数理解析研究所講究録
998 巻 1997 年 153-160

Jacobi 和の有理性問題について

九大 白谷克巳 (Katsumi Shiratani)
九大・数理 山田美枝子 (Mieko Yamada)

§1. 序

奇素数べき $q=p^f$ に対し有限体 GF(q) の乗法群 GF$(q)^\times$ の指標群は Teichmüller 指標 ω で生成される $q-1$ 次巡回群である. $\chi\in<\omega>$, $\chi\neq\omega^0$(単位指標), $\eta=\omega^{\frac{q-1}{2}}\in<\omega>$ に対し, $\chi\neq\eta$ のとき, Jacobi 和

$$J(\chi,\eta)=\sum_{x\in \mathrm{GF}(q)-\{0,1\}}\chi(x)\eta(1-x)$$

が有理数となるための χ と q に関する条件を求める. この問題は組合せ数学の問題と関係する.

Gauss 和 $g(\chi)$ は次で定義される.

$$g(\chi)=\sum_{x\in \mathrm{GF}(q)^\times}\chi(x)\zeta_p^{s(x)}$$

ここで, ζ_p は 1 の原始 p 乗根, $s(x)$ は x の GF(q)/GF(p) に関する trace $s(x)=x+x^p+\cdots+x^{p^{f-1}}$ である. Gauss 和 $g(\chi)$ と Jacobi 和 $J(\chi,\eta)$ には次の関係式が成り立つ.

$$J(\chi,\eta)=\frac{g(\chi)g(\eta)}{g(\chi\eta)}.$$

Gauss 和 $g(\omega^{-i})\in\mathbf{Q}(\zeta_p,\zeta_{q-1})$, $(0\leq i\leq q-2)$ を p 進体 $\mathbf{Q}_p(\zeta_p,\zeta_{q-1})$ に埋め込む. ζ_{q-1} は 1 の原始 $q-1$ 乗根を表わす. このとき, Gross-Koblitz の公式が成り立つ.

$$g(\omega^{-i})=-\varpi^{s_p(i)}\prod_{l=0}^{f-1}\Gamma_p\Big(\frac{p^l i}{q-1}-\sum_{j=1}^{l}i_{f-j}p^{l-j}\Big). \tag{1}$$

ここで, i の標準 p 進展開を $i=i_0+i_1p+\ldots+i_{f-1}p^{f-1}$, $0\leq i_j\leq p-1$ とするとき, $s_p(i)=\sum_{j=0}^{f-1}i_j$ であり, ϖ は $\mathbf{Q}_p(\zeta_p)$ の素元で, $\varpi=\sqrt[p-1]{-p}$, $\varpi\equiv\zeta_p-1\ (\mathrm{mod}\ (\zeta_p-1)^2)$ を満たすものを示し, $\Gamma_p(x)$ は p 進 gamma 関数である. 以下では $\varpi^{s_p(i)}$ を $g(\omega^{-i})$ の ϖ-part, $\prod_{l=0}^{f-1}\Gamma_p(\frac{p^l i}{q-1}-\sum_{j=1}^{l}i_{f-j}p^{l-j})$ を $g(\omega^{-i})$ の gamma product part と呼ぶ.

p 進 gamma 関数について, 次のノルム関係式 (N_p) と distribution relation (D_p) が成り立つ.

(N_p) $x \in \mathbf{Z}_p$に対して $\Gamma_p(x)\Gamma_p(1-x) = (-1)^{1+u(-x)}$

ここで $0 \leq u(-x) < p, u(-x) \equiv -x \pmod p$.

(D_p) $m \in \mathbf{N}$, $(m,p)=1$, $x \in \mathbf{Z}_p$に対し

$$\frac{\prod_{h=0}^{m-1} \Gamma_p(\frac{x+h}{m})}{\Gamma_p(x)\prod_{h=1}^{m-1}\Gamma_p(\frac{h}{m})} = m^{u(-x)} m^{\frac{1-p}{p}(u(-x)+x)}.$$

§2. 一般の場合

$J(\omega^{-i}, \omega^{\frac{q-1}{2}}) \in \mathbf{Q}$ と仮定する. このとき, 絶対値 $|J(\omega^{-i}, \omega^{\frac{q-1}{2}})| = \sqrt{q}$から $f \equiv 0 \pmod 2$ が必要である. 次に, $\sigma_{-1} \in \mathrm{Gal}(\mathbf{Q}(\zeta_p, \zeta_{q-1})/\mathbf{Q}(\zeta_p))$ を

$$\sigma_{-1}(\zeta_{q-1}) = \zeta_{q-1}^{-1}, \quad \sigma_{-1}(\zeta_p) = \zeta_p$$

