RIMS Kôkyûroku Bessatsu
B19 (2010), 7–22

Serre の保型性予想の紹介 (Introduction to Serre's modularity conjecture on Galois representations)

By

田口 雄一郎 (Yuichiro TAGUCHI)*

Abstract

This is a survey on Serre's modularity conjecture. Its precise formulation is given following Serre's original paper, and some of its consequences are discussed. Its proof by Khare-Wintenberger is sketched only very roughly. Possible generalizations of the conjecture are mentioned briefly.

Serre の保型性予想とは、有理数体の既約かつ odd な 2 次元 mod p Galois 表現は全て modular であらう、といふ予想である (詳しくは §1 で述べる)。その原型は 1973 年に提出され ([54])、1987 年の論文 [57] で詳しい定式化がなされた。そして多くの人々の努力と結果を経て、2007 年に Khare と Wintenberger により一般の場合の証明が公表された:[1]

定理 ([34]). Serre の保型性予想は正しい。

これは大雑把に言へば Langlands 予想 (for GL_2 over $\mathbb{Q}$) の mod p 版である。Langlands 予想といふのは Galois 表現と保型形式 (乃至、保型表現) がうまく対応するといふ予想であり、類体論の一つの非可換化であつた：

$$\begin{array}{ccc} \underline{\text{Galois 側}} & & \underline{\text{Hecke 側}} \\ (\text{Galois 表現 } \rho) & \longleftrightarrow & (\text{保型形式 } f) \\ L(s,\rho) & = & L(s,f) \end{array}$$

Received June 2, 2009. Revised August 25, 2009.
2000 Mathematics Subject Classification(s): 11F80, 11F11
Key Words: mod p Galois 表現, 保型形式, Serre の保型性予想
Partially supported by KAKENHI 19540036

* 〒 819-0395 福岡市西区元岡 744 九州大学大学院数理学研究院
Faculty of Mathematics, Kyushu University, 744, Motooka, Nishi-ku, Fukuoka, 819-0395 Japan
Email address: `taguchi@math.kyushu-u.ac.jp`

[1] 証明を述べた主論文 [34] 及び鍵の一つとなる $p=2$ の場合についての Kisin の論文 [35] は本稿執筆時点では未だプレプリントである事をお含みおき願ひたい。

この様な対応の御利益は、それぞれの側で得意不得意があつてそれらがずれてゐるので、互ひに補ひ合へる点にあるだらう。例へば次の様な事がある：
・右辺 $L(s,f)$ は解析的に良い性質を持つ事が比較的容易に証明される。一方、左辺 $L(s,\rho)$ は、ρ が代数幾何から来てゐる場合など、数論的に面白い性質 (係数 a_p の評価など) を持つ事が分かる場合がある。
・Hecke 側の対象は比較的計算し易い。実際、現在 (少なくとも elliptic modular の場合には) 膨大なデータベースがある (cf. e.g. [61])。一方 Galois 側も最近ではかなり計算出来る様になつて来たが、未だ扱へる多項式の次数はそれほど高くない様である (cf. e.g. [36])。
... 等々。

では何故 mod p 版を考へるのか？先づ、
・或る問題が難しくて解けない時、取敢へずそれを mod p してみるのは整数論人間の性である。
といふ事を別にしても、実際、
・「Serre 予想 + 持上げ」により、Fontaine-Mazur 予想 [18] (の一部) が幾つかの場合に解かれつつある。
など、ちやんと次のステップに繋がつて行くのである。

以下、本稿では

1. Serre 予想の定式化
2. Serre 予想の帰結
3. Serre 予想の証明
4. Serre 予想の一般化

について述べる。Serre 予想の証明は、素数 p, level N, weight k に関する複雑な帰納法になつてゐる。§2 で述べる「帰結」のうちの幾つかは Serre 予想自体に先立つて証明された。その或るものは「帰納法の第一段階」として使はれ、或るものは帰納法を進行させるのに役立つた。特に後者 (の精密化) のうち中心的なものが所謂「$R=\mathbb{T}$ 定理」である。これは Wiles [71], Taylor-Wiles [67] により Fermat 予想の証明とともにデビューして以来 12 年かけて深化し、今や Serre 予想のみならず佐藤-Tate 予想も殆ど証明出来る[2]までに成長した。$R=\mathbb{T}$ について、より詳しい事は [49] や [50] を参照されたい。また、佐藤-Tate 予想については [73] も参照されたい。証明についての解説 (§3) は極めて大雑把にならざるを得なかつた。詳しくは [50] や [72] を参照されたい。§4 では Serre 予想の一般化の可能性について少し述べた。ここでは安田正大氏から学んだ事が多かつたが、私の消化不足の故に不正確を免れてゐないと思ふ。読者の御叱正を賜りたい。

初稿及び改訂稿を注意深く読んで多くの誤りを正して下さつた査読者の方、最終節の改訂に関して何かと相談に乗つて下さつた伊藤哲史さん、今野拓也さん、安田正大さんに感謝申し上げます。

[2]最近、総実代数体上の楕円曲線に対する佐藤-Tate 予想は完全に証明出来たと称するプレプリント [3] が公表された。

§ 1. Serre 予想の定式化

$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,
p: 素数、
$\overline{\mathbb{F}}_p =$ (位数 p の有限体の代数閉包)、
とする。俗に「$\mathbb{Q}$ の mod p 表現」と呼び慣はされてゐるものは詳しく言ふと「$G_{\mathbb{Q}}$ の、$\overline{\mathbb{F}}_p$ 上の有限次元連続線型表現 $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_{\overline{\mathbb{F}}_p}(V)$」[3] の事である。Serre の保型性予想は 2 次元の mod p 表現についての予想である：

予想 ([57])[4]**.** 任意の odd かつ既約な表現 $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ は modular of type $(N(\bar{\rho}), k(\bar{\rho}), \varepsilon(\bar{\rho}))$ である。

ここに現れる用語及び記号はこれから説明するが、その前に：Modularity のタイプ $(N(\bar{\rho}), k(\bar{\rho}), \varepsilon(\bar{\rho}))$ を予想しない、単に「... は modular」といふだけの予想を Serre 予想の 弱形 と呼び (これに対し上の形を 強形 と呼ぶ)、「弱形が正しければ強形も正しい」といふ予想を ε-予想[5] と呼ぶ。

さて、用語と記号の意味は次の通り：
$\bar{\rho}$ が odd とは $\det\bar{\rho}$(複素共役) $= -1$ である事、
$\bar{\rho}$ が modular of type (N, k, ε) とは、それが level N, 重さ k, 指標 $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^{\times}$ の (Serre の意味での) mod p 保型形式に伴ふ表現と同型である事、即ち、
或る Hecke 固有尖点形式 f であつて level $= N$, 重さ $= k$, 指標 $= \varepsilon_0$ なるものが存在して、その T_ℓ-固有値を a_ℓ とするとき、

$$\det(X - \bar{\rho}(\mathrm{Frob}_\ell)) \;=\; X^2 - a_\ell X + \varepsilon_0(\ell)\ell^{k-1} \pmod{\mathfrak{p}}$$

