OHP 原稿

ささやかな数学体験
正七角形調和から楕円ガウス和へ

T. Asai / Oct. 23, 2008 / Nara WU

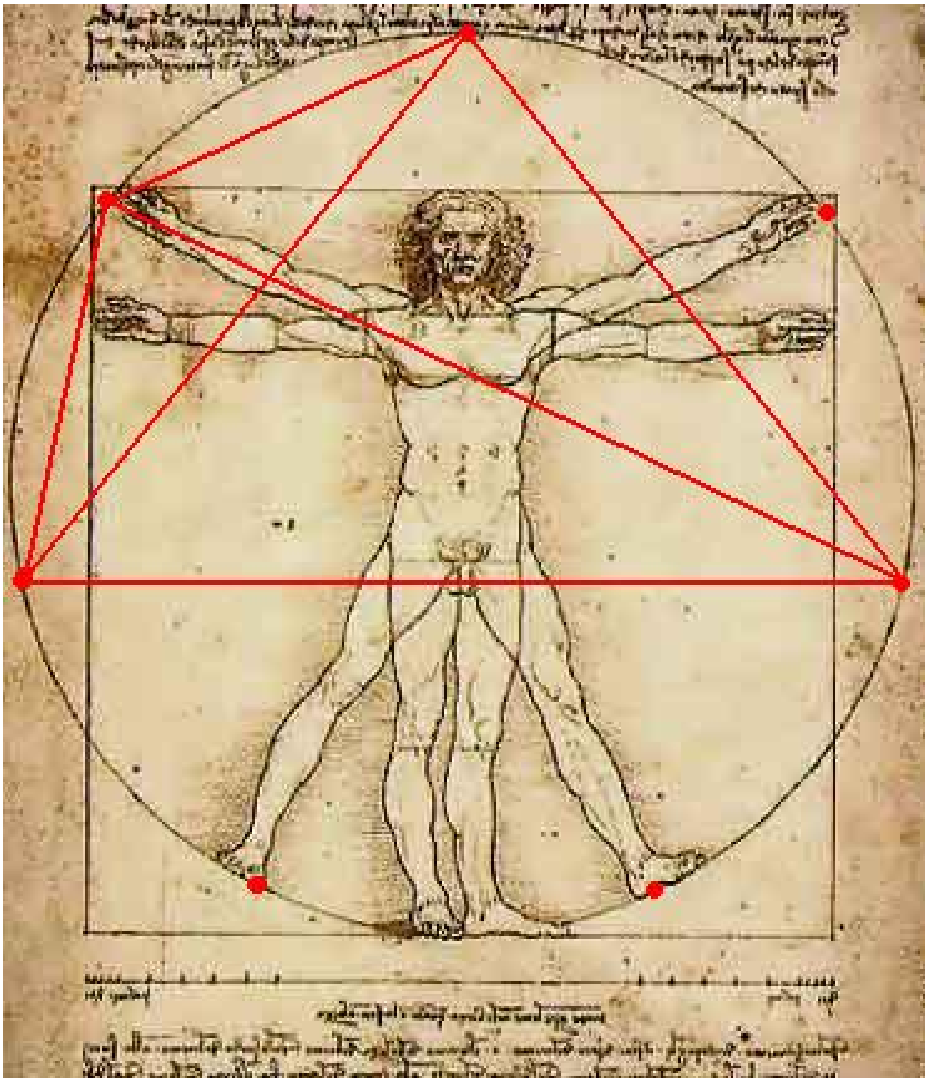
正七角形調和

正 7 角形の対角線の長さ (辺の長さも含める) を

$a_1 < a_2 < a_3$ **とするとき，**

$$\frac{1}{a_1} = \frac{1}{a_2} + \frac{1}{a_3}$$

$$a_2 \cdot a_3 = a_1 \cdot a_2 + a_1 \cdot a_3 \qquad (\,\text{Ptolemaios}\,)$$



類似の現象は？　実験！

A FACT

正 23 角形の対角線の長さ (辺の長さも含める) を
$a_1 < a_2 < a_3 < \cdots < a_{10} < a_{11}$ とするとき，

$$\frac{1}{a_1}+\frac{1}{a_3}+\frac{1}{a_9}+\frac{1}{a_{10}}=\frac{1}{a_2}+\frac{1}{a_4}+\frac{1}{a_5}+\frac{1}{a_6}+\frac{1}{a_7}+\frac{1}{a_8}+\frac{1}{a_{11}}$$

$$a_k=\sin\frac{\pi k}{p}=\begin{cases} a'_{k/2} & (k:\mathrm{even}) \\ a'_{(p-k)/2} & (k:\mathrm{odd}) \end{cases}$$

$$a'_k=\sin\frac{2\pi k}{p}\quad (1\le k\le (p-1)/2,\quad p=7,\ 23)$$

$$\frac{1}{a'_1}+\frac{1}{a'_2}-\frac{1}{a'_3}=0\qquad (\leftarrow\quad p=7,\qquad \downarrow\quad p=23)$$

$$\frac{1}{a'_1}+\frac{1}{a'_2}+\frac{1}{a'_3}+\frac{1}{a'_4}-\frac{1}{a'_5}+\frac{1}{a'_6}-\frac{1}{a'_7}+\frac{1}{a'_8}+\frac{1}{a'_9}-\frac{1}{a'_{10}}-\frac{1}{a'_{11}}=0$$

符号の規則性は？
$p=7,\ 23,\ \cdots$ の理由は？

$$1^2\equiv 1\ (\mathrm{mod}\ 7),\ 2^2\equiv 4\equiv -3\ (\mathrm{mod}\ 7),\ 3^2\equiv 2\ (\mathrm{mod}\ 7)$$

平方剰余記号

$p > 2$, 素数

p 元体 $\mathrm{Z}/p\mathrm{Z}$ の乗法群 $(\mathrm{Z}/p\mathrm{Z})^{\times}$ は位数 $p-1$

$\therefore \quad a^{p-1} \equiv 1 \pmod{p} \quad \therefore \quad a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

そこで，符号 $\left(\dfrac{a}{p}\right) = \pm 1$ を

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

で定める．半分が $+1$, 半分が -1 である．また，

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \quad \left(\frac{c^2}{p}\right) = \left(\frac{c}{p}\right)^2 = 1$$

したがって，平方剰余記号の名の示す通り：

$$\left(\frac{a}{p}\right) = 1 \iff a \equiv c^2 \pmod{p}\ (\exists c)$$

相互法則は表に出ない．次の性質（補充法則）を使う．

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \cdots \quad p \equiv 1 \pmod{4} \\ -1 & \cdots \quad p \equiv 3 \pmod{4} \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \cdots \quad p \equiv 1,\ 7 \pmod{8} \\ -1 & \cdots \quad p \equiv 3,\ 5 \pmod{8} \end{cases}$$

また，便宜上，次のように約束する．

$$a \equiv 0 \pmod{p} \text{ のときは } \left(\frac{a}{p}\right) = 0$$

$p = 7,\ 23$ に戻る．観察された現象は

$$\sum_{k=1}^{(p-1)/2} \left(\frac{k}{p}\right) a'_k = \sum_{k-1}^{(p-1)/2} \left(\frac{k}{p}\right) \csc \frac{2\pi k}{p} = 0$$

A FORMULATION

$p \equiv 7 \pmod 8$ なる素数 p について，

$$\sum_{k \,(\mathrm{mod}\, p)} \left(\frac{k}{p}\right) \csc \frac{2\pi k}{p} = 0$$

<u>一つの証明.</u> $\csc 2\theta = \dfrac{1}{\sin 2\theta} = \cot\theta - \cot 2\theta,$

$$\therefore \quad \boxed{\sum_{k \,(\mathrm{mod}\, p)} \left(\frac{k}{p}\right) \csc \frac{2\pi k}{p}}$$

$$= \sum_{k \,(\mathrm{mod}\, p)} \left(\frac{k}{p}\right) \cot \frac{\pi k}{p} - \left(\frac{2}{p}\right) \sum_{k \,(\mathrm{mod}\, p)} \left(\frac{2k}{p}\right) \cot \frac{\pi 2k}{p}$$

$$= \left\{1 - \left(\frac{2}{p}\right)\right\} \cdot \boxed{\sum_{k \,(\mathrm{mod}\, p)} \left(\frac{k}{p}\right) \cot \frac{\pi k}{p}} = 0\,.$$

$$\because \quad p \equiv 7 \pmod 8 \iff \left(\frac{-1}{p}\right) = -1,\ \left(\frac{2}{p}\right) = 1\,.$$

“類ガウス和”へと導かれた

ガウス和 (Gauss, May 1801 – Aug 1805)

$$\sum_{k \pmod p} \left(\frac{k}{p}\right) \sin\frac{2\pi k}{p} = \sqrt{p} \quad \cdots \quad p \equiv 3 \pmod 4,$$

$$\sum_{k \pmod p} \left(\frac{k}{p}\right) \cos\frac{2\pi k}{p} = \sqrt{p} \quad \cdots \quad p \equiv 1 \pmod 4$$

