数理解析研究所講究録
1091 巻 1999 年 64-75

有理数体上で定義される楕円曲線の canonical system とその応用

山本芳彦 (大阪大学 理学研究科)

1 Canonical system

C を有理数体上で定義される楕円曲線とする. C は minimal Weierstrass model

$$\mathrm{C}: Y^2+a_1XY+a_3Y=X^3+a_2X^2+a_4X+a_6 \quad (a_i\in\mathbb{Z})$$

で与えられているとし, その判別式と導手を $\Delta=\Delta(\mathrm{C})$, $N=\mathrm{cond}(\mathrm{C})$ とおく. C には無限遠点 O を零元とする 1 次元 abel 多様体 の構造が入る. X, Y を C 上の関数体の元と考えるとき X, Y は O において, それぞれ 2位, 3位の極を持つ. t を O における一つの局所変数で, X, Y が t のべき級数として有理整数係数で

$$X=t^{-2}+x_{-1}t^{-1}+x_0+x_1t+x_2t^2+\cdots \quad (x_i\in\mathbb{Z}) \qquad (1)$$
$$Y=t^{-3}+y_{-2}t^{-2}+y_{-1}t^{-1}+y_0+y_1t+\cdots \quad (y_j\in\mathbb{Z}) \qquad (2)$$

の形に展開されるとき, t を integral parameter と呼ぶ.

例 1.1 $t=X/Y$ とおくと, t は *integral parameter* である. 実際, $a_1,\cdots,a_6$ の整係数多項式を係数として次のように表される.

$$X=t^{-2}+a_1t^{-1}-a_2+a_3t-(a_1a_3+a_4)t^2+\cdots$$
$$Y=t^{-3}+a_1t^{-2}-a_2t^{-1}+a_3-(a_1a_3+a_4)t+\cdots$$

また, t をひとつの *integral parameter* とするとき,

$$t'=t+r_2t^2+r_3t^3+\cdots \quad (r_k\in\mathbb{Z})$$

とおくと, t' も *integral paramter* である. よって, C には無数の *integral parameter* が存在する.

t を O における local parameter とする. C の Neron differential ω の t 展開を

$$\omega = \frac{-dX}{2Y + a_1X + a_3} = f(t)\frac{dt}{t}$$

$$f(t) = \frac{-t\dfrac{dX}{dt}}{2Y + a_1X + a_3} = t + b_2t^2 + b_3t^3 + \cdots \tag{3}$$

とおくとき, 次が成り立つ.

Proposition 1.1 t が *integral* $\Longrightarrow$ $b_k \in \mathbb{Z}$ $(k = 1, 2, 3, \cdots)$

楕円曲線 C の zeta function を

$$L_C(s) = \sum_{n=1}^{\infty} c_n n^{-s}$$

とすると, 次の事実が知られている.

Proposition 1.2 t を *integral parameter* とする. 素数 p が C の判別式 Δ を割り切らないとき次が成り立つ.

$$b_p \equiv c_p \pmod{p}$$

上の命題と, 合同 zeta 関数に対して Riemann 予想の類似

$$|\, c_p \,| \leq 2\sqrt{p}$$

が成立することを用いると,

$$p \geq 17 \implies 2\sqrt{p} \leq \frac{p}{2}$$

だから, 各 $p \geq 17$ に対して, $f(t)$ の係数 b_p がわかると, zeta 関数の係数 c_p を個別に求めることが出来る. しかし, 合同であるということに由来する不定性のために, X, Y のべき級数展開より, 直接 $L_C(s)$ の性質を調べたり, 逆に, $L_C(s)$ から X, Y の性質を導くことは出来ない.

実は, 次に定義するような特別な性質を持つ都合のよい local parameter が存在することがわかる.

Defnition 1.1 C の O における *local parameter* t が次の 2 条件をみたすとき t を **canonical parameter** とよぶ.

(1) t は *integral parameter* である.
(2) すべての自然数 n に対して $b_n = c_n$ が成り立つ.

このとき, 次が成り立つ (→ §2, Theorem 2.2)

Theorem 1.1 *Canonical parameter* は存在し, 一意に定まる.

t を C の canonical parameter とするとき, X, Y の t に関するべき級数展開

$$X = X(t) = t^{-2} + x_{-1}t^{-1} + x_0 + x_1 t + x_2 t^2 + \cdots \quad (x_i \in \mathbb{Z}) \tag{4}$$
$$Y = Y(t) = t^{-3} + y_{-2}t^{-2} + y_{-1}t^{-1} + y_0 + y_1 t + \cdots \quad (y_j \in \mathbb{Z}) \tag{5}$$

を C の canonical series , $\{t, X(t), Y(t)\}$ を C の canonical system とよぶ.

