ある保型関数体の生成元と方程式

関 美智子

2001 年 2 月

1. 序文

本修士論文は, 保型関数体と呼ばれる $\mathrm{SL}_2(\mathbb{Z})$ の合同部分群に対する保型関数からなる体の生成元と, その生成元が満す方程式についての総合報告である. 本論文では, 石井伸郎 · 石田信彦 による論文 [II96], [II99], [II98] をもとに, 合同部分群 $\Gamma_1(N)$, $\Gamma(N)$ の保型関数体 $A_1(N)$, $A(N)$ の生成元とその生成元が満たす $\mathbb{Q}$ 上の方程式について考察する.

$A_1(N)$ については石井伸郎による論文 [Ish83] で定義される関数 $X_r(\tau)$ を用いて $\mathbb{C}$ 上２つの元で生成されることが, [II99] で示される. 一方, $A(N)$ については, 生成元が楕円曲線の j-invariant と Weber 関数と呼ばれる関数を用いて与えられることが古典的に知られているが, この場合その生成元の個数は多い. しかし, [II96] では N が素数のときに, [II98] では一般の N の場合に $A(N)$ が関数 $X_r(\tau)$ を用いて $\mathbb{C}$ 上2つの関数で生成されることを示している.

さらにこれらの論文では $A_1(N)$, $A(N)$ の生成元が満す方程式を１つ求めることにより, $\Gamma_1(N)$, $\Gamma(N)$ に対応する modular curve と呼ばれる曲線の affine model を与えている. しかしこの方程式は非特異ではないので非特異モデルを与えているわけではない. また N が素数の場合にはこの方程式を具体的に求めるアルゴリズムが存在するが, 一般の N についてはアルゴリズムが存在するとは言えない. だが一般の N についても, 方程式は原理的には求めることができる.

N を正整数として, $\mathrm{SL}_2(\mathbb{Z})$ の部分群 $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ を次のように定義する.

$$(1)\qquad \Gamma_0(N) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \equiv \left(\begin{array}{cc} * & * \\ 0 & * \end{array} \right) \mod N \right\}.$$

$$(2)\qquad \Gamma_1(N) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \equiv \left(\begin{array}{cc} 1 & * \\ 0 & 1 \end{array} \right) \mod N \right\}.$$

$$(3)\qquad \Gamma(N) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \equiv \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \mod N \right\}.$$

これらを $\mathrm{SL}_2(\mathbb{Z})$ の合同部分群と言う.

$\mathrm{SL}_2(\mathbb{Z})$ の上半平面 $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}\tau > 0\}$ の点 τ への作用を

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d} \qquad \left(\tau \in \mathbb{H},\ \gamma = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{SL}_2(\mathbb{Z}) \right)$$

で定める. $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ とおき, とくに $\mathbb{Q} \cup \{\infty\}$ の元を cusp という. $\mathrm{SL}_2(\mathbb{Z})$ の $\mathbb{H}$ への作用は $\mathbb{H}^*$ へ延長できる. 一般に, Γ を $\mathrm{SL}_2(\mathbb{Z})$ もしくは合同部分群とすると, $\mathbb{H}^*/\Gamma$ はある代数曲線 X_Γ に位相同型であり, このとき X_Γ を Γ に対応する modular curve と言う. $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ の場合には, $\mathbb{H}^*/\Gamma$ は射影曲線 $\mathbb{P}^1(\mathbb{C})$ に同型である.

ここで, Λ_τ を lattice: $\mathbb{Z}\tau + \mathbb{Z}$ とすれば, $\mathbb{C}$ 上の任意の楕円曲線 $E/\mathbb{C}$ はある $\tau \in \mathbb{H}$ に対して複素トーラス $\mathbb{C}/\Lambda_\tau$ と解析的に同型である. また, 2 つの楕円曲線 $\mathbb{C}/\Lambda_\tau$, $\mathbb{C}/\Lambda'_\tau$ が解析的に同型ということと, $\mathrm{SL}_2(\mathbb{Z})$ のある元 γ で, $\tau' = \gamma(\tau)$ となるものが存在することは同値である.

このことから, $\mathbb{H}/\Gamma$ の点は楕円曲線の同値類の全体と同型であることがわかる. 同様に, Γ が $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ の場合には次が成り立つ.

(1) $\Gamma = \Gamma_0(N)$ の場合
$\mathbb{H}/\Gamma$ の点は楕円曲線 E と E 上の点で位数 N の巡回部分群 C の組 (E, C) の同値類と対応する.

(2) $\Gamma = \Gamma_1(N)$ の場合
$\mathbb{H}/\Gamma$ の点は楕円曲線 E と E 上の order N の点 T の組 (E, T) に対応する.

(3) $\Gamma = \Gamma(N)$ の場合
$\mathbb{H}/\Gamma$ の点は楕円曲線 E と E 上の N 等分点の基底 $\{T_1, T_2\}$ で, $e_N(T_1, T_2) = \exp(2\pi i/N)$ を満すものの組 (E, T_1, T_2) に対応する. ここで, $e_N(T_1, T_2)$ は Weil pairing である.

上半平面上の有理型関数で, Γ の作用に関して不変であって 無限遠点でも有理型である関数を Γ の保型関数と言う. Γ の保型関数全体のなす体を 保型関数体 (modular function field) と言い, $\Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$ に関する保型関数体をそれぞれ $A_0(N)$, $A_1(N)$, $A(N)$ と表す.

$\Lambda = \mathbb{Z}\tau + \mathbb{Z}$ $(\tau \in \mathbb{H})$ を lattice として, 楕円曲線

$$E_\Lambda : \quad y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

を取る. ただし $g_2(\tau) = 60\sum_{0\neq\omega\in\Lambda}\omega^{-4}$, $g_3(\tau) = 140\sum_{0\neq\omega\in\Lambda}\omega^{-6}$ で, E_L の形の楕円曲線は Weierstrass の標準型と呼ばれる. また,

$$\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2,$$
$$j(\tau) = \frac{g_2(\tau)^3}{\Delta(\tau)},$$

として, $\mathbb{H}$ 上の関数 $f_a = f_a^1, f_a^2, f_a^3$ を

$$f_a(\tau) = f_a^1(\tau) = \frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)}\wp\left(a\begin{pmatrix}\tau\\1\end{pmatrix}; \tau, 1\right),$$
$$f_a^2(\tau) = \frac{g_2(\tau)^2}{\Delta(\tau)}\wp\left(a\begin{pmatrix}\tau\\1\end{pmatrix}; \tau, 1\right)^2,$$
$$f_a^3(\tau) = \frac{g_3(\tau)}{\Delta(\tau)}\wp\left(a\begin{pmatrix}\tau\\1\end{pmatrix}; \tau, 1\right)^3$$

とおく. 但し $a \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ で $\wp\left(a\binom{\tau}{1}; \tau, 1\right)$ は後に定義 2.3 で与えられる Weierstrass の $\wp$-関数である. (これらの関数において, 各右辺に $a\binom{\tau}{1}$ の代わりに $z \in \mathbb{C}$ を代入したものは Weber 関数と呼ばれる関数である.) このとき, $A_0(N)$, $A(N)$ の生成元について [Shi71] Propositions 2.10, 6.1 により次の定理が知られている.

定理 1.1.

(1) $$A_0(N) = \mathbb{C}\left(j(\tau), j(N\tau)\right).$$

(2) $$A(N) = \mathbb{C}\left(j(\tau), f_a(\tau) \mid a \in N^{-1}\mathbb{Q}^2 \setminus \mathbb{Z}^2\right).$$

本論文ではセクション 3 において, セクション 2 で定義する関数 $X_r(\tau)$ を用いて, $A(N), A_1(N)$ について次の定理が成り立つことを示す.

定理 3.13 関数 $X_2^{\epsilon_N N}, X_3^N$ は $\mathbb{C}$ 上 $A_1(N)$ を生成する.

定理 3.16 関数 $X_2^{\epsilon_N}, X_3$ は $\mathbb{C}$ 上 $A(N)$ を生成する.

さらにセクション 4 で, 生成元が満たす方程式が $\mathbb{Q}$ 上の方程式として得られる事を示し, N が素数の場合の方程式の求め方のアルゴリズムを述べる.

謝辞

本修士論文を書くに至るまで多忙ななか親切に御指導下さった雪江明彦先生, セミナー等でお世話いただいた高橋豊文先生、森田康夫先生に深く感謝の意を表します.

また, 私の疑問に耳を傾け, 時には一緒になって考えてくれた結城瑞穂氏、高角洋志氏をはじめ院生の方々に感謝いたします.

2. 関数 $X_r(\tau)$ の定義

N は 6 以上の整数とする. 関数 $X_r(\tau)$ の定義をするために, まず Weierstrass の σ-関数および ζ-関数の quasi-period map η について述べ, レベル N の Klein form を定義する. 以下 $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ を $\mathbb{Z}$-lattice とする.

定義 2.1. Weierstrass の σ-関数 $\sigma(z)$ を

$$\sigma(z) = \sigma(z;\Lambda) = z \prod_{0\neq\omega\in\Lambda} \left(1-\frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2\right)$$

で定義する.

このとき,

$$\begin{aligned}
&\log\left(\left(1-\frac{z}{\omega}\right)\exp\left(\frac{z}{\omega}+\frac{1}{2}\left(\frac{z}{\omega}\right)^2\right)\right)\\
&\quad = \log\left(1-\frac{z}{\omega}\right) + \frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2\\
&\quad = -\frac{1}{3}\left(\frac{z}{\omega}\right)^3 - \frac{1}{4}\left(\frac{z}{\omega}\right)^4 - \dots
\end{aligned}$$

より, $R>0$ を任意にとり $|z|<R$, $|\omega|>2R$ とすれば, $|\omega|-|z|>|\omega|/2$ となり, $|\omega|$ が十分大きいと $\log\left(1-\frac{z}{\omega}\right)$ が 1 価関数となるから

$$\begin{aligned}
&\left|\log\left(\left(1-\frac{z}{\omega}\right)\exp\left(\frac{z}{\omega}+\frac{1}{2}\left(\frac{z}{\omega}\right)^2\right)\right)\right|\\
&\quad \le \frac{1}{3}\left|\frac{z}{\omega}\right|^3 + \frac{1}{4}\left|\frac{z}{\omega}\right|^4 + \dots\\
&\quad \le \sum_{n=3}^{\infty}\left|\frac{z}{\omega}\right|^n = \frac{|z|^3}{(|\omega|-|z|)|\omega|^2} < \frac{2R^3}{|\omega|^3}
\end{aligned}$$

となる. ゆえに $|z| < R$ のとき

$$\sum_{|\omega|>2R,\ \omega\in\Lambda} \log\left(\left(1-\frac{z}{\omega}\right)\exp\left(\frac{z}{\omega}+\frac{1}{2}\left(\frac{z}{\omega}\right)^2\right)\right)$$

は絶対一様収束する. 従って σ-関数は $\mathbb{C}$ 上で正則である. また lattice Λ 上では 0 となり, $\mathbb{C}\setminus\Lambda$ では 零点を持たない.

定義 2.2. Weierstrass の ζ-関数 $\zeta(z)$ を

$$\zeta(z) = \frac{1}{z} + \sum_{0\neq\omega\in\Lambda}\left(\frac{1}{z-\omega}+\frac{1}{\omega}+\frac{z}{\omega^2}\right)$$

で定義する.

$\zeta(z) = (\log\sigma(z))'$ なので $\zeta(z)$ は $\mathbb{C}\setminus\Lambda$ 上で収束する.

定義 2.3. Weierstrass の $\wp$-関数 $\wp(a;\Lambda)$ を

$$\wp(a;\Lambda) = \frac{1}{z^2} + \sum_{0\neq\omega\in\Lambda}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)$$

で定義する.

ζ-関数と $\wp$-関数の間には次の関係が成り立つ.

$$\frac{d}{dz}\log\zeta(z) = -\wp(z).$$

このことから, $\wp$-関数は $\mathbb{C}\setminus\Lambda$ 上収束する.

定義より $\wp$-関数は lattice Λ を周期に持つので, $\omega\in\Lambda$ とすると $\zeta(z+\omega)-\zeta(z)$ は z に依らない ω の関数となる. そこで

$$\eta(\omega) = \zeta(z+\omega)-\zeta(z)$$

とおき, これを ζ-関数の quasi-period map という. 勿論これは Dedekind の η-関数とは異なる. また [Sil86] Proposition 5.2 より quasi-period map は Λ の線形写像である.

quasi-period map を用いて, $\mathrm{Im}(\omega_1/\omega_2) > 0$ のとき次の σ-関数の変換公式, および Legendre の関係式が成り立つ.

$$\begin{aligned}&\sigma(z+a\omega_1+b\omega_2;\omega_1,\omega_2)\\ &= (-1)^{ab+a+b}\sigma(z;\omega_1,\omega_2)\exp\left((a\eta(\omega_1)+b\eta(\omega_2))\left(z+\frac{1}{2}(a\omega_1+b\omega_2)\right)\right).\end{aligned} \tag{2.4}$$

$$\omega_1\eta(\omega_2)-\omega_2\eta(\omega_1) = 2\pi i. \tag{2.5}$$

定義 2.6. η を lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ についての Weierstrass の ζ-関数の quasi-period map とする. また, $\eta(\omega_1), \eta(\omega_2)$ をそれぞれ η_1, η_2 とおく. N を 1 以上の整数として, r, s を N を法として 0 と合同でない整数とする. このときレベル N の Klein form を次のように定義する.

$$\begin{aligned} K_{r,s}(\omega_1, \omega_2) &= K\left(\frac{r}{N}, \frac{s}{N}; \begin{pmatrix}\omega_1 \\ \omega_2\end{pmatrix}\right) \\ &= \exp\left(-\frac{1}{2}\frac{r\eta_1 + s\eta_2}{N}\frac{r\omega_1 + s\omega_2}{N}\right)\sigma\left(\frac{r\omega_1 + s\omega_2}{N}; \omega_1, \omega_2\right). \end{aligned}$$

[KL75] では定義式の exp の中の 1/2 が抜けていることに注意する.

