

Dedekind η 関数と佐藤 \sin^2 -予想

難波完爾

719-1117 岡山県総社市北溝手 463-3

tel/fax. 0866-90-1886

2005. 12. 07

この小論では、佐藤 \sin^2 -予想、つまり、現在 Sato-Tate 予想と呼ばれている予想の発端の頃の話の断片から始めようと思う。

このような記憶や事実もいずれ過去の影のゆらぎのなかに消えてしまうのである。そのようなことを思い、今は(自分には)自明の(時代の)ことを、文字の列のなかに記録として留めておこうと思う。多くの場合、いざ書き留めようと思った(死に近いなどの…)ときにはそれが(物理的に)不可能なことは先人の教える所である。(尤も、書かなければとか、知らなければ良かったと思うことも多い)


1. 当時の風景

私は、昭和 37 年 3 月に、岡山大学理学部数学科を卒業して、同年 4 月から東京教育大学理学系研究科数学専攻に入学した。同専攻の募集定員は 10 名で 13 人が受験し、私は受験番号が 13 番という縁起のよくなさそうなものであった。

その前の年には、岡山大学にも NEC の電子計算機が入り、後期には、教育大学からの岩村聯教授の計算機の講義もあった。確か、加法の code は 30 だったというようなことを記憶している。大学の seminar では稲垣武先生のところで Kuratowski の Topologie I,II という分厚い本を読んだ。

当時の数学教室は木造の兵舎をそのまま用いており、その 1 階の入り口の近くの火鉢のある部屋には富田稔先生がいて、そこで、一番安い 80 円の Gentzen のドイツ語の花文字の、表題が一番長く厚さは一番薄い、自然数論の無矛盾性証明(Widerspruchsfreiheitsbeweis)の海賊版の本を買い、謎を解くような気持ちになって楽しみまた眺めながら読んだ。

その頃、喫茶店でのコーヒーの値段というのは 30~40 円だったと思う。Mozart や Chopin を聞きながら(連続体 continuum の)謎に思いをめぐらせていたのであった。また、岡山の古本屋の店先に Sierpinski の Hypothese du continu という本が、まあ売れなくて当然か…、という雰囲気でおいてあったのに目がとまり、やはり 300 円位、といってもコーヒーの 7~8 回分か、ちょっと痛い出費だが…、と思ったが買って読んだ。そのときフランス語の中古の辞書も買ったのである。この本には K. Yoshioka. 1946. 9. 27(8)と記入がある。


1946. 9. 28.

この本との出会いも、最初のインキの匂いとともに、私に大きな影響を与えものである。この本が通ってきた道(histoire)には、私を奇妙な道(集合論)に引き込んだという意味も含め、今も興味をもっている。

また、竹之内脩先生は、私は関西一ものごとをハッキリいう男だが、日本一ものごとをハッキリいう竹内(外史)君の所にいったらどうか…、と進学を勧めて下さった。そして、Whyburn の Analytic topology や Whittaker-Watson の A course of modern analysis など紹介して頂き、自分も、部分的だが問題を解いたりして楽しんだ。問題は結構難しく、解けなくて当然と思えば、問題を眺めて夢をみているつもりで考えられて気楽であった。それでも何か真実の影を見付けたときは楽しい瞬間を味わった。

今になって思うのであるが、別な意味でやはり大きく心に残っているのは、富田稔先生の考えながら歩いて(立ち止まって)いる姿である。彼(あるいは、一般に人)があるとき構想していたものは、今の空間の認識の言語であったと思うのであるが…、とにかく「空間のなかにことばを創り出す」…、あるいは、そうしようという“意志”の姿や形であったと思う。

ものごととは成功裏に終わるとは限らない(成功したり実現したりしない方がよい場合も多い)。多くの夢は終わらない形で終わる。だから…夢。それで良いし、そうあるべきなのである。

夢としての使命や機能の最も重要な点は“停止”である。現実の、…悪夢から覚める…である。そこ(悪夢)への導かれることは、control の利かないことが多いのである。

夢は「実体」そのものではないが、自然の認識のための、夢…は現実中存在しつづけるであろう。

停止、の概念を、何か feed back の一種と考えるのは適切ではないと思う。むしろ、現在から未来に向けて最も関心を寄せるべき feed forward の概念の中心に位置するものと認識すべき対象である。

例えば、robotics でも、目的の対象を、如何に“そこ”に…自然に…“停止”(dimamic stop, settle)させる、つまり、落ち着かせる(落ち着くような場を設定する)かというような問題である。これは、多くの場合“力”の問題ではなくて、“概念”や“姿勢”の問題なのである。power や force はそこ(今の状態)からの、そこ(目的の安定状態へ向けて)への結果(状態の変化の傾向)である。

さて、この受験番号 13 番の学生(=私)のセミナーの担当は、当時助手の永島孝氏であった。セミナーの内容は竹内先生の論文を読むことで、内容の check という意味合いも含まれていた。あるとき、ここはチョット(=大いに)おかしい、といったら、竹内先生が間違えるはずがないという。例の学生は、えっ!。…でも、論文の内容は正しいかも知れないが…、人が間違えないというのは、(なんぼなんでも、絶対)間違いだ。…と答えたことは云うまでもない。(間違いでないことも稀にある。この場合には、一度 check を受け、正しさの確度を上げることになる)

兎も角、埒が開かないから先生のところに行こうということになり、竹内先生の所に行く。先生の言は、「そういうこともあるでしょう。だから、読んでもらっているのです」と…当然至極の返答である。先生の言はかくあるべき…と思う(明快である)。竹内先生の教育はこのような形(間接法)でも行われたのである。

この頃(昭和 37 年)、東京教育大学応用数理学科に電子計算機 HIPAC103 が入り、岩村先生の解析学の講義も計算機がらみとなり、私も例にもれず計算機にハマる。立教大学の島内剛一先生などと色々計算する。例えば、ある番地を clear する、つまり 0 を記憶する

代わりに、自分の内容同士の excluded or (排反和 xor) をとる。この場合 local、(bit-wise) に演算可能なので速い。記憶装置が磁気 core であったから、湖畔の宿状態で…書いては消し、書いて又消す(～湖畔のたより)…となり、加熱して error をおこす。…など私と(or) 島内さんが計算機を使うと、必ずとっていい程 error をおこし、日立の人が、“また” ですか?、とって対策を講じて修理する。それでも error がおこると“まだ” ダメでしたかなどと、設計・研究所の雰囲気となる。起こり得る error の表の作成と対策には少しは貢献していたであろう。

永島孝さんと故広瀬健さんには、ここでの主題の \sin^2 -予想の計算の出力関係や統計のプログラムでも(その他、雑談でも)お世話になった。私は出力の format など余りにしない質であったが、永島さんにはこれは許し難いことであったに違いない。(このような雰囲気が、湯気をともなって出ていた)。

勿論、私も、見た目も良い方と悪い方、内容が同じなら良い方を選ぶ。
兎も角、計算とプログラムの演習の書き方の初歩は素数表で、すぐ任意の 6 以上の偶数は 2 つの素数の和、

$$n \geq 3 \rightarrow \exists p \exists q (2n = p+q)$$

(p, q 素数) という予想などで遊びたくなるのは人の常で Goldbach などと(戯れ)遊ぶ。

解の個数も、例えば、n が 3 の倍数ならば p が mod 3 で 1 なら q は mod 3 で 2 である。しかし、例えば n が mod 3 で 1 なら、p が mod 3 で 1 なら q は mod 3 で 1 である。p が mod 3 で 2 なら q は 3 の倍数で(3 を除いて)素数でない。このように解の個数にはばらつきがあるというような当然のことを楽しんでいた。

ある夏の日の帰り道、岩村先生は中村橋、佐藤先生は所沢、自分は練馬で、西武(池袋)線の沿線に住んでいたのも、途中の池袋の西武デパートの屋上のビアガーデンで(ちょいと)一杯ということになった。そこで、難波君、今どんなことをやっていますかというような話になった。それで、Goldbach の解の個数が…などと話していたら、それも面白いかも知れないけれど、…少し意味のある計算をやってみませんか、ということになった。それで、楕円母数形式、志村・谷山…などの概念や文字列と遭遇することになったのである。

この頃は、まだ、西武デパートの新宿寄りには丸物デパート(今はパルコ)などがあった時代である。また、池袋の西武のある東口には岡本太郎のジュラルミン(duralumin)の objet (太陽の塔の前身みたいなもので、まだ顔の部分はなかった)が異様な金属の鈍い光を放っていた。

さて、例のパラメトロン計算機 103(一丸さん=いちまるさん、と呼んでいた)であるが、主記憶装置は 8kw(キロ word)で、1word は 48bit(32-bit machine ではない)、それに、処理速度の速い 1kw の磁気 core メモリーの構成である。これに、Dedekind の η 関数

$$\eta(x) = (1-x)(1-x^2)(1-x^3) \cdots$$

の係数を、ドラム(memory)の 1000~8000 番地までにぶちこみ、プログラムの方は(最初の 0~1023 が core メモリー)1kw(キロワットではない)の core(memory)に入れて、目的の楕円曲線

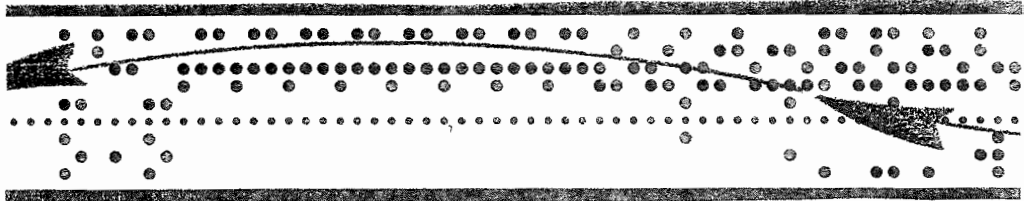
$$C: y^2 = x(x^2+x-1)$$

に対応する、楕円母数形式

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

の係数を、素数 $p = 2n+1$ として計算するのである。

必要な素数の表などは、予め紙テープに出力しておいて機械式の tape reader でカシヤカシヤと読みとるので 1 秒に数語の速度である。それでも、当時は sprocket の他、parity を含め 3+5 個の穴のテープの文字が自然に、かなり読めるようになっていたのであるから不思議である。(今は全然読めない)



当時は空調のある部屋は“貴重な” 計算機のある部屋のみという状態であり、徹夜して計算しているときなど、たまに parity の合わない出力があつたりして、それが認識できることがあつた。多くは理由は解らなかつたが、雷とか空調のスイッチの切れるときの火花などが関連したと認識できたものも相当あつた。まだ、計算機が重電機であつた時代である。

計算の速度も、加法 0.4ms(ミリ秒)、乗法 1.8ms、除法 6.5ms であつたから、ドラムから数値を読み出してドラムに書き込む一連の作業は、加法でさえ 1 秒に数百回程度であつたし、数値を書き込む場所も計算の終了の時間を見計らつて、ドラム上の縞模様の場所に記憶したこともあつた。計算の高速化に大いに気を使つていたのである。

尤も、このような計算の効率化の研究や必要は、歴史的には、例えば、高速 fourier 変換(FFT, fast fourier transformation)の発見の強い動機になつたものである。

ともあれ、このような状態で

$$\begin{aligned} \eta(x)^2 \eta(5x)^2 &= 1 + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4 + \cdots \\ &= 1 - 2x - x^2 + 2x^3 + x^4 + 0x^5 + 2x^6 + 2x^7 - 6x^8 - 4x^9 - \cdots \end{aligned}$$

などと計算し、素数 $p = 2n+1$ に対して、 b_n を a_p として、例えば、

$$a_3 = -2, a_5 = -1, a_7 = 2, a_{11} = 0, a_{13} = 2, \cdots$$

のような係数の列を求めていったのである。

例えば、 a_p について、上の例からでも $a_{17} = b_8 = -6$ であるが、2 次方程式

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

は常に、非実根(non-real solution)をもつこと、つまり

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

が(上の例では $6 < 2\sqrt{17} \approx 8.2462$)、Hasse の不等式として知られているから、解の絶対値は常に \sqrt{p} である。

佐藤先生が着目したのは解の偏角(argument)

$$\sqrt{p} e^{i\theta} = \sqrt{p} (\cos \theta \pm i \sin \theta) = (a_p \pm \sqrt{a_p^2 - 4p})/2$$

の θ の分布であつた。先生自身も手計算で、相当多くの場合に可能性のある(特定の)場合、つまり分布曲線の可能性を想定していたに違いないと思う。それは、もし真実を映したものであれば、簡潔な美しさをもつたものであらうということだと思う。それが、どんな形をもって表れてくるか…。それを確信のもてる形で見たかったのであろう。

HIPAC103 での計算では 7000 個の係数を用いたから、 $p = 2n+1$ で、14000 までの素数について data を得ることができた。恐らく、10000 位の素数で一個あたり数分を要したであろうが、当時は data が求まる毎に、なにか輝く星くず³(stardust)が誕生するように新鮮な感覚があった。また、入出力装置も printer と穴の「あり・なし」を針金の出し入れして探る機械式紙テープ読み取り装置と、パンチ式穴開け機がすべてである。

一つ数値が決まると、パチパチとタイプライター鳴り、とジャジャジャとテープパンチャーがテープを送り出し、次の素数をカシャカシャと読みとる。そして、健全な数値が出ているのを見て、ヨシヨシという気分になるのである。要するに、機械が、空調のバックグラウンド音、機械油とオゾンのおいの中で、全身全霊で動いているという気分、自分達(機械も仲間)が生きた時間と空間の中にいることが実感できるのである。

さっき、健全な数値といったが、そんなに低くない確率で、雑音か何か“ひろって”とんでもない巨大な、つまり $2\sqrt{p}$ より大きな数値をだすこともあり、それはそれで楽しみであった。こんな時は、一つ素数を戻して再計算し、それらしい数値を得て“これならよろしい”という気分になるのである。まあ、要するに退屈はしなかったということである。

計算機は大学の共同利用であったから、物理などの計算もこなしていたが、そこからは error の話、つまり誤動作の苦情(claim)は聞いたことはなかった。どうも、我々の時だけ選んで誤動作したとも思えないから、やはり相当の確率で誤動作はあったと思われる。我々は同じ所を高速で繰り返し“たたく”(beat)から誤動作の確率は高かったではあろうが…。他の人たちは謙虚だったのだろうか、気はついていて再計算していたのだろうか。

計算を開始すると、(常にはでないが)岩村先生や広瀬健氏やその他、外野の連中がガヤガヤと(error がおこる瞬間を見てやろうなど)集まるので、人体の発熱もあって、空調の冷房装置のスイッチの入る音、ガチャ・ウーン…バシッ・フーンという一連の雑音の回数も増すのである。

問題はこのバシッである。これは、空調の大電流が切られるときの音で、現実に空調機の中で青白い光と、金属の蒸気とオゾンの混じった青白い煙の糸がでること、そしてファン音だけの静けさに戻ることを意味している。この瞬間の衝撃電流や電磁波が error を引き起こすのを何回か経験した。日立の人がコンデンサーを並列に挿入して対策を講じることになる。

計算機の memory の kw(kiro-word)は少ないが、電力消費の kw(kiro-watt)は大きかった。所謂、熱の入った計算であった。

2. デデキンドの η 関数

Dedekind η 関数(η -function)は、 $x = e^{2\pi i}$ として、無限積

$$\eta(x) = x^{1/24} \prod_{n \in \mathbb{N}} (1-x^n) = x^{1/24} (1-x) (1-x^2) (1-x^3) (1-x^4) \cdots$$

で定義される級数である。この級数を用いて

$$(\eta(x) \eta(mx))^n$$

を無限級数として、

$$k = 24/(n(m+1))$$

が整数になるものについて、

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

を計算して、これを $y = x^{1/k}$ の級数として、

$$x^{1/k}(1+a_1x+a_2x^2+a_3x^3+\cdots) = y(b_1+b_{k+1}y^k+b_{2k+1}y^{2k}+b_{3k+1}y^{3k}+\cdots)$$

という表示の係数を具体的に計算する。つまり、個別には

$$b_{kn+1} = a_n$$

と見なすだけであるから、本質的な部分は a_n の計算である。

$k = 24/(n(m+1))$ が整数になる組合せの表

k	1	2	3	4	6	12
n, m	1, 23	1, 11	1, 7	1, 5	1, 3	1, 1
	2, 11	2, 5	2, 3	2, 2	2, 1	
	3, 7	3, 3	--	3, 1		
	4, 5	4, 2	4, 1			
	6, 3	6, 1				
	8, 2					
	12, 1					

先ず、良く知られている $\eta(x)$ の計算である。この関数を最初に計算した人はある程度の項の消去の後に感動したのではないだろうか。

良く知られている通り

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

であり、その3乗も美しい表示

$$\eta(x)^3 = \sum_{n=-\infty}^{\infty} (4n+1) x^{n(2n+1)}$$

をもつ。

先ず、最初の無限和の表示の話から始めよう。計算はこの様な公式から始めても良い訳であるが、私はそれは勧めない。公式集は先ず疑ってかかるべきである。(多くの式は論文や別の公式集からの写しである。誤植、活字の向き、条件の捨象など…)

結局のところ、ある程度の大きさの仕事を為すときは、1 (あるいは0) から始める。それが一番の早道なのである。(このことを知るには時間がかかった)

つまり、例えば、添字が0から始まるか1からか、 n と $n+1$ の間違い、そういったものを途中に含む計算は結局もとからやり直し、しかも不安を残した結果しか得られないからである。

そして、恐らく、一番の“深い”誤りは、計算結果が絶対に正しいと思いこむことである。正しい計算であっても(真実の場合には特に)何処かに誤りがあるかも知れないという心配が残るのが正常なのだ(私は)思う。

その理由の第一は、ある程度の計算を実行しようとする人はこれから実行しようという行為の系列について実の体験、とくに誤りについて(どんな時、どんな形で起こるか、そして誤りの結果、何がおこるか)体験していることが大切である。次のステップの(意欲、謙虚さ)礎になるからである。誤りの発見の“力”になるのは謙虚さである。

$\eta(x)$ の係数の生成の見則は、1から始めて、符号を変えて、ずらして加える。shift 数は1ずつ増やす。

1	-1																		
		-1	1																
1	-1	-1	1																
			-1	1	1	-1													
1	-1	-1	0	1	1	-1													
				-1	1	1	0	-1	-1	1									
1	-1	-1	0	0	2	0	0	-1	-1	1									
					-1	1	1	0	0	-2	0	0	1	1	-1				
1	-1	-1	0	0	1	1	1	-1	-1	-1	0	0	1	1	-1				
						-1	1	1	0	0	-1	-1	-1	1	1	1	0	0	-1
1	-1	-1	0	0	1	0	2	0	-1	-1	-1	-1	0	2	0	1	0	0	-1
							-1	1	1	0	0	-1	0	-2	0	1	1	1	0
1	-1	-1	0	0	1	0	1	1	0	-1	-1	-2	0	0	0	2	1	1	0
								-1	1	1	0	0	-1	0	-1	-1	0	1	1
1	-1	-1	0	0	1	0	1	0	-1	-1	-2	-1	0	-1	0	1	1	2	0
1	-1	-1	0	0	1	0	1	0	-1	-2	-1	0	-1	1	1	2	1	1	-1

(確定したところは太字)

結果は、二つの 2 次多項式の値となる所のみ残して 0 であり、それらの項も係数は ± 1 である。要約すれば

$$\prod_{n \in \mathbb{N}} (1 - x^n) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - x^{40} + x^{51} + x^{57} - x^{70} - x^{77} + x^{92} + x^{100} - x^{117} - x^{126} + \dots$$

となり、符号の変化は 2 個ずつ組になっている。それらの系列は

$$1, 5, 12, 22, 35, 51, 70, 92, 117, \dots$$

$$2, 7, 15, 26, 40, 57, 77, 100, 126, \dots$$

である。それぞれの系列は 2 次多項式

$$n(3n-1)/2, \quad n(3n+1)/2$$

で得られ、一方は n に $-n$ を代入したものになっている。従って、求める関数は

$$1 + \sum_{n=1}^{\infty} (-1)^n (x^{n(3n-1)/2} + x^{n(3n+1)/2}) = \sum_{n=-\infty}^{\infty} (-1)^n x^{n(3n+1)/2}$$

であることが解る。x の指数は、整数に対し非負の整数を対応させる 2 次式

$$n(3n+1)/2 : \mathbb{Z} \rightarrow \{0\} \cup \mathbb{N}$$

である。

だから、求める無限積の計算は、最初に記したように計算すれば大変な算法の回数を必要とする計算も、Gauss が云うように、例えば、 x^{100000} の項までの近似と云っても

$$(-1 - 7\sqrt{2449})/6 = -57.901 < n < 57.568 = (-1 + 7\sqrt{2449})/6$$

の範囲の -57 から 57 までの整数、つまり、 $2 \cdot 57 + 1 = 115$ 項ばかりの簡単な 2 次多項式の計算、言い換えると、平方根の計算量 (computational amount) で済む訳である。(10000 の平方根は 100) 例の計算も、これらの位置だけに ± 1 を置いて、計算を始めた訳である。

このようにして、例えば

$$\begin{aligned} &\eta(\tau)^2, \eta(\tau)\eta(2\tau), \eta(\tau)\eta(3\tau), \eta(\tau)\eta(5\tau), \eta(\tau)\eta(7\tau), \eta(\tau)\eta(11\tau), \eta(\tau)\eta(23\tau) \\ &\eta(\tau)^4, \eta(\tau)^2\eta(2\tau)^2, \eta(\tau)^2\eta(3\tau)^2, \eta(\tau)^2\eta(5\tau)^2, \eta(\tau)^2\eta(7\tau)^2, \eta(\tau)^2\eta(11\tau)^2 \\ &\eta(\tau)^6, \eta(\tau)^4\eta(2\tau)^2, \eta(\tau)^3\eta(3\tau)^2, \eta(\tau)^4\eta(5\tau)^2 \\ &\eta(\tau)^8, \eta(\tau)^8\eta(2\tau)^2, \eta(\tau)^6\eta(3\tau)^2 \\ &\eta(\tau)^{12} \\ &\eta(\tau)^{24} \end{aligned}$$

などを係数を順次計算していったのである。

例えば $\eta(\tau)^2$ の係数の先頭の部分を記しておくとな次のようである。

1	-2	-1	2	1	2	-2	0	-2	-2	1	0	0	2	3	-2	2	0	0	-2	-2	0	0	-2	-1
---	----	----	---	---	---	----	---	----	----	---	---	---	---	---	----	---	---	---	----	----	---	---	----	----

現実には $\eta(\tau)^2$ の値を長い紙テープに出力(記憶)して、それを再び計算機に入れる。tape は外部記憶装置であった。資源を有効に使う(使わざるを得ない)というのは一種の励みであった。

これから、例えば $\eta(\tau)^2\eta(5\tau)^2$ を計算する場合

1					-2					-1					2					1				
1	-2	-1	2	1	2	-2	0	-2	-2	1	0	0	2	3	-2	2	0	0	-2	-2	0	0	-2	-1
					-2	4	2	-4	-2	-4	4	0	4	4	-2	0	0	-4	-6	4	-4	0	0	4
										-1	2	1	-2	-1	-2	2	0	2	2	-1	0	0	-2	-3
															2	-4	-2	4	2	4	-4	0	-4	-4
																				1	-2	-1	2	1
1	-2	-1	2	1	0	2	2	-6	-4	-4	6	1	4	6	-4	0	-2	2	-4	6	-10	-1	-6	-3

のように計算していったのである。

この場合は $k=2$ であるから、 $p=2n+1$ であり 1,3,5,7,9,11,13,15,17,19,... が対応し、素数の部分を太字(bold face)で記しておいた。

[3, -2], [5, -1], [7, 2], [11, 0], [13, 2], [17, -6], [19, -4], [23, 6], [29, 6], [31, -4], [37, 2], [41, 6], [43, -10], [47, -6], [53, -6], [59, 12], [61, 2], [67, 2], [71, -12], [73, 2]
最初の 14 個の奇素数に対応している。

現在では、このような操作は比較的簡単に計算できるが、記憶容量の少ない当時の計算機では数値やプログラムを能率よく配置することに心を使う必要があったのである。

試みに、現在の古い形の計算機で計算してみたが 2 分程度で $p \approx 40000$ まで計算できたのでやはり隔世の感がある。(少し気の利いた計算機なら、実行時間は秒の単位、あるいはそれ以下、であろう)

広瀬健さんや島内剛一先生、そして米田信夫先生が存命であつたらどんな感想を述べたであろうか。

兎も角、14000 までの結果から、 $x^2 - a_p x + p = 0$ の複素根の分布の様子を見るため、佐藤先生は、掲示をだして 2 人の学生を雇った。50×80(cm)位のグラフ用紙に複素根を plot して