Canonical parameter t により Neron differential ω を

$$\omega = \frac{-dX}{2Y + a_1 X + a_3} = f(t)\frac{dt}{t}$$

$$f(t) = \frac{-t\dfrac{dX}{dt}}{2Y + a_1 X + a_3} = t + b_2 t^2 + b_3 t^3 + \cdots \tag{6}$$

とべき級数展開するとき, C の zeta 関数は

$$L_C(s) = \sum_{n=1}^{\infty} b_n n^{-s}$$

で与えられる.

注意. Canonical system は C の minimal Weierstrass model のとり方に depend するが, それらを結ぶ同型写像により互いに移り合う.

例 1.2 楕円曲線

$$C_1 : Y^2 + Y = X^3 - X^2 - 10X - 20 \ (\Delta = -11^5, N = 11)$$

C_1 は合同部分群 $\Gamma_0(11)$ に対応する *modular curve* $X_0(11)$ と同型で X, Y を $\Gamma_0(11)$ に関する *modular function* と考えて, *cusp* $z = i\infty$ におけ

る *local parameter* $q = \exp(2\pi iz)$ に関する展開は有理整数係数で次のようになる.

$$X_1 = X(q) = q^{-2} + 2q^{-1} + 4 + 5q + 8q^2 + q^3 + 7q^4 - 11q^5 + 10q^6 - 12q^7 + 18q^8 - 22q^9 + 26q^{10} - 11q^{11} + 41q^{12} + \cdots$$

$$Y_1 = Y(q) = q^{-3} + 3q^{-2} + 7q^{-1} + 12 + 17q + 26q^2 + 19q^3 + 37q^4 - 15q^5 - 16q^6 - 67q^7 - 6q^8 - 144q^9 + 92q^{10} - 66q^{11} + \cdots$$

$X_0(11)$ は *genus 1* の *modular curve* であるから, その第1種微分は *Neron diffferential* の定数倍となる. q 展開の係数を比べると

$$f = q - 2q - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} + \cdots$$

となり, $f(q)$ は $\Gamma_0(11)$ に関する *weight 2* の *cusp form* である. これが $X_0(11)$ の *zeta* 関数を与える (Eichlar – Shimura). よって, $\{q, X_1, Y_1\}$ は C_1 の *canonical system* である.

2 Canonical system の存在と構成

2.1 Formal group structures

楕円曲線 C が次の minimal Weierstrass model で与えられているとする.

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \quad (a_i \in \mathbb{Z})$$

また, t を零元 O における local parameter とし, X, Y, ω の t によるべき級数展開を (1), (2), (6) とおいて,

$$h(t) = \int f(t)\frac{dt}{t} = t + \frac{b_2}{2}t^2 + \frac{b_3}{3}t^3 + \cdots$$

により, $h(t)$ を定める. このとき,

$$\omega = h'(t)dt = d(h(t))$$

と表される. ここで, u, v に関する形式的べき級数 $F_t(u, v)$ を

$$F_t(u, v) = h^{-1}(h(u) + h(v)) = u + v + (\text{higher terms on } u \text{ and } v\ ) \in \mathbb{Z}[[u, v]]$$

により定めると,

Proposition 2.1 $F_t(u,v)$ は $\mathbb{Z}$ 上 (可換な) *formal group* を与える.

すなわち, 次をみたす.

$$F_t(F_t(u,v),w) = F_t(u,F_t(v,w))$$
$$F_t(u,v) = F_t(v,u)$$
$$F_t(0,v) = v$$

これは, $\mathbb{Z}$ 上の formal group $F_t(u,v)$ が $h(t)$ により formal additive group

$$G_a(u,v) = u+v$$

と $\mathbb{Q}$ 上同型であること意味している.

次に, C の zeta 関数 $L_C(s)$ に対して

$$g(t) = \sum_{k=1}^{\infty} \frac{c_k}{k} t^k$$

とおいて,

$$G_L(u,v) = g^{-1}(g(u)+g(v))$$

と定義すると, $G_L(u,v)$ も $\mathbb{Z}$ 上の formal group となる.

