,0,1,0,0,0,0,0,x^9,0,0\\
0,0,0,0,1,0,0,0,0,0,x^{10},0\\
0,0,0,0,0,1,0,0,0,0,0,x^{11}
\end{pmatrix}$$

$$B = \begin{pmatrix}
1,0,0,0,0,0,1,0,0,0,0,0\\
0,1,0,0,0,0,0,x^2,0,0,0,0\\
0,0,1,0,0,0,0,0,x^4,0,0,0\\
1,0,0,0,0,0,x^5,0,0,0,0,0\\
0,1,0,0,0,0,0,x^8,0,0,0,0\\
0,0,1,0,0,0,0,0,x^{10},0,0,0\\
0,0,0,1,0,0,0,0,0,1,0,0\\
0,0,0,0,1,0,0,0,0,0,x^2,0\\
0,0,0,0,0,1,0,0,0,0,0,x^4\\
0,0,0,1,0,0,0,0,0,x^6,0,0\\
0,0,0,0,1,0,0,0,0,0,x^8,0\\
0,0,0,0,0,1,0,0,0,0,0,x^{10}
\end{pmatrix}$$

$$C = \begin{pmatrix}
1,0,0,0,1,0,0,0,1,0,0,0\\
1,0,0,0,x^4,0,0,0,x^8,0,0,0\\
1,0,0,0,x^8,0,0,0,x^4,0,0,0\\
0,1,0,0,0,1,0,0,0,1,0,0
\end{pmatrix}$$

$$\begin{pmatrix}
0,1,0,0,0,x^4,0,0,0,x^8,0,0\\
0,1,0,0,0,x^8,0,0,0,x^4,0,0\\
0,0,1,0,0,0,1,0,0,0,1,0\\
0,0,1,0,0,0,x^4,0,0,0,x^8,0\\
0,0,1,0,0,0,x^8,0,0,0,x^4,0\\
0,0,0,1,0,0,0,1,0,0,0,1\\
0,0,0,1,0,0,0,x^4,0,0,0,x^8\\
0,0,0,1,0,0,0,x^8,0,0,0,x^4
\end{pmatrix}$$

このとき、

$$ABC = {}^tC{}^tB{}^tA = V = (x^9) =$$

$$\begin{pmatrix}
1,1,1,1,1,1,1,1,1,1,1,1\\
1,x,x^2,x^3,x^4,x^5,x^6,x^7,x^8,x^9,x^{10},x^{11}\\
1,x^2,x^4,x^6,x^8,x^{10},1,x^2,x^4,x^6,x^8,x^{10}\\
1,x^3,x^6,x^9,1,x^3,x^6,x^9,1,x^3,x^6,x^9\\
1,x^4,x^8,1,x^4,x^8,1,x^4,x^8,1,x^4,x^8\\
1,x^5,x^{10},x^3,x^8,x,x^6,x^{11},x^4,x^9,x^2,x^7\\
1,x^6,1,x^6,1,x^6,1,x^6,1,x^6,1,x^6\\
1,x^7,x^2,x^9,x^4,x^{11},x^6,x,x^8,x^3,x^{10},x^5\\
1,x^8,x^4,1,x^8,x^4,1,x^8,x^4,1,x^8,x^4\\
1,x^9,x^6,x^3,1,x^9,x^6,x^3,1,x^9,x^6,x^3\\
1,x^{10},x^8,x^6,x^4,x^2,1,x^{10},x^8,x^6,x^4,x^2\\
1,x^{11},x^{10},x^9,x^8,x^7,x^6,x^5,x^4,x^3,x^2,x
\end{pmatrix}$$

この行列表示 (= 行列因数分解, matrix factorization) は積表示 12 = 2×2×3 に応ずるもので、12 = 2×3×2 では

$$B_1 = \begin{pmatrix}
1,0,0,0,1,0,0,0,1,0,0,0\\
0,1,0,0,0,x^2,0,0,0,x^4,0,0\\
1,0,0,0,x^4,0,0,0,x^8,0,0,0\\
0,1,0,0,0,x^6,0,0,0,1,0,0\\
1,0,0,0,x^8,0,0,0,x^4,0,0,0\\
0,1,0,0,0,x^{10},0,0,0,x^8,0,0\\
0,0,1,0,0,0,1,0,0,0,1,0
\end{pmatrix}$$

$$\begin{pmatrix} 0,0,0,1,0,0,0,x^2,0,0,0,x^4 \\ 0,0,1,0,0,0,0,x^4,0,0,0,x^8,0 \\ 0,0,0,1,0,0,0,x^6,0,0,0,1 \\ 0,0,1,0,0,0,0,x^8,0,0,0,x^4,0 \\ 0,0,0,1,0,0,0,x^{10},0,0,0,x^8 \end{pmatrix}$$

