

EDS の p 進極限が, だいたい代数的数になる話

t888

2025 年 11 月 22 日

概要

本稿では参考文献 [2] について論ずる. 然るべき関係式を満たす数列に, 然るべき割り算に関する情報を加えた数列を EDS(elliptic divisibility sequence) という. 名前から察しがつくように, EDS は楕円曲線と密接な関係がある. 本稿では (ある条件を満たす)EDS の p 進極限が代数的数になることを見る.

キーワード: EDS, 楕円曲線, Weierstrass の $\wp, \sigma$ 関数, 代数的数, Weil divisor, Teichmüller 指標

1 Somos 数列の定義と性質 (と言っても一つだけ)

定義 1. k を 4 以上の整数とする. このとき数列 $\{s_n\}_{n \in \mathbb{Z}}$ が

$$s_{n+k}s_n = \sum_{i=1}^{\lfloor k/2 \rfloor} \alpha_i s_{n+k-i} s_{n+i}$$

を満たすとき, **Somos k 数列**であるという. ただし各 α_i は定数である. 特にすべての係数及び初期値を 1 にしたもの ($\alpha_i = 1(\forall i), s_0 = s_1 = \dots = s_{k-1} = 1$) を, **Somos (k) 数列**という.

定理 2. Somos (k) 数列 $\{s_n\}_{n \in \mathbb{Z}}$ に対して, $k = 4, 5, 6, 7$ のとき, すべての n に対して s_n は整数である.

注意 3. Somos (4) 数列の条件式は次のようになる.

$$s_{n+4}s_n = s_{n+3}s_{n+1} + s_{n+2}^2.$$

2 楕円曲線の準備

標数が 2 でない体 K 上の楕円曲線を E が, 次のように Weierstrass 形式で与えられているとする.

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

このとき

$$b_2 := a_1^2 + 4a_2, \quad b_4 := 2a_4 + a_1a_3, \quad b_6 := a_3^2 + 4a_6, \quad b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

とおく. この記号のもとで, **古典的な等分多項式 (division polynomial)** $\psi_n \in \mathbb{Z}[a_1, \dots, a_6, x, y]$ は次の漸化式で定義される.

$$\begin{aligned}\psi_0 &= 0, \quad \psi_1 = 1, \quad \psi_2 = 2y + a_1x + a_3, \quad \psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\ \psi_4 &= \psi_2 \cdot (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)), \\ \psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \quad (n \geq 2), \\ \psi_2\psi_{2n} &= \psi_{n-1}^2\psi_n\psi_{n+2} - \psi_{n-2}\psi_n\psi_{n+1}^2 \quad (n \geq 3), \\ \psi_{-n} &= -\psi_n \quad (n < 0).\end{aligned}$$

さらに二つの多項式 ϕ_n, ω_n を次のように定める.

$$\begin{aligned}\phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \\ 2(2y + a_1x + a_3)\omega_n &= \psi_{n-1}^2\psi_{n+2} + \psi_{n-2}\psi_{n+2}^2.\end{aligned}$$

このとき楕円曲線 E 上のねじれ点ではない任意の点 $P = (x_1, y_1)$ に対して, $[n]P = (x_n, y_n)$ は次のように表される.

$$(x_n, y_n) = \left(\frac{\phi_n(x_1, y_1)}{\psi_n(x_1, y_1)^2}, \frac{\omega_n(x_1, y_1)}{\psi_n(x_1, y_1)^3} \right).$$

この議論の流れは [3]ExerciseIII.3.7. を参照せよ. ここで証明は (計算が多いという意味で) 大変なのだが, 次が成り立つ.

定理 4. $m \geq n \geq 1$ に対して, 次が成り立つ.

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_n^2\psi_{m+1} - \psi_{n-1}\psi_m^2\psi_{n+1}.$$

次に $K = \mathbb{C}$ として, 楕円曲線 $E/\mathbb{C}$ について考える. このとき Riemann 面としての同型

$$\mathbb{C}/\Lambda \rightarrow E(\mathbb{C}), \quad z \mapsto [\wp(z), \wp'(z), 1]$$

が存在するような格子 $\Lambda \subset \mathbb{C}$ がとれる. ただし $\wp(z)$ は以下で定義される Weierstrass の $\wp$ 関数である.

$$\wp(z) = \wp(z, \Lambda) := \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

また **Weierstrass の σ 関数** を次で定める.

$$\sigma(z) = \sigma(z, \Lambda) := z \prod_{0 \neq \omega \in \Lambda} \left(1 - \frac{z}{\omega} \right) e^{(z/\omega) + \frac{1}{2}(z/\omega)^2}.$$

この二つの関数には, 次のような関係がある.

$$\frac{d^2}{dz^2} \log \sigma(z) = -\wp(z) \quad (z \in \mathbb{C} \setminus \Lambda).$$

この議論の流れは [3]VI を参照せよ. ここで証明は (計算が多いという意味で) 大変なのだが, 次が成り立つ.

$$\begin{aligned}
\psi_2(z) &= -\wp'(z), \\
\wp(2z) - \wp(z) &= \frac{1}{4} \left(\frac{\wp''(z)}{\wp'(z)} \right)^2 - 3\wp(z), \\
\wp(2z) - \wp(z) &= -\frac{\psi_1(z)\psi_3(z)}{\psi_2^2(z)}, \\
\wp(3z) - \wp(z) &= \frac{\wp'^2(z)(\wp'^4(z) - \psi_3(z)\wp''(z))}{\psi_3^2(z)}, \\
\wp(3z) - \wp(z) &= -\frac{\psi_2(z)\psi_4(z)}{\psi_3^2(z)}, \\
\wp''(z) &= 6\wp^2(z) - \frac{g_2}{2}.
\end{aligned}$$

ただし $g_2 = 60 \sum_{0 \neq \omega \in \Lambda} 1/\omega^4$ である.

3 Teichmüller 指標

本節では $\mathbb{Z}_p$ 上の Teichmüller 指標を定義する. その際 $p = 2$ のときとそれ以外のときで微妙に定義の仕方が異なるが, $p = 2$ のときは本稿には必要ないので, 以下では $p \geq 3$ のときについてのみ考える. 詳しくは [2, 7] を参照.

p を奇素数とする. $p \nmid a$ となる任意の $a \in \mathbb{Z}_p$ に対して

$$a \equiv \chi(a) \pmod{p}$$

となる 1 の原始 $p-1$ 乗根 $\chi(a) \in \mathbb{Z}_p$ が唯一つ存在する. これを示そう.

