氏名・(本籍)	金城謙作 (きんじょうけんさく)
学位の種類	博士(理学)
学位記番号	理博第2644号
学位授与年月日	平成23年9月8日
学位授与の要件	学位規則第4条第1項該当
研究科，専攻	東北大学大学院理学研究科(博士課程)数学専攻
学位論文題目	Canonical lifts and unit roots of ordinary elliptic curves via two-adic arithmetic-geometric mean (二進算術幾何平均による通常楕円曲線の標準持ち上げと単数根)
論文審査委員	(主査) 准教授 山崎隆雄 教授 雪江明彦 教授 都築暢夫

論文目次

B. Other arithmetic-geometric mean

B.1 Cubic arithmetic-geometric mean

B.2 4 variables arithmetic-geometric mean

論 文 内 容 要 旨

本博士論文は，標数2の有限体上定義された楕円曲線と超幾何級数の関係について纏めたものである．また応用として2進算術幾何平均列を用いて，楕円曲線の標準的な持ち上げと超幾何級数の関係を与える．

楕円曲線と算術幾何平均

実数体上の算術幾何平均列とは，正の実数a, bに対し，

$$a_0:= a,\ b_0:= b,\ a_{m+1}:= (a_m + b_m)/2,\ b_{m+1}:= (a_m b_m)^{1/2} \quad (m \geqq 0)$$

と帰納的に定義される数列である(平方根は正のものを選ぶ)．これらの数列は同一極限に収束する．Gaussは，算術幾何平均列の同一極限を用いた，実数体上の楕円曲線の周期の計算方法を発見した．算術幾何平均列の類似は色々考察されており，本博士論文では，算術幾何平均列のp進類似について考察する．

pを素数とし，KをQ_p上の有限次拡大体，vをKの正規付値とする (v (p) = 1)．Kの元a，bで，pが奇素数のとき $v(1-(a/b)) \geqq 1$, $p=2$ のとき $v(1-(a/b)) \geqq 3$ を満たすものに対し，数列 $\{a_m\}$, $\{b_m\}$ を

$$a_0:= a,\ b_0:= b,\ a_{m+1}:= (a_m + b_m)/2,\ b_{m+1}:= b_m (a_m b_m)^{1/2} \quad (m \geqq 0)$$

と帰納的に定義する．ここで a_m/b_m の平方根は1に近いほうを選ぶものとする．これらの数列はp進算術幾何平均列と呼ばれ，Henniartと Mestreによって初めて定義された．ここでp進算術幾何平均列の収束性について，次の命題が成立する．

命題.

a，bはKの元で，pが奇素数のとき $v(1-(a/b)) \geqq 1$，$p=2$ のとき $v(1-(a/b)) \geqq 3$ を満たすとする．また，数列 $\{a_m\}$, $\{b_m\}$ を初期値がa，bのp進算術幾何平均列とする．もしpが奇素数なら，$\{a_m\}$と$\{b_m\}$は収束する．$p=2$ のとき，2進算術幾何平均列が収束するための必要十分条件は $v(1-(a/b)) > 3$ である．各素数 $p \geqq 2$ に対し，p進算術幾何平均列が収束するなら，それらは同一極限を持つ．

同一極限を持つp進算術幾何平均列は乗法的還元を持つ楕円曲線と対応している．そしてHenniartとMestreは，p進算術幾何平均列の極限値を用いて乗法的還元を持つ楕円曲線の周期を計算した．

命題にあるように，$p=2$ のときに限り，収束しない2進算術幾何平均列を考えることが出来る．これは実数体上の場合とは異なる現象である．以下収束しない2進算術幾何平均列について考察する．

a，bはKの元で，$v(1-(a/b)) = 3$ を満たすものとする．また $\{a_m\}$, $\{b_m\}$ を，初期値がa，bの2進算術幾何平均列とし，$\mu_m := a_m/b_m$ とおく．各 $m \geqq 0$ に対し，方程式

$$E_{\mu m} : y^2 = x\,(x-1)\,(x-(\mu_m)^2) \qquad (1)$$

で定義される曲線は通常楕円曲線となり，$E_{\mu m}$ のj不変量 j_m は

$$j_m = 2^8 [(\mu_m - 1)^2 + \mu_m]^3 / [\mu_m^2 (\mu_m - 1)^2]$$

となる．Satohと Gaudryは，j不変量のなす列 $\{j_m\}$ は収束しないが部分列 $\{j_{mn}\}_{m \geq 0}$ は収束することに言及

している（nはKの剰余次数). 但し, 彼らは暗号理論に応用するためにKはQ_2上不分岐であることを仮定している. 著者と宮坂宥憲氏は共同で, KはQ_2上の任意の有限次拡大体で, 更に$\{\mu_m\}$自身が収束することを示した. より正確には, 次の定理を得た.

