ディオファントス問題と志村曲線の有理点

新井 啓介 (東京電機大学)

概 要

志村曲線の有理点の非存在に関して筆者が得た結果を, ディオファントス問題と関連づけて紹介する.

1 序文 (ディオファントス問題)

k を代数体とし, k の素点全体の集合を Ω_k で表す. $v \in \Omega_k$ に対し, k の v での完備化を k_v で表す. まず, 方程式

$$x^2 + y^2 + 3 = 0 \tag{1.1}$$

の解を考えよう.

(1.1) が k に解をもつ
$\iff$ $X^2 + Y^2 + 3Z^2 = 0$ が k に非自明な解 (つまり $(X, Y, Z) = (0, 0, 0)$ 以外の解) をもつ
$\iff$ 任意の $v \in \Omega_k$ に対して, $X^2 + Y^2 + 3Z^2 = 0$ が k_v に非自明な解をもつ
$\iff$ 任意の $v \in \Omega_k$ に対して, (1.1) が k_v に解をもつ
$\iff$ 任意の無限素点 $v \in \Omega_k$ および 3 を割る任意の $v \in \Omega_k$ に対して, (1.1) が k_v に解をもつ
$\iff$ k が実素点をもたず, 3 を割る任意の $v \in \Omega_k$ に対して拡大次数 $[k_v : \mathbb{Q}_3]$ が偶数である.

最初と 3 番目の同値は, 後の補題 5.1 による. 2 番目の同値は, 2 次形式に対する Hasse 原理 ([6, Theorem 5.3.3] を参照) による. 4 番目の同値は, 次の補題による.

補題 1.1. (1.1) は $\mathbb{R}$, $\mathbb{Q}_3$ に解をもたず, 3 以外の全ての素数 p に対し, $\mathbb{Q}_p$ に解をもつ.

証明. (1) $x, y \in \mathbb{R}$ なら, $x^2 + y^2 + 3 > 0$ である. よって (1.1) は $\mathbb{R}$ に解をもたない.

(2) $x, y \in \mathbb{Q}_3$, $x^2 + y^2 + 3 = 0$ として矛盾を導く. 付値 $v_3 : \mathbb{Q}_3^\times \longrightarrow \mathbb{Z}$ を $v_3(3) = 1$ となるようにとる. まず $x = 0$ とすると, $y^2 = -3$ から ($y \neq 0$ かつ) $1 = v_3(-3) = v_3(y^2) = 2v_3(y)$ となり, $v_3(y) \in \mathbb{Z}$ に反する. よって $x \neq 0$ である. 同様に $y \neq 0$ である. これより, $x = 3^a s$, $y = 3^b t$ $(a, b \in \mathbb{Z},\ s, t \in \mathbb{Z}_3^\times)$ と表される. このとき

$$3^{2a}s^2 + 3^{2b}t^2 + 3 = 0$$

である. $a \geq b$ と仮定してよい. まず $b \leq 0$ を示す. $b > 0$ とすると $-3 = 3^{2b}(3^{2(a-b)}s^2 + t^2)$ から $1 = v_3(-3) = v_3(3^{2b}(3^{2(a-b)}s^2 + t^2)) \geq 2b \geq 2$ となり, 矛盾. よって $b \leq 0$ である. 次に $a \leq 0$ を示す. $a > 0$ とすると $3^{2a}s^2 + 3 = -3^{2b}t^2$ から $1 = v_3(3^{2a}s^2 + 3) = v_3(-3^{2b}t^2) = 2b \leq 0$ となり, 矛盾. よって $a \leq 0$ である. $c = -a$, $d = -b$ とすると $c, d \geq 0$ かつ $c \leq d$ となる. また $3^{-2c}s^2 + 3^{-2d}t^2 + 3 = 0$ である. 3^{2d} を掛けて

$$3^{2(d-c)}s^2 + t^2 + 3^{2d+1} = 0$$

となる. これより $3^{2(d-c)}s^2+t^2=-3^{2d+1}$ である. $d>c$ とすると $0=v_3(3^{2(d-c)}s^2+t^2)=v_3(-3^{2d+1})=2d+1\geq 1$ となり, 矛盾. よって $c=d$ となる. このとき $s^2+t^2+3^{2d+1}=0$ である. mod 3 して $\mathbb{F}_3$ で考えると, $\overline{s}^2+\overline{t}^2=0$ となる. ここで $\overline{s},\overline{t}\in\mathbb{F}_3^\times=\{\pm 1\}$ より, $\overline{s}^2=\overline{t}^2=1$ である. よって $\mathbb{F}_3$ で $2=0$ となり, 矛盾. ゆえに (1.1) は $\mathbb{Q}_3$ に解をもたない.