まず任意の $\epsilon > 0$ に対して $N \geq 1$ を $p^{-(N+1)} < \epsilon$ となるようにとる. このとき $m \geq n \geq N$ に対して

$$\begin{aligned}
a^{p^m - p^n} &= (a^{p^N(p-1)})^{p^{n-N}(p^{m-n-1} + p^{m-n-2} + \dots + p+1)} \\
&\equiv 1 \pmod{p^{N+1}} \quad (\because \#(\mathbb{Z}_p/p^{N+1}\mathbb{Z}_p)^* = p^N(p-1))
\end{aligned}$$

より, $a^{p^m} \equiv a^{p^n} \pmod{p^{N+1}}$ が得られるので, 次が成り立つ.

$$|a^{p^m} - a^{p^n}|_p \leq p^{-(N+1)} \leq \epsilon.$$

以上から, まず $\{a^{p^n}\}_{n \geq 1}$ は Cauchy 列であることが分かった.

さて, $\mathbb{Q}_p$ は完備であるので, $\{a^{p^n}\}_{n \geq 1}$ は収束する. さらに $a^{p^n} \in \mathbb{Z}_p$ であり, $\mathbb{Z}_p$ は $\mathbb{Q}_p$ の閉部分集合であるから, $\lim_{n \rightarrow \infty} a^{p^n} \in \mathbb{Z}_p$ である. よって $\chi(a) := \lim_{n \rightarrow \infty} a^{p^n}$ とおけば

$$a \equiv \chi(a) \pmod{p\mathbb{Z}_p}$$

であり, $\#(\mathbb{Z}_p/p^{N+1}\mathbb{Z}_p)^* = p^N(p-1)$ に注意すれば

$$\chi(a)^{p-1} = \lim_{n \rightarrow \infty} a^{p^n(p-1)} = 1$$

となるので, $\chi(a)$ は 1 の原始 $p-1$ 乗根であることが分かった.

次に $\chi(a)$ の一意性を示す. 1 の原始 $p-1$ 乗根全体の集合を $\mu_p(\mathbb{Q}_p)$ で表す. すなわち

$$\mu_p(\mathbb{Q}_p) := \{\zeta \in \mathbb{Q}_p \mid \zeta^{p-1} = 1\}.$$

$\#\mu_p(\mathbb{Q}_p) = p - 1$ より, 各 $\bar{a} \in (\mathbb{Z}_p/p\mathbb{Z}_p)^*$ に対して, $a \equiv \chi(a)$ となる $\chi(a) \in \mu_p(\mathbb{Q}_p)$ は唯一つであることが分かる.

以上の議論から, 準同型

$$\chi: (\mathbb{Z}_p/p\mathbb{Z}_p)^* \rightarrow \mu_p(\mathbb{Z}_p)$$

が得られた. $\chi(p\mathbb{Z}_p) = 0$ とすることで, χ は次のように拡張できる.

$$\chi: \mathbb{Z}_p \rightarrow \mathbb{C}_p.$$

これを **Teichmüller 指標** という.

この $\mathbb{Z}_p$ 上の Teichmüller 指標の一般化として, $\mathbb{Z}_p$ 上の群スキーム上の Teichmüller 指標について定義する. $K/\mathbb{Q}_p$ を有限次拡大, R_K を K の整数環, $\mathfrak{p}_K$ を K の極大イデアル, k_K を K の剰余体, G/R_K を群スキームとする. 任意の点 $a \in G(R_K)$ に対して, 特殊ファイバー $G(k_K)$ における $\text{ord}(a \bmod p)$ を $\tau(a)$ で表す. このとき

$$G'(R_K) := \{a \in G(R_K) \mid p \nmid \tau(a)\}$$

と定義する. 還元写像 $G(R_K) \rightarrow G(k_K)$ の核を $G_1(R_K)$ とする. このとき $G_1(R_K)$ は副 p 群である. $q = p^e$ を, $q \equiv 1 \pmod{\tau(a)}$ となる最小のものとする. このとき $a^q \equiv a \pmod{\mathfrak{p}_K}$ であるので, $i < j$ に対して次が成り立つ.

$$a^{q^i} \cdot a^{-q^j} = (a^{q^{j-i}} - 1)^{q^j} \rightarrow 1_G \quad (i > j \rightarrow \infty).$$

ここで $a^{-q^{j-i}} \equiv a \pmod{\mathfrak{p}_K}$ より, $a^{-q^{j-i}-1} \in G_1(R_K)$ であることに注意する. よって $p^k \equiv 1 \pmod{\tau(a)}$ となる a に対して, $\{a^{p^k}\}_{k \geq 1}$ は Cauchy 列であることが分かった. すなわち極限

$$\chi(a) := \lim_{\substack{k \rightarrow \infty \\ p^k \equiv 1 \pmod{\tau(a)}}} a^{p^k}$$

は収束する. この χ も **Teichmüller 指標** という.

4 楕円数列

定義 5. 以下の条件を満たす数列 $\{W_n\}_{n \in \mathbb{Z}}$ を, **EDS(elliptic divisibility sequence)** という.

1. $W_{m+n}W_{m-n} = W_{m+1}W_n^2W_{m-1} - W_{n+1}W_m^2W_{n-1} \quad (m, n \in \mathbb{Z}),$
2. $n \mid m$ のとき, $W_n \mid W_m$.

注意 6. 条件式 1 において, $m = n = 0$ を代入すると, $W_0 = 0$ が得られる. また条件式 1 に $m = 0, n = 1$ を代入すると, $W_1 = \pm 1$ が得られる. 以下では $W_1 = 1$ を仮定する.

注意 7. $W_1 = 1$ より, EDS の条件式 1 において $W_{-1} = -1$ が成り立つことが分かる. さらに条件式 1 において $m = 0$ を代入すると, $W_{-n} = -W_n$ が得られる.

注意 8. 条件式 1 において, $n = 2$ を代入して $m = n - 2$ とすると

$$W_{n+4}W_n = W_2^2W_{n+3}W_{n+1} - W_1W_3W_{n+2}^2$$

が得られる。さらに $W_2 = W_3 = 1$ とすると、 $W_{-1} = -1$ に注意すれば

$$W_{n+4}W_n = W_{n+3}W_{n+1} + W_{n+2}^2$$

となり、この EDS は Somos (4) 数列であることが分かる。つまりすべての整数 n に対して、 W_n は整数である。

EDS の基本事項を述べる。そのために一言葉遣いを導入する。

定義 9. 一般の数列 $\{a_n\}_{n \in \mathbb{Z}}$ に対して、次の二つの条件を満たすとき、 $\{a_n\}_{n \in \mathbb{Z}}$ は *proper* であるという。

1. $a_0 = 0, a_1 = 1,$
2. $a_2 \neq 0$ or $a_3 \neq 0.$

これに加えて、次の条件を満たすとき、 $\{a_n\}_{n \in \mathbb{Z}}$ は *general* であるという。

$$a_2 \neq 0 \text{ かつ } a_3 \neq 0.$$

命題 10. EDS の条件式 1 の $W_{m+n}W_{m-n} = W_{m+1}W_n^2W_{m-1} - W_{n+1}W_m^2W_{n-1}$ を満たす *proper* な数列 $\{W_n\}_{n \in \mathbb{Z}}$ に対して、次の同値が成り立つ。

$$\{W_n\}_{n \in \mathbb{Z}} \text{ は EDS である。} \iff W_2, W_3, W_4 \text{ は整数で、} W_2 \mid W_4 \text{ を満たす。}$$