$C_1 =$

$$\begin{pmatrix} 1,0,0,0,0,0,1,0,0,0,0,0 \\ 1,0,0,0,0,0,x^6,0,0,0,0,0 \\ 0,1,0,0,0,0,0,1,0,0,0,0 \\ 0,1,0,0,0,0,0,x^6,0,0,0,0 \\ 0,0,1,0,0,0,0,0,1,0,0,0 \\ 0,0,1,0,0,0,0,0,x^6,0,0,0 \\ 0,0,0,1,0,0,0,0,0,1,0,0 \\ 0,0,0,1,0,0,0,0,0,x^6,0,0 \\ 0,0,0,0,1,0,0,0,0,0,1,0 \\ 0,0,0,0,1,0,0,0,0,0,x^6,0 \\ 0,0,0,0,0,1,0,0,0,0,0,1 \\ 0,0,0,0,0,1,0,0,0,0,0,x^6 \end{pmatrix}$$

とすれば、尤も $x^6 = -1$ だからこの行列は実行列であるが、

$$AB_1C_1 = V$$

が成立する。また、勿論、$12 = 3\times2\times2$ に対応しても

$A_1 =$

$$\begin{pmatrix} 1,0,0,0,1,0,0,0,1,0,0,0 \\ 0,1,0,0,0,x,0,0,0,x^2,0,0 \\ 0,0,1,0,0,0,x^2,0,0,0,x^4,0 \\ 0,0,0,1,0,0,0,x^3,0,0,0,x^6 \\ 1,0,0,0,x^4,0,0,0,x^8,0,0,0 \\ 0,1,0,0,0,x^5,0,0,0,x^{10},0,0 \\ 0,0,1,0,0,0,x^6,0,0,0,1,0 \\ 0,0,0,1,0,0,0,x^7,0,0,0,x^2 \\ 1,0,0,0,x^8,0,0,0,x^4,0,0,0 \\ 0,1,0,0,0,x^9,0,0,0,x^6,0,0 \end{pmatrix}$$

$$\begin{pmatrix} 0,0,1,0,0,0,0,x^{10},0,0,0,x^8,0 \\ 0,0,0,1,0,0,0,x^{11},0,0,0,x^{10} \end{pmatrix}$$

$B_2 =$

$$\begin{pmatrix} 1,0,0,0,0,0,1,0,0,0,0,0 \\ 0,1,0,0,0,0,0,x^3,0,0,0,0 \\ 1,0,0,0,0,0,x^6,0,0,0,0,0 \\ 0,1,0,0,0,0,0,x^9,0,0,0,0 \\ 0,0,1,0,0,0,0,0,1,0,0,0 \\ 0,0,0,1,0,0,0,0,0,x^3,0,0 \\ 0,0,1,0,0,0,0,0,x^6,0,0,0 \\ 0,0,0,1,0,0,0,0,0,x^9,0,0 \\ 0,0,0,0,1,0,0,0,0,0,1,0 \\ 0,0,0,0,0,1,0,0,0,0,0,x^3 \\ 0,0,0,0,0,1,0,0,0,0,0,x^6,0 \\ 0,0,0,0,0,1,0,0,0,0,0,x^9 \end{pmatrix}$$

$C_2 =$

$$\begin{pmatrix} 1,0,0,0,0,0,1,0,0,0,0,0 \\ 1,0,0,0,0,0,x^6,0,0,0,0,0 \\ 0,1,0,0,0,0,0,1,0,0,0,0 \\ 0,1,0,0,0,0,0,x^6,0,0,0,0 \\ 0,0,1,0,0,0,0,0,1,0,0,0 \\ 0,0,1,0,0,0,0,0,x^6,0,0,0 \\ 0,0,0,1,0,0,0,0,0,1,0,0 \\ 0,0,0,1,0,0,0,0,0,x^6,0,0 \\ 0,0,0,0,1,0,0,0,0,0,1,0 \\ 0,0,0,0,1,0,0,0,0,0,x^6,0 \\ 0,0,0,0,0,1,0,0,0,0,0,1 \\ 0,0,0,0,0,1,0,0,0,0,0,x^6 \end{pmatrix}$$

