楕円曲線上の不変量の計算 I. (CREMONA の解説)

森田 知真

目的: Cremona [C] に従って, 楕円曲線上の不変量の具体的な計算の仕方を紹介する．特に, modular form f に付随する楕円曲線 E_f の方程式を具体的に求めたい.

1. ホモロジーの決定

この章では, modular 曲線 X のホモロジー $H_1(X,\mathbb{Q})$ を求める具体的な計算方法を紹介する．modular symbol や M-symbol といったものを使うことで, ホモロジーという幾何的対象を純代数的に計算 (処理) できるようになる.

1.1. **modular symbol.** まずは, いくつかの notation を固定する．$\mathbb{H} = \{z = x+iy \in \mathbb{C} \mid y > 0\}$ を上半平面とし, それに cusp たちを付け加えたものを $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ とする．また, $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ とし, G を Γ の合同部分群で $[\Gamma : G] = e < \infty$ なるものとする．このとき, G は $\mathbb{H}^*$ に自然に作用し, 商空間 $X_G = G\backslash\mathbb{H}^*$ はコンパクトなリーマン面の構造を持つ.

1.1.1. *modular symbol* の定義．$\alpha, \beta \in \mathbb{H}^*$ を G の作用で同値になる 2 点とする, つまり, $\beta = \mathrm{M}(\alpha)$ $(\exists M \in G)$ を満たすものとする．このとき, α と β を結ぶ $\mathbb{H}^*$ 上の smooth な曲線は商空間 X_G において, closed path を定め, $H_1(X_G,\mathbb{Z})$ の元を定めることになる．この元を <u>modular symbol</u> と呼び

$$\{\alpha,\beta\}_G \text{ あるいは, 単に, } \{\alpha,\beta\}$$

と書くことにする．逆に, 任意の $H_1(X_G,\mathbb{Z})$ の元は modular symbol から得られる.

<u>三角形による分割</u> (上半平面において)

$M \in \Gamma$ に対して, 拡大された上半平面 $\mathbb{H}^*$ 上の $M(0)$ と $M(\infty)$ を結ぶ smooth な経路を

$$(M) = \{M(0), M(\infty)\}$$

とする．また, $\langle M\rangle$ によって

$$\begin{aligned} \text{頂点}: &\quad M(0), \quad M(1), \quad M(\infty) \\ \text{辺}: &\quad (M), \quad (MTS), \quad (M(TS)^2) \end{aligned}$$

Date: October 24, 2013.

Key words and phrases. modular forms, elliptic curves, L-functions.

なる三角形をあらわすものとする．但し，ここで，$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ なる Γ の生成元とする．

Remark 1.1. $(M)_G$ など，下付きの index を用いて，X_G への射影をあらわすものとするが，文脈などから明らかなときは，G を省略することもある．

1.1.2. *modular symbol* の基本的な性質．まず，$\langle M\rangle_G$ が三角形をなすことと辺の向きを考えることで，ふたつの関係式

$$
\begin{aligned}
(M)_G + (MTS)_G + (M(TS)^2)_G =& 0 \\
(M)_G + (MS)_G =& 0
\end{aligned}
$$

が得られる．また，明らかに，$(M'M)_G = (M)_G$ $(\forall M' \in G)$ を満たすので，Γ/G の代表元をとれば，X_G における closed path

$$
(M_1)_G, \ldots, (M_e)_G \qquad (\text{但し}, e = [\Gamma : G])
$$

さえ考えればよいことになる．

1.1.3. *modular symbol* によるホモロジー．$C(G)$ によって，上の $(M_1)_G, \ldots, (M_e)_G$ を形式的な symbol として基底と考えた $\mathbb{Q}$ 上の e 次元ベクトル空間とする．

<u>modular symbol による関係</u>　$B(G)$ によって

$$
\begin{aligned}
(M)_G + (MTS)_G + (M(TS)^2)_G \\
(M)_G + (MS)_G
\end{aligned}
$$

の形をした元で生成される $C(G)$ の部分ベクトル空間とする．

次に，$C_0(G)$ を G-cusp $[\alpha]_G$ $([\alpha]_G = [\beta]_G \Leftrightarrow \beta = M(\alpha), \exists M \in G)$ たちで $\mathbb{Q}$ 上張られるベクトル空間とする．

<u>modular symbol による境界作用素</u>　境界写像 $\delta : C(G) \to C_0(G)$ を

$$
\delta((M)_G) = [M(\infty)]_G - [M(0)]_G
$$

によって定義し，$Z(G) = \mathrm{Ker}\,(\delta)$ とおく．このとき，modular symbol によって，ホモロジー $H(G) = Z(G)/B(G)$ が定義される．

<u>ベッチ・ホモロジーとの対応</u>

Proposition 1.2. *modular symbol の元をベッチ・ホモロジーの元と考える対応によって，同型* $H(G) \simeq H_1(X_G, \mathbb{Q})$ *が得られる．*

Remark 1.3. G が Γ の合同部分群のときには，任意の cusp α, β を結ぶ modular symbol $\{\alpha, \beta\}$ は，Manin と Drinfeld によって，$\mathbb{Q}$-構造を持つ，つまり，$H_1(X_G, \mathbb{Q})$ の元を定めることが知られている．特に，$\{0, \infty\} \in H_1(X_G, \mathbb{Q})$ となる．

1.2. M**-symbol.** 上の命題によって, かなり代数的にホモロジーを計算できるようになった. この節では, M-symbol (M は Manin にちなむ) と呼ばれるものを導入することで, さらに代数的な計算に帰着できることを見たい. ここでは, $G = \Gamma_0(N)$ に特化し, $H(N) = H(\Gamma_0(N))$, $X_0(N) = X_{\Gamma_0(N)}$ のように略記することにする.

1.2.1. *M-symbol* の定義. $\gcd(c, d, N) = 1$ を満たすペアーたち $(c, d) \in \mathbb{Z}^2$ に対して, 次のように関係 $\sim$ を定義する

$$(c_1, d_1) \sim (c_2, d_2) \iff c_1 d_2 \equiv c_2 d_1 \pmod N.$$

この $\sim$ は同値関係をなすことが分かり, この (c, d) が定める同値類を $(c : d)$ と書き, $\underline{M\text{-symbol}}$ と呼ぶことにする. また, M-symbol の集合は射影直線 $\mathbb{P}^1(N) = \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ をなす.

◊ 覚え方　ふたつのペアー (c_1, d_1) と (c_2, d_2) が同値というのは, **たすき掛け**して, その差が N で割れるということ.

1.2.2. *M-symbol* によるホモロジー. 次の命題が示すように, M-symbol と modular symbol との間には, 1対1の対応がある.

$\underline{M\text{-symbol v.s. modular symbol}}$

Proposition 1.4. 次の全単射が存在する

$$\mathbb{P}^1(N) \longleftrightarrow [\Gamma : \Gamma_0(N)] \longleftrightarrow \{(M) : M \in [\Gamma : \Gamma_0(N)]\}.$$

なお, これらの対応は具体的に

$$(c : d) \longleftrightarrow M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longleftrightarrow (M) = \{b/d, a/c\}$$

によって与えられる. 但し, $a, b \in \mathbb{Z}$ は $ad - bc = 1$ を満たすものとする. *(*証明は *[C, Proposition 2.2.1]* からの帰結によるもので, 簡単に行うことができる.*)*

最右辺の modular symbol との対応で, M-symbol によって, ベッチ・ホモロジーが計算できると思われる. 実際に, 以下のように, 対応する計算がある.

$\underline{M\text{-symbol による関係}}$

$$(c : d) + (c + d : -c) + (d : -c - d)$$
$$(c : d) + (-d : c)$$

$\underline{M\text{-symbol による境界作用素}}$

$$\delta : (c : d) \mapsto [a/c] - [b/d]$$

これらを用いることによって, 純代数的にベッチ・ホモロジーを計算できることを見ることにする.

Example 1.5. M-symbol を用いることで, レベル 11 の modular 曲線 $X_0(11)$ のベッチ・ホモロジー $H_1(X_0(11), \mathbb{Q}) \simeq H(11)$ を具体的に計算する.

I. リストの作成

M-symbol は $(c:1)$ mod 11 と $(1:0)$ の 12 個のみ $\rightsquigarrow$ (c) と (∞) と書く.

