RIMS Kôkyûroku Bessatsu
B44 (2013), 99–110

Hypergeometric series and arithmetic-geometric mean over 2-adic fields

By

金城 謙作 (Kensaku KINJO) *
宮坂 宥憲 (Yuken MIYASAKA) **

Abstract

This article is a survey on author's result on unit root formulas associated to ordinary elliptic curves over a finite field of characteristic 2. This result is an analogy of a work by Dwork, who proved that the Gaussian hypergeometric function on p-adic numbers can be extended to a function which takes values of the unit roots of ordinary elliptic curves over a finite field of characteristic $p \geq 3$. We also present a relation between the canonical lift and the unit root of an elliptic curve over a finite field of characteristic 2 by using the 2-adic arithmetic-geometric mean.

§1. 序

奇素数 p に対し, p 進数上の Gauss の超幾何関数が標数 p の有限体上定義された通常楕円曲線の単数根を特殊値に持つ関数に延長される事を Dwork は発見した. 本稿は Dwork の結果の 2 進類似を与えた論文 [8] の紹介である. また, 2 進算術幾何平均列を用いることで, 標数 2 の有限体上の通常楕円曲線の単数根と標準持ち上げの関係が与えられることについても触れる.

パラメータ $a, b, c \in \mathbb{Q}$ $(c \notin \mathbb{Z}_{\leq 0})$ に付随する Gauss の超幾何関数 ${}_2F_1(a, b; c; z)$ とは,

$$ {}_2F_1(a, b; c; z) := 1 + \sum_{m \geq 1} \frac{(a)_m (b)_m}{(c)_m} \frac{z^m}{m!} \tag{1.1}$$

Received April 2, 2012. Revised February 27, 2013.
2000 Mathematics Subject Classification(s): 11G20, 33C05.
Key Words: p 進超幾何微分方程式, 算術幾何平均, 楕円曲線の単数根.
*Graduate School of Mathematical Sciences, the University of Tokyo, Komaba, Meguro-ku, Tokyo, 153-8914, Japan
e-mail: kensaku@ms.u-tokyo.ac.jp
**Mathematical Institute, Tohoku University, Aoba, Sendai, 980-8578, Japan
e-mail: sa7m27@tohoku.ac.jp

として与えられる級数である. 但し $(a)_m$ 等は Pochhammer 記号

$$(a)_m := a(a+1)\cdots(a+m-1)$$

である. また, 超幾何関数 ${}_2F_1(a,b;c;z)$ は次の微分方程式の解である:

$$z(1-z)f''(z)+(c-(a+b+1)z)f'(z)-abf(z)=0.$$

超幾何関数 ${}_2F_1(a,b;c;z)$ を p 進数上の関数と見做すと, その収束領域は素数 p, 及びパラメータ a,b,c に依存する. 例えば $p\geq 3$ の場合, ${}_2F_1(1/2,1/2;1;z)$ は $pW(\bar{\mathbb{F}}_p)$ 上でのみ収束する. 但し $W(\bar{\mathbb{F}}_p)$ は位数 p の有限体 $\mathbb{F}_p$ の代数閉包 $\bar{\mathbb{F}}_p$ 上の Witt ベクトルの為す環とする. しかしながら Dwork は次の定理を証明した.

定理 1.1 (Dwork [4]). p を奇素数とし, $F(z):={}_2F_1(1/2,1/2;1;z)$ を式 (1.1) で定義されるパラメータ $a=b=1/2, c=1$ の超幾何関数とする. このとき次の (1) と (2) を満たす関数 $\xi(z)$ が存在する:

(1) $pW(\bar{\mathbb{F}}_p)$ 上で, $\xi(z)=(-1)^{(p-1)/2}F(z)/F(z^p)$ となる.

(2) 関数 $\xi(z)$ は $\{z\in W(\bar{\mathbb{F}}_p)^\times; |(z-1)H(z)|\geq 1\}$ 上で rigid analytic 且つ可逆である. 但し $|\cdot|$ は $W(\bar{\mathbb{F}}_p)$ 上の p 進ノルムとし, $H(z):=\sum_{i=0}^{(p-1)/2}\binom{(p-1)/2}{i}^2 z^i$ は井草多項式とする.

また $\bar{\mu}\in\bar{\mathbb{F}}_p$ を $\bar{\mu}(\bar{\mu}-1)H(\bar{\mu})\neq 0$ となる元とし, $[\bar{\mu}]\in W(\mathbb{F}_{p^n})$ を $\bar{\mu}$ の Teichmüller 持ち上げとする ($n:=[\mathbb{F}_p(\bar{\mu}):\mathbb{F}_p]$). このとき $\prod_{i=0}^{n-1}\xi([\bar{\mu}]^{p^i})$ は $\bar{\mathbb{F}}_p$ 上の通常楕円曲線

$$E: y^2=x(x-1)(x-\bar{\mu}) \tag{1.2}$$

の単数根となる.

注. $p\geq 3$ の下で, $\bar{\mu}\in\bar{\mathbb{F}}_p$ に対して式 (1.2) で定義される曲線が $\bar{\mathbb{F}}_p$ 上の通常楕円曲線となるための必要十分条件は $\bar{\mu}(\bar{\mu}-1)H(\bar{\mu})\neq 0$ である. また, 有限体 $\mathbb{F}$ 上定義された通常楕円曲線 E の単数根 $u\in W(\mathbb{F})^\times$ とは

$$|E(\mathbb{F})|=1-\left(u+\frac{|\mathbb{F}|}{u}\right)+|\mathbb{F}|$$

を満たす唯一つの元である ($\mathbb{F}$ の標数は 2 でもよい).

定理 1.1 の証明には, 式 (1.2) で定義される通常楕円曲線の p 進族のコホモロジーに作用する Gauss-Manin 接続が用いられる. この Gauss-Manin 接続が 2 階線型常微分方程式

$$z(1-z)f''(z)+(1-2z)f'(z)-\frac{1}{4}f(z)=0 \tag{1.3}$$

を引き起こす. そして超幾何関数 ${}_2F_1(1/2,1/2;1;z)$ は式 (1.3) の級数解である.