とする転置表示（transpositional representation）を含む表現

$$A_1B_2C_2 = {}^tC_2{}^tB_2{}^tA_1 = V$$

となります。

Euclid-Vandermonde factorization theorem

Let $V = (x^{ij})$, and $x^n-1 = 0$,

$n = n_1 \times n_2 \times \cdots \times n_k$ $(n_k > 1)$ be any representation of n

Then there exist degree n matrix $A_1, A_2, \cdots, A_k$ such that

$A_1A_2 \cdots A_k = {}^tA_k \cdots {}^tA_2{}^tA_1 = V$,

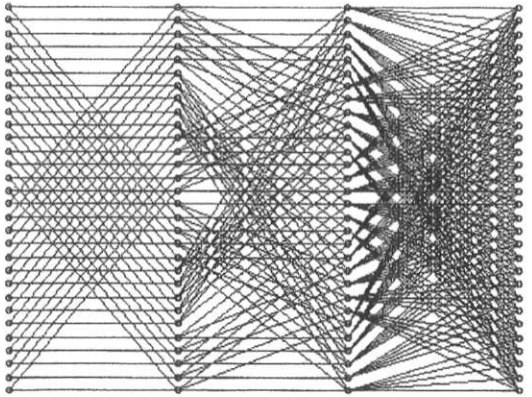
non zero elements in each row and column of A_i are n_i

合成数次数の Vandermonde 行列の因数分解は完全グラフ、つまり

$$n \times n = \{(i,j) : i,j \in n\},\ n = \{0,1,\cdots,n-1\}$$

$$n = n_1 \times n_2 \times \cdots \times n_k \quad (n_k > 1)$$

のグラフを k 個の n の guage 付き n_i 対 n_i 対応 (= $(n_i : n_i)$-correspondence, n_i to n_i guage , bi-n_i correspondence) の積に分解することです。guage、つまり、x^i の形の重みを除いたものは、例えば 30 = 2×3×5 の場合では



のようです。図の各結線には変調重み (modular weight, x^i の形の数) がついており、始点 (start point) $i \in n$ と終点 (terminal point) $j \in n$ の間の結線は一意的で変調重みの指数の和 (あるいは積) が積 ij mod n となるようにできる。これが moduar weight tagged Vandermonde graph の分解定理 (factorization theorem of modular weight tagged Vandermonde graph) である。

一般の記述には、混合進法、つまり、$u = [u_1 \cdots u_m]$ 進数 (u-ary number, system) や u-進展開 (u-ary expansion, digit) の概念が有効です。例えば、

$$u = [3, 14, 15, 9, 2, 6, 5]$$

進数での

$$n = [1, 4, 14, 2, 1, 3, 4]$$

の 3 桁目 14 は、10 進表示では 2 文字から成っていますが u-進法の 1 つの桁数 (digit) です。$\sqrt{2}$ = 1.414213562 … であるが末尾の数を 5 とすることはできない、所謂、桁上がりが生ずる。

$$6\times5 = 30,\ 30\times2 = 60,\ 60\times9 = 540,\ 540\times15 = 8100,\ 8100\times14 = 113400$$

であるから、

$$n = 1\times113400+4\times8100+14\times540+2\times60+1\times30+3\times6+5 = 153533$$

である。153533+1 = 153534 = [1,4,14,2,1,4,0]

例. u = [2,5,4,3], $x^{120}-1 = 0$

次数 n = 120 = 2×5×4×3 である。例えば A_i は n 次の 2-2 行列で、行を

$$i = [i_1, i_2, i_3, i_4]$$

としたとき、$A_i = (a_{ij})$ は 2 個の列の元を除いて 0 で

$$j \in [2, i_2, i_3, i_4] = \{[s, i_2, i_3, i_4] : s \in 2 = \{0,1\}\} = [i/2]\,(n/2) + i \bmod (n/2)$$