で定義する. $J(\omega^{-i}, \omega^{\frac{q-1}{2}})$ はσ_{-1}で固定されるので

$$\frac{g(\omega^{-i})}{g(\omega^{-i+\frac{q-1}{2}})} = \frac{g(\omega^{i})}{g(\omega^{i+\frac{q-1}{2}})}$$

が成り立つ. 両辺のϖ-part を計算すると

$1 \leq i < \frac{q-1}{2}$ のとき $\quad s_p(i) = s_p(\frac{q-1}{2}+i)$,

$\frac{q-1}{2} < i \leq q-2$ のとき $\quad s_p(i) = s_p(i-\frac{q-1}{2})$

となる. 一方

$$J(\omega^{-i}, \omega^{\frac{q-1}{2}}) = g(\omega^{\frac{q-1}{2}})\frac{g(\omega^{-i})}{g(\omega^{-i+\frac{q-1}{2}})}$$

から $J(\omega^{-i}, \omega^{\frac{q-1}{2}}) \in \mathbf{Q}$ は

(2) $$\frac{g(\omega^{-i})}{g(\omega^{-i+\frac{q-1}{2}})} = \pm 1$$

と同値である.

定理 1. $1 \leq i < \frac{q-1}{2}$ と仮定する. このとき $J(\omega^{-i}, \omega^{\frac{q-1}{2}}) \in \mathbf{Q}$ であるための必要十分条件は

(i) $f \equiv 0 \pmod 2$,

(ii) $s_p(i) = s_p(i + \frac{q-1}{2})$,

(iii) $$\prod_{l=0}^{f-1} \Gamma_p(\frac{p^l i}{q-1} - \sum_{j=1}^{l} i_{f-j} p^{l-j}) = \pm \prod_{l=0}^{f-1} \Gamma_p(\frac{p^l(i + \frac{q-1}{2})}{q-1} - \sum_{j=1}^{l} (i + \frac{q-1}{2})_{f-j} p^{l-j})$$

が成り立つことである.

§3. $f = 2$ の場合

$f = 2$ の場合を考察する. $1 \leq i < \frac{p^2-1}{2}$ の仮定のもとで, $i = i_0 + i_1 p$ を i の標準 p 進展開とするとき, 定理 1 の条件 (ii) は

$$\frac{p-1}{2} < i_0 \leq p-1, \quad 0 \leq i_1 < \frac{p-1}{2}$$

と書ける. (iii) の等式は

$$\Gamma_p(\frac{i_0 + i_1 p}{p^2 - 1}) \Gamma_p(\frac{i_1 + i_0 p}{p^2 - 1}) = \pm \Gamma_p(\frac{i_0 + i_1 p}{p^2 - 1} + \frac{1}{2}) \Gamma_p(\frac{i_1 + i_0 p}{p^2 - 1} - \frac{1}{2})$$

となる.

$$\frac{i_0 + i_1 p}{p^2 - 1} = \frac{\alpha}{d}, \quad \frac{i_1 + i_0 p}{p^2 - 1} = \frac{\beta}{d}, \quad (\alpha, d) = (\beta, d) = 1,$$

とおくと, $i_0 = \frac{1}{d}(\beta p - \alpha)$, $i_1 = \frac{1}{d}(\alpha p - \beta)$ で

$$g(\omega^{-i}) = -\varpi^{\frac{\alpha+\beta}{d}(p-1)} \Gamma_p(\frac{\alpha}{d}) \Gamma_p(\frac{\beta}{d}), \quad \beta \equiv p\alpha \pmod p$$

となる. $1 \leq i < \frac{p^2-1}{2}$ の仮定のもとで,

$$0 < \frac{\alpha}{d} < \frac{1}{2}, \quad \frac{1}{2} < \frac{\beta}{d} < 1$$

となり

$$g(\omega^{-i + \frac{p^2-1}{2}}) = -\varpi^{\frac{\alpha+\beta}{d}(p-1)} \Gamma_p(\frac{\alpha}{d} + \frac{1}{2}) \Gamma_p(\frac{\beta}{d} - \frac{1}{2}).$$

従って, $J(\omega^{-i},\omega^{-i+\frac{p^2-1}{2}})\in\mathbf{Z}$ は

$$\Gamma_p(\frac{\alpha}{d})\Gamma_p(\frac{\beta}{d})=\pm\Gamma_p(\frac{\alpha}{d}+\frac{1}{2})\Gamma_p(\frac{\beta}{d}-\frac{1}{2}) \tag{3}$$

が $(\alpha,d)=1, 1\le\alpha\le d$ である任意の数 α で成立することと同値である.