(3) (1.1) が $\mathbb{Q}_p$ (ただし $p\neq 2,3$) に解をもつことを示す. [15, 定理 2.15] より, $\sigma^2+\tau^2+3=0$ となるような $\sigma,\tau\in\mathbb{F}_p$ がある. $p\neq 3$ より $(\sigma,\tau)\neq(0,0)$ である. $\sigma\neq 0$ としてよい. $s,t\in\mathbb{Z}_p$ を, $\overline{s}=\sigma$, $\overline{t}=\tau$ となるようにとる. $F(X)=X^2+t^2+3\in\mathbb{Z}_p[X]$ とすると, $F'(X)=2X$ である. また $F(s)=s^2+t^2+3\equiv\sigma^2+\tau^2+3=0 \bmod p$ である. $p\neq 2$ より $F'(s)=2s\equiv 2\sigma\neq 0 \bmod p$ である. Hensel の補題 ([8, Theorem 3.4.1]) より, $u\in\mathbb{Z}_p$ で $u\equiv s \bmod p$, $F(u)=0$ となるようなものがある. このとき $u^2+t^2+3=0$ かつ $t,u\in\mathbb{Z}_p\subseteq\mathbb{Q}_p$ より, (1.1) は $\mathbb{Q}_p$ に解をもつ.

(4) (1.1) は $\mathbb{Q}_2$ に解をもつことを示す. $2^2+(\sqrt{-7})^2+3=0$ なので, $\sqrt{-7}\in\mathbb{Q}_2$ を示せばよい. 2 は $\mathbb{Q}(\sqrt{-7})$ で分解するので, 2 を割る $\mathbb{Q}(\sqrt{-7})$ の付値の 1 つを v とすれば, $\mathbb{Q}(\sqrt{-7})_v=\mathbb{Q}_2$ となる. よって $\mathbb{Q}(\sqrt{-7})\subseteq\mathbb{Q}(\sqrt{-7})_v=\mathbb{Q}_2$ であり, $\sqrt{-7}\in\mathbb{Q}_2$ となる. □

標数が 2 でない体 F と $a,b\in F^\times$ に対し,

$$\left(\frac{a,b}{F}\right)=F+Fe+Ff+Fef$$

を $e^2=a$, $f^2=b$, $ef=-fe$ により定まる 4 元数環とする. この記号の下で, 5 番目の同値を示そう.

($\Longrightarrow$) 無限素点 $v\in\Omega_k$ に対して (1.1) が k_v に解をもつとき, $k_v\neq\mathbb{R}$ であり, v は実素点ではない. $v\in\Omega_k$, $v\mid 3$ とする. (1.1) が k_v に解をもつとき, 補題 5.1 より $\left(\frac{-1,-3}{k_v}\right)\cong \mathrm{M}_2(k_v)$ である. ここで $\left(\frac{-1,-3}{k_v}\right)\cong\left(\frac{-1,-3}{\mathbb{Q}_3}\right)\otimes_{\mathbb{Q}_3}k_v$ であり, $\left(\frac{-1,-3}{\mathbb{Q}_3}\right)$ は補題 1.1, 5.1 より $\mathrm{M}_2(\mathbb{Q}_3)$ と同型ではない. つまり $\left(\frac{-1,-3}{\mathbb{Q}_3}\right)$ は, $\mathbb{Q}_3$ 上の唯一の 4 元数体である. よって [20, Ch.II, Théorème 1.3] より, $[k_v:\mathbb{Q}_3]$ は偶数である.

($\Longleftarrow$) k が実素点をもたないとき, 任意の無限素点 $v\in\Omega_k$ に対して $k_v=\mathbb{C}$ であり, (1.1) は k_v に解 $(x,y)=(\sqrt{-3},0)$ をもつ. $v\in\Omega_k$, $v\mid 3$ に対して $[k_v:\mathbb{Q}_3]$ は偶数とする. すると [20, Ch.II, Théorème 1.3] より $\left(\frac{-1,-3}{k_v}\right)\cong\left(\frac{-1,-3}{\mathbb{Q}_3}\right)\otimes_{\mathbb{Q}_3}k_v\cong\mathrm{M}_2(k_v)$ であり, 補題 5.1 により (1.1) は k_v に解をもつ.