$$a_{ij} = x\text{^}(si \bmod n)$$

である。また、例えば、A_3 では u = [2,5,4,3] を除き、v = [4,2,5,3] 進法を用いて

$$i = [i_1, i_2, i_3, i_4],\ t = 2\times5\times4 = 40,\ q = 2\times5$$

$$j \in [4, i_1, i_2, i_4] = \{[s, i_1, i_2, i_4] : s \in 4 = \{0,1,2,3\}\} = [i/t]\,(n/t) + i \bmod (n/t)$$

$$a_{ij} = x\text{^}(sqi \bmod n)$$

として得られる。A_3 は 4-4 行列 (4 to 4 matrix) である。このようにして Vandermonde 行列の素因子 (= 疎行列) 分解の一つ

$$A_1A_2A_3A_4 = V = (x^{ij})$$

が得られる。V は対称行列なので転置 (transepose) 行列の逆順序の積でも表現できる。この表現法を行優先 (row-first, row oriented) 法と、仮に、呼ぶ。

x の指数 (index, exponent) が積 ij になっていることの説明であるが、行列の積が

$$(b_{ij}) = (c_{ik})\,(d_{kj})$$

のように i 行の元は左の行列の i 行の成分の積であり x の指数は sqi となっており、i は共通であることからきている。

$$i = [i_1, i_2, i_3, i_4],\ j = [j_1, j_2, j_3, j_4]$$

$$ij = i\,(j_1\times5\times4\times3+\ j_2\times4\times3+j_3\times3+j_4)\ \mod n$$

行優先法では、

matrix	i	j
A_1	[2,5,4,3]	[2,5,4,3]
A_2	[2,5,4,3]	[5,2,4,3]
A_3	[2,5,4,3]	[4,2,5,3]
A_4	[2,5,4,3]	[3,2,5,4]

のように桁場所(radix, position)の置換(互換, permutation)が行われる。今の場合は、巡回置換の互換表現の「仲介」(mediation)と「盥回し」(rotation, send hand by hand)

$$(h, i, j, k) = (h, k)\,(h, j)\,(h, i) = (h, i)\,(i, j)\,(j, k)$$

がある。今の場合は先頭仲介方式である。

2, 3 進高速有限 Fourier 変換については、よく知られているので、結合図の例を示すに止める。

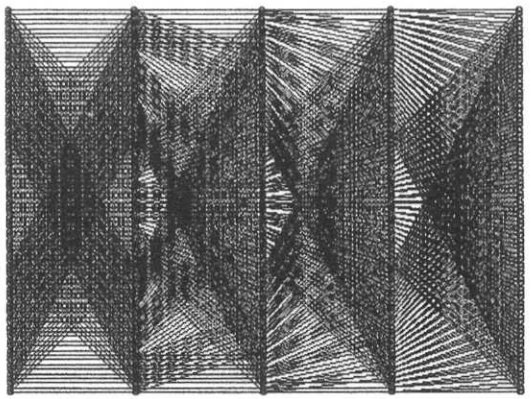
k = 4

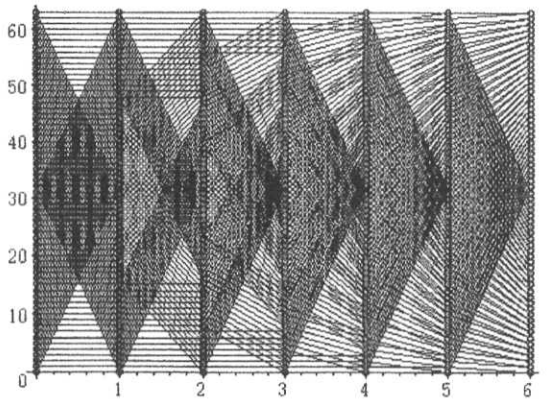
a:=n mod 27

a:=n mod 9: b:=floor(n/27) : c:=b*9+a

a:=n mod 3: b:=floor(n/9) mod 3: c:=floor(n/27) : d:=c*9+b*3+a

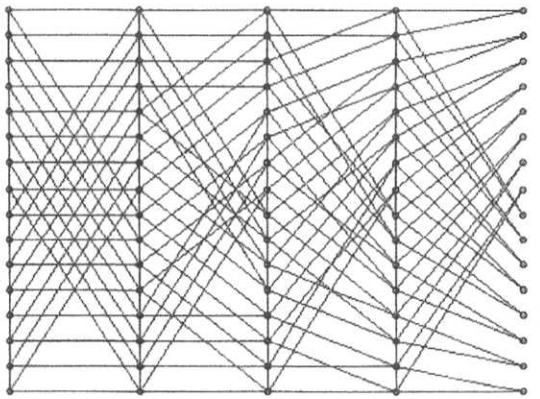
a:=floor(n/3)



