

総実代数体上の楕円曲線の保型性について

On modularity of elliptic curves over certain totally real fields; a résumé

By

吉川 祥* (Sho Yoshikawa)

Abstract

This article is a summary of [13]. We give an outline of the proof of author's recent result; that is, modularity of all elliptic curves over abelian totally real fields unramified at 3, 5, and 7.

§ 1. 主結果

F を総実代数体とする. F の代数閉体 $\bar{F}$ をひとつ固定し, F の絶対 Galois 群 $\text{Gal}(\bar{F}/F)$ を G_F とおく. また, E を F 上定義された楕円曲線とする. 各素数 p に対して, E の p 等分点 $E[p](\bar{F})$ や p 進 Tate 加群 $V_p(E) = (\varprojlim_n E[p^n](\bar{F}))[1/p]$ に対して G_F が自然に作用する. これらの作用によって, 2 次元法 p 表現

$$\bar{\rho}_{E,p}: G_F \rightarrow \text{GL}_2(\mathbb{F}_p)$$

と既約な 2 次元 p 進表現

$$\rho_{E,p}: G_F \rightarrow \text{GL}_2(\mathbb{Q}_p)$$

が得られる. 一方, f を F 上の Hilbert カスプ固有形式とする. 楕円曲線との対応を鑑み, f として重さ $(2, \dots, 2)$ であり $\mathbb{Q}$ 係数であるものを考える. このとき, 各素数 p に対し, f に付随して, 既約な 2 次元 p 進表現

$$\rho_{f,p}: G_F \rightarrow \text{GL}_2(\mathbb{Q}_p)$$

Received March 31, 2017. Revised June 1, 2018.

2010 Mathematics Subject Classification(s): 11G05, 11F41, 11F80

Key Words: Hilbert modular forms, elliptic curves, Galois representations.

This work is supported by the Program for Leading Graduate Schools, MEXT, Japan, and by JSPS KAKENHI Grant Number JP17H07074.

*学習院大学 理学部数学科 (講演時: 東京大学 数理科学研究科)

e-mail: yoshikawa@math.gakushuin.ac.jp

が得られる. $\rho_{f,p}$ は, Frobenius 共役類のトレースが f の Hecke 固有値に等しいという条件によって特徴づけられる. ある f に対する $\rho_{f,p}$ に同形な p 進 Galois 表現は, 保型的な p 進 Galois 表現と呼ばれる.

定義 1.1. F を総実代数体とし, E を F 上の楕円曲線とする. E が保型的であるとは, すべての素数 p に対して $\rho_{E,p}$ が保型的であることをいう.

注意 1.2. 楕円曲線 E が保型的であることは, E の Hasse-Weil L 関数がある Hilbert 保型形式の L 関数になっていることと同値である. 特に, 定義における「すべての素数 p 」を「ある素数 p 」に置き換えてもよい.

予想 1.3. F を総実代数体とし, E を F 上の楕円曲線とする. このとき E は保型的である.

保型形式に付随する L 関数は全平面に解析接続されることが知られているため, 予想を認めれば, E の Hasse-Weil L 関数も全平面に解析接続されることになる.

楕円曲線の保型性は GL_2 の大域 Langlands 対応の特別な場合とみなせる. 予想 1.3 に関連する結果としては, 例えば以下が知られている.

- (Wiles [12], Taylor-Wiles [9], Breuil-Conrad-Diamond-Taylor [2]) F が有理数体のとき, 予想 1.3 は正しい. この場合の予想 1.3 は志村-谷山予想と呼ばれ, 準安定楕円曲線に対する志村-谷山予想は Fermat 予想の解決において決定的な役割を果たした.
- (Freitas- Le Hung- Siksek [4]) F が実二次体であるとき, 予想 1.3 は正しい.
- (Thorne [11]) p を素数とし, F を $\mathbb{Q}$ の $\mathbb{Z}_p$ 円分拡大に含まれる総実代数体とする. F に対して予想 1.3 は正しい.

次が本論説の主定理である.

定理 1.4. F を有理数体 $\mathbb{Q}$ 上アーベルな総実代数体で, 3,5,7 で不分岐であるとする. このとき, 予想 1.3 は正しい.

次節で述べるように, 適切な仮定を課した楕円曲線の保型性は (保型性持ち上げ定理の帰結として) すでに知られている. しかし, 総実代数体 F が与えられたときに, F 上の**すべての**楕円曲線が保型的であることを示すことは困難であったと思われる.

定理 1.4 の新しい点は, 定理のような総実代数体 F に対しては, F 上のすべての楕円曲線の保型性は次節で述べるいずれかの保型性定理に帰着できることを見出した点である. 証明の概略は第 3 節で述べる.

