

An algorithm for determining the normal form of the genus two modular curves

早大理工数学科 村林直樹 (Naoki Murabayashi)

level N の modular curve $X_0(N)$ の定義方程式として modular equation $\Phi_N = 0$ がとってこられる事はよく知られている。 Φ_N は虚 2 次体上の虚数乗法論において重要な役割をはたす。しかし、 Φ_N の次数と係数は非常に大きくなるので、実際に取り扱うには非常に不便である。例えば

$$\begin{aligned}\Phi_2(x, y) = & x^3 + y^3 - x^2y^2 + 2^4 \cdot 3 \cdot 31xy(x+y) - 2^4 \cdot 3^4 \cdot 5^3(x^2 + y^2) \\ & + 3^4 \cdot 5^3 \cdot 4027xy + 2^8 \cdot 3^7 \cdot 5^6(x+y) - 2^{12} \cdot 3^9 \cdot 5^9\end{aligned}$$

である。一方、genus 2 の curve の場合には normal form $y^2 = f(x)$, $\deg f = 5$ or 6 という定義方程式がとってこれる。これは modular equation よりはるかに取り扱いやすい。ここでは genus 2 の modular curve と modular curve の quotient curve で genus が 2 となるものの normal form を weight 2 の cusp form の基底の Fourier 係数から統一的に求める方法を記述し、それを使って実際に normal form を計算する。

§1 normal form を求める algorithm

$X_0(N)$ で $\Gamma_0(N)$ を level N の modular curve / \mathbb{Q} を表わす。 W_N を行列 $\begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$ によって誘導される $X_0(N)$ の自己同型写像とし、 $X^*(N)$ を W_N によって生成される $\text{Aut } X_0(N)$ の部分群によって $X_0(N)$ を割って得られる quotient curve とする。 genus formula を用いて計算することにより次が成立する。

(1.1) p : 素数に対し、 $X_0(p)$ の genus = 2 $\Rightarrow p = 23, 29, 31, 37$.

更に、 $X^*(p)$ の genus = 2 $\Rightarrow p = 67, 73, 103, 107, 167, 191$.

以下 Γ は $\Gamma_0(p)$ ($p = 23, \dots, 37$), $\Gamma^*(p) = \langle \Gamma_0(p), \begin{bmatrix} 0 & -1 \\ p & 0 \end{bmatrix} \rangle$ ($p = 67, \dots, 191$) のいずれかを表わし、 X_Γ をそれに対応する modular curve とする。

Remark (1.2) Γ は素数 level の場合に限定するのは、四元数環の maximal order からつくられるテータ級数を用いることにより weight 2 の cusp form のなす空間 $S_2(\Gamma)$ の基底を q 展開した時の Fourier 係数が計算出来るからであり、今から述べる algorithm に関しては本質的な制限ではない。

$f_1 = \sum_{i=1}^g a_i q^i$, $f_2 = \sum_{j=1}^g b_j q^j$: $S_2(\Gamma)$ の基底, $q = \exp(2\pi i z)$ とする。§2 で $\{a_i, b_j\}$ を計算する方法を簡単に説明する。

○ $\{a_i, b_j\}$ から X_P の normal form を求める algorithm.

f_1, f_2 は次の様に正規化される。

Case 1: $i\omega$ が X_P の Weierstrass point の時.

$$f_1 = \sum_{i=3}^g a_i q^i (a_3 \neq 0), \quad f_2 = \sum_{j=1}^g b_j q^j (b_1 \neq 0).$$

Case 2: $i\omega$ が X_P の Weierstrass point でない場合.

$$f_1 = \sum_{i=2}^g a_i q^i (a_2 \neq 0), \quad f_2 = \sum_{j=1}^g b_j q^j (b_1 \neq 0).$$

$$x = \frac{f_2}{f_1} \text{ とおく.}$$

(1.3) $x \in \mathbb{Q}(X_P)$, x の degree は 2 になる。ここで、 $\mathbb{Q}(X_P)$ は X_P の \mathbb{Q} 上定義された有理型関数のなす体を表わす。

$\mathbb{Q}(X_P)/\mathbb{Q}(x)$ は 2 次拡大だから、或る $\mathbb{Q}(X_P)$ の元 y が存在し $\mathbb{Q}(X_P) = \mathbb{Q}(x, y)$, $y^2 = f(x)$, $f(T) (\in \mathbb{Q}[T])$ は分離多項式, f が成立する (この様な y は定数倍を除いて一意に定まる)。更に、 $f(T)$ の次数は Case 1, Case 2 の場合にそれぞれ 5, 6 となる。以下、Case 1 の場合に限定する (Case 2 の場合も殆ど同様に出来る)。

