複素数体$\mathbf{C}$上の楕円曲線

$$E : y^2 = x^3 + Ax + B,$$
$$A, B \in \mathbf{C},\ x^3 + Ax + B = 0 \text{重解なし}$$
$$E(\mathbf{C}) := \{(x, y) \in E \mid x, y \in \mathbf{C}\}.$$

多様体としての楕円曲線

$$E_\tau \cong \mathbf{C}/(\mathbf{Z} + \mathbf{Z}\tau),\ \tau \in \mathfrak{H}$$
$$\mathfrak{H} := \{a + bi \in \mathbf{C} \mid a, b \in \mathbf{R}, b > 0\},$$

複素上半平面.

$$\forall E,\ \exists \tau \text{ s.t. } E(\mathbf{C}) \cong E_\tau.$$

$$E_\tau \cong E_{\tau'} \Longleftrightarrow \tau' = \frac{a\tau + b}{c\tau + d}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathsf{SL}_2(\mathbf{Z}).$$
$$\mathsf{SL}_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{array}{l} a, b, c, d \in \mathbf{Z}, \\ ad - bc = 1 \end{array} \right\}.$$

$$\{\text{楕円曲線}E\text{の同型類}\} \overset{1:1}{\longleftrightarrow} \mathsf{SL}_2(\mathbf{Z})\backslash\mathfrak{H}.$$

$\mathfrak{H}^* := \mathfrak{H} \cup \mathbf{Q} \cup \{i\infty\}$.

$X(1)(\mathbf{C}) \cong \mathsf{SL}_2(\mathbf{Z}) \backslash \mathfrak{H}^*$.

となる代数曲線 $X(1)$ が存在する。

これを (レベル 1 の) モジュラー曲線という。

Level structure付の楕円曲線

$E[N] \cong (\mathbf{Z}/N\mathbf{Z}) \oplus (\mathbf{Z}/N\mathbf{Z})$.

E : 楕円曲線,

C : E の位数 N の巡回部分群

組 (E, C) の同型類を考える。

$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathsf{SL}_2(\mathbf{Z}) \mid c \equiv N \right\}$.

$X_0(N)(\mathbf{C}) \cong \Gamma_0(N) \backslash \mathfrak{H}^*$.

定理　(G. Shimura) $X_0(N)(\mathbf{C})$は、$\mathbf{Q}$上のモデル $X_0(N)$を持つ。
つまり、

- $X_0(N)$は、$\mathbf{Q}$係数の定義方程式を持つ

- $K/\mathbf{Q}$を体の拡大とすると、
  $X_0(N)(K) \cong \left\{(E,C)_{/K}\text{の同型類}\right\}$,
  $(E,C)_{/K}$はE,CがK上定義されている

p:素数、$p \nmid N$ならば

- $\tilde{X}_0(N) := X_0(N) \mod p$は、非特異曲線。

- $K/\mathbf{F}_p$は標数pの有限体の拡大。
  $\tilde{X}_0(N)(K) \cong \left\{(E,C)_{/K}\text{の同型類}\right\}$,
  $(E,C)_{/K}$はE,CがK上定義されている

正則微分形式

$$C: \text{代数曲線}$$
$$U \subset C: \text{開集合}$$
$$s, t: U\text{ 上の正則関数}$$

1. $d(s+t) = ds + dt$

2. $d(ks) = kds$, k:定数

3. $d(st) = sdt + tds$

これを貼り合わせたものを

$$\Omega^1_C: \text{正則微分形式のなす層}$$

という。

$$S_2(\Gamma_0(N)) \otimes \mathbf{C} \cong H^0(X_0(N), \Omega^1_{X_0(N)}).$$

これにより、正則微分形式の話が重さ２の cusp form の話に翻訳できる。

標準写像

C : 代数曲線.

g : C の種数.

