楕円曲線族に関するモジュラー多項式の構成と計算アルゴリズム

Construction of modular polynomials for families of elliptic curves and its algorithm

東京大学　　小貫 啓史 [*1]
Hiroshi Onuki
The University of Tokyo

Abstract

We describe an algorithm for computing modular polynomials for the coefficients of elliptic curves. In particular, we consider the modular polynomials for Montgomery curves and Hesse curves. The algorithm is based on the method of Bröker-Lauter-Sutherland and uses the action of the ideal class group of an imaginary quadratic field. We also present the results of the implementation of the algorithm.

1　はじめに

楕円曲線の位数 N のモジュラー多項式は, 2 変数整数係数多項式 $\Phi_N(X,Y)$ であり, 2 つの楕円曲線の間に N 次巡回同種写像が存在することとそれらの楕円曲線の j-不変量が Φ_N の根となることが同値であるという性質を持つ.

モジュラー多項式を具体的に求めることは数論アルゴリズムの重要な研究テーマの 1 つであり, j-不変量の複素関数としての性質を用いた方法 [Elk98], 小さな有限元体上で同種写像を計算し，中国式剰余定理で真の係数を求める方法 [CL05, BLS11] などが知られている. また，同種写像暗号にも応用されており, 鍵共有方式 [CK19] や同種写像問題の求解アルゴリズム [TKF+21, CRSCS22] において同種写像による像を計算することに利用される.

本稿では, SCIS 2023 [Onu23] で報告した楕円曲線の係数に関するモジュラー多項式のうち, Montgomery 曲線と Hesse 曲線に関するものの計算に [BLS11] のアルゴリズムを適用する方法について述べる. また, そのアルゴリズムの実装結果について報告する.

2　準備

2.1　記号の定義

本稿では, 断らない限り楕円曲線はすべて $\mathbb{C}$ 上の楕円曲線とする. $\mathfrak{H}$ を上半平面 $\{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ とする. $\mathbb{C}$ 上の多項式 f に対して, f の係数の絶対値の最大値を $|f|$ で表す. 体 K の元 j_0 に対して, j-不変量が j_0 となる楕円曲線を E_{j_0} で表す. ここで E_{j_0} は $\overline{K}$ 上の同型を除いて一意に定まる.

[*1] 〒 113-8656 文京区本郷 7-3-1　E-mail: hiroshi-onuki@g.ecc.u-tokyo.ac.jp

2.2 モジュラー多項式

$j : \mathfrak{H} \to \mathbb{C}$ を j-不変量とする．$\tau \in \mathfrak{H}$ に対して, $j(N\tau)$ は $\mathbb{Z}[j(\tau)]$ 上整となる．すなわち, $j(N\tau)$ の $\mathbb{Q}(\tau)$ 上の最小多項式は変数 X を用いて $\mathbb{Z}[X, j(\tau)]$ の元とみなせる．この 2 変数多項式を**位数 N のモジュラー多項式**と呼ぶ. 以下, 位数 N のモジュラー多項式を Φ_N と書く．

命題 1
N を正整数とする．このとき, Φ_N は以下を満たす.

1. Φ_N は X と Y に関して対称となる．
2. Φ_N は X に関してモニック．
3. Φ_N の X に関する次数は $N\prod_p \left(1+\frac{1}{p}\right)$．ここで p は N を割る素数全体を走る．
4. $j_1, j_2 \in \mathbb{C}$ に対して, $\Phi_N(j_1, j_2) = 0$ であることと E_{j_1} と E_{j_2} の間に巡回 N 次同種写像が存在することが同値.

標数 p の有限体上でも Φ_N の p における還元を取ることでモジュラー多項式を定義できる．これを $\Phi_N \bmod p$ とかく．$\Phi_N \mod p$ は $\overline{\mathbb{F}}_p$ 上の楕円曲線の間の同種写像に関して命題 1 の 4 を満たす.

2.3 モジュラー多項式の計算アルゴリズム

現在知られているモジュラー多項式を計算するアルゴリズムの中で最も良い計算量を持つものは [BLS11] による中国式剰余定理と虚数乗法を用いるアルゴリズムである．本小節では, このアルゴリズムについて簡単に説明する.

