有理関数の合成代数と虚数乗法

弘前大学教育学部数学教室

難波　完爾

knamba@cc.hirosaki-u.ac.jp

第 14 回　数学史シンポジウム

2003 年 10 月 25 日(土)、26 日(日)

津田塾大学 5 号館(AV センター棟)5206 教室

1. 有理関数の合成代数

ここでの課題の一つの中心は、有理関数の合成(composition)による代数である。

合成可換(compositionally commutative)な関数の自明な例は、その冪の全体の成す族

$$f^{\omega}=\{f^{n}(x) : n\in\omega\}$$

や、x の冪 x^n の一次変換による引き戻し(pull-back)

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

で生成される族

$$f(x)\Rightarrow x^{Z}=\{f(x)\Rightarrow x^{n} : n\in Z\}$$

などがある。これらは、例えば Tchebycheff の多項式や、正接(tangent)の加法公式

$$i(x+1)/(x-1)\Rightarrow x^{5}=i(x+1)/(x-1)\bullet(x+i)^{5}/(x-i)^{5}=x(x^{4}-10x^{2}+5)/(5x^{4}-10x^{2}+1)$$

などとして親しまれているものである。

ここでは、楕円関数と虚数乗法に関係した有理関数の合成可換代数(compositionally commutative algebra)についての断片について述べる。

一般に与えられた有理関数の合成素因数分解(compositional factorization)や合成冪乗根(compositional n-th root)を計算することは容易ではない。

例えば、絶対不変式 J(τ)の合成素因数分解では

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

のようである。

これは楕円関数の Legenndre family から Weierstrass family

$$L: y^{2}=x(x-1)(x-a)\qquad W: y^{2}=x^{3}+ax+b\quad j=-27b^{2}/4a^{3}$$

の変換が、Euler family と

$$E: y^{2}=x(x^{2}+ax+1)\qquad N: y^{2}=x^{3}+ax^{2}+b\quad j=-27b^{2}/a^{3}$$

のどちらを経由して成されるかに対応している。

また、例えば、楕円曲線 C: $y^2 = x(x^2+1)$ には 25 次 5 倍等式

$$[5](x)=\frac{x(x^{12}-50x^{10}-125x^{8}-300x^{6}-105x^{4}+62x^{2}+5)^{2}}{(5x^{12}+62x^{10}-105x^{8}-300x^{6}-125x^{4}-50x^{2}+1)^{2}}$$

の 5 次の交換可能な有理共役合成素因数分解(conjugate compositional factorization)

$$\frac{x(x^{2}+1-2i)^{2}}{(1-2i+x^{2})^{2}}\bullet\frac{x(x^{2}+1+2i)^{2}}{(1+2i+x^{2})^{2}}=\frac{x(x^{2}+1+2i)^{2}}{(1-2i+x^{2})^{2}}\bullet\frac{x(x^{2}+1-2i)^{2}}{(1+2i+x^{2})^{2}}$$

が存在する。このような合成平方根(compositional square root)などの存在条件について述べてみようと思う。

このような、有理共役合成素因数分解と交換可能族については、次のような例が知られている。楕円曲線の族としては、n倍射のx座標の関数

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

はn^2次の有理関数であり、その合成平方根

$$[\sqrt{n}](x) = \sqrt{x_n}(x)$$

が有理関数として存在する場合は n 次の有理関数である。この存在条件が Hilbert-Weber の類多項式(class polynomial)= 0、つまり類方程式として与えられる。

$$E:\ \ y^2 = x(x^2+ax+1) \qquad \bar{a} = a$$

$$[n](n) = x_n(x) = u(\bar{u}(x)) = \bar{u}(u(x))$$

1.1　n = 2m+1 の場合

$$u(x) = \frac{-x(x^m+a_1x^{m-1}+\cdots+(ki\pm\sqrt{n-k^2}))^2}{((ki\pm\sqrt{n-k^2})x^m+\cdots+a_1x+1)^2}$$

$$\bar{u}(x) = \frac{-x(x^m+\bar{a}_1x^{m-1}+\cdots+(-ki\pm\sqrt{n-k^2}))^2}{((-ki\pm\sqrt{n-k^2})x^m+\cdots+\bar{a}_1x+1)^2}$$

1.2　n = 2(2m+1)の場合

$$u(x) = \frac{-(x^2+ax+1)(x^m+b_1x^{m-1}+b_2x^{m-2}+\cdots b_2x^2+b_1x+1)^2}{x((ki\pm\sqrt{n-k^2})x^m+c_1x^{m-1}+c_2x^{m-2}+\cdots c_2x^2+c_1x+(ki\pm\sqrt{n-k^2}))^2}$$

$$\bar{u}(x) = \frac{-(x^2+ax+1)(x^m+\bar{b}_1x^{m-1}+\bar{b}_2x^{m-2}+\cdots \bar{b}_2x^2+\bar{b}_1x+1)^2}{x((-ki\pm\sqrt{n-k^2})x^m+\bar{c}_1x^{m-1}+\bar{c}_2x^{m-2}+\cdots \bar{c}_2x^2+\bar{c}_1x+(-ki\pm\sqrt{n-k^2}))^2}$$

1.3　n = 4m の場合

$$u(x) = \frac{-(x^{2m}+b_1x^{2m-1}+b_2x^{2m-2}+\cdots b_2x^2+b_1x+1)^2}{x(x^2+ax+1)((ki\pm\sqrt{n-k^2})x^{2m-2}+c_1x^{2m-3}+c_2x^{2m-4}+\cdots c_2x^2+c_1x+(ki\pm\sqrt{n-k^2})^2}$$

$$\bar{u}(x) = \frac{-(x^{2m}+\bar{b}_1x^{2m-1}+\bar{b}_2x^{2m-2}+\cdots \bar{b}_2x^2+\bar{b}_1x+1)^2}{x(x^2+ax+1)((-ki\pm\sqrt{n-k^2})x^{2m-2}+\bar{c}_1x^{2m-3}+\bar{c}_2x^{2m-4}+\cdots \bar{c}_2x^2+\bar{c}_1x+(-ki\pm\sqrt{n-k^2})^2}$$

の形の有理式で与えられることが知られている。また、係数は Hilbert-Weber 多項式= 0 の解の分解体の元である。

特に、k = 0 が合成平方根に相当する。このような、合成可換な有理関数族は、将来、有限体が物理学の諸現象の記述の標準的言語になった場合に、例えば、水素原子のスペクトル線の Balmer series などと関連していることが判明するかも知れない。私自身の興味としては物理学で登場する平均的な素数がどの程度の数か非常に興味がある。

例として述べてきたことであるが、理科年表 2003 によると、平均的恒星である太陽の質量と、陽子の質量(中性子も似た質量)は

$$s = 1.9891\times10^{30}\text{kg},\quad p = 1.67262\times10^{-27}\text{kg}$$

であり、その相乗平均は

$$\sqrt{sp} = 57.680\text{kg}$$

で日本人の青年の平均体重(≒犬猫牛馬等の動物の平均のあたりの重さ)である。

また、その比、これは数の次元であるが、は

$$s/p = 1.18921\times10^{58}$$

である。その6乗根、つまり平方根と立方根の比

$$(s/p)^{1/6} = \sqrt{s/p} \,/\, \sqrt[3]{s/p} = 3.2703\times10^9$$

のあたりに、人に関する基本的数、

世界人口 6.2×10^9 、人の脳細胞数 $15{\sim}20\times10^9$ 、人ゲノムサイズ 3.3×10^9

が分布してる。これから感ずることは、所謂、エルゴード性(ergodic, ergo=érgon 仕事 work)である。人という種がこの状態に止まる(止まり得る)時間のことである。固有性と多様性の調和点として、この点が選ばれたのではないかと思う。文明が発展した社会のみこのような仮説を提出できるので、任意の生命圏について成立することを主張している訳ではない。

