Vanishing Elliptic Gauss Sums and Bernoulli-Hurwitz Type Numbers

by Yoshihiro Ônishi@Meijo Univ.

第 40 回 愛知数論 seminar（@ 愛知工業大学 本山 satellite）

May 13, 2019

Contents

Main references

- Asai, T. : *Elliptic Gauss sums and Hecke L-values at $s = 1$*, RIMS Kôkyûroku Bessatsu, 2007. [Asai]
- Birch,B.J. and Swinnerton-Dyer,H.P.F. : *Notes on elliptic curves II*, Crelle, 1965. [BSD]
- Ônishi, Y. : *Congruence relations connecting Tate-Shafarevich groups with Hurwitz numbers*, Interdisciplinary Information Sciences, 2010
- Koblitz, N. : *Introduction to Elliptic Curves and Modular Forms (2nd ed.)*, G.T.M. **97**, 1993
- Lutz, E. : *Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques*, Crelle, **177**(1937).

Introduction

We give an analogy for Tate-Shafarevich groups of the following

Theorem. Let $p > 3$ be an odd rational prime, $h(-p)$ be the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$. Then we have

$$h(-p) \equiv \begin{cases} -2\, B_{\frac{p+1}{2}} \mod p & \text{if } p \equiv 3 \mod 4, \\ 2^{-1}\, E_{\frac{p-1}{2}} \mod p & \text{if } p \equiv 1 \mod 4. \end{cases}$$

Here B_n is the n-th Bernoulli number, E_n is the n-th Euler number. Moreover, the least residue of the RHS exactly equals to the value of LHS.

LHS comes from Dirichlet L-values $L(1, \left(\frac{\cdot}{p}\right))$.
RHS comes from "trigonometric" Gauss sums.

Elliptic Gauss sums were already used, in order to compute numerically the L-series attached to some elliptic curves over the rational numbers, in the famuous original paper [BSD] by Birch and Swinnerton-Dyer themseves. We wish to use them for investigation for L-series attached to some elliptic curves defined over an imaginary number field.

The lemniscatic sine function

積分

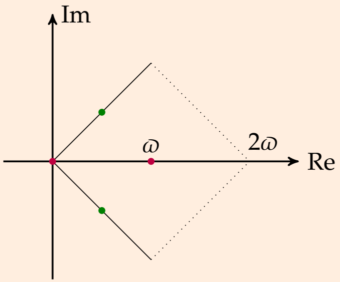
$$u = \int_0^t \frac{dt}{\sqrt{1-t^4}} = \sum_{n=0}^{\infty} (-1)^n \binom{-\frac{1}{2}}{n} \frac{t^{4n+1}}{4n+1} = t + \cdots$$

の逆函数 $u \mapsto t$ は lemniscatic sine 函数と呼ばれ $t = \mathrm{sl}(u)$ と記される. いま

$$\varpi = \int_1^{\infty} \frac{dx}{2\sqrt{x^3 - x}} = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}} = 2.262205\cdots$$

とおけば, $\mathrm{sl}(u)$ は周期格子 $(1-\boldsymbol{i})\,\varpi\,\mathbf{Z}[\boldsymbol{i}]$ を持つ楕円函数で, 因子は

$$\mathrm{div}(\mathrm{sl}) = (0) + (\varpi) - \left(\frac{\varpi}{1-\boldsymbol{i}}\right) - \left(\frac{\boldsymbol{i}\varpi}{1-\boldsymbol{i}}\right).$$



また

$$\mathrm{sl}(u) = u - \frac{1}{10}u^5 + \frac{1}{120}u^9 - \frac{11}{15600}u^{13} + \cdots$$
$$= \sum_{m=0}^{\infty} C_{4m+1}\, u^{4m+1}$$

と展開される.

The ray class field

以降では　$\varphi(u) = \mathrm{sl}\,((1-\boldsymbol{i})\,\varpi\,u))$　と記す．（周期格子は $\mathbf{Z}[\boldsymbol{i}]$.）

素数 $\ell \equiv 1 \bmod 4$, $\in \mathbf{Z}$.　$\ell = \lambda\bar{\lambda}$ such that $\lambda \equiv 1 \bmod (1+\boldsymbol{i})^3$.

$(\mathbf{Z}[\boldsymbol{i}]/(\lambda))^\times \simeq S \cup -S \cup \boldsymbol{i}S \cup -\boldsymbol{i}S$,　$|S| = \frac{\ell-1}{4}$ なる集合

$$S \subset \mathbf{Z}[\boldsymbol{i}]$$

を一つ選んで固定する．いま

$$\Lambda = \varphi\Big(\frac{1}{\lambda}\Big),\quad \mathscr{O}_\lambda = \text{“the ring of integers in } \mathbf{Q}(\boldsymbol{i},\Lambda)\text{”},$$

$$\tilde{\lambda} = \gamma(S)^{-1}\prod_{r\in S}\varphi\Big(\frac{r}{\lambda}\Big),\ \text{where}$$

$$\begin{cases} \{\pm1,\ \pm\boldsymbol{i}\} \ni \gamma(S) \equiv \prod_{r\in S} r \mod \lambda & \text{if } \ell \equiv 5 \bmod 8, \\ \{\pm\boldsymbol{i}\} \ni \gamma(S)^2 \equiv \prod_{r\in S} r^2 \mod \lambda & \text{if } \ell \equiv 1 \bmod 8 \end{cases}$$

とおく. このとき

$$(\lambda) = (\Lambda)^{\ell-1},\quad \Lambda \in \mathscr{O}_\lambda,\quad \tilde{\lambda}^4 = \Big(\frac{-1}{\lambda}\Big)_4\,\lambda.$$

$\mathbf{Q}(\boldsymbol{i},\Lambda)$ は $\mathbf{Q}(\boldsymbol{i})$ 上の conductor $(1+\boldsymbol{i})^3(\lambda)$ の ray class field.

