8.

特別な楕円モジュラー形式の高速計算理論について

横山 俊一[*1]（九州大学）

本稿は，第 25 回整数論サマースクール「楕円曲線とモジュラー形式の計算」における筆者の火曜午後の同題目の講演に基づいている．ここでは Edixhoven-Couveignes らによって開発された，特定の楕円モジュラー形式の高速計算の理論 [EC11] を俯瞰する（計算の正当性については，本報告集の木村巌氏の原稿を参照いただきたい）．

Edixhoven-Couveignes の理論の概説については，拙稿 [Yok16] がサーベイ原稿として出版されている．ここではより簡潔に，全体の概略を述べることにする．また，[EC11] に対する山内卓也氏の書評 [Yam15] が出版されているので，こちらも参考にされたい．

8.1 主定理

$M_k(\Gamma_1(N))$ を $\mathbb{Q}$ 上レベル N, 重さ k のモジュラー形式の空間とする．また

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod N \right\}$$

をレベル N の合同部分群とよぶ．とくに $\Gamma_1(1) = \mathrm{SL}_2(\mathbb{Z})$ である．各モジュラー形式 $f(z) \in M_k(\Gamma_1(N))$（$z \in \mathfrak{h}$：上半平面）は Fourier 級数展開を持ち

$$f = \sum_{n \geq 0} a_n q^n \quad \left(q = e^{2\pi i z}\right)$$

[*1] 本稿に関連する研究は JSPS 科研費 JP15K17515 の助成を受けたものです．
This work is supported by JSPS KAKENHI Grant Number JP15K17515.

と書ける．$a_0 = 0$ となる f を尖点形式 *cusp form* とよび，これらのなす空間を $S_k(\Gamma_1(N))$ と書く．

$M_k(\Gamma_1(N))$, $S_k(\Gamma_1(N))$ には Hecke 作用素とよばれる線型変換が導入される．n 番目の Hecke 作用素を T_n と書き，その作用を

$$T_n f = \sum_{m \geq 0} \left(\sum_{1 \leq d | \gcd(m,n)} d^{k-1} a_{mn/d^2} \right) q^m$$

と定義する．このとき全ての $n \geq 1$ に対して

$$T_n f = a_n f, \quad a_1 = 1$$

となるような f を正規化固有形式 *normalized eigenform* とよぶ．とくに $\mathbb{Q}$ 上レベル 1, 重さ 12 の正規化固有形式 $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ は唯一つ存在し，これを Δ と書いて discriminant form とよぶ．この n 番目の Fourier 係数は Ramanujan's tau $\tau(n)$ である：

$$\Delta = \sum_{n=1}^{\infty} \tau(n) q^n = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \cdots .$$

ここで Hecke 作用素 T_n は次の関係式をみたす：

$$T_{mn} = T_m T_n, \; T_{p^r} = T_{p^{r-1}} T_p - p^{11} T_{p^{r-2}}.$$

但し r, m, n は自然数で $\gcd(m,n) = 1$, p は素数である．従って素数番目の Hecke 作用素 T_p がどの程度の時間で計算出来るのかを調べることが本質的である．

このような背景から，R. Schoof は「$\tau(p)$（つまり T_p）が $\log p$ の多項式時間で計算可能か？」という問題を B. Edixhoven に提案したとされる．[EC11] は，この問題に対する肯定的解答を与えたものである．

定理 8.1.1 (Edixhoven-Couveignes et al.)．$\tau(p)$ は $\log p$ の多項式時間で計算可能である．

正確には，[EC11] で提案されているアルゴリズムは $\tau(p) \bmod \ell$（$p \neq \ell$, ℓ は素数）を計算するものである．これらがおよそ $\log p$ 以下の全ての素数 ℓ に対して求まれば，中国剰余定理により $\tau(p)$ の本来の値が求まる[*2]．

