# 本田・テイト理論と
# モジュラー曲線のレフシェッツ数
# （レジュメ）

津嶋　貴弘

## 1　概要

本講演では最初に一般の形で本田・テイト理論の主定理を述べ、それを楕円曲線の場合に特化してより詳しく述べる。楕円曲線に対する本田・テイト理論に基づき、モジュラー曲線のレフシェッツ数を軌道積分を用いて表示する公式を紹介する。

## 2　本田・テイト理論について ([Ho], [Ta1], [Ta2])

### 2.1　主定理

任意の体 $k$ 上のアーベル多様体の圏は、$\mathrm{Hom}_k(A,B)$ が $\mathbb{Z}$ 上有限生成自由加群となる乗法的圏をなす。この圏を少し修正した圏 $M(k)$ を定義する。対象を $k$ 上のアーベル多様体とし、射を

$$\mathrm{Hom}_{M(k)}(A,B) = \mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$$

とおく。$M(k)$ における同型射 $f\colon A \to B$ を $\underline{k \text{ 上の同種}}$ と呼ぶ。故に $M(k)$ の同型類を理解することはアーベル多様体を $k$ 上同種を除いて理解することになる。$M(k)$ は半単純である。即ち、この圏の対象は単純な対象の有限個の積に $M(k)$ において同型である。アーベル多様体が単純であるとは、自明なもの以外の部分アーベル多様体を持たないことである。アーベル多様体の同種類を理解するためには以下の二つのことを理解すればよい。

- $k$ 上単純アーベル多様体の $k$ 上同種類の集合。
- $k$ 上単純アーベル多様体 $A$ の自己準同型環 $\mathrm{End}_{M(k)}(A)$.

以下では、この二つの事柄を $k$ が $\underline{\text{有限体}}$ の場合に理解する。これが本田・テイト理論の内容である。

　$k$ を標数 $p$, 位数 $q$ の有限体とする。$k$ 上定義された単純アーベル多様体 $A$ を考えて $\pi_A \in \mathrm{End}_k(A)$ を $A$ の $k$ 上フロベニウス自己準同型写像とする。曲線の場合のヴェイユ予想により、$\pi_A$ は代数的数であって全ての埋め込み $\iota\colon \mathbb{Q}(\pi_A) \hookrightarrow \mathbb{C}$ に対して、$|\iota(\pi_A)| = q^{1/2}$ が成立する。このような性質を持つ代数的数を $\underline{\text{ヴェイユ } q \text{ 数}}$ と呼ぶ。二つのヴェイユ $q$ 数 $\pi_1, \pi_2$ が $\underline{\mathbb{Q} \text{ 上共役である}}$ とは、$\pi_1 \mapsto \pi_2$ となる体の同型 $\mathbb{Q}(\pi_1) \simeq \mathbb{Q}(\pi_2)$ が存在することである。

　本田・テイト理論の主定理は次の通り。

**定理 2.1.** *(i)*　対応 $A \mapsto \pi_A$ は $k$ 上の単純アーベル多様体の同種類の集合とヴェイユ $q$ 数の $\mathbb{Q}$ 上共役類の集合の間の一対一対応を誘導する。
*(ii)*　$A$ を $k$ 上単純アーベル多様体とする。このとき、$\mathbb{Q}$ 代数

$$F = \mathbb{Q}(\pi_A) \subset D = \mathrm{End}_{M(k)}(A)$$

を考えると、$D$ は $F$ 上の中心斜体である。更に、$F$ の各実素点で $D$ は分裂しない。$F$ の $p$ の上に無い任意の有限素点で $D$ は分裂する。更に $v$ を $p$ の上にある $F$ の有限素点とすると、$D$ の $v$ でのハッセ不変量が次の公式で与えられる。

$$\mathrm{inv}_v(D) \equiv \frac{v(\pi_A)}{v(q)}[F_v : \mathbb{Q}_p] \pmod 1. \tag{2.1}$$

但し $v(\cdot)$ は、$F_v$ の任意の素元で 1 となる正規化された離散付値とする。以上の条件で $D$ は唯一つに特徴付けられる。更に

$$2 \dim A = [D : F]^{1/2}[F : \mathbb{Q}] \tag{2.2}$$

が成り立つ。

**注 2.2.** 公式 (2.1) の証明については [MW, Theorem 2 in II] を参照。

## 2.2 $A$ の唯一性と $\mathrm{End}_{M(k)}(A)$ の構造

以下では定理 2.1(i) の単射性について解説する。

$A$ を標数 $p$ の体 $k$ 上のアーベル多様体とする。素数 $\ell \neq p$ を取る。$A$ の $\ell$ 進テイト加群を $T_\ell A$ と書く。$V_\ell A = T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ とおく。$\mathbb{F}$ を $k$ の代数閉包とする。$T_\ell A$ に $G = \mathrm{Gal}(\mathbb{F}/k)$ が作用する。$A \in M(k)$ に対して、$V_\ell A$ 上の $\pi_A$ の特性多項式は $\ell$ によらず、$\mathbb{Z}$ 係数の $2 \dim A$ 次のモニック多項式となることが知られている。それを $f_A$ と書く。$\pi_A$ は代数体 $F = \mathbb{Q}(\pi_A)$ の整数環 $\mathcal{O}_F$ に含まれる。更に $\pi_A$ は $\mathbb{Q}$ 上半単純環 $D$ の中心に入るから $V_\ell A$ への作用は半単純である。$V_\ell A$ への $\pi_A$ の作用は $\mathrm{Frob}_q \in G$ の作用と一致することを注意しておく。テイトは次を示した。