すなわち

$$\sum_{k \pmod p} \left(\frac{k}{p}\right) e^{2\pi i k/p} = \begin{cases} \sqrt{-p} & \cdots \quad p \equiv 3 \pmod 4 \\ \sqrt{p} & \cdots \quad p \equiv 1 \pmod 4 \end{cases}$$

類ガウス和

$$\sum_{k \pmod p} \left(\frac{k}{p}\right) \cot\frac{\pi k}{p} = \boxed{?} \quad \cdots \quad p \equiv 3 \pmod 4,$$

$$\sum_{k \pmod p} \left(\frac{k}{p}\right) \tan\frac{\pi k}{p} = \boxed{?} \quad \cdots \quad p \equiv 3 \pmod 4,$$

$$\sum_{k \pmod p} \left(\frac{k}{p}\right) \csc\frac{2\pi k}{p} = 0 \quad \cdots \quad p \equiv 7 \pmod 8,$$

$$\sum_{k \pmod p} \left(\frac{k}{p}\right) \csc\frac{2\pi k}{p} = \boxed{?} \quad \cdots \quad p \equiv 3 \pmod 8,$$

$$\sum_{k \pmod p} \left(\frac{k}{p}\right) \sec\frac{2\pi k}{p} = \boxed{?} \quad \cdots \quad p \equiv 1 \pmod 4$$

類ガウス和の計算はガウス和と$\boxed{\text{係数}}$に帰着する！

例. $\tan\dfrac{\pi k}{p} = -2\displaystyle\sum_{l=1}^{(p-1)/2}\sin\dfrac{4\pi kl}{p}$ (“**フーリエ展開**”)

$$\therefore \quad \sum_{k\,(\mathrm{mod}\,p)}\left(\frac{k}{p}\right)\tan\frac{\pi k}{p}$$

$$= -2\sum_{l=1}^{(p-1)/2}\sum_{k\,(\mathrm{mod}\,p)}\left(\frac{k}{p}\right)\sin\frac{4\pi kl}{p}$$

$$= \boxed{-2\left(\frac{2}{p}\right)\sum_{l=1}^{(p-1)/2}\left(\frac{l}{p}\right)}\cdot\sqrt{p} \quad (\text{類ガウス和の}\boxed{\text{係数}})$$

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

$$\tan\theta = \cot\theta - 2\cot 2\theta, \quad \csc 2\theta = \cot\theta - \cot 2\theta,$$

$$\therefore \quad \sum_{k\,(\mathrm{mod}\,p)}\left(\frac{k}{p}\right)\tan\frac{\pi k}{p}$$

$$= \left\{1 - 2\left(\frac{2}{p}\right)\right\}\cdot\sum_{k\,(\mathrm{mod}\,p)}\left(\frac{k}{p}\right)\cot\frac{\pi k}{p}$$

cf.

$$\sum_{k\,(\mathrm{mod}\,p)}\left(\frac{k}{p}\right)\csc\frac{2\pi k}{p}$$

$$= \left\{1 - \left(\frac{2}{p}\right)\right\}\cdot\sum_{k\,(\mathrm{mod}\,p)}\left(\frac{k}{p}\right)\cot\frac{\pi k}{p}$$

現象の観察（類ガウス和の係数）

$$\frac{1}{2}\sum_{k \pmod p}\left(\frac{k}{p}\right)\cot\frac{\pi k}{p} = A_p \cdot \sqrt{p}$$
$$\frac{1}{2}\sum_{k \pmod p}\left(\frac{k}{p}\right)\sec\frac{2\pi k}{p} = B_p \cdot \sqrt{p}$$

p	A_p	p	B_p
3	1/3	5	2
7	1	13	2
11	1	17	4
19	1	29	6
23	3	37	2
31	3	41	8
43	1	53	6
47	5	61	6
59	3	73	4
67	1	89	12
71	7	97	4

虚２次体の類数である！

どうしてそんなことに？

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \sum_{\substack{n=-\infty \\ n\equiv 1 \pmod 4}}^{\infty} \frac{1}{n}$$

$$\boxed{\frac{\pi}{p}\cot\frac{\pi k}{p} = \sum_{\substack{n=-\infty \\ n\equiv k \pmod p}}^{\infty} \frac{1}{n}}$$

$$\because \quad \pi\cot\pi x = \left[\sum_{n=-\infty}^{\infty}\frac{1}{x+n}\right] = \lim_{N\to\infty}\sum_{n=-N}^{n=N}\frac{1}{x+n}.$$

$$\therefore \quad \sum_{k \pmod p}\left(\frac{k}{p}\right)\cot\frac{\pi k}{p} = \frac{p}{\pi}\sum_{k \pmod p}\left(\frac{k}{p}\right)\sum_{\substack{n=-\infty \\ n\equiv k \pmod p}}^{\infty}\frac{1}{n}$$

$$= \frac{p}{\pi}\sum_{n=-\infty}^{\infty}\left(\frac{n}{p}\right)\frac{1}{n} = \frac{2p}{\pi}\sum_{n=1}^{\infty}\frac{\chi_p(n)}{n}, \quad \chi_p(n) = \left(\frac{n}{p}\right).$$

$$L(s,\,\chi_p) \doteq \sum_{n=1}^{\infty}\frac{\chi_p(n)}{n^s}, \qquad (\mathrm{Re}\, s > 1)$$

$L(1,\,\chi_p)$ と結びついた

$p \equiv 3 \pmod 4$ **のとき，**

$$\frac{1}{2}\sum_{k \pmod p}\left(\frac{k}{p}\right)\cot\frac{\pi k}{p} = \frac{p}{\pi}L(1,\,\chi_p)$$

類ガウス和の$\boxed{\text{係数}}$による類数公式

$$h(-p) \doteqdot \text{“虚2次体 } \mathbb{Q}(\sqrt{-p}) \text{ の類数”}$$

$$\boxed{\begin{aligned} h(-p) &= A_p \quad (p \equiv 3 \pmod 4, \quad p > 3) \\ h(-p) &= B_p \quad (p \equiv 1 \pmod 4) \end{aligned}}$$

$$\because \quad L(1,\, \chi_p) = \frac{\pi\, h(-p)}{\sqrt{p}}, \quad (\, p \equiv 3 \pmod p\,)\,)$$

(Dirichlet (1839?))

$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$

参考 Cor.（類数公式） ($d > 3$, d : square-free)

D		$h(-D)$
d	$d \equiv 7 \pmod 8$	$\displaystyle\sum_{k=1}^{\frac{d-3}{4}} \left(\frac{k}{d}\right)$
d	$d \equiv 3 \pmod 8$	$\displaystyle\frac{1}{3} \sum_{k=\frac{d+1}{4}}^{\frac{d-1}{2}} \left(\frac{k}{d}\right)$
$8d$	$d \equiv 3 \pmod 4$	$\displaystyle 2 \sum_{k=\left[\frac{d}{8}\right]+1}^{\left[\frac{3d}{8}\right]} \left(\frac{k}{d}\right)$
$4d$	$d \equiv 1 \pmod 4$	$\displaystyle 2\sum_{k=1}^{\frac{d-1}{4}} \left(\frac{k}{d}\right)$
$8d$	$d \equiv 1 \pmod 4$	$\displaystyle 2\sum_{k=1}^{\left[\frac{d}{8}\right]} \left(\frac{k}{d}\right) - 2 \sum_{k=\left[\frac{3d}{8}\right]+1}^{\frac{d-1}{2}} \left(\frac{k}{d}\right)$

感動！正七角形調和 $\longrightarrow$ 類ガウス和
$\longrightarrow$ $\boxed{\text{係数}}$公式 $\longrightarrow$ L 関数 $\longrightarrow$ $\boxed{\text{係数}=\text{類数}}$

ここまでのまとめ

$$\sum_{k \pmod p} \left(\frac{k}{p}\right) \cot \frac{\pi k}{p} \ \text{はおもしろい！}$$

$p \equiv 3 \pmod p, \ p > 3$

$$(1) \quad \frac{1}{2} \sum_{k \pmod p} \left(\frac{k}{p}\right) \cot \frac{\pi k}{p} = A_p \cdot \sqrt{p}, \quad A_p \in \mathrm{Z}$$

$$(2) \quad \left\{ 2 - \left(\frac{2}{p}\right) \right\} A_p = \sum_{l=1}^{(p-1)/2} \left(\frac{l}{p}\right) \quad \text{(係数公式)}$$

$$(3) \quad \frac{1}{2} \sum_{k \pmod p} \left(\frac{k}{p}\right) \cot \frac{\pi k}{p} = \frac{p}{\pi} L(1, \chi_p)$$

$$(4) \quad A_p = h(-p) \quad \text{(類数公式)}$$

It's a Prototype！

第一部　おわり

楕円ガウス和

$$\mathcal{G}_\lambda \doteq \frac{1}{4} \sum_{\nu \,(\mathrm{mod}\,\lambda)} \left(\frac{\nu}{\lambda}\right)_4 \mathrm{sl}\left(\frac{(1-i)\varpi\nu}{\lambda}\right)$$