主定理1. (K. -Miyasaka)

KをQ_2上の有限次拡大体とし, nをKの剰余次数とする. a, bをKの元で$v(1-(a/b))=3$を満たすとする. また, $\{a_m\}$, $\{b_m\}$を初期値がa, bの2進算術幾何平均列とし, $\mu_m:=a_m/b_m$とおく. 各整数$0\leqq i\leqq n-1$に対して次が成立する.

(1) 部分列$\{\mu_{mn+i}\}_{m\geq 0}$はQ_2上のn次不分岐拡大体$F_n\subset K$のある元$\mu_i^{\uparrow}$に収束する.

(2) $Gal(F_n/Q_2)$のFrobenius元σに対して, $\mu_{i+1}^{\uparrow}=(\mu_i^{\uparrow})^{\sigma}$が成立する.

(3) 各$m\geqq 0$に対し, $E_{\mu m}$は良い通常還元を持ち, $E_{\mu i}^{\uparrow}$は$E_{\mu i}$を還元して得られる曲線の標準持ち上げとなる. 但し, $E_{\mu m}$と$E_{\mu i}^{\uparrow}$は, (1)のようにLegendre型の方程式で定義された楕円曲線である.

2進超幾何級数

本博士論文では, 収束しない2進算術幾何平均列と標数2の有限体上の通常楕円曲線の単数根との関係を与える超幾何関数を構成している.

a, b, cを有理数とし, cが0以下の整数でないとき, 超幾何級数${}_2F_1(a, b; c; \lambda)$は

$$ {}_2F_1(a, b; c; \lambda):=\Sigma_{m\geq 0}(a)_m(b)_m\lambda^m/\{(c)_m\cdot m!\} $$

で定義される. 但し$(a)_m$はPochhammer 記号である:

$$ (a)_0:=1,\ (a)_m:=a(a+1)\cdots(a+m-1)\quad (m\geqq 1). $$

この超幾何関数をp進数上の関数と見做すと, 収束半径はパラメータと素数に依存する. 例えば$p\geqq 3$のとき, ${}_2F_1(1/2, 1/2; 1; \lambda)$は$pW(\bar{F}_p)$上で収束し, $W(\bar{F}_p)^{\times}$上では収束しない（$W(\bar{F}_p)$はWittベクトル). しかしDworkは, 超幾何級数の比をとることにより, 定義域が延長されることを見出した:

定理 (Dwork).

pを奇素数とする. このとき関数$\xi(\lambda)$が存在して次を満たす.

(1) $pW(\bar{F}_p)$上で, $\xi(\lambda)=(-1)^{(p-1)/2}\ {}_2F_1(1/2, 1/2; 1; \lambda)/\ {}_2F_1(1/2, 1/2; 1; \lambda^p)$が成立.

(2) $\xi(\lambda)$は, $\{\lambda\in W(\bar{F}_p)^{\times}; |\lambda(\lambda-1)H(\lambda)|=1\}$上で正則かつ可逆である. ここで$H(\lambda)$は井草多項式である.

更に, $\xi([\mu])\,\xi([\mu]^p)\cdots\xi([\mu]^{p^{n-1}})$は, 通常楕円曲線Eの単数根となる. 但し$\mu\in\bar{F}_p$は$\mu(\mu-1)H(\mu)\neq 0$を満たし, $n=[F_p(\mu):F_p]$, $[\mu]\in W(F_{p^n})$はμのTeichmuller持ち上げである. そして, Eは$y^2=x(x-1)(x-\mu)$で定義される楕円曲線である.

$\mu\in\bar{F}_p$が$\mu(\mu-1)H(\mu)\neq 0$であるから, Eは通常楕円曲線となる.

本博士論文ではDworkの定理の2進類似を考察した. Legendre型の方程式で定義された曲線は, 標数2の体上では特異点を持つため, 楕円曲線の定義方程式を取り替える必要がある. $\bar{F}_2$上の通常楕円曲線の定義方程式は$y^2+xy=x^3+\mu$ ($\mu\in\bar{F}_2$)で与えられることを用いて, 著者と宮坂宥憲氏の共同研究により次の定理を得た.

主定理2. (K. -Miyasaka)

$G(\lambda) := {}_2F_1(5/6, 7/6; 2; -432\lambda)$ とおき，B を $\lambda^{\pm 1}$ で生成される Z_2 係数の収束べき級数環とする．各 B 上の Z_2 代数準同型 ϕ で，$\phi(\lambda) \equiv \lambda^2 \pmod{2B}$ を満たすものに対し，$W(\bar{F}_2)\backslash\{0\}$ 上の関数 η_ϕ が存在し，

(1) $2W(\bar{F}_2)\backslash\{0\}$ 上で，$\eta_\phi(\lambda) = c_\phi G(\lambda)/G(\phi(\lambda))$ となる（c_ϕ はある $Z_2^\times$ の元）.

(2) $W(\bar{F}_2)^\times$ 上で η_ϕ は可逆となる.