$(\big(\mathbf{Z}[\boldsymbol{i}]/(1+\boldsymbol{i})^3\big)^\times \simeq \{\pm1,\ \pm\boldsymbol{i}\}$ に注意.)

Asai's theorem ($\ell \equiv 13 \bmod 16$ Case)

感じをつかむための典型的な例:

素数 $\ell \equiv 13 \bmod 16$. $\ell = \lambda\bar{\lambda}$ such that $\lambda \equiv 1 \bmod (1+\boldsymbol{i})^3$. $\chi_\lambda(r) = \left(\frac{r}{\lambda}\right)_4$.

$$\mathrm{egs}(\lambda) = \frac{1}{4}\sum_{r=1}^{\ell-1} \chi_\lambda(r)\,\mathrm{sl}\left((1-\boldsymbol{i})\,\varpi\frac{r}{\lambda}\right).$$

この和の各項は代数的整数で，$\mathrm{egs}(\lambda)$ は代数的整数である.

Theorem. ([Asai]) $\exists A_\lambda \in 1+2\mathbf{Z}$ such that

$$\mathrm{egs}(\lambda) = A_\lambda\,\tilde{\lambda}^3. \qquad \left(\tilde{\lambda} = \prod_{r\in S}\varphi\left(\tfrac{r}{\lambda}\right)\right)$$

特に $\mathrm{egs}(\lambda) \neq 0$.

Proof. 主に函数等式と Cassels-Matthews の公式を使ふ. （これはかなり深い結果.）
(BSD $\Longrightarrow$ Rationality of EGS $\Longrightarrow$ Cassels-Matthews.) $\square$

浅井氏に従つて A_λ を $\mathrm{egs}(\lambda)$ の係数と呼ぶ.

Remark. 上の $\mathrm{egs}(\lambda)$ の定義において χ_λ を $\chi(\boldsymbol{i}) = -\boldsymbol{i}$ でない別の指標 χ に置き換へると，その和は消失してしまふ.
各指標に対応する楕円函数は（ほとんど）決つてしまふのである.

The corresponding Hecke L-series

まづ $\left(\mathbf{Z}[\boldsymbol{i}]\big/(1+\boldsymbol{i})^2\right)^\times \simeq \{1,\ \boldsymbol{i}\}$ に注意して,

$$\chi_0{}'(\alpha) = \varepsilon^2 \quad \text{for} \quad \alpha \equiv \varepsilon \bmod (1+\boldsymbol{i})^2,\ \ \varepsilon \in \{1,\ \boldsymbol{i}\}$$

と定める．ここで

$$\tilde{\chi} = \chi_\lambda\, \chi_0{}'.$$

とおく． これは導手が $\left(\lambda(1+\boldsymbol{i})^2\right)$ の Hecke 指標となる.
これから得られる Hecke の L 函数 $L(s,\tilde{\chi})$ について,

Theorem. ([Asai])

$$L(1,\ \tilde{\chi}) = -\varpi\,(1-\boldsymbol{i})^{-1}\chi_\lambda(2)\lambda^{-1}\,\mathrm{egs}(\lambda).$$

証明は後で述べる.
上記の $L(s,\tilde{\chi})$ に対応する楕円曲線は $\mathscr{E}_{-\lambda} : y^2 = x^3 + \lambda x$ であり Deuring に依れば

$$L_{\mathscr{E}_{-\lambda}/\mathbf{Q}(\boldsymbol{i})}(s) = L(s,\ \tilde{\chi})\, L(s,\ \overline{\tilde{\chi}}\,).$$

Proposition. If the full statement of BSD conjecture for the curve $\mathscr{E}_{-\lambda} : y^2 = x^3 + \lambda x$ is ture, then $\sharp\,\text{Ш}\!\left(\mathscr{E}_{-\lambda}/\mathbf{Q}(\boldsymbol{i})\right) = |A_\lambda|^2.$

Some Congruence on the Coefficients of EGS

いま leminiscatic sine $u \mapsto \mathrm{sl}(u)$ の原点での展開係数を

$$\mathrm{sl}(u) = \sum_{m=0}^{\infty} C_{4m+1}\, u^{4m+1} = u - \tfrac{1}{10}u^5 + \tfrac{1}{120}u^9 - \tfrac{11}{15600}u^{13} + \cdots$$

と書くと,

Theorem. ([Ô])

$$\pm\sqrt{\sharp\,\text{Ш}\big(\mathscr{E}_{-\lambda}/\mathbf{Q}(i)\big)} \overset{?}{=} A_\lambda \equiv -\frac{1}{4}\, C_{\frac{3(\ell-1)}{4}} \mod \ell.$$

右辺の（絶対値）最小剰余が左辺の真の値を与へる（と思はれる）.
これは, 次の定理の拡張.

