

Hypergeometric series and elliptic curves over finite fields

広島大学理学部

小池 正夫

有限体上の超幾何関数は Gauss の和と Γ -関数の定義式の類似性に着目して、古典的な超幾何関数に対応する有限体上の対象として、Koblitz [3], Greene [2] によって定義され、研究が始められた。研究が始められてからまだ日も浅く、重要な結果の数多くある数論の中で Gauss の和のような独自の位置をえられるかどうかは不確定だが、有限体上の超幾何多項式に新しい定義式とよんだり、有限体上の代数曲線の研究に少しは新しい知識を加えることができると期待している。

$$E_\lambda: y^2 = x(x-1)(x-\lambda) \quad \lambda \neq 0, 1 \in \mathbb{C} \text{ \textit{Legendre の}}$$

楕円曲線とすると

$$\int_1^\infty \frac{dx}{y} = \int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} = \pi {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; \lambda\right)$$

という等式が知られている。

ここで ${}_2F_1(a, b; c; x)$ は Gauss の超幾何級数で

$${}_2F_1(a, b; c; x) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(1)_n (c)_n} x^n, \quad (a)_n = a(a+1) \cdots (a+n-1),$$

$$(a)_0 = 1$$

で定義されている。

一方 有限体上では 同じ形の楕円曲線

$$E_\lambda : y^2 = x(x-1)(x-\lambda) \quad \lambda \neq 0, 1 \in \mathbb{F}_p$$

の $\mathbb{F}_p$ 有理点の個数の計算が次の式で得られる:

$$\begin{aligned} N_\lambda &= 1 + \sum_{t \in \mathbb{F}_p} \left\{ 1 + \phi(t(t-1)(t-\lambda)) \right\} \\ &= 1 + p + \sum_{t \in \mathbb{F}_p^\times} \phi(t) \phi(1-t) \phi(1-t\lambda) \end{aligned}$$

ここで $\phi \in \hat{\mathbb{F}_p^\times}$ は Legendre 指標で $\phi(0)=0$ と $\mathbb{F}_p$ までの ϕ として考えられている。従って E_λ の合同ゼータ関数の分子に現れる Frobenius 写像の跡, $a_p(\lambda)$ は

$$a_p(\lambda) = - \sum \phi(t) \phi(1-t) \phi(1-t\lambda)$$

とかけ、この右辺を有限体上の超幾何関数の定義式でおきかえると、

$$a_p(\lambda) = -p \phi(-1) {}_2F_1\left(\phi, \phi \middle| \lambda\right)$$

となる。ここで ϕ は $\mathbb{F}_p^\times$ の単位指標を表す。これは $\mathbb{C}$ 上の楕円積分と超幾何関数でかいた式と類似している。

$$a_p(\lambda) \pmod{p} \text{ は Deuring によれば } {}_2F_1\left(\frac{1}{2}, \frac{1}{2} \middle| x\right)$$

の係数を有限体の元とみて、分子が 0 になる λ を λ とおいて得られる λ の $\frac{p-1}{2}$ 次式の多項式 (これを超幾何多項式

と呼ぶことにする。) で書くことは Manin によ, (解説が
与えられている。(Clemens [1] を参照) しかし modulo p する
前の等式は目新しい。

又 Legendre 型の楕円曲線について 超幾何多次式との関
係は Silverman [9], Clemens [1], Husemoller など詳しい解説を
みるが、その他の楕円曲線の族についての記述は不勉強、せ
いもあるがすぐ目につかない。だから上の等式を拡張するよ
うな楕円曲線の族と 超幾何関数の関係とかいとおくのは
無駄ではなっだろう。

研究集会の折に、伊原先生が注意してくださったのは
Dwork による p 進的な超幾何関数の研究についてでした。

最近の Young [10] の結果によれば 変数 λ と p 進数で
 $\lambda \pmod{p} = \lambda$ でも、 $a_p(\lambda)$ という Frobenius 字像の跡では
なくて、その Frobenius 字像の 2 つの固有値のうち p 進数で
、 p 進的な超幾何関数の総和値には、なります。後、 λ

modulo p するとどちらも同じ式になるわけですが、両者の
関係は注意されたいようです。Young [10] では [4] で
示した Apéry 数の合同式も p 進的な超幾何関数の研究の
応用で得られている。この点でも両者が平行している。

§1 難波氏の実験

$a_p(\lambda)$ を上にのべた λ の関数として、この関数に次のように行列を対応させる。それは一般的に $f: \mathbb{F}_p^{\times} \rightarrow \mathbb{C}$ が与えられているとする。 $\mathbb{F}_p^{\times}$ の生成元を r , $m = \frac{p-1}{2}$ として

$$c_i = f(r^i) - f(-r^i) \quad 0 \leq i \leq m-1$$

とおいて m 行 m 列の行列 $\Phi = \Phi_f$ を

$$\Phi = \Phi_f = \begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{m-1} \\ -c_{m-1} & c_0 & & & \\ -c_{m-2} & -c_{m-1} & \ddots & & \\ \vdots & \vdots & \ddots & \ddots & \\ -c_1 & -c_2 & \cdots & & c_0 \end{bmatrix}$$