II. 関係式を考える $\rightsquigarrow B(G)$

a). $(c:d)+(-d:c)=0$ より

$$\begin{aligned} (0)+(\infty)=0, \quad (1)+(-1)=0, \quad (2)+(5)=0,\\ (-2)+(-5)=0, \quad (3)+(-4)=0, \quad (-3)+(4)=0. \end{aligned}$$

例えば, $(2:1)+(-1:2)=0$ だが, たすき掛けの同値関係を見ると, $(-1)\cdot 1 \equiv 5\cdot 2 \pmod{11}$ より, $(-1:2)=(5:1)$ が成立し, $(2)+(5)=0$ となる.

b). $(c:d)+(c+d:-c)+(d:-c-d)=0$ より

$$\begin{aligned} (0)+(\infty)+(-1) &=0, \qquad (1)+(-2)+(5)=0,\\ (2)+(4)+(-4) &=0, \qquad (3)+(-5)+(-3)=0. \end{aligned}$$

例えば, $(1:1)+(2:-1)+(1:-2)=0$ だが, たすき掛けの同値関係を見ると, $2\cdot 1 \equiv (-2)\cdot(-1) \pmod{11}$ や $1\cdot 1 \equiv 5\cdot(-2) \pmod{11}$ より, $(2:-1)=(-2:1)$ や $(1:-2)=(5:1)$ が成立し, $(1)+(-2)+(5)=0$ となる.

$$\Downarrow$$

ここで, $A=(2)$, $B=(3)$, $C=(0)$ とおき, 連立一次方程式を解くと

$$\begin{cases} (0)=C, & (\infty) \quad =-C, \qquad (1)=(-1)=0,\\ (2)=(-2)=A, & (3) \quad =B, \qquad (-3)=A-B,\\ (4)=B-A, & (-4) \quad =-B, \qquad (5)=(-5)=-A. \end{cases}$$

このように, すべての M-symbol が A, B, C の線型結合で書ける.

III. 境界作用素を考える $\rightsquigarrow Z(G)$

$[a/b]=[0]$ if $b \not\equiv 0 \pmod{11}$, $[a/b]=[\infty]$ if $b\equiv 0 \pmod{11}$ が成立するので, ふたつの $\Gamma_0(11)$-cusp $[0]$ と $[\infty]$ が存在することになる. よって

$$\begin{aligned} \delta((m))=[1/m]-[0] &=0 \qquad m\not\equiv 0 \pmod{11} \text{ のとき}\\ \delta((0))=[\infty]-[0] &\neq 0 \end{aligned}$$

となるので, $A, B \in \mathrm{Ker}\,(\delta)$ かつ $C=(0)\notin \mathrm{Ker}\,(\delta)$ が分かる.

$$\Downarrow$$

$$H_1(X_0(11),\mathbb{Q}) \simeq H(11) \simeq \langle A, B\rangle \text{ となることが分かった.}$$

♣ ホモロジーの計算の仕方 (まとめ)

Example 1.5. の要領 I.⇒ II.⇒ III. で計算を行えばよいが, III. よりも II. を先に行い, 関係式を用いることで, パラメーターの数を減らし, 計算量を減らすのに成功している.

2. Hecke 作用素の計算とフーリエ係数の決定

この章では, Hecke 作用素に関する簡単な事実を復習した後, modular form f に対して, そのフーリエ係数 a_{p_0} を p_0 が小さい素数のときに, 直接の手計算, もしくは Heilbronn 行列を用いることで求めるのが目的である. なお, 次の章で, このフーリエ係数 a_{p_0} から, 他の大量の素数 p に対するフーリエ係数 a_p を求める方法を紹介する.

2.1. **Hecke 作用素.** ここでは, まず, $N \in \mathbb{N}$ をひとつ固定し, N を割り切らない素数 p に対して, Hecke 作用素 T_p がどのようにして作用するのかについてまとめておく.

modular symbol への作用

$T_p(\{\alpha,\beta\})$ は次の式で与えられる

$$\left[\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_{r \bmod p} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix}\right]\{\alpha,\beta\} = \{p\alpha, p\beta\} + \sum_{r \bmod p} \{\frac{\alpha+r}{p}, \frac{\beta+r}{p}\}.$$

また, この作用は modular symbol によって定義されたホモロジー $H(N)$ への自然な作用を誘導する.

modular form への作用

以下, $\Gamma_0(N)$ に対する重さ 2 の cusp form のみを考えるとし, その全体がなす $\mathbb{C}$ 上のベクトル空間を $S_2(N)$ と書くことにする. 一般に, 2×2 行列 $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $(ad-bc>0)$ の cusp form $f(z) \in S_2(N)$ への作用は

$$(f \mid M)(z) = \frac{ad-bc}{(cz+d)^2}\ f(\frac{az+b}{cz+d})$$

と定義した. よって, Hecke 作用素 $T_p = \left[\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_{r \bmod p} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix}\right]$ による cusp form $f(z)$ への作用は

$$(f \mid T_p)(z) = pf(pz) + \frac{1}{p}\sum_{r=0}^{p-1} f(\frac{z+r}{p})$$

で与えられ, $S_2(N)$ に作用することになる.

Hecke 作用素の両立性

任意の $\gamma \in H_1(X_0(N), \mathbb{Q})$ と $f \in S_2(N)$ に対して, 積分 $\int_\gamma 2\pi i f(z) dz$ を $\langle \gamma, f \rangle$ と書くことにする. このとき, 一般に, $\langle \{\alpha, \beta\}, f \mid M \rangle = \langle \{M\alpha, M\beta\}, f \rangle$ が成立することが分かるので, 特に, Hecke 作用素 T_p に対して

$$\langle \{\alpha, \beta\}, f \mid T_p \rangle = \langle \{T_p\alpha, T_p\beta\}, f \rangle$$

となり, Hecke 作用素 T_p の $H(N)$ と $S_2(N)$ への作用が両立していることが分かる.

Fricke involution W_q

N を割り切る素数 q に対して, $H(N)$ と $S_2(N)$ に作用する Fricke involution W_q について, 復習しておく. この作用素は 関数等式の計算 に登場するのはもちろん, L-関数の値を近似計算 する際に, 大きな力を発揮する. Hecke 作用素 T_p と Fircke involution W_q で $\mathbb{Q}$ 上生成される代数を Hecke 代数と呼び, $\mathbb{T}$ と書く. また, $W_N = \Pi_q W_q$ と定義すると, これは, $z \mapsto -1/Nz$ に対応するもので, 関数等式の計算に登場する.

まず, $\alpha \in \mathbb{N}$ を $q^\alpha \mid N$ かつ $q^{\alpha+1} \nmid N$ をなるものとし, $x, y, z, w \in \mathbb{Z}$ は $q^\alpha xw - (N/q^\alpha)yz = 1$ を満たすように選ぶ. このとき, 行列

$$W_q = \begin{pmatrix} q^\alpha x & y \\ Nz & q^\alpha w \end{pmatrix}$$

は $H(N)$ と $S_2(N)$ に作用し, $W_q^2 \in \Gamma_0(N)$ より involution になる. なお, この W_q は $x, y, z, w \in \mathbb{Z}$ の取り方に依存しない.

Example 2.1. (Example 1.5. の続き.)

modular 曲線 $X_0(11)$ のホモロジーは $H_1(X_0(11), \mathbb{Q}) \simeq H(11) \simeq \langle A, B \rangle$ で与えられた. このとき, M-symbol $A = (2:1)$ 上の Hecke 作用素 T_p $(p \neq 11)$ と Fricke involution W_{11} がどのように作用するかを見たい.

I. M-symbol から modular symbol への変換

M-symbol $A = (2:1)$ から modular symbol への変換は Proposition 1.4. の対応より (行列式が 1 となるように第 1 行を選ぶ), 例えば

$$A = (2:1) \longleftrightarrow M = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \longleftrightarrow (M) = \{0/1, 1/2\}$$

で与えられることになる.