命題 1 の 4 により, 合成数位数を持つモジュラー多項式はその約数のモジュラー多項式の終結式を用いて表すことができる．従って, 素数位数のモジュラー多項式を計算することが重要である．ここで, 素数 ℓ に対して, 以下が成り立つ ([BS09, Corollary 9]).

$$\log|\Phi_\ell| \leq 6\ell\log\ell + 18\ell. \tag{1}$$

本稿では, 式 (1) の右辺を B_ℓ とかく．素数の集合 $\mathcal{P}$ であって, $\sum_{p\in\mathcal{P}} \log p > B_\ell + \log 2$ を満たすものを選ぶ．このとき, $\Phi_\ell \bmod p$ を全ての $p \in \mathcal{P}$ について計算することで, 中国式剰余定理により Φ_ℓ を復元することができる.

$\Phi_\ell \bmod p$ は Vélu の公式 [Vél71] (あるいは [BDFLS20] によるその改善版) を用いて ℓ 次同種写像を約 ℓ^2 回計算することで求められる．この場合の計算コストは, は $\tilde{O}(\ell^{5/2})$ 回の $\mathbb{F}_p$ の演算である.

これをイデアル類群の作用を用いることでより効率化したのが [BLS11] の方法である．彼らの方法の計算コストは $O(\ell^2(\log p)^3 \log\log p)$ となる [BLS11, Lemma 6.5]．その計算手順は以下の通りである.

1. 虚二次体の整環 $\mathcal{O}$ で類数が $\ell+1$ よりも大きなものを取る．D を $\mathcal{O}$ の判別式とする.
2. p を $\frac{t^2-\ell^2 D}{4}$ の形の素数とする.
3. $\mathbb{F}_p$ 上の楕円曲線 E_0 であって $\mathcal{O}$ に虚数乗法を持つものを取る.
4. イデアル類群 $\mathrm{cl}(\mathcal{O})$ の小さなノルムの元からなる生成系をとり, それらの作用を同種写像を計算することで求めて, $\mathcal{O}$ に虚数乗法を持つ $\mathbb{F}_p$ 上の楕円曲線の j-不変量を全て求める．この集合を $\mathcal{J}$ とする.

5. E_0 を始域とする ℓ 次同種写像を 1 つ計算する．もし, 終域の楕円曲線の j-不変量が $\mathcal{J}$ に含まれていなければ, 終域の楕円曲線を E_0' とおく．もし, 含まれていたら, ℓ 次同種写像を取り直す.

6. E_0' は $\mathcal{O}' := \mathbb{Z} + \ell\mathcal{O}$ に虚数乗法を持つ．$\mathrm{cl}(\mathcal{O}')$ の小さなノルムの元からなる生成系をとり, それらの作用を用いて $\mathcal{O}'$ に虚数乗法を持つ $\mathbb{F}_p$ 上の楕円曲線の j-不変量を全て求める.

7. $\ell + 1$ 個の元からなる $\mathcal{J}$ の部分集合 S の全ての元 j に対して, 以下を計算する.

   (a) E_j と ℓ-同種な楕円曲線の j-不変量 $j_1, \ldots, j_{\ell+1}$ を全て求める．(これらは, $\mathrm{cl}(\mathcal{O})$ と $\mathrm{cl}(\mathcal{O}')$ の構造から, すでに計算した $\mathcal{J}, \mathcal{J}'$ から選択できる)

   (b) $\Phi_\ell(j, X) \pmod p = \prod_i (X - j_i)$ を計算する.

8. $\{\Phi_\ell(j, X)\}_{j\in S}$ のそれぞれの次数の係数に Lagrange 補間を適用し, $\Phi_\ell \bmod p$ を計算する.

3 モジュラー多項式の拡張

モジュラー多項式を j-不変量以外のモジュラー関数に拡張できることが知られている．g をレベル N のモジュラー関数, ℓ を N を割らない素数とする．このとき, $g(\ell\tau)$ の $\mathbb{C}(g(\tau))$ 上の最小多項式から g のモジュラー多項式を定義できる．この多項式を Φ_ℓ^g とかく．g の Fourier 展開の係数が整数となるとき, Φ_ℓ^g は $\mathbb{Z}$ 係数を持つ．[BLS11] では, いくつかのモジュラー関数についてそのモジュラー多項式を計算している.

