2-ADIC ARITHMETIC-GEOMETRIC MEAN AND ELLIPTIC CURVES

KENSAKU KINJO AND YUKEN MIYASAKA

E-mail : sa6m16@math.tohoku.ac.jp, sa7m27@math.tohoku.ac.jp

1. 導入

始めに実数体上の算術幾何平均列と楕円曲線との関係について述べる. $a \geq b > 0$ を満たす実数 a, b を初期値とする算術幾何平均列 $\{a_n\}, \{b_n\}$ を次のように帰納的に定義する:

$$\begin{aligned} a_0 &:= a, & b_0 &:= b, \\ a_{n+1} &:= \frac{a_n + b_n}{2}, & b_{n+1} &:= \sqrt{a_n b_n} > 0 \quad (n \geq 0). \end{aligned} \tag{1.1}$$

注 2. 算術幾何平均列 $\{a_n\}, \{b_n\}$ は同一極限に収束する.

数列 $\{a_n\}, \{b_n\}$ を初期値 a, b $(a > b)$ の算術幾何平均列とし, $\mu_n := a_n/b_n$ とおく. また各 $n \geq 0$ に対し, $\mathbb{R}$ 上の楕円曲線 E_n を

$$E_n : y^2 = x(x-1)(x-\mu_n^2)$$

で定義されるものとする. このとき以下の次数 2 の同種写像が存在する:

$$g_n : E_n \to E_{n+1}; \qquad (x, y) \mapsto \left(\frac{(x+\mu_n)^2}{4\mu_n x}, \frac{y(x^2-\mu_n^2)}{8(\sqrt{\mu_n})^3 x^2} \right). \tag{1.3}$$

各 g_n を合成することで次の図式を得る:

$$E_0 \overset{g_0}{\to} E_1 \overset{g_1}{\to} \cdots \overset{g_{n-1}}{\to} E_n \overset{g_n}{\to} \cdots .$$

この様にして得られる $\mathbb{R}$ 上の楕円曲線の族 $\{E_n\}$ を考察することで, 算術幾何平均列が同一極限に収束することと退化曲線の周期との関連付けから, $\mathbb{R}$ 上の楕円曲線の周期を計算することが出来る.

次に上述の理論の p 進類似を考察する. p を素数とし, K を $\mathbb{Q}_p$ 上有限次拡大体, v を K 上の加法的付値とする. $a, b \in K$ を, p が奇素数のとき $v(1-(a/b)) > 0$, $p = 2$ のとき $v(1-(a/b)) \geq v(8)$ を満たすものとする. このとき, a, b を初期値とする数列 $\{a_n\}, \{b_n\}$ を (1.1) のように帰納的に定義する.

注 4.

(1) 初期値の仮定により, 各 $n \geq 0$ に対して p 進体の元の平方根を標準的に選ぶことが出来る. このように選んで定義される数列を p 進算術幾何平均列と呼ぶ.

(2) p 進算術幾何平均列 $\{a_n\}, \{b_n\}$ が同一極限に収束するための必要十分条件は

$$\begin{cases} v(1-(a_0/b_0)) > 0 & (p > 2) \\ v(1-(a_0/b_0)) > v(8) & (p = 2) \end{cases}$$

である (p が 2 でも奇素数でも $v(1-(a_0/b_0)) > v(8)$). 特に $p = 2$ の時に限り, 収束しない 2 進算術幾何平均列を考察することが出来る.

p 進算術幾何平均列が同一極限に収束するときには, 乗法的還元を持つ楕円曲線の周期と p 進算術幾何平均列の極限値との間の関係が知られている (4 節参照).

同一極限に収束しない 2 進算術幾何平均列の場合, 次の定理が成立する.

定理 5 (Kinjo-Miyasaka[3])**.**

K は剰余次数 d の $\mathbb{Q}_2$ 上有限次拡大体で v は K 上の加法的付値とする. また $v(1-(a/b)) = v(8)$ を満たす $a, b \in K$ に対し, $\{a_n\}, \{b_n\}$ を初期値 a, b の 2 進算術幾何平均列とし, $\mu_n = a_n/b_n$ とおく. このとき各整数 $0 \leq i < d,\ 0 \leq n$ に対して

(1) $E_n : y^2 = x(x-1)(x-\mu_n^2)$ は良い通常還元を持つ.

(2) 部分列 $\{\mu_{dn+i}\}_{n\geq 0}$ は $K\backslash\{0,1\}$ 内に収束する ($\mu_i^{\uparrow} := \lim_{n\to\infty} \mu_{dn+i}$ とおく).