II. modular symbol 上への作用

ア). まずは, Hecke 作用素 T_p による作用を計算することにする. $p = 2$ のときに, 定義に従って, 手計算をすると

$$T_2(A) = T_2(\{0, \frac{1}{2}\}) = \{0, 1\} + \{0, \frac{1}{4}\} + \{\frac{1}{2}, \frac{3}{4}\}$$

で与えられる．ここで再び, modular symbol と M-symbol との対応を考えると最右辺は $(1:1)+(4:1)+(1:2)+(-4:1)=0+(B-A)+(-A)+(-B)=-2A$ となり

$$T_2(A)=-2A$$

が分かる． Hecke 作用素の両立性 における式より, $S_2(11)$ の rational newform $f(z)=\sum a_n e^{2\pi i n z}$ は

$$a_2=-2$$

を満たすと予想されるが, 実際にそれが正しいということは後に述べることにする (つまり, f と A が $\langle A,f\rangle\neq 0$ によって, 双対をなす).

イ)．次に, Fricke involution W_{11} による作用を計算することにする．W_{11} として, 例えば

$$W_{11}=\begin{pmatrix}0&-1\\11&0\end{pmatrix}\qquad (x=w=0, y=-1, z=1\text{ を選んだ})$$

が取れる．M-symbol から modular symbol に変換すれば, この行列表示を利用できるので, ア)．と同様にして, $W_{11}(A)$ は modular symbol $\left\{0,\frac{1}{2}\right\}$ を使って

$$W_{11}(A)=\begin{pmatrix}0&-1\\11&0\end{pmatrix}\left\{0,\frac{1}{2}\right\}=\left\{\infty,\frac{-2}{11}\right\}$$

となる．ここで, 再び, M-symbol に変換する手順を踏んで計算すると $\left\{\infty,0\right\}+\left\{0,-\frac{1}{5}\right\}+\left\{-\frac{1}{5},\frac{-2}{11}\right\}=(1:0)+(-5:1)+(11:5)=(\infty)+(-5)+(0)=-A$ となり, 結局, Fricke involution の作用は次の式で与えられることになった

$$W_{11}(A)=-A.$$

このことから, L-関数の関数等式の符号が + になることは後で (§5.1), 述べることにする．

♡ Hecke 作用素の計算の仕方

この章の目的は, modular form のフーリエ係数 a_{p_0} の p_0 が小さいときに, 具体的に求めることであるが, modular symbol 上への作用を直接, 手計算すればできるものである．

2.2. **Heilbronn 行列.** 上の方法で計算する難点は, せっかく純代数的な M-symbol を求めたにもかかわらず, T_p や W_q の作用を見るために, やや幾何的な modular symbol との間を行き来しなければならないことである．ここでは, 計算の速度を上げるために, M-symbol のみで計算できる Heilbronn 行列を簡単に紹介する．但し, 行われていることは, 理論的には前節と変わりはない．

前節では, modular symbol 上に, どのように T_p が作用するかを見るためには, $p+1$ 個の行列

$$\begin{pmatrix}p&0\\0&1\end{pmatrix},\qquad \begin{pmatrix}1&r\\0&p\end{pmatrix}\ (r \bmod p)$$

の作用を計算しておけばよかった. これに対応する M-symbol への作用が ([C, Proposition 2.4.1.]) にまとめられている. この計算から, 各素数 p に対して, $M_2(\mathbb{Z})$ の有限部分集合 R_p (Heilbronn 行列たち) で, T_p の M-symbol 上への作用が

$$T_p((c:d)) = \sum_{M \in R_p} (c:d)M$$

で与えられるものが存在することが分かる. 特筆すべきは, R_p が素数 p にしか依存しておらず, R_p を前もって計算しておけば, Hecke 作用の計算が非常に簡単になることである.

Proposition 2.2. *$p \nmid N$ を満たす奇素数とする. このとき, R_p は次のいずれかを満たす行列 $\begin{pmatrix} x & -y \\ y' & x' \end{pmatrix} \in M_2(\mathbb{Z})$ $(xx' + yy' = p)$ たちの集合である.*

(1) *$x > |y| > 0$, かつ $x' > |y'| > 0$, かつ $yy' > 0$; or*

(2) *$y = 0$, かつ $|y'| < x'/2$; or*

(3) *$y' = 0$, かつ $|y| < x/2$.*

いくつかの Heilbronn 行列

$$R_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \right\}$$

$$R_3 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & -3 \end{pmatrix} \right\}$$

$$R_5 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 5 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & -5 \end{pmatrix}, \begin{pmatrix} 5 & -2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -2 & 1 \\ 1 & -3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -3 & 5 \end{pmatrix} \right\}$$

Example 2.3. (Example 2.1. の続き)

modular 曲線 $X_0(11)$ のホモロジーは $H_1(X_0(11), \mathbb{Q}) \simeq H(11) \simeq \langle A, B \rangle$ で与えられ, このとき, M-symbol $A = (2:1)$ と modular symbol とを対応させ, $T_2(A) = -2A$ を示したが, ここでは Heilbronn 行列たち R_2 のデータから, M-symbol だけ

を使って計算する. $T_2(A) = (2:1)R_2$ は次で与えられる

$$
\begin{aligned}
(2:1)\begin{pmatrix}1&0\\0&2\end{pmatrix} + (2:1)\begin{pmatrix}2&0\\0&1\end{pmatrix} + (2:1)\begin{pmatrix}2&1\\0&1\end{pmatrix} + (2:1)\begin{pmatrix}1&0\\1&2\end{pmatrix}& \\
=&(2:2)+(4:1)+(4:3)+(3:2)\\
=&(1)+(4)+(5)+(-4)\\
=&0+(B-A)+(-A)+(-B)\\
=&-2A.
\end{aligned}
$$

ついでに, $T_3(A) = (2:1)R_3$ も計算してみると

$$
\begin{aligned}
(2:1)\begin{pmatrix}1&0\\0&3\end{pmatrix} &+(2:1)\begin{pmatrix}3&1\\0&1\end{pmatrix} + (2:1)\begin{pmatrix}1&0\\1&3\end{pmatrix}\\
&+(2:1)\begin{pmatrix}3&0\\0&1\end{pmatrix} + (2:1)\begin{pmatrix}3&-1\\0&1\end{pmatrix} + (2:1)\begin{pmatrix}-1&0\\1&-3\end{pmatrix}\\
&=(2:3)+(6:3)+(3:3)+(6:1)+(6:-1)+(-1:-3)\\
&=(8:1)+(2:1)+(1:1)+(6:1)+(5:1)+(4:1)\\
&=(A-B)+(A)+(0)+(-A)+(-A)+(B-A)\\
&=-A.
\end{aligned}
$$

♣ Hecke 作用素の計算の仕方 (まとめ)

modular form のフーリエ係数 a_{p_0} の p_0 が小さい素数のときに, 具体的に求めることを目的にしていた. ここで紹介した方法をまとめると

I. M-symbol と modular symbol を行き来し, 定義に従って, Hecke 作用素を手計算する. 少し煩わしく, 計算量が増える.

II. Heilbronn 行列を使って, M-symbol のみで Hecke 作用を計算する. 前もって, Heilbronn 行列を知っているとその計算は非常に簡単になる.

3. MODULAR FORM と楕円曲線

この章では, modular form と楕円曲線に関する簡単な事実を復習しておく. 今後, 考える modular form は重み 2, レベル N の rational な newform が主である.

3.1. modular な楕円曲線. f を rational newform としたときに, 周期格子 Λ_f を

$$\Lambda_f = \left\{\langle\left\{\alpha,\beta\right\}, f\rangle \mid \alpha,\beta\in\mathbb{H}^*, \alpha\equiv\beta \bmod \Gamma_0(N)\right\}$$

と定義すると, ランクが 2 の離散部分群 ($\subset\mathbb{C}$) になる. このとき

$$E_f = \mathbb{C}/\Lambda_f$$

は楕円曲線になり, f に付随する modular な楕円曲線と呼ぶ.

知られている事実

○ E_f は $\mathbb{Q}$ 上定義されている.

○ $L(E_f, s) = L(f, s)$.

○ E_f の導手は N

3.2. **フーリエ係数と Hecke 作用素.** rational newform を $f(z) = \sum_{n\geq 1} a_n q^n$ ($q = e^{2\pi i z}$) と書いたときに, $a_1 = 1$ と正規化されているものとする. このとき, 次が成立することが知られている.

○ $p \nmid N$ なる素数 p に対して, $f \mid T_p = a_p f$.