が全ての素数 $\ell \nmid pN$ に対して成り立つ事である (ここで、
　Frob_ℓ は ℓ の Frobenius 共役類 $\subset G_{\mathbb{Q}}$,
　$\mathfrak{p}$ は p の上にある $\overline{\mathbb{Q}}$ の或る素点、
　$\varepsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}^{\times}$ は $\varepsilon_0 \pmod{\mathfrak{p}} = \varepsilon$ となる Dirichlet 指標

[3] $G_{\mathbb{Q}}$ には Krull 位相を入れ、$\mathrm{GL}_{\overline{\mathbb{F}}_p}(V)$ には離散に位相を入れて考へる。従つて連続表現 $\bar{\rho}$ の像は有限であり、実際には或る有限体 $\mathbb{F}_q$ 上定義される。そこで、$\mathbb{Q}$ の mod p 表現とは即ち「有限次 Galois 拡大 $K/\mathbb{Q}$ とその Galois 群の $\mathrm{GL}_2(\mathbb{F}_q)$ への埋込の組」と思つて差し支へない。なほ、$\bar{\rho}$ といふ記号は「或る ρ の還元」といふ印象を与へるかもしれないが、それを仮定してゐる訳ではなく、「さうなる予定」といふぐらいの意味で慣用的に使つてゐる。

[4] この予想は、Serre 自身が指摘した様に、このままの形だと $p = 2, 3$ のとき反例がある (指標 $\varepsilon(\bar{\rho})$ が必ずしも予想通りに (即ち "p-part 無しに") 取れない。[57] に対する Serre 自身の Note 1 in 『Serre 全集 IV』, p. 641 や [24], §10.1 を参照)。証明されたのは、ε-予想の指標部分に関しては次の脚注に述べる仮定 $(*)$ の下に於いてであり、以下、単に「Serre 予想」と言つたら、「強形、但し指標に言及するときはこの仮定 $(*)$ を付ける」を意味する。Khare-Wintenberger が証明したのもこの版である。なほ、Edixhoven の定式化 (cf. この節末の註) を採用すればこの問題は起こらない (cf. 上記 Note 1 及び [24], §4).

[5]「谷山-志村 $+\ \varepsilon \Rightarrow$ Fermat」の ε の部分に相当する予想なのでかう呼ばれる (cf. §2.2). 次の場合には ε-予想は以前から解決済みであつた (cf. [13], Cor. 1.2):

$(*)$　$p > 3$, 又は $p = 3$ で $\bar{\rho}$ が $\mathbb{Q}(\sqrt{-3})$ の指標から誘導されないとき。

である)。
$N(\bar{\rho})$ は $\bar{\rho}$ の Artin 導手、
$k(\bar{\rho})$ は $\bar{\rho}$ の Serre weight,[6]
$\varepsilon(\bar{\rho}) : (\mathbb{Z}/N(\bar{\rho})\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^{\,\times}$ は $\bar{\rho}$ に伴ふ Dirichlet 指標
であり、以下の様に定義される：
$N(\bar{\rho})$ は p 以外の素数に亘る積 $N(\bar{\rho}) = \prod_{\ell \neq p} \ell^{n_\ell(\bar{\rho})}$ であり、その指数 $n_\ell(\bar{\rho})$ は次の式で定義される：

$$n_\ell(\bar{\rho}) \ := \ \sum_{i \geq 0} \frac{1}{(G_{\ell,0} : G_{\ell,i})} \dim_{\overline{\mathbb{F}}_p}(V/V^{G_{\ell,i}}),$$

ここに
V は $\bar{\rho}$ の表現空間、
$G_\ell = (\ell$ 上の素点の分解群 $\subset \mathrm{Im}(\bar{\rho}))$,
$G_{\ell,i} = ($第 i 分岐群 $\subset G_\ell)$, 特に $G_{\ell,0} = ($惰性群 $\subset G_\ell)$,
である。Artin 導手の指数 $n_\ell(\bar{\rho})$ は実は整数であり、$\bar{\rho}$ の ℓ での分岐の深さを測るものである。例へば「$\bar{\rho}$ が ℓ で分岐 $\Leftrightarrow n_\ell(\bar{\rho}) > 0$」である。

$k(\bar{\rho})$ の正確な定義は複雑だが、$k(\bar{\rho}) \pmod{p-1}$ 及び指標 $\varepsilon(\bar{\rho})$ は次の等式により定められる：

$$\det \bar{\rho} \ = \ \varepsilon(\bar{\rho})\chi^{k(\bar{\rho})-1}.$$

ここに $\chi : G_\mathbb{Q} \to \overline{\mathbb{F}}_p^{\,\times}$ は mod p 円分指標である。($G_\mathbb{Q}$ の $\overline{\mathbb{F}}_p$-値指標は、N をその導手とするとき、Dirichlet 指標 $(\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^{\,\times}$ と同一視する。逆も然り。)

Serre weight の正確な定義は次の通り：I を p での惰性群 $\subset G_\mathbb{Q}$, I_p をその最大 pro-p 部分群とし、$I^{\mathrm{tame}} := I/I_p$ とおく。これは有限体の乗法群 $\mathbb{F}_{p^n}^\times$ たちの norm に関する逆極限と自然に同一視出来る。指標 $\varphi : I^{\mathrm{tame}} \to \overline{\mathbb{F}}_p^{\,\times}$ は、この同一視 $I^{\mathrm{tame}} = \varprojlim \mathbb{F}_{p^n}^\times$ の下、$\mathbb{F}_{p^n}^\times$ を経由するが $\mathbb{F}_{p^m}^\times$ (m は n の約数 $< n$) を経由しないとき、<u>niveau n</u> であると言ふ (例へば niveau 1 の指標は mod p 円分指標 χ の冪である)。その中でも特に、第 n 射影 $I^{\mathrm{tame}} \to \mathbb{F}_{p^n}^\times$ と体の埋込み $\mathbb{F}_{p^n} \hookrightarrow \overline{\mathbb{F}}_p$ から来る $\mathbb{F}_{p^n}^\times \hookrightarrow \overline{\mathbb{F}}_p^{\,\times}$ とを合成して得られる n 個の群準同型 $\psi : I^{\mathrm{tame}} \to \overline{\mathbb{F}}_p^{\,\times}$ 達を <u>niveau n の基本指標</u> と呼ぶ。$\bar{\rho}$ を p での分解群 G_p に制限したものの半単純化 $\bar{\rho}^{\mathrm{ss}}$ には惰性群 I が I^{tame} 経由で作用するが、さらに

$$\bar{\rho}^{\mathrm{ss}}|_I \ \sim \ \begin{pmatrix} \varphi & \\ & \varphi' \end{pmatrix}$$

(ここに $\sim$ は $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ に於ける共役) と書くとき、φ, φ' は niveau 1 又は 2 である事が分かる。

<u>Niveau 2 の場合：</u>このとき φ と φ' とは $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-共役、即ち $\varphi' = \varphi^p$ である。$\psi, \psi' : I^{\mathrm{tame}} \to \overline{\mathbb{F}}_p^{\,\times}$ を niveau 2 の基本指標として、

$$\varphi \ = \ \psi^{a+pb} \ = \ \psi^a \psi'^b, \qquad 0 \leq a < b \leq p-1,$$

