RIMS Kôkyûroku Bessatsu
B51 (2014), 347–374

モジュラー曲線のヤコビ多様体の rational torsion について (Rational torsion in modular Jacobian varieties)

By

太田 雅己 (Masami Ohta)*

Abstract

Let $J_0(N)$ and $J_1(N)$ be the usual modular Jacobian varieties defined over the rational number field. In this article, we first review known results on their rational torsion subgroups. We then state and outline the proof of our recent results on these groups.

§1. 序：背景と結果

N は正整数とし，

$$\begin{cases} \Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\}, \\ \Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N) \;\middle|\; a \equiv d \equiv 1 \pmod{N} \right\} \end{cases} \tag{1.1}$$

とする．これらの群は複素上半平面

$$H := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\} \tag{1.2}$$

に一次分数変換で作用し，商空間 $\begin{cases} \Gamma_0(N)\backslash H \\ \Gamma_1(N)\backslash H \end{cases}$ には自然に（開）リーマン面の構造が入る．各々はカスプの集合 $\begin{cases} \Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q}) \\ \Gamma_1(N)\backslash\mathbb{P}^1(\mathbb{Q}) \end{cases}$ $(\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \infty)$ を付け加える事によりコンパクト リーマン面となる．これら（を $\mathbb{C}$ 上の代数曲線と見たもの）は自然な $\mathbb{Q}$ 上の

Received March 27, 2013. Revised August 9, 2013.
2010 Mathematics Subject Classification(s): 11G18, 14G35.
Key Words: *modular Jacobian variety, rational torsion, Eisenstein ideal.*
*東海大学 P.E.
e-mail: ohta@tokai-u.jp

モデル，志村の canonical model $\begin{cases} Y_0(N) \\ Y_1(N) \end{cases}$ 及び $\begin{cases} X_0(N) \\ X_1(N) \end{cases}$ を持つ（志村 [Sh, 6.7]）．但し，$Y_1(N) \subset X_1(N)$ については普通使われるモデルは 2 種類あるが，カスプ 0（即ち $0 \in \mathbb{P}^1(\mathbb{Q})$ の定める点）が $X_1(N)$ の $\mathbb{Q}$-有理点である方を上記の記号で表す事にしておく．（もう一方のカスプ ∞ が $\mathbb{Q}$-有理的であるモデル $Y_\mu(N) \subset X_\mu(N)$ も第 2 節で用いるが，$\mathbb{Q}$ 上の代数曲線として $X_1(N)$ と $X_\mu(N)$ は同型なので，Jacobi 多様体の rational torsion については一方のみ扱えば足りる．）

$\begin{cases} J_0(N) \\ J_1(N) \end{cases}$ で $\begin{cases} X_0(N) \\ X_1(N) \end{cases}$ の $\mathbb{Q}$ 上定義された Jacobi 多様体を表す事にする．小論で扱う対象はこれらの $\mathbb{Q}$-有理点のなす群のねじれ部分群（rational torsion subgroup）$J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ 及び $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$ である．なお，$J_0(N)$ については $N \leq 10, N = 12, 13, 16, 18, 25$ の時，$J_1(N)$ については $N \leq 10, N = 12$ の時（及びその時に限り）次元が 0 となるので当然 rational torsion も自明である．

まず背景について述べよう．一般に $X_0(N), X_1(N)$ のカスプは $\mathbb{Q}(e^{2\pi i/N})$ 上有理的であり，カスプに台をもつ次数 0 の因子類全体は $J_0(N)(\mathbb{Q}(e^{2\pi i/N}))$, $J_1(N)(\mathbb{Q}(e^{2\pi i/N}))$ の部分群をなす（cuspidal divisor class group）．Manin-Drinfel'd の定理 [Dr] によればこれらは有限群である．（より一般に $SL_2(\mathbb{Z})$ の合同部分群についても同じ事が言える．）しかし，彼らの議論からはそれらの位数（cuspidal class number）等のより詳しい情報は得られない．

まず N が素数 (≥ 5) の場合の $J_0(N)$ を考える．$X_0(N)$ のカスプは 0 と ∞ の 2 個で共に $\mathbb{Q}$-有理的である．よってこの場合の cuspidal divisor class group $\mathcal{C}_0(N)$ は $(0) - (\infty)$ で生成される $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ の巡回部分群であるが，Ogg [Og1] はその位数を計算した：

$$\mathcal{C}_0(N) \cong \mathbb{Z}/n\mathbb{Z}, \text{ 但し } n = ((N-1)/12 \text{ の分子 }) = (N-1)/(12, N-1). \tag{1.3}$$

Ogg [Og2] は更に，$\mathcal{C}_0(N)$ が $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ に一致する事を予想し，Mazur の 1977 年の大論文中で解決された：

定理 1.1 ([M, Theorem (1)]). N が 5 以上の素数の時

$$J_0(N)(\mathbb{Q})_{\mathrm{tors}} = \mathcal{C}_0(N).$$

これらの仕事のうち，cuspidal class number に関する部分は，1970 年代に始まる Kubert と Lang の一連の論文以降多くの人によって研究・拡張されてきた．それに触れる前に次の事を注意しておく：$N \geq 1$ は一般として，自然な $\mathbb{Q}$ 上の射 $X_1(N) \to X_0(N)$ があり，$X_1(N)$ は $\Gamma_0(N)/\{\pm 1\}\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$ （$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d \bmod N$）を Galois 群に持つ $X_0(N)$ の Galois 被覆である．$X_0(N)$ のカスプ 0 は $\mathbb{Q}$-有理的であるが，上の射による逆像（$X_1(N)$ の 0-カスプ（の集合）と呼ぶ）も全て $\mathbb{Q}$-有理的である．

$$\mathcal{C}_1(N) := (\text{0-カスプに台を持つ次数 0 の因子類全体}) \subseteq J_1(N)(\mathbb{Q})_{\mathrm{tors}} \tag{1.4}$$

とおく．次の結果が得られていた．

• Klimek（学位論文らしい）：p が 5 以上の素数の時の $|\mathcal{C}_1(p)|$ の公式；

• Kubert-Lang [KL]: p が 5 以上の素数の時の $|\mathcal{C}_1(p^r)|$ の公式；

• Yu [Y]: 一般の N での $|\mathcal{C}_1(N)|$ の公式；

• 高木 [T1], [T2] 等の一連の論文: p が素数の時（2 の偶数乗を除いて）$X_1(p^r)$ の（前頁の意味の）cuspidal class number の公式；

• 高木 [T3]: N が平方因子を持たない時の $X_0(N)$ の cuspidal class number の公式.

小論で扱うのは最初と最後の場合なので，Klimek 及び高木の公式を具体的に書いておく．まず，N が 5 以上の素数の時 (cf. [KL, Chapter 6, Theorem 3.4])：

$$|\mathcal{C}_1(N)| = N \cdot \prod_{\chi} \frac{B_{2,\chi}}{4} =: c_1(N). \tag{1.5}$$

ここで積は mod N の非自明かつ偶な Dirichlet 指標を動き，$B_{2,\chi}$ $(= \frac{1}{N}\sum_{a=1}^{N}\chi(a)a^2)$ は generalized Bernoulli 数である．

次に $N > 1$ が平方因子を持たないとし，$N = l_1 \cdots l_m$ を素因数分解とする．この時 $X_0(N)$ には 2^m 個のカスプがあり全て $\mathbb{Q}$-有理的である．よってその cuspidal divisor class group $\mathcal{C}_0(N)$ は $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ の部分群である．これについて (cf. [T3, Theorem 5.1]):

$$|\mathcal{C}_0(N)| = 2^a \times 3^b \times \prod_{\boldsymbol{\varepsilon}} \frac{1}{24}(l_1+\varepsilon_1)\cdots(l_m+\varepsilon_m) =: c_0(N). \tag{1.6}$$

ここで積は $\boldsymbol{\varepsilon} = (\varepsilon_1, \cdots, \varepsilon_m) \in \{\pm 1\}^m$ で $(+1, \cdots, +1)$ 以外の $2^m - 1$ 個の符号を動く．また，3 の指数 b は上の積に現れる $(1/24)(l_1+\varepsilon_1)\cdots(l_m+\varepsilon_m)$ のうちで 3-進整数でないものの個数である．（[T3] では a も具体的に与えられているが小論では使わないので省く.）

他方 rational torsion 自身については次の結果が知られていた．

• Lorenzini [Lo]: p は 5 以上の素数とする．$J_0(p^r)(\mathbb{Q})_{\mathrm{tors}}$ の prime-to-6p 部分は cuspidal divisor class group に含まれる．$p \not\equiv 11 \pmod{12}$ の時は prime-to-2p 部分について同じ事が言え，更にその群構造も具体的に記述される．

なお，Ling [Li] は $p \equiv 11 \pmod{12}$ の時にも prime-to-6p 部分の構造を決定している．

• Kamienny [Kam]: N が 5 以上の素数の時，素数 $p \geq 5$ が $|A(\mathbb{Q})_{\mathrm{tors}}|$（ここで $A := J_1(N)/(J_0(N)$ の像$)$）を割るならば p は $c_1(N)$ を割る．

• Agashe [Ag]: E は $\mathbb{Q}$ 上の，導手 N が平方因子をもたない楕円曲線とする.（従って $J_0(N) \twoheadrightarrow E$ がある.） $6N$ を割らない素数 p が $|E(\mathbb{Q})_{\mathrm{tors}}|$ を割るならば p は $c_0(N)$ の約数．

また，次の予想があった：

予想. (Conrad, Edixhoven and Stein [CES, Conjecture 6.2.2]) N が素数の時

$$J_1(N)(\mathbb{Q})_{\mathrm{tors}} = \mathcal{C}_1(N).$$

小論の目的は次の二つの結果の証明の概略を述べる事である.

主定理 I. N は素数とする. 上記 Conrad, Edixhoven 及び Stein の予想は 2-torsion 部分を除いて正しい : 奇素数 p に対して

$$J_1(N)(\mathbb{Q})[p^\infty] = \mathcal{C}_1(N)[p^\infty].$$

但し, 記号 "$[p^\infty]$" は p-torsion 部分を表す.

主定理 II. N は平方因子を持たないとする. p は奇素数とし, N が 3 で割り切れる時は更に $p \neq 3$ とする. この時

$$J_0(N)(\mathbb{Q})[p^\infty] = \mathcal{C}_0(N)[p^\infty].$$

以下第 2 節で主定理 I の, 第 3 節で主定理 II の証明のあらすじを述べる. 詳細については [Oh2], [Oh3] を見られたい.

§2. $J_1(N)$ (N: 素数) の場合

§2.1. モジュラー形式

$f(z)$ が複素上半平面 H 上の関数の時, 正整数 k と $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})^+$ に対して

$$(f|_k\gamma)(z) := \det(\gamma)^{k/2}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) \tag{2.1}$$

とおく.

$\Gamma_1(N)$ に関する重さ k のモジュラー形式 (resp. カスプ形式) とは H 上の正則関数 $f(z)$ で, 任意の $\gamma \in \Gamma_1(N)$ に対して $f|_k\gamma = f$ をみたし, かつ各カスプで正則な (resp. 消える) ものであった. 以下このようなもののなす $\mathbb{C}$ 上の線形空間を $M_k(\Gamma_1(N))$ (resp. $S_k(\Gamma_1(N))$) で表す.