定理 1.1 の 2 進類似を考察する際には, 通常楕円曲線を定義する方程式 (1.2) を取り替える必要がある. それは, 式 (1.2) で与えられる標数 2 の体上の曲線が特異点を持つからである. そこで $\bar{\mu} \in \bar{\mathbb{F}}_2$ に対し, $\bar{\mathbb{F}}_2$ 上の曲線

$$E_{\bar{\mu}} : y^2 + xy = x^3 + \bar{\mu} \tag{1.4}$$

が通常楕円曲線となる為の必要十分条件が $\bar{\mu} \neq 0$ である, という事実を用いる. 式 (1.4) で定義される通常楕円曲線による 2 進族のコホモロジーの上に作用する Gauss-Manin 接続は微分方程式

$$z(1+432z)f''(z) - (1+432z)f'(z) + 420f(z) = 0 \tag{1.5}$$

を引き起こす. そして $G(z) := z^2 \cdot {}_2F_1(5/6, 7/6; 3; -432z)$ が微分方程式 (1.5) の級数解を与える. このとき我々は次の定理を得た. ここで $\mathbb{Z}_2$ 係数収束べき級数環 $\mathbb{Z}_2\langle z \rangle$ を

$$\mathbb{Z}_2\langle z \rangle := \left\{ \sum_{m \geq 0} \alpha_m z^m \ ; \text{ 任意の } m \geq 0 \text{ に対して} \alpha_m \in \mathbb{Z}_2, \text{ 且つ } \lim_{m \to \infty} \alpha_m = 0 \right\} \tag{1.6}$$

とする.

定理 1.2 (Kinjo-Miyasaka [8]). 級数 $G'(z) := 2z \cdot {}_2F_1(5/6, 7/6; 2; -432z)$ を上述の $G(z)$ の導関数とし, $\phi(z) \in \mathbb{Z}_2\langle z \rangle$ を $\phi(z) \equiv z^2 \pmod{2\mathbb{Z}_2\langle z \rangle}$ となるものとする. このとき次の (1) と (2) を満たす $W(\bar{\mathbb{F}}_2) \setminus \{0\}$ 上の関数 $\eta_\phi(z)$ が存在する:

(1) $2W(\bar{\mathbb{F}}_2) \setminus \{0\}$ 上で $\eta_\phi(z) = c_\phi \cdot G'(z)/G'(\phi(z))$ となる ($c_\phi \in \mathbb{Z}_2^\times$ は定数).

(2) 関数 $\eta_\phi(z)$ は $W(\bar{\mathbb{F}}_2)^\times$ 上 rigid analytic 且つ可逆である.

また $\bar{\mu} \in \bar{\mathbb{F}}_2^\times$ とし, $n := [\mathbb{F}_2(\bar{\mu}) : \mathbb{F}_2]$ とおく. そして $[\bar{\mu}]_\phi \in W(\mathbb{F}_{2^n})$ を $\phi^n([\bar{\mu}]_\phi) = [\bar{\mu}]_\phi$ を満たす $\bar{\mu}$ の唯一の持ち上げとする. このとき $\prod_{i=0}^{n-1} \eta_\phi(\phi^i([\bar{\mu}]_\phi))$ は, 式 (1.4) で与えられる通常楕円曲線 $E_{\bar{\mu}}$ の単数根となる.

注. 定理 1.2 において $\phi(z) = z^2$ の場合, $[\bar{\mu}]_\phi$ は $\bar{\mu}$ の Teichmüller 持ち上げとなるため, 定理 1.2 は定理 1.1 の 2 進類似を与えている. また Dwork の定理 1.1 も定理 1.2 と同様に, $\mathbb{Z}_p$ 係数収束べき級数を用いて定式化することが出来る.

さらに 2 進算術幾何平均列により, $\bar{\mathbb{F}}_2$ 上の通常楕円曲線の単数根と標準持ち上げの間に関係を与えることが出来る (p9, 注を参照). 定理 1.2 の $\mathbb{Z}_2$ 係数収束べき級数 $\phi(z)$ として 2 進算術幾何平均列に由来する収束べき級数 $\phi_{\mathrm{AGM}}(z)$ を適応することで次の系を得る (ϕ_{AGM} の定義は (4.8) で述べる).

系 1.3. ϕ_{AGM} は上述のものとする. また $\bar{\mu} \in \bar{\mathbb{F}}_2^\times$ とし, $n := [\mathbb{F}_2(\bar{\mu}) : \mathbb{F}_2]$ とおく. このとき $\phi_{\mathrm{AGM}}^n(\mu^\uparrow) = \mu^\uparrow$ を満たす $\bar{\mu}$ の持ち上げ $\mu^\uparrow \in W(\mathbb{F}_{2^n})^\times$ が唯一つ存在する. さらに, 楕円曲線 $E^\uparrow : y^2 = x(x-1)(x-(1+8\mu^\uparrow)^2)$ は $E_{\bar{\mu}}$ の標準持ち上げとなる. また $G'(z)$ を定理 1.2 中の超幾何級数とすると, 次の (1), (2), (3) を満たす $W(\bar{\mathbb{F}}_2) \setminus \{0\}$ 上の関数 $\eta_{\mathrm{AGM}}(z)$ が存在する:

(1) $2W(\bar{\mathbb{F}}_2)\setminus\{0\}$ 上で $\eta_{\mathrm{AGM}}(z)=c\cdot G'(z)/G'(\phi_{\mathrm{AGM}}(z))$ となる ($c\in\mathbb{Z}_2^{\times}$ は定数).

(2) 関数 $\eta_{\mathrm{AGM}}(z)$ は $W(\bar{\mathbb{F}}_2)^{\times}$ 上 rigid analytic 且つ可逆である.

