数理解析研究所講究録
第768巻 1991年 167-175

有限体上の超幾何関数

広大 理 小池 正夫(Masao Koike)

§1 Introduction

整数論で重要な役割をはたすGaussの和をΓ関数の有限体アナログと見る視点がある。それは Γ関数の積分表示:

$$\Gamma(s) = \int_0^\infty t^s \cdot e^{-t} \cdot \frac{dt}{t}$$

を $\chi_s(t) := t^s$ は $\mathbb{R}_+^\times$ から $\mathbb{C}^\times$ への乗法的指標, $\lambda(t) := e^{-t}$ は $\mathbb{R}$ から $\mathbb{C}^\times$ への加法的指標, $\frac{dt}{t}$ は $\mathbb{R}_+^\times$ の Haar 測度と解釈して 実数体 $\mathbb{R}$ を 有限体 $\mathbb{F}_p$ でおきかえて, $\chi(t)$ を $\mathbb{F}_p^\times$ から $\mathbb{C}^\times$ への乗法的指標, $\lambda(t)$ を $\mathbb{F}_p$ から $\mathbb{C}^\times$ への加法的指標, そして 有限体上の不変測度は 平均をとること とすれば Gaussの和 $G(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t)\lambda(t)$ がでてくる。

$\lambda(t) = \zeta^t$, $\zeta = e^{\frac{2\pi i}{p}}$ と固定しておく。同様の考え方で Beta 関数の積分表示: $B(p,q) = \int_0^1 x^p(1-x)^q \frac{dx}{x(1-x)}$

から　この有限体アナログは　A, B を $\mathbb{F}_p^\times$ の乗法的指標として

$$J(A, B) = \sum_{t \in \mathbb{F}_p} A(t)\, B(1-t)$$

となり，Jacobi の和として知られているものとなる。

これから特殊関数に対して次の変換原理でその有限体アナログを見つけていく：

$$\begin{array}{lll} \int & \rightsquigarrow & \sum \\ t^{b} & \rightsquigarrow & B(t) \quad B : \mathbb{F}_p^\times \text{の乗法的指標} \\ t^{-b} & \rightsquigarrow & \bar{B}(t) \quad \bar{B}(t) = \overline{B(t)} \ \text{複素共役} \\ e^{-s} & \rightsquigarrow & \zeta^{s} \end{array}$$

不思議なことに有限体アナログは定義だけでなく，性質まで遺伝している；

$$B(p, q) = \frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)} \rightsquigarrow J(A, B) = \frac{G(A)G(B)}{G(AB)}$$

Γ関数の乗法公式　$\rightsquigarrow$　Davenport-Hasse の定理

$$\Gamma(z)\Gamma(z+\tfrac{1}{N}) \cdots \Gamma(z+\tfrac{N-1}{N}) = \Gamma(Nz)\, N^{\frac{1}{2}-Nz} (2\pi)^{\frac{N-1}{2}}$$

$N \mid p-1$

B : 位数 N の指標

$$G(A)\,G(AB) \cdots G(AB^{N-1}) = G(A^N)\, A^{-N}(N)\, G(B) \cdots G(B^{N-1})$$

以下　$A, B, C, \cdots \chi, \psi$ は $\mathbb{F}_p^\times$ の乗法的指標をあらわすこととする。

2項展開の有限体アナログは次の様に考える：

$$(1+x)^a = \sum_{k=0}^{\infty} \binom{a}{k} x^k$$

従って

$$A(1+x) = \delta(x) + \sum_{\chi \in \widehat{\mathbb{F}}_p^\times} f_{A,\chi}\, \chi(x), \quad x \in \mathbb{F}_p$$

$$\delta(x) = 1 \text{ if } x=0 \quad \delta(x)=0 \text{ if } x \neq 0,$$

の Fourier 係数 $f_{A,\chi}$ が 2項展開の有限体アナログである。これは簡単に計算できて $f_{A,\chi} = \dfrac{\chi(-1)}{p-1} J(A, \bar{\chi})$ となる. これを $\binom{A}{\chi}$ とかく。

同様に3項展開：$(1+x+y)^a = \sum \binom{a}{n,m} x^n y^m$ のアナログとして

$$\binom{A}{B,\ C} := \frac{BC(-1)}{(p-1)^2} J(A, \bar{B}, \bar{C})$$

が得られる。ここで $J(A,\bar{B},\bar{C})$ は Jacobi の和の一般化とよく知られている：

$$J(A, \bar{B}, \bar{C}) = \sum_{\substack{t_1+t_2+t_3=0 \\ t_i \in \mathbb{F}_p}} A(t_1) B(t_2) C(t_3)$$

Greene [G] は有限体上の超幾何関数を

$$ {}_2F_1\left(\begin{matrix} A,\ B \\ C \end{matrix} \middle| x\right) = \varepsilon(x) \frac{BC(-1)}{p-1} \sum_{y \in \mathbb{F}_p} B(y) \bar{B}C(1-y) \bar{A}(1-xy)$$