次にモジュラー形式の代数的理論について復習する. 簡単のため $N \geq 5$ とし, R を $\mathbb{Z}[1/N]$-algebra とする. R-スキーム S 上の楕円曲線 E と S-群スキームの閉埋め込み $i : \boldsymbol{\mu}_N \hookrightarrow E[N]$ ($\boldsymbol{\mu}_N$ は 1 の N 乗根のなす群スキーム ; "$[N]$" は N 倍の核) の組 (E, i) を分類する fine モジュライスキーム $Y_\mu(N)_{/R}$ が存在する. これの自然なコンパクト化を $X_\mu(N)_{/R}$ とする. ($X_\mu(N)_{/\mathbb{Q}} = X_\mu(N)$ が, カスプ ∞ が $\mathbb{Q}$-有理的な $\Gamma_1(N)\backslash(H \cup \mathbb{P}^1(\mathbb{Q}))$ の canonical model である. なお, $Y_1(N)$ は E と $\mathbb{Z}/N\mathbb{Z} \hookrightarrow E$ の組のモジュライスキーム.) これのカスプの部分スキーム

$$C_{/R} := X_\mu(N)_{/R} - Y_\mu(N)_{/R} \text{ (reduced な閉部分スキーム)} \tag{2.2}$$

は R 上有限エタールで，$X_\mu(N)_{/R}/R$ の effective な Cartier 因子（Katz-Mazur [KM, (1.1.1)]）である．$Y_\mu(N)_{/R}$ 上には上記のものの普遍族 $\pi : \mathcal{E} \to Y_\mu(N)_{/R}$（と $\boldsymbol{\mu}_N \hookrightarrow \mathcal{E}[N]$）が存在する．$\underline{\omega}_{/R} := \pi_*(\Omega^1_{\mathcal{E}/Y_\mu(N)_{/R}})$ は自然に（Tate 曲線を用いる事により，または $X_\mu(N)_{/R}$ を一般楕円曲線のモジュライと見る事により）$X_\mu(N)_{/R}$ 上の可逆層に延長でき，これも同じ記号 $\underline{\omega}_{/R}$ で表す．

$$\begin{cases} S_k(\Gamma_1(N); R) := H^0(X_\mu(N)_{/R}, \underline{\omega}^{\otimes k}_{/R}(-C_{/R})), \\ M_k(\Gamma_1(N); R) := H^0(X_\mu(N)_{/R}, \underline{\omega}^{\otimes k}_{/R}) \end{cases} \tag{2.3}$$

が Deligne-Rapoport [DR], Katz [Kat1], [Kat2] の意味での R 上定義されたカスプ形式とモジュラー形式の空間であった．(Diamond-Im [DI], Gross [G] に良いサーベイがある．)

$S_k(\Gamma_1(N); \mathbb{C})$, $M_k(\Gamma_1(N); \mathbb{C})$ は $S_k(\Gamma_1(N))$, $M_k(\Gamma_1(N))$ と標準的に同型である（ので以下同一視する）．また，(2.3) の空間の formation は $k \geq 2$ なら任意の $\mathbb{Z}[1/N]$-algebra の底変換と可換である．

Tate 曲線を用いて，$R = \mathbb{C}$ の時にはカスプ ∞ での Fourier 展開になる，q-展開写像

$$\begin{cases} S_k(\Gamma_1(N); R) \to qR[[q]], \\ M_k(\Gamma_1(N); R) \to R[[q]] \end{cases} \tag{2.4}$$

が定義される．左辺の元 f の右辺での像を

$$f(q) = \sum_{n=0}^{\infty} a(n; f) q^n \tag{2.5}$$

で表す．次はしばしば有用である：

q-expansion principle. 上の二つの写像は単射．更に，R_0 が R の $\mathbb{Z}[1/N]$-部分環の時，(2.3) の左辺の元 f が R_0 上定義されている必要十分条件は $f(q) \in R_0[[q]]$ となる事である．

これより，R が $\mathbb{C}$ の $\mathbb{Z}[1/N]$-部分環の時には，(2.3) の左辺は「素朴な R 上のカスプ（またはモジュラー）形式」の空間：

$$\begin{cases} \{f \in S_k(\Gamma_1(N)) \mid a(n; f) \in R, \forall n \geq 1\}, \\ \{f \in M_k(\Gamma_1(N)) \mid a(n; f) \in R, \forall n \geq 0\} \end{cases} \tag{2.6}$$

と同一視できる．

以下，本節では $k = 2$ の場合のみ考え，N は 5 以上の素数とする． 任意の $\mathbb{Z}[1/N]$-algebra R に対して小平-Spencer 同型

$$\underline{\omega}^{\otimes 2}_{/R} \cong \Omega^1_{/R}(C_{/R}), \text{ 但し } \Omega^1_{/R} = \Omega^1_{X_\mu(N)_{/R}/R} \tag{2.7}$$

があり，これにより重さ 2 のモジュラー形式は微分形式と同一視できる事にまず注意する．

$M_2(\Gamma_1(N))$ の Eisenstein 級数の空間（即ち Petersson metric に関する $S_2(\Gamma_1(N))$ の直交補空間）は次の $N-2$ 個の一次独立な元で張られる：

$$\begin{cases} E_2 = \frac{N-1}{24} + \sum_{n=1}^{\infty}(\sum_{\substack{0<t|n \\ N\nmid t}} t)q^n, \\ E_{2,\chi} = -\frac{B_{2,\chi}}{4} + \sum_{n=1}^{\infty}(\sum_{0<t|n} \chi(t)t)q^n, \\ E'_{2,\chi} = \sum_{n=1}^{\infty}(\sum_{0<t|n} \chi(\frac{n}{t})t)q^n. \end{cases} \tag{2.8}$$

ここで $q = e^{2\pi iz}$, χ は mod N の非自明かつ偶な Dirichlet 指標とした．これらのうち E_2 は $\Gamma_0(N)$ に関する Eisenstein 級数である．

前節で述べた Klimek の公式 (1.5) の右辺の $c_1(N)$ は 2 番目の Eisenstein 級数の定数項の積に $\pm N$ をかけたものである事に注意しよう．カスプ形式の Hecke 環の中の「Eisenstein イデアル」の指数が $c_1(N)$ にほぼ等しい事（§2.3 参照）が主定理 I の証明の key step になるのであるが，そのためには普通のモジュラー形式の空間は（上の 1 番目と 3 番目の「余計な」 Eisenstein 級数を含んでいて）大きすぎるので次の “hybrid” な空間を考える事にする：

定義 2.1. $\mathbb{Z}[1/N]$-algebra R に対して

$$M_2^{\infty}(\Gamma_1(N);R) := H^0(X_\mu(N)_{/R}, \underline{\omega}_{/R}^{\otimes 2}(-C_{0/R})) \cong H^0(X_\mu(N)_{/R}, \Omega^1_{/R}(C_{\infty/R}))$$

とおく．但し $C_{0/R}$, $C_{\infty/R}$ は $X_\mu(N)_{/R} \to X_0(N)_{/R}$ による，カスプ 0, ∞ の定める $X_0(N)_{/R}$ の切断の逆像とした．

従って

$$S_2(\Gamma_1(N);R) \subseteq M_2^{\infty}(\Gamma_1(N);R) \subseteq M_2(\Gamma_1(N);R) \tag{2.9}$$

であり，$M_2^{\infty}(\Gamma_1(N);R)$ は 0-カスプで消える（$\Leftrightarrow$ 対応する微分形式は ∞-カスプでのみ高々 1 位の極を持つ）モジュラー形式の空間である．$M_2^{\infty}(\Gamma_1(N);\mathbb{C})$ の Eisenstein 級数の空間は (2.8) の $E_{2,\chi}$ で張られる $(N-3)/2$ 次元部分空間となる．

空間 $M_2^{\infty}(\Gamma_1(N);R)$ の formation も任意の $\mathbb{Z}[1/N]$-algebra の底変換と可換であり，q-expansion principle も成り立つ．

§2.2. Hecke 環

以下しばらく（系 2.7 まで）R は $\mathbb{Z}[1/N]$-algebra とする．

$M_2(\Gamma_1(N);R)$ にはダイアモンド作用素 $\langle d\rangle$ $(d \in (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\})$ と Hecke 作用素 $T(n)$（n は自然数）が作用する：$Y_\mu(N)_{/R}$ は §2.1 のはじめで述べた組 (E,i) のモジュ

ライスキームであったが $(E,i)\mapsto(E,d\cdot i)$ により $X_\mu(N)_{/R}$ の自己同型が定まり，これによる微分形式の引き戻しとして $\langle d\rangle$ が定義される．また各素数 l に対して $X_\mu(N)_{/R}$ の Hecke 対応と呼ばれる代数的対応があり，それによる微分形式への（contravariant な）作用として $T(l)$ が定義される．一般の自然数 n に対しては $T(l)$ からよく知られた漸化式

$$\begin{cases} T(l^{e+1})=T(l)T(l^e)-l\langle l\rangle T(l^{e-1}),\ e\geq 1,\ l\nmid N \text{ の時},\\ T(l^e)=T(l)^e,\ l\mid N \text{ の時},\\ T(n_1n_2)=T(n_1)T(n_2),\ \text{但し } (n_1,n_2)=1 \end{cases} \tag{2.10}$$

により $T(n)$ が定まる．$f\in M_2(\Gamma_1(N);R)$ の q-展開の係数について

$$a(1;f\mid T(n))=a(n;f) \tag{2.11}$$

が全ての $n\geq 1$ に対して成り立つ．（次節では記号 “$f\mid_2 T(n)$” を使うがここでは重さ 2 の場合しか扱わないので添字 “$_2$” は省く．）

ダイアモンド作用素と Hecke 作用素は $M_2(\Gamma_1(N);R)$ の部分空間 $S_2(\Gamma_1(N);R)$ と $M_2^\infty(\Gamma_1(N);R)$ を自身に写す．それらの各部分空間への制限も同じ記号で表す事にする．

定義 2.2. $M_2(\Gamma_1(N);R)$, $M_2^\infty(\Gamma_1(N);R)$, $S_2(\Gamma_1(N);R)$ の Hecke 環

$$\begin{cases} H(\Gamma_1(N);R)\subseteq \mathrm{End}(M_2(\Gamma_1(N);R)),\\ H^\infty(\Gamma_1(N);R)\subseteq \mathrm{End}(M_2^\infty(\Gamma_1(N);R)),\\ h(\Gamma_1(N);R)\subseteq \mathrm{End}(S_2(\Gamma_1(N);R)) \end{cases}$$

をそれぞれ，全ての $\langle d\rangle$ と $T(n)$ で生成される R-部分環として定義する．

なお，どの場合も Hecke 環は可換であり，R 上 $\langle d\rangle$ と $T(l)$（l: 素数）のみでも，また全ての $T(n)$ のみでも生成される．次の定理は後で Eisenstein イデアルの指数を計算する際大事である：

定理 2.3. ペアリング

$$\begin{cases} S_2(\Gamma_1(N);\mathbb{Z}[1/N])\times h(\Gamma_1(N);\mathbb{Z}[1/N])\to\mathbb{Z}[1/N],\\ M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N])\times H^\infty(\Gamma_1(N);\mathbb{Z}[1/N])\to\mathbb{Z}[1/N] \end{cases}$$

をどちらも

$$(f,t):=a(1;f\mid t)$$

で定義するとこれらは有限階数の自由 $\mathbb{Z}[1/N]$-加群の完全なペアリングである．即ち左辺の 2 項のどちらもこのペアリングで他の $\mathbb{Z}[1/N]$-双対となる．

この定理のカスプ形式に関する方はよく知られている（例えば Ribet [Ri2, (2.2)]）けれども，後半は自明ではない．（なお，$M_2(\Gamma_1(N);\mathbb{Z}[1/N])$ と $H(\Gamma_1(N);\mathbb{Z}[1/N])$ については不成立．）次の（本質的に）Mazur による補題の系 2.5 を用いて証明される：

補題 2.4 (cf. [M, Chapter II, Lemma (5.9)]). $f \in M_2(\Gamma_1(N);R)$ の q-展開が，ある $\xi(q) \in R[[q]]$ について $\xi(q^N)$ の形であれば，[Kat1] の意味のレヴェル 1 ，重さ 2 のモジュラー形式（§3.1 参照）で q-展開が $\xi(q)$ であるものが存在する．

系 2.5. k は標数 $p \neq N$ の体とする．$M_2^\infty(\Gamma_1(N);k)$ の元で q-展開が q^N のべき級数となるものは 0 のみである．

上より弱い「q-展開が定数（$\in k$）であるものは 0 のみである」から定理 2.3 が出る．定理 2.3 の系として次も得られる：

系 2.6. 自然な準同型

$$H^\infty(\Gamma_1(N);\mathbb{Z}[1/N]) \otimes_{\mathbb{Z}[1/N]} R \to H^\infty(\Gamma_1(N);R)$$

は同型であり，上と同様に定義したペアリング

$$M_2^\infty(\Gamma_1(N);R) \times H^\infty(\Gamma_1(N);R) \to R$$

も完全；カスプ形式についても同様.

更に系 2.5 から次も得られる：

系 2.7. $H^\infty(\Gamma_1(N);R)$ は $T(N)$ なしで，即ち全ての $T(n)$ $(N \nmid n)$, または $T(l)$ (l は N と異なる素数) とダイアモンド作用素のみで R 上生成される．

なお，$\mathbb{Z}$ 上の Hecke 環

$$\begin{cases} H^\infty(\Gamma_1(N);\mathbb{Z}) \subseteq \mathrm{End}(M_2^\infty(\Gamma_1(N);\mathbb{Z}[1/N])) \subseteq \mathrm{End}(M_2^\infty(\Gamma_1(N);\mathbb{C})), \\ h(\Gamma_1(N);\mathbb{Z}) \subseteq \mathrm{End}(S_2(\Gamma_1(N);\mathbb{Z}[1/N])) \subseteq \mathrm{End}(S_2(\Gamma_1(N);\mathbb{C})) \end{cases} \tag{2.12}$$

を，全ての $\langle d\rangle$ と $T(n)$ で $\mathbb{Z}$ 上生成される環とし，$\mathbb{Z}[1/N]$-algebra とは限らない環についても

$$\begin{cases} H^\infty(\Gamma_1(N);R) := H^\infty(\Gamma_1(N);\mathbb{Z}) \otimes_{\mathbb{Z}} R, \\ h(\Gamma_1(N);R) := h(\Gamma_1(N);\mathbb{Z}) \otimes_{\mathbb{Z}} R \end{cases} \tag{2.13}$$

と定めておく事にする．本小節はじめに述べたように，ダイアモンド作用素と Hecke 作用素は $X_\mu(N)$ の代数的対応から定まったが $X_1(N)$ にも同様のものがあり，これらの（covariant な）作用から $J_1(N)$ の $\mathbb{Q}$ 上の自己同型 $\langle d\rangle$ と自己準同型 $T(l)$ が定まる．全ての $\langle d\rangle$ と $T(l)$ で生成される $\mathrm{End}(J_1(N))$ の部分環は自然に（即ち $J_1(N)_{/\mathbb{C}}$ の 0 での余接空間は標準的に $S_2(\Gamma_1(N))$ と同型だからここでの表現により）$h(\Gamma_1(N);\mathbb{Z})$ と同型となるので以下これらの環を同一視して

$$h(\Gamma_1(N);\mathbb{Z}) \subseteq \mathrm{End}(J_1(N)) \tag{2.14}$$

とみなす.