上の考察から, (1.1) の k における解の有無に関して, 表 1 のような例が挙げられる.

表 1: (1.1) の k における解の有無

解なし	解あり
• $[k:\mathbb{Q}]$ が奇数 • $k=\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{-2}),\mathbb{Q}(\sqrt{-5}),\mathbb{Q}(\sqrt{-2},\sqrt{-5})$	• $k=\mathbb{Q}(\sqrt{-1}),\mathbb{Q}(\sqrt{-3})$

$[k:\mathbb{Q}]$ が奇数のときや $k=\mathbb{Q}(\sqrt{2})$ のときは, k は実素点をもつ. 3 は $\mathbb{Q}(\sqrt{-2}),\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-2},\sqrt{-5})$ で完全分解し, $\mathbb{Q}(\sqrt{-1})$ で惰性し, $\mathbb{Q}(\sqrt{-3})$ で分岐する.

次に, 方程式

$$y^2=-(x^4+x^3-x^2-x+1)(7x^4+23x^3+5x^2-23x+7) \tag{1.2}$$

を考えよう.

補題 1.2. (1.2) は $\mathbb{R}$ に解をもたない.

証明. $x \in \mathbb{R}$ とする. $x \neq 0$ なら $x^4+x^3-x^2-x+1 = x^2((x-\frac{1}{x})^2+(x-\frac{1}{x})+1) = x^2((x-\frac{1}{x}+\frac{1}{2})^2+\frac{3}{4}) > 0$ であり, $x=0$ なら $x^4+x^3-x^2-x+1=1>0$ である. また, $x \neq 0$ なら $7x^4+23x^3+5x^2-23x+7 = x^2(7(x-\frac{1}{x})^2+23(x-\frac{1}{x})+19) = x^2(7(x-\frac{1}{x}+\frac{23}{14})^2+\frac{3}{28}) > 0$ であり, $x=0$ なら $7x^4+23x^3+5x^2-23x+7=7>0$ である. よって任意の $x \in \mathbb{R}$ に対して $-(x^4+x^3-x^2-x+1)(7x^4+23x^3+5x^2-23x+7) < 0$ となり, (1.2) は $\mathbb{R}$ に解をもたない. □

さて, (1.2) の代数体 k における解を考えよう. k が実素点をもつときは, 上の補題により解なしが分かるので, 実素点をもたない場合が非自明である. 今回得られた結果より, 例えば次のことが分かる.

命題 1.3. (1.2) は $k = \mathbb{Q}(\sqrt{2}, \sqrt{-13})$ に解をもたない.

注 1.4. $k = \mathbb{Q}(\sqrt{2}, \sqrt{-13})$ とする. このとき, 任意の $v \in \Omega_k$ に対し, (1.2) は k_v に解をもつ. よって, 方程式 (1.2) は k 上の Hasse 原理の反例を与える.

2 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 $\mathbb{Q}$ 上の粗モジュライのコンパクト化を $X_0(p)$ とする. すると $X_0(p)$ は $\mathbb{Q}$ 上の固有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 ([16, 定理 2.10] を参照). $X_0(p)$ の有理点に関して, 次の定理が知られている.

定理 2.1 ([11, Theorem 7.1])**.** $p > 163$ ならば, $X_0(p)$ の $\mathbb{Q}$ 有理点の集合 $X_0(p)(\mathbb{Q})$ はカスプのみから成る.

ここに, **カスプ**とはコンパクト化の際に加わる点であり, 楕円曲線とは対応しない点である. $X_0(p)(\mathbb{Q})$ のカスプはちょうど 2 個ある. $X_0(p)(\mathbb{C})$ のカスプもちょうど 2 個ある ([17, 定理 3.2] を参照).

例 2.2 ([5, p.2274], [12, §5])**.** $X_0(37)$ は, 方程式

$$y^2 = -x^6 - 9x^4 - 11x^2 + 37 \tag{2.1}$$

により定義される. さらに,

$$X_0(37)(\mathbb{Q}) = \{(2.1) \text{ の } \mathbb{Q} \text{ における解 }\} = \{(\pm 1, 4), (\pm 1, -4)\}$$

が成り立つ. ここに, 2 点 $(\pm 1, 4)$ はカスプであり, 2 点 $(\pm 1, -4)$ はカスプではない. $(\pm 1, -4)$ は CM 点でもない. **CM 点**とは虚数乗法をもつ楕円曲線と対応する点のことである.