$\mathbb{H}$ 上の有理型関数 $f(\tau)$ が $\left(\begin{smallmatrix}1 & 1 \\ 0 & 1\end{smallmatrix}\right)$ で不変なら, f は q のべき級数

$$f(\tau) = \sum_{n=\nu}^{\infty} a_n q^n$$

の形に展開できる. これを q-展開と言う. また $\mathbb{H}$ 上の有理型関数 $f(\tau)$ が $\left(\begin{smallmatrix}1 & N \\ 0 & 1\end{smallmatrix}\right)$ で不変なら, $x = \exp(2\pi i\tau/N)$ として f は x のべき級数

$$f(\tau) = \sum_{n=\nu}^{\infty} a_n x^n$$

の形に展開できる. これを x-展開と言う.

s を 合同部分群 Γ の cusp とすると $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ で $\sigma(i\infty) = s$ となるものが存在する. Γ_s を

$$\Gamma_s = \{\gamma \in \Gamma \,|\, \gamma(s) = s\}$$

とおく. このとき, ある正整数 h で

$$\sigma^{-1}\Gamma_s\sigma \cdot \{\pm 1\} = \left\{\pm\begin{pmatrix}1 & mh \\ 0 & 1\end{pmatrix} \,\middle|\, m \in \mathbb{Z}\right\} \tag{2.7}$$

となるものが存在する. この h に対して $z(\tau) = \exp(2\pi i\tau h)$ とおくと $z(\sigma^{-1}(\tau))$ は Γ の $i\infty$ での解析的局所パラメータになる. つまり $X = \Gamma\backslash\mathbb{H}^*$ を 1 次元複素多様体とみなしたとき cusp s に対応する X の点 P で $z(\sigma^{-1}(\tau))$ は P における解析的局所環の極大イデアルを生成する元になる.

よって $f(\tau)$ が Γ に関する保型関数のとき

$$f(\sigma(\tau)) = \sum_{n=\nu}^{\infty} a_n \exp\left(\frac{2\pi i\tau}{h}\right)^n$$

と展開され ν は f を X 上の有理型関数とみなしたときの f の P における位数である. なお, f の P における解析的位数と代数的位数は一致する.

もし $\Gamma = \Gamma(N)$ なら $\Gamma(N)$ は $\mathrm{SL}_2(\mathbb{Z})$ の正規部分群なので

$$\gamma \in \sigma^{-1}\Gamma_s\sigma \Longleftrightarrow \gamma \in \Gamma_{i\infty}$$

であることはすぐわかる．したがって

$$\sigma^{-1}\Gamma_s\sigma\cdot\{\pm1\}=\left\{\pm\begin{pmatrix}1&mN\\0&1\end{pmatrix}\middle|\, m\in\mathbb{Z}\right\}$$

ということが全ての cusp で成り立つ．だから全ての cusp で (2.7) の h が N にとれる．

一般の合同部分群 Γ に関して f を Γ に関する保型関数であるものとする．このとき f を $X=\Gamma\backslash\mathbb{H}^*$ 上の有理型関数とみなすと morphism

$$\phi : X\to\mathbb{P}^1$$

が定まる．すると

$$\phi^{-1}(\infty)=\sum_{\mathrm{ord}_P(f)<0}(-\mathrm{ord}_P(f))P$$

であるが, [Har77] Proposition 6.9 により

$$\begin{aligned}\deg(\phi^{-1}(\infty))&=\deg(\phi^{-1}(0))\\&=\sum_{\mathrm{ord}_P(f)<0}(-\mathrm{ord}_P(f))=[\mathbb{C}(X):\mathbb{C}(\mathbb{P}^1)]=[\mathbb{C}(X):\mathbb{C}(f)]\end{aligned}$$

であるので次がわかる．

命題 2.8. *f の極および零点における各位数の総和は等しく $[\mathbb{C}(X):\mathbb{C}(f)]$ である．*

命題 2.9. Klein form については次の (K1)〜(K3) が成り立つ.
(K1)　$\alpha=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(Z)$ ならば

$$K_{r,s}\left(\alpha\begin{pmatrix}\omega_1\\\omega_2\end{pmatrix}\right)=K_{(r,s)\alpha}\left(\begin{pmatrix}\omega_1\\\omega_2\end{pmatrix}\right)$$

(K2)　$$K_{r+aN,s+bN}(\omega_1,\omega_2)=(-1)^{ab+a+b}\exp\left(-2\pi i(as-br)/(2N)\right)K_{r,s}(\omega_1,\omega_2).$$

$\tau=\omega_1/\omega_2$, $q=\exp(2\pi i\tau)$, $\zeta=\exp(2\pi i/N)$ とする．$K_{r,s}(\tau)=K_{r,s}(\tau,1)$ とおくと

(K3)　$$\begin{aligned}&K_{r,s}(\tau)(2\pi i)\prod_{n=1}^{\infty}(1-q^n)^2\\&=-\exp\left(\frac{2\pi is(r-N)}{2N^2}\right)q^{\frac{r(r-N)}{2N^2}}\left(1-\zeta^sq^{r/N}\right)\prod_{n=1}^{\infty}\left(1-\zeta^sq^{n+r/N}\right)\left(1-\zeta^sq^{n-r/N}\right)\end{aligned}$$

証明. (K1)

$$
\begin{aligned}
&K_{r,s}\left(\alpha\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right)\\
&=K_{r,s}\begin{pmatrix}a\omega_1+b\omega_2\\ c\omega_1+d\omega_2\end{pmatrix}\\
&=\exp\left(-\frac{1}{2}\frac{r\eta(a\omega_1+b\omega_2)+s\eta(c\omega_1+d\omega_2)}{N}\frac{r(a\omega_1+b\omega_2)+s(c\omega_1+d\omega_2)}{N}\right)\\
&\quad\times\sigma\left(\frac{r(a\omega_1+b\omega_2)+s(c\omega_1+d\omega_2)}{N};a\omega_1+b\omega_2,c\omega_1+d\omega_2\right).
\end{aligned}
$$

$\alpha\in\mathrm{SL}_2(\mathbb{Z})$ より lattice $\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$ と $\mathbb{Z}\omega_1'+\mathbb{Z}\omega_2'$ ($\omega_1'=a\omega_1+b\omega_2,\ \omega_2'=c\omega_1+d\omega_2$) は同じ lattice を与え, quasi-period map の線型性により

$$
\begin{aligned}
&K_{r,s}\left(\alpha\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right)\\
&\quad=\exp\left(-\frac{1}{2}\frac{(ar+cs)\eta(\omega_1)+(br+ds)\eta(\omega_2)}{N}\frac{(ar+cs)\omega_1+(br+ds)\omega_2}{N}\right)\\
&\qquad\times\sigma\left(\frac{(ar+cs)\omega_1+(br+ds)\omega_2}{N};\omega_1,\omega_2\right)\\
&\quad=K_{(r,s)\alpha}(\omega_1,\omega_2).
\end{aligned}
$$

(K2)

$$
\begin{aligned}
&K_{r+aN,s+bN}(\omega_1,\omega_2)\\
&=\exp\left(-\frac{1}{2}\frac{(r+aN)\eta_1+(s+bN)\eta_2}{N}\frac{(r+aN)\omega_1+(s+bN)\omega_2}{N}\right)\\
&\quad\times\sigma\left(\frac{r\omega_1+s\omega_2}{N}+a\omega_1+b\omega_2;\omega_1,\omega_2\right)\\
&=\exp\left(\frac{1}{2}\frac{(r+aN)\eta_1+(s+bN)\eta_2}{N}\frac{(r+aN)\omega_1+(s+bN)\omega_2}{N}\right)(-1)^{ab+a+b}\\
&\quad\times\exp\left((a\eta_1+b\eta_2)\left(\frac{r\omega_1+s\omega_2}{N}+\frac{1}{2}(a\omega_1+b\omega_2)\right)\right)\sigma\left(\frac{r\omega_1+s\omega_2}{N};\omega_1,\omega_2\right)\\
&=(-1)^{ab+a+b}\exp\left(\frac{(a\eta_1+b\eta_2)(r\omega_1+s\omega_2)-(r\eta_1+s\eta_2)(a\omega_1+b\omega_2)}{2N}\right)K_{r,s}(\omega_1,\omega_2)\\
&=(-1)^{ab+a+b}\exp\left(\frac{(as-br)(\eta_1\omega_2-\eta_2\omega_1)}{2N}\right)K_{r,s}(\omega_1,\omega_2)\\
&=(-1)^{ab+a+b}\exp\left(\frac{-2\pi i(as-br)}{2N}\right)K_{r,s}(\omega_1,\omega_2).
\end{aligned}
$$

ここで, 最初のステップでは σ-関数の変換公式 (2.4) を使い, 最後のステップで Legendre の関係式 (2.5) を使った.

(K3) [Sil94] Theorem 6.4 より $u = \exp(2\pi iz)$ とおくと, σ-関数は q に関して

$$\sigma(z;\tau,1) = -\frac{1}{2\pi i}\exp\left(\frac{1}{2}\eta(1)z^2 - \pi iz\right)(1-u)\prod_{n=1}^{\infty}\frac{(1-q^nu)(1-q^nu^{-1})}{(1-q^n)^2}$$

と展開できる. このことから明らかである. □

定義 2.10. τ を上半平面の点, r を N を法として 0 と合同でない整数として, 関数 $X_r(\tau)$ を次のように定義する.

$$X_r(\tau) = \exp\left(-\frac{\pi i(r-1)(N-1)}{2N}\right)\prod_{s=0}^{N-1}\frac{K_{r,s}(\tau)}{K_{1,s}(\tau)}.$$

$X_r(\tau)$ に対しては次が成り立つ.

命題 2.11. (1) 任意の整数 k に対して,

$$X_{r+kN}(\tau) = (-1)^k X_r(\tau).$$

(2) $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ $(c \equiv 0 \mod N)$ に対して,

$$X_r(\gamma(\tau)) = (-1)^{b(r-1)}\exp\left(2\pi i\frac{(r^2-1)ab}{2N}\right)\frac{X_{ra}(\tau)}{X_a(\tau)}.$$

(3) $q = \exp(2\pi i\tau)$ とすると, $X_r(\tau)$ は $\Gamma(2N^2)$ の cusp $i\infty$ の近傍で次のように無限積に展開される.

$$X_r(\tau) = q^{(r-1)(r+1-N)/(2N)}\frac{1-q^r}{1-q}\prod_{n=1}^{\infty}\frac{(1-q^{Nn-r})(1-q^{Nn+r})}{(1-q^{Nn-1})(1-q^{Nn+1})}.$$

(4) $X_r(\tau)$ は レベル $2N^2$ の保型関数である.

(5) r が N を法として 0 に合同でないとき, $X_r(\tau)$ は $\mathbb{C}$ では零点も極ももたない.

証明. (1)

$$\begin{aligned}
X_{r+kN}(\tau) &= \exp\left(-\frac{\pi i(r+kN-1)(N-1)}{2N}\right)\prod_{s=0}^{N-1}\frac{K_{r+kN,s}(\tau)}{K_{1,s}(\tau)} \\
&= \exp\left(-\frac{\pi i(r-1)(N-1)}{2N}\right)\exp\left(-\frac{\pi ikN(N-1)}{2N}\right) \\
&\quad\times\prod_{s=0}^{N-1}\frac{(-1)^k\exp(-2\pi iks/(2N))K_{r,s}(\tau)}{K_{1,s}(\tau)} \\
&= \exp\left(-\frac{\pi i(r-1)(N-1)}{2N}\right)\exp\left(-\frac{\pi ik(N-1)}{2}\right) \\
&\quad\times\exp\left(-\pi i\frac{k}{N}\frac{1}{2}(N-1)N\right)(-1)^{kN}\prod_{s=0}^{N-1}\frac{K_{r,s}(\tau)}{K_{1,s}(\tau)} \\
&= (-1)^{-k(N-1)+kN}X_r(\tau) \\
&= (-1)^k X_r(\tau).
\end{aligned}$$

(2) $\gamma = \left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right)$ とおく. Klein form の性質 (K2) より,

$$K_{(r,s)\gamma}(\tau) = (-1)^{cs} \exp\left(-\frac{2\pi ics(rb+ds)}{2N}\right) K_{ra,rb+sd}(\tau),$$
$$K_{(1,s)\gamma}(\tau) = (-1)^{cs} \exp\left(-\frac{2\pi ics(b+ds)}{2N}\right) K_{a,b+sd}(\tau)$$

であるから, $X_r(\tau)$ の定義より,

$$\begin{aligned}
X_r(\gamma(\tau)) &= \exp\left(-\frac{\pi i(r-1)(N-1)}{2N}\right) \prod_{s=0}^{N-1} \frac{K_{(r,s)\gamma}(\tau)}{K_{(1,s)\gamma}(\tau)} \\
&= \exp\left(-\frac{\pi i(r-1)(N-1)}{2N}\right) \prod_{s=0}^{N-1} \exp\left(-\frac{2\pi ibcs(r-1)}{2N}\right) \frac{K_{ra,rb+sd}(\tau)}{K_{a,b+sd}(\tau)} \\
&= \exp\left(-\frac{\pi i(r-1)(N-1)}{2N}\right) \exp\left(-\frac{\pi ibcN(r-1)(N-1)}{2N}\right) \prod_{s=0}^{N-1} \frac{K_{ra,rb+sd}(\tau)}{K_{a,b+sd}(\tau)} \\
&= \exp\left(-\frac{\pi i(r-1)(N-1)(1+bcN)}{2N}\right) \prod_{s=0}^{N-1} \frac{K_{ra,rb+sd}(\tau)}{K_{a,b+sd}(\tau)} \\
&= \exp\left(-\frac{\pi i(r-1)(N-1)ad}{2N}\right) \prod_{s=0}^{N-1} \frac{K_{ra,rb+sd}(\tau)}{K_{a,b+sd}(\tau)}.
\end{aligned}$$

$ad - bcN = 1$ より d と N は互いに素である. よって s が 0 から $N-1$ まで動くとき, $rb+sd, b+sd$ はそれぞれ N を法として 0 から $N-1$ まで動くので

$$\prod_{s=0}^{N-1} \frac{K_{ra,rb+sd}(\tau)}{K_{a,b+sd}(\tau)} = \frac{K_{ra,0+a_0N}(\tau) K_{ra,1+a_1N}(\tau) \cdots K_{ra,(N-1)+a_{N-1}N}(\tau)}{K_{a,0+b_0N}(\tau) K_{a,1+b_1N}(\tau) \cdots K_{a,(N-1)+b_{N-1}N}(\tau)}$$

となる. ただし各 a_j, b_j $(j = 0 \ldots N-1)$ は整数である. 再び Klein form の性質 (K2) により,

$$\begin{aligned}
K_{ra,j+a_jN}(\tau) &= (-1)^{a_j} \exp\left(-2\pi i \frac{-raa_j}{2N}\right) K_{ra,j}(\tau) \\
&= (-1)^{a_j} \exp\left(\frac{\pi iraa_j}{N}\right) K_{ra,j}(\tau)
\end{aligned}$$

となるので,

$$\begin{aligned}
\prod_{j=0}^{N-1} K_{ra,j+a_jN}(\tau) &= \prod_{j=0}^{N-1} (-1)^{a_j} \exp\left(\frac{\pi iraa_j}{N}\right) K_{ra,j}(\tau) \\
&= (-1)^{\sum_{j=0}^{N-1} a_j} \exp\left(\frac{\pi ira}{N} \sum_{j=0}^{N-1} a_j\right) \prod_{j=0}^{N-1} K_{ra,j}(\tau)
\end{aligned}$$

