Fuchs polynomial related to elliptic curves and finite Fourier transformation

by Kanji Namba

463-3 Kitamizote Sojya Okayama 719-1117
tel/fax. 0866-90-1886
2015.12.13

finite field, finite Fourier transform (= fFt, Vandermonde tr. coefficient tr.), Legendre polynomial, Fuchsian polynomial, Hasse's inequality, elliptic curves, Poincaré-Mordell-Weil group, p-absolute value property, resultant transform

1. Introduction, definition and notions.

1.1 resultant

Let f(x) and g(x) be polynomials, then the resultant is (as temporary notion) denoted as

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

It satisfy, as for example,

$$f(x) ⓧ x\text{-}y = f(y)$$

$$f(x) ⓧ g(x) = (-1)^{nm} g(x) ⓧ f(x)$$

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

$$f(x)^n ⓧ g(x) = f(x) ⓧ g(x)^n$$

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

Consider for example of torus, which is the points distant 1 from the plane circle $s^2+t^2 = 9$, is obtained by, considering tangent line s = xt/y

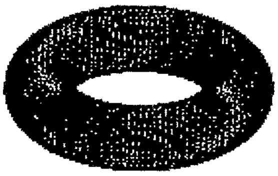
$$[s^2+t^2-9,\ (x-s)^2+(y-t)^2+z^2-1] =$$
$$[x^2t^2+y^2t^2-9y^2,\ x^2t^2-2x^2ty+x^2y^2+y^2t^2-2y^3t+y^4+y^2z^2-y^2]/y^2$$

and so

$$x^2t^2+y^2t^2-9y^2 ⓣ x^2t^2-2x^2ty+x^2y^2+y^2t^2-2y^3t+y^4+y^2z^2-y^2 =$$
$$y^4(x^2+y^2)^2(x^4+2x^2z^2+2x^2y^2-20x^2+z^4+16z^2-20y^2+64+2y^2z^2+y^4).$$

which is a standard domain with genus 1 of elliptic curves

$$x^4+2x^2z^2+2x^2y^2-20x^2+z^4+16z^2-20y^2+64+2y^2z^2+y^4 = 0$$



as for example, the case of genus 2 surface, though not smooth, points of distance 1 from radius 5 lemniscate:

$$(s^2+t^2)^2 = 25(s^2+t^2),\ (x-s)^2+(y-t)^2+z^2 = 1$$

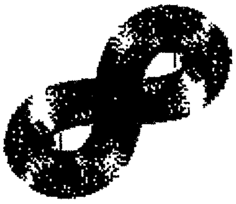
with tangent vector $[4ts^2+4t^3+50t,\ -4s^3-4s^2+50s,\ 0]$

$$(x-s)(4ts^2+4t^3+50t)+(y-t)(-4s^3-4st^2+50s) =$$
$$-100st+4xts^2+4xt^3+50xt-4ys^3-4yst^2+50ys = 0,$$

we have

$$((x-s)^2+(y-t)^2+z^2-1 \textcircled{t} (s^2+t^2)^2 = 25(s^2+t^2))$$
$$\textcircled{s} ((x-s)^2+(y-t)^2+z^2-1 \textcircled{t}-100st+4xts^2+4xt^3+50xt-4ys^3-4yst^2+50ys)$$

which is slightly big polynomial of x,y,z, with the figure:



1.2 finite fields

Finite prime field is the field consists of prime number p elements and denoted by

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

where GF(p), stand for Galois field. For least absolute value residue (= lavr), we mean the residue in the set, for odd prime,

$$\bar{p} = \{0, \pm 1,\cdots, \pm(p-1)/2\}.$$

General finite field consists of p^n elements, denoted by $F_{p{\wedge}n} = GF(p^n)$, is obtained as an algebraic extension, namely by quotient of degree n polynomials by an their irreducible polynomial p(x), and they are all isomorphic. (Wedderburn theorem, J. H. M. Weddurburn, 1882-1948).

$$F_{p{\wedge}n} = GF(p^n) = F_p{}^n[x]/(p(x))$$

Characteristic polynomial of finite field is

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

for prime field and for general case it is $x^{p{\wedge}n}\text{-}x = x(x^{p{\wedge}n-1}\text{-}1)$.

Legendre symbol, for odd prime, is defied by

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

Example 1. Count the number of solutions of elliptic curve in extended Weierstrass normal form in prime finite field F_p (= counting the order of Mordell-Weil group)

$$C\text{: } y^2 = f(x) = x^4+qx+r$$

The wanted number is (including unit element, which is $\propto$)

$$n_p = \mathrm{ord}(C) = 1+a_p+p$$

$$a_p = \textstyle\sum_{x \in p} (f(x)/p).$$

Note that

$$(f(x)/p) = f(x)^{(p-1)/2} = x^{2(p-1)}+\cdots+c_{p-1}x^{p-1}+\cdots+c_0$$

and we want to compute their sum in F_p, namely

$$\textstyle\sum_{x \in p}(f(x)/p) = \sum_{x \in p} (x^{2(p-1)}+\cdots+c_{p-1}x^{p-1}+\cdots+c_0) = -c_{p-1}.$$

For, only the coefficient of x^{p-1} will remain because $x(x^{p-1}-1) = 0$, or in other words

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

this means that, in F_p

$$\textstyle\sum_{x \in p} c_j x^j = -c_{p-1} \text{ if } j = p\text{-}1 \text{ else } 0$$

This coefficient is expressed as sum of terms of the form $m = (p-1)/2$

$$m!/(r!s!t!) \cdot a^s b^t \cdot x^{4r+s}$$

the condition is

$$r+s+t = (p-1)/2,\ 4r+s = p\text{-}1$$

solving this, we have

$$r = (p-1)/6+t/3,\ s = (p-1)/3-4t/3$$

the case $p = 6n+1$, $t = 3u$, we have

$$r = n+u,\ s = 2n-4u,\ t = 3u$$

and consider the ratio by shift $u-1$ to u of

$$r!s!t! = (n+u)!(2n-4u)!(3u)!$$

we have

$$\frac{(2n-4u+3)(2n-4u+2)(2n-4u+1)(2n-4u)}{(n+u)(3u-2)(3u-1)(3u)}$$

in this case $n = -1/6$,

$$n+u = 1/6\cdot(6u-1),$$
$$2n-4u+1 = -1/3(1+12u-3) = -2(6u-1)/3,$$
$$2n-4u+3 = -1/3(1+12u-9) = -4(3n-2)/3$$

so, two terms are cancellate to constant, namely

$$\frac{(2n-4u+3)(2n-4u+1)}{(n+u)(3u-2)} = \frac{-2(6u-1)/3\cdot -4(3n-2)/3}{1/6\cdot(6u-1)(3u-2)} = 16/3$$

remaining terms are

$$\frac{16(2n-4u+2)(2n-4u)}{27(u-1/3)u} = \frac{256(u-5/12)(u+1/12)}{27(u-1/3)u}$$

In the case $p = 6n-1$, $n = 1/6$ and

$$t = 3u+1$$
$$r = (p-1)/6+t/3 = n+(t-1)/3 = n+u,$$
$$s = (p-1)/3-4t/3 = 2n-2/3-4t/3 = 2n-2-4(t-1)/3 = 2n-2-4u$$

Consider the ratio by shift $u-1$ to u of

$$r!s!t! = (n+u)!(2n-4u-2)!(3u+1)!$$

we have

$$\frac{(2n-4u+1)(2n-4u)(2n-4u-1)(2n-4u-2)}{(n+u)(3u-1)(3u)(3u+1)}$$

in this case $n = 1/6$,

$$n+u = 1/6\cdot(6u+1),$$
$$2n-4u-1 = -1/3(-1+12u+3) = -2(6u+1)/3,$$
$$2n-4u+1 = -1/3(-1+12u-3) = -4(3n-1)/3$$

so, two terms are cancellate to constant, namely

$$\frac{(2n-4u-1)(2n-4u+1)}{(n+u)(3u-1)} = \frac{-2(6u+1)/3\cdot -4(3n-1)/3}{1/6\cdot(6u+1)(3u-1)} = 16/3$$

remaining terms are

$$\frac{16(2n-4u-2)(2n-4u)}{27(u-2/3)u} = \frac{256(u+5/12)(u-1/12)}{27(u-2/3)u}$$

and the Fuchsian polynomials

$$F(7/12,13/12,2/3,x) \quad \text{if } p = 1 \bmod 6$$
$$F(17/12,11/12,1/3,x) \quad \text{if } p = -1 \bmod 6$$
$$x = 256b^3/27a^4,\ f(x) \otimes f'(x) = -27a^4+256b^3$$

appear.

Relation with Legendre-Jacobi normal form is also interesting.

Example 2.

$$C:\ \ y^2 = f(x) = x^4+ax^2+b$$

In this case, fundamental relations are

$$r+s+t = (p-1)/2,\ 4r+2s = p-1$$

and the solution is simple, putting $m = (p-1)/2 = -1/2 \bmod p$, then

$$r = t,\ s = -2t+(p-1)/2.$$

In this case, $r!s!t! = t!^2(m-2t)!$, so the ratio by the process t-1 to t is

$$(m-2t+1)(m-2t)/t^2 = 4(t-1/4)(t+1/4)/t^2$$

and the Fuchsian polynomial is

$$F(5/4,3/4,1,x),\ x = 4b/a^2,\ f(x) \otimes f'(x) = 16b(4b-a^2)^2.$$

1.3 Vandermonde matrix

Let us begin with the notion of logarithmic differential (= logdif, lodi)

$$d[x]f(x) = d\log(f(x))/dx = d[x]f(x) = f'(x)/f(x).$$

This temporal notation d[x] satisfy

$$d[x](f(x)g(x)) = d[x]f(x)+d[x]g(x)$$
$$d[x](f(x)/g(x)) = d[x]f(x)-d[x]g(x)$$

and so

$$d[x]\prod_{i\in n}(x-a_i)\hat{}e_i = \sum_{i\in n} e_i/(x-a_i)$$

in the image, denominator does not have any multiple factor, namely the determinant of denominator does not vanish:

$$\det(g(x)) = g(x) \otimes g'(x) \neq 0$$

Inverse operation $\int[x]$ is called, integral exponential (= intexp, inex, temporal name, usual notion would be exponential integral)

Example 3. $p = 11$.

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

in this case the fractional

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

so, in lavr form

$$\int[x](x^4+x^3+x^2+x+1)/(x^4-x^3+x^2-x+1)$$
$$=\int[x](1+3/(x+4)-2/(x+9)-5/(x+5)-5/(x+3))$$
$$=x(x+4)^3/((x-2)^2(x+5)^5(x+3)^5)$$

denominator contains multiplicative factor, so its integral exponential does not exist.

$$d[x]((x^4+x^3+x^2+x+1)/(x^4-x^3+x^2-x+1))$$
$$=1/(x+2)+1/(x-4)+1/(x-5)+1/(x-3)-1/(x+4)-1/(x-2)-1/(x+5)-1/(x+3)$$
$$=-2(x-1)(x+1)(x^2-2)(x^2+5)$$
$$/((x+2)(x-4)(x-5)(x-3)(x+4)(x-2)(x+5)(x+3))$$

The notion of *finite Fourier transform* (= fFt, *coefficient transform, Vandermonde transform*) is little bit different. Let

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

be a prime field and $F_p{}^p[x]$ be p-dimensional linear space over F_p

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

this space can be considered simply a set of p sequence of elements of p, namely p^p.

Let q be a primitive root mod p, then *finite Fourier transform* $[q]$ is defined as

$$[q]: F_p{}^p[x]\rightarrow F_p{}^p[x]\ =p^p\rightarrow p^p=p3p$$
$$[q]\Sigma_{i\in p}\ a_ix^i=(1-x^{p-1})[q](\Sigma_{i\in p-1}\ a_i/(1-q^ix)+a_{p-1})$$
$$=(1-x^{p-1})(a_0/(1-x)+a_{10}/(1-qx)+\cdots+a_{p-2}/(1-q^{p-2}x)+a_{p-1}).$$

In this respect,

$$[q]\in \mathrm{Aut}(F_p{}^p[x])=p3p\rightarrow p3p=p4p$$

so the group generated by $[q]$'s for all primitive roots mod p,

$$G=\langle[q]: q\in \mathrm{proot}(p)\rangle\subset H=\mathrm{Aut}(F_p{}^p[x])$$

the structure problem of H/G is very interesting.

Historically, I first defined as *coefficient transform:* for a p-2 degree polynomial

$$f(x)\in F_p{}^{p-1}[x]=p^{p-1}$$
$$f(x)[q](x)=f(1)+f(q)x+\cdots+f(q^{p-2})x^{p-2}$$
$$[q]: F_p{}^{p-1}[x]\rightarrow F_p{}^{p-1}[x]$$
$$[q]\Sigma_{i\in p-1}\ a_ix^i=\Sigma_{i\in p-1}\ f(q^i)x^i=(1-x^{p-1})[q](\Sigma_{i\in p-1}\ a_i/(1-q^ix)).$$

For me it needs long time to notice that this is not a *property* but a *definition.*

The charactreristic polynomial of prime fiels F_p, namely

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

play the role of vacuum space, it is the stage, the space things develops. Key notion is Vandermonde matrix of $x\delta(x)$, namely

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

which is, matrix consists of coefficients

$$x(1-x^{p-1})/(1-x) = x(1+x+x^2+\cdots+x^{p-2})$$
$$x(1-x^{p-1})/(1-qx) = x(1+qx+q^2x^2+\cdots+q^{p-2}x^{p-2})$$
$$x(1-x^{p-1})/(1-q^2x) = x(1+q^2x+q^4x^2+\cdots+q^{2(p-2)}x^{p-2})$$
$$\cdots\quad\cdots\quad\cdots$$
$$x(1-x^{p-1})/(1-q^{p-2}x) = x(1+q^{p-2}x+q^{p-3}x^2+\cdots+qx^{p-2})$$
$$(x-x^p)/x = 1-x^{p-1},$$

Example 3. Vandermonde matrix generated by primitive root,

$$p = 7,\ q = 3,\ [q]$$

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

extended Vandermonde matrix $[q]$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 3 & 2 & -1 & -3 & -2 & 0 \\ 1 & 2 & -3 & 1 & 2 & -3 & 0 \\ 1 & -1 & 1 & -1 & 1 & -1 & 0 \\ 1 & -3 & 2 & 1 & -3 & 2 & 0 \\ 1 & -2 & -3 & -1 & 2 & 3 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

it includes original Vandermonde matrix as principal minor. It satisfy Fourier property, namely, 4-th power is identity $F^4 = E = \mathrm{id}$. Extended part can be used as parity part. $0/\infty$ part, namely the lowest row interact only with the first column, 0-dimensional momentum (mass, charge etc). Any how, $[q]^2$ of the above matrix is

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

as expected. To add parity bit corresponds to extend space p^{p-1} to p^p, which is known as *successor exponential law*

$$(p\wedge p)\wedge(p\wedge(p-1))=p\wedge(p\cdot p\wedge(p-1))=p\wedge(p\wedge p)\neq(p\wedge p)\wedge p=p\wedge p^2\neq(p\wedge p)^2$$

Note that the symmetric matrix,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & \textcircled{1} \\ 1 & 3 & 2 & -1 & -3 & -2 & 0 \\ 1 & 2 & -3 & 1 & 2 & -3 & 0 \\ 1 & -1 & 1 & -1 & 1 & -1 & 0 \\ 1 & -3 & 2 & 1 & -3 & 2 & 0 \\ 1 & -2 & -3 & -1 & 2 & 3 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

is singular in F_p and does not satisfy Fourier property, namely not Fourier matrix, its 4-th power is:

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

and it is not the identity matrix.