[6]Serre weight は、$p \neq 2$ なら $2 \leq k(\bar{\rho}) \leq p^2 - 1$ なる整数であり、$p = 2$ なら $k(\bar{\rho}) = 2$ または 4 である。

と書き、[7]

$$k(\bar{\rho}) \ := \ 1 + pa + b$$

と定義する。

<u>Niveau 1 の場合 :</u> このとき、さらに $\bar{\rho}|_{I_p}$ が自明 (i.e. $\bar{\rho}$ の p での分岐は高々 tame) か否かで場合分けする (因みに「$\bar{\rho}|_{I_p}$ が自明 $\Leftrightarrow$ $\bar{\rho}|_I$ は半単純 (完全可約)」である)。

$\bar{\rho}|_{I_p}$ が自明のとき、$\bar{\rho}|_I$ は次の形であるとしてよい :

$$\bar{\rho}|_I \ \sim \ \begin{pmatrix} \chi^a & \\ & \chi^b \end{pmatrix}, \qquad 0 \le a \le b \le p-2.$$

このとき

$$k(\bar{\rho}) \ := \ \begin{cases} 1 + pa + b & \text{if } (a,b) \neq (0,0), \\ p & \text{if } (a,b) = (0,0), \end{cases}$$

と定義する。

$\bar{\rho}|_{I_p}$ が非自明のとき、$\bar{\rho}|_I$ は次の形であるとしてよい :

$$\bar{\rho}|_I \ \sim \ \begin{pmatrix} \chi^\beta & * \\ & \chi^\alpha \end{pmatrix}, \qquad * \neq 0.$$

このとき

$$0 \le \alpha \le p-2, \quad 1 \le \beta \le p-1$$

と正規化し、

$$a \ := \ \min\{\alpha, \beta\}, \quad b \ := \ \max\{\alpha, \beta\}$$

と置き、基本的には

$$k(\bar{\rho}) \ := \ 1 + pa + b$$

と定義する。但し、 $\beta = \alpha + 1$ かつ $\bar{\rho}|_I$ は not finite[8] のときはこれでは足りないと思はれるので

$$k(\bar{\rho}) \ := \ 1 + pa + b + p - 1 \qquad \text{if } \beta = \alpha + 1 \text{ かつ } \bar{\rho}|_I \text{ は not finite かつ } p > 2,$$

と定義する。$p = 2$ のときは常に $a = 0$, $b = 1$ で、このとき $1 + pa + b$ の値は 2 となるが、これだと不安があるので

$$k(\bar{\rho}) \ := \ 4 \qquad \text{if } p = 2 \text{ かつ } \bar{\rho}|_I \text{ は not finite}$$

と定義する。

[7] 必要に応じて φ, φ' を入れ替へる事により $a < b$ と仮定してよい。

[8] $\bar{\rho}|_I$ が <u>finite</u> (<u>flat</u> と言ふ人もゐる) とは、それが $\mathbb{Q}_p$ の最大不分岐拡大の整数環上の有限平坦可換群 scheme の $\overline{\mathbb{Q}}_p$-有理点のなす加群上の表現として実現される事である。

註: **Edixhoven の版.** 上の "modular" の定義で、Serre は古典的な標数 0 の保型形式の Fourier 展開 (mod p) を使つたが、原論文 [57] の注意 (6) (p. 197) で既に Katz の mod p 保型形式を使へば a priori には「より多くの」mod p Galois 表現が得られるかもしれない、といふ可能性を示唆してゐる ([58], [59] も参照)。Edixhoven は Katz の保型形式を使ふ事を前提に、Serre weight の定義を修正した ([14], 定義 4.3)。その違ひは以下の二つの場合である：

・ Niveau 1, $\bar{\rho}|_I$ が自明のとき：
Serre の $k(\bar{\rho}) = p$ だつたが Edixhoven の $k(\bar{\rho}) = 1$.

・ Niveau 1, $p = 2$, $\bar{\rho}|_I$ not finite のとき：
Serre の $k(\bar{\rho}) = 4$ だつたが Edixhoven の $k(\bar{\rho}) = 3$.

Khare-Wintenberger が証明したのは Serre の original 版の予想の方で、Edixhoven 版は未だほんの少し残されてゐる ($\bar{\rho}$ が "exceptional" の時の weight に関して; cf. [14], §4)。

さて、上の様な Serre weight の定義は複雑で何の哲学も無い様に見えるかもしれない。しかし実はこの定義には次の様な「裏」がある：先づ、重さ $2 \le k \le p+1$ なる保型形式 f に伴ふ mod p 表現 $\bar{\rho}_f$ の、 p の惰性群への制限の様子が、Deligne と Fontaine により、次の様に知られてゐた (cf. [14], 2.5, 2.6)：

定理. $2 \le k \le p+1$ と仮定する。f は level N, 重さ k, 指標 ε の mod p 固有尖点形式とし、その T_p-固有値を a_p とする。f に伴ふ mod p Galois 表現を $\bar{\rho}_f$ と書く。
(1)(Deligne) $a_p \neq 0$ のとき、$\bar{\rho}_f|_{G_p}$ は可約で、次の形：

$$\bar{\rho}_f|_{G_p} \ \sim \ \begin{pmatrix} \chi^{k-1}\lambda(\varepsilon(p)/a_p) & * \\ & \lambda(a_p) \end{pmatrix}.$$

ここに $a \in \overline{\mathbb{F}}_p^{\times}$ に対し $\lambda(a) : G_p \to \overline{\mathbb{F}}_p^{\times}$ は $\lambda(a)(\mathrm{Frob}_p) = a$ なる不分岐指標、行列成分の空欄のところは 0 である。
(2)(Fontaine) $a_p = 0$ のとき、$\bar{\rho}_f|_{G_p}$ は既約で、$\bar{\rho}_f|_I$ は次の形：

$$\bar{\rho}_f|_I \ \sim \ \begin{pmatrix} \psi^{k-1} & \\ & \psi'^{k-1} \end{pmatrix}.$$

そこで、与へられた $\bar{\rho}$ がこのどちらかの形をしてゐれば、それが因つて来たるべき保型形式 f の重さ k の見当が付く。さうでない場合は、$\bar{\rho}$ を mod p 円分指標の適当な冪 χ^a で捻ると上の形になる。ところで、mod p 保型形式の空間には θ-作用素 ([53], [28]) といふものがあり、その作用は q-展開の言葉では

$$\theta = q\frac{d}{dq} : \ \sum a_n q^n \mapsto a_n n q^n$$

となつてゐる。$\chi(\mathrm{Frob}_\ell) = \ell$ (ℓ: 素数 $\neq p$) だから、保型形式側で θ を作用させる事は Galois 表現側で円分指標で捻る事と対応してゐる；

$$\bar{\rho}_{\theta f} \ = \ \bar{\rho}_f \otimes \chi.$$

冪級数 $f = \sum a_n q^n \in \overline{\mathbb{F}}_p[\![q]\!]$ に対し、それが重さ k の保型形式から来る様な k の最小値を f の filtration (cf. [53], [14]) と言ひ、$w(f)$ と記す。f に θ を次々と作用させて行くとき $w(\theta^a f)$ がどう変化するかを書き並べたもの $(w(\theta f), \ldots, w(\theta^{p-1} f))$ が Tate の θ-cycle である。これは (最初は Tate が seminar talk で発表したらしいが) Jochnowitz [26] によつて調べられた。$p = 2, 3$ の場合も含めた決定版は Edixhoven [14] の命題 3.3 である (この論文で Edixhoven は ε-予想の「重さ部分」 (Edixhoven 版) を解決した[9])。典型的なパターンとしては、θ を一回作用させるごとに filtration は $p+1$ ずつ上がつて行くが、$w(\theta^a f)$ が p で割れるとき一度ガクンと落ちる。Serre はこの仕組みを知つてゐて、Serre weight $k(\bar{\rho})$ を「逆算して」定義したと思はれる。