この結果は，直接的にモジュラー形式の空間を計算するのではなく，別の数学的対象を経由して効率的な計算を行うテクニックによって得られている．具

[*2] しかし主定理の強みは，p が 10^{1000} 程度の非常に大きなオーダーであっても $\tau(p) \bmod \ell$ が計算できるという所にある．この場合，実際の計算機資源の限界から ℓ の上限はおよそ 40 程度であることが知られている（2018 年 1 月現在）．

体的には mod ℓ Galois 表現を経由する．しかし mod ℓ Galois 表現そのものを計算するのは一般には容易ではない．

この方面でよく知られている手法の一つが Schoof のアルゴリズム [Sch85], [Sch95] である．これは，有限体 $\mathbb{F}_q$（q は素数べき）上の楕円曲線（より一般には代数曲線，およびそのヤコビ多様体）の有理点の個数 $E(\mathbb{F}_q)$ を高速に数え上げるアルゴリズムである．具体的には，楕円曲線の有理点そのものを直接攻めるのではなく，ℓ 等分点全体 $E(\mathbb{F}_q)[\ell]$ を考える．このとき $E(\mathbb{F}_q)[\ell]$ の構造は（$\mathbb{Z}/\ell\mathbb{Z}$-ベクトル空間として）よく分かっているので，幾何的フロベニウス元 Frob_q のトレースを計算し，最後に中国剰余定理を用いて復元するのである．これを改良したものが SEA（Schoof-Elkies-Atkin）アルゴリズムであり，本報告集の安田雅哉氏の解説で述べられている．

いま問題としている $\tau(p)$ の計算は，比較的高次（具体的には 11 次）の代数多様体の有理点の個数の計算に帰着される．とくに幾何的フロベニウス元 Frob_q は絶対 Galois 群 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の元として定まる．その mod ℓ Galois 表現による像のトレースをとったものが $\tau(p) \bmod \ell$ に一致する，という筋書きである．しかし，Schoof のアルゴリズムが適用できるとはいえ，高次の代数多様体上の有理点の計算が容易であるとは到底思えない．

そこで Edixhoven-Couveignes は mod ℓ Galois 表現をさらに “Ramanujan space” とよばれる空間に置き換えて計算を行う手法を提案した．この手法では計算量を削減するために「近似」の手法を用いる．これについて次章で具体的に解説する．

8.2 Edixhoven-Couveignes 理論の概要

まず，先ほど述べた主張を少し詳しい形で述べる．以降は [Yok16] の 3 章以降の多くと重複していることをお断りしておく．

定理 8.2.1 (Edixhoven-Couveignes et al., [EC11] 系 15.2.2)．$f = \sum_{n\geq 0} a_n q^n$ をレベル 1，重さ k のモジュラー形式とする．このとき重さ k と $a_i \in \mathbb{Z}$ $(0 \leq i \leq k/12)$ が与えられたとき，$a_n \in \mathbb{Z}$ を計算する確定的アルゴリズム[*3]が存在する．計算時間は k を一つ固定した場合 $\log n$ と $\max_{0\leq i\leq k/12} \log(1+|a_i|)$ の多項式時間となる．また GRH（一般 Riemann 予想）を仮定すれば k についても多項式時間となる．

[*3] 確定的アルゴリズム *deterministic algorithm* とは，大雑把に言えば「同じ入力に対して（実時間で計算可能かどうかはともかく）同じ出力を与えるアルゴリズム」のことである．これに対して「同じ入力に対して異なる出力を与える可能性のあるアルゴリズム」を確率的アルゴリズム *probabilistic algorithm* とよぶ．後者は素数判定アルゴリズムなどで知られている．一般に，確定的アルゴリズムよりも確率的アルゴリズムの方が早い時間で終了する．

続いて主定理を支える主張を二つ述べる．一つ目は Galois 表現の計算に関する定理である．以下では Hecke 作用素 T_n（$n \in \mathbb{N}$）で生成される $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_1(N)))$ の $\mathbb{Z}$ 部分代数を $\mathbb{T}(N,k)$ と書き Hecke 環とよぶ．$\mathbb{T}(N,k)$ は有限生成となる．