Example 4. $x(1-x^n)$ in complex number field:

Modified Vandermonde matrix is

$n = 1$:

$$A = \begin{pmatrix} 1 & 0 \\ a & -1 \end{pmatrix}$$

this matrix is Fourier matrix for any a.

$n = 2$:

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

this matrix is Fourier matrix only when $a = b(1+\sqrt{2})$ for any b.

$n = 3$: $\omega = (-1+i\sqrt{3})/2$

$$A = 1/\sqrt{3}\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & \omega & \omega^2 & 0 \\ 1 & \omega^2 & \omega & 0 \\ a & b & c & -\sqrt{3} \end{pmatrix}$$

this matrix is Fourier matrix only when $a = (b+c)(1+\sqrt{3})/2$ for any b, c.

$n = 4$:

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

if lowermost row is replaced by $(1 \quad 0 \quad 0 \quad 0 \quad -1)$ then it is not a Fourier matrix.

$n = 5$: $x(1-x^5)$

$$1/\sqrt{5}\cdot$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & \tau & \tau^2 & \tau^3 & \tau^4 & 0 \\ 1 & \tau^2 & \tau^4 & \tau & \tau^3 & 0 \\ 1 & \tau^3 & \tau & \tau^4 & \tau^2 & 0 \\ 1 & \tau^4 & \tau^3 & \tau^2 & \tau & 0 \\ (b+c+d+e)(1+\sqrt{5})/4 & b & c & d & e & -\sqrt{5} \end{pmatrix}$$

where

$$[\tau, \tau^2, \tau^3, \tau^4] =$$
$$[(-1+\sqrt{5}/4+i\sqrt{(10+2\sqrt{5})})/4,\ (-1-\sqrt{5}/4+i\sqrt{(10-2\sqrt{5})})/4,$$
$$(-1-\sqrt{5}/4-i\sqrt{(10-2\sqrt{5})})/4,\ (-1+\sqrt{5}/4-i\sqrt{(10+2\sqrt{5})})/4].$$

n = 6: $x(1-x^6)$

$$1/\sqrt{6}\cdot\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & (1+i\sqrt{3})/2 & (-1+i\sqrt{3})/2 & -1 & (-1-i\sqrt{3})/2 & (1-i\sqrt{3})/2 & 0 \\ 1 & (-1+i\sqrt{3})/2 & (-1-i\sqrt{3})/2 & 1 & (-1+i\sqrt{3})/2 & (-1-i\sqrt{3})/2 & 0 \\ 1 & -1 & 1 & -1 & 1 & -1 & 0 \\ 1 & (-1-i\sqrt{3})/2 & (-1+i\sqrt{3})/2 & 1 & (-1-i\sqrt{3})/2 & (-1+i\sqrt{3})/2 & 0 \\ 1 & (1-i\sqrt{3})/2 & (-1-i\sqrt{3})/2 & -1 & (-1+i\sqrt{3})/2 & (1+i\sqrt{3})/2 & 0 \\ a & b & c & d & e & f & -\sqrt{6} \end{pmatrix}$$

is Fourier matrix iff

$$b = -d-f+\sqrt{6}(a-d)/2,\ c = -a-e+\sqrt{6}(a+d)/2.$$

or

$$a = (2(c+e)-\sqrt{6}d)(2+\sqrt{6})/2,\ b = (-4d+2f+\sqrt{6}(c+e-f))(2+\sqrt{6})/2.$$

Any how, 2 independent relations appear here.

n = 7: lowest row

$$1/\sqrt{7}(a, b, c, d, e, f, g, -\sqrt{7})$$

Fourier condition is:

$$a = (d+e)(1+\sqrt{7})/2,\ b = d+e-g,\ c = d-f+e.$$

n = 8:

$$1/\sqrt{8}(a, b, c, d, e, f, g, h, -\sqrt{8})$$

$$a = (c+g+(1-\sqrt{2})e)(1+\sqrt{2}),\ b = ((d-4e+f+h)+\sqrt{2}(c+2e+g-d-f-h))(1+\sqrt{2})$$

n = 9:

$$1/3(a, b, c, d, e, f, g, h, i, -3)$$

$$a = (3f+3e+d+g)/2,\ b = e+f-i,\ c = f-h+e.$$

Behavior of mixed system, with interaction term via $0/\infty$ term works independently.

$$\begin{pmatrix} 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} & 0 & 0 & 0 & 0 & 0 \\ 1/\sqrt{3} & (-1/\sqrt{3}+i)/2 & (-1/\sqrt{3}-i)/2 & 0 & 0 & 0 & 0 & 0 \\ 1/\sqrt{3} & (-1/\sqrt{3}-i)/2 & (-1/\sqrt{3}+i)/2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/2 & 1/2 & 1/2 & 1/2 & 0 \\ 0 & 0 & 0 & 1/2 & i/2 & -1/2 & -i/2 & 0 \\ 0 & 0 & 0 & 1/2 & -1/2 & 1/2 & -1/2 & 0 \\ 0 & 0 & 0 & 1/2 & -i/2 & -1/2 & i/2 & 0 \\ a & b & c & d & e & f & g & -1 \end{pmatrix}$$

$$a = (b+c)(1+\sqrt{3})/2,\ d = e+f+g$$

Example 4. things and words (= 音沙汰)

Consider, temporary list

	0	1	2	3	4	5	6	7	8	9
0		sp	=	+	−	×	/	<	π	*i*
10	0	1	2	3	4	5	6	7	8	9
20	a	b	c	d	e	f	g	h	i	j
30	k	l	m	n	o	p	q	r	s	t
40	u	v	w	x	y	z	,	.		

and the a sequence of letters:

fourier coefficient vandermonde

in the finite field p = 61, p-1 = 60 = $2^2 \cdot 3 \cdot 5$. In the case p = 61, we have

pres(61) = {1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59}

proot(61) = {0, 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59}

with 16 = $2(2^1-1)/(2-1)\cdot(3-1)(5-1)$ elements.

Note that pres(p) is closed under - mod p-1, like -11 mod p-1 = 49, and proot(p) is closed under inverse mod p, like 1/6 mod p = 51, also the product of primitive roots, in general, is not a primitive root, as 2·6 = 12 is not a primitive root mod p.

The above letters corresponds to a sequence of 31 numbers:

[25,34,40,37,28,24,37,1,22,34,24,25,25,28,22,28,
24,33,39,1,41,20,33,23,24,37,32,34,33,23,24]

Consider this as a polynomial of $F_p^{p-1}[x]$, beginning with, for example x^7, namely

$$f(x) =$$

$$24x^{37}+23x^{36}+33x^{35}+34x^{34}+32x^{33}+37x^{32}+24x^{31}+23x^{30}+33x^{29}+20x^{28}$$
$$+41x^{27}+x^{26}+39x^{25}+33x^{24}+24x^{23}+28x^{22}+22x^{21}+28x^{20}+25x^{19}+25x^{18}$$
$$+24x^{17}+34x^{16}+22x^{15}+x^{14}+37x^{13}+24x^{12}+28x^{11}+37x^{10}+40x^{9}+34x^{8}+25x^{7}$$

take, for example, as a primitive root q = 18, then the finite Fourier transform [q] is:

$$f(x)[18](x) = \sum_{n\in p-1} f(q^n)x^n =$$

$$37x^{59}+49x^{58}+58x^{57}+7x^{56}+55x^{55}+19x^{54}+19x^{53}+26x^{52}+24x^{51}+37x^{50}+53x^{49}+38x^{48}$$
$$+27x^{47}+20x^{46}+9x^{45}+39x^{44}+30x^{43}+22x^{42}+56x^{41}+36x^{40}+29x^{39}+37x^{38}+27x^{37}+28x^{36}$$
$$+51x^{35}+12x^{34}+60x^{33}+18x^{32}+58x^{31}+31x^{30}+42x^{29}+60x^{28}+15x^{27}+44x^{26}+27x^{25}$$
$$+5x^{24}+52x^{23}+55x^{22}+10x^{21}+25x^{20}+52x^{19}+8x^{18}+13x^{17}+41x^{16}+37x^{15}+36x^{14}$$
$$+31x^{13}+45x^{12}+45x^{11}+28x^{10}+34x^{9}+x^{8}+13x^{7}+12x^{6}+13x^{5}+14x^{3}+32x^{2}+27x+1$$

or, as a sequence of coefficients:

[1, 27, 32, 14, 0, 13, 12, 13, 1, 34, 28, 45, 45, 31, 36, 37, 41, 13, 8, 52,

25, 10, 55, 52, 5, 27, 44, 15, 60, 42, 31, 58, 18, 60, 12, 51, 28, 27, 37, 29,
36, 56, 22, 30, 39, 9, 20, 27, 38, 53, 37, 24, 26, 19, 19, 55, 7, 58, 49, 37]

$$f(x)\,[18]^2(x)=$$

$$36x^{53}+27x^{52}+21x^{51}+24x^{50}+33x^{49}+37x^{48}+24x^{47}+60x^{46}+39x^{45}+27x^{44}+37x^{43}+36x^{42}$$
$$+36x^{41}+33x^{40}+39x^{39}+33x^{38}+37x^{37}+28x^{36}+22x^{35}+60x^{34}+20x^{33}+41x^{32}+28x^{31}+38x^{30}$$
$$+37x^{29}+24x^{28}+29x^{27}+27x^{26}+28x^{25}+38x^{24}+37x^{23}$$

[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 37, 38, 28, 27, 29, 24, 37, 38, 28, 41, 20, 60, 22, 28, 37, 33, 39,
33, 36, 36, 37, 27, 39, 60, 24, 37, 33, 24, 21, 27, 36, 0, 0, 0, 0, 0, 0]

its minus mod p is:

[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, e, d, n, o, m, r, e, d, n, a, v, □, t, n, e, i, c,
i, f, f, e, o, c, □, r, e, i, r, u, o, f, 0, 0, 0, 0, 0, 0]

hereafter, we write them in the coefficient form:

$$f(x)\,[18]^3(x)=$$

[60, 24, 12, 3, 54, 6, 42, 42, 35, 37, 24, 8, 23, 34, 41, 52, 22, 31, 39, 5,
25, 32, 24, 34, 33, 10, 49, 1, 43, 3, 30, 19, 1, 46, 17, 34, 56, 9, 6, 51,
36, 9, 53, 48, 20, 24, 25, 30, 16, 16, 33, 27, 60, 48, 49, 48, 0, 47, 29, 34]

$$f(x)\,[18]^4(x)=$$

[0, 0, 0, 0, 0, 0, 0, 25, 34, 40, 37, 28, 24, 37, 1, 22, 34, 24, 25, 25,
28, 22, 28, 24, 33, 39, 1, 41, 20, 33, 23, 24, 37, 32, 34, 33, 23, 24, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

which of course reproduce the original sequence, namely by Fourier property, $T^4 = E$.

[0, 0, 0, 0, 0, 0, 0, f, o, u, r, i, e, r, □, c, o, e, f, f,
i, c, i, e, n, t, □, v, a, n, d, e, r, m, o, n, d, e, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

is reproduced.

The invers of [q] is minus of $[q^{-1}]$, namely

$$[q]=[q]^3=-[q^{-1}].$$

In this case $18^{-1} = 1/18 = 17$ mod p, namely,

$$f(x)\,[18]\,[18]^{-1}(x)=-\,f(x)\,[18]\,(x)\,[17]\,(x)=f(x)$$

Let pres(p) the set of all primitive residues mod p-1 and proot(p) be the set of all primitive roots mod p.

$$\mathrm{pres}(p)=\{x\in p\text{-}1:\ (x,p\text{-}1)=1\},$$
$$\mathrm{proot}(p)=\{x\in p:\ \forall n\in p\text{-}1\,(x^n \bmod p\neq 1)\}$$

$$\exp, \log : \mathrm{pres}(p) \approx \mathrm{proot}(p)$$

$$\times : \mathrm{pres}(p) \times \mathrm{pres}(p) \to \mathrm{pres}(p)$$

$$\exp : \mathrm{proot}(p) \times \mathrm{pres}(p) \to \mathrm{proot}(p)$$

$$\log_q r = r//q : \mathrm{proot}(p) \times \mathrm{proot}(p) \to \mathrm{pres}(p)$$

$$q//q = 1,\ s//r \cdot r//q = s//q,\ q\wedge(r//q) = r$$

$$s//r^{-1} = s^{-1}//r = -(s//r) \mod p\text{-}1 \text{ (notice not mod p)}$$

$\log_q r = r//q$ is called *discrete logarithm* or *exponential quotient* (= *ratio, rate*). pres(p) is a multiplicative abelian group, and every primitive root of q determines a group operation ⟨q⟩ on the group proot(p) as q as its unit element.

For a fixed primitive root q, by set-notation,

$$q\wedge\mathrm{pres}(p) = \mathrm{proot}(p)$$

$$\log_q \mathrm{proot}(p) = q \log \mathrm{proot}(p) = \mathrm{pres}(p)$$

The product ⟨q⟩ of primitive roots is defined to be

$$r\langle q\rangle s = q\wedge(r//q \cdot s//q) = r\wedge(s//q) = s\wedge(r//q)$$

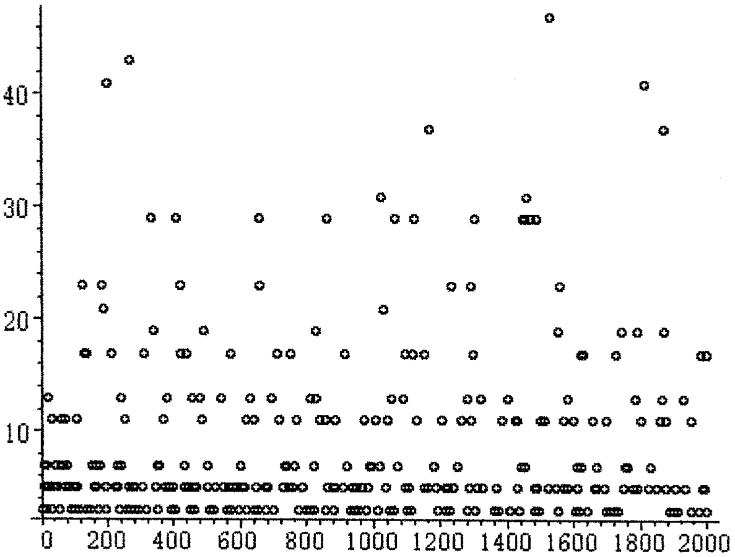
and q is the unit element with respect to ⟨q⟩.

$$(r\langle q^{-1}\rangle s) = r\langle q\rangle s^{-1},\ r\langle q\rangle s = s\langle q\rangle r,\ q\langle q\rangle s = s,\ (r\langle q\rangle s)\langle q\rangle t = r\langle q\rangle(s\langle q\rangle t) = r\langle q\rangle s\langle q\rangle t$$

Following is the graph of least element of residue-root mod p (resroot), namely the intersection

$$\mathrm{rsrt}(p) = \mathrm{pres}(p) \cap \mathrm{proot}(p)$$

$$\min(\mathrm{rsrt}(p)),\ p = 5 \sim 1999$$



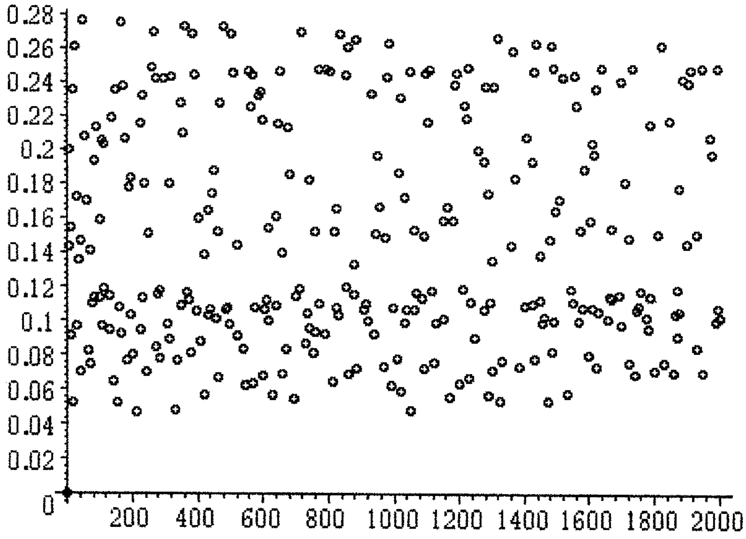
it is expected rsrt(p) = pres(p)∩proot(p) is not empty if p not 2, 3.

$$\mathrm{rsrt}(19) = \{13\}$$

and for p = 1531, least element of pres(p)∩proot(p) is 47, local maximal element.