類ガウス和 の 楕円アナローグ？

(三角関数から楕円関数へ！)

$$\mathbb{Z} \longrightarrow \mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$$

$$\left(\frac{k}{p}\right) \longrightarrow \left(\frac{\nu}{\lambda}\right)_4$$

$$\cot \pi x \longrightarrow \mathrm{sl}((1-i)\varpi u)$$

- **計算実験と観察のたのしみ**

$\longrightarrow$ **プログラミングのたのしみ！**

$\longrightarrow$ **実験計算は「解析」である！**

$\longrightarrow$ **実験データが燃料になる !?**

道具立て (1) $\boxed{\left(\dfrac{a}{p}\right) \longrightarrow \left(\dfrac{\alpha}{\lambda}\right)_4}$

$\mathcal{O} \doteq \mathrm{Z}[i] = \mathrm{Z}[\sqrt{-1}]$

p ： **素数**, $p \equiv 1 \pmod 4$

$p = \lambda\overline{\lambda} = a^2 + b^2, \quad \lambda = a + bi$ ： **ガウス素数**

4 べき (冪) 剰余記号

p **元体** $\mathcal{O}/(\lambda)$ **の乗法群** $(\mathcal{O}/(\lambda))^\times$ **は位数** $p-1$

$$\therefore \quad \alpha^{p-1} \equiv 1 \pmod \lambda, \quad \alpha^{\frac{p-1}{4}} \equiv \pm 1, \pm i \pmod \lambda$$

$$\left(\frac{\alpha}{\lambda}\right)_4 = \pm 1, \ \pm i \ : \quad \left(\frac{\alpha}{\lambda}\right)_4 \equiv \alpha^{\frac{p-1}{4}} \pmod \lambda$$

$$\left(\frac{\alpha}{\lambda}\right)_4 = 1 \iff \alpha \equiv \gamma^4 \pmod \lambda \ (\exists \gamma)$$

$$\left(\frac{i}{\lambda}\right)_4 = i^{(p-1)/4}, \quad \left(\frac{\alpha}{\lambda}\right)_4 \left(\frac{\beta}{\lambda}\right)_4 = \left(\frac{\alpha\beta}{\lambda}\right)_4$$

（相互法則は，表には出ないので省略）

プライマリな数　Z **と違って** $\mathcal{O}$ **の数を正負で分けることはできないが，奇数** ($(1+i) \nmid \lambda$) **については**

$$\mathcal{O} \ni \lambda \ : \ \text{primary} \stackrel{\cdot}{\longleftrightarrow} \lambda \equiv 1 \pmod{(1+i)^3}$$

によって $\pm\lambda, \ \pm i\lambda$ **の中の一つを特定することがある．**
(同型 $(\mathcal{O}/(1+i)^3)^\times \cong \{\pm 1, \pm i\}$ **に注意)**

道具立て (2) $\boxed{\cot \pi x \quad \longrightarrow \quad \mathrm{sl}((1-i)\varpi u)}$

レムニスケート・サイン

$$\varphi(u) \doteq \mathrm{sl}((1-i)\varpi u), \quad (\,\varpi = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}}\,)$$

ガウスの定義は後にして，性質で特徴付けると

$\varphi(u)$ **は周期格子** $\mathcal{O} = \mathrm{Z}[i]$ **の楕円関数，**

$\varphi(u) = \varphi(u+1) = \varphi(u+i)$

- $\mathrm{div}(\varphi) = (0) + ((1+i)/2) - (1/2) - (i/2)$
- $\varphi((1+i)/4) = \mathrm{sl}(\varpi/2) = 1$
- $\varphi(u) = (1-i)\,\varpi\, u + O(u^5)$
- $\varphi(i\,u) = i\,\varphi(u)$

周期格子 $\varpi\mathcal{O}$ **の** Weierstrass **関数で表せば**

$$(\,\wp'^2 = 4\,\wp^3 - 4\,\wp, \quad \zeta' = -\wp\,)$$

$$\varphi(u) = -2(1-i)\frac{\wp(\varpi u)}{\wp'(\varpi u)}$$

$$= -\frac{1-i}{2}\left\{\zeta\left(\varpi\left(u-\tfrac{1}{2}\right)\right) - \zeta\left(\varpi\left(u-\tfrac{i}{2}\right)\right) - \frac{\pi}{2\varpi}\right\}$$

- $\mathrm{sl}(u)$ **の周期格子は** $(1-i)\varpi\mathcal{O}$ **である．**

- lemn. sin は sin に似ている：

$$t = \mathrm{sl}\, u \iff u = \int_0^t \frac{dt}{\sqrt{1-t^4}},$$

$$\varpi = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}} = 2.62205755\cdots,$$

$$\text{cf.}\quad t = \sin u \iff u = \int_0^t \frac{dt}{\sqrt{1-t^2}},$$

$$\pi = 2\int_0^1 \frac{dt}{\sqrt{1-t^2}} = 3.14159265\cdots,$$

- lemn. sin は tan にも似ている：

$$\mathrm{sl}\,\varpi z = \varpi\, z \prod_{\mu}\left(1-\frac{z^4}{\mu^4}\right) \prod_{\nu}\left(1-\frac{z^4}{\nu^4}\right)^{-1},$$

$$\mu \in L,\quad \nu \in L' - \tfrac{1+i}{2},$$

$$\text{cf.}\quad \tan \pi z = \pi\, z \prod_{m}\left(1-\frac{z^2}{m^2}\right) \prod_{n}\left(1-\frac{z^2}{n^2}\right)^{-1},$$

$$m \in \mathrm{N},\quad n \in \mathrm{N} - \tfrac{1}{2},$$

$$L = \big\{a+bi \,|\, a,\, b \in \mathrm{Z},\ a \geq 1,\ b \geq 0\big\},$$

$$L' = \big\{a+bi \,|\, a,\, b \in \mathrm{Z},\ a \geq 1,\ b \geq 1\big\}.$$

・倍角公式・CM 公式を比べれば tan との類似はますます明らかとなる：

CM 公式・倍角公式

λ : primary prime, $\quad p = \lambda\bar{\lambda}$

$$\frac{\varphi(\lambda u)}{\varphi(u)} = \prod_{\nu \in \mathsf{R}} \varphi\left(u + \frac{\nu}{\lambda}\right), \quad \mathsf{R} = (\mathcal{O}/(\lambda))^{\times}$$

$$= \frac{U(t)}{t^{p-1}U(t^{-1})} \qquad (\, t = \varphi(u)\,)$$

$$U(\varphi(u)) = \prod_{\nu \in \mathsf{R}} \left(\varphi(u) - \varphi\left(\frac{\nu}{\lambda}\right)\right)$$

$$\begin{aligned} U(t) &= t^{p-1} + \cdots + \lambda \ \in \mathcal{O}[t] \quad (\text{Abel}) \\ &\equiv t^{p-1} \quad (\text{mod } \lambda) \quad (\text{Eisenstein}) \end{aligned}$$

特に $U(0)$ を比べて, $\boxed{\prod_{\nu \in \mathsf{R}} \varphi\left(\frac{\nu}{\lambda}\right) = \lambda}$

$$\text{cf.} \quad \frac{\tan pu}{\tan u} = (-1)^{\frac{p-1}{2}} \prod_{k=0}^{p-1} \tan\left(u + \frac{\pi k}{p}\right)$$

$$= (-1)^{\frac{p-1}{2}} \frac{V(t)}{t^{p-1}V(t^{-1})}$$

$$V(\tan u) = \prod_{k=1}^{p-1} \left(\tan u - \tan\frac{\pi k}{p}\right)$$

$$\begin{aligned} V(t) &= t^{p-1} + \cdots + (-1)^{\frac{p-1}{2}} p \ \in \mathbf{Z}[t] \\ &\equiv t^{p-1} \quad (\text{mod } p) \quad (p > 2 \ : \text{prime}) \end{aligned}$$

特に $F(0)$ を比べて, $\displaystyle\prod_{k=1}^{p-1} \tan\frac{\pi k}{p} = (-1)^{\frac{p-1}{2}} p$

- lemn. sin は cot に似ているだろうか：

$$\pi\ \cot \pi x = \left[\sum_{n\in \mathrm{Z}} \frac{1}{x+n}\right] = \sum_{n\in \mathrm{Z}} \frac{x}{x^2-n^2}$$

の第一類似は，　($[\cdots]$: not abs.conv. series)

$$\varpi\,\zeta(\varpi u) = \left[\sum_{\nu\in \mathcal{O}} \frac{1}{u+\nu}\right] = \sum_{\nu\in \mathcal{O}} \frac{u^3}{u^4-\nu^4}$$