$\frac{\alpha}{d}+\frac{\beta}{d}=1$ であるとき, 即ち $i=i_0+i_1p=k(p-1)$, $k=1,\cdots,p$ は解となることが分かる. 又, $\frac{\alpha}{d}=\frac{\beta}{d}-\frac{1}{2}$ 即ち, $i=i_0+i_1p=\frac{p+1}{2}k$, $k=1,3,\cdots,2(p-1)-1$ も解である.

定理 2. $1\le i<p^2-1$ とする. このとき, $i=(p-1)k$ $(k=1,\cdots,p)$, $i=\frac{p+1}{2}k$ $(k=1,3,\cdots,2(p-1)-1)$ ならば $J(\omega^{-i},\omega^{\frac{p^2-1}{2}})\in\mathbf{Z}$ である.

これらを自明な解と呼ぶことにする. 次に, 非自明な解を求める.
等式 $g(\omega^{-i})=\pm g(\omega^{-i+\frac{p^2-1}{2}})$ は, ζ_dを 1 の原始 d 乗根とするとき, Galois 群 $\mathrm{Gal}(\mathbf{Q}(\zeta_d)/\mathbf{Q})$ の元によって固定される. 従って (3) 式は

$$\begin{aligned}\Gamma_p(\frac{1}{d})\Gamma_p(\frac{\beta}{d}) &= \pm\Gamma_p(\frac{1}{d}+\frac{1}{2})\Gamma_p(\frac{\beta}{d}-\frac{1}{2}),\\ \beta\equiv p \pmod d, &\qquad \frac{1}{d}<\frac{\beta}{d}-\frac{1}{2}<\frac{\beta}{d}<\frac{1}{d}+\frac{1}{2}\end{aligned} \tag{4}$$

に同値である.

補題 1. ω^{-i} の位数を d とする. ω^{-i} が非自明な解を与えれば d は 4 で割れる.

証明. $\chi=\omega^{-i}$, $\eta=\omega^{\frac{p^2-1}{2}}$ と書いて, χの位数 d_χ又は$\chi\eta$の位数 $d_{\chi\eta}$は 2 で割れるから, $2||d_\chi$なら $2\not|d_{\chi\eta}$である. 従って, $2\not|d_\chi$としてよい.

$\sigma_2:\zeta_d\to\zeta_d^2$は $\mathrm{Gal}(\mathbf{Q}(\zeta_d)/\mathbf{Q})$ の元である. n を $2^n\equiv 1 \pmod d$ となる最小の正整数とする. Davenport-Hasse 関係式

$$\frac{\prod_{\psi^m=1} g(\chi\psi)}{g(\chi^m)\prod_{\psi^m=1} g(\psi)}=\chi(m^{-m})$$

の $m=2$ の場合を使って

$$g(\chi)^2 = \pm g(\chi)g(\chi\eta) = \pm\chi(2^{-2})g(\eta)g(\chi^2).$$

σ_2を繰り返し作用させて

$$g(\chi) = g(\chi^{2^n}) = \pm p^{-(2^n-1)}g(\chi)^{2^n}$$

を得る. Gross-Koblitz の公式 (1) から両辺のϖ-part を比べることにより,

$$-\varpi^{\frac{\alpha+\beta}{d}(p-1)} = (-\varpi^{\frac{\alpha+\beta}{d}(p-1)})^{2^n}p^{-(2^n-1)}.$$

故に $\alpha+\beta=d$. これは ω^{-i} が自明解であることを意味する.

等式 (2) $g(\omega^{-i}) = \pm g(\omega^{-i+\frac{p^2-1}{2}})$ と, 両辺を 2 乗した $g(\omega^{-i})^2 = g(\omega^{-i+\frac{p^2-1}{2}})^2$は同値である. Gauss 和の Davenport-Hasse 関係式は 2-torsion を除けば universal distribution である. 従って $g(\omega^{-i})^2 = g(\omega^{-i+\frac{p^2-1}{2}})^2$は Davenport-Hasse 関係式とノルム関係式から得られる. Davenport-Hasse 関係式とノルム関係式は Gross-Koblitz 公式を使うと p 進 gamma 関数の distriburtion relation とノルム関係式から導かれるので 式 (4)

$$\Gamma_p(\frac{1}{d})\Gamma_p(\frac{\beta}{d}) = \pm\Gamma_p(\frac{1}{d}+\frac{1}{2})\Gamma_p(\frac{\beta}{d}-\frac{1}{2})$$

は distribution relation とノルム関係式から得られるもののみが自明でない解を与える.