§ 2. 楕円曲線の保型性定理

p を素数とする. 2 次元 p 進 Galois 表現が保型的であることを証明するための道具として, 様々な保型性持ち上げ定理が示されている. 保型性持ち上げ定理とは, p 進表現 ρ

が与えられたとき、法 p 還元 $\bar{\rho}$ の保型性から ρ 自身の保型性を導くというタイプの主張である。ここで法 p 表現の保型性とは、大雑把に述べると、その法 p 表現が適切な Hilbert 保型形式に付随する p 進 Galois 表現の法 p 還元と同形であることをいう。

この節では、保型性持ち上げ定理の帰結として得られる楕円曲線の保型性定理を紹介する。これらは定理 1.4 の証明における重要な部品をなす。

定理 2.1. ([4, Theorem 3, Theorem 4]) $p = 3, 5$ または 7 とし、 E を総実代数体 F 上の楕円曲線とする。 $\bar{\rho}_{E,p}|_{G_{F(\zeta_p)}}$ が絶対既約であるならば、 E は保型的である。

法 p 剰余表現を $G_{F(\zeta_p)}$ に制限した時に絶対既約であるという条件は、Taylor-Wiles 条件と呼ばれる。既存の保型性持ち上げ定理の多くは Taylor-Wiles 条件のもとで証明されている。定理 2.1 はそうした強力な保型性持ち上げ定理の帰結である。

Taylor-Wiles 条件が成り立たない場合を扱うためには、以下に述べる二つの保型性定理が有用である。ひとつは、Thorne による保型性定理である。もうひとつは、剰余既約表現に対する Skinner-Wiles の保型性持ち上げ定理 ([8, Theorem 5.1], [6, Theorem 1]) を、楕円曲線の Tate 加群に適用したものである。

定理 2.2. ([10, Theorem 7.6]) F を $\sqrt{5} \notin F$ である総実代数体とし、 E を F 上の楕円曲線とする。 $\bar{\rho}_{E,5}$ が既約ならば、 E は保型的である。

定理 2.3. $p > 2$ を素数とし、 F を総実代数体とする。簡単のために p で不分岐であると仮定する。また、 E を F 上の楕円曲線とし、 $\bar{\rho}_{E,p}$ が既約であり $\bar{\rho}_{E,p}|_{G_{F(\zeta_p)}}$ が絶対可約であるとする。もし p を割るすべての素点で潜在的通常良還元を持つならば、 E は保型的である。

注意 2.4. 実際の Skinner-Wiles の保型性持ち上げ定理では、法 p 表現が χ_2 -good という性質を満たす保型的な p 進表現に持ち上がる、という条件が課されている。 $\bar{\rho}_{E,p}$ が既約かつ $\bar{\rho}_{E,p}|_{G_{F(\zeta_p)}}$ が絶対可約のとき、 $\bar{\rho}_{E,p}$ は二面体的であり、この条件は満たされることが知られている。例えば [1, Lemma 5.1.2] を参照せよ。

最後に、Freitas による楕円曲線の保型性定理を用意しておく。

定理 2.5. ([3, Theorem 6.3]) F を $\mathbb{Q}$ 上アーベルかつ 3 で不分岐な総実代数体とし、 E を F 上の楕円曲線とする。 E が 3 を割るすべての素点で準安定還元をもつならば、 E は保型的である。

§ 3. 証明の概略

以下、 F を総実代数体とし、 E を F 上の楕円曲線とする。 F が $3, 5, 7$ で不分岐かつ $\mathbb{Q}$ 上アーベルな拡大という仮定がどこで使われているかを明確にするため、以下の小節において F に関する仮定が必要になった際にその都度仮定を述べることにする。

§ 3.1. $p = 3, 5$, または 7 に対して $\bar{\rho}_{E,p}|_{G_F(\zeta_p)}$ が絶対既約の場合

この場合は F は一般の総実代数体でよく, 定理 2.1 を適用すれば E の保型性が分かる.

§ 3.2. $p = 3, 5$, かつ 7 に対して $\bar{\rho}_{E,p}|_{G_F(\zeta_p)}$ が絶対可約の場合

このとき, 以下の (1) から (3) のそれぞれの場合において E の保型性を証明することが出来る.

(1) $\bar{\rho}_{E,5}$ が既約である場合. この場合はさらに F が 5 で不分岐と仮定する. すると, E の保型性は定理 2.2 から従う.

(2) $\bar{\rho}_{E,7}$ が既約である場合. この場合はさらに F が 7 で不分岐と仮定する. 5 ではなく 7 の場合に Thorne の定理 2.2 の類似を示せばよい. Thorne は新たな $R = \mathbb{T}$ 定理を証明し, その系として定理 2.2 を導いていたが, 7 の場合の類似は Thorne の定理よりかはるかに簡単に示せる.

命題 3.1. F を 7 で不分岐である総実代数体とし, E を F 上の楕円曲線とする. $\rho_{E,7}$ が既約であり, $\bar{\rho}_{E,7}|_{G_F(\zeta_7)}$ が絶対可約ならば, E は 7 を割るすべての素点において潜在的に通常良還元を持つ (とくに, E に対応する 7 進表現は概通常である).

