

## ガウスの和の $l$ 進展開とその応用

都立大理 三木博雄 (Hiroo Miki)

この講演において、あるガウスの和の  $l$  進展開  $\text{mod } \pi^l$  の新しい explicit formula を与える。その応用として、

- (1) ヤコビの和に関する岩沢の合同式、伊原の合同式の一般化、
- (2) 岩沢の Invent. Math. (セール記念号) の主要結果の別証明がえられる。

$p$  を任意の素数、 $m > 1$  を  $p$  で割れない自然数、 $\zeta_m$  を複素数体  $\mathbb{C}$  内の 1 の原始  $m$  乗根とし、 $C_m = \mathbb{Q}(\zeta_m)$  とおく。 $p$  の上の  $C_m$  の素イデアル  $\mathfrak{p}$  を 1 つ固定して、 $N\mathfrak{p} = \mathfrak{p}$  とおくと、 $m \mid (p-1)$  である。 $\chi_{\mathfrak{p}}(x \text{ mod } \mathfrak{p}) = \left(\frac{x}{\mathfrak{p}}\right)_m$  ( $x \in \mathbb{Z}[\zeta_m]$ ) を  $C_m$  における  $m$  中剰余記号とする。すなわち、

$$\chi_{\mathfrak{p}}(x \text{ mod } \mathfrak{p}) \equiv x^{\frac{p-1}{m}} \pmod{\mathfrak{p}} \quad (\forall x \in \mathbb{Z}[\zeta_m])$$

で、 $\chi_{\mathfrak{p}}$  の  $\mathbb{F}_{\mathfrak{p}}^{\times}$  への制限は  $\mathbb{F}_{\mathfrak{p}}^{\times}$  の位数  $m$  の指標であり、 $\chi_{\mathfrak{p}}(0) = 0$  となる。ただし  $\mathbb{F}_{\mathfrak{p}}$  と  $\mathbb{Z}[\zeta_m]/\mathfrak{p}$  を同一視する。T

を  $\mathbb{F}_q$  から  $\mathbb{F}_p$  への trace として,  $\psi(a) = \zeta_p^{T(a)}$  ( $a \in \mathbb{F}_q$ ) とおくと,  $\psi$  は加法群  $\mathbb{F}_q$  から乗法群  $\mathbb{C}^\times$  への準同型となる。

定義. 各  $a \in \mathbb{Z}$  に対して,

$$g_m(p, a) = g(\chi_p^a) = g(a) = -\sum_{x \in \mathbb{F}_q} \chi_p^a(x) \psi(x)$$

において, これを ガウスの和 という。

明らかに,  $g(a) \in \mathbb{C}_{mp}$ 。

目標.  $m = l$  (素数) のとき,  $g(\chi_p^a)$  の  $l$  進展開 mod  $\pi^l$  の explicit な表示を求めること。

これについて昭和60年1月から2月にかけての金沢大・東工大における集中講義ですでに述べたが, ここではそれを少し改良した形で述べる。

$\overline{\mathbb{Q}}$  を  $\mathbb{Q}$  の  $\mathbb{C}$  における代数閉包,  $\overline{\mathbb{Q}_l}$  を  $l$  進数体  $\mathbb{Q}_l$  の代数閉包とし, 埋め込み  $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_l}$  をひとつ固定して  $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}_l}$  とみる。 $\pi$  を  $\pi^{l-1} = -l$  および  $\zeta_l \equiv \text{Exp } \pi \pmod{\pi^l}$  をみたす  $\mathbb{Q}_l(\zeta_l)$  の素元とする。ここに,  $\text{Exp } X = 1 + X + \frac{X^2}{2!} + \dots + \frac{X^{l-1}}{(l-1)!}$ 。

$\chi_p(x) = \zeta_p^{\lambda(x)}$  ( $x \in \mathbb{F}_q^\times$ ) によって,  $\lambda(x) \in \mathbb{Z}$  を定義する。 $\lambda(x)$  は mod  $l$  で確定するから,  $\lambda(x) \in \mathbb{F}_l$  とみれば,  $\lambda$  は乗法群  $\mathbb{F}_q^\times$  から加法群  $\mathbb{F}_l$  への準同型となる。

次に  $\mathbb{C}_l$  の円単数の定義を述べる。ガロア群  $G = G(\mathbb{C}_l/\mathbb{Q})$  と  $\mathbb{F}_l^\times = (\mathbb{Z}/l\mathbb{Z})^\times$  を対応  $\sigma_a \leftrightarrow a \pmod{l\mathbb{Z}}$  ( $a \in \mathbb{Z}$ ) によって同一視する。ここに,  $\sigma_a(\zeta_l) = \zeta_l^a$ 。従って,  $\hat{G}$  を  $G$  の指標

