志村曲線の虚2次体上の有理点について

新井 啓介 (東京電機大学)

概 要

k を類数が 1 でない虚 2 次体とする. このとき, $\mathbb{Q}$ 上の不定符号 4 元数体 B で, 付随する志村曲線 M^B が k 有理点をもつようなものは同型を除いて有限個しかない, という定理を得た. 本稿ではこの定理を, 以前に筆者が得ていた B の判別式の素因数に関するある種の合同式を仮定した部分的な結果から導く.

1 モジュラー曲線の有理点と基本問題

p を素数とし, 楕円曲線 E とその位数 p の巡回部分群 C の組 (E, C) の同型類を分類する $\mathbb{Q}$ 上の粗モジュライを $Y_0(p)$ とする. すると $Y_0(p)$ は $\mathbb{Q}$ 上のアファインスムーズ代数曲線であり, **モジュラー曲線**と呼ばれている ([17, 定理 2.10] を参照). $Y_0(p)$ をコンパクト化した $X_0(p)$ もよく用いられるが, ここでは扱わない. $Y_0(p)$ の有理点に関して, 次の定理が知られている.

定理 1.1 ([13, Theorem 7.1])**.** $p > 163$ ならば, $Y_0(p)$ の $\mathbb{Q}$ 有理点の集合 $Y_0(p)(\mathbb{Q})$ は空集合である.

注 1.2. 定理 1.1 は, 2 次体 (ただし類数 1 の虚 2 次体を除く) 上の有理点に関する結果へと拡張された ([16, Theorem B]).

ここで, 次の基本的な問題を考えよう.

問題 1.3. X をある種のアーベル多様体のモジュライとし (例えば $X = Y_0(p)$), k を代数体とする. X のレベル ($X = Y_0(p)$ のときはレベルは p) が上がるとき, k 有理点の集合 $X(k)$ は小さくなるか?

この問題は, いくつかの場合に解決されている. この節の残りの部分では, X が (構造付き) 楕円曲線のモジュライの場合に, 解決されている例を紹介する.

楕円曲線 E とその位数 p の点 P の組 (E, P) の同型類を分類する $\mathbb{Q}$ 上の粗モジュライを $Y_1(p)$ とする ($p > 3$ なら, $Y_1(p)$ は精モジュライである). すると $Y_1(p)$ も $\mathbb{Q}$ 上のアファインスムーズ代数曲線であり, やはり**モジュラー曲線**と呼ばれている ([17, 定理 8.34] を参照). $Y_1(p)$ の有理点に関して, 次の定理が知られている.

定理 1.4 ([14, Théorème], cf. [11, Theorem 3.4])**.** $d > 1$ を整数とし, k を次数 d の代数体とする. $p > d^{3d^2}$ なら, $Y_1(p)(k) = \emptyset$ である.

注 1.5. $(E, P) \mapsto (E, \langle P \rangle)$ により $\mathbb{Q}$ 上の射 $Y_1(p) \longrightarrow Y_0(p)$ が定まる. ここに, $\langle P \rangle$ は P が生成する E の部分群である. よって, 代数体 k に対して, $Y_0(p)(k) = \emptyset$ ならば $Y_1(p)(k) = \emptyset$ となることが分かる. $Y_0(p)$ と比べて $Y_1(p)$ の方が強いレベル構造を課しているので, 有理点が少なくなりがちである. 実際, 知られている結果もそのようになっている. つまり, 問題 1.3 は $X = Y_0(p)$ の場合は 2 次体までしか解決されていないが, $X = Y_1(p)$ の場合は任意の次数の代数体 (しかも次数を固定すれば体を動かしてもよい) で解決されている.

楕円曲線 E とその位数 p の部分群 A, B で $A \cap B = \{0\}$ となるものの順序をもたない対 $\{A, B\}$ の組 $(E,\{A,B\})$ の同型類を分類する $\mathbb{Q}$ 上の粗モジュライを $Y_{\mathrm{split}}(p)$ とする. すると $Y_{\mathrm{split}}(p)$ も $\mathbb{Q}$ 上のアファインスムーズ代数曲線であり, **モジュラー曲線**と呼ばれている ([15, p.115] を参照). $Y_{\mathrm{split}}(p)$ の有理点に関して, 次の定理が知られている.

