数理解析研究所講究録
1160 巻 2000 年 169-176

DETERMINATION OF ALL Q-RATIONAL CM-POINTS IN THE MODULI SPACE OF PRINCIPALLY POLARIZED ABELIAN SURFACES

村林 直樹 (Naoki Murabayashi)
梅垣 敦紀 (Atsuki Umegaki)†

1. 導入

$E/\mathbf{C}$ を楕円曲線とする. その自己準同型環 $\mathrm{End}(E)$ に対して, $\mathrm{End}(E)\otimes_{\mathbf{Z}}\mathbf{Q}$ は有理数体 $\mathbf{Q}$ または虚 2 次体 K に同型であることが知られている. 後者の場合 E は**虚数乗法 (CM)** をもつという. 以下に於いては, 特に, E が虚 2 次体 K の整数環 $\mathcal{O}_K$ に CM をもつこと, 即ち,

$$\mathrm{End}(E)\cong\mathcal{O}_K \quad (\exists K:\text{虚 2 次体})$$

を仮定する. $\mathbf{C}$ 上の楕円曲線は, 上半平面

$$\mathfrak{H}_1:=\{\tau\in\mathbf{C}\mid \mathrm{Im}(\tau)>0\}$$

の点 τ を用いて, 複素トーラス $\mathbf{C}/(\mathbf{Z}+\mathbf{Z}\tau)$ と同一視できる. よって, $\mathbf{C}$ 上の楕円曲線の moduli 空間 $\mathcal{A}_1$ は, 格子 $\mathbf{Z}+\mathbf{Z}\tau$ の同値類を考えることにより,

$$\mathcal{A}_1=\mathrm{SL}_2(\mathbf{Z})\backslash\mathfrak{H}_1$$

であって, modular j- 函数を介して affine 直線 $\mathbf{A}^1(\mathbf{C})$ と見做せるのであった. また, $\mathcal{A}_1$ に於いて, $\mathcal{O}_K$ に CM をもつ点からなる部分集合

$$\mathcal{A}_1^{\mathrm{CM}}:=\{[E]\in\mathcal{A}_1\mid \mathrm{End}(E)\cong\mathcal{O}_K\ (\exists K:\text{虚 2 次体})\}$$

を考える. 虚数乗法論からわかる次の事実は良く知られている:

Fact 1. $[E]\in\mathcal{A}_1^{\mathrm{CM}}$ に対して, 以下の 3 条件は同値である:
(1) E が $\mathbf{Q}$ 上定義される,
(2) E の j- 不変量 $j(E)$ が $\mathbf{Q}$ の元となる,
(3) K の類数 h_K が 1 である.

†本研究は科学研究費補助金 (特別研究員奨励費) の援助を受けています.

したがって, $\mathcal{A}_1^{\mathrm{CM}}$ の $\mathbf{Q}$- 有理点を決定することは類数 1 の虚 2 次体の決定問題に帰着されるが, これは Heegner-Baker-Stark によって解決されている:

Fact 2. 類数が 1 の虚 2 次体は $\mathbf{Q}(\sqrt{-d})$ $(d = 1,2,3,7,11,19,43,67,163)$ の 9 つである.

したがって, 以下の定理がわかる:

Theorem 1.1. $\mathcal{A}_1^{\mathrm{CM}}$ には丁度 9 個の $\mathbf{Q}$- 有理点が存在する.

さらに, この 9 つの $\mathbf{Q}$- 有理点に対して, 対応する楕円曲線 E を求めることができる.

Example 1.2. $K = \mathbf{Q}(\sqrt{-7})$ は類数が 1 の虚 2 次体である. i を虚数単位とするとき, 整数環 $\mathcal{O}_K$ は, $\tau = \dfrac{1+\sqrt{7}i}{2}$ と見做すことによって, 複素平面 $\mathbf{C}$ 内の格子

$$\mathcal{O}_K = \mathbf{Z} + \mathbf{Z}\tau$$

を定義する. このとき, 近似計算によって,

$$q = e^{2\pi i\tau} = -0.000245583\ldots,$$

$$j(q) = \frac{1}{q} + 744 + 196884\, q + \cdots = -3374.9999\ldots$$

という値が求まる. j- 不変量が -3375 となる楕円曲線は実際に CM をもつことが確認できる.

