# The number of linear factors of supersingular polynomials and sporadic simple groups

九州大学・多重ゼータ研究センター　中屋 智瑛*
Tomoaki Nakaya
Multiple Zeta Research Center, Kyushu University

講演では，あるレベル付き超特異多項式の既約分解における線形因子の個数を，虚二次体の類数の線形和として明示的に表した．さらにそれらの超特異多項式が線形因子のみに既約分解される素数の集合と，ある散在型単純群の位数の素因数の集合との一致をみた．本稿の内容は論文 [14] として既にアクセプトされているため証明の細部には立ち入らず，議論の大まかな流れと結果のみ述べる．詳細は論文の方を参照されたい．また最後に，論文や講演では触れていない合成数レベルの群に関する超特異多項式や，ある三角群に由来する超幾何多項式の既約分解についても簡単に触れる．

## 1　はじめに

標数 $p>0$ の体 $K$ 上の楕円曲線 $E$ が超特異的 (supersingular) であるとは，$E$ が $\overline{K}$ 上 $p$-torsion を持たないことをいう．この条件は $E$ の $j$ 不変量のみに依存し，超特異 $j$ 不変量は $p$ を固定するごとに有限個しかなく，かつそれらは全て $\overline{\mathbb{F}}_p$ に入ることが知られている．そこで超特異多項式 $ss_p(X)$ を，根がちょうど超特異 $j$ 不変量になるような次のモニック多項式で定める：

$$ss_p(X)=\prod_{\substack{E/\overline{\mathbb{F}}_p\\ E:\text{supersingular}}}\big(X-j(E)\big).$$

標数 $p$ の超特異 $j$ 不変量の集合は $\mathbb{F}_p$ 上の共役に関して stable であるから，$ss_p(X)\in\mathbb{F}_p[X]$ であることに注意する．Deuring による結果から超特異 $j$ 不変量が $\mathbb{F}_{p^2}$ に入ること，したがって $ss_p(X)$ を $\mathbb{F}_p$ 上既約分解すると高々二次因子までしか現れないことや，$ss_p(X)$ の次数（すなわち標数 $p$ の超特異楕円曲線の同型類の個数）

$$\deg ss_p(X)=\begin{cases}1 & \text{if } p=2 \text{ or } 3,\\ \frac{p-1}{12}+\frac{1}{4}\left(1-\left(\frac{-1}{p}\right)\right)+\frac{1}{3}\left(1-\left(\frac{-3}{p}\right)\right) & \text{if } p\geq 5\end{cases}$$

も分かっている ([6, 9] および [18, Ch.V §4] 参照)．ここで $(\frac{*}{p})$ は Legendre 記号である．なお $p=2,3$ に対して $ss_p(X)=X\pmod p$ である ([3, p.201])．

*t-nakaya@math.kyushu-u.ac.jp

さて, 特に興味深い $ss_p(X)$ の性質としてモンスター群 $\mathbb{M}$ の位数との関係があげられる. モンスター群 $\mathbb{M}$ は 26 個存在する散在型単純群の中で位数最大のものであり，位数は

$$\begin{aligned}\#\mathbb{M} &= 808017424794512875886459904961710757005754368000000000\\ &= 2^{46}\cdot 3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71\end{aligned}$$

である．初め Ogg が気付いたことであるが，これらの素因数 $p$ に対して超特異 $j$ 不変量は $\mathbb{F}_p$ 上定義される．すなわち，

$$ss_p(X) \text{ が線形因子のみに既約分解される} \iff p \mid \#\mathbb{M} \tag{1}$$

が成り立つ ([15, p.7], [5])．証明には $ss_p(X)$ の線形因子の個数に関する次の結果と，類数評価を用いる．

**Theorem 1.** $p$ を 5 以上の素数, $ss_p(X)$ の $\mathbb{F}_p$ 上の既約分解における線形因子の個数を $L(p)$, 虚二次体 $\mathbb{Q}(\sqrt{-p})$ の類数を $h(\sqrt{-p})$ とおくとき

$$L(p) = \begin{cases} \frac{1}{2}h(\sqrt{-p}) & \text{if } p \equiv 1 \mod 4,\\ 2h(\sqrt{-p}) & \text{if } p \equiv 3 \mod 8,\\ h(\sqrt{-p}) & \text{if } p \equiv 7 \mod 8.\end{cases}$$