他の拡張として, [Onu23] によりある条件を満たす曲線族に対して, その曲線の係数に関するモジュラー多項式を定義できることが示されている．本稿では, それらのうち Montgomery 曲線と Hesse 曲線に対するモジュラー多項式計算アルゴリズムについて述べる.

3.1 Montgomery 曲線

Montgomery 曲線は, 以下の形の楕円曲線である.

$$\mathcal{M}_A : y^2 = x^3 + Ax^2 + x. \tag{2}$$

$\mathcal{M}_A$ の点で x 座標が 1 となるものは位数 4 を持つ．さらにこれらの点は 2 倍すると $(0, 0)$ となる．4 次巡回群 $\{(1, \pm\sqrt{A+2}), (0, 0), \infty\}$ を C_A とかく．このとき, 二つの Montgomery 曲線 $\mathcal{M}_{A_1}, \mathcal{M}_{A_2}$ の間に C_{A_1} を C_{A_2} に移す同型写像が存在することと $A_1 = A_2$ が同値である.

[Onu23] により Montgomery 曲線の係数に関するモジュラー多項式の存在が示されている．即ち, 2 と互いに素な正整数 N に対して $\Phi_N^A \in \mathbb{Z}[X, Y]$ であって以下を満たすものが存在する.

1. Φ_N^A は X と Y に関して対称となる.

2. Φ_N^A は X に関してモニック.

3. Φ_N^A の X に関する次数は $N \prod_p \left(1 + \frac{1}{p}\right)$．ここで p は N を割る素数全体を走る.

4. $A_1, A_2 \in \mathbb{C}$ に対して, $\Phi_N^A(A_1, A_2) = 0$ であることと $\mathcal{M}_{A_1}$ と $\mathcal{M}_{A_2}$ の間に巡回 N 次同種写像であって C_{A_1} を C_{A_2} に移すものが存在することが同値.

3.2 Hesse 曲線

Hesse 曲線は, 以下の射影平面上定義される楕円曲線である.

$$\mathcal{H}_d : X^3 + Y^3 + Z^3 = 3dXYZ. \tag{3}$$

ω を 1 の原始 3 乗根 $e^{2\pi i/3}$ とする. $\mathcal{H}_d$ の点の順序付きペア $((-1:0:1),(-\omega:1:0))$ は 3-ねじれ部分群 $\mathcal{H}_d[3]$ の基底となる.

二つの Hesse 曲線 $\mathcal{H}_{d_1}, \mathcal{H}_{d_2}$ の間に $(-1:1:0)$ と $(-\omega:1:0)$ を保つ同型写像が存在することと $d_1 = d_2$ が同値である.

Montgomery 曲線と同様に Hesse 曲線の係数に関するモジュラー多項式の存在が示されている. 即ち, 3 と互いに素な正整数 N に対して $\Phi_N^d \in \mathbb{Z}[X,Y]$ であって以下を満たすものが存在する.

1. Φ_N^d は X と Y に関して対称となる.
2. Φ_N^d は X に関してモニック.
3. Φ_N^d の X に関する次数は $N\prod_p \left(1+\frac{1}{p}\right)$. ここで p は N を割る素数全体を走る.
4. $d_1, d_2 \in \mathbb{C}$ に対して, $\Phi_N^d(d_1,d_2) = 0$ であることと $\mathcal{H}_{d_1}$ と $\mathcal{H}_{d_2}$ の間に巡回 N 次同種写像であって $(-1:1:0)$ を保ち, $(-\omega:1:0)$ を $[\ell](-\omega:1:0)$ に移すものが存在することが同値.

4 曲線の係数に関するモジュラー多項式の計算アルゴリズム

Montgomery 曲線と Hesse 曲線の係数に関するモジュラー多項式を計算するアルゴリズムについて述べる. [BLS11] のアルゴリズムを適用する際に問題となるのは, 以下の 2 点である.

1. モジュラー多項式の係数の上界が不明であること.
2. $\mathbb{F}_p$ 上同型であっても, 係数が異なる Montgomery(Hesse) 曲線が存在すること.