定理 8.2.2 ([EC11] 定理 14.1.1)．重さ k，有限体 $\mathbb{F}$ と，Hecke 環から $\mathbb{F}$ への全射 $f : \mathbb{T}(1,k) \to \mathbb{F}$ が与えられているとする．f に付随する Galois 表現 $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ を考え，これが可約または $\mathrm{Im}(\rho) \supset \mathrm{SL}_2(\mathbb{F})$ であるとする．このとき ρ を計算するための確定的アルゴリズムが存在する．計算時間は k と $\#\mathbb{F}$ に関する多項式時間となる．

具体的に「ρ を計算する」とはどういうことか述べておく．簡単のため $\mathbb{F} = \mathbb{F}_\ell$ とし $\rho = \rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ を Δ に付随する mod ℓ Galois 表現とする．このとき Serre と Swinnerton-Dyer の結果から，$\ell \notin \{2,3,5,7,23,691\}$ ならば自動的に $\mathrm{Im}(\rho_\ell) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$，即ち $\mathrm{Im}(\rho_\ell)$ は非可解となる．このときは類体論による既存の計算手法が適用出来ない[*4]．そこで別の戦略を考える．

今 $\mathrm{Im}(\rho_\ell)$ は有限であるから，$\ker \rho_\ell$ に Galois 理論で対応する体 K_ℓ を考えると，$K_\ell/\mathbb{Q}$ は有限次拡大体，即ち代数体となる．このアルゴリズムではまず K_ℓ を $\mathbb{Q}$-代数として生成元 $\{e_i\}$ を求め，乗積表 $e_i e_j = \sum_k a_{i,j,k} e_k$ を計算する．更に $\rho_\ell(\mathrm{Frob}_p)$ を $\mathrm{GL}_2(\mathbb{F}_\ell)$ の元として計算する．結果 $p \neq \ell$ なる全ての p に対して

$$\mathrm{Tr}(\rho_\ell(\mathrm{Frob}_p)) = f(T_p),\ \det(\rho_\ell(\mathrm{Frob}_p)) = p^{11} \bmod \ell$$

が成り立つ．このとき $\rho_\ell(\mathrm{Frob}_p)$ は ℓ と $\log p$ の多項式時間で計算出来る．

ρ_ℓ の計算は次のように行う．まず Ramanujan subspace とよばれる以下のような空間を考える：

$$V_\ell := \bigcap_{1 \le i \le \frac{\ell^2-1}{6}} \ker\left(T_i - \tau(i), J_1(\ell)(\overline{\mathbb{Q}})[\ell]\right).$$

ここで $J_1(\ell)$ はモジュラー曲線 $X_1(\ell) = (\Gamma_1(\ell)\backslash\mathfrak{h})^*$ のヤコビアンである．以降同じ記号を使って $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_\ell)$ とする．[EC11] では ρ_ℓ, 即ち V_ℓ の計算法を 2 通り提示している．具体的には 1) $\mathbb{C}$ 上近似の手法，2) mod p の手法，である．これについては [Yok16] の 4 節と 5 節でそれぞれ詳しく述べている．

例えば $\mathbb{C}$ 上近似の場合，大雑把に言えば次のような戦略をとる：

[*4] 逆にこれまでに知られていた $\tau(n)$ に関する合同関係式は $\ell \in \{2,3,5,7,23,691\}$ を法としたものである．例えば $\tau(n) \equiv \sigma_{11}(n) \bmod 691$（但し $\sigma_k(n) = \sum_{d|n} d^k$）はとくに有名である．

- 求める Galois 表現を，少しレベルを取り換えたモジュラー曲線の Jacobi 多様体の ℓ-等分点に実現する．
- Abel-Jacobi の定理により，Jacobi 多様体の元を因子とみなす．
- この因子を数値的に近似し，計算による誤差がないことを保証する．

