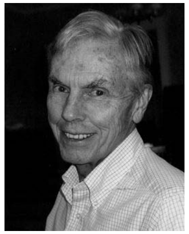
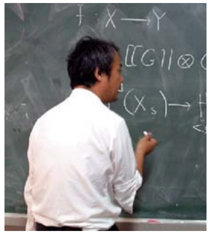
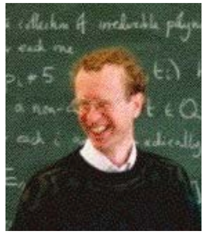
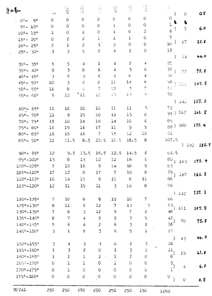
日本数学会・企画特別講演　　　　2009年3月26日(木) 13:00〜14:00

# 佐藤 - テイト予想の解決と展望

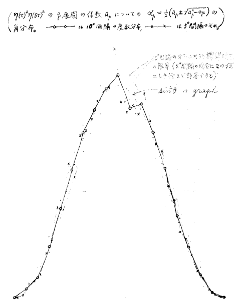
## —— 非可換類体論の進展 ——




伊藤 哲史

京都大学大学院理学研究科数学教室

# はじめに

整数論・数論幾何関連分野における大きな進展.

**2006** 年 佐藤 - テイト予想 **(**楕円曲線の **mod** $p$ 有理点の個数の分布**)**

クローゼル，ハリス，シェパード＝バロンとの共同研究に基づき

テイラーが **(**多くの場合に**)** 解決

**2007** 年 セール予想 **(**$\mathbb{Q}$ の **2** 次元 **mod** $\ell$ ガロア表現の保型性予想**)**

テイラー，キシンの画期的な仕事を受けて，

カーレ，ヴァンテンベルジェが解決

ワイルズ，テイラーによる谷山 - 志村予想，フェルマーの最終定理の証明の手法をさらに一般化・精密化することで証明.

# この講演では

- 佐藤 - テイト予想とは

  —— 今までは“果てしなく難しい予想” と思われていた.

- 証明の背後にある「非可換類体論」「ガロア表現の保型性予想」
- セール予想とは
- 佐藤 - テイト予想・セール予想の証明の方針

  現代数論幾何の深い定理を総動員.（ゼータ関数・$L$関数，保型表現の様々な“持ち上げ”，志村多様体，エタールコホモロジー，保型表現に伴うガロア表現，ガロア表現の変形・枠付き変形）

- 最近の進展・今後の展望

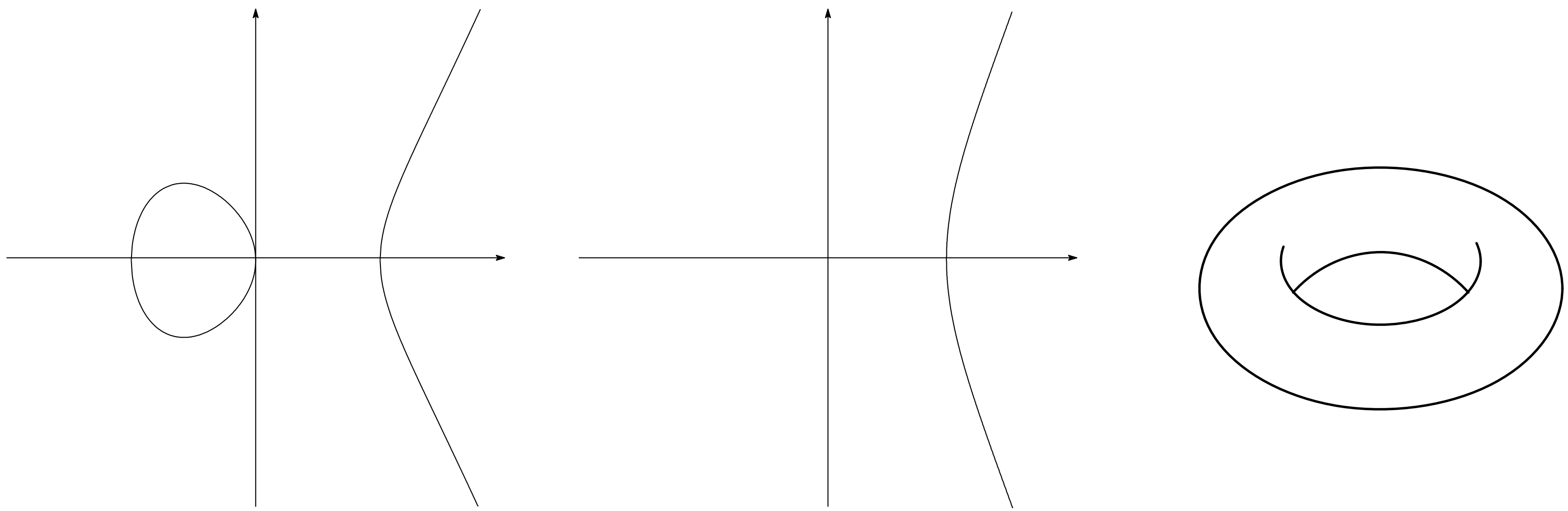
などについて，傍観者の視点から紹介する.

# 佐藤 - テイト予想

楕円曲線とは，**3**次方程式

$$E : y^2 = x^3 + ax + b \quad (a, b\text{は整数，}4a^3 + 27b^2 \neq 0)$$

で定義された曲線のこと．**(**注：楕円曲線**(3**次式**)** $\neq$ 楕円**(2**次式**))**



種数**1**の代数曲線．$\mathbb{C}$上ではドーナツの形**(2**次元トーラス**)**

整数論，代数幾何学，複素関数論，位相幾何学などで深く研究

楕円曲線 $E : y^2 = x^3 + ax + b$ ($a, b$は整数, $4a^3 + 27b^2 \neq 0$)の整数論的性質を研究したい.

$p \geqq 5$ : $4a^3 + 27b^2$を割らない素数 (“良い” 素数)

$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ : 位数$p$の有限体

四則演算ができる. ($p$で割った余りを同一視する. )

$$\begin{aligned}\#E(\mathbb{F}_p) &= \bigl(E\text{の}\mathbb{F}_p\text{-有理点の個数}\bigr)\\ &= \#\Bigl\{(x, y) \Bigm| x, y\text{は整数, } 0 \leqq x, y \leqq p-1,\\ &\qquad\qquad y^2-(x^3+ax+b)\text{が}p\text{で割り切れる}\Bigr\} + 1 \quad (\text{無限遠点})\end{aligned}$$

<u>問題</u> (楕円曲線の非可換相互法則)

$p$を動かしたとき, $\{\#E(\mathbb{F}_p)\}_p$はどのように分布するか?

**定理 (ハッセ, 1933年)**

$$p+1-2\sqrt{p} \ \leqq\ \#E(\mathbb{F}_p)\ \leqq\ p+1+2\sqrt{p}$$

そこで,

$$p+1-\#E(\mathbb{F}_p)=2\sqrt{p}\cos\theta_p \qquad (0\leqq\theta_p\leqq\pi)$$

とおく.