ここで, $X_0(37)(\mathbb{Q}) = \{(2.1) \text{ の } \mathbb{Q} \text{ における解 }\}$ の等号は必ずしも自明なものではない. 正確に言うと, $X_0(37)$ は方程式 (2.1) で定義されるアファイン代数曲線と

$$Y^2 = -1 - 9X^2 - 11X^4 + 37X^6$$

で定義されるアファイン代数曲線を, 関係式 $X = 1/x$, $Y = y/x^3$ により貼り合わせたものである (例えば [19, Exercise 2.14] を参照). よって, $X_0(37)$ の有理点を考える際には, (2.1) の解に加えて $X = 0$ と対応する「無限遠点」も考慮する必要があり, 標数 0 の体 F に対して

$$X_0(37)(F) = \{(2.1) \text{ の } F \text{ における解 }\} \sqcup \{X = 0,\, Y^2 = -1 \text{ の } F \text{ における解 }\}$$

となる. 方程式 $X = 0$, $Y^2 = -1$ は $\mathbb{Q}$ に解をもたないので,

$$X_0(37)(\mathbb{Q}) = \{(2.1) \text{ の } \mathbb{Q} \text{ における解 }\}$$

となる.

注 2.3. 定理 2.1 は, 2 次体上の有理点に関する結果へと拡張された ([13, Theorem B]).

ここで, 次の基本的な問題を考えよう.

問題 2.4. X をある種のアーベル多様体のモジュライとする (例えば $X = X_0(p)$). X のレベル ($X = X_0(p)$ のときはレベルは p) が上がるとき, 有理点の集合 $X(k)$ は小さくなるか?

具体的な未解決問題を 1 つ挙げよう.

例 2.5 ([1, Question 2.1])**.** k に依存した定数 $C(k)$ があって, $p > C(k)$ なら

$$X_0(p)(k) \subseteq \{ \text{カスプ, CM 点} \}$$

となるか?

3 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 $B \ncong \mathrm{M}_2(\mathbb{Q})$) 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 $d(B)$ とする. $d(B)$ は B の**判別式**と呼ばれ, 相異なる偶数個の素数の積に等しく, $d(B) > 1$ 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, 任意の極大整環は $a^{-1}\mathcal{O}a$(ただし $a \in B$) の形で表すことができる. $\mathbb{Q}$ 上の 4 元数環については, 例えば [17, §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 の自己準同型環を表す. $\mathcal{O}$ 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. M^B は $\mathbb{Q}$ 上の固有スムーズ代数曲線になり, **志村曲線**と呼ばれている. 本来は M^B でなくて $M^{\mathcal{O}}$ と書くべきかもしれないが, M^B の $\mathbb{Q}$ 上の同型類は B のみ (実は $d(B)$ のみ) に依存し, $\mathcal{O}$ のとり方にはよらないので, この表記は許されるであろう. M^B はコンパクト化をせずとも, はじめから固有である. また, $X_0(p)$ と異なり, 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, 次の定理は基本的である.

定理 3.1 ([18, Theorem 0])**.** $M^B(\mathbb{R}) = \emptyset$.

この定理より, 代数体 k が実素点をもてば, $M^B(k) = \emptyset$ となることが分かる. 特に, k の次数が奇数なら k は実素点をもつので, $M^B(k) = \emptyset$ となる. M^B の具体例を挙げよう.

例 3.2. $d(B)=6$ なら, M^B は方程式 (1.1): $x^2+y^2+3=0$ で定義される ([10, Theorem 1-1] を参照). この方程式は実数解をもたない.

正確に言うと, $d(B)=6$ 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, この方程式は非自明な実数解をもたない.