代数幾何的手法を用いること，そして数値的に近似計算を行うことから，複素数体 $\mathbb{C}$ 上の理論が展開される．とくに V_ℓ の計算可能性を保証するためには Arakelov 理論が用いられる．これについては，本報告集の内田幸寛氏の解説を参照されたい．結論として，以下のような主張が示される（ここでは簡単のため $N=1, \mathbb{F}=\mathbb{F}_\ell$ の場合の主張のみ述べておく）．

定理 8.2.3 ([EC11] 定理 2.5.13)．k を重さとし $2 < k \leq \ell+1$ を仮定する．全射 $f : \mathbb{F}_\ell \otimes \mathbb{T}(1,k) \to \mathbb{F}_\ell$ を考え，更に f に付随する Galois 表現 $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ は絶対既約であるとする．このとき，全ての $i \geq 1$ に対して $f_2(T_i) = f(T_i)$ をみたすような全射 $f_2 : \mathbb{F}_\ell \otimes \mathbb{T}(\ell,2) \to \mathbb{F}_\ell$ が唯一つ存在する．ここで $\mathfrak{m}_f := \ker(f_2)$ とし，その生成元を $(t_1, \cdots, t_r)$ とおく．このとき

$$V_\ell = \bigcap_{1 \leq i \leq r} \ker(t_i, J_1(\ell)(\overline{\mathbb{Q}})[\ell])$$

は 2 次元 $\mathbb{F}$-ベクトル空間であり $V_\ell = \rho_\ell$ が成り立つ．

証明においては「レベルと重さの取り替え」が鍵となる．具体的には「レベル 1，重さ k」の固有形式に付随する mod ℓ Galois 表現が，実は「レベル ℓ，重さ 2」の固有形式にも付随するという性質が導かれる．そしてさらに「レベル 5ℓ，重さ 2」の固有形式にも付随するという性質を導き[*5]，この世界で近似計算を適用するという戦略がとられている．

以上により V_ℓ，即ち ρ_ℓ が計算出来たと仮定する．このとき $K_\ell = \overline{\mathbb{Q}}^{\ker(\rho_\ell)}$ はある多項式 $P_\ell \in \mathbb{Q}[X]$（特に Δ の場合は $P_\ell \in \mathbb{Z}[X]$）の最小分解体として得られる．この多項式 P_ℓ の決定については J. Bosman の手法 [Bos08] を用いる（これまで述べてきた $\mathbb{C}$ 上近似の手法，および Arakelov 理論と格子簡約 LLL アルゴリズムを利用する）．しかしこの P_ℓ の次数は ℓ^2-1，つまり ℓ の 2 乗の速度で増大する．故に K_ℓ はすぐに巨大な体となり扱えなくなってしまう[*6]．そこで ρ_ℓ を projective な表現 $\rho_\ell^{\mathrm{proj}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ に取り換えて同様の計算を行う．この場合にも $K_\ell^{\mathrm{proj}} = \overline{\mathbb{Q}}^{\ker(\rho_\ell^{\mathrm{proj}})}$ はある多項式 $P_\ell^{\mathrm{proj}} \in \mathbb{Q}[X]$（特に Δ の場合は $P_\ell^{\mathrm{proj}} \in \mathbb{Z}[X]$）の最小分解体として得られ，更に P_ℓ^{proj} の次数は $\ell+1$ まで落ちるので，計算可能なクラスの問題として扱うことが出来る．Bosman はこれらをもとに次のような戦略を考えた：

[*5] この「5 倍」という数字は代数幾何学的に “よい” 性質を与えるためのものである．

[*6] K_ℓ が増大することは包含関係 $\mathrm{Gal}(K_\ell/\mathbb{Q}) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$ からも分かる．

- 小さい素数 ℓ に対し $\mathrm{Gal}(K_\ell^{\mathrm{proj}}/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$ であることを実際に計算して確かめる[*7].
- $\alpha \in \overline{\mathbb{Q}}$ を P_ℓ^{proj} の根とする．このとき α を固定するような $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の部分群と，$\mathbb{P}^1(\mathbb{F}_\ell)$ のある点を固定するような $\mathrm{PGL}_2(\mathbb{F}_\ell)$ の部分群が $\rho_\ell^{\mathrm{proj}}$ を介して対応していることを示す（cf. [EC11] 定理 7.1.3）.
- $\mathbb{C}$ 上近似によって求めたこの $\rho_\ell^{\mathrm{proj}}$ が，本当に Δ に付随する projective Galois 表現であることを Serre の保型性予想を用いて保証する.

