RIMS Kôkyûroku Bessatsu
B53 (2015), 279–304

楕円モジュラー形式の高速計算理論入門 (Introduction to the computational theory of elliptic modular forms*)

By

横山 俊一** (Shun'ichi YOKOYAMA)

Abstract

We survey a polynomial time algorithm by Edixhoven-Couveignes for computing Fourier coefficients of modular forms. Moreover, we introduce some generalized results and related topics on this algorithm.

§1. 序

1998 年のことである. R. Schoof は B. Edixhoven に対し, Ramanujan's tau function $\tau(n)$ に関する次のような質問をしたとされる[1].

問題 1.1. p を素数とする. このとき $\tau(p)$ は $\log p$ の多項式時間で計算可能か?

ここで $\tau(n)$ は以下の展開公式の係数として定義される.

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

それから約 10 年の時を経て, Edixhoven は J.-M. Couveignes と共にこの問題を肯定的に解決した.

Received March 26, 2014. Revised February 17, 2015.
2010 Mathematics Subject Classification(s): 11F30, 11F80, 11Y16, 11Y40.
Key Words: *Computational number theory, Computer algebra systems, Modular forms, Galois representations, Approximation techniques.*

*講演時のタイトルは「モジュラー形式を中心とした計算機数論入門」(Exploring modular forms using computer algebra systems) であったが, より内容を反映したものとするために変更した.

**Faculty of Mathematics, Kyushu University, Fukuoka 819-0395, Japan.
e-mail: s-yokoyama@math.kyushu-u.ac.jp

[1]正確な出自は不明だが, 複数の論文の序章にこのような記述がみられる. 例えば [33] など.

定理 1.2 (Edixhoven-Couveignes)**.** $\tau(p)$ は $\log p$ の多項式時間で計算可能である.

まず必要最低限の記号を準備する（詳しくは [31] の前半部分を参照されたい）. $M_k(\Gamma_1(N))$ 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. これは有限次元 $\mathbb{C}$ ベクトル空間をなす. ここで

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

をレベル N の合同部分群とよぶ. $N = 1$ のときこれは $\mathrm{SL}_2(\mathbb{Z})$ に一致する. 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

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

と書ける. 特に $a_0 = 0$ となる f を尖点形式とよび, 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

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

と定義する. 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 を正規化固有形式とよぶ. さて問題 1.1 は, $\mathbb{Q}$ 上レベル 1, 重さ 12 の正規化固有形式 $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ に関するもので, これは唯一つ存在する. これを Δ と書き discriminant form とよぶ. この n 番目の Fourier 係数が $\tau(n)$ 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な問題となる. 即ち問題 1.1 とは, 非常に大きな素数 p に対しても T_p の計算が $\log p$ の多項式時間で終了するか？(そのようなアルゴリズムが存在するか？）という問題であり, Edixhoven-Couveignes の結果はそれが正しい（多項式時間で終了するアルゴリズムが存在する）という主張である.

この成果を纏めた原稿 [10] は arXiv 等から無償ダウンロード可能となっており, 2011 年に書籍としても出版された. その分量は 400 ページを超えており, J. Bosman, F. Merkl, R. de Jong, P. Bruin らも contributors として参加している.

本稿では [10] の解説を中心として, $\mathbb{Q}$ 上のモジュラー形式の計算理論に関する最近の進展状況を概説する. そこでは Galois 表現を経由する新手法が導入されており, 加えて幾つかの近似（approximation）の技巧が鍵となる. 以下

2 節 具体的な計算（I）
3 節 Edixhoven-Couveignes の理論の俯瞰
4 節 $\mathbb{C}$ 上近似による計算法
5 節 法 p による計算法
6 節 具体的な計算（II）
7 節 応用例
8 節 素数判定に関する補足

の順に述べる. 但し 4,5,7 節については [10] が出版されて現在に至るまでの 2,3 年の間に幾つかの進展が見られたので, それらの結果も交えて解説する. 具体的には $\tau(p)$ の計算時間の評価に関して次のような結果が得られており, 現時点で最良の結果である. 記号に関する詳しい説明は 5 節を参照されたい.

定理 1.3 (Zeng-Yin, [37] 系 1.2 (2), 本稿の系 5.3)**.** $\tau(p)$ は $O(\log^{6+2\omega+\delta+\epsilon} p)$ で計算出来る.

また 7 節では Edixhoven-Couveignes の結果の応用として, Lehmer の非消滅予想の検証を紹介する. 命題 1.5 が現時点での最高記録であるが, これは [10] とモジュラー曲線に関する深い考察によって得られたものである.

予想 1.4 (Lehmer, [21], 本稿の予想 7.1)**.** $n \geq 1$ に対して $\tau(n) \neq 0$ が成り立つ.

命題 1.5 (Derickx-van Hoeij-Zeng, [8], 本稿の命題 7.3)**.**

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

に対して予想 *1.4* は正しい.

本節の最後に一つお断りしておく. 本稿では $\mathbb{Q}$ 上のモジュラー形式について, どのような数式処理システムを用いて, どのような計算が可能なのかという話題にはほとんど触れていない. また, 一般のモジュラー形式（e.g. Hilbert モジュラー形式, Siegel モジュラー形式, Bianchi モジュラー形式 etc.）の計算法については全く扱っていないので, 本稿では単にモジュラー形式と言ったら $\mathbb{Q}$ 上のもの, つまり楕円モジュラー形式を意味するものとする. 一般の場合については, 数式処理システム Magma [2] によるサンプルコードと共に解説した拙稿 [35] を参照頂きたい. なおこれを同様のシステム Sage [30] に対応させ

た [36] も筆者のウェブページにて公開している. また Magma 及び Sage に関する解説としては, Magma が [19], Sage が [20] に詳しいので, こちらもご一読頂きたい.

この場を借りて, 今回このような素晴らしい概説講演の機会を下さった研究集会の世話人の皆様, 特に研究代表者の落合理氏（大阪大学）に感謝する. また草稿に対し有益なコメントを下さった木村巌氏（富山大学）, 田口雄一郎氏（九州大学）と落合氏に御礼申し上げる. 加えて完成稿に至るまで, 丹念に原稿をチェックしコメントを下さった査読者の方に深謝する. 最後に, 筆者は本研究集会の参加にあたり, 京都大学数理解析研究所より旅費の援助を賜った. これについても深く感謝申し上げたい.

§2. 具体的な計算（I）

本節では, Edixhoven らの手法を用いない場合にどの程度の計算が出来るのかを試す. 以下は全て Intel Core i7-2630QM 3.30GHz プロセッサを 1 コアのみ使用した場合の結果である. OS は Windows 7 64 ビット版, 搭載メモリは 8GB とし, 数式処理システムとして Sage ver. 6.0 を採用する. まず内部関数によるベンチマークを行う. 具体的には, 例えば $p = 101$ ならば `sage: p=101` とし, 続いて

```
sage: S=CuspForms(SL2Z,12,prec=p+1)
sage: S.basis()
```

を実行する. q 展開は $O(q^{\mathtt{prec}})$ の精度, 即ち $q^{\mathtt{prec}-1}$ の項までが出力されるため, $\tau(p)$ を計算するには `prec=p+1` としなければならない.

p	実行時間 (cpusec)	$\tau(p)$ の桁数
10^2+1	0.14	11
10^3+9	7.16	17
10^4+7	2464.85	22
10^5+3	out of memory	—

ここでは上記のコードからも分かる通り, 尖点形式の空間を具体的に計算している. この場合は p が数千程度でメモリが溢れ, 計算が停止してしまう.

次に別の戦略として, 尖点形式の空間を用いることなく展開公式を使って計算する. まず 1 節でも登場した以下の公式はよく知られている：

$$\Delta = q\prod_{n\geq 1}(1-q^n)^{24}.$$

但しこれでは 24 乗の展開を高い精度で行わなければならず, 実用的ではない. 実は Δ にはより効率の良い（8 乗の）展開公式が存在する（cf. [26] Sec. 3.2）：

$$\Delta = q\left(\sum_{n=0}^{\infty}(-1)^n(2n+1)q^{n(n+1)/2}\right)^8.$$

この公式は Sage に既に実装されており

```
sage: delta_qexp(prec=p+1)
```

で実行出来る. これを用いた場合のベンチマーク結果は次のようになる.

p	実行時間 (cpusec)	$\tau(p)$ の桁数
10^2+1	≤ 0.01	11
10^3+9	0.014	17
10^4+7	0.072	22
10^5+3	0.96	28
10^6+3	18.92	33
10^7+19	172.03	39
10^8+7	out of memory	—

先程に比べるとかなりの効率化に成功しているが, それでもおよそ p が数千万程度になると限界を迎える.