であろうが，これは楕円関数ではない．しかし

$$\varpi\,\mathsf{Z}(u) \doteq \varpi\,\zeta(\varpi u) - \pi\,\overline{u}$$

と小修正すれば，2重周期関数となる．そして

$$\varpi\,\mathsf{Z}(u) = \lim_{s\to 1} \sum_{\nu\in\mathcal{O}} (\overline{u}+\overline{\nu})|u+\nu|^{-2s} \quad (u \notin \mathcal{O}) \quad (\spadesuit)$$

が成立つ．$\mathsf{Z}(u)$ は $\cot \pi x$ の <u>良い類似</u> と考えられるのだが，非複素解析的な関数である．$\varphi(u)$ 自身は

$$-(1+i)\,\varphi(u) = \mathsf{Z}(u+\tfrac{1}{2}) - \mathsf{Z}(u+\tfrac{i}{2}) \qquad (\clubsuit)$$

によって結ばれる．

$(\spadesuit)$ は $L(1,\,\widetilde{\chi}_\lambda)$ との橋渡しをする！

- $\mathrm{lemn.\,sin}$ は $\sec$ に似ている：

$$\begin{aligned}-(1+i)\,\varphi(u) &= \mathsf{Z}(u+\tfrac{1}{2})-\mathsf{Z}(u+\tfrac{i}{2}) \\ &= \sum_{\kappa \,(\mathrm{mod}\,2)} \chi_0^2(\kappa)\,\mathsf{Z}(u+\tfrac{\kappa}{2}) \quad (\clubsuit)\end{aligned}$$

$$\begin{aligned}\text{cf.}\quad 2\sec 2\pi x &= \cot(\pi(x+\tfrac{1}{4}))-\cot(\pi(x-\tfrac{1}{4})) \\ &= \sum_{k \,(\mathrm{mod}\,4)} \psi_0(k)\ \cot(\pi(x+\tfrac{k}{4}))\end{aligned}$$

χ_0^2，ψ_0 は $(\mathcal{O}/(2))^\times$，$(\mathrm{Z}/4\mathrm{Z})^\times$ の 2 次の指標．

$$\chi_0^2(\kappa)=\begin{cases}1 & \cdots \kappa\equiv 1 \pmod 2\\ -1 & \cdots \kappa\equiv i \pmod 2\\ 0 & \cdots (1+i)|\kappa\end{cases}$$

$$\psi_0(k)=\begin{cases}1 & \cdots k\equiv 1 \pmod 4\\ -1 & \cdots k\equiv 3 \pmod 4\\ 0 & \cdots 2|k\end{cases}$$

・これらの指標は後で用いることになる．

予備実験

$$\boxed{\mathcal{G}_\lambda \doteq \frac{1}{4} \sum_{\nu \pmod{\lambda}} \left(\frac{\nu}{\lambda}\right)_4 \varphi\left(\frac{\nu}{\lambda}\right)}$$

$$p = \lambda\overline{\lambda}, \quad p \equiv 13 \pmod{16} \quad \text{i.e.} \left(\frac{i}{\lambda}\right)_4 = -i$$

（後者は，自明に $\mathcal{G}_\lambda = 0$ とならぬための条件）

例 (by GP/PARI, **フリー・ソフト**)

$$13 = (3+2i)(3-2i), \quad 269 = (-13+2i)(-13-2i)$$

```
? G(3+2*I)
%2 = -0.8834210298249901 - 2.462903231165610*I
? G(3+2*I)^4
%3 = 9.000000000000000 - 46.00000000000000*I
? G(3+2*I)^4/(3+2*I)^3
%4 = -1.000000000000000 + 1.516007771 E-19*I
? G(-13+10*I)
%5 = 21.55259271671605 - 11.54499287155424*I
? G(-13+10*I)^4
%6 = -137943.0000000000 - 329670.0000000000*I
? G(-13+10*I)^4/(-13+10*I)^3
%7 = -81.00000000000000 - 1.255950716 E-16*I
```

$$\mathcal{G}_{(3+2i)}{}^4 = -(3+2i)^3, \ \cdots,$$
$$\mathcal{G}_{(-13+10i)}{}^4 = -3^4 \cdot (-13+10i)^3, \ \cdots,$$
$$\mathcal{G}_\lambda{}^4 = A_\lambda{}^4 \cdot (-\lambda)^3 \ ? \qquad \mathcal{G}_\lambda = A_\lambda \cdot \boxed{(\sqrt[4]{-\lambda})^3}\,?$$

$\sqrt[4]{-\lambda}$ の定め方？

一つの試み

$$p = \lambda\bar{\lambda} \equiv 5 \pmod 8), \quad \lambda : \text{primary prime},$$
$$\mathsf{S} \doteqdot \left\{ \nu \in \mathsf{R} = (\mathcal{O}/(\lambda))^{\times} \;\middle|\; \left(\frac{\nu}{\lambda}\right)_4 = 1 \right\},$$
$$\widetilde{\lambda} \doteqdot \prod_{\nu \in \mathsf{S}} \varphi\left(\frac{\nu}{\lambda}\right) \implies \widetilde{\lambda}^4 = -\lambda$$

なぜなら $\left(\frac{i}{\lambda}\right)_4 = i^{\frac{p-1}{4}} = \pm i$ であることから

$\mathsf{R} = \mathsf{S} \cup i\mathsf{S} \cup -\mathsf{S} \cup -i\mathsf{S}$ と (剰余類) 分解されるので

Abel & Eisenstein の積公式と合わせて

$$\lambda = \prod_{\nu \in R} \varphi\left(\frac{\nu}{\lambda}\right) = (-1)^{\frac{p-1}{4}} \cdot \left\{ \prod_{\nu \in S} \varphi\left(\frac{\nu}{\lambda}\right) \right\}^4 = -\widetilde{\lambda}^4 .$$

$\sqrt[4]{-\lambda}$ として $\widetilde{\lambda}$ を選ぶ

この選び方がマアマアであることは，後で分かってくる．

新たな実験と観察

$$\mathcal{G}_\lambda \doteq \frac{1}{4}\sum_{\nu\,(\mathrm{mod}\,\lambda)}\left(\frac{\nu}{\lambda}\right)_4 \varphi\left(\frac{\nu}{\lambda}\right) = A_\lambda\,\widetilde{\lambda}^3, \quad \widetilde{\lambda}^4 = -\lambda$$

p	λ	A_λ	p	λ	A_λ
13	$3+2i$	1	541	$-21+10i$	1
29	$-5+2i$	1	557	$19+14i$	-1
61	$-5+6i$	-1	653	$-13+22i$	-1
109	$3+10i$	1	701	$-5+26i$	1
157	$11+6i$	1	733	$27+2i$	1
173	$-13+2i$	-1	797	$11+26i$	-1
269	$-13+10i$	3	829	$27+10i$	-5
317	$11+14i$	-1	877	$-29+6i$	-1
349	$-5+18i$	1	941	$-29+10i$	3
397	$19+6i$	-1	1021	$11+30i$	-3
461	$19+10i$	-1	1069	$-13+30i$	-1
509	$-5+22i$	-1	1117	$-21+26i$	-5

400万 以下の素数 $p \equiv 13 \pmod{16}$ （35432 個）についての計算結果は ($p = \lambda\overline{\lambda}$, λ : primary prime)

$$-49 \le A_\lambda \le 49 \quad \text{for} \quad 13 \le p \le 3999949$$

であった．(by 加納成男氏)

予想から定理へ

$$\boxed{\mathcal{G}_\lambda = A_\lambda \cdot \widetilde{\lambda}^3, \quad A_\lambda \in \mathbb{Z}}$$

(I) $A_\lambda \in \mathbb{Q}(i)$ **はやさしい．体の理論によればよい：**

$$F \doteq \mathbb{Q}(i), \quad L \doteq F\left(\varphi(1/\lambda)\right)$$

$$\mathrm{Gal}(L/F) \cong \mathsf{R} \doteq (\mathcal{O}/(\lambda))^\times \quad \text{by} \quad \sigma_\mu \longleftrightarrow \mu\,,$$

$$\varphi\left(\frac{\nu}{\lambda}\right)^{\sigma_\mu} = \varphi\left(\frac{\mu\nu}{\lambda}\right) \qquad \text{(Abel, Eisenstein)}$$

$$\therefore \quad \mathcal{G}_\lambda{}^{\sigma_\mu} = \sum_{\nu \in \mathsf{S}} \varphi\left(\frac{\mu\nu}{\lambda}\right) = \sum_{\nu \in \mu\mathsf{S}} \varphi\left(\frac{\nu}{\lambda}\right) = \overline{\left(\frac{\mu}{\lambda}\right)_4} \cdot \mathcal{G}_\lambda,$$

$$\widetilde{\lambda}^{\sigma_\mu} = \prod_{\nu \in \mathsf{S}} \varphi\left(\frac{\mu\nu}{\lambda}\right) = \prod_{\nu \in \mu\mathsf{S}} \varphi\left(\frac{\nu}{\lambda}\right) = \left(\frac{\mu}{\lambda}\right)_4 \widetilde{\lambda}$$

$$\because \quad \mu\mathsf{S} = \varepsilon\mathsf{S} \quad (\exists \varepsilon = \pm 1, \pm i), \quad \left(\frac{\mu}{\lambda}\right)_4 = \left(\frac{\varepsilon}{\lambda}\right)_4 = \overline{\varepsilon}\,.$$

$$\therefore \quad A_\lambda{}^{\sigma_\mu} = \mathcal{G}_\lambda{}^{\sigma_\mu} \cdot (\widetilde{\lambda}^{\sigma_\mu})^{-3} = A_\lambda \qquad \therefore \quad A_\lambda \in F = \mathbb{Q}(i)\,.$$