Theorem. (再掲) $p > 3$ を奇素数とし, $\mathbf{Q}(\sqrt{-p})$ の類数を $h(-p)$ とすると,

$$h(-p) \equiv \begin{cases} -2\, B_{\frac{p+1}{2}} \mod p & \text{if } p \equiv 3 \bmod 4, \\ 2^{-1}\, E_{\frac{p-1}{2}} \mod p & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

ここに B_n は Bernoulli 数, E_n は Euler 数. 右辺の最小剰余が左辺の真の値を与へる.

証明は後で述べる.

ここまでのまとめ

$\boxed{\ell \equiv 13 \bmod 16}$ の場合は対応する楕円曲線が

$$\mathscr{E}_{-\lambda} : y^2 = x^3 + \lambda x$$

であり $L(1, \tilde{\chi}) \neq 0$ がわかつた． Coates-Wiles の定理により

$$\operatorname{rank} \mathscr{E}_{-\lambda}(\mathbf{Q}(\boldsymbol{i})) = 0.$$

$\boxed{\ell \equiv 5 \bmod 16}$ の場合は対応する楕円曲線が

$$\mathscr{E}_{\frac{1}{4}\lambda} : y^2 = x^3 - \frac{1}{4}\lambda x$$

となり，同様に $\operatorname{rank} \mathscr{E}_{\frac{1}{4}\lambda}(\mathbf{Q}(\boldsymbol{i})) = 0$ である．

ここからの話：

$\boxed{\ell \equiv 1 \bmod 8}$ の場合は [Asai] の表の 18 % 程度で $\operatorname{egs}(\lambda) = 0$ となる．
以下, この場合に注目する．

Our Hecke charactoers

$I(\mathfrak{f})\,/\,P(\mathfrak{f})$ = “the ray class group modulo $\mathfrak{f}$ of $\mathbf{Q}(\boldsymbol{i})$”.
導手 $\mathfrak{f}$ の Hecke 指標 $\tilde{\chi} : I(\mathfrak{f}) \longrightarrow \mathbf{C}^{\times}$ で,
行き掛り上

$$\tilde{\chi}((\alpha)) = \chi_1(\alpha)\,\overline{\alpha} \quad \text{provided that} \quad \gcd(\alpha, \mathfrak{f}) = 1$$

なるものを考へる. 但し, $(\lambda) \,\|\, \mathfrak{f}$ （$\mathfrak{f} = (\lambda)\,\mathfrak{b}$ とおく） で,
χ_1 : $(\mathbf{Z}[\boldsymbol{i}]/\mathfrak{f})^{\times} \longrightarrow \mathbf{C}^{\times}$ は
$\chi_1(\varepsilon) = \varepsilon$ for $\varepsilon \in \{\pm 1, \pm \boldsymbol{i}\}$ を満たさなくてはならない.
さらに, 合成

$$\chi_\lambda \ : (\mathbf{Z}[\boldsymbol{i}]/(\lambda))^{\times} \to (\mathbf{Z}[\boldsymbol{i}]/(\lambda))^{\times} \times (\mathbf{Z}[\boldsymbol{i}]/\mathfrak{b})^{\times} \simeq (\mathbf{Z}[\boldsymbol{i}]/\mathfrak{f})^{\times} \xrightarrow{\chi_1} \mathbf{C}^{\times}$$

が

$$\chi_\lambda(\,\cdot\,) = \left(\frac{\cdot}{\lambda}\right)_4$$

となる様にしたい.
\# これ以外の Hecke 指標については未考察.
次 slide で例を述べる.

$\ell \equiv 1 \bmod 8$ case

以下 ε は常に $\{\pm 1, \pm \boldsymbol{i}\}$ の元を表すものとする.
まず χ_0 を任意の $\alpha \neq 0 \in \mathbf{Z}[\boldsymbol{i}]$ について

$$\chi_0(\alpha) = \varepsilon \quad \text{if} \quad \alpha \equiv \varepsilon \bmod (1+\boldsymbol{i})^3 \qquad (\,\alpha \neq 0 \in \mathbf{Z}[\boldsymbol{i}]\,)$$

なる指標を考える.

$\boxed{\ell \equiv 1 \bmod 16}$ のとき

$\chi_\lambda(\boldsymbol{i}) = 1$ であり, $\chi_1 = \chi_\lambda \chi_0$ とすればよく，このとき $\tilde{\chi}((\alpha)) = \chi_1(\alpha)\overline{\alpha}$ であり,

前 slide の性質を満たす. また $\mathfrak{f} = (\lambda(1+\boldsymbol{i})^3)$ である.　このときは

$$L(1, \tilde{\chi}) = \omega\, \overline{\chi_\lambda(1+\boldsymbol{i})}\, 2^{-1} \lambda^{-1} \operatorname{egs}(\lambda).$$

但し $\operatorname{egs}(\lambda)$ は次の slide で説明する.