○ $q \mid N$ なる素数 q に対して, $f \mid W_q = \epsilon_q f$ ($\epsilon_q = \pm 1$) となり

$$a_q = \begin{cases} -\epsilon_q & \text{if } q^2 \nmid N \\ 0 & \text{if } q^2 \mid N. \end{cases}$$

なお, 素数の冪が高いときは

$$a_{p^{n+1}} = a_p a_{p^r} - \delta_N(p) p a_{p^{r-1}} \quad (r \geq 1)$$

のように, 帰納的に係数が決まっていく. 但し, ここで

$$\delta_N(p) = \begin{cases} 1 & \text{if } p \nmid N \\ 0 & \text{if } p \mid N. \end{cases}$$

さらには, n と m が互いに素であるならば, $a_{mn} = a_m a_n$ なる乗法性を満たす.

4. 実構造 $H^+(N)$ と $S_2(N)_{\mathbb{R}}$

次の章で, 実周期を考えることが重要になる. そのために, この章では, 実構造 $H^+(N)$ と $S_2(N)_{\mathbb{R}}$ についての簡単な事実をまとめておく.

$z \in \mathbb{H}$ に対して, involution $*$ を $z \mapsto z^* = -\overline{z}$ で定義する.

ホモロジー上への作用

このとき, modular symbol 上への自然な作用を考えると, $H_1(X_0(N), \mathbb{R})$ 上に $\mathbb{R}$-linear な involution $*$ が誘導される. ここで, $*$ に対する固有分解を行うと

$$H_1(X_0(N), \mathbb{R}) = H_1^+(X_0(N), \mathbb{R}) \oplus H_1^-(X_0(N), \mathbb{R})$$

が得られる. 但し, $H_1^{\pm}(X_0(N), \mathbb{R})$ はそれぞれ, 固有値 ± 1 に対応しているとする.

Remark 4.1. 環 $A \subset \mathbb{R}$ に対して, $H_1^{\pm}(X_0(N), A) = H_1^{\pm}(X_0(N), \mathbb{R}) \cap H_1(X_0(N), A)$ と定義することにする. また, $H^{\pm}(N)$ で, $H_1^{\pm}(X_0(N), \mathbb{Q})$ に対応する $H(N)$ の部分空間を表すものとする.

modular form 上への作用

$f \in S_2(N)$ に対して, $f^*(z) = \overline{f(z^*)}$ と定めると, $S_2(N)$ に $\mathbb{R}$-linear な involution $*$ が誘導される. $S_2(N)_{\mathbb{R}}$ で, $*$ による $S_2(N)$ の不変部分ベクトル空間をあらわすものとする. このとき

(1) $f(z) = \sum a_n q^n \Longleftrightarrow f^*(z) = \sum \overline{a_n} q^n \quad (q = e^{2\pi i z})$

(2) $\langle \gamma^*, f^* \rangle = \overline{\langle \gamma, f \rangle}$ for all f, γ

などが成立する. 特に, (2) より, $f \in S_2(N)_{\mathbb{R}}$ に対して, 次が成立する

$$\langle \gamma, f \rangle \in \mathbb{R} \iff \gamma \in H_1^+(X_0(N), \mathbb{R}), \quad \langle \gamma, f \rangle \in i\mathbb{R} \iff \gamma \in H_1^-(X_0(N), \mathbb{R}).$$

Remark 4.2. 実構造を使うと計算面において, M-symbol の計算を半分にする効果がある. $*$ の上半平面上への作用は $z \mapsto z^* = -\overline{z}$ で与えられ, 実構造 $H^+(N)$ を使うことは幾何的には上半平面を虚軸に関して, ふたつに折りたたんだものを考えているのと同じである. これにより, M-symbol 上には $(c : d) = (-c : d)$ という関係式が得られ, 計算の速度を上げることができる. 詳しくは [C, §2.5].

5. MODULAR FORM の決定

２章で求めた a_{p_0} (p_0: 小さい素数) から, L-関数を経由する手法を用いて, 他の大量の素数 p に対して, フーリエ係数 a_p を計算する方法を紹介し, modular form を決定したい.

5.1. L-関数についての簡単な復習. rational newform $f(z) = \sum_{n\geq 1} a_n q^n$ に対して, L-関数を $L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ $(\Re(s) > 2/3)$ と定義する. このとき, 次のような表示をもつことがわかる

Euler 積表示: $L(f,s) = \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p\mid N}(1 - a_p p^{-s})^{-1}$

Mellin 変換による表示: $L(f,s) = (2\pi)^s \Gamma(s)^{-1} \displaystyle\int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z}.$

この Mellin 変換により, $L(f,s)$ は全平面に解析接続される. さらに, 完備 L-関数をガンマー関数 $\Gamma(s)$ を用いて

$$\Lambda(f,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s) = \int_0^{\infty} f(iy/\sqrt{N}) y^{s-1} dy$$

と定義すると, s と $s-2$ に関して, 関数等式が成立する. Fricke involution W_N に対して, $f \mid W_N = \epsilon_N f$ $(\epsilon_N = \pm 1)$ とすると, W_N は $z \mapsto -1/Nz$ という変換に対応していたので, $f(-1/(Nz)) = \epsilon_N N z^2 f(z)$ となる. 特に, $z = iy/\sqrt{N}$ とすると $f(i/y\sqrt{N}) = -\epsilon_N y^2 f(iy/\sqrt{N})$ となり, よって, 次の関数等式を得ることができる

$$\Lambda(f, 2-s) = -\epsilon_N \Lambda(f,s).$$

また, この関数等式より, $\epsilon_N = +1$ のとき, $L(f,1) = 0$ ということが分かる.

5.2. **L-関数の値と周期との関係.** rational newform f に対して, f のある周期 $\Omega(f)$ を使って得られる比 $L(f,1)/\Omega(f)$ の値は, 楕円曲線 E_f に対する BSD 予想によって予測されている興味深い対象である. なお, Mellin 変換による L-関数の表示に $s=1$ を代入することで

$$L(f,1) = -2\pi i \int_0^{i\infty} f(z)dz = -\langle \{0,\infty\}, f\rangle$$

のように, すでに, 最右辺は f の (有理な) 周期で書けていることに注意する. この節では, 比 $L(f,1)/\Omega(f)$ とフーリエ係数 a_p を結びつけるということを考えたい.

5.2.1. 周期とフーリエ係数. $p \nmid N$ なる素数 p に対して, Hecke 作用素 T_p の modular symbol $\{0,\infty\}$ への作用は, 定義 (2 章) より, 次のように計算できる

$$T_p(\{0,\infty\}) = \{0,\infty\} + \sum_{k=0}^{p-1}\{k/p,\infty\} = (1+p)\{0,\infty\} + \sum_{k=0}^{p-1}\{k/p,0\}.$$

よって, 変形すれば

$$(1+p-T_p)\cdot\{0,\infty\} = \sum_{k=0}^{p-1}\{0,k/p\}$$

が得られ, $T_pf = a_pf$ に注意して, f による積分を考えると

$$(\spadesuit) \qquad (1+p-a_p)\cdot\langle\{0,\infty\},f\rangle = \sum_{k=0}^{p-1}\langle\{0,k/p\},f\rangle$$

となり, 周期とフーリエ係数 a_p を結びつけることができた. さらに, 右辺全体は実周期を与えるということを示すことができる.

5.2.2. $\Omega(f)$ の定義. $\Omega_0(f)$ によって, f の実周期の中で最小の正のものとする. このとき, f に対応する楕円曲線 E_f の実成分 $E_f(\mathbb{R})$ の連結成分の個数に応じて, $\Omega(f)$ を定義する

$$\Omega(f) = \begin{cases} 2\Omega_0(f) & E_f(\mathbb{R}) \text{ の連結成分の個数が } 2 \text{ 個} \\ \Omega_0(f) & E_f(\mathbb{R}) \text{ の連結成分の個数が } 1 \text{ 個.} \end{cases}$$

§6.1. において紹介するが, $\Omega(f)$ は f の周期格子をなす基底 $\{\omega_1,\omega_2\}$ の実部のうちで, 小さい方の 2 倍になることが分かる.