証明. $\Rightarrow$ は明らかなので $\Leftarrow$ を示す。まず $\{W_n\}_{n \in \mathbb{Z}}$ は整数列であり、さらに $W_2 \mid W_{2n}$ であることを示す。次に $n \mid m$ ならば $W_n \mid W_m$ となることを示す。これは帰納法で示すのだが、次の補題が成り立つことに注意する。

補題 11. EDS の条件式 1 の $W_{m+n}W_{m-n} = W_{m+1}W_n^2W_{m-1} - W_{n+1}W_m^2W_{n-1}$ を満たす *proper* な数列 $\{W_n\}_{n \in \mathbb{Z}}$ に対して、もし $W_m = W_{m+1}$ が成り立つような m が存在するならば、 $\forall n \geq 3$ に対して、 $W_n = 0$ である。

最後に一意性について。EDS の条件式 1 において $m \mapsto n+1$ や $m \mapsto n+1, n \mapsto n-1$ などとすることで

$$\begin{aligned} W_{2n+1}W_1 &= W_{n+2}W_n^3 - W_{n+1}W_{n-1} & (n \geq 1), \\ W_{2n}W_2 &= W_n(W_{n+2}W_{n-1}^2 - W_{n-2}W_{n+1}^2) & (n \geq 2) \end{aligned}$$

が得られる。特に $W_n = 1$ なら次が得られる。

$$\begin{aligned} W_{2n+1} &= W_{n+2}W_n^3 - W_{n+1}^3W_{n-1} & (n \geq 1), \\ W_{2n}W_2 &= W_n(W_{n+2}W_{n-1}^2 - W_{n-2}W_{n+1}^2) & (n \geq 2). \end{aligned}$$

これより W_2, W_3, W_4 が与えられれば、すべての項 W_n が一意に定まる。 □

EDS の由来について考える。Divisibility は EDS の条件 2 のことで、Sequence は数列の英訳であることはすぐに分かる。Elliptic の部分は、次で述べるように楕円曲線に由来している。

定理 12 (Ward). *general* な EDS $\{W_n\}_{n \in \mathbb{Z}}$ に対して次が成り立つような格子 Λ (と、それに付随する楕円曲線 E) が存在する。

$$W_n = \frac{\sigma(nz)}{\sigma(z)^{n^2}}.$$

これは定理 4 と, 次に述べる補題から従う.

補題 13. $W_2 \mid W_4, W_2 \neq 0, W_4 \neq 0$ を満たす整数の組 (W_2, W_3, W_4) に対して, $g_2, g_3 \in \mathbb{Q}$ と $z \in \mathbb{C}$ が存在し, 対応する $\wp$ 関数に対して次が成り立つ.

$$W_2 = \psi_2(z), W_3 = \psi_3(z), W_4 = \psi_4(z).$$

証明. 以下では $\psi_n(z)$ を ψ_n と略す. $W_2, W_3 \neq 0$ に対して次が成り立つ.

$$\begin{aligned} W_2 = \psi_2, W_3 = \psi_3, W_4 = \psi_4 \\ \iff W_2 = \psi_2, W_3 = \psi_3, \frac{W_2 W_4}{W_3^2} &= \frac{\psi_2 \psi_4}{\psi_3^2} \\ \iff -\wp' = W_2, W_3 = \psi_3, -\frac{\wp'^2(\wp'^4 - \psi_3 \wp'')}{\psi_3^2} &= \frac{W_2 W_4}{W_3^2} \\ \iff -\wp' = W_2, W_3 = \psi_3, \frac{W_2^4(-W_2^4 + W_3 \wp'')}{W_3^2} &= \frac{W_2 W_4}{W_3^2} \\ \iff -\wp' = W_2, \frac{W_3}{W_2^2} = \frac{\psi_3}{\psi_2^2}, \wp'' = \frac{W_2^5 + W_4}{W_2 W_3} &=: H \\ \iff -\wp' = W_2, \frac{W_3}{W_2^2} = \frac{1}{4} \frac{H^2}{W_2^2} + 3\wp, \wp'' = H \\ \iff -\wp' = W_2, \wp = \frac{H^2 + 4W_3}{12W_2^2} &=: G, 6\wp^2 - \frac{g_2}{2} = H \\ \iff -\wp' = W_2, \wp = G, g_2 = 12G^2 - 2H \\ \iff -\wp' = W_2, \wp = G, g_2 = 12G^2 - 2H, g_3 = 4\wp^3 - g_2\wp - \wp'^2 \\ \iff \wp' \text{ と } W_2 \text{ は異符号, } \wp = G, g_2 = 12G^2 - 2H, g_3 = 4G^3 - g_2G - W_2^2. \end{aligned}$$

よって $\wp'$ と W_2 が異符号になるような $z \in \mathbb{C}$ が格子のずれを除いて一意に定まる. □

注意 14. この定理は, 一般の Somos 4 数列に拡張できる. すなわち次が成り立つ.

Somos 4 数列 $\{s_n\}_{n \in \mathbb{Z}}$ に対して, 次が成り立つような格子 Λ と複素数 $a, b, u, v \in \mathbb{C}$ が存在する.

$$s_n = ab^n \frac{\sigma(nu + v)}{\sigma(u)^{n^2}}.$$

上の定理の代数的に言い換えると, 以下の通りである.

定理 15. $EDS\{W_n\}_{n \in \mathbb{Z}}$ に対して, $\mathbb{Q}$ 上定義された楕円曲線 E と $\mathbb{Q}$ -有理点 $P = (x, y) \in E(\mathbb{Q})$ が存在して, 次を満たす.

$$W_n = \psi_n(x, y).$$

例 16.

$$\begin{aligned} W_0 = 1, W_1 = 1, W_2 = 1, W_3 = -1, W_4 = -2, W_5 = -3, W_6 = -1, W_7 = 7, W_8 = 11, \\ W_9 = 20, W_{10} = -19, W_{11} = -87, W_{12} = -191, \dots \end{aligned}$$

は $E: y^2 + y = x^3 + x^2$ 上の点 $P(0, 0)$ に関する楕円数列である.

例 17.

$$W_0 = 1, W_1 = 1, W_2 = 1, W_3 = -3, W_4 = 11, W_5 = 38, W_6 = 249, W_7 = -2357, \dots$$

は $E: y^2 + y = x^3 + x^2 - 2x$ 上の点 $P(0, 0)$ に関する EDS である.