私は、基本的な粒子についても、s/pのような平凡な数の簡単な分数べき、例えば

$$\sqrt{s/p} = 1.09050\times10^{29}\text{、}\sqrt[3]{s/p} = 2.28254\times10^{19}\text{、}\sqrt[6]{s/p} = 3.2703\times10^9$$

のどれかのようなオーダーの素数や整数の離散的量の平均的ふるまいとして物理現象の記述がなされる、あるいは試みられることも十分可能性があることだと思っている。

情報処理の機構(生命圏、人体、計算機など)については、最適解は

個々の機構の大きさが空間の平方根、そのプログラムの大きさが立方根

であるというのが私の仮説である。

2. 楕円曲線族と有限体

有限体上の楕円曲線

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

の Poincaré-Mordell 群の位数は、標数0の場合の楕円積分

$$\int 1/\sqrt{f(x)}\ dx$$

に対応して、Legendre 記号、つまり mod.p での

$$(f(x)/p) = f(x)^{(p-1)/2} = 1/\sqrt{f(x)}$$

の和

$$a_p = \Sigma(f(x)/p) = \Sigma\ 1/\sqrt{f(x)}$$

を用いて、Hasse の不等式を満たす式

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

で与えられることが知られている。

勿論、値は絶対値最小剰余(least absolute value residue)として計算する。$p< 17$ では直接計算する必要がある。

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

compute least absolute value

p	[p/6]	(p±1)/4	$P_{[p/6]}(x)$	$a_{12}(z)\ \ z = x^2$
3	0	1	1	z
5	0	1	1	z
7	1	2	x	z^2
11	1	3	x	z^3
13	2	3	$(3x^2-1)/2$	$z^3(3z-1)/2$

17	2	4	$(3x^2-1)/2$	$z^4(3z-1)/2$
19	3	5	$x(5x^2-3)/2$	$z^5(5z-3)/2$
23	3	6	$x(5x^2-3)/2$	$z^6(5z-3)/2$
29	4	7	$(35x^4-30x^2+3)/8$	$z^7(35z^2-30z+3)/8$
31	5	8	$x(63x^4-70x^2+15)/8$	$z^8(63z^2-70z+15)/8$
37	6	9	$(231x^6-315x^4+105x^2-5)/16$	$z^9(231z^3-315z2+105z-5)/16$

のようである。この関数、擬多項式の mod.p での最小剰余を計算するのである。
以下、楕円曲線の族と対応する Fuchs 関数の表を与えておく。

	name of fammily	multiplier	parameter	degree
$y^2 = x(x-1)(x-q)$	Legendre family		$z = q$	$d = [p/2]$
$a_2(z) =$	$F(1/2,1/2,1,z)$	1		
$y^2 = x^3+(3qx+4)^2$	Hessian family		$z = 1/q^3$	$d = [p/3]$
$a_3(z) =$	$F(1/3,2/3,1,z)$	1		
$y^2 = x(x^2+px+q)$	Euler family		$z = 4p/q^3$	$d = [p/4]$
$a_4(z) =$	$F(1/4,3/4,1,z)$	1		
$y^2 = x^3 +px^2+q$			$z = -27p/q^3$	$d = [p/6]$
$a_6(z) =$	$F(1/6,5/6,1,z)$	1		
$y^2 = ?$	(2-fold) Euler family			$d= [p/8]$
$p = 8n+1,\ a_8(z) =$	$F(1/8,5/8,1,1-z)$	z^{3n}	z	$(z/p)=1$
		$z^{3n}/\sqrt{-2}$		$(z/p) = -1$
$p = 8n+3,\ a_8(z) =$	$F(3/8,7/8,1,1-z)$	z^{3n+1}		$(z/p)=1$
		$z^{3n+1}/\sqrt{-2}$		$(z/p) = -1$
$p = 8n+5,\ a_8(z) =$	$F(1/8,5/8,1,1-z)$	1		$\langle z/p\rangle = z^{2n+1} =1$
		$\sqrt{-1}$		$\langle z/p\rangle = -1$
		$\sqrt{\langle z/p\rangle /2}$		$(z/p) = -1$
$p = 8n+7,\ a_8(z) =$	$F(3/8,7/8,1,1-z)$	z^n		$(z/p) = 1$
		$z^n/\sqrt{2}$		$(z/p) = -1$
$y^2 = x^3 +px+q$	Weierstrass family			
$p = 4n+1,\ a_{12}(z) =$	$F(1/12,5/12,1,1-z)$	z^n	$z= -27p^2/q^3$	$d = [p/12]$
$p = 4n-1$	$F(7/12,11/12,1,1-z)$	z^n		
?				
$p = 6n+1,\ a_{6'}(z) =$	$F(1/6,1/3,1,x)$			
$p = 6n-1,\ a_{6'}(z) =$	$F(5/6,2/3,1,x)$			
$p = 6n+1,\ a_{6''}(z) =$	$F(1/6,1/2,2/3,x)$			
$p = 6n-1,\ a_{6''}(z) =$	$F(5/6,1/5,1/3,x)$			

これらの関数はガウスの微分方程式の解としての Fuchs の関数として計算できる。
標数(characteristic number)が正のとき、つまり有限体 F_p = GF(p) では、p に関係するが、

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

のようにd ＝ [p/12]次の多項式になっている。この様に、素数を固定する毎に、(素数に関連した次数の)多項式となるという意味で擬多項式(pseudo-polynomial)と呼んでいる。勿論、標数(characteristic number) 0 の体のなかでは無限級数である。

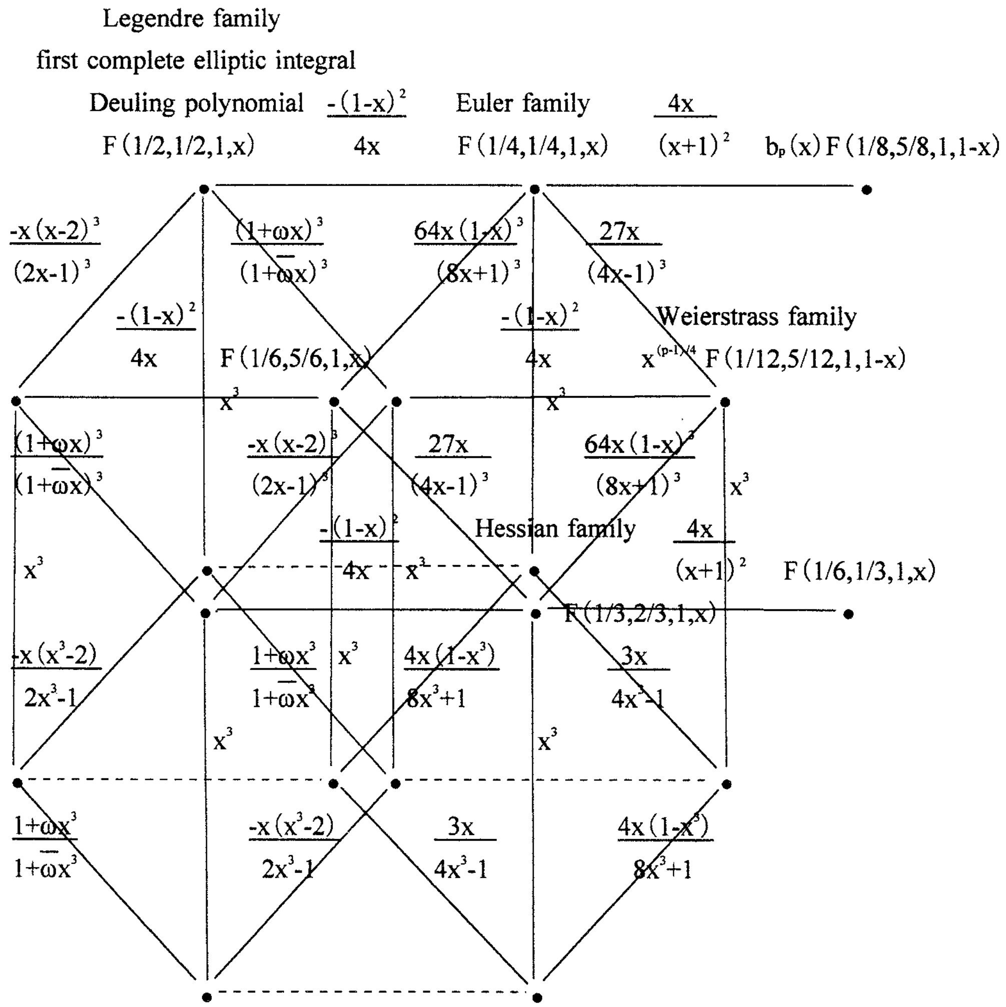
次の有理交換図式(commutative diagram of rational functions)は、二つの楕円曲線