もらうことにして、実行に移したのである。

恐らくそれは、仕事量が多く大変な注意を要すので学生が音を上げて、完成しなかったのではないと思う。私が記憶しているのは、計算機演習室の大きな机の上にグラフ用紙を広げ、学生達が根の最初の部分から書き始めた時の風景の所までである。グラフ用紙の中心を原点にしたか底辺上が原点だったか…どこにしたか。何か、あやふやな形で立ち消えになったのであろうか…政治家ではないが、アルバイト料は支払われたかなど…記憶がハッキリしない。

ここでも、既に、恐らくは昨日まで明白であったことが、今日には記憶のゆらぎの裡に消えようとしていることが解る。現実には明白でないことを明白だと思い込んでいたのかも知れない。危険なことである。

しかし、確かなことは、そう言った周辺の状況の設定を少しずつでも積み重ね、試みて行くことが **time scale** の長い計画には必要だという事実(経験)である。

私は、文明や個人の記憶や記録は、鋸歯状波(saw teeth wave)のような形をしていると思っている。ゆっくり時間をかけて登り、急激に(登った量より多く)落ちる。

房総沖の海底ではないが、通常はゆっくり沈み込むように振る舞い、地震のとき一気に大きく隆起して、平均的には隆起するという様な状態が、記憶や記録でもおこっていると思うのである。(ほとんどの時間でおこっていることが、大局的な傾向と信じてはならない)

つまり、通常は知識の量は増加の傾向にあると、個人的には信じて(思い込んで)いるのであるが、事実は減少しているという事があり得るということである。それは、個人の物理的な理由(死とか痴呆など病的な理由等々)によって、情報が一気にしかも大量に失われるからである。

しかもそれは、絶対に避けることができない形で、かつ(and)“失われた”という認識が(物理的に、当然、精神的にも)なされない形で、実行(失われる)ということである。認識可能性と事実の間には本質的な差があるということである。

文明(ある時代の文化の担い手の総体)の場合にも、例えば、秦の始皇帝の焚書とか、戦争、独裁、自然災害、など、何度もそういうものを体験して(あるいは、しようとして)いる。そして恐らくは我々の文明の“発展それ自体”による文明の自己消滅に至るであろうが、文明はそれ自身の消滅を(認識主体が消滅しているから、あるいは認識力の低下によって)認識できないのではないかと思う。

通常、この部分は(出来れば避けたいとか、考えたくない状況として)精神的に隠蔽され易いのである。勿論、事実は隠蔽されないで実現される。

話は戻って、

次のグラフは、

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

に対応する、楕円母数形式の2次方程式の根を(学生アルバイトではなく計算機が)表示したものである。次のものは、 $f(x)=x(x^2+x-1)$ とし $(f(x)/p)$ を Legendre 記号として、和

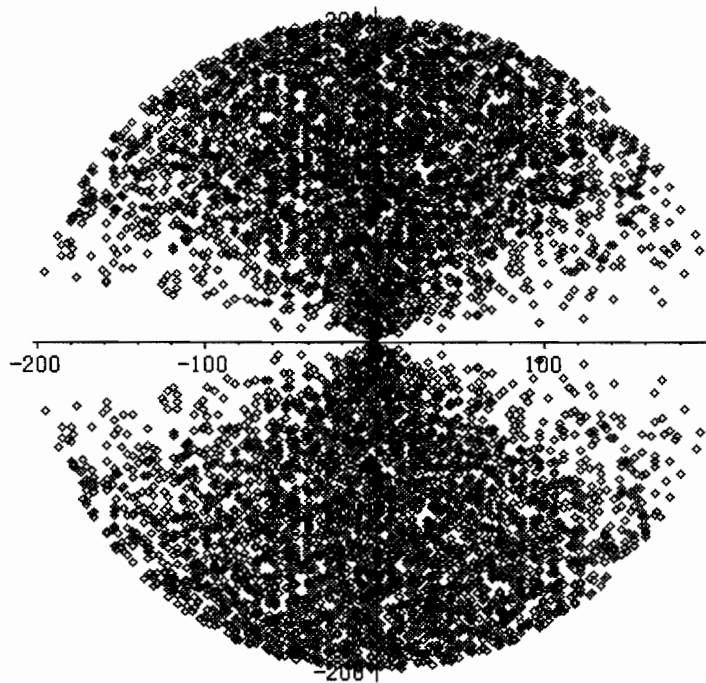
$$a_p = \sum_{x \in \mathbb{F}_p} (f(x)/p)$$

から、計算したものである。符号を除いて一致していることが解るであろう。

[3, -2], [5, 1], [7, 2], [11, 0], [13, -2], [17, 6], [19, -4], [23, 6], [29, -6], [31, -4], …

$$\eta(\tau)^2 \eta(5\tau)^2, p = 3 \sim 39989$$

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



ここでは、現代数学史の話としてであるから。少し、私的なものも含め、視点と資料を提示しようと思う。恐らく、他の人々はもっと沢山の、見方や資料をもっているものと思う。それらの総体は、この予想、つまり \sin^2 -予想がその端っこに位置するような数学的な文脈の真の姿を浮かび上がらせることであろうと思う。

最初のものは、佐藤先生が、計算してみようと思っていた

$$(\eta(\tau) \eta(m\tau))^n$$

の表で、それらの関数が、線で囲まれたり、波線が引かれたり、あるいはスミと書かれたり、?と記入されたものもある。これらの記入は相当長い期間に亘っていると思うが、 \sin^2 -分布、をまだ、確定的には想定しておらず、一様分布と点分布の他の分布の類型が何個にしばられるか…、あるいは極めて小数、つまり唯一つ、ということがあり得るかと思いをめぐらせていたときのものであろう。

この下半分は、佐藤先生が、更に一般の場合

$$(\eta(\tau) \eta(m\tau) \eta(n\tau) \eta(mn\tau))^{k/2}$$

$$1+n+m+nm = (1+n)(1+m) \mid 24$$

についても、手計算で計算して、具体的に解を求め、一つずつ当たって検討していることが解る。

$$\eta(x)^2 \eta(5x)^2 = 1 - 2x - x^2 + 2x^3 + x^4 + 0x^5 + 2x^6 + 2x^7 - 6x^8 - 4x^9 - \dots$$

に対応して、対応する楕円曲線

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

の判別式、 $\det(\text{res}(x(x^2+x-1), 3x^2+2x-1, x)) = -5$ であるから、2, 5 を除いた素数に対し
 $3, -1+\sqrt{2} \quad 7, 1+\sqrt{6} \quad 11, 0+\sqrt{11} \quad 13, 1+2\sqrt{3} \dots$

と(勿論)正しい結果を記している。むしろ、このような手計算の結果を参照しながら、計算機での結果と照合しながらプログラムが正しく書かれ、計算が誤りを含まない(であろう)ことを検証しながら計算を進めていったのである。

次のものは、HIPAC103 の printer での出力の例である。計算機は共同利用であったから、機械を長い時間占有することはできず、次はこの部分などと定めて実行し、計算結果を大抵は朝に佐藤先生が計算機室に取りに来られたときに手渡す。ふむふむ、と言いながら受け取って、その場で二三計算したり、上のメモに(当面の計算)の結果の検討をして、とんでもない分布とか、新しい種類の分布でなければスミと記したものでしょう。このメモの記入の終わり頃には、 $\sin, \sin^2, \sin^3 \dots$ のどれか、対称な分布の両端のあたりの減少ぐあいなど思いは一つの方向に向かっていったと思われる。

次の資料は、昭和 38 年 3 月 18 日付の速達です。これにはこの予想については書かれていない。しかし、次のはがきの表面に逆さまの向きに書かれた部分に

数日前に永島君 $1/2(a_p + \sqrt{a_p^2 - 4p})$ の角分布を出してくれました。

大体思った通りのものになったようです。役に立つ結論がでそうです。
と書かれています。これらの文面から、3 月の中旬には大体 \sin^2 -conjecture は固まっていたと思われます。他の類型と、虚数乗法をもつときの一様分布と点分布の話など、…では、それは何故か、など、色々思いをめぐらせている様子が判ります。

恐らく、このときが実質的に \sin^2 -予想が生まれたときでしょう。このはがきは普通便で、消印がありません。その意味で、昭和 38 年 3 月 18 日の速達の日付は昭和 38 年=1963 年という時期を明確に示しているのです。

次の、5 月 13 日、大阪大学理学部から、昭和 38 年 5 月 15 日消印のものは、肉眼で普通に見ると 38 の部分はもう読みとれません。現在の複写機の性能が優れているので 8 の字は読めますが、以前、東大の数理科学研究科にいた頃に撮った複写では、封書の色も茶色なのでこれは読みとれなかったのです。(複写したものから、8 であることを知って見ると明らかに読める)

この 2 枚目に

図と表から推定されるように、

α_p の角分布が $\sin^2 \theta$ に比例する。

という仮説は極めて確からしいと言えます。

と、書いて波線をしてあります。恐らく、この数日前には、ハッキリとこの予想を

$\sin^2 \theta$ -予想

として、発表することを決めたのだらうと思われます。

また、最後の計算機のタイプライター出力紙の裏に

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

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

と、大きな \sin^2 の曲線と、その下に

$$\boxed{\sin^2 \theta}$$

のように四角く囲い、その下にペンで何本もの波線を引いています。この用紙が、何月何日の時点で書かれたものかわかりません。

しかし、これは、佐藤先生が、例の分布が $\sin^2 \theta$ になるに違いないことを確信して、大きな机、恐らくは応用数理学科の計算準備室で、私も交えて、岩村聯先生と秋月康夫先生に予想に至った経緯を説明したときの用紙だと思います。

14000 と 1650 という数字が見えますが、これは、計算機でギリギリの 14000 までの素数で確かめたこと。そこまでに 1650 個の素数について分布をとって調べたことなどについて話ながら、 $\boxed{\sin^2 \theta}$ の下に波線を何度も書いています。そのとき、其処にいた人々の心の動きをその場で見ているような感じになります。

ですから、これは 5 月 15 日以降、佐藤先生が最初に東京教大学に出張して、岩村聯先生と秋月康夫先生に予想の背景など含めて話したときのもので、5 月 15 日からそんなに日は経っていないでしょう。

$$\frac{(m+1)n}{2+} = \frac{1}{N}$$

12 8 6 4 3 2 1
2 3 4 6 8 12 24

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

$m=1, 2, 3, 5, 7, 11, 23$

$$\eta = \begin{cases} 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 4 & 4 & 4 \\ 6 & 6 & 6 & 6 & 6 & 6 \\ 12 & 12 & 12 & 12 & 12 & 12 \end{cases}$$

$$N = \begin{cases} 12 & 8 & 6 & 4 & 3 & 2 & 1 \\ 6 & 4 & 3 & 2 & 1 & 1 & 1 \\ 4 & 3 & 2 & 1 & 1 & 1 & 1 \\ 3 & 2 & 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{cases}$$

$$\eta(\tau) \eta(\tau)$$

$$\begin{aligned} & \eta(\tau)^2 \cdot \eta(\tau)\eta(2\tau) \quad \eta(\tau)\eta(3\tau) \quad \eta(\tau)\eta(5\tau) \quad \eta(\tau)\eta(7\tau) \quad \eta(\tau)\eta(11\tau) \quad \eta(\tau)\eta(23\tau) \\ & \eta(\tau)^4 \cdot \eta(\tau)^2\eta(2\tau)^2 \quad \eta(\tau)^2\eta(3\tau)^2 \quad \eta(\tau)^2\eta(5\tau)^2 \quad \eta(\tau)^3\eta(7\tau)^3 \quad \eta(\tau)^2\eta(11\tau)^2 \quad \eta(\tau)^2\eta(23\tau)^2 \\ & \eta(\tau)^6 \cdot \eta(\tau)^2\eta(2\tau)^4 \quad \eta(\tau)^2\eta(3\tau)^4 \quad \eta(\tau)^2\eta(5\tau)^4 \quad \eta(\tau)^3\eta(7\tau)^3 \quad \eta(\tau)^2\eta(11\tau)^2 \quad \eta(\tau)^2\eta(23\tau)^2 \\ & \eta(\tau)^{12} \cdot \eta(\tau)^2\eta(2\tau)^8 \quad \eta(\tau)^2\eta(3\tau)^8 \quad \eta(\tau)^2\eta(5\tau)^8 \quad \eta(\tau)^3\eta(7\tau)^3 \quad \eta(\tau)^2\eta(11\tau)^2 \quad \eta(\tau)^2\eta(23\tau)^2 \\ & \eta(\tau)^{24} \cdot \eta(\tau)^2\eta(2\tau)^{16} \quad \eta(\tau)^2\eta(3\tau)^{16} \quad \eta(\tau)^2\eta(5\tau)^{16} \quad \eta(\tau)^3\eta(7\tau)^3 \quad \eta(\tau)^2\eta(11\tau)^2 \quad \eta(\tau)^2\eta(23\tau)^2 \end{aligned}$$

$$Q(\sqrt{7})$$

$$Q(\sqrt{11})$$

$$(\eta(\tau)\eta(m\tau))^2 = \frac{1}{q^{\frac{1}{N}}} (1 + a_1 q + a_2 q^2 + \dots) = \frac{1}{q^{\frac{1}{N}}} + a_1 \frac{1}{q^{\frac{N+1}{N}}} + a_2 \frac{1}{q^{\frac{2N+1}{N}}} + \dots = \sum_{\nu=1}^{\infty} a_{\nu} \frac{1}{q^{\frac{\nu}{N}}}$$

$$a_{\nu} = a_k, \quad \nu = kN+1$$

Step mN

$$(\eta(\tau)\eta(m\tau)\eta(n\tau)\eta(mn\tau))^2$$

$m=2, n=3, R=2, N=2$

$$\frac{1}{1+3^{-5}} \prod_{p \neq 2,3} \frac{1}{1 - c_p p^{-2} + p^{1-2s}}$$

$$p \neq 2,3 \quad \frac{1}{2}(c_p + \sqrt{c_p^2 - 4p})$$

5	$-1 + 2\sqrt{-1}$
7	$0 + \sqrt{-1}$
11	$2 + \sqrt{-1}$
13	$-1 + 2\sqrt{-3}$
17	$1 + 4\sqrt{-1}$
19	$-2 + \sqrt{-15}$
23	$-4 + \sqrt{-7}$
29	$3 + 2\sqrt{-5}$
31	$4 + \sqrt{-15}$
37	$3 + 2\sqrt{-7}$
41	$-3 + 4\sqrt{-2}$
43	$2 + \sqrt{-37}$
47	$0 + \sqrt{-47}$

全左, $R=4, N=1$

$$\frac{1}{1+2^{-5}} \prod_{p \neq 2,3} \frac{1}{1 - c_p p^{-2} + p^{1-2s}}$$

$$p \neq 2,3 \quad \frac{1}{2}(c_p + \sqrt{c_p^2 - 4p^2})$$

5	$3 + \sqrt{-25}$
7	$-8 + 3\sqrt{-31}$
11	$6 + \sqrt{-5 \cdot 7 \cdot 37}$
13	$19 + 6\sqrt{-3 \cdot 17}$

$m=2, n=7, R=2, N=1$

$$\frac{1}{1+2^{-5}} \prod_{p \neq 2,7} \frac{1}{1 - c_p p^{-2} + p^{1-2s}}$$

$$p \neq 2,7 \quad \frac{1}{2}(c_p + \sqrt{c_p^2 - 4p})$$

3	$-1 + \sqrt{-2}$
5	$0 + \sqrt{-5}$
11	$0 + \sqrt{-11}$
13	$-2 + 3\sqrt{-1}$
17	$3 + 2\sqrt{-2}$
19	$1 + 3\sqrt{-2}$
23	$0 + \sqrt{-23}$
29	$-3 + 2\sqrt{-5}$

$m=3, n=5, R=2, N=1$

$$\frac{1}{1+3^{-5}} \prod_{p \neq 3,5} \frac{1}{1 - c_p p^{-2} + p^{1-2s}}$$

$$p \neq 3,5 \quad \frac{1}{2}(c_p + \sqrt{c_p^2 - 4p})$$

2	$\frac{1}{2}(-1 + \sqrt{-7})$
7	$0 + \sqrt{-7}$
11	$-2 + \sqrt{-11}$
13	$-1 + 2\sqrt{-3}$
17	$1 + 4\sqrt{-1}$
19	$2 + \sqrt{-15}$
23	$0 + \sqrt{-23}$
29	$-1 + 2\sqrt{-7}$

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

$$\frac{1}{1+5^{-5}} \prod_{p \neq 2,5} \frac{1}{1 - c_p p^{-2} + p^{1-2s}}$$

$$p \neq 2,5 \quad \frac{1}{2}(c_p + \sqrt{c_p^2 - 4p})$$

3	$-1 + \sqrt{-2}$
7	$1 + \sqrt{-2}$
11	$3 + \sqrt{-11}$
13	$1 + 2\sqrt{-3}$
17	$-3 + 2\sqrt{-2}$
19	$-2 + \sqrt{-15}$
23	$3 + 2\sqrt{-5}$
29	$3 + 2\sqrt{-5}$
31	$-2 + 3\sqrt{-3}$
37	$1 + 6\sqrt{-1}$
41	$3 + 4\sqrt{-2}$

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

$$\frac{1}{1+11^{-5}} \prod_{p \neq 11} \frac{1}{1 - c_p p^{-2} + p^{1-2s}}$$

$$p \neq 11 \quad \frac{1}{2}(c_p + \sqrt{c_p^2 - 4p})$$

2	$-1 + \sqrt{-1}$
3	$\frac{1}{2}(-1 + \sqrt{-11})$
5	$\frac{1}{2}(1 + \sqrt{-19})$
7	$-1 + \sqrt{-7}$
13	$2 + 3\sqrt{-1}$
17	$-1 + 4\sqrt{-1}$
19	$0 + \sqrt{-19}$

$$\text{理論: } \sum_{-4p < s < 4p} H(s^2 - 4p) \delta\left(z - \frac{1}{2}(s \pm \sqrt{s^2 - 4p})\right)$$

$$\frac{1}{\sqrt{s^2 - 4p}} \delta\left(z^2 - sz + p\right) \left(\frac{1}{z-p} - \frac{1}{z-\bar{p}} \right) = \frac{1}{2i} \frac{p - \bar{p}}{z^2 - sz + p}$$

半注 \sqrt{p} の
(四角) - (四角)

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

$$\begin{aligned} &+1.-2.-1.+2.+1.-0.+2.+3.-6.-4. \\ &-4.+6.+1.+4.+6.-4.-0.-2.+2.-4. \\ &+6.-10.-1.-6.-3.+12.-6.-0.+8.+12. \\ &+2.+2.-2.+3.-12.-12.+2.-2.-0.+8. \\ &-11.+6.+6.-12.-6.+4.+8.+4.+2.-0. \\ &+6.+14.+4.-6.+2.-4.-6.-6.+2.-12. \\ &-11.-12.-1.+3.+20.+0.-8.-4.+18.-4. \\ &+12.-0.-6.+6.-6.+20.-6.+4.-22.+12. \\ &+12.-10.-0.+18.-9.-4.-6.+2.-24.-12. \\ &-10.-4.-2.+0.+8.-12.+26.+4.+18.+8. \\ &-4.+12.-6.+6.-0.-16.+24.+10.-8.-4. \\ &-12.-10.+1.-6.+14.-0.-6.+6.-16.-24. \end{aligned}$$

$$q(\tau)^6 \text{ coefficients from n to } 767$$

$$\begin{aligned} &+1.-6.+9.+10.-30.+0.+11.+4...+0.-70. \\ &+18.-54.+48.+90.+0.-24.-60.+0.-110.+0. \\ &+71.+180.-78.+0.+130.-180.+0.-10...-30.+80. \\ &+121.+24.+0.+0.+110.+0.-10...-10...-70.+170. \\ &+0.+0.-68.+330.+0.-38.+420.+0.-180.-390. \\ &+0.-108.+0.+0.+0.-300.+98.+44...+110.+0. \\ &+410.-198.+0.+0.-510.+578.-540.+138.+0.-130. \\ &-430.+0.+511.+570.+0.+0.+13...+0.+50.-150. \\ &+0.+110.+0.-630.-550.+0.+0.-510.+250.+0. \\ &+351.+650.+162.-550.+420.+0.+0.+378.+0.+650. \\ &-798.-456.-780.+0.+0.+98.-330.+0.+150.+0. \end{aligned}$$

$$(q(\tau))^{12} \quad 1 \rightarrow 768$$

$$\begin{aligned} &+1.-12.+54.-38.-99. \\ &+540.-418.-648.+594.+836. \\ &+1056.-4104.-209.+4104.-594. \\ &+4256.-6480.-4752.-298.+5016. \\ &+17226.-12100.-5346.-1296.-9063. \\ &-7128.+19494.+29160.-10032.-7668. \\ &-34736.+8712.-22572.+21812.+49248. \\ &-46872.+67562.+2508.-47520.-76912. \\ &-25191.+67716.+32076.+7128.+38754. \\ &+36784.-51072.+45144.-122398.-53460. \\ &+11286.-27256.+57024.+122364.+98902. \end{aligned}$$

$$q(\tau)^8 q(2\tau)^8 \quad 0 \rightarrow 768.$$

$$\begin{aligned} &+1.-8.+12.+64.-210.-96. \\ &+1016.-512.-2043.+1680.+1092. \\ &+768.+1382.-8128.-2520.+4096. \\ &+14706.+16344.-39940.-13440.+12192. \\ &-8736.+68712.-6144.-34025.-11056. \\ &-50760.+65024.-102570.+20160.+227552. \\ &-32768.+13104.-117648.-213360.-130752. \\ &+160526.+319520.+16584.+107520.+10842. \\ &-97536.-630748.+69888.+429030.-549696. \\ &+472656.+48152.+208713.+272200.+176472. \\ &+88448.-1494018.+406080.-229320.-520192. \\ &+479280.+820560.+2640660.-161280.+827702. \\ &-1820416.-2075688.+262144.-290220.-104832. \end{aligned}$$

と分断することの理論を知りたいと言っていたので、譲るようと思つていましたが、その機会がなくて残念でした。僕は21日夜、一度大阪大学へ行き、引越の仕度をして、23日に一たん東京へどり、月末か4月はじめに引越すつもりです。もしお互いに都合がつけば、4月になってきみが東京に来るときに途中ででも、大阪でお目にかかりましょう。では いづれまた。



難
波

完
雨

样

岡山県総社市北溝

四〇七、九

所坑王果

佐藤

幹丈

208 20
201-0

難波完爾様

先日 おはかき有難。● 僕は 4月8日
(3月26日付)

の夜行で大阪へ移ります。さしあたり、ひと月
くらい暫定的に下宿にとまり、その間にもっと
適当な場所を決める予定です。この処、
気ぜあわしたため、もっと早く返事を書い
と思ひ乍らのびのびになつてしまいました。
君のたよりにある $7(5^2+7(5^2)^2$ の係数 a_p
についての注意は、 $a_p \equiv p+1 \pmod{6}$ (★
と言ひ ~~同式~~ 合同式からすぐ証明できま

一般に、この種の級数は $\prod_p \frac{1}{1 - a_p p^{-\frac{1}{2}} p^{-\frac{1}{4}}}$

の形になることを示しましたが、この分母は、 p を u とおけば、 $1 - a_p + p^{k-1}u^2$ で、 $\therefore \Delta = 0$ 即ち $u=1$ のときの $(1 - a_p + p^{k-1})$ についてはいろいろな合同式が成立ちます。上記の場合($k=2$)は、 $1 - a_p + p \equiv 0 \pmod{6}$ 、 (\oplus) の式(4)
 $\eta(7)^2 \eta(11)^2$ の場合は $1 - a_p + p \equiv 0 \pmod{11}$
 $\eta(7)^{24}$ の場合は $1 - a_p + p^{11} \equiv 0 \pmod{2 \cdot 691}$



