9.

Modular 形式に付随する 2 次元法 l-Galois 表現の計算

木村 巌（富山大学）

9.1 イントロダクション

本稿の目的は，Edixhoven-Couveignes [EC11] に述べられている，複素数体 $\mathbb{C}$ 上の近似計算により，レベル 1 の Hecke 固有形式 f と素数 l に付随する法 l-Galois 表現を計算するアルゴリズムを説明することである．

Edixhoven-Couveignes らによる，法 l-Galois 表現の計算についての全体の流れやバリエーション，その後の研究については，本報告集所収の横山氏の論説 [横 18] をご覧頂きたい．

1 次元の場合を例として述べれば，円分指標 $\omega\colon (\mathbb{Z}/l\mathbb{Z})^\times \to \mathbb{C}^\times$ が与えられたとき，その核が固定する体 K を計算するために，$K = \mathbb{Q}[T]/(P(T))$ となる $P(T)$ を，数値的な近似で求める，ということである．$P(T) = \prod_x (T - a(x))$ となる $a(x)$ を構成し，その値を数値計算するのだが，どのくらいの桁数まで計算すれば，$P(T)$ の係数を有理数として正確に復元できるか，という見積もりが必要になり，そこから計算時間が評価できる．

本来の状況（法 l-Galois 表現）に戻って，もう少し詳しく説明する．まず l を素数，$2 < k \leq l+1$ を整数，レベル 1, 重さ k のモジュラー形式の空間に作用する Hecke 環 $\mathbb{T}(1,k)$ からの全射 $f\colon \mathbb{T}(1,k) \to \mathbb{F}$ をとる．さらに，f と l に対して定まる，2 次元法 l-Galois 表現（吉川氏の論説参照）$\rho = \rho_f\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ は絶対既約，$\mathrm{Im}(\rho) \supset \mathrm{SL}(V)$ を仮定する（ρ が既約で $l > 6(k-1)$ なら，ρ の像は $\mathrm{SL}(V)$ を含むことが示される．[EC11, Theorem 2.5.20] 参照）．$V = V_f \subset J_1(l)(\overline{\mathbb{Q}})[l]$ は ρ を実現する $\mathbb{F}$ 上のベクトル空間と

する．本稿で説明するのは，次の点である：

- $\mathbb{C}$ 上の近似計算を経由して，ρ を正確に計算する手続き
- その手続きの計算量評価（[EC11, Chap. 12, 14]）

まず，V の計算を $P_{D_0,f_l,m}(T) \in \mathbb{Q}(\zeta_l)[T]$ という多項式の計算に帰着する．そして，

$$A_{\mathbb{Q}(\zeta_l)} \coloneqq \mathbb{Q}(\zeta_l)[T]/(P_{D_0,f_l,m}(T))$$

という $\mathbb{Q}(\zeta_l)$ 代数から，$\mathbb{F}$ 上のベクトル空間 V を復元する（9.5.1 節，並びに [EC11, §14.5]）．さらにそこから，$\mathbb{Q}$ 代数 A を復元する（9.5.2 節，[EC11, § 14.6]）．さらに，V への Galois 作用を復元する議論を行う（[EC11, § 14.7]）．

まず，$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}(V) \curvearrowright V$ により，V は $G_{\mathbb{Q}}$ の連続な作用を持つ有限集合になる．Galois 理論により，$\mathbb{Q}$ 上の分離代数 A が対応して，$A = \mathbb{Q}[t]/(P(T))$ と書ける（$P(T) \in \mathbb{Q}[T]$ は分離的多項式）．A から V を得るには，まず集合として $V \coloneqq \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(A, \overline{\mathbb{Q}})$ とする．V の加法は A の余加法，$\mathbb{F}$ と V のスカラー積は A のスカラー余積から復元できる．

$\mathbb{Q}$ 上の分離代数 $A = \mathbb{Q}[T]/(P(T))$ の P を計算するには，A の $\mathbb{Q}$ 上の生成元 a を求め，その $\mathbb{Q}$ 上の最小多項式 $\prod_{x\in V}(T - a(x))$ を計算する．定数倍の違いを除いて，それが求める $P(T)$ である：

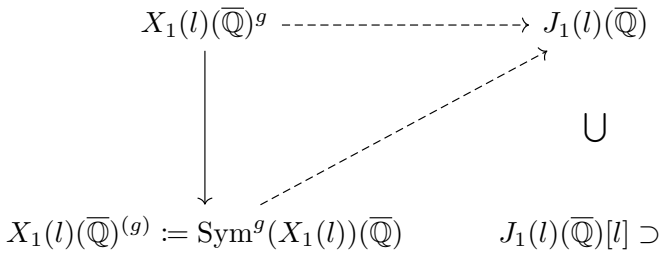
$$P(T) = \prod_{x\in V}(T - a(x)). \tag{9.1}$$

a が生成元であるためには，a が V 上の $\overline{\mathbb{Q}}$ 値写像として単射，すなわち，V の真の $G_{\mathbb{Q}}$ 集合としての商集合上の写像から誘導されない写像，であればよい．

これを，V が法 l-Galois 表現 ρ を実現する $\mathbb{F}$ 上の線型空間という状況で考える．おおまかな方針は，

- V と対応する $A = \mathbb{Q}[T]/(P(T))$ の $P(T)$ を数値的な近似計算で求める
- $P(T)$ の係数の高さの評価から，$P(T)$ を正確に求める（内田氏の論説 [内 18] 参照）
- $P(T)$ を数値的に近似計算するために（つまり，$a(x)$ を各 $x \in V$ に対して数値的に近似計算するために），$J_1(l)(\overline{\mathbb{Q}})$ での議論を，次の図式を経由して，直積集合 $X_1(l)(\overline{\mathbb{Q}})^g$ での議論に（更には，基本領域の直積集