(3) $E_i^{\uparrow} : y^2 = x(x-1)(x-(\mu_i^{\uparrow})^2)$ は E_i の剰余の canonical lift になる.

注 6. canonical lift とは, 次の Serre と Tate の定理により定義される楕円曲線である.

定理 7 (Serre-Tate)**.**

p を素数とし, F を $\mathbb{Q}_p$ 上の有限次不分岐拡大体, F の剰余体を $\mathbb{F}$ とする. このとき任意の $\mathbb{F}$ 上定義された通常楕円曲線 $\tilde{E}$ に対し, 次の条件を満たす F 上定義された楕円曲線 $E^{\uparrow}$ が F 同型の差を除き唯一つ存在する:

(1) $E^{\uparrow}$ の剰余と $\tilde{E}$ は $\mathbb{F}$ 上同型.

(2) $\mathrm{End}(\tilde{E}) \simeq \mathrm{End}(E^{\uparrow})$.

注 8. canonical lift が $\mathbb{Q}_2$ 上不分岐拡大体上で定義されるため, 定理 5 の $\mu_i^{\uparrow}$ は K の中の $\mathbb{Q}_2$ 上不分岐拡大体の元となる. 各 $\mu_i^{\uparrow}$ は Frobenius により写り合う関係にある.

注 9. 定理 5 の K が $\mathbb{Q}_2$ 上有限次不分岐拡大のときは Gaudry, Satoh, Mestre 等により成立することが示唆されていた ([4] 参照).

2. 極限の存在性と CANONIKAL LIFT の関係性

この節では, 定理 5 の数列 $\{\mu_{dn+i}\}$ の収束性を認めた上で, 2 進算術幾何平均列と canonical lift との関係について解説する.

補題 10.

K, E_n は定理 5 と同様とする. また $\mathbb{F}$ を K の剰余体とし, $\tilde{E}_n$ を E_n の剰余とする.

(1) 各 $n \geq 0$ に対し, $\tilde{E}_{n+1}$ は $\tilde{E}_n$ の 2-Frobenius 捻り $E_n^{(2)}$ と $\mathbb{F}$ 上同型となる.

(2) $\tilde{E}_{n+1}$ と $\tilde{E}_n^{(2)}$ を上の同型により同一視すると次の図式は可換となる:

$$\begin{array}{ccc} E_n(\bar{K}) & \xrightarrow{g_n} & E_{n+1}(\bar{K}) \\ {\scriptstyle \mathrm{red}}\downarrow & \circlearrowleft & {\scriptstyle \mathrm{red}}\downarrow \\ \tilde{E}_n(\bar{\mathbb{F}}) & \xrightarrow[\text{2-Frob.}]{} & \tilde{E}_n^{(2)}(\bar{\mathbb{F}}), \end{array}$$

但し $\bar{K}, \bar{\mathbb{F}}$ はそれぞれ $K, \mathbb{F}$ の代数閉包であり, g_n は (1.3) と同様にして定義される K 上の射である. また図式の縦の写像は還元写像である.

補題 10 の図式を各 n について合成することで次の可換図式を得る:

$$\begin{array}{ccccccccc} E_0(\bar{K}) & \to & E_1(\bar{K}) & \to & \cdots & \longrightarrow & E_d(\bar{K}) & \longrightarrow & \cdots \\ {\scriptstyle \mathrm{red}}\downarrow & & {\scriptstyle \mathrm{red}}\downarrow & & & & {\scriptstyle \mathrm{red}}\downarrow & & \\ \tilde{E}_0(\bar{\mathbb{F}}) & \to & \tilde{E}_0^{(2)}(\bar{\mathbb{F}}) & \to & \cdots & \to & \tilde{E}_0^{(2^d)}(\bar{\mathbb{F}}) = \tilde{E}_0(\bar{\mathbb{F}}) & \to & \cdots, \end{array}$$

但し $\tilde{E}_0$ が $\mathbb{F}$ 上定義されているため $\tilde{E}^{(2^d)} \simeq \tilde{E}_0$ となる. 数列 $\{\mu_{dn+i}\}$ の極限値を $\mu_i^{\uparrow}$ とすると, μ_i を $\mu_i^{\uparrow}$ と取り換えても補題 10 が成立し, それ故 μ_i を $\mu_i^{\uparrow}$ と取り替えた上述と同様の可換図式を得る. 今, $\mu_d^{\uparrow} = \mu_0^{\uparrow}$ であるため $E_d^{\uparrow} \simeq E_0^{\uparrow}$ となる. 従って図式の下の E_0 の Frobenius 自己準同型が $E_0^{\uparrow}$ の自己準同型に持ち上がり, 定理 7 から $E_0^{\uparrow}$ は $\tilde{E}_0$ の canonical lift となる.