で定義する。難波 [7], [8] では $a_p(i)$ と適当に定義して、対応する行列 Φ の計算を素数 p を変えて数値実験の結果、次の予想を提出している。

予想 $p \equiv 1 \pmod{4}$ のときは ${}^t\Phi \cdot \Phi = p^2 \cdot 1_m$

$p \equiv 3 \pmod{4}$ ${}^t\Phi \cdot \Phi = p^2 \cdot 1_m - 2(p+1)\Omega$

ここで Ω は (i, j) 成分が $(-1)^{i+j}$ となる行列。

[7], [8] では他の超幾何関数の類似物についても同様の現象が得られることも予想されている。

§2 Mellin 変換

難波氏の行列を定義するのに §1 では有限体 $\mathbb{F}_p$ にとったが、任意の有限体 F $|F| = q = p^a$ ときで同様の考察ができる。

F^X の生成元を r_i とおいて、 $m = \frac{q-1}{2}$ とおく。関数

$$f: F^X \rightarrow \mathbb{C} \text{ に対して } c_i = f(r_i) - f(-r_i), \quad 0 \leq i \leq m-1$$

とおいて m 行 m 列の行列 $\Phi = \Phi_f$ を同様に定義する。

一方、 f の Mellin 変換 $M_f(x)$, $x \in \hat{F}^X$ は

$$M_f(x) = \sum_{t \in F^X} x(t) f(t)$$

で定義する。

定理 次の 2 つの命題は同値である。

$$(A) \quad {}^t\Phi \cdot \Phi = \alpha \cdot I_m$$

$$(B) \quad \text{全ての奇指標 } \chi \text{ に対して } M_f(\chi) M_f(\bar{\chi}) = \alpha$$

ここで $\chi(-1) = -1$ のとき χ を奇指標といい、 $\bar{\chi}$ は χ の複素共役で得られる指標を表す。

§3 有限体上の超幾何関数

性質(B)をみたす有限体上の関数の例として有限体上の超幾何関数から得られるものがとれる。有限体上には他に Hermite 多項式 (Evans による) などあるが (B) を調べると成り立っていない。

有限体上の超幾何関数で Gauss の超幾何関数に相当するものは $A, B, C \in \hat{F}^X$ に対して $x \in F^X$

$${}_2F_1\left(\begin{matrix} A, B \\ C \end{matrix} \middle| x\right) = \frac{BC(-1)}{\#} \sum_{t \in F} B(t) \overline{BC}(1-t) \overline{A}(1-xt)$$

で定義される。ただし $A(0)=0, B(0)=0, C(0)=0$ とする。すると

この Fourier 展開は

$$= \frac{\#}{\#-1} \sum_{x \in \hat{F}^\times} \begin{pmatrix} Ax \\ x \end{pmatrix} \begin{pmatrix} Bx \\ Cx \end{pmatrix} \chi(x)$$

ここで $A, B \in \hat{F}^\times$ に対して $\begin{pmatrix} A \\ B \end{pmatrix} = \frac{B(-1)}{\#} J(A, \overline{B})$, Jacobi 和

とする。Mellin 変換と Fourier 変換の関係は明らかで、更に

それが簡単になる A, B, C の例として、

$$A = \psi, \quad B = \overline{\psi}, \quad C = \varepsilon \quad \psi \neq \varepsilon$$

が考えられ、そのとき

$$M_f(\chi) = \begin{pmatrix} \chi \\ \psi \end{pmatrix} \begin{pmatrix} \chi \\ \overline{\psi} \end{pmatrix}$$

となる。これは Gauss 和でかき直して $G(\chi)G(\overline{\chi}) = \chi(-1)\#$ と

用いると

補題 $\chi \neq \psi, \overline{\psi}, \varepsilon$ ならば $M_f(\chi)M_f(\overline{\chi}) = 1$

従って §2 の定理と合わせれば、

定理 ψ が自明でない偶指標とすると、 ${}_2F_1\left(\begin{matrix} \psi, \overline{\psi} \\ \varepsilon \end{matrix} \middle| x\right)$

からなる行列 Φ は、直交行列になる。

特に有限体 $\mathbb{F}_p$ で $\psi = \phi$ Legendre 指標のときが §1 の 難波氏の予想と関係して、 $p \equiv 1 \pmod{4}$ という条件は ϕ が偶指標と同値だから予想の証明がえられる。 $p \equiv 3 \pmod{4}$