例 18.

$$W_0 = 1, W_1 = 1, W_2 = -1, W_3 = 1, W_4 = 2, W_5 = -1, W_6 = -3, W_7 = -5, W_8 = 7, W_9 = -4, W_{10} = -23, W_{11} = 29, \\ W_{12} = 59, W_{13} = 129, W_{14} = -314, W_{15} = -65, W_{16} = 1529, W_{17} = -3689, W_{18} = -8209, W_{19} = -16264 \dots$$

は $E: y^2 + y = x^3 - x$ 上の点 $P(0, 0)$ に関する EDS である.

5 EDS の同値類を用いて, EDS を分類する

この節では EDS に以下で定義する同値類により, EDS のある種具体的な表示を与える.

定義 19 (数列の同値関係). $\mathbb{C}$ 上の数列 $\{a_n\}, \{b_n\}$ に対して, 同値関係 $\sim$ を次で定める.

$$\{a_n\} \sim \{b_n\} \iff \exists c \neq 0 \text{ s.t. } \forall n, b_n = c^{n^2-1} a_n.$$

また $\overline{\mathbb{Q}}$ 上の数列 $\{a_n\}$ がある整数列に同値である (すなわち $c \in \overline{\mathbb{Q}} \setminus \{0\}$ が存在して, $ca_n^{n^2-1} \in \mathbb{Z}$ が成り立つ) とき, $\{a_n\}$ は *essentially integral* であるという.

命題 20. $\{W_n\}$ を, $\wp(z; g_2, g_3)$ による表示を持つとする EDS とする. また $W_2 \neq 0$ かつ $W_3 \neq 0$ とする. このとき

証明. $\wp(z/c; c^4 g_2, c^6 g_3)$ の表示を持つ数列の四項目まで計算すれば分かる. □

以下では EDS の条件式

$$W_{m+n}W_{m-n} = W_{m+1}W_n^2W_{m-1} - W_{n+1}W_m^2W_{n-1} \quad (1)$$

を満たす数列を, 同値関係を用いて分類する.

命題 21 ($W_1 = 1$ となる解). 式 (1) を満たす $\mathbb{Q}$ 上の数列 $\{W_n\}$ は $W_0 = 0, W_1 = 1$ かつ $W_2 \neq 0$ または $W_3 \neq 0$ を満たすとする. このとき $\{W_n\}$ は *essential integral* である. 特に $W_2 \neq 0$ ならば, ある EDS と同値である.

命題 22 ($W_1 \neq \pm 1$ となる解). 式 (1) を満たす $\mathbb{C}$ 上の数列 $\{W_n\}$ は $W_1 \neq \pm 1$ を満たすとする. このとき $k, l \in \mathbb{Z}_{\geq 0}, \alpha, \beta \in \mathbb{C}$ が存在して, 次を満たす.

$$W_n = \begin{cases} \alpha & (n = 2k), \\ \beta & (n = 2l + 1), \\ 0 & (\text{otherwise}). \end{cases} \quad (2)$$

命題 23 ($W_2 = 0, W_3 \neq 0$ となる解). 式 (1) を満たす $\mathbb{C}$ 上の数列 $\{W_n\}$ は $W_1 = 1, W_2 = 0, W_3 \neq 0$ を満たすとする. このとき $m \in \mathbb{Z}_{\geq 1}$ に対して次が成り立つ.

$$W_m = \begin{cases} 0 & (m \text{ が偶数}), \\ (-1)^{n+1} W_3^{n(n+1)/2} & (m = 2n + 1). \end{cases} \quad (3)$$

命題 24 ($W_3 = 0$ となる解). 式 (1) を満たす $\mathbb{C}$ 上の数列 $\{W_n\}$ は $W_0 = 0, W_1 = 1, W_3 = 0$ を満たすとする. このとき次のいずれかが成り立つ.

1. 次を満たす $m \in \mathbb{Z}_{\geq 1}, \alpha \in \mathbb{C}$ が存在する.

$$W_n = \begin{cases} 1 & (n = 1), \\ \alpha & (n = 2m), \\ 0 & (\text{otherwise}). \end{cases} \quad (4)$$

2. 3 以上の奇数 l に対して, 数列 $\{\lambda_n(l)\}$ を

$$\lambda_n(l) = \begin{cases} 1 & (n \equiv 1 \pmod{l}), \\ -1 & (n \equiv -1 \pmod{l}), \\ 0 & (otherwise). \end{cases} \quad (5)$$

で定めると, $c \in \mathbb{C}^*$ に対して $\{\lambda_n c^{1-n\lambda_n}\}$ に同値である.

以上をまとめると次のようになる.

命題 25. 式 (1) を満たす $\mathbb{C}$ 上の数列 $\{W_n\}$ は, 有限個を除いて 0 になるものと, 次のいずれかに同値なものである.

$$W_n = \frac{\sigma(nz)}{\sigma^{n^2}(z)}, \quad W_n = \begin{cases} 0 & (n \text{ は偶数}) \\ (-1)^{\frac{n-1}{2}} W_3^{\frac{(n-1)(n+1)}{4}} & (n \text{ は奇数}) \end{cases}, \quad W_n = \lambda_n c^{1-n\lambda_n}.$$

σ によるものは, さらに singular なもの (対応する楕円曲線の判別式が 0), $W_n = n$ とそれ以外に分けられる. 「それ以外」のものは Lucas sequence と呼ばれ, $\frac{\sin nz}{\sin z}$ と表される数列と同値であることが知られている. これを踏まえると次のようになる.

命題 26. 式 (1) を満たす $\mathbb{C}$ 上の数列 $\{W_n\}$ は, 有限個を除いて 0 になるものと, 次のいずれかに同値なものである.

$$W_n = n, \quad W_n = \frac{\sin nz}{\sin z}, \quad W_n = \frac{\sigma(nz)}{\sigma^{n^2}(z)}, \quad W_n = \lambda_n c^{1-n\lambda_n}.$$

6 主定理

予想 27. $\{W_n\}_{n \in \mathbb{Z}}$ を EDS とし, p を素数とする. このとき, ある正整数 $N = N_p$ が存在して, すべての正整数 m に対して極限

$$\lim_{k \rightarrow \infty} W_{mp^{kN}}$$

は $\mathbb{Z}_p$ において収束し, さらに代数的数である.

注意 28. 整数係数多項式の根のことを代数的数という.

この予想は次に述べるように, “ほとんど” の EDS と “ほとんど” の素数について成り立つ.

主定理 29 ([2, Theorem20]). $\{W_n\}_{n \in \mathbb{Z}}$ を EDS とし, 対応する楕円曲線 E は $\mathbb{Q}$ 上最小 Weierstrass 形式で与えられているとする. また $\mathbb{Q}$ -有理点 $P \in E(\mathbb{Q})$ をとり, S は以下の条件のいずれかを満たす素数 p の集合とする.

1. $p = 2$,
2. $P \equiv \mathcal{O} \pmod{p}$,
3. $P \pmod{p}$ は $E \pmod{p}$ の特異点,
4. $E \pmod{p}$ は超特異.