このとき, 次の定理が成り立つ.

Theorem 2.1 (Honda) $\mathbb{Z}$ 上の *formal groups* $F_t(u,v)$ と $G_L(u,v)$ は強同型である. それらの間の強同型写像は一意に定まる.

一般に, $\mathbb{Z}$ 上の二つの formal groups $F(u,v)$ と $F'(u,v)$ が与えられたとき, 次の形の $\mathbb{Z}$ 上のべき級数

$$\phi(t) = t + r_2t^2 + r_3t^3 + \cdots \quad \in \mathbb{Z}[[t]]$$

で

$$\phi(F(u,v)) = F'(\phi(u),\phi(v))$$

を満たすものが存在するとき, この二つの formal grpups は強同型であるという.

Theorem 2.2 C 上に *canonical parameter* が存在して, 一意に定まる.

実際, 上の $h(t), g(t)$ を用いて, $t = \phi(t') = h^{-1}(g(t'))$ とおくと, t' は C の canonical parameter を与える.

いま, $\{t, X(t), Y(t)\}$ を C の canonical system とすると,

$$h(t) = g(t), \quad F_t(u,v) = G_L(u,v)$$

で, C における加法と, formal group における加法に関し, 次の対応が成り立つ.

$$\begin{array}{cccccc} & \mathrm{C} & & F_t = G_L & & G_a \\ \mathrm{P} & = (X(u), Y(u)) & \leftrightarrow & u & \leftrightarrow & h(u) \\ \mathrm{Q} & = (X(v), Y(v)) & \leftrightarrow & v & \leftrightarrow & h(v) \end{array}$$

$$\mathrm{P}+\mathrm{Q} = (X(w), Y(w)) \leftrightarrow w = F_t(u,v) \leftrightarrow h(u) + h(v)$$

2.2 Canonical system の構成

Honda の定理により canonical system が存在し一意的に定まることは示された. ここでは, canonical system を構成するアルゴリズムについて考察する.

C の零元 O における local paremeter t に関する X, Y のべき級数展開を (1), (2) とおくとき, X, Y が Weisrstrass の方程式をみたすことより, 各係数 x_k, y_k の間には次のような関係式が成り立つ.

$$\begin{aligned} 3x_{-1} - 2y_{-2} &= a_1 \\ 3x_0 - 2y_{-1} &= -a_2 + a_1 x_{-1} - 3x_{-1}^2 + a_1 y_{-2} + y_{-2}^2 \\ 3x_1 - 2y_0 &= a_3 - 2a_2 x_{-1} - x_{-1}^3 + \cdots \\ 3x_2 - 2y_1 &= -a_4 + \cdots \end{aligned}$$

一般に, 次のような関係式が成り立つ.

$$3x_n - 2y_{n-1} = A_n \qquad (n \geq -1)$$

$$A_n \in \mathbb{Z}[a_1, \cdots, a_6, x_{-1}, \cdots, x_{n-1}, y_{-2}, \cdots, y_{n-2}]$$

すなわち, A_n は $a_1, \cdots, a_6, x_{-1}, \cdots, x_{n-1}, y_{-2}, \cdots, y_{n-2}$ に関する $\mathbb{Z}$ 係数の多項式として表される.

また, Neron differential の定義式より

$$-t\frac{dX}{dt} = f(t)(2Y + a_1 X + a_3)$$

である. この両辺のべき級数展開を比較することにより, 次が成り立つ.

$$n\,x_n + 2\,y_{n-1} + 2b_{n+3} = B_n \qquad (n \geq -1)$$

where

$$B_n \in \mathbb{Z}[a_1, \cdots, a_6, x_{-1}, \cdots, x_{n-1}, \\ y_{-2}, \cdots, y_{n-2}, b_1, \cdots, b_{n-2}]$$

ここでは, B_n は $a_1, \cdots, a_6, x_{-1}, \cdots, x_{n-1}, y_{-2}, \cdots, y_{n-2}, b_1, \cdots, b_{n-2}$ に関する $\mathbb{Z}$ 係数の多項式である.