合での議論に）帰着する：



- そのために，うまく D_0 という $X_1(l)$ 上の因子を取って（D_0 は次数 g の正因子に取る），x が $J_1(l)(\mathbb{C})$ の或る稠密集合を動くとき，$Q_x = (Q_{x,1}, \ldots, Q_{x,g}) \in X_1(l)(\overline{\mathbb{Q}})^{(g)}$ が x に対して一意に存在して，$x = [Q_x - D_0]$ となるようにする．
- これによって，$J_1(l)(\overline{\mathbb{Q}})$ 上の話を $X_1(l)(\overline{\mathbb{Q}})^{(g)}$，ひいては $X_1(l)(\overline{\mathbb{Q}})^g$ の話に帰着できる．

以上の方針を実現するため，$X_1(l)$ を $X_1(5l)$ にして，また $\mathbb{Q}$ 上ではなく $\mathbb{Q}(\zeta_l)$ 上の分離代数として考える必要がある．

注意 9.1.1. Edixhoven-Couveignes の本では，以上の方針で計算量の評価を行うが，この方針が具体的に計算を遂行するのに最適な方法というわけではない．あくまで，計算量の評価を行うためのものである．

Bosman は，近似計算により解の候補を構成し，解の一意性定理（Serre 予想）からそれが解であることを証明する，という方針で，$\dim S_k = 1$ となる k と $l \leq 23$ なる素数に対して計算した（[横 18], [EC11, Chap. 7] 参照）．

9.2 D_0 を見つける議論

この節の主な参照先は Edixhoven-Couveignes [EC11, Chap. 8 § 1] である．レベルが $5l$（l は 5 とは異なる素数）とする．目的は：

次数が $X_1(5l)$ の種数と等しい，$X_1(5l)_{\mathbb{Q}(\zeta_l)}$ 上の適切な正因子 D_0 を取って，$J_1(5l)(\overline{\mathbb{Q}})$ のある稠密集合の任意の点 x に対して，ある $Q = Q_x \in X_1(5l)^{(g)}$ が一意に存在して $x = [Q - D_0]$．ここで，ある稠密集合は

$$\{\, x \in J_1(5l)(\overline{\mathbb{Q}}) \mid h^0(\mathcal{L}_x(D_0)) = 1 \,\}$$

でよいことが，$h^0(\mathcal{L}_x(D_0))$ の半連続性（つまり，

$$\{\, x \in J_1(5l)(\overline{\mathbb{Q}}) \mid h^0(\mathcal{L}_x(D_0)) \geq i \,\}$$

が閉集合であること）からわかる．

定理 9.2.1 ([EC11, Thm. 8.1.7]). $l \neq 5$ を素数とする．c を $X_1(5)$ の 2 つある $\mathbb{Q}$ 有理的尖点の 1 つとする．$X_1(5l)$ には，c 上の尖点で $\mathbb{Q}(\zeta_l)$ 上有理的なものが $2(l-1)$ 個ある．これらは $\mathbb{F}_l^\times$ の軌道 2 つに分かれる．それぞれの軌道には $\mathbb{F}_l^\times$ が自由に作用する．一方の軌道の各点に，$0, 1, 2, \ldots, l-2$ と係数をつけて得られる $X_1(5l)_{\mathbb{Q}(\zeta_l)}$ 上の因子を D_1 とする．もう一方の軌道に $0, 0, 1, 2, \ldots, l-3$ と係数をつけて得られる因子を D_2 とする．$D_0 \coloneqq D_1 + D_2$ とすると，D_0 は $X_1(5l)$ の種数と同じ次数を持つ正因子である．このとき，任意の $x \in J_1(5l)(\overline{\mathbb{Q}})$ で，「l 上のある素点で 0 に特殊化するもの」に対して

$$h^0(X_1(5l)_{\overline{\mathbb{Q}}}, \mathcal{L}_x(D_0)) = 1.$$

証明. 証明の鍵となる事実は，$X = X_1(5l)_{\mathbb{Q}(\zeta_l)}$ の半安定モデル $X_1(5l)_{\mathbb{Z}[\zeta_l, 1/5]}$，$J_1(5l)$ の Neron モデル J_{O_K}，$K \supset \mathbb{Q}(\zeta_l)$ の詳細な事柄である．

$X_{\overline{\mathbb{F}_l}} = X_1 \sqcup X_2$ を既約成分への分解とする（$\mathbb{F}_l$ 上の $X_1(5)$ のうえにある，レベル l の井草曲線．これらは超特異点でのみ横断的に交わる．例えば Hida [Hid12, Thm. 2.91.13]）．$\overline{D_0} = D_1 + D_2$, D_i は X_i 上に台を持つ．カスプは超特異点の集合 Σ と互いに疎なので，$\overline{D_0}$ は $X_{\overline{\mathbb{F}_l}}$ のスムーズローカスの上にある．

記号を簡単にするために，この証明の終わりまで，$X = X_{\overline{\mathbb{F}_l}}$, $D_0 = \overline{D_0}$ とする．$\Omega_X \coloneqq X$ の双対化層は可逆 $\mathcal{O}_X$ 加群で，$\Omega^1_{X_1}(\Sigma)$ と $\Omega^1_{X_2}(\Sigma)$ を Σ に沿って，X_1 上の Σ における剰余写像と X_2 上の Σ における剰余写像のマイナスとで貼り合わせたものである．Riemann-Roch の定理によって，示したいのは

$$h^1(X, O(D_0)) = 0$$

だが，Serre 双対定理により

$$h^0(X, \Omega_X(-D_0)) = 0$$

でもある．言い換えると，$\mathrm{H}^0(X, \Omega_X)$ の元で D_0 で消えるものは 0 である事である．X_1 への制限によって，次の短完全系列を得る：

$$0 \to \mathrm{H}^0(X_2, \Omega_{X_2/\overline{\mathbb{F}_l}}(-D_2)) \to \mathrm{H}^0(X, \Omega_X(-D_0)) \to \mathrm{H}^0(X_1, \Omega_{X_1/\overline{\mathbb{F}_l}}(\Sigma - D_1)) \to 0.$$