§2.3. Eisenstein イデアル

定義 2.8. 任意の環 R に対して $H^\infty(\Gamma_1(N);R)$, $h(\Gamma_1(N);R)$ の Eisenstein イデアル $\mathcal{I}_{\infty,R}$, $I_{\infty,R}$ をそれぞれ $\eta(l):=T(l)-(1+l\langle l\rangle)$ （l は N と異なる素数），$T(N)-1$ 及び $\tau:=\sum_d\langle d\rangle$ （d は $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm1\}$ を動く）で生成されるイデアルと定める.

自然な全射準同型 $H^\infty(\Gamma_1(N);R)\twoheadrightarrow h(\Gamma_1(N);R)$ が作用素の制限によって得られるが，明らかに $I_{\infty,R}$ はこれによる $\mathcal{I}_{\infty,R}$ の像である．一般に K が標数 0 の体の時 $H^\infty(\Gamma_1(N);K)$-加群としてのただ一つの直和分解

$$M_2^\infty(\Gamma_1(N);K)=S_2(\Gamma_1(N);K)\oplus \mathrm{Eis}_2^\infty(K) \tag{2.15}$$

がある.（K が 1 の原始 $(N-1)/2$ 乗根を含んでいれば $\mathrm{Eis}_2^\infty(K)=\sum_\chi K\cdot E_{2,\chi}$；$E_{2,\chi}$ は (2.8) の Eisenstein 級数，である.）Eisenstein イデアルという用語は次により正当化される（と思われる）:

補題 2.9. R が標数 0 の体 K を商体に持つ整域の時 $\mathcal{I}_{\infty,R}\subseteq H^\infty(\Gamma_1(N);R)$ は $\mathrm{Eis}_2^\infty(K)$ の零化イデアルである.

また，系 2.7 より次もわかる：

補題 2.10. R が $\mathbb{Z}[1/N]$-algebra の時 $\mathcal{I}_{\infty,R}$ は，従って $I_{\infty,R}$ も，$T(N)-1$ なしで，即ち $\eta(l)$ と τ のみで，生成される.

次の定理は主定理 I を証明する上で最も重要なステップである.

定理 2.11. p が奇素数の時

$$|\,h(\Gamma_1(N);\mathbb{Z}_p):I_{\infty,\mathbb{Z}_p}\,|=|\,\mathbb{Z}_p:c_1(N)\mathbb{Z}_p\,|$$

即ち Eisenstein イデアル $I_{\infty,\mathbb{Z}}$ の $h(\Gamma_1(N);\mathbb{Z})$ での指数は 2 べきを除いて (1.5) の $c_1(N)$ に等しい.

本小節の残りではこの定理の証明を概説する.

$p=N$ の場合は後にまわす事にして，当面 $p\neq 2,N$ と仮定する．一般に R を整域，K をその商体とする．平坦な R-加群の完全系列とその K 上の splitting:

$$\begin{cases} 0\to A\xrightarrow{i}B\xrightarrow{\pi}C\to 0 \ \text{(exact)},\\ 0\leftarrow A\otimes_R K\xleftarrow{t}B\otimes_R K\xleftarrow{s}C\otimes_R K\leftarrow 0 \ \text{(exact)}\end{cases} \tag{2.16}$$

（即ち，添字 “$_K$” で K への係数拡大を表せば $t\circ i_K$ と $\pi_K\circ s$ は恒等写像）が与えられたとする．この時自然な同型写像のなす可換図式

$$\begin{array}{ccc} B/(i(A)+B\cap s(C)) & \xrightarrow[\sim]{\pi} & C/\pi(B\cap s(C)) \\ {\scriptstyle t}\downarrow\wr & & \wr\downarrow \\ t(B)/A & \xrightarrow[\sim]{} & (t(B)\oplus C)/B \end{array} \tag{2.17}$$

がある．これらの加群を同一視して (2.16) に付随する合同加群と呼ぶ．この概念は肥田 [Hi] 等によるもの（を僅かに手直ししたもの；[Oh1, 1.1]）である．ここで更に A, B, C がランク有限の自由 R-加群の場合を考える． “$^\vee$” で R- または K-双対を表す事にすると (2.16) から次の完全系列と K 上での splitting が得られる：

$$\begin{cases} 0\to C^\vee \xrightarrow{\pi^\vee} B^\vee \xrightarrow{i^\vee} A^\vee\to 0 \ \text{(exact)}, \\ 0\leftarrow C^\vee\otimes_R K \xleftarrow{s^\vee} B^\vee\otimes_R K \xleftarrow{t^\vee} A^\vee\otimes_R K\leftarrow 0 \ \text{(exact)}. \end{cases} \tag{2.18}$$

次は容易にわかる：

補題 2.12. 以上の仮定と記号の下で，R が単項イデアル整域の時，(2.16) と (2.18) に付随する合同加群は同型．

定義 2.1 で述べた $C_{\infty/\mathbb{Q}}=:C_\infty$ は $(N-1)/2$ 個の $\mathrm{Spec}(\mathbb{Q})$ の直和と同型で，ダイアモンド作用素により $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm1\}$ はこれらの直和因子の上に simply transitive に作用する．$\mathbb{Z}_p[C_\infty]^0$ でこの集合上の自由 $\mathbb{Z}_p$-加群の次数 0 の部分を表す．写像

$$\mathbf{Res}: M_2^\infty(\Gamma_1(N);\mathbb{Z}_p)\to\mathbb{Z}_p[C_\infty]^0;\ \ f\mapsto\sum_d a(0;f\mid\langle d\rangle)\cdot(\langle d\rangle\infty) \tag{2.19}$$

が得られ，次が完全である事がわかる：

$$0\to S_2(\Gamma_1(N);\mathbb{Z}_p)\to M_2^\infty(\Gamma_1(N);\mathbb{Z}_p)\xrightarrow{\mathbf{Res}}\mathbb{Z}_p[C_\infty]^0\to 0. \tag{2.20}$$

これに $\mathbb{Q}_p$ をテンソルすると (2.15) から（$\mathbb{Q}_p[C_\infty]^0$ には $M_2^\infty(\Gamma_1(N);\mathbb{Q}_p)$ の商加群の構造を入れれば）$H^\infty(\Gamma_1(N);\mathbb{Q}_p)$-加群としてただ一通りに split する．これを上の (2.16) のものとする．すると (2.18) のはじめの完全系列は系 2.6 より

$$0\to\mathbb{Z}_p[C_\infty]^{0\vee}\to H^\infty(\Gamma_1(N);\mathbb{Z}_p)\to h(\Gamma_1(N);\mathbb{Z}_p)\to 0 \ \text{(exact)} \tag{2.21}$$

となり，3 番目の写像は自然な準同型である．ここで，(2.18) の記号を使えば，$H^\infty(\Gamma_1(N);\mathbb{Z}_p)\cap t^\vee(h(\Gamma_1(N);\mathbb{Z}_p))$ が丁度 $\mathcal{I}_{\infty,\mathbb{Z}_p}$ となり，(2.21) に付随する合同加群が $h(\Gamma_1(N);\mathbb{Z}_p)/I_{\infty,\mathbb{Z}_p}$ である事がわかる．よって補題 2.12 により問題の指数は（ずっと易しい）(2.20) の合同加群の計算に帰着する．

最も簡単な $N=5$ の場合にどうなるか見てみよう.(一般の場合は計算が煩雑になるだけである.) $M_2^\infty(\Gamma_1(5);\mathbb{Z}_p)$ の Eisenstein 級数は $\chi_0=\left(\frac{\ }{5}\right)$ (Legendre 記号) についての E_{2,χ_0} のみであり, $\mathbb{Z}_p[C_\infty]^0$ は $\infty-\langle 2\rangle\infty$ で生成されるランク 1 の自由 $\mathbb{Z}_p$-加群である.(本当は $S_2(\Gamma_1(5);\mathbb{Z}_p)=\{0\}$ だから合同加群は消え, 実際 $c_1(5)=5(B_{2,\chi_0}/4)=1$ なのだがこれには目をつぶって頂く事にして) ∞ の係数への射影により $\mathbb{Z}_p[C_\infty]^0\xrightarrow{\sim}\mathbb{Z}_p$ となり, **Res** は $f\mapsto a(0;f)$ と同一視できる. また "$B\cap s(C)$" $=M_2^\infty(\Gamma_1(5);\mathbb{Z}_p)\cap\mathbb{Q}_p\cdot E_{2,\chi_0}$ で, E_{2,χ_0} の q^5 の係数は 1 だからこれは $\mathbb{Z}_p\cdot E_{2,\chi_0}$ に等しい. 従って "$C/\pi(B\cap s(C))$" $\cong\mathbb{Z}_p/a(0;E_{2,\chi_0})\mathbb{Z}_p=\mathbb{Z}_p/(B_{2,\chi_0}/4)\mathbb{Z}_p=\mathbb{Z}_p/c_1(5)\mathbb{Z}_p$ となる.

次に $p=N$ の時を考える. ここでも次の §2.4 でもこの場合は別に扱う必要があるのだが, Ribet [Ri1] 以来 Wiles [W] や Mazur-Wiles [MW1] 等によって, 円分体の整数論に関連して, 寧ろ詳しく調べられている場合でもあり, 知られた結果を援用できる.

$(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm1\}$ の指標は, 値を N-進体にとるものと考えると, Teichmüller 指標 ω の偶数乗全体である. $d\mapsto\langle d\rangle$ により $h(\Gamma_1(N);\mathbb{Z}_N)$ には $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm1\}$ が作用するので通常のように

$$h(\Gamma_1(N);\mathbb{Z}_N)=\bigoplus_{\substack{i\,(\mathrm{mod}\,N-1)\\ i:\mathrm{even}}} h(\Gamma_1(N);\mathbb{Z}_N)^{(i)} \tag{2.22}$$

但し "(i)" は ω^i-固有空間, と環の直和に分解される. これに応じて Eisenstein イデアルも

$$I_{\infty,\mathbb{Z}_N}=\bigoplus_{\substack{i\,(\mathrm{mod}\,N-1)\\ i:\mathrm{even}}} I^{(i)}_{\infty,\mathbb{Z}_N} \tag{2.23}$$

と分解される. $\tau=\sum_d\langle d\rangle$ の $h(\Gamma_1(N);\mathbb{Z}_N)^{(i)}$ への像は $i\equiv 0\ (\mathrm{mod}\ N-1)$ なら $(N-1)/2\in\mathbb{Z}_N^\times$ であり, それ以外は 0 となる.(従って $i\not\equiv 0\ (\mathrm{mod}\ N-1)$ なら $I^{(i)}_{\infty,\mathbb{Z}_N}$ は $\eta(l)$ と $T(N)-1$ で生成される見慣れた Eisenstein イデアルである.) これよりまず, $h(\Gamma_1(N);\mathbb{Z}_N)^{(0)}/I^{(0)}_{\infty,\mathbb{Z}_N}=\{0\}$ となる. ところで $c_1(N)=N(B_{2,\omega^{-2}}/4)\times$ (残りの $B_{2,\omega^i}/4$ の積) であるが, よく知られているように $N(B_{2,\omega^{-2}}/4)\in\mathbb{Z}_N{}^\times$ で他の $B_{2,\omega^i}/4$ は $\mathbb{Z}_N$ に属する. よってこの場合の定理 2.11 は $i\not\equiv 0\ (\mathrm{mod}\ N-1)$ の時の

$$h(\Gamma_1(N);\mathbb{Z}_N)^{(i)}/I^{(i)}_{\infty,\mathbb{Z}_N}\cong\begin{cases}\{0\},\ i\equiv -2\ (\mathrm{mod}\ N-1)\text{ の時},\\ \mathbb{Z}_N/B_{2,\omega^i}\mathbb{Z}_N,\ \text{その他}\end{cases} \tag{2.24}$$

から出る. この事の証明は「手抜き」ができて, 実際 (Λ-adic な場合を扱った) [Oh1, (1.5.5) (cf. (3.2.4) の後の注意)] を特殊化する事により示される.