Because, for example, prime of the form $p = k\cdot m!+1$, smallest of rspr(p) is bigger than m.

[p, #rsrt(p)/p], p = 5 ~ 1999



there are, examples rsrt(p) of

[211, [17, 29, 41, 127, 131, 149, 167, 181, 187, 191]]

[331, [29, 37, 41, 59, 97, 101, 107, 137, 217, 221, 227, 277, 301, 307, 311, 317]]

in this case, rates are

$$1/19 = 0.052631,\ 10/211 = 0.047393,\ 16/331 = 0.048338,\ 50/1051 = 0.047573$$

and so p = 211's ratio 10/211 is the smallest in this range of pime numbers, is this really the minimum for all primes?, or what is the minimum or minimal, what would be the limit density function (seems not uniform), how about lower-upper limit, are they algebraic?···, *presroot-problem.*

2. Elliptic curves

In general, elliptic curve in the form

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

is known to be transformed by bi-rational transformation, ie. Cremona transformation,

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

or its inverse

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

to, Weierstrass normal form

$$t^2 = s^3-(a^2/3+4c)s+2a^3/27+b^2-8ca/3.$$

Note that, this transformation does not change their determinant

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

except for its signature, namely, a discriminant reflector (= *discrefl.*):

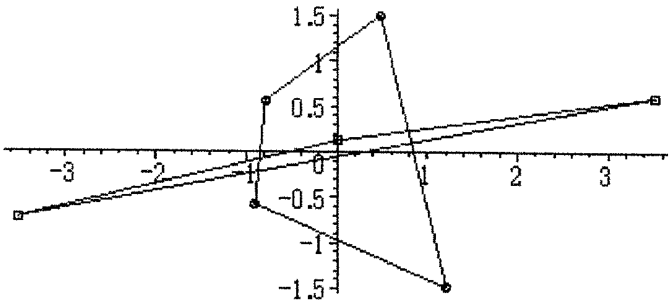
$$\det(x^4+ax^2+bx+c) + \det(s^3-(a^2/3+4c)s+2a^3/27+b^2-8ca/3) = 0$$

or more explicitly

$$x^4+ax^2+bx+c \textcircled{x} 4x^3+2ax+b$$
$$= -4a^3b^2-27b^2+16a^4c-128c^2a^2+144cab^2+256c^3$$
$$= -(s^3-(a^2/3+4c)s+2a^3/27+b^2-8ca/3 \textcircled{s} 3s^2-(a^2/3+4c)).$$

Following is an example of their roots figure:

$$x^4+ax^2+bx+c,\ s^3-(a^2/3+4c)s+2a^3/27+b^2-8ca/3 = 0,$$
$$a = 1+i,\ b = 2i+3,\ c = 3+i$$



Examle 5. Congruent number $62 = 2\cdot 31$

Congruent number is a number which is the area of right rational triangle, namely

$$n = ab/2,\ a^2+b^2 = c^2$$

and so,

$$c^2 \pm 4n = a^2+b^2 \pm 2ab = (a \pm b)^2.$$

this means that $(a-b)^2$, c^2, $(a+b)^2$ have equal difference 4n, and related to an elliptic curve of the form

$$y^2 = x(x^2-q^2).$$

with non-trivial (squared) solution.

Note that, for the equations

$$y^2 = f(x)g(x),\ y^2 = f(x)/g(x)$$

solvability is equivalent because, last one is $(yg(x))^2 = f(x)g(x)$. this principle is called prod/div-principle (= *prodiv-principle*).

The example case $q = 62$.

$$y^2 = x^2(x^4-q^2) = x(x^2+q)(x(x^2+q))$$

it is equivalent to

$$z^2 = x(x^2+q)/(x(x^2-q)) = (x^2+q)/(x^2-q)$$

and to

$$z^2 = (x^2+q)/(x^2-q),\ x^2 = q(z^2+1)/(z^2-1) \quad \text{or } x^2 = q(z^2+1)(z^2-1).$$

Right side fraction, in the case q is separated, at least as

$$x^2 = q(z^2+1)/(z^2-1),\ x^2 = 2q(z^2+1)/((z^2-1)/2)$$
$$x^2 = ((z^2+1)/2)/(2q(z^2-1)),\ x^2 = (z^2+1)/(q(z^2-1)).$$

In this case, we consider, the third one

$$x^2 = ((z^2+1)/2)/(2q(z^2-1))$$

and the equation of denominator

$$s^2 = 2q(z^2-1) \quad \text{or } t^2 = (z+1)/(2q(z-1)),$$

Last one is equivalent to

$$z = (2t^2q+1)/(2t^2q-1),$$

substitute this to $x^2 = q(z^2+1)(z^2-1)$, then we have

$$x^2 = 1/4 \cdot (4t^4q^2+1)/t^2.$$

Since other terms are complete square, it is necessary to solve

$$u^2 = 4t^4q^2+1$$

in rational numbers. We have a solution $t = 5727/84560$ for $q = 62$.

$$x^2 = 4229297547568411201/58630597962753600,$$
$$x = 2056525601/242137560 = (13\cdot37\cdot41\cdot104281)/(2^3\cdot3\cdot5\cdot7\cdot23\cdot83\cdot151)$$

and the elliptic curve

$$y^2 = x(x^2-62^2)$$
$$[x,y] = [4229297547568411201/58630597962753600,$$
$$4445629502796064172685463199/14196669932042127585216000]$$

solution. Since this point is a double point, we search for original point. Let

$$(x-a)(-3a^2+3844)+2(y-b)b = 0$$

be the tangent line at (a,b), which pass $[x,y]$ is

$$(4229297547568411201/58630597962753600-a)(-3a^2+3844)$$
$$+2(4445629502796064172685463199/14196669932042127585216000-b)b = 0.$$

With the condition $b^2 = a(a^2-62^2)$, we have factors

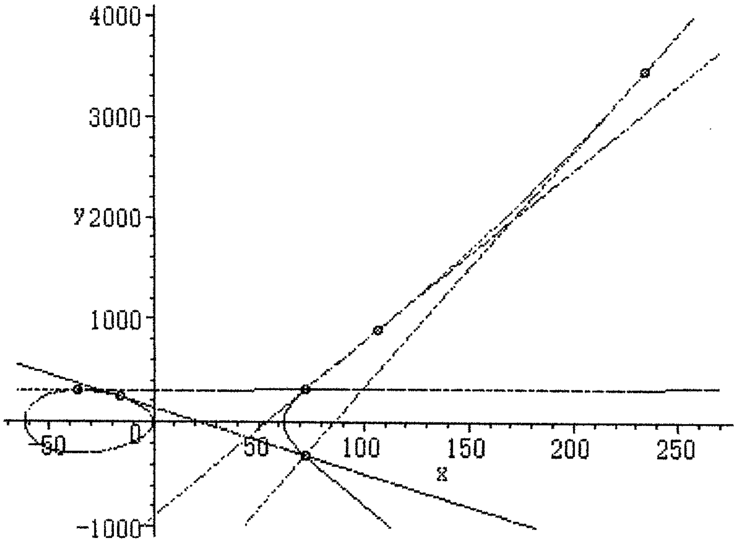
$$(19600a+706831)(22801a-2430400)(62001a+1016738)(529a-124002)$$

from which we have

$$[-706831/19600,\ 2430400/22801,\ -1016738/62001,\ 124002/529]$$

$$-31\cdot 151^2/(2^4\cdot 5^2\cdot 7^2),\ 2^6\cdot 5^2\cdot 7^2\cdot 31/151^2,\ -2\cdot 23^2\cdot 31^2/(3^2\cdot 83^2),\ 2\cdot 3^2\cdot 83^2/23^2.$$

$a = 124002/529 = 2\cdot(3\cdot 83/23)^2$could easily be obtained by direct search.



$$(19600a+706831)(22801a-2430400)(62001a+1016738)(529a-124002)$$
$$=(a^2-3844)^2-(2056525601/121068780)^2a(a-62)(a+62)+15376a^2$$
$$=(a^2-124a-3844)^2-(770844001/121068780)^2$$

and on the curve

$$x^2-y^2=4\cdot 62,$$

the smallest point is

$$[x,y]=[33,29],$$
$$[x,y]=[2056525601/121068780,\ 770844001/121068780]$$

is also on the curve. By a parametric representation

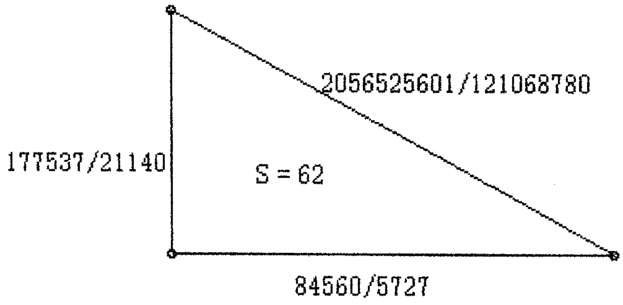
$$x=(33t^2-58t+33)/(t^2-1),\ y=-(29t^2-66t+29)/(t^2-1)$$

corresponding point is $t = 44039/31159$.

From the view point of complexity, search by both methods

$$u^2=4t^4q^2+1,\ t=5727/84560,\ \log(5727\cdot 84560)=19.99816373$$
$$y^2=x(x^2-62^2),\ x=124002/529,\ \log(124002\cdot 529)=17.99904141$$

are similar, but direct search, in this case, is little bit simpler. It is interesting, probably by chance, that both logarithm seems to be near integer.



In another direction, $y^2 = x^4-62^2$ is deformed by

$$s = 2y+2x^2,\ t = 4yx+4x^3,$$

$$y = 1/4\cdot(2s^3-t^2)/s^2,\ x = 1/2\cdot t/s$$

to $t^2 = s(s^2+15376)$, and

$$x = 2056525601/242137560,$$

$$y = 21617185317967087 99/58630597962753600,$$

$$s = 7150393600/32798529,$$

$$t = 695599219282240/187837175583$$

corresponds, but in this case, (s,t) is not a double point, so, search by this direction seems not reduce computational complexity.

Example 6. C: $y^2 = f(x) = x^4-62^2$, $d = -2^{14}\cdot 31^6$

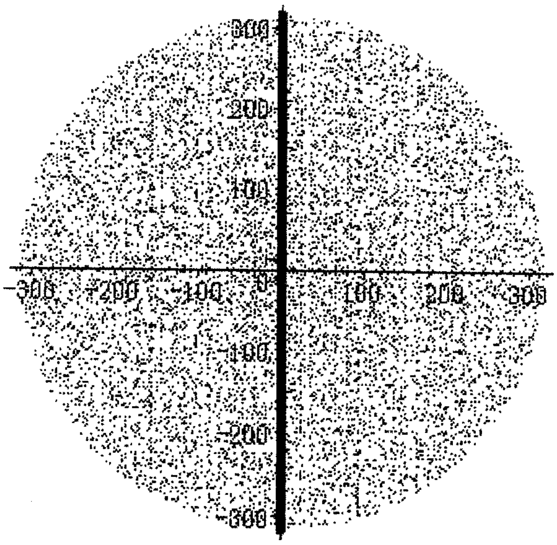
Distribution of complex roots of congruence zeta polynomial

$$x^2+a_px+p,\ a_p = 1+\sum_{x\in p}(f(x)/p)$$

of above elliptic curve is stated below:

$$x^2+a_px+p = 0,$$

$$p = 3 \sim 99991$$



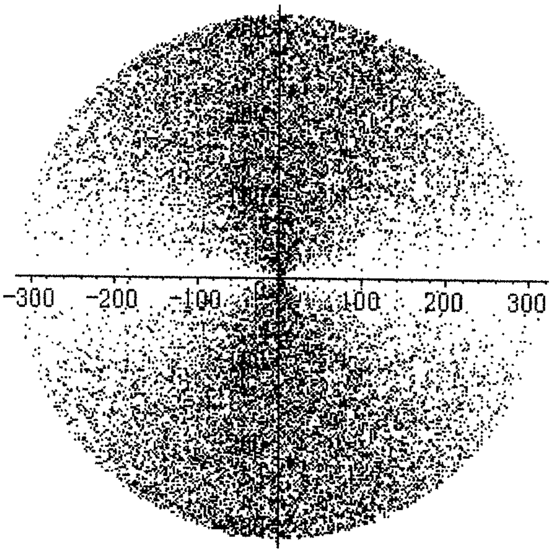
Angular distribution is 1/2 uniform for $p = 1 \bmod 4$, 1/2 pure imaginary for $p = -1 \bmod 4$. This curve have *complex multiplication.*

Next curve is modified by adding +x to the above curve:

$$\text{D:}\quad y^2 = f(x) = x^4+x-62^2$$

$$d = -1459\cdot 1723\cdot 5784283$$

$$x^2+a_px+p = 0,\ p = 3 \sim 99991,\ 9592 \text{ primes}$$

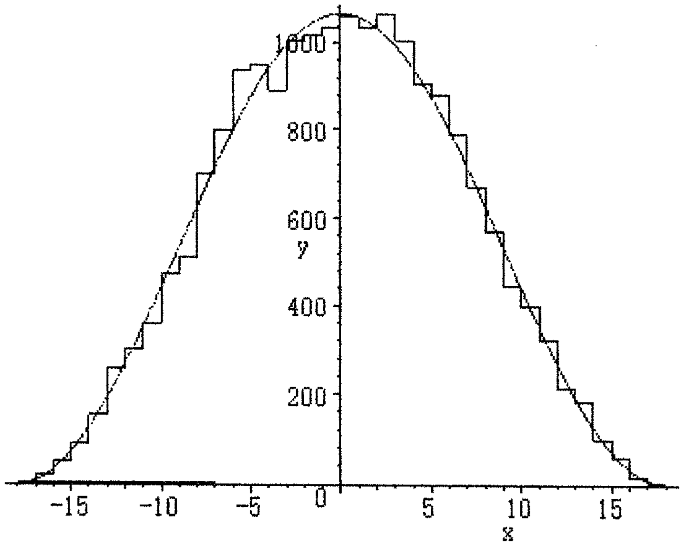


Angular distribution is proportional to $\sin^2\theta$, so called Sato-Tate $\sin^2$-distribution, and it is now known as R. Taylor's $\sin^2$-theorem.