そこで次の戦略として, 幾つかの ℓ (ℓ は素数) に対して $\tau(p) \bmod \ell$ を計算し, 中国剰余定理 (CRT) を用いて $\tau(p)$ を復元する方法を考える. Deligne の定理より $|\tau(p)| < 2p^{11/2}$ であるから, ℓ たちの積が $4p^{11/2}$ を超えた時点で CRT を適用出来る. 目安としてはおよそ $\log p$ 以下の ℓ に対して $\tau(p) \bmod \ell$ が計算出来れば良い. Sage で $\tau(p) \bmod \ell$ を計算するには

```
sage: delta_qexp(prec=p+1,K=GF(l))
```

とオプション部を変更すればよい. 例として $\ell = 19$ の場合を試す.

p	実行時間 (cpusec)	$\tau(p) \bmod 19$
10^2+1	≤ 0.01	7
10^3+9	≤ 0.01	11
10^4+7	0.041	2
10^5+3	0.52	5
10^6+3	6.82	1
10^7+19	111.54	6
10^8+7	out of memory	—

実行時間の若干の短縮が見られるが, 結果としては同程度の p で限界を迎えている. 更なる高速化として展開公式を C 言語等で実装し, 並列計算のために最適化させるといった手段も考えられるが, それでもおよそ p が十数桁程度で限界を迎えると予想される[2]. 従って, 展開公式の逐次計算に頼らない別の手法を考えなければならない.

[2]筆者の環境では $p \approx 10^{10}$ 程度でメモリが溢れ, 計算が停止した.

更に別の戦略を考える. いま $\dim S_{12}(\mathrm{SL}_2(\mathbb{Z})) = 1$ であることから Eichler-Selberg 跡公式（trace formula）を用いることが出来る. 具体的には

$$\tau(p) = -\sum_{0<t\leq 2\sqrt{p}} P(t,p)H(4p-t^2) + \frac{p^5}{2}H(4p) - 1$$

が成り立つ. 但し $P(t,p) = t^{10} - 9t^8p + 28t^6p^2 - 35t^4p^3 + 15t^2p^4 - p^5$ であり, $H(n)$ は Hurwitz 類数である. 従ってこの場合は $H(n)$ の高速計算が要求される. しかしながら, $H(n)$ を計算する確定的アルゴリズムのうち, 現存する最良の評価は $O(n^{1/4+\epsilon})$ 程度であり, 結論として $\tau(p)$ の計算には $O(p^{3/4+\epsilon})$ 程度の計算を要する[3]. 従って展開公式と比較しても, ほぼ同程度の難しさであることが分かる.

これらの手法に対し, Edixhoven らの手法は後述の通り本質的に異なっている. この手法を用いると, 例えば p が千桁程度という非常に巨大な素数であっても, $\tau(p) \bmod \ell$ の計算が実時間で終わってしまう. 以下は [10] の序盤に掲げられたデータの一部である. Edixhoven らによる詳細なベンチマーク結果は公表されていないため, 時間表記は除いている. 計算結果に符号 $\pm$ が付いているが, これについては 4 節で理由を述べる.

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

このような驚くべき情報が求まる理由は勿論 $\log p$ の多項式時間という圧倒的な計算効率化にある. 従来法では p そのものに対して指数時間, よくても p の多項式時間程度の計算が要求されていた. これに対し本手法では, 端的に言えば $p = 10^r$ のとき, その計算はおよそ $\log p = r$ の多項式時間程度ということになるので, 非常に大きな p を選択した場合にも計算可能となるのである.

但しここで重要なのは, Edixhoven らの結果は素数 $p \approx 10^{1000}$ に対して $\tau(p) \bmod 19$ の計算が出来たという主張であって, **同程度の p に対して $\tau(p)$ そのものを計算出来る訳ではない** ということである. 実際 $p \approx 10^{1000}$ の場合, $\tau(p) \bmod \ell$ の計算は $\ell \leq 30$ 程度が限界である（6 節を参照）. $\tau(p)$ を CRT で求めるには $\log p$ 以下の ℓ に対する情報が必要であるから, $\tau(p)$ の計算限界は p が数十桁程度で訪れてしまい, $p \approx 10^{1000}$ ともなれば絶望的となるのである.

[3]確率的アルゴリズムを適用した場合の評価は $O(p^{1/2+\epsilon})$ と見積もられている（cf. [6]）.

§3. Edixhoven-Couveignes の理論の俯瞰

いよいよ本題に入る. まず 1 節で紹介した [10] の主定理について詳しく述べる. この結果はより一般に, モジュラー形式の空間 $M_k(\mathrm{SL}_2(\mathbb{Z}))$ に対して成立するものである.

定理 3.1 (Edixhoven-Couveignes et al., [10] 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[4], $a_n \in \mathbb{Z}$ を計算する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 $\log n$ 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.

続いて, この主定理を支えている二つの主張を述べる. これらも [10] では主定理扱いとなっている. 一つ目は Galois 表現の計算に関する定理である. 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. $S_k(\Gamma_1(N))$ が $\mathbb{Z}$ 上の構造を持ち, それが Hecke 作用素によって保たれることから, 後述の命題 4.3 の通り $\mathbb{T}(N,k)$ は有限生成となる.

定理 3.2 ([10] 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.

この主張は「Galois 表現 ρ が計算出来る」というものであるが, 具体的に ρ を計算するとはどういうことかについて考えてみよう. 議論を簡単にするために, $\mathbb{F} = \mathbb{F}_\ell$ 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[5]. 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.

具体的には 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：

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

[4] $k/12$ 番目以下の係数たちでモジュラー形式は決定される. cf. 命題 4.3.

[5] 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 $\sigma_k(n) = \sum_{d|n} d^k$) は有名である.

ここで $J_1(\ell)$ はモジュラー曲線 $X_1(\ell) = (\Gamma_1(\ell)\backslash\mathfrak{h})^*$ の Jacobian である．さて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．[10] では ρ_ℓ, 即ち V_ℓ の計算法を 2 通り提示しており, それぞれについては 4 節及び 5 節で詳細に述べる．なお V_ℓ が計算可能であることを保証するためには Arakelov 理論が用いられる．ここでは関数 $\iota : V_\ell \to \mathbb{A}^1_{\mathbb{Q}}$ を導入し, 多項式

$$P(X) := \prod_{\alpha \in V_\ell - \{0\}} (X - \iota(\alpha))$$

の係数の高さが $O(\ell^\delta)$（δ は ℓ に依存しない定数）で抑えられることを示す．関数 ι は Bruin の学位論文 [4] によって精密に調べられている．Bruin はこの中で [10] の結果を一般のレベルに拡張している．

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．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．但しこのままでは実用上問題があるため, 幾つかの工夫が必要となる．これについては 4 節で解説する．

続いて二つ目の定理を述べる．これは Hecke 作用素の計算に関するものである．

定理 3.3 ([10] 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[6]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．

GRH を仮定する理由を含めて少し補足する．まず, 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 $\mathbb{T}_{\mathbb{Q}} = \mathbb{T}(1,k) \otimes \mathbb{Q}$ 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 [10] 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 [11] が引用されている）ため, [10] では唯一つの代数体 K での $\mathbb{T}(1,k)$ の像を A と書いて $\mathbb{T}(1,k)$ と同一視しているようである．さて, 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 $\bmod \ell$ 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[7].

命題 3.4 (Weinberger, [34])**.** 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 $\#(\mathcal{O}_K/\widetilde{\mathfrak{m}}) \le x$ 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：

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

[6] ここで「計算する」とは T_n を T_i（$1 \le i \le k/12$）の多項式で書き表すことを意味する．cf. 命題 4.3.

[7] 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）確定出来なかった．この命題は [10] の記述に従って引用したものである．

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[8].

以上, 二つの定理の帰結として主定理（本稿の定理 3.1）が導かれる. 以降より詳しく Galois 表現 ρ_ℓ（つまり V_ℓ）の計算法について見ていく.

§4. $\mathbb{C}$ 上近似による計算法

ここからは V_ℓ を如何に効率的に計算出来るかについて考えよう. 本節では一つ目の戦略として, $\mathbb{C}$ 上近似を用いた手法を紹介する. ここで Galois 表現を $\mathbb{C}$ 上近似で計算するとは, 大雑把に言えば以下のような戦略を指す.

- 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（本稿の定理 4.4）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. まず最初に重要な定理を（少し一般の形で）述べる.

定理 4.1 ([10] 定理 2.5.7). k を重さ, $N \in \mathbb{Z}_{\geq 1}$ とし, $\mathbb{F}$ を標数 ℓ の有限体とする. $2 < k \leq \ell + 1$ を仮定し, *Hecke* 環から $\mathbb{F}$ への全射 $f : \mathbb{T}(N, k) \to \mathbb{F}$ を考え, 更に f に付随する *Galois* 表現 $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ 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 $f_2 : \mathbb{T}(N\ell, 2) \to \mathbb{F}$ が唯一つ存在する. ここで $\mathfrak{m}_f := \ker(f_2)$ とし, V_f を全ての $t \in \mathfrak{m}_f$ に対して $tx = 0$ をみたすような $x \in J_1(N\ell)(\overline{\mathbb{Q}})$ のなす $\mathbb{F}$-ベクトル空間とする. このとき V_f は有限かつ非零であり $V_f = \rho_f^{\oplus m}$（m は重複度）と書ける. 特に $k < \ell$ のときは $m = 1$, 即ち $V_f = \rho_f$ が成り立つ.