楕円曲線は 1 次元の abel 多様体であるから, 上述の事実を 2 次元の場合で考察してみる. 総実代数体の総虚 2 次拡大を **CM 体**という. $K/\mathbf{Q}$ を 4 次 CM 体として, F を K に含まれる実 2 次体, $\mathcal{O}_K$ を K の整数環とする. $\mathcal{O}_K$ に CM をもつ abel 曲面, 即ち, abel 曲面 $A/\mathbf{C}$, A の偏極 $\mathcal{C}$ と単射 $\theta\colon K \hookrightarrow \mathrm{End}(A)\otimes\mathbf{Q}$ で条件

$$\theta^{-1}(\mathrm{End}(A)) = \mathcal{O}_K \tag{1.1}$$

を満たすものからなる 3 つ組 $(A,\mathcal{C},\theta)$ を考える.

Definition 1.3. K の部分体 k に対して, $\mathbf{C}$ の部分体 M_k が以下の性質を満たすとき, $(A,\mathcal{C},\theta|_k)$ の **moduli の体**という:

任意の $\tau \in \mathrm{Aut}(\mathbf{C})$ に対して, $\tau \in \mathrm{Aut}(\mathbf{C}/M_k)$ となるための必要十分条件は

$$\exists\lambda\colon A \xrightarrow{\sim} A^{\tau} : \text{同型} \quad \text{s.t.} \quad \begin{cases} \lambda(\mathcal{C}) = \mathcal{C}^{\tau}, \\ \lambda\circ\theta(a) = \theta^{\tau}(a)\circ\lambda \ \text{ for } \forall a \in k \end{cases}$$

となることである.

Remark 1.4. 楕円曲線に対しては, moduli の体と定義体は一致したが, 一般の abel 多様体に対しては, moduli の体と定義体は必ずしも一致しない.

$\mathcal{A}_2$ を $\mathbf{C}$ 上の主偏極 abel 曲面の moduli 空間とする. $\mathcal{A}_2$ は Siegel 上半空間

$$\mathfrak{H}_2 := \{\tau \in \mathrm{M}_2(\mathbf{C}) \mid \tau = \tau^t,\ \mathrm{Im}(\tau) > 0\}$$

を用いて, $\mathcal{A}_2 = \mathrm{Sp}_2(\mathbf{Z})\backslash\mathfrak{H}_2$ とかける. ここで, その部分集合

$$\mathcal{A}_2^{\mathrm{CM}} := \{[(A,\mathcal{C})] \in \mathcal{A}_2 \mid \mathrm{End}(A) \cong \mathfrak{o}_K\ (\exists K :4 \text{ 次 CM 体})\}$$

を考える. Theorem 1.1 の自然な拡張として次の問題が生ずる:

Problem 1.5. $\mathcal{A}_2^{\mathrm{CM}}$ の $\mathbf{Q}$- 有理点, 即ち, $M_{\mathbf{Q}} = \mathbf{Q}$ となる点はどれくらい存在するか?

Example 1.6. 種数 2 の曲線

$$y^2 = x^5 - 1$$

の jacobi 多様体は明らかに, $K = \mathbf{Q}(\zeta_5) = \mathbf{Q}(\alpha)$ $(\alpha^4 + 5\alpha + 5 = 0)$ に CM をもつから, $\mathcal{A}_2^{\mathrm{CM}}$ に少なくとも 1 つの $\mathbf{Q}$- 有理点が存在する.

この問題に対する答として, 次の結果を得た:

Theorem 1.7 (M-U [3]). $\mathcal{A}_2^{\mathrm{CM}}$ の $\mathbf{Q}$- 有理点は丁度 19 個存在する.

以下に於いて, この定理について考察する.

2. 証明の概略

Theorem 1.7 の証明には, 2 つの定理が重要な役割を果たす. 1 つ目は 1 次元の場合の Fact 1 に対応するものであり, 2 つ目は Fact 2 に相当する結果を得るために必要となる解析数論の手法を用いた定理である.