(II) $A_\lambda \in \mathcal{O} \doteq \mathbb{Z}[i]$ **はやや数論的か．環上の理論：**

$\mathcal{G}_\lambda = A_\lambda \cdot \widetilde{\lambda}^3$ **は代数的整である一方** $\widetilde{\lambda}^4\,(= -\lambda)$ **が** $\mathcal{O}$ **の素数である．よって** $F \ni A_\lambda$ **は分母を持ち得ない．**

<u>**参考**</u>**．** $\varphi(1/\lambda)$ **の最小多項式が** Eisenstein **型** mod λ **であることから，** $\mathfrak{P} = (\varphi(1/\lambda))$ **は** L **の素イデアルで，** $(\lambda) = \mathfrak{P}^{p-1}, \quad (\widetilde{\lambda}) = \mathfrak{P}^{\frac{p-1}{4}}$ **(完全分岐) となっている．**

(III)　$A_\lambda \in \mathrm{Z}$　は自明ではない．少し長くなる．
$A_\lambda = \overline{A}_\lambda$ を示すことが目標になる．

楕円ガウス和と L 関数との関連 は？

まず 類ガウス和と Dirichlet L との関連を反芻：

$\chi(-1) = -1$ (e.g. $\chi = \chi_p$, $p \equiv 3 \pmod 4$) ならば

$$L(1,\chi) = \left[\sum_{n=1}^{\infty} \frac{\chi(n)}{n}\right] = \frac{1}{2}\left[\sum_{n\in\mathrm{Z}} \frac{\chi(n)}{n}\right]$$

左右に延びた和 が 周期関数 (cot, etc) と結びつく！

（$p \equiv 1 \pmod 4$) のときは $\chi_p(-1) = 1$.　これを
$\chi = \chi_p \cdot \psi_0$ と “小修正” すれば $\chi(-1) = -1$.
そして $L(1,\chi)$ が sec の類ガウス和で表される.)

$\mathcal{O} = \mathrm{Z}[i]$ では次のように考えてはどうだろう．
剰余類指標 χ_1 が $\chi_1(i) = i$ を満たすならば

$$\left[\sum_{\nu\in\mathcal{O}} \frac{\chi_1(\nu)}{\nu}\right] = \left[\sum_{\nu\in\mathcal{O}} \frac{\chi_1(\nu)\overline{\nu}}{|\nu|^{2s}}\right]_{s=1}$$

を考えれば，これは上下左右に延びる和 である！
右辺は左辺の和を正当化するための一つの方法．

われわれの場合に戻る．

$p = \lambda\overline{\lambda} \equiv 13 \pmod{16}$, λ: primary prime

$\chi_\lambda(\nu) \doteq \left(\dfrac{\nu}{\lambda}\right)_4$ $(\therefore\ \chi_\lambda(i) = -i)$ **を "小修正" する．**

$\chi_{1,\lambda}(\nu) \doteq \chi_\lambda(\nu)\cdot{\chi_0}^2(\nu) \quad \therefore \quad \chi_{1,\lambda}(i) = i$

$\chi_{1,\lambda}(\nu)$ **は** mod (2λ) **の剰余類指標．**

$\widetilde{\chi}_\lambda(\mathfrak{a}) \doteq \chi_{1,\lambda}(\nu)\overline{\nu} \quad$ for $\quad \mathfrak{a} = (\nu)$

$\widetilde{\chi}_\lambda$ **はイデアル** $\mathfrak{a} = (\nu)$ **の乗法的関数** (Hecke **指標**)

$$\boxed{L(s,\,\widetilde{\chi}_\lambda) \doteq \sum_{\mathfrak{a}} \frac{\widetilde{\chi}_\lambda(\mathfrak{a})}{N\mathfrak{a}^s} = \frac{1}{4}\sum_{\nu\in\mathcal{O}} \frac{\chi_1(\nu)\overline{\nu}}{|\nu|^{2s}} \quad (\mathrm{Re}\, s > \tfrac{3}{2})}$$

これが Hecke L (**の一つ**). $s \in \mathrm{C}$ **へ解析接続される．**

楕円ガウス和 $\mathcal{G}_\lambda$ **と** $L(1,\,\widetilde{\chi}_\lambda)$ **との関連は期待通り：**

$$\boxed{-(1+i)\,\chi_\lambda(2)\,\mathcal{G}_\lambda = \frac{2\lambda}{\varpi}\,L(1,\,\widetilde{\chi}_\lambda) \qquad (\mathcal{G}\&L)}$$

$(\mathcal{G}\&L)$ **の証明は先述の２等式を用いれば難かしくない．**

$$\varpi\,\mathsf{Z}(u) = \lim_{s\to 1}\sum_{\nu\in\mathcal{O}} (\overline{u}+\overline{\nu})|u+\nu|^{-2s} \qquad (\spadesuit)$$

$$-(1+i)\,\varphi(u) = \sum_{\kappa\,(\mathrm{mod}\,2)} \chi_0^2(\kappa)\,\mathsf{Z}(u+\tfrac{\kappa}{2}) \qquad (\clubsuit)$$

併せて，類比 $\boxed{\cot : \mathsf{Z} = \sec : \varphi}$ **を思い出すとよい．**

$\mathcal{G}_\lambda = A_\lambda \cdot \widetilde{\lambda}^3$.　$A_\lambda = \overline{A_\lambda}$ を示そうとしている．
$\longrightarrow$　$\mathcal{G}_\lambda$ と $\overline{\mathcal{G}_\lambda}$ の関係を知りたい ⋯
$\longrightarrow$　$L(1,\,\widetilde{\chi}_\lambda)$ と $\overline{L(1,\,\widetilde{\chi}_\lambda)}$ の関係を知りたい ⋯

Aha! 鍵は ヘッケ L の関数等式 であった！

$$\Lambda(s,\ \widetilde{\chi}_\lambda) = C(\widetilde{\chi}_\lambda)\,\Lambda(2-s,\ \overline{\widetilde{\chi}_\lambda}),$$

ただし $\Lambda(s,\ \widetilde{\chi}_\lambda) = \left(\dfrac{2\pi}{\sqrt{16p}}\right)^{-s} \Gamma(s)\,L(s,\ \widetilde{\chi}_\lambda),$

$$C(\widetilde{\chi}_\lambda) = -i\,\frac{1}{2\lambda} \sum_{\kappa\,(\mathrm{mod}\,2\lambda)} \chi_{1,\lambda}(\kappa)\,e^{2\pi i\,\mathrm{Re}\left(\frac{\kappa}{2\lambda}\right)}$$

$s=1$ として central value equation が得られる：

$$L(1,\,\widetilde{\chi}_\lambda) = C(\widetilde{\chi}_\lambda)\,\overline{L(1,\,\widetilde{\chi}_\lambda)} \qquad \text{(cvEq)}$$

$\because$　$\overline{L(s,\,\widetilde{\chi}_\lambda)} = L(\overline{s},\,\overline{\widetilde{\chi}_\lambda}),\quad L(1,\,\overline{\widetilde{\chi}_\lambda}) = \overline{L(1,\,\widetilde{\chi}_\lambda)}$

残るは “root number” $C(\widetilde{\chi}_\lambda)$ の値．結果は

$$C(\widetilde{\chi}_\lambda) = -i\,\widetilde{\lambda}^{-1}\,\overline{\widetilde{\lambda}} \qquad \text{(rtNo)}$$

この証明は後回しにして，$\boxed{\text{係数}}$ $A_\lambda \in \mathbb{Z}$ を解決しよう．

楕円ガウス和 $\boxed{\text{係数}}$ の有理性

(III)　$A_\lambda = \overline{A}_\lambda$　$(\therefore A_\lambda \in \mathbb{Z})$ を示す．