1. 先ず, C の zeta 関数 $L_C(s)$ がすでにわかっている場合を考えよう. この場合には, c_n $(n \geq 1)$ がすべて既知だから, $b_n = c_n$ とおいて, 次の連立方程式

$$\begin{cases} 3x_n - 2y_{n-1} = A_n \\ nx_n + 2y_{n-1} = B_n - 2c_{n+3} \end{cases}$$

を $n = -1, 0, 1, 2, \cdots$ と順に解けば, 整数解 (x_n, y_{n-1}) が順に定まってゆく. このとき, (1), (2) で与えられる. $X = X(t), Y = Y(t)$ が C の canonical system を与える.
2. 次に, zeta 関数 $L_C(s)$ がわかっていない場合を考えよう. この場合にも, 次の定理により, caninical system を, 同時に zeta 関数も, 求めることが出来る.

Theorem 2.3 連立方程式

$$(*) \quad \begin{cases} 3x_n - 2y_{n-1} = A_n \\ nx_n + 2y_{n-1} + 2b_{n+3} = B_n \end{cases}$$

は次の条件 (i) *and* (ii) の下に, ただ一つの整数解

$$\{x_i, y_j, b_k : i \geq -2, j \geq -3, k \geq 1\}$$

をもつ.

(i) $(m, n) = 1$ のとき, $b_{mn} = b_m\, b_n$.

(ii) p が素数のとき, 次をみたす.

(a1) $|b_p| \leq 2\sqrt{p}$
(a2) $a_1 \equiv a_3 \equiv 0 \pmod 2$ のとき, $b_2 = 0$.
(b1) $p \nmid \Delta$ のとき, $b_{p^k} = b_p b_{p^{k-1}} - p b_{p^{k-2}}$ $(k \geq 2)$.
(b2) $p \mid \Delta$ のとき, $b_{p^k} = {b_p}^k$ $(k \geq 2)$.

実際, 連立不定方程式 (*) を定理の条件 (i), (ii) の下に, $n = -1$ から始めて $n = 0, 1, 2, \cdots$ と再帰的に解けばよい. その際, $n+3$ が 13 以下の素数 p となるときには, 条件 $(a1)$ をみたす b_p は一意ではないが, それらの中でただ一つのみが, すべての条件を満たすことが出来る.

注意. 定理の条件 $(a1)$ は次の条件 $(a1')$ で置き換えることが出来る.

$$(a1') \quad |b_p| \leq \begin{cases} \frac{1}{2}p & if\ p \geq 17 \\ 2\sqrt{p} & if\ p < 17 \end{cases}$$

例 2.1 導手 11 の楕円曲線 C_2, C_3 の *canonical system*

(a) $C_2 : Y^2 + Y = X\ 3 - X^2 - 7820X - 263580$
$(\Delta = -11,\ N = 11)$

Canonical system $\{q, X_2, Y_2\}$

$$\begin{aligned} X_2 =& q^{-2} + 2q^{-1} + 4 + 5q + 1570q^2 - 3123q^3 + 38551q^4 \\ & - 149501q^5 + 992122q^6 - 4816670q^7 + 26533203q^8 - \cdots \\ Y_2 =& q^{-3} + 3q^{-2} + 7q^{-1} + 12 - 1545q + 1588q^2 - 75507q^3 \\ & + 227396q^4 - 2598721q^5 + 12040848q^6 - 85035369q^7 + \cdots \end{aligned}$$

(b) $C_3 : Y^2 + Y = X^3 - X^2$
$(\Delta = -11,\ N = 11)$

Canonical system $\{q, X_3, Y_3\}$

$$\begin{aligned} X_3 =& q^{-2} + 2q^{-1} + 4 + 5q + 6q^2 + 5q^3 + 3q^4 - q^5 - 6q^6 \\ & - 10q^7 - 11q^8 - 8q^9 + 11q^{11} + 22q^{12} + \cdots \\ Y_3 =& q^{-3} + 3q^{-2} + 7q^{-1} + 12 + 19q + 24q^2 + 25q^3 + 18q^4 \\ & + 3q^5 - 20q^6 - 45q^7 - 62q^8 - 60q^9 - 31q^{10} + 26q^{11} + \cdots \end{aligned}$$

C_3 は *modular* 群 $\Gamma_1(11)$ に対応する *modular curve* $X_1(11)$ と同型であることが知られている. 楕円曲線 C_2 と C_3 はともに 例 1.2 の C_1 と *isogeneous* である. よって, *zeta* 関数に対応する $f(q)$ はすべて一致する. このとき, $q = e^{2\pi iz}$ とおくと, $f(e^{2\pi iz})$ は z の関数として $\Gamma_0(11)$ に関する *weight 2* の *cusp form* であることより,

$$X_i(e^{2\pi iz}),\ Y_i(e^{2\pi iz}) \quad (i = 2, 3)$$

は *modular functions of level 11* であることがわかる.