郵便はがき

難波完爾様

岡山県総社市
北溝牛407-9

東京郡板橋已
成増七三五
峰村方
佐々木
貞

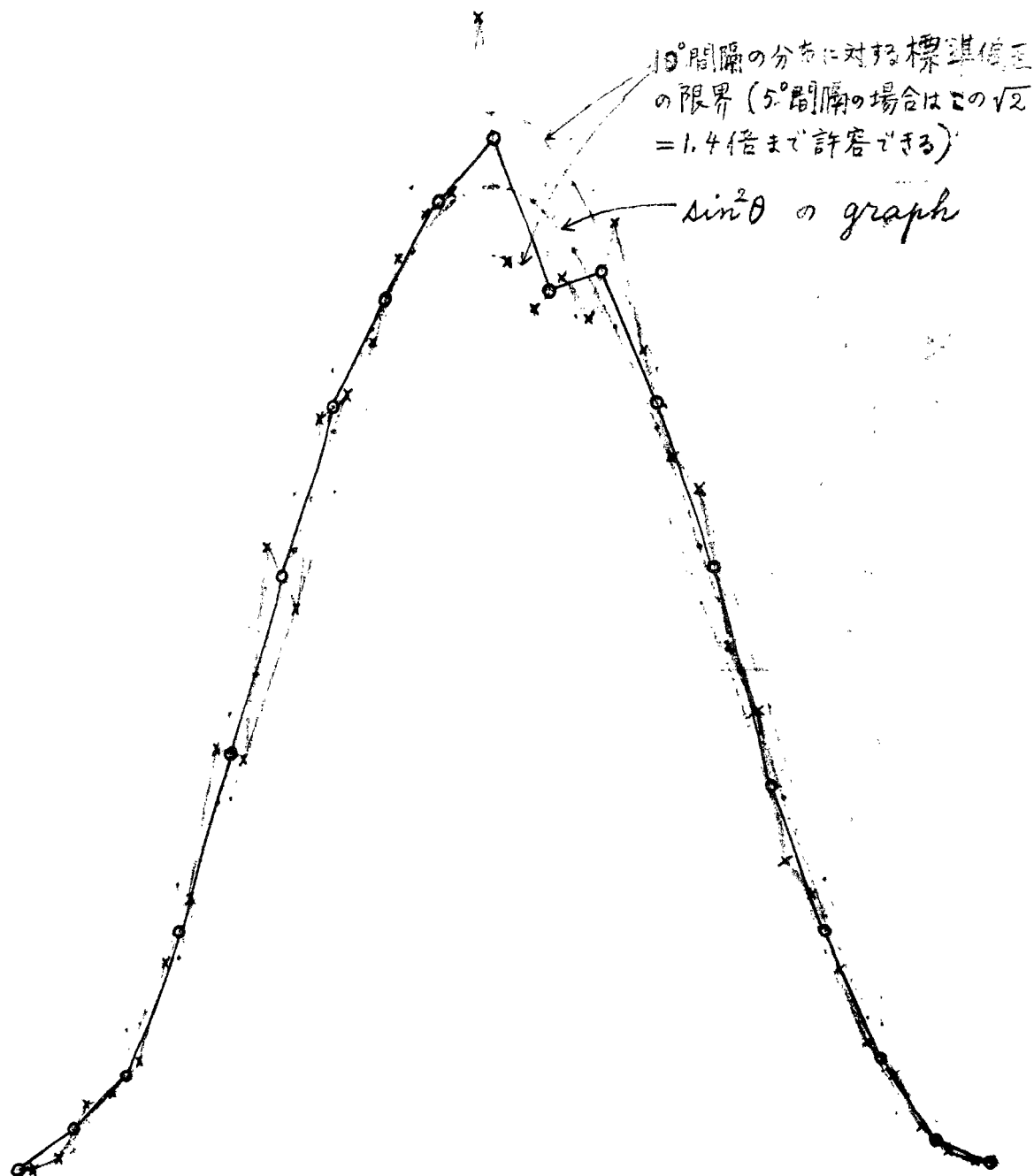
夫

といふことは、 $\frac{1}{2}(a+b+\sqrt{a^2+b^2})$ の角分布
 を出してゐた。大体思つた通りである。
 たゞ、後になつては、 $\frac{1}{2}(a+b+\sqrt{a^2+b^2})$
 といふ値が出てゐた。

7-8

	2507	3593	5717	7937	9211	2583	total		
0°- 5°	0	0	0	0	0	0	0	0	0.5
5°- 10°	0	0	0	0	1	0	1	1	
10°- 15°	1	0	2	0	1	0	6	7	6.0
15°- 20°	0	2	2	1	1	1	7	7	
20°- 25°	2	1	2	3	2	0	10	17	21.8
25°- 30°	3	3	5	2	4	2	19	19	
								44	46.0
30°- 35°	5	5	4	1	4	2	25	25	
35°- 40°	9	3	8	6	4	3	32	77	75.8
40°- 45°	3	9	3	6	5	8	42	42	
45°- 50°	10	3	6	8	11	14	58	110	107.5
50°- 55°	11	8	6	7	10	3	52	52	
55°- 60°	5	12	11	10	10	13	70	70	
								142	137.3
60°- 65°	11	16	10	10	11	11	72	72	
65°- 70°	11	9	15	10	11	13	77	162	161.5
70°- 75°	15	10	14	16	14	10	85	85	
75°- 80°	16	15	16	17	11	9	89	180	177.4
80°- 85°	16	15	16	7	15	12	91	91	
85°- 90°	12	21.5	8.5	22.5	16.5	18.5	107.5	107.5	
								192	182.9
90°- 95°	12	9.5	13.5	16.5	12.5	14.5	84.5	84.5	
95°-100°	13	8	13	12	12	16	80	163	177.4
100°-105°	7	10	16	9	14	18	83	83	
105°-110°	17	12	8	17	7	10	79	167	161.5
110°-115°	16	14	15	9	15	8	88	88	
115°-120°	12	11	15	11	3	16	76	76	
								142	137.3
120°-125°	7	10	8	9	15	10	66	66	
125°-130°	8	11	9	12	7	13	63	111	107.5
130°-135°	7	8	3	12	9	7	48	48	
135°-140°	8	7	4	6	9	3	42	70	75.8
140°-145°	5	6	4	2	6	3	28	28	
145°-150°	3	1	6	3	6	5	25	25	
								43	46.0
150°-155°	3	4	3	3	0	2	18	18	
155°-160°	1	3	2	0	3	3	11	19	21.8
160°-165°	1	1	1	2	1	2	8	8	
165°-170°	0	1	1	0	1	0	3	3	
170°-175°	0	1	0	0	0	0	1	1	6.0
175°-180°	0	0	0	0	0	0	0	0	0.5
TOTAL	250	250	250	250	250	250	150	1650	

$(\eta(\tau)^2 \eta(5\tau)^2)$ の q 展開の係数 a_p についての $\alpha_p = \frac{1}{2}(a_p \pm \sqrt{a_p^2 - 4p})$ の
 角分布。 $\circ-\circ-\circ$ は 10° 間隔の度数分布, $\times-\times-\times$ は 5° 間隔のそれ。



難波 完二様

5月13日

その後、元気のよいと思います。こちら、大阪へ移って、ひと月あまり経ち、だいぶ当地にも慣れてきました。大学の研究仲間についても、いま住んでいく下宿の環境についても、申分ないと思いますが、研究以外の雑用がふやみと多いのには、些か消耗しています。大学での勤務時間、かう言っても、実働量から言っても、教育大の先生達の、確かに2倍は、大学へ survive していると思います。

それは、さておき、同封するのは、3月に君が計算した例の、楕円曲線型式

$$\eta(\tau)\eta(5\tau)^2 = \sum_{n \equiv 1 \pmod{4}} a_n \tau^n \quad \text{の係数 } a_p \quad (p \geq 5; \quad p < 14000)$$

について、 $1 - a_p u + pu^2 = (1 - \alpha_p u)(1 - \bar{\alpha}_p u)$ と因数分解した

$$\text{とこの} \quad \alpha_p = \frac{1}{2}(a_p + \sqrt{a_p^2 - 4p}) = \sqrt{p} \cdot e^{i\theta_p} \quad (0 < \theta_p < 180^\circ)$$

の偏角 θ_p の分布を、水島君に実行して貰った結果に、少し整理を加えたものです。

第一表は、ii. は 水島君に作ってもらった data のコピー。

第二表は、第一列が $p=5, 7, 11, \dots$ 以下 250番目まで、第二列が $p=1607(251番目)$

から 500番目まで、最後の列が $p=12583(1501番目)$ から 13777(1650番目)まで。

Total の欄の右側は、角度を 10° 区切りに あらわした 場合の 度数分布。

一番左は、分布が $\sin^2 \theta$ に 比例するものと仮定して、各々の

sector における期待値を

$$\int_{-5^\circ}^{+5^\circ} \sin^2 \theta d\theta, \quad \int_{5^\circ}^{15^\circ} \sin^2 \theta d\theta, \quad \dots, \quad \int_{175^\circ}^{185^\circ} \sin^2 \theta d\theta$$

に 比例する ように 計算したものを。

グラフ の 方も、見れば 意味は 解るでしょう。この場合、実際の度数分布

を「確率変数」と見るとき、期待値のずれの大きさを示す標準偏差と真値を示しておきました。(これは、正しくは二項分布を使って算出すべきだが、近似的に Poisson 分布で代用する。そうすると、図中の平均値 $N (= \frac{1650}{180} = 9.17)$ とすると、期待値の曲線は $2N \cdot \sin^2 \theta$ 、標準偏差は $\sqrt{2N \cdot \sin^2 \theta} = \sqrt{2N} \cdot \sin \theta$ 従って真値の曲線は $2N \cdot \sin^2 \theta \pm \sqrt{2N} \cdot \sin \theta$ となる)

図と表とから推定されるように、

α_p の角分布が $\sin^2 \theta$ に比例する。

と云う仮説は 極めて確からしいと言えよう。このことは、落着いて充分時間をかけて考えれば、現在の我々の能力でも たいへん理論的に説明できるだろう、と思うのですが、いま差当っては そのような heavy な頭脳労働は気が重いのぞ、それはしばらく後述しにして、もう少しというところ、筋肉労働で実行する資料収集もしたいと考えています。そのために、阪大の計算機も利用出来るなら利用したいと思つて、少しそちらの方に さぐりを入れている所です。土井君はじめ、阪大の若い人達もこのプランには 相当乗氣でいます。

「数理科学」に載せるための原稿も そのうち書くつもりです。書き上げたら、あと、計算のプログラムに關することと君に書き足してもらふと思つてゐる。いつかにせよ、なまじく学会のときまでには 或程度 目鼻をつけたいと思つてゐる。

$\eta(\pi)^2 \eta(5\pi)^2$ 以外の方、つまり $\eta(\pi)^2 \eta(14\pi)^2$, $\eta(\pi)^4 \eta(5\pi)^4$, $\eta(\pi)^4 \eta(2\pi)^4$, $\eta(\pi)^8 \eta(4\pi)^4$

$\eta(\pi)^{12}$, $\eta(\pi)^{24}$ など、についても、永島君の Program を使つて、 α_p の分布表を作つてくれないか。僕の予想では、これらはすべて 上の同じ $\sin^2 \theta$ 型に従うだろうと、期待しているのですが。

$n \gg 14000$ 超 n について、全然別つた法で α_p を求めらることに、~~君~~ 最近にちよと会つたとき話したことが、あつた memory ~~容量~~ 容量が (命令の分は外は) 86 人必要なので、試作中の HITACHI 5020 を利用させて貰ふことが出来れば、あつたところから、更に更に出来れば plan を準備したいと思つてゐます。

他にもいろいろ著書があることがありますが、時間がないので、この位にし
て置きます。本書に少し書いたが、右村先生や竹内先生によろしく。水島君
にも別に手紙とかいってありますが、どうぞよろしく伝えて下さい。

佐藤幹夫

東京大学理学部 数学科
東京大学理学部 数学科
難波 完二 様

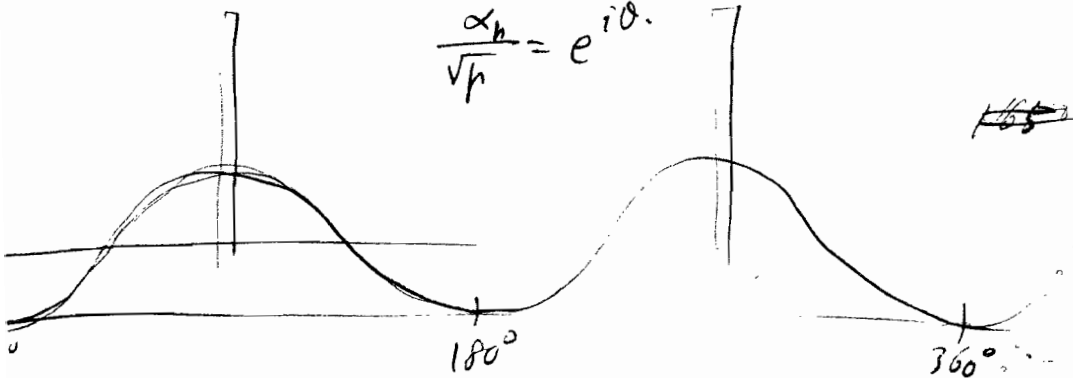


東京大学理学部 数学科

佐藤幹夫

$$1 - a_h u + \mu u^2 = (1 - \alpha_h u)(1 - \bar{\alpha}_h u) \quad |y_h| = |\bar{\alpha}_h| = \sqrt{\mu}$$

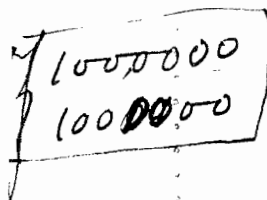
$$\frac{\alpha_h}{\sqrt{\mu}} = e^{i\theta}$$



0



14000



$$k=6. \quad \gamma(\tau)^{1/2}$$

$$k=8 \quad \gamma(\tau)^8 \gamma(2\tau)$$

$$k=12 \quad \gamma(\tau)^{12}$$

$$k=2 \quad \frac{a_h}{\sqrt{\mu}} \left\{ \begin{array}{l} \gamma(\tau)^2 \gamma(5\tau)^2 \\ \gamma(\tau)^2 \gamma(11\tau)^2 \\ \gamma(\tau)^2 \gamma(2\tau)^2 \end{array} \right.$$

$$\frac{a_h}{\sqrt{\mu} k+1} \quad k=4$$

$$\left\{ \begin{array}{l} \gamma(\tau)^4 \gamma(5\tau)^4 \\ \gamma(\tau)^4 \gamma(2\tau)^4 \\ \gamma(\tau)^4 \end{array} \right.$$

~~165~~
mm

3. 計算例

以前にも述べたように関数

$$\begin{aligned} &\eta(\tau)^2, \eta(\tau)\eta(2\tau), \eta(\tau)\eta(3\tau), \eta(\tau)\eta(5\tau), \eta(\tau)\eta(7\tau), \eta(\tau)\eta(11\tau), \eta(\tau)\eta(23\tau) \\ &\eta(\tau)^4, \eta(\tau)^2\eta(2\tau)^2, \eta(\tau)^2\eta(3\tau)^2, \eta(\tau)^2\eta(5\tau)^2, \eta(\tau)^2\eta(7\tau)^2, \eta(\tau)^2\eta(11\tau)^2 \\ &\eta(\tau)^6, \eta(\tau)^4\eta(2\tau)^4, \eta(\tau)^3\eta(3\tau)^3, \eta(\tau)^4\eta(5\tau)^4 \\ &\eta(\tau)^8, \eta(\tau)^8\eta(2\tau)^8, \eta(\tau)^6\eta(3\tau)^6 \\ &\eta(\tau)^{12} \\ &\eta(\tau)^{24} \end{aligned}$$

や、今少し複雑な

$$\begin{aligned} &\eta(\tau)\eta(2\tau)\eta(3\tau)\eta(6\tau), \eta(\tau)\eta(2\tau)\eta(7\tau)\eta(14\tau), \eta(\tau)\eta(3\tau)\eta(5\tau)\eta(15\tau) \\ &(\eta(\tau)\eta(2\tau)\eta(3\tau)\eta(6\tau))^2 \end{aligned}$$

について、以下に簡単に分布の型を記しておく。

1 は一様分布、 $\pi/2, 0$ は $\theta = \pi/2, 0$ の点分布、つまり実数と純虚数、 $\sin^2\theta$ は sine-square 分布である。

$$k = 2$$

$$x^2 - a_p x + p^{k-1} = x^2 - a_p x + p = 0$$

$\eta(\tau)^4$	$\eta(\tau)^2\eta(2\tau)^2$	$\eta(\tau)^2\eta(3\tau)^2$	$\eta(\tau)^2\eta(5\tau)^2$	$\eta(\tau)^2\eta(11\tau)^2$
$p = 6n+1$	$p = 4n+1$	$p = 3n+1$	$p = 2n+1$	$p = n+1$
1	1	1	$\sin^2\theta$	$\sin^2\theta$

$\eta(\tau)\eta(2\tau)\eta(3\tau)\eta(6\tau)$	$\eta(\tau)\eta(2\tau)\eta(7\tau)\eta(14\tau)$	$\eta(\tau)\eta(3\tau)\eta(5\tau)\eta(15\tau)$
$p = 2n+1$	$p = n+1$	$p = n+1$
$\sin^2\theta$	$\sin^2\theta$	$\sin^2\theta$

$$k = 3$$

$$x^2 - a_p x + p^{k-1} = x^2 - a_p x + p^2 = 0$$

$\eta(\tau)^6$	$\eta(\tau)^3\eta(3\tau)^3$	$\eta(\tau)^3\eta(7\tau)^3$
$p = 4n+1$	$p = 2n+1$	$p = n+1$
1	1	$1+0^*$

$$k = 4$$

$$x^2 - a_p x + p^{k-1} = x^2 - a_p x + p^3 = 0$$

$\eta(\tau)^8$	$\eta(\tau)^4\eta(2\tau)^4$	$\eta(\tau)^4\eta(5\tau)^4$
$p = 3n+1$	$p = 2n+1$	$p = n+1$
1	$\sin^2\theta$	$\sin^2\theta$

$(\eta(\tau)\eta(2\tau)\eta(3\tau)\eta(6\tau))^2$
$p = n+1$
$\sin^2\theta$

$$k = 6$$

$$x^2 - a_p x + p^{k-1} = x^2 - a_p x + p^5 = 0, p^3 x^2 - a_p x + p^3 = 0$$

$\eta(\tau)^{12}$	$\eta(\tau)^6 \eta(3\tau)^6$
$p = 2n+1$	$p = n+1$
$\sin^2\theta$	$\sin^2\theta$

$$k = 8$$

$$x^2 - a_p x + p^{k-1} = x^2 - a_p x + p^7 = 0, p^3 x^2 - a_p x + p^4 = 0$$

$\eta(\tau)^8 \eta(2\tau)^8$
p
$\sin^2\theta$

$$k = 12$$

$$x^2 - a_p x + p^{k-1} = x^2 - a_p x + p^{11} = 0, p^4 x^2 - a_p x + p^6 = 0$$

$\eta(\tau)^{24}$
p
$\sin^2\theta$

特に、 $\eta(\tau)^{24}$ に対応する 2 次多項式

$$x^2 - a_p x + p^{11}$$

の 1 での値については神秘的約数 $p = 691$ や、 $2/3$ 以上での $p = 23$ が知られている。

$$1 - a_p + p^{11}$$

p	a_p	$1 - a_p + p^{11}$
2	-24	$3 \cdot 691$
3	252	$2^8 \cdot 691$
5	4830	$2^{10} \cdot 3 \cdot 23 \cdot 691$
7	-16744	$2^9 \cdot 3^3 \cdot 23 \cdot 691$
11	534612	$2^8 \cdot 3 \cdot 5^3 \cdot 11 \cdot 17 \cdot 23 \cdot 691$
13	-577738	$2^{10} \cdot 3^5 \cdot 7 \cdot 691 \cdot 1489$
17	-6905934	$2^{11} \cdot 3^2 \cdot 23 \cdot 691 \cdot 116993$
19	10661420	$2^8 \cdot 3^6 \cdot 5^2 \cdot 23 \cdot 691 \cdot 1571$

また、同一判別式に属する

$$px^2 - a_p x + p^{10}$$

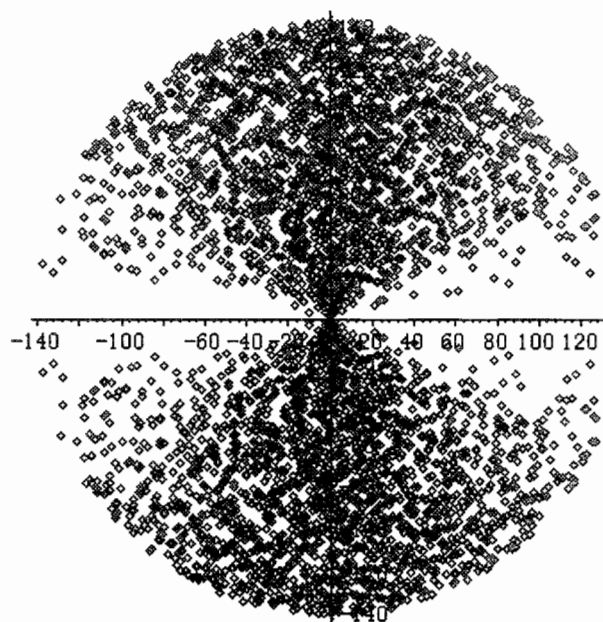
の奇素数 p に関する 1 での値の共通因数 $8400 = 2^4 \cdot 3 \cdot 5^2 \cdot 7$ など知られている。

勿論、この場合も、偏角の分布は $\sin^2 \theta$ である。次のグラフは、

$$p^5 x^2 - a_p x + p^6 = 0$$

に関するもので、偏角の分布は元のものと同じで、見やすいように絶対値は \sqrt{p} となっている。

$$p = 2, 3, \dots, 19997$$



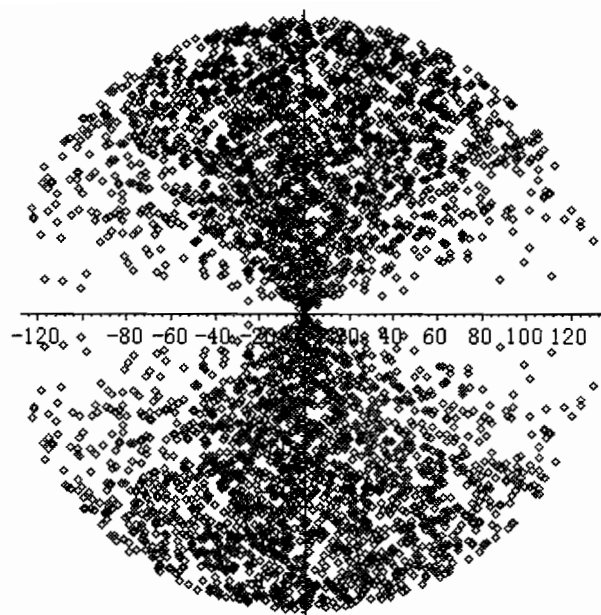
また、 $k = 6$ に属する

$$\eta(\tau)^6 \eta(3\tau)^6$$

がある。これも $\sin^2 \theta$ に比例するのであろうか。その通りである。

$$p^3 x^2 - a_p x + p^3 = 0$$

$$p = 2, 3, \dots, 18097$$

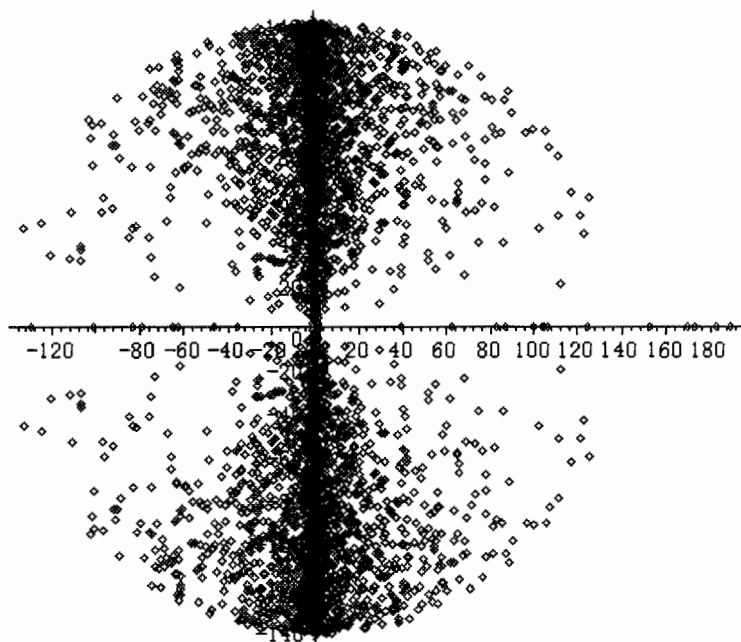


例えば、次のグラフは

$$\eta(\tau)^6 \eta(3\tau)^6 = x \sum b_n x^n = \sum a_n x^n$$

とした場合の、 $p = n+1$ が素数(従って n は素数でない)の場合の a_n についての偏角の分布である：

$$n^2 x^2 - a_n x + n^3 = 0$$



当然のことであろうが、この偏角の分布は $\sin^2 \theta$ とは明らかに異なる。

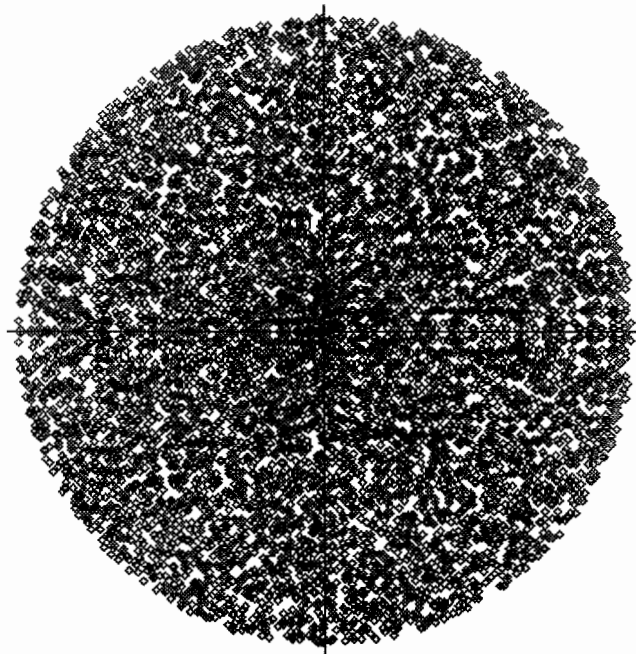
最初、 x を乗ずることを忘れ、従って $p = n+1$ に於いて、 p の代わりに n が素数と考え、この(美しい?)分布をみてハッと驚き、まさか…と反省したのである。手書きの佐藤先生の?の記号の意味はこのことかと思ったりしたのであるが、冷静に計算し見直すと、やはり!… $\sin^2 \theta$ なのであった。