この結果も本質的には Deuring によるものである ([3, §10]，[4, eq.(9)])．しかしここで述べた形とは若干違う形で主張されている ([16, Lemma 2.6], [1, p.97] を参照)．この記号の下で先程の主張 (1) は

$$\deg ss_p(X) = L(p) \iff p \mid \#\mathbb{M} \tag{2}$$

と書き直される．しかし類数評価を用いた証明は，何故このような一致が生じるのか，という疑問に対して解答を与えてくれない．

## 2　主結果

本節で述べる結果は，超特異多項式のレベル付き類似物の線形因子の個数の明示公式と，(2) の一般化である．以下，5 以上の素数 $p$ に対して数 $\nu, \delta, \varepsilon \in \{0, 1\}$ を Legendre 記号を用いて

$$\nu = \frac{1}{2}\left(1 - \left(\frac{-2}{p}\right)\right),\ \delta = \frac{1}{2}\left(1 - \left(\frac{-3}{p}\right)\right),\ \varepsilon = \frac{1}{2}\left(1 - \left(\frac{-1}{p}\right)\right)$$

と定める．超特異多項式の標数 0 への様々な持ち上げが研究されている．例えば，素数 $p \geq 5$ に対して $m = [p/12]$ とおくとき ($[\cdot]$ は Gauss 記号)，

$$ss_p(X) = X^{m+\delta}(X - 1728)^{\varepsilon}\,{}_2F_1\left(-m, \frac{5}{12} - \frac{2\delta - 3\varepsilon}{6}; 1; \frac{1728}{X}\right) \pmod p \tag{3}$$

が成り立つ (これも本質的には Deuring による)．ここで ${}_2F_1(\alpha, \beta; \gamma; x)$ は Gauss の超幾何級数である：

$${}_2F_1(\alpha, \beta; \gamma; x) = \sum_{n=0}^{\infty} \frac{(\alpha)_n(\beta)_n}{(\gamma)_n}\frac{x^n}{n!}.$$

記号 $(\alpha)_n$ は $(\alpha)_0=1$，$(\alpha)_n=\alpha(\alpha+1)\cdots(\alpha+n-1)$ $(n\geq 1)$ で定める．したがって特に $\alpha,\beta$ が負整数の場合に多項式を与えることに注意する．

Atkin 直交多項式と呼ばれる，超特異多項式の標数 0 への持ち上げが存在する ([10])．そのレベル付き類似物の研究において，超特異多項式のレベル付き類似物が研究されている．より具体的には，合同部分群 $\Gamma_0(N)$ $(N=2,3,4)$ に関する超特異多項式 $ss_p^{(N)}(X)$ が Tsutsumi [19] により，Fricke 群 $\Gamma_0^*(N)$ $(N=2,3)$ に関する超特異多項式 $ss_p^{(N*)}(X)$ が Koike [11]，Sakai [17] によって定義されており，特に後者の超幾何多項式表示は，素数 $p\geq 5$ に対して $m_2=[p/8], m_3=[p/6]$ とおくとき

$$ss_p^{(2*)}(X)=X^{m_2+\varepsilon}(X-256)^{\nu}{}_2F_1\left(-m_2,\frac{3}{8}-\frac{\varepsilon-2\nu}{4};1;\frac{256}{X}\right)\pmod p,$$
$$ss_p^{(3*)}(X)=X^{m_3+\delta}(X-108)^{\delta}{}_2F_1\left(-m_3,\frac{1}{3}+\frac{\delta}{3};1;\frac{108}{X}\right)\pmod p$$

である．なお，$N,p\in\{2,3\}$ に対しては $ss_p^{(N*)}(X)=X \pmod p$ である．また次数は各々

$$\deg ss_p^{(2*)}(X)=m_2+\varepsilon+\nu=\frac{p-1}{8}+\frac{3}{8}\left(1-\left(\frac{-1}{p}\right)\right)+\frac{1}{4}\left(1-\left(\frac{-2}{p}\right)\right),$$
$$\deg ss_p^{(3*)}(X)=m_3+2\delta=\frac{p-1}{6}+\frac{2}{3}\left(1-\left(\frac{-3}{p}\right)\right).$$

これらのレベル付き超特異多項式を既約分解したとき，モンスター群以外の散在型単純群の位数と何らかの対応がつくのではないか，という素朴な発想のもと研究を行った結果，以下を得た．

**Theorem 2.** ([14, Theorem 4]) 素数 $p\geq 5$ に対して以下が成り立つ：

$$L^{(2*)}(p)=\frac{1}{8}\left\{2+\left(1-\left(\frac{-1}{p}\right)\right)\left(4+\left(\frac{-2}{p}\right)\right)\right\}h(\sqrt{-p})+\frac{1}{4}h(\sqrt{-2p}),$$
$$L^{(3*)}(p)=\delta L(p)+\frac{1}{8}\left\{2+\left(1+\left(\frac{-1}{p}\right)\right)\left(2+\left(\frac{-2}{p}\right)\right)\right\}h(\sqrt{-3p}).$$