§2.4. Rational torsion

以下でも p は奇素数とする. $J_1(N)$ には $h(\Gamma_1(N);\mathbb{Z})$ が作用したから (2.14), $J_1(N)(\mathbb{Q})[p^\infty]$ には $h(\Gamma_1(N);\mathbb{Z}_p)$ が作用する.

定理 2.13. Eisenstein イデアル $I_{\infty,\mathbb{Z}_p}$ は $J_1(N)(\mathbb{Q})[p^\infty]$ を零化する．

これは以下のようにして証明される．Eisenstein イデアルは $\eta(l), T(N)-1$ と τ で生成されていた（定義 2.8）．

• $\eta(l) = T(l) - (1 + l\langle l\rangle)$ が $J_1(N)(\mathbb{Q})[p^\infty]$ を零化する事は寧ろよく知られている：$J_1(N)_{/\mathbb{Z}_l}$ で $J_1(N)$ の $\mathbb{Z}_l$ 上の Néron モデルを，$J_1(N)_{/\mathbb{F}_l}$ でその閉ファイバーを表せば，後者は $l \nmid N$ だから Abel 多様体で，その上で Eichler-志村の合同関係式

$$T(l) = \mathrm{Frob}_l + \langle l\rangle \mathrm{Ver}_l$$

（Frob_l は Frobenius, Ver_l は Verschiebung）が成り立つ．$p = l$ の時は（$p \neq 2$ だから）Raynaud [Ra, Théorème 3.3.3]（または Katz [Kat3, Appendix]）を用いれば，$J_1(N)(\mathbb{Q})[p^\infty]$ の $J_1(N)_{/\mathbb{Z}_l}$ でのスキーム的閉包は常に定数群スキームとなるので上から結論が従う．

• $T(N)-1$ については，$p \neq N$ の時は補題 2.10 により $I_{\infty,\mathbb{Z}_p}$ は $T(N)-1$ なしで生成されたから「手抜き」ができる．

$p = N$ の時は次のようにする．$A := J_1(N)/(J_0(N)$ の像$)$ とおく．$X_1(N) \to X_0(N)$ の次数が（N と素な）$(N-1)/2$ である事より

$$J_1(N)(\mathbb{Q})[N^\infty] \cong J_0(N)(\mathbb{Q})[N^\infty] \times A(\mathbb{Q})[N^\infty]$$

となり，Mazur（定理 1.1）により $J_0(N)(\mathbb{Q})[N^\infty] = \{0\}$ であるから，問題は $A(\mathbb{Q})[N^\infty]$ の方に帰着する．A は $\mathbb{Q}(e^{2\pi i/N} + e^{-2\pi i/N})$ 上では N を割る（ただ一つの）素点で good reduction を持つので，Eichler-志村の合同関係式のかわりに Mazur-Wiles の $T(N)$ の合同関係式 [MW1, Chapter 3, §3, Proposition 2] 及び [MW2, §3] を使って証明される．

• τ については 2-torsion も含めて $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$ を零化する事が，次のように二つの深い結果を用いて示される．$\alpha : J_1(N) \to J_0(N)$ を自然な (Albanese) 射とすると τ は α を通って factor する事がわかるので，$\alpha(J_1(N)(\mathbb{Q})_{\mathrm{tors}}) = \{0\}$ を言えばよい．“$_{/\mathbb{Z}}$” で $\mathbb{Z}$ 上の Néron モデルを表せば，まず [CES] の主定理（またはタイトルそのもの (!)）により $J_1(N)_{/\mathbb{Z}}$ のファイバーは（N でも）連結：

$$J_1(N)_{/\mathbb{Z}} = J_1(N)^0_{/\mathbb{Z}}.$$

従って α は

$$J_1(N)(\mathbb{Q}) = J_1(N)^0_{/\mathbb{Z}}(\mathbb{Z}) \to J_0(N)^0_{/\mathbb{Z}}(\mathbb{Z})$$

を引き起こすが，Mazur は定理 1.1 の証明の中で $J_0(N)^0_{/\mathbb{Z}}(\mathbb{Z})_{\mathrm{tors}} = \{0\}$ を示している．□

主定理 I を証明するためにはもう一つステップが要る．“$\hat{}$” で Pontrjagin 双対を表す事にする．

命題 2.14. (1) $p \neq N$ の時，$J_1(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty][I_{\infty,\mathbb{Z}_p}]\widehat{\ }$ は $h(\Gamma_1(N);\mathbb{Z}_p)$-加群として巡回的．

(2) $i \not\equiv 0 \pmod{N-1}$ の時 $A_{/\mathbb{F}_N}(\overline{\mathbb{F}}_N)[N^\infty]^{(i)}[I^{(i)}_{\infty,\mathbb{Z}_N}]$ は巡回群．ここで $A_{/\mathbb{F}_N}$ は A の $\mathbb{Z}[e^{2\pi i/N}+e^{-2\pi i/N}]$ 上 の Néron モデルの標数 N の閉ファイバーとした．

(1) の証明には [M, Chapter II, §14], [MW1, Chapter 5, §2] の議論を使う．$J_1(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty] =: \Gamma$ とおく．$h(\Gamma_1(N);\mathbb{Z}_p) = \oplus_{\mathfrak{P}} h(\Gamma_1(N);\mathbb{Z}_p)_{\mathfrak{P}}$ と有限個の極大イデアルでの局所化の直和に分解し，Γ もそれに応じて $\oplus_{\mathfrak{P}}\Gamma_{\mathfrak{P}}$ と分解する．Cartier-Serre の同型 [Se1, Proposition 10] を使うと $\Gamma[\mathfrak{P}]$ の $h(\Gamma_1(N);\mathbb{Z}_p)/\mathfrak{P}$ 上の次元は高々 1 である事がわかる．これより $\Gamma_{\mathfrak{P}}[\mathfrak{P}]\widehat{\ } = \Gamma_{\mathfrak{P}}\widehat{\ }/\mathfrak{P}\Gamma_{\mathfrak{P}}\widehat{\ }$，従って中山の補題により $\Gamma_{\mathfrak{P}}\widehat{\ }$ も $h(\Gamma_1(N);\mathbb{Z}_p)_{\mathfrak{P}}$ 上巡回的となり，これから (1) が従う． (2) は [MW1, Chapter 3, §3, Proposition 4′] から直接出る．

以上の事をあわせると主定理 I が次のように導かれる：まず $p \neq 2, N$ とする．定理 2.13 及び Raynaud または Katz の結果から mod p の還元により単射

$$J_1(N)(\mathbb{Q})[p^\infty] \hookrightarrow J_1(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty][I_{\infty,\mathbb{Z}_p}]$$

が得られる．命題 2.14, (1) から

$$| J_1(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty][I_{\infty,\mathbb{Z}_p}] | \leq | h(\Gamma_1(N);\mathbb{Z}_p) : I_{\infty,\mathbb{Z}_p} |$$

となり，故に定理 2.11 から

$$| J_1(N)(\mathbb{Q})[p^\infty] | \leq | \mathbb{Z}_p : c_1(N)\mathbb{Z}_p | = | \mathcal{C}_1(N)[p^\infty] |$$

が得られる．はじめから $J_1(N)(\mathbb{Q})[p^\infty] \supseteq \mathcal{C}_1(N)[p^\infty]$ は自明だから結論が従う．

$p = N$ の時は $\mathcal{C}_1(N)[N^\infty]^{(i)} \cong \mathbb{Z}_N/B_{2,\omega^i}\mathbb{Z}_N$（但し $i \not\equiv 0, -2 \pmod{N-1}$）である事 [KL, Chapter 6, Theorem 2.1] 及び (2.24) を用いて上と同様の議論をすれば

$$J_1(N)(\mathbb{Q})[N^\infty]^{(i)} = \mathcal{C}_1(N)[N^\infty]^{(i)} \cong \begin{cases} \{0\}, & i \equiv 0, -2 \pmod{N-1} \text{ の時,} \\ \mathbb{Z}_N/B_{2,\omega^i}\mathbb{Z}_N, & \text{その他} \end{cases}$$

が得られる． □

§3. $J_0(N)$ (N: square-free）の場合

§3.1. モジュラー形式

§2.1 はじめと同様 $M_k(\Gamma_0(N))$, $S_k(\Gamma_0(N))$ で，$\Gamma_0(N)$ に関する重さ k のモジュラー形式，カスプ形式の空間を表す．

($\mathbb{Z}$-) スキーム S 上の楕円曲線 E とその $\Gamma_0(N)$-構造 C_N，即ち C_N は $E[N]$ のランク N の有限平坦かつ（[KM, (1.4)] の意味で）巡回的な S-部分群スキーム，の組 (E, C_N)

の coarse モジュライスキーム $Y_0(N)_{/\mathbb{Z}}$ が存在する．$X_0(N)_{/\mathbb{Z}}$ をその自然なコンパクト化とし，環 R に対して

$$\begin{cases} Y_0(N)_{/R} := Y_0(N)_{/\mathbb{Z}} \otimes_{\mathbb{Z}} R, \\ X_0(N)_{/R} := X_0(N)_{/\mathbb{Z}} \otimes_{\mathbb{Z}} R \end{cases} \tag{3.1}$$

とおく．$Y_0(N)_{/\mathbb{Q}}$, $X_0(N)_{/\mathbb{Q}}$ が以前の $Y_0(N)$, $X_0(N)$ である．$X_0(N)_{/\mathbb{Z}[1/N]}$ は $\mathbb{Z}[1/N]$ 上スムースであるが，$p \parallel N$ （即ち $p \mid N$, $p^2 \nmid N$）の時 $X_0(N)_{/\mathbb{F}_p}$ は [DR, Chapter VI, §6] により次のように記述される：

命題 3.1. $X_0(N)_{/\mathbb{F}_p}$ は $X_0(N/p)_{/\mathbb{F}_p}$ と標準的に同型な二つの既約成分を持ち，それらは互いに $\mathbb{F}_p$-共役な supersingular（な楕円曲線に対応する）点でのみ transversal に交わる．

$Y_0(N)_{/\mathbb{Z}}$ が coarse モジュライスキームでしかないため，かつレヴェルを割る素数での「手抜き」ができないため，モジュラー形式の扱いは §2.1 より煩雑になる．以下で考えるのは次のものである：

$$\begin{cases} S_k^{\mathrm{A}}(\Gamma_0(N); R) \subseteq M_k^{\mathrm{A}}(\Gamma_0(N); R), \\ S_k^{\mathrm{B}}(\Gamma_0(N); R) \subseteq M_k^{\mathrm{B}}(\Gamma_0(N); R), \\ S_2^{\mathrm{reg}}(\Gamma_0(N); R) \subseteq M_2^{\mathrm{reg}}(\Gamma_0(N); R) \end{cases} \tag{3.2}$$

（“A” と “B” は，[M, Chapter II, § 4] の記号では $M_2^{\mathrm{A}}(\Gamma_0(N); R)$ が $\mathrm{A}(R)$，$M_2^{\mathrm{B}}(\Gamma_0(N); R)$ が $\mathrm{B}(R)$ となっている事による）．

まず $S_k^{\mathrm{A}}(\Gamma_0(N); R)$ と $M_k^{\mathrm{A}}(\Gamma_0(N); R)$ であるが，小論ではこれらは $\mathbb{Z}[1/N]$-algebra R についてのみ考える．（この時下の C_N はエタール群スキームであり，「巡回的」の意味も明らかなもの．）各々 [Kat1, 1.1, 1.2], [Kat2, 2.1] のように代数的に定義されるものである：$f \in S_k^{\mathrm{A}}(\Gamma_0(N); R)$（resp. $M_k^{\mathrm{A}}(\Gamma_0(N); R)$）とは，$R$-スキーム S 上の楕円曲線 $p : E \to S$ とその $\Gamma_0(N)$-構造 C_N の各組に対して $f(E, C_N) \in H^0(S, \underline{\omega}_{E/S}^{\otimes k})$（$\underline{\omega}_{E/S} := p_* \Omega^1_{E/S}$）を対応させる規則で，$R$-スキームの cartesian square と可換で，各カスプで消える（resp. 正則な）ものである．(詳細は上記 Katz の論文を参照されたい．)（カスプ ∞ での）q-展開写像

$$\begin{cases} S_k^{\mathrm{A}}(\Gamma_0(N); R) \to qR[[q]], \\ M_k^{\mathrm{A}}(\Gamma_0(N); R) \to R[[q]] \end{cases} \tag{3.3}$$

があり，§2.1 と同じ q-expansion principle が成立する．これらの空間の formation は平坦な底変換と可換である（が一般には可換でない）．