よって，D_1 としては $\mathrm{H}^0(X_1, \Omega_{X_1/\overline{\mathbb{F}_l}}(\Sigma - D_0)) = 0$ となるものが，D_2 としては $\mathrm{H}^0(X_2, \Omega_{X_2/\overline{\mathbb{F}_l}}(-D_2)) = 0$ となるものが取れればよい．

$X_1 \to X_1(5)_{\overline{\mathbb{F}_l}}$ は Σ で完全分岐しその他で不分岐な被覆で，$X_1(5)$ は種数 0 である．Hurwitz の公式から，X_1 の種数 g_1 は

$$2g_1 - 2 = -2(l-1) + (l-1)(l-2), \quad g_1 = \frac{1}{2}(l-2)(l-3).$$

よって，D_1, D_2 が取れたとすれば

$$d_1 \coloneqq \deg D_1 = g_1 + \#\Sigma - 1 = \frac{1}{2}(l-1)(l-2),$$
$$d_2 \coloneqq \deg D_2 = \frac{1}{2}(l-2)(l-3),$$

でなければならない．

さて，$X_1(5)_{\overline{\mathbb{F}_l}}$ 上の座標 z を次のように取る：

$$z\colon X_1(5)_{\overline{\mathbb{F}_l}} \to \mathbb{P}^1_{\overline{\mathbb{F}_l}}, \quad z(\Sigma) \neq 0, \infty, \quad z^{-1}0 = X_1(5)_{\overline{\mathbb{F}_l}}\text{上の有理カスプ } 0.$$

f を，z のモニック多項式で，その零点が Σ と一致し，零点の位数が 1 であるものとする．すると，X_1 も X_2 も，$y^{l-1} = f$ で与えられる $X_1(5)_{\overline{\mathbb{F}_l}}$ の被覆と同型になることが示される．

このことから，$\mathrm{H}^0(X_1, \Omega^1_{X_1/\overline{\mathbb{F}_l}}(\Sigma))$ の基底が計算できて，

$$\mathrm{H}^0(X_1, \Omega^1_{X_1/\overline{\mathbb{F}_l}}(\Sigma)) = \bigoplus_{i+j\leq l-3} \overline{\mathbb{F}_l} z^i y^j \frac{dz}{y^{l-1}}. \tag{9.2}$$

すると，D_1 も次のように取ることができる．z が零点を持つ $l-1$ 個の点に重複度を与える．z と y による座標でこれらの点は

$$\left\{ (0,b) \;\middle|\; b \in \overline{\mathbb{F}_l}^{\times} \text{ s.t. } b^{l-1} = f(0) \right\}.$$

D_1 は，これらの点の上に，任意に重複度 $0, 1, \ldots, l-2$ を指定する．

主張：式 (9.2) の右辺の基底の線形結合で，D_1 上の点で 0 になるようなものは 0 に限る．

実際，ω を式 (9.2) の右辺の元で，D_1 上の点で 0 になるものとして，

$$\omega = \sum_{i+j\leq l-3} \lambda_{i,j} z^i y^j$$

と書く．D_1 上の点で z は一位の零点をもつ．ω が D_1 上で重複度込みで 0 になったとする．D_1 上の重複度が正の点は $l-2$ 個．一方，多項式 $\sum_j \lambda_{0,j} y^j$ は次数が高々 $l-3$ なので，この多項式も 0 である．また，D_1 上の重複度が 1 より大きい点は $l-3$ 個．多項式 $\sum_j \lambda_{1,j} z y^j$ の次数は高々 $l-4$ なのでこの多項式も 0. このようにして，主張が従う．

D_2 の取り方もほぼ同様である．

$$\mathrm{H}^0(X_2, \Omega^1_{X_2/\overline{\mathbb{F}_l}}) = \bigoplus_{i+j\leq l-4} \overline{\mathbb{F}_l} z^i y^j \frac{dz}{y^{l-2}}. \tag{9.3}$$

であることがわかる．D_2 として，z の零点に $0, 0, 1, 2, \ldots, l-3$ という重複度を任意に指定する．すると，D_1 のときと同様の議論から，右辺の基底の線形結合で，D_2 上 0 になるものは 0 に限ることが示される．

以上の議論は，$X_1(5)$ の 2 つある $\mathbb{Q}$ 有理カスプを一つ固定して行ったが，これらは $\mathbb{F}_5^\times$ の作用で入れ替わるので，カスプの指定に依らない． □

定理 9.2.1 が D_0 を $X_1(5l)_{\mathbb{Q}(\zeta_l)}$ 上に見つけるので，V を $J_1(5l)(\overline{\mathbb{Q}})[l]$ に埋め込む．そのために，degeneracy map（木村 [木 18] の式 (1.5) を参照）

$$\pi = B_{5l,l,1} \colon X_1(5l) \to X_1(l)$$

（次数は $5^2 - 1 = 24$, $\gcd(l, 24) = 1$）を使って，

$$\frac{1}{24}\pi^*\pi_* \colon J_1(5l)(\overline{\mathbb{Q}})[l] \twoheadrightarrow \pi^* J_1(l)(\overline{\mathbb{Q}})[l] \subset J_1(5l)(\overline{\mathbb{Q}})[l], \tag{9.4}$$