(1.4) $\{a_i, b_j\}$ から x を q -展開した時の係数が計算出来る。

従って、 X^k ($k \in \mathbb{N}$) を q -展開した時の係数が計算出来る。

$(2\pi i f_1(z) dz, 2\pi i f_2(z) dz)$ は $H^0(X_p, \Omega^1)$ の基底となり、 $\frac{dx}{y} (\neq 0) \in H^0(X_p, \Omega^1)$ だから、或る $(s, t) (\neq (0, 0)) \in \mathbb{Q}^2$ が存在し

$$\frac{dx}{y} = s \cdot 2\pi i f_1(z) dz + t \cdot 2\pi i f_2(z) dz$$

が成立する。 $\frac{dx}{y}$, $2\pi i f_1(z) dz$, $2\pi i f_2(z) dz$ は $\overline{\mathbb{C}}$ でそれぞれ 2位, 2位, 0位の零点を持つから、 $t=0$ が成立しなくてはならない。
従って次の等式を得る。

$$(1.5) \quad \frac{dx}{y} = s \cdot 2\pi i f_1(z) dz.$$

$W := s \cdot y$, $g(T) := s^2 \cdot f(T)$ とおくと、明らかに $\mathbb{Q}(X_p) = \mathbb{Q}(x, W)$, $W^2 = g(x)$ が成立する。 $W = \frac{dx}{2\pi i f_1(z) dz}$ だから、 W を q -展開した時の係数が計算でき、その結果として

(1.6) W^2 を q -展開した時の係数が計算出来る。

$g(T) = u_0 T^5 + u_1 T^4 + \dots + u_5$ とおき、 $g(x)$ を q -展開した時の係数と W^2 を q -展開した時の係数を比較することにより u_0, u_1, \dots, u_5 が順次決定出来る(より正確に、Case 1 の場合には $\{a_3, \dots, a_3, b_1, \dots, b_{11}\}$ から、Case 2 の場合には $\{a_2, \dots, a_8, b_1, \dots, b_7\}$ から計算出来る)。

従って $\{a_i, b_j\}$ から X_p の normal form $W^2 = g(x)$ が計算出来る。

§2. $\{a_i, b_j\}$ の計算方法.

この section に最も適した参考文献として A. Pizer, 「An algorithm for computing modular forms on $\Gamma_0(N)$ 」, Journal of Algebra 64 (1980), P340 ~ P390 と M. Eichler, 「The basic problem for modular forms and the trace of the Hecke operators」, Lecture Note No. 320, P75 ~ P151 を挙げておく。 \mathcal{O} を \mathbb{Q} 上の定符号四元数環, D を \mathcal{O} の判別式とする。 D と互いに素で square free な正の整数 H を固定し, \mathcal{O} を level H の Eichler 型 order とする。 I_1, \dots, I_r を left \mathcal{O} -ideal 類の完全代表系とし $\mathcal{O}_j = \{a \in \mathcal{O} \mid I_j a \subseteq I_j\}$ ($1 \leq j \leq r$) とおき, \mathcal{O}_j を I_j の right order と呼ぶ。 $e_j := \#\{u \in \mathcal{O}_j \mid N(u) = 1\}$ 。 ここで任意の正の整数 n に対し, $b_{ij}(n) = \frac{1}{e_j} \times \#\{\alpha \in I_j^{-1} I_i \mid N(\alpha) = n \times \frac{N(I_i)}{N(I_j)}\}$, $b_{ij}(0) = \frac{1}{e_j}$ とおく。 $B(n; D, H) = (b_{ij}(n))$ ($n \geq 0$) を Brandt 行列と言う。

$$(2.1) \quad A = \begin{bmatrix} 1 & e_1 e_1^{-1} & \dots & e_1 e_r^{-1} \\ \vdots & -1 & & 0 \\ & & \ddots & \\ 1 & 0 & & -1 \end{bmatrix} \text{ とおくと, } A B(n; D, H) A^{-1} = \begin{bmatrix} b(n) & 0 & \dots & 0 \\ 0 & & & \\ \vdots & B(n; D, H) & & \\ 0 & & & \end{bmatrix}$$

ここで $B(n; D, H)$ は $(r-1) \times (r-1)$ の行列, $b(n)$ は norm が n になる left integral \mathcal{O} -ideal の個数。

$$\Theta(z; D, H) = \sum_{n=0}^{\infty} B(n; D, H) \cdot \exp(2\pi i n z) = (\theta_{ij}(z)) \text{ とおく。 } \theta(D, H) \text{ を}$$