(3) $\Pi_{i=0}^{n-1}(\eta_{\mathrm{AGM}}(\mu^{\uparrow}))^{\sigma^i}$ は通常楕円曲線 $E_{\bar{\mu}}$ の単数根となる. ここで $\sigma\in\mathrm{Gal}(K/\mathbb{Q}_2)$ は Frobenius 元である (K は $W(\mathbb{F}_{2^n})$ の商体).

定理 1.1 の類似の研究について紹介する. Dwork は [5] において, Kloosterman 和を用いた Bessel 関数に対する類似を証明し, Sperber により超 Kloosterman 和を用いて Dwork の [5] の結果の高次元化が得られた ([14] 参照). また Adolphson と Sperber により, [1] でトーリック指数和に対する定理 1.1 の類似が得られている. 定理 1.1 の高次元化の例として, Yu による有限体上の Calabi-Yau 多様体の場合の研究がある ([16] 参照).

§2. Monsky-Washnitzer Cohomology

この節では式 (1.4) で与えられる標数 2 の有限体上のアフィン通常楕円曲線 $E_{\bar{\mu}}^{*}$ の Monsky-Washnitzer コホモロジーについて解説する. 一般の場合に関しては [12, 10, 11, 15] に詳しく掲載されている.

各 $\bar{\mu}\in\bar{\mathbb{F}}_2^{\times}$ に対して $n:=[\mathbb{F}_2(\bar{\mu}):\mathbb{F}_2]$ とおき, 位数 2^n の有限体 $\mathbb{F}_{2^n}$ 上の Witt ベクトルのなす環 $W(\mathbb{F}_{2^n})$ の商体を K とおく. そして K 係数過収束べき級数環を

$$K\langle x,y\rangle^{\dagger}:=\left\{\sum_{i,j\geq 0}a_{ij}x^iy^j;\ \begin{array}{c}a_{ij}\in K\text{ 且つ, ある実数 }\rho>1\text{ が存在して}\\ \lim_{i+j\to\infty}|a_{ij}|\rho^{i+j}=0\text{ が成立する}\end{array}\right\}\tag{2.1}$$

と定義する. また, $\bar{\mu}$ の持ち上げ $\tilde{\mu}\in W(\mathbb{F}_{2^n})$ に対し, $\mathcal{A}^{\dagger}:=K\langle x,y\rangle^{\dagger}/(y^2+xy-x^3-\tilde{\mu})$ とおく. K 上の微分加群 $\Omega^1_{\mathcal{A}^{\dagger}/K}$

$$\Omega^1_{\mathcal{A}^{\dagger}/K}:=(\mathcal{A}^{\dagger}dx\oplus\mathcal{A}^{\dagger}dy)/((2y+x)dy+(y-3x^2)dx)$$

とし, $E_{\bar{\mu}}^{*}$ の Monsky-Washnitzer コホモロジーを, $\mathcal{A}^{\dagger}$ から $\Omega^1_{\mathcal{A}^{\dagger}/K}$ への外微分写像 $d_{/K}$ の余核

$$H^1_{\mathrm{MW}}(E_{\bar{\mu}}^{*};K):=\mathrm{Coker}[d_{/K}:\mathcal{A}^{\dagger}\to\Omega^1_{\mathcal{A}^{\dagger}/K}]\tag{2.2}$$

として定義する. これは $\bar{\mu}$ の持ち上げ $\tilde{\mu}$ の取り方に依存しない ([15, Section 2] 参照). また,

$$\dim_K H^1_{\mathrm{MW}}(E_{\bar{\mu}}^{*};K)=2\tag{2.3}$$

が成立する.

注. $\bar{\mu} \in \bar{\mathbb{F}}_2^{\times}$ に対し, $n := [\mathbb{F}_2(\bar{\mu}) : \mathbb{F}_2]$ とおく. 2^n 乗する $E_{\bar{\mu}}^*$ の Frobenius 自己準同型は $\mathcal{A}^\dagger$ 上の写像に持ち上がり, さらに Monsky-Washnitzer コホモロジー $H^1_{\mathrm{MW}}(E_{\bar{\mu}}^*; K)$ の自己準同型 $\mathcal{F}_*$ を誘導する. この $\mathcal{F}_*$ は $\bar{\mu}$ の持ち上げ $\tilde{\mu}$ の取り方に依存しない ([15, Theorem 2.4.4] 参照). 式 (2.3) より Frobenius 写像の固有値は 2 つある為, それらを a_1, a_2 とおく. 今 $E_{\bar{\mu}}^*$ が通常楕円曲線であるので,

$$a_1, a_2 \in W(\mathbb{F}_{2^n}), a_1 + a_2 \in W(\mathbb{F}_{2^n})^{\times}, a_1 a_2 = 2^n$$

が成立するので, a_1, a_2 のうち $W(\mathbb{F}_{2^n})^{\times}$ に属する固有値が楕円曲線 $E_{\bar{\mu}}$ の単数根となる. またこれらの固有値を用いると, 楕円曲線 $E_{\bar{\mu}}$ のゼータ関数 $Z(E_{\bar{\mu}}/\mathbb{F}_{2^n}, T)$ は

$$Z(E_{\bar{\mu}}/\mathbb{F}_{2^n}, T) = \frac{(1 - a_1 T)(1 - a_2 T)}{(1 - T)(1 - 2^n T)}$$

の形で記述される ([11] 参照).

§ 3. Gauss-Manin Connection

この節では, 式 (1.4) で定義されるアフィン通常楕円曲線 $E_{\bar{\mu}}^*$ の 2 進族のコホモロジー H^1 を定義する. そして, H^1 上に作用する Gauss-Manin 接続と Frobenius 写像を導入する.