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

を結ぶもので、モノドロミー群の生成元が有理関数の合成で表現される場合の一つである。実体としては、対称群 S_4 ＝ 4!の組成列を表現したもので、その群が可解(solvable group)であることを表現したものとも、楕円曲線

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

の2倍射(duplication map)と3倍射の合成平方根(compositional square root)が交換可能という式を表現したものとも考えられる。



$$[2](x)=x(1-8x^3)/4(x^3+1)=x(x+4)/4(x+1)\bullet x(x-2)/(x+1),\ [\sqrt{3}](x)=-(x^3+4)/3x^2$$

$$[3](x)=(x^9-96x^6+48x^3+63)/9x^2(x^3+4)=-(x^3+4)/3x^2\bullet-(x^3+4)/3x^2$$

$$-1/x^3 \Rightarrow -(x^3+4)/3x^2=27x/(4x-1)^3,\ -1/x^3 \Rightarrow x(1-8x^3)/4(x^3+1)=64x(1-x)^3/(8x+1)^3$$

点線の部分の有理関数は存在するのであろうか。

3. 超楕円曲線と Sato-$\sin^2$-conjecture の拡張の試み

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

の場合、虚数乗法をもたなければ、この曲線に付随する可換群の位数は $z = -27b^3/4c^2$

$$n_p = 1+a_p+p$$

$$a_p = \Sigma x \in p \ (f(x)/p) = \begin{cases} x^{(p-1)/4}\ F(1/12,5/12,1,1-z) \\ x^{(p+1)/4}\ F(7/12,11/12,1,1-z) \end{cases}$$

と表現され、

$$x^2+a_px+1 = 0$$

の複素数解

$$x = \sqrt{p}\ (\cos\theta_p + i\sin\theta_p)$$

の偏角 θ_p の分布が $\sin^2\theta$ に比例するであろうというのが予想である。

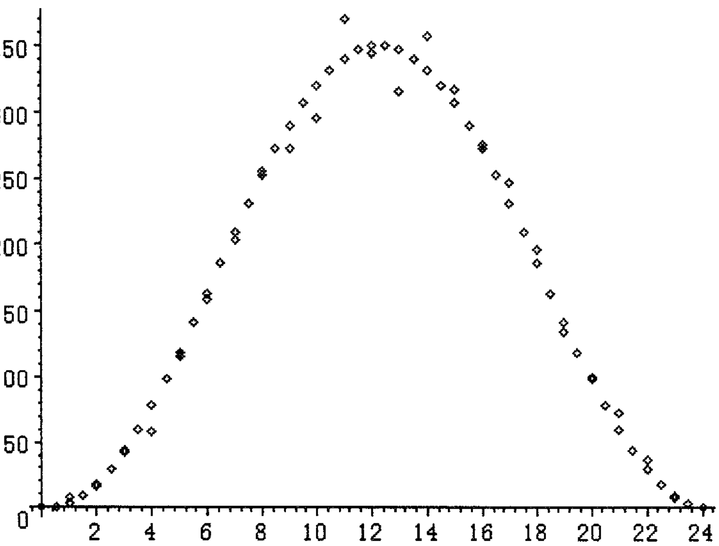
例えば、次の表(7.5° mesh) は楕円曲線

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

について、$p = 3$ から 39989 までの 4204 個の素数について

$x^2+a_px+1 = 0$

の 8408 個の複素数解の偏角をグラフにしたものである。$\sin^2$ -予想の意味をかなり良く表現していると思う。 90° の近くに $\sqrt{n}$ のオーダーのばらつきが見られるが、恐らく Gibbs phenomena であろう。これはガウス整数とアイゼンスタイン整数としての退化(Gaussean and Eisenstein's integers, $p \neq -1$ mod.12)のためと考えられる。



$$a_{12}(z) = \Sigma x \in p(f(x)/p) = z^{[p/4]}P_{[p/6]}(\sqrt{z}), \quad z = -27b^2/a^3$$

これは、$a_p/2\sqrt{p}$ の分布が、

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

に比例すると云っても良いし、或いは、Hamilton の quaternion H の単位球、つまり 3 次元単位球面

$$S^3 = \{a+bi+cj+dk \in H: a^2+b^2+c^2+d^2=1\}$$

上の一様分布の実軸への射影の分布ということもできる。また、帯球関数、つまり Legendre の多項式 $P_n(x)$ を用いて

$$a_p = x^{\pm 1/4} P_{[p/6]}(\sqrt{x})$$

とも記すことができることも知られているので、3 次元空間の[p/12]次の斉次調和関数とも考えられる。計算は絶対値最小剰余である。p ≥ 17 なら一意に定まるが、17 よりも小さい数に於いても mod.p では一致している。

関数 $a_p(x)$ については、有限素体の乗法群

$$F_p^* = p-1 = \{1,2,\cdots,p-1\}$$

での表現行列、つまり、i 行 j 列の元を $a_p(ij)$ とした行列

$$A = (a_{12}(ij))$$

の固有多項式が 0,2,4 個の $\pm\sqrt{p}$ の固有空間(Gaussean and Eisenstein's integers, $p \neq -1$ mod.12)を除いて $\pm p$ の固有空間になることが予想(既に証明されている？)されている。

$$a_{12}(z) = \Sigma x \in p(f(x)/p) = z^{[p/4]} P_{[p/6]}(\sqrt{z}), \quad z = -27b^2/a^3$$

table of characteristic polynomials

$$A = (a_{12}(ij)) \approx (a_{12}(b^{i+j}))$$

(b: prim. root mod. p)

p = 5	5	$1/5\cdot(5x^2-1)$	$(x-1)(x+1)$
7	-5	$1/7\cdot(7x^2-1)$ $1/7\cdot(7x^2-1)$	$(x-1)^3(x+1)$ $(x-1)^2(x+1)^2$
11	-1	1	$(x-1)^6(x+1)^4$ $(x-1)^5(x+1)^5$
13	1	$1/13^2\cdot(13x^2-1)^2$	$(x-1)^5(x+1)^3$
17	5	$1/17\cdot(17x^2-1)$	$(x-1)^7(x+1)^7$
19	-5	$1/19\cdot(19x^2-1)$	$(x-1)^8(x+1)^8$
23	-1	1	$(x-1)^{10}(x+1)^{12}$
29	5	$1/29\cdot(29x^2-1)$	$(x-1)^{13}(x+1)^{13}$
31	-5	$1/31\cdot(31x^2-1)$	$(x-1)^{14}(x+1)^{14}$
37	1	$1/37^2\cdot(37x^2-1)^2$	$(x-1)^{17}(x+1)^{15}$
41	5	$1/41\cdot(41x^2-1)$	$(x-1)^{20}(x+1)^{18}$
43	-5	$1/43\cdot(43x^2-1)$	$(x-1)^{20}(x+1)^{20}$
47	-1	1	$(x-1)^{22}(x+1)^{24}$
53	5	$1/53\cdot(53x^2-1)$	$(x-1)^{25}(x+1)^{25}$
59	-1	1	$(x-1)^{30}(x+1)^{28}$
61	1	$1/61^2\cdot(61x^2-1)^2$	$(x-1)^{29}(x+1)^{27}$
67	-5	$1/67\cdot(67x^2-1)$	$(x-1)^{32}(x+1)^{32}$
71	-1	1	$(x-1)^{34}(x+1)^{36}$