定理 1.6 ([7, Theorem 1.1], cf. [6, Theorem 1.2])**.** $p \geq 11$, $p \neq 13$ ならば, $Y_{\mathrm{split}}(p)(\mathbb{Q})$ の任意の点は (もしあれば) CM 点である. ここに, CM 点とは CM 楕円曲線と対応するような点のことである.

注 1.7. モジュラー曲線の有理点に関しては, [1, §2] も参照.

2 志村曲線の有理点と主結果

B を $\mathbb{Q}$ 上の 4 元数環とし, 不定符号 (すなわち $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$) かつ斜体 (すなわち $B \ncong \mathrm{M}_2(\mathbb{Q})$) であるとする. $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \ncong \mathrm{M}_2(\mathbb{Q}_p)$ を満たす素数 p 全ての積を B の**判別式**と呼び, $d(B)$ で表す. B は不定符号なので $d(B)$ は相異なる偶数個の素数の積に等しく, B は斜体なので $d(B) > 1$ である. B の同型類は $d(B)$ により一意的に定まる. B の極大整環 $\mathcal{O}$ を 1 つとり, 固定しておく. $\mathcal{O}$ のとり方は一意的ではないが, B の任意の極大整環は $a^{-1}\mathcal{O}a$ (ただし $a \in B^{\times}$) と表される. $\mathbb{Q}$ 上の 4 元数環については, 例えば [18, §3.5–3.6, 特に定理 3.5, 3.10] を参照.

$\mathcal{O}$ による乗法をもつ **QM アーベル曲面**とは, 2 次元アーベル多様体 A と環の単射準同型 $i : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ で $i(1) = id$ を満たすものの組 (A, i) のことである. ここに, $\mathrm{End}(A)$ は A の自己準同型環である. $\mathcal{O}$ による乗法をもつ QM アーベル曲面を分類する $\mathbb{Q}$ 上の粗モジュライを M^B とする. すると M^B は $\mathbb{Q}$ 上の固有スムーズ代数曲線であり, **志村曲線**と呼ばれている. M^B の $\mathbb{Q}$ 上の同型類は $d(B)$ により一意的に定まる. M^B はアファインな $Y_0(p)$, $Y_1(p)$, $Y_{\mathrm{split}}(p)$ とは異なり, 固有である. また, M^B はカスプをもたない. QM アーベル曲面や志村曲線については, 例えば [9, p.93] を参照.

M^B の有理点に関して, 次の基本的な結果が知られている.

定理 2.1 ([19, Theorem 0])**.** $M^B(\mathbb{R}) = \emptyset$.

定理 2.1 より, 代数体 k に実素点があれば, $M^B(k) = \emptyset$ となることが分かる. 特に $M^B(\mathbb{Q}) = \emptyset$ である. M^B の具体例を挙げよう.

例 2.2. $d(B) = 6$ なら M^B は方程式 $X^2 + Y^2 + 3Z^2 = 0$ で定義される $\mathbb{Q}$ 上の射影代数曲線であり ([12, Theorem 1-1] を参照), この方程式は非自明な実数解 (すなわち方程式を満たす実数の 3 つ組 (X, Y, Z) で $(0, 0, 0)$ でないもの) をもたない.

今回の主結果は以下の通りである.

定理 2.3 ([3, Theorem 1.1])**.** k を類数が 1 でない虚 2 次体とする. このとき k に依存した正の整数の有限集合 $D(k)$ が存在して, 次の条件を満たす: $d(B) \notin D(k)$ ならば, $M^B(k) = \emptyset$.

注 2.4. (1) $X = M^B$ のレベルを $d(B)$ と思った場合, 類数が 1 でない虚 2 次体 k に対して, 問題 1.3 が解決されたことになる.
(2) QM アーベル曲面にレベル構造を付加し, $Y_0(p)$ や $Y_1(p)$ の類似となるような志村曲線を考えることもできる. それらに対して問題 1.3 が解決された例については, それぞれ [5, Theorem 1.3], [8, Theorem 1.1] を参照. 後者の結果は, 局所体に関するより強い結果になっている.
(3) 志村曲線の有理点に関しては, [4] も参照.