Proof. 証明の概略を述べる. $\rho_{E,7}$ が既約かつ $\bar{\rho}_{E,7}|_{G_F(\zeta_7)}$ が絶対可約のとき, [4, Proposition 9.1] により像 $\rho_{E,7}(G_F)$ の射影像が S_3 または D_4 に同形であることが知られている. 特に, $\rho_{E,7}(G_F)$ の射影像は位数 6 または 8 の元を持たない. 一方, $v|7$ で潜在的に乗法的還元または潜在的に超特異良還元を持つと仮定すると, 惰性群 I_v への制限 $\rho_{E,7}|_{I_v}$ の表示を調べることにより, $\rho_{E,7}(I_v)$ が位数 6 または 8 の元を持つことが示される. (v で準安定還元を持たない場合の $\rho_{E,7}|_{I_v}$ の表示は Kraus[5] を用いる.) $\square$

命題 3.1 と定理 2.3 により, E は保型的であることがわかる.

注意 3.2. 命題 3.1 と同様の方法では定理 2.2 を再証明することは出来ない. 実際, $\rho_{E,5}$ が既約かつ $\bar{\rho}_{E,5}|_{G_F(\zeta_5)}$ が絶対可約であっても, 5 で潜在的に超特異良還元を持つ場合を排除できない. したがって, 定理 2.3 を適用できない.

(3) $\bar{\rho}_{E,5}$ と $\bar{\rho}_{E,7}$ が可約である場合. この場合はさらに F が 3 で不分岐かつ $\mathbb{Q}$ 上アーベルと仮定する.

補題 3.3. $\bar{\rho}_{E,5}$ と $\bar{\rho}_{E,7}$ が可約であるとする. このとき, E の二次捻り E' であって, 3 を割る F のすべての素点 v において準安定還元をもつものが存在する.

Proof. 証明の概略のみを述べる. 各 $v|3$ について, $E_v = E \otimes_F F_v$ のある二次捻りが準安定還元を持てばよい. E が v で潜在的に乗法的還元を持つ場合は, このことは Tate

曲線の理論から知られている. E が v で潜在的に良還元を持つ場合は, $\bar{I}_v = \bar{\rho}_{E,\ell}(I_v)$ (ℓ によらない) の位数が 1 か 2 であることを示せば十分である. $\bar{\rho}_{E,\ell}(\ell = 5, 7)$ が可約なため, $\bar{I}_v$ は $\mathrm{GL}_2(\mathbb{F}_\ell)$ ($\ell = 5, 7$) の Borel 部分群に入っており, このことから $\bar{I}_v$ の位数は 1 または 2 であることが計算できる. $\square$

定理 2.5 によって, 補題における E' は保型的であることが知られている. 保型的であるかどうかは二次捻りによって変わらないので, E の保型性が示される.

3.1 節と 3.2 節の (1), (2), (3) を合わせて, 定理 1.4 が従う.

References

- [1] P. B. Allen, *Modularity of nearly ordinary 2-adic residually dihedral Galois representations*, Compositio Mathematica 150. 08 (2014), 1235–1346.
- [2] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843–939.
- [3] N. Freitas, *Recipes for Fermat-type equation of the form $x^r + y^r = Cz^p$* , Mathematische Zeitschrift 279 (2015), no. 3-4, 605–639.
- [4] N. Freitas, B. Le Hung, S. Siksek, *Elliptic Curves over Real Quadratic Fields are Modular*, Inventiones Mathematicae 201 (2015), 159–206.
- [5] A. Kraus, *Détermination du poids et du conducteur associés aux représentations des points de p -torsion d'une courbe elliptique*, Warszawa: Instytut Matematyczny Polskiej Akademii Nauk, 1997.
- [6] C. Skinner, *Nearly ordinary deformation of residually dihedral representations*, preprint.
- [7] C. Skinner, A. Wiles, *Residually reducible representations and modular forms*, Publications mathématiques de l' I.H.É.S., tome 89 (1999), 5–126.
- [8] C. Skinner, A. Wiles, *Nearly ordinary deformations of irreducible residual representations*, Annales de la Faculté des sciences de Toulouse : Mathématiques (2001) Volume: 10, Issue: 1, page 185–215.
- [9] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics 141 (1995), no. 3, 553–572.
- [10] J. Thorne, *Automorphy of some residually dihedral Galois representations*, Mathematische Annalen 364 (2016), No. 1-2, pp. 589–648.
- [11] J. Thorne, *Elliptic curves over $\mathbb{Q}_\infty$ are modular*, Preprint.
- [12] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics 141 (1995), no. 3, 443–551.
- [13] S. Yoshikawa, *Modularity of elliptic curves over abelian totally real fields unramified at 3, 5, and 7*, to appear in Journal de Théorie des Nombres de Bordeaux; also available at <https://arxiv.org/abs/1606.06597>.