$$\text{D:}\quad y^2 = f(x) = x^4+x-62^2$$

$$p = 3 \sim 99991,\ 9592 \text{ primes}$$

$$a\cdot\sin^2\theta,\ \theta = \pi(x-18)/36,\ a = 9592/9$$



3 Elliptic counting polynomials and fFt

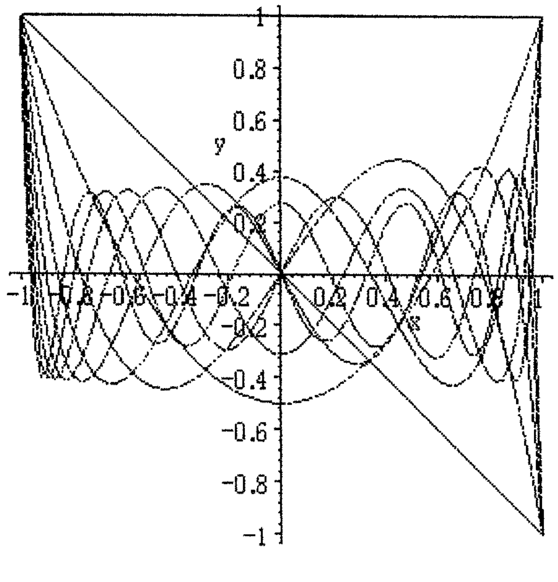
3.1 Legendre-Fuchs polynomial

Legendre-Fuchs polynomial is defined by

$$P_n(1-2x) = F(-n,n+1,1,x)$$
$$= \sum_{r\leqq n} (-n)_r(n+1)_r/r!^2 \cdot (-x)^r,\ (n)_r = n(n-1)\cdots(n-r+1)$$

and initial examples are

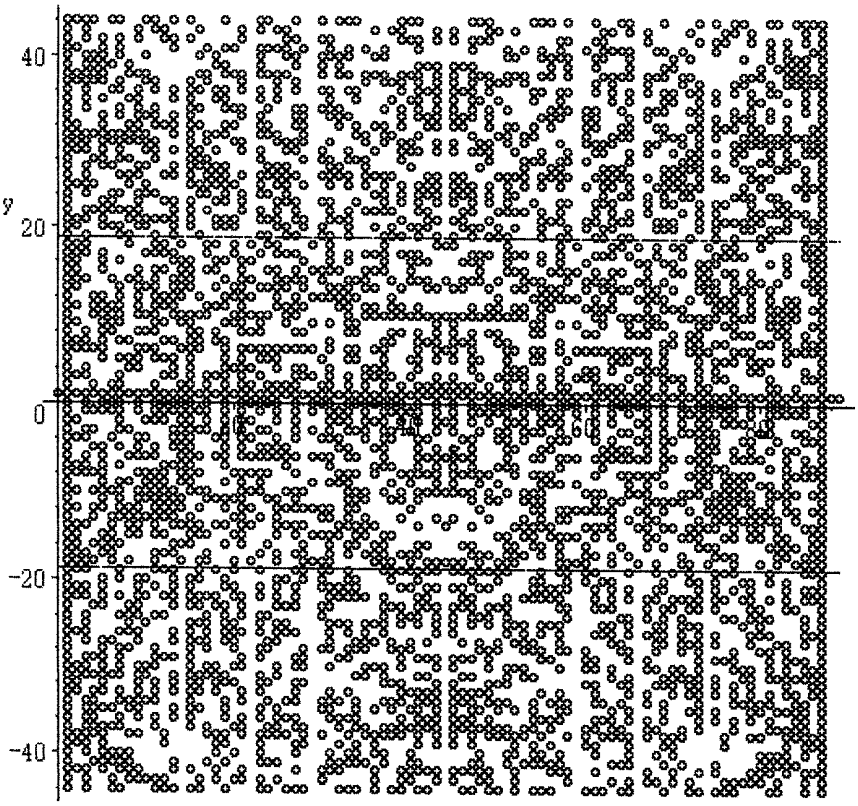
$[0, 1],[1, 1-2x],[2, 1-6x+6x^2],[3, 1-12x+30x^2-20x^3],[4, 1-20x+90x^2-140x^3+70x^4],$
$[5, 1-30x+210x^2-560x^3+630x^4-252x^5],[6, 1-42x+420x^2-1680x^3+3150x^4-2772x^5+924x^6],$
$[7, 1-56x+756x^2-4200x^3+11550x^4-16632x^5+12012x^6-3432x^7],$
$[8, 1-72x+1260x^2-9240x^3+34650x^4-72072x^5+84084x^6-51480x^7+12870x^8],$
$[9, 1-90x+1980x^2-18480x^3+90090x^4-252252x^5+420420x^6-411840x^7+218790x^8-48620x^9]$



We consider these polynomials in the finite field.

Example. $p = 89$

$$\{(n,y) : y = F(-n,n+1,1,x) \text{ lavr. mod } p,\ x \in p\}$$



in the above graph, two level line are Hasse's bound, namely

$$|F(-n,n+1,1,x) \text{ lavr. mod } p| < 2\sqrt{89} = 18.86796226$$

there are 7 slits of void line outside of this bound, namely

$$[14,22,29,44,59,66,74]$$

which is

$$-[1/6,1/4,1/3,1/2,2/3,3/4,5/6] \text{ mod } p = [74, 22, 59, 44, 29, 66, 14]$$

so, they are *Legendre-Fuchs polynomials*

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

of degree $[p/6]$, $[p/4]$, $[p/3]$, $[p/2]$ respectively, and satisfy Hessian condition.

Following family, for example, of elliptic curves are known:

name of family	curve form	polynomial	case
(Whock) family	$y^2 = x^3+qx^2+r$	F(1/6, 5/6, 1, x)	
Euler family	$y^2 = x(x^2+qx+r)$	F(1/4, 3/4, 1, x)	

Hessian family	$y^3+x^3+qxy+r = 0$	$F(1/3, 2/3, 1, x)$	
Legendre family	$y^2= x(x-1)(x-q)$	$F(1/2, 1/2, 1, x)$	
Weierstrass family	$y^2= x^3+qx+r$	$x^{(p-1)/4} F(1/12, 5/12, 1, 1-x)$	$p = 1\ (4)$
		$x^{(p+1)/4} F(7/12, 11/12, 1, 1-x)$	$p = -1\ (4)$

There are three types od fundamental properties fo elliptic counting polynomials (= elops). Hessian property, p-valued property images of p-1th root of unit, and separation property.

Example 7. $p = 29$, $Pn(1-2x) = F(-n,n',1,x)$ lavr.

$$[0, 1],[1, 1-2x],[2, 1-6x+6x^2],[3, 1-12x+x^2+9x^3],[4, 1+9x+3x^2+5x^3+12x^4],$$
$$[5, 1-x+7x^2-9x^3-8x^4+9x^5],[6, 1-13x+14x^2+2x^3-11x^4+12x^5-4x^6],$$
$$[7, 1+2x+2x^2+5x^3+8x^4+14x^5+6x^6-10x^7],[8, 1-14x+13x^2+11x^3-5x^4-7x^5+13x^6-5x^7-6x^8],$$
$$[9, 1-3x+8x^2-7x^3-13x^4-10x^5+7x^6-11x^7+14x^8+13x^9],$$
$$[10, 1+6x+12x^2-13x^3-11x^4-x^5-x^6-14x^7+10x^8-14x^9-3x^{10}],$$
$$[11, 1+13x-2x^2-x^3-7x^4+7x^5+14x^6-5x^7-14x^8+5x^9-5x^{10}-7x^{11}],$$
$$[12, 1-11x+3x^2+8x^3-14x^4-12x^5+13x^6+10x^7-12x^8+6x^9+3x^{10}+13x^{11}-7x^{12}],$$
$$[13, 1-8x+12x^2+7x^3+9x^4+2x^5-2x^6+14x^7-4x^8+4x^9-6x^{10}+11x^{11}-x^{12}-11x^{13}],$$
$$[14, 1-7x-13x^2-5x^3-7x^4+x^5-5x^6+13x^7-5x^8+x^9-7x^{10}-5x^{11}-13x^{12}-7x^{13}+x^{14}]$$
$$\mathrm{proot}(29)= [2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27]$$
$$\mathrm{pres}(29)= [3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27]$$

Here, we consider the case of elliptic counting (order) polynomials (= *elcp, elop*) and, as example, 7 symmetric cyclic involutions (= sci) related to this elop.

First, consider the case $F(1/6, 5/6, 1, x)$, for which

$$[-1/6, -5/6] \bmod 29 = [24, 4]$$

and so $-5/6 \bmod 29 = 4 = [29/6]$ is the degree of elop, take $q = 2$ as primitive root.

$$F(1/6, 5/6, 1, x)= f(x)= 1+9x+3x^2+5x^3+12x^4$$

In this case, in lavr form, its fFt [q] is:

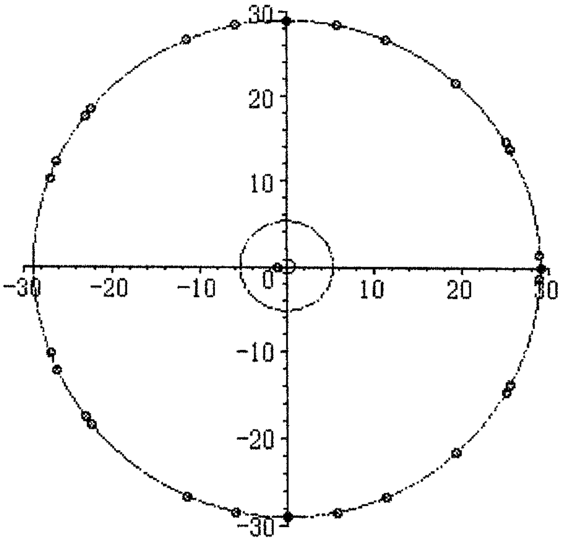
$$F(1/6, 5/6, 1, x)[2](x)= \textstyle\sum_{n\in p-1} f(q^n)x^n =$$
$$4x^{27}+9x^{26}-6x^{25}-5x^{24}-5x^{23}+10x^{22}-9x^{21}-2x^{20}-3x^{19}-9x^{18}-6x^{17}+10x^{16}$$
$$+2x^{15}+2x^{14}+x^{13}-2x^{12}-6x^{10}-6x^9+4x^8+4x^6+2x^5+x^4+9x^3-3x^2+2x+1.$$

Cyclotomic factorization of characteristic polynomial of the field $F_p = p$ is:

$$x^{p-1}-1 = x^{28}-1 =$$
$$(x-1)(x+1)(x^2+1)(x^6+x^5+x^4+x^3+x^2+x+1)(x^6-x^5+x^4-x^3+x^2-x+1)(x^{12}-x^{10}+x^8-x^6+x^4-x^2+1)$$

value distribution of images of complex p-1st root of 1 by fFt polynomial, in figure:

$$F(1/6, 5/6, 1, x)[2](e^{2\pi ik/(p-1)}),\ k = 0\sim p-2$$



and it means, there is no Gauss nor Eisenstein integer reduction (there is no image points on the circle of radius $\sqrt{p}$), but reduct at $x = 1$, namely $g(1) = -1$ but $g(1) = p$.

Let the residue matrix $f(x)\ [x]\ g(x)$ for polynomial $f(x)$ and degree d polynomial is defined to be:

$$f(x)\ [x]\ g(x) = (c_{ij}) \quad d = \text{degree}(g(x))$$

$$c_{ij} = \text{coeff}(\text{rem}(x^{j-1} f(x), g(x), x), x, d-i)$$

namely the matix determined by the coefficient x^{d-1} of reminder of $x^{j-1}f(x)$ by degree d polynomial $g(x)$.

Hence, in this case, for any $g(x)$ split mod p, namely a factor of characteristic polynomial of finite prime fields x^p-x in F_p, and if $g(1) \neq 0$, then the residue matrix

$$F(1/6, 5/6, 1, x)\ [2]\ (x)\ [x]\ g(x) = F(1/6, 5/6, 1, x)\ [2|x]\ g(x),$$

$$A = 1/p \cdot F(1/6, 5/6, 1, x)\ [2|x]\ g(x),$$

A is an involution ie. $A^2 = E$, if moreover, A is symmetric cyclic, then it is called *symmetric cyclic involution* (= sci.)

The case $g(x) = x^7 - 1 = x(x^6+x^5+x^4+x^3+x^2+x+1)$, since $g(1)$,

$$A = F(1/6, 5/6, 1, x)\ [2|x]\ x^7 - 1 =$$

$$\begin{pmatrix} 7 & 6 & -14 & -8 & -4 & 18 & -6 \\ 6 & -14 & -8 & -4 & 18 & -6 & 7 \\ -14 & -8 & -4 & 18 & -6 & 7 & 6 \\ -8 & -4 & 18 & -6 & 7 & 6 & -14 \\ -4 & 18 & -6 & 7 & 6 & -14 & -8 \\ 18 & -6 & 7 & 6 & -14 & -8 & -4 \\ -6 & 7 & 6 & -14 & -8 & -4 & 18 \end{pmatrix}$$

is symmetric cyclic but not produce sci, namely

$$A^2 = \begin{pmatrix} 721 & -120 & -120 & -120 & -120 & -120 & -120 \\ -120 & 721 & -120 & -120 & -120 & -120 & -120 \\ -120 & -120 & 721 & -120 & -120 & -120 & -120 \\ -120 & -120 & -120 & 721 & -120 & -120 & -120 \\ -120 & -120 & -120 & -120 & 721 & -120 & -120 \\ -120 & -120 & -120 & -120 & -120 & 721 & -120 \\ -120 & -120 & -120 & -120 & -120 & -120 & 721 \end{pmatrix}$$

but

$$1/p \cdot F(1/6, 5/6, 1, x)\,[2|x]\,x^6+x^5+x^4+x^3+x^2+x+1 = 1/p \cdot \begin{pmatrix} -1 & -21 & -15 & -11 & 11 & -13 \\ -20 & -14 & -10 & 12 & -12 & 1 \\ 6 & 10 & 32 & 8 & 21 & 20 \\ 4 & 26 & 2 & 15 & 14 & -6 \\ 22 & -2 & 11 & 10 & -10 & -4 \\ -24 & -11 & -12 & -32 & -26 & -22 \end{pmatrix}$$

is not symmetric but it is an involution.