元の $ss_p(X)$ の場合と異なり，線形因子の個数が虚二次体 $\mathbb{Q}(\sqrt{-p})$ と $\mathbb{Q}(\sqrt{-Np})$ の類数の線形和となっていることが特徴的である．さらに，これらの線形因子の個数の明示式を用いて類数評価を行うことで，$ss_p^{(2*)}(X)$ が線形因子のみ持つような素数と，ベビーモンスター群 $\mathbb{B}$，Fischer 群 $Fi'_{24}$ の位数

$$\begin{aligned}\#\mathbb{B}&=4154781481226426191177580544000000\\&=2^{41}\cdot 3^{13}\cdot 5^6\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 31\cdot 47,\\ \#Fi'_{24}&=1255205709190661721292800\\&=2^{21}\cdot 3^{16}\cdot 5^2\cdot 7^3\cdot 11\cdot 13\cdot 17\cdot 23\cdot 29.\end{aligned}$$

の素因数との関係を得た．

**Theorem 3.** ([14, Theorem 5]) 素数 $p$ に対して以下が成り立つ：

$$\deg ss_p^{(2*)}(X) = L^{(2*)}(p) \Longleftrightarrow p \mid \#\mathbb{B},$$
$$\deg ss_p^{(3*)}(X) = L^{(3*)}(p) \Longleftrightarrow p \mid \#Fi'_{24}.$$

これらの結果は Brillhart-Morton による Legendre 多項式の既約分解に関する結果と，Tsutsumi，Koike，Sakai によるレベル付き超特異多項式に関する結果を巧妙に組み合わせることで得られる．その際に鍵となるのは超幾何級数の代数変換公式 (Kummer's relation) [8, §2.1.5., eq.(27)]

$$ {}_2F_1\left(2\alpha, 2\beta; \alpha+\beta+\frac{1}{2}; z\right) = {}_2F_1\left(\alpha, \beta; \alpha+\beta+\frac{1}{2}; 4z(1-z)\right) \tag{4}$$

である．これに加えて，合同部分群 $\Gamma_0(N)$ と Fricke 群 $\Gamma_0^*(N)$ に関するモジュラー関数 $j_N(\tau), j_N^*(\tau)$ $(N=2,3)$ が満たす代数関係式

$$\frac{256}{j_2^*(\tau)} = 4\cdot\frac{64}{j_2(\tau)}\left(1-\frac{64}{j_2(\tau)}\right), \quad \frac{108}{j_3^*(\tau)} = 4\cdot\frac{27}{j_3(\tau)}\left(1-\frac{27}{j_3(\tau)}\right)$$

と (4) の変数部分がうまく対応することにも注意しておく．

## 2.1 Legendre 多項式の既約分解

Brillhart と Morton は次の (超幾何) 多項式 $W_m(x) \pmod p$ の既約分解における線形因子の個数を具体的に求めた：

$$W_m(X) := \sum_{r=0}^{m} \binom{m}{r}^2 X^r = {}_2F_1(-m, -m; 1; X).$$

良く知られているように，Legendre 標準形

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

の Hasse 不変量は $W_{(p-1)/2}(\lambda)$ で与えられ，楕円曲線 $E_\lambda$ が超特異となるのは $W_{(p-1)/2}(\lambda) \equiv 0 \pmod p$ のときかつそのときに限る．以下の結果についても各々適当な楕円曲線の標準形との関係がある．

**Theorem 4** (Brillhart, Morton [1])**.** 素数 $p \geq 5$ に対して $N_1(p,m)$ で多項式 $W_m(X) \pmod p$ の線形因子の個数を表す．このとき，

$$N_1\left(p, \left[\frac{p}{4}\right]\right) = \frac{1}{4}\left\{2+\left(1-\left(\frac{-1}{p}\right)\right)\left(4+\left(\frac{-2}{p}\right)\right)\right\} h(\sqrt{-p}) - \varepsilon,$$
$$N_1\left(p, \left[\frac{p}{3}\right]\right) = \delta\,(2L(p)-1),$$

ここで $L(p)$ は元々の $ss_p(X)$ の線形因子の個数である．

多項式 $W_m(X)$ と $P_m(X)$ には以下のような関係が成り立つことに注意する [1, p.80]：

$$W_m(X) = (1-X)^m P_m\left(\frac{1+X}{1-X}\right).$$

これにより両者の既約分解における線形因子の個数が一致するため，$ss_p^{(N)}(X)$ の線形因子の個数が分かることに注意する．さらに Morton は Legendre 多項式の特定の二次因子の個数に関し，以下を示している．

**Theorem 5** (Morton [12, 13])．素数 $p \geq 5$ に対して $B(p,m)$ で Legendre 多項式 $P_m(X) \pmod p$ の既約二次因子のうち $X^2+C$ という形をしているものの個数を表す．このとき，

$$B\left(p, \left[\frac{p}{4}\right]\right) = \frac{1}{4}\left\{h(\sqrt{-2p}) - 2(\varepsilon+\nu)\right\}, \quad B\left(p, \left[\frac{p}{3}\right]\right) = \frac{1}{4}\left\{a_p h(\sqrt{-3p}) - 4\delta\right\},$$