ここで　$\varepsilon(x)=0$ if $x=0$　$\varepsilon(x)=1$ if $x\neq 0$,

で定義した。これは 超幾何関数の Euler 積分表示：

$$ {}_2F_1\left(\begin{matrix}\alpha,\ \beta\\ \gamma\end{matrix}\middle|\, z\right) = \frac{\Gamma(\gamma)}{\Gamma(\beta)\Gamma(\gamma-\beta)}\int_0^1 t^{\beta}(1-t)^{\gamma-\beta}(1-tz)^{-\alpha}\frac{dt}{t(1-t)} $$

を変換原理で移したものである。但し定数倍は都合のよいようにかえてある。この時 超幾何関数の Taylor 展開：

$$ {}_2F_1\left(\begin{matrix}\alpha,\ \beta\\ \gamma\end{matrix}\middle|\, z\right) = \sum_{n=0}^{\infty}\frac{(\alpha)_n(\beta)_n}{(\gamma)_n\,(1)_n}\,z^n $$

に対応して 次の式が成り立つ：

$$ {}_2F_1\left(\begin{matrix}A,\ B\\ C\end{matrix}\middle|\, x\right) = \varepsilon(x)\sum_{\chi\in\widehat{\mathbb{F}_p^{\times}}}\binom{A\chi}{\chi}\binom{B\chi}{C\chi}\chi(x) $$

同様に

$$ {}_{n+1}F_n\left(\begin{matrix}A_0,\ A_1,\ \cdots,\ A_n\\ B_1,\ \cdots,\ B_n\end{matrix}\middle|\, x\right) := \varepsilon(x)\sum_{\chi}\binom{A_0\chi}{\chi}\cdots\binom{A_n\chi}{B_n\chi}\chi(x) $$

と定義する。

Greene [G] はこの関数の性質を 古典的な超幾何関数の持つ性質と対応させながら Kummer の変換, 2次変換 … を調べている。我々の興味は Greene が有限体上の超幾何関数の特殊値に関する次の結果にある：

(1)　$$ {}_2F_1\left(\begin{matrix}A,\ B\\ C\end{matrix}\middle|\, 1\right) = A(-1)\binom{B}{\bar{A}C} $$

(2) $${}_2F_1\left(\begin{matrix} A, & B \\ & \bar{A}B \end{matrix} \middle| -1\right) = \begin{cases} 0 & \text{if } B \neq \text{square}, \\ \binom{C}{A} + \binom{\phi C}{A} & \text{if } B = C^2, \end{cases}$$

ここで　$B \neq$ square とは $\mathbb{F}_p^\times$ の乗法的指標 C で $C^2 = B$ をみたすものがないことをいう。ϕ は $\mathbb{F}_p^\times$ の位数 2 の乗法的指標をあらわす。

(3)　$A, B, A B\bar{C}$ がそれぞれ自明な指標でないとする。

$${}_3F_2\left(\begin{matrix} A, & B, & C \\ & \bar{A}C, & \bar{B}C \end{matrix} \middle| 1\right) = \begin{cases} 0 & \text{if } C \neq \text{square} \\ AB(-1)\left\{\binom{D}{A}\binom{B\bar{D}}{AB\bar{D}} + \binom{\phi D}{A}\binom{\phi B\bar{D}}{\phi AB\bar{D}}\right\} & \text{if } C = D^2. \end{cases}$$

(4)

$${}_3F_2\left(\begin{matrix} \phi, & \phi, & \phi \\ & \varepsilon, & \varepsilon \end{matrix} \middle| -1\right) = \frac{1}{(p-1)^2}\begin{cases} -p\,\phi(2) & \text{if } p \equiv 5, 7 \pmod 8, \\ \phi(2)(4c^2 - p) & \text{if } p \equiv 1, 3 \pmod 8) \end{cases}$$

ここで　$p = c^2 + 2d^2$ とする．

§2　応用

有限体上の超幾何関数に関する Greene の特殊値の計算を Apery 数の合同式の証明に利用する。Apery 数というのは

2項係数を使って次の式で定義される：

$$a_n = \sum_{k=0}^{n} \binom{n+k}{k}^2 \binom{n}{k}^2$$

この数は $\zeta(3)$ の無理数性を証明するのに使われたが，その後 Beukers 等によって代数幾何学的な対象とのつながりが明らかにされてきた．[S-B] を参照．

Apery数の合同式を説明する前に一般化された Apery数：

$$a_n^{(m,\ell)} = \sum_{k=0}^{n} \binom{n+k}{k}^m \binom{n}{k}^\ell \qquad m, \ell \geq 0$$