5.2.3. 二つの式の比較. 5.2.1. における周期 $\sum_{k=0}^{p-1}\langle\{0,k/p\},f\rangle$ は実周期であり, また実周期 $\Omega_0(f)$ の最小性より, $\Omega_0(f)$ の整数倍になっている. このことに注意して, 5.2.1. の (♠) と 5.2.2. における定義を比べると, ある整数 $n(p,f)$ (いわば, 回転数) が存在して

$$(*) \qquad \frac{L(f,1)}{\Omega(f)} = \frac{n(p,f)}{2(1+p-a_p)}$$

と書ける. 但し, 右辺の分母は, a_p に対する評価 $|\, a_p \,| < 2\sqrt{p}$ より non-zero である. この式 $(*)$ は非常に重要であり, 今後の計算において活躍する.

5.2.4. 式 $(*)$ の重要性について. 式 $(*)$ は二つの意味において重要である.

ア). ひとつの素数 p_0 に対して, a_{p_0} と $n(p_0, f)$ さえ分かれば, BSD 予想で予測されている値を求めることができる.

イ). ひとつの素数 p_0 に対して, a_{p_0} と $n(p_0, f)$ さえ分かれば, 式 $(*)$ の左辺の L-関数の値を経由して, 他の素数 p に対して

$$\frac{n(p, f)}{2(1 + p - a_p)} = \frac{n(p_0, f)}{2(1 + p - a_{p_0})}$$

が成立するので, $n(p, f)$ さえ計算できれば, フーリエ係数 a_p を大量に計算することができる. 実際に, この式を用いることで, 2 章で求めた a_{p_0} (p_0: 小さい素数) から, 他の大量の素数 p に対して, フーリエ係数 a_p を計算し, modular form を決定する.

5.3. **フーリエ係数の計算.** 式 $(*)$ を用いることで, 大量のフーリエ係数の計算を行いたい. (小さい) 素数 p_0 に対しては, a_{p_0} と $n(p_0, f)$ は計算が確定しているとする.

$L(f, 1) \neq 0$ のとき

このときは, 式 $(*)$ より, $n(p_0, f) \neq 0$ となるので, 素数 p に対して

$$a_p = 1 + p - \frac{n(p, f)(1 + p_0 - a_{p_0})}{n(p_0, f)}$$

が成立する. よって, この式から, フーリエ係数 a_p を求めることができる. なお, $n(p, f)$ は, 周期 $\sum_{k=0}^{p-1}\langle\{0, k/p\}, f\rangle$ が最小の正の実周期 $\Omega_0(f)$ の何倍になっているかをあらわしているので, $\sum_{k=0}^{p-1}\{0, k/p\}$ が $H^+(N)$ の生成元の何倍になっているかを見れば計算できる (4 章を参照).

Example 5.1. (Example 2.3. の続き)

modular 曲線 $X_0(11)$ のホモロジーは $H_1(X_0(11), \mathbb{Q}) \simeq H(11) \simeq \langle A, B\rangle$ で与えられ, このとき, M-symbol $A = (2:1)$ に対して, $T_2(A) = -2A$, つまり, $a_2 = -2$ を示した. また, A に対応する modular symbol は $\{0, 1/2\}$ であった. このことより, $A = A^*$ が分かり, $H^+(11) \simeq \langle A\rangle$ となる. よって

$$(1 + 2 - a_2)L(f, 1) = \langle\{0, 1/2\}, f\rangle = \langle A, f\rangle = \Omega(f)$$

が成立することになる (Example 6.1. の **Type 1** になる). これを変形すると

$$(*) \qquad \frac{L(f, 1)}{\Omega(f)} = \frac{1}{5}$$

を得ることができる. 前に述べたように, この式 $(*)$ の意義について見ていきたい.

ア). もちろん, 周期の計算は必要ではあるが, ひとつのフーリエ係数 a_2 より, $L(f, 1) \neq 0$ が分かった. つまり, $E_f(\mathbb{Q})$ の Mordell-Weil rank が 0 であることが分かる.

イ). 式 $(*)$ を用いて, 他の大量のフーリエ係数 a_p を求めたい. 上で述べたことより

$$\sum_{k=0}^{p-1}\{0,k/p\}=\frac{n(p,f)}{2}A$$

となる整数 $n(p,f)$ を求めればよい. つまり, $H^+(11)$ の生成元 A の何倍になっているのか?

$\diamondsuit$ 注意　整数 $n(p,f)$ を求める際に, 2 倍するべきかどうかをよく検討せよ.

$\circ$ $p=3$ のとき

$$\{0,1/3\}+\{0,2/3\}=\{0,1/3\}+\{0,1/2\}+\{1/2,2/3\}$$

を M-symbol に変換し, A の何倍で書けるかを見ればよくて

$$=(3:1)+(2:1)+(3:2)=(3)+(2)+(7)=B+A+(-B)=A$$

となるので, $a_3=1+3-\frac{5}{2}n(3,f)=-1$ が分かった.

$\circ$ $p=5$ のとき

$$\{0,1/5\}+\{0,2/5\}+\{0,3/5\}+\{0,4/5\}=A$$

となるので, $a_5=1+5-\frac{5}{2}n(5,f)=1$ が分かる.

$\circ$ $p=7$ のとき

$$\{0,1/7\}+\{0,2/7\}+\{0,3/7\}+\{0,4/7\}+\{0,5/7\}+\{0,6/7\}=2A$$

となるので, $a_7=1+7-\frac{5}{2}n(7,f)=-2$ が分かる.

他にも, $a_{13}=4$ などが分かる. これらをもとに, 節 3.2. に従って, $n=16$ までのフーリエ係数 a_n を求め, それを書いておく

$$a_1=1,a_2=-2,a_3=-1,a_4=2,a_5=1,a_6=2,a_7=-2,a_8=0,$$
$$a_9=-2,a_{10}=-2,a_{11}=1,a_{12}=-2,a_{13}=4,a_{14}=4,a_{15}=-1,a_{16}=-4.$$

これだけのフーリエ係数があれば, 周期 Λ_f や E_f の方程式を決定するための近似計算には十分である.

$L(f,1)=0$ のとき

例えば, E_f の導手が $N=37$ のときは, このような状況になる. 式 $(*)$ より, $n(p_0,f)=0$ となるので, 上と同様の手段では他の a_p が求められない. そこで, ちょっとした細工を行うことで切り抜けたい. $\alpha=n/d\in\mathbb{Q}$ $(\gcd(d,N)=1)$ に対して

$$(1+p-T_p)\cdot\{\alpha,\infty\}=\{\alpha,p\alpha\}+\sum_{k=0}^{p-1}\{\alpha,\frac{\alpha+k}{p}\}$$

を考え, さらに, integral な modular symbol の和で書くと (つまり, $H_1(X_0(N),\mathbb{Z})$ の元)

$$\{0,p\alpha\}+\sum_{k=0}^{p-1}\{0,\frac{\alpha+k}{p}\}-(p+1)\{0,\alpha\}$$

となる. modular form f に関する積分を考えると, 前と同じ議論によって, ある整数 $n(\alpha,p,f)$ が存在して

$$(*)'\qquad \frac{\Re\langle\{\alpha,\infty\},f\rangle}{\Omega(f)}=\frac{n(\alpha,p,f)}{2(1+p-a_p)}$$

と書ける. この式 $(*)'$ を用いれば, $L(f,1)\neq 0$ のときと同様にして, 他の大量のフーリエ係数を求めることができる.

♣ 大量のフーリエ係数の計算の仕方 (まとめ)

ここでは, $L(f,1)\neq 0$ のときの計算方法についてまとめる. $L(f,1)=0$ のときも, 上に述べた修正版を使えば, 同様に計算できる.

まず, 2 章で計算したフーリエ係数 a_{p_0} (p_0: 小さい素数) を用意する.

I. $\langle A_i,f\rangle=\Omega(f)$ となるような $H^+(N)$ を生成する M-symbol たち A_i を計算する.

II. $\sum_{k=0}^{p_0-1}\{0,k/p_0\}$ を M-symbol たち A_i の和で書き, $n(p_0,f)$ を求める.

III. 素数 p に対して, 式 $(*)$ より変形して得られる

$$a_p=1+p-\frac{n(p,f)(1+p_0-a_{p_0})}{n(p_0,f)}$$

を使って, フーリエ係数 a_p を求める. 但し, $n(p,f)$ は II. の手順で求めればよい.