群とすると,  $\psi \in \hat{G}$  ならば,  $\psi(\sigma_a) = \psi(a)$  ( $a \in \mathbb{F}_l^\times$ ) で,  
 $\psi(a) \in \mathbb{Z}[\zeta_{l-1}] \subset \mathbb{Z}_l$ . 各  $\psi \in \hat{G}$  に対して,

$$e_\psi = \frac{1}{l-1} \sum_{a=1}^{l-1} \psi(a)^{-1} \sigma_a \in \mathbb{Z}_l[G]$$

とあき,  $\psi = \omega^{-i}$  ( $i \in \mathbb{Z}$ ) のときは,  $e_\psi = e_i$  とかく。ここに,  
 $\omega \in \hat{G}$  は Teichmüller 指標, すなわち,  $\omega(a) \equiv a \pmod{l\mathbb{Z}_l}$   
なる指標である。以下  $l \geq 5$  とし,  $\psi = \omega^{-2i}$  ( $1 \leq i < \frac{l-1}{2}$ )  
のとき,  $\sum_{a=1}^{l-1} \psi(a)^{-1} = 0$  だから,  $\sum_{a=1}^{l-1} m_a = 0$  および  $\mu \equiv e_\psi$   
 $(\text{mod } l\mathbb{Z}_l[G])$  をみたす  $\mu = \sum_{a=1}^{l-1} m_a \sigma_a \in \mathbb{Z}[G]$  ( $m_a \in \mathbb{Z}$ ) が存  
在する。

定義.  $E_{2i} = (1 - \zeta_l)^\mu = \prod_{a=1}^{l-1} (1 - \zeta_l^a)^{m_a}$  ( $1 \leq i < \frac{l-1}{2}$ )

とあいて, これを  $\mathbb{C}_l$  の (実) 冪単数 という。

定理. 上の記号と仮定のもとで, 各  $1 \leq i < l$  に対して,

$$g(\chi_f^a) \equiv \text{Exp} \left( \alpha_1 (a\pi) + \sum_{i=1}^{(l-3)/2} \beta_{2i} \cdot \frac{(a\pi)^{2i+1}}{(2i+1)!} + \frac{f-1}{2l} \pi^{l-1} \right) \pmod{\pi^l}.$$

ここに,  $\alpha_1 = -\sum_{x \in \mathbb{F}_f^\times} \lambda(x) \psi(x)$ ,  $\beta_{2i} = -\lambda(E_{2i} \text{ mod } f)$  ( $1 \leq i < \frac{l-1}{2}$ ).

以下, 上の定理の応用を 2 つ述べる。

応用 (I) ヤコビの和の合同式.

$a = (a_1, \dots, a_r) \in \overbrace{\mathbb{Z}/m\mathbb{Z} \times \dots \times \mathbb{Z}/m\mathbb{Z}}^r$  に対して,

$$J_a(f) = (-1)^{r+1} \sum_{\substack{x_1 + \dots + x_r = -1 \\ x_1, \dots, x_r \in \mathbb{F}_f}} \chi_f(x_1)^{a_1} \dots \chi_f(x_r)^{a_r}$$

とあいて, これを ヤコビの和 という。

上の定理の応用として、直ちに次のヤコビの和の合同式がえられる。

系.  $m = l \geq 5$ ,  $a = (a_1, \dots, a_r)$  のとき,

$$J_a(\beta) \equiv \text{Exp} \left\{ \sum_{i=1}^{\frac{l-3}{2}} \left( \sum_{j=1}^r a_j^{2i+1} - \left( \sum_{j=1}^r a_j \right)^{2i+1} \right) \beta_{2i} \frac{\pi^{2i+1}}{(2i+1)!} \right\} \pmod{\pi^{l-1}}.$$

この合同式は、岩沢の合同式 ([2], Theorem 1) の一般化であって、 $m$  が  $l$  のべきのときも全く同様にしてヤコビの和の合同式  $\pmod{\pi^{l-1}}$  ( $\pi$  は  $C_m$  の素元) が得られ、それは伊原の合同式 ([1], Corollary to Theorem 7) の一般化になっている。

### 応用 (II) 岩沢 [3] の主要結果の別証明。

岩沢 [3] においては、局所類体論におけるノルム剰余記号の explicit formula に関する Artin-Hasse の公式が重要な手段になっているが、ここではその代りに上の定理を用いることにより初等的な証明が可能となる (以下の ① ② 参照)。