同様に,

$$\prod_{j=0}^{N-1} K_{a,j+b_jN}(\tau) = (-1)^{\sum_{j=0}^{N-1} b_j} \exp\left(\frac{\pi i a}{N} \sum_{j=0}^{N-1} b_j\right) \prod_{j=0}^{N-1} K_{a,j}(\tau)$$

となる. ここで a_j, b_j の決め方から, $\sum_{s=0}^{N-1}(rb+sd) = \sum_{j=0}^{N-1}(j+a_jN)$ であるから,

$$\sum_{j=0}^{N-1} a_j = rb + \frac{d-1}{2}(N-1)$$

となる. 同様に

$$\sum_{j=0}^{N-1} b_j = b + \frac{d-1}{2}(N-1).$$

ゆえに,

$$\begin{aligned}
&\prod_{j=0}^{N-1} \frac{K_{ra,j+a_jN}(\tau)}{K_{a,j+b_jN}(\tau)} \\
&= (-1)^{b(r-1)} \exp\left(\frac{\pi i a}{N}\left(r\sum_{j=0}^{N-1} a_j - \sum_{j=0}^{N-1} b_j\right)\right) \prod_{j=0}^{N-1} \frac{K_{ra,j}(\tau)}{K_{a,j}(\tau)} \\
&= (-1)^{b(r-1)} \exp\left(\frac{\pi i a}{N}\left((r^2-1)b + \frac{d-1}{2}(N-1)(r-1)\right)\right) \prod_{j=1}^{N-1} \frac{K_{ra,j}(\tau)}{K_{a,j}(\tau)}.
\end{aligned}$$

$$\frac{X_{ra}(\tau)}{X_a(\tau)} = \exp\left(-\frac{\pi i(N-1)(r-1)a}{2N}\right) \prod_{j=1}^{N-1} \frac{K_{ra,j}(\tau)}{K_{a,j}(\tau)}$$

より,

$$\prod_{j=1}^{N-1} \frac{K_{ra,j}(\tau)}{K_{a,j}(\tau)} = \exp\left(\frac{\pi i(N-1)(r-1)a}{2N}\right) \frac{X_{ra}(\tau)}{X_a(\tau)}$$

となる. したがって,

$$\begin{aligned}
&\prod_{j=0}^{N-1} \frac{K_{ra,j+a_jN}(\tau)}{K_{a,j+b_jN}(\tau)} \\
&= (-1)^{b(r-1)} \exp\left(\frac{\pi i(r^2-1)ab}{N}\right) \exp\left(\frac{\pi i a(d-1)(N-1)(r-1)}{2N}\right) \\
&\quad \times \exp\left(\frac{\pi i a(N-1)(r-1)}{2N}\right) \frac{X_{ra}(\tau)}{X_a(\tau)} \\
&= (-1)^{b(r-1)} \exp\left(\frac{\pi i(r^2-1)ab}{N}\right) \exp\left(\frac{\pi i(N-1)(r-1)ad}{2N}\right) \frac{X_{ra}(\tau)}{X_a(\tau)}.
\end{aligned}$$

ゆえに,

$$X_r(\gamma(\tau)) = (-1)^{b(r-1)} \exp\left(\frac{\pi i(r^2-1)ab}{N}\right) \frac{X_{ra}(\tau)}{X_a(\tau)}.$$

(3) Klein form の性質 (K3) より成り立つ.
(4) $X_1(\tau) = 1$ に注意すれば, 命題 2.11 (2) より $X_r(\tau)$ は レベル $2N^2$ の保型関数であることがわかる.
(5) $\sigma((r\omega_1 + s\omega_2)/N; \omega_1, \omega_2)$ は r, s が共に N を法として 0 に合同でない場合はゼロにならないので, $X_r(\tau)$ の定義より, $X_r(\tau)$ は $\mathbb{C}$ では零点も極も持たないことがわかる. □

$$\epsilon_N = \begin{cases} 1 & \text{N が奇数のとき} \\ 2 & \text{N が偶数のとき} \end{cases}$$

とおくと先の命題から次が成り立つ.

命題 2.12. r が奇数なら $X_r(\tau) \in A(N)$, r が偶数なら $X_r(\tau)^{\epsilon_N} \notin A(N)$ かつ $X_r(\tau) \in A(N)$ である.

証明. $\Gamma(N)$ の任意の元 γ は N を法として $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ に合同なので, $\gamma = \left(\begin{smallmatrix} 1+aN & bN \\ cN & 1+dN \end{smallmatrix}\right)$ $(a, b, c, d \in \mathbb{Z})$ とおくと, 命題 2.11 (2) により

$$X_r(\gamma(\tau)) = (-1)^{bN(r-1)} \exp\left(2\pi i \frac{(r^2-1)(1+aN)bN}{2N}\right) \frac{X_{r+arN}(\tau)}{X_{1+aN}(\tau)}$$

となるが, 命題 2.11(1) により,

$$X_{1+aN}(\tau) = (-1)^a X_1(\tau) = (-1)^a$$
$$X_{r+aN}(\tau) = (-1)^{ra} X_r(\tau)$$

であるから,

$$\begin{aligned} X_r(\gamma(\tau)) &= (-1)^{(a+bN)(r-1)} \exp\left(\pi i(1+aN)b(r^2-1)\right) X_r(\tau) \\ &= (-1)^{(a+bN)(r-1)+(1+aN)b(r^2-1)} X_r(\tau). \end{aligned}$$

r が奇数なら明らかに $X_r(\gamma(\tau)) = X_r(\tau)$ となる.
r を偶数とする. γ の行列式が 1 であることから

$$a + d + (ad - bc)N = 0 \tag{2.13}$$

である. もし N が奇数なら

$$\begin{aligned} (a+bN)(r-1) + (1+aN)b(r^2-1) &\equiv (a+bN) + (1+aN)b \\ &\equiv a + b + b + ab \\ &\equiv a(1+b) \mod 2. \end{aligned}$$

$a(1+b)$ が奇数と仮定すると, a が奇数かつ b が偶数であるが, このとき, (2.13) より

$$0 = a + d + adN - bcN \equiv 1 + d + d \equiv 1 \mod 2$$

となり矛盾が生じる．したがって $a(1+b)$ は偶数である．ゆえに, N が奇数なら $X_r(\tau) \in A(N)$ が成り立つ.

もし N が偶数なら

$$\begin{aligned}(a+bN)(r-1)+(1+aN)b(r^2-1) &\equiv (a+bN)+(1+aN)b \\ &\equiv a+b \mod 2.\end{aligned}$$

この場合, γ として $\left(\begin{smallmatrix}1+aN & N\\ -a^2N & 1-aN\end{smallmatrix}\right)$ をとると, $a+b=a+1$ は a が偶数のとき奇数となる．ゆえに, N が偶数の時, $X_r(\tau) \notin A(N)$ だが $X_r(\tau)^2 \in A(N)$ となる．以上により, r が偶数ならば, $X_r(\tau)^{\epsilon_N} \in A(N)$ が成り立つ. □

3. $A(N)$ と $A_1(N)$ の生成元

N が 5 以下の整数の場合には古典的に知られているので, N が 6 以上の整数の場合のみ考察する．r を N を法として 0 と合同でない整数とする．$A_1(N)$ の元については次の補題が成り立つ.

補題 3.1. m, n を整数とする．このとき

$$X_2^m X_3^n \in A_1(N) \Longleftrightarrow 3m+8n \equiv 0 \mod \epsilon_N N.$$

証明. $X_2^{\epsilon_N}, X_3 \in A(N)$ で $\Gamma_1(N)$ は $\Gamma(N)$ と $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ で生成されるので, $X_2^m X_3^n$ が $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ で不変であるための必要十分条件さえ調べれば良い．Klein form の性質 (K1) により r, s を N を法として 0 と合同でない整数とするとき, $K_{r,s}(\tau+1) = K_{r,s+r}(\tau)$ が成り立つことに注意すれば

$$\begin{aligned}X_2^m X_3^n(\tau+1) &= \left(\prod_{s=0}^{N-1} \frac{K_{2,s}(\tau+1)}{K_{1,s}(\tau+1)}\right)^m \left(\prod_{s=0}^{N-1} \frac{K_{3,s}(\tau+1)}{K_{1,s}(\tau+1)}\right)^n \\ &\quad \times \left(\prod_{s=0}^{N-1} \frac{K_{2,s}(\tau)}{K_{1,s}(\tau)}\right)^{-m} \left(\prod_{s=0}^{N-1} \frac{K_{3,s}(\tau)}{K_{1,s}(\tau)}\right)^{-n} X_2^m X_3^n(\tau) \\ &= \prod_{s=0}^{N-1} \left(\frac{K_{1,s}(\tau)K_{2,s+2}(\tau)}{K_{2,s}(\tau)K_{1,s+1}(\tau)}\right)^m \left(\frac{K_{1,s}(\tau)K_{3,s+3}(\tau)}{K_{3,s}(\tau)K_{1,s+1}(\tau)}\right)^n X_2^m X_3^n(\tau) \\ &= \left(\frac{K_{1,0(\tau)}}{K_{1,N}(\tau)} \frac{K_{2,N(\tau)}}{K_{2,0}(\tau)} \frac{K_{2,N+1(\tau)}}{K_{2,1}(\tau)}\right)^m \\ &\quad \times \left(\frac{K_{1,0(\tau)}}{K_{1,N}(\tau)} \frac{K_{3,N(\tau)}}{K_{3,0}(\tau)} \frac{K_{3,N+1(\tau)}}{K_{3,1}(\tau)} \frac{K_{3,N+2(\tau)}}{K_{3,2}(\tau)}\right)^n X_2^m X_3^n(\tau).\end{aligned}$$

となる．ここで (K2) より

$$\begin{aligned}\frac{K_{1,0}(\tau)}{K_{1,N}(\tau)} &= -\exp\left(\frac{-\pi i}{N}\right), \\ \frac{K_{2,N}(\tau)}{K_{2,0}(\tau)} &= \frac{K_{2,N+1}(\tau)}{K_{2,1}(\tau)} = -\exp\left(\frac{2\pi i}{N}\right), \\ \frac{K_{3,N}(\tau)}{K_{3,0}(\tau)} &= \frac{K_{3,N+1}(\tau)}{K_{3,1}(\tau)} = \frac{K_{3,N+2}(\tau)}{K_{3,2}(\tau)} = -\exp\left(\frac{3\pi i}{N}\right)\end{aligned}$$

であるから,

$$X_2^m X_3^n(\tau+1) = \exp\left(\frac{\pi i(3m+8n+mN)}{N}\right) X_2^m X_3^n(\tau) \tag{3.2}$$

このことから $3m+8n+mN \equiv 0 \mod 2N$ ならば $X_2^m X_3^n \in A_1(N)$ である.

逆に $3m+8n+mN \equiv 0 \mod 2N$ であるならば, $\mu = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ とおくと (3.2) より

$$X_2^m X_3^n(\mu(\tau)) = X_2^m X_3^n(\tau)$$

である. ゆえに, $3m+8n+mN \equiv 0 \mod 2N$ なら m は ϵ_N で割り切れるので, $X_2^m = (X_2^{\epsilon_N})^{m/\epsilon_N}$ となる. よって $X_2^m X_3^n \in A_1(N)$ である. したがって

$$X_2^m X_3^n \in A_1(N) \Longleftrightarrow 3m+8n+mN \equiv 0 \mod 2N$$

が成り立つ.

また, $3m+8n+mN \equiv 0 \mod 2N$ ならば, N が奇数のとき

$$3m+8n \equiv -mN \equiv 0 \mod \epsilon_N N.$$

N が偶数のときは $3m$ が偶数となるので m は偶数で,

$$3m+8n \equiv -mN \equiv 0 \mod \epsilon_N N.$$

逆に, $3m+8n \equiv 0 \mod \epsilon_N N$ ならば, 整数 k で

$$3m+8n+m\epsilon_N N = k\epsilon_N N \tag{3.3}$$

となるものが存在する. N が奇数の場合, k が奇数であると仮定すると, (3.3) の右辺は奇数で左辺は偶数となって矛盾が生じる. ゆえに k は偶数である. よって $k\epsilon_N N = 3m+8n+m\epsilon_N N \equiv 0 \mod 2N$ となる. N が偶数の場合は, $\epsilon_N = 2$ で $3m$ は偶数なので m は偶数で,

$$3m+8n+mN = 2Nk - mN = N(2k-m) \equiv 0 \mod \epsilon_N N.$$

したがって,

$$3m+8n+mN \equiv 0 \mod 2N \Longleftrightarrow 3m+8n \equiv 0 \mod \epsilon_N N$$

である. □

$A_1(N)$ の定数でない元 f に対して, $\mathbb{C}(f)$ と $A_1(N)$ の拡大次数を $\mathrm{d}(f)$ とおくと次の補題は明らかである.

補題 3.4. $A_1(N)$ の元 $f_0, f_1, \ldots f_n$ が定数でないならば, $A_1(N)$ が $\mathbb{C}$ 上 $f_0, f_1, \ldots f_n$ で生成されることと, $\mathrm{d}(f_0), \mathrm{d}(f_1) \ldots \mathrm{d}(f_n)$ の最大公約数が 1 になることは同値である.

このことを用いて, $\mathrm{d}(f_0), \mathrm{d}(f_1), \mathrm{d}(f_2)$ の最大公約数が 1 となるような $A_1(N)$ の関数 f_0, f_1, f_2 を見つける. 命題 2.8 より拡大次数 $\mathrm{d}(f)$ は f の極での位数の総和に一致しているので, まず関数 $X_2^m X_3^n \in A_1(N)$ の極での位数を調べる.