一様分布になる例として、(どれでも良いのであるが)

$$\eta(\tau)^6, \eta(\tau)^2 \eta(2\tau)^2$$

の graph を示しておく。例えば $\eta(\tau)^6$ の場合 2 次方程式は $x^2 - a_p x + p^2 = 0$ であるが、そのままでは解が原点の近くに集中するので、解の偏角を変えず、絶対値が \sqrt{p} になるようにして表示した。

$$\begin{aligned} & \eta(\tau)^6 \\ & \sqrt{p}x^2 - a_p x + p^{3/2} = 0 \\ & p = 5 \sim 79997, k = 3, p = 4n+1 \end{aligned}$$



この場合、 a_p に関する $[p,]$ の表の最初の部分は

$$\begin{aligned} & [[5, -6], [13, 10], [17, -30], [29, 42], [37, -70], [41, 18], \\ & [53, 90], [61, -22], [73, -110], [89, -78], [97, 130], \dots \end{aligned}$$

のようであり、例えば $p = 53 = 13 \cdot 4 + 1$ の場合は

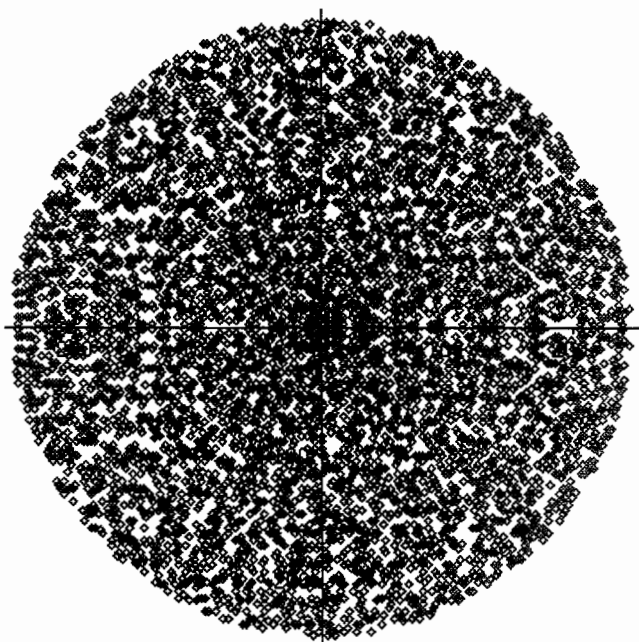
$$x^2 - 90x + 53 = (x-45)^2 + (53-45^2) = (x-45)^2 + 28^2 = 0$$

であり、解は Gauss 整数である。つまり $4n+1 = p$ の平方和の表示を意味している。

$$\eta(\tau)^2 \eta(3\tau)^2$$

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

$$p = 3 \sim 59971, k=2, p = 3n+1$$



$p = 3n+1$ に対する $[p, a_p]$ の表の最初の部分は

$$[[7, -1], [13, 5], [19, -7], [31, -4], [37, 11], [43, 8],$$

$$[61, -1], [67, 5], [73, -7], [79, 17], [97, -19], \dots$$

のようである。例えば、 $67 = 22 \cdot 3 + 1$ の場合は

$$x^2 - 5x + 67 = (x - 5/2)^2 + 3(9/2)^2$$

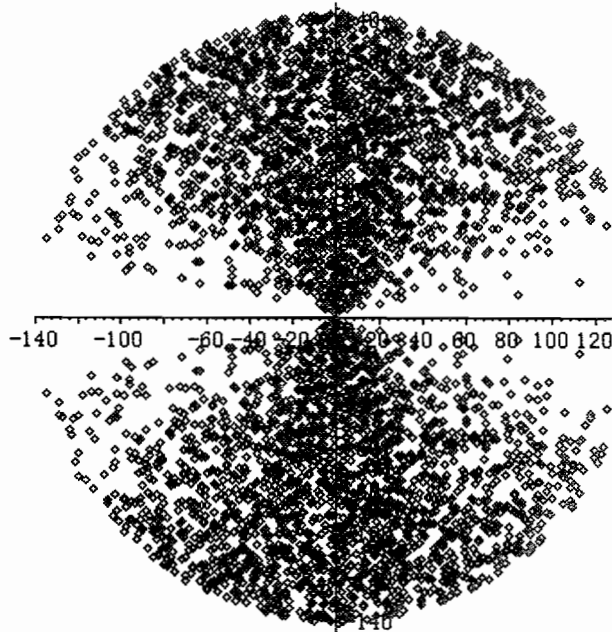
のように、 $p = 3n+1$ 、つまり 3 で割ると 1 余る整数を Eisenstein の整数 $Z((1+\sqrt{-3})/2)$ の norm として表現することを意味している。従って、上の二つのグラフは Gauss 整数と Eisenstein 整数の分布図そのものである。

後半の $\eta(\tau)^2 \eta(3\tau)^2$ について、目の錯覚かも知れないが、-140 のあたりに始まり、-250 のあたりを中心とする円弧の上に、とびとびの規則的な小さな間隙が見えるが、これは当然な現象であろうか。

$$\eta(\tau)\eta(3\tau)\eta(5\tau)\eta(15\tau)$$

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

$$p = 3 \sim 19997, k = 2, p = n+1$$



この分布も勿論 $\sin^2 \theta$ に比例すると予想される。

ここで述べた $\eta(x)$ から計算した全ての場合の解の分布は、ここには載せてないが、すべて 20000 までの素数までは確かめたのが上記の表である。

余談であるが、 $\eta(x)^{24}$ に対応する a_p 及び 2 次式

$$1 - a_p + p^{11}$$

の $x = 1$ での値については、100 までの範囲で(美しい表示ではないが)

$$[p, 1 - a_p + p^{11}]$$

[2, 3·691], [3, 2⁸·691], [5, 2¹⁰·3·23·691], [7, 2⁹·3⁵·23·691], [11, 2⁸·3·5³·11·17·23·691],
 [13, 2¹⁰·3⁵·7·691·1489], [17, 2¹¹·3²·23·691·116993], [19, 2⁸·3⁶·5²·23·691·1571],
 [23, 2⁹·3·23·691·39030947], [29, 2¹⁰·3·5²·7·691·32842837], [31, 2¹¹·3⁵·5³·691·591091],
 [37, 2¹⁰·3⁶·23·691·863·17377], [41, 2¹²·3·5³·7·17·691·1153·3779],
 [43, 2⁸·3⁵·7·13·23·691·10329029], [47, 2¹⁰·3·17·691·68505944237],
 [53, 2¹⁰·3³·23·503·691·1669·25127], [59, 2⁸·3·5²·11²·17·23²·691·2088829],
 [61, 2¹⁰·3⁵·5⁴·19·23·29·89·359·691], [67, 2⁸·3⁵·23·79·691·95561·16363],
 [71, 2⁹·3⁵·5⁴·7·29·691·572104367], [73, 2¹¹·3⁷·13²·19·107·691·295033],
 [79, 2¹⁰·3⁵·5²·23·103·691·73452851], [83, 2⁸·3·7·13·23·691·977·1186741027],
 [89, 2¹¹·3²·5²·23·691·378941106829], [97, 2¹¹·3⁴·7²·23·691·5475101·3371]]

である。20000 までに 2262 個の素数があり、 q が $1 - a_p + p^{11}$ の約数になるこの範囲での素数 p の個数は

[23, 1500], [691, 2262]

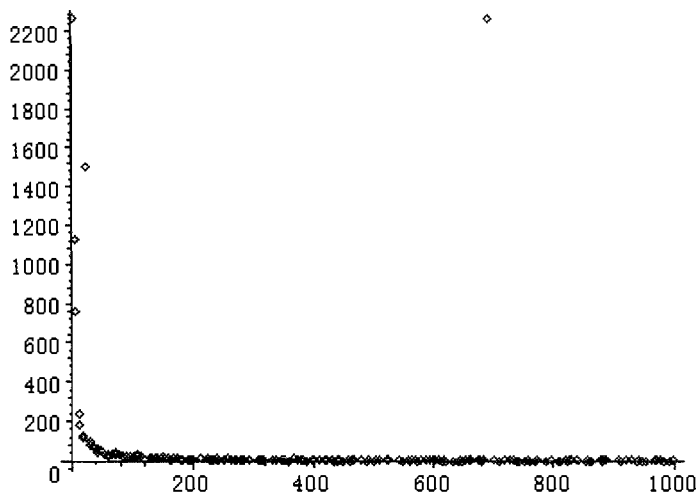
である。つまり、勿論 691 は全ての素数で当然であるが、 $q = 23$ は 1500 個あり、2, 3, 5, 7 というような小さい素数は別にすると特別な意味をもつてゐる。

$$1500/2262 = 0.6631299735 \approx 0.666 \cdots = 2/3$$

この密度は $2/3$ に収束するかどうかは(私は)知りませんが、23 と 691 の二つの数は特別の意味をもっていることは Ramanujan 以来知られていることです。

次のものはこの統計である。

$$\# \{q < 20000: p \mid 1-a_q+q^{11}\}$$



23, 691 の外の数はいはば逆数に比例していることが解る。

また、 $\zeta(2k)$ と関連してオイラー (Euler, 1734) によって

$$\zeta(2k)/\pi^{2k} = m/n = (-1)^{k-1} (2\pi)^{2k} / 2(2k)! \cdot B_{2k}$$

$$F(z) = ze^z/(e^z-1) = \sum_{k=0}^{\infty} B_k z^k/k!$$

であることが知られど、の既約分母 n の因数も $2k+1$ を越えないことが知られている。

$2k$	m	n
2	1	$6 = 2 \cdot 3$
4	1	$90 = 2 \cdot 3^2 \cdot 5$
6	1	$945 = 3^3 \cdot 5 \cdot 7$
8	1	$9450 = 2 \cdot 3^3 \cdot 5^2 \cdot 7$
10	1	$93555 = 3^5 \cdot 5 \cdot 7 \cdot 11$
12	691	$3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$
14	2	$3^6 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
16	3617	$2 \cdot 3^7 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$
18	43867	$3^9 \cdot 5^3 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19$
20	283・617	$3^9 \cdot 5^5 \cdot 7^2 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19$

3. 楕円曲線と解の個数

有限素体

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

で、曲線

$$C: y^2 = x^3 + qx + r$$

上の点の個数を考える。個数を#で記す。

(a/p) をルジャンドル (Adrien Marie Legendre) の記号とする。定義は、 a が体 F_p で 0 でない数の平方であるとき $(a/p) = 1$ 、 $a = 0$ のとき $(a/p) = 0$ 、そうでないとき $(a/p) = -1$ と定める。つまり、2 次方程式 $x^2 = a$ の F_p での解の個数から 1 を引いたものが Legendre symbol なのである。

$$(a/p) = a^{(p-1)/2} = 1/\sqrt{a} = \#x \in p (x^2 = a) - 1.$$

この式を $1/\sqrt{a}$ と記すことには抵抗があるが…。

現実には、その自乗は 0 または 1 で $1/a$ とは必ずしもならないのであるが、標数 (characteristic) 0 の体の平方根に非常に近い性質をもつるのでそのように記した。

この中央部分の式であるが、これはオイラー (Leonhard Euler) の式である。 F_p の定義方程式が

$$F_p = \{x : x^p - x = x(x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1) = 0\} = p$$

であることの別表現とも見ることができる。もう一つの、平方根の逆数という意味は指数について $(p-1)/2 = -1$ という体での関係式からの類推である。

例えば、有限体上の楕円曲線

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

について、 F_p では $(a/p) = 1/\sqrt{a}$ と“みなす”ことにして、式

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

を考える。C で定まるアーベル群 (Poincaré-Mordell group) の位数は、単位元である無限遠点を含めて

$$n_p = 1 + a_p + p$$

であり、この式は複素数体 \mathbb{C} のような標数 0 の体での所謂、完全楕円積分 (complete elliptic integral)、つまり楕円関数の周期を表す積分

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

に対応しており、“周期 = 群の位数”、という等式の標数有限のものと標数 0 での (おそらく) 同一概念の異なる表示なのであろうと思う。

一般的なこととして、角度の分布が $\sin^2 \theta$ に比例するということは、実部 $x = \cos \theta$ から見れば、 $y = \sqrt{1-x^2}$ に比例することということも出来るし、恐らく、もっと自然な見方は、ハミルトンの四元数 (Hamilton's quaternion) の (3 次元) 単位球 S^3 上の一様分布の実軸への射影の分布であらう。

いつの日か、 S^3 上を一様に覆う軌道の射影であるなどというような解釈が可能になるかも知れないというのは一つの夢である。

通常は、例えば、Weierstraß の標準形で表示された楕円曲線

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

などの有限素体 $F^p = GF(p)$ での解の個数に、加法の単位元である無限遠点を加えた個数

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

から定まる 2 次方程式

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

が実数解をもたないことは良く知られている。これは Hasse の不等式

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

とも、有限 Riemann 定理とも呼ばれている。ここでの主眼は、更に詳しくその角分布が、虚数乗法 (complex multiplication) をもたない場合は、 $\sin^2 \theta$ であろうと予想した訳である。

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

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

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

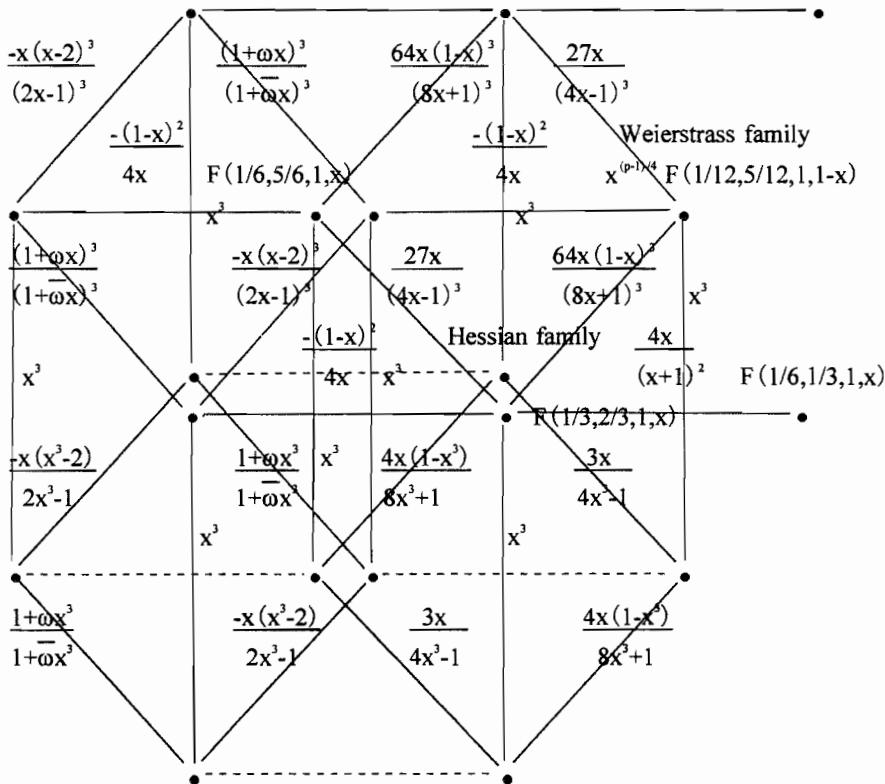
$$D: y^2 = x^3 + 1$$

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。

Legendre family

first complete elliptic integral

$$\begin{array}{llll} \text{Deuling polynomial} & \frac{-(1-x)^2}{4x} & \text{Euler family} & \frac{4x}{(x+1)^2} \\ F(1/2, 1/2, 1, x) & & F(1/4, 1/4, 1, x) & b_p(x) F(1/8, 5/8, 1, 1-x) \end{array}$$



上記、交換図式に表れる関数についてであるが、

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

に関する 4 次(有理式)の 2 倍射 (duplication map) [2] (x) と 9 次の 3 倍射 (triple map) [3] (x) の合成平方根 (a compositional square root) $[\sqrt{3}]$ (x) を含むものである。

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

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

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

点線の部分の有理関数は存在するのであろうか。

このような有理交換図式は、可解群 (solvable group) の正規列に対応して存在するであろう。上記の図式は、可解群が 4 次対称群 $S_4 = 4!$ の場合の有理関数の合成代数系である。

j-invariant $x = -27b^3/4a^2$ の関数 $a_p(x)$ については、有限素体の乗法群

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

での表現行列、つまり、i 行 j 列の元を $a_p(ij)$ とした行列 (ij は F_p^* での積)

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

の固有多項式が 0, 2, 4 個の $\pm\sqrt{p}$ の固有空間 (Gaussian and Eisenstein's integers, $p \neq -1 \pmod{12}$) 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。

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

table of characteristic polynomials

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

(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、探査等にも応用が可能であると思う。

先ず、 a_p を、楕円曲線

$$C: y^2 = x^3 + qx + r = f(x)$$

の j -不変量 (j -invariant) を変数 (variable) とみなして、 $z = j = -27r^2/4q^3$ の関数として

$$a_{12}(z) = \sum_{x \in p} (f(x)/p)$$

を表現することを考える。結果は、

$$\begin{aligned} a_{12}(z) &= x^{(p-1)/4} P_{(p/6)}(\sqrt{x}) \\ &= x^{(p-1)/4} F(1/12, 5/12, 1, 1-x) \text{ if } p \equiv 1 \pmod{4} \\ &= x^{(p+1)/4} F(7/12, 11/12, 1, 1-x) \text{ if } p \equiv -1 \pmod{4} \end{aligned}$$

である。勿論、この関数は有限体

$$F_p = p = \{0, 1, 2, \dots, p-1\}$$

で、絶対値最小剰余として計算する。

多項式としては $[p/12]$ 次の多項式に x の $[(p+1)/4]$ 乗を掛けたものであり、常に Hasse の不等式を充たしている。勿論、 $p = 13$ 以下の場合には直接計算する必要がある。

例 $p = 73$

この場合は、 $p = 73 = 12 \cdot 6 + 1$ であるから、 $p \equiv 1 \pmod{12}$ であり、

$$(p-1)/4 = 18, [p/12] = 6$$

である。Fuchs の関数の部分 $F(1/12, 5/12, 1, x)$ の係数は

$$\begin{aligned} 1/12 &= -6, 5/12 = -30 \\ 1 + (6 \cdot 30)x + (6 \cdot 5 \cdot 30 \cdot 29)x^2/2 + \dots \end{aligned}$$

と計算して、 $1/12 = -6$ であるから、勿論 x^6 の項で終わっている。つまり 6 次式である。具体的には、 F_n での計算で

$$6 \cdot 30 = 180 = 34, 34(5 \cdot 29)/4 = 28, \dots$$

と計算を進め、結果は x^n の係数列は

$$[1, 34, 28, 24, 12, -13, -7]$$

である。従って、

$$F(1/12, 5/12, 1, x) = 1 + 34x + 28x^2 + 24x^3 + 12x^4 - 13x^5 - 7x^6$$

であり、求める $a_{12}(x)$ は $F(1/12, 5/12, 1, x)$ の x に $1-x$ を代入したものと x^{18} の積

$$\begin{aligned} a_{12}(x) &= x^{18} F(1/12, 5/12, 1, 1-x) \\ &= x^{18} (-7x^6 - 18x^5 - 12x^4 - 21x^3 + 10x^2 - 30x + 6) \end{aligned}$$

である。次の列は $a_{12}(0), a_{12}(1), a_{12}(2), \dots$ を絶対値最小剰余として求めたものである。

$$\begin{aligned} &[a_{12}(x) : x = 0..72] \\ &[0, 1, -11, -13, -9, -16, -10, -8, 6, 9, -6, 7, -4, -4, 7, 11, 8, -2, 2, -10, \\ &4, 11, 6, -2, -14, -3, 4, 8, 0, 10, -14, -3, -14, 4, 1, 2, 11, 2, -13, 10, \\ &-7, 4, -14, 1, 2, -10, 10, -6, 2, 5, -6, 10, -6, 3, 4, -2, 14, -12, 4, 11, \\ &-1, 16, -14, -5, 0, -15, -12, -6, 8, -2, -1, -9, -7] \end{aligned}$$

Hasse の不等式は

$$|a_{12}(x)| < 2\sqrt{73} = 17.08800749$$

であるから、 ± 17 が限界であるが、上の数値では ± 16 が各々 1 回出ている。

また、Deuling によると $a_{12}(x)$ は F_p の 2 次拡大のなかでは完全に一次式の積に分解される、つまり、多項式環 (polynomial ring) $F_p[x]$ で高々 2 次の因子に分解されることが知られている。実際、この場合は

$$a_{12}(x) = 66x^{18}(x+9)(x+45)(x^2+9x+54)(x^2+23x+48)$$

である。

例えば、Euler family

$$E: y^2 = x(x^2+qx+r)$$

から、Weierstrass family

$$W: y^2 = x^3+qx+r$$

の関数変換

$$27x/(4x-1)^3 : F(1/4, 1/4, 1, x) \rightarrow x^{18}F(1/12, 5/12, 1, 1-x)$$

を考えてみよう。合成を \bullet で記すと、例えば因子 $x+9$ 、について、

$$\begin{aligned} x+9 \bullet 27x/(4x-1)^3 &= 27x/(4x-1)^3 + 9 = (64x^3 - 48x^2 + 15x - 1)/(4x-1)^3 \\ &= 64(x^2+64x+30)(x+63)/(4x-1)^3 \end{aligned}$$

$$\begin{aligned} (x^2+9x+54) \bullet 27x/(4x-1)^3 &= 27(8192x^6 - 12288x^5 + 8256x^4 - 2992x^3 + 615x^2 - 57x + 2)/(4x-1)^6 \\ &= 67(x^2+55x+60)(x^2+63x+55)(x^2+63x+14)/(4x-1)^6 \end{aligned}$$

となっている。ついでに

$$a_{12}(x) \bullet 27x/(4x-1)^3 = a_{12}(27x/(4x-1)^3)$$

の因数分解について記しておく、

$$\begin{aligned} 67x^{18}(x+68)(x+63)(x^2+64x+30)(x^2+25x+14)(x^2+55x+60)(x^2+12x+57) \\ (x^2+59x+60)(x^2+63x+55)(x^2+71x+31)(x^2+63x+14)/(4x-1)^{72} \end{aligned}$$

などとなっている。分母は $(4x-1)^{72}$ であり $x = 1/4 = -18$ を除いて 1 である。

尚、

$$\begin{aligned} F(1/4, 3/4, 1, x) = \\ 67(x+21)(x+51)(x^2+72x+41)(x^2+52x+2)(x^2+72x+69) \\ (x^2+72x+8)(x^2+61x+23)(x^2+72x+16)(x^2+10x+12)(x^2+19x+55) \end{aligned}$$

であるから何か一次変換の自由さがあるのであろう。

また、例えば Hessian family

$$H: x^3+3qxy+y^3 = 1$$

と Weierstrass family

$$W: y^2 = x^3+qx+r$$

の関数変換

$$64x(1-x)^3/(8x+1)^3 : F(1/3, 2/3, 1, x) \rightarrow x^{18}F(1/12, 5/12, 1, 1-x)$$

についても同様なのであろうか。こちらは、

$$\begin{aligned} x+9 \bullet 64x(1-x)^3/(8x+1)^3 &= -9(x^2+34x+10)(x^2+37x+22)/(8x+1)^3 \\ x+45 \bullet 64x(1-x)^3/(8x+1)^3 &= 64(x+68)(x^3+7x^2+49x+72)/(8x+1)^3 \end{aligned}$$

$$(x^2+9x+54) \bullet 64x(1-x)^3/(8x+1)^3 = 4(x^2+66x+20)(x^6+2x^5+4x^4+40x^3+69x^2+54x+56)/(8x+1)^6$$

などと、因数分解は複雑である。

尚、

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

$$66(x^2+2x+63)(x^2+72x+70)(x^2+72x+66)(x^2+21x+30)(x^2+50x+52)(x^2+69x+66) \\ (x^2+72x+65)(x^2+70x+1)(x^2+8x+72)(x^2+x+72)(x^2+72x+72)(x^2+63x+8)$$