**定理 2.3.** $k$ を有限体とする。このとき、任意の $k$ 上のアーベル多様体 $A$, $B$ に対して以下の自然な写像は同型を誘導する。

$$\mathrm{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_G(T_\ell A, T_\ell B).$$

上の命題は、単純アーベル多様体 $A$ についての次の自然な射

$$\alpha_\ell \colon \mathrm{End}_{M(k)}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to \mathrm{End}_G(V_\ell A) \tag{2.3}$$

の全単射性に帰着される。単射性 は $k$ が有限であることに依拠しない一般の体上のアーベル多様体に対して成立する事実である ([Mi, Lemma 10.6] を参照)。全射性 の証明には $k$ が有限であることを使う。定理 2.3 は アーベル多様体の場合のテイト予想 と同値であることを注意しておく。この定理の帰結として以下が成立する。

**定理 2.4.** $A$, $B$ を有限体 $k$ 上のアーベル多様体とする。$f_A$, $f_B$ をそれぞれ $A$, $B$ の $k$ 上フロベニウス自己準同型の特性多項式とする。

*(a)* 以下は同値である。

- $B$ は $A$ の $k$ 上定義された部分アーベル多様体に $k$ 上同種である。
- ある $\ell$ について $V_\ell B$ から $V_\ell A$ への $G$ 同変な単射がある。
- $f_B$ は $f_A$ を割り切る。

*(b)* 以下は同値である。

- $A$ と $B$ は $k$ 上同種である。
- $f_A = f_B$.

## 2.3 与えられたヴェイユ数からアーベル多様体を構成する

以下では、本田・テイト理論の定理 2.1(i) の全射性を示す。これは、[Ho] において示された。以下では、[Ta2] の議論に従う。本節の目標は、与えられたヴェイユ $q$ 数 $\pi$ に対して、そのフロベニウス自己準同型が $\pi$ と $\mathbb{Q}$ 上共役になるような $k$ 上のアーベル多様体 $A$ を構成することである。虚数乗法論を使って数体上のアーベル多様体を構成し、それの還元として欲しいアーベル多様体を作るというのがおおまかなアイデアである。証明中で志村・谷山公式を使う。

$\pi$ をヴェイユ $p^a$ 数とする。$\pi$ が効果的であるとは、$\mathbb{F}_{p^a}$ 上の単純アーベル多様体 $A$ が存在してそのフロベニウス自己準同型写像 $\pi_A$ と $\pi$ が $\mathbb{Q}$ 上共役であることとする。

**補題 2.5.** $N$ を 1 以上の整数とする。このとき、$\pi^N$ が効果的ならば $\pi$ も効果的である。

$F = \mathbb{Q}(\pi)$ とおく。定理 2.1(ii) において、$\pi_A$ を $\pi$ と取り替えて唯一つに定まる $F$ 上の中心斜体を $D$ と書く。総実体上の総虚二次拡大体を CM 体と呼ぶ。

**補題 2.6.** $F$ を含む *CM* 体 $L$ で次をみたすものが存在する。

- $[L:F] = [D:F]^{1/2}$
- $D$ は $L$ 上分裂する。

### 2.3.1 虚数乗法論

$L$ を CM 体とする。$\rho$ を $L$ の位数 2 の自己同型写像で、任意の埋め込み $L \hookrightarrow \mathbb{C}$ に対して複素共役と両立するものとする。$C$ を標数零の代数閉体とする。$\Phi$ を $\mathrm{Hom}(L, C)$ の部分集合で次をみたすものとする。

$$\Phi \sqcup \Phi\rho = \mathrm{Hom}(L, C).$$

組 $(L, \Phi)$ を CM 型と呼ぶ。$\mathcal{C}$ を $C$ の部分環とする。$\mathcal{C}$ 上のアーベルスキーム $\mathcal{A}$ が $(L, \Phi)$ 型であるとは、アーベル多様体 $A = \mathcal{A} \times_{\mathcal{C}} C$ に対して、ある埋め込み $L \hookrightarrow \mathrm{End}_{M(C)}(A)$ が存在して、$A$ の接空間 $t_A$ が $L$ の表現として $\bigoplus_{\varphi \in \Phi} \varphi$ と同型であることとする。このようなアーベルスキーム $\mathcal{A}$ を $(L, \Phi)$ 型のアーベルスキームと呼ぶ。$2 \dim A = [L : \mathbb{Q}]$ が成立する。