もつと intrinsic な定義はないのか？と思はれるだらうが、実際それは Serre 予想の一般化に於ける中心的課題の一つである (cf. §4).

§2. Serre 予想の帰結

§2.1. 持上げ

$\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ が modular といふ事は、或る保型形式 f に伴ふ p 進表現 $\rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ の reduction mod $\mathfrak{p}$ になつてゐるといふ事なので、特に $\bar{\rho}$ が標数 0 に持上がるといふ事を含んでゐる。これが Deligne が最初 Serre 予想を信じなかつた理由の一つであると言はれてゐる。実際、これは素朴に考へると信じ難い事である (少なくとも私には)。例へば、$p \geq 5$ で $\mathrm{Im}(\bar{\rho})$ が $\mathrm{SL}_2(\mathbb{F}_p)$ を含めば $\bar{\rho}$ は少なくとも連続な $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ には持上がらない。そこで Serre 予想とは取敢へず独立に、mod p 表現を p 進表現に持上げようといふ研究が現れた (絶対既約な $\bar{\rho}$ の普遍変形環の次元 (の下からの評価) は Mazur により Galois 表現の変形理論登場当初から計算されてゐたが、混標数の完備離散附値環上に持ち上がるか (或いは、普遍変形環が $\mathbb{Z}_p$ 上平坦か) 等は知られてゐなかつた)。この方面では、$\bar{\rho}$ が可約の場合に Khare [29] が、また、$\bar{\rho}$ が絶対既約の場合に Ramakrishna [43] が、それぞれ Witt 環上への持上げが可能である (但し分岐する場所を増やす) 事を示したのが最初期の研究と思はれる。その後、同じく Ramakrishna の [44] や Gee [19], 冨山 [68] などもこれを一般化してゐる。Ramakrishna の方法は純粋に Galois cohomology の計算に依つたが、その後 Taylor [64], [66] により「潜保型性」(potential modularity) を経由して持上げる方法が開発され、Serre 予想の証明への重要なステップとなつた。

§2.2. Level の最適化

p 進表現 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ の導手は、mod $\mathfrak{p}$ すると一般には減つてしまふ[10] し、そもそも ρ は通常 p では激しく分岐してゐる。従つて mod p の $\bar{\rho}$ が modular な $\rho_{f,\mathfrak{p}}$ に持上がつてゐたとしても、その保型形式 f の level を $\bar{\rho}$ の Artin 導手 $N(\bar{\rho})$ に等しく取れるとは限らなさうに思はれる。これも Deligne が当初 Serre 予想を信じなかつた理由の一つ

[9] Serre の original 版の ε-予想の「重さ部分」 (の $p = 2$ の場合) は [34]+[35] により結果的に解決した。
[10] しかし減り方は分かる。Cf. [9], [38].

と言はれてゐる。Serre 予想は、f に「$\mathrm{level}(f)=N(\bar\rho)$」といふ条件を課しても、weight を少し大き目 (即ち (素朴な値) $+(p-1)$) に取つておけば、適当な f が存在するといふ事を主張してゐる。そこで、mod p 表現 $\bar\rho$ が或る level N の保型形式から来てゐるといふ仮定の下で、(weight を変へてもいいから) level $N(\bar\rho)$ の保型形式からも来るか? といふ問題が自然に考へられる (これは「ε-予想の level 部分」である)。この方面の著しい研究として Ribet の有名な仕事 [46] (Fermat 予想を谷山-志村予想に帰着した、あれ) がある。その後の発展については [47] に詳しい。

§ 2.3. Mod p 表現の非存在と有限性

定義より $k(\bar\rho)\le p^2-1$ であり、円分指標の適当な冪 χ^a で捻る事により $k(\chi^a\otimes\bar\rho)\le p+1$ に出来る。Level N, weight k の尖点形式の空間 $S_k(\Gamma_1(N))$ は有限次元だから、与へられた (N,k) に対し、$(N(\bar\rho),k(\bar\rho))=(N,k)$ となる modular な $\bar\rho$ の同型類は有限個しかない。 従つて Serre 予想が正しければ、標数 p を固定するとき、与へられた Artin 導手 $N(\bar\rho)$ を有する $\bar\rho$ の同型類は有限個[11] である事が従ふ。さらに、小さい N と k (例へば $N=1$ なら $k\le 11$ 及び $k=13$) に対しては $S_k(\Gamma_1(N))=0$ となるから、p と $N(\bar\rho)$ が小さいとき、その様な $\bar\rho$ は存在しない事も従ふ。この方面の研究は Tate [62] が先鞭をつけた (この論文は元々、Serre 予想の最初の版が述べられた Serre から Tate への手紙 (1973 年 5 月) への返信 (1973 年 7 月) であつた)。ここで Tate は $p=2$, $N=1$ の場合の非存在を示してゐる。$p=3$, $N=1$ の場合は Serre [56] による。これらは Serre 予想の $N=1$ の場合の証明 (p に関する帰納法) の「第一段階」となつた。この方面の研究として、他に [4], [39], [40], [41] などがある。[50] の第 2 巻所収の筆者の解説記事も参照されたい。

§ 2.4. Serre 予想の応用

Serre 予想の応用として次の事が従ふ。これらのうち (5) 以外は Serre 自身が既に原論文 [57] で述べてゐる。

(1) Fermat 予想. Serre 予想を仮定すると Fermat 予想が簡単に従ふ。[12] 実際、p を素数 ≥ 5 として、$a^p+b^p+c^p=0$ を満たす 0 でない整数 a,b,c があつたと仮定して、Frey の楕円曲線 $E: y^2=x(x-a^p)(x+b^p)$ を作り、その p-等分点上の Galois 表現 $\bar\rho: G_{\mathbb{Q}}\to \mathrm{Aut}(E[p])\simeq \mathrm{GL}_2(\mathbb{F}_p)$ を考へる。この表現は絶対既約であり、さらに、E が特殊な形をしてゐるため $\bar\rho$ の分岐は小さく、$(N(\bar\rho),k(\bar\rho))=(2,2)$ である事が分かる (楕円曲線から来る $\bar\rho$ の通例として、$\varepsilon(\bar\rho)=1$ である)。Serre 予想に依ればこの $\bar\rho$ は或る保型形式 $f\in S_2(\Gamma_0(2))$ から来る筈であるが、この空間は 0 なので矛盾、となる。