$\omega_1, \omega_2, \cdots, \omega_g \in H^0(C, \Omega_C^1)$ を基底とする.

$$
\begin{aligned}
\varphi : C &\longrightarrow \mathbf{P}^{g-1} \\
z &\longmapsto (\omega_1, \omega_2, \cdots, \omega_g)
\end{aligned}
$$

を標準写像という。

C が超楕円曲線のとき $\varphi : C \xrightarrow{2:1} \mathrm{Im}\varphi \cong \mathbf{P}^1$

C が非超楕円曲線のとき $C \cong \mathrm{Im}\varphi$.

非超楕円曲線のときの$\mathrm{Im}\varphi$を、標準曲線という。

$X_0(N)$ の定義方程式

種数 $g = 0, 1$ の場合は昔から知られている。
よって、種数 $g \geq 2$ を扱う。

$X_0(N)$ の方程式としては、モジュラー方程式と呼ばれる非常に数論的性質のよい方程式が知られている。

モジュラー方程式の欠点

係数と次数が非常に大きく、数値計算をするのが難しい。

この講演で求める定義方程式の形

超楕円的のときは、

$$y^2 = f(x)\ , f(x) \in \mathbf{Q}[x]\ , deg f(x) = 2g + 2.$$

非超楕円的のときは、
いくつかの２次と３次の超曲面の共通部分

どちらの係数の大きさも非常に小さい。

$X_0(N)$が超楕円曲線のとき

定理　(Ogg) 超楕円的$X_0(N)$となるNは次の19個

$g = 2; N = 22, 23, 26, 28, 29, 31, 37, 50$

$g = 3; N = 30, 33, 35, 39, 40, 41, 48$

$g = 4; N = 47$

$g = 5; N = 46, 59$

$g = 6; N = 71.$

$X_0(N)$は次のような形の方程式になる。

$$y^2 = f(x)\ , f(x) \in \mathbf{Q}[x]\ , deg f(x) = 2g + 2.$$

定義方程式を求めるアルゴリズム (村林の方法の一般化)

$f_1, \ldots, f_g \in \mathsf{S}^2(N)$ を基底とすると、それらの線形結合によって

$$\begin{cases} g_1(z) = q^g + s_{1,g+1}q^{g+1} + \cdots + s_{1,3g+3}q^{3g+3} + \cdots \\ g_2(z) = q^{g-1} + s_{2,g}q^g + \cdots + s_{2,3g+2}q^{3g+2} + \cdots \\ \quad \vdots \\ g_g(z) = q + s_{g,2}q^2 + \cdots . \end{cases}$$

という形の基底が取れる。$(q = e^{2\pi iz})$.

$$\begin{cases} x := \frac{g_2}{g_1} \\ y := \frac{q}{g_1}\frac{dx}{dq} \end{cases}$$

$$\begin{cases} y^2 = q^{-(2g+2)} + \cdots \\ x = q^{-1} + \cdots \end{cases}$$

$X_0(N)$ の定義方程式の係数 $a_1, a_2, \ldots$ は次のように帰納的に求まる。

$$\begin{cases} y^2 - x^{2g+2} = a_1 q^{-2g+1} + \cdots \\ y^2 - x^{2g+2} - a_1 x^{2g+1} = a_2 q^{-2g} + \cdots \\ \cdots\cdots . \end{cases}$$

よって定義方程式は、

$$y^2 = x^{2g+2} + a_1 x^{2g+1} + \cdots + a_{2g+2}.$$

となる。

注 1 定義方程式を求めるために必要な係数は、
$\{s_{1,g+1}, \cdots, s_{1,3g+3}, s_{2,g}, \cdots, s_{2,3g+2}\}$.