Theorem 2.1 (M [2]). $K/\mathbf{Q}$ を 4 次 CM 体として, $[(A,\mathcal{C})] \in \mathcal{A}_2$ が $\mathrm{End}(A) \supseteq \mathfrak{o}_K$ を満たすとする. このとき, $[(A,\mathcal{C})] \in \mathcal{A}_2^{\mathrm{CM}}$ かつ $M_{\mathbf{Q}} = \mathbf{Q}$ となる必要十分条件は K が以下の条件 (a), (b) を満たすことである:
(a) K が

$$K = \mathbf{Q}(\sqrt{-q_1 \cdots q_t \varepsilon_F \sqrt{p}}) \quad (t \geq 0),$$

という形の表示をもつ. 但し, ε_F は $\varepsilon_F > 0$ を満たす $F = \mathbf{Q}(\sqrt{p})$ の基本単数であって, $p, q_1, \ldots, q_t$ は以下の 3 条件 (a_1), (a_2), (a_3) のうちの 1 つを満たす相異なる素数である:

(a_1) $p \equiv 5 \pmod 8$ であって, さらに $t \geq 1$ ならば,

$$q_i \equiv 1 \pmod 4 \quad \text{かつ} \quad \left(\frac{p}{q_i}\right) = -1 \quad (i = 1, \ldots, t)$$

を満たす.
(a_2) $p \equiv 5 \pmod 8$, $t \geq 1$, $q_1 = 2$ であって, さらに $t \geq 2$ ならば,

$$q_i \equiv 1 \pmod 4 \quad \text{かつ} \quad \left(\frac{p}{q_i}\right) = -1 \quad (i = 2, \ldots, t)$$

を満たす.

(a$_3$) $p=2$ であって, さらに $t \geqq 1$ ならば,

$$q_i \equiv 5 \pmod 8 \quad (i=1,\dots,t)$$

を満たす.

(b) K の相対類数 h_K^- が 2^t となる.

Remark 2.2. [2] に於いては, 主偏極の場合だけでなく, 一般の偏極をもつ abel 曲面に対しても同様の結果が得られている.

定理の条件 (b) の右辺の t は条件 (a) に現れる異なる素数の個数と同一であることに注意する. 定理から,

$$K=\mathbf{Q}(\sqrt{-r\varepsilon_F\sqrt{p}}),\ r=q_1\cdots q_t\in\mathbf{N}$$

という形の CM 体のみを考えればよい. 特に, $K/\mathbf{Q}$ は巡回拡大であって, $\mathrm{Gal}(K/\mathbf{Q})$ の生成元として,

$$\sigma\colon \sqrt{-a-b\sqrt{p}}\mapsto\sqrt{-a+b\sqrt{p}}$$

がとれる. 但し, $a+b\sqrt{p}:=r\varepsilon_F\sqrt{p}$ である. また, 虚数乗法論により, 巡回拡大 $K/\mathbf{Q}$ に自己準同型環をもつような abel 曲面は単純であることが知られている.

Theorem 2.3 (Louboutin [1]). $K/\mathbf{Q}$ を $2^m=2n\geq 4$ 次巡回 CM 体とする. f_K を K の導手として, d_K を K の判別式とする. このとき,

$$h_K^-\geq\frac{2c_K}{e(2n-1)}\left(\frac{\sqrt{f_K}}{\pi(\log f_K+0.05)}\right)^n$$

が成り立つ. 但し,

$$c_K=1-\frac{2\pi n e^{\frac{1}{n}}}{d_K^{\frac{1}{2n}}}\quad \text{または}\quad \frac{2}{5}\exp\left(-\frac{2n\pi}{d_K^{\frac{1}{2}}}\right)$$

である.

この定理を用いて, $K/\mathbf{Q}$ で分岐する素数の個数を評価できる.

Proposition 2.4. $K/\mathbf{Q}$ を (a$_1$) かつ (b) を満たす 4 次 CM 体とする. このとき,

$$0\leq t\leq 3$$

が成り立つ.