と完全に 2 次以下の因子に分解されているから、 $F(1/3, 2/3, 1, x)$ の因子との間には、多くのこれから研究すべき未知な関係があることを示している。

例 $p = 17$

ここでは、有限体 F_p の乗法群

$$F_p^* = p-1 = p - \{0\} = \{1, 2, \dots, p-1\}$$

と、ちょっと誤解を招きそうな記法であるが、を用いる。勿論、前半の $p-1$ は集合としての差で

$$p-1 = \{0, 1, 2, \dots, p-1\} - \{0\} = \{1, 2, \dots, p-1\}$$

であり、 $p-1$ の元としての、つまり $\{1, 2, \dots, p-1\}$ の $p-1$ は数としての $p-1$ で、集合としては

$$p-1 = \{0, 1, 2, \dots, p-2\}$$

である。- の font を本当は区別すべきところである。

これらの対応関係は ' (後者 successor, +1) で結ばれている。

$$': p-1 \approx p-1$$

そこで、 $p-1$ の正方行列、つまり (ij) 元を $a_{12}(ij)$ あるいは $a_{12}(ij)$ を要素とする行列

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

$$B = (a_{12}(i/j))$$

を考えようというのである。これらの行列の固有値の絶対値は、円分方程式

$$x^{p-1} - 1 = 0$$

に於ける、原始 4 乗根、つまり $x^2 + 1 = 0$ の解 $i = \sqrt{-1}$ と原始 3 乗根の方程式 $x^2 + x + 1 = 0$ の解 $\omega = (-1 \pm \sqrt{-3})/2$ の個数を除いて 1 であるという (予想、定理?) である。つまり、Gauss の整数と Eisenstein の整数の部分だけ退化がおり、残りの部分は距離を保つ変換であるということである。今少し具体的にいうと

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

$$B = (a_{12}(i/j))/p$$

の固有値の絶対値は 1 または $1/\sqrt{p}$ であり、退化する $1/\sqrt{p}$ のものの個数は

$p \bmod 12$	1	5	-5	-1
$1/\sqrt{p}$	4	2	2	0

ということである。特に、 $p = -1 \bmod 12$ のとき、例えば $p = 11, 23, 47, \dots$ のときは実対称行列 A は直交行列であり

$$A^2 = E$$

つまり、 A は involution である。また、index 変換により巡回行列としての直交行列を得る。

添字変換 (index) 変換は乗法群

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

の原始根 r を用いて

$$r^{p-1}: \{1, 2, \dots, p-1\} \rightarrow \{1, 2, \dots, p-1\}$$

という置換を意味している。例えば、 $p = 7$ では 3, 5 は原始根で、

n	1	2	3	4	5	6
3^{n-1}	1	3	2	6	4	5

$$[3] = (1)(2,3)(4,6,5)$$

n	1	2	3	4	5	6
5^{n-1}	1	5	4	6	2	3

$$[5] = (1)(2,5)(4,6,3)$$

等となっている。これを、行列で表示すれば、表現関数(representing function)

$$[r] = \langle j = r^{i-1 \bmod p-1} \bmod p \rangle$$

左辺の $[r]$ は、原始根 r で生成される $p-1 = \{1, 2, \dots, p-1\}$ 上の置換である。

具体的には、例えば、上述の $p = 7$ での $[3]$ は

$$[1, 0, 0, 0, 0, 0]$$

$$[0, 0, 1, 0, 0, 0]$$

$$[0, 1, 0, 0, 0, 0]$$

$$[0, 0, 0, 0, 0, 1]$$

$$[0, 0, 0, 1, 0, 0]$$

$$[0, 0, 0, 0, 1, 0]$$

である。例えば、 $p = 17$ では、原始根は

$$\{3, 5, 6, 7, 10, 11, 12, 14\}$$

であり、それぞれの添字変換(index transformation)は

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

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

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

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

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

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

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

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

などと循環節の長さもまちまち(区々)である。

さて、本題に戻って、 $p = 17$ では $[p/12] = 1$ 、 $p \equiv 1 \pmod{4}$ 、 $(p-1)/4 = 4$ であるから、

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

を得る。従って、 x に $1-x$ を代入し、 x^4 を掛けて

$$a_{12}(x) = x^4(10x+8) \bmod p$$

である。 $a_{12}(x)$ の値を絶対値最小剰余(least absolute value residue)として、 $0 \sim p-1$ での値として記すと

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

である。これを、原始根 q のべき(power, exponent)の順

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

の順に並べる。 $a_{12}(0)$ が最初にあるので、次の $a_{12}(1)=1$ から順に、

$$a_{12}(1)=1, a_{12}(3)=1, a_{12}(9)=4, a_{12}(10)=7, \dots$$

と並べて

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

を得る。これから、通常の巡回行列(cyclic matrix)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

逆行巡回行列(anti-cyclic matrix)

$$B = (a_{12}(q^{i(j-2)}))$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

を得る。

前者は巡回行列として、後者は実対称行列としてユニタリー行列 (unitary matrix) を用いて対角化 (diagonalize) 可能である。そして、それらは列の反転、あるいは行の反転の行列、例えば (小さい次数だが)

$$\begin{aligned} & [0,0,0,0,1] \\ & [0,0,0,1,0] \\ & [0,0,0,1,0,0] \\ & [0,0,1,0,0,0] \\ & [0,1,0,0,0,0] \\ & [1,0,0,0,0,0] \end{aligned}$$

のような形の行列 (行天動地 ≠ 驚天動地)、つまり反対角 (anti-diagonal) 行列

$$C = \langle (i+j=p) \rangle$$

を (左から) 掛けることで移り合うことのできる行列である。つまり、両者の固有値の絶対値は不変である。所謂、ゲージ変換 (gauge transformation) である。

勿論、 $C^2 = E$ で、所謂単位 E の平方根、つまり対合 (involution) で、固有値は $1, -1$ で、次数が偶数なら、跡 (trace) は 0 、奇数なら 1 である。 C の平方根 (E の 4 乗根の一つ) は偶数次数なら、 $1/\sqrt{2}$ ・

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

奇数なら、 $1/\sqrt{2}$ ・

$$\begin{pmatrix} 1, 0, 0, 0, 0, 0, 1 \\ 0, 1, 0, 0, 0, 1, 0 \\ 0, 0, 1, 0, 1, 0, 0 \\ 0, 0, 0, \sqrt{2}, 0, 0, 0 \\ 0, 0, 1, 0, -1, 0, 0 \\ 0, 1, 0, 0, 0, -1, 0 \\ 1, 0, 0, 0, 0, 0, -1 \end{pmatrix}$$

のような形の行列である。

我々の主張したいことの主眼は、 $a_{12}(x)$ が F_p の 2 次拡大で完全分解すること、そこでフロベニウス写像 (Frobenius map)、 x は F_p の 2 次拡大の元として

$$x^p : F_p(x) \rightarrow F_p(x)$$

が対合であるということと、これから述べようとする、

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

の因子、 $x^4 - 1, x^3 - 1$ に対応する成分、つまり整数環 Z 、Gauss 整数 $Z(i)$ 、Eisenstein 整数 $Z(\omega)$ を除いて $a_{12}(x)$ の index 変換の逆行巡回行列の円分射影 (cyclomatic projection) 成分がすべ

て対合であることである。私は現在その証明は知らないが(実験的)事実はそのことを示している。

さて、 $p = 17$ で $a_{12}(3^{p-1})$ の列は

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

であることは既に述べた。これを多項式の係数とみた関数は

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

である。 $0x^{15}$ の項は消えている。巡回行列の固有値は、これに 1 の $p-1$ 乗根を代入したものである。つまり、対角化された行列の対角成分は $f(x)$ に 1 の原始 $p-1$ 乗根のべきを巡に代入したものになっている。

終結式(resultant)を用いて記せば

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

である。

そこで、少し記法等など約束事と概念の復習(数学史)の話になるが、 $f(x)$ と $g(x)$ の終結式を(ここだけの記法として)消去積(elimination product これも造語)と呼び

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

と記すことにする。 \otimes の結合力は最弱とする。

つまり、例えば

$$x^3 + 3 \otimes x^2 + x + 1$$

を $x^3 + (3 \otimes x^2 + x + 1)$ とか $x^3 + (3 \otimes x^2) + x + 1$ としてはいけない。

Sylvester の終結式も通常(巡回)と逆行を考える。

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

$$g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m$$

それは、巡回形と

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n & \cdots & 0 \\ & & \cdots & & \cdots & & & \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n \\ b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m & \cdots & 0 \\ & & \cdots & & \cdots & & & \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m \end{pmatrix}$$

逆行形の

$$\begin{pmatrix} 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n \\ & & \cdots & & \cdots & & & \\ 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n & \cdots & 0 \\ a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m \\ & & \cdots & & \cdots & & & \\ 0 & b_0 & b_1 & \cdots & b_{m-1} & b_m & \cdots & 0 \\ b_0 & b_1 & \cdots & b_{m-1} & b_m & 0 & \cdots & 0 \end{pmatrix}$$

が考えられる。これらは、前述の反対角行列を対角 block のもつ行列で移り合える。行列式の符号も

$$(-1)^{n(n-1)m(m-1)/4}$$

だけの差である。

これらの行列で、下の方の多項式の係数の一次結合を引き去って上右半分に n 次の正方行列を残すことを考える。つまり、 $x^k f(x)$ を $g(x)$ で割った剰余の係数を並べた行列である。

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

や、逆行行列では

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

として、

$$\begin{aligned} f(x) \otimes g(x) &= \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ & & \cdots & \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{pmatrix} & f(x) [x] g(x) &= \begin{pmatrix} d_{11} & d_{12} & \cdots & d_{1n} \\ d_{21} & d_{22} & \cdots & d_{2n} \\ & & \cdots & \\ d_{n1} & d_{n2} & \cdots & d_{nn} \end{pmatrix} \end{aligned}$$

などを書くことにする。行列と行列式に同じ記号を用いるのは混乱のもとであるが、行列式か行列かは文脈から判断することにする。

行列式については

$$\begin{aligned} f(x) &= a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = a_0 (x-c_1)(x-c_2) \cdots (x-c_n) \\ g(x) &= b_0 x^m + b_1 x^{m-1} + \cdots + b_{m-1} x + b_m = b_0 (x-d_1)(x-d_2) \cdots (x-d_m) \end{aligned}$$

とすると、

$$f(x) \otimes g(x) = b_0^n f(d_1) f(d_2) \cdots f(d_m) = a_0^m g(c_1) g(c_2) \cdots g(c_n)$$

である。

特に、 $f(x)$, $g(x)$ がモニック (monic)、つまり $a_0 = b_0 = 1$ の場合は、積分配律 (multiplicative distributive law) が成立する。つまり、 $f(x)$, $g(x)$, $h(x)$ を monic とすると、

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

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

などが成立する。また、割り算について、

$$f(x) = q(x) g(x) + r(x)$$

ならば、

$$f(x) \otimes g(x) = f(d_1) f(d_2) \cdots f(d_m) = r(x) \otimes g(x)$$

$$g(x) \otimes f(x) = f(d_1) f(d_2) \cdots f(d_m) = g(x) \otimes r(x)$$

などが成立する。

また、最初に記すべきかも知れないが、定数倍を除いて、交換法則 (commutative law)

$$f(x) \otimes g(x) = c(g(x) \otimes f(x)) \approx g(x) \otimes f(x)$$

や、結合法則

$$f(x) \otimes (g(x, y) \oplus h(y)) \approx (f(x) \otimes g(x, y)) \oplus h(y)$$

が成立する。代数的整数を係数とする monic な方程式の解は代数的整数であることの証明などの簡潔な記述ができる。例えば、

$$x^3 + \sqrt{2}x^2 + 2\omega x + 3i = 0$$

の解をもつ monic な整数係数の代数方程式は、 $\sqrt{2}, \omega, i$ の方程式が

$$x^2 - 2 = 0, x^2 + x + 1 = 0, x^2 + 1 = 0$$

であるから、

$$x^3 + yx^2 + 2zx + 3w \oplus y^2 - 2 \otimes z^2 + z + 1 \oplus w^2 + 1$$

を左から巡に終結式を計算すればよい。結果は

$$x^{24} - 16x^{22} + 112x^{20} - 364x^{18} + 448x^{16} + 152x^{14} - 1850x^{12} + 4208x^{10} - 32x^8 + 468x^6 + 3888x^4 - 5832x^2 + 6561$$

で、勿論 (monic な多項式の終結式は monic だから) monic である。

例えば、巡回行列

$$A = (a_{ij}(q^i))$$

の固有値は、係数列

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

の表現多項式

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

を用いれば、1 の p-1 乗根の方程式

$$x^{16} - 1 = (x-1)(x+1)(x^2+1)(x^4+1)(x^8+1) = 0$$

を用いて、 $y-f(x)$ と $x^{16}-1$ の x に関する終結式である。つまり、その方程式は

$$y-f(x) \otimes x^{16}-1 =$$

$$(y-f(x) \otimes x-1)(y-f(x) \otimes x+1)(y-f(x) \otimes x^2+1)(y-f(x) \otimes x^4+1)(y-f(x) \otimes x^8+1)$$

と因数分解される。剰余を rem あるいは \diamond で記すと

$g(x)$	$x-1$	$x+1$	x^2+1	x^4+1	x^8+1
$f(x) \diamond g(x)$	17	-17	-x-4	$17x^3$	$-4x^7-11x^6+8x^5+5x^4+x^3+7x^2-2x+3$

であるから個別に計算することもできる。

$$y+x+4 \otimes x^2+1 = y^2+8y+17 = 0$$

これは Eisenstein 整数 $Z(\omega)$ で因数分解でき、解の絶対値は $\sqrt{17}$ である。

$$y-17x^3 \otimes x^4+1 = y^4+83521 = y^4+17^4 = 0$$

この解の絶対値は 17 でそれに 1 の原始 8 乗根が掛かっている。

$$y-(-4x^7-11x^6+8x^5+5x^4+x^3+7x^2-2x+3) \otimes x^8+1$$

$$=$$

$$y^8-24y^7-136y^6+6936y^5-78608y^4+2004504y^3-11358856y^2-579301656y+6975757441$$

で、見かけは厳めしいが $y = 17x$ と思えば 17^7 を除いて

$$17x^8-24x^7-8x^6+24x^5-16x^4+24x^3-8x^2-24x+17 = 0$$

である。この方程式の解の絶対値がすべて 1 であることを直接証明するのは少し面倒かも知れない。

実際には、

$$y-(-4x^7-11x^6+8x^5+5x^4+x^3+7x^2-2x+3) \otimes x^8+1$$

の終結式の左上正方行列は(行列版の表現で)、 x^8+1 の剰余では 8 項後に-を掛けて加えるから、最後の項の符号を反転して初項として、

$$-4x^7-11x^6+8x^5+5x^4+x^3+7x^2-2x+3 \otimes x^8+1$$

$$=$$

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

などを得る。この行列を A とすると

$$1/17 \cdot A$$

は直交行列であるから、この固有多項式の解として絶対値が 1 なのである。

最初の主張は、この行の上下を反転した(逆行)終結行列

$$-4x^7-11x^6+8x^5+5x^4+x^3+7x^2-2x+3[x]x^8+1$$

$$=$$

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

を考える。この行列を B とすると

$$1/17 \cdot B$$

の固有方程式は

$$(x^2-1)^4$$

であり、最小多項式(minimal polynomial)は x^2-1 である。つまり、 $1/17 \cdot B$ は対合である。
同様にして、

$$\begin{aligned} & 17x^3[x]x^4+1 \\ &= \\ & \begin{pmatrix} -17, & 0, & 0, & 0 \\ 0, & 0, & 0, & 17 \\ 0, & 0, & 17, & 0 \\ 0, & 17, & 0, & 0 \end{pmatrix} \end{aligned}$$

を A とすれば、 $1/17$ の固有方程式は $(x^2-1)^2$ で最小多項式は x^2-1 である。 $\text{tr}(A) = 0$ であることは $-17+17=0$ から解る。

因子 x^2+1 からは $-x-4$ が剰余として生じるが、これから

$$\begin{aligned} & -x-4[x]x^2+1 \\ &= \\ & \begin{pmatrix} -4 & -1 \\ -1, & 4 \end{pmatrix} \end{aligned}$$

が求まる。この(実対称)行列の固有方程式は

$$x^2-17=0$$

その解の絶対値は \sqrt{p} である。最初の表の

$$(17x^2-1)(x^2-1)^7$$

の意味はこれらのこと、つまり、円分 block 分解(cyclotomic block decomposition)からの結論である。

まとめて記せば、ある unitary 行列 U を用いて、対角線上に固有値 $\pm\sqrt{p}$ と p , $-p$ が 7 個ずつ並んだ対角行列 T , $a_{12}(3^{11})$ を巡に並べた

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

を第一行とする逆行巡回行列が

$$U^{-1}TU$$

の形に表現できることを意味している。 U^{-1} は unitary 行列 U の転置(transposition)の共役(conjugate) U^* である。恐らく、この $\pm\sqrt{p}$ への Gauss 整数と Eisenstein 整数への退化が \sin^2 -予想の曲線が中央付近、つまり $\pi/2$ 付近の値に、標準偏差程度、言い換えると sample の個数の平方根の程度の“ゆらぎ”をもたらしているのではないかと考えている。

例えば、 $p=19$ では

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

である。原始根 2 として $a_{12}(2^{11})$ の列は

$$[1, -2, 2, -6, 2, -3, 5, -7, -6, 4, -1, -4, -8, -5, 1, 0, 4, 4]$$

であり、表現多項式は

$$f(x)=1-2x+2x^2-6x^3+2x^4-3x^5+5x^6-7x^7-6x^8+4x^9-x^{10}-4x^{11}-8x^{12}-5x^{13}+x^{14}+4x^{16}+4x^{17}$$

である。

表現多項式の F_p での一次因子への分解性については興味ある性質がある。

例えば、 $p=19$ で上記の $f(x)$ について F_{19} で

$$f(x) = 4(x+1)(x+2)(x+3)(x+4)(x+5)(x+6)^2(x+7)(x+9)(x+10) \\ (x+11)(x+12)(x+13)(x+14)(x+15)(x+17)(x+18)$$

など完全に分解している。何故、 $(x+8)(x+16)$ がなくて $(x+6)^2$ のように重複因子があるのかなど、謎の多い部分である。

一般には、一次因子に完全には分解しない。しかし、 $1/10$ 程度の一次因子を除いて一次因子が表れるなど興味ある問題である。ここでは、小さな素数に関する因数を表にするに留める。

$$f(x)/(x^{p^1}-1) \text{ in } F_p$$

p	q	f(x)	$x^{p^1}-1$
17	3	1	$(x+10)(x+13)$
19	2	$x+6$	$(x+8)(x+16)$
23	5	$x+19$	$(x+4)(x+20)$
29	2	$(x+1)(x+7)$	$(x+6)(x+3)(x+12)$
31	2	$(x+8)(x+29)$	$(x+16)(x+17)(x+26)$
37	2	$(x+4)(x+11)(x+23)$	$(x+17)(x+27)(x+34)(x+31)$
41	6	$(x+5)(x^2+23x+27)$	$(x+10)(x+19)(x+29)(x+32)$
43	3	$x^3+19x^2+28x+3$	$(x+10)(x+25)(x+32)(x+37)$
47	5	x^3+23x^2+45	$(x+8)(x+12)(x+13)(x+40)$
53	2	$(x+36)(x^3+24x^2+51x+2)$	$(x+15)(x+17)(x+30)(x+34)(x+35)$
59	2	$(x+7)(x+52)(x^2+8x+3)$	$(x+21)(x+25)(x+41)(x+42)(x+50)$
61	2	$(x+49)(x^2+34x+27)(x^2+55x+19)$	$(x+9)(x+11)(x+18)(x+35)(x+36)$ $(x+48)$
67	2	$(x^2+10x+61)(x^3+14x^2+16x+35)$	$(x+5)(x+9)(x+10)(x+18)(x+36)$ $(x+38)$
71	7	$(x+4)(x^3+36x^2+67x+27)$	$(x+17)(x+22)(x+34)(x+44)(x+65)$ $(x+68)$
73	5	$(x^5+32x^4+31x^3+68x^2+10x+37)$ $(x+66)$	$(x+4)(x+6)(x+9)(x+20)(x+27)$ $(x+30)(x+45)$
79	3	$(x+50)(x^4+54x^3+32x^2+x+50)$	$(x+16)(x+24)(x+37)(x+48)(x+58)$ $(x+65)(x+72)$
83	2	$(x+73)(x^2+10x+28)$ $(x^3+34x^2+11x+38)$	$(x+15)(x+30)(x+33)(x+37)(x+49)$ $(x+60)(x+66)$
89	3	$(x^6+36x^5+70x^4+41x^3+39x^2+64x+87)$ $(x+87)$	$(x+11)(x+22)(x+25)(x+44)(x+50)$ $(x+57)(x+73)(x+88)$
97	5	$(x^3+8x^2+3x+28)$ $(x^5+13x^4+49x^3+84x^2+15x+87)$	$(x+1)(x+36)(x+47)(x+49)(x+72)$ $(x+73)(x+85)(x+91)(x+94)$

話を元にもどして、谷、既約円分多項式による剰余の表は次のようである。

$g(x)$		$x^n f(x) \oslash g(x)$
$x-1$	1	-19
$x+1$	1	19
x^2+x+1	x	$5x+3$
	1	$-3x+2$
x^2-x+1	x	$-19x+19$
	1	$-19x$
x^6+x^3+1	x^5	$19x^5+19x^2$
	x^4	$19x^4+19x$
	x^3	$19x^3+19$
	x^2	$-19x^5$
	x	$-19x^4$
	1	$-19x^3$
x^6-x^3+1	x^5	$-x^5+16x^4+10x^3-7x^2-2x-6$
	x^4	$6x^5-x^4+16x^3+4x^2-7x-2$
	x^3	$2x^5+6x^4-x^3+14x^2+4x-7$
	x^2	$7x^5+2x^4+6x^3-8x^2+14x+4$
	x	$-4x^5+7x^4+2x^3+10x^2-8x+14$
	1	$-14x^5-4x^4+7x^3+16x^2+10x-8$

である。例えば、 x^6-x^3+1 に応ずる行列は

$$\begin{pmatrix} -14, -4, 7, 16, 10, -8 \\ -4, 7, 2, 10, -8, 14 \\ 7, 2, 6, -8, 14, 4 \\ 2, 6, -1, 14, 4, -7 \\ 6, -1, 16, 4, -7, -2 \\ -1, 16, 10, -7, -2, -6 \end{pmatrix}$$

これらは、遅延 feed back、つまり $x^6 = x^3-1$ をもった回路の特性方程式や差分方程式の解である。

この行列を A とすると $1/19 \cdot A$ も対合である。勿論、固有多項式は $(x^2-1)^3$ で最小多項式は x^2-1 である。尚、原始根を $q=3$ とすると x^6-x^3+1 に応ずる行列は

$$\begin{pmatrix} -2, 10, 7, -14, -6, -8 \\ 10, 7, -16, -6, -8, 2 \\ 7, -16, 4, -8, 2, -10 \\ -16, 4, -1, 2, -10, -7 \\ 4, -1, -14, -10, -7, 16 \\ -1, -14, -6, -7, 16, -4 \end{pmatrix}$$

など、異なるものになっているが固有多項式や最小多項式は同じである。このような対合行列の間の同値群の代数構造の研究も興味ある対象である。

因子 x^2+x+1 から

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

を得る。固有多項式は x^2-19 である。また、この行転置

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

の固有多項式は $x^2-7x+19$ で、固有値は Eisenstein 整数 $(7 \pm 2\sqrt{-3})/2$ で絶対値は $\sqrt{19}$ である。

一般に、素数 p に対する多項式 x^p-1 に対応した円分射影影子からは大きな size の巡回対合 (cyclic involution) が得られる。例えば、 $p = 47$ の場合

$$x^{46}-1 = (x^{23}-1)(x^{23}+1)$$

$$1/47 \cdot$$

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

のような巡回行列は巡回対合である。例えば、このような大きさの信号を発信し、受信者は同じ大きさ号列との内積をとれば、どれだけの強さの信号がどれだけの遅延の後に到着したかなどが解る。大きな素数 p を選べば \sqrt{p} 程度の振幅の長さ p の直交巡回数列、つまり、周期と異なる長さだけずらした列との内積が 0 の数列、を得ることができる。

例えば、次の列は、上記行列の 5~9 列を 3,1,4,1,5 倍して加えたもの(このような計算は少し以前の data 列のみを用いて逐次計算できる)

[-109, 24, 42, 5, 32, 28, 65, 90, -30, 4, -122, -79,
-100, -103, -22, -76, 5, -84, 19, -144, -39, -86, 22]

を5で割った数列に、仮の雑音として

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

を加え、結果の平均が0にした数列に一番近い整数(nint = near integer)の列を考える。

次のものがそれである：

[-21, 6, 9, 2, 7, 6, 14, 19, -5, 2, -24, -15, -19, -20, -4, -14, 2, -16, 5, -28, -7, -16, 5]