Input:

$$\begin{cases} f_1(z) = a_{1,1}q + a_{1,2}q^2 + \cdots + a_{1,3g+3}q^{3g+3} + \cdots \\ f_2(z) = a_{2,1}q + a_{2,2}q^2 + \cdots + a_{2,3g+3}q^{3g+3} + \cdots \\ \quad \vdots \\ f_g(z) = a_{g,1}q + a_{2,2}q^2 + \cdots + a_{2,3g+3}q^{3g+3} + \cdots. \end{cases}$$

Output:

$$y^2 = x^{2g+2} + a_1 x^{2g+1} + \cdots + a_{2g+2}.$$

$(X_0(46), g=5)$

f_1	$q - q^3 - q^4 - 2q^6 + 2q^7 - q^8 + 2q^9 + 2q^{10} - 4q^{11} + 3q^{12} + 3q^{13} + 2q^{14} - 4q^{15} + 2q^{17} + \cdots$
f_2	$q^2 - 2q^3 - q^4 + 2q^5 + q^6 + 2q^7 - 2q^8 - 2q^{10} - 2q^{11} + q^{12} + 2q^{15} + \cdots$
f_3	$q^2 - q^6 - q^8 - 2q^{12} + 2q^{14} - q^{16} + 2q^{18} + \cdots$
f_4	$q^4 - 2q^6 - q^8 + 2q^{10} + q^{12} + 2q^{14} - 2q^{16} - 2q^{20} + \cdots$
f_5	$q - q^2 + q^4 + 4q^5 - 4q^7 - q^8 - 3q^9 - 4q^{10} + 2q^{11} - 2q^{13} + 4q^{14} + q^{16} - 2q^{17} + \cdots$
g_1	$q^5 + q^6 - q^7 - q^9 - 2q^{10} + q^{11} - q^{12} - q^{13} + q^{15} + q^{16} - q^{17} + \cdots$
g_2	$q^4 - 2q^6 - q^8 + 2q^{10} + q^{12} + 2q^{14} - 2q^{16} - 2q^{20} + \cdots$
x	$q^{-1} - 1 - q^2 + q^3 - q^4 + q^5 - q^6 + 2q^7 - 2q^8 + 2q^9 - 2q^{10} + 3q^{11} - 3q^{12} + \cdots$
y	$-q^{-6} + q^{-5} - 2q^{-4} + q^{-3} - q^{-2} - 3q^{-1} + 8 - 22q + 47q^2 - 92q^3 + 160q^4 - 275q^5 + 459q^6 - \cdots$

$X_0(46)$:

$$y^2 = x^{12} - 2x^{11} + 5x^{10} + 6x^9 - 26x^8 + 84x^7 - 113x^6 + 134x^5 - 64x^4 + 26x^3 + 12x^2 + 8x - 7$$

$X_0(N)$が非超楕円曲線のとき

定理　(Petri) Cを種数$g(\geq 4)$の標準曲線とする。すると、Cは次のように表される。

(i) Cが非特異平面５次曲線、またはCから$\mathbf{P}^1$への３次の写像が存在するとき。

いくつかの２次超曲面と、少なくとも一つの３次超曲面の共通部分になる。

(ii) (i)以外のとき。

いくつかの２次超曲面の共通部分になる。

定義方程式を求めるアルゴリズム

$f_1, \ldots, f_g \in \mathsf{S}^2(N)$ を基底とする

$f_i f_j$, $(1 \le i, j \le g)$,

$f_i f_j f_k$, $(1 \le i, j, k \le g)$ を考える。

● ２次の関係式

$\#\{2$次の単項式$\} = {}_gH_2$,

線形独立な２次の単項式の個数

$= (2 \times 2 - 1)(g - 1)$

よって、２の関係式の数は、

${}_gH_2 - (2 \times 2 - 1)(g - 1) = (g - 2)(g - 3)/2$

これらの関係式を

$$P_1(f_1, \ldots, f_g) = 0,$$
$$\vdots$$
$$P_{(g-2)(g-3)/2}(f_1, \ldots, f_g) = 0.$$

とする。

• 3次の関係式

3次の関係式の個数

＝#{3次の単項式}

− 線形独立な3次の単項式の個数

−{2次の関係式から得られる三次の関係式のランク}.