主結果 (定理 3.3, 3.6) を定式化するために, 4 元数環のあるクラスを定めよう. 素数 q に対し,

$$\begin{cases} B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-q})\ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q})) & (q\neq 2 \text{ のとき}),\\ B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-1})\ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-1})) \text{ かつ } B\otimes_{\mathbb{Q}}\mathbb{Q}(\sqrt{-2})\ncong \mathrm{M}_2(\mathbb{Q}(\sqrt{-2})) & (q=2 \text{ のとき}) \end{cases}$$

を満たすような $\mathbb{Q}$ 上の不定符号 4 元数体 B の同型類の集合を $\mathcal{B}(q)$ で表す. $\mathcal{O}_k$ を k の整数環とする. 素数 q を割る $\mathcal{O}_k$ の極大イデアル $\mathfrak{q}$ に対し, $\mathfrak{q}$ の $k/\mathbb{Q}$ での分岐指数を $e_{\mathfrak{q}}$, 剰余次数を $f_{\mathfrak{q}}$ とし, また $\mathrm{N}_{\mathfrak{q}}:=q^{f_{\mathfrak{q}}}$ とおく. このとき, 剰余体 $\mathcal{O}_k/\mathfrak{q}$ の元の個数は $\mathrm{N}_{\mathfrak{q}}$ である.

定理 3.3 ([2, Theorem 1.1])**.** 以下を仮定する.

- $[k:\mathbb{Q}]$ は偶数.
- $\mathfrak{q}$ は $\mathcal{O}_k$ の極大イデアルであり, 剰余標数は q である.
- q を割る $\mathcal{O}_k$ の極大イデアルは $\mathfrak{q}$ のみである.
- $f_{\mathfrak{q}}$ は奇数.
- $B\in\mathcal{B}(q)$.

このとき, k と $\mathfrak{q}$ に依存した素数の有限集合 $P_1(k,\mathfrak{q})$ が存在して, 次の条件を満たす. $d(B)$ の素因数 p で $P_1(k,\mathfrak{q})$ に入らないものがあれば, $M^B(k)=\emptyset$ となる.

注 3.4. (1) $d(B)$ は平方因子を含まない. よって, 「$d(B)$ の素因数 p で有限集合 $P_1(k,\mathfrak{q})$ に入らないものがある」ことは, 大雑把に言えば「$d(B)$ が十分大きい」ことと同値である. つまり, 定理 3.3 は次のように解釈できる: ある仮定の下, $d(B)$ が十分大なら, $M^B(k)=\emptyset$ となる. 従って, この定理は問題 2.4 の部分的な解答を与えている.

(2) k が 2 次体の場合には, 定理 3.3 は $B\otimes_{\mathbb{Q}}k\cong \mathrm{M}_2(k)$ の場合に Jordan により ([9, Theorem 6.3] を参照), $B\otimes_{\mathbb{Q}}k\ncong \mathrm{M}_2(k)$ も含めた場合に (ごく緩い仮定の下) Rotger, de Vera-Piquero により示されている ([14, Theorem 1.1] を参照).

例外集合 $P_1(k,\mathfrak{q})$ は, 以下のように明示的に定めることができる. 正の整数 N,e に対して,

$$\mathcal{C}(N,e):=\left\{\beta^e+\overline{\beta}^e\in\mathbb{Z}\;\middle|\;\begin{array}{l}\beta,\overline{\beta}\in\mathbb{C}\text{ は }T^2+sT+N=0\ (s\in\mathbb{Z},\\ s^2\leq 4N)\text{ の形の方程式の解}\end{array}\right\},$$
$$\mathcal{D}(N,e):=\{a,a\pm N^{\frac{e}{2}},a\pm 2N^{\frac{e}{2}},a^2-3N^e\in\mathbb{R}\,|\,a\in\mathcal{C}(N,e)\}$$

とおく. e が偶数なら, $\mathcal{D}(N,e)$ は $\mathbb{Z}$ に含まれる. $\mathbb{Z}$ の部分集合 $\mathcal{D}$ に対し, $\mathcal{D}$ の 0 でない元の素因数全体の集合を $\mathcal{P}(\mathcal{D})$ で表す.

$$\widetilde{P}_1(k,\mathfrak{q}):=\begin{cases}\mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}},e_{\mathfrak{q}})) & (B\otimes_{\mathbb{Q}}k\cong\mathrm{M}_2(k)\text{ かつ }e_{\mathfrak{q}}\text{ が偶数のとき}),\\ \mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}},2e_{\mathfrak{q}})) & (B\otimes_{\mathbb{Q}}k\ncong\mathrm{M}_2(k)\text{ のとき})\end{cases}$$

とおく. すると, 定理 3.3 では $P_1(k,\mathfrak{q})=\widetilde{P}_1(k,\mathfrak{q})$ ととれる.