**問題 (楕円曲線の非可換相互法則(2))**

$p$を動かしたとき，ハッセの定理の“誤差項”を表す角度$\{\theta_p\}_p$はどのように分布するか？

## 佐藤 - テイト予想 (佐藤幹夫，1963年春)

$E: y^2 = x^3 + ax + b$ ($a, b$は整数, $4a^3 + 27b^2 \neq 0$)

$E$は虚数乗法を持たないと仮定する.

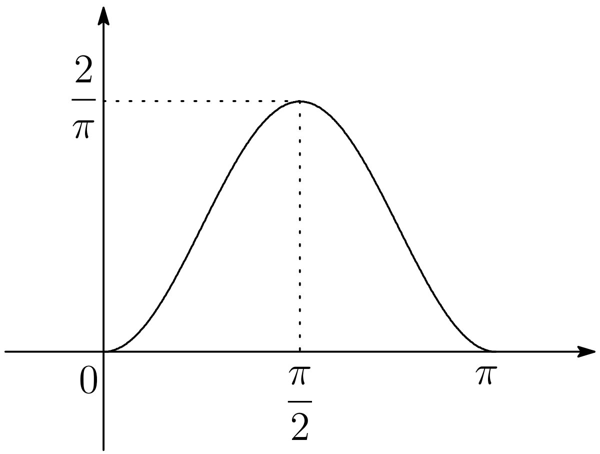
$\theta_p$ ($0 \leqq \theta_p \leqq \pi$) を$p + 1 - \#E(\mathbb{F}_p) = 2\sqrt{p}\cos\theta_p$で定める.

このとき，任意の$0 \leqq \alpha < \beta \leqq \pi$に対し，以下が成り立つ.

$$\lim_{N\to\infty} \frac{\#\{p \mid p\text{は素数，} p \leqq N\text{，} \alpha \leqq \theta_p \leqq \beta\}}{\#\{p \mid p\text{は素数，} p \leqq N\}} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta\, d\theta$$

『角度$\{\theta_p\}_p$は $y = \frac{2}{\pi}\sin^2\theta$

のグラフの形に分布する』



2006年春： クローゼル，ハリス，シェパード=バロン，テイラーが
(多くの場合に)佐藤 - テイト予想を解決.

Publ. Math. IHES 108 (2008), 1–181 & 183–239, Ann. of Math. (to appear)




定理　もし，$E$ の $j$-不変量

$$j(E) = \frac{1728 \cdot 4a^3}{4a^3 + 27b^2}$$

が整数でなければ，佐藤 - テイト予想は正しい.

より一般に総実代数体上の楕円曲線 $E$ で $j(E)$ が代数的整数でないものに対し，同様の定理を証明している.

# 佐藤 - テイト予想・非可換類体論の歴史

**1963年** 「佐藤予想」の定式化，「テイト予想」の提出

**1968年** セール「$\ell$進アーベル表現と楕円曲線」，対称積$L$関数

**1970年〜** 保型表現論の進展，保型$L$関数の研究，保型表現の様々な
“持ち上げ定理”，非可換類体論の定式化(ラングランズ予想)
エタールコホモロジー，ヴェイユ予想・ラマヌジャン予想の解決

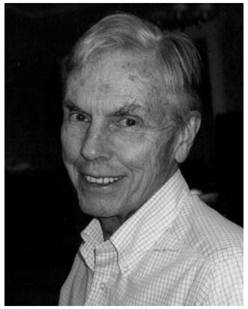
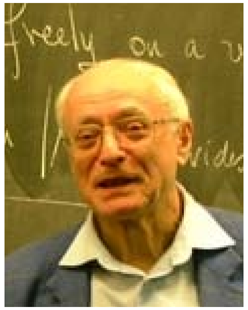
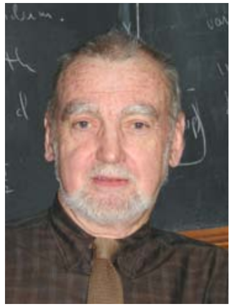
**1980年〜** 志村多様体論の進展，岩澤主予想(メイザー - ワイルズ)
ガロア表現・$p$進ホッジ理論の進展

**1990年〜** 谷山 - 志村予想(半安定な場合)，フェルマーの最終定理
$\mathbf{GL}_n$の局所ラングランズ予想（$n$次元非可換局所類体論）

**2001年〜** 谷山 - 志村予想の完全解決，佐藤 - テイト予想(多くの場合)
セール予想の解決，$\mathbf{GL}_2(\mathbb{Q}_p)$の$p$進ラングランズ対応の確立

1963年春： 計算機による実験結果に基づき佐藤幹夫が予想

テイト，セールが$L$関数を用いて理論的背景を整理

アイデア　ゼータ関数・$L$関数を定義する．それらの解析的性質(極・零の位置など)から，素数に関する密度定理を得る．

密度定理の例　算術級数定理 (ディリクレ)，素数定理 (アダマール，ド・ラ・ヴァレ＝プーサン)

$\boxed{\text{佐藤 - テイト予想 ＝ “非可換密度定理”}}$

## $L$ 関数・対称積 $L$ 関数

$$\alpha_p = \sqrt{p}e^{i\theta_p},\ \ \beta_p = \sqrt{p}e^{-i\theta_p}$$ **(フロベニウス元 Frob$_p$ の固有値)**

$$L(s,E) = \prod_p \frac{1}{(1-\alpha_p\,p^{-s})(1-\beta_p\,p^{-s})}$$ **($L$ 関数)**

$$L(s,E,\mathbf{Sym}^n) = \prod_p \prod_{k=0}^{n} \frac{1}{1-\alpha_p^k\,\beta_p^{n-k}\,p^{-s}}$$ **(対称積 $L$ 関数)**

楕円曲線に伴う $\ell$ 進ガロア表現の対称積

$$\mathbf{Sym}^n\rho_{E,\ell}\colon \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}_2(\overline{\mathbb{Q}}_\ell) \longrightarrow \mathbf{GL}_{n+1}(\overline{\mathbb{Q}}_\ell)$$

は既約表現で，その $L$ 関数は $L(s,E,\mathbf{Sym}^n)$ に等しい．

**定理** **(テイト，セール)**　もし，

『$L(s,E,\mathbf{Sym}^n)$ が $\mathbf{Re}(s) \geqq 1+\frac{n}{2}$ で正則かつ零点を持たない』

ならば，佐藤 - テイト予想は正しい．

方針　$L(s, E, \mathbf{Sym}^n)$を保型形式・保型表現の$L$関数と結びつけることで，その解析的性質を調べる.

非可換類体論によれば，$(n+1)$次元ガロア表現$\mathbf{Sym}^n\rho_{E,\ell}$は保型的であるはず．すなわち，

$$L(s+\tfrac{n}{2}, \mathbf{Sym}^n\rho_{E,\ell}) = L(s+\tfrac{n}{2}, E, \mathbf{Sym}^n) = L(s, \pi)$$

をみたす$\mathbf{GL}_{n+1}(\mathbb{A}_{\mathbb{Q}})$の保型表現$\pi$が存在するはず.