次に $S_k^{\mathrm{B}}(\Gamma_0(N); R)$ と $M_k^{\mathrm{B}}(\Gamma_0(N); R)$ であるが，これらは寧ろ古典的なモジュラー形式に近い， Serre, Swinnerton-Dyer 式のものである．まず，q-展開について (2.5) の記

号の下で

$$\begin{cases} S_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) := \{f \in S_k(\Gamma_0(N)) \mid a(n;f) \in \mathbb{Z}, \forall n \geq 1\}, \\ M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) := \{f \in M_k(\Gamma_0(N)) \mid a(n;f) \in \mathbb{Z}, \forall n \geq 0\} \end{cases} \tag{3.4}$$

とし，任意の環に対して

$$\begin{cases} S_k^{\mathrm{B}}(\Gamma_0(N);R) := S_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) \otimes_{\mathbb{Z}} R, \\ M_k^{\mathrm{B}}(\Gamma_0(N);R) := M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}) \otimes_{\mathbb{Z}} R \end{cases} \tag{3.5}$$

とおく．これらについて (3.3) と同じ形の q-展開写像が定義から存在し，q-expansion principle が成り立つ事は容易で，また任意の底変換との可換性も自明に成り立つ．

$M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{C})$, $M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{C})$ は自然に（q-展開を保って）$M_k(\Gamma_0(N))$ と同型であり，以下これらを同一視する．すると q-expansion principle より $M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{Z}[1/N]) = M_k^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z}[1/N])$ となり，従って

$$R \text{ が } \mathbb{Z}[1/N] \text{ 上平坦なら } M_k^{\mathrm{A}}(\Gamma_0(N);R) = M_k^{\mathrm{B}}(\Gamma_0(N);R) \tag{3.6}$$

であり，一般には q-展開を保つ（事から）単射（となる）

$$M_k^{\mathrm{B}}(\Gamma_0(N);R) \hookrightarrow M_k^{\mathrm{A}}(\Gamma_0(N);R) \tag{3.7}$$

が任意の $\mathbb{Z}[1/N]$-algebra R に対して存在する．カスプ形式についても同様．

d が N の正の約数で $(d, N/d) = 1$ の時

$$W_d := \begin{bmatrix} dx & y \\ Nz & dw \end{bmatrix} \quad (x,y,z,w \in \mathbb{Z},\ \det W_d = d) \tag{3.8}$$

は $\Gamma_0(N)$ を正規化し，$X_0(N)_{/\mathbb{C}}$ の，d のみに依存する（Atkin-Lehner）involution を引き起こす [AL, §2]．これは次のように代数的に記述される：(E, C_N) が（N が可逆とは仮定しない一般の）S 上の楕円曲線と $\Gamma_0(N)$-構造の組の時

$$w_d(E, C_N) := (E/C_N[d], E[d]/C_N[d] \times_S C_N/C_N[d]) \tag{3.9}$$

も同様の組で，対応 $(E, C_N) \mapsto w_d(E, C_N)$ は coarse モジュライスキーム $Y_0(N)_{/\mathbb{Z}}$ とコンパクト化 $X_0(N)_{/\mathbb{Z}}$ の involution w_d を引き起こす．これから底変換で得られる $Y_0(N)_{/R}$ と $X_0(N)_{/R}$ の involution も w_d で表せば，$\mathbb{C}$ 上ではこれが上で述べたものになっている．$N = l_1^{e_1} \cdots l_m^{e_m}$ を素因数分解とすると

$$G_{\mathrm{AL}} := \{w_d \mid 0 < d \mid N,\ (d, N/d) = 1\} \subseteq \mathrm{Aut}(X_0(N)_{/\mathbb{Z}}) \tag{3.10}$$

は $w_{l_i^{e_i}}$ たちで生成される位数 2^m の $(2, \ldots, 2)$ 型初等的 Abel 群である．

以下 k は正の偶数とする．R が $\mathbb{Z}[1/N]$-algebra の時 $f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ に対して

$$(f\,|_k\, w_d)(E, C_N) := d^{-k/2}\pi^* f(w_d(E, C_N)), \text{ 但し } \pi : E \to E/C_N[d] \text{ は商射} \tag{3.11}$$

で $f\,|_k\, w_d \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ を定める事ができる．この作用 "$|_k\, w_d$" は involution であり，$M_k(\Gamma_0(N))$ では (2.1) の意味での "$|_k\, W_d$" に等しい．特に $M_k^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z}[1/N])$ はこの（Atkin-Lehner）involution で stable になっている．Mazur の扱った N が素数の場合には更に w_N は $M_2^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z})$ も保ったのだが一般の場合には（oldform があるため）この事は成立しない．そこで次のものを考える事にする．

以下 N は **square-free** も仮定する．この時任意の環 R について $X_0(N)_{/R} \to \mathrm{Spec}(R)$ は完全交叉で，$X_0(N)_{/R}$ 上の，次のように記述される，正則微分のなす可逆層 $\Omega_{/R}$ が存在する [DR, Chapter I, § 2], [M, Chapter II, § 3], Mazur-Ribet [MR, § 7]:

(i) $\Omega_{/R}$ の formation は任意の底変換と可換．

(ii) $X_0(N)_{/R} \to \mathrm{Spec}(R)$ の smooth locus に $\Omega_{/R}$ を制限したものは Kähler 微分の層．($\Omega_{/R}$ は (i), (ii) から一意に定まる可逆層である．)

(iii) $p \mid N$，k が標数 p の体の時 $\pi : \widetilde{X_0(N)}_{/k} \to X_0(N)_{/k}$ を正規化とする．(命題 3.1 により $\widetilde{X_0(N)}_{/k}$ は二つの曲線の直和．) $X_0(N)_{/k}$ の開集合 U 上での $\Omega_{/k}$ の切断は，$\pi^{-1}(U)$ 上の微分 ω で U の singular locus の逆像でのみ高々一位の極を持ち，かつ $P \in U(\overline{k})$ が特異点で $\pi^{-1}(P) = \{P_1, P_2\}$ ならば $\mathrm{Res}_{P_1}\omega + \mathrm{Res}_{P_2}\omega = 0$，をみたすもの全体．

定義 3.2. 任意の環 R に対して

$$\begin{cases} S_2^{\mathrm{reg}}(\Gamma_0(N); R) := H^0(X_0(N)_{/R}, \Omega_{/R}), \\ M_2^{\mathrm{reg}}(\Gamma_0(N); R) := H^0(X_0(N)_{/R}, \Omega_{/R}(C_{/R})) \end{cases}$$

と定義する．但し $C_{/R} := X_0(N)_{/R} - Y_0(N)_{/R}$.

これらは R 上のランク有限の自由加群であり，その formation は任意の底変換と可換である事がわかる．また，カスプ ∞ に対応して射 $\mathrm{Spec}(R((q))) \to X_0(N)_{/R}$ があるが，これによる $\omega \in M_2^{\mathrm{reg}}(\Gamma_0(N); R)$ の引き戻しは $f_\omega(q)(dq/q)$ の形であり，対応 $\omega \mapsto f_\omega(q)$ により（単射とは限らない）q-展開写像

$$\begin{cases} S_2^{\mathrm{reg}}(\Gamma_0(N); R) \to qR[[q]], \\ M_2^{\mathrm{reg}}(\Gamma_0(N); R) \to R[[q]] \end{cases} \tag{3.12}$$

が定義できる．上の性質 (ii) より $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Q}) = H^0(X_0(N)_{/\mathbb{Q}}, \Omega^1_{X_0(N)_{/\mathbb{Q}}/\mathbb{Q}}(C_{/\mathbb{Q}})) \cong M_2^{\mathrm{B}}(\Gamma_0(N); \mathbb{Q})$ 等であるから q-展開を保つ写像

$$\begin{cases} S_2^{\mathrm{reg}}(\Gamma_0(N); R) \to S_2^{\mathrm{B}}(\Gamma_0(N); R), \\ M_2^{\mathrm{reg}}(\Gamma_0(N); R) \to M_2^{\mathrm{B}}(\Gamma_0(N); R) \end{cases} \tag{3.13}$$

がまず $R=\mathbb{Z}$ の場合に，従って底変換により任意の R に対して定まる．R が $\mathbb{Z}$ 上平坦ならばこれらは単射である．

$X_0(N)_{/R}$ には自己同型 w_d があったが，$\omega\in M_2^{\mathrm{reg}}(\Gamma_0(N);R)$ に対して

$$\omega\,|_2\,w_d:=w_d^*(\omega) \tag{3.14}$$

と定めると，この作用は (3.13) で右辺の “$|_2\,w_d$” と両立する．[M, Chapter II, § 4], [G, Proposition 8.4] と同様の議論で次がわかる：

命題 3.3. $M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z})\hookrightarrow M_2^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z})$ の像は

$$\{f\in M_2^{\mathrm{B}}(\Gamma_0(N);\mathbb{Z})\mid \text{全ての } w_d\in G_{\mathrm{AL}} \text{ に対して } (f\,|_2\,w_d)(q)\in\mathbb{Z}[[q]]\}.$$

カスプ形式についても同様.

以下しばしば $M_2^{\mathrm{reg}}(\Gamma_0(N);R)$ の元を f で表し，その q-展開も $f(q)$ で表す．

次に $M_2(\Gamma_0(N))$ の Eisenstein 級数について述べておく．$N=l_1\cdots l_m$ を素因数分解とし，$N>1$ とする．

$$\boldsymbol{E}:=\{\pm1\}^m \tag{3.15}$$

とおく．一般に M が $\mathbb{Z}[1/2][G_{\mathrm{AL}}]$-加群の時，$\boldsymbol{\varepsilon}=(\varepsilon_1,\cdots,\varepsilon_m)\in\boldsymbol{E}$ に対して

$$M^{\boldsymbol{\varepsilon}}:=\{m\in M\mid w_{i_i}m=\varepsilon_i m\ \ (i=1,\cdots,m)\} \tag{3.16}$$

とおけば

$$M=\oplus_{\boldsymbol{\varepsilon}\in\boldsymbol{E}}M^{\boldsymbol{\varepsilon}} \tag{3.17}$$

と直和分解される．以下では符号

$$\begin{cases}\boldsymbol{\varepsilon}_+:=(+1,\cdots,+1),\\ \boldsymbol{\varepsilon}_H:=\left(\left(\frac{l_1}{3}\right),\cdots,\left(\frac{l_m}{3}\right)\right),\ \ 3\nmid N \text{ の時},\\ \boldsymbol{\varepsilon}_H^{\pm}:=\left(\pm1,\left(\frac{l_2}{3}\right),\cdots,\left(\frac{l_m}{3}\right)\right),\quad 3\mid N \text{ で } l_1=3 \text{ の時}\end{cases} \tag{3.18}$$

が特別な扱いを要する．

Hecke [He, § 2] によればレヴェル 1，重さ 2 の非正則 Eisenstein 級数

$$K(z)=\frac{1}{8\pi y}-\frac{1}{24}+\sum_{n=1}^{\infty}\Big(\sum_{0<t|n}t\Big)e^{2\pi inz} \tag{3.19}$$

($z = x + yi \in H$) があった． $\boldsymbol{E} \ni \boldsymbol{\varepsilon} = (\varepsilon_1, \cdots, \varepsilon_m)$ に対して

$$E_{\boldsymbol{\varepsilon}} := K\,|_2 \prod_{i=1}^{m}(1 + \varepsilon_i w_{l_i}) \tag{3.20}$$

とおくと，$\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_+$ ならば上の非正則項は消え，次がわかる：

命題 3.4. $\boldsymbol{E} \ni \boldsymbol{\varepsilon} = (\varepsilon_1, \cdots, \varepsilon_m) \neq \boldsymbol{\varepsilon}_+$ の時，$E_{\boldsymbol{\varepsilon}} \in M_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}}$ であり，q-展開は

$$E_{\boldsymbol{\varepsilon}}(q) = \pm\frac{1}{24}\prod_{i=1}^{m}(l_i + \varepsilon_i) + \sum_{n=1}^{\infty} a_n q^n$$

ここで $a_n \in \mathbb{Z}$，$(n, N) = 1$ なら $a_n = \sum_{0<t|n} t$，の形である．これらの $2^m - 1$ 個の $E_{\boldsymbol{\varepsilon}}$ は $M_2(\Gamma_0(N))$ の Eisenstein 級数の空間の基底をなす．一般に $E_{\boldsymbol{\varepsilon}} \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}[1/6])^{\boldsymbol{\varepsilon}}$ であり，$\boldsymbol{\varepsilon} \neq \boldsymbol{\varepsilon}_H, \boldsymbol{\varepsilon}_H^{\pm}$ ならば $E_{\boldsymbol{\varepsilon}} \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z}[1/2])^{\boldsymbol{\varepsilon}}$ である．

高木の公式 (1.6) に現れた $c_0(N)$ は上の $E_{\boldsymbol{\varepsilon}}(q)$ の定数項の積に $(\pm 1)\times$ (2, 3 のべき) をかけたものである事に注意しよう．