上の定理により, レベル N, 重さ k の $\bmod \ell$ 固有形式に付随する Galois 表現 ρ_f の計算は $J_1(N\ell)(\overline{\mathbb{Q}})$ 上の計算に帰着される. 特に $N = 1$ の場合は次が成り立つ.

定理 4.2 ([10] 定理 2.5.13). k を重さ, $\mathbb{F}$ を標数 ℓ の有限体とし $2 < k \leq \ell + 1$ を仮定する. 全射 $f : \mathbb{F}_\ell \otimes \mathbb{T}(1, k) \to \mathbb{F}$ を考え, 更に f に付随する *Galois* 表現 $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ 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

[8] 一般に次数の高い K に対して $\mathrm{Disc}(\mathcal{O}_K)$ を計算するのは容易ではなく, そのボトルネックは整数環 $\mathcal{O}_K$ の計算にある. 戦略としては次の二つが代表的である： 1) $\mathcal{O}_K$ を近似計算する（cf. [5]）. 2) K の定義多項式を P_K としたとき, まず $\mathrm{Disc}(P_K)$ を計算し（この計算は容易）, 関係式 $\mathrm{Disc}(P_K) = c^2\mathrm{Disc}(\mathcal{O}_K)$ $(c \in \mathbb{Z})$ を用いる. 特に 2) の場合は, $\mathrm{Disc}(P_K)$ に含まれる巨大な合成数 C^2 が $C \mid c$ であることを示すことで $\mathrm{Disc}(\mathcal{O}_K)$ を特定する手法が用いられる.

たすような全射 $f_2 : \mathbb{F}_\ell \otimes \mathbb{T}(\ell, 2) \to \mathbb{F}$ 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

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

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

定理 4.1 とは異なり, こちらは仮定 $k < \ell$ は必要ない. Edixhoven の論文 [9] の最後に示されている “重複度 1 定理”（multiplicity one theorem）を用いると

- $2 \le k < \ell$ をみたす,
- $k = \ell$ かつ Hecke 作用素と Galois 表現の ℓ での分岐に関する条件をみたす,
- $k = \ell + 1$ かつ $S_2(\Gamma_1(N), \varepsilon)$（$\varepsilon$ は Dirichlet 指標）が消えている,

の何れかが成り立てば $V_f = \rho_f$ が示され, 定理 4.2 の状況はこれらを全てみたす（例えば $\dim S_2(\mathrm{SL}_2(\mathbb{Z})) = 0$ である）. 故に $2 < k \le \ell + 1$ の状況下で重複度が 1 であることが保証される.

実際に定理 4.2 の $\mathfrak{m}_f$ の生成元を求めるには次のような手順をふむ. まず整数 $i \in \{1, 2, \cdots, (\ell^2 - 1)/6\}$ に対し, $f(T_i)$ が $f(T_j)$（$j < i$）たちの $\mathbb{F}_\ell$-係数での一次結合で書けるかを調べる. もし出来ない場合は $t_i = 0$ とする. 一方 $f(T_i) = \sum_{j<i} a_{i,j} f(T_j)$ と書けた場合は $t_i = T_i - \sum_{j<i} a_{i,j} T_j$ と定義する. 最終的に 0 でないものを集めたものが $\mathfrak{m}_f$ の生成元となる. i の上限 $(\ell^2 - 1)/6$ は Sturm の定理とよばれている次の結果から従う.

命題 4.3 (Sturm bound). *Hecke* 環 $\mathbb{T}(N, k)$ は T_i $(1 \le i \le k[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)]/12)$ たちにより生成される. 即ち, 任意の *Hecke* 作用素 T_n（$n \in \mathbb{N}$）はこれらの多項式として書ける.

ここで $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = N^2 \prod_{p|N}(1 - 1/p^2)$（$p$ は素数）と書けることはよく知られている. よって $N = \ell$, $k = 2$ とすれば i の上限値に一致する.

さて, 再び定理 4.2 をよく眺めてみる. この定理の驚くべき所は「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している（同じ mod ℓ Galois 表現を与えている）」という点にある. そして重さを 2 にとることにより, この Galois 表現がモジュラー曲線 $X_1(\ell)$ の Jacobi 多様体の ℓ-等分点 $J_1(\ell)(\overline{\mathbb{Q}})[\ell]$ に実現出来ることも重要である. 即ちこれらの結果により, 3 節で述べた ρ_ℓ の計算が Ramanujan subspace

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

の計算によって実現されることが保証される.

では $J_1(\ell)(\overline{\mathbb{Q}})[\ell]$ を直接計算することは容易だろうか？ – 答えは否である．まず Buchberger アルゴリズムの類似といった計算代数的手法では Jacobi 多様体はまともに計算出来ない．何故ならば，ℓ-等分多項式の次数 d を見積もると

$$d = \ell^{2g(X_1(\ell))} \quad (g(X_1(\ell)) \text{ は } X_1(\ell) \text{ の種数})$$

となり，次数が急激に増大するからである．今欲しいのは $\#V_\ell$ の多項式時間程度で終了するアルゴリズムである．そのために次のような戦略を考える．

以降，定理 3.2 で述べられていた条件 $\mathrm{Im}(\rho_\ell) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$ を仮定する．Δ に付随する Galois 表現を考える場合は $\ell \geq 11$, $\ell \notin \{23, 691\}$ であれば $\mathrm{Im}(\rho_\ell) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$ をみたす．まずモジュラー曲線間の射

$$\mathcal{B}_{N,N',d} : X_1(N) \to X_1(N') \quad (N' \mid N)$$

を考える．これは $X_1(N)$ の cusp ∞ を，やはり $X_1(N')$ の cusp ∞ に写す．モジュライの言葉で解釈するならば (E, P) を $(E/\langle (N/d)P \rangle, d'P)$（$dd' = N/N'$, $\langle * \rangle$ は diamond 作用素）に写していることになる．故に射 $\mathcal{B}_{N,N',d}$ の対応は

$$(\mathbb{C}/(\mathbb{Z}z + \mathbb{Z}), 1/N) \mapsto (\mathbb{C}/(\mathbb{Z}zd + \mathbb{Z}), 1/N')$$

となっている．これは引き戻しにより

$$\mathcal{B}^*_{N,N',d} : J_1(N') \to J_1(N)$$

を引き起こす．これを $f \in S_k(\Gamma_1(N'))$ の q 展開として作用を記述すると

$$\mathcal{B}^*_{N,N',d} f = \sum_{i \geq 1} a_i(f) q^{di}$$

と書ける．これは単に q を q^d に取り換えているだけであるから，$S_k(\Gamma_1(N))$ の基底は

$$\coprod_{N' \mid N} \coprod_{d \mid (N/N')} \mathcal{B}^*_{N,N',d} S_k(\Gamma_1(N'))^{\mathrm{new}}$$

と記述出来る．ここで $S_k(\Gamma_1(N'))^{\mathrm{new}}$ は newform の有限集合を表す．さて，この射において $(N, N', d) = (5\ell, \ell, 1)$ とする．即ち

$$\mathcal{B}_{5\ell,\ell,1} : X_1(5\ell) \to X_1(\ell), \ \mathcal{B}^*_{5\ell,\ell,1} : J_1(\ell) \to J_1(5\ell)$$

を考える．このとき $W_\ell := \mathcal{B}^*_{5\ell,\ell,1}(V_\ell)$ と定義すると

$$W_\ell \subset J_1(5\ell)$$

が成り立つ．これにより定理 4.2 の主張を更に変えて「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 5ℓ，重さ 2 の固有形式にも付随している（同じ

mod ℓ Galois 表現を与えている）」と結論付けられる．$J_1(5\ell)$ の元は $X_1(5\ell)$ の因子で記述されるので, W_ℓ の各類の因子の（十分にシャープな）$\mathbb{C}$ 上の近似計算を行うことで $J_1(5\ell)$ を調べよう, というのがアイデアである．5ℓ というレベルを選んだのは, この近似計算において必要な cuspidal 因子を正確に求める上で非常に都合が良いからである．このあたりの精密な議論は代数幾何の範疇であるから, 著者の力量では不正確さを免れないと思うので割愛する．興味のある方は [10] の 8 節を参照されたい．

$\mathbb{C}$ 上近似を行うため, 最初に $J_1(5\ell)(\mathbb{C})$ を複素トーラスと同一視する．ここでは Abel-Jacobi の古典的な定理を適用する．$g = g(X_1(N))$ を $X_1(N)$ の種数とし

$$\Lambda_N := \left\{ \int_\gamma (f_1, \cdots, f_g) \frac{dq}{q} : \ [\gamma] \in H_1(X_1(N)(\mathbb{C}), \mathbb{Z}) \right\} \subset \mathbb{C}^g$$