以下は志村・谷山の虚数乗法論 ([ST]) の帰結である。

**補題 2.7.** $C$ に含まれるある数体の整数環上定義された $(L, \Phi)$ 型のアーベルスキーム $\mathcal{A}$ が存在する。

以下では、$C$ を $\mathbb{Q}_p$ の代数閉包とする。$w$ を $p$ の上にある $L$ の素点とする。$\mathrm{Hom}_{\mathbb{Q}_p}(L_w, C)$ を $\mathrm{Hom}(L, C)$ の部分集合とみなし、$H_w$ と書く。$(L, \Phi)$ を CM 型とする。$\Phi_w = \Phi \cap H_w$ とおく。このとき、次の分解が成り立つ。

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{w|p} L_w.$$

更に次が成立する。

$$\mathrm{Hom}(L, C) = \bigcup_{w|p} H_w, \quad \Phi = \bigcup_{w|p} \Phi_w.$$

**補題 2.8.** **志村・谷山公式** $\mathcal{A}$ を $p$ 進体の整数環 $\mathcal{O}$ 上定義された $(L, \Phi)$ 型のアーベルスキームとする。$k_0$ を $\mathcal{O}$ の剰余体とし、位数を $q_0$ と書く。$A_0$ を $\mathcal{A}$ の還元とする。このとき、$L$ のある元 $\pi_0$ が存在して、埋め込み $L \hookrightarrow \mathrm{End}_{M(k_0)}(A_0)$ によるその像が $\pi_{A_0}$ と一致し、更に次が成り立つ。$p$ の上にある $L$ の各素点 $w$ に対して

$$\frac{w(\pi_0)}{w(q_0)} = \frac{|\Phi_w|}{|H_w|}. \tag{2.4}$$

### 2.3.2 全射性の証明

元の設定に戻り $\pi,\ q,\ D,\ F$ は全て前節の通りとする。$L$ は補題 2.6 の条件をみたす CM 体とする。

**主張 2.9.** 以下の等式をみたす *CM* 型 $(L,\Phi)$ が存在する。$p$ の上にある $L$ の各素点 $w$ に対して

$$\frac{w(\pi)}{w(q)}=\frac{|\Phi_w|}{|H_w|}. \tag{2.5}$$

この主張の CM 型 $(L,\Phi)$ に対して補題 2.7 を適用すると数体の整数環 $\mathcal{O}$ 上の $(L,\Phi)$ 型のアーベルスキーム $\mathfrak{A}$ を得る。$\mathcal{O}$ の $p$ の上にある素イデアル $\mathfrak{p}$ を一つ取り、底変換 $\mathfrak{A}_{\mathcal{O}_\mathfrak{p}}$ を $\mathcal{A}$ と書く。その還元を $A_0$ と書く。$\mathcal{O}_\mathfrak{p}$ の剰余体の位数を $q_0$ とし、補題 2.8 により存在が分かっている $\pi_0\in L$ を考える。この補題の主張より $\pi_0$ は勿論、効果的である。

**命題 2.10.** ある整数 $N,\ N_0$ が存在して $\pi^N=\pi_0^{N_0}$ が成り立つ。更に $\pi$ は効果的である。

**証明.** (2.4), (2.5) より

$$\frac{w(\pi)}{w(q)}=\frac{w(\pi_0)}{w(q_0)}\quad (w\mid p).$$

$q$ と $q_0$ を冪で取り替えることにより、$q=q_0$ であると仮定してよい。よって $p$ の上にある全ての $L$ の素点 $w$ に対して

$$w(\pi)=w(\pi_0)$$

が成り立つとしてよい。$\pi$ も $\pi_0$ も絶対値が $p$ 冪であるから $p$ の外の素点では $\pi$ も $\pi_0$ も単元である。更にすべての無限素点で絶対値が等しいから、結局 $\pi/\pi_0$ は $L$ の全ての素点で絶対値が 1 である。故に $\pi/\pi_0$ は 1 の冪根であることがわかる。よって必要ならば更に冪をとり、最初の主張を得る。$\pi_0$ が効果的だから $\pi_0^{N_0}$ も効果的であり、結果 $\pi^N$ が効果的とわかる。補題 2.5 より $\pi$ が効果的であることがわかり二つ目の主張が従う。 □

これより全射性がわかった。

## 2.4 楕円曲線に対する本田・テイト理論

後で楕円曲線の場合が必要なのでこの場合に特化して定理 2.1 を述べる。その後で楕円曲線の超特異性・通常性の概念を思い出し、以下の定理との関係を述べる。この節の基本文献は [Si] や [W, Chapter 4] である。また、[P] が非常に参考になった。

**定理 2.11.** $k$ は前定理の通りとする。$E$ を $k$ 上の楕円曲線とする。$\pi_E$ を $E$ の $k$ 上フロベニウス自己準同型とする。$f_E$ をその特性多項式とする。

*(a)* $D=\mathrm{End}_{M(k)}(E)$ は $F=\mathbb{Q}(\pi_E)$ 上の中心斜体である。更に次が成立する。

$$[D:\mathbb{Q}]=2 \text{ または } 4.$$

*(b)* 以下の条件は同値である。

- $[D:\mathbb{Q}]=2.$
- $f_E$ が重根を持たない。
- $D=F.$
- $D$ は可換である。

*(c)* 以下の条件は同値である。

- $[D:\mathbb{Q}]=4$.
- $f_E$ が一次式の二乗になる。
- $F=\mathbb{Q}$.
- $D$ は $p$ と $\infty$ でのみ分岐する $\mathbb{Q}$ 上の *quaternion algebra* に同型である。