§ 3.1. H^1 の定義

$\mathbb{Z}_2$ 係数収束 Laurent 級数環 B を

$$B := \mathbb{Z}_2\langle z^{\pm 1}\rangle := \left\{ \sum_{m \in \mathbb{Z}} \alpha_m z^m \ ; \text{ 任意の } m \in \mathbb{Z} \text{ に対して} \alpha_m \in \mathbb{Z}_2, \text{ 且つ } \lim_{m \to \pm\infty} \alpha_m = 0 \right\}$$

とおく. B 上の Gauss ノルム

$$\left\| \sum_{i \in \mathbb{Z}} a_i z^i \right\| := \sup_{i \in \mathbb{Z}} |a_i| \qquad \left(\sum_{i \in \mathbb{Z}} a_i z^i \in B \right)$$

を用いて, 式 (2.1) と同様にして B 係数過収束べき級数環 $B\langle x, y\rangle^\dagger$ が定義出来る. $A := B\langle x, y\rangle^\dagger/(y^2 + xy - x^3 - z)$ とし, $B_{\mathbb{Q}} := B \otimes_{\mathbb{Z}} \mathbb{Q}$ 上の $A_{\mathbb{Q}} := A \otimes_{\mathbb{Z}} \mathbb{Q}$ の相対微分加群 $\Omega^1_{A_{\mathbb{Q}}/B_{\mathbb{Q}}}$ を

$$\Omega^1_{A_{\mathbb{Q}}/B_{\mathbb{Q}}} := (A_{\mathbb{Q}} dx \oplus A_{\mathbb{Q}} dy)/((2y + x)dy + (y - 3x^2)dx)$$

とおく. このとき, 通常楕円曲線 $E_{\bar{\mu}}^*$ の 2 進族のコホモロジー H^1 を $A_{\mathbb{Q}}$ から $\Omega^1_{A_{\mathbb{Q}}/B_{\mathbb{Q}}}$ への外微分写像 d の余核

$$H^1 := \mathrm{Coker}\left[d : A_{\mathbb{Q}} \to \Omega^1_{A_{\mathbb{Q}}/B_{\mathbb{Q}}} \right]$$

として定義する. $A_{\mathbb{Q}}$ の $B_{\mathbb{Q}}$ 上の相対微分加群 $\Omega^1_{A_{\mathbb{Q}}/B_{\mathbb{Q}}}$ は階数 1 の自由 $A_{\mathbb{Q}}$ 加群である. 実際, $P(x), Q(x), R(x), S(x) \in B[x]$ を

$$(2y+x)(yP(x)+Q(x))+(3x^2-y)(yR(x)+S(x)) \equiv 1 \pmod{(y^2+xy-x^3-z)}$$

を満たす多項式とし,

$$\frac{dx}{2y+x} := (yP(x)+Q(x))dx + (yR(x)+S(x))dy$$

とおくと, $\Omega^1_{A_{\mathbb{Q}}/B_{\mathbb{Q}}} = A_{\mathbb{Q}} \cdot dx/(2y+x)$ が成立する. 一方で H^1 は階数 2 の自由 $B_{\mathbb{Q}}$ 加群である. 実際 $\omega, xy\omega \in H^1$ をそれぞれ $dx/(2y+x), xydx/(2y+x) \in \Omega^1_{A_{\mathbb{Q}}/B_{\mathbb{Q}}}$ の H^1 での像とおくと

$$H^1 = B_{\mathbb{Q}}\omega \oplus B_{\mathbb{Q}}xy\omega \tag{3.1}$$

が成立する.

注. 各 $\bar{\mu} \in \bar{\mathbb{F}}_2^{\times}$ に対し $n := [\mathbb{F}_2(\bar{\mu}) : \mathbb{F}_2]$ とし, $\tilde{\mu} \in W(\mathbb{F}_{2^n})$ を $\bar{\mu}$ の持ち上げとする. このとき $B_{\mathbb{Q}}$ の生成元 z に $\tilde{\mu}$ を代入する写像により H^1 を $B_{\mathbb{Q}}$ 加群と見做すことで同型

$$H^1 \otimes_{B_{\mathbb{Q}}} K \simeq H^1_{\mathrm{MW}}(E^*_{\bar{\mu}}; K) \tag{3.2}$$

を得る. 但し, $H^1_{\mathrm{MW}}(E^*_{\bar{\mu}}; K)$ は式 (2.2) で定義されるアフィン通常楕円曲線 $E^*_{\bar{\mu}}$ の Monsky-Washnitzer コホモロジーである.

§ 3.2. H^1 上の Frobenius 写像

B 上の自己準同型 ϕ を $\phi(z) \equiv z^2 \pmod{2B}$ を満たすものとする. A が B 上滑らかであることから Artin の漸近定理を用いることで, A の ϕ 線型な環自己準同型 Fr が存在して, 任意の A の元 a に対し $\mathrm{Fr}(a) \equiv a^2 \pmod{2A}$ を満たす ([2, 3]). この A の自己準同型 Fr は, H^1 上の ϕ 線型の自己準同型 F_* を誘導する. つまり任意の $b \in B_{\mathbb{Q}}, m \in H^1$ に対し,

$$F_*(bm) = \phi(b)F_*(m)$$

が成立する. F_* は自己準同型 Fr の取り方に依らない.

