数理解析研究所講究録
第837巻 1993年 14-24

3次のGauss和の偏角を近似する初等的な積について.

名大 理 伊藤 博 (Hiroshi Ito)

1. 主結果. (The main result of this note is stated in Ito [I]). $\rho = e^{2\pi i/3}$ とし, ω を $\mathbb{Q}(\rho)$ の素 ideal で1次かつ3と素なものの生成元とする. さらに, $\omega \equiv 1 \pmod 3$ と取られているとし, $p = \omega\bar{\omega}$ とおく ($\bar{\omega}$ は ω の複素共役). まず 3次の Gauss 和 $\tau_3(\omega)$ を

$$\tau_3(\omega) = \sum_{a=1}^{p-1} \left(\frac{a}{\omega}\right)_3 e^{2\pi i a/p}$$

で定義する. 但し $\left(\frac{a}{\omega}\right)_3$ は, $\mathbb{Q}(\rho)$ の3乗剰余記号である. 次に, 標題の「初等的な積」を定義するため, mod ω の $\frac{1}{3}$-代表系 S をひとつとる. (「mod ω の $\frac{1}{3}$-代表系」とは, $\mathbb{Z}[\rho]$ の $(p-1)/3$ 個の元からなる部分集合 S で, $r, \rho r, \rho^2 r$ $(r \in S)$ の全体が, $\mathbb{Z}[\rho]/\omega\mathbb{Z}[\rho]$ の既約剰余類群の完全代表系となるようなもののことを言う). さらに

$$e(z) = \exp\left(2\pi \frac{z - \bar{z}}{\sqrt{3}}\right), \quad z \in \mathbb{C}$$

とおいて, 次の積 $\delta_3(\omega)$ を考える:

$$(1.1)\qquad \delta_3(\omega)=\alpha(S)\cdot\prod_{\lambda\in S}\left\{e\left(\frac{\lambda}{\omega}\right)+\rho e\left(\frac{\rho\lambda}{\omega}\right)+\rho^2 e\left(\frac{\rho^2\lambda}{\omega}\right)\right\}.$$

ここで，$\alpha(S)$ は，-1 の 3 乗根で，

$$\alpha(S)\equiv\prod_{\lambda\in S}\lambda \qquad (\mathrm{mod}\ \omega)$$

なる条件で定まるものとする（$\alpha(S)$ の存在は，Wilson の定理の帰結である）．$\delta_3(\omega)$ が，S のとり方に依らないことは容易にわかる．次の定理が，この小論の主結果で，Loxton [L] により予想されたものである．

<u>定理 1</u> $\quad \arg\left\{\left(\frac{3}{\omega}\right)_3^{-1}\tau_3(\omega)\,\delta_3(\omega)\right\}\longrightarrow 0 \quad (p\to\infty).$

なお，Loxton [L2] により，任意の $\varepsilon>0$ について，

$$\arg\left\{-\omega\,\delta_3(\omega)^3\right\}=O(p^{-\frac{1}{2}+\varepsilon}) \qquad (p\to\infty)$$

となることが示されているので，上の定理から

$$\arg\left\{\left(\frac{3}{\omega}\right)_3^{-1}\tau_3(\omega)\,\delta_3(\omega)\right\}=O(p^{-\frac{1}{2}+\varepsilon}) \quad (p\to\infty)$$

が従う．

<u>2.</u> 背景および関連する諸結果．(Related results)．

奇素数 p に対して 2 次の Gauss 和

$$\tau_2(p)=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta^a \qquad (\zeta\neq 1,\ \zeta^p=1)$$

を考える（$\left(\frac{a}{p}\right)$ は $\mathbb{Q}$ の平方剰余記号）と，よく知られているように，

$$(2.1) \qquad \tau_2(p) = \prod_{\substack{a=1 \\ a\equiv 1 \ (\mathrm{mod}\ 2)}}^{p-1} (\zeta^{a} - \zeta^{-a})$$

が成り立ち，このことと $\tau_2(p)^2 = \left(\frac{-1}{p}\right)p$ から，ζ として特に $e^{2\pi i/p}$ をとれば，

$$\tau_2(p) = \begin{cases} \sqrt{p}, & p \equiv 1 \pmod 4, \\ i\sqrt{p}, & p \equiv 3 \pmod 4 \end{cases}$$