を考え，これにより，$V \subset J_1(l)(\overline{\mathbb{Q}})[l]$ を $\pi^*V \subset J_1(l)(\overline{\mathbb{Q}})[l] \subset J_1(5l)(\overline{\mathbb{Q}})[l]$ に埋め込む．

命題 9.2.2 ([EC11, 8.2.2]). $l \neq 5$ を素数とする．$2 < k \leq l+1$, $f \colon \mathbb{T}(1,k) \to \mathbb{F}$ を全射準同型とする．$\rho = \rho_f \colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ を f に付随する法 l-表現，$\mathrm{Im}\rho \supset \mathrm{SL}_2(\mathbb{F})$ と仮定する．$V \subset J_1(5l)(\overline{\mathbb{Q}})[l]$ を ρ を実現する $\mathbb{F}$ 上の線形空間，D_0 を定理 9.2.1 で構成した $X_1(5l)_{\mathbb{Q}(\zeta_l)}$ 上の因子とする．このとき，任意の $x \in V$ に対して $h^0(X_1(5l)_{\overline{\mathbb{Q}}}, \mathcal{L}_x(D_0)) = 1$.

証明. 任意の $x \in V$ に対して，$\overline{\mathbb{Q}}$ の l 上にある素点 λ で，x が λ で 0 に specialize するものが存在する．

このことと，$J_1(5l)_{\mathbb{Z}[\zeta_l]}$ の Neron model についての事実から．つまり，

$$J_{\mathbb{Z}[\zeta_l]} \coloneqq J_1(5l) \text{ の } \mathbb{Z}[\zeta_l] \text{ 上の Neron モデル}$$

とすると，V は $J_{\mathbb{Q}(\zeta_l)}$ 内の $\mathbb{F}$-ベクトル空間スキーム $\mathcal{V}_{\mathbb{Q}(\zeta_l)}$ の $\overline{\mathbb{Q}}$ 点集合である．$\mathcal{V}$ を $J_{\mathbb{Z}[\zeta_l]}$ での $\mathcal{V}_{\mathbb{Q}(\zeta_l)}$ の Zariski 閉包とする．このとき，$\mathcal{V}_{\mathbb{Q}(\zeta_l)}$ は有限局所自由 $\mathbb{Z}[\zeta_l]$ 加群．（参照：Gross [Gro90, § 12], Edixhoven [Edi92, § 6]）．

また，$\mathcal{V}_{\mathbb{Q}(\zeta_l)}$ の $\mathbb{F}$-ベクトル空間スキームの局所成分としての次元は，$f(T_l) \neq 0, = 0$ に応じて 1 もしくは 2 である．

よって，l 上の $\overline{\mathbb{Q}}$ の各素点に対して，ある $x \in V, x \neq 0$ が存在して x はその素点上 0 に特殊化する．仮定から $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))$ の像は $\mathrm{SL}(V)$ を含む．よって，$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))$ は $V \setminus \{0\}$ に推移的に作用する．

以上から，各 $x \in V$, $x \neq 0$ に対して，$\overline{\mathbb{Q}}$ の l 上のある素点が存在して，x はその素点で 0 に特殊化することが示された． □

注意 9.2.3. D_0 が $X_1(5l)_{\mathbb{Q}(\zeta_l)}$ 上にあることから，議論を $\mathbb{Q}$ 上ではなく，$\mathbb{Q}(\zeta_l)$ 上で行う必要がある．

$X_l \coloneqq X_1(5l)_{\mathbb{Q}}$, g_l を X_l の種数，$A_{\mathbb{Q}(\zeta_l)}$ を $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))$ 集合 V に対応する $\mathbb{Q}(\zeta_l)$ 代数とする．

命題 9.2.2 より，各 $x \in V$ に対して一意的に，因子 $D_x = \sum_{i=1}^{g_l} Q_{x,i}$, で $x = [D_x - D_0]$ となるものが定まる（最後の等式は $J_l(\overline{\mathbb{Q}})$ でのもの）．

この D_x を，

$$D_x = D_x^{\mathrm{fin}} + D_x^{\mathrm{cusp}},$$

ただし D_x^{fin} はサポートがカスプと素なもの，D_x^{cusp} はサポートが $X_1(l)_{\overline{\mathbb{Q}}}$ のカスプに乗っているもの，とする．

補題 9.2.4 ([EC11, 8.2.6])．上の状況で，

$$V \ni x \mapsto D_x^{\mathrm{fin}} \in \mathrm{Div}(X_{l,\overline{\mathbb{Q}}})$$

は単射で，かつ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))$ 同変写像である．

証明．結論を否定して，$x_1, x_2 \in V$, $x_1 \neq x_2$ で $D_{x_1}^{\mathrm{fin}} = D_{x_2}^{\mathrm{fin}}$ なるものが存在したとする．V で $x_1 - x_2 \neq 0$ である．$D_{x_1} - D_{x_2}$ はカスピダル因子であることに注意する．また，X_l のカスプは $\mathbb{Q}(\zeta_l)$ 上有理的である．よって，$x_1 - x_2$ を用いて，次の単射 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))$ 同変射を定義することができる（$\mathbb{F}$ への $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))$ の作用は自明とする）：

$$\mathbb{F} \ni a \mapsto a(x_1 - x_2) = a(D_{x_1} - D_{x_2}) \in V.$$

包含制限原理により，ゼロでない射

$$\mathbb{F}[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))] \to V$$

が得られるが，V の既約性から全射．すると，$\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(V)$ の像が Abel になる．ρ は奇だから，$\rho(c)$,（c は複素共役）の異なる二つの固有値に応じて，表現が 1 次元空間の直和になるが，これは ρ の既約性に反する．

同変写像であること：$X_{l,\overline{\mathbb{Q}}}$ のカスプは，$\overline{\mathbb{Q}}$ 安定集合である．よって，任意の $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))$ に対して，

$$D_{gx}^{\mathrm{fin}} = gD_x^{\mathrm{fin}}, \quad D_{gx}^{\mathrm{cusp}} = gD_x^{\mathrm{cusp}}.$$