3 Modular Parametrization

$\mathbb{Q}$ 上の楕円曲線 C に対して, ある Modular curve $X_1(N) = \Gamma_1(N)\backslash H^*$ から C への non-constant morphism π

$$\pi : X_1(N) \longrightarrow C$$

で $\pi(i\infty) = O$ かつ C の Neron differential ω の π による pull-back $\pi^*\omega$ が $\Gamma_1(N)$ に関する normalized new form $f(q)$ of level N の定数 $c(\pi)(\neq 0)$ 倍として

$$\pi^*\omega = c(\pi) f(q) \frac{dq}{q} \quad (q = e^{2\pi iz})$$

と表されるものが存在するとき, C は modular curve of level N といい, π を C の modular parametrization という (cf. [S]).

Modular curve C に対応する newform $f(q)$ の cusp $i\infty$ における q-展開を

$$f(q) = \sum_{n=1}^{\infty} c_n q^n$$

とするとき, C の zeta 関数は

$$L_C(s) = \sum_{n=1}^{\infty} c_n n^{-s}$$

で与えられる (Shimura[Sh]). よって, t を C の零元 O における canonical parameter とすると, $\omega = f(t)dt/t$ が成り立つことより, $\pi^*t = q$, すなわち, modular parametrization π は $X_1(N)$ の cusp $i\infty$ において不分岐である. よって, $c(\pi) = 1$ が成り立つ. このとき, $q = e^{2\pi iz}$ のべき級数

$$X(q) = \sum_{n=-2}^{\infty} x_n q^n, \quad Y(q) = \sum_{n=-3}^{\infty} y_n q^n$$

は modular 部分群 $\Gamma_1(N)$ に関する modular 関数である.

Theorem 3.1 C を $\mathbb{Q}$ 上定義される *modular curve of level* N, $\{t, X(t), Y(t)\}$ をその *canonical system* とするとき, $X(q), Y(q)$ $(q = e^{2\pi iz})$ は *modular* 部分群 $\Gamma_1(N)$ に関する保型関数である. このとき, C の関数体より *madular* 関数体への *inclusion map*

$$\mathbb{Q}(X,Y) \longrightarrow \mathbb{Q}(X(e^{2\pi iz}), Y(e^{2\pi iz})) \subset \mathbb{Q}(\mathrm{X}_1(N))$$

によって定まる *modular parametrization*

$$\pi : \mathrm{X}_1(N) \longrightarrow \mathrm{C}$$

に対して, $c(\pi) = 1$ が成り立つ.

例 3.1 $\mathbb{Q}$ 上定義された楕円曲線 C の導手 N が *square free* ならば, C は *modular* である (Wiles[W]). よって, C の *canonical system* $\{t, X(t), Y(t)\}$ により, C の関数体 $\mathbb{Q}(X,Y)$ は $\Gamma_1(N)$ に関する *modular* 関数体の部分体と同一視することが出来る.

4 Isogeny と canonical system

$\mathbb{Q}$ 上定義された 2 つの楕円曲線 C と C′ の間に degree d の $\mathbb{Q}$-isogeny

$$\lambda : \mathrm{C} \longrightarrow \mathrm{C}'$$

があるとする. $\{t, X(t), Y(t)\}$, $\{t', X'(t'), Y'(t')\}$ をそれぞれ C , C′ の canonical sytem とするとき, C の $\mathbb{Q}((t))$-有理点 $P(t) = (X(t), Y(t))$ の λ による像は C′ の $\mathbb{Q}((t))$-有理点 $P'(t) = (X'(t), Y'(t))$ の整数倍となる.

$$\lambda(P(t)) = m_\lambda P'(t) \quad (m_\lambda \in \mathbb{Z})$$

により, 整数 m_λ を定める. λ^* を λ の dual isogeny とすると, $\lambda^*\lambda = d\ \mathrm{id}_\mathrm{C}$, $\lambda\lambda^* = d\ \mathrm{id}_{\mathrm{C}'}$ より, 次が成り立つ.