$\ell \geq 5$ のとき，上の一つ目から $\rho_\ell^{\mathrm{proj}}$ の絶対既約性が導かれる．更に $\rho_\ell^{\mathrm{proj}}$ が奇 *odd* であることも，モジュラー形式から来ていることから従う．そして Δ が属する尖点形式の空間 $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ の次元は（$\mathbb{C}$-ベクトル空間として）1 であるから Δ は唯一の固有形式となる．これら全てをみたしている状況下で，Serre の保型性予想 - 現在は Khare-Wintenberger の定理を適用する.

定理 8.2.4 (Khare-Wintenberger, [KW09]). $\mathbb{Q}$ 上の既約かつ奇な 2 次元 mod ℓ Galois 表現 ρ はモジュラーである．つまり type $(N(\rho), k(\rho), \varepsilon(\rho))$ の尖点固有形式から来る.

Bosman は重さ 12 の場合だけではなく $\dim_{\mathbb{C}} S_k(\mathrm{SL}_2(\mathbb{Z})) = 1$ となるもの全て，即ち $k = 16, 18, 20, 22, 26$ の場合についても計算を試みている[*8].

以上から，後は $\mathrm{Gal}(K_\ell/\mathbb{Q})$ の元 Frob_p がどの共役類に属するかを調べれば $\mathrm{Tr}(\rho_\ell(\mathrm{Frob}_p))$ を決定出来る（同じ共役類に属している限り $\mathrm{Tr}(\rho_\ell(\mathrm{Frob}_p))$ の値は不変である）．これについては，最近 Dokchitser 兄弟による，線形代数および多変数多項式の計算に帰着させる手法 [Dok13] が知られている.

* * *

続いて二つ目，Hecke 作用素の計算に関する定理を述べる.

定理 8.2.5 ([EC11] 定理 15.2.1). 重さ k，自然数 n とその素因数分解 $n = \prod_i p_i^{e_i}$ が与えられているとする．このとき n 番目の Hecke 作用素 $T_n \in \mathbb{T}(1, k)$ を計算する[*9]ための確定的アルゴリズムが存在する．計算時間は k を一つ固定した場合 $\log n$ の多項式時間となる．また代数体に関する GRH を仮定すれば k についても多項式時間となる.

先述の通り，T_n の計算は素数番目の Hecke 作用素 T_p の計算に帰着される．これを求めるために Hecke 環 $\mathbb{T}(1, k)$ に $\mathbb{Q}$ をテンソルして $\mathbb{Q}$-代数

[*7] Bosman は計算代数システム Magma の主要開発者の一人である．Magma において Galois 群を計算する場合，Stauduhar の相対分解式を用いたアルゴリズムが用いられる.

[*8] 但し $k = 26$ のときは $\ell = 29$ が最小となり，P_{29}^{proj} の次数（この場合 30）の大きさ故に計算することが出来なかった.

[*9] ここで「計算する」とは T_n を T_i（$1 \leq i \leq k/12$）の多項式で書き表すことを意味する.