を $\mathbb{C}^g$ の full rank の格子とする．ここで $\{f_1, \cdots, f_g\}$ は $S_2(\Gamma_1(N))$ の基底であり

$$\int_\gamma (f_1, \cdots, f_g) \frac{dq}{q} = \left(\int_\gamma f_1 \frac{dq}{q}, \cdots, \int_\gamma f_g \frac{dq}{q} \right)$$

とする．

定理 4.4 (Abel-Jacobi)**.**

$$J_1(N)(\mathbb{C}) \simeq \mathbb{C}^g / \Lambda_N, \quad \sum_i (Q_i - P_i) \mapsto \sum_i \int_{P_i}^{Q_i} (f_1, \cdots, f_g) \frac{dq}{q}$$

が成り立つ．

このとき重要なのは $J_1(5\ell)(\mathbb{C})[\ell]$ が複素トーラス内に埋め込まれることである．より正確には格子 $\Lambda := \Lambda_{5\ell}$ を用いて次の同型が導かれる：

$$W_\ell(\mathbb{C}) \subset J_1(5\ell)(\mathbb{C})[\ell] \simeq \frac{1}{\ell}\Lambda/\Lambda \subset \mathbb{C}^g/\Lambda.$$

この同型を用いて, 次のように射を組み合わせることにより W_ℓ を $\mathbb{C}$ 上の計算に帰着させることを企むわけである．

$$\begin{array}{rcl} \varphi : \mathcal{F}^g \to (X_1(5\ell)(\mathbb{C}))^g \to \mathrm{Sym}^g X_1(5\ell)(\mathbb{C}) \to & J_1(5\ell)(\mathbb{C}) & \simeq \mathbb{C}^g/\Lambda \\ & \cup & \cup \\ & J_1(5\ell)(\mathbb{C})[\ell] & \simeq \frac{1}{\ell}\Lambda/\Lambda \\ & \cup & \\ & W_\ell(\mathbb{C}) & \end{array}$$

写像 φ は $\varphi : \mathcal{F}^g \to \mathbb{C}^g/\Lambda$（上段左端から右端への写像）である．$\mathcal{F}$ は $\Gamma_1(5\ell)$ の（楕円モジュラー形式論においての）基本領域である．

さて $\phi : \mathrm{Sym}^g X_1(5\ell)(\mathbb{C}) \to \mathbb{C}^g/\Lambda$ とする．この写像を用いて, W_ℓ の情報から $X_1(5\ell)$ の因子の情報を（$\mathrm{Sym}^g X_1(5\ell)(\mathbb{C})$ を介して）引き抜く．具体的には次の 3 段階の操作で進行する．

1. $\phi^{-1}(W_\ell(\mathbb{C})-\{0\})$ を Newton-Raphson 法により近似計算する.
2. 各 $x\in W_\ell\subset\frac{1}{\ell}\Lambda/\Lambda$ に対して $\phi(Q')\approx x$ をみたすような $Q'=(Q'_1,\cdots,Q'_g)$ を近似計算する.
3. Arakelov 理論及び格子簡約 LLL アルゴリズムを用いて $\phi(Q)=x$ をみたすような $Q=(Q_1,\cdots,Q_g)\approx Q'$ を決定する.

最終的に得られた Q を φ によって更に引き戻し, 更に W_ℓ と本来の表現空間であった V_ℓ との対応を合わせて, 最終的に $v\in V_\ell(\mathbb{C})-\{0\}$ に対して $\varphi(Q_F)=v$ を（正確な等式として）みたすような $Q_F=(Q_{F,1},\cdots,Q_{F,g})\in\mathcal{F}^g$ が求まる. この情報を用いて, P_ℓ（K_ℓ はこの多項式の $\mathbb{Q}$ 上の最小分解体として書けるのだった）は次のように近似出来る.

命題 4.5 ([10], 6.4.2 節の変形版)**.**

$$P_\ell(X)=\prod_{v\in V_\ell(\mathbb{C})-\{0\}}(X-\alpha_v)=\sum_i a_iX^i\ (a_i\in\mathbb{R}),\ \alpha_v:=\sum_{i=1}^{g}\psi(Q_i)$$

を用いて $P_\ell(X)\in\mathbb{Q}[X]$ を実数係数多項式で近似出来る. 但し Q を引き戻した先にある Q_F は $\varphi(Q_F)=v$ をみたすように選ぶ. また $\psi\in\mathbb{Q}(X_1(5\ell))$ である.

以上により P_ℓ が計算出来ることは保証されたが, ここで問題が生じる. 実はこの 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[9]. 例えば最も小さい $\ell=11$ の場合であっても, P_{11} は 120 次多項式となる. そこで, 得られる情報を少しだけ犠牲にして計算可能なクラスの問題を解くことを考える. この方面の計算を初めて本格的に行ったのは Bosman [3] とされる. 具体的には 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. 引き戻す領域は $V_\ell-\{0\}$ を $\mathbb{P}(V_\ell)$ に取り換えればよい. Bosman はこのアイデアを基にして, 次のような戦略を考えた.

- 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. Galois 群の次数が大きいため, 計算代数的アルゴリズムを用いる.
- $\alpha\in\overline{\mathbb{Q}}$ 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. [10] 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 Galois 表現であることを Serre の保型性予想を用いて保証する.

[9] 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.

$\ell \geq 5$ 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 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, 三つ目の条件 – 現在では Khare-Wintenberger の定理 [17] を適用することで, 近似計算により求めた mod ℓ Galois 表現こそが真に求めたかったものと一致することが証明出来る. Khare-Wintenberger の定理を念のため述べておく. この定理に関しては [32] に詳細な解説があるのでそちらを参照されたい.

定理 4.6 (Khare-Wintenberger, [17]). $\mathbb{Q}$ 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. 即ち *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 $\dim S_k(\mathrm{SL}_2(\mathbb{Z})) = 1$ 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[10]. このあたりの実際のデータは 6 節で紹介する. 一つ目の条件で要求されている $\mathrm{Gal}(K_\ell^{\mathrm{proj}}/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$ の計算についても同様とする.

さて, 最後に $\mathrm{Gal}(K_\ell^{\mathrm{proj}}/\mathbb{Q})$ の元 Frob_p がどの共役類に属するかを調べるステップが残されている. これが確定することにより, Frob_p の特性多項式の係数から $\tau(p)$ mod ℓ（但し up to sign）が求まる[11]. これに関しては, 最近 Dokchitser 兄弟によるアルゴリズムの改善 [7] がみられた. ここでは分解式（resolvent）を用いた手法が導入されている. 計算上は $\mathrm{Gal}(K_\ell^{\mathrm{proj}}/\mathbb{Q})$ に対し適用するが, より一般に $\mathrm{Gal}(K_\ell/\mathbb{Q})$ の状況で述べる. projective case の場合は $\ell^2 - 1$ を $\ell + 1$ に取り換えれば良い.

命題 4.7 (Dokchitser-Dokchitser, [7]). $(a_i)_{1 \leq i \leq \ell^2 - 1}$ を P_ℓ の根とする. ある多項式 $h(x) \in \mathbb{Q}[x]$ と共役類 $C \subset \mathrm{Gal}(K_\ell/\mathbb{Q})$ に対して関数

$$\Gamma_C^h(X) := \prod_{\sigma \in C} \left(X - \sum_{1 \leq i \leq \ell^2 - 1} h(a_i)\sigma(a_i) \right)$$

を定義する. このとき, ほとんど全ての素数 p に対して同値関係

$$\mathrm{Frob}_p \in C \Longleftrightarrow \Gamma_C^h \left(\mathrm{Tr}_{\frac{\mathbb{F}_p[x]}{P_\ell}/\mathbb{F}_p} (h(x)x^p) \right) \equiv 0 \bmod p$$

が成り立つ. 但し “ほとんど全て” とは, 以下の三つを全てみたすものに限るという意味である：

1. P_ℓ の係数（先頭項を除く）の分母を割らない.
2. P_ℓ の先頭項の係数を割らない.

[10] 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.

[11] 正確に述べると, Frob_p の特性多項式は $x^2 - \tau(p)x + p^{11}$ と法 ℓ で合同となる. 但し先程の議論から $\mathrm{Gal}(K_\ell^{\mathrm{proj}}/\mathbb{Q}) \simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$ であったから, 符号の情報が失われている.

3. 任意の二つの共役類 C, C'（$C \neq C'$）に対して定まる終結式 $\mathrm{Res}_X(\Gamma_C^h(X), \Gamma_{C'}^h(X))$ を割らない.

上の定理において使われている多項式は, $\deg(h) \leq \ell^2 - 2$ であって C, C'（$C \neq C'$）に対して $\mathrm{Res}_X(\Gamma_C^h(X), \Gamma_{C'}^h(X)) \neq 0$ となるように定められている. [7] では具体的な例を（多項式 $h(x)$ の選び方も含めて）数多く丁寧に解説している. 本稿 6 節にそのうちの一つを紹介したので, そちらも参照されたい.