例 3.5. (1) $d(B)=39$, $k=\mathbb{Q}(\sqrt{2},\sqrt{-13})$ のとき, $(p,q)=(13,2)$ とおくことで, 定理 3.3 から $M^B(k)=\emptyset$ が得られる. このとき, $P_1(k,\mathfrak{q})=\mathcal{P}(\mathcal{D}(2,4))=\{2,3,5,7,47\}$ である ([2, Table 1] を参照). 実は $d(B)=39$ のとき, M^B は方程式 (1.2) により定義される ([7, Theorem 4.5] を参照). このことより, 命題 1.3 が従う.

$d(B)=39$ とする. より詳しくは, M^B の有理点と方程式 (1.2) の解には, 次のような関係がある. 正確に言うと, M^B は方程式 (1.2) で定義されるアファイン代数曲線と

$$Y^2=-(1+X-X^2-X^3+X^4)(7+23X+5X^2-23X^3+7X^4)$$

で定義されるアファイン代数曲線を, 関係式 $X=1/x$, $Y=y/x^4$ により貼り合わせたものである. よって, 標数 0 の体 F に対して

$$M^B(F)=\{(1.2)\text{ の }F\text{ における解}\}\sqcup\{X=0,\,Y^2=-7\text{ の }F\text{ における解}\}$$

となる. このとき,

$$\begin{cases}\sqrt{-7}\notin F\text{ なら }M^B(F)=\{(1.2)\text{ の }F\text{ における解}\},\\ \sqrt{-7}\in F\text{ なら }M^B(F)=\{(1.2)\text{ の }F\text{ における解}\}\sqcup\{(X,Y)=(0,\sqrt{-7}),(0,-\sqrt{-7})\}\end{cases}$$

である. さらに, 次の同値が言える.

$$M^B(F)=\emptyset\iff\{(1.2)\text{ の }F\text{ における解}\}=\emptyset. \tag{3.1}$$

これを示そう.
($\Longrightarrow$) $\{(1.2)\text{ の }F\text{ における解}\}$ が $M^B(F)$ の部分集合であることから従う.
($\Longleftarrow$) $\{(1.2)\text{ の }F\text{ における解}\}=\emptyset$ とする. まず $\sqrt{-7}\notin F$ を示す. $\sqrt{-7}\in F$ を仮定すると, $(x,y)=(0,\sqrt{-7})$ が (1.2) の F における解となり, $\{(1.2)\text{ の }F\text{ における解}\}=\emptyset$ に反する. よって $\sqrt{-7}\notin F$ である. このとき, $M^B(F)=\{(1.2)\text{ の }F\text{ における解}\}=\emptyset$ である.

(2) 注 1.4 で述べたことは, 次のようにして分かる. まず $d(B)=39$ とすると, [9, Example 6.4] より, 任意の $v\in\Omega_{\mathbb{Q}(\sqrt{-13})}$ に対して $M^B(\mathbb{Q}(\sqrt{-13})_v)\neq\emptyset$ となる. よって, $k=\mathbb{Q}(\sqrt{2},\sqrt{-13})$ とすれば, 任意の $v\in\Omega_k$ に対して $M^B(k_v)\neq\emptyset$ となる. (3.1) より, 任意の $v\in\Omega_k$ に対して (1.2) が k_v に解をもつことが分かる.

定理 3.3 において, 「q を割る $\mathcal{O}_k$ の極大イデアルは $\mathfrak{q}$ のみである」という仮定は強いように思われる. そこで, この仮定を外そうと試み, 次の定理 3.6 を得た. k のイデアル類群 Cl_k の各元の位数のうち最大のものを h_k' とする. つまり, $Cl_k\cong\mathbb{Z}/m_1\mathbb{Z}\times\cdots\times\mathbb{Z}/m_r\mathbb{Z}$ (ただし $m_1,\dots,m_r$ は正の整数, $m_r\mid\cdots\mid m_2\mid m_1$) ならば $h_k'=m_1$ である. また,

$$\widetilde{P}_2(k,\mathfrak{q}):=\mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}},2h_k'))$$

とおく.

定理 3.6 ([4])**.** 以下を仮定する.