$\mathbb{T}_{\mathbb{Q}} = \mathbb{T}(1,k) \otimes \mathbb{Q}$ を考える．このとき $\mathbb{T}_{\mathbb{Q}} = \prod_i K_i$ と有限個の代数体の積として書けるが，少なくとも [EC11] で扱われているケースでは 2 つ以上の代数体の積になることはない（その根拠として [FJ02] が引用されている）ため，[EC11] では唯一つの代数体 K での $\mathbb{T}(1,k)$ の像を A と書いて $\mathbb{T}(1,k)$ と同一視している（と思われる）．ここで素数 ℓ を含む A の極大イデアル $\mathfrak{m}$ をとると，写像 $\mathbb{T}(1,k) \to A/\mathfrak{m}$ から定まる mod ℓ Galois 表現での Frobenius 写像 Frob_p が計算出来る．これを ℓ と $\mathfrak{m}$ を取り替えて繰り返し行い，A における T_p の像を復元することで T_p を得る，という戦略である．代数体に関する GRH を仮定したのは，ℓ を動かす範囲とそれ毎に定まる $A/\mathfrak{m}$ の位数の評価に利用するためである．詳細な評価が幾つか得られており，例えば次の結果が役に立つ．

命題 8.2.6 (Weinberger, [Wei84])．K を代数体，$x \in \mathbb{R}$ とする．$\pi(x,K)$ を $\mathcal{O}_K$ の極大イデアル $\widetilde{\mathfrak{m}}$ で $\#(\mathcal{O}_K/\widetilde{\mathfrak{m}}) \leq x$ をみたすものの個数とする．このとき GRH を仮定すると，$x > 2$ に対してある定数 $c_1 \in \mathbb{R}$ が存在して次をみたす：

$$|\pi(x,K) - \mathrm{li}(x)| \leq c_1 \sqrt{x} \log\left(\mathrm{Disc}(\mathcal{O}_K) x^{\dim_{\mathbb{Q}} K}\right).$$

但し $\mathrm{li}(x) = \int_2^x (1/\log y) dy$（対数積分），$\mathrm{Disc}(\mathcal{O}_K)$ は整数環 $\mathcal{O}_K$ の判別式である．

この種の結果は Weinberger 以前にもあると推察されるが，詳しい出典は（少なくとも筆者には）特定出来なかった．この命題は [EC11] の記述に従って引用したものである．

* * *

最後に，実際に $\tau(p)$ が $\log p$ の多項式時間で計算可能であることに関して，詳細な計算量の見積もりを与える主張を紹介する．なおこの結果は $\mathbb{C}$ 上近似ではなく mod p の手法で得られたものである．

命題 8.2.7 (Zeng-Yin, [ZY15] 系 1.2 (2))．p を素数とする．このとき $\tau(p)$ は $O(\log^{6+2\omega+\delta+\epsilon} p)$ で計算出来る．

定数 ω は区間 $[2,4] \subset \mathbb{R}$ に含まれる．これはヤコビ多様体の群演算の困難性から来る定数で，具体的には $J_1(\ell)$ での見積もりは $O(g^\omega)$（$g = g(X_1(\ell))$）となる．ω の最良評価は Khuri-Makdisi [KM07] による $\omega = 2.376$ である．δ は 2 以上の定数であり，V_ℓ の計算困難性に依存する．δ の評価については，例えば [EC11] の 11 節を参照されたい．

8.3 計算例

まず Bosman による P_ℓ^{proj} のデータを示す.

ℓ	P_ℓ^{proj}
11	$x^{12} - 4x^{11} + 55x^9 - 165x^8 + 264x^7 - 341x^6 + 330x^5$ $-165x^4 - 55x^3 + 99x^2 - 41x - 111$
13	$x^{14} + 7x^{13} + 26x^{12} + 78x^{11} + 169x^{10} + 52x^9 - 702x^8 - 1248x^7$ $+494x^6 + 2561x^5 + 312x^4 - 2223x^3 + 169x^2 + 506x - 215$
17	$x^{18} - 9x^{17} + 51x^{16} - 170x^{15} + 374x^{14} - 578x^{13} + 493x^{12}$ $-901x^{11} + 578x^{10} - 51x^9 + 986x^8 + 1105x^7 + 476x^6 + 510x^5$ $+119x^4 + 68x^3 + 306x^2 + 273x + 76$
19	$x^{20} - 7x^{19} + 76x^{17} - 38x^{16} - 380x^{15} + 114x^{14} + 1121x^{13}$ $-798x^{12} - 1425x^{11} + 6517x^{10} + 152x^9 - 19266x^8 - 11096x^7$ $+16340x^6 + 37240x^5 + 30020x^4 - 17841x^3 - 47443x^2$ $-31323x - 8055$
23	$x^{24} - 2x^{23} + 115x^{22} + 23x^{21} + 1909x^{20} + 22218x^{19}$ $+9223x^{18} + 121141x^{17} + 1837654x^{16} - 800032x^{15}$ $+9856374x^{14} + 52362168x^{13} - 32040725x^{12} + 279370098x^{11}$ $+1464085056x^{10} + 1129229689x^9 + 3299556862x^8$ $+14586202192x^7 + 29414918270x^6 + 45332850431x^5$ $-6437110763x^4 - 111429920358x^3 - 12449542097x^2$ $+93960798341x - 31890957224$