ここで

$$a_p = \frac{1}{2}\left\{2 + \left(1 + \left(\frac{-1}{p}\right)\right)\left(2 + \left(\frac{-2}{p}\right)\right)\right\}.$$

## 2.2 $\Gamma_0(N)$ $(N=2,3)$ に関する超特異多項式

Tsutsumi は [19] において低レベルの合同部分群に関する超特異多項式を定義し，その超幾何多項式表示を求めた．その際に，楕円モジュラー関数 $j(\tau)$ と $\Gamma_0(N)$ $(N=2,3)$ に関するモジュラー関数 $j_N(\tau)$ の満たす代数関係式

$$\begin{aligned}(j_2(\tau)+192)^3 - j(\tau)\,(j_2(\tau)-64)^2 &= 0,\\ j_3(\tau)\,(j_3(\tau)+216)^3 - j(\tau)\,(j_3(\tau)-27)^3 &= 0.\end{aligned} \tag{5}$$

を元にしている．より具体的には，まず集合 $S_N$ を

$$S_N := \{j_N \in \overline{\mathbb{F}}_p \,|\, \text{the } j\text{-invariant determined by (5) is supersingular}\}$$

と定める ($p$ にも依存していることに注意)．さらに元の $ss_p(X)$ の場合に倣って，

$$ss_p^{(N)}(X) = \prod_{j_N \in S_N} (X - j_N) \in \overline{\mathbb{F}}_p[X]$$

と定めるのである． 例えば $ss_2(X) = X \pmod 2$ より 0 が標数 2 における超特異 $j$ 不変量であるから $(j_2-192)^3 - 0\cdot(j_2-64)^2 \equiv 0 \pmod 2$ となり，これを解いて $j_2 \equiv 0 \pmod 2$ が標数 2 における超特異 $j_2$ 不変量となる．したがってこの場合 $S_2 = \{0\}, ss_2^{(2)}(X) = X \pmod 2$ となる．集合 $S_N$ は $\mathbb{F}_p$ 上の共役に関して stable より，$ss_p^{(N)}(X) \in \mathbb{F}_p[X]$ であることに注意しておく．

**Proposition 6** (Tsutsumi [19])． (i) 素数 $p \geq 5$ に対して $m = [p/4]$ とおく．このとき

$$ss_p^{(2)}(X) = X^{m+\varepsilon}\,{}_2F_1\left(-m, \frac{3}{4} - \frac{\varepsilon}{2}; 1; \frac{64}{X}\right) \pmod p.$$

(ii) 素数 $p \geq 5$ に対して $m = [p/3]$ とおく．このとき

$$ss_p^{(3)}(X) = X^{m+\delta}{}_2F_1\left(-m, \frac{2}{3} - \frac{\delta}{3}; 1; \frac{27}{X}\right) \pmod{p}.$$

これらの多項式の次数は以下で与えられる．

$$\deg ss_p^{(2)}(X) = \frac{p-1}{4} + \frac{1}{2}\varepsilon, \quad \deg ss_p^{(3)}(X) = \frac{p-1}{3} + \frac{2}{3}\delta.$$

**Proposition 7.** 素数 $p \geq 5$ に対して，$L^{(N)}(p)\,(N = 2, 3)$ で $ss_p^{(N)}(X) \pmod{p}$ の線形因子の個数を表す．このとき

$$L^{(2)}(p) = N_1\left(p, \left[\frac{p}{4}\right]\right) + \varepsilon, \quad L^{(3)}(p) = N_1\left(p, \left[\frac{p}{3}\right]\right) + \delta.$$

したがって，定理 1 と定理 4 より $L^{(N)}(p)\,(N = 2, 3)$ は類数 $h(\sqrt{-p})$ の定数倍である．

$N = 2, 3$ に対して，$ss_p^{(N)}(X) \pmod{p}$ と Brillhart-Morton の用いた多項式 $W_m(X)$ は (変数の適当な一次分数変換のもとで) ほぼ等しい．これにより上の命題が分かる．

さて，ここまでに現れた超特異多項式はある超幾何多項式によって表示されたが，それ以外にも興味深い表示をもつ．例えば多項式 $ss_p^{(2)}(X) \pmod{p}$ はその超幾何多項式表示に注目することで

$$X^{[p/4]+\varepsilon}{}_2F_1\left(\frac{1}{4}, \frac{3}{4}; 1; \frac{64}{X}\right)$$

の多項式部分の法 $p$ 還元と見なせる．したがって簡単な二項係数の計算から，次のような $ss_p^{(2)}(X)$ の表示が分かる．$ss_p^{(3)}(X)$ の場合も同様の計算から分かる．