主結果を少し言い換えておく．定理 2.3 は次の定理 2.5 と同値である．同値であることは, $d(B)$ が平方因子をもたないことから従う．

定理 2.5 ([3, Theorem 1.2])**.** k を類数が 1 でない虚 2 次体とする．このとき k に依存した素数の有限集合 $P(k)$ が存在して, 次の条件を満たす: $d(B)$ の素因数で $P(k)$ に入らないものがあれば, $M^B(k) = \emptyset$.

注 2.6. 有限集合 $P(k)$ の上界は, 高々1 つの元を除いて評価が可能である．

定理 2.5 の $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ の場合は, Jordan により証明されていた．

定理 2.7 ([9, Theorem 6.6])**.** k を類数が 1 でない虚 2 次体とする．このとき k に依存した素数の有限集合 $P_J(k)$ が存在して, 次の条件を満たす: $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ であり, さらに $d(B)$ の素因数で $P_J(k)$ に入らないものがあれば, $M^B(k) = \emptyset$.

虚 2 次体 k の類数が 1 の場合は, $M^B(k)$ は異なる挙動を示す．

定理 2.8 ([9, Proposition 6.5])**.** k を類数が 1 の虚 2 次体とすると, $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ ならば $M^B(k) \neq \emptyset$.

3　主結果 (定理 2.5) の部分的な結果 (定理 2.7, 3.1) への帰着

筆者は, 以前に定理 2.5 の $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ の場合を部分的に証明していた．$B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ の場合が $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ の場合と比べて難しい理由は, 次節で述べる．

定理 3.1 ([2, Theorem 1.2])**.** k を類数が 1 でない虚 2 次体とする．このとき k に依存した素数の有限集合 $P_0(k)$ が存在して, 次の条件を満たす: $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ であり, さらに $d(B)$ の素因数 p で条件

- p は $P_0(k)$ に入らない.
- 「p は k で分解しない」または「p は k で分解し, さらに $p \equiv 1 \bmod 4$」.

を共に満たすものがあれば, $M^B(k) = \emptyset$.

定理 2.7, 3.1 より定理 2.5 が簡単に導かれることが分かったので, その証明を記す．証明の鍵となるのは, 志村曲線の局所体上の有理点の有無を判定する次の定理である．

定理 3.2 ([10, Theorems 2.5, 5.1, 5.4, 5.6])**.** L を $\mathbb{Q}_p$ の有限次拡大とし, e を分岐指数, f を剰余次数とする．
(1) p が $d(B)$ を割らない場合.
  (a) f が偶数なら, $M^B(L) \neq \emptyset$.
  (b) f が奇数なら, $M^B(L) = \emptyset$ は次の条件と同値.

  $|s| < 2p^{\frac{f}{2}}$ を満たす任意の $s \in \mathbb{Z}$ に対して, α が方程式 $x^2 + sx + p^f = 0$ の解ならば, 次のいずれかが成り立つ.

  (i) $B \otimes_{\mathbb{Q}} \mathbb{Q}(\alpha) \ncong \mathrm{M}_2(\mathbb{Q}(\alpha))$.
  (ii) $\frac{\alpha}{p}$ が代数的整数であり, さらに p が $\mathbb{Q}(\alpha)$ で分解する.

(2) p が $d(B)$ を割る場合.

(a) f が偶数なら, $M^B(L) \neq \emptyset$.

(b) f が奇数で e が偶数なら, $M^B(L) \neq \emptyset$ は次のいずれかの条件が成り立つことと同値.

(i) $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-p}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-p}))$.

(ii) $p = 2$ かつ $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1}))$.

(c) f も e も奇数なら, $M^B(L) \neq \emptyset$ は次のいずれかの条件が成り立つことと同値.

(i) $p \equiv 1 \bmod 4$ かつ $d(B) = 2p$.

(ii) $p = 2$ かつ $d(B) = 2q_1 \cdots q_{2r-1}$, ただし q_i $(1 \leq i \leq 2r-1)$ は $q_i \equiv 3 \bmod 4$ を満たす相異なる素数.

実際に証明に用いるのは, 定理 3.2 の特別な場合 (p が $d(B)$ を割り, さらに $L = \mathbb{Q}_p$ の場合) である.