となることが導けることも周知の通りである．

1970年代に，Cassels の周辺の数学者たちにより，(2.1) の類似を3次の Gauss 和に関して求めるという方向の研究がなされている．その動機は，さしあたり3次の Gauss 和 $\tau_3(\omega)$ の偏角の分布に関する Kummer の問題であると言ってよかろうと思う．(2.1) の右辺の類似として考えられたものは，大別して2通りあり，そのひとつが，すでに記した積 (1.1) である．もうひとつは，楕円関数の等分値を用いるもので，例えば次のような積である（記号は 1 と同じとし，さらに $\wp$ を $\wp'^2 = 4\wp^3 - 1$ をみたす Weierstraß の関数，θ を $\mathbb{Z}[\rho]\theta$ が $\wp$ の周期格子となるような正の実数とする）：

$$(2.2) \qquad \alpha(S)^{-1} p^{1/3}\omega \cdot \prod_{\lambda \in S} \wp\left(\frac{\lambda\theta}{\omega}\right).$$

$\tau_3(\omega)^3 = -p\omega$ と

$$(2.3) \qquad \prod_{a=1}^{p-1} \wp\left(\frac{a\theta}{\omega}\right) = \omega^{-2}$$

から，$\tau_3(\omega)$ と積 (2.2) は，1の3乗根を除いて等しいこ

とがすぐにわかる. 実は両者が完全に等しいことがすでに証明されている. すなわち,

<u>定理2</u> (Mathews [M]) $\tau_3(\omega) = \alpha(S)^{-1} p^{1/3} \omega \prod_{\lambda \in S} \wp\left(\frac{\lambda\theta}{\omega}\right)$.

この定理の証明は, 簡単とは言い難いが, 有限体 $\mathbb{F}_p$ 上で考えられた楕円曲線 $y^2 = 4x^3 - 1$ の p 分点の性質を用いた大変興味深いものである. 現在の所,

定理1と定理2が, 2次のGauss和に関する古典的な等式(2.1)の3次のGauss和への拡張と見なすことのできる結果のすべてであると言ってよかろうと思われる. さらに, 今の所, 定理1は定理2を経由してでなければ証明できない(<u>3</u>参照)ので, 本質的なのは定理2だけであるかも知れない. また, 前述のように, 2つの定理とも, 元々Kummerの問題を動機として予想された後証明されたものであるから, "この問題が一応の解決を見た(Heath-Brown and Patterson [HP])現在, 定理1, 2のような結果にどれほどの意味があるのか?"という疑問も当然ながら湧いてくる. これらのことも念頭に置いたいくつかのremarkと問題提起は<u>4</u>でまとめて述べることにし, この小節では, 4次と6次の場合についてのみ, 簡単に触れておく.

4次，6次のGauss和について，定理1，2に相当する結果が成立するであろうと期待するのは，極めて自然であり，6次の場合への定理1の拡張を除いて既に証明されているし（Matthews [M2]参照），残っている場合も肯定的に解決されるだろうことは，まず間違いない．ところで，実は，4次のGauss和について定理1に相当するものは，[M2] により，我々の定理1よりも早く証明されてしまっている．この辺の事情を概説して，この小節を閉じる．ϖ を $\mathbb{Z}[i]$ の1次の素 ideal の生成元で，$\varpi \equiv 1 \pmod{(1+i)^3}$ なるものとし，

$$\varpi = a + bi \quad , \quad p = \varpi\bar{\varpi} \qquad (a, b \in \mathbb{Z})$$

とおくと，4次のGauss和

$$\tau_4(\varpi) = \sum_{r=1}^{p-1} \left(\frac{r}{\varpi}\right)_4 e^{2\pi i r/p}$$

について，定理2に相当する積公式が成り立つ．いまの場合，この積公式は，さらに Dedekind の η-関数を用いた表示に変形することができ，η-関数の変換公式から，

$$(2.4) \qquad \tau_4(\varpi) = -\beta(\varpi)\left(\frac{2i}{\varpi}\right)_4 p^{1/4}\left(\frac{2|b|}{a}\right)_2 \sqrt{(-1)^{(p-1)/4}\cdot\bar{\varpi}}$$

が導ける．但し，右辺の最後の $\sqrt{\ }$ は実部が正になるようにとり，また，$\left(\frac{\cdot}{\cdot}\right)_4$ は $\mathbb{Q}(i)$ の4乗剰余記号，$\left(\frac{\cdot}{\cdot}\right)_2$ は $\mathbb{Q}$ の平方剰余記号である．さらに，$\beta(\varpi)$ は，-1 の平方根であり，$\beta(\varpi) \equiv \frac{p-1}{2}! \pmod{\varpi}$ により定まるものである．

(以上, [M2]). 一方で, Loxton [L] は, 今の状況で (1.1) に相当するもの $\delta_K(\varpi)$ を定義し, 定理1に相当するものを予想として提出している. 彼は, 同じ論文で, さらに, この予想が, (2.4) と同値であることを, 巧みな方法で証明している. したがって, [M2] により, (2.4) と4次の場合に定理1に相当するものとが同時に証明された. 以上は4次の場合であるが, 3次の場合には, (2.4) に相当する公式を得るのは, 少し無理があるようである. これが, 大雑把ではあるが, 定理1の型の結果が, 4次の場合について, 3次の場合についてよりも先に証明された事情である.