$\Gamma(N) \subset \Gamma_1(N)$ より $X(N)$ から $X_1(N)$ への canonical map が存在する. それを ψ として, ψ から導かれる $A_1(N)$ から $A(N)$ への写像を ψ^* とする. [Sil86] PROPOSITION 3.6 により, $A_1(N)$ の元 f の divisor (f) の ψ^* による像 $\psi^*((f))$ は $f \cdot \psi$ の divisor に

一致している. ここで, 点 P を $X_1(N)$ の点として, 点 P での ψ の分岐指数を e_P とおくと, $X(N)$ は $X_1(N)$ の次数 N のガロワ被覆なので divisor (P) の ψ^* による像は, $\{P_1 \dots P_{N/e_P}\}$ を P の上にある $X(N)$ の点の全体とすれば,

$$\psi^*((P)) = e_P \left(\sum_{j=1}^{N/e_P} P_j \right)$$

となる. 点 P での f の位数を $\mathrm{ord}_P(f)$, 点 P_j $(j = 1 \dots N/e_P)$ での $f \cdot \psi$ の位数を $\mathrm{ord}_{P_j}(f)$ とおくと, 点 P_j の選び方に依らず, $\mathrm{ord}_P(f) = \mathrm{ord}_{P_j}(f)/e_P$ となる. $X_2^m X_3^n \in A_1(N)$ ならば

$$\mathrm{ord}_P(X_2^m X_3^n) = \frac{1}{e_P} \left(\frac{m}{\epsilon_N} \mathrm{ord}_{P_j}(X_2^{\epsilon_N}) + n \, \mathrm{ord}_{P_j}(X_3) \right) \tag{3.5}$$

となる. 定義より, $X_2^m X_3^n$ は $\Gamma_1(N)$ の cusp でのみ零点もしくは極を持つので, cusp での $X_2^m X_3^n$ の位数のみ計算すれば良いが, (3.5) により $\Gamma(N)$ の cusp での $X_2^m X_3^n$ の位数から $\Gamma_1(N)$ の cusp での位数を求めることができる.

そこで, $\Gamma(N)$, $\Gamma_1(N)$ に対して集合 V, U を次のように定める.
N が奇数のときには

$$\begin{aligned} V = &\{(u,v) \mid 1 \le u \le (N-1)/2, \ 1 \le v \le N, \ \mathrm{GCD}(u,v,N) = 1\} \\ &\cup \{(0,v) \mid 1 \le v \le (N-1)/2, \ (v,N) = 1\}. \end{aligned}$$

N が偶数のときには

$$\begin{aligned} V = &\{(u,v) \mid 1 \le u \le N/2 - 1, \ 1 \le v \le N, \ \mathrm{GCD}(u,v,N) = 1\} \\ &\cup \{(N/2,v) \mid 1 \le N/2, \ \mathrm{GCD}(v, N/2) = 1\} \\ &\cup \{(0,v) \mid 1 \le v \le N/2, \ \mathrm{GCD}(v,N) = 1\} \end{aligned}$$

とする. また,

$$U = \left\{ (u,v) \;\middle|\; \begin{array}{c} u, v \in \mathbb{Z}, 1 \le v \le N, \mathrm{GCD}(v,N) =: d \text{ とすると} \\ 0 \le u \le d/2 \text{ かつ } \mathrm{GCD}(u,d) = 1 \end{array} \right\}$$

とする. このとき, U は V に含まれていることに注意する.

2 つの整数の組 (u,v), (u',v') で u と v, u' と v' は互いに素であるものとすると, (u,v) と (u',v') が $\Gamma(N)$ の同値な cusp を与えることと, $(u,v) \equiv \pm(u',v') \mod N$ となることは同値である. ゆえに $\Gamma(N)$ の cusp に対応する整数の組 (u,v) については u, v ともに N を法として考えて良い. また, (u,v) と (u',v') が $\Gamma_1(N)$ の同値な cusp を与えることとある整数 a に対して $(u,v) \equiv \pm(u'+av', v') \mod N$ となることは同値である. さらに, I を単位行列とすれば, $i\infty$ への $\pm I$ の作用は等しいので, 集合 V, U の元は $\Gamma(N), \Gamma_1(N)$ の cusp の代表系を与えていることがわかる.

各 $(u,v) \in V \cup U$ に対して行列 $B(u,v) \in \mathrm{SL}_2(\mathbb{Z})$ を

$$B(u,v) \equiv \begin{pmatrix} u & * \\ v & * \end{pmatrix} \mod N$$

となるものとすると次が成り立つ.

補題 3.6. 集合 $\{B(u,v)(i\infty) \mid (u,v) \in V\}, \{B(u,v)(i\infty) \mid (u,v) \in U\}$ は $\Gamma(N), \Gamma_1(N)$ の互いに同値でない cusp の完全代表系を与える.

$B(u,v)(i\infty)((u,v) \in U)$ で表される $\Gamma_1(N)$ の cusp を $P(u,v)$ と書くことにする. $B(u,v)(i\infty)((u,v) \in V)$ で表される $\Gamma(N)$ の cusp を $P'(u,v)$ とする. $x = \exp(2\pi i\tau/N)$ とおくと, cusp $P'(u,v)$ での $X_r(\tau)$ の位数 $\nu_{u,v}(X_r(\tau))$ は $X_r(B(u,v)(\tau))$ の cusp $i\infty$ での x-展開の位数として定義される. 便宜上, $m, w \in \mathbb{Z}$ に対して $\langle w\rangle_m$ を m を法として w と合同な最小の非負整数とし, 関数 $\alpha_m(w)$ を $\alpha_m(w) = \langle w\rangle_m(\langle w\rangle_m - m)$ で定める.

命題 3.7.

$$\nu_{u,v}(X_2(\tau)) = \frac{\epsilon_N}{2}(\alpha_d(2u) - \alpha_d(u))$$
$$\nu_{u,v}(X_3(\tau)) = \frac{1}{2}(\alpha_d(3u) - \alpha_d(u)).$$

証明. $B(u,v) \in \mathrm{SL}_2(\mathbb{Z}), B(u,v) \equiv \left(\begin{smallmatrix} u & u' \\ v & v' \end{smallmatrix}\right) \mod N$ とすれば, (K1) より

$$K_{r,s}(B(u,v)(\tau)) = K_{(r,s)B(u,v)}(\tau)$$

であるが, (K2) より $K_{r,s}(\tau)$ は r, s を N を法として考えても定数倍しか違わないので,

$$K_{(r,s)B(u,v)}(\tau) = c^* K_{\langle ru+sv\rangle_N, \langle rv+sv'\rangle_N}(\tau)$$

となる. ただし, c^* はゼロでない定数である. また $K_{r,s}(\tau)$ の x-展開は (K3) より

$$\begin{aligned} & K_{r,s}(\tau) 2\pi i \prod_{n=1}^{\infty}(1-x^{nN})^2 \\ &= -\exp\left(\frac{2\pi i s(N-1)}{2N^2}\right) \\ &\quad \times x^{\frac{r(r-N)}{2N}}(1-x^r\zeta^s)\prod_{n=1}^{\infty}\left(1-\zeta^s x^{nN+r}\right)\left(1-\zeta^s x^{nN-r}\right). \end{aligned} \tag{3.8}$$

よって, $K_{r,s}(\tau)$ の 零点と極の位数は r, s を N を法として考えても変わらないので, 適当な定数 c を取ると,

$$X_r(B(u,v)(\tau)) = c\prod_{s=0}^{N-1}\frac{K_{\langle ru+sv\rangle_N, \langle rv+sv'\rangle_N}(\tau)}{K_{\langle u+sv\rangle_N, \langle v+sv'\rangle_N}(\tau)}$$

となる. よって $0 < r < N$ なら, $nN \pm r, r > 0$ なので (3.8) より

$$\begin{aligned} \nu_{u,v}(X_r(\tau)) &= \frac{1}{2N}\sum_{s=0}^{N-1}(\langle ru+sv\rangle_N(\langle ru+sv\rangle_N - N) - \langle u+sv\rangle_N(\langle u+sv\rangle_N - N)) \\ &= \frac{1}{2N}\sum_{s=0}^{N-1}(\alpha_N(ru+sv) - \alpha_N(u+sv)). \end{aligned}$$

r が奇数の場合, $\mathrm{GCD}(v,N)=1$ ならば, s が 1 から $N-1$ まで動くとき, 任意の整数 w に対して $w+sv$ は N を法として 1 から $N-1$ まで動く. このことに注意すれば,

$$\sum_{s=0}^{N-1}\alpha_N(w+sv)=\sum_{s=0}^{N-1}\alpha_N(s)$$

が成り立つ. ゆえに,

$$\nu_{u,v}(X_r(\tau))=\sum_{s=0}^{N-1}(\alpha_N(s)-\alpha_N(s))=0.$$

したがって,

$$\nu_{u,v}(X_r(\tau))=0=(1/2)(\alpha_1(ru)-\alpha_1(u)).$$

$\mathrm{GCD}(v,N)=d\neq 1, v=kd$ とすると, $\mathrm{GCD}(k,N)=1$ となるので,

$$\begin{aligned}\nu_{u,v}(X_r(\tau))&=\frac{1}{2N}\sum_{s=0}^{N-1}(\alpha_N(ru+skd)-\alpha_N(u+skd))\\&=\frac{1}{2N}\sum_{s=0}^{N-1}(\alpha_N(ru+sd)-\alpha_N(u+sd))\\&=\frac{d}{2N}\sum_{s=0}^{N/d-1}(\alpha_N(ru+sd)-\alpha_N(u+sd)).\end{aligned}$$

ここで, 任意の整数 w に対して

$$\sum_{s=0}^{N/d-1}\alpha_N(w+sd)=\sum_{t=0}^{N/d-1}(\langle w\rangle_d+td)(\langle w\rangle_d+td-N) \tag{3.9}$$

が成り立つ. なぜならば, $w=ad+b$ $(a,b\in\mathbb{Z}\ a>0\ 0\leq b<d)$ とおくと 関数 α_N は $\mod N$ で考えても同じなので $0<w<N$ と仮定して良く, $N=kd$ とすれば, $0<ad+b<N$ なので, $0\leq a<(N-b)/d\leq N/d=k$ である. ゆえに,

$$\begin{aligned}&\sum_{s=0}^{N/d-1}\alpha_N(w+sd)\\&=\sum_{s=0}^{N/d-1}\langle(a+s)d+b\rangle_N(\langle(a+s)d+b\rangle_N-N)\\&=\sum_{s=a}^{N/d-1+a}\langle sd+b\rangle_N(\langle sd+b\rangle_N-N)\\&=\sum_{s=a}^{k-1}\langle sd+b\rangle_N(\langle sd+b\rangle_N-N)+\sum_{s=k}^{N/d-1+a}\langle sd+b\rangle_N(\langle sd+b\rangle_N-N)\\&=\sum_{s=a}^{k-1}(sd+b)(sd+b-N)+\sum_{s=k}^{N/d-1+a}\langle sd+b\rangle_N(\langle sd+b\rangle_N-N).\end{aligned}$$

$k \le s \le N/d - 1 + a$ なら,

$$\begin{aligned} kd + b \le sd + b &\le N - d + ad + b \\ &= N + (a-1)d + b \end{aligned}$$

となるので,

$$N + b \le sd + b < 2N$$

である. したがって

$$\sum_{s=k}^{N/d-1+a} \langle sd+b\rangle_N(\langle sd+b\rangle_N - N) = \sum_{t=0}^{a-1}(td+b)(td+b-N)$$

となる. よって

$$\begin{aligned} \sum_{s=0}^{N/d-1} \alpha_N(w+sd) &= \sum_{s=a}^{k-1}(sd+b)(sd+b-N) + \sum_{t=0}^{a-1}(td+b)(td+b-N) \\ &= \sum_{t=0}^{k-1}(td+b)(td+b-N). \end{aligned}$$

$\langle w\rangle_d = b$ より (3.9) が成り立つ. このことから

$$\begin{aligned} \nu_{u,v}(X_r(\tau)) = \frac{d}{2N} \sum_{s=0}^{N/d-1} &\left((\langle ru\rangle_d + sd)\left(\langle ru\rangle_d + sd - N\right)\right. \\ &\left. - \left(\langle u\rangle_d + sd\right)\left(\langle u\rangle_d + sd - N\right)\right). \end{aligned}$$

$w = \langle ru\rangle_d$ または $\langle u\rangle_d$ とすると,

$$\begin{aligned} (w+sd)(w+sd-N) &= w(w-d) + w(2sd+d-N) \\ &= \alpha_d(w) + w(2sd+d-N) \end{aligned}$$

より

$$\begin{aligned} \nu_{u,v}(X_r(\tau)) &= \frac{d}{2N} \sum_{s=0}^{N/d-1} (\langle ru\rangle_d(\langle ru\rangle_d - d) - \langle u\rangle_d(\langle u\rangle_d - d)) \\ &\quad + \frac{d}{2N} \sum_{s=0}^{N/d-1} (\langle ru\rangle_d - \langle u\rangle_d)(2sd+d-N) \\ &= \frac{d}{2N} \sum_{s=0}^{N/d-1} (\alpha_d(ru) - \alpha_d(u)) + \frac{d^2}{2N}\left(\langle ru\rangle_d - \langle u\rangle_d\right) \sum_{s=0}^{N/d-1} (2s+1-N/d) \\ &= \frac{1}{2}\left(\alpha_d(ru) - \alpha_d(u)\right). \end{aligned}$$

同様にして r が偶数のときは

$$\nu_{u,v}(X_r(\tau)) = (\epsilon_N/2)\left(\alpha_d(ru) - \alpha_d(u)\right)$$

であることが示される. □

(u,v) を V の元とすれば, u の範囲に注意すると

$$\langle u\rangle_d = u\ ,\ \langle 2u\rangle_d = 2u.$$

ここで, $\nu_{u,v}(X_2^{\epsilon_N}(\tau)) < 0$ となるのは, $u < d/3$ のときである. また, $0 < \alpha \in \mathbb{Z}, \alpha - 3u = dk$ とおくと, $\alpha = 3u + dk$ であるが, $1 \le u \le d/2$ なら, $3 \le 3u \le 3d/2$ となることから

$$\langle 3u\rangle_d = \begin{cases} 3u - d & u \ge d/3 \\ 3u & u < d/3 \end{cases}$$

となる. したがって, 次が成り立つ.

命題 3.10. $\Gamma(N)$ の cusp $P'(u,v)$ での $X_r(\tau)$ の位数を $\nu_{u,v}(X_r(\tau))$ とおくと,

$$\nu_{u,v}(X_2^{\epsilon_N}(\tau)) = \frac{\epsilon_N(3u-d)u}{2}$$
$$\nu_{u,v}(X_3(\tau)) = \begin{cases} \left(8u^2 - 8ud + 2d^2\right)/2 & u \ge d/3 \\ 4u^2 - ud & u < d/3 \end{cases}$$

系 3.11.

$$\mu_{u,v}(X_3) < 0 \Longrightarrow \mu_{u,v}(X_2^{\epsilon_N}) < 0$$

また [Sil86, p.350] によると, $P(u,v)$ での $\psi : X(N) \to X_1(N)$ の分岐指数は $\mathrm{GCD}(v,N)$ なので, 命題 3.7 により次が成り立つ.