系 3.3. p が $d(B)$ を割るとき, $M^B(\mathbb{Q}_p) \neq \emptyset$ は次のいずれかの条件が成り立つことと同値である.

(i) $p \equiv 1 \bmod 4$ かつ $d(B) = 2p$.

(ii) $p = 2$ かつ $d(B) = 2q_1 \cdots q_{2r-1}$, ただし q_i $(1 \leq i \leq 2r-1)$ は $q_i \equiv 3 \bmod 4$ を満たす相異なる素数.

定理 2.7, 3.1 $\Longrightarrow$ 定理 2.5 の証明. $P_J(k)$, $P_0(k)$ を, それぞれ定理 2.7, 3.1 にある素数の有限集合とし,

$$P(k) := P_J(k) \cup P_0(k) \cup \{2\}$$

とする. $d(B)$ の素因数 p で $P(k)$ に入らないものがあったとする. すると特に $p \neq 2$ である. このとき, $M^B(k) = \emptyset$ を示す.

(i) $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ とする. $p \notin P_J(k)$ なので, 定理 2.7 から $M^B(k) = \emptyset$ が従う.

(ii) $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ とする. さらに「p は k で分解しない」または「p は k で分解し, さらに $p \equiv 1 \bmod 4$」とする. $p \notin P_0(k)$ なので, 定理 3.1 から $M^B(k) = \emptyset$ が従う.

(iii) (i) でも (ii) でもないとする. このとき $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ であり, さらに「p は k で分解する」かつ「$p \not\equiv 1 \bmod 4$」となる. $p \neq 2$ かつ $p \not\equiv 1 \bmod 4$ に注意して, 系 3.3 より $M^B(\mathbb{Q}_p) = \emptyset$ が分かる. p は k で分解より, 体の埋め込み $k \hookrightarrow \mathbb{Q}_p$ がある. よって $M^B(k) \subseteq M^B(\mathbb{Q}_p)$ となる. $M^B(\mathbb{Q}_p) = \emptyset$ なので, $M^B(k) = \emptyset$ が従う. □

注 3.4. 筆者は, 定理 2.7, 3.1 の仮定でカバーされていない場合を, 次節で述べるようなガロア表現を用いた大域的な手法で調べようとしていた. しかしながら, 数年間うまくいかなかった. あきらめかけて別の問題に取り組んでいて, 局所的な結果である定理 3.2 を用いて計算をしていた. その過程で, 定理 3.2 が定理 2.7, 3.1 の未解決部分にぴたりとはまることに気付いた. この道筋を書き残すことが, 本稿の主要な目的である.

4　定理 3.1 の証明の概略

以前に Jordan は $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ の場合に問題を解決し, 今回筆者は $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ の場合に問題を解決したわけだが, $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ の場合の方が難しい理由は次の 2 つである.

(i) $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ なら, $d(B)$ の素因数で k で分解するものは無い. 一方で, $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ なら, そのような素因数が (必ず) あるので, 扱わなければならないケースが増える.

(ii) まず定理を述べる.

定理 4.1 ([9, Theorem 1.1])**.** F を標数 0 の体とし, $x \in M^B(F)$ とする. このとき, x が F 上の QM アーベル曲面 (A, i) と対応するための必要十分条件は, $B \otimes_{\mathbb{Q}} F \cong \mathrm{M}_2(F)$ である.

> 有理点 $x \in M^B(k)$ をとる. 定理 4.1 より, $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ なら x は k 上の QM アーベル曲面 (A, i) と対応するので, k 上の幾何が使える. 一方で $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ の場合には, x は k 上の QM アーベル曲面 (A, i) と対応しないので, k 上の幾何が使えない.

$B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ と仮定し, この場合の筆者によるアイデアを説明する. Jordan の $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ の場合の議論を改良したものである. まず, 有理点 $x \in M^B(k)$ があったとする. x は k 上の QM アーベル曲面とは対応しない. K を k の 2 次拡大のうち, $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$ を満たすものとする. このような K は常に (無限個) 存在する. すると定理 4.1 により, x は K 上の QM アーベル曲面 (A, i) と対応する. p を $d(B)$ の素因数とし, T_pA を A の p 進 Tate 加群とする. T_pA は階数 1 の自由 $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ 加群の構造をもつ. K の絶対ガロア群 G_K の T_pA への作用から p 進表現

$$R_p \colon \mathrm{G}_K \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T_pA) \cong (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{\times}$$