これに、元の行列を掛ける(再生を試みる)と

[-39, -51, -47, -35, 1291, 396, 1741, 398, 2165, -37, -69,
-39, -29, -38, -14, -37, -65, -16, -38, -53, -38, -36, -46]

のような数値が得られる。仮の基準として400程度の数で割ると

[-0.097, -0.127, -0.117, -0.087, 3.227, 0.990, 4.352, 0.995,
5.412, -0.092, -0.172, -0.097, -0.072, -0.095, -0.035, -0.092,
-0.162, -0.040, -0.095, -0.132, -0.095, -0.090, -0.115]

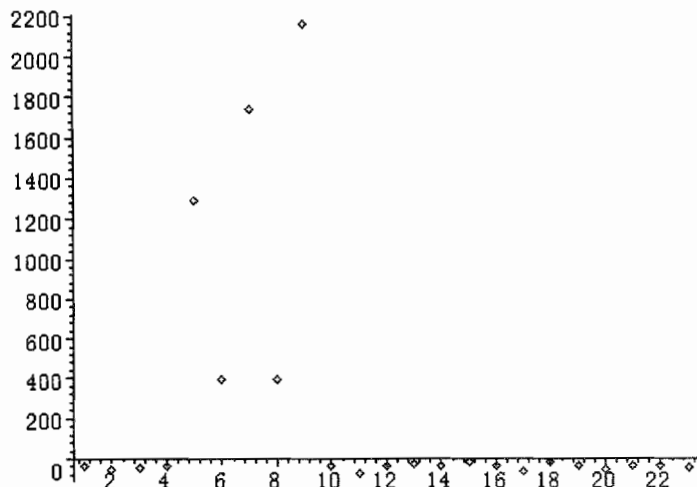
である。ここでは、離散的な整数値を用いるように記述しているが、むしろ analog な処理に適していると思う。

雑音や欠落の影響など考慮しても31415というもとの数列がまあ読みとれるであろう。

私の個人的な感覚であるが音波カメラ(sonic [movie, still] camera)などに応用可能なのではないかと考えている。音波は物体の最深部を見ることができる非破壊的な手段である。

特に現在通常用いられている衝撃的(強く短い)波に対して(周波数が高いが長時間の弱い、そして分解能の高い=優しい?)波がもつ意義・役割は大きいと思う。沢山の情報の重ね合わせの度合の解析も重要な研究課題である。

少し(=大いに)、話が本道でない、横道にそれてしまった。取りあえずこのあたりで中断する。



例 $p = 197$

次の図は、原始根 $q = 2$ による $a_{12}(x)$ の表現変換 (representation transformation)

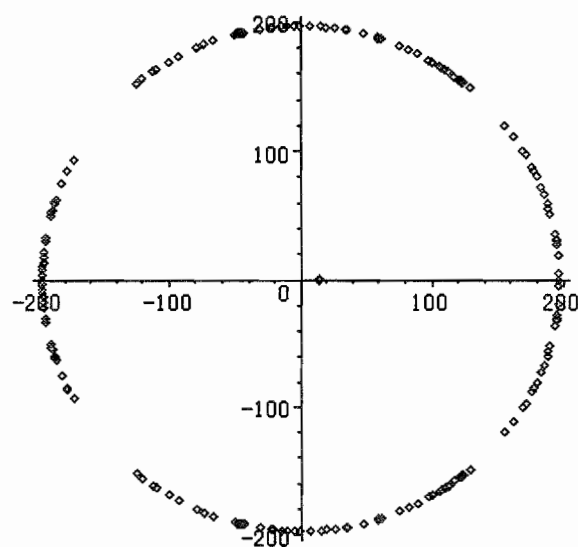
$$f(x) = \overline{a_{12}}(x) = \sum_{n \in \mathbb{F}_p} a_{12}(q^{n-1}) x^{n-1}$$

の 1 の原始 $p-1$ 乗根での値と、表現変換方程式 $f(x) = 0$ の解の分布である。

1 の原始 $p-1$ 乗根での $f(x)$ の値

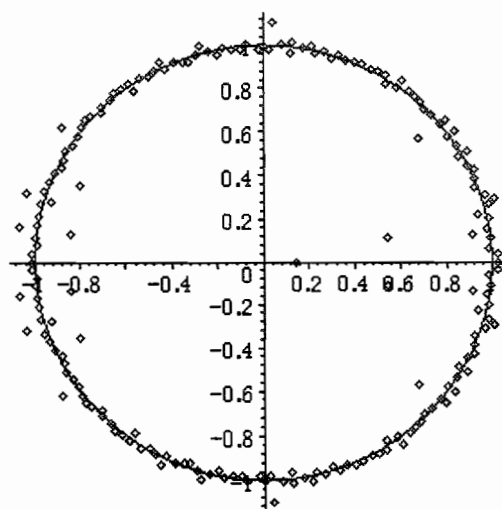
$$p = 197, q = 2$$

(原点の近くに絶対値 $\sqrt{197}$ の 2 点がある)



表現変換方程式 $f(x) = 0$ の解

$$p = 197, q = 3$$



これらを見ると、1 の原始 $p-1$ 乗根での $f(x)$ の値は思いの外、偏りのある分布であるが。表現変換方程式 $f(x) = 0$ の解は、これも意外に単位円周の近くの一様に分布していることが解る。

なお、 $f(x) = 0$ の素体上には極めて多くの解が存在する、つまり多くの一次因子をもつ。例えば、

[0, 7, 14, 21, 26, 37, 63, 68, 78, 111, 117, 125, 136, 140, 154, 173, 178, 189]

での対応する mod 197 での最小剰余値は、次のようである：

[1, -53, 28, -29, -20, -9, 42, 17, -27, 98, -12, 23, -9, 12, -65, -10, -68, 81]

上の列に属さない数は全て解である。

$f(x)/x^{p-1}-1$ の F_p での既約分数では

$$\begin{aligned} &6(x+147)(x+193)(x^3+156x^2+116x+53)(x^3+186x^2+16x+47) \\ &(x^4+117x^3+148x^2+54x+156)(x^4+195x^3+145x^2+55x+138) \end{aligned}$$

が分子で、分母は

$$\begin{aligned} &(x+176)(x+80)(x+183)(x+129)(x+57)(x+19)(x+43)(x+61)(x+72) \\ &(x+190)(x+119)(x+160)(x+86)(x+24)(x+171)(x+8)(x+134) \end{aligned}$$

の 19 個の因子である。 $(x+147)(x+193)$ は $f(x)$ の重複因子である。

これらの事実の断片だけでも、ここに大きな未開の世界があることを窺わせるに十分なものがある。

例えば、 $p = 10^{12}$ 程度の素数を考え、この素数から生じるデータ 10^6 程度の大きさの、長さ 10^{12} データ列を考えてみよう。仮に、一秒間に 10^6 個程度の速度で送信可能とすると、11~12 日間の列であるが…。

このような長さの周期列に message を載せるとしたら、宇宙のどの程度の所まで受信が可能であろうか。相方がこの対合を知っていて、受信記号を数学的に処理可能な文明をもっていたら、どんな返信をしてくるであろうか。送信者としては相方が、恐らくは、こんな素数を選ぶであろうというような大きな有名な素数でなければならない。これは恐らく人類の文明の品格を象徴する数を選ぶということである。人類の代表としては p として何を選びますか。2005. 12. 15 に見つかったという 43 番目の Mersenne prime

$$M_{43} = 2^{30402457} - 1$$

の指数 30402457 などは候補の一つですが…。また、酒の席の肴として、いいもの(素数)があったら教えてください。

もっと、現実的な話は、星からの反射波であろう。これも、色々と想像の物語の考えられる部分である。例の sonic camera の話は、2~3m の空間の音の話なのである。

4. 超楕円曲線と \sin^2 -予想

ここでは、種数 (genus) の高い、所謂、超楕円曲線 (hyper-elliptic curve)

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

と、それに対応する合同ゼータ核、つまり終結変換多項式 (resultant transform polynomial) の根の分布についての予想について述べる。

ここでは、 $f(x)$ は奇数次 $d = 2g+1$ の多項式とする。各素数に対して、次のような終結式

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

$$f_2(u_1, u_2) = f(x) \otimes x^2+u_1x+u_2$$

$$f_3(u_1, u_2, u_3) = f(x) \otimes x^3+u_1x^2+u_2x+u_3$$

のように $f_n (n = 1, \dots, g)$ を定める。更に、各 n に対し Legendre 記号の n 重和

$$a_p = \sum_{x \in p} (f_1(x)/p)$$

$$b_p = \sum_{x,y \in p} (f_2(x,y)/p)$$

...

と定める。このとき、 $f(x)$ の終結変換多項式を

$$x^{2g} + a_p x^{2g-1} + b_p x^{2g-2} + \dots + d_p x^{g+1} + \dots + b_p p^{g-2} x^2 + a_p p^{g-1} x + p^g$$

と定義する。

例、

$$y^2 = x^5 + 2x^3 + x^2 + x + 5 = f(x)$$

では、

$$f_1(u) = f(x) \otimes x+u = u^5 + 2u^3 - u^2 + u - 5$$

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

$$-5u^5 + u^4v + (-v^2 + 25v - 10)u^3 + (2v^3 - 4v^2 + 2v + 5)u^2 + (3v^3 - 27v^2 + 29v - 5)u + v^5 - 4v^4 + 6v^3 - 3v^2 - 9v + 25$$

であり、

$$a_p = \sum_{x \in p} (f_1(x)/p)$$

$$b_p = \sum_{x,y \in p} (f_2(x,y)/p)$$

とすれば、終結変換多項式は

$$x^4 + a_p x^3 + b_p x^2 + a_p p x + p^2$$

である。例えば、最初の 100 までの奇素数での $[p, a_p, b_p]$ の表は

$$\begin{aligned} &[3, 1, 5], [5, 1, 0], [7, 1, 5], [11, -2, -2], [13, -1, 4], [17, -1, -24], [19, -1, -7], \\ &[23, 3, 13], [29, 8, 38], [31, -6, 24], [37, 3, 29], [41, 0, 32], [43, 0, 58], [47, 1, -26], \\ &[53, -1, 9], [59, -7, 62], [61, 11, 92], [67, -6, -10], [71, -15, 85], [73, 2, 102], \\ &[79, -10, 100], [83, 2, -10], [89, 2, -22], [97, -3, -103] \end{aligned}$$

となる。 $p = 5$ では、平方剰余の表、つまり Legendre symbol の表は

$$[0, 1, -1, -1, 1]$$

$f_1(x)$ の値とその符号 (=Legendre symbol) の表は

$$[0, 3, 1, 1, 0]$$

$$[0, -1, 1, 1, 0]$$

であり、和は 1 である。また、 $f_2(x,y)$ の値とその符号の表は

$$[0, 1, 1, 2, 0, 0, 1, 2, 0, 1, 0, 4, 0, 4, 1, 0, 0, 3, 3, 0, 3, 2, 3, 1]$$

$[0, 1, 1, -1, 0, 0, 1, -1, 0, 1, 0, 1, 1, 0, 0, -1, -1, -1, 0, -1, -1, -1, 1]$ であり、0 が 9 個、1, -1 がそれぞれ 8 個 ($5^2 = 25 = 9+8+8$) で和 0 である。これが

$$[p, a_p, b_p] = [5, 1, 0]$$

の意味である。従って、 $p = 5$ に対応する終結多項式と方程式は

$$x^4 + x^3 + 5x + 25 = 0$$

である。一般に

$$x^4 + ax^3 + bx^2 + apx + p^2 = (x^2 + ux + p)(x^2 + vx + p)$$

なる、 u, v を 2 根とする方程式は

$$x^4 + ax^3 + bx^2 + apx + p^2 \otimes x^2 + ux + p = (u^2 - au + 2p - b)p^2$$

から、

$$u^2 - au + 2p - b = 0$$

である。従って、この場合は

$$u^2 - u + 10 = 0$$

となり、2 実根は

$$u = (1 \pm \sqrt{41})/2$$

であり、これらは、Hasse の不等式

$$|u| < 2\sqrt{5}$$

を満たしている。従って 4 根の絶対値は $\sqrt{5}$ で、それらは

$$1 \pm \sqrt{41} \pm \sqrt{-38 \pm \sqrt{41}}$$

である。後半の根号の中は $-38 \pm \sqrt{41}$ は常に負である。

$$b_p = \sum_{x,y \in p} (f_2(x,y)/p)$$

などの計算では、

$$-5u^3 + u^4v + (-v^3 + 25v - 10)u^3 + (2v^3 - 4v^2 + 2v + 5)u^2 + (3v^3 - 27v^2 + 29v - 5)u + v^3 - 4v^4 + 6v^3 - 3v^2 - 9v + 25$$

といった複雑さの項を p^2 個 mod p で計算する必要が生じる。この計算は階差法によるのが能率がよいであろう。

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 6 & 14 & 30 \\ 0 & 0 & 0 & 6 & 36 & 150 \\ 0 & 0 & 0 & 0 & 24 & 240 \\ 0 & 0 & 0 & 0 & 0 & 120 \end{pmatrix} \begin{pmatrix} v^3 - 4v^4 + 6v^3 - 3v^2 - 9v + 25 \\ 3v^3 - 27v^2 + 29v - 5 \\ 2v^3 - 4v^2 + 2v + 5 \\ -v^3 + 25v - 10 \\ v \\ -5 \end{pmatrix}$$

この積の転置は

$$[v^3 - 4v^4 + 6v^3 - 3v^2 - 9v + 25, 5v^3 - 32v^2 + 57v - 15, 4v^3 - 14v^2 + 168v - 200, -6v^3 + 186v - 810, -1200 + 24v, -600]$$

である。これを、初期値として、例えば $v = 0$ のときは

$$a_0 = 25, a_1 = -15, a_2 = -200, a_3 = -810, a_4 = -1200, a_5 = -600$$

あるいは、mod p での剰余。(一般にはこのようにする)として

$$a_0 = a_0 + a_1: a_1 = a_1 + a_2: a_2 = a_2 + a_3: a_3 = a_3 + a_4: a_4 = a_4 + a_5$$

として計算すればよい。勿論、初項の多項式 $v^3 - 4v^4 + 6v^3 - 3v^2 - 9v + 25$ も階差を用いて計算した方がよいであろう。大きな素数では 2 段目の階差法の効果はそんなには大きくないが、それでも計算時間の効果はある。

以下では、各種数に対する超楕円曲線

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

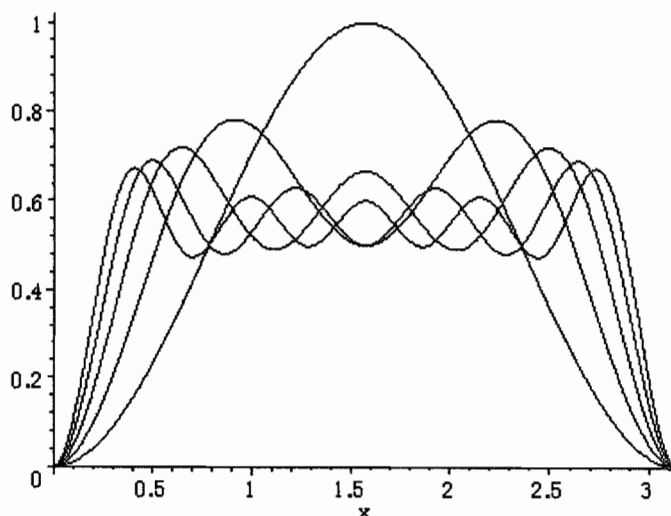
に対応する終結変換方程式の解の偏角の分布の類型を、複素根の分布図、度数の分布、その Fourier sin/cos coefficients の図などを挙げておく。

予想は、一般的に(特殊な事情のため退化しない場合)は、種数 g の曲線の偏角の分布は

\sin^2 -予想：

$$\sin^2 x + \sin^2 2x + \cdots + \sin^2 gx$$

に比例する。



関数

$$h_n(x) = \sin^2 x + \sin^2 2x + \cdots + \sin^2 nx$$

の n を大きくした極限は一様分布に収束することが知られている。

これらの予想に至る過程では、昭和 39 年頃から、日立中央研究所の試作第一号機 HITAC5020 など使用させて頂いた。しかし、例えば

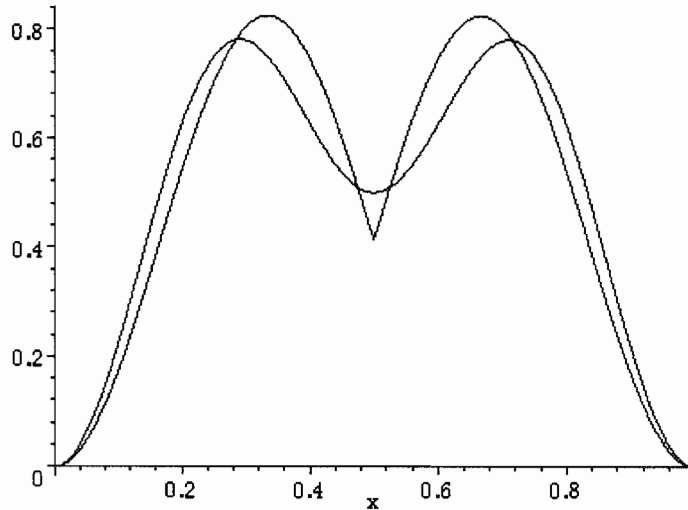
$$C: y^2 = x^3 + 5x + 5$$

の場合でも、ある程度重点的に計算しても、 $p = 300$ 程度までの data しか得られず、当時は、解の偏角の分布の類型が非常に多いのではないかとの思いもあって、確信をもってこの予想をすることはできなかった。2004 年度の第 14 回数学史シンポジウム(2004. 10. 26)の段階($p = 3 \sim 12413, 1481$ 個)でさえ、この分布を記述している真の分布は何であろうかと

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

というような、とても美しいとは云えない分布をあてはめてみては、真実を反映した分布がこのように複雑である筈がないと…疑いながら、しかし、何か(美しい式が)存在する筈と確信していた。それが、どんな姿で登場するのであるかと楽しみであった。

結果は、 \sin^2 -予想を、最も忠実に継承した、そして最も簡潔な形をもって現れてきたことに深い感動を覚えたのであった。



$$\frac{3\pi}{(2+3\pi)} \cdot \max(\max(0, \sin(3\pi x/2))^2, \max(0, \sin(3\pi(x-1/3)/2))^2) \\ (\sin^2(2\pi x) + \sin^2(4\pi x))/2$$

ここには多くの問題があると思う。

一つは、例えば、種数 $g = 2$ の場合、Hilbert-Weber の類多項式の

$$g(x) = (1 - 16x^{24})/12x^{16}$$

による簡約形

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

などの場合は、quaternion multiplication (虚数乗法 complex multiplication に対応) などが関係してであろうが、退化 (重複、あるいは相互作用がない場合とかの理由) がおこって分布は楕円曲線の場合と同様に $(\sin^2 x + \sin^2 2x)$ ではなくて)

$$\sin^2 x$$

に比例している。なお、上記の例は $p = 47$ の Hilbert-Weber の類多項式

$$248832x^5 + 27371520x^4 + 20908800x^3 + 277542000x^2 + 162855000x + 252209375$$

の、簡約化であり、判別式はそれぞれ 47^2 , 79^2 である。すべての類数 5 の虚二次体の整数環を生ずる素数

$$47, 79, 103, 127, 131, 179, 227, 347, 443, 523, 571, 619, 683, 691,$$

$$739, 787, 947, 1051, 1123, 1723, 1747, 1867, 2203, 2347, 2683$$

に対応した種数 2 の超楕円曲線で $\sin^2 x$ の角分布をもつものが存在するか…とか、この分布型をもつ曲線の判別条件など興味ある問題である。

また、偏角の分布

$$\sin^2 2x$$

をもつ超楕円曲線は存在するか。予想は否定されることも多いが、今は、存在しないかなと思っている。

種数 $g = 2$ の場合の偏角分布の種類の全体像の列挙の問題は大切な課題である。

種類の全体像は、現在のところ私には決定できないが、そんなに複雑ではないであろう

が、逆にそんなに簡単でもないかも知れない。

例えば、多くの因数をもつ

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

のような場合には、 $\sin^2 x$ でも、一般の $\sin^2 x + \sin^2 2x$ 型でもなく、主要な要素は何か

$$1+\sin x+\sin^2 x+\sin^3 x+\dots?$$

(今は見当がつかない)型であろうなど…、現在、楽しん(苦しん)でいる状態である。

真実の定義であるが…、幾らかの時間の後に、…真実を反映する式に行き当たると思うが、その式は如何なる冗談や悪意や妄想もしなやかに受け入れ(流し)て、品位のある微笑をもって応じてくれるものであろう。確かなことは可能な全ての場合を、現実に合わせてはめて…見ることである。

変な予想でも、これが存在すれば、“そんなこと(甘く)はない筈”と一つでも調査が進むことを期待してのことである。

これは、漆黒の空間から、燦然と輝く銀河を望むような視点なのである。

私は、そんなもの(視点)が存在するということを見せてくれる一つの世界が数の世界であると思っている。兎も角、多くの意外な分布がありそうである。

現在、(2006. 01. 02)連続な密度をもつ分布では、私は

$$?(\sin x), \sin^2 x, \sin^2 x + \sin^2 2x$$

の3個の類型しか知らないが、新しいタイプの登場を楽しみにしている。

ここに記述した $?(\sin x)$ 型の登場は、 $y^2 = f(x)$ の $f(x)$ が既約でない場合ではあるが、 \sin^2 -予想を標榜していた…自分にとっても、大きな驚きであった。勿論、例えば

$$C: y^2 = x^5 - 2$$

などのように \sqrt{p} に原始4乗根、原始8乗根で定まる、角度、つまり $\pi/4, \pi/2, 3\pi/4$ と一様分布の和となるようなものも存在する。

また、終結変換多項式であるが、例えば、 $n=3$ では

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

であるが、これは、Tschirnhaus 変換(チルナウス: W. von Tschirnhaus, 1651-1708)と呼ばれている変換や標準形であることはよく知られていると思う。この時代は、近松、西鶴、そして芭蕉が旅立ち、ニュートンの principia、ハレー彗星の再来の予言などの時代である。

このような17世紀の代数学の歴史的・古典的素材のなかに未知の花園がそよ風を楽しんでいるのである。

現在はまだそのタイプのすべてを尽くすまでは調査がされていないと思うが、これらは多くの人々の手を必要としている、やりがいのある(新しい視点を啓く可能性のある)仕事であろうと思う。

以下、資料として、HITAC5020 を用いて

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

について、解を手で plot した、恐らくは1964年頃の graph など、現在でもとにある資料を挙げておく。この時点では、偏角のグラフの類型は非常に多く、複雑であろうとの(私の)先入観もあって