[11]Serre 予想以前に、mod p Hecke 固有値系の個数の有限性は (Atkin, Tate, Serre らの先行研究を経て) Jochnowitz [27] が示してゐた。Serre 予想の「$k(\bar\rho)\le p^2-1$」といふ部分はその精密化とも言へる。

[12]Serre 予想が証明されたので、では Fermat 予想の別証明が得られたのか? といふと、Khare-Wintenberger の証明は、Wiles による Fermat の証明に於いても鍵であつた $R=\mathbb{T}$ をより派手に駆使したものなので、「別証明」とは言ひ難い。

その他にも Serre は Fermat 予想の variant[13] を上と同様にして Serre 予想から導いてゐる。その後、Darmon らも幾つかの Diophantine 方程式の解の非存在を Serre 予想から導いてゐる。解説論文 [12] などを参照されたい。

(2) 或る種の半安定楕円曲線の分類. E を $\mathbb{Q}$ 上の楕円曲線とする。もし E が $\mathbb{Q}$ 上至る所半安定ならば、素数 $p \geq 11$ に対しその p-等分点上の表現 $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ は絶対既約であり、さらに E の判別式が (整数)^p の形ならば $(N(\bar{\rho}), k(\bar{\rho})) = (1, 2)$ となる。そこで Serre 予想より、(1) と同様の議論に依つて、この様な E と p があつたとすると $p \leq 7$ であり、$E(\mathbb{Q})$ は位数 p の点を持つ事が従ふ。(これは元々 Brumer-Kramer [5] により提起された問題であつた。)

(3) 有限 p 群 scheme の分類. $G_{\mathbb{Q}}$ の 2 次元 mod p 表現は $\mathbb{Q}$ 上の (p, p) 型 (= rank p^2 の p-torsion) 有限平坦可換群 scheme からも生じる。上と大体同じ原理で、Serre 予想から次の命題を導ける：$p \geq 3$ のとき $\mathbb{Z}$ 上の (p, p) 型有限平坦群 scheme は次のいづれかと同型である：$(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$, $(\mathbb{Z}/p\mathbb{Z}) \oplus \mu_p$, $\mu_p^{\oplus 2}$. 実際、Serre 予想により対応する Galois 表現が可約である事が従ひ、可約ならば Tate-Oort [63] により sub と quotient はそれぞれ $\mathbb{Z}/p\mathbb{Z}$ か μ_p でなければならず、それらの拡大は Fontaine [17] により自明なものしかない ($p = 2$ のときは非自明な拡大 "Katz-Mazur の群 scheme" が一つある)。

(4) 谷山-志村予想. これも Serre 予想から従ふ。E を $\mathbb{Q}$ 上の楕円曲線とし、その導手を N とする。各素数 p に対し $E[p]$ 上の Galois 表現 $\bar{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ を考へると、殆ど全ての p に対し $\bar{\rho}_p$ は絶対既約で $(N(\bar{\rho}_p), k(\bar{\rho}_p)) = (N, 2)$ となる。そこで Serre 予想を仮定すると、各 p に対し正規化された Hecke eigenform $f_p = \sum_{n \geq 1} a_{n,p} q^n \in S_2(\Gamma_0(N))$ ($a_{n,p} \in \overline{\mathbb{Q}}$) があつて、$\ell \nmid Np$ に対し

$$1 - \#E(\mathbb{F}_\ell) + \ell \pmod{p} \;=\; \mathrm{Tr}(\bar{\rho}_p(\mathrm{Frob}_\ell)) \;=\; a_{\ell,p} \pmod{\mathfrak{p}}$$

となる。この様な f_p は実際には有限個しかないから、或る $f = \sum a_n q^n$ があつて、$1 - \#E(\mathbb{F}_\ell) + \ell \equiv a_\ell \pmod{\mathfrak{p}}$ が無限個の p に対して成り立つ。従つて実は $1 - \#E(\mathbb{F}_\ell) + \ell = a_\ell$, 即ち E は modular である。

同様の事が、$\mathbb{Q}$ 上実乗法を持つ (= GL_2-型の) Abel 多様体 $/\mathbb{Q}$ についても成り立つ ([48])。即ち、Serre 予想を認めると、この様な Abel 多様体 A は或る modular Jacobian $J_1(N)$ の商 (= 或る Hecke eigenform $f \in S_2(\Gamma_1(N))$ に対する志村の Abel 多様体 A_f と同種) になる (A の導手は $N^{\dim(A)}$ の形で、f の level N はこの N に取れる)。これは或る代数体 E を係数とする rank 2 の motif の話になるため、($\Gamma_0(N)$ でなく) $\Gamma_1(N)$ が必要である事に注意されたい。

[13]方程式

$$a^p + b^p + L^\alpha c^p \;=\; 0, \quad p\text{: 素数} \geq 11,\ \alpha\text{: 整数} \geq 0,$$
$$L\text{: 素数 } (\neq p) \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}$$

は非自明な整数解を持たない、といふ事。

さらに同様の事が、或る種の代数多様体の cohomology についても言へる。即ち、X が $\mathbb{Q}$ 上の滑らかな射影多様体で、その m 次 Betti cohomology 群 $H^m_{\mathrm{B}}(X(\mathbb{C}),\mathbb{C})$ (m は一つ任意に固定して考へる) が次を満たしてゐるとする:
(i) $\dim H^m_{\mathrm{B}}(X(\mathbb{C}),\mathbb{C})=2$;
(ii) $H^m_{\mathrm{B}}(X(\mathbb{C}),\mathbb{C})$ の Hodge 分解は $(m,0)+(0,m)$ 型。
このとき、Serre 予想を仮定すると、$H^m_{\text{ét}}(X\otimes_{\mathbb{Q}}\overline{\mathbb{Q}},\mathbb{Q}_p)$ は或る level N の或る Hecke eigenform $f\in S_{m+1}(\Gamma_0(N))$ に付随する[14] Galois 表現の双対と同型になる。例へば $\dim H^3=2$ なる 3 次元 Calabi-Yau 多様体の H^3 についてはこれが成り立つ ([20])。

(5) Artin 予想. GL(2) の場合の Artin 予想は (Serre 予想とは独立に) 多くの場合に知られてゐた (特に、像が可解の場合 ([37], [69]) や射影像が正二十面体群で或る種の局所条件をみたす場合 ([8], [65]))。しかし Serre 予想から GL(2), odd, の場合の Artin 予想が従ふ ([30]) ので、今や次が正しい：

定理. 任意の既約かつ odd な連続表現 $\rho: G_{\mathbb{Q}}\to \mathrm{GL}_2(\mathbb{C})$ は重さ 1 の $\Gamma_1(N)$ に関する保型形式から来る。

