

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 [II]). $p = e^{2\pi i/3}$ とし, ω を $\mathbb{Q}(p)$ の素 ideal で 1 次かつ 3 と素なものとする. さらに, $\omega \equiv 1 \pmod{3}$ と取られている の生成元 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 $T_3(\omega)$ を

$$T_3(\omega) = \sum_{a=1}^{p-1} \left(\frac{a}{\omega} \right)_3 e^{2\pi i a/p}$$

で定義する. 但し $\left(\frac{a}{\omega} \right)_3$ は, $\mathbb{Q}(p)$ 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, $\text{mod } \omega$ の $\frac{1}{3}$ -代表系 S をひとつとる. (「 $\text{mod } \omega$ の $\frac{1}{3}$ -代表系」とは, $\mathbb{Z}[p]$ の $(p-1)/3$ 個の元からなる部分集合 S で, $\lambda, p\lambda, p^2\lambda$ ($\lambda \in S$) の全体が, $\mathbb{Z}[p]/\omega\mathbb{Z}[p]$ 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

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

とあって, 次の積 $\delta_3(\omega)$ を考える:

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

ここで, $\alpha(S)$ は, -1 の 3 乗根で,

$$\alpha(S) \equiv \prod_{\lambda \in S} \lambda \pmod{\omega}$$

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.

定理 1 $\arg \left\{ \left(\frac{3}{\omega}\right)_3^{-1} \tau_3(\omega) \delta_3(\omega) \right\} \rightarrow 0 \quad (p \rightarrow \infty).$

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

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

となることが示されているので, 上の定理から

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

が従う.

2. 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

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

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,

$$(2.1) \quad \tau_2(p) = \prod_{\substack{a=1 \\ a \equiv 1 \pmod{2}}}^{p-1} (\zeta^a - \zeta^{-a})$$

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おくと思う. (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 $\underline{1}$ と同じとし, さらに ρ を $\rho^2 = 4\rho^3 - 1$ をみたす Weierstrass の関数, θ を $\mathbb{Z}[\rho]\theta$ が ρ の周期格子となるような正の実数とする):

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

$$(2.3) \quad \tau_3(\omega)^3 = -p\omega \text{ と } \prod_{a=1}^{p-1} \rho\left(\frac{a\theta}{\omega}\right) = \omega^{-2}$$

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、

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

この定理の証明は、簡単とは言えないが、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、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 (三参照) ので、本質的なものは定理 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。これらのことを^も念頭に置いたいくつかの remark は 4 で と問題提起 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、簡単に解れておく。

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 (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. ω を $\mathbb{Z}[i]$ の 1 次素 ideal の生成元で, $\omega \equiv 1 \pmod{(1+i)^3}$ なるものとし,

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

とあくと, 4次の Gauss 和

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

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,

$$(2.4) \quad \tau_*(\omega) = -\beta(\omega) \left(\frac{2i}{\omega}\right)_4 p^{1/4} \left(\frac{2|b|}{a}\right)_2 \sqrt{(-1)^{(p-1)/4} \omega}$$

が導ける. 但し, 右辺の最後の $\sqrt{\quad}$ は実部が正になるようにとり, また, $(\frac{\cdot}{\cdot})_4$ は $\mathbb{Q}(i)$ の 4 乗剰余記号, $(\frac{\cdot}{\cdot})_2$ は $\mathbb{Q}$ の平方剰余記号である. さらに, $\beta(\omega)$ は, -1 の平方根であり, $\beta(\omega) \equiv \frac{p-1}{2}! \pmod{\omega}$ 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 $\delta_x(\omega)$ 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(把)難ではあるが, 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, $\frac{1}{\theta}$ 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:

$$(3.1) \quad f(z+r) = f(z), \quad g(z+r) = g(z), \quad r \in \mathbb{Z}[p],$$

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

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

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で問題になっているのは, $\tau_3(\omega)$ 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.

定理1' $\arg \left\{ \prod_{\lambda \in S} g\left(\frac{\lambda}{\omega}\right) f\left(\frac{\lambda}{\omega}\right)^{-1} \right\} \rightarrow 0 \quad (p \rightarrow \infty).$

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

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

とおく. 容易に,

$$M = \{z \in \mathbb{C}; z \equiv 0, \pm \frac{1}{\sqrt{3}i}, \frac{1}{3}, \frac{p}{3}, \frac{p^2}{3} \pmod{\mathbb{Z}[p]}\}$$

$$= \{z \in \mathbb{C}; g(z) = 0\}$$

$$= \{z \in \mathbb{C}; f(z) = 0, \infty\} \quad \text{少し荒い表現をすれば}$$

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, とともに M の各点の回りで, 我

目的の

我々のためには 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,

$$h(z+\lambda) = h(z), \quad \lambda \in \mathbb{Z}[p],$$

$$h(pz) = h(z), \quad h(\bar{z}) = \overline{h(z)}$$

となる. そこで, $\mathbb{C}$ が単連結であることに基いて,

連続 $t(z) = \arg h(z) = \operatorname{Im}(\log h(z)), \quad t(0)=0$

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

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

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

$$(3.5) \quad t(pz) = t(z)$$

がわかる. ^{注1)} よって,

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

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.

定理 1'' $\sum_{a=1}^p t\left(\frac{a}{\omega}\right) \rightarrow 0 \quad (p \rightarrow \infty).$

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, $p \rightarrow \infty$ のとき, 積分

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

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

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

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 $\mathbb{Z}[p]$ 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 $T_3(\omega)$ 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) のような種々の間々関係は, 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る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, $t(p) = t(p^2) = t(1)$. また, (3.4) から $t(p) = -t(p^2)$ ゆえ, $t(p) = t(1) = 0$ となる. これから, (3.5) を示したのと同じ論法により, $t(2)$ が, 周期 $\mathbb{Z}[p]$ 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 (1999).

[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).

[L2] _____, Products related to Gauss sums, Crelle J. 268/269 (1974).

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

[M2] _____, 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).