**Theorem 8.** 素数 $p \geq 5$ に対して，

$$ss_p^{(2)}(X) = \sum_{n=0}^{(p-1+2\varepsilon)/4} \binom{2n}{n}\binom{4n}{2n} X^{(p-1+2\varepsilon)/4-n} \pmod{p},$$

$$ss_p^{(3)}(X) = \sum_{n=0}^{(p-1+2\delta)/3} \binom{2n}{n}\binom{3n}{n} X^{(p-1+2\delta)/3-n} \pmod{p}.$$

同様にして，超幾何級数に関する Clausen の公式 [8, §4.3., eq.(1)]

$${}_2F_1(\alpha, \beta; \alpha + \beta + 1/2; x)^2 = {}_3F_2(2\alpha, 2\beta, \alpha + \beta; 2\alpha + 2\beta, \alpha + \beta + 1/2; x)$$

を用いて係数を計算することで，$SL_2(\mathbb{Z}), \Gamma_0^*(N)\ (N = 2, 3)$ に関する超特異多項式の平方の，二項係数を用いた表示を得る．

**Theorem 9.** 素数 $p \geq 5$ に対して

$$ss_p(X)^2 = (X - 1728)^{\varepsilon} \sum_{n=0}^{(p-1+8\delta)/6} \binom{2n}{n}\binom{3n}{n}\binom{6n}{3n} X^{(p-1+8\delta)/6-n} \pmod{p},$$

$$ss_p^{(2*)}(X)^2 = (X - 256)^{\nu} \sum_{n=0}^{(p-1+6\varepsilon)/4} \binom{2n}{n}^2\binom{4n}{2n} X^{(p-1+6\varepsilon)/4-n} \pmod{p},$$

$$ss_p^{(3*)}(X)^2 = X^{\delta}(X - 108)^{\delta} \sum_{n=0}^{(p-1+2\delta)/3} \binom{2n}{n}^2\binom{3n}{n} X^{(p-1+2\delta)/3-n} \pmod{p}.$$

## 2.3　レベル 5 以上 71 以下に対する予想

本節以降，文字 $N$ は常にモンスター群の位数の素因数を表すとする．

$$N \in \mathfrak{S} := \{2,3,5,7,11,13,17,19,23,29,31,41,47,59,71\}.$$

合同部分群のときと同様に，レベル $N$ の Fricke 群 $\Gamma_0^*(N)$ に関する超特異多項式 $ss_p^{(N*)}(X)$ は楕円モジュラー関数 $j(\tau)$ と $\Gamma_0^*(N)$ に関するモジュラー関数 $j_N^*(\tau)$ の満たす代数関係式を通じて定義する．レベル 5,7 に対してもはや超幾何多項式による簡単な表示は望めない (と思われる) が，Heun 多項式を用いた予想式は存在する．ここでは超特異多項式の平方に関する予想を述べるにとどめる．数 $u_5^*(n), u_7^*(n)$ を

$$u_5^*(n) = \binom{2n}{n}\left\{\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}\right\},\ u_7^*(n) = \sum_{k=0}^{n}\binom{n}{k}^2\binom{2k}{n}\binom{n+k}{k}$$

で定義する．後者の和は，二項係数が消えることから $k = \lceil n/2 \rceil$ から始まるとしてもよい．なお，$\{u_5^*(n)/\binom{2n}{n}\}_{n\geq 0}$ は Apéry が $\zeta(2)$ の無理性 ($\zeta(3)$ ではない) を証明する際に用いた数列である．

**Conjecture 10.**　(i) 素数 $p \geq 7$ に対して

$$ss_p^{(5*)}(X)^2 = (X^2 - 44X - 16)^{\mu_5} \sum_{n=0}^{2(m_5+\mu_5)} u_5^*(n) X^{2(m_5+\mu_5)-n} \pmod p.$$

(ii) 素数 $p = 5$，$p \geq 11$ に対して

$$ss_p^{(7*)}(X)^2 = (X+1)^{\mu_7}(X-27)^{\mu_7} \sum_{n=0}^{2(m_7+\mu_7)} u_7^*(n) X^{2(m_7+\mu_7)-n} \pmod p.$$

ここで，

$$m_5 = \frac{p-1}{4} + \frac{1}{4}\left(1 - \left(\frac{-1}{p}\right)\right) - \mu_5, \quad \mu_5 = \frac{1}{2}\left(1 - \left(\frac{-5}{p}\right)\right),$$
$$m_7 = \frac{p-1}{3} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) - \mu_7, \quad \mu_7 = \frac{1}{2}\left(1 - \left(\frac{-7}{p}\right)\right).$$

さらに散在型単純群との関係も予想される．$HN$ を Harada-Norton 群，$He$ を Held 群とする．これらの群の位数は

$$\#HN = 273030912000000 = 2^{14}\cdot 3^6\cdot 5^6\cdot 7\cdot 11\cdot 19,$$
$$\#He = 4030387200 = 2^{10}\cdot 3^3\cdot 5^2\cdot 7^3\cdot 17.$$