$$m_\lambda m_{\lambda^*} = d$$

いま, $d = \deg\lambda = p$ (p は素数) とすると, $m_\lambda = \pm 1$ または $m_\lambda = \pm p$ のいずれか一方のみが成り立つ. そこで, ある素数 p に対して $m_\lambda = \pm 1$ のときに, 両者の大小関係を $\mathrm{C} > \mathrm{C}'$ と定義して, 記号で

$$\mathrm{C} \xrightarrow{p} \mathrm{C}'$$

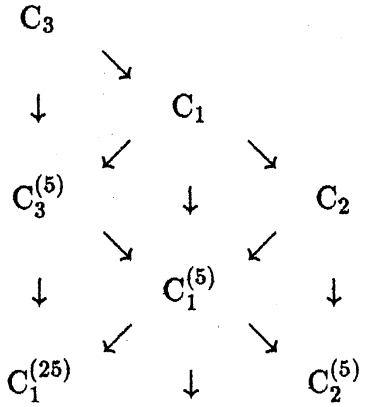
と表すと, C の $\mathbb{Q}$-isogeny class の集合より $\mathbb{Q}$-同型類を頂点とする有向グラフが定義される. これは, Stevens [St] の定義したものと同じものになる.

注. 以下の有向グラフでは p が自明な場合 p を略して $C \longrightarrow C'$ と記す.

例 4.1 導手 $N = 11$ の楕円曲線.
例 2.1 より, 導手 11 をもつ $\mathbb{Q}$ 上の楕円曲線は 唯1つの *isogeny class* よりなり, それらは C_i $(i = 1, 2, 3)$ により代表される 3 つの同型類よりなる. このとき, 次の有向グラフを得る.

$$C_3 \xrightarrow{5} C_1 \xrightarrow{5} C_2$$

C_i の m 倍写像 $< p >= mid_{C_i}$ による像を $C_i^{(m)}$ とかくとき, 次のような 5-*isogeny* の *diagram* ができる.



ここで, 斜めの矢印は 5-*isogeny* を縦の矢印は 5 倍写像 $< 5 >$ を表している.

C_i の *canonical system* を $\{X_i(t), Y_i(t)\}$ とし,

$$m(X_i(t), Y_i(t)) = (X_i^{(m)}, Y_i^{(m)})$$

とおくとき, $C_i^{(m)}$ の関数体は $\mathbb{Q}(X_i^{(m)}, Y_i^{(m)})$ で与えられる.

C_1, C_3 の関数体は, それぞれ, $\Gamma_0(11), \Gamma_1(11)$ に関する保型関数体と一致する. たとえば, 上の *diagram* より $C_3^{(5)}$ の関数体は, $\Gamma_0(11)$ に関する保型関数体の *index* 5 の部分体で, かつ C_3 の関数体と同型な体, であることがわかる. このとき, $X_3^{(5)}, Y_3^{(5)}$ により与えられる $C_3^{(5)}$ の定義方程式は *minimal* ではなく, *minimal model* の判別式 11 の 5^{12} 倍になっている.

また, C_2 に対応する保型関数体 $\mathbb{Q}(X_2(q), Y_2(q))$ は楕円 *modular* 関数体 $\mathbb{Q}(J(z))$ を含まない.

例 4.2 導手 $N = 14$ の楕円曲線.
唯1つの *isogeny class* よりなり, 6 つの同型類よりなる. *Cremona* の *table* [C] の記号を用いて記すと次のような有向グラフが出来る.

$$\begin{array}{ccccc} A_4 & \xrightarrow{3} & A_1 & \xrightarrow{3} & A_3 \\ \downarrow & & \downarrow & & \downarrow \\ A_6 & \xrightarrow{3} & A_2 & \xrightarrow{3} & A_5 \end{array}$$

ここで, $A_4 = \mathrm{X}_1(14)$, $A_1 = \mathrm{X}_0(14)$ で与えられる.

References

[Sh] Shimura, G. : On the zeta-functions of the algebraic curves uniformized by certain automorphic functions, J. Math. Soc. of Japan, 13(1961), 175-331.

[H] Honda, T. : On the thoery of commutative formal groups, J. Math. Soc. Japan 22(1970),213-246.

[C] Cremona,J.E. : Algorithms for modular elliptic curves, Cambridge 1992.

[W] Wiles, A. : Modular elliptic curves and Fermat's Last Theorem, Annals of Math. 142(1995), 443-551

[St] Stevens, D. : Stickelberger elements and modular parametrization of elliptic curves, Inv. Math., 98(1989), 75-106