§ 3.3. 特殊関数 η の構成

各 B 上の自己準同型 ϕ と $\bar{\mu} \in \bar{\mathbb{F}}_2^{\times}$ に対し, $[\bar{\mu}]_\phi \in W(\mathbb{F}_{2^n})$ を $\phi^n([\bar{\mu}]_\phi) = [\bar{\mu}]_\phi$ を満たす $\bar{\mu}$ の唯一の持ち上げとする ($n := [\mathbb{F}_2(\bar{\mu}) : \mathbb{F}_2]$). このとき z に $[\bar{\mu}]_\phi$ を代入することにより得られる同型 (3.2) は $F_*^n \otimes \mathrm{id}_K$ と $\mathcal{F}_*$ の作用と両立する:

$$F_*^n \otimes \mathrm{id}_K \curvearrowright H^1 \otimes_{B_{\mathbb{Q}}} K \simeq H^1_{\mathrm{MW}}(E^*_{\bar{\mu}}; K) \curvearrowleft \mathcal{F}_*. \tag{3.3}$$

さて, $\omega, xy\omega \in H^1$ は (3.1) で定義したものとする. また $H := B\omega \oplus Bxy\omega$ とおく. このとき H の直和因子 U で, $F_*(U)$ で生成された B 加群と U が一致するものが一意的に存在する ([8, Lemma 3.2] 参照) [1]. だから U の B 加群としての生成元 u は $F_*(u) = \eta u$ $(\eta \in B^\times)$ を満たす.

$$\begin{array}{ccc} u \otimes 1 & \longmapsto & v \\ \Big\downarrow{\scriptstyle F_*^n \otimes \mathrm{id}_K} & \circlearrowright & \Big\downarrow{\scriptstyle \mathcal{F}_*} \\ \eta^{\phi^0} \cdots \eta^{\phi^{n-1}}(u \otimes 1) & \longmapsto & (\eta^{\phi^0} \cdots \eta^{\phi^{n-1}})([\bar{\mu}]_\phi) \cdot v = \mathcal{F}_*(v). \end{array}$$

ここで v は $u \otimes 1$ の $H^1_{\mathrm{MW}}(E^*_{\bar{\mu}}; K)$ での像であり, η^{ϕ^i} は ϕ を η に i 回作用させたものとする. このとき η が $B^\times$ の元だから積 $\prod_{i=0}^{n-1} \eta^{\phi^i}([\bar{\mu}]_\phi)$ は $W(\mathbb{F}_{2^n})^\times$ の元, つまり通常楕円曲線 $E_{\bar{\mu}}$ の単数根となる.

§ 3.4. H^1 上の Gauss-Manin 接続

$A_\mathbb{Q}$ の $\mathbb{Q}_2$ 上の微分加群 $\Omega^1_{A_\mathbb{Q}/\mathbb{Q}_2}$ を

$$\Omega^1_{A_\mathbb{Q}/\mathbb{Q}_2} := (A_\mathbb{Q}dx \oplus A_\mathbb{Q}dy \oplus A_\mathbb{Q}dz)/((2y+x)dy + (y-3x^2)dx - dz)$$

として定義する. このとき $A_\mathbb{Q}$ 加群の完全列

$$0 \to A_\mathbb{Q}dz \to \Omega^1_{A_\mathbb{Q}/\mathbb{Q}_2} \to \Omega^1_{A_\mathbb{Q}/B_\mathbb{Q}} \to 0$$

が存在する. そこで $\tau \in \Omega^1_{A_\mathbb{Q}/\mathbb{Q}_2}$ を $dx/(2y+x) \in \Omega^1_{A_\mathbb{Q}/B_\mathbb{Q}}$ の持ち上げとすると, $\Omega^1_{A_\mathbb{Q}/\mathbb{Q}_2} = A_\mathbb{Q}dz \oplus A_\mathbb{Q}\tau$ となる. 外微分写像 $d^1 : \Omega^1_{A_\mathbb{Q}/\mathbb{Q}_2} \to \Omega^2_{A_\mathbb{Q}/\mathbb{Q}_2} = A_\mathbb{Q}dz \wedge \tau$ を用いて, 各 $a \in A_\mathbb{Q}$ に対し, $L(a) \in A_\mathbb{Q}$ を $d^1(a\tau) = L(a)dz \wedge \tau$ として定義する. 微分加群 $\Omega^1_{A_\mathbb{Q}/B_\mathbb{Q}}$ 間の加法的写像 $adx/(2y+x) \mapsto L(a)dx/(2y+x)$ は H^1 上の写像 ∇ を誘導する. この写像 $\nabla : H^1 \to H^1$ は well-defined 且つ加法的であり, 各 $b \in B_\mathbb{Q}, m \in H^1$ に対し,

$$\nabla(bm) = b\nabla(m) + \frac{db}{dz}(z)m$$

を満たす. この ∇ を Gauss-Manin 接続という. Gauss-Manin 接続 ∇ に対して, $xy\omega \in H^1$ を (3.1) のものとすると次の事実が成立する:

$$\begin{aligned} &H^1 = B_\mathbb{Q}xy\omega \oplus B_\mathbb{Q}\nabla(xy\omega), \\ &z(1+432z)\nabla^2(xy\omega) - (1+432z)\nabla(xy\omega) + 420xy\omega = 0. \end{aligned} \tag{3.4}$$

この (3.4) を用いると $\mathrm{Ker}\ \nabla$ の構造がわかる. $\zeta \in H^1$ に対して, 常微分方程式 (1.5) を満たす $f \in B_\mathbb{Q}$ を用いて $\zeta = \frac{1}{z}(f\nabla(xy\omega) - f'xy\omega)$ となるとき, またそのときに限り

[1] この U は H の単数根部分 (unit root part) と呼ばれる.

$\zeta \in \mathrm{Ker}\ \nabla$ となる. また B 上の自己準同型 ϕ を $\phi(z) \equiv z^2 \pmod{2B}$ を満たすものとし, F_* を 3.2 節で定義した H^1 上の ϕ 線型な Frobenius 写像とする. このとき

$$\nabla \circ F_* = \frac{d\phi(z)}{dz} F_* \circ \nabla \tag{3.5}$$

が成立する.

注. Gauss-Manin 接続 ∇ を用いることで 3.3 節で述べた H の単数根部分 U の生成元は, 唯一つの B の元 ν に対し

$$u = \nu\nabla(xy\omega) - (1/z)xy\omega \tag{3.6}$$

の形で取ることができる.