式 (4) が $(m,p)=1$ である m 乗法の distribution relation と連立解を持つとき m-reducible と呼ぶ. 等式が成り立つことと, ある奇素数 l があって, $l||d$ で l-reducible であることは同値である. 言い換えれば m-reducible ならば l-reducible である.

補題 2. ω^{-i}が非自明な解を与え, l-reducible であれば, l は 3 か又は 5 である. ω^{-i}の位数を d とすると, 等式が成り立つのは, $d=24$ で $p\equiv 17,19 \pmod{24}$ か, 又は $d=60$ で $p\equiv 41,49 \pmod{60}$ のときである.

証明.

$$\frac{\prod_{x=0}^{l-1}\Gamma_p(\frac{1}{d}+\frac{x}{l})}{\Gamma_p(\frac{l}{d})\prod_{x=1}^{l-1}\Gamma_p(\frac{x}{l})} = l^{u(-\frac{l}{d})}l^{\frac{1-p}{p}(u(-\frac{l}{d})+\frac{l}{d})} \tag{5}$$

において， $\frac{\beta}{d}=\frac{1}{d}+\frac{h}{l}$, $(h,l)=1$, 又は， $\frac{3}{2}-\frac{\beta}{d}=\frac{1}{d}+\frac{h}{l}$, $(h,l)=1$ となる $0<h<l$ が存在するときに非自明な解が得られる．このとき， $\frac{1}{d}+\frac{m}{l} \pmod{\frac{l}{d}}$ となる m が唯一つ存在する．$\sigma_p:\zeta_d \to \zeta_d^p$ を Gauss 和に作用させて，$0 \le j < h$ $j \ne m$ について

$$\Gamma_p(\frac{1}{d}+\frac{j}{l})\Gamma_p(\frac{1}{d}+\frac{h-j}{l})$$

が Gauss 和 $g(\chi\xi_l)$ の gamma product part であることが分かる．ξ_l は位数 l の指標である．等式は $g(\chi)$ を $g(\chi\xi_l)$ へ写す Galois 群 $\mathrm{Gal}(\mathbf{Q}(\zeta_d)/\mathbf{Q})$ の元で固定される．

同様に $0<j<l-h$ について

$$\Gamma_p(\frac{1}{d}+\frac{h+j}{l})\Gamma_p(\frac{1}{d}+\frac{l-j}{l})$$

も Gauss 和の gamma product part で等式の解である．従って， $\frac{1}{d}+\frac{j}{l}$, $\frac{1}{d}+\frac{h-j}{l}$ と $\frac{1}{d}+\frac{h+j}{l}$, $\frac{1}{d}+\frac{l-j}{l}$ について，どちらか一方が $\frac{1}{2}$ より小さく， 残りは $\frac{1}{2}$ より大きくなければならない．しかし後者は両方とも $\frac{1}{2}$ より大きい．従って $h=l-1, m=\frac{1}{2}(l-1)$.

式 (5) と

$$\frac{\prod_{x=0}^{l-1}\Gamma_p(\frac{\beta}{d}-\frac{1}{2}+\frac{x}{l})}{\Gamma_p(\frac{l\beta}{d}-\frac{l}{2})\prod_{x=1}^{l-1}\Gamma_p(\frac{x}{l})} = l^{u(-\frac{l\beta}{d}+\frac{l}{2})} l^{\frac{1-p}{p}(u(-\frac{l\beta}{d}+\frac{l}{2})+\frac{l\beta}{d}-\frac{l}{2})}$$

から

$$\Gamma_p(\frac{l}{d})\Gamma_p(\frac{1}{2}-\frac{1}{d}+\frac{1}{2l}) = \pm\Gamma_p(\frac{l}{d}+\frac{1}{2})\Gamma_p(\frac{1}{2l}-\frac{1}{d})$$

を得る．$\frac{d}{2l}\equiv 1 \pmod{l}$ と補題 1 から 奇数 $k\ge 1$ で $d=2l(kl+1)$ と書ける．

$l\ge 7$, $l=3, k\ge 5$, $l=5, k\ge 3$ ならば $\frac{\alpha}{d}$, $\frac{\beta}{d}<\frac{1}{2}$ となる自己同型写像が作れる．故に，$l=3, k=1$ のとき，$d=24, p\equiv 17 \pmod{24}$， $l=3, k=3$ のとき，$d=60, p\equiv 41 \pmod{60}$， $l=5, k=1$ のとき，$d=60, p\equiv 49 \pmod{60}$ が求まる．$\frac{3}{2}-\frac{\beta}{d}=\frac{1}{d}+\frac{h}{l}$ のときも同様な議論で $d=24, p\equiv 19 \pmod{24}$， $d=60, p\equiv 41, 49 \pmod{60}$ が得られる．