1. の係数の上界は中国式剰余定理を適用する際にどれだけの素数 p を選べばよいかを決定するために必要である. 2. はイデアル類群の作用から計算される係数が条件を満たす同種写像から決まる係数と一致しない可能性があることを示している.

1. についてはレベル N のモジュラー関数のモジュラー多項式の係数の場合と同様に以下が予想される.

予想 1
素数 $\ell \geq 3$ と *Montgomery* 曲線の係数に関するモジュラー多項式 Φ_ℓ^A に対して, 以下が成り立つ.

$$\log|\Phi_\ell^A| \leq B_\ell/6. \tag{4}$$

予想 2
素数 $\ell \geq 5$ と *Hesse* 曲線の係数に関するモジュラー多項式 Φ_ℓ^d に対して, 以下が成り立つ.

$$\log|\Phi_\ell^d| \leq B_\ell/12. \tag{5}$$

実際にこれらのモジュラー多項式の計算アルゴリズムを実装し計算した結果, $\ell \approx 1000$ まではこれらの予想が成り立つことが確認されている. ただし, $\ell = 2$ のとき Hesse 曲線の係数に関するモジュラー多項式は式 (5) を満たさない.

2. については, 虚二次体の整環と素数 p をうまく取ることで解決できる. 具体的には以下が成り立つ.

定理 2
$D < 0$ を $D \equiv 4 \pmod{16}$ を満たす整数, $\mathcal{O}$ を虚二次体の整環で判別式が D となるものとする.

$$p = \frac{t^2 - v^2 D}{4}, \quad t, v \in \mathbb{Z},\ v \notin 2\mathbb{Z}$$

の形の素数をとる. このとき, $\mathcal{O}$ に虚数乗法を持つ $\mathbb{F}_p$ 上の楕円曲線 E に対して E と $\mathbb{F}_p$ 上同型な *Montgomery* 曲線がただ *1* つ存在する.

証明 概略を述べる.
E を $\mathcal{O}$ に虚数乗法を持つ $\mathbb{F}_p$ 上の楕円曲線とする. このとき, $\#E(\mathbb{F}_p) = p + 1 - t \equiv 0 \bmod 4$ であることから E と $\mathbb{F}_p$ 上同型な Montgomery 曲線 $\mathcal{M}_A$ が存在する.
$v \notin 2\mathbb{Z}$ より, $\mathcal{O}$ の導手 2 の部分環に虚数乗法を持つ $\overline{\mathbb{F}}_p$ 上の j-不変量は $\mathbb{F}_p$ の元とならない. 従って, $(0,0) \in \mathcal{M}_A$ が $\mathcal{M}_A(\mathbb{F}_p)$ の唯一の位数 2 の点である. これより, $\mathbb{F}_p$ 上の Montgomery 曲線の間の同型写像 $\iota : \mathcal{M}_A \to \mathcal{M}_{A'}$ は $\iota((0,0)) = (0,0)$ を満たす. このことから $A^2 = A'^2$ が従う. しかし, $p \equiv 3 \bmod 4$ より, $\mathcal{M}_A$ と $\mathcal{M}_{-A}$ は $\mathbb{F}_p$ 上同型でない. よって, $A = A'$ である. ∎

定理 3
$D < 0$ を $D \equiv 1 \pmod{3}$ を満たす整数, $\mathcal{O}$ を虚二次体の整環で判別式が D となるものとする.

$$p = \frac{t^2 - v^2 D}{4}, \quad t, v \in \mathbb{Z},\ v \notin 3\mathbb{Z}$$

の形の素数をとる. このとき, $\mathcal{O}$ に虚数乗法を持つ $\mathbb{F}_p$ 上の楕円曲線 E に対して E と $\mathbb{F}_p$ 上同型な *Hesse* 曲線がただ *1* つ存在する.