3. 定理1の証明について (Proof of the main result).

定理1は, 定理2から次のようにして導かれる. 詳しくは [I] を参照していただくことにして, ここでは概略を記すに止める. まず, $\mathbb{C}$ 上の2つの関数 $f(z)$, $g(z)$ を次で定義する:

$$f(z)=\frac{\sigma((z-\frac{1}{3})\theta)\,\sigma((z-\frac{\rho}{3})\theta)\,\sigma((z-\frac{\rho^2}{3})\theta)}{\sigma(z\theta)\,\sigma((z-\frac{1}{\sqrt{3}i})\theta)\,\sigma((z+\frac{1}{\sqrt{3}i})\theta)},$$

$$g(z)=e(z)+\rho e(\rho z)+\rho^2 e(\rho^2 z).$$

但し, 記号は, 1 で定義したものと同じで, $\sigma(z)$ は $\mathbb{Z}[\rho]\theta$ に関する Weierstraß の関数である. $f(z)$, $g(z)$ は次の性質をもつ:

$$(3.1)\qquad f(z+\gamma)=f(z),\quad g(z+\gamma)=g(z),\quad \gamma\in\mathbb{Z}[\rho],$$

$$(3.2)\qquad f(\rho z)=\rho^{-1}f(z),\quad g(\rho z)=\rho^{-1}g(z),$$

$$(3.3)\qquad f(\bar{z})=\overline{f(z)},\quad g(\bar{z})=\overline{g(z)}.$$

まず，定理2の変形として，

$$\tau_3(\omega)=B\left(\frac{3}{\omega}\right)_3\alpha(S)^{-1}\prod_{\lambda\in S}f\left(\frac{\lambda}{\omega}\right)^{-1}$$

が得られる．ここで，Bは正の実数でpに依存して決まるが，定理1で問題にしているのは，$\tau_3(\omega)$の偏角であるから，重要なものではない．次に，$\delta_3(\omega)$と$g(z)$の定義から，

$$\delta_3(\omega)=\alpha(S)\prod_{\lambda\in S}g\left(\frac{\lambda}{\omega}\right).$$

よって，定理1は，次の定理1'に帰着する．

<u>定理1'</u> $\arg\left\{\prod_{\lambda\in S}g\left(\frac{\lambda}{\omega}\right)f\left(\frac{\lambda}{\omega}\right)^{-1}\right\}\longrightarrow 0\quad(p\to\infty).$

これを示すため，$M=\{z\in\mathbb{C}\,;\,g(z)=0$ または $f(z)=0,\infty\}$ とおき，

$$h(z)=\frac{g(z)\,|f(z)|}{|g(z)|\,f(z)},\quad z\notin M$$

とおく．容易に，

$$\begin{aligned}M&=\left\{z\in\mathbb{C}\,;\,z\equiv 0,\pm\frac{1}{\sqrt{3}i},\frac{1}{3},\frac{\rho}{3},\frac{\rho^2}{3}\pmod{\mathbb{Z}[\rho]}\right\}\\&=\{z\in\mathbb{C}\,;\,g(z)=0\}\\&=\{z\in\mathbb{C}\,;\,f(z)=0,\infty\}\end{aligned}$$
（少し荒い表現をすれば）

がわかる．さらに，若干の考察（主に$g(z)$に関する）から，$g(z)/|g(z)|$ と $f(z)/|f(z)|$ は，ともにMの各点の回りで，我

我の目的のためには error term と見なせる項を除いて一致することがわかる（例えば，0の回りでは，両者は $\bar{z}/|z|$ で十分良く近似される）．このことから，$h(z)$ は $\mathbb{C}$ 全体に連続に拡張されること，および $h(0)=1$ がわかる．また，(3.1)〜(3.3)により，

$$h(z+\lambda)=h(z),\qquad \lambda\in\mathbb{Z}[\rho],$$
$$h(\rho z)=h(z),\qquad h(\bar{z})=\overline{h(z)}$$