兎も角、p = -1 からは p-1 次の成分が $2\sqrt{p}$ 以下の絶対値の整数で分母 p の p-1 次巡回直交行列が常に存在する。この行列は通信や位置測定、探査等に応用が可能であると思う。

3.1 超楕円曲線と佐藤 $\sin^2$- conjecture

ここで述べようと考えていることは、一つの例であるが、

$$C: y^5 = x^5+5x+5 = f(x)$$

についてである。

f(x) と g(x) の x に関する終結式(resultant)を

$$f(x) \otimes g(x) = \mathrm{res}(f(x),g(x),x)$$

のように略記する。そして、

$$f(u) = f(x) \otimes x-u$$

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

などを考える。$(x/p) = x^{(p-1)/2}$ を Legendre symbol として、それらの和

$$a_p = \Sigma x \in p\,(f(x)/p)$$

$$b_p = \Sigma x,y \in p\,(f(x,y)/p)$$

に対し、4 次多項式

$$x^4+a_px^3+b_px^2+a_ppx+p^2 = (x^2+c_px+p)\,(x^2+d_px+p)$$

を考えると、4 個の絶対値 $\sqrt{p}$ の実数でない解をもつことが証明されている。

これに関しては、例えば、$x^5+5x+5 = f(x)$ の場合、狭義の Hasse の不等式は

$$|\,a_p\,| \leq 3\sqrt{p}$$

で、例外的な場合、例えば p = 4463, 7583 などを除いて成立している。勿論、この場合も

$$|\,a_p\,| \leq 4\sqrt{p}$$

が成立している。

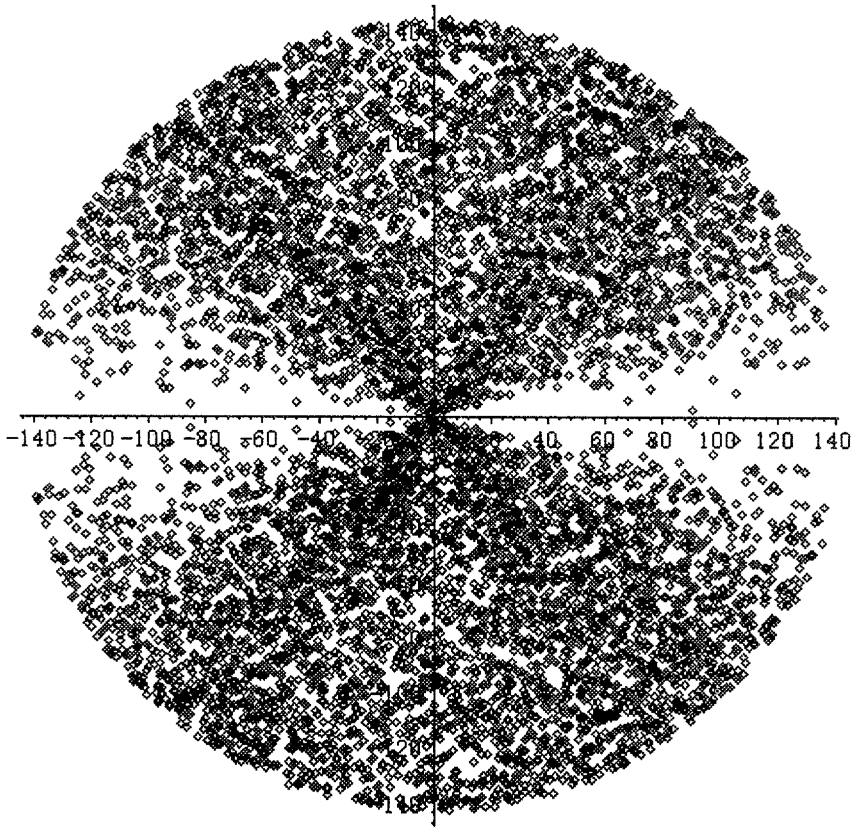
この例について、p = 3 ~ 20509 までの 2314 個の場合の統計を取ってみた。計算のプログラムは Maple 5 のものである。

```
c:=[]:k:={}:
for p from 3 to 20000 do: if isprime(p)=true then t:=[]:
for n from 0 to p-1 do: a:=n^((p-1)/2) mod p: if a>(p-1)/2 then a:=a-p fi: t:=[op(t),a]: od:
f:=x->x^5+5*x+5;
g:=(u,v)->v^5+10*v^3+(-20*u^2-25*u)*v^2+(5*u^4+25*u^3+25)*v+25-5*u^5-25*u;
a:=0: for n from 0 to p-1 do: a:=a+t[(f(n) mod p)+1]: od:
b:=0: for n from 0 to p-1 do:
e4:=240:e3:=210:e2:=(90-40*n^2-50*n) mod p:
e1:=(36-20*n^2-25*n+5*n^4+25*n^3) mod p:e0 :=(25-5*n^5-25*n) mod p:
for m from 0 to p-1 do: e0:=e0+e1:e1:=e1+e2:e2:=e2+e3:e3:=e3+e4:e4:=e4+120:
b:=b+t[(e0 mod p)+1]:od: od:
d:=evalf((a+sqrt(a^2-4*b+8*p))/(2*sqrt(p))):e:=evalf((a-sqrt(a^2-4*b+8*p))/(2*sqrt(p))):
print(p,a,b,b-2*p,d,e); c:=[op(c),[p,a,b]]:> k:={op(k),d,e}: fi:od: print(c,k);
```

このプログラムは良く練られたものでは決してないし美しいものでもない。所謂、人にお見せできるものではないのであるが。kernel の部分

```
e0:=e0+e1:e1:=e1+e2:e2:=e2+e3:e3:=e3+e4:e4:=e4+120
```

は同時に複数の adder で実行できる形であるから、並列計算可能である。本格的に計算を試みれば現在の計算機では 100000 程度の p までは計算可能であろう。