§4. 主結果の証明の概略

§4.1. 定理 1.2 の証明の概略

超幾何関数 $G(z) := z^2 \cdot {}_2F_1(5/6, 7/6; 3; -432z)$ は微分方程式 (1.5) の解であり, 微分方程式 (1.5) を満たす B の元は $G(z)$ の $\mathbb{Z}_2$ 倍となる. 従って 3.3 節にある $\mathrm{Ker}\ \nabla$ に属するための必要十分条件から $\lambda := (G'(z)/z)xy\omega - (G(z)/z)\nabla(xy\omega)$ とおくと ($G'(z) := dG(z)/dz = 2z\,{}_2F_1(5/6, 7/6; 2; -432z)$),

$$\mathrm{Ker}\ \nabla = \mathbb{Z}_2 \cdot \lambda$$

が成立する. 式 (3.5) より H^1 上の Frobenius 写像 F_* は $\mathrm{Ker}\ \nabla$ に作用し, $F_*(\lambda) = c_\phi \lambda$ ($c_\phi \in \mathbb{Z}_2^\times$) となる. よって $F_*(B\lambda)$ で生成される B 加群は $B\lambda$ と一致する. また $H := B\omega + Bxy\omega$ とおくと $B\lambda \subset H$ となり, 3.2 節の注釈から $B\lambda = Bu$ となる ($u \in H$ は式 (3.6) で定義されたもの). そして u の形から

$$\lambda = G'(z)u \tag{4.1}$$

がわかる. $\eta_\phi \in B^\times$ を $F_*(u) = \eta_\phi u$ を満たすものとし, 式 (4.1) の両辺に F_* を作用させると,

$$c_\phi G'(z)u = c_\phi\lambda = F_*(\lambda) = F_*(G'(z)u) = G'(\phi(\lambda))F_*(u) = G'(\phi(z))\eta_\phi u$$

が成立するので, $\eta_\phi = c_\phi G'(z)/G'(\phi(z))$ となる.

§4.2. 2 進算術幾何平均列と楕円曲線

位数 2^n の有限体 $\mathbb{F}_{2^n}$ に対し, K を $W(\mathbb{F}_{2^n})$ の商体とし, v を K 上の正規付値とする ($v(2) = 1$). $\alpha, \beta \in K$ は $v(1 - (\alpha/\beta)) \geq 3$ を満たすものとし, 2 進算術幾何平均列

$\{\alpha_m\}_{m\geq 0}, \{\beta_m\}_{m\geq 0}$ を

$$\begin{aligned} &\alpha_0 := \alpha, && \beta_0 := \beta, \\ &\alpha_{m+1} := \frac{\alpha_m + \beta_m}{2}, && \beta_{m+1} := \beta_m \sqrt{\frac{\alpha_m}{\beta_m}} \quad (m \geq 0) \end{aligned} \tag{4.2}$$

と帰納的に定義する. ここで α_m/β_m の平方根 $\sqrt{\alpha_m/\beta_m}$ は $v(1-\sqrt{\alpha_m/\beta_m}) \geq 2$ を満たすものとする. 各 $m \geq 0$ に対し, $v(1-(\alpha_m/\beta_m)) \geq 3$ から $v(1-(\alpha_{m+1}/\beta_{m+1})) \geq 3$ が従うので, 各 $m \geq 0$ に対し, β_{m+1} の定義は意味を持つ.

注. 2 進算術幾何平均列 $\{\alpha_m\}_{m\geq 0}, \{\beta_m\}_{m\geq 0}$ が収束するための必要十分条件は

$$v(1-(\alpha_0/\beta_0)) > 3$$

である. また収束する 2 進算術幾何平均列は同一極限を持つ. 一般に奇素数 p に対しても (4.2) と同様にして p 進算術幾何平均列を定義することが出来, その p 進算術幾何平均列は同一極限に収束する. 従って 2 進数上の場合に限り, 収束しない算術幾何平均列という特異な現象を考察することが出来る.

次に収束しない 2 進算術幾何平均列を楕円曲線と結びつける. $\alpha, \beta \in K$ を $v(1-(\alpha/\beta)) = 3$ を満たす元とし, $\{\alpha_m\}, \{\beta_m\}$ を式 (4.2) で定義される初期値 α, β の 2 進算術幾何平均列とし, $\nu_m := \alpha_m/\beta_m$ とおく $(m \geq 0)$. そして各 $m \geq 0$ に対し, K 上の楕円曲線 E_m を

$$E_m : y^2 = x(x-1)(x-\nu_m^2) \tag{4.3}$$

で定義されるものとする. このとき E_m は K 上良い通常還元を持つ. さらに次の定理が成立する. ここで数列 $\{\nu_m\}$ に関して,

$$\nu_{m+1} = \Psi(\nu_m), \quad \left(\Psi(X) := \frac{1+X}{2\sqrt{X}}\right) \tag{4.4}$$

が任意の $m \geq 0$ で成立する.

定理 4.1 ([7], Theorem 1.1, Proposition 3.2). K を $W(\mathbb{F}_{2^n})$ の商体とし, $\alpha, \beta \in K$ を $v(1-(\alpha/\beta)) = 3$ を満たすものとし, $\{\alpha_m\}, \{\beta_m\}$ を式 (4.2) で定義される初期値 α, β の 2 進算術幾何平均列とする. また, $\nu_m := \alpha_m/\beta_m$ とおく $(m \geq 0)$. このとき数列 $\{\nu_m\}$ は一般に収束しないが, 部分列 $\{\nu_{mn}\}_{m\geq 0}$ はある元 $\nu^{\uparrow} \in W(\mathbb{F}_{2^n})^{\times}$ に収束する. また,

$$\nu^{\uparrow} \equiv \nu_0 \pmod 2, \ (\nu^{\uparrow})^{\sigma} = \Psi(\nu^{\uparrow})$$

が成立する. 但し Ψ は式 (4.4) で与えられるものとし, $\sigma \in \mathrm{Gal}\,(K/\mathbb{Q}_2)$ は Frobenius 元とする. さらに楕円曲線

$$E^{\uparrow} : y^2 = x(x-1)(x-(\nu^{\uparrow})^2)$$

は, 式 (1.4) で定義される通常楕円曲線 $E_{\bar{\nu}}$ の K 上の標準持ち上げを与える ($\bar{\nu} := \nu_0 \pmod{2W(\mathbb{F}_{2^n})}$).