このとき $p \notin S$ を満たすすべての素数 p に対して, 正整数 $N = N_P$ が存在して, すべての正整数 m に対して極限

$$\lim_{k \rightarrow \infty} W_{mp^{kN}}$$

は $\mathbb{Z}_p$ において収束し, さらに代数的数である.

以下ではこの主定理 28 の証明を行う.

定義 30. 正整数 n に対して $[n](z) \in K[[z]]$ を, 楕円曲線 E/K の形式群における n 倍写像とする. ω を E の不変微分とする. このとき (素元 z に関する) **正規化された n 等分多項式** $F_n \in K(E)$ を

1. $(F_n) = [n]^*(\mathcal{O}) - n^2(\mathcal{O})$ as a divisor,
2. $\left(\frac{z^{n^2} F_n}{[n](z)} \right) (\mathcal{O}) = \left(\frac{\omega}{dz}(\mathcal{O}) \right)^{1-n^2}.$

を満たす唯一の有理関数として定める.

注意 31. 関数が定める因子について復習しておく. $K(E)$ を楕円曲線 E/K の関数体とし, $f \in K(E)$ に対して, f に付随する因子を次のように定める.

$$(f) = \text{div}(f) := \text{ord}_{P \in E}(f)(P).$$

n 等分多項式 F_n の条件式 1 において, F_n の極と零点の情報が決定され, 条件式 2 でスカラーの調節をしているので, F_n は一意に定まる.

注意 32. $n \neq 0$ (in K) なら, $[n](z) = nz + O(z^2)$ である. よって正規化された n 等分多項式 F_n の条件式 2 は, 次が成り立つことに他ならない.

$$(z^{n^2-1}F_n)(\mathcal{O}) = n.$$

補題 33. すべての正整数 m, n に関して, 次が成り立つ.

$$F_{mn} = (F_n \circ [m]) \cdot F_m^{n^2}.$$

証明. F_n の条件式をもとに, 計算を頑張る. □

補題 34. $E/\mathbb{C}$ を楕円曲線とし, $\Phi: \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$ を同型射とする. また E に付随する古典的な n 等分多項式を ψ_n とし, 正規化された n 等分多項式を F_n とする. このとき次を満たす定数 $\gamma \in \mathbb{C}^*$ が存在する.

$$F_n(\Phi(\zeta)) = \gamma^{1-n^2} \psi_n(\zeta) \quad (\zeta \in \mathbb{C}, n \geq 1).$$

証明. $\mathbb{C}/\Lambda$ における n 等分多項式 ψ_n は $F_n \circ \Phi$ と同じ因子を持つ (ψ_n の極と零点に関する情報は F_n と一致している. 特に $(F_n) = [n]^*(\mathcal{O}) - n^2(\mathcal{O})$ が成り立つ) ので

$$F_n(\Phi(\zeta)) = c_n \psi_n(\zeta) \quad (\zeta \in \mathbb{C}) \tag{6}$$

となる (n に依る) 定数 c_n が存在する. さて, Wierstrass の σ 関数は $\sigma(\zeta) = \zeta + O(\zeta^2)$ ($\zeta \rightarrow 0$) を満たすので, $\psi_n = \frac{\sigma(n\zeta)}{\sigma(\zeta)^{n^2}}$ に注意すれば次が成り立つ.

$$\psi_n(\zeta) = \frac{n}{\zeta^{n^2-1}}(1 + O(\zeta^2)) \quad (\zeta \rightarrow 0).$$

ここで Φ は同型射で, ζ と z はそれぞれ 0 の近くで 0 となり, $\mathcal{O} = \Phi(0)$ であるから, 次を満たす $\gamma \in \mathbb{C}^*$ が存在する.

$$(z \circ \Phi)(\zeta) = \gamma \zeta + O(\zeta^2) \quad (\zeta \rightarrow 0).$$

よって次が得られる.

$$F_n(\Phi(\zeta)) = F_n(\gamma \zeta + O(\zeta^2)) = \frac{n}{(\gamma \zeta)^{n^2-1}}(1 + O(\zeta^2)) = \gamma^{1-n^2} \psi_n(\zeta).$$

これと式 (1) より, 題意が得られる. □

補題 35. $\{W_n\}_n$ を非特異な EDS とし, 対応する楕円曲線を $E/\mathbb{Q}$, 非特異な点を $P \in E(\mathbb{Q})$ とする. また F_n を E 上の正規化された n 等分多項式とする. このとき次を満たす $\gamma \in \mathbb{Q}^*$ が存在する.

$$W_n = \gamma^{n^2-1} F_n(P) \quad (n \geq 1).$$

さらに $P \bmod p$ が非特異となるような素数 p に対して, $\text{ord}_p(\gamma) \geq 0$ である.

証明. EDS $\{W_n\}_n$ に付随する格子 Λ と $\xi \in \mathbb{C}$ をとる. すなわち $W_n = \psi_n(\xi)$ とする. また $\Phi: \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$ を同型射とする. このとき補題 33 より, 次を満たす $\gamma \in \mathbb{C}$ が存在する.

$$F_n(\Phi(\zeta)) = \gamma^{1-n^2} \psi_n(\zeta) \quad (\zeta \in \mathbb{C}, n \geq 1).$$

$\zeta = \xi, \mathcal{P} = \Phi(\xi)$ と置き換えることにより、次が得られる.

$$F_n(\mathcal{P}) = \gamma^{1-n^2} \psi_n(\xi) = \gamma^{1-n^2} W_n \quad (\forall n \geq 1).$$

上式において $n = 2, 3$ を代入すると、仮定より $P \in E(\mathbb{Q})$ であるから、それぞれ $\gamma^3, \gamma^8 \in \mathbb{Q}$ が得られる. それゆえ $\gamma \in \mathbb{Q}$ となる ($\gamma^8 = (\gamma^2)^3 \cdot \gamma^2$ ゆえ $\gamma^2 \in \mathbb{Q}$ で, $\gamma^3 = \gamma \cdot \gamma^2$ に注意せよ). さて $W_n \in \mathbb{Z}$ に注意すると、次が分かる.

$$\text{ord}_p(F_n(P)) = \text{ord}_p(W_n) - (n^2 - 1)\text{ord}_p(\gamma) \geq -(n^2 - 1)\text{ord}_p(\gamma).$$

$P \bmod p$ が非特異となるような素数 p をとる. このとき $P \bmod p$ の order は 2, 3 をそれぞれとらないので, $F_2(P)$ と $F_3(P)$ の少なくとも一方は $\not\equiv 0 \bmod p$ である. よって上の不等式より

$$0 = \text{ord}_p(F_2(P)) \geq -3\text{ord}_p(\gamma) \quad \text{or} \quad 0 = \text{ord}_p(F_3(P)) \geq -8\text{ord}_p(\gamma)$$

が成り立つので, $\text{ord}_p(\gamma) \geq 0$ が得られる. □

この補題 34 により

$$W_n = \gamma^{n^2-1} F_n(\mathcal{P}) \quad (n \geq 1). \tag{7}$$

を満たす有理数 $\gamma \in \mathbb{Q}^*$ が取れる. 今 $P \bmod p$ は非特異であると仮定しているので, $\text{ord}_p(\gamma) \geq 0$ である. よって, もし $\text{ord}_p(\gamma) > 0$ ならば

$$\text{ord}_p(W_n) \geq (n^2 - 1)\text{ord}_p(\gamma) \rightarrow \infty \quad (n \rightarrow \infty)$$

となるので, $\lim_{n \rightarrow \infty} W_n = 0$ (in $\mathbb{Z}_p$) が得られる. もちろん 0 は代数的数であることに注意する.