**(**$n=1$の場合が谷山 - 志村予想．**)**

$\Rightarrow$ 対称積$L$関数$L(s, E, \mathbf{Sym}^n)$が良い解析的性質を持つ

$\Rightarrow$ 佐藤 - テイト予想

クローゼル，ハリス，シェパード＝バロン，テイラーは，$\mathbf{Sym}^n \rho_{E,\ell}$ に対する非可換類体論を弱い形 (**$\mathbf{Sym}^n \rho_{E,\ell}$ の潜保型性**) で証明し，その系として佐藤 - テイト予想を証明した．(**保型性は未解決**)

**定理** (クローゼル，ハリス，シェパード＝バロン，テイラー)
任意の奇数 $m$ に対し，総実代数体 $F/\mathbb{Q}$ が存在して，任意の奇数 $n \leq m$ に対し，$\mathbf{Sym}^n \rho_{E,\ell}$ の制限

$$(\mathbf{Sym}^n \rho_{E,\ell})|_F : \mathbf{Gal}(\overline{F}/F) \longrightarrow \mathbf{GL}_{n+1}(\overline{\mathbb{Q}}_\ell)$$

は保型的である．

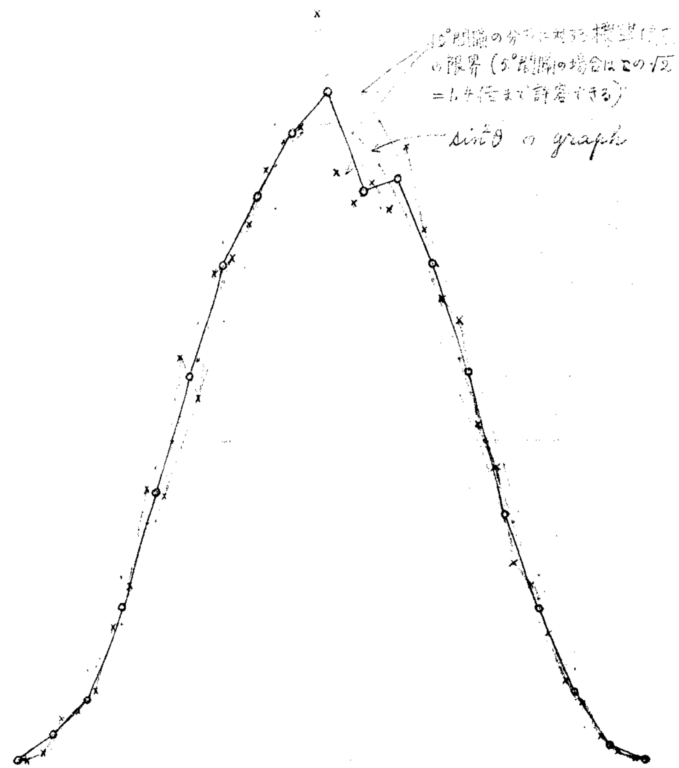
この定理 ＋ ブラウアー誘導定理 ＋ "$\alpha$"
(アーサー - クローゼル基底変換定理 (の逆)，ランキン - セルバーグ積)

$\Rightarrow$ 佐藤 - テイト予想

# 資料１（数値実験結果．10°間隔の度数分布）

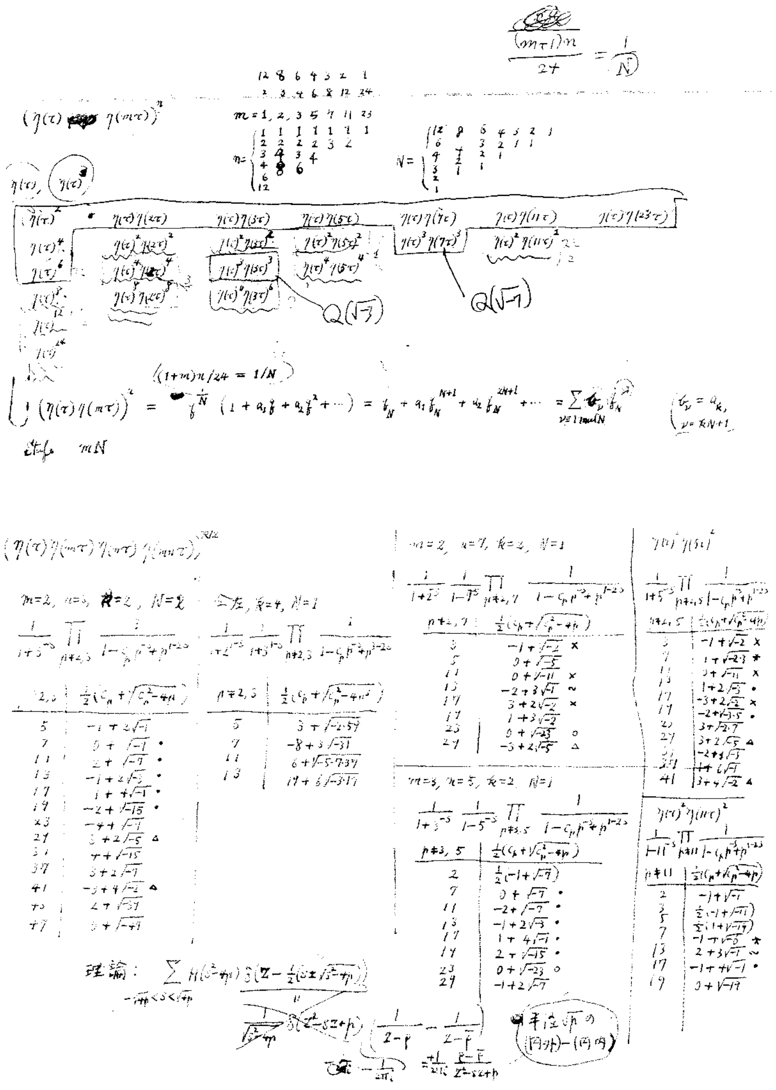
| 第二表 | | | | | | | | | ) 0 | 0.5 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0°- 5° | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | |
| 5°- 10° | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | | |
| 10°- 15° | 1 | 0 | 2 | 0 | 1 | 0 | 2 | 6 | ) 7 | 6.0 |
| 15°- 20° | 0 | 2 | 2 | 1 | 1 | 1 | 0 | 7 | | |
| 20°- 25° | 2 | 1 | 2 | 3 | 2 | 0 | 0 | 10 | ) 17 | 21.8 |
| 25°- 30° | 3 | 3 | 5 | 2 | 4 | 2 | 0 | 19 | | |
| | | | | | | | | | ) 44 | 46.0 |
| 30°- 35° | 5 | 5 | 4 | 1 | 4 | 2 | 4 | 25 | | |
| 35°- 40° | 9 | 3 | 8 | 6 | 4 | 3 | 6 | 39 | ) 77 | 75.8 |
| 40°- 45° | 3 | 9 | 3 | 6 | 5 | 8 | 4 | [illegible] | | |
| 45°- 50° | 10 | 3 | 6 | 8 | 11 | 14 | 6 | 58 | ) [illegible] | 107.5 |
| 50°- 55° | 11 | 8 | [illegible] | 7 | 10 | 3 | 7 | [illegible] | | |
| 55°- 60° | 5 | 12 | 11 | 10 | 10 | 13 | [illegible] | 70 | | |
| | | | | | | | | | ) 142 | 137.3 |
| 60°- 65° | 11 | 16 | 10 | 10 | 11 | 11 | 3 | 72 | | |
| 65°- 70° | 11 | 9 | 15 | 10 | 11 | 13 | 8 | 77 | ) 162 | 161.5 |
| 70°- 75° | 15 | 10 | 14 | 16 | 14 | 10 | 6 | 85 | | |
| 75°- 80° | 16 | 15 | 16 | 17 | 11 | 9 | 5 | 89 | ) 180 | 177.4 |
| 80°- 85° | 16 | 15 | 16 | 7 | 15 | 12 | 10 | 91 | | |
| 85°- 90° | 12 | 21.5 | 8.5 | 22.5 | 16.5 | 18.5 | 8 | 107.5 | | |
| | | | | | | | | | ) 192 | 182.4 |
| 90°- 95° | 12 | 9.5 | 13.5 | 16.5 | 12.5 | 14.5 | 6 | 84.5 | | |
| 95°-100° | 13 | 8 | 13 | 12 | 12 | 16 | 6 | 80 | ) 163 | 177.4 |
| 100°-105° | 7 | 10 | 16 | 9 | 14 | 18 | 9 | 83 | | |
| 105°-110° | 17 | 12 | 8 | 17 | 7 | 10 | 8 | 79 | ) 167 | 161.5 |
| 110°-115° | 16 | 14 | 15 | 9 | 15 | 8 | 11 | 88 | | |
| 115°-120° | 12 | 11 | 15 | 11 | 3 | 16 | 8 | 76 | | |
| | | | | | | | | | ) 142 | 137.3 |
| 120°-125° | 7 | 10 | 8 | 9 | 15 | 10 | 7 | 66 | | |
| 125°-130° | 8 | 11 | 9 | 12 | 7 | 13 | 3 | 63 | ) 111 | 107.5 |
| 130°-135° | 7 | 8 | 3 | 12 | 9 | 7 | 2 | 48 | | |
| 135°-140° | 8 | 7 | 4 | 6 | 9 | 3 | 5 | 42 | ) 70 | 75.8 |
| 140°-145° | 5 | 6 | 4 | 2 | 6 | 3 | 2 | 28 | | |
| 145°-150° | 3 | 1 | 6 | 3 | 6 | 5 | 1 | 25 | | |
| | | | | | | | | | ) 43 | 46.0 |
| 150°-155° | 3 | 4 | 3 | 3 | 0 | 2 | 3 | 18 | | |
| 155°-160° | 1 | 3 | 2 | 0 | 1 | 3 | 1 | 11 | ) 19 | 21.8 |
| 160°-165° | 1 | 1 | 1 | 2 | 1 | 2 | 0 | 8 | | |
| 165°-170° | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 3 | ) 4 | 6.0 |
| 170°-175° | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | | |
| 175°-180° | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ) 0 | 0.5 |
| TOTAL | 250 | 250 | 250 | 250 | 250 | 250 | 150 | 1650 | | |