- $[k:\mathbb{Q}]$ は偶数.
- $\mathfrak{q}$ は $\mathcal{O}_k$ の極大イデアルであり, 剰余標数は q である.
- $f_{\mathfrak{q}}$ は奇数.

- $B \in \mathcal{B}(q)$.

このとき, $d(B)$ の素因数 p で

(i) p は $\widetilde{P}_2(k, \mathfrak{q})$ に入らず,

(ii) p を割る $\mathcal{O}_k$ の任意の極大イデアル $\mathfrak{p}$ に対して, $f_{\mathfrak{p}}$ は奇数

となるようなものがあるとすると, $M^B(k) = \emptyset$ となる.

$\mathfrak{q}$ の一意性の仮定が無くなった代わりに, p についての仮定が加わった.

例 3.7. $d(B) = 122$, $k = \mathbb{Q}(\sqrt{-39}, \sqrt{-183})$ のとき, $(p, q) = (61, 3)$ とおくことで, 定理 3.6 から $M^B(k) = \emptyset$ が得られる. このとき, $Cl_k \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $h'_k = 8$ であり, $\mathcal{P}(\mathcal{D}(\mathrm{N}_{\mathfrak{q}}, 2h'_k)) = \mathcal{P}(\mathcal{D}(3, 16)) = \{2, 3, 5, 7, 11, 17, 23, 31, 47, 97, 113, 191, 193, 353, 383, 2113, 3457, 30529, 36671\}$ である. さらに [14, Table 1] より, 任意の $v \in \Omega_k$ に対して $M^B(k_v) \neq \emptyset$ となることが分かる. $d(B) = 122$ のときの M^B の定義方程式は, 知られていないようである.

注 3.8. 定理 3.3 から例 3.5 は得られるが, 例 3.7 は得られない. また, 定理 3.6 から例 3.7 は得られるが, 例 3.5 は得られない. 詳細は [3, §3] を参照.

4 証明の概略

志村曲線の有理点について, その field of definition と field of moduli が一致するとは限らない. これらの体が一致する条件は, 次の定理で与えられる.

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.

この定理より, $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ の場合には有理点 $x \in M^B(k)$ は k 上の QM アーベル曲面 (A, i) と対応しない. 従って, k 上の幾何が使えない. このことが障害となり, $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ の場合は有理点の研究がなかなか進まなかった ([9, p.93 最後の 2 行]). ここでは, その障害を克服するためのアイデアを紹介する. そのアイデアは, 実はごく単純なものである.

まずは, $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$ の場合の Jordan の手法を振り返ってみよう ([9, §4] を参照). 有理点 $x \in M^B(k)$ があったとすると, 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. $\overline{R}_p := R_p \bmod p$ とすると, 必要なら共役で取り替えることにより, 法 p 表現

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

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 $d(B)$ を割り, そのために $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{F}_p \cong \{\begin{pmatrix} a & * \\ 0 & a^p \end{pmatrix} \in \mathrm{M}_2(\mathbb{F}_{p^2})\}$ が指標を生じさせるような特別な環構造をしていることがポイントである．仮に p が $d(B)$ を割らなければ, $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{M}_2(\mathbb{Z}_p)$, $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{F}_p \cong \mathrm{M}_2(\mathbb{F}_p)$ であり, 証明の鍵となる ϱ_p は生じない．定理 3.3, 3.6 では, ϱ_p の分類を用いて p が有限な例外集合に入ることを示す．

次に, $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ の場合の筆者によるアイデアを説明する．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 次拡大とし, $B \otimes_{\mathbb{Q}} K \cong \mathrm{M}_2(K)$ を満たすものとする．このような K は常に (無限に) 存在する．すると x は K 上の QM アーベル曲面 (A, i) と対応する．p を $d(B)$ の素因数とすると, 先と同様に p 進表現

$$R_{p,K} \colon \mathrm{G}_K \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T_p A) \cong (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$$

および指標

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

が得られる．定理 3.3, 3.6 では, K をうまくとってやると, $\varrho_{p,K}$ の分類を用いて p が有限な例外集合に入ることが示せる．

Rotger, de Vera-Piquero は, $B \otimes_{\mathbb{Q}} k \ncong \mathrm{M}_2(k)$ の場合に別の手法を用いた．表現 $R_p \colon \mathrm{G}_k \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T_p A) \cong (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$ は無いが, 代わりに射影表現 $\mathrm{G}_k \longrightarrow (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times / \{\pm 1\}$ を定義し ([14, §2.1–2.3] を参照), 調べることで結果を導いている．