さて, 命題 4.7 の手法は非常に有用であるが, $\mathbb{C}$ 上近似のアイデアを用いたデメリットも請け負っている. 具体的には P_ℓ の根を表現する際に要求される（$\mathbb{C}$ 上の元の）精度が高く, 計算負荷がかかり易いという問題が生じる. そこで N. Mascot は “quotient representation trick” とよばれる技巧を用いて計算量を削減することを試みた. 更に $\mathrm{GL}_2(\mathbb{F}_\ell)$ の商をとる際に $\mathrm{PGL}_2(\mathbb{F}_\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)/\mathbb{F}_\ell^\times$ とするのではなく, 若干「ずらして」商をとることにより, Bosman の手法で失われた符号の情報を保持しつつ効率化に成功している. 詳細は [23] を参照されたい.

§5. 法 p による計算法

$\mathbb{C}$ 上近似において要求される精度が ℓ に伴い急激に上昇するという問題を回避するため, V_ℓ の計算の二つ目の戦略を紹介する. それが法 p による手法である. 即ち

$$V_\ell \bmod p = \bigcap_{1 \leq i \leq \frac{\ell^2-1}{6}} \ker\left(T_i - \tau(i), J_1(\ell)(\mathbb{F}_p)[\ell]\right)$$

を小さな p に対してたくさん計算し, CRT で持ち上げるというアイデアをとる. 本節ではまず [10] の 13 節で述べられている Couveignes の方法を概説し, その後の進展について紹介する.

決定的に異なるのは, $\mathbb{C}$ 上近似が確定的アルゴリズムであったのに対し, この計算が確率的アルゴリズムであるという点である. ここで確率的アルゴリズムと言っているのは, 計算の過程においてランダムな元（例えば代数多様体上の点）をとる操作が含まれるようなものを指す. 名前の通り, このアルゴリズムは一定の確率で計算に失敗することがあるが, その場合は計算に失敗したことを明示的に出力出来るため, 誤ったデータを気付かず用いてしまうといったトラブルは避けられる. 一方計算に成功した場合は, その出力は数学的に正しいことが保証されている. 例えば [10] の 5 節には乱択アルゴリズムにおける計算が成功する確率の評価について述べられており, 具体的な確率の評価を得ることも重要である.

もう少し詳細を述べる. この手法では途中 $X_1(5\ell)/\mathbb{F}_q$（$\mathbb{F}_q \subset \overline{\mathbb{F}}_p$）の Picard 群の ℓ^k-等分点 $\mathrm{Pic}(X_1(5\ell)/\mathbb{F}_q)[\ell^k]$ を（ランダムにとった幾つかの点を基に）計算する. これにより $V_\ell \bmod p$（正確には以下に述べる通り $W_\ell \bmod p = \mathcal{B}^*_{5\ell,\ell,1}(V_\ell \bmod p)$）を求めるわけだが, このアルゴリズムを確定的に実行した場合, 現実的な時間内に計算が終了しない. 従って現時点では確率的アルゴリズムを採用せざるを得ない. $\mathrm{Pic}(X_1(5\ell)/\mathbb{F}_q)[\ell^k]$ の計算

アルゴリズムに関しては [10] の定理 13.6.2 を参照されたい（これによると, 計算に成功する確率は 1/2 以上とある）.

定理 5.1 ([10], 定理 13.7.3 の特別な場合)**.** 記号は全て 4 節のものに従う. 重さを k とし, mod ℓ *Galois* 表現 $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ を考え, これが既約かつ $\mathrm{Im}(\rho_\ell) \supset \mathrm{SL}_2(\mathbb{F}_\ell)$ であるとする. このとき $W_\ell \bmod p$（但し $p \neq 5, \ell$）を計算するための確率的アルゴリズムが存在する. 計算時間はある正定数 Θ を用いて $(p \times \#(V_\ell \bmod p))^\Theta$ 以下で抑えられる.

法 p による計算においても, やはりレベル 5ℓ での処理が鍵となる. Ω を $X_1(5\ell)$ の cuspidal 因子とする. このアルゴリズムでは, $\#V_\ell$ 個の effective 因子 $(Q_i)_{1 \leq i \leq \#V_\ell}$（$Q_i$ の次数は $g = g(X_1(5\ell))$）を, 因子類 $[Q_i - \Omega]$ たちが W_ℓ の $\mathbb{F}_q$-有理点を全て与えるようにとる処理が含まれている. 因子類間の関係の解析にはペアリング（pairing）が用いられる. 特に Couveignes の手法では Weil ペアリングと Tate-Lichtenbaum-Frey-Rück ペアリングが考察されている（それぞれ [10] の補題 13.3.2, 13.3.3 を参照）.

さて, 法 p による計算については [10] が出版された後, より精密な（かつ改良された）評価が J. Zeng と L. Yin によって得られた. 彼らの論文 [37] は 2012 年に初めて公開され, そこではレベルが ℓ のままで計算されているなど Couveignes の手法とは若干異なる. 具体的には Couveignes の代数幾何的手法を用いず, モジュラー曲線に対して定まる関数体 $\mathbb{Q}(X_1(\ell))$ での解析を行う.

定理 5.2 (Zeng-Yin, [37] 定理 1.1, 系 1.2 (1))**.** $\ell \geq 13$ とし, p を

$$d_p := \min_{t \geq 1} \left\{ t : \ X^t \equiv 1 \bmod (X^2 - \tau(p)X + p^{11} \bmod \ell) \right\} < \ell$$

をみたすものとする. このとき $V_\ell \bmod p$ は $O(\ell^{4+2\omega+\epsilon} \log^{1+\epsilon} p \cdot (\ell + \log p))$ で計算出来る. *CRT* で V_ℓ を復元する処理まで行うと $O(\ell^{5+2\omega+\delta+\epsilon})$ と見積もられる.

定数 ω は区間 $[2, 4]$ に含まれる. これは Jacobi 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 [18] による $\omega = 2.376$ である. δ は $\dim V_\ell = 2$ 以上の定数であるが, ここで 3 節を思い出す. $\iota : V_\ell \to \mathbb{A}^1_{\mathbb{Q}}$ とすると V_ℓ の計算可能性は

$$P(X) := \prod_{\alpha \in V_\ell - \{0\}} (X - \iota(\alpha))$$

の係数の高さが $O(\ell^\delta)$ で抑えられることで保証されるのであった. この δ についても幾つかの評価が存在する. 詳細は例えば [10] の 11 節を参照されたい.

V_ℓ の計算は次のように進行する. まず素数 p を一つとって固定し, $J_1(\ell)(\mathbb{F}_q)$ 上の点をランダムにとる. 但し q は拡大 $\mathbb{F}_q/\mathbb{F}_p$ の次数が d_p 以下となるようにとる. 次にこの点をスカラ倍することにより ℓ-等分点 $J_1(\ell)(\mathbb{F}_q)[\ell]$ の点を求める. 但しスカラは $\#J_1(\ell)(\mathbb{F}_q)$ を割

り切るような数からうまく選ぶ. このようにして得られた点を $(V_\ell \bmod p) \subset J_1(\ell)(\mathbb{F}_q)[\ell]$ に写す. この操作を p を取り換えて繰り返し行い, 十分な量が計算出来たら CRT で持ち上げて V_ℓ を得る. これにより定理 5.2 が得られ, 更に次の系が従う.

系 5.3 (Zeng-Yin, [37] 系 1.2 (2))**.** p を素数とするとき $\tau(p)$ は $O(\log^{6+2\omega+\delta+\epsilon} p)$ で計算出来る.

この結果により Lehmer 予想とよばれる $\tau(p)$ の非消滅予想の検証結果が改良出来る（詳細は 7 節で述べる）. また Zeng-Yin の仕事の直後, P. Tian によって同様の応用が 2013 年に示されている[12]. Tian の論文 [33] は未出版（プレプリント）であるが, ここではモジュラー曲線上の理論をより深く用いることで効率的な計算を実現している. 更にその後, Derickx-van Hoeij-Zeng [8] は Zeng-Yin と Tian の手法をベースに計算の効率化を行った. 具体的な計算例としては [8] が現時点で最も進んだ結果となっている.

補足. Zeng は中国清華大学に所属しており, 2011 年から 2012 年にかけて Edixhoven と Couveignes がここで集中講義を行ったことをきっかけに Magma を用いた実装に取り組んだようである. Couveignes の法 p による手法は Hess のアルゴリズムを用いるが, これは当時既に Magma に実装されていた. Zeng は更に楕円曲線の同種写像が Magma でよく扱えることに注目し, この手法に特化した Hecke 作用素の計算アルゴリズムを開発した. 彼は最終的にモジュラー曲線 $X_1(31)$ での計算に成功し, 従来の Bosman の結果における ℓ の上限値 23 を更新することになる. この問題設定は M. Derickx によって与えられ, ここで登場する plane model は M. van Hoeij によって提供された. その後 Derickx と van Hoeij はこのアイデアを用いた効率化を進め, Zeng と共に ℓ の上限値を 41 に更新した.