が得られる. ここに $\mathrm{Aut}_{\mathcal{O}}(T_pA)$ は, T_pA の $\mathbb{Z}_p$-線形自己同型のうち $\mathcal{O}$ の作用と可換なもの全体のなす群である. $\overline{R}_p := R_p \bmod p$ とする. 必要なら共役と取り替えることにより,

$$\overline{R}_p \colon \mathrm{G}_K \longrightarrow \left\{ \begin{pmatrix} a & * \\ 0 & a^p \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_{p^2}) \right\}$$

が得られる. $\overline{R}_p$ の $(1,1)$ 成分からガロア群の指標

$$\varrho_p \colon \mathrm{G}_K \longrightarrow \mathbb{F}_{p^2}^{\times}$$

が得られる. ϱ_p は **canonical isogeny character** と呼ばれる ([9, Definition 4.5] を参照). ここでは, p が $d(B)$ を割るので

$$\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{F}_p \cong \left\{ \begin{pmatrix} a & * \\ 0 & a^p \end{pmatrix} \in \mathrm{M}_2(\mathbb{F}_{p^2}) \right\}$$

となる ([20, Chapitre II, Corollaire 1.7] を参照). この環が指標を生じさせるような特別な構造をしていることが重要である. もし p が $d(B)$ を割らなければ, $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{M}_2(\mathbb{Z}_p)$, $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{F}_p \cong \mathrm{M}_2(\mathbb{F}_p)$ となり, 証明の鍵となる ϱ_p は得られない.

ところで, x は k 有理点なので, K ではなく k に関する情報が欲しい. そこで合成写像

$$\varphi : \mathrm{G}_k \xrightarrow{\mathrm{tr}_{K/k}} \mathrm{G}_K^{\mathrm{ab}} \xrightarrow{\varrho_p^{\mathrm{ab}}} \mathbb{F}_{p^2}^{\times}$$

をとる. ここに $\mathrm{tr}_{K/k}$ は移送 (transfer) であり, $\mathrm{G}_K^{\mathrm{ab}}$ は K の最大アーベル拡大の K 上のガロア群であり, ϱ_p^{ab} は ϱ_p から自然に導かれる写像である. そして

(i) φ^{12} を分類する (φ は K に依存するが, φ^4 や φ^{12} は p 乗を除けば K に依存しない).

(ii) φ^{12} の各分類に応じて, 必要なら K を都合の良い (つまり ϱ_p が計算しやすい) ものと取り替える.

(iii) ϱ_p を計算して, p が有限集合に入ることを示す.

もう少し詳細を説明する.

(a) p が k で惰性するとき.

$\mathfrak{p} = p\mathcal{O}_k$ とおく. 必要なら K を取り替えて, $\mathfrak{p}$ が K で惰性するようにする. $\mathfrak{P} = \mathfrak{p}\mathcal{O}_K$ $(= p\mathcal{O}_K)$ とおく. $K_{\mathfrak{P}}$ を K の $\mathfrak{P}$ での完備化とし, $\mathrm{G}_{K_{\mathfrak{P}}}$ を $K_{\mathfrak{P}}$ の絶対ガロア群とする. $I_{\mathfrak{P}} \subseteq \mathrm{G}_{K_{\mathfrak{P}}}$ を惰性群とし, 埋め込み $\mathrm{G}_{K_{\mathfrak{P}}} \subseteq \mathrm{G}_K$ を 1 つ固定しておく. $\overline{R}_p$ の $I_{\mathfrak{P}}$ への制限 $\overline{R}_p|_{I_{\mathfrak{P}}}$ は $\begin{pmatrix} \psi & * \\ 0 & \psi^p \end{pmatrix}$ という形と共役になる (ψ は ϱ_p の $I_{\mathfrak{P}}$ への制限).

(1) $\psi \neq \psi^p$ のときは, p が有限集合に入ることを示すのは難しくない.