Consider another case $x^7+1 = (x+1)(x^6-x^5+x^4-x^3+x^2-x+1)$

$$1/p \cdot F(1/6, 5/6, 1, x)\,[2|x]\,x^7+1 = 1/p \cdot \begin{pmatrix} -3 & -8 & -2 & 14 & 18 & -10 & 12 \\ -8 & -2 & 14 & 18 & -10 & 12 & 3 \\ -2 & 14 & 18 & -10 & 12 & 3 & 8 \\ 14 & 18 & -10 & 12 & 3 & 8 & 2 \\ 18 & -10 & 12 & 3 & 8 & 2 & -14 \\ -10 & 12 & 3 & 8 & 2 & -14 & -18 \\ 12 & 3 & 8 & 2 & -14 & -18 & 10 \end{pmatrix}$$

this matrix is not a cyclic, because the first element -3, when inserted as last element the sign is changed to 3, but this an involution. Now consider the checker bord transformation, namely multiply $(-1)^{i+j}$ to each matrix element, does not change involution property because the degree is odd, and it is achieved by changing sign of x, namely by taking F(1/6, 5/6, 1, -x) instead of F(1/6, 5/6, 1, x):

$$1/p \cdot F(1/6,\ 5/6,\ 1,\ -x)\ [2|x]\, x^7\text{-}1 = 1/p \cdot$$

$$\begin{pmatrix} -3 & 8 & -2 & -14 & 18 & 10 & 12 \\ 8 & -2 & -14 & 18 & 10 & 12 & -3 \\ -2 & -14 & 18 & 10 & 12 & -3 & 8 \\ -14 & 18 & 10 & 12 & -3 & 8 & -2 \\ 18 & 10 & 12 & -3 & 8 & -2 & -14 \\ 10 & 12 & -3 & 8 & -2 & -14 & 18 \\ 12 & -3 & 8 & -2 & -14 & 18 & 10 \end{pmatrix}$$

this matrix is sci as expected.

$$F(1/4,\ 3/4,\ 1,\ x) = 1+2x+2x^2+5x^3+8x^4+14x^5+6x^6-10x^7$$

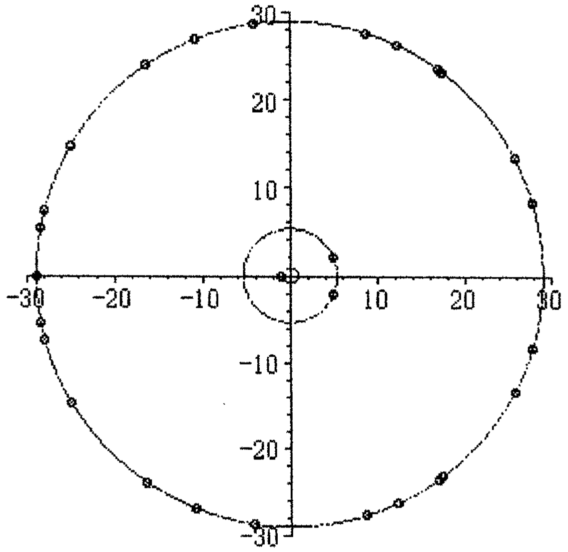
In this case, in lavr form, all coefficient positive exponents are even,

$$F(1/4,\ 3/4,\ 1,\ x)\ [2]\ (x) =$$

$$-2x^{26}-6x^{24}+6x^{23}-6x^{22}+10x^{21}+2x^{20}-6x^{19}-10x^{18}+2x^{17}+6x^{16}+4x^{15}+6x^{14}$$

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

$$f(x) = F(1/4,\ 3/4,\ 1,\ x)\ [2]\ (e^{2\pi ik/(p-1)}),\ k = 0\sim p\text{-}2$$



in this case Gaussian reduction occur, namely $p = 29 = 5^2+2^2 = (5+2i)(5\text{-}2i)$, it means the value of cyclotomic factor x-1, x^2+1 is reduced, or

$$f(1) = -1,\ f(-1) = -29,\ f(i) = 5+2i,\quad f(-i) = 5\text{-}2i.$$

So, in this case, only

$$1/p \cdot F(1/4,\ 3/4,\ 1,\ -x)\ [2|x]\, x^7\text{-}1 = 1/p \cdot$$

$$\begin{pmatrix} -6 & 6 & -24 & -12 & 6 & -2 & 3 \\ 6 & -24 & -12 & 6 & -2 & 3 & -6 \\ -24 & -12 & 6 & -2 & 3 & -6 & 6 \\ -12 & 6 & -2 & 3 & -6 & 6 & -24 \\ 6 & -2 & 3 & -6 & 6 & -24 & -12 \\ -2 & 3 & -6 & 6 & -24 & -12 & 6 \\ 3 & -6 & 6 & -24 & -12 & 6 & -2 \end{pmatrix}$$

is sci.

$$F(1/3, 2/3, 1, x) = 1-3x+8x^2-7x^3-13x^4-10x^5+7x^6-11x^7+14x^8+13x^9$$

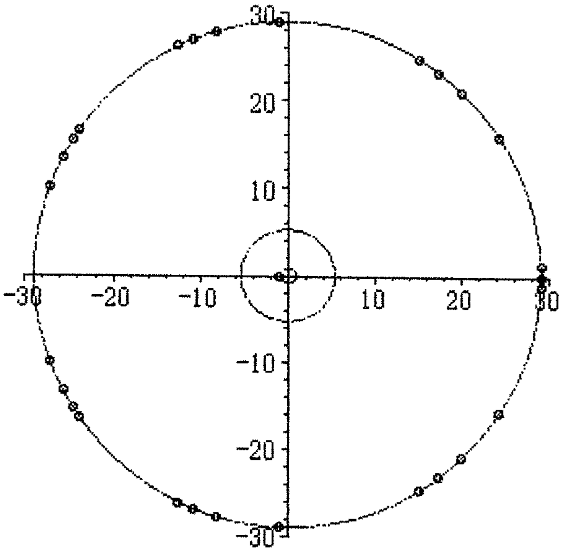
In this case, in lavr form, all coefficient positive exponents are multiple of 3,

$$F(1/3, 2/3, 1, x)[2](x) =$$

$$3x^{26}+6x^{25}+9x^{24}-9x^{23}-6x^{22}+3x^{21}-6x^{20}+9x^{19}-3x^{18}-6x^{17}+6x^{16}$$

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

$$f(x) = F(1/3, 2/3, 1, x)[2](e^{2\pi ik/(p-1)}), k = 0 \sim p-2$$



In this case g(1) = -1, g(-1) = 29, and no Gauss-Eisenstein reduction, only 7-sci is:

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

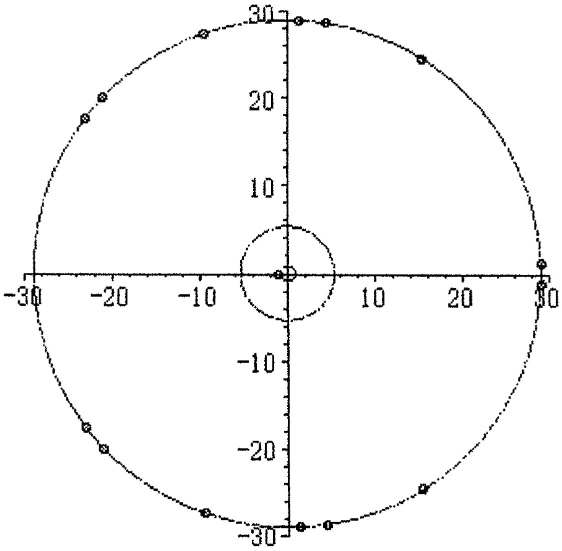
$$\begin{pmatrix} -3 & 6 & -6 & 24 & 12 & -6 & 2 \\ 6 & -6 & 24 & 12 & -6 & 2 & -3 \\ -6 & 24 & 12 & -6 & 2 & -3 & 6 \\ 24 & 12 & -6 & 2 & -3 & 6 & -6 \\ 12 & -6 & 2 & -3 & 6 & -6 & 24 \\ -6 & 2 & -3 & 6 & -6 & 24 & 12 \\ 2 & -3 & 6 & -6 & 24 & 12 & -6 \end{pmatrix}$$

This case, as a result, is the same as $1/p \cdot F(1/4, 3/4, 1, -x)\,[2|x]\,x^7-1$ except for the order of elements.

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

In this case, in lavr form, all coefficient positive exponents are of the form 4n+2,

$$F(1/2, 1/2, 1, x)\,[2]\,(x) =$$
$$10x^{27}+6x^{26}-6x^{25}-2x^{24}-2x^{23}-2x^{22}+6x^{21}-2x^{20}+6x^{19}+6x^{18}+6x^{17}-2x^{16}+2x^{15}$$
$$-10x^{14}-2x^{13}-2x^{12}-6x^{11}+6x^{10}-6x^9-2x^8-6x^7-2x^6+2x^5-2x^4+6x^3+6x^2-10x+1$$
$$f(x) = F(1/2, 1/2, 1, x)\,[2]\,(e^{2\pi i k/(p-1)}),\ k = 0 \sim p-2$$



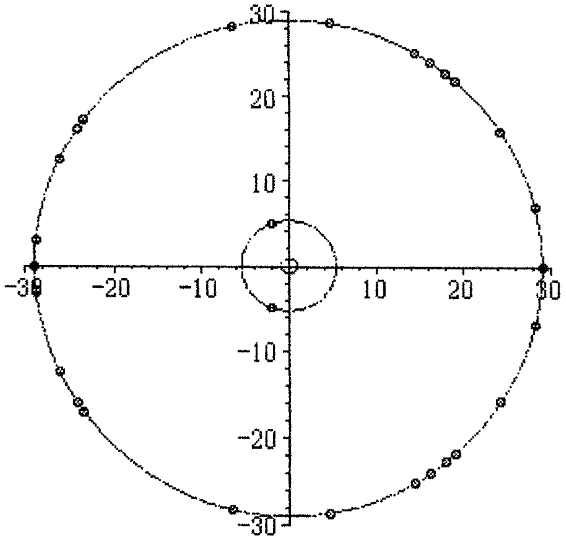
In this case $g(1) = g(-1) = -1$, so 7-sci both of the form

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

does not exist, because a factor of x^7-1, x^7+1 are degenerate.

How about in the case of Weierstrass form, $p = 29 = 1 \bmod 4$, in this case

$$F(1/12, 5/12, 1, x) = 8x^2-5x+1$$
$$x^{(p-1)/4}\,F(1/12, 5/12, 1, 1-x) = x^7(8x^2-11x+4)$$
$$x^{(p-1)/4}\,F(1/12, 5/12, 1, 1-x)\,[2]\,(x) =$$
$$-6x^{27}-9x^{27}+4x^{25}-3x^{24}-5x^{23}-4x^{22}-x^{21}+10x^{20}-3x^{19}+5x^{18}-2x^{17}+2x^{16}$$
$$+6x^{14}-7x^{13}-8x^{11}-2x^{10}+6x^9-2x^8+8x^7+6x^6-6x^5-9x^4-3x^3-x^2-6x+1$$



In this case

$$[g(1),\ g(-1),\ g(i),\ g(-i)] = [-29,\ 29,-2+5i,\ -2-5i]$$

so only the degenerate factor is x^2+1, and Gaussian reduction occurs, so both of them produce 7-sci.

$$1/p\cdot x^{(p-1)/4}\ F(1/12,\ 5/12,\ 1,\ 1-x)\ [2|x]x^7-1 = 1/p\cdot$$

$$\begin{pmatrix} 3 & -18 & -8 & -10 & 2 & -12 & 14 \\ -18 & -8 & -10 & 2 & -12 & 14 & 3 \\ -8 & -10 & 2 & -12 & 14 & 3 & -18 \\ -10 & 2 & -12 & 14 & 3 & -18 & -8 \\ 2 & -12 & 14 & 3 & -18 & -8 & -10 \\ -12 & 14 & 3 & -18 & -8 & -10 & 2 \\ 14 & 3 & -18 & -8 & -10 & 2 & -12 \end{pmatrix}$$

$$1/p\cdot x^{(p-1)/4}\ F(1/12,\ 5/12,\ 1,\ 1-x)\ [2|x]x^7+1 =$$

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

but the latter is trivial one.

Uppermost row of 7-sci's obtained above are

$$[-3,\ 8,\ -2,\ -14,\ 18,\ 10,\ 12],\ [-6,\ 6,\ -24,\ -12,\ 6,\ -2,\ 3],$$

[-3, 6, -6, 24, 12, -6, 2], [3, -18, -8, -10, 2, -12, 14]

and if change sign so as to make the sum to p and sort them, then they fall in to two cases,

[-6, -6, -3, 2, 6, 12, 24], [-14, -3, -2, 8, 10, 12, 18]

and moreover, if by τ denote the signature of sci, the sum of elements of a row ±p, then they have opposite sign:

$$\tau(1/p\cdot x^{(p-1)/4}\,F(1/12, 5/12, 1, 1-x)\,[2|x]x^7-1)+\tau(1/p\cdot F(1/6, 5/6, 1, -x)\,[2|x]x^7+1)=0$$

$$\tau(1/p\cdot F(1/3, 2/3, 1, -x)\,[2|x]x^7+1)+\tau(1/p\cdot F(1/4, 3/4, 1, -x)\,[2|x]x^7+1\,)=0$$

The condition of 7-sci's is as in ideal basis (or in equational form, insert = 0):

$$[ad+be+cf+dg+ea+fb+gc,\ ac+bd+ce+df+eg+fa+gb,$$
$$ab+bc+cd+de+ef+fg+ga,\ a+b+c+d+e+f+g-p]$$

Number of variables a,bc,d,e,f,g is 7 and number of conditions is 4.

$$e = -(ad+a^2-cd+ac+df+2fa-bc+fb+cf+f^2-fp-pa)/(a-d)$$

$$g = (-ab-bc+ad+bd+d^2+2df-dp+fa+fb+cf+f^2-fp)/(a-d)$$

and eliminated two formulas are

$$-2adb-c^2b+d^3+2adc-a^3+fpb+cfa-2fa^2+2fd^2-f^2a-a^2b-dfb+2dcf-fcp-dfp-d^2p$$
$$+cd^2+bd^2+b^2c-a^2c+pa^2+dbc-dcp-bf^2+df^2+fc^2+cf^2-fb^2+fpa-2fab+abp-abc,$$
$$pabc+f^2ab+bcdp+3f^3a+2cf^3+2f^3b-2ad^2p+b^2d^2-bd^2p+5cf^2a+4cf^2+cdf^2-3cdfb-2cfd^2$$
$$-2cf^2p+f^4+c^2f^2-2f^2bp+2fb^2d-2fb^2a-2b^2cf-2bc^2f+f^2b^2-4f^2a*p+7adf^2-4df^2p+3df^3-2d^2fp$$
$$+5df^2b+4d^2fb-2a^2fb-2a^2fp+3a^2f^2+3d^2f^2-2dc^2f+2c^2fa+2adfb+6d^2fa+6dfa^2+p^2af+fp^2d$$
$$+f^2p^2-2f^3p-cd^3+3a^2cd-2ac^2b-a^3b-2a^2cb+a^3d+cd^2p-2cd^2a+2c^2db-2a^2dp+pa^2b+p^2ad$$
$$-2c^2ad+c^2a^2-cpa^2+c^2d^2+a^2b^2-3cfpa+cdfp-3cfab+2cdfa-6adfp+fpab-3fbdp+2bcfp$$
$$-2ab^2d-2a^2bd+2ab^2c+b^2c^2+2a^2d^2+3abd^2+ad^3-2bcd^2-2b^2cd.$$

By total search of 7-sci for p = 29, we have, 5 sorted sequences

[-6, -6, -3, 2, 6, 12, 24], [-14, -3, -2, 8, 10, 12, 18]

[-19, 4, 4, 4, 12, 12, 12], [-8, -4, -2, -2, 10, 13, 22], [-12, -8, 0, 8, 12, 13, 16]

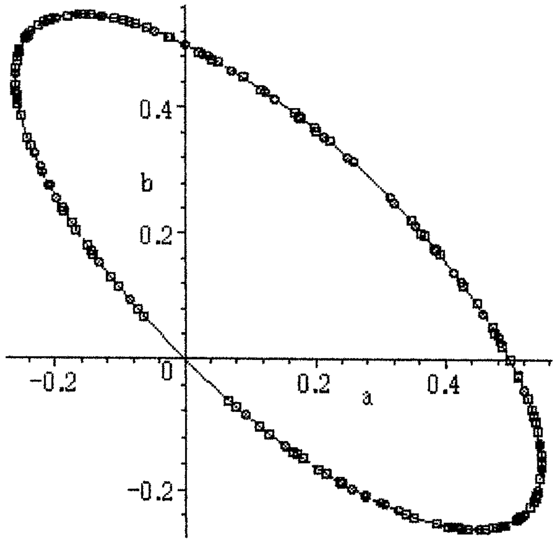
first two are obtained as residue matrix of elops corresponding to

$$F(1/3, 2/3, 1, -x)\,[2|x]x^7+1 \approx [-6, -6, -3, 2, 6, 12, 24]$$

$$x^{(p-1)/4}\,F(1/12, 5/12, 1, 1-x)\,[2|x]x^7-1 \approx [-14, -3, -2, 8, 10, 12, 18]$$

[p-3 (a+b), a,a,b,a,b,b]

$[a,b]/p,\ p = (2a^2+3ab+2b^2)/(a+b),\ p = 2\sim 997$



[4/29, 12/29],[-10/43, 14/43],[-14/71, 18/71],[24/113, 40/113],[-30/127, 66/127]