先述の通り $k = 12$ の場合は $\ell \geq 11, \ell \notin \{23, 691\}$ という仮定があるので [EC11] には $\ell = 23$ の結果は掲載されていないが，Bosman はこの場合を含めて 5 個の ℓ に対して結果を得ている．またこれ以外にも $k = 16, 18, 20, 22$ に対しては次ページの ℓ に対して結果を得ている．これは尖点形式の空間の次元が 1 であるため，一意に固有形式が定まるからである[*10]．ちなみに上の表において P_{23}（proj でない）を実際に計算すると 528 次式となり，その係数は最大 2000 桁程度まで膨れ上がる．

[*10] 次元が 2 となる最小の k は 24 である．この場合も同様に P_ℓ^{proj} を計算することは可能であるが，$\mathbb{C}$ 上近似で求まった mod ℓ Galois 表現がどの固有形式から来るのかについては Edixhoven-Couveignes の方法では判定出来ない（そもそも彼らの手法はモジュラー形式自体の計算を「回避」するアイデアであった）．これについては最近 Mascot [Mas13] が新しい結果を得ている．

k	ℓ
16	$17, 19, 23$
18	$17, 19, 23$
20	$19, 23$
22	23

最終的に得られた $\tau(p) \bmod \ell$ の値をいくつか紹介しておく．この表は [EC11] の裏表紙にも掲載されている．

p	$\tau(p) \bmod 19$
$10^{1000} + 1357$	± 4
$10^{1000} + 7383$	± 2
$10^{1000} + 21567$	± 3
$10^{1000} + 27057$	0
$10^{1000} + 46227$	0
$10^{1000} + 57867$	0
$10^{1000} + 64749$	± 7

その後，Mascot は Edixhoven-Couveignes の手法では決定できなかった符号の確定までを可能とした（[Mas13], [MasTb]）．この手法は “quotient representation trick” と呼ばれている．

p	$\tau(p) \bmod 19$
$10^{1000} + 1357$	4
$10^{1000} + 7383$	2
$10^{1000} + 21567$	3
$10^{1000} + 27057$	0
$10^{1000} + 46227$	0
$10^{1000} + 57867$	0
$10^{1000} + 64749$	7

8.4 応用例

最後に，$\tau(p) \bmod \ell$ の高速計算の応用例として “Lehmer の非消滅予想” を紹介する．この $\tau(n)$ に関する予想は数十年前に提唱されて以来未解決であり，関連する整数論的な話題（Bernoulli 数やゼータ関数）とも深く関連する予想である．

予想 8.4.1 (Lehmer, [Leh47]). $n \geq 1$ に対して $\tau(n) \neq 0$ が成り立つ．

[Leh47] では $n < 3316799$ の範囲で検証されていたが，現時点（2018 年 1 月現在）では Derickx-van Hoeij-Zeng [Der13] による次の結果まで更新されている．

命題 8.4.2 (Derickx-van Hoeij-Zeng, [Der13] 系 1.2)．

$$n < 816212624008487344127999 \approx 8.16 \times 10^{23}$$

に対して Lehmer 予想は正しい．

証明のアイデアは，$\tau(p) = 0$ を仮定したときに p がみたすべき条件を定め，その対偶を考えるというものである．p がみたすべき条件としては次の Serre の規準が用いられる．