(3) $\eta_\phi([\mu]_\phi)\eta_\phi(\phi([\mu]_\phi))\cdots\eta_\phi(\phi^{n-1}([\mu]_\phi))$ は楕円曲線 $y^2+xy=x^3+\mu$ の単数根となる．但し，μ は $\bar{F}_2^\times$ の元で，$n=[F_2(\mu):F_2]$ であり，$[\mu]_\phi$ は $\phi^n([\mu]_\phi)=[\mu]_\phi \in W(F_{2^n})$ を満たす μ の唯一の持ち上げである.

特に $\phi(\lambda)=\lambda^2$ のとき，$[\mu]_\phi$ は μ の Teichmuller 持ち上げとなり，Dwork の定理の 2 進類似となる.

次に，ϕ として $\phi_{AGM}(\lambda) := [-(1+8\lambda)+\{(1+8\lambda)^2+16\lambda^2(1+8\lambda)\}^{1/2}]/[8(1+8\lambda)]$ をとる．これは 2 進算術幾何平均列から由来した Z_2 代数準同型であり，主定理 1 より $W(F_{2^n})$ の元 $\mu^\uparrow$ で，$\phi^n{}_{AGM}(\mu^\uparrow)=\mu^\uparrow$ を満たすものが存在する．以上をまとめることで，次の系を得る．これは $p=2$ のときのみ起こりうる現象である.

<u>系.</u>

任意の $\mu \in \bar{F}_2^\times$ に対し，$\mu^\uparrow$ を μ の持ち上げで，$\phi^n{}_{AGM}(\mu^\uparrow)=\mu^\uparrow$ を満たすものとする（$n=[F_2(\mu):F_2]$）．主定理 1 により，$y^2=x(x-1)(x-(\mu^\uparrow)^2)$ は E_μ の標準持ち上げを与える．このとき，$W(\bar{F}_2)\backslash\{0\}$ 上の関数 $\eta(\lambda) := \eta_{\phi_{AGM}}(\lambda)$ が存在して，

(1) $2W(\bar{F}_2)\backslash\{0\}$ 上で，$\eta(\lambda) = c \cdot G(\lambda)/G(\phi_{AGM}(\lambda))$ となる（c はある $Z_2^\times$ の元）.

(2) $W(\bar{F}_2)^\times$ 上で $\eta(\lambda)$ は可逆となる.

(3) $\eta(\mu^\uparrow)\eta(\mu^\uparrow)^\sigma\cdots\eta(\mu^\uparrow)^{\sigma^{n-1}}$ は楕円曲線 E_μ の単数根となる．但し σ は $Gal(F_n/Q_2)$ の Frobenius 元である（F_n は Q_2 上の n 次不分岐拡大体）.

論文審査の結果の要旨

算術幾何平均はごく素朴な数の遊びのような概念だが、Gauss が楕円積分との関係を発見したことにより真剣な数学の研究対象となった。この関係は、正確には実数体上定義された楕円曲線の周期が算術幾何平均を用いて表せるということになる。ここでいう算術幾何平均は、(正の) 実数の組に対して (実数の位相を用いて) 定義されるものを指しているが、その p- 進類似を考えるのはごく自然である。この類似は Tate 曲線と呼ばれる楕円曲線 (すなわち、分裂乗法的還元を持つ場合) では並行的に議論を進めることができることが Henniart と Mestre により示されている。(本博士論文の附録 A には、ほぼ同等な内容が Fontaine の p- 進周期の環を用いた現代的な取り扱いで解説されている。)

楕円曲線が良い還元を持つ場合は同様な理論を展開することはできない。しかしながら、$p=2$ の場合だけは Serre と Tate により導入された「標準持ち上げ」と算術幾何平均を関係づけることができる。このような理論は、Gaudry や佐藤孝和により基礎体が不分岐という条件のもとで考察されていたが、金城謙作は宮坂宥憲と共同で分岐した場合を許す一般的な理論を構築した。本博士論文の 2 章ではこの結果が解説されている。

Dwork は楕円曲線の族から派生する p- 進微分方程式を考察することで、楕円曲線の単数根を p- 進超幾何関数により表示するという素晴らしい結果を得たが、$p=2$ の場合はさまざまな技術的な理由により除外されていた。金城は宮坂と共同で、Dwork 理論の類似を $p=2$ の場合に展開した。ただし、ここで現れる超幾何級数は Dwork の扱ったものとは違うパラメーターを持っており、Dwork の理論の単純な移植とは言えない内容を含んでいる。また、この結果と 2 章で導入された算術幾何平均を結びつけることができる。すなわち、フロベニウス写像の持ち上げとして算術幾何平均から導出される冪級数を採用することで、算術幾何平均・標準持ち上げ・超幾何級数・単数根がすべて結びつくのである。このような現象が起きうるのは $p=2$ の場合だけであり、真に新しい現象を捕まえている。これらが本博士論文 3 章の内容である。

以上の通り、本博士論文は独創的な研究成果を豊富に含んでおり、筆者が将来に渡り自立して研究活動を行うに必要な高度の研究能力と学識を有することを示している。したがって、金城謙作提出の博士論文は、博士 (理学) の学位論文として合格と認める。