$p = 43$

[-12, -6, -6, -2, 18, 24, 27], [-10, -10, -10, 14, 14, 14, 31],
[-21, -6, 6, 6, 12, 16, 30], [-16, -4, -1, 2, 8, 22, 32],
[-14, -1, 2, 2, 2, 14, 38]

$$F(1/6,5/6,1,x) = 1-13x-18x^2+14x^3-17x^4+9x^5+15x^6+8x^7$$

$$1/p\cdot F(1/6,5/6,1,-x)\ [6|x]x^7-1 \approx [16, 1, -8, -22, 4, -32, -2]$$

$$F(1/4,3/4,1,x) = 1+19x+3x^2-6x^3-17x^4+x^5-7x^6-21x^7+11x^8-11x^9-15x^{10}$$

$$1/p\cdot F(1/4,3/4,1,-x)\ [6|x]x^7-1 \approx [24, -6, 18, -6, -2, -12, 27]$$

$$F(1/3,2/3,1,x) =$$
$$1+5x-2x^2-12x^3-2x^4-2x^5+10x^6+21x^7+18x^8-2x^9+11x^{10}-13x^{11}+16x^{12}-13x^{13}+8x^{14}$$

$$1/p\cdot F(1/3,2/3,1,-x)\ [6|x]x^7-1 \approx [12, -27, -24, 6, -18, 6, 2]$$

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

$1/p\cdot F(1/2,1/2,1,\pm x)\ [6|x]x^7-1$ do not give any sci.

$$x^{(p+1)/4}\, F(1/12, 5/12, 1, 1-x) = x^{11}(-21+17x-3x^2+8x^3)$$

$$1/p\cdot x^{(p+1)/4}\, F(1/12, 5/12, 1, 1-x)\ [6|x]x^7-1 \approx [4, 1, -32, -8, -2, -22, 16]$$

It is also true that:

$$1/p\cdot F(1/6,5/6,1,-x)\ [6|x]x^7-1 \approx 1/p\cdot x^{(p+1)/4}\, F(1/12, 5/12, 1, 1-x)\ [6|x]x^7-1$$

$$1/p\cdot F(1/4,3/4,1,-x)\ [6|x]x^7-1 \approx 1/p\cdot F(1/3,2/3,1,-x)\ [6|x]x^7-1$$

$p = 71$

[-18, -10, -6, -2, 22, 27, 58], [-18, -12, -8, -5, 28, 42, 44],

$$[-14, -14, -14, 18, 18, 18, 59],\ [-12, -9, -6, 6, 8, 18, 66],$$
$$[-38, -2, 4, 7, 22, 38, 40]$$

we also have 5 patterns.

$p = 71,\ q = 7$

$$F(1/6,5/6,1,x) = 1+10x+30x^2+6x^3+26x^4+17x^5+11x^6-26x^7+22x^8+10x^9+10x^{10}+24x^{11}$$

$$1/p \cdot F(1/6,5/6,1,-x)\ [7|x]\, x^7-1 \approx [44, -12, 42, -5, -18, -8, 28]$$

$$F(1/4,3/4,1,x) =$$
$$1-22x-32x^2-22x^3-4x^4+6x^5+25x^6+16x^7-27x^8+7x^9$$
$$-35x^{10}-19x^{11}+20x^{12}+23x^{13}-16x^{14}-14x^{15}-33x^{16}-17x^{17}$$

$$1/p \cdot F(1/4,3/4,1,-x)\ [7|x]\, x^7-1 \approx [6, -6, 8, -12, 66, 18, -9]$$

$$F(1/3,2/3,1,x) =$$
$$1+16x+x^2+34x^3+24x^4+9x^5-24x^6+31x^7+26x^8+30x^9-25x^{10}+8x^{11}+24x^{12}$$
$$+3x^{13}+11x^{14}+6x^{15}+6x^{16}+19x^{17}-21x^{18}+25x^{19}+7x^{20}-19x^{21}+5x^{22}+15x^{23}$$

$$1/p \cdot F(1/3,2/3,1,-x)\ [7|x]\, x^7-1 \approx [-12, 66, 18, -9, 6, -6, 8]$$

$$F(1/2,1/2,1,x) =$$
$$x^{35}+18x^{34}+19x^{33}+27x^{32}+24x^{31}-26x^{30}-11x^{29}+30x^{28}-23x^{27}+6x^{26}+15x^{25}+10x^{24}$$
$$-31x^{23}+29x^{22}+18x^{21}-13x^{20}-7x^{19}+20x^{18}+20x^{17}-7x^{16}-13x^{15}+18x^{14}+29x^{13}$$
$$-31x^{12}+10x^{11}+15x^{10}+6x^9-23x^8+30x^7-11x^6-26x^5+24x^4+27x^3+19x^2+18x+1$$

$1/p \cdot F(1/2,1/2,1,\pm x)\ [7|x]\, x^7-1$ do not give any sci.

$$x^{(p+1)/4}\, F(1/12, 5/12, 1, 1-x) = x^{18}(7+14x-13x^2-9x^3-26x^4+28x^5)$$

$$1/p \cdot x^{(p+1)/4}\, F(1/12, 5/12, 1, 1-x)\ [7|x]\, x^7-1 \approx [8, -42, -28, 5, -44, 18, 12]$$

for this case also

$$1/p \cdot F(1/6,5/6,1,-x)\ [7|x]\, x^7-1 \approx 1/p \cdot x^{(p+1)/4}\, F(1/12, 5/12, 1, 1-x)$$
$$1/p \cdot F(1/4,3/4,1,-x)\ [7|x]\, x^7-1 \approx 1/p \cdot F(1/3,2/3,1,-x)\ [7|x]\, x^7-1$$

Problem (Conjecture): For any prime p mod 7 = 1,

$$F(1/6,5/6,1,-x)\ [7|x]\, x^7-1 \approx x^{(p+1)/4}\, F(1/12, 5/12, 1, 1-x)\ [7|x]\, x^7-1$$
$$F(1/4,3/4,1,-x)\ [7|x]\, x^7-1 \approx F(1/3,2/3,1,-x)\ [7|x]\, x^7-1$$

last one contain only one odd and not multiple of 3 number.

For p = 113, at least 8

$$[-18, -10, -6, -2, 22, 27, 58],\ [-18, -12, -8, -5, 28, 42, 44],$$
$$[-14, -14, -14, 18, 18, 18, 59],\ [-12, -9, -6, 6, 8, 18, 66],$$
$$[-38, -2, 4, 7, 22, 38, 40],\ [-68, -6, 17, 24, 42, 46, 58],$$
$$[-31, -18, -12, -6, 48, 54, 78],\ [-44, -36, 12, 17, 48, 52, 64]$$

Cocerning to the number 5, there is well known

five fifth-power problem (= ffpp)

$$a^5+b^5+c^5+d^5+e^5 = 0$$

asking for non-trivial integer solution not

[27, 84, 110, 133, -144], [-220, 5027, 6237, 14068, -14132].

Example 8. Separability

p = 314159441. primitive root q = 3.

$$x^7-1 =$$

$$(x+21258977)(x+258937828)(x+13866133)(x+231627809)$$
$$(x+314159440)(x+85037092)(x+17591044)$$

This means that the 7th root of 1 in F_p are

[292900464, 55221613, 300293308, 82531632, 1, 229122349, 296568397]

for example,

$$n = (p-1)/7 = 44879920,$$
$$q^{44879920} \bmod p = 3^{44879920} \bmod p = 296568397.$$

In this case, as for example the smallest 55221613. By the following Farey series

[1/14,1/7,1/6,3/14,1/4,2/7,1/3,5/14,3/7,1/2]

in the fFt

$$F(1/6,5/6,1,x) = \sum_{n\in[p/6]} (1/6)_n(5/6)_n/n!^2\cdot x^n$$
$$= (1-x^{p-1})\sum_{n\in[p/6]} (1/6)_n(5/6)_n/n!^2\cdot 1/(1-q^n x)$$

only one index n = (p-1)/7 = 44879920 is necessary for the computation of

$$1/p\cdot F(1/6,5/6,1,x)\,[3|x]\,x^7-1 = 1/p\cdot$$

cyclic matrix generated by

[72873704, 111835922, -110011218, 23191871,
-113130006, -76100886, -222818828]

because, other factor m < p/6, m ≠ (p-1)/7 = 44879920, the polynomial

$$(1-x^{p-1})/(1-q^m x)$$

is divisible by x^7-1, so the remainder by x^7-1 is 0 (simple but essential), only on n = (p-1)/7 = 44879920 remain.

In this case, we take as 7-th root 55221613,

$$(1/6)_n(5/6)_n/n!^2 = -91340613,\ n = (p-1)/7 = 44879920$$
$$-118202954/7\cdot(1-x^7)/(1-55221613x) = \text{lavr}$$

[72873704, 111835922, -110011218, 23191871,
-113130006, -76100886, 91340613]

but this does not determine sci. but, in this case, 91340613-p = -222818828 produce a sci. Usually, some other places would be replaced by ±p change of the numbers.

$$F(1/4,3/4,1,x) = \sum_{n\in[p/4]} (1/4)_n(3/4)_n/n!^2\cdot x^n$$

$$= (1-x^{p-1}) \sum_{n\in[p/6]} (1/4)_n (3/4)_n/n!^2 \cdot 1/(1-q^n x)$$

Because 1/4 < 2/7, only the index n = (p-1)/7 = 44879920 is necessary for the computation of

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

cyclic matrix generated by

[-23191871, 113130006, 76100886, 222818828,
-72873704, -111835922, 110011218]

$$n = (p-1)/7,\ (1/4)_n (3/4)_n/n!^2 = 151816344$$

$$151816344/7 \cdot (1-x^7)/(1-55221613x) = \text{lavr}$$

[-23191871, 113130006, 76100886, -91340613, -72873704, -111835922, 110011218]

in this case the third element 222818828-p = -91340613 is the place of change.

In the case of F(1/3,2/3,1,x), we need to compute two coefficients because

1/7, 2/7 < 1/3,

for n = (p-1)/7,

$$(1/3)_n (2/3)_n/n!^2 = -43934091,$$

$$(1/3)_{2n} (2/3)_{2n}/(2n)!^2 = -87861714.$$

For me, it is big surprise that, the second one is about the twice;

$$87861714 = 2 \cdot 43934091-6468,\ 6468 = 2^2 \cdot 3 \cdot 7^2 \cdot 11$$

Any way it is computed as,

$$55221613^2 = 229122349,$$

$$(1-x^7)/7 \cdot (-43934091/(1-55221613x)-87861714//(1-229122349x)) = \text{lavr}$$

[26051948, -105589262, -46140554, -123355843,
-49306634, -138543385, 122724289]

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

cyclic matrix generated by

[26051948, -105589262, -46140554, 190803598, -49306634, 175616056, 122724289]

this matrix is 7-sci. In this case, the difference of lavr and 7-sci is on two places

[0, 0, 0, -314159441, 0, -314159441, 0]

namely,

190803598 = p-105589262, 175616056 = p-46140554

For the relation of F(1/3,2/3,1,x), F(1/4,3/4,1,x), we have

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

[-23191871, 113130006, 76100886, 222818828,
-72873704, -111835922, 110011218]

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

$$[26051948, -105589262, -46140554, 190803598,$$
$$-49306634, 175616056, 122724289]$$

and there seems no obvious relation.

For $p = 314159441 \bmod 4 = 1$, $(p-1)/4 = 78539860$,

$$1/4 < 2/7 < 1/3,\ n = (p-1)(2/7-1/4) = 11219980$$
$$(1/12)_n(5/12)_n/(n!(1/2)_n) = -9441060$$
$$-9441060/7\cdot(1-x^7)/(1-55221613x) =$$
$$[-46228643, 114374716, 25921726, -11262213, 1420615, -102260115, 18033914]$$

but

$$x^{78539860}\cdot F(1/12, 5/12, 1, 1-x)[3|x](x^7-1) = x^{78539860}\cdot F(1/12, 5/12, 1/2, x)[3|x](x^7-1)$$
$$x^{78539860}\cdot F(1/12, 5/12, 1/2, -x)[3|x](x^7+1)$$

seems not determine 7-sci. Probably $F(1/12, 5/12, 1/2, \pm 1) = \pm 1$.

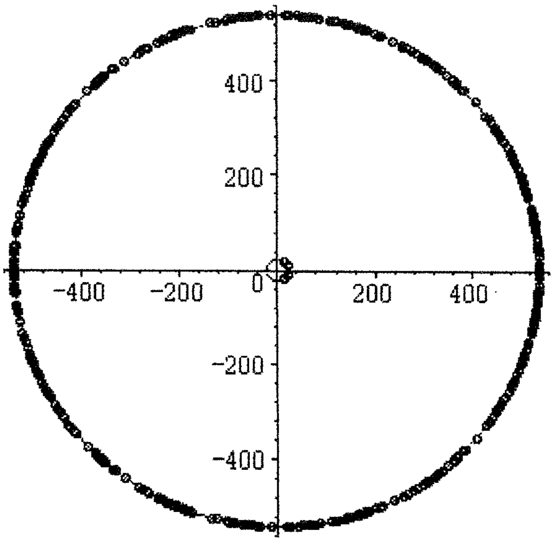
Example 9. Uniform angular distribution of values of p-1th root of 1.

Consider Weierstrass elop fFt for $p = 541$, $q = 2$

$$x^{(p-1)/4}F(1/12, 5/12, 1, 1-x) =$$
$$x^{135}(-29x^{45}-143x^{44}-95x^{43}-163x^{42}+191x^{41}+249x^{40}+242x^{39}+23x^{38}+61x^{37}+262x^{36}+35x^{35}$$
$$-220x^{34}+65x^{33}-139x^{32}+99x^{31}-102x^{30}-163x^{29}-50x^{28}+243x^{27}+101x^{26}-219x^{25}-200x^{24}$$
$$-21x^{23}+7x^{22}-218x^{21}-x^{20}-113x^{19}-33x^{18}-178x^{17}+33x^{16}+25x^{15}-16x^{14}-40x^{13}+2x^{12}$$
$$+108x^{11}-100x^{10}+269x^{9}-60x^{8}+254x^{7}+3x^{6}-236x^{5}+47x^{4}+35x^{3}-265x^{2}-48x-42)$$
$$g(x) = x^{(p-1)/4}F(1/12, 5/12, 1, 1-x)[2](x)$$

and their images of (complex) p-1th root of 1.

$$x^{(p-1)/4}F(1/12, 5/12, 1, 1-x)[2](e^{2\pi ik/(p-1)})$$
$$p = 541,\ k = 0 \sim 540$$



in this case, we have Gauss and Eisenstein's reduction, namely for, $\omega = (-1+\sqrt{-3})/2$,

$$g(\pm i) = 21\pm 10i,\ g(\pm\omega) = (29-21(\pm\sqrt{-3}))/2$$

in this case $g(\pm 1) = 541$ and $p-1 = 540 = 2^2\cdot 3^3\cdot 5$, so both $x^5\pm 1$ produce 5-sci.

$$1/p\cdot x^{(p-1)/4}F(1/12, 5/12, 1, 1-x)\,[2|x]x^5-1 =$$

5-sci produced by [0, 0, 0, 1, 0]

$$1/p\cdot(-x)^{(p-1)/4}F(1/12, 5/12, 1, 1+x)\,[2|x]x^5-1 =$$

5-sci produced by [264,-312,172,141,276].

also, since the reduction polynomials are x^2+1, x^2+x+1, other cyclotomic polynomial of $x^{p-1}-1$ such as x^3+1, x^9+1, $x^{27}+1$, $\cdots$, $x^{135}+1$ produce a sci.