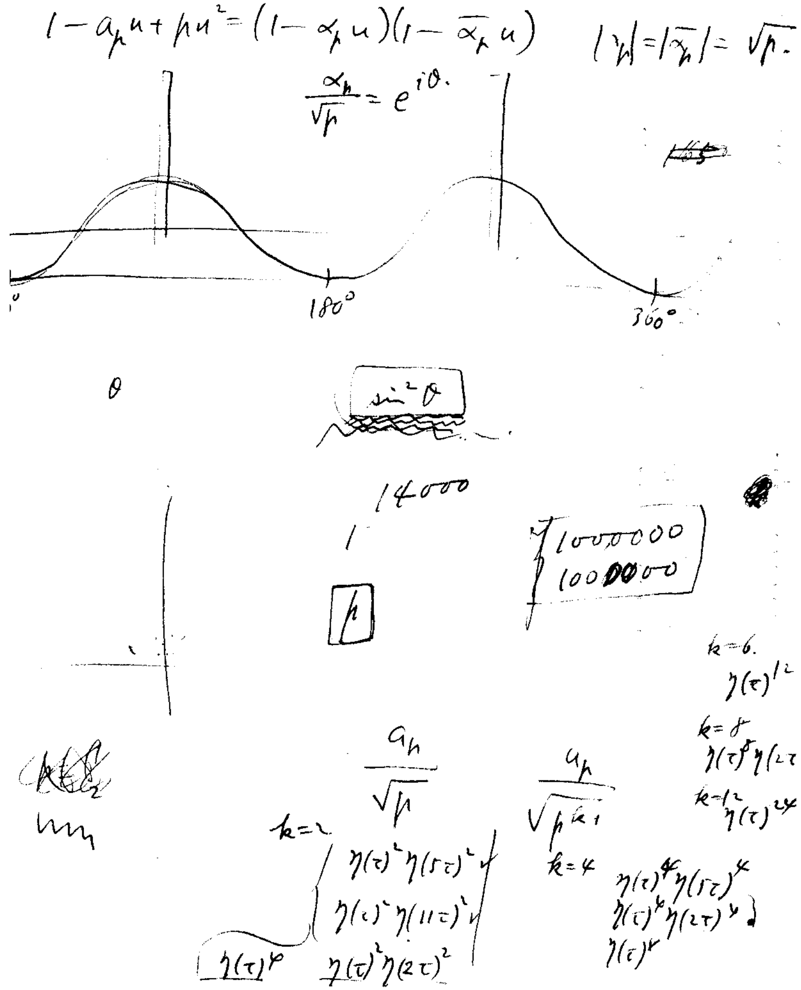
（$\eta(\tau)^2\eta(5\tau)^2$ の $q$ 展開の係数 $a_p$ についての $\alpha_p = \frac{1}{2}(a_p \pm \sqrt{a_p^2 - 4p})$ の角分布。—○—○— は 10° 間隔の度数分布，—×—×— は 5° 間隔のそれ。）




- 難波完爾,『Dedekind$\eta$関数と佐藤sin$^2$-予想』, 2006津田塾大学, 数学・計算機科学研究所，第16回数学史シンポジウム報告集

# 資料２（「佐藤予想」について議論した時の計算用紙)



# 資料3 (1963年5月13日，佐藤幹夫から難波完爾への手紙)

難波 完二様　　　　5月13日

その后も元気のことと思います。　こちらも、大阪へ移ってひと月あまり経ち だいぶ当地にも慣れて来ました。大学の研究仲間についても、いま住んでいる下宿の環境についても申分ないと思いますが、研究以外の雑用がむ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ら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service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母数型式

$$\eta(\tau)^2\eta(5\tau)^2=\sum_{l\equiv 1(\mathrm{mod}\,2)} a_n q^l$$

の係数 $a_p$ $(p\neq 2,5;\ p<14000)$

について、$1-a_p u+pu^2=(1-\alpha_p u)(1-\overline{\alpha_p}\,u)$ と因数分解したときの

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

の偏角 $\theta_p$ の分布を、永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 i, ii は永島君に作ってもらったdataのコピー。