を定義する．

Beukers 等の見つけた合同式で我々の興味があるのは p を奇素数，$f = \frac{p-1}{2}$ とおいた時 $a_f^{(m,\ell)}$ を modulo p で表示する場合である．$m+\ell \leq 2$ は省略して（[B] 参照）

$$(5) \qquad a_f^{(1,2)} \equiv \begin{cases} 0 \pmod{p} & \text{if} \quad p \equiv 3 \pmod 4, \\ 4a^2 \pmod{p} & \text{if} \quad p \equiv 1 \pmod 4 \\ & p = a^2 + b^2,\ a \equiv 1 \pmod 4. \end{cases}$$

$$(6) \qquad a_f^{(2,2)} \equiv \gamma_p \pmod{p}$$

ここで $\sum_{n=1}^{\infty} \gamma_n e^{2\pi i n z} = \eta(2z)^4 \eta(4z)^4$，$\eta(z)$ は Dedekind の η-関数とする．

$a_f^{(2,1)}$ の合同式もあるが，それは [S-B] を参照．

当然，m, ℓ を大きくした時どうなっているか興味がわく。

谷川氏の見つけた予想：

$$a_f^{(2,4)} \equiv c_p \pmod{p}$$

ただし $\displaystyle\sum_{n=1}^{\infty} c_n e^{2\pi i n z} = \eta(z)^8 \eta(4z)^4 + 8\eta(4z)^{12}$.

Greene の結果を利用するために、有限体上の指標とか、超幾何関数の値を p 進数の中にうめこんで考える。

Teichmüller 指標 $\omega : \mathbb{F}_p^\times \to \mathbb{Q}_p^\times$　$\omega(x) \bmod p = x$.

すると $\widehat{\mathbb{F}_p^\times} = \{ \omega^k \mid 0 \le k \le p-2 \}$ となる。この時

<u>Lemma</u>

$$\binom{\omega^k}{\omega^i} \equiv \begin{cases} \binom{k}{i} \pmod{p} & \text{if } 0 \le i \le k, \\ 0 \pmod{p} & \text{if } k < i \le p-2. \end{cases}$$

すなわち　2項係数の有限体アナログが modulo p で眺めれば又2項係数と一致する。これを定義式にあてはめれば、

<u>Proposition</u>

$$a_f^{(m,\ell)} \equiv {}_{m+\ell}F_{m+\ell-1}\left(\begin{matrix} \phi, \phi, \cdots, \phi \\ \varepsilon, \cdots, \varepsilon \end{matrix} \,\middle|\, (-1)^\ell \right) \pmod{p}.$$

この合同式の右辺に Greene の結果を適用すると、例えば $(m,\ell)=(1,2)$ とすれば

$$a_f^{(1,2)} \equiv \begin{cases} 0 \pmod{p} & \text{if } \phi \ne \text{square}, \\ \binom{\frac{3}{2}f}{f}\binom{\frac{3}{2}f}{\frac{1}{2}f} & \text{if } \phi = \text{square}. \end{cases}$$

明らかに $\phi = square \iff p \equiv 1 \pmod 4$ だし、古典的な Gaussの合同式（[B-E], [I-R]参照）

$$\binom{\frac{3}{2}f}{f} \equiv (-1)^f 2a \pmod p$$

を用いれば Beukersの合同式(5)が得られる。しかしこの方法では ${}_4F_3$ の特殊値は計算できていないので (6)は出ない。

他の利点をいうと、Apery数の $\frac{p-1}{2}$ 番目を考えたことは modulo p で見ると $\omega^{\frac{p-1}{2}} = \phi$ という式を通じて 命題のような 超幾何関数とつながって 合同式が存在していた。

だから $\frac{p-1}{3}$, $\frac{p-1}{4}$, … を考えれば 超幾何関数の有限体の指標を 位数3, 4, … の指標におきかえればよい。

3項係数を定義しておいたのは Appelleの超幾何関数の有限体アナログの Fourier展開としてそれらが あらわれてくるからなのだが、時間がつきたので ここではのべない。Beukersの考察と同様のことが調べられてしかるべきだと思う。

有限体の超幾何関数という立場は 最近、有限体上の楕円曲線の族から得られる直交行列の研究にも役立っている。

References

[B] F.Beukers, Arithmetical properties of Picard-Fuchs equations, Sem. de Theorie des Nombres, Paris 1982-1983, 33-38, Progress Math.51, Basel, Boston, Stuttgart, Birkhauser 1984.

[B-E] B. Berndt and R. Evans, Sums of Gauss, Jacobi and Jacobstahl, J. Number Theory 11 (1979), 349-398.

[G] J. Greene, Hypergeometric functions over finite fields, Trans. Amer. Math. Soc. 301 (1987), 77-101.

[G-S] J. Greene and D. Stanton, A character sum evaluation and Gaussian hypergeometric series, J. Number Theory 23 (1986), 136-148.

[I-R] K. Ireland and M. Rosen, A classical introduction to modern number theory, GTM 84, Springer-Verlag, New York heidelberg Berlin, 1982.

[S-B] J. Stienstra and F. Beukers, On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces, Math. Ann. 271 (1983), 269-304.