$$g(-x)\,[x]x^3-1 = [0, 1, 0]$$

$$g(-x)\,[x]x^9-1 = 1/541\cdot[-84, 35, 301, 100, 319, -178, -16, 187, -123]$$

$$g(-x)\,[x]x^{15}-1 = 1/541\cdot$$

[88, -104, -123, 47, 92, 88, -104, 418, 47, 92, 88, -104, -123, 47, 92]

$$g(-x)\,[x]x^{27}-1 = 1/541\cdot$$

[-32, 56, 165, 68, 203, -199, 115, 6, -153, -49, 19, -11, 35,
163, 64, -140, -8, -88, -3, -40, 147, -3, -47, -43, 9, 189, 118]

$$g(-x)\,[x]x^{45}-1 = 1/541\cdot$$

[-31, -119, 101, -17, 77, 7, -124, 150, 26, 51, 95, 84, -25, -30,
98, 23, -62, -96, 65, -36, 60, 2, 180, -89, -3, -22, -122, -187, 7,
-54, 96, 77, -128, -1, 51, 21, 18, 88, 110, 44, 15, -66, 89, 70, 48]

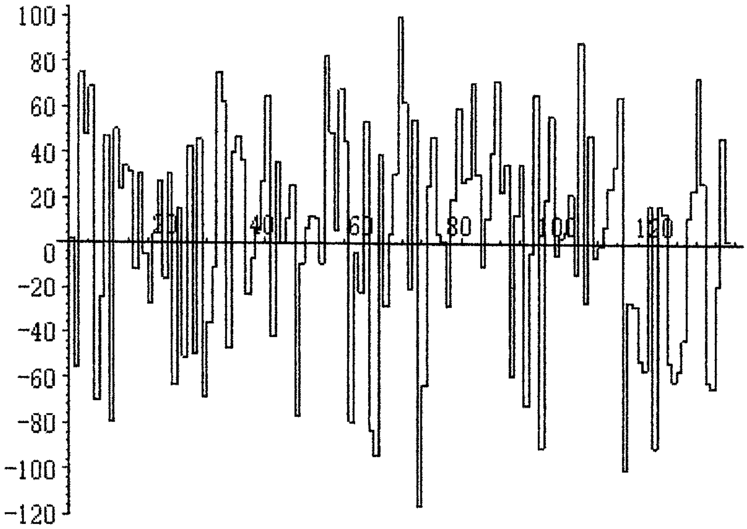
$$g(-x)\,[x]x^{135}-1 = 1/541\cdot$$

[2, -55, 75, 48, 69, -70, -25, 47, -79, 50, 24, 34, 32, -12, 31, -5, -27, 4, 27, -16,
31, -63, 15, -51, 43, -49, 46, -68, -36, -11, 75, 62, -47, 40, 47, 37, -23, -7, 6,

27, 65, -42, 36, 0, 11, 26, -77, -9, 7, 12, 11, -9, 83, 49, 6, 68, 45, -79, -4, -22,
54, -83, -94, 39, -28, 4, 31, 100, 62, -20, 55, -116, -63, 26, 47, 4, 1, -28, 20,
60, 27, 29, 71, 31, -10, 11, 40, 72, 23, 35, -59, 13, 35, -72, -4, 66, -90, 20,
56, -5, 3, 5, 22, -14, 89, -26, 48, -6, -1, 8, 25, 34, 65, -100, -26, -28, -52,
-56, 17, -90, 17, 14, -53, -61, -56, -43, 12, 24, 73, 27, -61, -64, -19, 47, 2]

wave form

$g(-x)$ [x] $x^{135}-1$, 135-sci for p = 541



Following are invariant graphs, invariant under the choice of primitive roots, of images under fFt of elops of p-1st root of 1, and conjectured to have uniform angular distribution.

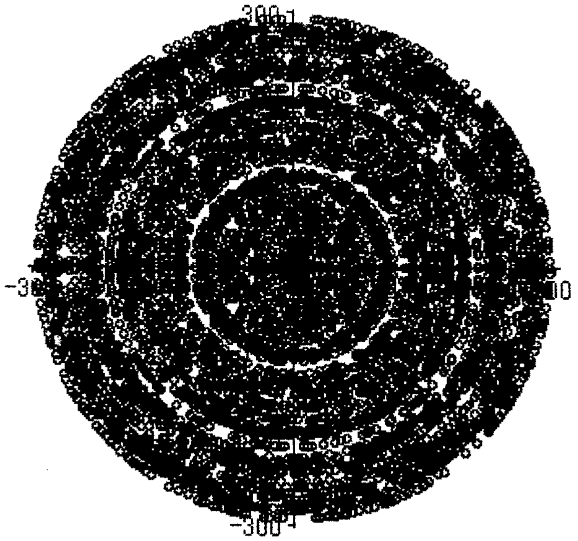
$y^2 = x^3+qx+r$, Weierstrass family

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

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

$a_{12}(x)$ [r] $(e^{2\pi ik/(p-1)})$

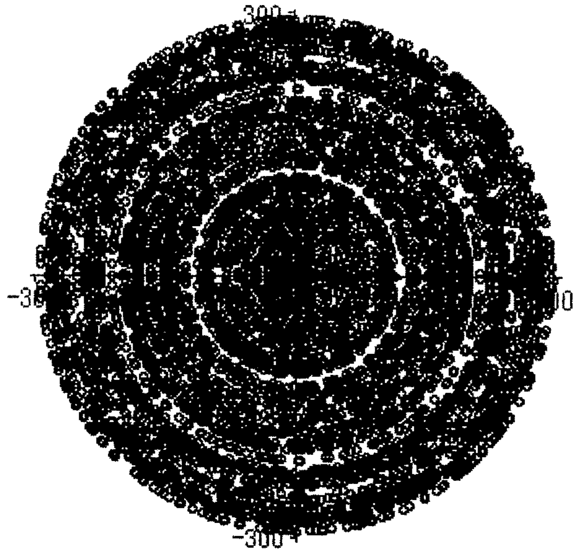
$k = 0 \sim p-1$, $p = 5 \sim 293$



$a_6(x) = F(1/6, 5/6, 1, x)$, $y^2 = x^3+qx^2+r$, Whock family

$a_6(x)\,[r]\,(e^{2\pi i k/(p-1)})$

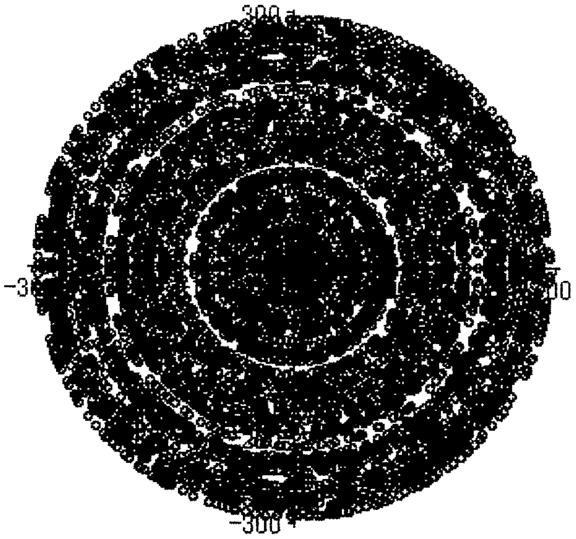
$k = 0 \sim p-1$, $p = 5\sim293$



$a_4(x) = F(1/4, 3/4, 1, x)$, $y^2 = x(x^2+qx+r)$, Euler family

$a_4(x)\,[r]\,(e^{2\pi i k/(p-1)})$

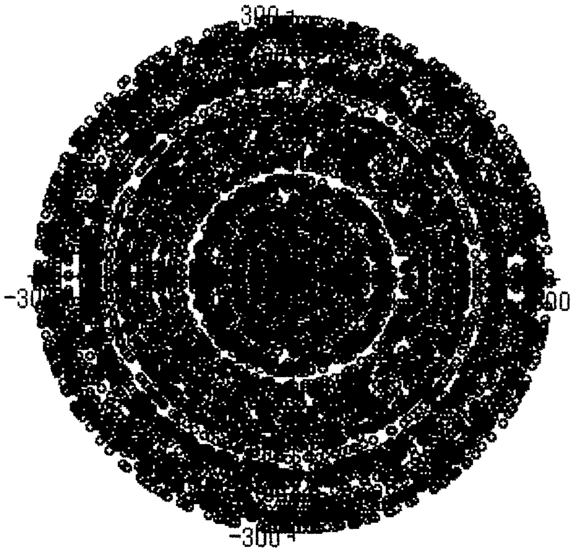
$k = 0 \sim p-1$, $p = 5\sim293$



$a_3(x) = F(1/3, 2/3, 1, x)$, $y^3+x^3+qxy+r = 0$, Hessian family

$a_3(x)\,[r]\,(e^{2\pi ik/(p-1)})$

$k = 0 \sim p\text{-}1$, $p = 5\sim293$



$a_2(x) = F(1/2, 1/2, 1, x)$, $y^2 = x(x\text{-}1)(x+q)$, Legendre family

$a_2(x)\,[r]\,(e^{2\pi ik/(p-1)})$

$k = 0 \sim p\text{-}1$, $p = 5\sim293$

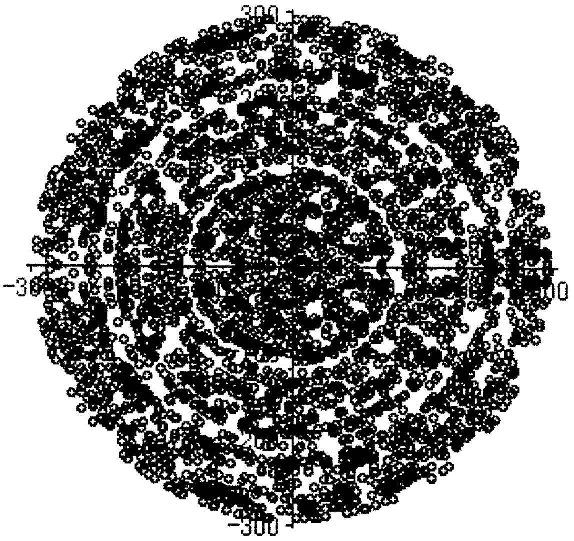


Image of Legendre case looks thinner, because fFt of Legendre elops all image points are double point except for roots of $x^{12}-1$.

Example 10. $p = 97$, $q = 5$,

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

$$x^{48}-24x^{47}+35x^{46}+27x^{45}+4x^{44}+11x^{43}+18x^{42}-31x^{41}+33x^{40}-2x^{39}-44x^{38}+4x^{37}+3x^{36}$$

$$-43x^{35}-2x^{34}-12x^{33}+2x^{32}+43x^{31}-47x^{30}+47x^{29}+4x^{28}-36x^{27}-43x^{26}+36x^{25}+33x^{24}$$

$$+36x^{23}-43x^{22}-36x^{21}+4x^{20}+47x^{19}-47x^{18}+43x^{17}+2x^{16}-12x^{15}-2x^{14}-43x^{13}+3x^{12}$$

$$+4x^{11}-44x^{10}-2x^{9}+33x^{8}-31x^{7}+18x^{6}+11x^{5}+4x^{4}+27x^{3}+35x^{2}-24x+1$$

$$F(1/2,1/2,1,x)\,[5]\,(x) =$$

$$14x^{95}+2x^{94}-10x^{93}+18x^{92}+2x^{91}-6x^{90}+2x^{89}+2x^{88}+18x^{87}-6x^{86}-10x^{85}-14x^{84}-6x^{83}-14x^{82}$$

$$+10x^{81}-14x^{80}-6x^{79}+10x^{78}+2x^{77}-14x^{76}+2x^{75}+2x^{74}-2x^{73}+2x^{72}+6x^{71}-14x^{70}+14x^{69}+2x^{68}$$

$$+14x^{67}+10x^{66}-2x^{65}+2x^{64}-14x^{63}+18x^{62}-18x^{61}-14x^{60}+10x^{59}+2x^{58}+10x^{57}+2x^{56}-10x^{55}$$

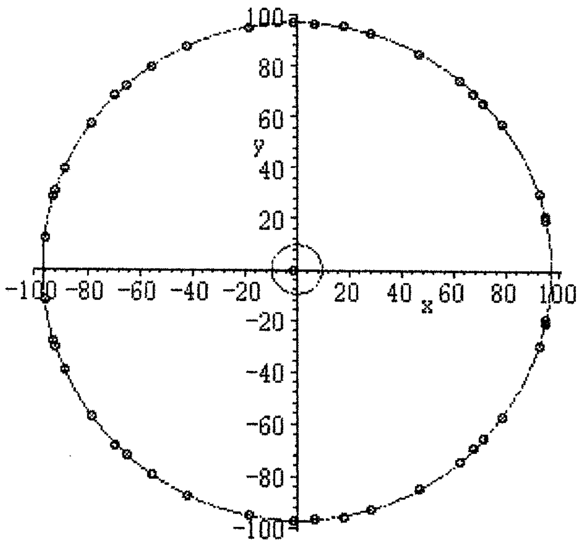
$$+2x^{54}+2x^{53}+2x^{52}+6x^{51}+10x^{50}+2x^{49}+18x^{48}-2x^{47}+10x^{46}-6x^{45}+2x^{44}-2x^{43}+2x^{42}+10x^{41}$$

$$+2x^{40}-10x^{39}+2x^{38}-10x^{37}-14x^{36}+18x^{35}+18x^{34}+14x^{33}+2x^{32}+2x^{31}+10x^{30}-14x^{29}+2x^{28}$$

$$-14x^{27}-14x^{26}-6x^{25}+2x^{24}+2x^{23}+2x^{22}-2x^{21}-14x^{20}-2x^{19}+10x^{18}+6x^{17}-14x^{16}-10x^{15}$$

$$-14x^{14}+6x^{13}-14x^{12}+10x^{11}-6x^{10}-18x^{9}+2x^{8}-2x^{7}-6x^{6}-2x^{5}+18x^{4}+10x^{3}+2x^{2}-14x+1$$

$$F(1/2,1/2,1,x)\,[5]\,(e^{2\pi ik/96}),\ k = 0 \sim 95$$



Cyclotomic factorization of characteristic polynomial for p is:

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

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

$$(x^8-x^4+1)\,(x^8+1)\,(x^{16}-x^8+1)\,(x^{16}+1)\,(x^{32}-x^{16}+1)$$

The resultant, for example, with a cyclotomic factor

$$h(z) = y^2+pzy+p^2 \textcircled{y}\ y-g(x) \textcircled{x}\ x^8-x^4+1$$

discribes, that the image $y = g(x)$ for a p-1st root of 1 have absolute value p, and resultant for y with $y^2+pzy+p^2$, z is a real number in interval $[-2,2]$.