なお，$\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H, \boldsymbol{\varepsilon}_H^{\pm}$ の時は $E_{\boldsymbol{\varepsilon}}(q)$ の定数項は 3-進整数ではなく，$3E_{\boldsymbol{\varepsilon}}$ に 3-進単数をかけたものは標数 3 の Hasse 不変量（の定めるレヴェル 1, 重さ 2 のモジュラー形式）の標数 0 への持ち上げになっている．

§3.2. Hecke 環

本小節でも k は正の偶数とし，$N = l_1 \cdots l_m > 1$ は square-free とする．R が $\mathbb{Z}[1/N]$-algebra の時 $M_k^{\mathrm{A}}(\Gamma_0(N); R)$ には，各素数 l について Hecke 作用素 $T(l)$ が定まる（[G, §3] では $M_k(\Gamma_1(N); R)$ の場合が扱われているが，それが $M_k^{\mathrm{A}}(\Gamma_0(N); R)$ の Hecke 作用素を引き起こす；なお $l \mid N$ の時はしばしば記号 $U(l)$ が用いられる）．$f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ の q-展開が $f(q) = \sum_{n=0}^{\infty} a_n q^n$ ならば

$$\begin{cases} (f\,|_k\, T(l))(q) = \sum_{n=0}^{\infty} a_{nl} q^n + l^{k-1} \sum_{n=0}^{\infty} a_n q^{nl}, & l \nmid N \text{ の時}, \\ (f\,|_k\, T(l))(q) = \sum_{n=0}^{\infty} a_{nl} q^n, & l \mid N \text{ の時} \end{cases} \tag{3.21}$$

であった．これらは $M_k^{\mathrm{A}}(\Gamma_0(N); \mathbb{Z}[1/N]) = M_k^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z}[1/N])$ (3.6) 上ではもちろん古典的な Hecke 作用素で，上から明らかに $M_k^{\mathrm{B}}(\Gamma_0(N); \mathbb{Z})$ を自身に写すから底変換で任意の R について $M_k^{\mathrm{B}}(\Gamma_0(N); R)$ に $T(l)$ が定まる．

一般に $M_k^{\mathrm{A}}(\Gamma_0(N); R)$ や $M_k^{\mathrm{B}}(\Gamma_0(N); R)$ 上 $l \nmid N$ の時の $T(l)$ と Atkin-Lehner involution w_d (3.11) は可換である．（古典的な場合はよく知られている事であり，“M_k^{A}”についても [G, §3], [Kat1, 1.11] の $T(l)$ の記述と (3.11) からわかる．）命題 3.3 から $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{Z})$ も $T(l)$（$l \nmid N$）で stable で，底変換により任意の $M_2^{\mathrm{reg}}(\Gamma_0(N); R)$ にも $T(l)$（$l \nmid N$）が定まる．（実際は $l \mid N$ でも定まる．）今迄の $T(l)$ は全てカスプ形式を自身に写す．

定義 3.5. 任意の環 R に対して Hecke 環

$$\begin{cases} \boldsymbol{T}(N;R) \subseteq \mathrm{End}(M_2^{\mathrm{reg}}(\Gamma_0(N);R)), \\ \mathbf{T}(N;R) \subseteq \mathrm{End}(S_2^{\mathrm{reg}}(\Gamma_0(N);R)) \end{cases}$$

をそれぞれ $T(l)$（$l \nmid N$）と w_{l_i}（$i = 1, \cdots, m$）で R 上生成される右辺の（可換）部分環と定める．

R が $\mathbb{Z}[1/N]$ 上平坦な場合は上の “M_2^{reg}” を “M_2^{A}” や “M_2^{B}” にしても同じである（カスプ形式でも同様）．なお，上の環は §2.2 で考えたタイプの Hecke 環，即ち全ての $T(l)$ で生成される環とは異なる．一般にはレヴェル N のモジュラー形式の空間が oldform を含んでいるため，後者の環は（newform だけでなく）モジュラー形式全体を統制するのに適していないように思われる．ちなみに N が素数の時 Mazur が [M, Chapter II, §6] で考えた Hecke 環は上の形のものであった．（もっともこの場合は §2.2 のタイプのものと同じなのであるが．）

定義から $\boldsymbol{T}(N;R)$ と $\mathbf{T}(N;R)$ は $R[G_{AL}]$-algebra であるから，R で 2 が可逆の場合は (3.17) のように

$$\begin{cases} \boldsymbol{T}(N;R) = \oplus_{\boldsymbol{\varepsilon} \in \boldsymbol{E}} \boldsymbol{T}(N;R)^{\boldsymbol{\varepsilon}}, \\ \mathbf{T}(N;R) = \oplus_{\boldsymbol{\varepsilon} \in \boldsymbol{E}} \mathbf{T}(N;R)^{\boldsymbol{\varepsilon}} \end{cases} \tag{3.22}$$

と環の直和に分解する．$\boldsymbol{T}(N;R)^{\boldsymbol{\varepsilon}}$（resp. $\mathbf{T}(N;R)^{\boldsymbol{\varepsilon}}$）は $T(l)$（$l \nmid N$）全体で R 上生成される $\mathrm{End}(M_2^{\mathrm{reg}}(\Gamma_0(N);R)^{\boldsymbol{\varepsilon}})$（resp. $\mathrm{End}(S_2^{\mathrm{reg}}(\Gamma_0(N);R)^{\boldsymbol{\varepsilon}})$）の部分環である．（但し，後者の空間が $\{0\}$ の時は前者の環も $\{0\}$．）

以下 $\mathbb{Z}_{(p)}$ で $\mathbb{Z}$ の (p) での局所化を表す．

定理 3.6. p は奇素数とする．ペアリング

$$\begin{cases} S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \times \mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \to \mathbb{Z}_{(p)}, \\ M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \times \boldsymbol{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \to \mathbb{Z}_{(p)} \end{cases}$$

を定理 2.3 と同じく $(f,t) = a(1; f|_2 t)$ で定義する．前者は常に完全であり，後者は $p = 3$ で $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H$ または $\boldsymbol{\varepsilon} = \boldsymbol{\varepsilon}_H^{\pm}$ (3.18) の場合を除いて完全である．

この定理の証明に必要な，かつ他でも用いられる，命題をいくつか述べる．まず基本的なのは（本質的に）Mazur による，補題 2.4 に類似の次の結果である（古典的な場合は [AL, Lemma 16] である）：

補題 3.7. R は $\mathbb{Z}[1/N]$-algebra とし，l は N を割る素数とする．$f \in M_k^{\mathrm{A}}(\Gamma_0(N);R)$ の q-展開 $f(q)$ が q^l のべき級数であれば

$$\begin{cases} f = l^{-k/2} g|_k w_l, \\ f(q) = g(q^l) \quad ((= g \text{ の } q\text{-展開の } q \text{ に } q^l \text{ を代入したもの })) \end{cases}$$

をみたす $g \in M_k^{\mathrm{A}}(\Gamma_0(N/l); R)$ が（ただ一つ）存在する．

Atkin-Lehner の newform の理論では [AL, §3, Theorem 1] が基礎になっていた．一般の環や正標数の体上では newform の理論の類似は期待できないが，上の補題を用いるとその定理の次の弱い version が証明できる：

命題 3.8. R は $\mathbb{Z}[1/N]$-algebra とし，$l_1, \cdots, l_s$ は N を割る素数とする．$f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)$ の q-展開 $f(q)$ に於て，n がある l_i $(i = 1, \cdots, s)$ で割り切れる時のみ $a(n; f) \neq 0$ かつ $f|_k w_{l_s} = \pm f$ であるならば，n がある l_i $(i = 1, \cdots, s-1)$ で割り切れる時のみ $a(n; f) \neq 0$（$s = 1$ の時は $f(q)$ は定数（$\in R$））となる．

特に R が $\mathbb{Z}[1/2N]$-algebra で $f \in M_k^{\mathrm{A}}(\Gamma_0(N); R)^{\epsilon}$ について，$(n, N) = 1$ の時 $a(n; f) = 0$ となっていれば $f(q)$ は定数．

この命題から，定理 3.6 の二つのペアリングで $\mathbb{Z}_{(p)}$ を $\mathbb{Q}$ で置き換えたものは完全になる事が言える．$\mathbb{Z}_{(p)}$ 上でも完全である事を示すためには更に議論を要する．Serre は [Se2, Théorème 11] で，trace 写像を用いて，奇素数 p に対して $M_2^{\mathrm{B}}(\Gamma_0(p); \mathbb{F}_p) = M_{p+1}^{\mathrm{B}}(\Gamma_0(1); \mathbb{F}_p)$ を示したが，類似の議論で次が証明できる：

命題 3.9. p は N を割る奇素数とし，$M = N/p$ とおく．q-展開を保つ写像

$$\varphi_p : M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) \to M_{p+1}^{\mathrm{A}}(\Gamma_0(M); \mathbb{F}_p)$$

で，M の正の約数 d で $(d, M/d) = 1$ （$\Leftrightarrow (d, N/d) = 1$）をみたすものについて

$$\varphi_p(f|_2 w_d) = \left(\frac{d}{p}\right) \varphi_p(f)|_{p+1} w_d$$

であるものが存在する．（$p \geq 5$ なら値域は $M_{p+1}^{\mathrm{B}}(\Gamma_0(M); \mathbb{F}_p)$ になる．）

これにより $p \mid N$ の時の $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)$ に関する問題がしばしば $M_{p+1}^{\mathrm{A}}(\Gamma_0(M); \mathbb{F}_p)$ に持ち込める．この命題と Serre-Katz の $\theta\,(= q(d/dq))$-作用素や filtration に関する結果及び命題 3.8 を用いると次が得られる：

命題 3.10. p は奇素数とし，$f \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)$ に対して，$(n, N) = 1$ ならば $a(n; f) = 0$ であると仮定すると次が成り立つ：

$p \mid N$ の時は $(n, N/p) = 1$ ならば $a(n; f) = 0$ となる．

また一般に $f \in M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)^{\epsilon}$ であれば $f(q)$ は定数．

なお $p \nmid N$ の時は q-展開写像 $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p) \to \mathbb{F}_p[[q]]$ は単射であるが，前小節で述べた正則微分の性質 (iii) 及び $p \mid N$ の時 w_p が $X_0(N)_{/\mathbb{F}_p}$ の二つの既約成分を入れ替える事から：

補題 3.11. $p \mid N$ でも $M_2^{\mathrm{reg}}(\Gamma_0(N); \mathbb{F}_p)[w_p \pm 1]$ に制限すれば q-展開写像は単射である．

命題 3.12. $M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{F}_p)^{\boldsymbol{\varepsilon}}$ の元で，q-展開が 0 でない定数であるものが存在する必要十分条件は $p=3$ で次が成り立つ事である：

$$\begin{cases} 3\nmid N \text{ で } \boldsymbol{\varepsilon}=\boldsymbol{\varepsilon}_H \text{ かつ } \boldsymbol{\varepsilon}_H\neq\boldsymbol{\varepsilon}_+, \\ 3\mid N \text{ で } \boldsymbol{\varepsilon}=\boldsymbol{\varepsilon}_H^+ \text{ かつ } \boldsymbol{\varepsilon}_H^+\neq\boldsymbol{\varepsilon}_+, \text{ または } \boldsymbol{\varepsilon}=\boldsymbol{\varepsilon}_H^-. \end{cases}$$

十分性は §3.1 最後で注意した．逆は（存在が $p=3$ の時に限る事は容易にわかり）標数 3 の Hasse 不変量を，$3\nmid N$ の時，$M_2^{\mathrm{A}}(\Gamma_0(N);\mathbb{F}_3)$ の元と見ると符号 $\boldsymbol{\varepsilon}_H$ に属する事と命題 3.9 から出る．

以上の事とスタンダードな議論から定理 3.6 が導かれる．

§3.3. Eisenstein イデアル

記号と仮定は §3.2 と同じとする．以下で Hecke 作用素 $T(l)$ は N と素な素数 l についてのみ考える．

定義 3.13. 任意の環 R に対して Hecke 環（定義 3.5）の Eisenstein イデアル

$$\begin{cases} \mathcal{I}_R\subseteq\boldsymbol{\mathcal{T}}(N;R), \\ I_R\subseteq\mathbf{T}(N;R) \end{cases}$$

をそれぞれ（上の約束下で）全ての $T(l)-(1+l)$ で生成されるイデアルと定める．R で 2 が可逆の時は 分解 (3.22) に応じて Eisenstein イデアルも

$$\begin{cases} \mathcal{I}_R=\oplus_{\boldsymbol{\varepsilon}\in\boldsymbol{E}}\mathcal{I}_R^{\boldsymbol{\varepsilon}}, \\ I_R=\oplus_{\boldsymbol{\varepsilon}\in\boldsymbol{E}}I_R^{\boldsymbol{\varepsilon}} \end{cases}$$