よって写像の同変性が従う． □

次の目標は，$f_l\colon X_l \to \mathbb{P}^1\mathbb{Q}$ という関数を作ることである．この関数によって，$\{ D_x^{\mathrm{fin}} \mid x \in V \}$ を，単射かつ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))$ 同変に，$\{ f_{l,*}D_x^{\mathrm{fin}} \mid x \in V \} \subset \mathrm{Div}(\mathbb{A}^1_{\mathbb{Q}})$ に写す．

9.3 $P(T)$ の構成

本節では，式 (9.1) の $P(T)$ を，$P(T) = P_{D_0,f_l,m}(T) \in \mathbb{Q}(\zeta_l)[T]$ として構成し，その係数の高さに関する評価を述べる．

Edixhoven-Couveignes [EC11] の記述とは逆に，最終的に構成されるべき $P_{D_0,f_l,m}(T)$ の構成をさかのぼっていく方向で説明する．

まず，$P_{D_0,f_l,m}(T)$ は

$$P_{D_0,f_l,m}(T) \coloneqq \prod_{x\in V}(T - a_{D_0,f_l,m}(x))$$

とする．ここで $a_{D_0,f_l,m}\colon V \to \overline{\mathbb{Q}}$ は，整数 m を，$0 \le m \le g(\#\mathbb{F})^4$ の範囲で適切に（$a_{D_0,f_l,m}$ が単射になるように）とって，

$$a_{D_0,f_l,m}(x) \coloneqq P_{D_0,f_l,x}(m) \in \overline{\mathbb{Q}}$$

とする．

ここで $P_{D_0,f_l,x}(t)$ は，

$$P_{D_0,f_l,x}(t) \coloneqq \prod_{i=1}^{d_x}(t - f_l(Q_{x,i})) \in \overline{\mathbb{Q}}[t]$$

である．$Q_{x,i}$ は，$D_x^{\mathrm{fin}} = \sum_{i=1}^{d_x} Q_{x,i}$ で定める．このとき，補題 9.2.4 から，$x \mapsto P_{D_0,f_l,x}(t)$ は単射で $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_l))$ 同変である．

最後に，$f_l\colon X_1(5l) = X_l \to \overline{\mathbb{Q}}$ を，$f_l = b_l + nx_l'$ が次の条件を満たすようにとる：

- b_l, x_l' は，$Y_1(5l)_{/\mathbb{Z}[1/5l]}$ 上の関数で，$Y_1(5l)_{/\mathbb{Z}[1/5l]}$ のモジュライとしての解釈から定まるもの（(9.5) 参照）
- $n \in \mathbb{Z}$ は，$x \in V$ が動いたとき，$f_{l,*}D_x^{\mathrm{fin}}$ が相異なるようにとる（そのようにとれる）

b_l, x_l' は以下のようにとる．$Y_1(5l)$ は $\mathbb{Z}[1/5l]$ 上定義されるのだった．任意の $\mathbb{Z}[1/5l]$ 代数 A について，$Q \in Y_1(5l)(A)$ が（$Y_1(5l)$ のモジュライ解釈から）$Q \leftrightarrow (E, P_5, P_l)$ と対応するとする．ここで，E は A 上の楕円曲線，$P_5 \in E(A)$ は位数 5 の点，$P_l \in E(A)$ は位数 l の点．

このとき，$b_l(Q) \in A$ は，$(E/A, P_5)$ が

$$\begin{cases} E/A\colon y^2 + (b_l(Q)+1)xy + b_l(Q)y = x^3 + b_l(Q)x^2, \\ P_5 = (0,0) \end{cases} \tag{9.5}$$

となるものである．また x_l' は，上の表示で $P_l = (x_l(Q), y_l(Q))$ と書いたときに，

$$l^{-1}P_5 + P_l = (x_l'(Q), y_l'(Q)),$$
$$l^{-1}P_5 = R, \quad P_5 = lR \text{ となる } E[5](A) \text{ の唯一の点},$$

によって定める．

注意 9.3.1. $(b_l, x'_l)\colon Y_1(5l)_{\mathbb{Z}[1/5l]} \to \mathbb{A}^2_{\mathbb{Z}[1/5l]}$ は埋め込みになる.

定理 9.3.2 ([EC11, 11.7.6]). $P_{D_0,f_l,m}(T) = \sum_{i=1}^{\#V} P_j T^j \in \mathbb{Q}(\zeta_l)[T]$ を上で構成したものとする. このとき, P_j の高さ $h(P_j)$ について次の評価が成立する:

$$h(P_j) \leq c l^{14} (\#\mathbb{F})^2,$$

ここで c は絶対定数であり, 不等式は任意の l, V, D_0, f_l, m に対して成立する.

この主張の証明については, 内田氏の報告 [内 18, 定理 10.3.1] を参照のこと.

9.4 計算量

k を $2 < k$ なる整数, l は素数で $l > 6(k-1)$ なるもの, $\mathbb{F}$ は標数 l の有限体, $f\colon \mathbb{T}(1,k) \to \mathbb{F}$ は全射とする. 計算したいのは, ρ_f である.

実際には, $f_2\colon \mathbb{T}(l,2) \to \mathbb{F}$ を, $f_2(T_m) = f(T_m)$, $1 \leq m \in \mathbb{Z}$ を満たす唯一の環準同型とすると, ρ_f を実現する V_f は,

$$V_f \coloneqq \bigcap_{1 \leq i \leq r} \ker(t_i, J_1(l)[l](\overline{\mathbb{Q}})) \tag{9.6}$$

で与えられるのだった ($\{t_1, \ldots, t_r\}$ は $\ker(f_2)$ の生成系. $r = (l^2-6)/6$ であることが示される.). 実際に計算されるのは, V_f を $B^*_{5l,l,1}$ で $J_1(5l)$ に送った

$$W_f \coloneqq B^*_{5l,l,1}(V_f) \subset J_1(5l)(\overline{\mathbb{Q}}).$$

(この空間については, 横山氏の論説 [Yok15] 参照).