いまや必要な等式はすべて出揃っている．

$$\boxed{\begin{array}{lr}
\mathcal{G}_\lambda = A_\lambda \cdot \widetilde{\lambda}^3, \quad \widetilde{\lambda}^4 = -\lambda, \quad A_\lambda \in \mathbb{Z}[i] & \text{(II)} \\
-(1+i)\,\chi_\lambda(2)\,\mathcal{G}_\lambda = \dfrac{2\lambda}{\varpi} L(1,\,\widetilde{\chi}_\lambda) & (\mathcal{G}\&L) \\
L(1,\,\widetilde{\chi}_\lambda) = C(\widetilde{\chi}_\lambda)\,\overline{L(1,\,\widetilde{\chi}_\lambda)} & \text{(cvEq)} \\
C(\widetilde{\chi}_\lambda) = -i\,\widetilde{\lambda}^{-1}\,\overline{\widetilde{\lambda}} & \text{(rtNo)}
\end{array}}$$

(cvEq) と (rtNo)，(II) と $(\mathcal{G}\&L)$ から，それぞれ

$$\widetilde{\lambda}\,L(1,\,\widetilde{\chi}_\lambda) = -i\,\overline{\widetilde{\lambda}\,L(1,\,\widetilde{\chi}_\lambda)}\,,$$

$$\frac{2\widetilde{\lambda}}{\varpi} L(1,\,\widetilde{\chi}_\lambda) = (1+i)\,\chi_\lambda(2)\,A_\lambda\,.$$

$$\therefore \quad -i\,\chi_\lambda(2)\,A_\lambda = \overline{-i\,\chi_\lambda(2)\,A_\lambda}\,.$$

ところが　$-i\,\chi_\lambda(2) = \chi_\lambda(2i) = \chi_\lambda(1+i)^2 = \pm 1.$

$$\therefore \quad A_\lambda = \overline{A_\lambda}\,.$$

証明がおわった．

Cor.　$$\frac{(1+i)\widetilde{\lambda}}{\varpi} L(1,\,\widetilde{\chi}_\lambda) = -\chi_\lambda(2i)\,A_\lambda \in \mathbb{Z}$$

Root number $C(\widetilde{\chi}_\lambda)$ の計算

$$\boxed{C(\widetilde{\chi}_\lambda) \doteq -i\,\frac{1}{2\lambda} \sum_{\nu\,(\mathrm{mod}\,2\lambda)} \chi_{1,\lambda}(\nu)\, e^{2\pi i\,\mathrm{Re}\left(\frac{\nu}{2\lambda}\right)}}$$

$\chi_{1,\lambda}(\nu) = \chi_\lambda(\nu)\,{\chi_0}^2(\nu)$ だから

$$C(\widetilde{\chi}_\lambda) = -i\,\frac{1}{2\lambda}\,\chi_\lambda(2)\,{\chi_0}^2(\lambda)\,g({\chi_0}^2)\,g(\chi_\lambda)\,,$$

$$\begin{aligned} g({\chi_0}^2) &= \sum_{\nu\,(\mathrm{mod}\,2)} {\chi_0}^2(\nu)\, e^{2\pi i \mathrm{Re}(\nu/2)} \\ &= \sum_{\delta=1,\,i} \delta^2\, e^{2\pi i \mathrm{Re}(\delta/2)} = -2, \\ g(\chi_\lambda) &= \sum_{\nu\,(\mathrm{mod}\,\lambda)} \chi_\lambda(\nu)\, e^{2\pi i \mathrm{Re}(\nu/\lambda)} \quad (\downarrow \lambda = \boxed{a} + bi) \\ &= \sum_{r\,(\mathrm{mod}\,p)} \chi_\lambda(r)\, e^{2\pi i a r/p} = \overline{\chi}_\lambda(a)\,\boxed{G_4(\lambda)}\,. \end{aligned}$$

$$\because \quad (\mathcal{O}/(\lambda))^\times \cong (\mathrm{Z}/p\mathrm{Z})^\times, \quad \nu\,(\mathrm{mod}\,\lambda) \leftrightarrow r\,(\mathrm{mod}\,p),$$

$$\mathrm{Re}(\nu/\lambda) = \mathrm{Re}(r\overline{\lambda}/p) = ar/p \quad (a = \mathrm{Re}\,\lambda)$$

$${\chi_0}^2(\lambda) = 1 \text{ (obvious)}, \quad \chi_\lambda(a) = 1 \text{ (Eisenstein)}$$

$$\therefore \quad C(\widetilde{\chi}_\lambda) = i\,\chi_\lambda(2)\,\lambda^{-1}\,\boxed{G_4(\lambda)}$$

ここで $G_4(\lambda)$ は <u>4次のガウス和</u> である：

$$p \equiv 1 \pmod 4, \quad p = \lambda\overline{\lambda}, \quad \lambda : \text{primary prime}$$

$$G_4(\lambda) \doteq \sum_{r=1}^{p-1} \left(\frac{r}{\lambda}\right)_4 e^{2\pi i r/p}$$

$(\mathcal{O}/(\lambda))^\times \cong (\mathrm{Z}/p\mathrm{Z})^\times$ であるから well-defined.
高次ガウス和の値を決定することは古くからの難問．
$|G_4(\lambda)| = \sqrt{p}, \quad G_4(\lambda)^4 = \lambda^3\,\overline{\lambda}$ などは知られている．

1979 になって Matthews は 3 次，4 次のガウス和の explicit formula を発表した．Cassels が計算機実験によって予想した公式を証明 (検証) したのである．
Cassels-Matthews の公式の原型は $\wp, \wp'$ の等分値を用いて表されるが，複雑である．われわれの $\widetilde{\lambda} = \sqrt[4]{-\lambda}$ を用いると，同じ公式がたいへん簡明に表される．

G_4-formula (Matthews)

$$G_4(\lambda) = \chi_\lambda(-2)\,\widetilde{\lambda}^3\,\overline{\widetilde{\lambda}}$$

この G_4-formula を用いれば root number の公式 (rtNo) を得るのはやさしい．

$$C(\widetilde{\chi}_\lambda) = i\,\chi_\lambda(2)\,\lambda^{-1}\,G_4(\lambda) = -i\,\widetilde{\lambda}^{-1}\,\overline{\widetilde{\lambda}}.$$

$$\because \quad \chi_\lambda(2)\,\chi_\lambda(-2) = \chi_\lambda(2i)^2 = \chi_\lambda(1+i)^4 = 1$$

これですべてが証明されて，予想が定理となった！

正七角形調和 $\longrightarrow$ 類ガウス和
$\longrightarrow$ 楕円ガウス和 (楕円アナローグ)
$\longrightarrow$ 係数の有理性 (新たな現象？)
$\longrightarrow$ 証明 (関数等式, G_4-公式を経て)

- **係数 A_λ の意味づけ？**
  類ガウス和では 係数＝類数，この類似は？
  $L(s, \widetilde{\chi}_\lambda)$ はある楕円曲線の L 関数でもある．
  Birch & Swinnerton-Dyer **予想との関連？**
  $A_\lambda{}^2$ =“Tate-Shafarevich **群の位数**”？
- **係数 A_λ の整数公式はないか？**
  類ガウス和では 有限フーリエ展開 が有効
  楕円ガウス和に適用すると？ （第三部で！）

文献案内

・**高木貞治：近世数学史談（岩波文庫） すべての人に！**
・**竹内端三：楕円関数論（岩波全書）**
・**ヴェイユ（金子訳）：楕円関数論（東京スプリンガー）**
• Lemmermyer : Reciprocity Laws, Springer
• Asai : Elliptic Gauss Sums, RIMS B4, 2007

第二部　おわり

証明の短縮

$$\text{(III)} \qquad \mathcal{G}_\lambda = A_\lambda \cdot \widetilde{\lambda}^3, \quad A_\lambda = \overline{A_\lambda}$$

有限フーリエ変換のきれいな公式 $(\star)$ **を用いるならば，Hecke** L **を経由することなく (III) が証明される．**

$\beta \equiv 1 \pmod 2$ **とする．**

$$(\star) \qquad \varphi\left(\frac{\nu}{\beta}\right) = \frac{1}{\overline{\beta}} \sum_{\mu \,(\mathrm{mod}\, \beta)} \overline{\varphi\left(\frac{\mu}{\beta}\right)} \, e^{2\pi i \,\mathrm{Re}(2\mu\nu/\beta)}$$