3. 2 進体上の楕円曲線と算術幾何平均

この節では 2 進体上定義された楕円曲線の同型類の, 2 進算術幾何平均列を通して見た挙動について解説する. なおこの力学系は, 定理 5 の恩恵により初めて考察できる現象である.

K を $\mathbb{Q}_2$ 上の有限次拡大体とし, v は K 上の加法的付値とする. また $\lambda \in K$ に対し, 楕円曲線 E_λ を

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

で定義されるものとする. 更に $\mu \in K$ が $v(1-\mu) \geq v(8)$ を満たすとき, 帰納的に定義される数列を $\{\mu_n\}$ とおく:

$$\mu_0 := \mu, \quad \mu_{n+1} := \frac{\mu_n + 1}{\sqrt{\mu_n}} \quad (n \geq 0). \tag{3.11}$$

注 12. 式 (3.11) は 1 と μ を初期値とする 2 進算術幾何平均列の比が満たす漸化式である.

case 1. E が K 上で乗法的還元を持つとき, $v(1-\mu) > v(8)$ を満たす $\mu \in K$ が存在して $E \simeq E_{\mu^2}$ となる. そこで数列 $\{\mu_n\}$ を (3.11) として定義する. このとき 2 進算術幾何平均列が同一極限に収束するため, 数列 $\{\mu_n\}$ は 1 に収束することがわかる. 従って $E_{\mu_n^2}$ の j 不変量 $j(E_{\mu_n^2})$ の付値は $-\infty$ に発散する.

case 2. E が K 上で良い通常還元を持つとする. このとき $v(1-\mu) = v(8)$ を満たす $\mu \in K$ が存在して, $E \simeq E_{\mu^2}$ となる. ここで数列 $\{\mu_n\}$ を (3.11) のように定義する. すると定理 5 より数列 $\{\mu_n\}$ は周期的に収束することがわかる. 更に $\{j(E_{\mu_n^2})\}$ は canonical lift の j 不変量に周期的に収束する.

case 3. E が K 上で超特異還元を持つとする. このとき $0 < v(\mu-1) < v(8)$ または $v(\mu) = v(\mu-1) = 0$ をみたす $\mu \in K$ が存在して $E \simeq E_{\mu^2}$ となる. この場合 μ の平方根の標準的な選び方が存在しないため, 2 進算術幾何平均列を関連付けることは出来ない. 各段階で平方根の選び方を固定することで数列 $\{\mu_n\}$ を (3.11) のように強引に定義すると, $\{\mu_n\}$ は発散する. そして $\{j(E_{\mu_n^2})\}$ も発散してしまう. しかし $E_{\mu_n^2}$ の j 不変量の付値は 0 に収束する.

図 1 は, 楕円曲線の同型類を j 不変量を介して $\mathbb{P}^1$ の点と見做した時の上述の様子を視覚化したものである. ここで ordinary の部分の円は, 同じ剰余を持つ楕円曲線の同型類の集合を表している.

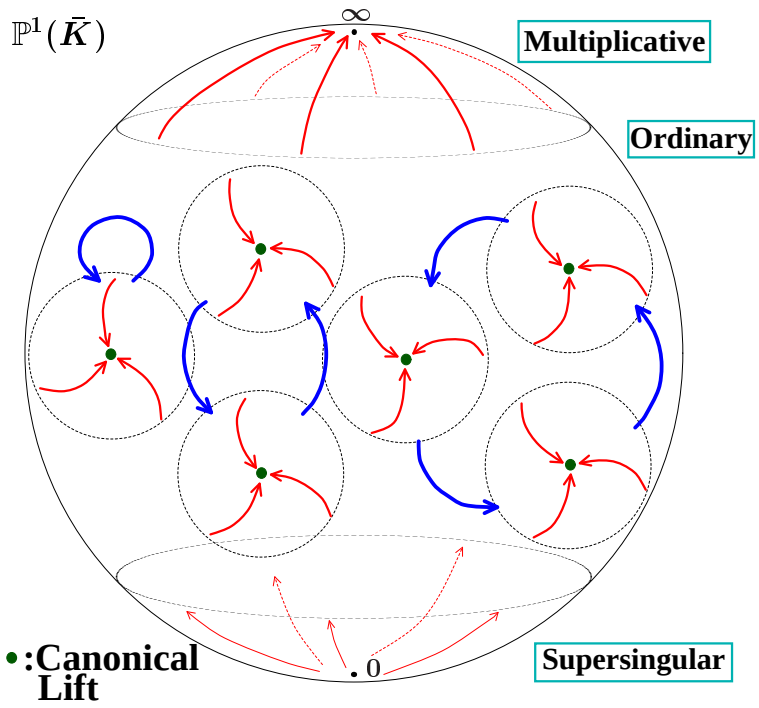

図 1

4. 補足

この節では同一極限に収束する p 進算術幾何平均列と楕円曲線の Hodge-Tate 周期との関係について解説する．これは Gauss による実数体上の算術幾何平均列と楕円曲線の周期の関係の p 進類似となっている．