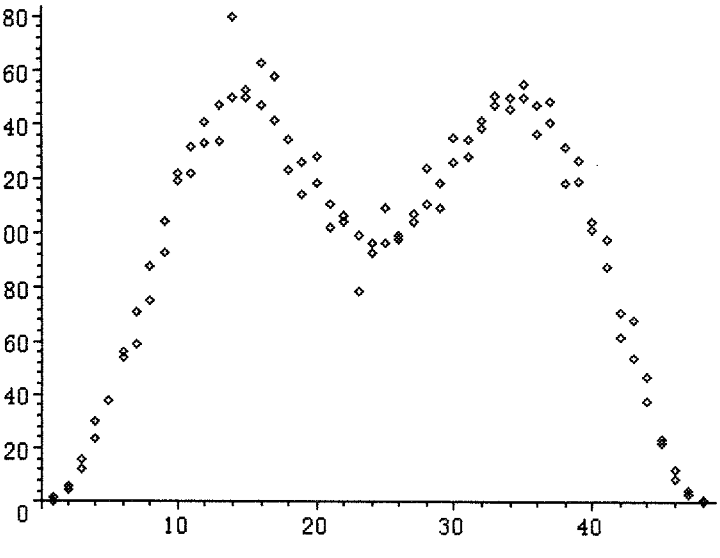
以下のグラフは 7.5° の mesh での統計である。予想される分布は

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

である。津田塾での話の(2004. 10. 26(日))段階では

$$\max(\max(0,\sin(3\pi x/2))^2, \max(0,\sin(3\pi(x-1/3)/2))^2$$

のような怪しげな予想(p = 3~12413, 1481 個)で確信がもてなかった。



その後、色々な既約な5次多項式について、計算を試みた。

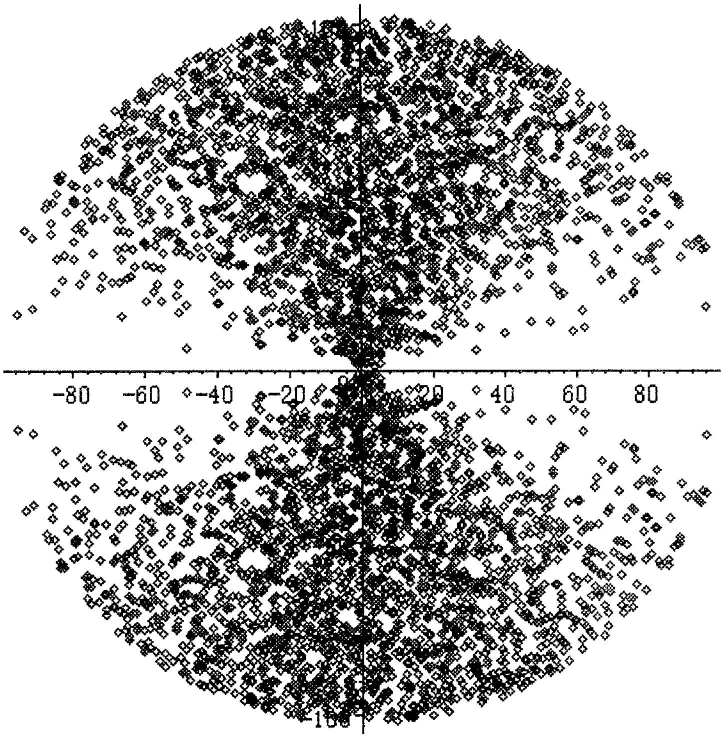
例えば、類数5の虚2次体 $Z(\sqrt{-47})$ の Hilbert-Weber の多項式の立方根の多項式の有理関数

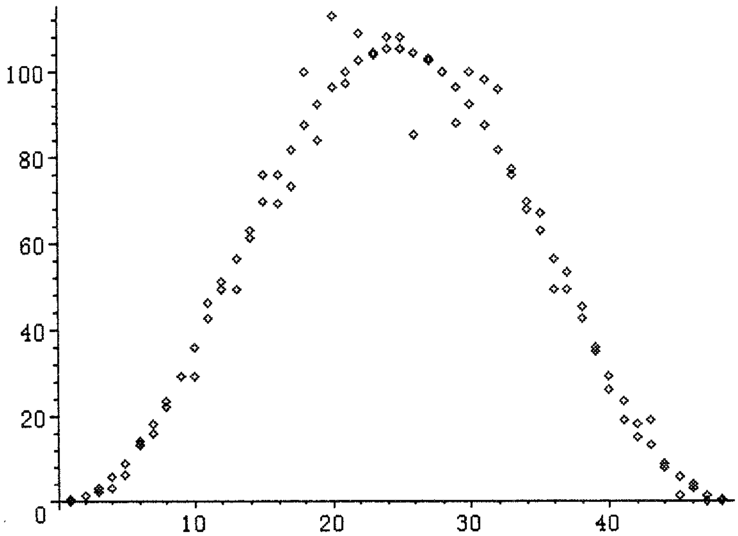
$$g_3(4x^8) = (1-16x^{24})/12x^{16}$$

による簡約多項式に対応する超楕円曲線

$$y^2 = x^5-x^3-2x^2-2x-1$$

では、genus 1、つまり通常の虚数乗法をもたない楕円曲線の場合と同様に $\sin^2 x$ に比例する分布になっている。





現在、超楕円曲線に関して、虚数乗法をもつ場合に相当する場合、つまり $\sin^2 x$ に比例する分布になっている場合として、やはり類数 5 の Hilbert-Weber の多項式の立方根の多項式の有理関数

$$g_3(4x^8) = (1-16x^{24})/12x^{16}$$

による簡約多項式に対応する超楕円曲線

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

が知られている。類数 5 の他の簡約形例示の表

47	$g_3(4x^8)$	$(x^5-x^3-2x^2-2x-1)(x^5-x^3+2x^2-2x+1)$
79	$g_3(4x^8)$	$(x^5+3x^4+2x^3+x^2+x+1)(x^5-3x^4+2x^3-x^2+x-1)$
103	$g_3(4x^8)$	$(x^5-x^4-3x^3-3x^2-2x-1)(x^5+x^4-3x^3+3x^2-2x+1)$
127	$g_3(4x^8)$	$(x^5+3x^4-x^3-2x^2+x+1)(x^5-3x^4-x^3+2x^2+x-1)$
131	$k_6(x)$	$(x^5-x^4-x^3+3x^2+5x+1)(x^5+x^4-x^3-3x^2+5x-1)$
	$h(2x)$	$x^5-8x^4+8x^3-11x^2+6x-4$
179	$k_6(x)$	$(x^5-2x^4+5x^3-x^2+6x-1)(x^5+2x^4+5x^3+x^2+6x+1)$
	$h(2x)$	$x^5-10x^4-19x^3-16x^2-5x-4$
227	$k_6(x)$	$(x^5-5x^4+9x^3-9x^2+9x-1)(x^5+5x^4+9x^3+9x^2+9x+1)$
	$h(2x)$	$x^5-19x^4+12x^3+29x^2-19x-20$
347	$k_6(x)$	$(x^5+7x^4+21x^3+27x^2+13x-1)(x^5-7x^4+21x^3-27x^2+13x+1)$
	$h(2x)$	$x^5+45x^4-60x^3+203x^2-125x+100$
443	$k_6(x)$	$(x^5+4x^4-3x^3-17x^2+22x+1)(x^5-4x^4-3x^3+17x^2+22x-1)$
	$h(2x)$	$x^5+91x^4+317x^3+219x^2-219x+55$
523	$h(2x)$	$x^5+141x^4+27x^3+59x^2+51x+45$
571	$h(2x)$	$x^5+188x^4+702x^3+1067x^2+754x+204$
619	$h(2x)$	$x^5+236x^4-558x^3+941x^2-806x+348$
683	$k_6(x)$	$(x^5-6x^4-5x^3+41x^2+56x+1)(x^5+6x^4-5x^3-41x^2+56x-1)$
	$h(2x)$	$x^5+325x^4-1980x^3+5533x^2-4415x+3400$
691	$h(2x)$	$x^5-348x^4+1203x^3-2050x^2+1743x-792$
739	$h(2x)$	$x^5-436x^4+90x^3-868x^2+613x-696$
787	$h(2x)$	$x^5-545x^4-1160x^3-847x^2-265x-100$
947	$k_6(x)$	$(x^5+5x^4+7x^3-103x^2+125x-1)(x^5-5x^4+7x^3+103x^2+125x+1)$
	$h(2x)$	$x^5-1126x^4+12159x^3-43417x^2+45012x-30613$
1051	$h(2x)$	$x^5+1718x^4+3915x^3+3200x^2-641x+5658$
1123	$h(2x)$	$x^5-2282x^4-3551x^3-1062x^2-891x-2538$
1723	$h(2x)$	$x^5+18531x^4-40848x^3+44189x^2-22539x+6390$
1747	$h(2x)$	$x^5-19984x^4-21888x^3-5161x^2-3734x-3180$
1867	$h(2x)$	$x^5+28923x^4+64404x^3+115583x^2+59559x+79182$
2203	$h(2x)$	$x^5+76738x^4+140194x^3+233675x^2-71500x+242000$
2347	$h(2x)$	$x^5+113935x^4+146965x^3+95193x^2+36855x+7425$
2683	$h(2x)$	$x^5+274001x^4+451692x^3+13199x^2-50399x+204450$