結論は次のようになる:

定理 9.4.1 ([EC11, 12.10.7, 12.14.1]). 次のような確定的アルゴリズムが存在する:

入力 精度パラメタ $m \in \mathbb{Z}$, $1 \leq m$, 整数 $k \geq 2$, l は素数で $l > 6(k-1)$ なるもの, $\mathbb{F}$ は標数 l の有限体, $f\colon \mathbb{T}(1,k) \to \mathbb{F}$ は全射とする. また, Ω を $X_1(5l)$ 上のカスピダル因子 (定理 9.2.1 で構成したもの), $\exp(-m)$ の精度で計算した各 $x \in W_f$,

仮定 $\mathrm{Im}(\rho_f) \supset \mathrm{SL}(V_f)$,

出力 1. 各 $x \in W_f$ に対する $Q'_x = \sum_{n=1}^{g} Q'_{x,n}$, つまり, Ramanujan 因子 Q_x, $Q_x - \Omega \in [x]$) で, $d_{\mathrm{Sym}^g X}(Q_x, Q'_x) \leq \exp(-m)$ なるもの, ただし各 Q'_x は, 対 $(r,q) \in \Xi \times F_{w_r}$ で与えられる. $F_{w_r} \subset D(0, \exp(-\pi/w_r))$ は [EC11, 12.1.1] 参照のこと.

2. 各 $x \in W_f$ に対する，次数 g の（一意に定まる）正因子 Q_x で，$Q_x - \Omega \in [x]$ となるもの．ただし Q_x は，$Q_x = Q_x^{\mathrm{cusp}} + Q_x^{\mathrm{fin}}$ と書いたとき，$Q_x^{\mathrm{fin}} = \sum_i Q_{x,i}^{\mathrm{fin}}$, $Q_{x,i}^{\mathrm{fin}}$ は $X_1(5l)$ の平面モデル C_l のアフィン座標 $(b(Q_{x,i}), x(Q_{x,n}))$ の複素数近似として与えられる．

実行時間 (1), (2) の実行時間は，絶対定数 Θ が存在して，$(m\#V_f)^{\Theta}$ で押さえられる．

この結果は，[EC11, Chap. 11] で，Riemann 面 $X_1(5l)$ 上の様々な量の詳細な評価などを組み合わせて証明される．

9.5 結論

定理 9.5.1 ([EC11, Thm. 14.1.1]). $k > 0$, 有限体 $\mathbb{F}$, 全射準同形 $f\colon \mathbb{T}(1,k) \to \mathbb{F}$ で，付随する Galois 表現 $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ は可約か，または $\mathrm{SL}_2(\mathbb{F})$ を含むとする．

このとき，k と $\#\mathbb{F}$ についての確定的多項式時間アルゴリズムで，次の性質を満たすものを具体的に与えることができる：f を，$\{ f(T_i) \mid i = 1, 2, \ldots, [k/12] \}$ として入力する．出力として，

1. $\ker\rho$ に Galois 理論によって対応する $\mathbb{Q}$ の有限次 Galois 拡大 K を，$\mathbb{Q}$ 代数として $K = \sum_i \mathbb{Q}e_i$ として与える e_i と，それらの乗積表 $e_i e_j = \sum_k a_{i,j,k} e_k$,
2. $\mathrm{Gal}(K/\mathbb{Q})$ の元の K への作用を与える，$\{ e_i \}$ に関する行列表示,
3. $\mathrm{Gal}(K/\mathbb{Q}) \subset \mathrm{GL}_2(\mathbb{F})$ と見なしたときの，$\mathrm{Gal}(K/\mathbb{Q})$ の 2 次の行列表示,

ここで $K/\mathbb{Q}$ は，$\mathbb{F}$ の標数 l の外で不分岐で，素数 $p \neq l$ に対しては，$\mathbb{F}$ での次の等式が成り立つ：

$$\mathrm{tr}(\rho(\mathrm{Frob}_p)) = f(T_p), \quad \det(\rho(\mathrm{Frob}_p)) = p^{k-1}.$$

ただし，アルゴリズムの実行時間を完全に明示的に与えることは困難である．これは，例えば定理 9.3.2 の実行時間の評価などにあらわれる定数を，完全に明示的に与えることからくる．

定理 9.5.1 と同じ状況で，ρ が既約の場合を考える．次の命題により，重さが $l+1$ 以下の場合に帰着される：

命題 9.5.2 ([EC11, Prop. 14.3.1], [Edi92, Th. 3.4]). $2 \leq k' \leq l+1$ なる整数 k' と，$f'\colon \mathbb{T}(1,k') \to \mathbb{F}$ なる全射，$i \in \mathbb{Z}/(l-1)\mathbb{Z}$ が存在して，$\rho \cong \rho' \otimes \chi_l^i$. ただし，$\rho'\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ は f' に付随する Galois 表現，χ_l は法 l 円分指標.