第二表は、第1列が $p=3,7,11,\cdots$ 以下250番目まで、第2列が $p=1607$ (251番目) から500番目まで、最右の列が $p=12583$ (1501番目) から13777 (1650番目) まで。Totalの欄の右側は、角度を10°区切りにあらくした場合の度数分布。一番右は、分布が $\sin^2\theta$ に比例するものと仮定して、各々のsectionにおける期待値を

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

に比例するように計算したもの。

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、期待値からのズレの大きさを示す標準偏差を点線で示しておきました。（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分布で代用できる。そうすると、図中の平均値を $N\ \left(=\frac{1650}{18}=91.7\right)$ とすると、期待値の曲線は $2N\cdot\sin^2\theta$，標準偏差は $\sqrt{2N\cdot\sin^2\theta}=\sqrt{2N}\cdot\sin\theta$ 従って点線の曲線は $2N\cdot\sin^2\theta\pm\sqrt{2N}\cdot\sin\theta$ となる）

図と表とから推定されるように、

$\alpha_p$ の角分布が $\sin^2\theta$ に比例する。

と言う仮説は極めて確からしいと言えます。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ぶ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theoryな頭脳労働は気が重いので、それはしばらく後廻しにして、もう少しいろいろと、筋肉労働で実行できる資料収集を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っ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気でいます。

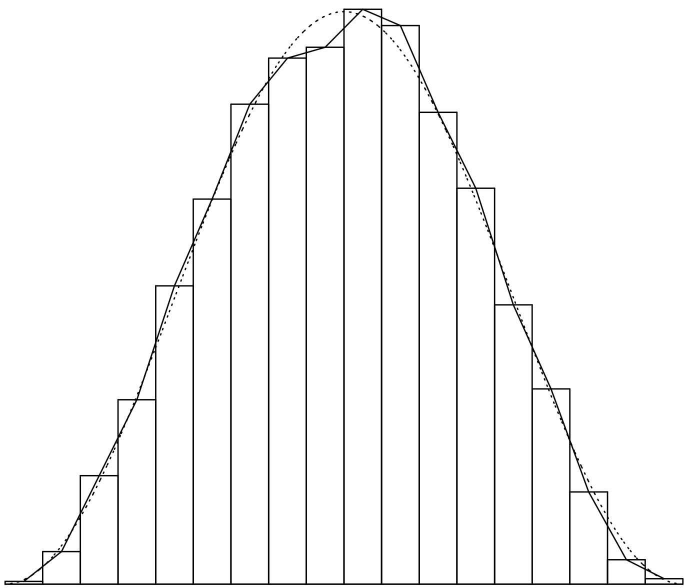
「数理科学」に載せるための原稿もそのうち書くつもりです。書き上げたら、あと、計算のプログラムに関することを君に書き足してもらおうと思います。いずれにせよ、なるべく学会のときまでには或程度目鼻をつけたいと思います。

$\eta(\tau)^2\eta(5\tau)^2$ 以外の分、つまり $\eta(\tau)^2\eta(11\tau)^2$, $\eta(\tau)^4\eta(5\tau)^4$, $\eta(\tau)^4\eta(2\tau)^4$, $\eta(\tau)^6\eta(2\tau)^6$, $\eta(\tau)^{12}$, $\eta(\tau)^{24}$ などについても、永島君のProgramを使って、$\theta_p$ の分布表を作ってくれませんか。僕の予想では、これらはすべて上と同じ $\sin^2\theta$ 型則に従うだろうと、期待しているのですが。

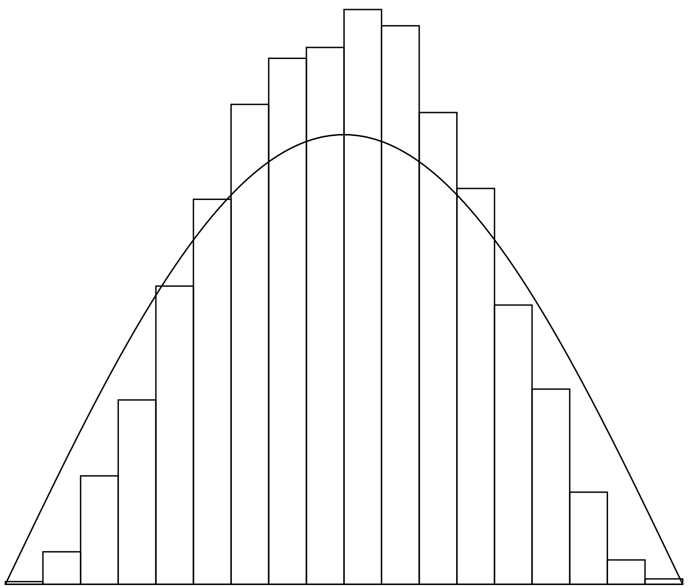
$p\gg 14000$ なる $p$ について、全然別の方法で $a_p$ を求められることを、最近ちょっと会ったとき話しましたが、あれは memory 容量が（命令の分以外は）殆んど不要なので、試作中の HITAC 5020 を利用させて貰うことが出来れば、おあつらえ向きゆえ、夏ころまでに出来れば plan を準備したいと思っています。

## 資料４ (導手11の楕円曲線での実験結果．最初の1900個の素数(11を除く)で計算)

| | | | | | |
|---|---|---|---|---|---|
| $0^\circ \le \theta < 10^\circ$ | 1 | $60^\circ \le \theta < 70^\circ$ | 177 | $120^\circ \le \theta < 130^\circ$ | 146 |
| $10^\circ \le \theta < 20^\circ$ | 12 | $70^\circ \le \theta < 80^\circ$ | 194 | $130^\circ \le \theta < 140^\circ$ | 103 |
| $20^\circ \le \theta < 30^\circ$ | 40 | $80^\circ \le \theta < 90^\circ$ | 198 | $140^\circ \le \theta < 150^\circ$ | 72 |
| $30^\circ \le \theta < 40^\circ$ | 68 | $90^\circ \le \theta < 100^\circ$ | 212 | $150^\circ \le \theta < 160^\circ$ | 34 |
| $40^\circ \le \theta < 50^\circ$ | 110 | $100^\circ \le \theta < 110^\circ$ | 206 | $160^\circ \le \theta < 170^\circ$ | 9 |
| $50^\circ \le \theta < 60^\circ$ | 142 | $110^\circ \le \theta < 120^\circ$ | 174 | $170^\circ \le \theta \le 180^\circ$ | 2 |

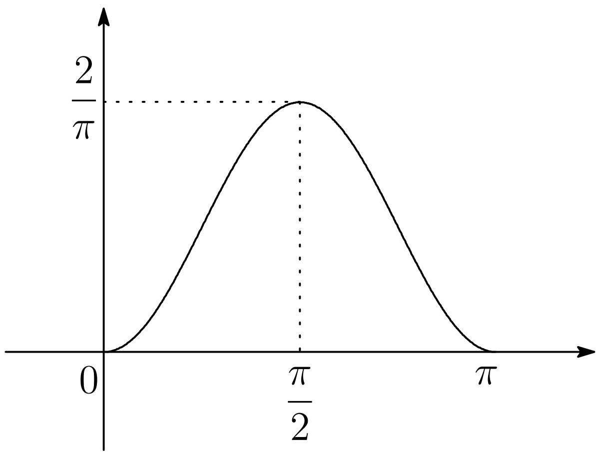


$\sin^2\theta$と比較



$\sin\theta$と比較

## 資料５（類似に注目）




と

は似ている !?