$\{\theta_{ij}(z) \mid 1 \leq i, j \leq h-1\}$ によって生成される \mathbb{C} 上のベクトル空間とし、正の整数 k に対し、 $\theta(D, H)^k = \{\theta(kz) \mid \theta(z) \in \theta(D, H)\}$ とおく。

(2.2) N を square free な正の整数、 $N = p_1 \cdots p_r$ を素因数分解とした時

$$S_2(\Gamma_0(N)) = \theta(p_1, p_2, \dots, p_r) \oplus \theta(p_2, p_3, \dots, p_r) \oplus \theta(p_3, p_4, \dots, p_r) \oplus \cdots \oplus \sum_{k \mid p_1 \cdots p_{r-1}} \theta(p_r, 1)^k$$

が成立する。

Pizer は level H の Eichler 型の order が見つけられたという仮定のもとで、 $D=p$, p は素数の場合に Brandt 行列 $\{B(n; p, H)\}_{n \geq 0}$ を計算するアルゴリズムを与えている。一方、level 1 の Eichler 型 order (= maximal order) の \mathbb{Z} 上の基底は具体的に書き下せる。従って $S_2(\Gamma_0(p))$ の基底を q -展開した時の係数が計算出来る。

$S_2(\Gamma^*(p)) = \{\theta \in S_2(\Gamma_0(p)) \mid \theta| [w_p] = \theta\}$, ここで $\theta| [w_p]$ は w_p の θ の作用を表わす。この時次の等式が成立する。

$$(2.3) \quad (\theta_{ij}| [w_p]) = -B'(p; p, 1) \times \sum_{n=0}^{\infty} B'(n; p, 1) \cdot \exp(2\pi i n z).$$

従って $(\theta_{ij}) = (1_{h-1} - B'(p; p, 1)) \times \sum_{n=0}^{\infty} B'(n; p, 1) \cdot \exp(2\pi i n z)$ とおくと、 $S_2(\Gamma^*(p))$ は $\{\theta_{ij} \mid 1 \leq i, j \leq h-1\}$ によって張られる。

故に、 $S_2(\Gamma^*(p))$ の基底を q -展開した時の係数が計算出来る。

§3. genus 2 の modular curve の normal form

§1 と §2 を組み合わせることにより我々は次の表を得ることが出来る。

level P	normal form $w^2 = g(x)$	$j(\Gamma)$ の判別式
$X_0(23)$	$w^2 = x^6 - 8x^5 + 2x^4 + 2x^3 - 11x^2 + 10x - 7$	$2^{12} \cdot 23^6$
$X_0(29)$	$w^2 = x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$	$2^{12} \cdot 29^5$
$X_0(31)$	$w^2 = x^6 - 8x^5 + 6x^4 + 18x^3 - 11x^2 - 14x - 3$	$2^{12} \cdot 31^4$
$X_0(37)$	$w^2 = x^6 + 8x^5 - 20x^4 + 28x^3 - 24x^2 + 12x - 4$	$2^{12} \cdot 37^3$
$X^*(67)$	$w^2 = x^6 - 4x^5 + 6x^4 - 6x^3 + 9x^2 - 14x + 9$	$2^{12} \cdot 67^2$
$X^*(73)$	$w^2 = x^6 - 4x^5 + 6x^4 + 2x^3 - 15x^2 + 10x + 1$	$2^{12} \cdot 73^2$
$X^*(103)$	$w^2 = x^6 - 10x^4 + 22x^3 - 19x^2 + 6x + 1$	$2^{12} \cdot 103^2$
$X^*(107)$	$w^2 = x^6 - 4x^5 + 10x^4 - 18x^3 + 17x^2 - 10x + 1$	$2^{12} \cdot 107^2$
$X^*(167)$	$w^2 = x^6 - 4x^5 + 2x^4 - 2x^3 - 3x^2 + 2x - 3$	$2^{12} \cdot 167^2$
$X^*(191)$	$w^2 = x^6 + 2x^4 + 2x^3 + 5x^2 - 6x + 1$	$2^{12} \cdot 191^2$

Remark (3.1) $g(T)$ の判別式各素因数の指数は $w^2 = g(x)$ により定義される \mathbb{Z} 上の model と X_P の \mathbb{Z} 上の minimal regular model との gap を表わしている。このことから、特に我々が求めた $X^*(P)$ の normal form は非常によいものであることがわかる。