$(\star)$ **の証明は後に回して (III) を証明する．**

$$p = \lambda\overline{\lambda} \equiv 13 \pmod{16}, \ \lambda\colon \text{primary prime}$$

$$\begin{aligned}
\mathcal{G}_\lambda &= \frac{1}{4} \sum_{\nu \,(\mathrm{mod}\, \lambda)} \chi_\lambda(\nu)\, \varphi\left(\frac{\nu}{\lambda}\right) \qquad \left(\chi_\lambda(\nu) = \left(\frac{\nu}{\lambda}\right)_4\right) \\
&= \sum_{\nu \,(\mathrm{mod}\, \lambda)} \chi_\lambda(\nu) \frac{1}{4\overline{\lambda}} \sum_{\mu \,(\mathrm{mod}\, \lambda)} \overline{\varphi\left(\frac{\mu}{\lambda}\right)} \, e^{2\pi i \,\mathrm{Re}(2\mu\nu/\lambda)} \\
&= \frac{1}{4\overline{\lambda}} \sum_{\mu \,(\mathrm{mod}\, \lambda)} \overline{\varphi\left(\frac{\mu}{\lambda}\right)} \sum_{\nu \,(\mathrm{mod}\, \lambda)} \chi_\lambda(\nu)\, e^{2\pi i \,\mathrm{Re}(2\mu\nu/\lambda)} \\
&= \frac{g(\chi_\lambda)}{\overline{\lambda}} \overline{\chi}_\lambda(2) \frac{1}{4} \sum_{\mu \,(\mathrm{mod}\, \lambda)} \overline{\chi}_\lambda(\mu)\, \overline{\varphi\left(\frac{\mu}{\lambda}\right)} \\
&= \frac{g(\chi_\lambda)}{\overline{\lambda}} \overline{\chi}_\lambda(2)\, \overline{\mathcal{G}_\lambda} = \widetilde{\lambda}^3 \overline{\widetilde{\lambda}}^{-3} \overline{\mathcal{G}_\lambda}.
\end{aligned}$$

$$\therefore \quad A_\lambda = \mathcal{G}_\lambda \widetilde{\lambda}^{-3} = \overline{\mathcal{G}_\lambda \widetilde{\lambda}^{-3}} = \overline{A_\lambda} \qquad \text{Q.E.D. !!}$$

ただし Matthews': $g(\chi_\lambda) = \chi_\lambda(-2)\, \widetilde{\lambda}^3 \overline{\widetilde{\lambda}}$ **は用いた．**

有限フーリエ変換

最初に伊藤の補題を準備し，それによって，有限フーリエ変換に関して自己共役的となる楕円関数が系統的に導かれることを見る．lemn. sine もその内の一つである．

格子は $\mathcal{O} = \mathrm{Z}[i]$ に限定しつつ，部分的に [Weil] の記号に従う．

$$K_1(u, u_0, s) \doteq \sum_{\mu\in\mathcal{O}}{}^{*} e^{\pi(\overline{u}_0\mu - u_0\overline{\mu})} (\overline{u} + \overline{\mu}) |u+\mu|^{-2s} \quad (\mathrm{Re}\, s > 3/2)$$

$$\pi^{-s}\,\Gamma(s)\,K_1(u, u_0, s) = e^{\pi(\overline{u}_0 u - u_0\overline{u})}\,\pi^{s-2}\,\Gamma(2-s)\,K_1(u_0, u, 2-s)$$

$$E_1^*(u) \doteq K_1(u, 0, 1) = K_1(0, u, 1)$$

Lemma (Hiroshi Ito, 1987)

$$\overline{E_1^*(\lambda/\beta)} = \frac{-i}{\beta} \sum_{\mu\,(\mathrm{mod}\,\beta)} E_1^*(\mu/\beta) e^{2\pi i\,\mathrm{Re}(\lambda\mu/\beta)}$$

Proof. $\mathrm{Re}\, s > 3/2$ として計算してから解析接続をする．

$$K_1(0, \overline{\lambda/\beta}, s) = -i \sum_{\nu\in\mathcal{O}}{}^{*} e^{2\pi i\,\mathrm{Re}(\lambda\nu/\beta)}\,\overline{\nu}|\nu|^{-2s}$$

$$= -i \sum_{\mu\,(\mathrm{mod}\,\beta)} e^{2\pi i\,\mathrm{Re}(\lambda\nu/\beta)} \left\{ \sum_{\nu\equiv\mu \pmod{\beta}}{}^{*} \overline{\nu}|\nu|^{-2s} \right\}$$

$$= -i \sum_{\mu\,(\mathrm{mod}\,\beta)} e^{2\pi i\,\mathrm{Re}(\lambda\nu/\beta)} \left\{ \sum_{\kappa\in\mathcal{O}}{}^{*} (\overline{\mu+\beta\kappa})|\mu+\beta\kappa|^{-2s} \right\}$$

$$= -i\cdot\overline{\beta}|\beta|^{-2s} \sum_{\mu\,(\mathrm{mod}\,\beta)} e^{2\pi i\,\mathrm{Re}(\lambda\nu/\beta)}\,K_1(\mu/\beta, 0, s)$$

$s = 1$ として証明が終る． $\overline{E_1^*(u)} = E_1^*(\overline{u})$ に注意．

- Lemma は，結局，K_1 の関数等式 (at $s = 1$) に基いている！

楕円関数を導くために $E_1^*(u)$ からわれわれの $\mathsf{Z}(u)$ に乗り換える．

$$\varpi\,\mathsf{Z}(u) \doteq \varpi\,\zeta(\varpi u) - \pi\,\overline{u}$$
$$\varpi\,\mathsf{Z}(u) = E_1^*(u) \quad (u \notin \mathcal{O}), \qquad (E_1^*(0) = 0,\ \mathsf{Z}(0) = \infty\,!!)$$

Ito's Lemma (言い替え)

$$\overline{\mathsf{Z}(\lambda/\beta)} = \frac{-i}{\beta} \sum_{\mu\,(\mathrm{mod}\,\beta)}{}' \mathsf{Z}(\mu/\beta) e^{2\pi i\,\mathrm{Re}(\lambda\mu/\beta)} \quad (\lambda \not\equiv 0\ (\mathrm{mod}\,\beta))$$

Twist of Z by χ

$$\phi_\chi(u) \doteq \sum_{\kappa\,(\mathrm{mod}\,\gamma)} \chi(\kappa)\,\mathsf{Z}(u + \kappa/\gamma)$$

ただし χ は primitive character mod γ.
$N\gamma > 1$ のとき $\phi_\chi(u)$ は 真の楕円関数である．

<u>例 (Twist of Z)</u>　(以下は加法公式によって確かめられる！)

$$
\begin{array}{lrcl}
(1) & \phi_{\chi_0^2}(u) & = & \mathsf{Z}(u+\tfrac{1}{2}) - \mathsf{Z}(u+\tfrac{i}{2}) \\
 & & = & -(1+i)\,\varphi(u) \\
(2) & \phi_{\chi_0}(u) & = & -(1-i)\{\psi(u) + \psi(i\,u)\} \\
(3) & \phi_{\overline{\chi}_0}(u) & = & -(1-i)\{-\psi(u) + \psi(i\,u)\} \\
(4) & \phi_{\chi_4}(u) & = & 2\sqrt{2}\cdot\varphi(2u)\,\varphi(u)^{-1} \\
(5) & \phi_{\overline{\chi}_4}(u) & = & 2\sqrt{2}\cdot i\cdot\varphi(2u)\,\varphi(u)
\end{array}
$$

ただし，$\psi(u) = \mathrm{cl}((1-i)\varpi u) = \varphi(u + \frac{1+i}{4})$　(lemn. cos)
また，character たちはそれぞれつぎのように定義されるもの：
$\chi_0\ :\ \mathcal{O}/(1+i)^3 \cong \{\pm 1, \pm i\}$ i.e. $\chi_0(\nu) \equiv \nu\ (\mathrm{mod}\ (1+i)^3)$
$\chi_0^2(\nu) = \chi_0(\nu)^2$, **ただし** χ_0: mod $(1+i)^3$, χ_0^2: mod (2).
$\chi_4(\nu) = \left(\dfrac{-1}{\nu}\right)_4 \chi_0(\nu)$, χ_4: mod (4) **である．**

ϕ_χ の有限フーリエ変換・自己共役性

> $\beta,\ \gamma$ は coprime とする．
>
> $$\overline{\phi_\chi(\nu/\beta)} = -\frac{i\,g(\overline{\chi})}{\gamma}\cdot\frac{\chi(\beta)}{\beta}\sum_{\mu\,(\mathrm{mod}\,\beta)}\phi_\chi(\mu/\beta)\,e^{2\pi i\,\mathrm{Re}(\mu\nu\gamma/\beta)}$$

ただし　$g(\overline{\chi}) = \displaystyle\sum_{\kappa\,(\mathrm{mod}\,\gamma)}\overline{\chi}(\kappa)\,e^{2\pi i\,\mathrm{Re}(\kappa/\gamma)}$　(ガウス和)