に表れる関数や、その他、手当たり次第の既約多項式、例えば

$$5: x^5+x^4-4x^3-3x^2+3x+1,\ D_5: x^5-5x+12,\ M_{20}: x^5+2,\ A_5: x^5+20x+16,\ S_5: x^5-x+1$$

Henri. Cohen: *A course in computational algebraic number theory*, Graduate Texts in Mathematics 138, Springer-Verlag, 1993, p327.

$$5: x^5+x^4-4x^3-3x^2+3x+1,\ F_{20}: x^5+x^4+2x^3+4x^2+x+1,\ A_5: x^5+x^4-2x^2-2x-2,\ S_5: x^5-x^3-x^2+x+1$$

Gunter. Malle, B.Heinrich. Matzat: *Inverse Galois Theory*, Springer Monographs in Mathematics, Springer 1999, Appendix: Example of polynomials p.413.

などはすべて

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

に従うと予想される。

上記の本の

$$D_5: x^5-x^3-2x^2-2x-1$$

は Hilbert-Weber の簡約形である。この場合は

$$\sin^2 x$$

型である。

何れにしても、多くの試みた既約多項式について、常に

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

の類型に属しているという経験から、Hilbert-Weber の多項式の一部を除いて

> 超楕円曲線
> $y^2 = f(x)$
> $f(x)$ は既約 5 次多項式
> の一般形 (generic form) に対応する分布は
> $\sin^2 x + \sin^2 2x$
> に比例する。

という予想(問題であるが)をしてみようと思う。

既約でない多項式では角度の点分布などが出てくる。その場合でも、0°, ±π/4 と一様分布の和などである。類型は

$$0, \pm\pi/4 + \text{uniform},\quad \sin^2 x,\quad \sin^2 x + \sin^2 2x$$

の 3 種類のみであろうか。これ以外の分布にはどのようなものがあるのであろうか興味はつきない。

尚、種数 3 の楕円曲線

$$y^2 = x^7+2x^6-x^5-x^4+x^3-x^2-x+1$$

についてもある程度の計算の試みが成されている。

$$a_p = \Sigma x\in p(f(x)/p),\ b_p = \Sigma x,y\in p(f(x,y)/p),\ c_p = \Sigma x,y,z\in p(f(x,y,z)/p)$$

に対し、6 次多項式

$$x^6+a_px^5+b_px^4+c_px^5+pb_px^4+p^2a_px+p^3 = (x^2+d_px+p)\,(x^2+e_px+pe^{iy})\,(x^2+e_px+pe^{-iy})$$

では、一つの 2 次因数は定数項は p であるが、他のもについては絶対値は p であるが複素数の範囲でしか因数に分解されない場合がある。この角分布も大いに面白い課題であろう。

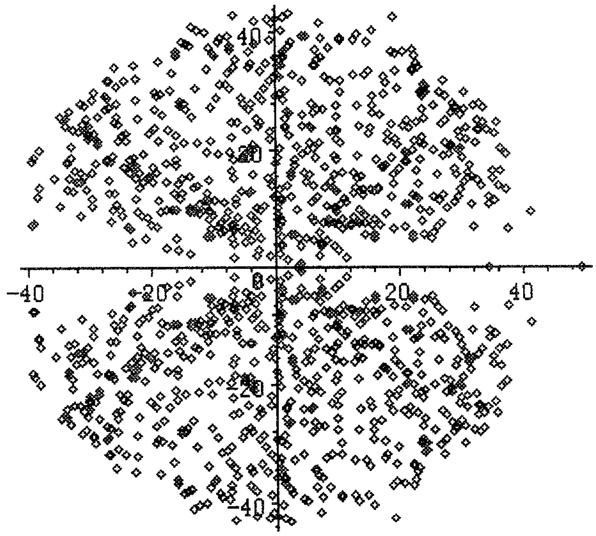
以下の計算結果は

$$y^2 = x^7+x^6-x^5+x^3-x^2-x+1$$

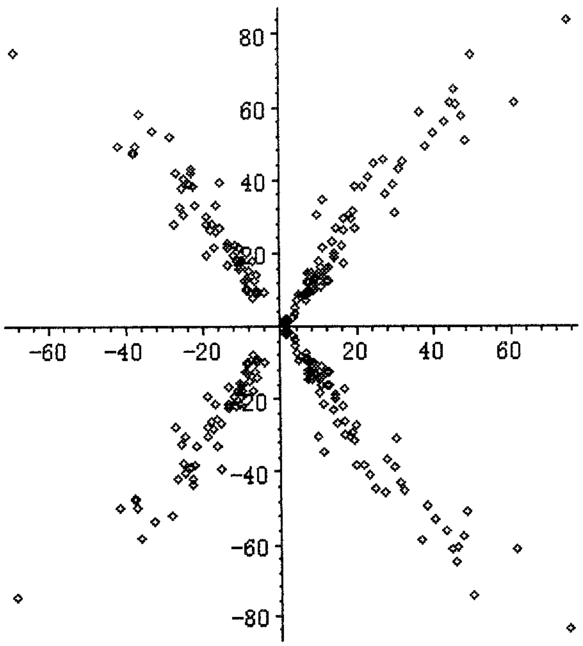
の素数 p = 3 ~ 1873 について、2 次の因数の定数項が p のものについての角分布についてのグラフである。ここでも、

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

を想像させる分布が見られる。正確な予想は現段階では(自分には)できない。



次は、2 次因数の一つだけの素数 p = 3, 7, 11, 19, 23, 31, 79, 163, 167, 223, 307, …,1667, 1723, 1747, 1811, 1831, 1847 の 66 個の素数に対応する根の分布である。$\sqrt{p}$ のものが 1/3。



尚、これらの素数に対応する絶対値 $\sqrt{p}$ の根の角分布は $\pm\pi/4$ に集中している。上記多項式は類数 7 の虚 2 次体 $Z(\sqrt{-79})$ に関する Hilbert-Weber 多項式の一つの簡約形である。

将来、ここに挙げたような現象は理論的に証明あるいは否定されることになるであろうが、現実にこのような実験式を作るにはある程度の計算の効率についての配慮が必要である。