**補題 2.12.** $E$ を有限体 $k=\mathbb{F}_q$ 上の楕円曲線とする。
1. 次が成り立つ。

$$f_E=f_E(X)=X^2-a_q(E)X+q,\quad a_q(E)=q+1-|E(\mathbb{F}_q)|. \tag{2.6}$$

また、$|a_q(E)|\le 2\sqrt{q}$ が成立する。
2. $F=\mathbb{Q}(\pi_E)\neq\mathbb{Q}$ ならば $F$ は $\mathbb{Q}$ 上の総虚二次拡大体である。

**定義 2.13.** $k$ の代数閉包を $\mathbb{F}$ と書く。
1. $k$ 上の楕円曲線 $E$ が <u>通常である</u> とは、$\mathrm{End}_{M(\mathbb{F})}(E)$ が可換であることとする。
2. $k$ 上の楕円曲線 $E$ が <u>超特異である</u> とは、$E$ が通常でないこととする。

次の同値性はよく知られている。

**補題 2.14.** $E$ を $k$ 上の楕円曲線とする。以下は同値である。

- $E$ は超特異である。
- $a_q(E)\equiv 0 \pmod{p}$.

楕円曲線 $E$ が通常ならば定理 2.11 において $(b)$ の場合になる。但し、$(b)$ だからといって $E$ が通常であるとは限らない。以下の演習問題 2.17 を参照。一方で、$(c)$ の条件をみたすならば、楕円曲線 $E$ は超特異になる。

**補題 2.15.** $E$ を $k$ 上の楕円曲線とする。
1. 以下の条件は同値である。

- $E$ は超特異である。
- ある自然数 $n$ が存在して $\pi_E^n\in\mathbb{Q}$ である。

2. 以下の条件は同値である。

- $E$ は通常である。
- $D=F$ かつ $F$ において $p$ は分裂する。

この同値条件を満たすとき、$(p)=\mathfrak{p}\mathfrak{p}'$ $(\mathfrak{p}\neq\mathfrak{p}')$ とおくと、$v_{\mathfrak{p}}(\pi_E)$, $v_{\mathfrak{p}'}(\pi_E)$ の内のいずれかは零になる。

**系 2.16.** $E$ を $k$ 上の楕円曲線とする。このとき、代数体 $F=\mathbb{Q}(\pi_E)$ の $p$ の上にある素点 $v$ で $\pi_E$ の付値 $v(\pi_E)$ が正となるものが唯一つ存在する。

**演習問題 2.17.** 次のアフィン方程式を持つ $\mathbb{F}_3$ 上の楕円曲線 $E_1$, $E_2$ を考える。

$$E_1\colon x^3-x=y^2,$$
$$E_2\colon x^3-x=y^2-1.$$

1. $f_{E_1}$, $f_{E_2}$ を求めよ。その結果、$E_1$, $E_2$ は定理 2.11 $(b)$ の場合になることを確認せよ。
2. $E_1$, $E_2$ は超特異楕円曲線であることを示せ。
3. イデアル (3) は $F_1=\mathbb{Q}(\pi_{E_1})$ で分岐することを確認せよ。
4. $(E_1)_{\mathbb{F}_{3^2}}$ は定理 2.11 $(c)$ の場合になり、$(E_2)_{\mathbb{F}_{3^2}}$ は定理 2.11 $(b)$ の場合になることを確認せよ。
5. $E_1$ と $E_2$ は $\mathbb{F}_{3^2}$ 上同種にならないことを示せ。また $\mathbb{F}_{3^3}$ 上同型であることを示せ。

**演習問題 2.18.** 1. 定理 2.11(*b*) の場合となる $\mathbb{F}_q$ 上の超特異楕円曲線 $E$ で $(p)$ が代数体 $F=\mathbb{Q}(\pi_E)$ で素イデアルであるような例を挙げよ。
2. 通常楕円曲線の例を挙げよ。

本田・テイト理論を楕円曲線の場合に特化して、[Sch, Theorem 10.4] の形にまとめる。その前に簡単に楕円曲線の 1 次クリスタリンコホモロジーについてまとめる。$E$ を $\mathbb{F}_q$ 上の楕円曲線とする。$q=p^r$ と書く。$\mathbb{Q}_p$ の不分岐 $r$ 次拡大体を $\mathbb{Q}_q$ と書く。その整数環を $\mathbb{Z}_q$ と書く。$\sigma\in\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$ を $p$ 乗フロベニウス自己同型写像の持ち上げとする。$E$ の 1 次クリスタリンコホモロジー $H_p=H^1_{\mathrm{cris}}(E/\mathbb{Z}_q)$ は階数 2 の $\mathbb{Z}_q$ 上自由加群である。更に二つの $\sigma$-線型写像 $F$ (i.e. $F(xv)=x^\sigma F(x)$ $(x\in\mathbb{Z}_q,\ v\in H_p)$) と $\sigma^{-1}$-線型写像 $V$ を持ち、$F\circ V=V\circ F=p$ をみたす。同型 $H_p\otimes_{\mathbb{Z}_q}\mathbb{Q}_q\simeq\mathbb{Q}_q^2$ を一つ固定する。$F$ は $\sigma$ 線型なので、ある $\delta\in GL_2(\mathbb{Q}_q)$ が存在して、$F=\delta\sigma$ と書ける。