以下では $\text{ord}_p(\gamma) = 0$ とする. すなわち $\gamma \in \mathbb{Z}_p^*$ とする. Teichmüller 指標 χ を用いて, すべての正整数 m に対して次が得られる.

$$\lim_{k \rightarrow \infty} \gamma^{mp^k-1} = \chi(\gamma)^m \gamma^{-1} \quad (\text{in } \mathbb{Z}_p).$$

よって, 等式 (2) より, すべての正整数 m に対して, 極限 $\lim_{k \rightarrow \infty} F_{mq^k}(P)$ が $(\mathbb{Z}_p$ において) 収束するような p べき $q = p^N$ が存在して, さらにこれが代数的数であることを示せばよい ($\chi(\gamma) \in \mu_{p-1}$ は代数的数であることに注意).

補題 36 ((Mazur-Tate の p 進 σ 関数)). $K/\mathbb{Q}_p$ を有限次拡大とし, R_K を K の整数環とする. また E/K を楕円曲線とし, E の Néron モデル $\mathcal{E}/R_K$ は $p \geq 3$ で *good ordinary reduction* を持つとし, $\mathcal{E}^f$ を $\mathcal{E}$ の形式群とする. このとき次を満たすべき級数 $\sigma \in z + z^2 R_K[[z]]$ が唯一つ存在する.

$$\sigma(n\mathcal{Q}) = \sigma(\mathcal{Q})^{n^2} F_n(\mathcal{Q}) \quad (\mathcal{Q} \in \mathcal{E}^f(\overline{R_K})).$$

証明. σ の構成のみ述べる. 詳しくは [5] を参照して頂きたい. $C_n := \text{Ker}([p^n]: \mathcal{E}^f \rightarrow \mathcal{E}^f)(\subset \mathcal{E}^f(R_K))$ とおくと, 包含 $0 \subset C_1 \subset C_2 \subset \dots$ が得られる. さらに $E_n := (E/C_n)(R_K)$ とおくと, p 倍写像のなす列 $E = E_0 \rightarrow E_1 \rightarrow E_2 \rightarrow \dots$ が得られる. この列により, 合成写像 $b_n: E_0 \rightarrow E_n$ が得られ, また $a_n: E_n \rightarrow E_0$ を

$$a_n \circ b_n = [p^n]_{E_0}, \quad b_n \circ a_n = [p^n]_{E_n}$$

を満たす唯一の同種写像として定める. このとき形式群としての同型

$$a_n^f: \mathcal{E}_n^f \xrightarrow{\cong} \mathcal{E}^f$$

が引き起こされる. さて関数 $\phi_n, \widehat{\phi}_n$ をそれぞれ次が成り立つように定める.

$$(\phi_n) = a_n^{-1}(\mathcal{O}) - p^{-n}\mathcal{O}, \quad \widehat{\phi}_n \circ a_n = \phi_n|_{\mathcal{E}_n^f}$$

$p > 2$ のとき, $\sigma = \sigma_E \in R_K[[t]]$ を次で定める.

$$\sigma := \lim_{n \rightarrow \infty} \sigma_n, \quad \sigma_n := \left. \frac{\omega}{dt} \right|_{t=0} (t^{p^n} \widehat{\phi}_n).$$

一方 $p = 2$ のとき, $\sigma^2 = \sigma_E^2 \in R_K[[t]]$ を次で定める.

$$\sigma^2 := \lim_{n \rightarrow \infty} \sigma_n, \quad \sigma_n^2 := \left. \left(\frac{\omega}{dt} \right)^2 \right|_{t=0} (t^{2p^n} \widehat{\phi}_n^2).$$

実はこのように定めた関数 σ が題意を満たすことが示せる. □

$r := \text{ord}(P \bmod \mathfrak{p}_K)$ に対して, 補題 32 より

$$(F_r \circ [n]) \cdot F_n^{r^2} = F_{nr} = F_{rn} = (F_n \circ [r]) \cdot F_r^{n^2}$$

が得られるので, 次が成り立つ.

$$F_n^{r^2} = \frac{(F_n \circ [r]) \cdot F_r^{n^2}}{F_r \circ [n]}.$$

よって $P \in E$ に対して, 次のように計算できる.

$$\begin{aligned} F_n^{r^2}(P) &= \frac{(F_n(rP))F_r(P)^{n^2}}{F_r(nP)} \\ &= \frac{(\sigma(nrP)/\sigma(rP)^{n^2})F_r(P)^{n^2}}{F_r(nP)} \\ &= \frac{\sigma(rnP)}{F_r(nP)} \cdot \left(\frac{F_r(P)}{\sigma(rP)} \right)^{n^2}. \end{aligned} \tag{8}$$

まず $p \nmid r$ のときについて考える. χ を Teichmüller 指標とし, $T := \chi(P) \in E[r]$, $\mathcal{Q} := P - T \in \mathcal{E}^f(R_K)$ とおく. $\tau_T: \mathcal{E} \rightarrow \mathcal{E}$ を, T に関する平行移動とする (すなわち $\tau_T(P) := P + T$). このとき $p \nmid r$ に注意すると, 次が成り立つ.

$$F_r \circ \tau_T = z \cdot g_T.$$

ただし $g_T \in K(E)$ は $g_T(\mathcal{O}) \in R_K^*$ を満たす. 実際 $(F_r \circ \tau_T)(\mathcal{O}) = F_r(T) = \mathcal{O}$ でより, z が $\mathcal{O}$ の素元であるとする. $F_r \circ \tau_T$ は z を因数に持つ. しかもその商 g_T は $\mathcal{O}$ で極を持たない正則関数である. 式 (3) の右側について考える. $\mathcal{Q} \in \mathcal{E}^f(R_K)$, $\sigma(z) = z + O(z^2)$ ($z \rightarrow 0$, すなわち $\mathcal{Q} \rightarrow \mathcal{O}$) 及び $p \nmid r$ に注意すると, 次が得られる.