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

などは思ってもいなかった。もう一つは、早急な決定的な方向づけが将来に誤った傾向性

をもたせるかも知れないという配慮であり、それは本質的に大切なことである。

後でこれを見ればこれを想定できたと思うかも知れない。しかし、それは既に見た人の感想であって、事実はずっと迷いに満ちていたのである。

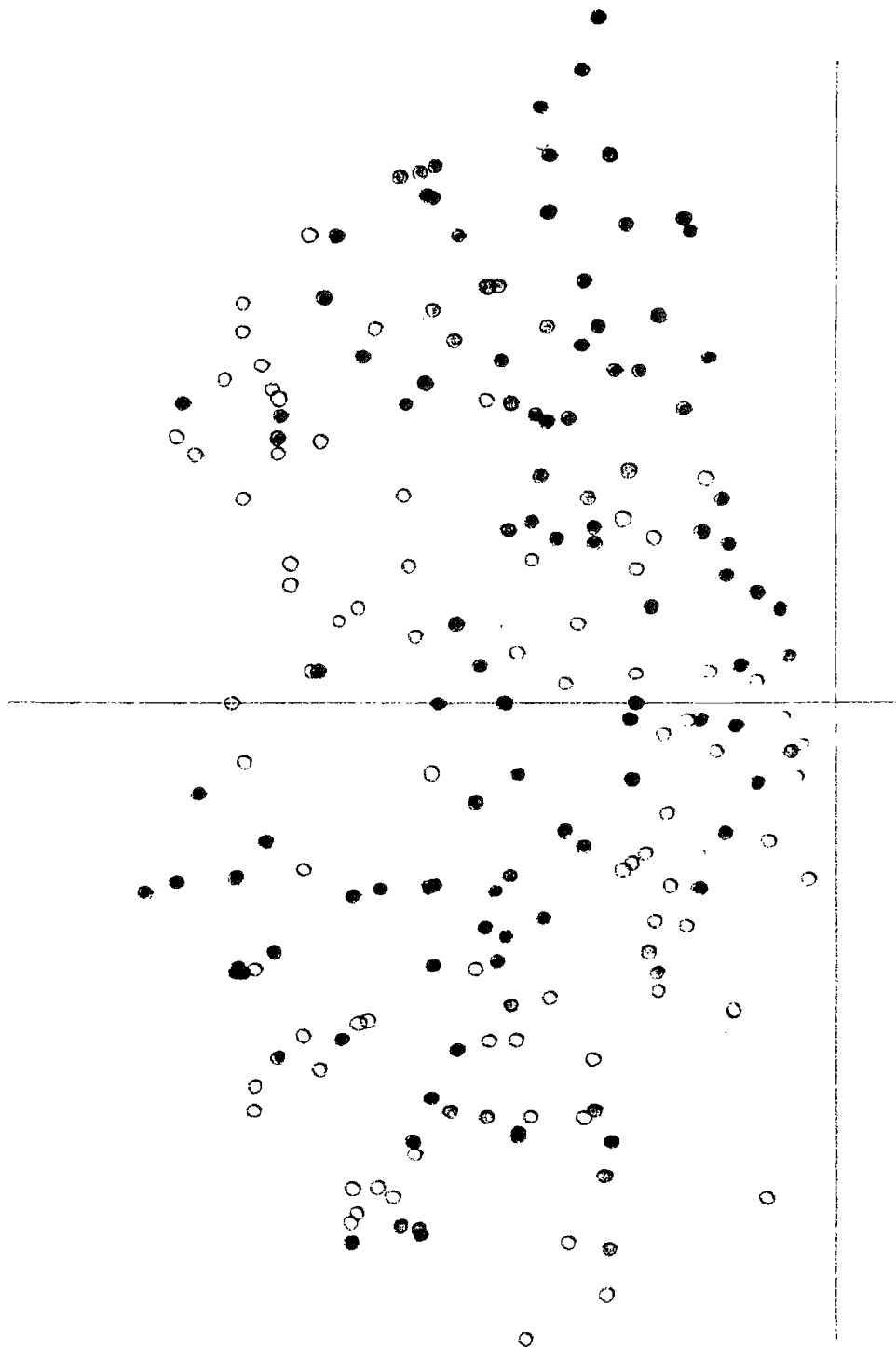
そこに、確かに存在することを知って見るのと、(安定した極限が) “あるかないか” さえ未知のときに眺める(見る)のとは本質的に異なるのである。

references

- [1] Kanji Namba: Hyper-elliptic curves over finite fields and an extension of Sato-sin²-conjecture
2003 年度応用数学合同研究集会報告集 REC Hall, Ryukoku Univ. 2003. pp.31-36
- [2] 難波完爾：有理関数の合成代数と虚数乗法、第 14 回 数学史シンポジウム(2003) 津田塾大学、津田塾大学 数学・計算機科学研究所報 25, 2004. pp.103-122
- [3] Kanji Namba: hyper-elliptic curves and extended Sato-sin²-conjecture, 2004 年度応用数学合同研究集会報告集 REC Hall, Ryukoku Univ. 2004. pp.33-38

$$f(x) = x^5 + 5x + 5$$

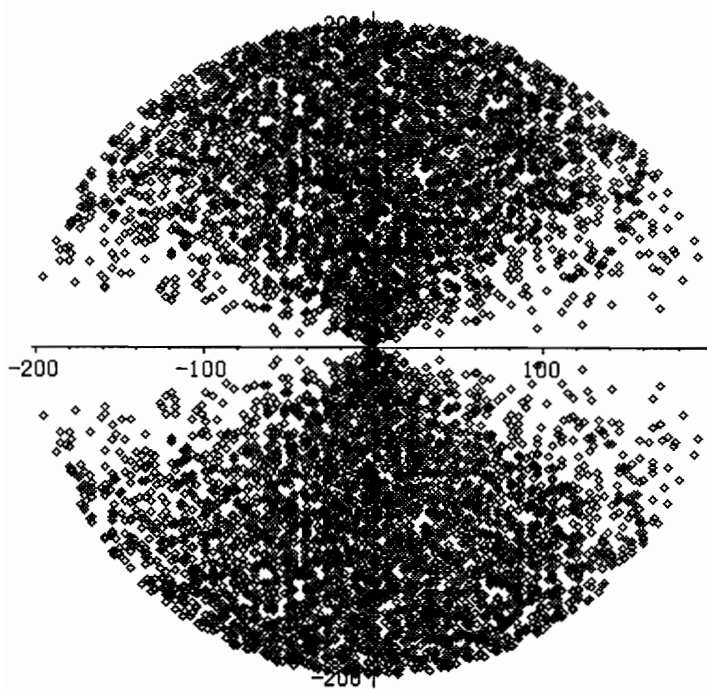
$$x = \sqrt[5]{e^{iA}}$$



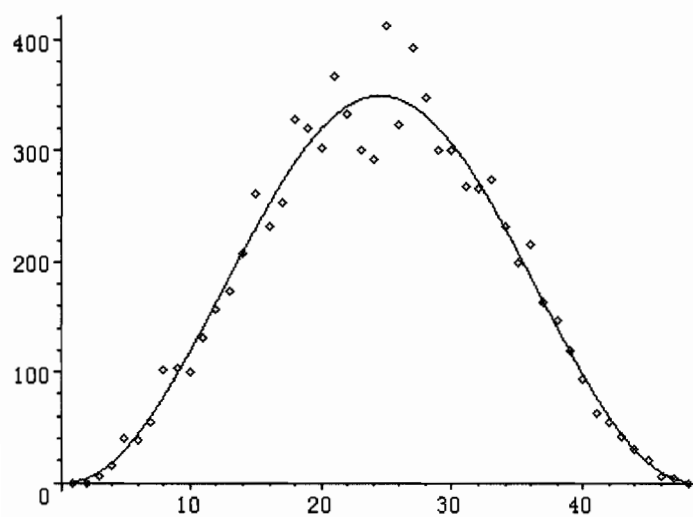
$$\eta(\tau)^2 \eta(5\tau)^2$$

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

$$p = 2n+1 \ (3 \sim 39989)$$



angular distribution

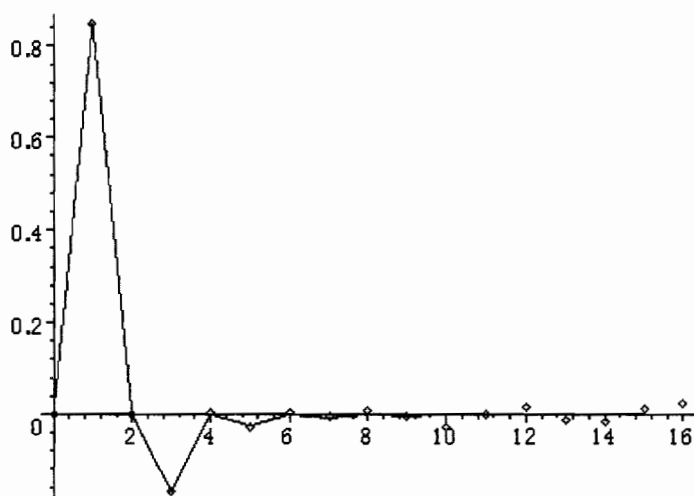


frequency

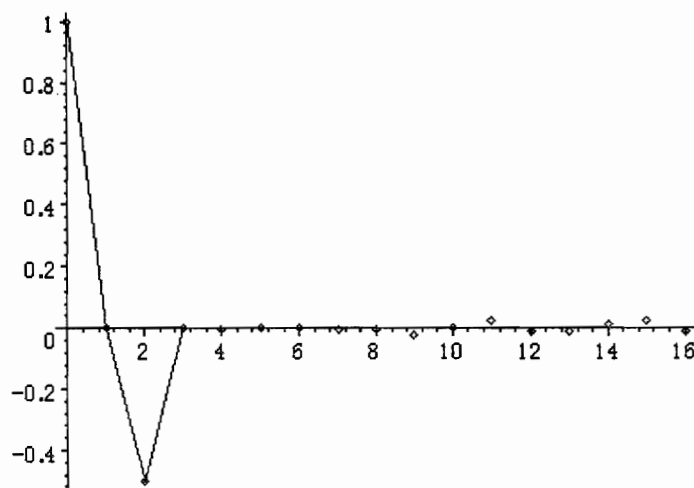
$p = 3 \sim 39989$ (8404 primes)

[[1, 0], [2, 0], [3, 6], [4, 16], [5, 40], [6, 38], [7, 54], [8, 102],
 [9, 104], [10, 100], [11, 132], [12, 158], [13, 174], [14, 208], [15, 262], [16, 232],
 [17, 254], [18, 328], [19, 320], [20, 302], [21, 368], [22, 334], [23, 300], [24, 292],
 [25, 414], [26, 324], [27, 394], [28, 348], [29, 300], [30, 300], [31, 268], [32, 266],
 [33, 274], [34, 232], [35, 200], [36, 216], [37, 164], [38, 148], [39, 120], [40, 94],
 [41, 62], [42, 54], [43, 42], [44, 30], [45, 20], [46, 6], [47, 4], [48, 0]]

Fourier sin coefficients



Fourier cos coefficients

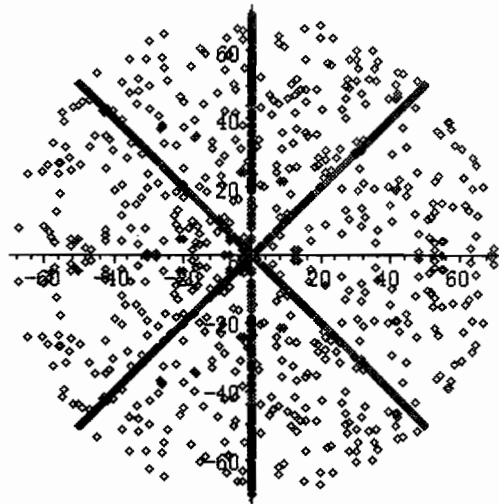


$$C: y^2 = x^5 - 2$$

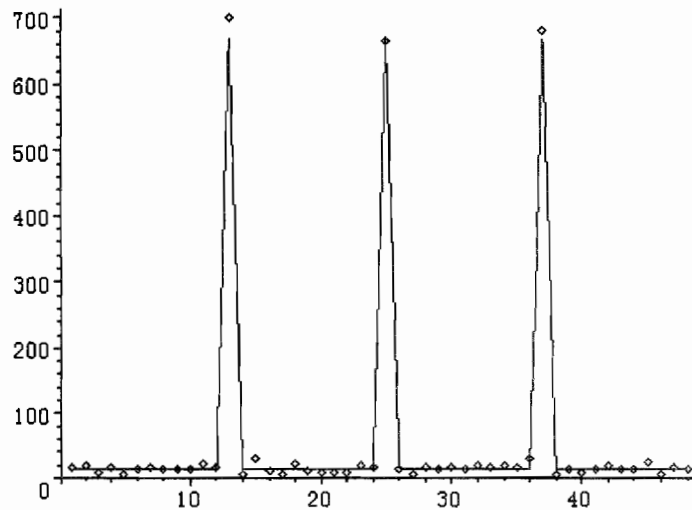
angular distribution of resultant transform

$$x^4 + a_p x^3 + b_p x^2 + a_p p x + p^2 = 0$$

$$p = 3 \sim 5003 \text{ (2676 roots)}$$



uniform distribution and point distribution at $\pi/4, \pi/2, 3\pi/4$
with each of them weight $1/4$.



for $p = 2, 3 \pmod{5}$

$$x^4 + a_p x^3 + b_p x^2 + a_p p x + p^2 = x^4 + p^2$$

for $p = 4 \pmod{5}$

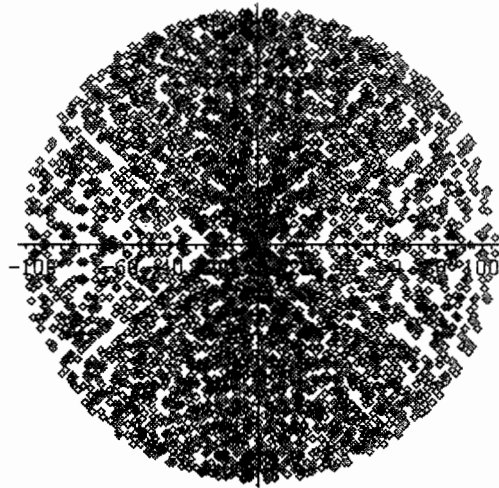
$$x^4 + a_p x^3 + b_p x^2 + a_p p x + p^2 = (x^2 + p)^2$$

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

angular distribution of resultant transform

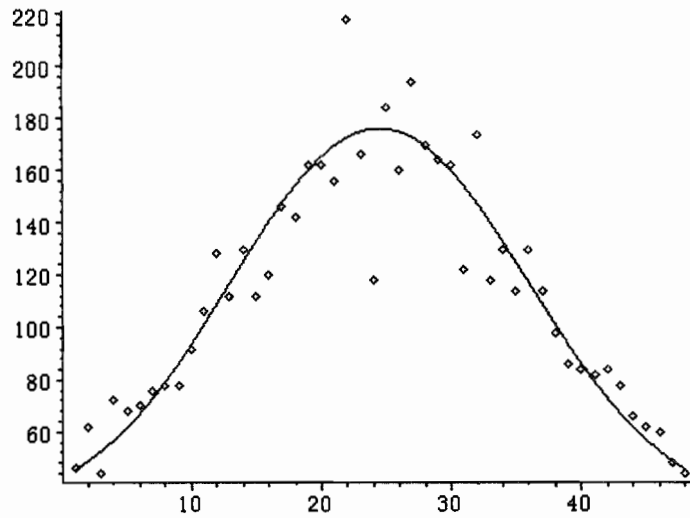
$$x^4 + a_p x^3 + b_p x^2 + a_p p x + p^2 = 0$$

$$p = 3 \sim 11197 \text{ (5420 roots)}$$



(supposed distribution)

$$1 + \sin(x) + \sin^2(x) + \sin^3(x)$$



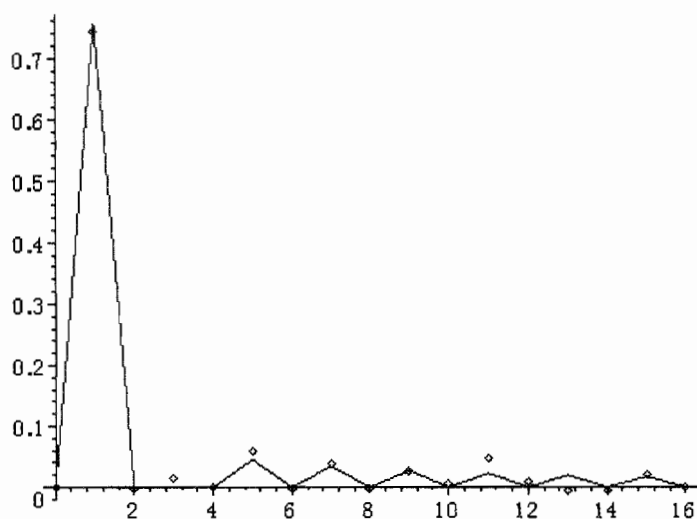
though, the distribution is only for a trial, but it is sure that, it is different from both

$$\sin^2 x, \sin^2 x + \sin^2 2x.$$

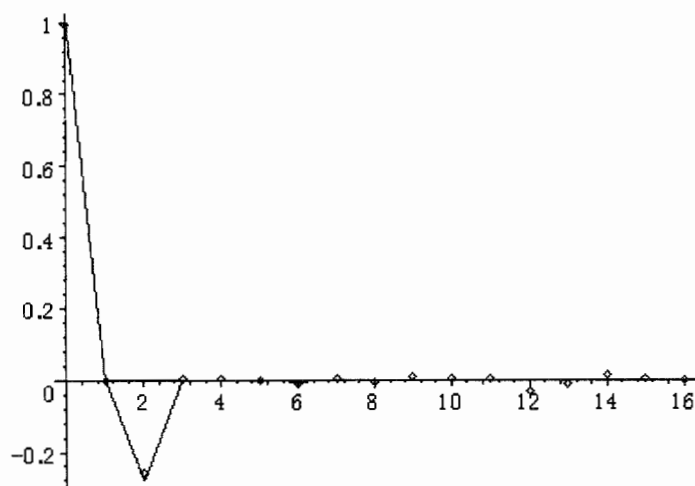
(note that density at $0, \pi$ seems to be $1/4$)

$[1, 46], [2, 62], [3, 44], [4, 72], [5, 68], [6, 70], [7, 76], [8, 78],$
 $[9, 78], [10, 92], [11, 106], [12, 128], [13, 112], [14, 130], [15, 112], [16, 120],$
 $[17, 146], [18, 142], [19, 162], [20, 162], [21, 156], [22, 218], [23, 166], [24, 118],$
 $[25, 184], [26, 160], [27, 194], [28, 170], [29, 164], [30, 162], [31, 122], [32, 174],$
 $[33, 118], [34, 130], [35, 114], [36, 130], [37, 114], [38, 98], [39, 86], [40, 84],$
 $[41, 82], [42, 84], [43, 78], [44, 66], [45, 62], [46, 60], [47, 48], [48, 44]]$

Fourier sin coefficient
 $1 + \sin(x) + \sin^2(x) + \sin^3(x)$



Fourier cos coefficient

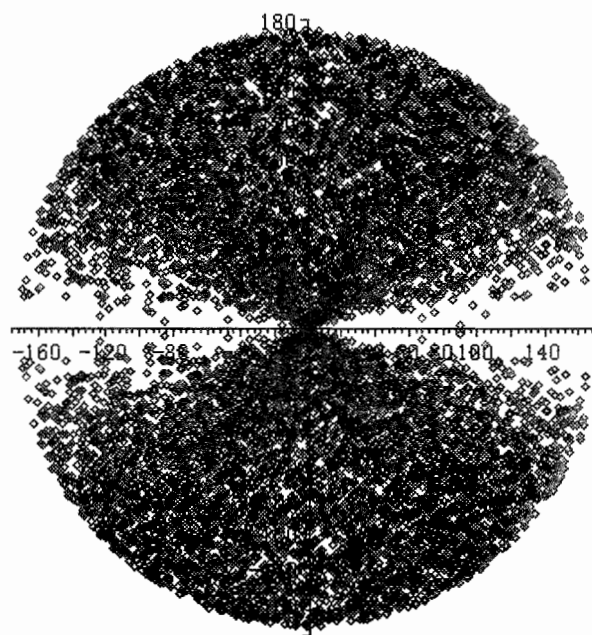


$$y^2 = x^4 + 5x + 5$$

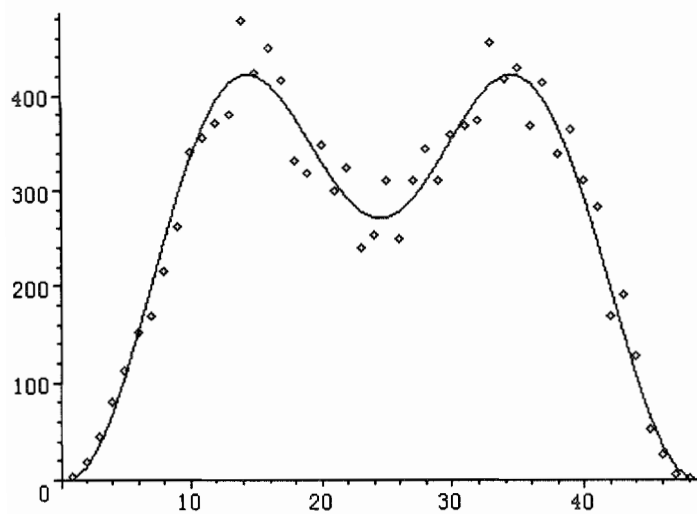
angular distribution of resultant transform

$$x^4 - a_p x^3 + b_p x^2 - a_p p x + p^2 = 0$$

$p = 3 \sim 30047$ (12992 roots)



angular distribution

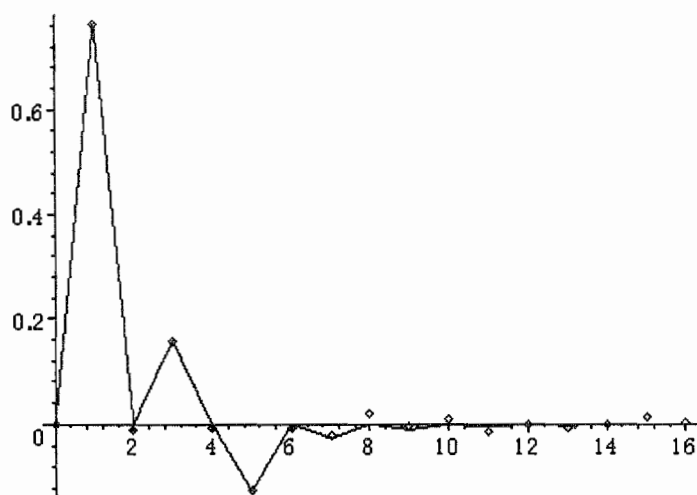


frequency

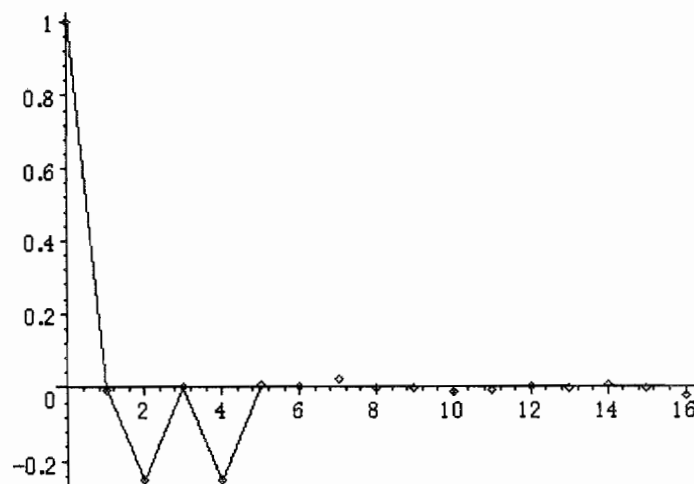
(12992 points)

[[1, 4], [2, 18], [3, 44], [4, 80], [5, 112], [6, 152], [7, 168], [8, 216],
[9, 262], [10, 342], [11, 356], [12, 372], [13, 380], [14, 478], [15, 424], [16, 450],
[17, 416], [18, 332], [19, 318], [20, 348], [21, 300], [22, 324], [23, 240], [24, 254],
[25, 312], [26, 250], [27, 312], [28, 346], [29, 312], [30, 360], [31, 370], [32, 376],
[33, 456], [34, 418], [35, 430], [36, 370], [37, 414], [38, 340], [39, 366], [40, 312],
[41, 284], [42, 168], [43, 192], [44, 128], [45, 52], [46, 26], [47, 6], [48, 2]]