**定理 2.19.** $\mathbb{F}_q$ を標数 $p$ の有限体とする。$\ell\neq p$ とし、$q=p^r$ と書く。
*1.* 任意の楕円曲線 $E/\mathbb{F}_q$ に対して、$H^1(E_{\bar{\mathbb{F}}},\mathbb{Q}_\ell)$ 上のフロベニウス作用は半単純である。その特性多項式 $\pi_E\in\mathbb{Z}[T]$ は $\ell$ によらない。更に、$F$ が $H^1_{\mathrm{cris}}(E/\mathbb{Z}_q)\otimes_{\mathbb{Z}_q}\mathbb{Q}_q$ に $\delta\sigma$ で作用しているとすると、$N\delta=\delta\sigma(\delta)\cdots\sigma^{r-1}(\delta)$ は半単純であって、その特性多項式は $\pi_E$ に等しい。
*2.* $\gamma_E\in GL_2(\mathbb{Q})$ は半単純元で、その特性多項式が $\pi_E$ であると仮定する。
*(a).* 以下の三条件をみたす $GL_2(\mathbb{Q})$ の半単純元 $\gamma$ の共役類の集合 $\mathfrak{S}$ を考える。

- $\gamma$ の特性多項式が $X^2-aX+q\in\mathbb{Z}[X]$ と書ける。
- $\gamma$ の $GL_2(\mathbb{R})$ における像 $\gamma_\infty$ が楕円的である *(i.e.* $\gamma_\infty$ の最小多項式が $\mathbb{R}$ 上既約であること。*)*
- $\gamma$ の根 $\pi$ を取る。代数体 $\mathbb{Q}(\pi)$ の有限素点 $v$ で $v(\pi)>0$ なるものが唯一つ存在する。

このとき、対応 $E\mapsto\gamma_E$ は $\mathbb{F}_q$ 上の楕円曲線の同種類の集合と $\mathfrak{S}$ との間の一対一対応を与える。
*(b).* $G_{\gamma_E}$ を $\gamma_E$ の中心化群とする。次が成立する。

$$(\mathrm{End}_{M(\mathbb{F}_q)}(E)\otimes_{\mathbb{Q}}\mathbb{Q}_\ell)^\times\simeq G_{\gamma_E}\otimes\mathbb{Q}_\ell\quad(\ell\neq p),$$
$$(\mathrm{End}_{M(\mathbb{F}_q)}(E)\otimes_{\mathbb{Q}}\mathbb{Q}_p)^\times\simeq G_{\delta\sigma}(\mathbb{Q}_q)=\{y_p\in GL_2(\mathbb{Q}_q)\mid y_p^{-1}\delta y_p^\sigma=\delta\}.$$

**演習問題 2.20.** $f(X)=X^2-2X+8$ を特性多項式に持つ $GL_2(\mathbb{Q})$ の半単純元 $\gamma$ を考える。$f(X)=0$ の根 $\pi$ はヴェイユ 8 数であるが、本田・テイト理論の意味でこれに対応するアーベル多様体の次元は 3 であることを示せ。また、$\gamma$ は定理 2.19 の $(a)$ の三条件のうち最初の二つを満たすが、最後の条件を満たさないことを確認せよ。

# 3 有理点の個数を勘定する ([Cl, §3], [Ko, §16], [Sch, §5])

## 3.1 ヘッケ対応と問題設定 ([Ko, §6])

ヘッケ対応について復習する。

$p$ を素数とする。$\mathbb{A}_f^p$ を $p$ の部分が自明な $\mathbb{Q}$ の有限アデール環とする。$\widehat{\mathbb{Z}}^p=\prod_{\ell\neq p}\mathbb{Z}_\ell$ を $\mathbb{A}_f^p$ の整数環とする。$\mathbb{A}_f^p=\widehat{\mathbb{Z}}^p\otimes_{\mathbb{Z}}\mathbb{Q}$ が成り立つ。$K^p$ を $GL_2(\mathbb{A}_f^p)$ の開コンパクト部分群とする。後に $K^p$ は

$$K(N)=\{g\in GL_2(\widehat{\mathbb{Z}}^p)\mid g\equiv 1\pmod N\},\quad (p,N)=1,\quad N\geq 3$$