$$\begin{aligned} \frac{F_r(T + \mathcal{Q})}{\sigma(r\mathcal{Q})} &= \frac{z(\mathcal{Q}) \cdot g_T(\mathcal{Q})}{\sigma(r\mathcal{Q})} \\ &= \frac{z(\mathcal{Q})}{z(r\mathcal{Q})} \cdot \frac{z(r\mathcal{Q})}{\sigma(r\mathcal{Q})} \cdot g_T(\mathcal{Q}) \\ &\equiv \frac{1}{r} g_T(\mathcal{O}) \pmod{\mathfrak{p}_K}. \end{aligned}$$

今 q を $N(\mathfrak{p}_K)$ べきとして $n = mq^k$ と表せば、次が得られる。

$$\lim_{k \rightarrow \infty} \left(\frac{F_r(TQ)}{\sigma(rQ)} \right)^{(mq^k)^2} = \chi \left(\frac{g_T(\mathcal{O})}{r} \right)^{m^2}.$$

ここで右辺は Teichmüller 指標の特殊値であるから、特に右辺は K における 1 のべき根であり、代数的数である。さて式 (3) の左側について考える。 $n = mq^k$ と表しておく。ただし q は p べきで、 k 正整数とする。今 $p \nmid r$ であるから、次のように仮定してよい。

$$q = (N\mathfrak{p}_K)^e, \quad q \equiv 1 \pmod{rt}.$$

特に $q \equiv 1 \pmod{r}$ より、 $n \equiv m \pmod{r}$ であり、 $T \in E[r]$ ゆえ (k に依らずに) $nT = mT$ が成り立つ。そこで $Q_k := nQ = mq^k Q$ とおく。 $r \nmid m$ のとき、 $mT \neq \mathcal{O}$ であるから次が成り立つ。

$$\begin{aligned} \frac{\sigma(rP)}{F_r(P)} &= \frac{\sigma(rQ_k)}{F_r(mT + Q_k)} \quad (\because nP = nT + nQ = mT + Q_k, rnP = rmT + rQ_k = rQ_k) \\ &= \frac{\sigma(rQ_k)}{z(Q_k) \cdot g_{mT}(Q_k)} \quad (\because F_r \circ \tau_T = z \cdot g_T) \\ &= \frac{\sigma(rQ_k)}{z(rQ_k)} \cdot \frac{z(rQ_k)}{z(Q_k)} \cdot \frac{1}{g_{mT}(Q_k)} \\ &\xrightarrow[Q_k \rightarrow \mathcal{O}]{r} \frac{r}{g_{mT}(\mathcal{O})}. \end{aligned}$$

一方 $r \mid m$ のとき、 $T \in E[r]$ であるから $mT = \mathcal{O}$ である。また関数 $\sigma \circ [r]$ は $\mathcal{O}$ で 1 位の零点をとり、 F_r は $\mathcal{O}$ で $r^2 - 1$ の極を持つ。ゆえに $\sigma \circ [r] \setminus F_r$ は $\mathcal{O}$ で r^2 位の極を持つので、次が得られる。

$$\frac{\sigma(rQ_k)}{F_r(mT + Q_k)} = \frac{\sigma(rQ_k)}{F_r(Q_k)} \xrightarrow[Q_k \rightarrow \mathcal{O}]{} 0.$$

以上から、次が分かった。

$$\lim_{k \rightarrow \infty} F_{mq^k}(P)^{r^2} = \begin{cases} 0 & (r \mid m), \\ \frac{r}{g_{mT}(\mathcal{O})} \cdot \chi \left(\frac{g_T(\mathcal{O})}{r} \right)^{m^2} \neq 0 & (r \nmid m). \end{cases} \quad (9)$$

さて $A_k := F_{mq^k}(P)$ とおく。このとき実は数列 $\{F_n(P) \pmod{\mathfrak{p}_K}\}$ は周期 rt を持ち、 $q \equiv 1 \pmod{rt}$ であるから、 $\{A_k \pmod{\mathfrak{p}_K}\}$ は定数列である。この証明は面白い (かつ本質的) のだが、紙面の都合上証明は省略して、正確な主張のみ述べることにする。

定理 37 ([2, Theorem 8, Corollary 9]). $\mathbb{F}$ を有限体とし、 $E/\mathbb{F}$ を $\mathbb{F}$ 上定義された楕円曲線とする。 $P \in E(\mathbb{F})$ とし、 $r := \text{ord}(P) \geq 2$ とする。このとき定数 $a, b \in \mathbb{F}^*$ が存在して、次が成り立つ。

1. $r \geq 3$ のとき、 $F_{kr+n}(P) = a^{kn} b^{k^2} F_n(P) \quad (k, n \in \mathbb{Z}_{\geq 0})$,
2. $r = 2$ のとき、 $F_{2k}(P) = 0, F_{2k+1}(P) = a^k b^{\frac{1}{2}(k^2 - k)} \quad (k \in \mathbb{Z}_{\geq 0})$.

特に数列 $\{F_n(P)\}_{n \geq 0}$ は周期 rt を持つ。ただし $q := \#\mathbb{F}$ とするとき、 t は次を満たす。

1. $r \geq 3$ のとき、 $t \mid q - 1$,
2. $r = 2$ のとき、 $t \mid 2q - 2$.

従って

$$mq^k \equiv m \pmod{rt}$$

となるので、次が成り立つ。

$$A_k = F_{mq^k}(P) \equiv F_m(P) = A_0 \pmod{\mathfrak{p}} \quad (k \geq 0).$$

極限 $\lim_{k \rightarrow \infty} A_k^{r^2}$ は R_K において存在するので、極限 $\lim_{k \rightarrow \infty} A_k$ も R_K において存在する。ここで、次の補題に注意した。

補題 38. $K/\mathbb{Q}_p$ を有限次拡大体, R_K を K の整数環, $\mathfrak{p}_K$ を R_K の極大イデアルとする。また R^* における数列 $\{A_k\}_{k \geq 0}$ は, $\{A_k \bmod \mathfrak{p}_K\}_{k \geq 0}$ が定数列であるようなものとする。このとき $p \nmid n$ となる整数 n に対して、次が成り立つ。

$$\lim_{k \rightarrow \infty} A_k^n \text{ は } R_K \text{ において収束する。} \iff \lim_{k \rightarrow \infty} A_k \text{ は } R_K \text{ において収束する。}$$

証明. $\Leftarrow$ は明らかなので, $\Rightarrow$ を示す。まず仮定より, すべての $k \geq 0$ に対して $\alpha \equiv A_k \bmod \mathfrak{p}_K$ となる $\alpha \in R_K^*$ を固定することができる。このとき任意の $j, k \geq 0$ に対して

$$\sum_{l=0}^{n-1} A_j^l \cdot A_k^{n-1-l} \equiv n\alpha^{n-1} \not\equiv 0 \pmod{\mathfrak{p}}$$

であるから、次が成り立つ。

$$\lim_{j,k \rightarrow \infty} |A_j - A_k| = \lim_{j,k \rightarrow \infty} \frac{|A_j^n - A_k^n|}{\sum_{l=0}^{n-1} |A_j^l \cdot A_k^{n-1-l}|} = \lim_{j,k \rightarrow \infty} \frac{1}{n} |A_j^n - A_k^n| = 0.$$