$\boxed{\ell \equiv 9 \bmod 16}$ のときは

$\chi_\lambda(\boldsymbol{i}) = -1$ であり, $\chi_1 = \chi_\lambda \overline{\chi_0}$ とすればよく，このとき $\tilde{\chi}((\alpha)) = \chi_1(\alpha)\overline{\alpha}$ であり,

前 slide の性質を満たす．また $\mathfrak{f} = (\lambda(1+\boldsymbol{i})^3)$ である.　このときも

$$L(1, \tilde{\chi}) = \omega\, \overline{\chi_\lambda(1+\boldsymbol{i})}\, 2^{-1} \lambda^{-1} \operatorname{egs}(\lambda).$$

$\operatorname{egs}(\lambda)$ は次の slide で説明する.

The elliptic Gauss sum

素数 $\ell \equiv 1 \bmod 8$, を採る.

$\ell = \lambda\overline{\lambda}$, $\lambda \equiv 1 \bmod (1+\boldsymbol{i})^3$,

$\chi_\lambda(\nu) = \left(\dfrac{\nu}{\lambda}\right)_4$. このとき $\chi_\lambda(\boldsymbol{i}) = \boldsymbol{i}^{\frac{\ell-1}{4}} = \pm 1$.

また $\mathrm{cl}(u) = \mathrm{sl}\left(u + \frac{\varpi}{2}\right)$ を用いて, $\psi(u) = \mathrm{cl}\left((1-\boldsymbol{i})\,\varpi u\right)$ とし,

これらから elliptic Gauss sum を

$$\mathrm{egs}(\lambda) = \sum_{\nu \in S \cup \boldsymbol{i}S} \chi_\lambda(\nu)\,\psi\!\left(\frac{\nu}{\lambda}\right)$$

で定義する. このとき

Proposition. ([Asai] 再掲)

$$L(1, \tilde{\chi}) = \varpi\,\overline{\chi(1+\boldsymbol{i})}\,2^{-1}\lambda^{-1}\,\mathrm{egs}(\lambda).$$

The coefficients of EGS

We recall Asai's following result:

Theorem. ([Asai]) Let $\zeta_8 = \exp(2\pi \boldsymbol{i}/8)$. There exists $A_\lambda \in \mathbf{Z}[\zeta_8]$ such that

$$\mathrm{egs}(\lambda) = A_\lambda \, \tilde{\lambda}^3.$$

where A_λ is given by

$\ell \bmod 16$	$\chi_\lambda(1+\boldsymbol{i}) = 1$	$\chi_\lambda(1+\boldsymbol{i}) = -1$	$\chi_\lambda(1+\boldsymbol{i}) = i$	$\chi_\lambda(1+\boldsymbol{i}) = -i$
1	$\boldsymbol{i}\sqrt{2} \cdot a_\lambda$	$\sqrt{2} \cdot a_\lambda$	$\zeta_8 \cdot a_\lambda$	$\boldsymbol{i}\zeta_8 \cdot a_\lambda$
9	$\boldsymbol{i}\zeta_8 \cdot a_\lambda$	$\zeta_8 \cdot a_\lambda$	$\boldsymbol{i}\sqrt{2} \cdot a_\lambda$	$\sqrt{2} \cdot a_\lambda$

where $a_\lambda \in \mathbf{Z}$.

Remark. Asai observed that $a_\lambda \in 2\mathbf{Z}$.

Expression of $L(1,\tilde{\chi})$ by an EGS (1)

$L(1,\tilde{\chi})$ の EGS による表示の気分的な説明.

我々の場合 $\eta = \zeta(u+\omega) - \zeta(\omega)$, $-\eta\boldsymbol{i} = \zeta(u+\omega\boldsymbol{i}) - \zeta(u)$ であるので,

$$\mathsf{Z}(z) = \zeta(\varpi z) - \eta\,\overline{z}$$

は $\mathbf{Z}[\boldsymbol{i}]$ を周期とする周期函数となる. これは非解析的ではあるが, 全平面でほぼ有理型で, 格子点 $\mathbf{Z}[\boldsymbol{i}]$ において, 1 位の極を持つから,

$$\mathsf{Z}(z) \overset{!}{=} \frac{1}{\varpi}\sum_{\mu\in\mathbf{Z}[\boldsymbol{i}]}\frac{1}{z-\mu} = \frac{1}{\varpi}\sum_{\mu\in\mathbf{Z}[\boldsymbol{i}]}\frac{1}{z+\mu}.$$

$\mathfrak{f} = (f)$ と書くと

$$L(1,\tilde{\chi}) = \sum_{\substack{(\alpha):\,\text{ideal in }\mathbf{Z}[\boldsymbol{i}]\\ \gcd((\alpha),\,\mathfrak{f})=1}}\frac{\tilde{\chi}(\alpha)}{N(\alpha)} = \frac{1}{4}\sum_{\substack{\alpha\in\mathbf{Z}[\boldsymbol{i}]\\ \gcd((\alpha),\,\mathfrak{f})=1}}\frac{\chi_1(\alpha)}{\alpha} \quad (\alpha = \nu + \mu f)$$

$$= \frac{1}{4}\sum_{\substack{\nu \bmod f\\ \gcd((\nu),\,f)=1}}\ \sum_{\mu\in\mathbf{Z}[\boldsymbol{i}]}\frac{\chi_1(\nu)}{\nu+\mu f}$$

$$= \frac{1}{4f}\sum_{\substack{\nu \bmod f\\ \gcd((\nu),\,f)=1}}\chi_1(\nu)\sum_{\mu\in\mathbf{Z}[\boldsymbol{i}]}\frac{1}{\frac{\nu}{f}+\mu} = \frac{\varpi}{4f}\sum_{\substack{\nu \bmod f\\ \gcd((\nu),\,f)=1}}\chi_1(\nu)\,\mathsf{Z}\left(\frac{\nu}{f}\right).$$