この命題の k', f', i は，次のようにして具体的な手続きで得られる．

1. $2 \leq k' \leq l+1$ なる各 k' について，$\mathbb{F}_l$ 代数 $\mathbb{F}_l \otimes \mathbb{T}(1,k')$ を計算する．
2. 各 $i \in \mathbb{Z}/(l-1)\mathbb{Z}$ と，各 $2 \leq k' \leq l+1$ について，次の線型写像が存在するか否かを決定する：

$$\mathbb{F}_l \otimes \mathbb{T}(1,k') \to \mathbb{F}, \quad T_m \mapsto m^{-i} f(T_m), \quad 1 \leq m \leq \frac{l^2+1}{12},\ l \nmid m.$$

3. もしそのような線型写像があれば，それは $\mathbb{F}_l$ 代数の射である．

従って，定理 9.5.1 の ρ の計算は，ρ' についての計算に帰着される．このとき ρ' は，$J_1(l)[l](\overline{\mathbb{Q}})$ 内に，式 (9.6) のように実現される．

9.5.1 V の計算

定理 9.4.1 により，ρ' を実現する V の解析的な記述が得られている．任意の埋め込み $\sigma\colon \mathbb{Q}(\zeta_l) \to \mathbb{C}$ に対して，D_x の σ による埋め込みの近似 $D_{\sigma,x}$ が，$\#\mathbb{F}$ と，必要な桁数（精度）の多項式時間で計算できる．これらの近似は，$X_l(\mathbb{C})$ の点 $Q_{\sigma,x,i}$ の g_l 個の和として与えられ，また，$1 \leq i \leq g_l$ の番号付けと σ とは相互に無関係に取れる．

同様にして，$b_l(Q_{x,i})$, $x'_l(Q_{x,i})$ などは，$\#\mathbb{F}$ と必要な桁数（精度）の多項式時間で計算できる．

これらの近似値から，どの (σ,x,i) に対して $Q_{\sigma,x,i}$ がカスプを近似するかを計算することができる（詳細は省略するが，j 不変量の逆数の零点を b_l で記述する結果を用いる：[EC11, Prop. 8.2.8]）．この結果から，$D^{\mathrm{fin}}_{\sigma,x} = \sum_{i=1}^{d_x} Q_{\sigma,x,i}$ の d_x も求められる．

整数 n を，$0 \leq n \leq l^4(\#\mathbb{F})^4$ の範囲で，$f_l = b_l + nx'_l$ が $Q_{x,i}$ を単射に埋め込むように取るには，一つの埋め込み $\sigma\colon \mathbb{Q}(\zeta_l) \to \mathbb{C}$ を取って，異なる $Q_{\sigma,x,i}$, $Q_{\sigma,y,j}$ に対して f_l の像が異なるようになるまで，n を動かしてチェックすればよい．m の取り方も同様である．この n, m の取り方が計算時間に与える寄与は，議論にあらわれる点の高さの評価から見積もることができる．

さらに，定理 9.3.2 から

$$P(T) = P_{D_0,f_l,m}(T) = \sum_{i=1}^{\#V} P_j T^j \in \mathbb{Q}(\zeta_l)[T]$$

の係数の高さは $h(P_j) \leq cl^{14}(\#\mathbb{F})^2$ と押さえられる．P_j を $\mathbb{Q}(\zeta_l)$ の $\mathbb{Q}$ 基底 $\{\,\zeta_l^i \mid i = 0,\dots,l-2\,\}$ で書いて

$$P_j = \sum_{i=0}^{l-2} P_{j,i}\zeta_l^i, \quad P_{j,i} \in \mathbb{Q}$$

を求めるため，$\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ で添え字づけられた連立一次方程式

$$\sum_{i=0}^{l-2} P_{j,i}\sigma(\zeta_l^i) = \sigma(P_j)$$

を考える．代数体における高さ関数 h の性質（[EC11, lem 4.2.6]）などから，

$$h(P_{j,i}) \leq l\log l + lh(P_j) = O(l^{15}(\#\mathbb{F})^2).$$

従って，$P_{j,i}$ を近似値から求めるには，$O(l^{15}(\#\mathbb{F})^2)$ だけの精度があればよい．

以上のように，$\mathbb{C}$ 上の近似計算から $A_{\mathbb{Q}(\zeta_l)} = \mathbb{Q}(\zeta_l)[T]/(P(T))$ を計算することができ，その計算量も見積もることができる．

9.5.2 V の演算の復元

$\mathbb{Q}(\zeta_l)$ 代数 $A_{\mathbb{Q}(\zeta_l)} = \mathbb{Q}(\zeta_l)[T]/(P(T))$ から，ベクトル空間 $V_{\mathbb{Q}(\zeta_l)}$ の演算を復元しなければならない（[EC11, § 14.5]）．V の加法は $A_{\mathbb{Q}(\zeta_l)}$ の余加法

$$+^*\colon A_{\mathbb{Q}(\zeta_l)} \to A_{\mathbb{Q}(\zeta_l)} \otimes_{\mathbb{Q}(\zeta_l)} A_{\mathbb{Q}(\zeta_l)} = \mathbb{Q}(\zeta_l)[U,V]/(P(U),P(V))$$

から得られる．これは，$A_{\mathbb{Q}(\zeta_l)}$ の生成元 a の，余加法での像を与えることと同値である．この像は，U,V の高々 $(\#\mathbb{F})^2$ 次の多項式である．よって，

$$a(x+y) = \sum_{i,j} \mu_{i,j} a(x)^i a(y)^j, \quad x,y \in V$$

となる $\mu_{i,j}$ を，各 $x \in V$ に対しての $a(x+y), a(x), a(y)$ が既知として求めればよい．

スカラー倍 $\mathbb{F} \times V \to V$ を $A_{\mathbb{Q}(\zeta_l)}$ の余スカラー倍から復元もほぼ同様である．

また，$A_{\mathbb{Q}(\zeta_l)}$ から $\mathbb{Q}$ 代数 A を抽出しなければならない（[EC11, § 14.6]）．これには，

$$A = \left\{ x \in A_{\mathbb{Q}(\zeta_l)} \;\middle|\; \tau(x) = x,\ \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}) \right\}$$