2次の関係式から得られる三次の関係式のランクは、

$\langle x_i P_j(x_1, \ldots, x_g)\rangle$ のランク

$1 \leq i \leq g, 1 \leq j \leq (g-2)(g-3)/2$

これを種数 $g = 3, 4, 5, 6$ の $X_0(N)$ に適用する。

- $g = 3$

  2次と3次の関係式はない。

  4次の関係式の個数を計算すると、

  $${}_3H_4 - (2 \times 4 - 1)(3 - 1) = 1.$$

  $X_0(N)$の定義方程式は、この4次式。

- $g = 4$

  2次と3次の関係式が1個ずつ。

- $g = 5$

  2次の関係式が3個。(計算してみると、3次の関係式は出てこない)

- $g = 6$

  2次の関係式が6個。(計算してみると、3次の関係式は出てこない)

注 2 $g \geq 7$ の場合も、全く同じ方法で計算できる。

また、$g \geq 5$ の全ての $X_0(N)$ で3次の関係式は出てこない。[長谷川-志村]

定義方程式の一例

$(g=3,$ 非超楕円的$)$

$$X_0(64) : x^4 + y^4 - z^4 = 0$$

$(g=4,$ 非超楕円的$)$

$$X_0(81) : \begin{cases} xy - w^2 = 0 \\ x^3 + 27y^3 - z^3 + 9xyw = 0 \end{cases}$$

$(g=5,$ 非超楕円的$)$

$X_0(42)$:

$$\begin{cases} 2x^2 + 6xy + 4zw - zu + 2wu - u^2 = 0 \\ -x^2 + 9y^2 + zu - 2wu = 0 \\ 4x^2 + 3z^2 + 20zw + 12w^2 - 2zu + 4wu - 5 \end{cases}$$

$X_0(N)$の間の被覆写像

NがMを割るとき、$X_0(M)$ から $X_0(N)$への自然な被覆写像がある。この被覆写像を既に求めた定義方程式に関して求めよう。これは$X_0(M)$と$X_0(N)$が超楕円的かどうかで三つの場合に分かれる。

- $X_0(M)$ と $X_0(N)$ が超楕円的なとき。

  これは、$M = 46,\ N = 23$の場合のみ。

  $X_0(46)$:

  $y^2 = (x^3 - 2x^2 + 3x - 1)$

  $\times (x^3 + x^2 - x + 7)$

  $\times (x^6 - x^5 + 4x^4 - x^3 + 2x^2 + 2x + 1)$

$X_0(23)$:
$y^2 = (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7)$

$(x, y) \longmapsto$
$\left(\dfrac{x^3 - x^2 + 2x}{x - 1}, \dfrac{y(x^3 - 2x^2 + x - 1)}{(x-1)^3}\right)$

- $X_0(M)$ と $X_0(N)$ 共に非超楕円的のとき $S_2(\Gamma_0(M))$ の基底 $\{f_1, \ldots, f_{g_n}, \ldots, f_{g_m}\}$ を $\{f_1, \ldots, f_{g_n}\}$ が $S_2(\Gamma_0(N))$ の基底になるようにとる。
  (x_i) を $\{f_i\}$ に対応する座標とすると、
  $X_0(M) \longrightarrow X_0(N)$
  $(x_1, \ldots, x_{g_n}, \ldots, x_{g_m}) \longmapsto (x_1, \ldots, x_{g_n})$
  は被覆写像になる。

- $X_0(M)$ が非超楕円的、 $X_0(N)$ は超楕円的のとき (例のみ)

  $X_0(22)$:

  $y^2 = x^6+6x^5+11x^4+24x^3+11x^2+18x-7$

  $X_0(44)$

  $$\begin{cases} x^2+8y^2+16z^2-w^2+4xy+4xz \\ +16yz=0 \\ y^3+16yz^2+8y^2z+16z^3-zw^2=0 \end{cases}$$

  $$X_0(44) \longrightarrow X_0(22)$$

  $$(x,y,z,w) \longmapsto (xy^2, xw(x+4y+8z), y^3)$$

  $$= (y^2, w(x+4y+8z), z(x+4y+4z)).$$