ここで N は ρ の普通の (特定の因子を除いたりしない) Artin 導手である。Artin 予想の Serre 予想からの導き方は前項 (4) と似てゐる。与へられた ρ の適当な整数環上の model を取り、それを素 ideal $\mathfrak{p}$ で還元したもの $\bar\rho_{\mathfrak{p}}$ に Serre 予想を適用する。殆ど全ての $\mathfrak{p}$ では $\bar\rho_{\mathfrak{p}}$ は絶対既約かつ $\mathfrak{p}$ の下にある素点 p で不分岐なので、Gross [21], Coleman-Voloch [11] らの結果を合せるとこの剰余表現は Katz の意味の重さ 1 の保型形式から来る事が分かる。p が十分大きければ Katz の保型形式は古典的な保型形式に持ち上がり (cf. [15], [30]), level N を固定すれば重さ 1 の保型形式の空間 $S_1(\Gamma(N))$ は有限次元だから無限個の $\mathfrak{p}$ に対し $\bar\rho_{\mathfrak{p}}$ は或る一つの $f\in S_1(\Gamma(N))$ から来る事が分かり、従つて元の ρ も然り、となる。

Khare-Wintenberger ([34], I, Th. 10.1 (ii)) は (上より少しだけ一般に) ある種の ℓ 進表現の両立系の保型性を証明し、その系として Artin 予想を導いてゐる。

§3. Serre 予想の証明

証明の流れは大体次の様になつてゐる。

1. $N(\bar\rho)=1$ の場合。p に関する帰納法。$p=2,3,5$ の場合はそれぞれ Tate [62], Serre [56], Schoof [51] 及び Brumer-Kramer [6] (+ Taylor の結果) により知られてゐた。即ち、

定理. $p=2,3,5$ のとき、全ての[15] p の外不分岐な $\bar\rho: G_{\mathbb{Q}}\to\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ は可約である。

[14] ここでは Serre の論文に倣つて motif の係数を $\mathbb{Q}$ に限つたので $\Gamma_0(N)$ に取れる筈であるが、係数体 E を付けると $\Gamma_1(N)$ が必要になると思はれる。
[15] Oddness は不要 (cf. [40]).

(N.B. 可約な $\bar{\rho}$ は類体論により modular[16] であり、帰納法を進めるには Skinner-Wiles [60] の $R = \mathbb{T}$ が使へる。)

2. $N(\bar{\rho})$ が一般の場合。$N(\bar{\rho})$ の素因子の個数に関する帰納法。その中でも、先づ $\bar{\rho}$ が "locally good dihedral"[17] の場合を証明し、後に一般の場合をこれに帰着する。

いづれの帰納法も次の二つが柱になつて進行する (ここに出て来る「条件」は勿論状況に依つて異なる)：

(LT) = Lifting Theorem.
$2 \leq k(\bar{\rho}) \leq p+1$ かつ $\mathrm{Im}(\bar{\rho})$ は非可解と仮定する。このとき、$\bar{\rho}$ の strictly compatible system への持上げ $(\rho_\ell)_\ell$ であつて与へられた局所条件を満たすものが存在する。

(MLT) = Modularity Lifting Theorem.
$\bar{\rho}$ は modular かつ適当な条件を満たすと仮定する。$\bar{\rho}$ の $\overline{\mathbb{Q}}_p$ 上への持上げ ρ で適当な条件を満たすものが存在すると仮定する。このとき ρ は modular である。

これらを使つて帰納法は次の様に進行する：
・ $\bar{\rho}$ が与へられたとき、
・ (LT) によりそれを strictly compatible system $(\rho_\ell)_\ell$ に持上げ、
・ 適当な ℓ について $\rho_\ell \pmod{\ell}$ を見、
・ 幸ひそれが modular と知られてゐれば (MLT) により ρ_ℓ も modular,
・ 従つて $(\rho_\ell)_\ell$ 全体が modular, 従つて $\bar{\rho}$ も modular.
・ もし $\rho_\ell \pmod{\ell}$ が modular でなければ再び (LT) を頼つて modularity 探しの旅に出る、
・ これが有限回で終了する (事が証明出来る)。

(LT) と (MLT) の証明については、安田氏の講演ではさらに次の様に分けて解説された：(LT) は
(1) 潜保型性[18] (と Taylor-Wiles patching argument) 及び
(2) 大域変形環 R の Krull 次元の下からの評価
から従ひ、(MLT) は
(3) $R = \mathbb{T}$ 型定理、及び
(4) 局所条件付き automorphic lift の存在
から従ふ。これらについて、詳しい事は [72] 等を参照されたい。

---

[16]保型性とは、$\bar{\rho}$ の 半単純化 $\bar{\rho}^{\mathrm{ss}}$ が保型形式に伴ふ、といふ事なので、可約なら $\bar{\rho}^{\mathrm{ss}} = (\mathrm{abel}) \oplus (\mathrm{abel})$ だから類体論に帰するのである。

[17]これは如何にも技術的な条件に思はれるが、これを考へると何故か上手く行く。

[18]これは次の形の定理である ([64], [66])：

定理. $\bar{\rho}$ は odd かつ既約とし、さらに或る条件を満たすと仮定する。このとき、或る有限次総実代数体 F であつて $\mathbb{Q}$ 上 Galois (かつ、場合によつては多少の条件を課す) があり、$\bar{\rho}$ の G_F への制限 $\bar{\rho}|_{G_F}$ は Hilbert modular となる。

この様な定理は次の様に証明される：等分点が一定の性質 (或る $\mathfrak{p}$ では知りたい mod p 表現になつてをり、別の $\mathfrak{p}'$ では modular である事が分かつてゐる表現となる、といふ性質) を持つ GL_2-型の Abel 多様体の moduli scheme を考へ、それが、局所的に (関係する素点で) は有理点を持つ事を示す。すると Moret-Bailly の定理 [42] により十分大きな総実代数体上有理点を持つ事が従ふ。

§4. Serre 予想の一般化

Serre 予想は幾つかの一般化が提唱されてゐる。一般化の方向は二種あつて、一つは基礎体 $\mathbb{Q}$ を他の大域体に一般化する方向、もう一つは的の群 GL_2 を他の代数群に一般化する方向である。ここでは先づ、曖昧な形ながら、なるべく一般的な定式化を考へてみよう。

F を大域体、$\mathbb{A}$ をその adèle 環、$\mathbb{A}_\mathrm{f}$ を有限 adèle 環とし、G を F 上の連結簡約代数群、${}^LG$ をその L-群 (G の Langlands 双対と $G_F = \mathrm{Gal}(\overline{F}/F)$ との半直積) とする。