§6. 具体的な計算（II）

本節では 3 節から 5 節までに述べた内容を振り返りながら, 具体的な計算データを考察していくことにする. まず [10] の 6 節及び 7 節に倣い, Bosman による検証結果 [3] を概観する. まず $K_\ell^{\mathrm{proj}} = \mathrm{Spl}(P_\ell^{\mathrm{proj}})$ の例を挙げる.

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	$x^{14} + 7x^{13} + 26x^{12} + 78x^{11} + 169x^{10} + 52x^9 - 702x^8 - 1248x^7 + 494x^6$ $+2561x^5 + 312x^4 - 2223x^3 + 169x^2 + 506x - 215$

[12] Tian は Schoof の指導学生であった.

ℓ	P_ℓ^{proj}
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	$x^{24}-2x^{23}+115x^{22}+23x^{21}+1909x^{20}+22218x^{19}+9223x^{18}+121141x^{17}$ $+1837654x^{16}-800032x^{15}+9856374x^{14}+52362168x^{13}-32040725x^{12}$ $+279370098x^{11}+1464085056x^{10}+1129229689x^9+3299556862x^8$ $+14586202192x^7+29414918270x^6+45332850431x^5-6437110763x^4$ $-111429920358x^3-12449542097x^2+93960798341x-31890957224$

4 節で述べた通り $k=12$ の場合は $\ell\geq 11$, $\ell\notin\{23,691\}$ という仮定があるので [10] 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 $k=16,18,20,22$ に対しては以下の ℓ に対して結果を得ている. これは 4 節でも述べたように, 尖点形式の空間の次元が 1 であるため unique に固有形式が定まるからである[13]. 因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.

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

続いてこれらが $\mathrm{Gal}(K_\ell^{\mathrm{proj}}/\mathbb{Q})\simeq \mathrm{PGL}_2(\mathbb{F}_\ell)$ であることを示す. ここでは実際に Galois 群を計算し, 射影一般線形群への同型写像を具体的に構成する. 即ち置換群の元としての生成元 $\in \mathrm{Gal}(K_\ell^{\mathrm{proj}}/\mathbb{Q})\subset S_d$（$d$ は $K_\ell^{\mathrm{proj}}/\mathbb{Q}$ の拡大次数）と, $\mathbb{F}_\ell$ 係数の 2 次正方行列としての生成元 $\in \mathrm{PGL}_2(\mathbb{F}_\ell)$ を関連付ける処理を行う. Magma では以下で実行出来る.

```
magma: G:=GaloisGroup(f);
magma: PGL:=ProjectiveGeneralLinearGroup(2,ell);
magma: _,map:=IsIsomorphic(G,PGL);
```

但し `f`=P_ℓ^{proj} である. 関数 `ProjectiveGeneralLinearGroup` は長いので単に `PGL` としても良い. 3 行目の `IsIsomorphic` は `G` と `PGL` が同型であるかを判別するだけではなく,

[13]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 [24] が新しい結果を得ている.

`true` の場合は同型写像まで構成して `map` に格納する．直前のアンダースコアは, 一つ目の返り値（真偽）を格納しないという意味である．以下 $k = 12$ の場合に検証する．環境は 2 節と同じとし, 数式処理システムとして Magma ver. 2.20-2 を採用した．

ℓ	実行時間 (cpusec)	$\#\mathrm{Gal}(K_\ell^{\mathrm{proj}}/\mathbb{Q})$
11	0.546	1320
13	0.624	2184
17	2.902	4896
19	2.605	6840
23	3.129	12144

24 次という高次の Galois 群が僅か 3 秒強で求まるのには理由がある．勿論その Galois 群が $\mathrm{PGL}_2(\mathbb{F}_\ell)$ というよく知られた構造であることも関係しているが, 本質は Magma が採用しているアルゴリズムにある． まずよく知られた古典的アルゴリズムとしては Soicher-McKay の絶対分解式を用いたアルゴリズム [28] と Stauduhar の相対分解式を用いたアルゴリズム [29] の二つが存在する．このうち Magma が採用しているのは後者（Stauduhar 流）を拡張したものであり, Geissler-Klüners [14], Geissler [13] や最近の進展である Fieker-Klüners [12] の結果に基づいている．また Galois 群が primitive である場合は, Soicher-McKay 流の手法と Stauduhar 流（の拡張）を組み合わせたハイブリッドな手法も用いられる．

続いて Frob_p の計算について概説する．今回扱う $\mathrm{PGL}_2(\mathbb{F}_\ell)$ では少し大き過ぎるので, Dokchitser の論文 [7] の 7 節に従って簡単な例を紹介する．$f(x) = x^3 - 2 \in \mathbb{Z}[x]$ の $\mathbb{Q}$ 上の最小分解体を K とすると $\mathrm{Gal}(K/\mathbb{Q}) \simeq S_3$（3 次対称群）となる．この Galois 群の共役類は三つ存在し, それぞれ $C_1 = [(1)]$, $C_2 = [(1\ 2)]$, $C_3 = [(1\ 2\ 3)]$ と置換群の記法で表すことにする．また $f(x)$ の K における根を $a_1 = \sqrt[3]{2}$, $a_2 = \zeta\sqrt[3]{2}$, $a_3 = \zeta^2\sqrt[3]{2}$ とする．但し ζ は 1 の原始 3 乗根とする．更に $h(x) = x^2/6 \in \mathbb{Q}[x]$ と選ぶ．このとき定理 4.7 より

$$\Gamma_C^h(X) := \prod_{\sigma\in C}\left(X - \sum_{1\le i\le 3}\frac{a_i^2}{6}\sigma(a_i)\right)$$

は各 C_i（$1 \le i \le 3$）に対して次のように計算出来る．

$$\begin{aligned}
\Gamma_{C_1}^h(X) &= X - \frac{1}{6}\left(a_1^2a_1 + a_2^2a_2 + a_3^2a_3\right)\\
&= X - 1,\\
\Gamma_{C_2}^h(X) &= \left(X - \frac{1}{6}(a_1^2a_2 + a_2^2a_1 + a_3^3)\right)\left(X - \frac{1}{6}(a_1^2a_3 + a_2^3 + a_3^2a_1)\right)\\
&\qquad\qquad \cdot\left(X - \frac{1}{6}(a_1^3 + a_2^2a_3 + a_3^2a_2)\right)\\
&= \left(X - \frac{1}{3}(\zeta + \zeta^2 + 1)\right)\left(X - \frac{1}{3}(\zeta^2 + 1 + \zeta)\right)\left(X - \frac{1}{3}(1 + \zeta + \zeta^2)\right)\\
&= X^3,
\end{aligned}$$

$$\begin{aligned}\Gamma^h_{C_3}(X) &= \left(X - \frac{1}{6}(a_1^2a_2 + a_2^2a_3 + a_3^2a_1)\right)\left(X - \frac{1}{6}(a_1^2a_3 + a_2^2a_1 + a_3^2a_2)\right)\\ &= \left(X - \frac{1}{3}(\zeta + \zeta + \zeta)\right)\left(X - \frac{1}{3}(\zeta^2 + \zeta^2 + \zeta^2)\right) = (X - \zeta)(X - \zeta^2)\\ &= X^2 + X + 1.\end{aligned}$$

さて, 定理 4.7 で述べられていた判定条件を書き換えると

$$\mathrm{Frob}_p \in C \Longleftrightarrow \Gamma^h_C\left(\mathrm{Tr}_{\frac{\mathbb{F}_p[x]}{x^3-2}/\mathbb{F}_p}\left(\frac{x^{p+2}}{6}\right)\right) \equiv 0 \bmod p$$

となる. $p = 3m + k$ ($k = 1, 2$) として右辺を計算してみると

$$\Gamma^h_C\left(\mathrm{Tr}_{\frac{\mathbb{F}_p[x]}{x^3-2}/\mathbb{F}_p}\left(\frac{x^{p+2}}{6}\right)\right) = \mathrm{Tr}_{\frac{\mathbb{F}_p[x]}{x^3-2}/\mathbb{F}_p}\left(\frac{1}{6}2^{m+1}x^{k-1}\right)$$

となるので, トレースの値は

- $k = 1$ のとき 2^m, 即ち $p \equiv 1 \bmod 3$ のとき $2^{(p-1)/3}$,
- $k = 2$ のとき 0, 即ち $p \equiv 2 \bmod 3$ のとき 0,

と計算出来る. 従って Frob_p が属する共役類は以下のように決定される.

- $p \equiv 1 \bmod 3$, かつ $2 \in (\mathbb{F}_p)^{\times 3}$ ならば $\mathrm{Frob}_p \in C_1$,
- $p \equiv 1 \bmod 3$, かつ $2 \notin (\mathbb{F}_p)^{\times 3}$ ならば $\mathrm{Frob}_p \in C_2$,
- $p \equiv 2 \bmod 3$ ならば $\mathrm{Frob}_p \in C_3$.