である．$L^{(N*)}(p)$ を $ss_p^{(N*)}(X)$ の線形因子の個数とするとき以下が成り立つと予想される．

**Conjecture 11.** 素数 $p$ に対して

$$\deg ss_p^{(5*)}(X) = L^{(5*)}(p) \iff p \mid \#HN,$$
$$\deg ss_p^{(7*)}(X) = L^{(7*)}(p) \iff p \mid \#He.$$

レベルが5以上の超特異多項式に対して証明できていることは全くないが，計算機実験によってその次数および線形因子の個数について統一的な予想を立てることはできている．

**Conjecture 12.** $p \geq 5$ を素数とし $N \in \mathfrak{S} - \{2\}$ かつ $N \neq p$ であるとする．このとき，

$$\begin{aligned}\deg ss_p^{(N*)}(X) = \frac{(N+1)(p-1)}{24} + \frac{1}{8}\left(1+\left(\frac{-1}{N}\right)\right)\left(1-\left(\frac{-1}{p}\right)\right) \\ + \frac{1}{6}\left(1+\left(\frac{-3}{N}\right)\right)\left(1-\left(\frac{-3}{p}\right)\right) + \frac{1}{2}\left(1-\left(\frac{-N}{p}\right)\right)\deg ss_N(X).\end{aligned}$$

いま $N \in \mathfrak{S}$ は素数なので $ss_N(X)$ は定義されていることに注意する．

**Conjecture 13.** $p \geq 5$ を素数とし $N \in \mathfrak{S} - \{2\}$ かつ $N \neq p$ であるとする．このとき，

$$\begin{aligned}L^{(N*)}(p) = \frac{1}{2}\left(1+\left(\frac{-p}{N}\right)\right)L(p) \\ + \frac{1}{8}\left\{2+\left(1-\left(\frac{-1}{Np}\right)\right)\left(2+\left(\frac{-2}{Np}\right)\right)\right\}h(\sqrt{-Np}).\end{aligned}$$

さて主結果の一つは，例えばレベル $N=2$ については

$$\deg ss_p^{(2*)}(X) = L^{(2*)}(p) \iff p \mid \#\mathbb{B} \tag{6}$$

という形をしていた．つまり固定されたレベルに対してある性質を持つような素数 $p$ の集合に関する主張であった．これとは逆に (小さい)$p$ を固定したとき，レベルと素数に関するある種の「双対性」を見て取ることができる．

**Observation 1.** $N \in \mathfrak{S}$ に対して，以下が成り立つ．

$$\begin{aligned}\deg ss_2^{(N*)}(X) = L^{(N*)}(2) &\iff N \mid \#\mathbb{B}, \\ \deg ss_3^{(N*)}(X) = L^{(N*)}(3) &\iff N \mid \#Fi'_{24}, \\ \deg ss_5^{(N*)}(X) = L^{(N*)}(5) &\iff N \mid \#HN, \\ \deg ss_7^{(N*)}(X) = L^{(N*)}(7) &\iff N \mid \#He.\end{aligned}$$

(6) の左から右への矢印は無限個の素数 $p$ に対して確認する必要がある．そのため証明の際には類数評価を用いて有限個の素数 $p$ に対する計算に落とし込む必要があった．一方でこちらは有限個の素数 $N$(=モンスター群の位数の素因数) に対して確認すればよい．この「双対性」の意味は今のところよく分からない．

## 3　その他の観察・予想

本節では講演や論文 [14] では扱っていないタイプの超特異多項式の既約分解について，計算機実験の結果をごく簡単に紹介する．

### 3.1 合成数レベルの場合

ここまでの議論から分かるように，楕円モジュラー関数 $j(\tau)$ と適当な群のモジュラー関数の満たす代数関係式を用いて，その群に関する超特異多項式を (形式的には) 定義することができる．さて，モンスター群 $\mathbb{M}$ の共役類は 194 個あり，対応するモジュラー関数 (いわゆる McKay-Thompson 級数) の具体形は Conway-Norton [2] にある．例えば彼らの記号で $NA$ という共役類は Fricke 群 $\Gamma_0^*(N)$ $(N \in \mathfrak{S})$ に関するモジュラー関数 $j_N^*(\tau)$ と対応しているが，これ以外の幾つかのレベル (共役類) に対しても超特異多項式を定義し，次数や線形因子の個数を求める計算機実験を行った．以下ではレベル 6 の場合の (Conway-Norton の記号では $6A$ から $6F$ に対応する) 予想を紹介する．