例えば、終結式の Legendre 記号の 3 重和

$$c_p = \Sigma x,y,z\in p \ \left(f(x,y,z)/p\right)$$

では、p = 1800 の場合で $1800^3 = 5.832\times10^9$ 個程度の Legendre 記号の和を計算することになる。

$$y^2 = x^7+x^6-x^5+x^3-x^2-x+1 = f(x)$$

では、先ず x^3+ux^2+vx+w との x に関する終結式

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

は、例えば、u について整理して

$$\begin{gathered}
u^7 + (3w+v-1)u^6 + (3w^2+2wv-v^2-8v-4w-1)u^5 + (6w^2v-wv^2-v^3+w^3-5v^2-18wv-5w^2+5w+5v)u^4 \\
+(5w^2v^2+2w^4-5v^3w+15w^3v+6v^3-19w^2v-7w^3-6wv^2+20v^2+16w^2+22wv+5v-5w+1)u^3 \\
+(3w^5-20v^3w^2+8w^4v-6w^3v^2-5v^4w+v^5+4v^4-14w^2v^2+9v^3w-17w^4+6v^3 \\
+19w^3+19w^2v-29w^3v+20wv^2-20wv-17w^2-5v^2+v-2w+1)u^2 \\
+(+v^6-6w^3v^3-4w^4v^2+8v^5w+5w^2v^4+w^5v+3w^6-11w^5+25v^3w^2+15v^4w+21w^3v^2-2w^4v-v^5 \\
+22w^4+3w^2v^2+25w^3v-v^3w-8v^4-19wv^2-15v^3-29w^2v-12w^3+7wv-6v^2+3w^2+2w-2v-1)u \\
+(-w^6v+v^4w^3-v^6w-w^5v^2+v^5w^2-v^7+w^7+6w^4v^2+w^5v-5w^2v^4-4v^5w-2w^3v^3-3v^6-4w^6-w^4v-17w^3v^2-13v^3w^2 \\
-2v^4w+5w^5-3v^5-w^2v^2+6v^3w-10w^3v-2v^4-6w^4+14w^2v-v^3+4w^3+14wv^2+3wv-3v^2+w^2-w-3v-1)
\end{gathered}$$

といった複雑さの式である。これを 10^9 も計算するのは時間がかかる。

初期条件は代数的に与えて、階差法で数値的に順次求めるのが得策であろう。階差も前進、後退があるが、並列計算に即した後退階差が良いであろう。

n^0~n^7 の階差行列

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 2 & 6 & 14 & 30 & 62 & 126 \\
0 & 0 & 0 & 6 & 36 & 150 & 540 & 1806 \\
0 & 0 & 0 & 0 & 24 & 240 & 1560 & 8400 \\
0 & 0 & 0 & 0 & 0 & 120 & 1800 & 16800 \\
0 & 0 & 0 & 0 & 0 & 0 & 720 & 15120 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 5040
\end{pmatrix}$$

との各次数の係数の列ベクトルの積をとればよい。

昭和 38 年(大学院 2 年の頃)佐藤幹夫先生にはこのような色々な計算方法について教えて頂いて $\sin^2$-conjecture に至る計算を行った。

当時の東京教育大学の応用数理学科の HIPAC103 という parametron 計算機で計算した。word=48bit で 1kword が磁気 core 、8kword の磁気 drum である。p=14000 まで計算したのは 7000 個の係数を記憶し、残り 1kword を program に当てたからである。基本演算は加減算 0.4ms、乗法 1.8ms、除法 6.5ms(永島孝氏による)であった。 計算の周辺では故広瀬健氏にも大変にお世話になった。当時、広瀬さんの(後に結婚)奥さんは立教大学の計算機室に勤めていた。.一松信先生は立教大学で HIPAC101 を使っておられた。後に東大に移って

からは parametron 計算機の生みの親、後藤英一先生と話す機会も何度かあった。彼の一つの夢であった量子 parametron 効果を用いた計算機の構想を熱く語っていたのを思い出す。現在は計算機の主流はこの方向には向いていないが将来この構想が実現されることを強く期待している。並列計算や sensor としての機能も同時に備えた情報処理の機構である。

尚、genus 3 の楕円曲線についての計算については、ほんの一部の情報しか持ち合わせていないが、

$$y^2 = f(x) \qquad f(x) \text{は 7 次式}$$

の研究は非常に重要であるとの印象を受けた。それは、一つには 3 個の穴の曲面が分岐曲面の生成元であること、2 個の穴の曲面は回線として、1 個の穴の曲面、つまり楕円曲線の場合は端点としての構造をもっているからである。

また、$Z(\sqrt{-7})$ の類数が 1 であることも重要な意味をもっていると思う。

$Z(\sqrt{-p})$ の整数環の類数が 1 になる素数 p は

1, 2, 3, 7, 11, 19, 43, 67, 163

であるが、有限体の上の物理学(将来このような分野が確立されたらの場合であるが…)では単項 ideal 環になる場合は特別な意味をもつと考えられるからである。

このような虚 2 次体の整数環に関する Hilbert-Weber の類多項式は次のような有理関数で簡約化可能である。

$$-8x(2x^3+1)/3$$

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

$$= -8(x+1)(x-2)(x^6+2x^3-8)/(x^2+2x-2)^4$$

	Hilbert-Weber pol.	cubic root	$-8x(2x^3+1)/3$	$(x+1)(x-2)/(x^2+2x-2)$
2	27x-125	3x-5		
3	x	x	x	(x+1)(x-2)
7	64x+125	4x+5	$8x^2+4x-3$	x^2+x+2
11	27x+512	3x+8	x+1	$2x^2+x-4$
19	x+512	x+8	x-1	x
43	x+512000	x+80	x+2	(x-1)(x+2)
67	x+85184000	x+440	x-3	(x+4)(2x-1)
163	x+151931373056000	x+53360	x+10	(x+3)(3x-2)

reference

[1] Kanji Namba: Legendre polynomial over finite fields and factorization of integers. Int. Symp. in mem. of Hua Loo Keng. Beijin I, 1991, pp.209-223.

[2] Kanji Namba: Complex multiplication of elliptic functions and compositional square root of rational functions. 2001 年度応用数学合同研究集会 REC Hall, Ryukoku Univ. 2001, pp.41-46.

[3] Kanji Namba: Elliptic curves over finite field and Hilbert-Weber polynomial of degree 5. 2002 年度応用数学合同研究集会 REC Hall, Ryukoku Univ. 2002, pp.37-42.

[4] Kanji Namba: Hyper-elliptic curves over finite fields and an extension of Sato-$\sin^2$ -conjecture. 2003 年度応用数学合同研究集会 REC Hall, Ryukoku Univ. 2003, pp.31-36.

有理関数の合成代数と虚数乗法

資料について

a) これは佐藤先生が p=14000 までの計算結果から、$\sin^2$-予想を確信して、それを私や岩村先生や秋月先生などに説明しながら話したときの用紙だと思います。$\sin^2\theta$ の下に何重もの波線を引きながら話している様子が伺われます。14000 というのもその予想のために計算した素数の範囲です。

b) ⓪~⑥の番号のついた手書きの資料は、佐藤先生と今後計算の計画について話しながら書いた一枚の紙の裏表を成すものです。103 は東京教育大学のパラメトロン計算機 HIPAC103 のこと。5020 は当時、日立中央研究所の HITAC5020 の試作第 1 号機の意味です。