と分解し，$\mathcal{I}_R^{\boldsymbol{\varepsilon}}$（resp. $I_R^{\boldsymbol{\varepsilon}}$）は $\boldsymbol{\mathcal{T}}(N;R)^{\boldsymbol{\varepsilon}}$ (resp. $\mathbf{T}(N;R)^{\boldsymbol{\varepsilon}}$)（零環の事もある）の，全ての $T(l)-(1+l)$ で生成されるイデアルである．

ここでの主結果は定理 2.11 にあたる，以下の定理 3.14 である．それを述べるために各 $\boldsymbol{\varepsilon}=(\varepsilon_1,\cdots,\varepsilon_m)\in\boldsymbol{E}$ に対して次のように定める：

$$c(N;\boldsymbol{\varepsilon}):=\begin{cases} 1,\ \boldsymbol{\varepsilon}=\boldsymbol{\varepsilon}_+ \text{ の時}, \\ \frac{1}{8}\prod_{i=1}^m(l_i+\varepsilon_i),\ \boldsymbol{\varepsilon}\neq\boldsymbol{\varepsilon}_+, \text{ かつ } \boldsymbol{\varepsilon}=\boldsymbol{\varepsilon}_H \text{ または } \boldsymbol{\varepsilon}_H^{\pm} \text{ の時}, \\ \frac{1}{24}\prod_{i=1}^m(l_i+\varepsilon_i),\ \boldsymbol{\varepsilon}\neq\boldsymbol{\varepsilon}_+,\ \boldsymbol{\varepsilon}_H,\ \boldsymbol{\varepsilon}_H^{\pm} \text{ の時}. \end{cases} \tag{3.23}$$

ここに現れる 2 べき部分はこの後何の役割も果たさないが $E_{\boldsymbol{\varepsilon}}(q)$ の定数項（命題 3.4）にあわせて書いておいた．なお，$M_2(\Gamma_0(N))^{\boldsymbol{\varepsilon}_+}$ には Eisentstein 級数がなかった事を思い出しておく．

定理 3.14. 以上の記号の下で，各 $\varepsilon \in \boldsymbol{E}$ に対して

$$\mathbf{T}(N;\mathbb{Z}[1/2])^{\varepsilon}/I^{\varepsilon}_{\mathbb{Z}[1/2]} \cong \mathbb{Z}[1/2]/c(N;\varepsilon)\mathbb{Z}[1/2]$$

換言すれば任意の奇素数 p に対して

$$\mathbf{T}(N;\mathbb{Z}_{(p)})^{\varepsilon}/I^{\varepsilon}_{\mathbb{Z}_{(p)}} \cong \mathbb{Z}_{(p)}/c(N;\varepsilon)\mathbb{Z}_{(p)}$$

が成り立つ．

以下この小節ではこの定理の証明を概説する．
まず，次に注意する：

補題 3.15. $c(N;\varepsilon)$ が $\mathbb{Z}[1/2]$ の単元でなければ $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q})^{\varepsilon} \neq \{0\}$.

実際仮定の下で $c(N;\varepsilon)$ を割る奇素数 p があるが，この時（$p=3$ であっても）$E_{\varepsilon} \in M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\varepsilon}$ かつ p は $E_{\varepsilon}(q)$ の定数項を割る事から，$E_{\varepsilon} \pmod p$ は $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{F}_p)^{\varepsilon}$ の 0 でない元を与える．

これより $S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Q})^{\varepsilon} = \{0\}$ の時は定理 3.14 の主張は自明な $\{0\}/\{0\} \cong \{0\}$ となるので，以下ではそうでないとして議論する．

$\varepsilon = \varepsilon_+$, または $p=3$ で $\varepsilon = \varepsilon_H, \varepsilon_H^{\pm}$ の時は別に扱う事にして，そうではない場合を考える．この場合は §2.3 と同じ方法が使える：$X_0(N)$ のカスプの集合を C とすると G_{AL} はこの上に simply transitive に作用し (2.19) と同様に $\mathbf{Res} : M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)}) \to \mathbb{Z}_{(p)}[C]^0$ が定まり，完全系列

$$0 \to S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\varepsilon} \to M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\varepsilon} \overset{\mathbf{Res}}{\to} (\mathbb{Z}_{(p)}[C]^0)^{\varepsilon} \to 0 \tag{3.24}$$

も得られる．（$(\mathbb{Z}_{(p)}[C]^0)^{\varepsilon}$ に $M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{Z}_{(p)})^{\varepsilon}$ の商加群の構造を入れれば）この完全系列は $\mathbb{Q}$ 上では $\boldsymbol{T}(N;\mathbb{Q})^{\varepsilon}$-加群としてただ一通りに split する．付随する合同加群は §2.3 で（やや中身の乏しい）$\Gamma_1(5)$ の場合に例示したのと同じ理由で $\mathbb{Z}_{(p)}/c(N;\varepsilon)\mathbb{Z}_{(p)}$ と同型になる．この事と定理 3.6 の双対性と補題 2.12 から考えている場合の定理 3.14 が従う．

残った場合は個別に対応する必要がある．まず次が成り立つ：

命題 3.16. $p=3$ とし，$3 \nmid N$ の時は $\varepsilon = \varepsilon_H$, $3 \mid N$ の時は $\varepsilon = \varepsilon_H^{\pm}$ とすると

$$I^{\varepsilon}_{\mathbb{Z}_{(3)}} = \mathbf{T}(N;\mathbb{Z}_{(3)})^{\varepsilon}.$$

結論を否定すると環の全射

$$\mathbf{T}(N;\mathbb{Z}_{(3)})^{\varepsilon} \twoheadrightarrow \mathbf{T}(N;\mathbb{Z}_{(3)})^{\varepsilon}/I^{\varepsilon}_{\mathbb{Z}_{(3)}} \twoheadrightarrow \mathbb{F}_3$$

があるから定理 3.6 より $f \in S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{F}_3)^{\varepsilon}$ で，$(n,N)=1$ なら $a(n;f) = \sum_{0<t|n} t$ であるものが存在する．命題 3.16 の証明には Mazur [M, p. 86] による次のトリックを用いる：

補題 3.17. 一般に a, b を N と素な正整数とすると次の図式を可換にする単射 “$\times a$” がただ一つ存在する：

$$\begin{array}{ccc} M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{Z}/b\mathbb{Z}) & \xrightarrow{\text{“}\times a\text{”}} & M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{Z}/ab\mathbb{Z}) \\ \downarrow & & \downarrow \\ \mathbb{Z}/b\mathbb{Z}[[q]] & \xrightarrow[\times a]{} & \mathbb{Z}/ab\mathbb{Z}[[q]] \end{array}$$

ここで左右の写像は q-展開写像，下の写像は a 倍： $\mathbb{Z}/b\mathbb{Z} \hookrightarrow \mathbb{Z}/ab\mathbb{Z}$ から引き起こされるものである．“$\times a$” の像は q-展開が $a \cdot \mathbb{Z}/ab\mathbb{Z}[[q]]$ に属する $M_k^{\mathrm{A}}(\Gamma_0(N);\mathbb{Z}/ab\mathbb{Z})$ の元全体である．また，“$\times a$” は w_d と可換である．

$3 \nmid N$ とする．上の f に Hasse 不変量をかけた $f' \in S_4^{\mathrm{A}}(\Gamma_0(N);\mathbb{F}_3)$ は f と同じ q-展開を持ち，$f'|_4 w_{l_i} = f'$ $(i = 1, \cdots, m)$ をみたす．$E_4 \in M_4^{\mathrm{B}}(\Gamma_0(1);\mathbb{Z})$ を普通の Eisenstein 級数：

$$E_4(q) = 1 + 240\sum_{n=1}^{\infty}(\sum_{0<t|n} t^3)q^n$$

とし，$E_4' = E_4|_4 \prod_{i=1}^m (1 + w_{l_i})$ とおく．$E_4'(q)$ の定数項は 3-進単数である．さて上の記号で $G' := E_4' \pmod 9 - 80 \cdot \text{“}\times 3\text{”} f' \in M_4^{\mathrm{A}}(\Gamma_0(N);\mathbb{Z}/9\mathbb{Z})$ に命題 3.8 を用いると $G'(q) \in (\mathbb{Z}/9\mathbb{Z})^\times$ となり，更に補題 3.7 を用いて $G \in M_4^{\mathrm{A}}(\Gamma_0(1);\mathbb{Z}/9\mathbb{Z})$ で $G(q) = 1$ であるものの存在が結論される．$E_4 \pmod 9 - G$ にもう一度上の補題を用いると $M_4^{\mathrm{A}}(\Gamma_0(1);\mathbb{F}_3)$ の元で $80\sum_{n=1}^{\infty}(\sum_{0<t|n} t^3)q^n$ を q-展開に持つものが存在する事になるがこれは Deligne [De, Proposition 6.2, (II)] に反する．

$3 \mid N$ の時も f に命題 3.9 を使って $M_4^{\mathrm{A}}(\Gamma_0(N/3);\mathbb{F}_3)$ に持ち込んで（少し余計な手間はかかるが）類似の議論をする事により命題 3.16 が示される．

次を言えば定理 3.14 の証明が完了する：

命題 3.18. 任意の奇素数 p に対して

$$I^{\boldsymbol{\varepsilon}+}_{\mathbb{Z}_{(p)}} = \mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}+}.$$

結論を否定すると前命題と同様 $f \in S_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{F}_p)$ で次をみたすものが存在する：

$$(*) \qquad \begin{cases} (n, N) = 1 \text{ なら } a(n;f) = \sum_{0<t|n} t, \\ N \text{ を割る各素数 } l_i \text{ に対して } f|_2 w_{l_i} = f. \end{cases}$$

まず $p \nmid N$ の場合を考え，$m \geq 2$ とする．必要なら $l_1, \cdots, l_m$ の順を変えて（$p = 3$ の時も）$\boldsymbol{\varepsilon}_0 := (-1, +1, \cdots, +1) \neq \boldsymbol{\varepsilon}_H$ と仮定できる．次が命題 3.18 の証明の key step である：

Claim: $(*)$ をみたす $f \in M_2^{\mathrm{A}}(\Gamma_0(N);\mathbb{F}_p)$ があれば N を N/l_1 に変えた $(*)$ をみたす $g \in M_2^{\mathrm{A}}(\Gamma_0(N/l_1);\mathbb{F}_p)$ が存在する．

この inductive step は類似の議論を Agashe [Ag, Proposition 3.5] が行っていて，それに示唆されたものである．（もっとも Agashe はこのアイデアを（$m = 1$ の時を扱った）Mazur [M, p. 114] に帰しているが．）f が claim の仮定をみたしている時，$h := f - E_{\boldsymbol{\varepsilon}_0} \pmod p \in M_2^{\mathrm{A}}(\Gamma_0(N);\mathbb{F}_p)$ に命題 3.8 を用いると $h(q)$ は q^{l_1} のべき級数になる．すると補題 3.7 より $g' \in M_2^{\mathrm{A}}(\Gamma_0(N/l_1);\mathbb{F}_p)$ で $h(q) = g'(q^{l_1})$ をみたすものがある．この g' を定数倍して正規化した g が求める条件をみたす事が証明できる．

これにより素数レヴェル l で $(*)$ をみたすものが存在する事になり，$p = 3$, $l \equiv 2 \pmod 3$ の場合を除くと更にもう一回 claim が使える．後は Mazur に倣って各個の場合に矛盾を導ける．

$p \mid N$ の時も似たような事を考える．$l_1 = p$ とし $\boldsymbol{\varepsilon}_0 = (-1, +1, \cdots, +1)$ とおく．$p = 3$ で $\boldsymbol{\varepsilon}_+ = \boldsymbol{\varepsilon}_H^+$ の場合は命題 3.16 で済んでいるから，$p = 3$ ならそうではない，従って $\boldsymbol{\varepsilon}_0 \neq \boldsymbol{\varepsilon}_H^-$ と仮定できる．よって $h := f - E_{\boldsymbol{\varepsilon}_0} \pmod p \in M_2^{\mathrm{reg}}(\Gamma_0(N);\mathbb{F}_p)$ を考える事ができ，命題 3.8 - 3.10 を使うと今度は $h(q) = 0$ が出る．これより正則微分 f は supersingular 点で正則である事がわかり，$M_2^{\mathrm{A}}(\Gamma_0(N/p);\mathbb{F}_p)$ の元で，N を N/p に変えた $(*)$ をみたすものの存在が示せ，先に述べた場合に帰着して命題 3.18 が言える．