定理 3. $J(\omega^{-i}, \omega^{\frac{p^2-1}{2}})\in\mathbf{Q}$ であるための必要十分条件は 自明解以外に $p\equiv 17, 19 \pmod{24}$ で ω^{-i} の位数が 24, $p\equiv 41, 49 \pmod{60}$ で ω^{-i} の位数が 60 である．

証明．これらが解となることはノルム関係式 (N_p) と distribution relation (D_p) を使って容易に確かめられる．

$J(\omega^{-i}, \omega^{\frac{p^2-1}{2}})$ の値は 次のようになる.

定理 4. 非自明解, 即ち $d = 24,\ p \equiv 17, 19 \pmod{24},\ d = 60,\ p \equiv 41, 49 \pmod{60}$ のとき, $J(\omega^{-i}, \omega^{\frac{p^2-1}{2}}) = -p$ であり, 自明解 $i = \frac{1}{2}(p+1)k$のとき, $J(\omega^{-i}, \omega^{\frac{p^2-1}{2}}) = -(\frac{-1}{p})p$, $i = (p-1)k$のとき, $J(\omega^{-i}, \omega^{\frac{p^2-1}{2}}) = p$ である. ここで $(\frac{-1}{p})$ は Legendre 記号を示す.

証明. $d = 24,\ p \equiv 17 \pmod{24}$ の場合は

$$\frac{\Gamma_p(\frac{1}{24})\Gamma_p(\frac{9}{24})\Gamma_p(\frac{17}{24})}{\Gamma_p(\frac{1}{8})\Gamma_p(\frac{1}{3})\Gamma_p(\frac{2}{3})} = 3^{u(-\frac{1}{8})-\frac{16}{17}(u(-\frac{1}{8})+\frac{1}{8})} = 1,$$

$$\frac{\Gamma_p(\frac{5}{24})\Gamma_p(\frac{13}{24})\Gamma_p(\frac{21}{24})}{\Gamma_p(\frac{5}{8})\Gamma_p(\frac{1}{3})\Gamma_p(\frac{2}{3})} = 3^{u(-\frac{5}{8})-\frac{16}{17}(u(-\frac{5}{8})+\frac{5}{8})} = 1$$

とノルム関係式 (N_p) を使って

$$\Gamma_p(\frac{1}{24})\Gamma_p(\frac{17}{24}) = \Gamma_p(\frac{5}{24})\Gamma_p(\frac{13}{24})$$

が得られ, $g(\omega^{\frac{p^2-1}{2}}) = (-1)^{\frac{p+1}{2}}p$ から $J(\omega^{-i}, \omega^{\frac{p^2-1}{2}}) = -p$ となる. 他の場合についても同様に求まる.

Davenport-Hasse 関係式から定理 3 の条件は一般の拡大において十分条件であることが分かる.

参考文献

[1] N. Aoki, *Abelian fields generated by a Jacobi sums*, Commentarii Mathematici Universitatis Sancti Pauli 45 (1966), 1-21.

[2] R.F. Coleman, *The Gross-Koblitz formula*, Adv. Stud. Pure Math. 12 (1987), 21-52.

[3] H. Davenport und H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen* , J. Reine Angew. Math. 172 (1935), 151-182.

[4] M. Ishibashi, H. Sato, K. Shiratani, *On the Hasse invariants of elliptic curves*, Kyushu J. Math. 48 (1994), 307-321.

[5] T. Ito, H. Ishibashi, A. Munemasa and M. Yamada, *The Terwilliger Algebras of cyclotomic schemes and rationality of Jacobi sums*, Algebraic Combinatorics (Fukuoka 1993), 43-44.

[6] N. Koblitz, p-adic Analysis: a short course on recent works, Cambridge University Press, Cambridge, 1980.

[7] M. Koike, *Orthogonal matrices obtained from hypergeometric series over finite fields and elliptic curves over finite fields*, Hiroshima Math. J. 25. (1995), 43-52.

[8] C.G. Schmidt, *Die Relationenfaktorgruppen von Stickelberger-Elementen und Kreiszahlen*, J. Reine Angew. Math. 315 (1980), 60-72.

[9] L.G.Washington, Introduction to Cyclotomic Fields, Grad. Texts in Math. 83, Springer, 1982.

[10] K. Yamamoto, *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*, J. Combin. Theory 1 (1966), 476-489.

[11] K. Yamamoto, *The gap group of multiplicative relationships of Gaussian sums*, Sympos. Math. 15 (1975), 427-440.