命題 3.12. $X_2^m X_3^n \in A_1(N)$ とする. 関数 $X_2^m X_3^n$ は $\Gamma_1(N)$ の cusp でのみ極もしくは零点をもち, cusp $P(u,v)$ $((u,v) \in U)$ での位数 $\mu_{u,v}(X_2^m X_3^n)$ は次のようになる.

$$\mu_{u,v}(X_2^m X_3^n) = \begin{cases} \dfrac{(3m+8n)u^2 - (m+2n)du}{2d} & u < \frac{d}{3} \\ \dfrac{(3m+8n)u^2 - (m+8n)du + 2d^2 n}{2d} & u \ge \frac{d}{3} \end{cases}$$

ただし, d は v と N の最大公約数とする.

定理 3.13. 関数 $X_2^{\epsilon_N N}, X_3^N$ は $\mathbb{C}$ 上 $A_1(N)$ を生成する.

証明. $X_2^{Ni\epsilon_N} + X_3^{Nj}$ の形の生成元を考える. N が奇数のとき $\epsilon_N = 1$ で, 補題 3.12 より, $X_2^{Ni} + X_3^{Nj}$ は $\Gamma_1(N)$ の cusp でしかも X_2 が極を持つ cusp でのみ極を持つ. ゆえに $u < d/3$ のみ考えればよい. cusp $P(u,v)$ $\left(\binom{u}{v} \in U\right)$ での X_2^N, X_3^N の位数は,

$$\mu_{u,v}\left(X_2^N\right) = \frac{3u^2 - du}{2}\frac{N}{d}\ ,\ \mu_{u,v}\left(X_3^N\right) = (4u^2 - du)\frac{N}{d}.$$

ここで, $i < 2j$ とすれば,

$$\mu_{u,v}\left(X_2^{Ni}\right) - \mu_{u,v}\left(X_3^{Nj}\right) < 0 \Longleftrightarrow u > \frac{(2j-i)d}{8j-3i}$$

となる. そこで

$$1 < \frac{(2j-i)N}{8j-3i} < 2 \tag{3.14}$$

となるような整数の組 (i,j) を取ると, cusp $P(1,N)$ を除いては,

$$\mu_{u,v}\left(X_2^{Ni}\right) < \mu_{u,v}\left(X_3^{Nj}\right)$$

が成り立つ. このとき,

$$\begin{aligned}\mathrm{d}\left(X_2^{Ni}+X_3^{Nj}\right) &= -\left(\sum_{P(u,v)}\mu_{u,v}\left(X_2^{Ni}\right)-\mu_{1,N}\left(X_2^{Ni}\right)+\mu_{1,N}\left(X_3^{Nj}\right)\right)\\ &= i\mathrm{d}\left(X_2^{N}\right)+\frac{3-N}{2}i-(4-N)j.\end{aligned} \tag{3.15}$$

ただし, 和 $\sum_{P(u,v)}$ は, $\Gamma_1(N)$ の cusp を動くものとする.

$$(i_1,j_1)=\left(N-3,\frac{N-1}{2}\right)\ ,\ (i_2,j_2)=\left(N-5,\frac{N-3}{2}\right)$$

とすれば, (i_1,j_1), (i_2,j_2) は不等式 (3.14) を満たす. (3.15) より,

$$\begin{aligned}\mathrm{d}\left(X_2^{Ni_1}+X_3^{Nj_1}\right) &= i_1\mathrm{d}\left(X_2^{N}\right)+\frac{N-5}{2},\\ \mathrm{d}\left(X_2^{Ni_2}+X_3^{Nj_2}\right) &= i_2\mathrm{d}\left(X_2^{N}\right)+\frac{N-3}{2}.\end{aligned}$$

したがって,

$$\begin{aligned}&\mathrm{GCD}\left(\mathrm{d}\left(X_2^{\epsilon_N N}\right),\ \mathrm{d}\left(X_2^{Ni_1}+X_3^{Nj_1}\right),\ \mathrm{d}\left(X_2^{Ni_2}+X_3^{Nj_2}\right)\right)\\ &=\mathrm{GCD}\left(\mathrm{d}\left(X_2^{\epsilon_N N}\right),\ \frac{N-3}{2},\ \frac{N-5}{2}\right)=1\end{aligned}$$

となる. ゆえに,

$$A_1(N)=\mathbb{C}\left(X_2^{\epsilon_N N},X_2^{Ni_1}+X_3^{Nj_1},X_2^{Ni_2}+X_3^{Nj_2}\right).$$

一方, X_2^N, X_3^N は $\mathbb{C}\left(X_2^N,X_2^{Ni_1}+X_3^{Nj_1},X_2^{Ni_2}+X_3^{Nj_2}\right)$ の元なので, $\mathbb{C}\left(X_2^N,X_3^N\right)$ は $\mathbb{C}\left(X_2^N,X_2^{Ni_1}+X_3^{Nj_1},X_2^{Ni_2}+X_3^{Nj_2}\right)$ に含まれる. 逆の包含関係も明らかなので,

$$\mathbb{C}\left(X_2^N,X_3^N\right)=\mathbb{C}\left(X_2^N,X_2^{Ni_1}+X_3^{Nj_1},X_2^{Ni_2}+X_3^{Nj_2}\right)=A_1(N).$$

N が偶数のときは, $j>i\geq 0$ ならば

$$\mu_{u,v}\left(X_2^{Ni\epsilon_N}\right)-\mu_{u,v}\left(X_3^{Nj}\right)<0 \Longleftrightarrow u>\frac{(j-i)d}{4j-3i}$$

となる. そこで, $j>i\geq 0$ を満たし, しかも

$$1<\frac{(j-i)N}{4j-3i}<2$$

となるような整数の組 (i,j) を探せば良い.

$$(i_1,j_1)=(2N-12,2N-9)\ ,\ (i_2,j_2)=(3N-16,3N-12)$$

とすれば, 以下奇数の場合と同様にして主張が示される. □

$A(N)$ の生成元についても同様の計算で次のことが確かめられる.

定理 3.16. 関数 $X_2^{\epsilon_N}, X_3$ は $\mathbb{C}$ 上 $A(N)$ を生成する.

証明. 定数値関数でない $A(N)$ の関数 f に対して, $\mathrm{d}^*(f) = [A(N) : \mathbb{C}(f)]$ とおく. N が奇数のときは 定理 3.13 の証明と同様に (i_1, j_1), (i_2, j_2) をとると,

$$\mathrm{d}^*(X_2^{i_1} + X_3^{j_1}) = i_1 \mathrm{d}^*(X_2) + (N-5)/2,$$
$$\mathrm{d}^*(X_2^{i_2} + X_3^{j_2}) = i_2 \mathrm{d}^*(X_2) + (N-3)/2$$

となるから,

$$\mathrm{GCD}(\mathrm{d}^*(X_2),\ \mathrm{d}^*(X_2^{i_1} + X_3^{j_1}),\ \mathrm{d}^*(X_2^{i_2} + X_3^{j_2}))$$
$$= \mathrm{GCD}(\mathrm{d}^*(X_2),\ (N-5)/2,\ (N-3)/2) = 1.$$

N が偶数のときも $A_1(N)$ の証明と同様にして $A(N) = \mathbb{C}(X_2^2, X_3)$ が示される. □

さらに, 定理 3.13 により次の定理が成り立つ.

定理 3.17. m_0, n_0 は $3m_0 + 8n_0 = \epsilon_N N$ を満す整数とする. このとき $X_2^{m_0} X_3^{n_0}, X_2^8 X_3^{-3}$ は $\mathbb{C}$ 上 $A_1(N)$ を生成する.

証明. 3.1 より, $X_2^{m_0} X_3^{n_0}, X_2^8 X_3^{-3} \in A_1(N)$ である. 定理 3.13 と

$$X_2^{\epsilon_N N} = (X_2^{m_0} X_3^{n_0})^3 \left(X_2^8 X_3^{-3}\right)^{n_0}$$
$$X_3^N = (X_2^{m_0} X_3^{n_0})^{8/\epsilon_N} \left(X_2^8 X_3^{-3}\right)^{-m_0/\epsilon_N}$$

より, $X_2^{m_0} X_3^{n_0}, X_2^8 X_3^{-3}$ は $A_1(N)$ の生成元であることがわかる. □

4. $X(N), X_1(N)$ の定義方程式

前のセクションの定理 3.16 より, 関数 $X_2^{\epsilon_N}, X_3$ は $\mathbb{C}$ 上 $A(N)$ を生成することがわかった. ここではまず, X_3 が $\mathbb{Q}[X_2^{\epsilon_N}]$ 上整であることを示し, さらに $\mathbb{Q}[X_2^{\epsilon_N}]$ 上の X_3 のモニックな既約方程式 $F_N(X_2^{\epsilon_N}, Y) = 0$ を求める. N が素数の場合には方程式 $F_N(X, Y) = 0$ の係数は 各 cusp での $X_2^{\epsilon_N}$, X_3 の Fourier 展開をそれぞれ X, Y に代入して, 帰納的に係数がわかっていない項のなかで最小次の項の係数を 0 とおくことにより, 各項の係数を具体的に求めるアルゴリズムが得られる. 一方, N が素数でない場合にはそのようなアルゴリズムが存在するとは言えないが, すべての係数を決定することは原理的には可能である.

また $A_1(N)$ については同様に, $X_2^{m_0} X_3^{n_0}$ が $\mathbb{Q}[X_2^8 X_3^{-3}]$ 上整であることが示され, 方程式 $F_N(X, Y) = 0$ から $\mathbb{Q}[X_2^8 X_3^{-3}]$ 上の $X_2^{m_0} X_3^{n_0}$ を根にもつモニックな方程式 $E_N(X_2^8 X_3^{-3}, Y) = 0$ を 1 つ導くことができる. もしこの方程式の次数が $[A_1(N) : \mathbb{C}(X_2^{m_0} X_3^{n_0})]$ と一致すれば, この方程式は既約方程式である.

補題 4.1. X_3 は $\mathbb{C}[X_2^{\epsilon_N}]$ 上整である.

証明. $A=\mathbb{C}[X_2^{\epsilon_N}]$, B を $A(N)$ のなかでの A の整閉包とする．B は Dedekind 環 なので B の (0) でない素イデアル $\mathfrak{p}$ は極大イデアルで B の $\mathfrak{p}$ による局所化 $B_{\mathfrak{p}}$ は離散付値環である．さらに

$$B=\cap B_{\mathfrak{p}}$$

である． もし $X_3\notin B$ ならある $\mathfrak{p}$ が存在して $X_3\notin B_{\mathfrak{p}}$ となる．$\mathfrak{p}$ は $X(N)$ のある点 P と対応し X_3 はこの点 P で極を持つ．すると系3.11 より $X_2^{\epsilon_N}$ もこの点 P で極をもつので $X_2^{\epsilon_N}\notin B_{\mathfrak{p}}$ である．$B_{\mathfrak{p}}\supset A\ni X_2^{\epsilon_N}$ なのでこれは矛盾である．よって X_3 は A 上整である． □

上の補題より X_3 の $\mathbb{C}(X_2^{\epsilon_N})$ 上の最小多項式は $\mathbb{C}[X_2^{\epsilon_N}][Y]$ のモニックな多項式から取れる.

補題 4.2. 関数 X_3 は次の形の多項式 $F_N(X,Y)$ に対して, 既約方程式 $F_N(X_2^{\epsilon_N},X_3)=0$ を満す.

$$F_N(X,Y)=Y^{d_2}+\Phi_{d_2-1}(X)Y^{d_2-1}+\cdots+\Phi_1(X)Y+\Phi_0(X)\in\mathbb{Q}[X,Y].$$

$\Phi_{d_2-1}(X),\dots\Phi_1(X),\Phi_0(X)$ は共通因子を持たない $\mathbb{Q}$ 上の X についての多項式.

証明. $d_2=[A(N):\mathbb{C}(X_2^{\epsilon_N})]$ とおく． このとき, $A(N)=\mathbb{C}(X_2^{\epsilon_N},X_3)$ より, 拡大 $A(N)/\mathbb{C}(X_2^{\epsilon_N})$ の拡大次数は d_2 で, 補題 4.1 より $\mathbb{C}(X_2^{\epsilon_N})$ 上次数 d_2 の X_3 のモニックな既約方程式 $\Psi_N(Y)=0$ が存在する.

$\zeta_N=\exp(2\pi i/N)$, $k_N=\mathbb{Q}(\zeta_N)$ とおいて, $\mathfrak{F}_N$ を $A(N)$ の元で cusp $i\infty$ での Fourier 係数が k_N-有理的であるものの全体とすると, $\mathfrak{F}_N$ は $A(N)$ の部分体である. また, $\mathfrak{F}_N$ と $\mathbb{C}$ は k_N 上 linearly disjoint で $A(N)=\mathbb{C}\mathfrak{F}_N$ が成り立つ ([Shi71] Chapter 6 6.2). ゆえに $A(N)=\mathbb{C}(X_2^{\epsilon_N},X_3)$ により体の拡大 $\mathbb{C}/k_N$ は忠実平坦なので $\mathfrak{F}_N$ は k_N 上 $X_2^{\epsilon_N}$ と X_3 で生成されることがわかる. 従って, とくに $\Psi_N(Y)$ として $k_N(X_2^{\epsilon_N})[Y]$ の元が取れる.

$$\Psi_N(Y)=F_N(X,\ Y)$$

とおくと, $F_N(X,Y)\in k_N[X,Y]$ で, Y についての次数は d_2 なので

$$F_N(X,Y)=Y^{d_2}+\Phi_{d_2-1}(X)Y^{d_2-1}+\cdots+\Phi_1(X)Y+\Phi_0(X)$$

の形になっている. ここで $\Phi_{d_2-1}(X),\dots,\Phi_1(X),\Phi_0(X)$ は共通因子を持たない $k_N[X]$ の元である.