証明 概略を述べる.
E を $\mathcal{O}$ に虚数乗法を持つ $\mathbb{F}_p$ 上の楕円曲線とする. このとき, $\#E(\mathbb{F}_p) = p + 1 - t \equiv 0 \bmod 3$ であることから E と $\mathbb{F}_p$ 上同型な Hesse 曲線 $\mathcal{H}_d$ が存在する.
ω を $\overline{F}_p$ 上の 1 の原始 3 乗根とする. $p \equiv 2 \bmod 3$ より, $\omega \notin \mathbb{F}_p$ である. よって, $\pm(-1:0:1) \in \mathcal{H}_d$ が $\mathcal{H}_d(\mathbb{F}_p)$ の位数 3 の点の全てである. また, $\mathcal{H}_d[3]$ 上の p 乗 Frobenius 写像の固有ベクトルは, これらの点と $\pm(-\omega:1:0)$ のみである. 従って, $\mathbb{F}_p$ 上の Hesse 曲線の間の同型写像 $\iota : \mathcal{H}_d \to \mathcal{H}_{d'}$ は $\iota((-1:0:1)) = \pm(-1:0:1)$ および $\iota((-\omega:1:0)) = \pm(-\omega:1:0)$ を満たす. ここで ι が Weil pairing を保つことを用いると, これらの符号が一致することが示される. よって, ι もしくは $-\iota$ が $(-1:0:1)$ と $(-\omega:1:0)$ を保つ同型写像となる. 即ち, $d = d'$ である. ∎

5 実装実験

Montgomery 曲線と Hesse 曲線の係数に関するモジュラー多項式の計算アルゴリズムを実装し計算した結果について述べる. アルゴリズムは ℓ 次同種写像計算に Vélu の公式を用いたものとイデアル類群を用いる [BLS11] の方法の 2 つを実装した. 実装は Julia およびその拡張パッケージである Nemo を用いて行った. 実験環境は, Apple M2 Pro, 16GB RAM, macOS 14.2.1, Julia 1.10.2, Nemo 0.40.1 である. 表 1 に Montgomery 曲線と Hesse 曲線の係数に関するモジュラー多項式の計算時間を示す. 表中の Vélu は ℓ 次同種写像計算に Vélu の公式を用いる方法, BLS11 はイデアル類群を用いる [BLS11] の方法である.

表 1: Montgomery 曲線と Hesse 曲線の係数に関するモジュラー多項式の計算時間 (秒). ”Vélu”は ℓ 次同種写像計算に Vélu の公式を用いる方法, ”BLS11”はイデアル類群を用いる [BLS11] の方法.

ℓ	Montgomery		Hesse	
	Vélu	BLS11	Vélu	BLS11
101	14	122	101	41
103	17	125	66	34
107	22	137	78	39
109	21	139	83	38
151	78	272	323	76
503	8,132	13,7750	51,240	5,233

謝　辞

本研究は、総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」の成果である。

参 考 文 献

[BDFLS20] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. In Steven Galbraith, editor, *ANTS-XIV - 14th Algorithmic Number Theory Symposium*, volume 4 of *Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV)*, pages 39–55, Auckland, New Zealand, 2020. Mathematical Sciences Publishers.

[BLS11] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278):1201–1231, 2011.

[BS09] Reinier Broker and Andrew Sutherland. An explicit height bound for the classical modular polynomial. *Ramanujan Journal*, 22:293–313, 09 2009.

[CK19] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. In *Number-Theoretic Methods in Cryptology 2019*, 2019.

[CL05] Denis Charles and Kristin Lauter. Computing modular polynomials. *LMS Journal of Computation and Mathematics*, 8:195–204, 2005.

[CRSCS22] Maria Corte-Real Santos, Craig Costello, and Jia Shi. Accelerating the Delfs–Galbraith algorithm with fast subfield root detection. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 285–314, Cham, 2022. Springer Nature Switzerland.

[Elk98] Noam Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational Perspectives on Number Theory*, pages 21–76, 1998.

[Onu23] *Modular polynomials for enhanced elliptic curves*, In Proc. of SCIS 2023, 2023.

[TKF+21] Yasushi Takahashi, Momonari Kudo, Ryoya Fukasaku, Yasuhiko Ikematsu, Masaya Yasuda, and Kazuhiro Yokoyama. Algebraic approaches for solving isogeny problems of prime power degrees. *Journal of Mathematical Cryptology*, 15(1):31–44, 2021.

[Vél71] J. Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendues de l'Académie des Sciences*, 273:238–241, 1971.