6. 周期格子 Λ_f の決定

この章では, 前章までに求めたフーリエ係数を使うことによって, ランク 2 の離散部分群 Λ_f ($\subset\mathbb{C}$) の計算を行いたい.

6.1. いくつかの準備. $\gamma_1,\gamma_2,\dots,\gamma_{2g}$ を $H_1(X_0(N),\mathbb{Z})$ の $\mathbb{Z}$ 上の基底とし, この基底を用いて, $H(N)$ を $\mathbb{Q}$ 上の縦ベクトルのなす空間と同一視し, その双対は横ベクトルであらわされるものとする.

(1). 各 rational newform f に対して, Hecke 作用素と Fricke involution に関しては同じ固有値を持ち, $*$-作用素による固有値がそれぞれ 1 と -1 となるもの (横ベクトル) を次のようにおく

$$v^+,\ v^-.$$

(2). $\exists\gamma^\pm\in H^\pm(N)$ (縦ベクトル) で, 次を満たすものを固定する

$$v^+\cdot\gamma^+=v^-\cdot\gamma^-=1.$$

(3). $\mathbb{R}$ の元 x, y を次で定める

$$x = \langle \gamma^+, f \rangle, \ y = -i\langle \gamma^-, f \rangle.$$

このとき, 以下の事実が成立する.

Type 1: $v^+ \equiv v^- \pmod 2$ のとき (実の連結成分が 1 個)

$\Longrightarrow$ 周期は $\omega_1 = 2x$, $\omega_2 = x + yi$ となる.

Type 2: $v^+ \not\equiv v^- \pmod 2$ のとき (実の連結成分が 2 個)

$\Longrightarrow$ 周期は $\omega_1 = x$, $\omega_2 = yi$ となる.

Example 6.1. (Example 5.1. の続き)

M-symbol $A = (2:1)$, $B = (3:1)$ を用いて, modular 曲線 $X_0(11)$ のホモロジーは $H_1(X_0(11), \mathbb{Q}) \simeq H(11) \simeq \langle A, B \rangle$ で与えられていた. $*$ の M-symbol への作用は明らかに, $(c) \mapsto (-c)$ で与えられるので, $A^* = A$, $B^* = A - B$ が分かる. よって, A と B に関して, この作用 $*$ を行列表示すると $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$ となるので, 左固有ベクトル $v^\pm$ は

$$v^+ = (2, 1), \ v^- = (0, 1)$$

で与えられる. よって, 周期格子 Λ_f は **Type 1** であることが分かった.

6.2. **x と y の計算.** この節では, x と y を求めるふたつの方法, direct method と indirect method とを紹介し, 周期格子 Λ_f を計算したい.

6.2.1. *direct method (L-関数を使わない).* $\langle \gamma, f \rangle = (v^+ \cdot \gamma)x + (v^- \cdot \gamma)yi$ が成立するので, あるひとつのサイクル γ で, $v^+ \cdot \gamma$ と $v^- \cdot \gamma$ がともに non-zero なものを選んで, $\langle \gamma, f \rangle$ を計算すれば, x と y が求まる.

記号

$$I_f(\alpha, \beta) = \int_\alpha^\beta 2\pi i f(z) dz, \qquad I_f(\alpha) = I_f(\alpha, \infty)$$

ここで, $I_f(\alpha, M(\alpha)) = I_f(\alpha) - I_f(M(\alpha))$ と書け, この積分は基点 α の取り方には依存しないことが示せる. この f と経路 $\{\alpha, M(\alpha)\}$ による周期を $P_f(M)$ と書くことにする. この周期 $P_f(M)$ の近似計算の方法を紹介するのが, この小節の目的である. 周期 $P_f(M)$ を近似計算するのに, 次の lemma は強力である.

Lemma 6.2. *$f = \sum a_n e^{2\pi i n z}$ ($z = x + iy \in \mathbb{H}$) を重み 2 の cusp form とすると, $z_0 = x_0 + iy_0 \in \mathbb{H}$ に対して, 次が成立する*

$$I_f(z_0) = \int_{z_0}^\infty 2\pi i f(z) dz = -\sum_{n=1}^\infty \frac{a_n}{n} e^{2\pi i n x_0} e^{-2\pi n y_0}.$$

証明は単に, 各項ごとの積分を実行することによって得られている. 積分 $I_f(z_0)$ は, 和が $e^{-2\pi n y_0}$ の形で展開されているので, ある程度の数のフーリエ級数 a_n を求めて代入すれば, 良い近似が得られる.

Tingley の方法

上の lemma において, $e^{-2\pi n y_0}$ に注目すれば, y_0 が大きければ大きいほど, はやく収束する. 収束をはやめるために, 与えられた M に対して Tingley は (うまい) 基点 α を次のように選んだ

$$\alpha = \frac{-d+i}{cN}, \quad M(\alpha) = \frac{a+i}{cN}.$$

但し, ここで, $M = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N)$ とおいた. 代入すると以下が得られる.

Proposition 6.3. 上の状況において, 次が成立する

$$\begin{aligned} P_f(M) =& I_f(\frac{-d+i}{cN}) - I_f(\frac{a+i}{cN}) \\ =& \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-2\pi n/cN}(e^{2\pi i n a/cN} - e^{-2\pi i n d/cN}). \end{aligned}$$

♡ x と y の計算の仕方 (direct method)

あるひとつのサイクル $\gamma = \{\alpha, M(\alpha)\}$ で, $v^+ \cdot \gamma$ と $v^- \cdot \gamma$ がともに non-zero なものを選んで, $P_f(M) = \langle \gamma, f \rangle$ を計算すれば

$$x = \frac{\Re(P_f(M))}{v^+ \cdot \gamma}, \qquad y = \frac{\mathrm{Im}\,(P_f(M))}{v^- \cdot \gamma}$$

によって, x と y が求まる. この小節では, $P_f(M)$ を e^{-ny} 型の収束のはやい級数で表示する方法を紹介した.

6.2.2. *indirect method (L-関数を使う).* 比 $L(f,1)/\Omega(f)$ の値は, 前章において, 求めて分かっているので, $L(f,1)$ の値から, 実周期 $\Omega(f)$ を求めようというのが, この小節の目的である. また, $L(f,1) = 0$ となるときや虚周期を求めるためには, 2 次指標 χ でひねった $L(f \otimes \chi, 1)$ を使うことになる.

$L(f,1) \neq 0$ のとき

rational newform f に対して, $L(f,1) \neq 0$ となるときの実周期 $\Omega(f)$ を求める方法を紹介する. なお, L-関数の値自体について言えば, ここで用いられる方法によって, ある程度の数のフーリエ係数 a_n から, 非常に精度の良い $L(f,1)$ の近似値を求められることになる.

rational newform f に対して, $\epsilon_N = \pm 1$ を Fricke involution W_N に関する固有値とする. このとき, 以下のようにして, $L(f,1)$ を計算していく

$$\begin{aligned} L(f,1) = -\int_0^{i\infty} 2\pi i f(z)dz =& I_f(\infty, 0) \\ =& I_f(\infty, i/\sqrt{N}) + I_f(i/\sqrt{N}, 0) \\ =& I_f(\infty, i/\sqrt{N}) + \epsilon_N I_f(i/\sqrt{N}, \infty) \\ =& (\epsilon_N - 1) I_f(i/\sqrt{N}). \end{aligned}$$

ここで, $L(f,1) \neq 0$ と仮定していたので, $L(f,1) = -2I_f(i/\sqrt{N})$ となる. この値の精度の良い近似値を求めるのに, lemma 6.2 を使う.

Proposition 6.4. $f = \sum_{n=1}^{\infty} a_n e^{2\pi n z}$ と書き, $f \mid W_N = -f$ を満たすならば, $L(f,1)$ は次の表示を持つ

$$L(f,1) = 2\sum_{n=1}^{\infty} \frac{a_n}{n} e^{-2\pi n/\sqrt{N}}.$$

$L(f,1)$ を定義に従って, 計算しようとすると $L(f,1) = \sum a_n/n$ となり, 収束がおそい. 一方で, 上の Proposition における表示によると, $e^{-2\pi/\sqrt{N}}$ による級数展開になっているので, いかに, 収束のはやい表示が得られたかが分かる.