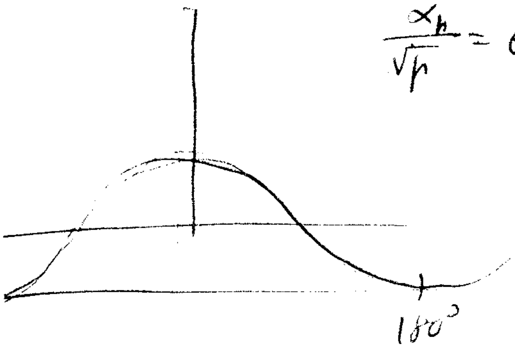
c) このラインプリンターに印刷されたものは

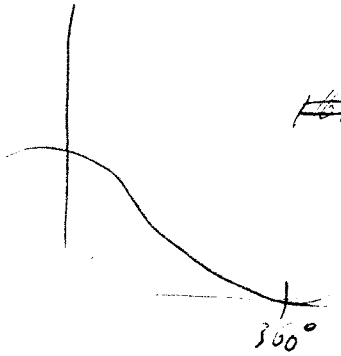
$$y^2 = x^5-x^4-7x^3+x^2+6x$$

p = 263 まで a_p, b_p を計算したものです。(昭和 39 年 6 月頃と思われる)日立中央研究所の HITAC5020 の試作機ではソフトウエアシステム開発はこの試作機のみで行われ開発担当者は深夜まで交代で使用していたが、朝方 4 時～ 5 時頃は疲れ切って、次の交代まで 30 分とか 1 時間位、計算機は使用されない時間がたまにあくことがあるので、ずっと待機していてその時間計算機を使わせてもらえることがあった。これは東大で TAC を開発にたずさわって来た村田健朗先生が日立に移って、恐らくは佐藤幹夫・岩村聯・秋月康夫先生の紹介もあって便宜をはかってもらったのであろうと思う。この計算機は今も国立科学博物館に保存されていると聞いている。この計算結果から、僅かの個数であるが $\sin^2\theta$ の分布と異なるかも知れないグラフを書いて保存してあったのを今回の計算を再度試みるにあたって思い出した。しかし、当時は、genus 2 での統計的類型は非常に沢山であろうと思っていた。

$1 - a_p u + p u^2 = (1 - \alpha_p u)(1 - \bar{\alpha}_p u)$ $\quad |\alpha_p| = |\bar{\alpha}_p| = \sqrt{p}.$

$\frac{\alpha_p}{\sqrt{p}} = e^{i\theta}.$





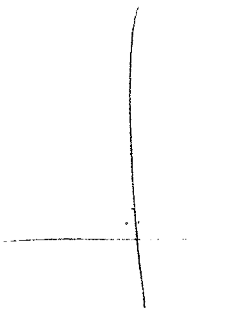
θ

$\sin^2\theta$

14000

1

1000000
1000000



$\boxed{p}$

$k=6.$ $\eta(\tau)^{12}$

$k=8$ $\eta(\tau)^8\eta(2\tau)$

$k=12$ $\eta(\tau)^{24}$

$\frac{a_p}{\sqrt{p}}$ $\quad \frac{a_p}{\sqrt{p^{k-1}}}$

$k=2$

$\eta(\tau)^2\eta(5\tau)^2$

$\eta(\tau)^2\eta(11\tau)^2$

$\eta(\tau)^4$ $\quad \eta(\tau)^2\eta(2\tau)^2$

$k=4$

$\eta(\tau)^4\eta(5\tau)^4$

$\eta(\tau)^4\eta(2\tau)^4$

$\eta(\tau)^8$

⓪ $y^2 = x(x^2 \pm x \pm 1)$　$2y^2 = x^3 - \cdots$ の2例で．$p < 10^5$

① のういものて．　ax^3+bx^2+cx+d ⟶ ~~標準形に直す~~　（あとで）

から．$g_2,\ g_3,\ \Delta,\ J,\ J-12^3$ を求め．

$\mathrm{Max}(|a|, |b|, |c|, |d|)$ の小さい順．

$J = \dfrac{Q}{P}$，$J - 12^3 = \dfrac{R}{P}$　（キヤク分数とする）．

~~$\mathrm{Max}(P, Q, R)$~~ が小さいものがほしい．

$\mathrm{Max}(P, \mathrm{Min}(Q,R))$

~~$a \geq |d| \geq 0$~~

$a \geq |d| \geq 0$

$$J = \frac{12^3 g_2^3}{\Delta} = \frac{D \times \bigcirc}{D \times \Delta_1} \qquad J - 12^3 = \frac{36^3 g_3^2}{\Delta} = \frac{D \times \bigcirc}{D \times \Delta_1}$$

$\Delta = g_2^3 - 27 g_3^2$

$\Delta = D \times \Delta_1$

$g_2,\ g_3$　$\underbrace{\Delta_1,\ D}$

$$4x^3 + \frac{4b}{a}x^2 + \frac{4c}{a}x + \frac{4d}{a}$$

$$\left(x - \frac{b}{3a}\right)^3 + \frac{b}{a}\left(x - \frac{b}{3a}\right)^2 + \frac{c}{a}\left(x - \frac{b}{3a}\right) + \frac{4d}{a}$$

$D = (12^3 g_2^3,\ 36^3 g_3^2,\ \Delta)$

$$\frac{b^2}{3a^2} - \frac{2b^2}{3a^2} + \frac{c}{a} = \frac{-b^2 + 3ac}{3a^2} = g_2 \times (-4)$$

g

c^2　c^3

$4x^3 - g_2 x - g_3$

$$g_2 = -4 \times \frac{-b^2 + 3ac}{3a^2} \quad (\times (3a)^2)$$

$$= -12(-b^2 + 3ac)$$

$g_3 = \boxed{\text{3次式}}$

② (10^3? / 5020で. data. a, b, c, d, g_2, g_3, ~~[illegible]~~ Δ, $J = \frac{○}{○}$, $J - 12^3 = \frac{○}{○}$

①の方から抽出した cases につき.

$a_p = -\sum_{x \bmod p} \left(\frac{f(x)}{p}\right)$ を求めて. 比較的小さな p ~~[illegible]~~ の範囲で table を作る. $p < 1000$ 程度 ~~1000~~ 500

~~[illegible]~~ もし出来たら ($N_p = 1 - a_p + p$ $(p \nmid \Delta)$ の最大公約数.)

③ ~~5020~~ $f(x)$ 5次式. $x^5 - 1$, $x^5 - x$, $\binom{x}{5}$. 等.

$p < 1000$ くらいで. $(a_p, b_p - 2p)$ を求める. table

④ 5020 a_p の分布. ②のうちの J が non-integer の ~~[illegible] example~~ を抽出して. ~~[illegible]~~ $p < 1$万

⑤ 5020 ~~[illegible]~~ $(a_p, b_p - 2p)$ の分布を, (③のうちから いくつか よいものを えらんで,) ~~[illegible]~~ しらべる.

⑥ Legendre, 一つの example で. $p <$ 約10万

A	B	C	D	E	F
1	-1	-7	1	6	0

3	2	3	-20	65
5	0	-5	-65	65
7	4	0	-30	0
11	10	-11	-25	0
13	10	-65	-55	0
17	8	-17	-35	0
19	4	114	50	-20
23	18	-92	-40	0
29	18	-87	-35	0
31	18	-186	-60	0
37	26	74	0	0
41	32	-492	0	0
43	34	-86	-20	0
47	34	188	15	0
53	40	424	50	0
59	40	0	-15	0
61	36	0	-15	0
67	46	-268	-30	0
71	46	213	10	0
73	48	438	25	0
79	56	632	40	0
83	66	249	5	0
89	64	0	-10	0
97	72	1164	70	0
101	86	0	-10	0
103	76	-1030	-45	0
107	64	-749	-40	0
109	86	1635	0	0
113	62	226	0	0
127	96	254	0	0
131	88	-2489	0	0
137	100	4384	0	0
139	94	1946	0	0
149	102	1490	35	0
151	110	2114	60	0
157	114	-2512	-60	0
163	124	2445	55	0
167	114	1002	15	0
173	134	4152	0	0
179	126	3222	0	0
181	134	-1086	-25	0
191	132	-573	-15	0
193	134	-2702	-50	0
197	150	-591	-15	0
199	152	5373	0	0
211	160	1688	20	0
223	144	-6021	0	0
227	146	454	0	0
229	164	2061	25	0
233	178	3029	35	0
239	176	3585	45	0
241	166	7230	0	0
251	154	-3765	-50	0
257	192	4112	45	0
263	184	1578	15	0