一方, $f(\tau)\in\mathfrak{F}_N$ の Fourier 展開を $f(\tau)=\sum c_nq^n$ とすれば, $\mathrm{Gal}\,(k_N/\mathbb{Q})$ の任意の元 σ の $\mathrm{Gal}\,(\mathfrak{F}_N/\mathbb{Q})$ への拡張は $f^\sigma=\sum c_n^\sigma q^n$ で定まる. このことから定数値関数 $F_N(X_2^{\epsilon_N},X_3)\equiv 0$ を考えると $X_2^{\epsilon_N},X_3$ は命題2.11 より cusp $i\infty$ で整係数を持つから,

$$F_N(X,Y)=\sum_{i,j}C_{i,j}X^iY^j,\quad C_{i,j}\in k_N$$

とおくと,

$$0=F_N(X_2^{\epsilon_N},X_3)^\sigma=\sum_{i,j}C_{i,j}^\sigma X_2^{\epsilon_N i}X_3^j.$$

$\sum C_{i,j}^{\sigma} X_2^{\epsilon_N i} X_3^j$ はまた $\mathbb{C}(X_2^{\epsilon_N})$ 上の X_3 の最小多項式となる. したがって, $h_\sigma \in k_N^\times$ が存在し, $F_N^\sigma = h_\sigma F_N$ である. しかし Y^{d_2} の係数が 1 なので $h_\sigma = 1$ となる. ゆえに $C_{i,j}^\sigma = C_{i,j}$ が任意の $\sigma \in \mathrm{Gal}\,(k_N/\mathbb{Q})$ に対して成り立つ. このことから, $C_{i,j} \in \mathbb{Q}$ となる. □

補題 4.3.

$$\max\{\deg \Phi_k(X) \mid 0 \leq k < d_2\} = d_3.$$

証明. 一般に $\mathbb{C}(A, B)$ を $\mathbb{C}$ 上超越次数 1 の体で, A, B はともに $\mathbb{C}$ の元でないものとする.

$$\begin{aligned} \phi: \quad \mathbb{C}[X, Y] &\longrightarrow \mathbb{C}(A, B) \\ X &\longrightarrow A \\ Y &\longrightarrow B \end{aligned}$$

の kernel I は素イデアル で $\mathbb{C}[X, Y]/I$ の超越次元が 1 なので Noether の正規化定理 ([Mat80, p.91] Corollaly 1) と [Mat80, p.92] Corollaly 3 より I は高さ 1 のイデアルである. $\mathbb{C}[X, Y]$ は素元分解環なので, I はある既約元 $F(X, Y)$ で生成され, F は定数倍を除いて一意的に決まる ([Mat80, p.141] Theorem 47).

ここで

$$d = [\mathbb{C}(X, Y) : \mathbb{C}(X)], \quad d' = [\mathbb{C}(X, Y) : \mathbb{C}(X)]$$

とおき,

$$Y^d + a_1(X)Y^{d-1} + \cdots + a_d(X) = 0 \quad (a_i(X) \in \mathbb{C}(X))$$

を Y の $\mathbb{C}(X)$ 上の最小多項式とする. $\mathbb{C}(X)$ の元を掛けて

$$\begin{aligned} b_0(X)Y^d + b_1(X)Y^{d-1} + \cdots + b_d(X) = 0 \quad (b_i(X) \in \mathbb{C}[X]), \\ \mathrm{GCD}(b_0, \cdots, b_d) = 1 \end{aligned}$$

が成り立っていると仮定して良い.

$$G(X, Y) = b_0(X)Y^d + \cdots + b_d(X)$$

とおき, $R = \mathbb{C}[X]$ とすると R は素元分解環であり, $G(X, Y)$ は $R[Y]$ の元として原始多項式である. $G(X, Y)$ は $\mathbb{C}(X)[Y]$ の元としては既約なので, $R[Y] = \mathbb{C}[X, Y]$ の元として既約である. $G(A, B) = 0$ で, G は既約なので G は F の定数倍である. よって $F(X, Y)$ の Y の多項式としての次数は d である. X と Y を入れ替えて, $F(X, Y)$ の X の多項式としての次数は d' である. 補題 4.3 は上の考察を $A = X_2^{\epsilon_N}, B = X_3$ にあてはめればわかる. □

$F_N(X, Y)$ を補題 4.2 の多項式とする. $\mathbb{C}(X_2^{\epsilon_N})$ から $A(N)$ への埋め込みから, $X(N)$ から 1 次元射影空間 $\mathbb{P}^1(\mathbb{C})$ への morphism φ で

$$\varphi(Q) = \begin{cases} (X_2^{\epsilon_N}(Q), 1) & (X_2^{\epsilon_N}(Q) \neq \infty) \\ (1, 0) & (X_2^{\epsilon_N}(Q) = \infty) \end{cases} \tag{4.4}$$

となるものが導かれる. 任意の点 $\alpha \in \mathbb{P}^1(\mathbb{C})$ に対して, φ の逆像 φ^* は

$$\varphi^*(\alpha) = \sum_{i=1}^{r} e_i Q_i \tag{4.5}$$

で与えられる $X(N)$ の divisor である. ここで, $\{Q_1, \cdots, Q_r\}$ は $X(N)$ の点で $X_2(Q_i) = \alpha$ となる点の全体であり, e_i は, $\alpha \neq \infty$ なら $X_2 - \alpha$ の点 Q_i での位数とし, $\alpha = \infty$ ならば $1/X_2$ の点 Q_i での位数とする. 補題 3.12 より,

$$\varphi^*(\infty) = -\sum_{\substack{(u,v)\in V \\ u\leq d/3}} \frac{\epsilon_N}{2}(3u^2 - du)P_{u,v},$$

$$\varphi^*(0) = \sum_{\substack{(u,v)\in V \\ d/3\leq u}} \frac{\epsilon_N}{2}(3u^2 - du)P_{u,v}.$$

一方, (4.5) で $\alpha = \infty$ ならば [Iwa93] Chapters 1,2 よりより次のように言いかえられる.

$T = 1/X_2^{\epsilon_N}$ とおく. $\mathbb{C}(X_2^{\epsilon_N})$ において T に対応する付値を v とおくと, v は $\infty \in \mathbb{P}^1$ に対応している. 剰余体は $\mathbb{C}$ で代数閉体なので, $\mathbb{C}(X_2^{\epsilon_N})$ の完備化は $\mathbb{C}((T))$ である. $X_2^{\epsilon_N}$ が極を持つ $A(N)$ の cusp $P'(u,v)$ の定める付値による完備化を $Q_{u,v}$ とすると,

$$A(N) \otimes \mathbb{C}((T)) \cong \oplus Q_{u,v} \tag{4.6}$$

となる. ただし $Q_{u,v}$ は $X_2^{\epsilon_N}$ が極を持つ $A(N)$ の cusp $P'(u,v)$ の定める付値による完備化の全体をわたるものとする. また v の剰余体は代数閉体なので, 剰余次数はすべて 1 である. ゆえに拡大 $[A(N) : \mathbb{C}(X_2^{\epsilon_N})]$ は完全分岐で, 分岐指数 $e_{u,v}$ は $[Q_{u,v} : \mathbb{C}((T))]$ となる.

$$\Psi(T, Y) = T^{d_3} F_N(1/T, Y)$$

とおくと,

$$A(N) = \mathbb{C}(T)[Y]/(\Psi(T, Y))$$

であり, $\mathbb{C}((T))[Y]$ で $\Psi(T,Y) = \prod G_{u,v}(Y)$ と既約多項式の積に分解される. ただし, $G_{u,v}$ は cusp $P'(u,v)$ に対応する $\mathbb{C}[[T]][Y]$ の原始多項式で, $\deg G_{u,v}(Y) = e_{u,v}$ である. また, 埋め込み

$$A(N) \hookrightarrow Q_{u,v}$$

による X_3 の像は $G_{u,v}(Y)$ の根である.

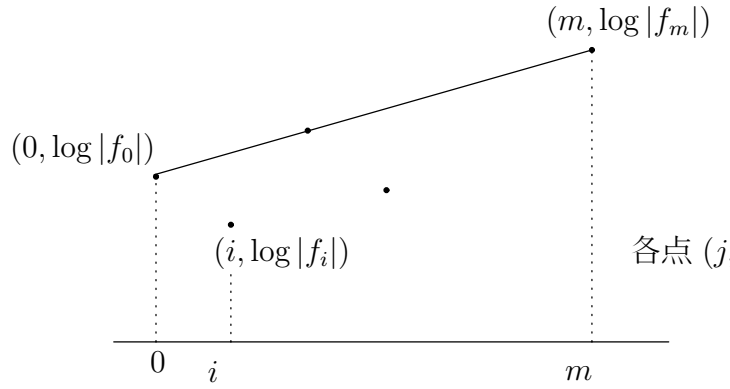
$|\ \ |$ を $\mathbb{C}((T))$ での付値で, $|T| = \lambda$ $(0 < \lambda < 1)$ となるものとする. 多項式

$$f(Y) = f_m Y^m + f_{m-1} Y^{m-1} + \cdots + f_0 \in \mathbb{C}((T))[Y]$$

において $0 \leq j \leq m$ なる任意の j に対して,

$$\log |f_j| \leq \frac{\log |f_m| - |f_0|}{m} j + \log |f_0|$$

となっているとき, つまり



各点 $(j, \log|f_j|)$ は線分の下にある.

このようになっているとき, $f(X)$ は pure であるという. (pure は [Cas86] CHAPTER SIX の Newton polygon の性質の一つある.) また $(m, (\log|f_m| - \log|f_0|)/m)$ を $f(Y)$ のタイプという.

[Cas86] CHAPTER SIX THEOREM 3.1 より次が成り立つ.

補題 4.7. $f(Y) \in \mathbb{C}((T))[Y]$ が既約多項式であるならば pure である.

逆に, pure であっても既約とは限らない.

上の補題より, $G_{u,v}(Y)$ は既約多項式なので pure である.

$$G_{u,v}(Y) = g_{u,v,e_{u,v}} Y^{e_{u,v}} + \cdots + g_{u,v,1} Y + g_{u,v,0}$$

とする. このとき各 k に対して $g_{u,v,k} \in \mathbb{C}[[T]]$ かつ $\mathrm{GCD}(g_{u,v,e_{u,v}}, \cdots g_{u,v,0}) = 1$ である. $G_{u,v}(Y)$ のタイプは $(e_{u,v}, \gamma_{u,v})$ で,

$$\gamma_{u,v} = \frac{\log\left|g_{u,v,e_{u,v}}\right| - \log|g_{u,v,0}|}{e_{u,v}} \tag{4.8}$$

である. 正数 $c_{u,v}$ を $\log c_{u,v} = -\gamma_{u,v}$ となるように取ると,

$$\frac{\log|g_{u,v,j}| - \log|g_{u,v,0}|}{j} \leq \gamma_{u,v} = -\log c_{u,v}$$

より, $|g_{u,v,j}| c_{u,v}^j \leq |g_{u,v,0}|$ であるから, 各 (u, v) に対して

$$|g_{u,v,0}| \geq |g_{u,v,j}| c_{u,v}^j \quad (j = 0, 1, \cdots e_{u,v}) \tag{4.9}$$

となる.

(4.8) より,

$$\left|\frac{g_{u,v,e_{u,v}}}{g_{u,v,0}}\right| = c_{u,v}^{-e_{u,v}} \tag{4.10}$$

となる. $\pi_{u,v}$ を $Q_{u,v}$ の素元として, $f_{u,v}$ を X_3 の位数とすると, (4.10) より $c_{u,v} = |\pi|_{u,v}^{f_{u,v}}$, $(|\pi|_{u,v} = \lambda^{1/e_{u,v}})$ となる. したがって

$$c_{u,v} = \lambda^{\frac{f_{u,v}}{e_{u,v}}},\ \gamma_{u,v} = \frac{f_{u,v}}{e_{u,v}} \log \lambda.$$

集合 $\{(i, j) \mid 0 \leq i \leq d_3, 0 \leq j < d_2, C_{i,j} \neq 0\}$ を $\mathfrak{I}$ とおく. このとき, $\mathfrak{I}$ の元 (i, j) については次が成り立つ.

補題 4.11. (i,j) が $\mathfrak{I}$ の元ならば,

(1) $3i\epsilon_N + 8j \equiv 8d_2 \mod \epsilon_N N$
(2) $\frac{(N-3)}{2} i\epsilon_N + (N-4)j \leq (N-4)d_2$

が成り立つ.

証明. (1) 命題 2.11(2) により, A として $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ をとると, $\zeta_N = \exp\left(\frac{2\pi i}{N}\right)$ として $X_1(\tau) = 1$ に注意すると,

$$X_2(\tau+1) = \exp\left(2\pi i \frac{3}{2N}\right)(-1)X_2(\tau) = \zeta_N^{\frac{3+N}{2}} X_2(\tau).$$
$$X_3(\tau+1) = \exp\left(2\pi i \frac{8}{2N}\right) X_3(\tau) = \zeta_N^4 X_3(\tau).$$

したがって,

$$\begin{aligned} &F_N\left(X_2^{\epsilon_N}(\tau+1), X_3(\tau+1)\right) \\ &= X_3^{d_2}(\tau+1) + \sum_{i,j} C_{i,j} X_2^{i\epsilon_N}(\tau+1) X_3^j(\tau+1) \\ &= \zeta_N^{4d_2} X_3^{d_2}(\tau) + \sum_{i,j} C_{i,j} \zeta_N^{\frac{3+N}{2} i\epsilon_N + 4j} X_2^{i\epsilon_N}(\tau) X_3^j(\tau) \\ &= 0. \end{aligned}$$

ゆえに, $C_{i,j} \neq 0$ ならば, $\zeta_N^{4d_2} = \zeta_N^{\frac{3+N}{2} i\epsilon_N + 4j}$ すなわち

$$4d_2 \equiv \frac{3+N}{2} i\epsilon_N + 4j \mod N. \tag{4.12}$$

N が奇数のとき, $\epsilon_N = 1$ となるので, (4.12) より

$$\begin{aligned} &8d_2 \equiv (N+3)i + 8j \equiv 3i + 8j \mod N \\ \iff &3i + 8j \equiv 8d_2 \mod N. \end{aligned}$$

N が偶数のときは, $\epsilon_N = 2$ なので (4.12) より

$$8d_2 \equiv (N+3)i\epsilon_N + 8j \equiv 3i\epsilon_N + 8j \mod \epsilon_N N.$$

$(i,j) \in \mathfrak{I}$ なので主張が成り立つ.
(2) $X_2^{\epsilon_N}$ が極をもつような $\Gamma(N)$ の cusp の全体を $\mathfrak{U}$ とおくと,

$$\mathfrak{U} = \{(u,v) \mid \mathrm{GCD}(v,N) = d_v > 3,\ \mathrm{GCD}(u,d_v) = 1,\ 0 < u < d_v/3\}$$

である. 先の議論から,

$$\Psi(T,Y) = T^{d_3} F_N\left(\frac{1}{T}, Y\right) = \prod_{(u,v)\in\mathfrak{U}} G_{u,v}(Y)$$

と分解される. $G_{u,v}(Y)$ は cusp $P'(u,v)$ に対応する既約因子である. $G_{u,v}(Y)$ は pure で, そのタイプ $(e_{u,v},\gamma_{u,v})$ において, $e_{u,v}$ は $G_{u,v}(Y)$ の次数, すなわち cusp $P'(u,v)$ での $X_2^{\epsilon_N}$ の極の位数であるから

$$e_{u,v}=\frac{\epsilon_N(d_vu-3u^2)}{2}.$$

また $\gamma_{u,v}$ については,

$$\begin{aligned}\gamma_{u,v}&=-\frac{X_3\text{ の cusp }P'(u,v)\text{ での位数}}{e_{u,v}}\log\lambda\\&=\frac{4(d_vu-4u^2)}{(d_vu-3u^2)\epsilon_N}\log\lambda\\&=\frac{d_v-4u}{d_v-3u}\frac{4}{\epsilon_N}\log\lambda.\end{aligned}$$

$\log\lambda<0$ でありしかも $(d_v-4u)/(d_v-3u)$ は $(u,v)=(1,N)$ のとき最大であることはすぐわかるので, $\mathfrak{U}$ の任意の元 (u,v) に対して $\gamma_{u,v}\geq\gamma_{1,N}$ である. ゆえに

$$c_{u,v}\leq c_{1,N}\tag{4.13}$$

が成り立つ. 簡単のため, $c=c_{1,N}$ とおく.