Proof. 条件を満たす K に対して,

$$f_K=pr,\ d_K=f_K^2f_F=p^3r^2,\ c_K=1-\frac{4\pi e^{\frac{1}{2}}}{d_K^{\frac{1}{4}}}$$

が成り立つ. Louboutin の定理を適用すると,

$$
\begin{aligned}
h_K^- &\geq \frac{2}{3e}\left(1-\frac{4\pi e^{\frac{1}{2}}}{p^{\frac{3}{4}}r^{\frac{1}{2}}}\right)\frac{pr}{\pi^2(\log pr+0.05)^2} \\
&= \frac{2}{3e\pi^2}\cdot\frac{pr-4\pi e^{\frac{1}{2}}p^{\frac{1}{4}}r^{\frac{1}{2}}}{(\log pr+0.05)^2} \\
&> \frac{2}{3e\pi^2}\cdot\frac{pr-4\pi e^{\frac{1}{2}}(pr)^{\frac{1}{2}}}{(\log pr+0.05)^2}
\end{aligned}
$$

となる. ここで, 右辺の pr の部分を変数と見て, 函数

$$
f(x) := \frac{2}{3e\pi^2}\cdot\frac{x-4\pi e^{\frac{1}{2}}x^{\frac{1}{2}}}{(\log x+0.05)^2}
$$

を定義する. このとき, 函数 $f(x)$ は $x>108$ のとき単調増加函数となることがわかる. また, 数列

$$
\alpha_t := \prod_{i=0}^{t}(5+4i)
$$

を考えれば, 任意の t に対して, $pr=pq_1\cdots q_t>\alpha_t$ が成り立つ. このことから, $t\geq 2$ ならば

$$
f(pr) > f(\alpha_t)
$$

となる. あとは, $f(\alpha_t)>2^t$ となるような t の範囲を求めれば良いが, 帰納法によって,

$$
t\geq 4 \Longrightarrow f(\alpha_t) > 2^t
$$

を示すことができ, 命題が得られる. □

条件 (a_2), (a_3) に対しても同様の結果を得ることができる. 相対類数が 20 以下の 4 次巡回 CM 体は Park-Kwon [4] によって全て決定されている. これと Theorem 2.1 と併せると, 以下の定理がわかる:

Theorem 2.5. $K/\mathbf{Q}$ を (a) かつ (b) を満たす 4 次 CM 体とする. このとき, K は次の 13 個の体のいずれかである:

K	p	ε_F	r
$\mathbf{Q}\left(\sqrt{-(2+\sqrt{2})}\right)$	2	$1+\sqrt{2}$	1
$\mathbf{Q}\left(\sqrt{-(5+2\sqrt{5})}\right)$	5	$\frac{1+\sqrt{5}}{2}$	1
$\mathbf{Q}\left(\sqrt{-(13+2\sqrt{13})}\right)$	13	$\frac{3+\sqrt{13}}{2}$	1
$\mathbf{Q}\left(\sqrt{-(29+2\sqrt{29})}\right)$	29	$\frac{5+\sqrt{29}}{2}$	1
$\mathbf{Q}\left(\sqrt{-(37+6\sqrt{37})}\right)$	37	$6+\sqrt{37}$	1
$\mathbf{Q}\left(\sqrt{-(53+2\sqrt{53})}\right)$	53	$\frac{7+\sqrt{53}}{2}$	1
$\mathbf{Q}\left(\sqrt{-(61+6\sqrt{61})}\right)$	61	$\frac{39+5\sqrt{61}}{2}$	1
$\mathbf{Q}\left(\sqrt{-5(2+\sqrt{2})}\right)$	2	$1+\sqrt{2}$	5
$\mathbf{Q}\left(\sqrt{-(5+\sqrt{5})}\right)$	5	$\frac{1+\sqrt{5}}{2}$	2
$\mathbf{Q}\left(\sqrt{-13(5+2\sqrt{5})}\right)$	5	$\frac{1+\sqrt{5}}{2}$	13
$\mathbf{Q}\left(\sqrt{-17(5+2\sqrt{5})}\right)$	5	$\frac{1+\sqrt{5}}{2}$	17
$\mathbf{Q}\left(\sqrt{-(13+3\sqrt{13})}\right)$	13	$\frac{3+\sqrt{13}}{2}$	2
$\mathbf{Q}\left(\sqrt{-5(13+2\sqrt{13})}\right)$	13	$\frac{3+\sqrt{13}}{2}$	5

表中の線より上の体は類数が 1 であり, 下の体は類数が 2 であることを注意しておく. ここ迄の考察によって, 自己準同型環となりうる 4 次 CM 体は決定できた. 次に, それらの体を自己準同型環にもつような主偏極 abel 曲面が実際に存在するかどうかを調べる.