の場合も §2 の途中の計算をたどることで同様に得られる。

§4. 楕円曲線の族と超幾何関数

解けている場合に限るために有限体を改めて $\mathbb{F}_p$ の場合とする。難波 [7], [8] との関連から次の 4 つの Case が次の対象として現れる。

$$\text{Case 1} \quad p \equiv 1 \pmod{2} \quad \psi = \omega^{\frac{p-1}{2}}$$

$$\text{Case 2} \quad p \equiv 1 \pmod{3} \quad \psi = \omega^{\frac{p-1}{3}}$$

$$\text{Case 3} \quad p \equiv 1 \pmod{4} \quad \psi = \omega^{\frac{p-1}{4}}$$

$$\text{Case 4} \quad p \equiv 1 \pmod{6} \quad \psi = \omega^{\frac{p-1}{6}}$$

ここで ω は Teichmüller 指標とする。

これらの 4 つの Case では $p {}_2F_1(\psi, \bar{\psi}/x)$ に対応する行列

$\bar{\Phi}_f$ は有理整数係数となる。Case 1 では楕円曲線

$$y^2 = x(x-1)(x-\lambda) \quad \text{の} \quad a_p(\lambda) \quad \text{と超幾何関数} \quad {}_2F_1(\phi, \phi/\lambda) \quad \text{との}$$

関係式がある。たよりに、残りの Case でも楕円曲線との関係が期待される。実際 Case 3, Case 4 については、次の結果が得られる。

定理 素数 $p \geq 101$ とする。楕円曲線 E_λ^2 :

$$E_\lambda^2: y^2 = x^3 + x^2 + \frac{\lambda}{4}x \quad \lambda \neq 0, 1$$

の Frobenius 写像の跡を $a_p(\lambda, 2)$ とかくと

$$a_p(\lambda, 2) = -p {}_2F_1(\psi, \bar{\psi}/\lambda)$$

ただし ψ は Case 3 の指標.

定理 同じ p についての条件で 楕円曲線 E_λ^1

$$E_\lambda^1: y^2 = x^3 + x^2 - \frac{4}{27}\lambda \quad \lambda \neq 0, 1$$

の Frobenius 写像の跡 $a_p(\lambda, 1)$ について

$$a_p(\lambda, 1) = -p {}_2F_1\left(\psi, \bar{\psi} \middle| \lambda\right)$$

ただし ψ は Case 4 の指標

Case 2 の場合を残したのは 楕円曲線の族としては

$x^3 + y^3 + z^3 = 3\mu xyz$ の Frobenius 写像の跡と関係する:

とは 金子氏から教ったのだが、他の Case と違うところは

は関数の定義域が μ^3 のところと注意するところであり、この等式が成立することが証明できない。

難波 [7] [8] では 楕円曲線の族から出発して予想を得ているので、上の定理のまうに有限体上の超幾何関数との関係式が、いえは、§3 の結果が使えて予想の証明ができる。

だから 有限体上の超幾何関数との関係がわからない場合の予想は未だ解けていない。特に大きく残っているのは

$p \equiv 2 \pmod{3}$ の場合には 位数 3 の指標 ψ は $\widehat{\mathbb{F}_p^\times}$ には

存在しない。ところが $a_p(\lambda)$ は定義できて、予想もある。

$p \equiv 3 \pmod{4}$, $p \equiv 5 \pmod{6}$ の場合も同様である。これは有限体上の超幾何を使う証明は未だない。

References

- [1] C.Clemens. A Scrapbook of Complex Curve Theory, Plenum Press, 1980.(Chapter 2).
- [2] J.Greene, Hypergeometric functions over finite fields, Trans.A.M.S.,301,77-101,1987.
- [3] N.Koblitz, The number of points of certain families of hypersurfacea over finite fields, Compositio Math., 48, 3-23, 1983.
- [4] M.Koike, Hypergeometric series over finite fields and Apéry numbers, Hiroshima Math. J.,22, 461-467, 1992.
- [5] M.Koike, Shift orthogonal matrices obtaines from hypergeometric series over finite fields and elliptic curves over finite fields, preprint.
- [6] K.Namba, Legendre polynomial over finite fields and factorization of integers, Proc. Int. Symp., Hua Lookeng, Springer 1991.
- [7] K.Namba, Elliptic curves over finite fields and cyclic rational orthogonal matrix, 応用数学合同研究集会 1990年
- [8] K.Namba, Elliptic curves over finite fields and cyclotomic polynomials, 応用数学合同研究集会 1991年
- [9] J. Silverman, The arithmetic of elliptic curves, GTM 106, Springer-Verlag,1986.
- [10] P.T.Young,Apéry numbers,Jacobi sums, and special values of generalized p-adic hypergeometric functions, J.Number Theory,41,231-255,1992.