(2) $\psi = \psi^p$ のときは, まず指標の分類から自動的に $p \equiv 1 \bmod 4$ となる. 2 次指標に付随するディリクレ L 関数の特殊値の評価という解析的な手法を用いて, p が有限集合に入ることを示す. この解析的な部分で, 「k が 2 次体」という仮定が必要になる. なお, p が入る有限集合の上界の評価は, 高々1 つの元を除いて可能である. また, 評価できない高々1 つの素数は, ジーゲルゼロ (Siegel zero) と関係している.

(b) p が k で分解するとき.

(a) の (2) と同様の議論ができるが, 「$p \equiv 1 \bmod 4$」を仮定する必要がある.

(c) p が k で分岐するとき.

そのような p は有限個しかない.

なお, 「$p \equiv 1 \bmod 4$」という条件の使い道は次のようなものである.

- そのような p は, 2 次体 $\mathbb{Q}(\sqrt{p})$ の判別式である.
- 2 でも p でもない素数 q に対して, $\left(\dfrac{q}{p}\right) = \left(\dfrac{p}{q}\right)$ となる. ただしこれらは平方剰余記号である.
- $\mathbb{F}_{p^2}^{\times}$ のある元 α が $\alpha^{12} = 1$ および $\alpha^{\frac{p+1}{2}} = 1$ を満たすとき, $p \equiv 1 \bmod 4$ であれば $\frac{p+1}{2}$ が奇数なので $\alpha^3 = 1$ となる.

謝辞

2018 年 8 月に大分県別府市の立命館アジア太平洋大学において第 12 回福岡数論研究集会が行われた. 本稿は, そこでの筆者の講演にもとづいて作成されたものである. 講演の機会を与えてくださった主催者の金子昌信氏 (九州大学), 権寧魯氏 (九州大学), 岸康弘氏 (愛知教育大学), 高妻倫太郎氏 (立命館アジア太平洋大学) に感謝したい.

本研究は科研費 (16K17578) の助成を受けたものである.

参考文献

[1] K. Arai, *Galois images and modular curves*, In: Algebraic number theory and related topics 2010, 145–161, RIMS Kôkyûroku Bessatsu, B32, Res. Inst. Math. Sci. (RIMS), Kyoto, 2012.

[2] K. Arai, *Points on Shimura curves rational over imaginary quadratic fields in the non-split case*, preprint, arXiv:1411.1162v1.

[3] K. Arai, *Points on Shimura curves rational over imaginary quadratic fields in the non-split case*, preprint, arXiv:1411.1162v2.

[4] K. Arai, *A survey of rational points on Shimura curves*, In: Algebraic number theory and related topics 2015, RIMS Kôkyûroku Bessatsu, to appear.

[5] K. Arai and F. Momose, *Algebraic points on Shimura curves of* $\Gamma_0(p)$*-type*, J. Reine Angew. Math. **690** (2014), 179–202.

[6] Y. Bilu and P. Parent, *Serre's uniformity problem in the split Cartan case*, Ann. of Math. (2) **173** (2011), no. 1, 569–584.

[7] Y. Bilu, P. Parent and M. Rebolledo, *Rational points on* $X_0^+(p^r)$, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984.

[8] P. Clark and X. Xarles, *Local bounds for torsion points on abelian varieties*, Canad. J. Math. **60** (2008), no. 3, 532–555.

[9] B. Jordan, *Points on Shimura curves rational over number fields*, J. Reine Angew. Math. **371** (1986), 92–114.

[10] B. Jordan and R. Livné, *Local Diophantine properties of Shimura curves*, Math. Ann. **270** (1985), no. 2, 235–248.

[11] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.

[12] A. Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25** (1979), no. 3, 277–300.

[13] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[14] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1–3, 437–449.

[15] F. Momose, *Rational points on the modular curves* $X_{\mathrm{split}}(p)$, Compositio Math. **52** (1984), no. 1, 115–137.

[16] F. Momose, *Isogenies of prime degree over number fields*, Compositio Math. **97** (1995), no. 3, 329–348.

[17] 斎藤毅, フェルマー予想, 岩波書店, 東京, 2009.

[18] 清水英男, 保型関数 I–III, 第 2 版. 岩波書店基礎数学, 8. 代数, vii. 岩波書店, 東京, 1984.

[19] G. Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 135–164.

[20] M.-F. Vignéras, Arithmétique des algèbres de quaternions, Lecture Notes in Mathematics, 800, Springer, Berlin, 1980.