For example,

$$y^2+pzy+p^2 \textcircled{y}\ y-F(1/2,1/2,1,x)\,[5]\,(x) \textcircled{x}\ x^8-x^4+1$$

From the figure $a_2(\pm 1) = -1$, no other component degenerates. Note that resultants are associative and distributive for multiplication, we list factors for components:

$$[x^2+x+1,\ (97z-2)^2],\ [x^2-x+1,\ (97z-2)^2],\ [x^2+1,\ (97z-130)^2],$$

these are the factors of $x^{12}-1 = 0$, for other factors exponents are no less than 4, meaning that the image is multiple point.

$$[x^4-x^2+1,\ (97z-130)^4],\ [x^4+1,\ (97z+94)^4],\ [x^8-x^4+1,\ (97z+190)^8],$$

$$[x^8+1,\ (9409z^2-6596z-23932)^4],$$

$$[x^{16}-x^8+1,\ (88529281z^4+226342904z^3-52765672z^2-328679456z-42485744)^4],$$

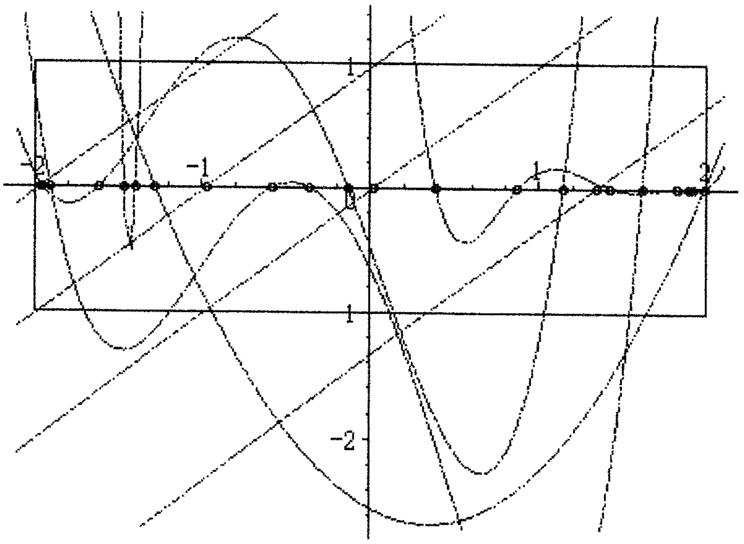
$$[x^{16}+1,\ (88529281z^4+109520760z^3-228601064z^2-251352608z-57504752)^4],$$

$$[x^{32}-x^{16}+1,(7837433594376961z^8-4266149420444366 4z^7+4700627618215332 8z^6$$

$$+1194989538624179 84z^5-2813481655560590 40z^4+5012728503046784 0z^3$$

$$+2859514588169848 32z^2-2358198397035489 28z+5045807286956876 8)^4]]$$

all roots are in $[-2,2]$



Example 10

$p = 97 = 1 \bmod 8,\ q = 5$

$$F(1/8,5/8,1,x) =$$
$$10x^{12}+67x^{11}+51x^{10}+x^{9}+82x^{8}+22x^{7}+65x^{6}+93x^{5}+63x^{4}+36x^{3}+32x^{2}+41x+1$$

and put

$$f(x) = x^{12}\cdot F(1/8,5/8,1,1-x) \text{ if } (x/p) = 1$$
$$7\sqrt{2}\cdot x^{12}\cdot F(1/8,5/8,1,1-x) \text{ if } (x/p) = -1$$

note that $2x^2 = 1$ in F_{97} is satisfied by $x = 7 = 1/\sqrt{2}$ in F_{97}, so $7\sqrt{2} = 7\cdot\sqrt{2}$ is a product of an element of finite field and a complex (in this case real) number which have a role of unit element. This kind of unit number which is a bridge of different kind of characteristics (or, character) would play very important role, especially in the representation of polynomial like F(1/8,5/8,1,x), and call them temporarily, *fin/comp-unit* (finite/complex-unit) or *disc/cont-unit* (discrete/continuous-unit) etc.

$$g(x) = f(x)\,[5]\,(x) =$$
$$x^{96}+12\sqrt{2}x^{95}+6x^{94}+6\sqrt{2x}^{93}-2x^{92}+7\sqrt{2x}^{91}-10x^{90}+3\sqrt{2x}^{89}-14x^{88}-11\sqrt{2x}^{87}-6x^{86}+6\sqrt{2x}^{85}$$
$$-10x^{84}+\sqrt{2}x^{83}+4x^{82}-5\sqrt{2x}^{81}-12x^{80}-3\sqrt{2x}^{79}-18x^{78}+13\sqrt{2x}^{77}-10x^{76}+7\sqrt{2x}^{75}+10x^{74}-8\sqrt{2x}^{73}$$
$$+2x^{72}+6\sqrt{2}x^{71}-12x^{70}-4\sqrt{2x}^{69}-14x^{68}-6x^{66}-2x^{64}-9\sqrt{2x}^{63}-4x^{62}-8\sqrt{2x}^{61}+8x^{60}-9\sqrt{2x}^{59}-16x^{58}$$
$$-5\sqrt{2}x^{57}-6x^{56}+2\sqrt{2x}^{55}-16x^{54}-3\sqrt{2x}^{53}-2x^{52}+10\sqrt{2x}^{51}+2x^{50}+11\sqrt{2x}^{49}+8x^{48}+14x^{46}+9\sqrt{2x}^{45}$$
$$-2x^{44}-12\sqrt{2}x^{43}-14x^{42}+3\sqrt{2x}^{41}+10x^{40}-2\sqrt{2x}^{39}+2x^{38}+10\sqrt{2x}^{37}-8x^{36}+\sqrt{2x}^{35}-2x^{34}+14x^{32}$$
$$-5\sqrt{2}x^{31}+6x^{30}-7\sqrt{2x}^{29}-2x^{28}+3\sqrt{2x}^{27}-18x^{26}-3\sqrt{2x}^{25}+10x^{24}+3\sqrt{2x}^{23}-8x^{22}-4\sqrt{2x}^{21}-14x^{20}$$
$$+4\sqrt{2}x^{19}+10x^{18}+10\sqrt{2x}^{17}-12x^{16}-6\sqrt{2x}^{15}+14x^{14}-10\sqrt{2x}^{13}+2x^{12}+7\sqrt{2x}^{11}+18x^{10}-12\sqrt{2x}^{9}$$
$$+2x^{8}-2x^{6}+4\sqrt{2}x^{5}+2x^{4}-9\sqrt{2x}^{3}-3\sqrt{2x}+1$$

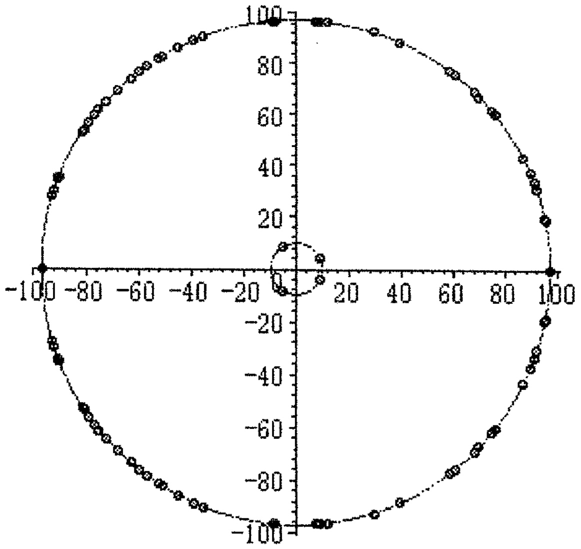
note that coefficients are in Hasse's range $\sqrt{p}[-2,2]$. Image of p-1st root of 1 is figured below, it satisfy p-circle property:

$$f(x) = x^{12} \cdot F(1/8, 5/8, 1, 1-x), \ (x/p) = 1$$

$$7\sqrt{2} \cdot x^{12} \cdot F(1/8, 5/8, 1, 1-x), \ (x/p) = -1$$

$$g(x) = f(x)\,[5]\,(x)$$

$$g(x) - 1, \quad x = \exp(2\pi ik/(p-1)) = e^{2\pi ik/(p-1)}, \ k \in p-1$$



p-circle property is proved logically by the fact, real coefficient polynomial

$$h(z) = y^2 + pzy + p^2 \ \textcircled{y} \ y - (g(x) - 1)\,(x) \ \textcircled{x} \ x^{p-1} - 1$$

all the roots are real, by approximation of sufficient accuracy or by Sturm's method.

p = 101 = 5 mod 8, q = 2

$$F(1/8, 5/8, 1, x) =$$

$$1 + 49x + 22x^2 + 21x^3 + 27x^4 + 29x^5 - 4x^6 + 3x^7 - 50x^8 + 45x^9 - 18x^{10} + 46x^{11} + 11x^{12}$$

$$a(x) = F(1/8, 5/8, 1, 1-x) =$$

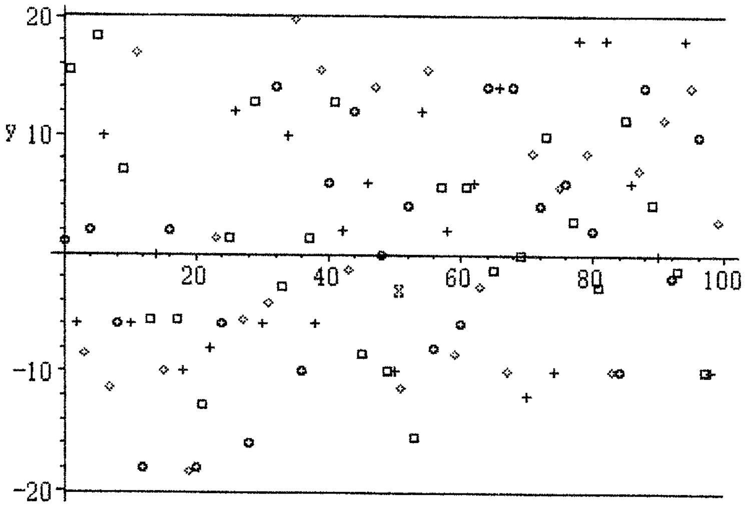
$$-20 + 40x - 26x^2 + 18x^3 + 42x^4 + 15x^5 + 36x^6 - 28x^7 - 45x^8 + 33x^9 + 2x^{10} + 24x^{11} + 11x^{12}$$

Of course, the coefficients of $a(x)\,[2]\,(x)$ do not satisfy Hasse's condition, so define , for $x = q^n$ and index n, we separate in cases:

$$b(x) = a(x) \ \text{ if } n = 0 \bmod 4, \ 45\sqrt{2} \cdot a(x) \ \text{ if } n = 1 \bmod 4$$

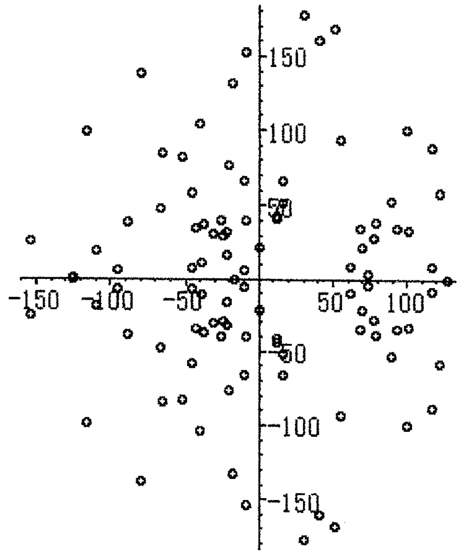
$$5 \cdot 2 \cdot a(x) \ \text{ if } n = 2 \bmod 4, \ 46\sqrt{2} \cdot a(x) \ \text{ if } n = 3 \bmod 4$$

then, the coefficients satisfy Hasse's condition



but, the image of p-1st root of 1 is not on the p-circle:

$$b(x)\,[q]\,(e^{2\pi/k/100}),\ k = 0\sim 99$$



but, coefficient replaced by fin/comp-unit version

$$c(x) =$$

$$a(q^n)\ \text{ if } n = 0 \bmod 4,\ 45(1+i)\cdot a(q^n)\ \text{ if } n = 1 \bmod 4$$

$$5\cdot 2i\cdot a(q^n)\ \text{ if } n = 2 \bmod 4,\ 46(-1+i)\cdot a(q^n)\ \text{ if } n = 3 \bmod 4$$

then we have

$$b(x)\,[2]\,(x) =$$

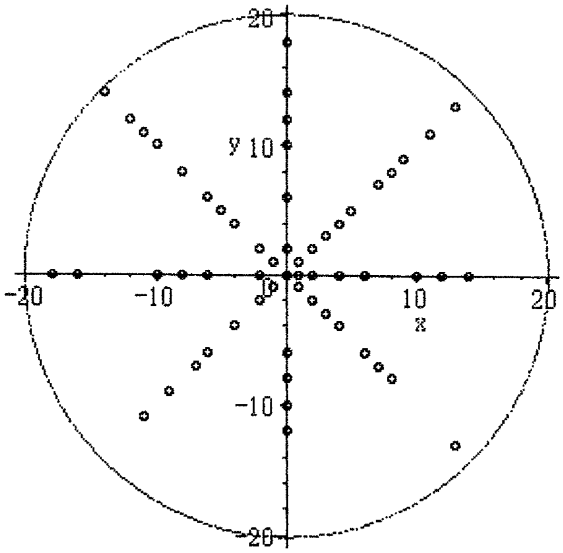
[1, 11+11i, -6i, 6-6i, 2, 13+13i, 10i, 8-8i, -6, 5+5i, -6i, -12+12i, -18, -4-4i, 0, 7-7i, 2, -4-4i, -10i,13-13i, -18, -9-9i, -8i, -1+i, -6, 1+i, 12i, 4-4i, -16, 9+9i, -6i, 3-3i, 14, -2-2i, 10i, -14+14i, -10, 1+i,-6i, -11+11i, 6, 9+9i,

2*i*, 1-*i*, 12, -6-6*i*, 6*i*, -10+10*i*, 0, -7-7*i*, -10*i*, 8-8*i*, 4, -11-11*i*, 12*i*, -11+11*i*,
-8,4+4*i*, 2*i*, 6-6*i*, -6, 4+4*i*, 6*i*, 2-2*i*, 14, -1-*i*, 14*i*, 7-7*i*, 14, 0, -12*i*, -6+6*i*, 4,
7+7*i*, -10*i*, -4+4*i*, 6, 2+2*i*,18*i*, -6+6*i*, 2, -2-2*i*, 18*i*, 7-7*i*, -10, 8+8*i*, 6*i*,
-5+5*i*, 14, 3+3*i*, 0, -8+8*i*, -2, -1-*i*, 18*i*, -10+10*i*, 10,-7-7*i*, -10*i*, -2+2*i*]

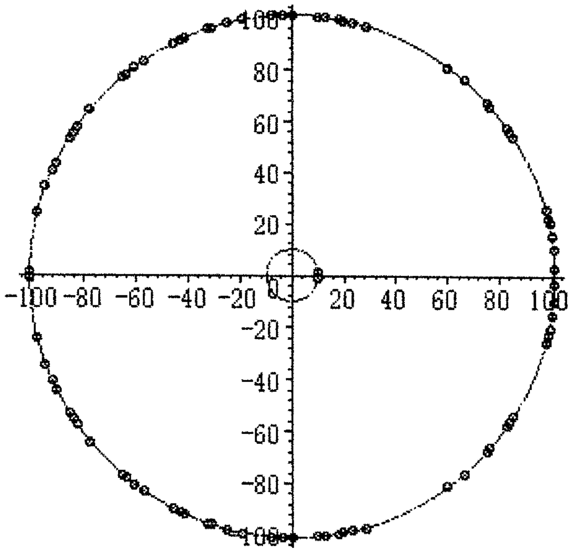
and the Gaussian integer coefficients are in the complex

$$2\sqrt{p} = 2\sqrt{101} =20.09975124$$

radius Hasse's complex circle:



c (x) [2] ($e^{2\pi ik/100}$), k = 0~99



These are only a partial fractional results and the research for special polynomials such as Fuchs polynomials like

F (1/5,4/5,1,x), F (1/8,3/8,1,x), F (1/10,3/10,1,x), etc and also of Jacobi polynomials are of the special interest.

References

[1] Kanji Namba, Hyper-elliptic curves over finite fields and Tschebysheff-shift, Reports of Institute for Mathematics and Computer Science 36, Reports of 25th Symp. on the Hist. of Math. (2014), Tsuda College, 2015, pp.237-282

[2] Kanji Namba, Finite Fourier transform and Legendre polynomial, Report of 2015 Applied Mathematics Symposium, Ryukoku Univ. Seta, pp. 38-43

[3] Kanji Namba, *Mathematics and Logic,* (Japanese), Asakura lecture series(mathematical methods) 23, 2011

[4] Richard K. Gui, Unsolved Problems in Number Theory, 3rd ed. Springer, 2004, (translation by Shigeru Kanemitsu: *Dictionary of Unsolved Problems in Number Theory*), Asakura, 2010