論文題目 On modularity of elliptic curves over abelian totally real fields
(総実アーベル拡大体上の楕円曲線の保型性について)

氏　　名 吉川 祥

背景

K を総実代数体とする．K 上の楕円曲線 E が与えられると，各素数 p に対して p 進 Tate 加群を考えることにより，２次元 p 進 Galois 表現 $\rho_{E,p}:\mathrm{Gal}(\bar{K}/K)\to\mathrm{GL}_2(\mathbb{Q}_p)$ が定義される．一方で，K 上定義された有理数係数 Hilbert カスプ固有形式 f が与えられると，各素数 p に対して，f に付随した 2 次元 p 進 Galois 表現 $\rho_{f,p}:\mathrm{Gal}(\bar{K}/K)\to\mathrm{GL}_2(\mathbb{Q}_p)$ が構成される．志村-谷山予想 (現在では保型性定理とも呼ばれる) とは，次のように $K=\mathbb{Q}$ の場合に楕円曲線と保型形式との間のつながりを述べる予想である．

定理 1（志村-谷山予想） 有理数体上定義されたすべての楕円曲線 E は保型的である．すなわち，有理数係数かつ重さ 2 の適切なカスプ固有形式 f が存在して，すべての (または少なくとも一つの) 素数 p に対して $\rho_{E,p}\simeq\rho_{f,p}$ が成り立つ.

20 世紀の整数論における最大の到達点のひとつとして，Wiles による Fermat 予想の解決が挙げられる．Frey，Serre，Ribet は Fermat 予想が志村-谷山予想に帰着されることを見出し，Wiles が Taylor と共に準安定な楕円曲線に対する志村-谷山予想を証明 [7, 10] したことにより，Fermat 予想は解決されたのであった．そして後に Breuil-Conrad-Diamond-Taylor[1] によって，一般の志村-谷山予想も解決された．Wiles が考案した手法の核心のひとつは，Galois 表現の変形環と局所 Hecke 環との間の同形を証明する機構を与えるものである．彼はそれを用いることにより保型性持ち上げ定理を証明している．ここで保型性持ち上げ定理とは，p 進 Galois 表現の保型性をその mod p 還元の保型性から導くというタイプの定理である．Wiles の手法はその後 Diamond-藤原や Kisin によって改良され，現在までにより強力な保型性持ち上げ定理が証明されている．また，楕円曲線の mod 5 表現の保型性を別の楕円曲線の mod 3 表現の保型性から導くという，いわゆる 3-5 トリックの考案も，Wiles の証明において重要な役割を果たしている．

Wiles が切り開いた数学は更に発展し，Taylor らが潜在的保型性定理を用いて佐藤-Tate 予想の大部分を解決し，Khare-Wintenberger は保型性持ち上げ定理や潜在的保型性定理を駆使することで Serre の保型性予想をも解決するに至った.

そして現在では，2 次元表現だけではなく，より高次元の表現の保型性を扱う流れがある．その一方で，保型性持ち上げ定理の発展を受けて，志村-谷山予想を総実代数体へ一般化する試みもある．(本論文では後者を考察する．)

予想 2 総実代数体 K 上のすべての楕円曲線 E は保型的である．すなわち，有理数係数かつ重さ $(2,...,2)$ である K 上定義された Hilbert カスプ固有形式 f が存在し，すべての (または少なくとも一つの) 素数 p に対して $\rho_{E,p}\simeq\rho_{f,p}$ が成り立つ.

この予想のことを，ここでは保型性予想と呼ぶことにする．既存の保型性持ち上げ定理を用いれば多くの楕円曲線に対して保型性を証明できるが，総実代数体 K を固定したとき，K 上のすべての楕円曲線が保型的であることを証明することは一般には困難であると思われる．その理由は，保型性持ち上げ定理の仮定を満たさない楕円曲線が存在しうるためである．このような制約の中，様々な総実代数体に対する保型性予想について，現在までに次のような結果が得られている．

1. Le Hung は彼の博士論文 [5] において，総実代数体 K を与えたとき，K 上の楕円曲線はほとんどすべて保型的であることを証明した．また，5 と 7 で不分岐な実二次体に対して，保型性予想を証明した．
2. Freitas-Le Hung-Siksek[3] は，すべての実二次体に対して，保型性予想を証明した．
3. Thorne[9] は，p を素数として，総実代数体 K が $\mathbb{Z}_p$ 円分拡大に含まれている場合に保型性予想を証明した．

主結果

本論文の主目的は，保型性予想の新たな場合を証明することである．本論文には二つの主定理がある．

(i) まず，一つ目の主定理を述べる．

定理 3 総実代数体 K が有理数体上アーベルかつ $3, 5, 7$ が不分岐であるとする．このような K に対して保型性予想は正しい．

定理 3 により，先行研究 [5],[3],[9] において考察されていた特殊な定義体の多くを含みつつ，かなり広いクラスの定義体に対して保型性予想が証明されたと言える．