**Conjecture 14.** $\nu_n := \frac{1}{2}\left(1 - \left(\frac{-n}{p}\right)\right)$ とする．このとき素数 $p \geq 5$ に対して

$$\begin{aligned}
&\deg ss_p^{(6F)}(X) = \frac{3(p-1)}{4} + \frac{3}{2}\nu_1, \quad \deg ss_p^{(6E)}(X) = p-1,\\
&\deg ss_p^{(6D)}(X) = \frac{p-1}{2} + \nu_2, \quad \deg ss_p^{(6C)}(X) = \frac{p-1}{2} + \nu_3,\\
&\deg ss_p^{(6B)}(X) = \frac{p-1}{2} + \nu_6, \quad \deg ss_p^{(6A)}(X) = \frac{p-1}{4} + \frac{1}{2}(\nu_2+\nu_3+\nu_6).
\end{aligned}$$

**Conjecture 15.** 素数 $p \geq 5$ に対して $L^{(6w)}(p)$ で $ss_p^{(6w)}(X) \pmod p$ の線形因子の個数を表すとする．また $L^{(2)}(p)$ は命題 7 で見たように $ss_p^{(2)}(X) \pmod p$ の線形因子の個数とする．このとき

$$\begin{aligned}
L^{(6F)}(p) &= \left(2 + \left(\frac{-3}{p}\right)\right) L^{(2)}(p),\\
L^{(6E)}(p) &= 2\nu_3\, L^{(2)}(p),\\
L^{(6D)}(p) &= \nu_3\, L^{(2)}(p) + \frac{1}{4}\left(1 + \left(\frac{-3}{p}\right)\right) h(\sqrt{-2p}),\\
L^{(6C)}(p) &= \nu_3\, L^{(2)}(p) + \frac{1}{8}\left\{2 + \left(1 + \left(\frac{-1}{p}\right)\right)\left(4 + \left(\frac{-2}{p}\right)\right)\right\} h(\sqrt{-3p}),\\
L^{(6B)}(p) &= \nu_3\, L^{(2)}(p) + \frac{1}{4} h(\sqrt{-6p}),\\
L^{(6A)}(p) &= \frac{\nu_3}{2} L^{(2)}(p) + \frac{1}{8}\left(1 + \left(\frac{-3}{p}\right)\right) h(\sqrt{-2p})\\
&\quad + \frac{1}{8}\left\{2 + \left(1 + \left(\frac{-1}{p}\right)\right)\left(4 + \left(\frac{-2}{p}\right)\right)\right\} h(\sqrt{-3p}) + \frac{1}{8} h(\sqrt{-6p}).
\end{aligned}$$

超特異多項式 $ss_p^{(6w)}(X)$ $(w = A, B, \ldots, F)$ の平方についても明示的な予想式があるが，ここでは一つだけを取り上げる．

**Conjecture 16.** 素数 $p \geq 5$ に対して

$$ss_p^{(6B)}(X)^2 = (X^2 - 34X + 1)^{\nu_6} \sum_{n=0}^{p-1} \left\{ \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \right\} X^{p-1-n} \pmod p.$$

なお，右辺の係数は Apéry による $\zeta(3)$ の無理性の証明に現れている．

## 3.2　ある三角群に由来する超幾何多項式の既約分解

前節で考えたのは群のレベルを上げる，あるいは代数関係式の次数を上げる方向への超特異多項式の一般化である．これらの場合，経験的には超特異多項式を超幾何多項式 ${}_2F_1$ で表すことは難しいと考えられる．そこで少し視点を変えてみる．良く知られているように

$$PSL_2(\mathbb{Z}) \simeq \langle S, T \mid S^2 = (ST)^3 = I \rangle$$

であって，これは符号 $(2,3,\infty)$ に対する三角群と同型である．この三角群 $\Delta(2,3,\infty)$ と超特異多項式 $ss_p(X)$ が対応していると思うことにする．さて，Elkies [7, §3.3] により三角群 $\Delta(2,4,6)$ に対応する，志村曲線 $\chi^*(1) \pmod p$ の超特異点を根に持つような超幾何多項式の具体形が既に知られている：

$$\begin{cases} {}_2F_1\left(\frac{1}{24}, \frac{5}{24}; \frac{1}{2}; t\right) & \text{if } p \equiv 1, 5 \mod 24, \\ {}_2F_1\left(\frac{7}{24}, \frac{11}{24}; \frac{1}{2}; t\right) & \text{if } p \equiv 7, 11 \mod 24, \\ {}_2F_1\left(\frac{13}{24}, \frac{17}{24}; \frac{3}{2}; t\right) & \text{if } p \equiv 13, 17 \mod 24, \\ {}_2F_1\left(\frac{19}{24}, \frac{23}{24}; \frac{3}{2}; t\right) & \text{if } p \equiv 19, 23 \mod 24. \end{cases}$$

素数 $p \geq 5$ は

$$p - 1 = 24m + 4\nu_3 + 6\nu_1 + 12\nu_6, \quad m \in \mathbb{Z}_{\geq 0},\ \nu_n = \frac{1}{2}\left(1 - \left(\frac{-n}{p}\right)\right)$$