補題 8.4.3 (Serre, [Ser85])．$\tau(p) = 0$ とする．このとき次が成り立つ：

- $p \equiv -1 \bmod 2^{14}3^7 5^3 691$,
- $p \equiv -1, 19, 31 \bmod 7^2$,
- $\left(\frac{p}{23}\right) = -1$（左辺は Legendre 記号）．

対偶命題を考えることにより，それぞれの否定命題を一つでもみたせば $\tau(p) \neq 0$ が成り立つ．ここに $\tau(p) \bmod \ell$ の計算結果を組み合わせることで p を更に引き上げるというアイデアである．Derickx-van Hoeij-Zeng [Der13] では $\tau(p) \bmod 41$ の計算を成功させたことにより，記録を大幅に更新している．

参考文献

[Bos08] J. Bosman, Explicit computations with modular Galois representations, *Ph.D thesis*, Universiteit Leiden (2008), 112pp.

[Der13] M. Derickx, M. van Hoeij and J. Zeng, Computing Galois representations and equations for modular curves $X_H(\ell)$, *preprint* (2013), 17pp. `arXiv:math/1312.6819`.

[Dok13] T. Dokchitser and V. Dokchitser, Identifying Frobenius elements in Galois groups, *J. of Algebra and N. Theory* **7** (2013), no.6, pp.1325-1352.

[EC11] B. Edixhoven and J.-M. Couveignes (eds.), Computational aspects of modular forms and Galois representations, *Ann. of Math. Studies, Princeton Univ. Press* (2011), 440pp. Also available from `arXiv:math/0605244`.

[FJ02] D. Farmer and K. James, The irreducibility of some level 1 Hecke polynomials, *Math. Comp.* **71** (2002), no.239, pp.1263-1270.

[KM07] K. Khuri-Makdisi, Asymptotically fast group operations on Jacobians of general curves, *Math. Comp.* **76** (2007), pp.2213-2239.

[KW09] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture (I), (II), *Invent. Math.* **178** (2009), pp.485-504 (I), pp.505-586 (II).

[Leh47] D. H. Lehmer, The vanishing of Ramanujan's function $\tau(n)$, *Duke Math. J.* **10** (1947), pp.429-433.

[Mas13] N. Mascot, Computing modular Galois representations, *Publié dans Rendiconti del Circolo Matematico di Palermo* **62** (2013), no.3, pp.451-476.

[MasTb] N. Mascot, Tables of modular Galois representations, `https://warwick.ac.uk/fac/sci/maths/people/staff/mascot/galreps/tables.pdf`.

[Sch85] R. Schoof, Elliptic curves over finite fields and the computation of square root mod p, *Math. Comp.* **44** (1985), no.170, pp.483-494.

[Sch95] R. Schoof, Computing points on elliptic curves over finite fields, *J.*

Théor. Nombres Bordeaux **7** (1995), no.1, pp.219-254.

[Ser85] J.-P. Serre, Sur la lacunarité des puissances de η, *Glasgow Math. J.* **27** (1985), pp.203-221.

[Wei84] P. J. Weinbeger, Finding the number of factors of a polynomial, *J. of Algorithms*, **5** (1984), no.2, pp.180-186.

[Yam15] 山内卓也, 書評：B. Edixhoven and J.-M. Couveignes (eds.), Computational aspects of modular forms and Galois representations, 数学 **67-3** (2015), pp.317-322.

[Yok16] 横山俊一, 楕円モジュラー形式の高速計算理論入門, 京都大学数理解析研究所講究録別冊 **B53** (2016), pp.279-304.

[ZY15] J. Zeng and L. Yin, On the computation of coefficients of modular forms: the reduction modulo p approach, *Math. Comp.*, **84** (2015), no.293, pp.1469-1488.

Shun'ichi Yokoyama
Faculty of Mathematics, Kyushu University
s-yokoyama@math.kyushu-u.ac.jp