$K/\mathbf{Q}$ を 4 次 CM 体として, K の $\mathbf{C}$ への埋め込みのなす集合 $I := \{\iota : K \hookrightarrow \mathbf{C}\}$ を考える. また, 複素共役を $\bar{\cdot}$ で表わすことにする.

Definition 2.6. $\Phi = \{\sigma_1, \sigma_2\}$ $(\sigma_i \in I)$ が

$$\{\sigma_1, \sigma_2\} \cup \{\bar{\sigma_1}, \bar{\sigma_2}\} = I$$

を満たすとき, **CM-type** という.

任意の CM-type $\Phi = \{\sigma_1, \sigma_2\}$ は同型

$$\Phi\colon K \otimes_{\mathbf{Q}} \mathbf{R} \xrightarrow{\sim} \mathbf{C}^2, \quad \alpha \otimes a \mapsto (a\alpha^{\sigma_1}, a\alpha^{\sigma_2})$$

を誘導する. 任意の K のイデアル $\mathfrak{a}$ に対して, $\Lambda_{\mathfrak{a}} := \Phi(\mathfrak{a})$ は $\mathbf{C}^2$ の格子となるから, 複素トーラス $\mathbf{C}^2/\Lambda_{\mathfrak{a}}$ を考えることができる. $\eta \in K$ を

$$\bar{\eta} = -\eta, \ \mathrm{Im}(\eta^{\tau}) > 0 \quad \text{for} \ \tau = \sigma_1, \sigma_2$$

満たすようにとると, 複素トーラス $\mathbf{C}^2/\Lambda_{\mathfrak{a}}$ に対応する Riemann form

$$E(\Phi(x),\Phi(y)) := \mathrm{Tr}_{K/\mathbf{Q}}(\eta x\bar{y}) \quad \text{for } \forall x,y \in K$$

が得られる. よって, $(\mathbf{C}^2/\Lambda_{\mathfrak{a}},\eta)$ の組は abel 曲面を定める.

Definition 2.7. **これを type (K,Φ) の abel 曲面**という.

逆に, $\mathcal{O}_K$ に CM をもつ abel 曲面 $(A,\mathcal{C},\theta)$ に対して, CM-type Φ, K のイデアル $\mathfrak{a}$, $\eta \in K$ が定まる. よって, abel 曲面 $(A,\mathcal{C},\theta)$ と $(K,\Phi;\mathfrak{a},\eta)$ の組とを同一視できる.

$K/\mathbf{Q}$ が巡回拡大のとき, CM-type の取り方は

$$\Phi_1=\{1,\sigma\},\Phi_2=\{1,\sigma^{-1}\},\Phi_3=\{\sigma^2=\bar{\cdot},\sigma\},\Phi_4=\{\sigma^2,\sigma^{-1}\}$$

の 4 通りがある. $\mathcal{A}_2^{\mathrm{CM}}$ に於いて type (K,Φ) の主偏極 abel 曲面の同型類からなる部分集合 $\mathcal{A}_2^{\mathrm{CM}}(K,\Phi)$ を考える. $K/\mathbf{Q}$ が巡回拡大のとき,

$$\mathcal{A}_2^{\mathrm{CM}}(K,\Phi_1)=\mathcal{A}_2^{\mathrm{CM}}(K,\Phi_2)=\mathcal{A}_2^{\mathrm{CM}}(K,\Phi_3)=\mathcal{A}_2^{\mathrm{CM}}(K,\Phi_4)$$

が成り立つから, CM-type として $\Phi = \{1,\sigma\}$ のみを考えれば十分である. さらに, $N_{F/\mathbf{Q}}(\varepsilon_F) = -1$ のとき, 各イデアル類に対して主偏極 $\mathcal{C}$ は存在すれば一意的に定まることもわかる. したがって, 今考えている 13 個の体のイデアル類 19 個各々に対し, 高々 1 つしか主偏極 abel 曲面は存在しない.

Definition 2.8. $(A,\mathcal{C},\theta)$ に対応するイデアル $\mathfrak{a}$ の $\mathbf{Z}$- 基底 (v_1,v_2,v_3,v_4) が

$$(E(\Phi(v_i),\Phi(v_j))) = \begin{pmatrix} & I_2 \\ -I_2 & \end{pmatrix}$$

を満たすとき, $\mathfrak{a}$ の **symplectic basis** という.