§3.4. Rational torsion

記号と仮定は今までと同じとする．特に $c(N;\boldsymbol{\varepsilon}) \in \mathbb{Z}[1/2]$ は (3.23) のものとする．§2.2 最後と同様自然に

$$\mathbf{T}(N;\mathbb{Z}) \subseteq \mathrm{End}(J_0(N)) \tag{3.25}$$

とみなせる．p が奇素数ならば (3.17) のように

$$J_0(N)(\mathbb{Q})[p^\infty] = \oplus_{\boldsymbol{\varepsilon}\in\boldsymbol{E}} J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}} \tag{3.26}$$

と分解し，各 $J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}$ は $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$-加群となる．

§1 の主定理 II より少し詳しい次の定理が本節の主結果である：

定理 3.19. p は奇素数とし，$3 \mid N$ の時は更に $p \neq 3$ も仮定する．各 $\boldsymbol{\varepsilon} \in \boldsymbol{E}$ について次が成り立つ：

$$J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}} = \mathcal{C}_0(N)[p^\infty]^{\boldsymbol{\varepsilon}} \cong \mathbb{Z}_{(p)}/c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)}.$$

以下この定理の証明のあらすじを辿って行く．

まず，定理 2.13 にあたる事：

補題 3.20. p が奇素数の時 Eisenstein イデアル $I_{\mathbb{Z}_{(p)}}$ は $J_0(N)(\mathbb{Q})[p^\infty]$ を零化する．従って $I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}$ は $J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}$ を零化する．

これは今度は容易で，Eisenstein イデアルは $T(l)-(1+l)$ たち（のみ）で生成されていたから，定理 2.13 の後に述べたのと同様に Eichler-志村の合同関係式と Raynaud または Katz の結果から直ちに従う．

$\boldsymbol{E}\ni\boldsymbol{\varepsilon}=(\varepsilon_1,\cdots,\varepsilon_m)$ の時準同型 $\prod_{i=1}^m(1+\varepsilon_i w_{l_i}):J_0(N)\to\prod_{i=1}^m(1+\varepsilon_i w_{l_i})\cdot J_0(N)$ は $J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}$ 上では単射で，対応する余接空間の写像の像は $S_2^{\mathrm{B}}(\Gamma_0(N);\mathbb{Q})^{\boldsymbol{\varepsilon}}$ と標準的に同型となる．従って $S_2^{\mathrm{B}}(\Gamma_0(N);\mathbb{Q})^{\boldsymbol{\varepsilon}}=\{0\}$ の時は $J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}}=\{0\}$ で，また補題 3.15 より $\mathbb{Z}_{(p)}/c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)}$ も $\{0\}$ となるので定理 3.19 は自明に成り立つ．よって以下では $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}\neq\{0\}$ の場合を扱う．

定理 3.19 の証明には命題 2.14 にあたる事も必要となる．以前と同じく $J_0(N)_{/\mathbb{Z}_{(p)}}$ で $J_0(N)$ の $\mathbb{Z}_{(p)}$ 上の Néron モデルを，$J_0(N)_{/\mathbb{F}_p}$ でその閉ファイバーを表す．また “$\widehat{\ }$” で Pontrjagin 双対を表す．

定理 3.21. p は奇素数とし，$3\mid N$ の時は $p\neq 3$ も仮定する．この時 $J_0(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty]^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}]^{\widehat{\ }}$ は $\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}}$-加群として巡回的である．

この定理の証明のポイントは次のとおり：

• $p\nmid N$ の時は $J_0(N)$ は p で good reduction を持つので，命題 2.14, (1) と同様に Cartier-Serre の同型を用いて証明できる．

• よって $p\mid N$ とする．$\Gamma:=J_0(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty]$ とおく．また $\Phi:=J_0(N)_{/\overline{\mathbb{F}}_p}/J_0(N)^0_{/\overline{\mathbb{F}}_p}$ を $J_0(N)_{/\overline{\mathbb{F}}_p}$ の連結成分のなす群とする．よく知られているように，$J_0(N)^0_{/\mathbb{F}_p}$ の極大トーラスを T とすると $J_0(N)^0_{/\mathbb{F}_p}/T$ は（命題 3.1 から）$J_0(M)_{/\mathbb{F}_p}$（$M:=N/p$）二個の直積と標準的に同型となるので完全系列

$$0\to(J_0(M)_{/\mathbb{F}_p}\times J_0(M)_{/\mathbb{F}_p})(\overline{\mathbb{F}}_p)[p^\infty]\to\Gamma\to\Phi[p^\infty]\to 0$$

がある．

• $p\geq 5$ としたのは次の事を使うためである：$X_0(N)_{/\mathbb{F}_p}$ の二つの連結成分を Z_∞, Z_0 とするとこれらの上の自由 Abel 群の次数 0 の部分 D からの自然な準同型

$$\theta:D=\mathbb{Z}\cdot(Z_\infty-Z_0)\to\Phi$$

があり，その余核は 12 で零化され，かつ w_p の Φ への作用は D 上の -1 倍，他の N を割る素数 l についての w_l では D 上の恒等写像と両立する（Ribet [Ri3, Theorem 2.4], [Lo, §2]；後者の方がわかり易い）．

• $l_1=p$, $\boldsymbol{\varepsilon}_0=(-1,+1,\cdots,+1)$ とおく．上と命題 3.18 を使うと

$$\Gamma^{\boldsymbol{\varepsilon}_0}[I^{\boldsymbol{\varepsilon}_0}_{\mathbb{Z}_{(p)}}]\hookrightarrow\Phi[p^\infty]^{\boldsymbol{\varepsilon}_0}[I^{\boldsymbol{\varepsilon}_0}_{\mathbb{Z}_{(p)}}](=\Phi[p^\infty]^{\boldsymbol{\varepsilon}_0})$$

となる事が言え，この群自身が巡回群である．$\boldsymbol{\varepsilon}\neq\boldsymbol{\varepsilon}_0$ の時は $\boldsymbol{\varepsilon}=(\pm1,\boldsymbol{\varepsilon}')$ とすると

$$J_0(M)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty]^{\boldsymbol{\varepsilon}'}\xrightarrow{\sim}\Gamma^{\boldsymbol{\varepsilon}}$$

となって $p \nmid N$ の場合に帰着できる．□

以上から定理 3.19，主定理 II が次のようにして導ける：各 $\boldsymbol{\varepsilon} \in \boldsymbol{E}$ に対して

$$| J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}} | \leq | \mathbb{Z}_{(p)} : c(N;\boldsymbol{\varepsilon})\mathbb{Z}_{(p)} | \tag{3.27}$$

が言えれば高木の公式 (1.6) より

$$| J_0(N)(\mathbb{Q})[p^\infty] | \leq | \mathbb{Z}_{(p)} : c_0(N)\mathbb{Z}_{(p)} | = | \mathcal{C}_0(N)[p^\infty] |$$

となって主定理 II が出て，$\mathcal{C}_0(N)[p^\infty]^{\boldsymbol{\varepsilon}}$ の巡回性も示せるので定理 3.19 も証明が終わる．

$S_2^{\mathrm{B}}(\Gamma_0(N);\mathbb{Q})^{\boldsymbol{\varepsilon}} = \{0\}$ の時に (3.27) の成り立つ事は既に見たので，$\mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} \neq \{0\}$ と仮定できる．

この時は前節最後と同様で，補題 3.20 より mod p の還元による単射

$$J_0(N)(\mathbb{Q})[p^\infty]^{\boldsymbol{\varepsilon}} \hookrightarrow J_0(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty]^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}]$$

が得られ，上の定理から

$$| J_0(N)_{/\mathbb{F}_p}(\overline{\mathbb{F}}_p)[p^\infty]^{\boldsymbol{\varepsilon}}[I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}}] | \leq | \mathbf{T}(N;\mathbb{Z}_{(p)})^{\boldsymbol{\varepsilon}} : I^{\boldsymbol{\varepsilon}}_{\mathbb{Z}_{(p)}} |$$

となって定理 3.14 から (3.27) が従う．

以上の議論で仮定「$3 \mid N$ の時は $p \neq 3$」を用いたのは定理 3.21 の証明に於いてのみであった．定理 3.21 がこの仮定なしで言えれば，定理 3.19 と主定理 II も同仮定なしで成立する事に注意しておく．

References

[Ag] A. Agashe, Rational torsion in elliptic curves and the cuspidal subgroup, preprint.

[AL] A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann., **185** (1970), 134–160.

[CES] B. Conrad, B. Edixhoven and W. Stein, $J_1(p)$ has connected fibers, Documenta Math., **8** (2003), 331–408.

[De] P. Deligne, Courbes elliptiques: Formulaire, d'après J. Tate, In: Modular functions of one variable IV, Lecture Notes in Math., **476** (1975), 53–73.

[DR] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, In: Modular functions of one variable II, Lecture Notes in Math., **349** (1973), 143–316.

[DI] F. Diamond and J. Im, Modular forms and modular curves, In: Seminar on Fermat's last theorem, CMS conference proceedings, **17** (1995), 39–133.

[Dr] V. G. Drinfel'd, Two theorems on modular curves, Funct. Anal. Appl., **7** (1973), 155–156.

[G] B. Gross, A tameness criterion for Galois representations associated to modular forms (mod p), Duke Math. J., **61** (1990), 445–517.

[He] E. Hecke, Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik, Abh. Math. Sem. Hamburg, **5** (1927), 199–224 (Math. Werke No. 24).

[Hi] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. Sci. Éc. Norm. Sup. (4), **19** (1986), 231–273.

[Kam] S. Kamienny, On torsion in $J_1(N)$, Acta Arith., **120** (2005), 185–190.

[Kat1] N. Katz, p-adic properties of modular schemes and modular forms, In: Modular functions of one variable III, Lecture Notes in Math., **350** (1973), 69–190.

[Kat2] N. Katz, p-adic interpolation of real analytic Eisenstein series, Ann. Math., **104** (1976), 459–571.

[Kat3] N. Katz, Galois properties of torsion points on abelian varieties, Invent. Math., **62** (1981), 481–502.

[KM] N. Katz and B. Mazur, Arithmetic moduli of elliptic curves, Ann. of Math. Stud., **108** (1985).

[KL] D. Kubert and S. Lang, Modular units, Springer-Verlag (1981).

[Li] S. Ling, On the $\mathbf{Q}$-rational cuspidal subgroup and the component group of $J_0(p^r)$, Israel J. Math., **99** (1997), 29–54.

[Lo] D. Lorenzini, Torsion points on the modular jacobian $J_0(N)$, Comp. Math., **96** (1995), 149–172.

[M] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. IHES, **47** (1977).

[MR] B. Mazur and K. Ribet, Two-dimensional representations in the arithmetic of modular curves, Astérisque, **196-197** (1991), 215–255.

[MW1] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbf{Q}$, Invent. Math., **76** (1984), 179–330.

[MW2] B. Mazur and A. Wiles, On p-adic analytic families of Galois representations, Comp. Math., **59** (1986), 231–264.

[Og1] A. Ogg, Rational points on certain elliptic modular curves, Proc. Symp. Pure Math., **24** (1973), 221–231.

[Og2] A. Ogg, Diophantine equations and modular forms, Bull. AMS, **81** (1975), 14–27.

[Oh1] M. Ohta, Congruence modules related to Eisenstein series, Ann. Sci. Éc. Norm. Sup., (4) **36** (2003), 225–269.

[Oh2] M. Ohta, Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties, J. Math. Soc. Japan, **65** (2013), 733–772.

[Oh3] M. Ohta, Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II, to appear in Tokyo J. Math.

[Ra] M. Raynaud, Schémas en groupes de type $(p, ..., p)$, Bull. Soc. Math. Fr., **102** (1974), 241–280.

[Ri1] K. Ribet, A modular construction of unramified p-extension of $\mathbf{Q}(\mu_p)$, Invent. Math., **34** (1976), 151–162.

[Ri2] K. Ribet, Mod p Hecke operators and congruences between modular forms, Invent. Math., **71** (1983), 193–205.

[Ri3] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, Invent. Math., **100** (1990), 431–476.

[Se1] J.-P. Serre, Sur la topologie des variétés algébriques en caractéristique p, Symp. Int. Top. Alg., Mexico (1958), 24–53 (Œuvre I, No. 38).

[Se2] J.-P. Serre, Formes modulaires et fonctions zêta p-adiques, In: Modular functions of one variable III, Lecture Notes in Math., **350** (1973),191–268.

[Sh] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten and Princeton Univ. Press (1971).
[T1] T. Takagi, Cuspidal class number formula for the modular curves $X_1(p)$, J. Alg., **151** (1992), 348–374.
[T2] T. Takagi, The cuspidal class number formula for the modular curves $X_1(p^m)$, J. Alg., **158** (1993), 515–549.
[T3] T. Takagi, The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free, J. Alg., **193** (1997), 180–213.
[W] A. Wiles, Modular curves and the class group of $\mathbf{Q}(\zeta_p)$, Invent. Math., **58** (1980), 1–35.
[Y] J. Yu, A cuspidal class number formula for the modular curves $X_1(N)$, Math. Ann., **252** (1980), 197–216.