希望. 各 compact 開部分群 $\mathbb{K} \subset G(\mathbb{A}_\mathrm{f})$ と、G の $\overline{\mathbb{F}}_p$ 上の代数的既約表現[19] V ごとに「G の、 level $= \mathbb{K}$, weight (+ Nebentypus) V の Hecke 環」$\mathbb{T}_{\mathbb{K},V}$ が定まる。それは恐らく $\mathbb{K}\backslash G(\mathbb{A}_\mathrm{f})/\mathbb{K}$ の Hecke 環の「$(\mathbb{K}, V)$ 型の保型表現」 $S(\mathbb{K}, V)$ 上の像として定義するのがよく、この保型表現は $H^*(G(F)\backslash G(\mathbb{A})/\mathbb{K}K_\infty, V)$ (ここに K_∞ は $G(F_\infty)$ の 極大連結 compact mod center 部分群) の組成因子として構成されるであらう。そして、次の (G) と (H) との間に良い対応があるであらう：
(G) 完全可約な Galois 表現 $\bar{\rho} : G_F \to {}^LG(\overline{\mathbb{F}}_p)$;
(H) 半単純 $\mathbb{T}_{\mathbb{K},V}$-加群 π.
この対応は局所因子を保つ ($\bar{\rho} \leftrightarrow \pi$ ならば $\bar{\rho}_v \leftrightarrow \pi_v$). さらに (G) のうちの "odd[20] なもの" と対応すべき (H) の対象が特徴付けられるべきである。それは "cohomological[21] なもの" を含み、"代数的[22] なもの" に含まれるであらう (もしかしたら mop p の世界では全て "代数的" かもしれない)。

一般化された Serre 予想とは、このうち (G) から (H) を作る予想であると言へる。

(H) から (G) を作る方も一般には殆ど出来てゐないが、或る種の G の場合には Gross の予想 ([22], [23]) があり、Gross の意味の algebraic modular forms は odd な Galois 表現を産むと期待されてゐる。

Serre 予想の真骨頂は level $N(\bar{\rho})$ と weight $k(\bar{\rho})$ を精密に予言する点にあつた。そこで上の対応を精密化する事が問題となる：

問題. 与へられた Galois 表現 $\bar{\rho} : G_F \to {}^LG(\overline{\mathbb{F}}_p)$ に対し、然るべき level $\mathbb{K}$ と weight (+ Nebentypus) V を特定する事。

この方面で現在よく研究されてゐるのは
(i) F が総実代数体で $G = \mathrm{GL}_2$ のとき ([7]) と、
(ii) $F = \mathbb{Q}$, $G = \mathrm{GL}_n$ (n は任意の整数 ≥ 1) のとき ([2], [1], [25])

---

[19] この文脈では、Serre weight (と指標を合せたもの) を「G の $\overline{\mathbb{F}}_p$ 上の代数的既約表現の同型類」と解釈するのが筋が良い。$\mathrm{GL}(2)/\mathbb{Q}$ の場合はその最高 weight が即ち $k(\bar{\rho})$ である。

[20] Galois 表現の oddness の定義は、或る種の G の場合には Gross がしてゐるが、一般には未だされてゐない様である。一般にもそれが定義され、意味のあるクラスの保型表現に対応すべきである。例へば $\mathrm{GL}(2)/\mathbb{Q}$ の場合、$\bar{\rho}$ の oddness は保型形式の "正則性" に対応する。

[21] 標数 0 の表現については [70] を参照。$\mathrm{GL}(2)/\mathbb{Q}$ の場合、それは重さ 2 以上の正則保型形式から来る事を意味する。

[22] $\mathrm{GL}(n)$ の場合の標数 0 の表現については [10] を参照。$\mathrm{GL}(2)/\mathbb{Q}$ の場合、それは (重さ 1 以上の) 正則保型形式及び実解析的保型形式（Laplacian の固有値 $\lambda = 1/4$ なるもの） から来る事を意味する。

で、どちらも "Serre weights の集合"

$$W(\bar{\rho}) \;=\; \{V \mid \bar{\rho} \text{ の相方が } S(\mathbb{K}, V) \text{ に現れる }\}$$

を決めよう、といふ態度で予想を立ててゐる。その他、
(iii) F が虚二次体で $G = \mathrm{GL}_2$ のとき ([16], [52])
にも予想がなされてゐるが、未だ十分精密化されてゐない様である。

References

[1] A. Ash, D. Doud and D. Pollack, *Galois representations with conjectural connections to arithmetic cohomology,* Duke Math. J. **112** (2002), 521–579

[2] A. Ash and W. Sinnott, *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod-p cohomology of* $\mathrm{GL}(n, \mathbb{Z})$, Duke Math. J. **105** (2000), 1–24

[3] T. Barnet-Lamb, D. Geraghty, M. Harris and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, preprint available at: `http://www.math.harvard.edu/~rtaylor/cy2.pdf`

[4] S. Brueggeman, *The nonexistence of certain Galois extensions unramified outside* 5, J. Number Theory **75** (1999), 47–52

[5] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 715–743

[6] A. Brumer and K. Kramer, *Non-existence of certain semistable abelian varieties*, Manuscripta Math. **106** (2001), 291–304

[7] K. Buzzard, F. Diamond and A. F. Jarvis, *On Serre's conjecture for mod ℓ Galois representations over totally real fields*, preprint

[8] K. Buzzard, M. Dickinson, N. Shepherd-Barron and R. Taylor, *On icosahedral Artin representations*, Duke Math. J. **109** (2001), 283–318

[9] H. Carayol, *Sur les representations galoisiennes modulo ℓ attachees aux formes modulaires*, Duke Math. J. **59** (1989), 785–801

[10] L. Clozel, *Motifs et formes automorphes: applications du principe de fonctorialité*, in: "Automorphic forms, Shimura varieties, and L-functions", Vol.I (Ann Arbor, MI, 1988), 77–159, Perspect. Math. **10**, Academic Press, Boston, MA, 1990

[11] R. Coleman and J. F. Voloch, *Companion forms and Kodaira-Spencer theory*, Invent. Math. **110** (1992), 263–281

[12] H. Darmon, *A fourteenth lecture on Fermat's Last Theorem*, Number theory, 103–115, CRM Proc. Lecture Notes **36**, Amer. Math. Soc., Providence, RI, 2004

[13] F. Diamond, *The refined conjecture of Serre*, in: Elliptic curves, modular forms, and Fermat's Last Theorem (Hong Kong, 1993), J. Coates and S.-T. Yau (eds.), Internat. Press, Cambridge, MA, 1995 pp. 22–37 in the first ed. (pp. 172–186 in the 2nd ed.)

[14] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), 563–594

[15] B. Edixhoven, *Serre's conjecture*, in: "Modular forms and Fermat's Last Theorem" (Boston, MA, 1995), pp. 209–242, Springer, New York, 1997

[16] L. Figueiredo, *Serre's conjecture for imaginary quadratic fields*, Compositio Math. **118** (1999), 103–122.

[17] J-M. Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$, Invent. Math. **81** (1985), 515–538

[18] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, in: Elliptic Curves, Modular Forms, and Fermat's Last Theorem (Hong Kong, 1993), J. Coates and S.-T. Yau (eds.), Internat. Press, Cambridge, MA, 1995 pp. 41–78 in the first ed. (pp. 190–227 in the 2nd ed.)