ただし最後の等式が成り立つのは, A_k^n は $k \rightarrow \infty$ とすれば収束するという仮定があるからである。このことから $\{A_k\}_{k \geq 0}$ は Cauchy 列であることが分かるので, $\{A_k\}_{k \geq 0}$ は R_K において収束する (R_K は完備であることに注意する)。□

主定理の証明に戻って, $r = p^j$ ($j \geq 1$) のときについて考える。 $m \mid n$ に対して

$$\left(\frac{F_n}{F_m} \right) = [m]^* \left(\left[\frac{n}{m} \right]^* (\mathcal{O}) - (\mathcal{O}) \right) - (n^2 - m^2)(\mathcal{O}) \geq -(n^2 - m^2)(\mathcal{O})$$

であり, $m = p^k, n = p^{k+1}$ とすれば, 次が成り立つ。

$$\left(\frac{F_{p^{k+1}}}{F_{p^k}} \right) \geq -(p^{2(k+1)} - p^{2k})(\mathcal{O}) = -p^{2k}(p^2 - 1)(\mathcal{O}).$$

よって関数 $\frac{F_{p^{k+1}}}{F_{p^k}}$ は $\mathcal{O}$ 以外に極を持たないことが分かる。よって F_n の定義より, $E[p^{k+1}] \setminus E[p^k]$ で 0 をとるような関数 f_{p^k} を用いて, 次のように書ける。

$$F_{p^{k+1}} = F_{p^k} \cdot f_{p^k}. \quad (10)$$

$K(E[p^{j+1}])$ の極大イデアルを $\mathfrak{p}_j$ とする。 $T \equiv P \pmod{\mathfrak{p}_j}$ となる点 $T \in E[p^j]$ を固定し, $k \geq j$ とする。このとき $T + T' \equiv T \equiv P \pmod{\mathfrak{p}_k}$ となる $T' \in E^f[p^{k+1}] \setminus E^f[p^k]$ が存在するので, 次が得られる。

$$f_k(P) \equiv f_k(T + T') = 0 \pmod{\mathfrak{p}_k}.$$

今 $f_k(P) \in K$ ゆえ $f_k(P) \equiv 0 \pmod{\mathfrak{p}_K}$ である. よって等式 (5) を複数回用いると

$$F_{p^k}(P) = F_{p^j}(P) \prod_{i=j}^{k-1} f_{p^i}(P) \equiv 0 \pmod{\mathfrak{p}_K^{k-j}} \quad (k \geq j).$$

となり, これより次が得られる.

$$\lim_{k \rightarrow \infty} F_{p^k}(P) = 0. \quad (11)$$

もっと一般に, 自然数 $m = m'p^l$ (ただし $p \nmid m'$) に対して, 次が成り立つ.

$$\begin{aligned} \lim_{k \rightarrow \infty} F_{mp^k}(P) &= \lim_{k \rightarrow \infty} F_{m'p^{k+l}}(P) \\ &= \lim_{k \rightarrow \infty} F_{p^{k+l}}(m'P) F_{m'}(P)^{p^{k+l}} \quad (\because \text{補題 32}) \\ &= 0 \quad (\because \text{等式 (6)}). \end{aligned}$$

最後に $p \mid r$ だが, r が p べきでないときについて考える. $r = p^j r'$ (ただし $j \geq 1, r' \geq 2, p \nmid r'$) と表し, $P' := p^j P$ とおく. このとき次が成り立つことに注意する.

$$F_{mq^k}(P) = F_{mp^{-j}q^k}(p^j P) F_{p^j}(P)^{(mp^{-j}q^k)^2}. \quad (12)$$

等式 (7) の右辺について考える. 左側は $k \rightarrow \infty$ とすれば収束する ($p \nmid r$ のときに帰着される). 右側は $k \rightarrow \infty$ とすれば $\chi(F_{p^j}(P))$ べきになる. よって $\lim_{k \rightarrow \infty} F_{mq^k}(P)$ は代数的数となる.

7 最後に

最後まで (もしくは飛ばし読みで) 読んで頂きありがとうございます. 今回紹介したのはいわゆる古典的な EDS であり, 現代の EDS は定義が多少違います. と言っても楕円曲線の n 倍写像で定めるだけですけどね. EDS を研究している方は (少なくとも日本では) 少ないと思います. しかし楕円曲線や今回紹介できなかった代数幾何関連について習得すると, 研究することが山ほどあります. 例えば割と最近出た EDS 関連の論文として, 次の二つがあります.

1. 石塚裕大, 伊藤哲史, 大下達也, 谷口隆, 内田幸寛, *Periods modulo p of integer sequences associated with division polynomials of genus 2 curves.*
2. 佐野薫, *The number of rational iterated preimages of the origin under unicritical polynomial maps.*

そいえば私の自己紹介をしていませんでした. t888 と申します. 普段は**数論力学系**, 特に最近**非 Archimedes 体上の力学系**をやっています. キーワードは p 進 **Fatou 集合**です. 学部ときは代数的整数論, 特に楕円曲線が好きであいよあによしてました. しかし, とある方が「**楕円曲線上で力学系をする**」という (当時の私にとって) パワーワードを見たのがきっかけで数論力学系をやり始めました. 中々マイナーな分野だとは思いますが, 整数論, 代数幾何, 複素力学系の少なくとも一つに馴染みがあると参入しやすい分野です. 面白い問題は山ほどあるので, 是非皆さん一緒に数論力学系をやしましょう.

もし質問やコメント等ありましたら, 私の Twitter(現 X)@t88897937768 までお願いします. ではでは.

参考文献

- [1] Osman Bizim, Betül Gezer, *Operations on elliptic divisibility sequences*, Bull. Korean Math. Soc. 55 (2018), No. 3, pp. 763-776.
- [2] Joseph H. Silverman, *p -adic properties of division polynomials and elliptic divisibility sequences*, Mathematische Annalen, 332, 443-471, 2005.
- [3] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer, New York, 2009 (和訳：鈴木治郎, **楕円曲線の数論**, 共立出版.)
- [4] Joseph H. Silverman, *The Arithmetic of Dynamical Systems*, Graduate Texts in Mathematics, vol. 241.
- [5] B. Mazur, J. Tate, *The p -adic sigma function*, Duke Mathematical Journal Vol.62, No.3, 1991.
- [6] 内田幸寛, *Somos 4 数列の付値と楕円曲線上の局所高さ*.
- [7] 福田隆, **重点解説 岩澤理論**, サイエンス社, SGC ライブラリ 145.
- [8] 由良文孝, **楕円曲線と $Hankel$ 行列式**, 応用力学研究所研究集会報告. 26AO-S2 (30), pp.163-169, 2015-03. 九州大学応用力学研究所.