# 資料6 (銅鐸の進化，sin $\rightarrow$ sin$^2$)

$\longrightarrow$


# セール予想

セール予想は「$\mathbb{Q}$の2次元 mod $\ell$ ガロア表現の保型性予想」である.

まずは，類体論について簡単に復習.

**$\mathbb{Q}$の類体論** **(＝ 円分体論 ＝ Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)の1次元表現の保型性)**

「$\mathbb{Q}$のアーベル拡大は円分拡大$\mathbb{Q}(\zeta_N)$ $(\zeta_N = e^{2\pi i/N})$に含まれる」

「1次元ガロア表現 $\rho$: **Gal**$(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$に対し，

ディリクレ指標**(GL$_1$**$(\mathbb{A}_\mathbb{Q})$の保型表現**)** $\chi: (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$

が存在し，両者の$L$関数が一致する **(**$\rho$は$\chi$に伴う**)**」

これを代数体に一般化したのが高木貞治，アルチンによる類体論.

## 代数体の類体論　(高木貞治，アルチン(~1920年代))

「アーベル体は類体である」

「$F$を代数体とする．1次元ガロア表現 $\rho\colon \mathbf{Gal}(\overline{F}/F) \to \mathbb{C}^\times$に対し，

　ヘッケ指標(**GL**$_1(\mathbb{A}_F)$の保型表現) $\chi\colon \mathbb{A}_F^\times/F^\times \to \mathbb{C}^\times$が存在し，

　両者の$L$関数が一致する」

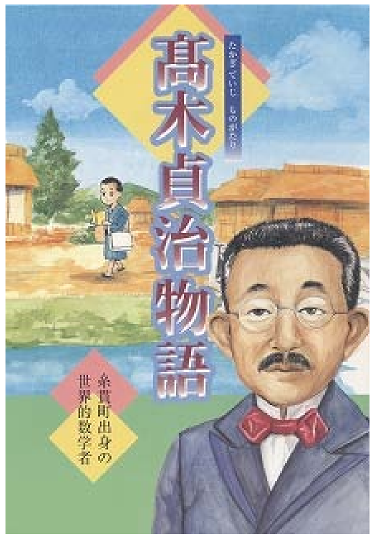
(**Gal**$(\overline{F}/F)$の**1**次元表現の保型性)

## クロネッカーの青春の夢

『虚二次体$F$のアーベル拡大は楕円関数

　の等分点での値で生成される』

高木類体論の完成とともに解決.



<u>非可換類体論</u>とは，$L$ 関数を保つ対応

$$\boxed{n\text{次元ガロア表現} \leftrightarrow \mathbf{GL}_n(\mathbb{A}_{\mathbb{Q}})\text{の保型表現}}$$

<u>ガロア表現</u>とは，連続準同型 $\rho$: $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}(V)$ のこと．

$V$ は体 $k$ 上の有限次元ベクトル空間． $k = \mathbb{C}$ のとき $\rho$ をアルチン表現，

$k = \overline{\mathbb{Q}}_\ell$ のとき $\rho$ を $\ell$ 進表現， $k = \overline{\mathbb{F}}_\ell$ のとき $\rho$ を **mod** $\ell$ 表現という．

$$\boxed{\text{ガロア表現は代数学・方程式論の世界の対象}}$$

保型形式 (= $\mathbf{GL}_2(\mathbb{A}_{\mathbb{Q}})$ の保型表現) とは正則関数

$$f\colon \left\{z\in\mathbb{C}\ \middle|\ \mathrm{Im}(z)>0\right\}\longrightarrow\mathbb{C}$$

であって，保型性をみたすもの.

$$f\left(\frac{az+b}{cz+d}\right)=\varepsilon(d)(cz+d)^k f(z)\qquad \left(ad-bc=1,\ c\text{ は }N\text{ の倍数}\right)$$

$\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times\to\mathbb{C}^\times$ を指標，$k$ を重さ，$N$ をレベルという.

例 $$\Delta(q)=q\prod_{n=1}^{\infty}(1-q^n)^{24}=\sum_{n=1}^{\infty}\tau(n)q^n\qquad (q=e^{2\pi iz})$$

は重さ **12**，レベル **1** の保型形式. **(**ラマヌジャンの $\Delta$ 関数**)**

$\boxed{\text{保型形式は解析学・表現論の世界の対象}}$

## 「保型側$\Rightarrow$ガロア側」(保型形式に伴うガロア表現の構成)

定理 (アイヒラー，志村五郎，ドリーニュ，セール (~1970年代))

$f = \sum_{n=1}^{\infty} a_n q^n$ を保型形式(尖点的，ヘッケ作用素の同時固有形式)とする．既約な2次元$\ell$進表現($f$に伴うガロア表現) $\rho\colon \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}_2(\overline{\mathbb{Q}}_\ell)$ が存在して，ほとんど全ての$p$に対し $\mathbf{Tr}\,\rho(\mathbf{Frob}_p) = a_p$ をみたす．

$\mathbf{Frob}_p$はフロベニウス元．$\rho$は「奇」($\mathbf{det}\,\rho$(複素共役) $= -1$)．

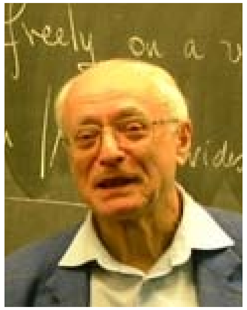
$k \geqq 2$のときは，モジュラー曲線のエタールコホモロジーをヘッケ作用素で分解して作る．$k = 1$のときは，保型形式の合同性を使って重さが大きい場合に帰着．

セール予想（「ガロア側$\Rightarrow$保型側」の**mod $\ell$ バージョン**，**1987年**)

「奇」な2次元既約 mod $\ell$ 表現$\overline{\rho}$: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ に対し，保型形式$f = \sum_{n=1}^{\infty} a_n q^n$が存在して，ほとんど全ての$p$に対し $\mathrm{Tr}\,\overline{\rho}(\mathrm{Frob}_p) \equiv a_p \pmod{\ell}$ をみたす.

定理 (カーレ，ヴァンテンベルジェ (2007年))

セール予想は正しい.

※ $\overline{\rho}$の分岐の様子から，$f$の**レベル**や**重さ**を具体的に決定できる.