① ある仮定のもとで,  $\sum_{a=1}^{l-1} a \delta(a) \neq 0$  の代数的証明。ここ

に  $\delta \in \hat{G}$  は odd character, すなわち,  $\delta(-1) = -1$ 。

$\sum_{a=1}^{l-1} a \delta(a) \neq 0$  の一般的証明は Dirichlet の L 関数の  $s=1$  の値が 0 でないということからでてくるが、代数的証明は特別の場合にしかわかっていない。その場合のうちの一つが岩沢 [3] にある。ここでは、上の定理を用いる初等的証明を与

える。

$\delta \neq \omega$  としてよい。  $l \mid (p-1)$  なる素数  $p$  をとって、  $f(x_p)$  を考えると、

$$(*) \quad (f(x_p)) = \beta^{d\theta} \quad (\text{Stickelberger の定理}),$$

ここに、  $d = (p-1)/l$  ,  $\theta = \sum_{a=1}^{l-1} a \sigma_a^{-1} \in \mathbb{Z}[G]$  で、  $\beta$  は  $f$  の上の  $\mathbb{C}_{l,p}$  の唯一つの素イデアルである。

$\delta$  の位数を  $g$  とし、  $\alpha_\delta$  を  $G/\text{Ker } \delta$  の生成元の代表元 ( $1 >$  固定) として、

$$\alpha_\delta = \left( \sum_{\sigma \in \text{Ker } \delta} \sigma \right) \prod_{p'} (1 - \alpha_\delta^{g/p'}) \in \mathbb{Z}[G]$$

とおく。ここに  $p'$  は  $p \nmid p'$  なるすべての素数をうごく。

Ullom [5] によつて、

$$\sum_{a=1}^{l-1} a \delta(a)^{-1} = 0 \iff \left( \sum_{a=1}^{l-1} a \sigma_a^{-1} \right) \alpha_\delta = 0.$$

従つて、もし  $\sum_{a=1}^{l-1} a \delta(a)^{-1} = 0$  ならば、(\*) に  $\alpha_\delta$  を作用させて、 $(f(x_p)^{\alpha_\delta}) = 1$ 、従つて、 $f(x_p)^{\alpha_\delta}$  は単数になり、 $f(x_p)^{\alpha_\delta} = 1$  が容易に示される。一方、 $\delta = \omega^{2i_0+1}$  ( $1 \leq i_0 < \frac{l-1}{2}$ ) とかけるが、Čebotarev の密度定理 (この場合は代数的にわかっている。cf. Wojcik [7]) によつて、もし  $E_{2i_0} \notin \mathbb{C}_l^l$  ならば、ある  $f$  をうまくとつて、 $\beta_{2i_0} \neq 0$  および  $\beta_{2i} = 0$  ( $1 \leq i < i_0$ ) がいえる。このとき、上の定理から、 $f(x_p)^{\alpha_\delta} \neq 1$  がわかる。これは矛盾。よつて、 $\sum_{a=1}^{l-1} a \delta(a)^{-1} \neq 0$ 。

② 他の岩沢 [3] の主要結果 ( $\varepsilon_{2i} \in \mathbb{C}_\ell^*$  となるための必要十分条件) の別証明。

Uehara [4] でヤコビの和を用いた別証明が与えられているが、それとは異なる証明が得られる。われわれの方法は上の定理と Weil-岩沢の定理 (Weil [6], Theorem; 岩沢 [2], Theorem 2) を用いるもので、証明はかなり短くなる。

### 文 献

- [1] Y. Ihara, Profinite braid groups, Galois representations and complex multiplications, to appear in Ann.of Math.
- [2] K. Iwasawa, A note on Jacobi sums, Symposia Math.15(1975), 447-459.
- [3] K. Iwasawa, A note on cyclotomic fields, Invent.Math.36 (1976), 115-123.
- [4] T. Uehara, On cyclotomic units connected with p-adic characters, J. Math. Soc. Japan 37(1985), 65-77.
- [5] S. Ullom, The nonvanishing of certain character sums, Proc. Amer. Math. Soc. 45(1974), 164-166.
- [6] A. Weil, Jacobi sums as "Grossencharaktere", Trans. Amer. Math. Soc. 73(1952), 487-495.
- [7] J. Wojcik, A purely algebraic proof of special cases of Tchebotarev's theorem, Acta Arith.28(1975), 137-145.