Fourier sin coefficients



Fourier cos coefficients



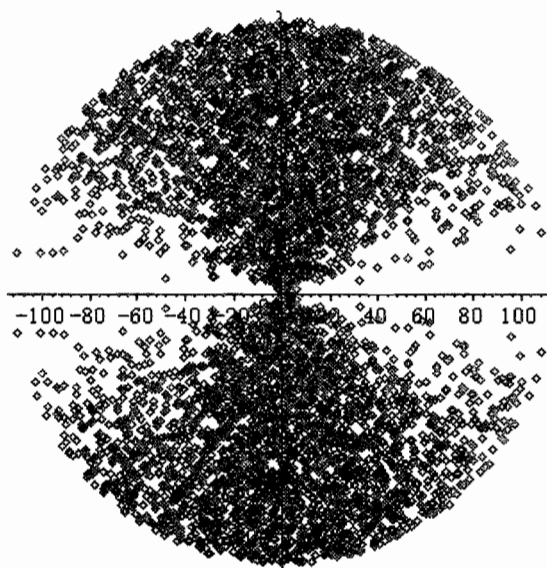
$$y^2 = x^5 - x^3 - 2x^2 - 2x - 1$$

angular distribution of resultant transform

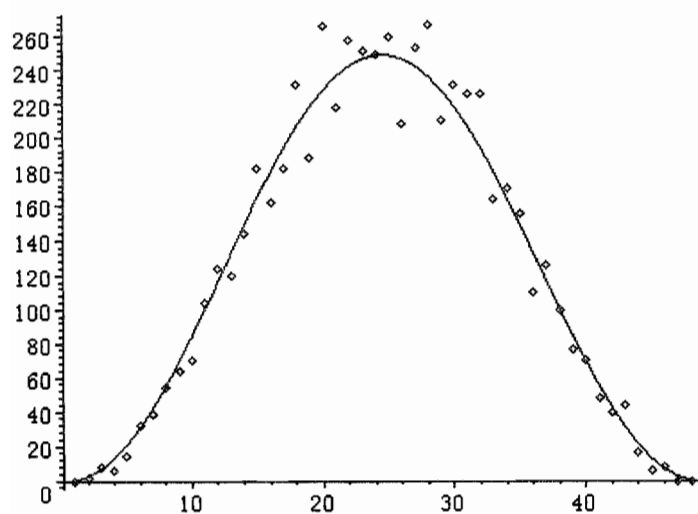
$$\det(f(x)) = 47^2$$

$$x^4 - a_p x^3 + b_p x^2 - p a_p x + p^2 = 0$$

$$p = 3 \sim 12541 \text{ (5988 primes)}$$



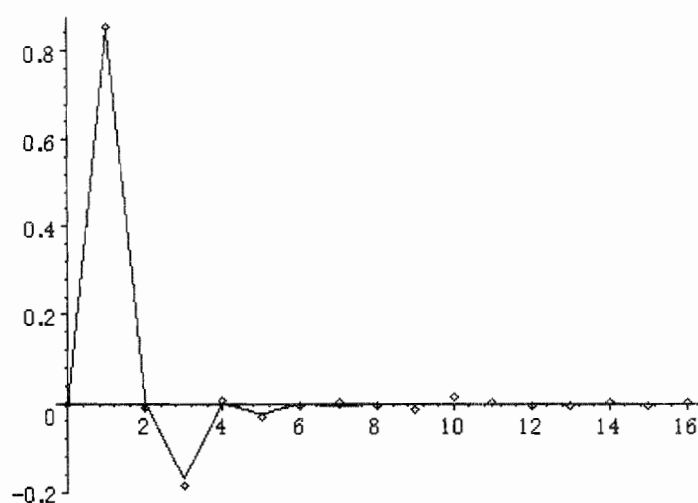
angular distribution



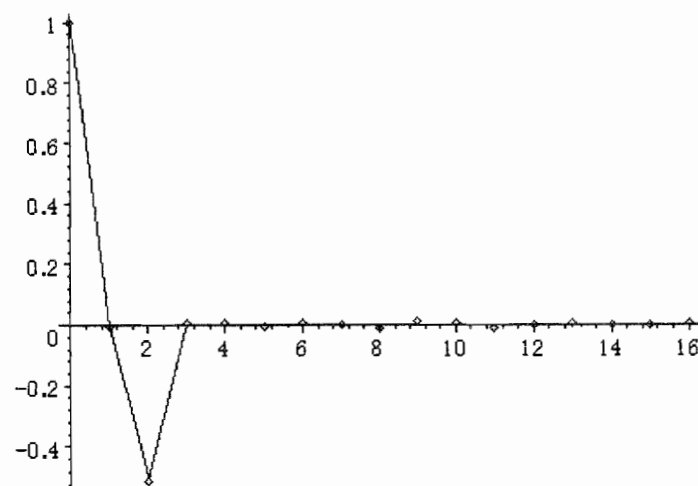
frequency

$[1, 0]$, $[2, 2]$, $[3, 8]$, $[4, 6]$, $[5, 14]$, $[6, 32]$, $[7, 38]$, $[8, 54]$,
 $[9, 64]$, $[10, 70]$, $[11, 104]$, $[12, 124]$, $[13, 120]$, $[14, 144]$, $[15, 182]$, $[16, 162]$,
 $[17, 182]$, $[18, 232]$, $[19, 188]$, $[20, 266]$, $[21, 218]$, $[22, 258]$, $[23, 252]$, $[24, 250]$,
 $[25, 260]$, $[26, 208]$, $[27, 254]$, $[28, 268]$, $[29, 210]$, $[30, 232]$, $[31, 226]$, $[32, 226]$,
 $[33, 164]$, $[34, 170]$, $[35, 156]$, $[36, 110]$, $[37, 126]$, $[38, 100]$, $[39, 76]$, $[40, 70]$,
 $[41, 48]$, $[42, 40]$, $[43, 44]$, $[44, 16]$, $[45, 6]$, $[46, 8]$, $[47, 0]$, $[48, 0]$

Fourier sin coefficients



Fourier cos coefficients

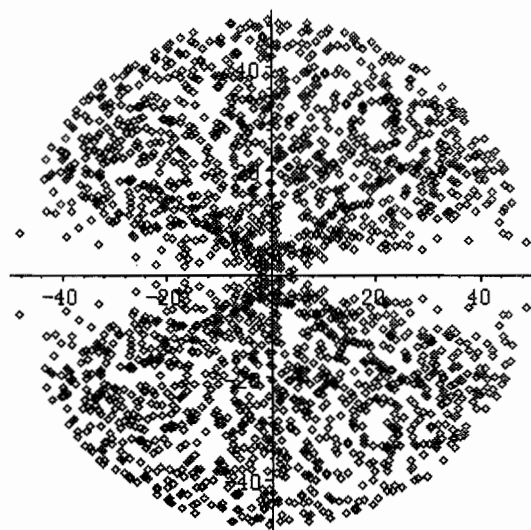


$$y^2 = x^7 + x^6 - x^5 + x^3 - x^2 - x + 1$$

angular distribution of resultant transform

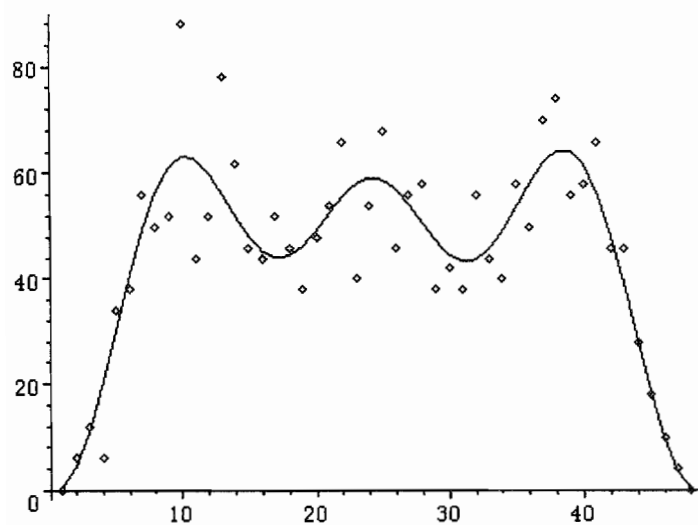
$$x^6 + a_p x^5 + b_p x^4 + c_p x^3 + b_p p x^2 + a_p p^2 x + p^3 = 0$$

$$p = 3 \sim 2411$$



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

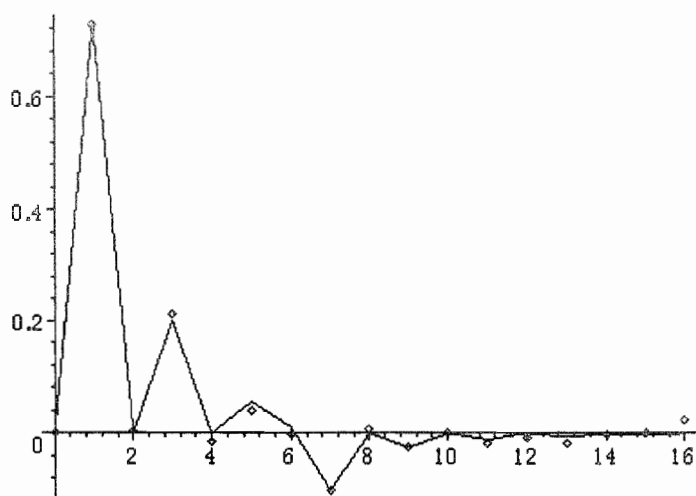
$$p = 3 \sim 2411 \text{ (2136 roots)}$$



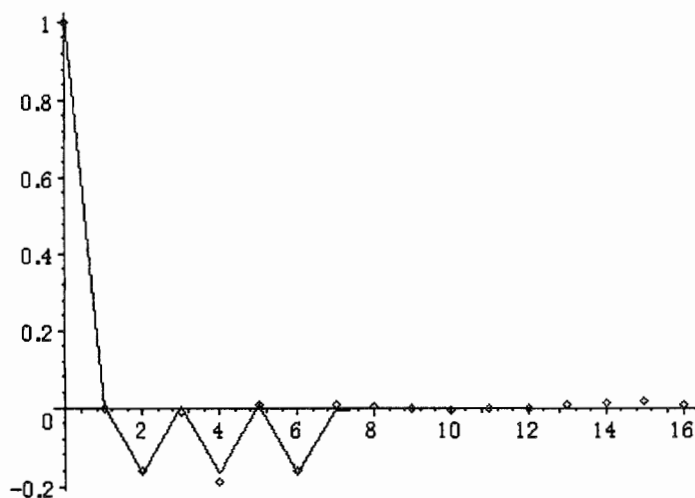
2136 roots

[[1, 0], [2, 6], [3, 12], [4, 6], [5, 34], [6, 38], [7, 56], [8, 50],
[9, 52], [10, 88], [11, 44], [12, 52], [13, 78], [14, 62], [15, 46], [16, 44],
[17, 52], [18, 46], [19, 38], [20, 48], [21, 54], [22, 66], [23, 40], [24, 54],
[25, 68], [26, 46], [27, 56], [28, 58], [29, 38], [30, 42], [31, 38], [32, 56],
[33, 44], [34, 40], [35, 58], [36, 50], [37, 70], [38, 74], [39, 56], [40, 58],
[41, 66], [42, 46], [43, 46], [44, 28], [45, 18], [46, 10], [47, 4], [48, 0]]

Fourier sin coefficients



Fourier cos coefficients

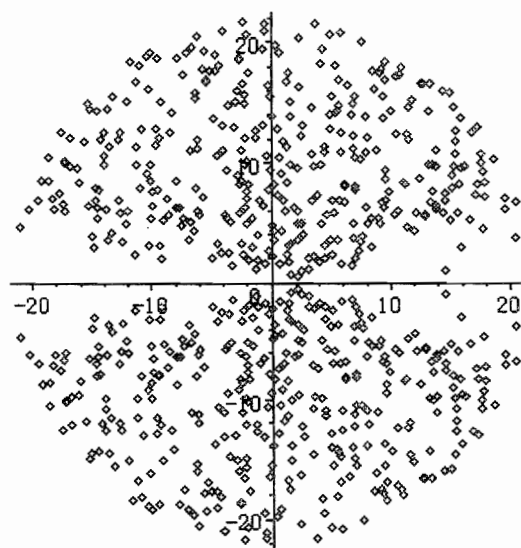


$$y^2 = x^9 - 2x^7 - x^4 - 4x^3 + 2x^2 + 2x - 1$$

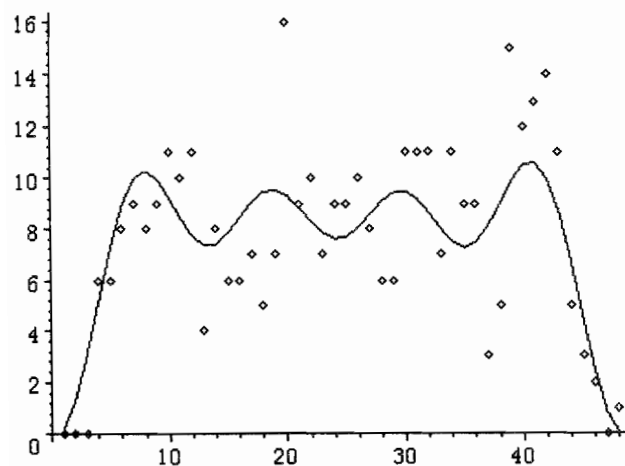
angular distribution of resultant transform

$$x^8 + a_p x^7 + b_p x^6 + c_p x^5 + d_p x^4 + c_p p x^3 + b_p p^2 x^2 + a_p p^3 x + p^4 = 0$$

$$p = 3 \sim 479$$



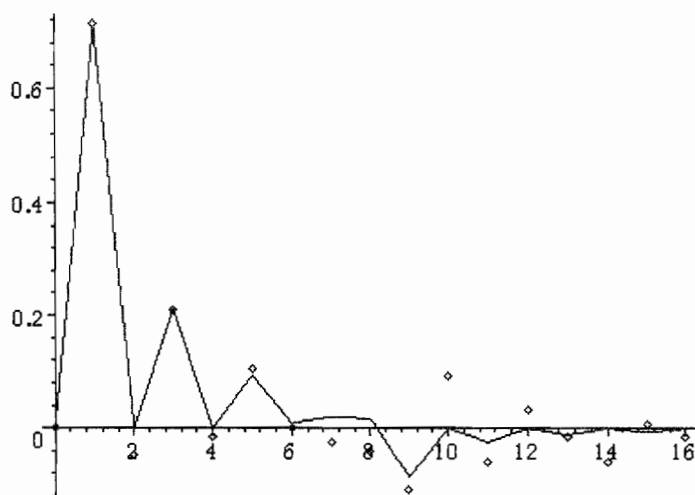
$$\sin^2(x) + \sin^2(2x) + \sin^2(3x) + \sin^2(4x)$$



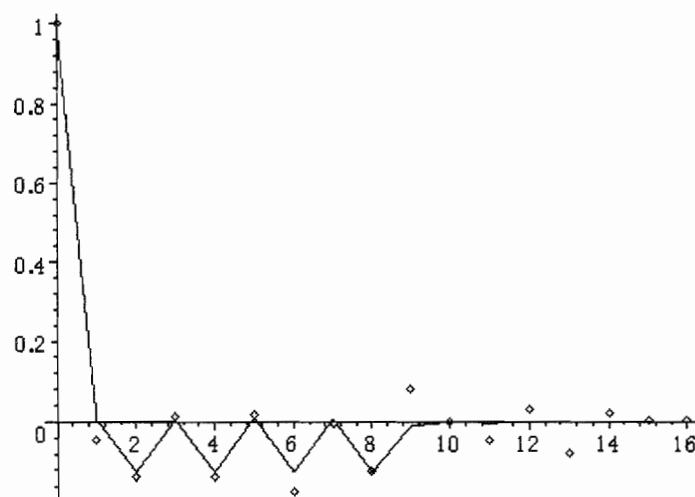
364 roots

[[1, 0], [2, 0], [3, 0], [4, 6], [5, 6], [6, 8], [7, 9], [8, 8],
 [9, 9], [10, 11], [11, 10], [12, 11], [13, 4], [14, 8], [15, 6], [16, 6],
 [17, 7], [18, 5], [19, 7], [20, 16], [21, 9], [22, 10], [23, 7], [24, 9],
 [25, 9], [26, 10], [27, 8], [28, 6], [29, 6], [30, 11], [31, 11], [32, 11],
 [33, 7], [34, 11], [35, 9], [36, 9], [37, 3], [38, 5], [39, 15], [40, 12],
 [41, 13], [42, 14], [43, 11], [44, 5], [45, 3], [46, 2], [47, 0], [48, 1]]

Fourier sin coefficients



Fourier cos coefficients



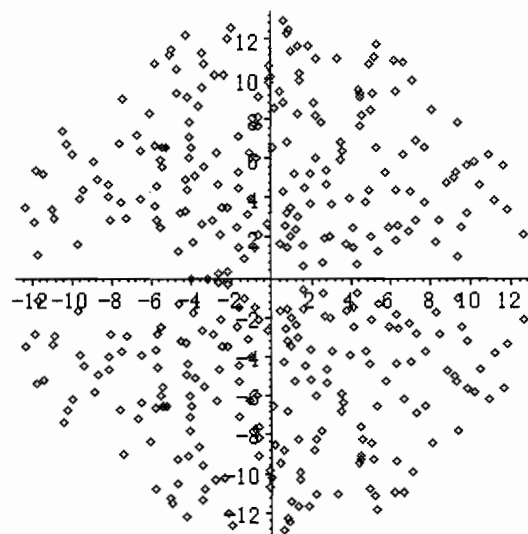
$$y^2 = x^{11} + x^8 + x^5 + x^2 + 1$$

$$\det(f(x)) = f(x) \otimes f'(x) = 13 \cdot 89 \cdot 173 \cdot 1531031$$

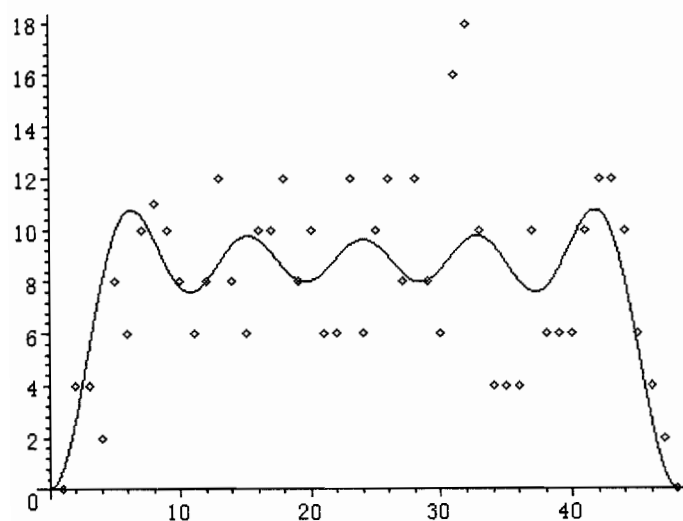
angular distribution of resultant transform

$$x^{10} + a_p x^9 + b_p x^8 + c_p x^7 + d_p x^6 + e_p x^5 + d_p p x^4 + c_p p^2 x^3 + b_p p^3 x^2 + a_p p^4 x + p^5 = 0$$

$$p = 3 \sim 167$$



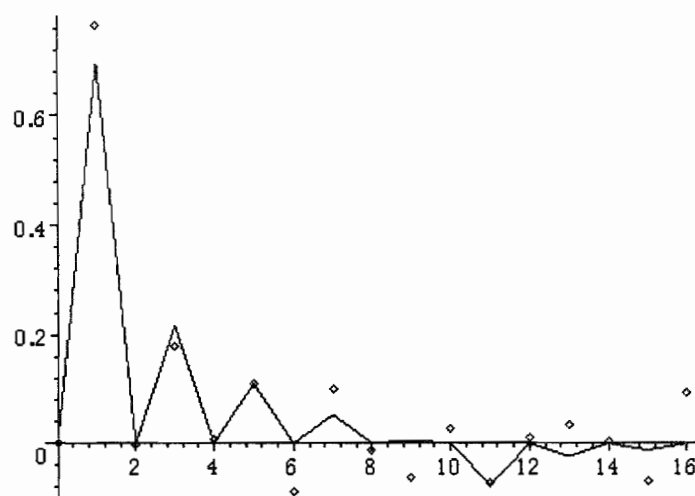
$$\sin^2(x) + \sin^2(2x) + \sin^2(3x) + \sin^2(4x) + \sin^2(5x)$$



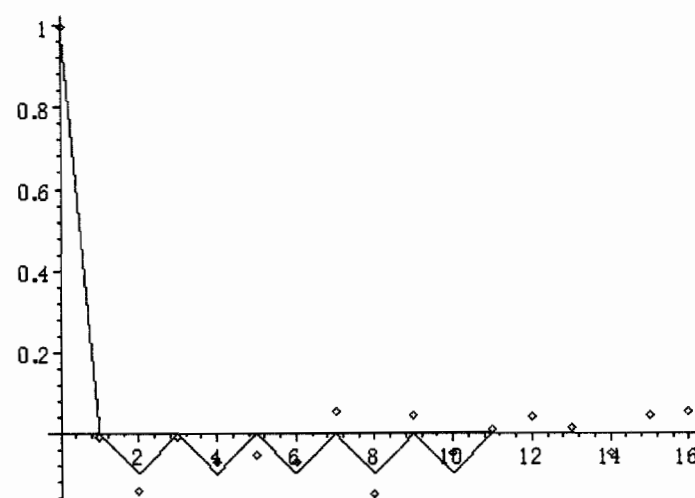
380 roots

[[1, 0], [2, 4], [3, 4], [4, 2], [5, 8], [6, 6], [7, 10], [8, 11],
 [9, 10], [10, 8], [11, 6], [12, 8], [13, 12], [14, 8], [15, 6], [16, 10],
 [17, 10], [18, 12], [19, 8], [20, 10], [21, 6], [22, 6], [23, 12], [24, 6],
 [25, 10], [26, 12], [27, 8], [28, 12], [29, 8], [30, 6], [31, 16], [32, 18],
 [33, 10], [34, 4], [35, 4], [36, 4], [37, 10], [38, 6], [39, 6], [40, 6],
 [41, 10], [42, 12], [43, 12], [44, 10], [45, 6], [46, 4], [47, 2], [48, 0]]

Fourier sin coefficients



Fourier cos coefficients



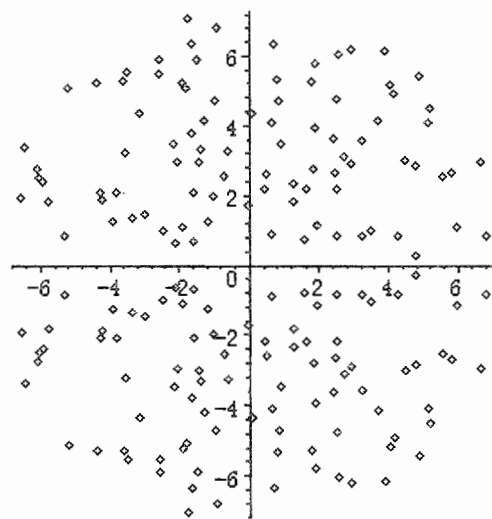
$$y^2 = x^{13} - x^{11} + x^7 + x^5 + x^3 + x^2 + x + 1$$

$$\det(f(x)) = f(x) \otimes f'(x) = 2^2 \cdot 31 \cdot 71 \cdot 227 \cdot 1427 \cdot 3750917$$

angular distribution of resultant transform

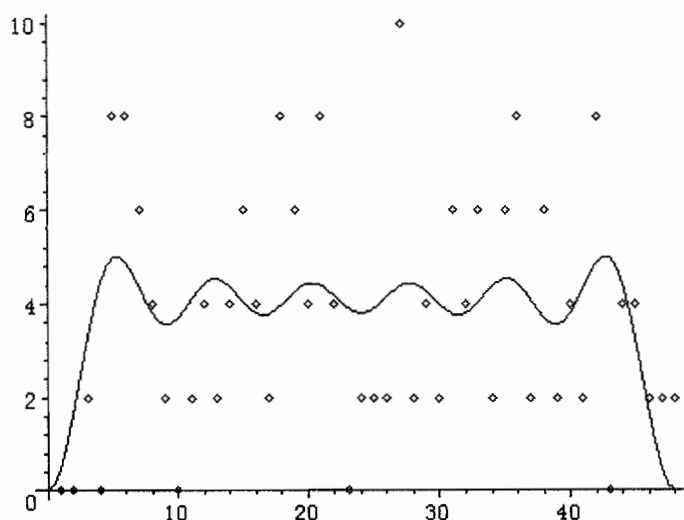
$$x^{12} + a_p x^{11} + b_p x^9 + c_p x^9 + d_p x^8 + e_p x^7 + f_p x^6 + e_p p x^5 + d_p p^2 x^4 + c_p p^3 x^3 + b_p p^4 x^2 + a_p p^5 x + p^6 = 0$$

$$p = 3 \sim 53$$



$$\sin^2(x) + \sin^2(2x) + \sin^2(3x) + \sin^2(4x) + \sin^2(5x) + \sin^2(6x)$$

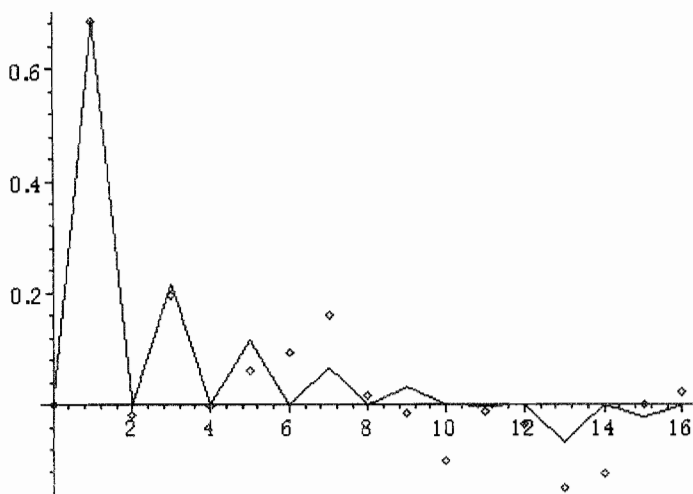
(supposed to be)



180 roots

[[1, 0], [2, 0], [3, 2], [4, 0], [5, 8], [6, 8], [7, 6], [8, 4],
 [9, 2], [10, 0], [11, 2], [12, 4], [13, 2], [14, 4], [15, 6], [16, 4],
 [17, 2], [18, 8], [19, 6], [20, 4], [21, 8], [22, 4], [23, 0], [24, 2],
 [25, 2], [26, 2], [27, 10], [28, 2], [29, 4], [30, 2], [31, 6], [32, 4],
 [33, 6], [34, 2], [35, 6], [36, 8], [37, 2], [38, 6], [39, 2], [40, 4],
 [41, 2], [42, 8], [43, 0], [44, 4], [45, 4], [46, 2], [47, 2], [48, 2]]

Fourier sin coefficients



Fourier cos coefficients