[7] の例 7.6 では Galois 群が $\mathrm{GL}_2(\mathbb{F}_3)$ に同型となる場合も紹介されている. この Galois 群の位数は 48 であり, 対応する拡大体は 8 次の多項式の $\mathbb{Q}$ 上の最小分解体となっている. こちらは 8 種類の共役類が登場し, Γ^h_C の係数も最大で 20 桁程度まで膨れ上がる.

以上の結果から Frob_p が計算出来たことにより, $\tau(p) \bmod \ell$ の計算が符号を除いて完了する. Bosman の結果からは $\ell = 11, 13, 17, 19$ に対して非常に大きな p であっても $\tau(p) \bmod \ell$ の値が求まる. Zeng-Yin [37] 及び Tian [33] はこれを $\ell = 29, 31$ にも行えるように改良している. 例えば $\ell = 31$ の場合, P^{proj}_ℓ は次で与えられる.

ℓ	P^{proj}_ℓ
31	$x^{32} - 4x^{31} - 155x^{28} + 713x^{27} - 2480x^{26} + 9300x^{25} - 5921x^{24} + 24707x^{23}$ $+127410x^{22} - 646195x^{21} + 747906x^{20} - 7527575x^{19} + 4369791x^{18}$ $-28954961x^{17} - 40645681x^{16} + 66421685x^{15} - 448568729x^{14} + 751001257x^{13}$ $-1820871490x^{12} + 2531110165x^{11} - 4120267319x^{10} + 4554764528x^9$ $-5462615927x^8 + 4607500922x^7 - 4062352344x^6 + 2380573824x^5$ $-1492309000x^4 + 521018178x^3 - 201167463x^2 + 20505628x - 1261963$

5 節の最後にも述べたが, 現時点での最高記録は Derickx-van Hoeij-Zeng [8] による $\ell \leq 41$ の結果であり, 今の所これよりも大きな ℓ で計算をすることは出来ない. これは $\tau(p) \bmod \ell$ の計算が $\log p$ と ℓ の多項式時間であることから分かる通り, ℓ の増加が p の増加に比べて計算を極めて困難にするためである. 3 節で述べたように, CRT により真の $\tau(p)$ を求めるためにはおよそ $\log p$ 以下のほとんど全ての ℓ に対して $\tau(p) \bmod \ell$ を計算しなければならないので, $p \approx 10^{1000}$ のクラスの問題では絶望的である.

さて Mascot [23] は Bosman らの手法を改良し, 符号の情報を残しつつ効率的に計算を行うことに成功した. ここでは $\rho_\ell(\mathrm{Frob}_p)$ の similarity class の情報も示されている. これにより, 2 節の最後に紹介した表の符号を確定させることが出来る. これに関しては論文 [23] の他に, プレプリント [25] にデータ一覧が掲載されている.

p	similarity class	$\tau(p) \bmod 19$
$10^{1000}+1357$	$\begin{bmatrix} 17 & 1 \\ 0 & 17 \end{bmatrix}$	4
$10^{1000}+7383$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	2
$10^{1000}+21567$	$\begin{bmatrix} 11 & 1 \\ 0 & 11 \end{bmatrix}$	3
$10^{1000}+27057$	$\begin{bmatrix} 10 & 0 \\ 0 & 9 \end{bmatrix}$	0
$10^{1000}+46227$	$\begin{bmatrix} 0 & 14 \\ 1 & 0 \end{bmatrix}$	0
$10^{1000}+57867$	$\begin{bmatrix} 17 & 0 \\ 0 & 2 \end{bmatrix}$	0
$10^{1000}+64749$	$\begin{bmatrix} 13 & 1 \\ 0 & 13 \end{bmatrix}$	7

Mascot の手法を用いた場合は $\ell \leq 29$ が限界である. この計算を行うにあたり, 最大で約 1800 万ビット（10 進換算で小数点以下約 540 万桁）精度での $\mathbb{C}$ 上の計算が用いられる[14].

§7. 応用例

$\tau(p) \bmod \ell$ を非常に大きな p に対して求められることは幾つかの応用（恩恵）をもたらす. 本節では二種類の応用について, 最近の結果と共に述べる.

まず非常に有名な “Lehmer の非消滅予想” を紹介する. この予想は数十年前に提唱されて以来未解決であり, 関連する整数論的話題（Bernoulli 数やゼータ関数）とも深く関連する予想である.

[14] これは定理 4.7 の検証（Frob_p の計算）で要求される.

予想 7.1 (Lehmer, [21])**.** $n \geq 1$ に対して $\tau(n) \neq 0$ が成り立つ.

[21] では既に $n < 3316799$ の範囲で検証されていたが, 数多くの更新を経て Bosman [3] が 2007 年に圧倒的な拡張を得ている.

命題 7.2 (Bosman, [3] 系 4.1)**.**

$$n < 22798241520242687999 \approx 2.28 \times 10^{19}$$

に対して予想 *7.1* は正しい.

この結果は Zeng-Yin [37] 及び Tian [33] により, 9.82×10^{20} 程度の n まで拡張された. 現在の最高記録は Derickx-van Hoeij-Zeng [8] による次の結果である.

命題 7.3 (Derickx-van Hoeij-Zeng, [8] 系 1.2)**.**

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

に対して予想 *7.1* は正しい.

命題 7.2 と 7.3（Zeng-Yin, Tian の結果も含む）はほとんど同じアイデアで証明される. 具体的には $\tau(p) = 0$ 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. 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 7.4 (Serre [27])**.** $\tau(p) = 0$ とする. このとき次が成り立つ.

- $p \equiv -1 \bmod 2^{14}3^7 5^3 691$,
- $p \equiv -1, 19, 31 \bmod 7^2$,
- $\left(\dfrac{p}{23}\right) = -1$（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. Bosman [3] は補題 7.4 の 3 条件を全てみたしつつ $\tau(p) \equiv 0 \bmod 11 \cdot 13 \cdot 17 \cdot 19$ をみたすような最小の p が 22798241520242687999 であることを計算によって確かめたわけである. その後 Zeng-Yin [37] と Tian [33] は $\tau(p) \bmod 31$ の計算を, Derickx-van Hoeij-Zeng [8] は $\tau(p) \bmod 41$ の計算を成功させたことにより, 記録を更新している.

もう一つ（現時点ではすぐに適用出来ないが）応用例を紹介する[15]. これは Δ に関する超特異素数についての結果である. まず最初に超特異素数を定義する.

定義 7.5. $\tau(p) \equiv 0 \bmod p$ をみたすような素数 p を, 固有形式 Δ に関する超特異素数（supersingular prime）とよぶ.

[15] これは主に木村巌氏（富山大学）から教えて頂いた内容に基づく.

名前からも推察出来る通り, このような素数はほとんど見つからない. 現在知られている結果の中で最も進んだものは次の Lygeros-Rozier の結果 [22] である.

命題 7.6 (Lygeros-Rozier, [22]). Δ に関する 10^{18} 未満の超特異素数は次の 6 個しか存在しない：

$$p = 2, 3, 5, 7, 2411, 7758337633.$$

特に $p = 7758337633$ については

$$\begin{aligned}\tau(p) &= 36341180311258200572533785506288217478604720527726228 82\\ &= 2 \times 31481 \times 7758337633 \times 74396385791962097778349200167647112298 17\end{aligned}$$

が成り立つ.

[22] では跡公式を用いた手法で計算を行っているが, 本稿で述べた計算法を更に改良出来れば超特異素数の探索に利用出来る可能性がある. これについては今後の課題としておく.

超特異素数という概念は複数の分野に跨る概念であり, その重要度も高い. 例えば楕円曲線に関する超特異素数とは, $\mathbb{Q}$ 上の楕円曲線を法 p 還元すると超特異楕円曲線（$\overline{\mathbb{F}}_p$ 上に非自明な p-等分点を持たない $\mathbb{F}_p$ 上の楕円曲線[16]）となるような p を指す. 超特異楕円曲線は, 例えば楕円曲線の岩澤理論など整数論のみならず, 近年では楕円曲線暗号の理論でも注目されている.

以上 Edixhoven-Couveignes の結果 [10] を中心として, 楕円モジュラー形式論における様々な理論的・計算機的進展について報告した. 特にここ 4,5 年の進展は目覚ましく, またそれらを支える数式処理システムの開発環境が整ってきたことも大きい. 筆者が初めてモジュラー形式の計算理論について興味を持ったきっかけとなったのは W. Stein による書籍 [31] であった. 出版当時はまだ Sage の開発も発展途上であったが, 現在では無料とは思えないような豊富な機能を揃えた一大システムとなった. 更にオープンソース（内部コードのほぼ全てを閲覧・変更可能な仕組み）であることを活かして, 世界中の計算機数論研究者が開発に協力出来るようになっている. 本稿をきっかけとして, 実際に数式処理ソフトに触れて頂き, モジュラー形式の計算理論に興味を持って頂ければ望外の喜びである. また, より便利な実装・パッケージの開発が急速に進み, これによって数論研究に数多くの良い影響や相乗効果が生まれることを願って止まない.