注. 有限体 $\mathbb{F}$ 上の通常楕円曲線 E に対し, F 上の楕円曲線 $E^{\uparrow}$ が E の標準持ち上げであるとは, 次の条件を満たすものである (F は $W(\mathbb{F})$ の商体とする):

$$\begin{aligned} &\tilde{E}^{\uparrow} \simeq_{/\mathbb{F}} E, \\ &\mathrm{End}\ (E^{\uparrow}) \simeq \mathrm{End}\ (E). \end{aligned} \tag{4.5}$$

この (4.5) を満たす楕円曲線 E の持ち上げ $E^{\uparrow}$ は F 同型の差を除いて一意的に存在する (Serre と Tate の特徴付け, [9] 参照). つまり次の図式が可換となるように, E の Frobenius 自己準同型写像が $E^{\uparrow}$ の自己準同型へ持ち上がる:

$$\begin{array}{ccc} E^{\uparrow}(\bar{F}) & \longrightarrow & E^{\uparrow}(\bar{F}) \\ {\scriptstyle \mathrm{red.}}\downarrow & \circlearrowright & \downarrow{\scriptstyle \mathrm{red.}} \\ E(\bar{\mathbb{F}}) & \xrightarrow[\mathrm{Frob}]{} & E(\bar{\mathbb{F}}). \end{array}$$

但し $\bar{F}$ と $\bar{\mathbb{F}}$ はそれぞれ F と $\mathbb{F}$ の代数閉包を表し, 図式の下の写像は楕円曲線 E の Frobenius 写像, 縦の写像は還元写像を表す.

定理 4.1 で述べた 2 進算術幾何平均列の比の為す列の “収束性” と通常楕円曲線の標準持ち上げの関係について解説する. 各 $m \geq 0$ に対し, E_m を還元して得られる楕円曲線を $\tilde{E}_m$ とすると,

$$\tilde{E}_{m+1} \simeq \tilde{E}_m^{(2)} \tag{4.6}$$

が成立する ($\tilde{E}_m^{(2)}$ は $\tilde{E}_m$ の Frobenius 写像 $(x, y) \mapsto (x^2, y^2)$ により得られる楕円曲線). このとき各 $m \geq 0$ に対し, E_m から E_{m+1} への次数 2 の同種写像 g_m

$$g_m : E_m \to E_{m+1}; (x, y) \mapsto \left(\frac{x + \nu_m^2}{4\nu_m x}, \frac{y(x^2 - \nu_m^2)}{8\sqrt{\nu_m}^3 x^2} \right)$$

は, (4.6) による同一視の下で次の図式を可換にする:

$$\begin{array}{ccc} E_m(\bar{K}) & \xrightarrow{g_m} & E_{m+1}(\bar{K}) \\ {\scriptstyle \mathrm{red.}}\downarrow & \circlearrowright & \downarrow{\scriptstyle \mathrm{red.}} \\ \tilde{E}_m(\bar{\mathbb{F}}_2) & \xrightarrow[\mathrm{Frob}_2]{} & \tilde{E}_m^{(2)}(\bar{\mathbb{F}}_2). \end{array} \tag{4.7}$$

$\tilde{E}_0$ が $\mathbb{F}_{2^n}$ 上定義されているから, 図式 (4.7) を n 回合成することで

$$\begin{array}{ccccccc} E_0(\bar{K}) & \xrightarrow{g_0} & E_1(\bar{K}) & \xrightarrow{g_1} & \cdots & \xrightarrow{g_m} & E_n(\bar{K}) \\ {\scriptstyle \mathrm{red.}}\downarrow & \circlearrowright & \downarrow{\scriptstyle \mathrm{red.}} & \circlearrowright & & & \downarrow{\scriptstyle \mathrm{red.}} \\ \tilde{E}_0(\bar{\mathbb{F}}_2) & \xrightarrow[\mathrm{Frob}_2]{} & \tilde{E}_0^{(2)}(\bar{\mathbb{F}}_2) & \xrightarrow[\mathrm{Frob}_2]{} & \cdots & \xrightarrow[\mathrm{Frob}_2]{} & \tilde{E}_0^{(2^n)}(\bar{\mathbb{F}}_2) \xrightarrow{\sim} \tilde{E}_0(\bar{\mathbb{F}}_2) \end{array}$$

を得る．故に数列 $\{\nu_{nm}\}_{m\geq 0}$ が K のある元 $\nu^{\uparrow}$ に収束するなら，楕円曲線 $E^{\uparrow}: y^2 = x(x-1)(x-(\nu^{\uparrow})^2)$ の自己準同型として Frobenius 写像が持ち上がるので，Serre と Tate の特徴付けから $E^{\uparrow}$ は E_0 を還元して得られる曲線の標準持ち上げを与える．

注．　式 (4.3) で与えられる K 上の楕円曲線 E_m の j 不変量 j_m は

$$j_m = \frac{2^8((\nu_m-1)^2+\nu_m)^3}{\nu_m^2(\nu_m-1)^2}$$

となる．このとき，数列 $\{j_m\}$ は収束しないが，その部分列 $\{j_{nm}\}_{m\geq 0}$ は位数 2^n の有限体上定義されたある通常楕円曲線の標準持ち上げの j 不変量に収束することが Gaudry[6] と Satoh[13] に述べられている．定理 4.1 では，数列 $\{\nu_{nm}\}_{m\geq 0}$ 自体が収束することを示した．

同一極限を持つ 2 進算術幾何平均列に対して式 (4.3) のようにして楕円曲線を定義すると，その楕円曲線は乗法的還元を持つ．また，奇素数 p に対して p 進算術幾何平均列を (4.2) と同様に定義すると，それらは同一極限を持つ．そして，p 進算術幾何平均列に対して式 (4.3) のように定義された楕円曲線も乗法的還元を持つ．