となる．そこで，$\mathbb{C}$ が単連結であることに基づいて，

$$t(z)=\arg h(z)=\mathrm{Im}(\log h(z)),\qquad t(0)=0$$

により $\mathbb{C}$ 上の連続関数 $t(z)$ を定めると，明らかに，

(3.4) $$t(\bar{z})=-t(z).$$

さらに $t(\rho z)-t(z)\in 2\pi\mathbb{Z}$ ゆえこの関数は $\mathbb{C}$ 上定数でなければならず，$z=0$ を考えることにより結局

(3.5) $$t(\rho z)=t(z)$$

がわかる．[注1] よって，

$$\sum_{\lambda\in S} t\left(\frac{\lambda}{\omega}\right)=\frac{1}{3}\sum_{a=1}^{p-1} t\left(\frac{a}{\omega}\right)=\frac{1}{3}\sum_{a=1}^{p} t\left(\frac{a}{\omega}\right).$$

以上により，定理1′を示すためには，次を示せば十分であることがわかる．

<u>定理1″</u> $$\sum_{a=1}^{p} t\left(\frac{a}{\omega}\right)\longrightarrow 0\qquad (p\to\infty).$$

ところで,

$$\frac{1}{p}\sum_{a=1}^{p} t\left(\frac{a}{\omega}\right) = \frac{1}{p}\sum_{a \bmod \omega} t\left(\frac{a}{\omega}\right)$$

は, $p \to \infty$ のとき, 積分

$$\int_{\mathbb{C}/\mathbb{Z}[\rho]} t(z)\, dx\, dy$$

に収束する. さらに, (3.4) よりこの積分は0に等しい. そこで, この収束の状態を少し詳しく調べると, 任意の $\varepsilon > 0$ について,

$$\frac{1}{p}\sum_{a=1}^{p} t\left(\frac{a}{\omega}\right) = O\left(p^{-5/4+\varepsilon}\right)$$

となることがわかり, 定理1″が示される.

4. 若干の注意と問題 (Some remarks and problems).

1° (注意). 計算機による実験により, Matthews の結果 (定理2) は, ω が $\mathbb{Z}[\rho]$ の素数でないときについても, $\alpha(S)$ の定義を少し工夫すれば同様な形で成立するであろうことが, 最近わかった. 現段階ではまだ予想であるが, 証明はそれほど難かしくないと思われる.

2° (注意). 定理2の5次の Gauss 和についての類似があれば, 大変興味深い. そのためには, まず (2.3) の類似物が必要である. Grant [G] が, この問題に関連した結果を出しているが, 彼の結果がどの程度ここでの問題に役立つかどうか, 今の所不明である.

3° (問題). 定理1を用いて, 3次の Gauss 和 $\tau_3(\omega)$ の偏角の一様

分布を証明できないか？

4°(問題). 定理1を直接に(定理2を経由しないで)証明できないか？(これは，次の問題を考える上でのヒントを与えるかもしれない．Reshetukha [R] の扱い方が参考になる可能性がある)．

5°(問題). 定理1を何らかの形で5次(以上)のGauss和について拡張できないか？また，できるとすれば，その拡張を用いてGauss和の偏角の一様分布を示すことはできないか？

以上，箇条書きにして述べたが，筆者の問題意識は，一言で言えば，"Gauss和と(1.1)のような積の間の関係は，どの程度普遍性をもつものであるのか，またそれがあるとすればどのような事情によるのか？"ということである．

注1) (p.8) とくに((3.5)より)，$t(\rho)=t(\rho^2)=t(1)$．また，(3.4)から $t(\rho)=-t(\rho^2)$ ゆえ，$t(\rho)=t(1)=0$ となる．これから，(3.5)を示したのと同じ論法により，$t(z)$ が，周期 $\mathbb{Z}[\rho]$ をもつことがわかる．

文献:

[G] D. Grant, A generalization of a formula of Eisenstein, Proc. London Math. Soc. (3) 62 (1991).

[HP] D. R. Heath-Brown and S. J. Patterson, The distribution of Kummer sums at prime arguments, Crelle J. 310 (1979).

[I] H. Ito, On a product related to the cubic Gauss sum, Crelle J. 395 (1989).

[L] J. H. Loxton, Some conjectures concerning Gauss sums, Crelle J. 297 (1978).

[L 2] ________, Products related to Gauss sums, Crelle J. 268/269 (1974).

[M] C. R. Matthews, Gauss sums and elliptic functions I, Invent. Math. 52 (1979).

[M 2] ________, Gauss sums and elliptic functions II, Invent. Math. 54 (1979).

[R] I. V. Reshetukha, A product related to the cubic Gauss sum, Ukrain. Mat. Zh. 37 (1985) (ロシア語, 英訳あり).