- 定理の主張は「**1** つの **mod** $\ell$ 表現」に関するものだが，証明はとても難しい．総実代数体上のヒルベルト保型形式に伴う$\ell$進表現に関するありとあらゆるテクニックを総動員．

- 可約なガロア表現はアイゼンシュタイン級数に伴う．

- 「偶」なガロア表現にはマースの波動形式が伴うと予想されているが,「保型側$\Rightarrow$ガロア側」「ガロア側$\Rightarrow$保型側」ともに未解決．

- セール予想は$\rho$の像が可解群の場合は知られていた(ラングランズ-タンネルの定理の系).(ワイルズによるフェルマーの最終定理の証明では「$\mathbf{GL}_2(\mathbb{F}_3)$が可解群」なことが本質的だった.)

- カーレ，ヴァンテンベルジェの定理の応用として得られるもの.
  - フェルマーの最終定理の“やさしい”別証明(ラングランズ-タンネルの定理，リベットのレベル下げ定理を使わない)
  - $\mathbf{GL}_2$型アーベル多様体やリジッドなカラビ-ヤウ多様体の保型性(谷山-志村予想の高次元版)
  - ２次元「奇」なアルチン予想：『奇な２次元既約アルチン表現$\rho$: $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}_2(\mathbb{C})$の$L$関数$L(s,\rho)$は複素平面全体で正則』

# 証明の方針

佐藤 - テイト予想・セール予想は，ともに，非可換類体論 (ガロア表現の保型性) を特別な場合に確立することにより証明される.

佐藤 - テイト予想 ＝ 高次元ガロア表現の非可換類体論の潜バージョン
$(\mathbf{Sym}^n \rho_{E,\ell})|_F$ の保型性 ($F/\mathbb{Q}$ は総実代数体)

セール予想 ＝ 2次元ガロア表現の非可換類体論の **mod** $\ell$ バージョン

証明には共通のテクニックが用いられる.

- ガロア表現の整合系を使って「$\ell$ を動かす」 (($\ell, \ell'$)- トリック)
- 保型性の持ち上げ定理 (ガロア表現の変形・枠付き変形，テイラー - ワイルズ系)

## ガロア表現の整合系

$\ell$進ガロア表現の整合系とは，$\ell$進ガロア表現の(素数$\ell$ごとの)集まり

$$\left\{\rho_\ell\colon \mathrm{\mathbf{Gal}}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{\mathbf{GL}}_n(\overline{\mathbb{Q}}_\ell)\right\}_\ell$$

であって，$L$関数$L(s,\rho_\ell)$が$\ell$によらないもののこと(谷山豊).

$E$を$\mathbb{Q}$上定義された楕円曲線とし，$\rho_{E,\ell}\colon \mathrm{\mathbf{Gal}}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{\mathbf{GL}}_2(\overline{\mathbb{Q}}_\ell)$をEの$\ell$進テイト加群から定まる2次元ガロア表現とする．$\{\rho_{E,\ell}\}_\ell$は整合系をなす．一般に，$\mathbb{Q}$上の代数多様体$X$に対し，$\ell$進エタールコホモロジーの集まり$\left\{H^*_{\text{ét}}(X\otimes_{\mathbb{Q}}\overline{\mathbb{Q}},\overline{\mathbb{Q}}_\ell)\right\}_\ell$は整合系をなす(と期待されている).

## 保型性の持ち上げ定理

$\ell$進ガロア表現 $\rho$: $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}_n(\overline{\mathbb{Q}}_\ell)$ が保型的なら，
$\rho \pmod{\ell}$: $\mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}_n(\overline{\mathbb{F}}_\ell)$ はもちろん保型的である．

ワイルズは，ある**(**技術的な**)**条件下で，この逆

「$\rho \pmod{\ell}$は保型的 $\Rightarrow$ $\rho$は保型的」

を示した**(**保型性の持ち上げ定理，テイラー - ワイルズ系の方法**)**．

ダイアモンド，藤原一宏，スキナー，キシンらにより多くの一般化・精密化が得られた．特に，$\rho \pmod{\ell}$が可約な場合**(**スキナー-ワイルズ**)**と，キシンによるガロア表現の枠付き変形を用いた精密化**(**とても弱い局所条件下での保型性の持ち上げ定理**)**が重要．

## 佐藤 - テイト予想の証明(概略)

整合系と保型性の持ち上げ定理を使って「保型性の道」をつなげる.

(($\ell, \ell'$)- トリック ： ワイルズによる(3, 5)- トリックの一般化)

カラビ - ヤウ多様体とモレ - ベイイーの定理を使って，総実代数体 $F/\mathbb{Q}$ と整合系 $\left\{\tau_\ell \colon \mathbf{Gal}(\overline{F}/F) \longrightarrow \mathbf{GL}_{n+1}(\overline{\mathbb{Q}}_\ell)\right\}_\ell$ であって，

$$\tau_\ell \equiv (\mathbf{Sym}^n \rho_{E,\ell})|_F \pmod{\ell}, \qquad \tau_{\ell'} \equiv \mathbf{Ind}_K^F \psi_K \pmod{\ell'}$$

($K$ は CM 体，$K/F$ は $(n+1)$ 次巡回拡大，$\psi_K$ はヘッケ指標)

となるものをうまく作る．すると，

「$\mathbf{Ind}_K^F \psi_K$ は保型的 $\Rightarrow$ $\mathbf{Ind}_K^F \psi_K \pmod{\ell'}$ は保型的

$\Rightarrow$ $\tau_{\ell'}$ は保型的 $\Rightarrow$ $\tau_\ell$ は保型的 $\Rightarrow$ $(\mathbf{Sym}^n \rho_{E,\ell})|_F$ は保型的」

だから，$\mathbf{Sym}^n \rho_{E,\ell}$ は潜保型的である．(技術的には枠付き変形を用いて伊原の補題を回避するところがポイント．)　**Q.E.D.**

## セール予想の証明(概略)

まず，2次元 **mod** $\ell$ 表現 $\overline{\rho}\colon \mathbf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL}_2(\overline{\mathbb{F}}_\ell)$ を，ガロア表現の整合系$\{\tau_\ell\}_\ell$に埋め込む．素数 $\ell' \neq \ell$ をとり，**mod** $\ell'$ 表現 $\tau_{\ell'}$ $(\mathrm{mod}\ \ell')$ を考える．これをどんどん繰り返す．レベル(**$\ell$の外の分岐**)を減らしていく．セールの重さ(**$\ell$での分岐**)も減らしていく．

『$\ell = 2, 3, 5$のときは，既約な2次元 **mod** $\ell$ガロア表現で$\ell$の外で不分岐なものは存在しない(セール，テイト，ブルメール，クラメール，スクーフ)』から，いつかは**mod** $\ell$表現は可約になってしまう．スキナー - ワイルズの定理を出発点にして，「保型性の道」をどんどん辿ると，最初に与えられた$\overline{\rho}$の保型性が分かる．**Q.E.D.**

## $\mathbf{GL}_2$の非可換類体論予想 —— 「奇」な場合は完成に近づく (キシン)

予想 (フォンテーヌ - メイザー ＋ ラングランズ予想)

$\rho$: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\overline{\mathbb{Q}}_\ell)$ を2次元既約$\ell$進表現とし，有限個の素数を除き不分岐で,「$\ell$でド・ラーム」と仮定する.