ととる。$GL_2(\mathbb{Z}_p)K^p$ レベル構造を有するモジュラー曲線を $X_{K^p}$ と書くことにする。以下では $X_{K^p}$ が $p$ で良い還元を持つので、還元して $\mathbb{F}_p$ 上のスキームとみなす。$g\in GL_2(\mathbb{A}_f^p)$ を一つ固定する。これは次のヘッケ対応を誘導する。

$$X_{K^p}\xleftarrow{a}X_{K_g^p}\xrightarrow{b}X_{K^p}.\tag{3.1}$$

但し、ここで $K^p_g = K \cap gK^pg^{-1}$ とおく。射 $a$ は包含写像 $g^{-1}K^p_g g \subset K^p$ から誘導される被覆写像 $X_{g^{-1}K^p_g g} \to X_{K^p}$ と、同型 $K^p_g \xrightarrow{\sim} g^{-1}K^p_g g;\ h \mapsto g^{-1}hg$ が誘導する同型 $X_{K^p_g} \xrightarrow{\sim} X_{g^{-1}K^p_g g}$ の合成とする。射 $b$ は単に包含写像 $K^p_g \subset K^p$ が誘導する被覆写像 $X_{K^p_g} \to X_{K^p}$ とする。このヘッケ対応 (3.1) を $f$ と書く。

$X_{K^p}$ 上の $p$ 乗フロベニウス自己準同型写像 $\Phi_p$ を考える。$q = p^r$ に対して $\Phi_p^r$ を単に $\Phi_q$ と書く。「合成 $\Phi_q \circ f$ $(q = p^r)$ の固定点」を勘定する。この合成の意味を説明する。写像 $\Phi_q$ とヘッケ対応 $f$ の合成は次のヘッケ対応になる。

$$X_{K^p} \xleftarrow{a} X_{K^p_g} \xrightarrow{c} X_{K^p}.$$

但し、ここで $c$ は合成 $\Phi_q \circ b$ である。合成 $\Phi_q \circ f$ の固定点とは、$X_{K^p_g}(\mathbb{F})$ の元であって $a$ と $c$ の像が一致するもののこととする。

有限体 $k$ 上の楕円曲線 $E$ に対して

$$H^1(E_{\mathbb{F}}, \widehat{\mathbb{Z}}^p) = \prod_{\ell \neq p} H^1(E_{\mathbb{F}}, \mathbb{Z}_\ell), \quad H^1(E_{\mathbb{F}}, \mathbb{A}^p_f) = H^1(E_{\mathbb{F}}, \widehat{\mathbb{Z}}^p) \otimes_{\mathbb{Z}} \mathbb{Q}$$

とおく。

$K^p$ を $GL_2(\mathbb{A}^p_f)$ の任意の開コンパクト部分群とする。以下ではモジュラー曲線 $X_{K^p}$ の $\mathbb{F}$ 有理点は組 $(E, \eta)$ の以下の意味の同種類とする。$E$ は $\mathbb{F}$ 上の楕円曲線とし、$\eta$ はある同型 $\eta_0 \colon (\mathbb{A}^p_f)^2 \xrightarrow{\sim} H^1(E, \mathbb{A}^p_f)$ の $K^p$ 軌道の集合 $\{\eta_0 \circ x \mid x \in K^p\}$ とする。二つの組 $(E, \eta)$, $(E', \eta')$ が同種であるとは、ある $p$ と素な同種 $f \colon E \to E'$ が存在して $\eta = f^* \circ \eta'$ となることとする。このような点の解釈の下で、ヘッケ作用素 $\Phi_q \circ f$ の固定点 $(E, \eta) \in X_{K^p_g}(\mathbb{F})$ は $E$ が $\mathbb{F}_q$ 上の楕円曲線であり、$\eta \circ g \equiv \pi_E \circ \eta \pmod{K^p}$ をみたすもののことである (cf. [Ko, p.429 の最終段落])。

この固定点の個数を計算することが次の節の目標である。

$\ell$ を $p$ と異なる素数とする。$GL_2(\mathbb{A}^p_f)$ の連続 $\ell$ 進表現 $\xi$ を考える。これは $X_{K^p}$ 上のスムーズ $\ell$ 進層 $\mathscr{F}_{K^p}$ を誘導する。

## 3.2 レフシェッツ数

$m$ を $p$ と素な 3 以上の整数とする。

$$K^p = \{y \in GL_2(\widehat{\mathbb{Z}}^p) \mid g \equiv 1 \pmod{m}\}$$

とおく。この場合の $X_{K^p}$ はいわゆるフルレベル構造付きのモジュラー曲線 $X(m)$ と一致する。このことを $\mathbb{F}$ 有理点のところで復習する。$X(m)$ の $\mathbb{F}$ 有理点は $\mathbb{F}$ 上の楕円曲線 $E$ と同型 $\phi \colon (\mathbb{Z}/m)^2 \xrightarrow{\sim} E[m]$ の組の同型類 $(E, \phi)$ である。$\phi$ を同型 $\widetilde{\phi} \colon (\widehat{\mathbb{Z}}^p)^2 \to T^p_f E$ に持ち上げて $\otimes_{\mathbb{Z}} \mathbb{Q}$ すると同型 $(\mathbb{A}^p_f)^2 \xrightarrow{\sim} V^p_f E$ を得る。これの双対を取って同型 $(\mathbb{A}^p_f)^2 \simeq H^1(E, \mathbb{A}^p_f)$ を得る。これの $K^p$ 軌道を考えれば、軌道は $\widetilde{\phi}$ の取り方によらない。この軌道を $\eta_\phi$ と書くと対応 $(E, \phi) \mapsto (E, \eta_\phi)$ は全単射 $X_{K^p}(\mathbb{F}) \simeq X(m)(\mathbb{F})$ を誘導する。