Expression of $L(1, \tilde{\chi})$ by an EGS (2)

$\ell \equiv 1 \bmod 16$ とする．任意の $\alpha \in \mathbf{Z}[\boldsymbol{i}]$ は

$$\alpha \equiv (1+\boldsymbol{i})^3 \kappa + \lambda\,\varepsilon \mod \left(\lambda(1+\boldsymbol{i})^3\right)$$

と書ける．ここに κ は $\mathbf{Z}[\boldsymbol{i}]/(\lambda)$ の代表元として一意的．$\varepsilon \in \{\pm 1, \pm \boldsymbol{i}\}$．これより

$$\begin{aligned}
\varpi^{-1} L(1, \tilde{\chi}) &= \frac{1}{4(1+\boldsymbol{i})^3 \lambda} \sum_{\alpha \bmod \lambda(1+\boldsymbol{i})^3} \chi_1(\alpha)\, \mathsf{Z}\left(\frac{\alpha}{\lambda(1+\boldsymbol{i})^3}\right) \\
&= \frac{1}{4(1+\boldsymbol{i})^3 \lambda} \overline{\chi_\lambda(1+\boldsymbol{i})} \sum_{(1+\boldsymbol{i})^3 \kappa + \lambda\,\varepsilon \bmod \lambda(1+\boldsymbol{i})^3} \varepsilon\, \chi_\lambda(\kappa)\, \mathsf{Z}\left(\frac{(1+\boldsymbol{i})^3 \kappa + \lambda\,\varepsilon}{\lambda(1+\boldsymbol{i})^3}\right) \\
&= \frac{-(1+\boldsymbol{i})}{4 \cdot 4\lambda} \overline{\chi_\lambda(1+\boldsymbol{i})} \sum_{\kappa \bmod \lambda} \chi_\lambda(\kappa) \sum_{\varepsilon} \varepsilon\, \mathsf{Z}\left(\frac{\kappa}{\lambda} + \frac{\varepsilon}{(1+\boldsymbol{i})^3}\right).
\end{aligned}$$

ここで

$$\sum_{\varepsilon} \varepsilon\, \mathsf{Z}\left(u - \frac{\varepsilon}{(1+\boldsymbol{i})^3}\right) = -(1-\boldsymbol{i})\left(\psi(u) + \psi(iu)\right)$$

より

$$\begin{aligned}
&= \frac{-(1+\boldsymbol{i})}{4 \cdot 4\lambda} \overline{\chi_\lambda(1+\boldsymbol{i})} \sum_{\kappa \bmod \lambda} \chi_\lambda(\kappa)\, (-(1-\boldsymbol{i}))\left(\psi\left(\frac{\kappa}{\lambda}\right) + \psi\left(i\frac{\kappa}{\lambda}\right)\right) \\
&= \frac{1}{8\lambda} \overline{\chi_\lambda(1+\boldsymbol{i})} \sum_{\kappa \in S \cup -S \cup \boldsymbol{i}S \cup -\boldsymbol{i}S} \chi_\lambda(\kappa)\left(\psi\left(\frac{\kappa}{\lambda}\right) + \psi\left(i\frac{\kappa}{\lambda}\right)\right) \\
&= \frac{1}{4\lambda} \overline{\chi_\lambda(1+\boldsymbol{i})} \sum_{\kappa \in S \cup \boldsymbol{i}S} \chi_\lambda(\kappa)\left(\psi\left(\frac{\kappa}{\lambda}\right) + \psi\left(i\frac{\kappa}{\lambda}\right)\right) \;=\; \frac{1}{2\lambda} \overline{\chi_\lambda(1+\boldsymbol{i})} \sum_{\kappa \in S \cup \boldsymbol{i}S} \chi_\lambda(\kappa)\, \psi\left(\frac{\kappa}{\lambda}\right).
\end{aligned}$$

Arithmetic on the elliptic curve associated to the EGS for $\ell \equiv 1 \bmod 8$

$\ell = 8n+1 = \lambda\bar{\lambda}$ のとき, λ に対応する EGS に対応する Hecke の L 函数は楕円曲線

$$\mathscr{E}_\lambda : y^2 = x^3 - \lambda x \quad \text{(minimal model ではない)}$$

の L 函数の因子である. この曲線の導手は $((1+\boldsymbol{i})^3\lambda)^2$ であり (See [Serre-Tate], Thm.12),
$(1+\boldsymbol{i})$ における reduction は III 型,
λ における reductoin は I_2^* 型である.
玉河数と $\tau_{\mathfrak{p}}$ と A_λ = "the coeff. of $\mathrm{egs}(\lambda)$" は下記の表の通り:

$\ell \bmod 16$	Invariants	$\chi_\lambda(1+\boldsymbol{i}) = 1$	$\chi_\lambda(1+\boldsymbol{i}) = -1$	$\chi_\lambda(1+\boldsymbol{i}) = i$	$\chi_\lambda(1+\boldsymbol{i}) = -i$
1	A_λ	$\boldsymbol{i}\sqrt{2}\cdot a_\lambda$	$\sqrt{2}\cdot a_\lambda$	$\zeta_8\cdot a_\lambda$	$\boldsymbol{i}\zeta_8\cdot a_\lambda$
	$\tau_{(\lambda)}$	2	2	2	2
	$\tau_{(1+\boldsymbol{i})}$	4	4	2	2
9	A_λ	$\boldsymbol{i}\zeta_8\cdot a_\lambda$	$\zeta_8\cdot a_\lambda$	$\boldsymbol{i}\sqrt{2}\cdot a_\lambda$	$\sqrt{2}\cdot a_\lambda$
	$\tau_{(\lambda)}$	2	2	2	2
	$\tau_{(1+\boldsymbol{i})}$	2	2	4	4

Asai observed that $a_\lambda \in 2\mathbf{Z}$ (follows from the full BSD, currently a conjecture).

It is quite certain that $\left(\frac{1}{2}a_\lambda\right)^2 = \sharp Ш(\mathscr{E}_\lambda)$.

The congruence for $\ell \equiv 1 \bmod 8$

Lemniscateic cosine $u \mapsto \mathrm{cl}(\mathrm{u})$ の原点での展開係数を

$$\mathrm{cl}(u) = 1 + \sum_{j=2}^{\infty} C_{2j}\, u^{2j}$$

とおく．以下，話しを絞つて $\ell \equiv 1 \bmod 16$ の場合について述べる．以前の通りに

$$\ell = \lambda\overline{\lambda}, \quad \lambda \equiv 1 \bmod (1+\boldsymbol{i})^3$$

とし，S を $\left(\mathbf{Z}[\boldsymbol{i}]/(\lambda)\right)^{\times} = S \cup -S \cup \boldsymbol{i}S \cup -\boldsymbol{i}S$，$|S| = \frac{\ell-1}{4}$ となる様に選んでおく．
ここで $\chi_\lambda(\nu) \equiv \nu^{\frac{\ell-1}{4}} \bmod \ell$ であるから $\chi(\boldsymbol{i}) = 1$，である. $\psi(u) = \mathrm{cl}\big((1-\boldsymbol{i})\varpi u\big)$ とおき，

$$\mathrm{egs}(\lambda) = \sum_{\nu \in S \cup \boldsymbol{i}S} \chi_\lambda(\nu)\, \psi\!\left(\frac{\nu}{\lambda}\right) = A_\lambda\, \tilde{\lambda}^{3}.$$

Theorem. ([Ô] と同様) $\mathbf{Z}[\zeta_8]$ において，次の合同式が成り立つ：

$$A_\lambda \equiv -\frac{1}{2}\, C_{\frac{3(\ell-1)}{4}} \bmod \ell.$$

$\Big($ [Asai] の表との比較では $\frac{1}{2} A_\lambda \equiv -\frac{1}{4}\, C_{\frac{3(\ell-1)}{4}} \bmod \ell$ $\Big)$

Remark. $\mathbf{Z}[\zeta_8]$ は Euclid 環である．上の合同式で，右辺の絶対値最小剰余を採れば，それが左辺の真の値と一致することは確実である．

Proof of the congruence (1)

Recall

$$\Lambda := \varphi\left(\frac{1}{\lambda}\right),\ \ \tilde{\lambda} := \prod_{r\in S}\varphi\left(\frac{r}{\lambda}\right) \equiv \Lambda^{\frac{\ell-1}{4}} \bmod \Lambda^{\frac{\ell-1}{4}+1},\ \ \tilde{\lambda}^4 = \left(\frac{-1}{\lambda}\right)_4 \lambda.$$

Let g be a generator of the cyclic group $\left(\mathbf{Z}[\boldsymbol{i}]/(\lambda)\right)^\times$. Write $\chi_\lambda = \chi$ for simplicity.

$$\mathrm{egs}(\lambda) = \sum_{j=0}^{\frac{\ell-3}{2}} \chi(g^j)\,\mathrm{cl}(g^j u)\Big|_{u=(1-\boldsymbol{i})\varpi\frac{1}{\lambda}} = \sum_{j=0}^{\frac{\ell-3}{2}} \chi(g^j)\,\mathrm{cl}\left(g^j \sum_{n=0}^{\infty}(-1)^n\binom{-\frac{1}{2}}{n}\frac{t^{4n+1}}{4n+1}\right)\Big|_{t=\Lambda} \qquad \left(t=\mathrm{sl}(u)\right)$$

$$= \sum_{j=0}^{\frac{\ell-3}{2}} \chi(g^j) \sum_{m=0}^{\infty} C_{2m}\left(g^j \sum_{n=0}^{\infty}(-1)^n\binom{-\frac{1}{2}}{n}\frac{t^{4n+1}}{4n+1}\right)^{2m}\Big|_{t=\Lambda}$$

$$= \sum_{m=0}^{\infty}\left(\sum_{j=0}^{\frac{\ell-3}{2}} \chi(g^j)\, g^{2jm}\right) C_{2m}\left(\sum_{n=0}^{\infty}(-1)^n\binom{-\frac{1}{2}}{n}\frac{t^{4n+1}}{4n+1}\right)^{2m}\Big|_{t=\Lambda}.$$