Proof.　つぎの第二の等式のところで，β の代わりに $\beta\gamma$ として Ito's Lemma を用いる．その際，mod $\beta\gamma$ の代表を $\mu\gamma+\kappa'\beta$;　$\mu\,(\mathrm{mod}\,\beta),\ \kappa'\,(\mathrm{mod}\,\gamma)$　のように選ぶ．同時に $(\nu\gamma+\kappa\beta)(\mu\gamma+\kappa'\beta)\equiv\mu\nu\gamma^2+\kappa\kappa'\beta^2$ (mod $\beta\gamma$) にも注意．

$$\overline{\phi_\chi(\nu/\beta)} = \sum_{\kappa\,(\mathrm{mod}\,\gamma)}\overline{\chi}(\kappa)\,\overline{\mathsf{Z}\left(\frac{\nu\gamma+\kappa\beta}{\beta\gamma}\right)}$$

$$= \sum_{\kappa\,(\mathrm{mod}\,\gamma)}\overline{\chi}(\kappa)\cdot\frac{-i}{\beta\gamma}\sum_{\substack{\mu\,(\mathrm{mod}\,\beta)\\ \kappa'\,(\mathrm{mod}\,\gamma)}}\mathsf{Z}\left(\frac{\mu}{\beta}+\frac{\kappa'}{\gamma}\right)\,e^{2\pi i\,\mathrm{Re}(\gamma\mu\nu/\beta+\kappa\kappa'\beta/\gamma)}$$

$$= -\frac{i}{\beta\gamma}\sum_{\substack{\mu\,(\mathrm{mod}\,\beta)\\ \kappa'\,(\mathrm{mod}\,\gamma)}}\left\{\sum_{\kappa\,(\mathrm{mod}\,\gamma)}\overline{\chi}(\kappa)\,e^{2\pi i\,\mathrm{Re}(\kappa\kappa'\beta/\gamma)}\right\}\mathsf{Z}\left(\frac{\mu}{\beta}+\frac{\kappa'}{\gamma}\right)\,e^{2\pi i\,\mathrm{Re}(\gamma\mu\nu/\beta)}$$

$$= -\frac{i}{\beta\gamma}\,g(\overline{\chi})\,\chi(\beta)\sum_{\mu\,(\mathrm{mod}\,\beta)}\left\{\sum_{\kappa'\,(\mathrm{mod}\,\gamma)}\chi(\kappa')\,\mathsf{Z}\left(\frac{\mu}{\beta}+\frac{\kappa'}{\gamma}\right)\right\}e^{2\pi i\,\mathrm{Re}(\gamma\mu\nu/\beta)}$$

$$= -\frac{i\,g(\overline{\chi})}{\gamma}\chi(\beta)\cdot\frac{1}{\beta}\sum_{\mu\,(\mathrm{mod}\,\beta)}\phi_\chi(\mu/\beta)\,e^{2\pi i\,\mathrm{Re}(\gamma\mu\nu/\beta)} \qquad \square$$

特に $\chi=\chi_0^2,\ \gamma=2$ として，$\phi_{\chi_0^2}=-(1+i)\,\varphi$ の自己共役性すなわち $(\star)$ を示すことができた．

附録

有限フーリエ変換についても Prototype として三角関数公式集を参照することができる．その源はガウスの昔に遡る．([DA] §362)

$$\bar{B}_1(x) \doteq \begin{cases} x - [x] - \frac{1}{2} & \cdots \quad x \notin \mathrm{Z} \\ 0 & \cdots \quad x \in \mathrm{Z} \end{cases}$$

$$\begin{aligned} \bar{E}_0(x) &\doteq 2\,\bar{B}_1(x + \tfrac{1}{4}) - 2\,\bar{B}_1(x - \tfrac{1}{4}) \\ &= \begin{cases} 1 & \cdots \quad \frac{1}{4} < x - [x] < \frac{3}{4} \\ -1 & \cdots \quad x - [x] < \frac{1}{4} \quad \text{or} \quad \frac{3}{4} < x - [x] \\ 0 & \cdots \quad x - [x] = \frac{1}{4} \quad \text{or} \quad x - [x] = \frac{3}{4} \end{cases} \end{aligned}$$

- $d > 0$

$$2i\,\bar{B}_1(h/d) = -\frac{1}{d} \sum_{\substack{k \,(\mathrm{mod}\, d) \\ k \not\equiv 0}} \cot \frac{\pi k}{d}\, e^{2\pi i\, hk/d}$$

$$\cot \frac{\pi k}{d} = 2i \sum_{h \,(\mathrm{mod}\, d)} \bar{B}_1(h/d)\, e^{2\pi i\, hk/d} \qquad (k \not\equiv 0)$$

- $d > 0, \quad d \equiv 1 \pmod 2$

$$(-1)^{\frac{d+1}{2}}\, \bar{E}_0(h/d) = \frac{1}{d} \sum_{k \,(\mathrm{mod}\, d)} \sec \frac{2\pi k}{d}\, e^{8\pi i\, hk/d}$$

$$\sec \frac{2\pi k}{d} = (-1)^{\frac{d+1}{2}} \sum_{h \,(\mathrm{mod}\, d)} \bar{E}_0(h/d)\, e^{8\pi i\, hk/d}$$

- $d > 0, \quad d \equiv 1 \pmod 2$

$$2i\,\bar{B}_1(h/d + \tfrac{1}{2}) \;=\; -\frac{1}{d} \sum_{\substack{k \,(\mathrm{mod}\, d) \\ k \not\equiv 0}} \csc\frac{2\pi k}{d}\, e^{4\pi i\, hk/d}$$

$$\csc\frac{2\pi k}{d} \;=\; 2i \sum_{h \,(\mathrm{mod}\, d)} \bar{B}_1(h/d + \tfrac{1}{2})\, e^{4\pi i\, hk/d} \qquad (k \not\equiv 0)$$

- $d > 0, \quad d \equiv 1 \pmod 2$

$$i\,\bar{E}_0(h/d + \tfrac{1}{4}) \;=\; -\frac{1}{d} \sum_{k \,(\mathrm{mod}\, d)} \tan\frac{\pi k}{d}\, e^{4\pi i\, hk/d}$$

$$\tan\frac{\pi k}{d} \;=\; i \sum_{h \,(\mathrm{mod}\, k)} \bar{E}_0(h/d + \tfrac{1}{4})\, e^{4\pi i\, hk/d}$$

Corollary (Gauss) $\quad \tan\dfrac{\pi k}{d} = -2 \displaystyle\sum_{h=1}^{\frac{d-1}{2}} \sin\frac{4\pi hk}{d}$, etc.

Twists of Cotangent

$$\sum_{k \,(\mathrm{mod}\, 4)} \left(\frac{-4}{k}\right) \cot\left(\theta + \frac{\pi k}{4}\right) = 2\,\sec 2\theta$$

$$\sum_{k \,(\mathrm{mod}\, 8)} \left(\frac{8}{k}\right) \cot\left(\theta + \frac{\pi k}{8}\right) = -4\sqrt{2}\cdot\frac{\sin 2\theta}{\cos 4\theta}$$

$$\sum_{k \,(\mathrm{mod}\, 8)} \left(\frac{-8}{k}\right) \cot\left(\theta + \frac{\pi k}{8}\right) = 4\sqrt{2}\cdot\frac{\cos 2\theta}{\cos 4\theta}$$

Corollary (class number) $\quad d > 0$, square-free

$$\sum_{k \,(\mathrm{mod}\, d)} \left(\frac{k}{d}\right) \frac{\sin 2\pi k/d}{\cos 4\pi k/d} = -h(-8d)\sqrt{d} \quad \cdots \quad d \equiv 3 \pmod 4$$

$$\sum_{k \,(\mathrm{mod}\, d)} \left(\frac{k}{d}\right) \frac{\cos 2\pi k/d}{\cos 4\pi k/d} = h(-8d)\sqrt{d} \quad \cdots \quad d \equiv 1 \pmod 4$$

類ガウス和の係数 A_p **は有限フーリエ変換 (パーセバル等式) を用いることで，いとも簡単に，その整数表示が得られる．楕円ガウス和では，そのことは失敗するが，その代わりに，有理性** $\boxed{A_\lambda = \overline{A_\lambda}}$ **の「短縮証明」が得られたわけである．**

これには，つぎのような単純な事情がある．

L **関数の** special value ($s = 1$ **とは限らない整数点での値**) **を，類ガウス和や楕円ガウス和の形で表示したとき，**L **関数の関数等式が，** special value **ではパーセバル等式に対応する．**

今回扱った楕円ガウス和では，$s = 1$ **での値が** central value **であったために，** central value equation (cvEq) **に対応するのが，当然にも** $\mathcal{G}_\lambda$, $\overline{\mathcal{G}_\lambda}$ **の間の等式であったのである．類ガウス和** (Dirichlet L) **の場合は, 同じ** $L(1, \chi)$ **であるが，これは** central value **ではない．パーセバル等式の右辺が整数表示されたのは，関数等式で対応する** $L(0, \chi)$ **の値が一般ベルヌイ数表示されただけのことで不思議はない．一般の** special value **でもそうなっている．**

一方，さりながら，$A_\lambda \in \mathbb{Z}$ **なのだから，その整数表示公式を期待するのも人情であろう．さらにそれが，** Matthews **の公式の別証明を導くのであれば，それはたいへんに望ましい！** Matthews **の公式は，係数有理性** $\boxed{A_\lambda = \overline{A_\lambda}}$ **と同値である．**

第三部　おわり