$E_0$ を $\mathbb{F}_q$ 上の楕円曲線とする。$\mathscr{F}_{K^p}$ を $GL_2(\mathbb{A}^p_f)$ の有限次元表現 $\xi$ に対応するスムーズ層と仮定する。$g \in GL_2(\mathbb{A}^p_f)$ とする。以下のレフシェッツ数を計算したい。

$$T(E_0, \xi, g) = \sum_x \mathrm{tr}(\Phi_q \circ f;\ \mathscr{F}_x).$$

ここで、$x$ は $X_{K^p_g}$ の固定点 $(E, \eta)$ に対応し $E$ は $E_0$ に $\mathbb{F}_q$ 上同種であるもの全体を走る。この添字の集合を $\mathcal{M}_m(\mathbb{F}_q)(E_0)$ と書く。

$$H^p = H^1(E_{0,\mathbb{F}}, \mathbb{A}^p_f), \quad H_p = H^1_{\mathrm{cris}}(E_0/\mathbb{Z}_q) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$$

とおく。$x \in \mathcal{M}_m(\mathbb{F}_q)(E_0)$ を任意に取る。$H^p$ の基底を取ると、$H^p$ の自己同型写像 $\pi_{E_0}$ から元 $\boxed{\gamma \in GL_2(\mathbb{A}_f^p)}$ を得る。定理 2.19 の直前に述べた様に、$H_p$ の基底を取ると、$H_p$ 上のフロベニウス自己準同型写像 $F$ から等式 $F = \delta\sigma$ で特徴付けられる $\boxed{\delta \in GL_2(\mathbb{Q}_q)}$ が定まる。本田・テイト理論により、$E_0$ から決まる $\gamma_0 \in GL_2(\mathbb{Q})$ の $GL_2(\mathbb{A}_f^p)$, $GL_2(\mathbb{Q}_p)$ における像はそれぞれ $\gamma$, $N\delta$ と共役になる。同型 $(\mathbb{A}_f^p)^2 \simeq H^p$, $\mathbb{Q}_q^2 \simeq H_p$ を固定する。

**補題 3.1.** $\Gamma = (\mathrm{End}_{M(k)}(E_0))^\times$, $K_p = GL_2(\mathbb{Z}_q)$ とおく。

$$Y^p = \{y \in GL_2(\mathbb{A}_f^p)/K_g^p \mid y^{-1}\gamma y \in gK^p\}$$
$$Y_p = \left\{x \in GL_2(\mathbb{Q}_q)/K_p \mid x^{-1}\delta x^\sigma \in K_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K_p \right\}$$

とおくとき、$\mathcal{M}_m(\mathbb{F}_q)(E_0)$ は $\Gamma \setminus (Y^p \times Y_p)$ と自然に同一視される。

以下では写像

$$\mathcal{M}_m(\mathbb{F}_q)(E_0) \to \Gamma \setminus (Y^p \times Y_p)$$

の構成のみ与える。$x = (E_x, \phi) \leftrightarrow (E_x, \eta_\phi) \in \mathcal{M}_m(\mathbb{F}_q)(E_0)$ を考える。軌道 $\eta_\phi$ の元 $\widetilde{\phi}$ を一つとる。同種 $f\colon E_0 \to E_x$ を取る。$p$ の外をまず見る。次の可換図式で定まる $y^p \in GL_2(\mathbb{A}_f^p)$ を取る。

$$\begin{tikzcd}
(\mathbb{A}_f^p)^2 \arrow[r, "\widetilde{\phi}", "\simeq"'] \arrow[d, "y^p"] & H^1(E_{x,\mathbb{F}}, \mathbb{A}_f^p) \arrow[d, "f^*", "\simeq"'] \\
(\mathbb{A}_f^p)^2 \arrow[r, "\text{fixed}", "\simeq"'] & H^p.
\end{tikzcd}$$

すると $y^p K_g^p \in GL_2(\mathbb{A}_f^p)/K_g^p$ を得る。これは軌道の元 $\widetilde{\phi}$ の取り方によらない。固定点の定義の $\eta_\phi \circ g \equiv \pi_E \circ \eta_\phi \pmod{K^p}$ を考える。これを翻訳すると $y^p K_g^p \in Y^p$ を得る。

次に $Y_p$ の方を考える。次の状況を考える。

$$\mathbb{Q}_q^2 \simeq H_p \xleftarrow{f^*} H^1_{\mathrm{cris}}(E_x/\mathbb{Z}_q) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q. \tag{3.2}$$