- $\rho$が「奇」なら，$\rho$は正則保型形式に伴う.
- $\rho$が「偶」なら，$\rho$はマースの波動形式 $(\lambda = 1/4)$ に伴う.

$p$進ホッジ理論 $(p = \ell)$ を用いて精密な予想が定式化される.

$\mathbf{GL}_n$への一般化 ： 「$n$次元ガロア表現で$\ell$でド・ラームなもの」

と「$\mathbf{GL}_n(\mathbb{A}_\mathbb{Q})$の代数的な保型表現」の間の$L$関数を保つ対応.

専門家向け 「1つの$\ell$」に関する予想．整合系，“モチーフ” は不要.

“ラングランズ双対群” などの仮想的な群も不要.

# 最近の進展・今後の展望

「$j(E)$が整数でない」という仮定を外す —— 射程圏内に入ってきた

$\mathbf{GL}_n(\mathbb{A}_F)$の保型表現に伴うガロア表現の構成がかなりできるようになった．基本補題の解決(ローモン，ンゴー，ヴァルジュプルジェ)と，ユニタリ型志村多様体・井草多様体の研究(シン，モレルら)により，重さが大きい場合(十分正則な場合)はOK.

保型表現の$p$進族(Eigenvariety)の構成(ベライシュ - シュヌビエ)により，重さが小さい場合(佐藤 - テイト予想の解決に必要な場合)にもガロア表現の構成の道が開かれつつある.

## 「基礎体が総実代数体」の仮定を外す —— 一般には全くできていない

定理 **(I.)** $F$ を代数体 **(**総実とは限らない**)**，$E$ を $F$ 上定義された虚数乗法を持たない楕円曲線とする．もし，

**1.** $j(E) \in \mathbb{Q}$ かつ $j(E)$ は整数でない．

**2.** $F/\mathbb{Q}$ は巡回拡大 **(**の塔**)** であるか，または $[F:\mathbb{Q}] = 3$.

が成り立てば，$E$ に対する佐藤 - テイト予想は正しい．

証明の方針 $F/\mathbb{Q}$ が巡回拡大 **(**の塔**)** の場合： 潜保型性とアーサー - クローゼルの巡回基底変換定理をうまく組み合わせる．

$[F:\mathbb{Q}] = 3$ の場合： 潜保型性と **JPSS** の定理 **(3** 次拡大に関するヘッケ指標からの保型誘導**)**，**GL**$(2) \times$ **GL**$(3)$ から **GL**$(6)$ への持ち上げ定理 **(**キム - シャヒディ**)** をうまく組み合わせる．

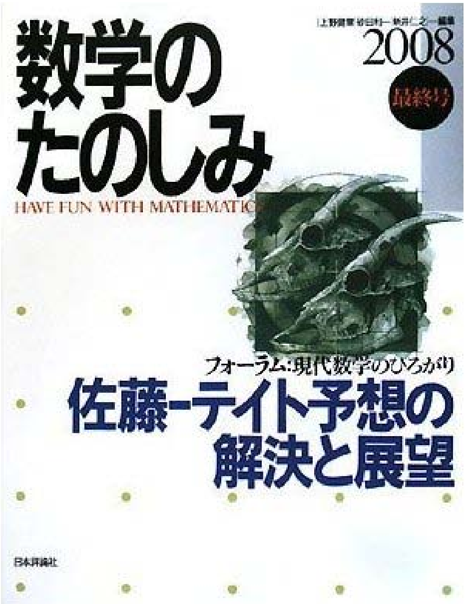
これ以外にも最近は様々な方向に進展がある．ほんの一部を挙げる．

- 総実でない代数体上のガロア表現の変形，$R = \mathbb{T}$ 定理
  (メイザー，カレガリ，エマートン)
- $p$ 進保型形式の表現論的扱い，$p$ 進ラングランズ対応の応用
  (キシン，コルメッツ，エマートン)
- 総実代数体上の $\mathbf{GL}(2)$ のセール予想
  (バザード，ダイアモンド，ジャービス，ジー)
- $\mathbf{GL}(n)$ のセール予想 (セールの重さ) の定式化 (ヘルチッヒ)
- 枠付き変形環の構造の詳細な研究．$R^{\mathbf{red}} = \mathbb{T}$ 定理の一般化・応用．
  (ジー，今井)

# まとめ

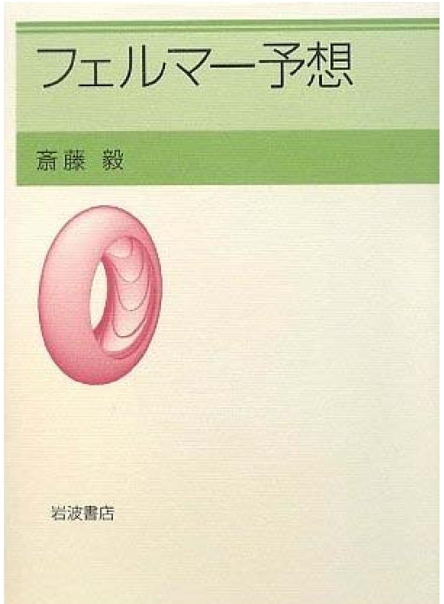
最近の佐藤-テイト予想・セール予想の解決は非可換類体論に大きな進展を与えた．その証明は，ワイルズの仕事をさらに発展させたもので，多くの新しいアイデア(特に幾何学的なアイデア)に基づいている．テイラーによる潜保型性と，キシンによるガロア表現の枠付き変形が重要．既成の分野にとらわれない発想で取り組むことが大切．もちろん個々の定理は大切だが，定理の背後にある理論，定理が成り立っている“仕組み”を理解することが，これからはますます大切になってくる．最近は若い研究者による貢献が大きい．皆さん，がんばってください．

# 参考文献

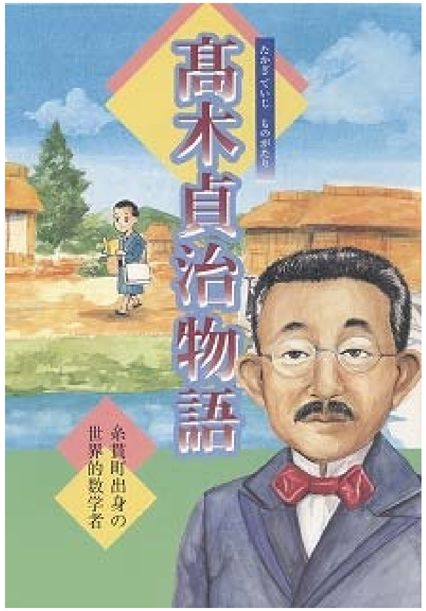


数学のたのしみ
2008
最終号
HAVE FUN WITH MATHEMATICS
フォーラム:現代数学のひろがり
佐藤-テイト予想の解決と展望
日本評論社


類体論と非可換類体論 1
フェルマーの最終定理・
佐藤-テイト予想解決への道
加藤和也
岩波書店

フェルマー予想
斎藤 毅
岩波書店

高木貞治物語
糸貫町出身の世界的数学者