[19] T. Gee, *Companion forms over totally real fields II*, Duke Math. J. **136** (2007), 275–284

[20] F. Q. Gouvêa, N. Yui, *Rigid Calabi-Yau threefolds over* $\mathbb{Q}$ *are modular: A footnote to Serre*, preprint, arXiv:0902.1466v2

[21] B. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. **61** (1990), 445–517

[22] B. H. Gross, *Modular forms (mod p) and Galois representations*, Internat. Math. Res. Notices 1998, 865–875

[23] B. H. Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), 61–93

[24] A. Herremans, *A combinatorial interpretation of Serre's conjecture on modular Galois representations*, Ann. Inst. Fourier (Grenoble) **53** (2003), 1287–1321

[25] F. Herzig, *The weight in a Serre-type conjecture for tame n-dimensional Galois representations*, Duke Math. J. **149** (2009), 37–116

[26] N. Jochnowitz, *A study of the local components of the Hecke algebra mod ℓ*, Trans. Amer. Math. Soc. **270** (1982), 253–267

[27] N. Jochnowitz, *Congruences between systems of eigenvalues of modular forms*, Trans. Amer. Math. Soc. **270** (1982), 269–285

[28] N. Katz, *A result on modular forms in characteristic p*, in: "Modular functions of one variable, V" pp. 53–61. Lecture Notes in Math. **601**, Springer-Verlag, Berlin, 1977

[29] C. Khare, *Base change, lifting, and Serre's conjecture*, J. Number Theory **63** (1997), 387–395

[30] C. Khare, *Remarks on mod p forms of weight one*, Internat. Math. Res. Notices, 1997, 127–133

[31] C. Khare, *Serre's modularity conjecture: the level one case*, Duke Math. J. **134** (2006), 557–589

[32] C. Khare, M. Larsen and G. Savin, *Functoriality and the inverse Galois problem*, Compos. Math. **144** (2008), 541–564,
Functoriality and the Inverse Galois problem II: Groups ot type B_n and G_2, preprint available at:
`http://www.math.ucla.edu/~shekhar/papers/galois.pdf`

[33] C. Khare and J.-P. Wintenberger, *On Serre's conjecture for 2-dimensional mod p representations of the absolute Galois group of the rationals*, to appear in Annals of Math., preprint available at
`http://www.math.utah.edu/~shekhar/serre.pdf`

[34] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I), (II)*, preprint (2007) available at
`http://www.math.ucla.edu/~shekhar/papers/results.pdf`
`http://www.math.ucla.edu/~shekhar/papers/proofs.pdf`

[35] M. Kisin, *Modularity of 2-adic Barsotti-Tate representations*, preprint (2007) available at `http://www.math.uchicago.edu/~kisin/preprints.html`

[36] J. Klüners and G. Malle, *A Database for Number Fields*,
`http://www.math.uni-duesseldorf.de/~klueners/minimum/minimum.html`

[37] R. P. Langlands, *Base change for* GL(2), Ann. Math. Stud. **96**, Princeton Univ. Press, Princeton, N.J.; Univ. of Tokyo Press, Tokyo, 1980

[38] R. Livné, *On the conductors of mod ℓ Galois representations coming from modular forms*, J. Number Theory **31** (1989), 133–141
[39] H. Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), 156–165
[40] H. Moon and Y. Taguchi, *Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations*, Documenta Math. Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 641–654
[41] H. Moon and Y. Taguchi, *The non-existence of certain mod 2 Galois representations of some small quadratic fields*, Proc. Japan Acad., Ser. A, **84** (2008), 63–67
[42] L. Moret-Bailly, *Groupes de Picard et problèmes de Skolem II*, Ann. Sci. École Norm. Sup. **22** (1989), 181–194
[43] R. Ramakrishna, *Lifting Galois representations,* Invent. Math. **138** (1999), 537–562
[44] R. Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur,* Ann. of Math. **156** (2002), 115–154
[45] M. Raussen and C. Skau, *Interview with Jean-Pierre Serre*, Notices of the AMS **51** (2004), 210–214
[46] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476
[47] K. A. Ribet, *Report on mod ℓ representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, in: "Motives" (Seattle, WA, 1991), pp. 639–676, Proc. Sympos. Pure Math. **55**, Part 2, Amer. Math. Soc., Providence, RI, 1994
[48] K. A. Ribet, *Abelian varieties over* $\mathbb{Q}$ *and modular forms*, Algebra and Topology 1992 (Daejeon), pp. 53–79, KAIST, Daejeon, 1992
[49] 斎藤毅『Fermat 予想』, 岩波書店, 2009 年
[50] 斎藤毅, 山下剛, 安田正大 (編), 『$R = \mathbb{T}$ の最近の発展 1, 2』, 「$R = \mathbb{T}$ の最近の発展についての勉強会」
`http://www.kurims.kyoto-u.ac.jp/~gokun/R=T.html`
の報告集, 2009 年
[51] R. Schoof, *Abelian varieties over* $\mathbb{Q}$ *with bad reduction in one prime only*, Compos. Math. **141** (2005), 847–868
[52] M. H. Şengün, *The non-existence of certain representations of the absolute Galois group of quadratic fields*, Proc. Amer. Math. Soc. **137** (2009), 27–35
[53] J.-P. Serre, *Congruences et formes modulaires (d'apres H. P. F. Swinnerton-Dyer)*, Séminaire Bourbaki, 24e annee (1971/1972), Exp. 416, pp. 319–338, in: Lecture Notes in Math. **317**, Springer-Verlag, Berlin, 1973
[54] J.-P. Serre, *Valeurs propres des opérateurs de Hecke modulo ℓ*, Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, 1974), pp. 109–117, Astérisque **24-25**, Soc. Math. France, Paris, 1975
[55] J.-P. Serre, *Lettre à J.-F. Mestre*, 13 Août, 1985, in: Œuvres, vol. IV, pp. 101–106
[56] J.-P. Serre, Note $229._2$ on p. 710, Œuvres III, Springer-Verlag, 1986
[57] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230
[58] J.-P. Serre, Résumé des cours au Collège de France, 1987–1988
[59] J.-P. Serre, *Two letters on quaternions and modular forms (mod p)*, With introduction, appendix and references by R. Livné, Israel J. Math. **95** (1996), 281–299
[60] C. Skinner and A. Wiles, *Residually reducible representations and modular forms*, Inst. Hautes Études Sci. Publ. Math. **89** (1999), 5–126

[61] W. Stein, *The Modular Forms Database*,
`http://modular.fas.harvard.edu/Tables/`

[62] J. Tate, *The non-existence of certain Galois extensions of* $\mathbb{Q}$ *unramified outside* 2, in: "Arithmetic Geometry", pp. 153–xs156, Contemp. Math. **174**, Amer. Math. Soc., Providence, RI, 1994

[63] J. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3**, 1970, 1–21

[64] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu **1** (2002), 125–143

[65] R. Taylor, On icosahedral Artin representations. II, Amer. J. Math. **125** (2003), 549–566

[66] R. Taylor, *On the meromorphic continuation of degree two L-functions*, Doc. Math. 2006, Extra Vol., 729–779

[67] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553–572

[68] Y. Tomiyama, *Lifting Galois representations over arbitrary number fields*, preprint (2008)

[69] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. **5** (1981), 173–175

[70] D. Vogan, Jr. and G. Zuckerman, *Unitary representations with nonzero cohomology*, Compositio Math. **53** (1984), 51–90

[71] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443–551

[72] 安田正大, 「2009 年度整数論サマースクール報告集」に掲載予定の Serre 予想の証明についての解説記事

[73] 『数学のたのしみ』2008 年最終号, 日本評論社