また, $\mathbb{C}((T))[Y]$ の任意の元 $f(Y)=f_mY^m+f_{m-1}Y^{m-1}+\cdots f_1Y+f_0$ に対して付値 $|\quad|_c$ を次のように定義する.

$$|f(Y)|_c=\max_j\left\{|f_j|c^j\right\}$$

[Cas86] CHAPTER SIX LEMMA 1.1 より $|\quad|_c$ は $\mathbb{C}((T))$ の付値の $\mathbb{C}((T))[Y]$ への拡張になっている.

(4.9) より

$$|G_{u,v}(Y)|_c=\max_j\{|g_{u,v,j}|c^j\}\leq\max_j\{|g_{u,v,0}|c_{u,v}^{-j}c^j\}=|g_{u,v,0}|\max_j\left\{\left(\frac{c}{c_{u,v}}\right)^j\right\}$$

となるが, (4.13) より, $c/c_{u,v}\geq1$ なので, 右辺は $j=e_{u,v}$ のとき最大になる. したがって,

$$|G_{u,v}(Y)|_c\leq|g_{u,v,0}|\left(\frac{c}{c_{u,v}}\right)^{e_{u,v}}=|g_{u,v,0}|c_{u,v}^{-e_{u,v}}c^{e_{u,v}}$$

である. (4.10) より,

$$|g_{u,v,0}|c_{u,v}^{-e_{u,v}}=|g_{u,v,e_{u,v}}|$$

が成り立つので,

$$|G_{u,v}(Y)|_c\leq|g_{u,v,e_{u,v}}|c^{e_{u,v}}$$

が成り立つ. $|G_{u,v}(Y)|_c$ の定義より

$$|G_{u,v}(Y)|_c=\max_j\{|g_{u,v,j}|c^j\}\geq|g_{u,v,e_{u,v}}|c^{e_{u,v}}$$

となるので,

$$|G_{u,v}(Y)|_c = |g_{u,v,e_{u,v}}|c^{e_{u,v}}$$

が成り立つ.

$F_N(X,Y)$ で Y^{d_2} の係数は 1 なので, $\Psi(T,Y)$ では Y^{d_2} の係数は

$$T^{d_3} = \prod g_{u,v,e_{u,v}}$$

である. したがって

$$|\Psi(T,Y)|_c = \prod_{(u,v)\in\mathfrak{U}} |G_{u,v}(Y)|_c = \prod_{(u,v)\in\mathfrak{U}} |g_{u,v,e_{u,v}}|c^{e_{u,v}} = \left|T^{d_3}\right| c^{d_2} = \lambda^{d_3} c^{d_2}$$

が成り立つ. 一方, 定義より

$$|\Psi(T,Y)|_c = \max_j \left\{\left|\Phi_j(1/T)T^{d_3}c^j\right|\right\} = \max_j \left\{\lambda^{d_3-\deg\Phi_j(X)}c^j\right\}$$

となるので,

$$\lambda^{d_3-\deg\Phi_j(X)}c^j \le \lambda^{d_3}c^{d_2}$$

が成り立つ. 両辺の対数をとれば,

$$-\gamma_{1,N} = \log c = 4(N-4)(N-3)^{-1}{\epsilon_N}^{-1}\log\lambda$$

より

$$(d_3 - \deg\Phi_j(X))\log\lambda - j\log c \le d_3\log\lambda + d_2\log c.$$

ゆえに,

$$-\deg\Phi_j(X)\log\lambda\epsilon_N - j\frac{4(N-4)}{(N-3)}\log\lambda \le -d_2\frac{4(N-4)}{(N-3)}\log\lambda$$

である. $0<\lambda<1$ より, $-\log\lambda > 0$ なので上の不等式より補題の不等式が成り立つ. □

$\Phi_j(X) = \sum_{i=0}^{d_3} C_{i,j}X^i$, $(C_{i,j}\in\mathbb{Q})$ とおくと,

$$F_N(X_2^{\epsilon_N}, Y) = Y^{d_2} + \sum_{i,j} C_{i,j}X^{i\epsilon_N}Y^j.$$

但し, 和 $\sum_{i,j}$ は $\{(i,j)\mid 0\le i\le d_3, 0\le j<d_2\}$ を動くものとする.

次に N が素数 p の場合, $C_{i,j}$ を具体的に求める方法を述べる. この場合 $\epsilon_N = \epsilon_p = 1$ である. $X_r(\tau)(r=2,3)$ の $\Gamma(p)$ の cusp での x-展開を考える. ただし $x = \exp(2\pi i\tau/p)$ である. $\Gamma(p)$ の cusp $P'(u,p)$ $((u,p)\in V)$ は有理数 u/p で表される. 各 u に対して

$$B_u = B(u,N) = \begin{pmatrix} u & b \\ p & * \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ ub\equiv 0 \mod 2$$

となる b が取れる. 簡単のため, $\nu_{u,p}(X_r(\tau))$ を $\nu_{r,u}$ と書くことにする. cusp $P'(u,p)$ での $X_r(\tau)$ の x-展開は 命題 2.11 より

$$X_r(B_u(\tau)) = \pm\zeta_p^{\frac{(r^2-1)ub}{2}} x^{\nu_{r,u}}(1+O(x))$$

である. ただし $O(x^n)$ は, 最小次の項が x^n であるようなべき級数を表すものとする. (i,j) を

$$\begin{cases} 0 \le i \le d_3 \\ i < 2(d_2-j)(p-4)(p-3)^{-1} \\ 0 \le j < d_2 \\ 3i+8j \equiv 8d_2 \mod p \end{cases} \tag{4.14}$$

を満す整数の組, もしくは $(0,d_2)$ とする. i についての 2 つ目の条件は命題 4.11 (2) に対応している. このとき

$$X_2(B_u(\tau))^i X_3(B_u(\tau))^j = \pm\zeta_N^{\frac{(3i+8j)ub}{2}} x^{\nu_{2,u}i+\nu_{3,u}j}(1+O(x))$$

であるが, $3i+8j \equiv 8d_2 \mod p$ なので,

$$X_2(B_u(\tau))^i X_3(B_u(\tau))^j = \zeta_N^{4ubd_2}\Theta_{u,i,j}(x)$$

となる. ここで $\Theta_{u,i,j}(x)$ は $\mathbb{Z}[[x]]$ の元で, 最高次の係数は ±1 である. 方程式 $F_N(X,Y)=0$ において, $X=X_2(B_u(\tau))$, $Y=X_3(B_u(\tau))$ とすると,

$$C_{0,d_2}\Theta_{u,0,d_2}(x) + \sum_{(i,j)} C_{i,j}\Theta_{u,i,j}(x) = 0.$$

但し, $C_{0,d_2}=1$, 和 $\sum_{(i,j)}$ は (4.14) を満す整数の組を動くものとする. 集合 S_0 を

$$S_0 = \{(i,j) \mid \text{条件 (4.14) を満す整数の組 }\} \cup \{(0,d_2)\}$$

とする. また, S_1 を S_0 の部分集合で,

$$\begin{cases} (i,j) \in S_1 & \text{なら, } C_{i,j} \text{ の値が決定されている} \\ (i,j) \in S_0 \setminus S_1 & \text{なら, } C_{i,j} \text{ の値が決定されていない} \end{cases}$$

となっているものとする. 以下 S_1 に新たな項を増やせることを示す.

まず, $C_{0,d_2}=1$ がわかってることから, $S_1=\{(0,d_2)\}$ ととれる.

$$\sum_{(i,j)\in S_0\setminus S_1} C_{i,j}\Theta_{u,i,j} = -\sum_{(i,j)\in S_1} C_{i,j}\Theta_{u,i,j} \tag{4.15}$$

において右辺の各項は決定されているので左辺の項について考える. 各 u ($(u,N)\in V$) に対して, 整数 $m(u)$ を

$$m(u) = \min\{\mathrm{ord}_x(\Theta_{u,i,j}(x)) = \nu_{2,u}i+\nu_{3,u}j \mid (i,j)\in S_0\setminus S_1\}$$

とおく. 主張が成り立つことを示すためには次が言えれば良い.

補題 4.16. $\nu_{2,u}i+\nu_{3,u}j = m(u)$ が唯 1 つの解 $(i_u,j_u)\in S_1\setminus S_0$ を持つような整数 u が存在する.

実際, 補題 4.16 が成り立つならば, (4.15) の左辺は $C_{i_u,j_u}x^{m(u)}+O(x^{m(u)+1})$ となり, C_{i_u,j_u} の値が具体的に求められる. (i_u,j_u) を S_1 に付け加えて同じ議論を繰り返せば, 有限回の操作で $S_0=S_1$ が具体的に得られる. 以下, 補題 4.16 を示す.

証明. すべての $u \in \mathbb{Z}$ $(p/3 < u < p/2)$ に対して, 補題 4.16 の等式を満す $S_0 \setminus S_1$ の元が 2 つ存在すると仮定する. この 2 つを $(i_{u,1}, j_{u,1}), (i_{u,2}, j_{u,2})$ $(j_{u,1} > j_{u,2})$ とおく.

$$\nu_{2,u}(i_{u,1} - i_{u,2}) + \nu_{3,u}(j_{u,1} - j_{u,2}) = 0$$

となるが, $\nu_{2,u} = (1/2)(3u^2 - pu)$ と $\nu_{3,u} = 4u^2 - 4up + p^2$ は

$$4u^2 - 4up + p^2 = (p - 3u)(p - u) + u^2$$

より互いに素なので, $j_{u,1} - j_{u,2}$ (> 0) は $\nu_{2,u}$ (> 0) の倍数である. ゆえに, ある正整数 w_u で

$$j_{u,1} - j_{u,2} = \nu_{2,u} w_u$$

となるものが存在する. $p = 7$ の場合, $p/3 < u < p/2$ を満す整数は $u = 3$ のみで, このとき補題 3.12 より $\nu_{2,3} = d_2 = 3$ である. ゆえに, $j_{u,1} - j_{u,2} > 3$ となる. 一方, $(i_{u,1}, j_{u,1}), (i_{u,2}, j_{u,2}) \in S_0 \setminus S_1$ より, $0 < j_{u,1},\ j_{u,2} < 3$ である. したがって矛盾が生じる. また $p > 7$ のときは, $p/3 < u < p/2$ を満す整数 u は 2 つ以上存在するので, それらを $u > u'$ とおくと. $m(u),\ m(u')$ の最小性から

$$\begin{aligned} \nu_{2,u'} i_{u,2} + \nu_{3,u'} j_{u,2} &\geq \nu_{2,u'} i_{u',1} + \nu_{3,u'} j_{u',1} \\ \nu_{2,u} i_{u',1} + \nu_{3,u} j_{u',1} &\geq \nu_{2,u} i_{u,2} + \nu_{3,u} j_{u,2} \end{aligned}$$

となる. 従って

$$\begin{aligned} \nu_{2,u'}(i_{u,2} - i_{u',1}) + \nu_{3,u'}(j_{u,2} - j_{u',1}) &\geq 0 \\ \nu_{2,u}(i_{u',1} - i_{u,2}) + \nu_{3,u}(j_{u',1} - j_{u,2}) &\geq 0. \end{aligned} \tag{4.17}$$

$j_{u',1} > j_{u,2}$ と仮定すると, $i_{u,2} - i_{u'1} > 0$ であるが, (4.17) より

$$(\nu_{2,u'} - \nu_{2,u})(i_{u',1} - i_{u,2}) + (\nu_{3,u'} - \nu_{3,u})(j_{u',1} - j_{u,2}) \leq 0$$

となり, これは $\nu_{2,u} > \nu_{2,u'} > 0$ かつ $\nu_{3,u'} > \nu_{3,u} > 0$ に矛盾する. 従って $j_{u',1} \leq j_{u,2}$ である.

$$L = \left[\frac{p}{3}\right] + 1\ ,\ M = \left[\frac{p}{2}\right],$$

とおく. ただし [ ] は Gauss 記号である. このとき

$$\begin{aligned} j_{M,1} - j_{L,2} &= j_{M,1} - j_{M,2} + j_{M,2} - j_{L,2} \\ &\geq \sum_{L}^{M} (j_{u,1} - j_{u,2}) = \sum_{M}^{L} \nu_{2,u} w_u \\ &\geq \sum_{L}^{M} \nu_{2,u} \geq \sum_{M}^{L} \frac{1}{2}(3u^2 - pu). \end{aligned}$$

いま, p は素数なので, 命題 3.7 より 最終項の総和は X_2 の零点の位数の総和になっているので d_2 に等しい. ゆえに, $j_{M,1} - j_{L,2} \geq d_2$ である. しかし, $(i_{M,1}, j_{M,1})$, $(i_{L,2}, j_{L,2})$ は $S_0 \setminus S_1$ の元なので, $0 \leq j_{L,2} < j_{M,1} < d_2$ となり, 矛盾が生じる. よって主張が示された. □

注 4.18. この証明は, N が素数でない場合には $X_2^{\epsilon_N}$, X_3 の $\Gamma(N)$ の cusp での位数を比較することになるが, このとき命題 3.7 より, 各 cusp $P'(u,v)$ での $\nu_{u,v}(X_2^{\epsilon_N})$, $\nu_{u,v}(X_3)$ の値は $\mathrm{GCD}(v,N)$ に依存するので, 上の証明のように $\nu_{u,v}(X_2^{\epsilon_N})$ の大小関係を一般的に決定することはできない. このことから一般の N についてはこの証明は成り立たない.

補題 4.16 の証明に基いて素数 p に対して $A(p)$ の生成元 $X_2, X_3(\tau)$ の満たす $\mathbb{Q}$ 上の方程式 $F_N(X,Y)=0$ を求めるアルゴリズムが得られる.

アルゴリズム.

(1) : 7 以上の素数 p を入力する.

(2) : $S_0 \leftarrow \{(4.14)$ を満す整数の組 $(i,j)\} \cup \{(0,d_2)$.
$S_1 \leftarrow \{(0,d_2)\}$.
$C_{0,d_2}=1$ として C_{0,d_2} を出力する.

(3) : $\mathfrak{L} \leftarrow S_0 \setminus S_1, \quad l \leftarrow |\mathfrak{L}|$.
もし $l=0$ ならばアルゴリズムは終る.