注 4.2. ここで, 命題 1.3 がどうやって示されたかを整理してみよう．方程式 (1.2) のモジュライ解釈を見つけ, そのモジュライの有理点から定まる幾何的対象のガロア表現を調べることにより, 有理点の非存在が分かり, 従って解の非存在が分かる, という流れである．このような視点を紹介することが, 筆者の今回の講演および本稿の狙いである．

5 補足

補題 5.1. F を標数が 2 でない体とし, $a, b \in F^\times$ とする．2 つの方程式

$$x^2 - ay^2 - b = 0, \tag{5.1}$$

$$X^2 - aY^2 - bZ^2 = 0 \tag{5.2}$$

を考える．このとき, 次は同値である．

(i) (5.1) は F に解をもつ．

(ii) (5.2) は F に非自明な解をもつ．

(iii) $\left(\frac{a,b}{F}\right) \cong \mathrm{M}_2(F)$.

証明. (i) $\Longrightarrow$ (ii) : (x, y) を (5.1) の F における解とすると, $(X, Y, Z) = (x, y, 1)$ は (5.2) の F における非自明な解である．

(ii) $\Longrightarrow$ (i) : (X, Y, Z) を (5.2) の F における非自明な解とする．

(1) $Z \neq 0$ なら, $(x, y) = (X/Z, Y/Z)$ は (5.1) の F における解である．

(2) $Z = 0$ とする．すると $X^2 - aY^2 = 0$ かつ $(X, Y) \neq (0, 0)$ となる．$Y = 0$ なら $X = 0$ となり矛盾なので, $Y \neq 0$ である．すると $a = (X/Y)^2$ となる．簡単のために $u = X/Y$ とおく

と, $a = u^2$ である. $a \neq 0$ より $u \neq 0$ となる. このとき (5.1) は $x^2 - u^2y^2 = b$ と同値であり, $(x + uy)(x - uy) = b$ とも同値である. ここで

$$\begin{cases} x + uy = b \\ x - uy = 1 \end{cases}$$

とすると, $2x = b+1$, $2uy = b-1$ から $(x, y) = (\frac{b+1}{2}, \frac{b-1}{2u})$ となり, これが (5.1) の解を与える. (ii) $\Longleftrightarrow$ (iii) : [15, 定理 2.10] を参照. □

謝辞

2016 年 8 月に九州大学・伊都キャンパスにおいて第 10 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) に感謝したい. なお, 筆者の講演は, 2016 年 5 月〜6 月に函館アリーナで行われた Hakodate workshop on arithmetic geometry 2016 において, Yifan Yang 氏 (National Chiao Tung University, 台湾) と筆者との志村曲線の定義方程式に関する議論に触発されてなされた. 氏にも感謝したい.

本研究は科研費 (16K17578) および東京電機大学総合研究所研究費 (Q16K-06) 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, *Non-existence of points rational over number fields on Shimura curves*, Acta Arith. **172** (2016), no. 3, 243–250.

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

[4] K. Arai, *Rational points on Shimura curves and the Manin obstruction*, to appear in Nagoya Math. J.

[5] K. Arai and F. Momose, *Rational points on* $X_0^+(37M)$, J. Number Theory **130** (2010), no. 10, 2272–2282.

[6] H. Cohen, Number theory. Vol. I. Tools and Diophantine equations, Graduate Texts in Mathematics, 239, Springer, New York, 2007.

[7] J. González and S. Molina, *The kernel of Ribet's isogeny for genus three Shimura curves*, J. Math. Soc. Japan **68** (2016), no. 2, 609–635.

[8] F. Gouvêa, p-adic Numbers. An introduction. Second edition, Universitext, Springer-Verlag, Berlin, 1997.

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

[10] 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.

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

[12] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

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

[14] V. Rotger and C. de Vera-Piquero, *Galois representations over fields of moduli and rational points on Shimura curves*, Canad. J. Math. **66** (2014), no. 5, 1167–1200.

[15] 斎藤秀司, 整数論, 共立出版, 東京, 1997.

[16] 斎藤毅, フェルマー予想, 岩波書店, 東京, 2009.

[17] 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.

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

[19] J. Silverman, The arithmetic of elliptic curves. Second edition, Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.

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