§ 4.3.　$\eta_{\mathbf{AGM}}$ の構成

$B = \mathbb{Z}_2\langle z^{\pm 1}\rangle$ とし，$\chi_B : B \to 1+8B; g \mapsto 1+8g$ による同一視を用いた写像

$$B \overset{\chi_B}{\to} 1+8B \overset{\Psi}{\to} 1+8B \overset{\chi_B^{-1}}{\to} B$$

を考察する．但し Ψ は式 (4.4) で与えられるものとし，$1+8g(z) \in 1+8B$ $(g(z)\in B)$ の平方根を

$$\sqrt{1+8g(z)} := \sum_{i=0}^{\infty} \binom{\frac{1}{2}}{i} (8g(z))^i$$

と定義する．そこで 2 進算術幾何平均列に由来する B の自己準同型 $\phi_{\mathrm{AGM}} : B \to B$ は，

$$\phi_{\mathrm{AGM}}(z) := \left(\chi_B^{-1}\circ\Psi\circ\chi_B\right)(z) = \frac{-(1+8z)+\sqrt{(1+8z)^2+16z^2(1+8z)}}{8(1+8z)} \tag{4.8}$$

を B 上の $\mathbb{Z}_2$ 代数の準同型に延長したものとして定義される．

注．　2 次方程式 $4(1+8X^2)+(1+8z)X-z^2=0$ の解の一つは $X=\phi_{\mathrm{AGM}}(z)$ なので，$\phi_{\mathrm{AGM}}(z) \equiv z^2 \pmod{2B}$ を満足する．

§ 4.4.　系 1.3 の証明の概略

$\bar{\mu} \in \bar{\mathbb{F}}_2$ に対して $n := [\mathbb{F}_2(\bar{\mu}) : \mathbb{F}_2]$ とおき，$W := W(\mathbb{F}_{2^n})$ とおく．また同相写像 $\chi : W^\times \overset{\sim}{\to} 1+8W^\times; a \mapsto 1+8a$ による同一視の下，可換図式

$$\begin{array}{ccc} W^\times & \xrightarrow{\chi} & 1+8W^\times \\ {\scriptstyle\Phi}\downarrow & & \downarrow{\scriptstyle\Psi} \\ W^\times & \xleftarrow[\chi^{-1}]{} & 1+8W^\times \end{array}$$

を得る (Ψ は式 (4.4) で与えられるものとし, $\Phi := \chi^{-1} \circ \Psi \circ \chi$ とする). そこで $\bar{\mu}$ の持ち上げ $\mu \in W^\times$ に対し, 数列 $\{\mu_m\}_{m\geq 0}$ を

$$\mu_0 := \mu,\ \mu_{m+1} := \Phi(\mu_m) \quad (m \geq 0) \tag{4.9}$$

と帰納的に定義することで, $W^\times$ 上の 2 進算術幾何平均列の比のなす数列が得られる. 定理 4.1 より数列 $\{\chi(\mu_{nm})\}_{m\geq 0}$ は K の元に収束するので, 数列 $\{\mu_{mn}\}_{m\geq 0}$ もある元 $\mu^\uparrow \in K$ に収束する (K は W の商体). そして $\phi_{\mathrm{AGM}}(\mu^\uparrow) = \Phi(\mu^\uparrow)$ が成立するので, 定理 4.1 より $\Phi^n(\mu^\uparrow) = \mu^\uparrow$ つまり $\phi^n_{\mathrm{AGM}}(\mu^\uparrow) = \mu^\uparrow$ が成立する. そこで定理 1.2 の ϕ と $[\bar{\mu}]_\phi$ の代わりに ϕ_{AGM} と $\mu^\uparrow$ を用いることで, 系 1.3 を得る.

References

[1] A. Adolphson and S. Sperber, On unit root formulas for toric exponential sums, Algebra Number Theory, **6** (2012), 573–585.

[2] M. Artin, On the solutions of analytic equations, Invent. Math., **5** (1968), 277–291.

[3] S. Bosch, A rigid analytic version of M. Artin's theorem on analytic equations, Math. Ann., **255** (1981), 395–404.

[4] B. Dwork, p-adic cycles, Publ. Math. Inst. Hautes Études Sci., **37** (1969), 27–115.

[5] B. Dwork, Bessel functions as p-adic functions of the argument, Duke Math. J., **41** (1974), 711–738.

[6] P. Gaudry, A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2, Advances in cryptology-ASIACRYPT 2002, 311–327, Lecture Notes in Comput. Sci., **2501**, Springer, Berlin, 2002.

[7] K. Kinjo and Y. Miyasaka, 2-adic arithmetic-geometric mean and elliptic curves, Interdiscip. Inform. Sci., **16** (2010), 5–15.

[8] K. Kinjo and Y. Miyasaka, Hypergeometric series and arithmetic-geometric mean over 2-adic fields, Int. J. Number Theory, **8** (2012), 831–844.

[9] W. Messing, The crystals associated to Barsotti-Tate groups: with applications to abelian schemes, Lecture Notes in Math., **264**, Springer, 1972.

[10] P. Monsky, Formal cohomology. II. The cohomology sequence of a pair, Ann. of Math., **88** (1968), 218–238.

[11] P. Monsky, Formal cohomology. III. Fixed point theorems, Ann. of Math., **93** (1971), 315–343.

[12] P. Monsky and G. Washnitzer, Formal cohomology. I, Ann. of Math., **88** (1968), 181–217.

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

[14] S. Sperber, p-adic hypergeometric functions and their cohomology, Duke Math. J., **44** (1977), 535–589.

[15] M. van der Put, The cohomology of Monsky and Washnitzer, Mém. Soc. Math. Fr., **23** (1986), 33–59.

[16] J.-D. Yu, Variation of the unit root along the Dwork family of Calabi-Yau varieties, Math. Ann., **343** (2009), 53–78.