この式を $\bmod \Lambda^{\frac{3(\ell-1)}{4}+1}$ で観察すると

$$\equiv \sum_{m=0}^{\frac{3(\ell-1)}{8}}\left(\sum_{j=0}^{\frac{\ell-3}{2}} \chi(g^j)\, g^{2jm}\right) C_{2m}\left(\sum_{n=0}^{\infty}(-1)^n\binom{-\frac{1}{2}}{n}\frac{t^{4n+1}}{4n+1}\right)^{2m}\Big|_{t=\Lambda} \bmod \left(\Lambda^{\frac{3(\ell-1)}{4}+1}\right)$$

$$\equiv \sum_{m=0}^{\frac{3(\ell-1)}{8}}\left(\sum_{j=0}^{\frac{\ell-3}{2}} g^{\frac{j(\ell-1)}{4}}\, g^{2jm}\right) C_{2m}\left(\sum_{n=0}^{\infty}(-1)^n\binom{-\frac{1}{2}}{n}\frac{t^{4n+1}}{4n+1}\right)^{2m}\Big|_{t=\Lambda} \bmod \left(\Lambda^{\frac{3(\ell-1)}{4}+1}\right)$$

$$\equiv \sum_{m=0}^{\frac{3(\ell-1)}{8}}\left(\sum_{j=0}^{\frac{\ell-3}{2}} g^{j\left(\frac{\ell-1}{4}+2m\right)}\right) C_{2m}\left(\sum_{n=0}^{\infty}(-1)^n\binom{-\frac{1}{2}}{n}\frac{t^{4n+1}}{4n+1}\right)^{2m}\Big|_{t=\Lambda} \bmod \left(\Lambda^{\frac{3(\ell-1)}{4}+1}\right).$$

Proof of the congruence (2)

ここで

$$\sum_{j=0}^{\frac{\ell-3}{2}} g^{j\left(\frac{\ell-1}{4}+2m\right)} = \begin{cases} 0 & \text{if } (\ell-1) \nmid \left(\frac{j(\ell-1)}{4}+2m\right), \\ \frac{\ell-1}{2} & \text{if } (\ell-1) \mid \left(\frac{j(\ell-1)}{4}+2m\right), \end{cases} \quad 0 \le 2m \le \frac{3(\ell-1)}{4}$$

であるから, 前 slide の $2m = \frac{3(\ell-1)}{4}$ の箇所以外は消える. よつて

$$\equiv \frac{\ell-1}{2} C_{\frac{3(\ell-1)}{4}} \cdot \left(\sum_{n=0}^{\infty} (-1)^n \binom{-\frac{1}{2}}{n} \frac{t^{4n+1}}{4n+1} \right)^{\frac{3(\ell-1)}{4}} \Bigg|_{t=\Lambda} \bmod \left(\Lambda^{\frac{3(\ell-1)}{4}+1}\right)$$

$$\equiv \frac{\ell-1}{2} C_{\frac{3(\ell-1)}{4}} \cdot \Lambda^{\frac{3(\ell-1)}{4}} \bmod \left(\Lambda^{\frac{3(\ell-1)}{4}+1}\right).$$

これより

$$\mathrm{egs}(\lambda) \equiv A_\lambda \Lambda^{\frac{3(\ell-1)}{4}} \equiv \frac{\ell-1}{2} C_{\frac{3(\ell-1)}{4}} \cdot \Lambda^{\frac{3(\ell-1)}{4}} \bmod \left(\Lambda^{\frac{3(\ell-1)}{4}+1}\right)$$

がわかり, 次を得る :

$$A_\lambda \equiv -\frac{1}{2} C_{\frac{3(\ell-1)}{4}} \bmod \left((\Lambda) \cap \mathbf{Z}[\zeta_8]\right).$$

([Asai] の表との比較では $\frac{1}{2} A_\lambda \equiv -\frac{1}{4} C_{\frac{3(\ell-1)}{4}} \bmod \left((\Lambda) \cap \mathbf{Z}[\zeta_8]\right)$)

A_λ の “整数性” (Asai の定理) によつて $\bmod \ell$ の合同式が得られる.
計算実験では絶対値に関する最小剰余が [Asai] の表と完全に一致する.

An analogue of the congruence numbers (1)

Koblitz の本に, 次の様な事実が述べられてゐる.

Theorem. $n \in \mathbf{Z}$ に対し, 楕円曲線 $\mathscr{E}_{n^2} : y^2 = x^3 - n^2 x$ を考へる.
次の 3 つは同値 :

(1) $\exists u, \exists v \in \mathbf{Q}$ such that $n^2 = u^4 - v^2$,

(2) n は合同数,

(3) $\operatorname{rank} \mathscr{E}_{n^2}(\mathbf{Q}) > 0$.

An analogue of the congruence numbers (2)

$\ell \equiv 1 \bmod 8$: 素数. $\ell = \lambda\overline{\lambda}$, $\lambda \equiv 1 \bmod (1+\boldsymbol{i})^3$.
簡易的な数値実験によると, 上の定理 (Koblitz の本) の次の様な類似が成り立つと思はれる.