と一意的に書けることに注意し，上記の超幾何表示をまとめて

$$S_p(t) := {}_2F_1\left(-m, -m + \frac{1}{6} - \frac{\nu_3}{3}; \frac{1}{2} + \nu_6; t\right) \pmod p$$

と表す．その線形因子の個数を $N(p)$ と表すとき，計算機実験からは以下が予想される．

**Conjecture 17.** 素数 $p \geq 5$ に対して

$$\begin{aligned} N(p) = {} & \frac{1}{16}\left(1 + \left(\frac{-3}{p}\right)\right)\left\{2 + \left(\frac{-2}{p}\right)\left(1 - \left(\frac{-1}{p}\right)\right)\right\} h(\sqrt{-p}) \\ & + \frac{1}{8}\left(1 - \left(\frac{-3}{p}\right)\right) h(\sqrt{-2p}) + \frac{1}{16}\left\{2 + \left(\frac{-2}{p}\right)\left(1 + \left(\frac{-1}{p}\right)\right)\right\} h(\sqrt{-3p}) \\ & + \frac{1}{8} h(\sqrt{-6p}) - (\nu_1 + \nu_3 + \nu_6). \end{aligned}$$

これより $S_p(t)$ の定義に，ある $\nu_1, \nu_3, \nu_6$ 次の一次式の積を含めた方が自然なのかもしれない．上の予想を認めると，類数評価から以下が成り立つことが分かる：

$$\deg S_p(t) = m = N(p) \iff p \in \{5 \leq p \leq 97, 107, 109, 113, 137\}.$$

多項式 $S_p(t) \pmod p$ が線形因子のみに既約分解されるような素数 $p$ は，モンスター群のような対象と何か思いがけない関係をもつだろうか？

# 参考文献


[1] J. Brillhart and P. Morton. Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial. *Journal of Number Theory*, **106**(1):79–111, 2004.

[2] J. H. Conway and S. P. Norton. Monstrous moonshine. *Bull. London Math. Soc*, **11**(3):308–339, 1979.

[3] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, **14**:197–272, 1941.

[4] M. Deuring. Die Anzahl der Typen von Maximalordungen einer definiten Quaternionenalgebra mit primer Grundzahl. *Jahresber. Deutsch. Math. Verein*, **54**:21–41, 1944.

[5] J. F. R. Duncan and K. Ono. The Jack Daniels Problem. *Journal of Number Theory*, **161**:230–239, 2016.

[6] M. Eichler. Über die Idealklassenzahl total definiter Quaternionenalgebren. *Math. Z*, **43**:102–109, 1938.

[7] N. D. Elkies. Shimura curve computations. In *Algorithmic number theory (Portland, OR, 1998)*, volume **1423** of *Lecture Notes in Comput. Sci.*, pages 1–47. Springer, Berlin, 1998.

[8] A. Erdélyi, W. Magnus, F. Oberhettinger, and F. G. Tricomi. *Higher transcendental functions. Vols. I.* McGraw-Hill Book Company, Inc., New York-Toronto-London, 1953. Based, in part, on notes left by Harry Bateman.

[9] J. Igusa. Class number of a definite quaternion with prime discriminant. *Proceedings of the National Academy of Sciences*, **44**(4):312–314, 1958.

[10] M. Kaneko and D. Zagier. Supersingular $j$-invariants, hypergeometric series, and Atkin's orthogonal polynomials. *AMS/IP Studies in Advanced Mathematics*, **7**:97–126, 1998.

[11] M. Koike. On supersingular $j_2^*$-polynomials for $\Gamma_0^*(2)$. unpuplished, 2009.

[12] P. Morton. Legendre polynomials and complex multiplication, I. *Journal of Number Theory*, **130**(8):1718–1731, 2010.

[13] P. Morton. The cubic Fermat equation and complex multiplication on the Deuring normal form. *The Ramanujan Journal*, **25**(2):247–275, 2011.

[14] T. Nakaya. The number of linear factors of supersingular polynomials and sporadic simple groups. *Journal of Number Theory*, 2019. in press.

[15] A. P. Ogg. Automorphismes de courbes modulaires. *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, **16**(1):1–8, 1975.

[16] A. Pizer. A note on a conjecture of Hecke. *Pacific Journal of Mathematics*, **79**(2):541–548, 1978.

[17] Y. Sakai. The Atkin orthogonal polynomials for the low-level Fricke groups and their application. *International Journal of Number Theory*, **7**(06):1637–1661, 2011.

[18] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer New York, 2nd edition, 2009.

[19] H. Tsutsumi. The Atkin orthogonal polynomials for congruence subgroups of low levels. *The Ramanujan Journal*, **14**(2):223–247, 2007.