p を素数とし，K を $\mathbb{Q}_p$ 上の有限次拡大体，v を K 上の付値とする．また $a, b \in K$ は $v((a/b)-1) > v(8)$ を満たすとする．このとき初期値 a, b の p 進算術幾何平均列 $\{a_n\}, \{b_n\}$ は同一極限 $M(a,b)$ に収束する．更に楕円曲線 E_0 を

$$E_0 : y^2 = x(x-1)(x-(a/b)^2)$$

と定義すると E_0 は K 上乗法的還元を持つ．ここで Tate の一意化定理より，ある $q \in K$ $(v(q) > 0)$ が存在して

$$\phi_0 : \bar{K}^\times / \langle q \rangle \simeq E_0(\bar{K})$$

となる．また $dx/y, dt/t$ をそれぞれ $E_0, \mathbb{G}_m/\langle q \rangle$ の不変微分形式とおき，$u \in K^\times$ を

$$\phi_0^*(dx/y) = u \cdot dt/t$$

として定義する．このとき次の定理が成立する．

定理 13 (Henniart-Mestre[2])**.**

$$u^2 = M(a/b, 1)^{-2}.$$

次に E_0 の Tate 加群 $T_p(E_0)$ に対し, $e_{E_0} \in T_p(E_0)$ を次で定義する. 各 $n \geq 0$ に対し, $\epsilon_n \in \{x \in \bar{K}; x^{p^n} = 1\}$ を次のように帰納的に定義する:

$$\epsilon_0 = 1,\ \epsilon_1 \neq 1,\ \epsilon_{n+1}^p = \epsilon_n,\ (n \geq 0).$$

そこで $\epsilon := (\epsilon_n) \in T_p(\bar{K}/\langle q \rangle)$ に対し, $e_{E_0} := \phi_{0*}(\epsilon)$ として定義する (但し $\phi_{0*} : T_p(\bar{K}/\langle q \rangle) \to T_p(E_0(\bar{K}))$ は一意化写像 ϕ_0 が誘導する写像である). このとき定理 13 を用いることで次の定理を得る ([3, Appendix. B] 参照).

定理 14 (Kinjo-Miyasaka)**.**
E_0, ω_0, e_{E_0} は上述の通りとする. また

$$\langle \cdot, \cdot \rangle : T_p(E_0) \times \mathrm{H}^0(E_0, \Omega^1_{E_0}) \to \mathbb{C}_p(1)$$

を Fontaine が [1] で定義した pairing とする (但し $\mathbb{C}_p(1)$ を K の代数閉包を完備化した体 $\mathbb{C}_p$ の Tate 一回捻りとする). このとき

$$\langle e_{E_0}, \omega_0 \rangle = \frac{\varpi}{M(a/b, 1)}$$

が (符号の差を除き) 成立する. 但し $\varpi := \langle \epsilon, dt/t \rangle$ とする.

注 15. 実数 a, b $(a > b > 0)$ を初期値とする算術幾何平均列の極限値を $M(a, b)$ とおく. このとき $\mathbb{R}$ 上の楕円曲線

$$E : y^2 = x(x-1)(x-(a/b)^2)$$

の複素周期は

$$\frac{2\pi i}{M(a/b, 1)}$$

で与えられる. 従って定理 14 は実数体上の楕円曲線の周期の p 進類似となっている.

参考文献

[1] Jean-Marc Fontaine. Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux. *Invent. Math.*, 65(3):379–409, 1981/82.

[2] Guy Henniart and Jean-François Mestre. Moyenne arithmético-géométrique p-adique. *C. R. Acad. Sci. Paris Sér. I Math.*, 308(13):391–395, 1989.

[3] Kinjo Kensaku and Miyasaka Yuken. 2-adic arithmetic-geometric mean and elliptic curves. *to appear.*

[4] Takakazu Satoh. On p-adic point counting algorithms for elliptic curves over finite fields. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 43–66. Springer, Berlin, 2002.