Remark 6.5. 上の変形において, Fricke involution を巧みに使うことで, $I_f(i/\sqrt{N}, 0)$ の計算を $\epsilon_N I_f(i/\sqrt{N}, \infty)$ の計算に置き換えて, $e^{-2\pi/\sqrt{N}}$ 型の収束のはやい表示が得られたということを注意しておく (朝倉先生に教わった).

Example 6.6. (Example 6.1. の続き)

modular 曲線 $X_0(11)$ のホモロジーは $H_1(X_0(11), \mathbb{Q}) \simeq H(11) \simeq \langle A, B\rangle$ で与えられており, さらに, Example 5.1. において, $A \simeq \{0, 1/2\}$ を使うことによって, 次が得られていた

$$(*) \qquad \frac{L(f,1)}{\Omega(f)} = \frac{1}{5}.$$

一方で, Example 6.1. より, Λ_f は **Type 1** であることが分かったので, $(\omega_1, \omega_2) = (2x, x+iy)$ となり

$$\omega_1 = \Omega(f) = 5L(f,1)$$

が分かる．ここで, Example 5.1. で計算した $n=16$ までのフーリエ係数 a_n と上の Proposition 6.4. を使って, $L(f,1)$ を近似計算すると

$$\begin{aligned}L(f,1)\sim 2\cdot\{&\frac{1}{1}\cdot(0.15)+\frac{-2}{2}\cdot(0.15)^2+\frac{-1}{3}\cdot(0.15)^3+\frac{2}{4}\cdot(0.15)^4\\&+\frac{1}{5}\cdot(0.15)^5+\frac{2}{6}\cdot(0.15)^6+\frac{-2}{7}\cdot(0.15)^7+\frac{0}{8}\cdot(0.15)^8\\&+\frac{-2}{9}\cdot(0.15)^9+\frac{-2}{10}\cdot(0.15)^{10}+\frac{1}{11}\cdot(0.15)^{11}+\frac{-2}{12}\cdot(0.15)^{12}\\&+\frac{4}{13}\cdot(0.15)^{13}+\frac{4}{14}\cdot(0.15)^{14}+\frac{-1}{15}\cdot(0.15)^{15}+\frac{-4}{16}\cdot(0.15)^{16}\}\\&=0.2538418608559\cdots\quad(\text{但し, }e^{-2\pi/\sqrt{11}}\text{を }0.15\text{ として計算})\end{aligned}$$

となり, 急速に収束しているのが分かる．よって, 最終的には, 次のように, 実周期の近似値が得られることになる

$$\omega_1=\Omega(f)\sim 1.269209304279\cdots.$$

一般のとき

ここでは, $L(f,1)=0$ のときや, 虚周期を計算するために, 2 次指標 χ を使って, $L(f,1)$ の variation $L(f\otimes\chi,1)$ を考える．l をレベル N を割らない奇素数とし, χ を l を法とした 2 次指標とする．つまり, $\chi(\cdot)=(\cdot/l)$ (ルジャンドル記号) とする．このとき

$$(f\otimes\chi)=\sum_{n=1}^{\infty}\chi(n)a_n e^{2\pi inz}\in S_2(Nl^2)$$

とし, さらに, L-関数の variation を次で定義する

$$L(f\otimes\chi,s)=(2\pi)^s\Gamma(s)^{-1}\int_0^{i\infty}(-iz)^s(f\otimes\chi)(z)\frac{dz}{z}.$$

Proposition 6.4. の variation として, 次の表示が得られ, 近似計算で強力なツールとなる．

Proposition 6.7. $\chi(-N)=-\epsilon_N$ のとき, $L(f\otimes\chi,1)$ は次のような表示を持つ

$$L(f\otimes\chi,1)=2\sum_{n=1}^{\infty}\frac{\chi(n)a_n}{n}e^{-2\pi n/l\sqrt{N}}.$$

次に, $L(f\otimes\chi,1)$ と周期とを結びつけて, $L(f,1)/\Omega(f)=n(p,f)/2(1+p-a_p)$ の variation を考えたい．まず, $\gamma_l=\sum_{k=0}^{l-1}\chi(k)\{0,k/l\}$ とおき, f との周期 $\langle\gamma_l,f\rangle$ を $P(l,f)$ と書く．このとき, 簡単な計算により

$$P(l,f)=\sqrt{\chi(-1)l}\cdot L(f\otimes\chi,1)$$

が成立する．$*$-作用素に対して, $(\gamma_l)^*=\chi(-1)\gamma_l$ がなりたつので, $\chi(-1)=\pm1$ で場合分けを実行する．

ア). $\underline{x\text{ の決定 }(\chi(-1)=1\text{ のとき})}$

このとき, $\chi(-1)=1$ より, $(\gamma_l)^*=\gamma_l$ となるので, $\gamma_l \in H^+(N)$ が分かる. よって, $P(l,f)$ は実周期 $\Omega_0(f)$ の整数倍になり, 結局, $m^+(l,f)x$ ($m^+(l,f)$ は整数) という形になる. つまり, $m^+(l,f)$ が non-zero ならば, x は以下のようにして, 求めることができる

$$x=\sqrt{l}\ \frac{L(f\otimes\chi,1)}{m^+(l,f)}=\frac{P(l,f)}{m^+(l,f)}.$$

イ). $\underline{y\text{ の決定 }(\chi(-1)=-1\text{ のとき})}$

このとき, $\chi(-1)=-1$ より, $(\gamma_l)^*=-\gamma_l$ となるので, $\gamma_l \in H^-(N)$ が分かる. 上と同様の理由により, ある整数 $m^-(l,f)$ が存在して, $P(l,f)=m^-(l,f)yi$ と書けることになる. つまり, $m^-(l,f)$ が non-zero ならば, y は以下のようにして, 求めることができる

$$y=\sqrt{l}\ \frac{L(f\otimes\chi,1)}{m^-(l,f)}=\frac{P(l,f)}{im^-(l,f)}.$$

Remark 6.8. f のレベル N が perfect square でないときは, Murty-Murty の結果より, $m^+(l,f)$ も $m^-(l,f)$ も non-zero となる素数 l が存在することは保証されている. しかし, N が perfect square のときは, 関数等式の符号により, どちらか一方は常に 0 になる. 実際, $N=49$ のときには, 常に, $m^-(l,f)=0$ となり, y を求めることはできない ([C, Appedix, Example 4: N=49] を参照). このため, レベル N が perfect square のときは, 前小節の direct method を使うしかない.

Example 6.9. (Example 6.6. の続き)

modular 曲線 $X_0(11)$ のホモロジーは $H_1(X_0(11),\mathbb{Q}) \simeq H(11) \simeq \langle A,B\rangle$ で与えられており, さらに, Example 6.6. において, $H^+(11)$ の生成元 A を使うことによって, 実周期 ω_1 を求めた. ここでは, 虚周期 y (i.e. ω_2) を求めるために, $l\equiv 3 \pmod 4$ となる素数 l を使って, 上のイ). の方法で y を求めたい. 奇素数 l として, $l=3$ をとれば,

$$\gamma_3=\bigl\{0,\frac{1}{3}\bigr\}-\bigl\{0,\frac{-1}{3}\bigr\}=(3)-(-3)=-A+2B\neq 0$$