最初の同型による $H_p$ の格子 $H^1_{\mathrm{cris}}(E_0/\mathbb{Z}_q)$ の $\mathbb{Q}_q^2$ における像を $\Lambda$ と書く。二つの同型 (3.2) を通じた $H^1_{\mathrm{cris}}(E_x/\mathbb{Z}_q)$ の $\mathbb{Q}_q^2$ における像は、ある元 $y_p K_p \in GL_2(\mathbb{Q}_q)/K_p$ が存在して $y_p\Lambda$ と書ける。この格子は $F$ と $V$ で安定であるため、$Fy_p\Lambda \subset y_p\Lambda$ かつ $Vy_p\Lambda \subset y_p\Lambda$ が成立する。この条件は $FV = p$ を用いると結局

$$py_p\Lambda \subset Fy_p\Lambda \subset y_p\Lambda$$

と書ける。$F = \delta\sigma$ だったから

$$p\Lambda \subset y_p^{-1}\delta y_p^\sigma \Lambda \subset \Lambda \tag{3.3}$$

を得る。ヴェイユペアリングは $H_p$ の $\mathbb{Q}_q$ 上の第二外積と $\mathbb{Q}_q(-1)$ の同型を導く。よって $v(\det(\delta)) = 1$ がわかる。$v(\det(y_p^{-1}\delta y_p^\sigma)) = 1$ を得る。するとカルタン分解より

$$y_p^{-1}\delta y_p^\sigma \in K_p \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} K_p$$

と書ける。これより $y_pK_p \in Y_p$ を得る。逆に $y_pK_p \in Y_p$ とすれば (3.3) をみたす。全単射性はエタール被覆の理論とデュドネ理論から従う。

既に前述の中心化部分群

$$G_\gamma(\mathbb{A}_f^p) = \{y \in GL_2(\mathbb{A}_f^p) \mid y^{-1}\gamma y = \gamma\},$$
$$G_{\delta\sigma}(\mathbb{Q}_p) = \{x \in GL_2(\mathbb{Q}_q) \mid x^{-1}\delta x^\sigma = \delta\}$$

を考える。$\boxed{f^p}$ を $gK^p$ の特性関数をこの群の体積で割った関数とする。$\boxed{\phi_{p,0}}$ を

$$GL_2(\mathbb{Z}_q)\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}GL_2(\mathbb{Z}_q)$$

の特性関数を $GL_2(\mathbb{Z}_q)$ の体積で割った関数とする。任意の $GL_2(\mathbb{A}_f^p)$ 上のコンパクト台を持つスムーズな関数 $f$ に対して軌道積分

$$O_\gamma(f) = \int_{G_\gamma(\mathbb{A}_f^p)\backslash GL_2(\mathbb{A}_f^p)} f(y^{-1}\gamma y)dy$$

を考える。$GL_2(\mathbb{Q}_q)$ 上のコンパクト台を持つ任意のスムーズ関数 $\phi$ に対して twisted 軌道積分

$$TO_{\delta\sigma}(\phi) = \int_{G_{\delta\sigma}(\mathbb{Q}_p)\backslash GL_2(\mathbb{Q}_q)} \phi(x^{-1}\delta x^\sigma)dx$$

も考える。以下の定理は [Sch, Corollary 5.2] と [Ko, (19.2)] にある。

**定理 3.2.** $g \in GL_2(\mathbb{A}_f^p)$ とする。このとき、次が成立する。

$$T(E_0, \xi, g) = \mathrm{vol}(\Gamma\backslash(\mathrm{End}(E_0)\otimes\mathbb{A}_f)^\times)O_\gamma(f^p)TO_{\delta\sigma}(\phi_r)\,\mathrm{tr}\,\xi(\gamma_0).$$

# References


[Cl] L. Clozel, *Nombre de points des variétés de Shimura sur un corps fini*, Séminaire Bourbaki (1992-1993) Exposé 766, 121–149.

[Ho] T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95.

[Ko] R. E. Kottwitz, *Points on some Shimura varieties over finite fields*, J. Amer. Math. Soc., **5** (1992), 373–444.

[Mi] J.S. Milne, *Abelian varieties*, in Course Notes in his homepage.

[MW] J.S. Milne and W. C. Waterhouse, *Abelian varieties over finite fields*, Proc. Symp. Pure Math. **20** (1971), 53–64.

[P] M. Papikian, *Honda-Tate theorem for elliptic curves*, in Expository Notes in his homepage.

[Sch] P. Scholze, *The Langlands-Kottwitz method for the modular curve*, Int. Math. Res. Not. no. 15 (2011), 3368–3425.

[Si] J. Silverman, *The arithmetic of elliptic curves*, GTM 106.

[ST] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, no. 6, 1961.

[Ta1] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[Ta2] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'apres T. Honda),* Sém. Bourbaki Nov. 1968, Exposé 352, 95–109.

[W] W. C. Waterhouse, *Abelian varieties over finite fields*, Annales scientifiques de l'École Normale Superieure **2** (1969), 521–560.