$\mathfrak{a}$ の symplectic basis (v_1,v_2,v_3,v_4) を用いて, $(A,\mathcal{C})$ に対応する Siegel 上半空間 $\mathfrak{H}_2$ 上の点が

$$\tau := -\begin{pmatrix} v_3 & v_4 \\ v_3^\sigma & v_4^\sigma \end{pmatrix}^{-1}\begin{pmatrix} v_1 & v_2 \\ v_1^\sigma & v_2^\sigma \end{pmatrix} \in \mathfrak{H}_2$$

で与えられる.

Remark 2.9. 19 個全てのイデアル類に対して, イデアル類の代表 $\mathfrak{a}$ を固定する. このとき, $\eta \in K$ を適当に選び, $\mathfrak{a}$ の symplectic basis を具体的に求めることにより, 主偏極 abel 曲面の存在が確認でき, Theorem 1.7 が得られる.

前述の通り, これら 19 個の $\mathbf{Q}$- 有理点に対応する主偏極 abel 曲面は単純であったから, 種数 2 の曲線の jacobi 多様体と見做せる. 1 次元の場合 (cf. Remark 1.2) と同等の近似計算を行なうことにより, 対応する種数 2 の曲線を求めることができる.

Example 2.10. 例えば, 類数 1 の 7 個の 4 次 CM 体を自己準同型環にもつ主偏極 abel 曲面に対応する種数 2 の曲線は以下で与えられる:

p	n	C
2	1	$y^2 = x^5 + 3x^4 - 2x^3 - 6x^2 + 3x + 1$
5	1	$y^2 = x^5 - 1$
13	1	$y^2 = x^5 - 156x^4 + 10816x^3 - 421824x^2 + 8998912x - 80427776$
29	1	$y^2 = 116x^5 - 928x^4 + 2552x^3 - 2900x^2 + 1492x - 289$
37	1	$y^2 = 131769x^5 - 951786x^4 - 497048x^3 - 113232x^2 - 12336x - 544$
53	1	$y^2 = 70241161x^5 + 54250213x^4 + 21706954x^3 + 4502426x^2 + 446045x + 16697$
61	1	$y^2 = 5191138125x^5 + 859281075x^4 - 70429502x^3 + 2736582x^2 - 214719x + 6095$

これらの曲線が全て $\mathbf{Q}$ 上定義されていることに注意されたい (cf. Remark 1.4). 同様の計算により, 19 個の abel 曲面全てに対して, 定義体も $\mathbf{Q}$ であることが検証できる.

Remark 2.11. van Wamelen も沢山の CM 体を走らせて数値計算を実行し $\mathbf{Q}$ 上定義される種数 2 の曲線を探索している ([5]). さらに, それらの曲線の jacobi 多様体が実際に CM をもつことも確認している ([6]).

References

1. S. Louboutin, *CM-fields with cyclic ideal class groups of 2-power orders*, J. Number Theory **67**, 11-28, 1997.
2. N. Murabayashi, *The field of moduli of abelian surfaces with complex multiplication*, J. reine angew. Math. **470**, 1-26, 1996.
3. N. Murabayashi and A. Umegaki, *Determination of all* $\mathbf{Q}$*-rational CM-points in the moduli space of principally polarized abelian surfaces*, preprint, 1999.
4. Y. Park and S. Kwon, *Determination of all non quadratic imaginary cyclic number fields of 2-power degree with relative class number* ≤ 20, Acta Arith. **133**, no. 3, 211-223, 1998.
5. P. van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68**, no. 225, 307-320, 1999.
6. P. van Wamelen, *Proving that a genus 2 curve has complex multiplication,* Math. Comp. **68**, no. 228, 1663–1677, 1999

(村林 直樹) 山形市小白川町 1-4-12 山形大学理学部数理科学科

E-mail address: `murabaya@sci.kj.yamagata-u.ac.jp`

(梅垣 敦紀) 新宿区大久保 3-4-1 51 号館 17F 早稲田大学理工学研究科数学専攻・日本学術振興会特別研究員

E-mail address: `umegaki@gm.math.waseda.ac.jp`