となり, $m^-(3,f)\neq 0$ が分かるので, イ). の方法が使える. 整数 $m^-(3,f)$ を求めるには, 上の γ_3 を $H^-(11)=H(11)/H^+(11)$ に射影し, $H^-(11)$ の生成元の何倍になっているかを見ればよい. $H^+(11)\simeq\langle A\rangle$ だったので, 明らかに, B の係数 2 が $m^-(3,f)$ になりそうだが, きちんと式を書いて求めることにする. 上のサイクル γ_3 は縦ベクトル ${}^t(-1,2)$ であらわされ, 横ベクトル $v^-=(0,1)$ との内積が $m^-(3,f)$ を与え, 実際に, $m^-(3,f)=2$ となる. よって, 上のイ). より, 次の式が得られる

$$y=\frac{1}{2i}P(3,f)=\frac{\sqrt{3}}{2}L(f\otimes 3,1).$$

後は Proposition 6.7. と $n=16$ までのフーリエ係数 a_n を使って, $L(f\otimes 3,1)$ の近似値を求めれば

$$\begin{aligned}
L(f\otimes 3,1) \sim 2\cdot\bigl\{&1\cdot\frac{1}{1}\cdot(0.53)-1\cdot\frac{-2}{2}\cdot(0.53)^2+0\cdot\frac{-1}{3}\cdot(0.53)^3\\
&+1\cdot\frac{2}{4}\cdot(0.53)^4-1\cdot\frac{1}{5}\cdot(0.53)^5+0\cdot\frac{2}{6}\cdot(0.53)^6\\
&+1\cdot\frac{-2}{7}\cdot(0.53)^7-1\cdot\frac{0}{8}\cdot(0.53)^8+0\cdot\frac{-2}{9}\cdot(0.53)^9\\
&+1\cdot\frac{-2}{10}\cdot(0.53)^{10}-1\cdot\frac{1}{11}\cdot(0.53)^{11}+0\cdot\frac{-2}{12}\cdot(0.53)^{12}\\
&+1\cdot\frac{4}{13}\cdot(0.53)^{13}-1\cdot\frac{4}{14}\cdot(0.53)^{14}+0\cdot\frac{-1}{15}\cdot(0.53)^{15}\\
&+1\cdot\frac{-4}{16}\cdot(0.53)^{16}\bigr\}\\
=&1.6845\cdots \quad (\text{但し, } e^{-2\pi/3\sqrt{11}}\text{を } 0.53 \text{ として計算})
\end{aligned}$$

となり, $y\sim 1.4588\cdots$ が分かる. 周期格子 Λ_f は **Type 1** だったので, $\omega_2=x+yi$ となり, その値は

$$\omega_2 \sim 0.634604652139\cdots + 1.4588\cdots i$$

で与えられることが分かった.

♡ x と y の計算の仕方 (indirect method)

$L(f,1)/\Omega(f)$ の値は 5 章で求めたので, $L(f,1)\neq 0$ ならば, $L(f,1)$ をある程度の数のフーリエ係数 a_n を使って, 近似計算し, そこから, 実周期 $\Omega(f)$ の近似値が得られた. 一般には, うまく奇素数 l を選んで, $L(f\otimes l,1)$ の近似計算を行うことで, 実周期も虚周期も求めることができた.

♣ 周期格子Λ_fの計算の仕方 (まとめ)

I. $*$-作用素の行列表示を求め, 固有値が ±1 の左固有ベクトル $v^{\pm}$ を計算する. これによって, Λ_f の **Type** を決定する.

Type 1 $\Longrightarrow$ $\omega_1=2x$, $\omega_2=x+yi$ が Λ_f の基底

Type 2 $\Longrightarrow$ $\omega_1=x$, $\omega_2=yi$ が Λ_f の基底

II. x と y の決定は L-関数を使わない direct method か, L-関数を使う indirect method による. ともに, 積分を e^{-nk} 型の級数で表示し, ある程度の数のフーリエ係数から, 近似値を求めるというものである.

7. 楕円曲線 E_f の方程式の決定

この章では, 6 章で計算した周期格子 Λ_f を用いることで, 楕円曲線 $E_f=\mathbb{C}/\Lambda_f$ の方程式を決定する.

不変量 c_4と c_6 $(\in \mathbb{Z})$

まず, ω_1/ω_2 あるいは ω_2/ω_1 のどちらかは上半平面の元になり, それを τ とおく. 次に, 上半平面上の変換によって, τ が $|\ \Re(\tau)\ | \leq 1/2$ かつ $|\ \tau\ | \geq 1$ となるように動かせるので, はじめから, τ がこの領域に含まれているとする. このとき, $q = e^{2\pi i\tau}$ とおき, 不変量 $c_4(= 12g_2)$ と $c_6(= 216g_3)$ を次のように定める

$$c_4 = \left(\frac{2\pi}{\omega_2}\right)^4 \left(1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1-q^n}\right),\ c_6 = \left(\frac{2\pi}{\omega_2}\right)^6 \left(1 - 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1-q^n}\right).$$

このとき, $|\ q\ | < 0.005$ より, これらの収束はかなりはやいと言える. E_f は $\mathbb{Q}$ 上定義されているので, c_4 と c_6 は有理数であることが分かる. さらに, 強く, Edixhoven の結果により, これらは整数になることが分かっている. よって, c_4 と c_6 に対して, 十分に精度の高い近似値を与えれば, その整数を見当付けることができる. さらに, c_4 と c_6 は導手 N の楕円曲線の不変量であるので

(1) $c_4^3 - c_6^2 = 1728\Delta$. ここで, Δ (判別式) は N で割り切れる整数,

(2) 5 以上の素数 p で N を割り切るものに対して $p \mid c_4 \iff p \mid c_6 \iff p^2 \mid N$,

(3) $c_6 \not\equiv 9 \pmod{27}$,

(4) $c_6 \equiv -1 \pmod 4$, or $c_4 \equiv 0 \pmod{16}$ かつ $c_6 \equiv 0,\ 8 \pmod{32}$ のどちらか

などの条件を満たし, これらから絞り込むことが可能である.

E_fの方程式の決定

$[a_1, a_2, a_3, a_4, a_6]$ によって, 楕円曲線 $E_f : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ をあらわすものとする. このとき, c_4, c_6 とこれらの係数との関係は

$$\begin{cases} b_2 = -c_6 \bmod 12 \in \{-5, \ldots, 6\}; \\ b_4 = (b_2^2 - c_4)/24; \\ b_6 = (-b_2^3 + 36b_2b_4 - c_6)/216; \\ a_1 = b_2 \bmod 2 \in \{0, 1\}; \\ a_3 = b_6 \bmod 2 \in \{0, 1\}; \\ a_2 = (b_2 - a_1)/4; \\ a_4 = (b_4 - a_1a_3)/2; \\ a_6 = (b_6 - a_3)/4 \end{cases}$$

で与えられるので, c_4 と c_6 から楕円曲線 E_f を決定できる. 今までの計算の総まとめとして, レベル 11 の rational newform f に付随する楕円曲線 E_f の方程式を求める.

Example 7.1. (Example 6.9. の続き)

周期格子 $\Lambda_f = \langle \omega_1, \omega_2 \rangle$ は, これまでの計算によって

$$\begin{aligned} \omega_1 &\sim 1.269209304279\cdots \\ \omega_2 &\sim 0.634604652139\cdots + 1.4588\cdots i \end{aligned}$$

で与えられることが分かっていた. これを c_4, c_6 を与える式に代入すると $c_4 \sim 495.99$, $c_6 \sim 20008.09$ という近似値 ($n = 16$ までのフーリエ係数 a_n だけで) が得られ, ともに整数であることより

$$c_4 = 496, \ c_6 = 20008$$

であることが予想される. ちなみに, $n = 100$ までのフーリエ係数 a_n だと $c_4 \sim 495.9999999999954$, $c_6 \sim 20008.0000000085$ となる. 実際に, この値で計算すると, 導手 11 の楕円曲線

$$y^2 + y = x^3 - x^2 - 10x - 20$$

となり, これで E_f の方程式が得られたことになる.

♣ 方程式 E_f の決定の仕方 (まとめ)

6 章で得られた ω_1 と ω_2 の近似値から c_4 と c_6 の近似値を求める. Edixhoven の結果より c_4 と c_6 は 整数 なので, この近似値より, 見当をつけ, それで計算し, 得られる不変量が導手 N の楕円曲線の不変量と矛盾しないかを確かめる.

総まとめ

1. M-sybmol で, 純代数的にホモロジーを決定する.
2. フーリエ係数 a_{p_0} (p_0 が小さい素数) を手計算する.
3. L-関数を通して, 他の素数 p に対するフーリエ係数 a_p を決定する.
4. フーリエ係数で L-関数を近似して, 周期の近似値を求める.
5. 不変量 c_4 と c_6 (整数になる) に周期を代入して, 見当をつける.

References

[C] Cremona, J.E.: *Algorithms for modular elliptic curves. Second edition.* Cambridge University Press, Cambridge, 1997. vi+376 pp.

Department of Mathematics, Hokkaido University, Sapporo 060-0810, Japan

E-mail address: morita@math.sci.hokudai.ac.jp