超特別な種数 5 一般化 Howe 超楕円曲線の存在性と数え上げについて

On the existence and enumeration of superspecial genus-5 generalized Howe hyperelliptic curves

大橋 亮 (Ryo Ohashi)[1], 工藤 桃成 (Momonari Kudo)[2]
[1] 東京大学 (The university of Tokyo), [2] 福岡工業大学 (Fukuoka Institute of Technology)
e-mail : ryo-ohashi@g.ecc.u-tokyo.ac.jp

1　研究背景

超特別曲線は数論や代数幾何学における重要な研究対象であり, 自然数 g と素数 p に対して

問題. 標数 p における種数 g の超特別曲線は存在するか. 存在すれば, その同型類の個数を求めよ.

は根源的な問いである. この問題は先行研究により $g \leq 3$ では解決されているが, 一方で $g \geq 4$ では一般に未解決となっている. 最近になり $g = 4$ の場合に曲線のクラスを限定することで, 小標数での部分的な問題解決を試みる先行研究がいくつか報告されている. その例として, 大橋-工藤-原下 [3] は, 種数 4 の一般化 Howe 超楕円曲線

$$y^2 = x^{10} + ax^8 + bx^6 + cx^4 + dx^2 + 1, \quad a, b, c, d \in \overline{\mathbb{F}}_p$$

に着目して, そのうち超特別なものが任意の標数 $19 \leq p \leq 6691$ で存在することを計算機を利用して確認した. また, 大橋-工藤 [2] は更に条件を加えた種数 4 の一般化 Howe 超楕円曲線

$$y^2 = x^{10} + ax^8 + bx^6 + bx^4 + ax^2 + 1, \quad a, b \in \overline{\mathbb{F}}_p$$

に制限した場合でも超特別なものが同じ p の範囲で存在することを示し, 加えて各 $19 \leq p < 500$ に対してそのような曲線の同型類の個数を数え上げた. 本稿では, 種数 5 の一般化 Howe 超楕円曲線に関して同様の条件を加えた場合に, 超特別なものの存在性と数え上げについて議論する.

2　種数 5 の一般化 Howe 超楕円曲線

種数 5 の一般化 Howe 超楕円曲線 (定義は [1] を参照のこと) は

$$y^2 = x^{12} + ax^{10} + bx^8 + cx^6 + dx^4 + ex^2 + 1, \quad a, b, c, d, e \in \overline{\mathbb{F}}_p$$

に同型である. 本稿では $p > 11$ を仮定して, 更に条件を加えた種数 5 の一般化 Howe 超楕円曲線

$$y^2 = x^{12} + ax^{10} + bx^8 + cx^6 + bx^4 + ax^2 + 1, \quad a, b, c \in \overline{\mathbb{F}}_p \tag{1}$$

に着目する. 曲線 (1) の自己同型群は $(\mathbb{Z}/2\mathbb{Z})^3$ を含み, 逆に自己同型群が $(\mathbb{Z}/2\mathbb{Z})^3$ を含む種数 5 の超楕円曲線はこの形で書ける. また

$$\begin{cases} \alpha + \beta + \gamma = a, \\ \alpha\beta + \beta\gamma + \gamma\alpha = b - 3, \\ \alpha\beta\gamma = c - 2a \end{cases} \tag{2}$$

を満たす元 $\alpha, \beta, \gamma \in \overline{\mathbb{F}}_p$ をとれば, 式 (1) の右辺は $(x^4 + \alpha x^2 + 1)(x^4 + \beta x^2 + 1)(x^4 + \gamma x^2 + 1)$ と因数分解できる (曲線の非特異性から $\alpha \neq \beta \neq \gamma \neq \alpha$ かつ $\alpha, \beta, \gamma \notin \{2, -2\}$ が成立する). このとき

$$\lambda := -\frac{2 + \alpha}{2 - \alpha}, \quad \mu := -\frac{2 + \beta}{2 - \beta}, \quad \nu := -\frac{2 + \gamma}{2 - \gamma} \tag{3}$$

と定義しておく.

命題 1. 曲線 (1) が超特別的であることと, 種数 1 曲線

$$\begin{aligned} E_1 &: Y^2 = (X-\lambda)(X-\mu)(X-\nu), \\ E_2 &: Y^2 = X(X-\lambda)(X-\mu)(X-\nu), \\ E_3 &: Y^2 = (X-1)(X-\lambda)(X-\mu)(X-\nu) \end{aligned} \tag{4}$$

が全て超特異的かつ種数 2 曲線

$$C_{\lambda,\mu,\nu} : Y^2 = X(X-1)(X-\lambda)(X-\mu)(X-\nu) \tag{5}$$

が超特別的であることは同値である (このとき $\lambda, \mu, \nu \in \mathbb{F}_{p^2}$ が成立する).

3 数え上げアルゴリズムと実行結果

命題 1 を利用することで, 次のように超特別的な曲線 (1) の同型類の個数を数え上げられる.

アルゴリズム 2. 入力: 素数 $p > 11$. 出力: 超特別的な曲線 (1) の同型類個数.

Step 1: 種数 2 超特別曲線の同型類を全て列挙し, その集合を $\mathsf{SSp}_2(p)$ とする.

Step 2: 各 $C \in \mathsf{SSp}_2(p)$ に対して, 式 (5) の曲線 $C_{\lambda,\mu,\nu}$ が C と同型となる $\{\lambda, \mu, \nu\} \subset \mathbb{F}_{p^2}$ を全て計算し (そのような λ, μ, ν を C の *Rosenhain* 不変量という), その集合を $\mathsf{Ros}(C)$ とする.

Step 3: 各 $C \in \mathsf{SSp}_2(p)$ と $\{\lambda, \mu, \nu\} \in \mathsf{Ros}(C)$ に対して, 式 (4) の E_1, E_2, E_3 が全て超特異的か確認し, そうであれば式 (2) と式 (3) を用いて得られた曲線 (1) を全て保存する.

Step 4: *Step 3* で保存された全ての曲線 (1) に対して同型判定を行い, 同型類の個数を出力する.

詳細は省略するが, アルゴリズム 2 の実行に必要となる漸近計算量は $\widetilde{O}(p^3)$ と見積もられる. 上記のアルゴリズムを Magma で実装したコードを

`https://sites.google.com/view/m-kudo-official-website/english/code/hyp`

で公開している. これを実行することで, 次の結果が得られた.

定理 3. 各素数 $11 < p < 1000$ に対して, 超特別的な曲線 (1) の同型類個数は

`https://drive.google.com/file/d/1BJiYOycvxd9YRfYap5xD7mcT18i_e-5H`

に掲載されている表の最右列で示されている.

実験結果から, いくつかの p に対しては (種数 4 とは異なり) 超特別的な曲線 (1) が存在していない. そこで, 今後の課題として, より広いクラスでの超特別的な種数 5 超楕円曲線の数え上げも行いたい.

参考文献

[1] T. Katsura and K. Takashima: *Decomposed Richelot isogenies of Jacobian varieties of hyperelliptic curves and generalized Howe curves*, Comment. Math. Univ. St. Pauli **72**, No. 1, 3–17, 2024.

[2] R. Ohashi and M. Kudo: *Computing superspecial hyperelliptic curves of genus 4 with automorphism group properly containing the Klein 4-group*, J. Comput. Algebra **11**, Paper No. 100020, 2024.

[3] R. Ohashi, M. Kudo and S. Harashita: *Fast enumeration of superspecial hyperelliptic curves of genus 4 with automorphism group V_4*, LNCS **13638**, 107–124, 2023.