§8. 素数判定に関する補足

2 節及び 6 節で $p \approx 10^{1000}$ 程度の素数に対して $\tau(p) \bmod 19$ の値を掲載したが, そもそもこのような巨大な p をどうやって探すのかについて簡単に補足する[17]. 素数判定に関する文献は数多く出版されており, 数論の文献から暗号・セキュリティの文献に至るまで多種多様である. ここでは少し古い文献であるが読み易いものとして報告書 [15] を挙げておく. 興味のある方はこちらをご一読頂きたい. ここで最も強調しておきたいのは

[16] 正確にはこの曲線は「良い超特異還元（good supersingular reduction）を持つ楕円曲線」と言う.
[17] この話題は, 川田浩一氏（岩手大学）から頂いた御質問に基づいている.

「ある巨大な数 n が与えられたとき, それが素数であるか否かを判定する」

という問題の難しさと,

「ある巨大な数 n が与えられたとき, それを素因数分解する」

という問題の難しさは **全く異なる** という点である. 一般に巨大な素数を生成するには, 確率的素数判定アルゴリズムを繰り返し適用して行う. 代表的なものとして Fermat テスト, Miller-Rabin テストなどが挙げられる. なお GRH を仮定すれば Miller-Rabin テストは多項式時間アルゴリズムとなり, 高速に動作する. これに対して確定的素数判定アルゴリズムとしては古くから知られている Erathosthenes の篩法や AKS 素数判定法などが挙げられる. また特殊な素数に対する判定法も幾つか存在する. これらは実際に素因数分解を与えている訳ではないということに注意が必要である. 勿論 n が素数である場合は, 素数判定と素因数分解は等価となる. これに対し, 暗号・セキュリティの観点からは $n = pq$（p, q は巨大な素数）という形の合成数を利用する. これは「n が合成数であると判定する」ことと「実際に $n = pq$ と分解してみせる」ことが全く異なるという事実を利用している.

現在 RSA 暗号において推奨されている二つの素数の合成数 n はおよそ 4000 ビット（10^{1000} 程度）である. 現時点での分解記録が 768 ビット（10^{231} 程度）であることからも分かる通り, このレベルの素因数分解は無理と思われる. その一方で, 素数判定（ここでは素数生成と思って良い）の世界記録は 2013 年 1 月の $p = 2^{57885161} - 1$（$\approx 10^{17425169}$）である. これは 48 番目の Mersenne 素数であり, 分散計算を行うプロジェクト GIMPS[18] で得られた結果である. 従って $p \approx 10^{1000}$ 程度の素数判定は既に実時間で解決出来る問題となっている.

例として 2 節の表に登場した $p = 10^{1000} + 1357$ を確率的アルゴリズムを用いて素数判定してみる. Magma には G. Jaeschke [16] によるアルゴリズムが実装されており

```
magma: IsPrime(10^1000+1357: Proof:=false);
```

で実行出来る（`Proof:=false` が確率的アルゴリズムを採用せよという指令である）. 2 節・6 節と同様の環境でわずか 1.388 秒で高確率で素数であると判定する. Magma には他にも Atkin-Morain [1] による楕円曲線を用いた ECPP（Elliptic Curve Primary Proving）法が実装されているが, こちらは 100 桁以上の入力については未だ高速化されておらず, Miller-Rabin 法と比較しても低速となっている.

References

[1] A. O. L. Atkin and F. Morain, Elliptic curves and primality proving, *Math. Comp.* **61** (1993), pp.29-68.

[18] Great Internet Mersenne Prime Search の略. `http://www.mersenne.org/`

[2] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *Journal of Symbolic Computation*, **24** (1997), pp.235-265.
[3] J. Bosman, Explicit computations with modular Galois representations, *Ph.D thesis*, Universiteit Leiden (2008), 112pp.
[4] P. Bruin, Modular curves, Arakelov theory, algorithmic applications, *Ph.D thesis*, Universiteit Leiden (2010), 240pp.
[5] J. A. Buchmann and H. W. Lenstra, Approximating rings of integers in number fields, *Journal of Théor. Nombres Bordeaux* **6**, no.2 (1994), pp.221-260.
[6] D. X. Charles, Computing the Ramanujan tau function, *The Ramanujan Journal*, **11**, Issue 2 (2006), pp.221-224.
[7] T. Dokchitser and V. Dokchitser, Identifying Frobenius elements in Galois groups, *Journal of Algebra and Number Theory* **7**, no.6 (2013), pp.1325-1352.
[8] 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`.
[9] B. Edixhoven, The weight in Serre's conjectures on modular forms, *Invent. Math.* **109** (1992), pp.563-594.
[10] B. Edixhoven and J.-M. Couveignes (eds.), Computational aspects of modular forms and Galois representations, *Annals of Mathematics Studies, Princeton University Press* (2011), 440pp. Also available from `arXiv:math/0605244`.
[11] D. Farmer and K. James, The irreducibility of some level 1 Hecke polynomials, *Math. Comp.* **71**, no.239 (2002), pp.1263-1270.
[12] C. Fieker and J. Klüners, Computation of Galois groups of rational polynomials, *to appear in LMS Computational Section* (2013), 26pp.
[13] K. Geissler, Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern, *Ph.D thesis*, TU-Berlin (2003), 217pp.
[14] K. Geissler and J. Klüners, The determination of Galois groups, *J. Symbolic Comp.* **30** (2000), no.6, pp.653-674.
[15] 独立行政法人情報処理推進機構（IPA）編, 素数生成アルゴリズムの調査・開発：調査報告書 (2003), `http://www.ipa.go.jp/security/fy14/crypto/prime_num/invest.pdf` より入手可能, 50pp.
[16] G. Jaeschke, On strong pseudoprimes to several bases, *Math. Comp.* **61** (1993), pp.915-926.
[17] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture (I), (II), *Invent. Math.* **178** (2009), pp.485-504 (I), pp.505-586 (II).
[18] K. Khuri-Makdisi, Asymptotically fast group operations on Jacobians of general curves, *Math. Comp.* **76** (2007), pp.2213-2239.
[19] 木田雅成, 初心者のための Magma 入門, *MI* レクチャーノート **29**, 「*Magma* で広がる数学の世界」(2010), pp.1-13.
[20] 木村巌, 数論研究者のための Sage, *RIMS Kôkyûroku Bessatsu* **B32** (2012), pp.125-144.
[21] D. H. Lehmer, The vanishing of Ramanujan's function $\tau(n)$, *Duke Math. J.* **10** (1947), pp.429-433.
[22] N. Lygeros and O. Rozier, A new solution to the equation $\tau(p) \equiv 0 \pmod{p}$, *Journal of Integer Sequences* **13**, Article 10.7.4 (2010).
[23] N. Mascot, Computing modular Galois representations, *Publié dans Rendiconti del Circolo Matematico di Palermo* **62** (2013), no.3, pp.451-476.
[24] N. Mascot, Tables of modular Galois representations, *preprint* (2013), 32pp. `arXiv:math/1312.6418`.

[25] N. Mascot, Tables of modular Galois representations, *preprint* (2013), 24pp.
[26] K. Ribet and W. Stein, Lectures on modular forms and Hecke operators, available on `http://wstein.org/books/ribet-stein/main.pdf` (2011), 274pp.
[27] J.-P. Serre, Sur la lacunarité des puissances de η, *Glasgow Math. J.* **27** (1985), pp.203-221.
[28] L. H. Soicher and J. McKay, Computing Galois groups over the rationals, *J. Number Theory* **20** (1985), pp.273-281.
[29] R. P. Stauduhar, The determination of Galois groups, *Math. Comp.* **27** (1973), pp.981-996.
[30] W. Stein et al., Sage Mathematics Software (Version 6.0), *The Sage Development Team*, 2014, `http://www.sagemath.org`.
[31] W. Stein, Modular Forms: A Computational Approach, *AMS Graduate Studies in Mathematics* **79**, 282pp.
[32] 田口雄一郎, Serre の保型性予想の紹介, *RIMS Kôkyûroku Bessatsu* **B19** (2010), pp.7-22.
[33] P. Tian, Further computations of Galois representations associated to modular forms, *preprint*, 14pp. `arXiv:math/1311.0577`.
[34] P. J. Weinbeger, Finding the number of factors of a polynomial , *Journal of Algorithms*, **5**, no.2 (1984), pp.180-186.
[35] 横山俊一, Serre の保型性予想をめぐって：計算機的保型形式論入門, *MI* レクチャーノート **29**, 「*Magma* で広がる数学の世界」(2010), pp.107-133.
[36] 横山俊一, Serre の保型性予想をめぐって：計算機的保型形式論入門 - Sage ユーザーのための改訂版, *MathLibre Docs* に収録予定, 筆者のウェブページよりダウンロード可能：`http://imi.kyushu-u.ac.jp/~s-yokoyama/files/ModularInstructionForSage.pdf`.
[37] J. Zeng and L. Yin, On the computation of coefficients of modular forms: the reduction modulo p approach, *to appear in Math. Comp.*, 16pp.