という関係を使う．

$A_{\mathbb{Q}(\zeta_l)}$ の生成元 a を，D_0 も明記して a_{D_0} と書く．a_{D_0} への $G = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ への作用は，$\tau \in G$ に対して

$$\tau(a_{D_0}) = a_{\tau(D_0)}.$$

埋め込み $\sigma\colon \mathbb{Q}(\zeta_l) \to \mathbb{C}$ と $x \in J_l(\mathbb{C})$ に対して，$a_{\sigma,D_0}(x)$, $a_{\sigma,\tau D_0}(x)$ をそれぞれ近似計算で得られた値とする．

生成元（原始根）$\tau \in G \cong \mathbb{F}_l^\times$ を固定する．すると，$\{\, c_i \,\} \subset \mathbb{Q}(\zeta_l)$ が一意に定まり，

$$\tau(a) = \sum_i c_i a^i.$$

これら $\{\, c_i \,\}$ は，$\overline{\mathbb{Q}}$ 内の方程式

$$a_{\tau D_0}(x) = \sum_{i=0}^{(\mathbb{F})^2-1} c_i a_{D_0}(x)^i, \quad x \in V$$

で特徴づけられる．$h(c_i) = O(l^{14}(\#\mathbb{F})^6)$ という評価（[EC11, lem. 4.2.6]）があるので，$c_i = \sum_{j=0}^{l-2} c_{i,j}\zeta_l^j$, $c_{i,j} \in \mathbb{Q}$ と書けば，$h(c_{i,j}) = O(l^{15}(\#\mathbb{F})^6)$．よって $\mathbb{C}$ 上での近似値 $a_{\sigma,D_0}(x)$, $a_{\sigma,\tau D_0}(x)$ から，A が抽出できる．

最後に，V への $G_\mathbb{Q}$ 作用を復元する（[EC11, § 14.7]）．$V \times V \cong \mathrm{Hom}_\mathbb{F}(\mathbb{F}^2, V)$ という同型の左辺には $\mathrm{GL}_2(\mathbb{F})$ が右から作用し，よって $A \times A$ には左から作用する．この作用は $A \times A$ の余加法と $\mathbb{F}^\times$ 作用で記述できる．B を，$\mathrm{Isom}_\mathbb{F}(\mathbb{F}^2, V) \subset \mathrm{Hom}_\mathbb{F}(\mathbb{F}^2, V)$ に対応する $\mathbb{Q}$ 代数とする．

$A \times A$ の idempotent，つまり $A \otimes A$ の元で，$\mathrm{Isom}(\mathbb{F}^2, V)$ 上 1，その補集合で 0 となる元を構成する．$A_{\mathbb{Q}(\zeta_l)} = \mathbb{Q}(\zeta_l)[T]/((1-T)P_l(T))$ と書いて，$a_1 = P_l/P_l(1)$ とすると，これは $\{\, 0 \,\} \subset V$ の特性関数である．よって $a_1 \in A$ となり，ここから $a_2 = 1 - a_1$ とすると a_2 は $V \setminus \{\, 0 \,\}$ の特性関数．さらに $a_3 \in A \otimes A$ を，

$$a_3 \coloneqq \prod_{g \in \mathrm{GL}_2(\mathbb{F})} g(a_2 \otimes 1)$$

とすると，a_3 は $\mathrm{Isom}(\mathbb{F}^2, V)$ の特性関数になる．すると，$\mathbb{Q}$ 上の線形代数と $\mathrm{GL}_2(\mathbb{F})$ 作用から，$B = (A \otimes A)/(1 - a_3)$ が計算できる．

また，B を体の直和に分解することは，LLL アルゴリズムを用いて多項式時間で可能である（Artin 代数の計算については，Vasconcelos [Vas98, Chap. 4] 参照．また LLL アルゴリズムについては [Coh93, Chap. 2] 参照）．B の成分であるそれぞれの体 K は ρ の核が固定する体で，$G \subset \mathrm{GL}_2(\mathbb{F})$ を（一つ選んだ体）K の固定部分群とすると $G = \mathrm{Gal}(K/\mathbb{Q})$ であり，$G \subset \mathrm{GL}_2(\mathbb{F})$ が G の 2 次元線形表現である．

以上で定理 9.5.1 の証明が終わった．

参考文献

[Coh93] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993. MR 94i:11105

[EC11] Bas Edixhoven and Jean-Marc Couveignes (eds.), *Computational aspects of modular forms and Galois representations*, Annals of Mathematics Studies, vol. 176, Princeton University Press, Princeton, NJ, 2011, How one can compute in polynomial time the value of Ramanujan's tau at a prime. MR 2849700

[Edi92] Bas Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594. MR 1176206

[Gro90] Benedict H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. **61** (1990), no. 2, 445–517. MR 1074305

[Hid12] Haruzo Hida, *Geometric modular forms and elliptic curves*, second ed., World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012. MR 2894984

[Vas98] Wolmer V. Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, Algorithms and Computation in Mathematics, vol. 2, Springer-Verlag, Berlin, 1998, With chapters by David Eisenbud, Daniel R. Grayson, Jürgen Herzog and Michael Stillman. MR 1484973

[Yok15] Shun'ichi Yokoyama, *Introduction to the computational theory of elliptic modular forms*, Algebraic number theory and related topics 2013, RIMS Kôkyûroku Bessatsu, B53, Res. Inst. Math. Sci. (RIMS), Kyoto, 2015, pp. 279–304. MR 3525179

[横 18] 横山俊一, 特別な楕円モジュラー形式の高速計算理論について, 本報告集.

[内 18] 内田幸寛, 高さと *Arakelov* 理論，それらの *Galois* 表現の計算への応用, 本報告集.

[木 18] 木村巌, 楕円モジュラー形式の導入, 本報告集.