(4) : $u \leftarrow (p-1)/2$.

(5) : $(i,j) \in \mathfrak{L}$ に対して関数 $X_2^i X_3^j$ の cusp P_u での位数 $o_u(i,j)=\nu_{2,u}i+\nu_{3,u}j$ を計算して

$$o_u(i_{u,1},j_{u,1}) \le o_u(i_{u,2},j_{u,2}) \le \cdots \le o_u(i_{u,l},j_{u,l})$$

となるように並べかえる.

(6) : もし $l \le 2$ かつ $o_u(i_{u,1},j_{u,1})=o_u(i_{u,2},j_{u,2})$ であるならば, $u \leftarrow u-1$ として 5 に戻る.

(7) : m を l 以下の最大の整数で

$$o_u(i_{u,1},j_{u,1}) < o_u(i_{u,2},j_{u,2}) < \cdots < o_u(i_{u,m-1},j_{u,m-1}) < o_u(i_{u,m},j_{u,m})$$

となるようなものとする.
もし $m<l$ ならば, $m \leftarrow m-1, K \leftarrow o_u(i_{u,m},j_{u,m})$ とする.
$(i,j) \in S_1 \cup \{(i_{u,1},j_{u,1}),(i_{u,2},j_{u,2}),\cdots,(i_{u,m},j_{u,m})\}$ に対して, $\Theta_{u,i,j}(x) \mod x^{K+1}$ の x-展開を計算する.

$$\sum_{s=1}^{m} C_{i_{u,s},j_{u,s}} \Theta_{u,i_u,s,j_{u,s}}(x) \equiv -\sum_{(i,j)\in S_1} C_{i,j}\Theta_{u,i,j}(x) \mod x^{K+1}$$

より, $C_{i_{u,s},j_{u,s}}(s=1,..,m)$ を決定する.
$S_1 \leftarrow S_1 \cup \{(i_{u,1},j_{u,1}),(i_{u,2},j_{u,2}),\cdots,(i_{u,m},j_{u,m})\}$
として 3 に戻る.

N が素数でない場合はこのように具体的なアルゴリズムは存在するとは言えない. しかし $\mathbb{Q}$ 上の多項式 $f(X,Y)$ において, $f(X_2^{\epsilon_N},X_3)=0$ が成り立っていて, しかも $f(X,Y)$ の X についての次数が d_3 で Y についての次数が d_2 なら, $f(X,Y)$ は $F_N(X,Y)$ の定数倍になるので, 生成元のあらゆる cusp での Fourier 展開を $f(X_2^{\epsilon_N},X_3)=0$ に代入して係数についての連立方程式を解くことにより, 計算は膨大になるがすべての係数が決定することが原理的には可能である.

次に $A(N)$ の方程式から $A_1(N)$ の方程式を 1 つ導く方法を述べる.
整数 m_0,n_0 は

$$3m_0+8n_0=\epsilon_N N, m_0\geq 0, n_0\leq 0$$

を満たすものとする. 簡単のために,

$$\Lambda=X_2^{m_0}X_3^{n_0}, \Theta=X_2^8X_3^{-3}$$

とおく. また

$$3i_0\epsilon_N+8j_0=\min\{3i\epsilon_N+8j\ (i,j)\in\mathfrak{I}\}$$

とする. このとき, 補題 4.11 により, 任意の $(i,j)\in\mathfrak{I}$ に対して,

$$3i_0\epsilon_N+8j_0\equiv 3i\epsilon_N+8j\equiv 8d_2 \mod \epsilon_N N.$$

(i_0,j_0) の決め方から, ある正整数 k で, $3(i-i_0)\epsilon_N+8(j-j_0)=\epsilon_N Nk$ となるものが存在する. $3m_0+8n_0=\epsilon_N N$ だったので

$$3(i\epsilon_N-i_0\epsilon_N-m_0k)+8(j-j_0-n_0k)=0$$

となるが, GCD(3,8)=1 なので,

$$i\epsilon_N-i_0\epsilon_N-m_0k=-8l, j-j_0-n_0k=3l$$

となる整数 l が存在する. このとき $X_2^iX_3^j=\Lambda^k\Theta^{-l}X_2^{i_0}X_3^{j_0}$ で補題 4.11 (2) より

$$\begin{aligned}3i\epsilon_N+8j &\leq \frac{6(N-4)}{N-3}(d_2-j)+8j\\ &\leq \frac{6(N-4)}{N-3}d_2+\left(8-\frac{6(N-4)}{N-3}\right)j\end{aligned}$$

$0<8-6(N-4)/(N-3)$ なので, $3i\epsilon_N+8j\leq 8d_2$ で, 等号成立は $(i,j)=(0,d_2)$ のときである. さらに, $n_0\leq 0$ なので, $l=(j-j_0-n_0k)/3$ は $(i,j)=(0,d_2)$ のとき最大となる. そこで

$$k_0=\frac{-3i_0\epsilon_N+8(d_2-j_0)}{\epsilon_N N},\ l_0=\frac{d_2-j_0-n_ok_o}{3}$$

とおき, $(i,j) \in \mathfrak{I}$ に対しては,

$$k(i,j) = \frac{3(i-i_0)\epsilon_N + 8(j-j_0)}{\epsilon_N N}\ ,\ l(i,j) = \frac{j - j_0 - n_o k(i,j)}{3}$$

とおくと,

$$F_N\left(X_2^{\epsilon_N}, X_3\right) = X_2^{i_0} X_3^{j_0} \left(\Lambda^{k_0} \Theta^{-l_0} + \sum_{(i,j)\in\mathfrak{I}} C_{i,j} \Lambda^{k(i,j)} \Theta^{-l(i,j)} \right) = 0$$

となる. したがって,

$$\Lambda^{k_0} + \sum_{(i,j)\in\mathfrak{I}} C_{i,j} \Lambda^{k(i,j)} \Theta^{l_0 - l(i,j)} = 0.$$

$E_N(X,Y) = Y^{k_0} + \sum_{(i,j)\in\mathfrak{I}} C_{i,j} X^{l_0 - l(i,j)} Y^{k(i,j)}$ とおけば, $A_1(N)$ の生成元 $\Lambda =, \Theta$ が満たす $\mathbb{Q}$ 上モニックな方程式 $E_N(X,Y)$ が得られる.

5. $F_N(X^{\epsilon_N}, Y) = 0, E_N(X,Y) = 0$ の例

セクション 4 で与えたアルゴリズムを用いて $F_N(X^{\epsilon_N}, Y), E_N(X,Y)$ を実際に求めることができる. ここでは各 N についてそのいくつかの例を挙げ, F_N, E_N から求まる算術種数と $X(N)$, $X_1(N)$ の実際の種数を比較してみることにする. もし算術種数と曲線の種数が一致していれば, 与えた方程式は非特異な affine model を与えていることがわかる. $X(N)$, $X_1(N)$ の種数をそれぞれ, $g(N)$, $g_1(N)$ とおく. 方程式 F_N, E_N から求まる算術種数は次数を d とすれば, $(d-1)(d-2)2^{-1}$ で与えられる. F_N, E_N の算術種数をそれぞれ $g'(N), g_1'(N)$ とおく. $X(N)$, $X_1(N)$ の種数 $g(N)$, $g_1(N)$ は [Ste99] Proposition 8.5 より次の式で与えられている.

$$g(N) = 1 + \frac{(N-1)N^2}{24} \prod_{\substack{p|N \\ p:\text{素数}}} \left(1 - \frac{1}{p^2}\right) \quad (N > 2),$$

$$g_1(N) = 1 + \frac{N^2}{24} \prod_{\substack{p|N \\ p:\text{素数}}} \left(1 - \frac{1}{p^2}\right) - \frac{1}{4} \sum_{\substack{d|N \\ d:\text{正整数}}} \varphi(d)\varphi\left(\frac{N}{d}\right) \quad (N > 4).$$

ただし, φ は Eular 関数で, $\varphi(N) = \sharp\left(\mathbb{Z}/N\mathbb{Z}\right)^\times$ である.

(1) $N = 7 \quad (m_0 = 5, n_0 = -1)$

$$F_7(X,Y) = Y^3 - X^3 Y + X,$$
$$E_7(X,Y) = Y^3 - XY^2 + X^2.$$

$g(7) = 3, g'(7) = 3, g_1(7) = 0, g_1'(7) = 1$

(2) $N = 8 \quad (m_0 = 8, n_0 = -1)$

$$F_8(X,Y) = Y^7 + 2Y^5 + Y^3 - X^4 Y^2 + X^4,$$
$$E_8(X,Y) = Y^2 + (2X - X^2)Y + X^2 + X^3.$$

$g(8) = 5, g'(8) = 15, g_1(8) = 0, g_1'(8) = 1$

(3) $N = 9 \quad (m_0 = 3, n_0 = 0)$

$$\begin{aligned} F_9(X,Y) &= Y^6 - (X^5 - X^2)Y^3 + X^7 - 2X^4 + X, \\ E_9(X,Y) &= Y^5 - XY^4 + XY^3 + X^2Y^2 - 2X^2Y + X^2. \end{aligned}$$

$g(9) = 10, g'(9) = 21, g_1(9) = 0, g_1'(9) = 6$

(4) $N = 10 \quad (m_0 = 12, n_0 = -2)$

$$\begin{aligned} F_{10}(X,Y) &= Y^{14} + 4X^2Y^{10} + 2Y^9 - X^6Y^7 - 2X^4Y^6 + 3X^2Y^5 + Y^4 \\ &\quad + X^8Y^3 - 3X^6Y^2 + 3X^2Y - X, \\ E_{10}(X,Y) &= Y^5 + (4X^2 - X^3)Y^4 + (X^5 - 2X^4 + 2X^3)Y^3 \\ &\quad + 3(X^5 - X^6)Y^2 + (X^6 + 3X^7)Y - X^8. \end{aligned}$$

$g(10) = 13, g'(10) = 78, g_1(10) = 0, g_1'(10) = 21$

(5) $N = 11 \quad (m_0 = 9, n_0 = -2)$

$$\begin{aligned} F_{11}(X,Y) &= Y^{12} - X^7Y^8 + 2X^6Y^7 - 4X^5Y^6 + 5X^4Y^5 - 2X^3Y^4 \\ &\quad + (X^{13} + X^2)Y^3 - (3X^{12} + X)Y^2 + 3X^{11}Y - X^{10} \\ E_{11}(X,Y) &= Y^7 - X^2Y^6 + 2X^3Y^5 + (X^5 - 4X^4)Y^4 \\ &\quad - (3X^6 - 5X^5)Y^3 + (3X^7 - 2X^6)Y^2 - (X^8 - X^7)Y. \end{aligned}$$

$g(11) = 26, g'(11) = 105, g_1(11) = 1, g_1'(11) = 28$

(6) $N = 12 \quad (m_0 = 8, n_0 = 0)$

$$\begin{aligned} F_{12}(X,Y) &= Y^{21} - 2Y^{18} + (6X^2 + 1)Y^{15} - (X^4 - 14X^2)Y^{12} \\ &\quad - (7X^4 + X^2)Y^9 + (X^6 + 6X^4 + 9X^2)Y^6 \\ &\quad - (2X^6 - 4X^4 + 2X^2)Y^3 + X^6 - 2X^4 + X^2, \\ E_{12}(X,Y) &= Y^6 - (X^3 - 6X^2 + 2X)Y^5 + (X^5 - 7X^4 + 14X^3 + X^2)Y^4 \\ &\quad - (2X^6 - 6X^5 + X^4)Y^3 + (X^7 + 4X^6 + 9X^5)Y^2 \\ &\quad - (2X^7 + 2X^6)Y + X^7. \end{aligned}$$

$g(12) = 25, g'(12) = 190, g_1(12) = 1, g_1'(12) = 28$

(7) $N = 13 \quad (m_0 = 7, n_0 = -1)$

$$\begin{aligned}
F_{13}(X,Y) &= Y^{20} + XY^{18} - X^2Y^{16} - X^9Y^{15} + 2X^3Y^{14} + 2X^{10}Y^{13} \\
&\quad - 5X^4Y^{12} - 7X^{11}Y^{11} - X^5Y^{10} + 14X^{12}Y^9 + (X^{19} + 6X^6)Y^8 \\
&\quad - 10X^{13}Y^7 - (3X^{20} + 7X^7)Y^6 + (4X^{14} - X)Y^5 + (3X^{21} + 5X^8)Y^4 \\
&\quad - 4X^{15}Y^3 - X^{22}Y^2 + 2X^{16}Y - X^{10}, \\
E_{13}(X,Y) &= Y^{10} - (X^2 - X)Y^9 + (2X^3 - X^2)Y^8 + (X^5 - 7X^4 + 2X^3)Y^7 \\
&\quad - (3X^6 - 14X^5 + 5X^4)Y^6 + (3X^7 - 10X^6 - X^5)Y^5 \\
&\quad - (X^8 - 4X^7 - 6X^6)Y^4 - (4X^8 + 7X^7)Y^3 + (2X^9 + 5X^8)Y^2 \\
&\quad - X^8Y - X^{10}
\end{aligned}$$

$$g(13) = 50, g'(13) = 325, g_1(13) = 2, g_1'(13) = 66$$

参考文献

[Cas86] J. W. S. Cassels. *Local Fields*, volume 3 of *London Math. Soc. Student Text*. Cambridge University Press, 1986.

[Har77] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1977.

[II96] N. Ishida and N. Ishii. The equations for modular function fiels of principl congruence subgroups of prime level. *Manuscripta Math.*, 90:271–285, 1996.

[II98] N. Ishida and N. Ishii. Generator and equations for modular function fields of principal congruence subgroups. *Acta Arith.*, 85, 3:197–207, 1998.

[II99] N. Ishida and N. Ishii. The equation for tha modular curve $X_1(N)$ derived from the equation for the modular curve $X(N)$. *Tokyo J. Math.*, 22, 1:167–175, 1999.

[Ish83] N. Ishii. Construction of generators of modular function fiels. *Math Japon.*, 38:655–681, 1983.

[Iwa93] K. Iwasawa. *Algebraic functions*, volume 118 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, 1993.

[KL75] D. Kubert and S. Lang. Units in the modular function fields. *Math. Ann.*, 218:175–189, 1975.

[Mat80] H. Matsumura. *Commutative Algebra*, volume 56 of *Mathematics Lecture Note Series* . Benjamin/Cummings Publishing Co., Inc., Reading, 1980.

[Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Iwanami/Princeton University Press, Princeton, 1971.

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Heidelberg, New York, 1994.

[Ste99] S. A. Stepanov. *Codes on algebraic curves*. Kluwer Academic / Plenum Publishers, New York, 1999.