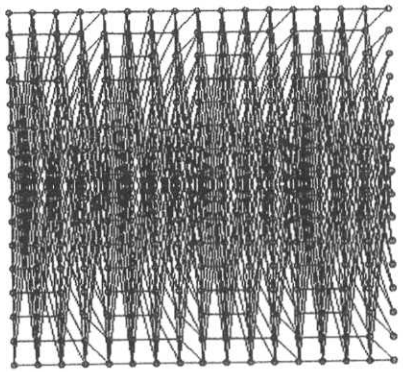


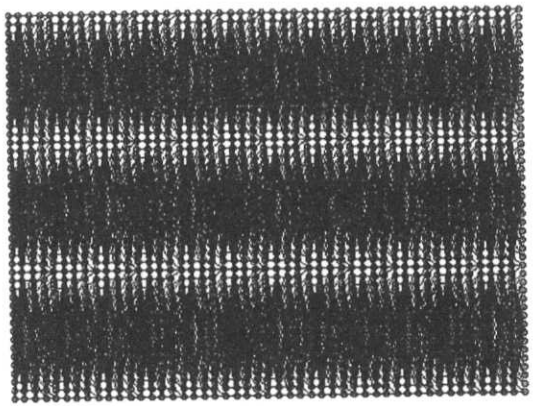
ここにも記した通り、有限 Fourier 変換(有限高速 Fourier 変換)は周期 4 をもつ変換、$F^4 = E$、であり、このような変換の結合体系の設計や構築と認識科学などとの関係は基本的であり興味ある関心事です。

図は $2^4 = 16$ の fftt の回路



を 4 回繋いだものですが、左端の入力が右端で(遅延時間の後に)再生されています。





下の図は、これを 3×3 個単に境界で繋いだものです。これは delay resister としての作用以上の機能をもっています。このようなものを結線や線・面接続した情報処理構造物 (information prosessor) の設計や機能 design は非常に興味ある研究対象です。

上の例では

$$16 = (2+2)^2 = (2\times2)^2 = (2^2)^2 = 2^{(2+2)} = 2^{(2\times2)} = 2^{(2^2)}$$

を基本の数とした例について記しましたが、ffFt の回路は

$$2,\ 3,\ 4 = 2+2 = 2\times2 = 2^2,\ 5,\ 6 = 2\times3,\ 7,\ 8 = 2^3,\ 9 = 3^2,\ 10 = 2\times5,\ \cdots$$

などについても基本的な役割をもっています。特に、有限体といっても、有限の対象が輪の状態を成しているものであれば何でもよいのですから、

化学物質の世界の平凡な対象物ですし、(有限)周期的な過程はすべてこの範疇に属します。

特に 2, 3, 4 と云った小さい数に関する ffFt 回路(機構)は、例えば、化学反応の random な試行のなかからも十分発生・生成可能な複雑性をもったものです。ffIt の Fourier 性 $F^4 = id$ は受識想行 (= sense, memory, image, action = reproduce) に相当する機能ですから、生命活動の基本要素、仮に、生命片 (lifelet) と呼びますが、は素粒子や化学反応のうち(裡)にその萌芽が含まれているのではないかと(私は)思っています。

References

[1] Kanji Namba, Fuchs polynomial related to elliptic curves and finite Fourier transformation, Reports of 26th Symposium on the History of Mathematics (2015), Rep. Inst. Math. and Comp. Sci. 37, Institute for Mathematics and Computer Sciences, Tsuda College, 2016. pp. 135-179

[2] 難波完爾, 有限フーリエ変換と有限高速フーリエ変換, 2016 年度 応用数学合同研究集会 予稿集, 龍谷大学 瀬田キャンパス, 日本数学会応用数学分科会, 協賛 日本応用数理学会, 龍谷大学理工学部, 2016, pp. 88-93

[3] 松田修, 渡辺守邦, 花田富二夫 校注, 浅井了意作, 伽婢子, 巻之三(三) 牡丹灯籠, 新日本古典文学大系, 岩波書店 p. 76-85