定理 3 の証明の概略を述べる．K を定理で述べた総実代数体とし，E を K 上の楕円曲線とする．本証明において重要なステップは、E の保型性は既に知られている保型性持ち上げ定理に帰着できるという点である．そのような帰着の手法を見出したことが，本研究の意義である．さて，素数 p に対して，p 等分点が定める 2 次元 mod p Galois 表現を $\bar{\rho}_{E,p}$ と書く．$p = 3, 5, 7$ における $\bar{\rho}_{E,p}|_{\mathrm{Gal}(\bar{K}/K(\zeta_p))}$ や $\bar{\rho}_{E,p}$ の既約性によって場合を分け考察する．

$p = 3, 5,$ または 7 において $\bar{\rho}_{E,p}|_{\mathrm{Gal}(\bar{K}/K(\zeta_p))}$ が絶対既約である場合は，$\bar{\rho}_{E,p}$ に対して既存の保型性持ち上げ定理を適用でき，E の保型性が証明できる．

$p = 3, 5,$ かつ 7 において $\bar{\rho}_{E,p}|_{\mathrm{Gal}(\bar{K}/K(\zeta_p))}$ が絶対可約である場合は，さらに細かく場合をわけてゆく．

- $\bar{\rho}_{E,5}$ が既約ならば，Thorne の定理 [8] によって E が保型的であることが示される．
- $\bar{\rho}_{E,7}$ が既約ならば，$\bar{\rho}_{E,7}$ の射影像は S_3 または A_4 となる．すると，E は 7 を割る素点で潜在的超特異還元を持ち得ないことが確認できる．このことは，不分岐な p 進体上の楕円曲線が定める mod p 表現の記述を用いて示される．この記述は Kraus[4] による．超特異性を排除した結果，Skinner-Wiles の保型性持ち上げ定理 [6] を適用することが可能となり，E の保型性が示される．

- 最後に考察するべき場合は，$\bar{\rho}_{E,5}$ と $\bar{\rho}_{E,7}$ が同時に可約となる場合である．この場合は E の適切な二次捻りをとることによって，3 を割るすべての素点において E が準安定還元を持つ場合に帰着される．そのような楕円曲線の保型性は，Freitas[2] によって証明されているため，定理 3 の証明が完成する．

(ii) 次が本論文の二つ目の主定理である．

定理 4　p を 5 または 7 とし，X をモジュラー曲線 $X_0(3p)$ とする．(このモジュラー曲線は同時に楕円曲線でもある．) K を有限個の実二次体の合成体で，$2, 3, p$ を割る素点で不分岐なものとする．$\mathrm{Gal}(K/\mathbb{Q})$ の 2 次指標 s すべてについて，X の 2 次捻り $X^{(s)}$ が有理点を有限個しかもたないと仮定する．このとき，K に関して保型性予想は正しい．

定理 4 は [9] と同様，二次体の結果 [3] をより一般の体に拡張する試みである．[9] は Galois 群が巡回的な定義体を考えているのに対し，定理 4 では Galois 群が $\mathbb{Z}/(2)$ の直積である定義体を考えるため，両者は別方向の一般化と言える．証明の手法はどちらもモジュラー曲線の有理点を考察するものであるが，定理 4 の証明の手法は，モジュラー曲線の二次捻りの有理点を考察するという意味で，[3] において用いられた手法に近いものとなっている．

以下，定理 4 の証明の概略を述べる．E を K 上の楕円曲線とする．$\bar{\rho}_{E,p}$ が既約な場合は (i) の証明の概略で述べたようにして既に E の保型性は分かっているため，$\bar{\rho}_{E,p}$ が可約な場合が問題となる．この場合，E はあるモジュラー曲線の K 値点を定める．このモジュラー曲線は，定理で述べた X，または X の二次被覆であるもう一つのモジュラー曲線である．証明の重要なステップは，$X(K) = X(\mathbb{Q})$ を証明することである．これにより，本質的には E が有理数体上か実二次体上の楕円曲線の底変換として得られることが示される．その結果，E の保型性は定理 1 や Freitas-Le Hung-Siksek[3] から従うことがわかり，定理 4 の証明が完成する．

参考文献

[1] 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.

[2] 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.

[3] N. Freitas, B. Le Hung, S. Siksek, *Elliptic Curves over Real Quadratic Fields are Modular*, Inventiones Mathematicae 201 (2015), 159-206.

[4] A. Kraus, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique*, Warszawa: Instytut Matematyczny Polskiej Akademi Nauk, 1997.

[5] B. Le Hung, *Modularity of some elliptic curves over totally real fields*, available at http://arxiv.org/abs/1309.4134.

[6] C. Skinner, A. Wiles, *Nearly ordinary deformations of irreducible residual representations*, Annales de la Faculte des sciences de Toulouse : Mathematiques (2001) Volume: 10, Issue: 1, page 185-215.

[7] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics **141** (1995), no. 3, 553-572.

[8] J. Thorne, *Automorphy of some residually dihedral Galois representations*, Mathematische Annalen 364 (2016), No. 1-2, pp. 589-648.

[9] J. Thorne, *Elliptic curves over* $\mathbb{Q}_\infty$ *are modular*, Preprint.

[10] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), no. 3, 443-551.