Conjecture. (合同数の類似) 1 次の Gauss 素数 λ は

$$(\bigstar) \qquad \lambda = -\alpha^4 + \beta^2 \boldsymbol{i}, \quad (\alpha,\ \beta \in \mathbf{Q}(\boldsymbol{i}))$$

と書けるとき，かつその時に限り $\mathrm{egs}(\lambda) = 0$.

Remark. λ が ($\bigstar$) の型 $\Rightarrow$ $\ell = \lambda\overline{\lambda} \equiv 1 \mod 8$.

[Asai] の表の範囲では成立してゐる.
[Asai] の表で $\mathrm{egs}(\lambda) = 0$ となる λ のうち $\lambda\overline{\lambda} = 4817$ 以外は $\alpha, \beta \in \mathbf{Z}[\boldsymbol{i}]$ と取れる.
$\lambda = -\alpha^4 + \beta^2 \boldsymbol{i}$ について $(x, y) = (\alpha^2 \boldsymbol{i}, \pm\alpha\beta)$ は, $\mathscr{E}_\lambda$ の (Gauss 数体上の) 有理点. 実際,

$$x^3 - \lambda x = -\alpha^6 \boldsymbol{i} - (-\alpha^4 + \beta^2 \boldsymbol{i})\,\alpha^2 \boldsymbol{i} = (\beta\,\alpha)^2 = y^2.$$

これは, 無限位数である.
(Nagell-Lutz の定理（論法）より $\mathscr{E}_\lambda(\mathbf{Q}(\boldsymbol{i}))$ の torsion 部分は $\{(0,0), \infty\}$.)

BSD 予想と EGS

ここまでの状況について, EGS の言葉で BSD を書けば

$$\operatorname{rank} \mathscr{E}_\lambda(\mathbf{Q}(\boldsymbol{i})) > 0 \iff \lambda = -\alpha^4 + \beta^2 \boldsymbol{i} \text{ 型} \overset{?}{\Longleftarrow}\!\!\Rightarrow \operatorname{egs}(\lambda) = 0.$$

An example

Example. $\lambda = 41 + 56i$, $\ell = \lambda\overline{\lambda} = 4817$ のとき,

$$\alpha = \frac{\boldsymbol{i}(1+2\boldsymbol{i})(2+3\boldsymbol{i})}{3}, \quad \beta = \frac{\boldsymbol{i}\,7(1+\boldsymbol{i})(2+\boldsymbol{i})(4+\boldsymbol{i})}{3^2}$$

とすれば $\lambda = -\alpha^4 + \beta^2\boldsymbol{i}$ である. MAGMA によると, この場合の $\mathscr{E}_\lambda$ の Modell-Weil rank は 2 と予測されてゐるらしく, その場合は $(\alpha^2, \pm\alpha\beta)$ が $\mathbf{Z}[i]$ 加群としての生成元になると思はれる.

Remark.

$$L(s,\tilde{\chi})\,L(s,\overline{\tilde{\chi}}) = L_{\mathscr{E}_\lambda/\mathbf{Q}(\boldsymbol{i})}(s)$$

であるので, BSD 予想の下で, MW-rank of $\mathscr{E}_\lambda$ over $\mathbf{Q}(\boldsymbol{i})$ は偶数である.
[Asai] の表にあるものについての MAGMA の返答は, どれも MW-rank は 2,
つまり $\mathbf{Z}[i]$ 加群としての rank は 1 になつてゐる.

消えるEGSとKummer型合同式

次の様な現象が観測できたので記録しておく.

$$\mathrm{cl}(u) = 1 + \sum_{j=2}^{\infty} G_{2j} \frac{u^{2j}}{(2j)!} \quad \left(C_{2j} = \frac{G_{2j}}{(2j)!} \right)$$

で係数 G_{2j} を定義する.

楕円曲線 $y^2 = x^3 - x$ の p における Hasse invariant を A_p とおく:

$$A_p = \text{“}(x^3 - x)^{\frac{p-1}{2}} \text{ の } x^{p-1} \text{ の係数”.}$$

$\mathrm{egs}(\lambda) = 0$ であるためには,

$$\ell \,\Big|\, G_{\frac{3}{4}(\ell-1)}$$

が成り立つことが必要十分であることは,

ほとんど ($|\mathrm{egs}(\lambda)|$ の $\ell \to \infty$ に際しての漸近的な挙動が小さいことを除いて, の意)

証明できてゐる.

`PARI/gp` を使つての数値実験によると, さらに次が成り立つと思はれる.

EGS and Kummer-type congruences

Conjecture. (EGS v.s. Kummer 型合同式)

第 1 節の記号を使ふ．次の 8 つの条件は同値．

(1) $\mathrm{egs}(\lambda) = 0$.

(2) $\ell \mid G_{\frac{3}{4}(\ell-1)}$.

(3) $\ell \mid G_{\frac{7}{4}(\ell-1)}$.

(4) ある整数 $a \geq 0$ について $\ell \,\Big|\, \dfrac{G_{\frac{3}{4}(\ell-1)+a(\ell-1)}}{\frac{3}{4}(\ell-1)+a(\ell-1)}$.

(5) 任意の整数 $a \geq 0$ について $\ell \,\Big|\, \dfrac{G_{\frac{3}{4}(\ell-1)+a(\ell-1)}}{\frac{3}{4}(\ell-1)+a(\ell-1)}$.

(6) 次の合同式が成り立つ：

$$A_\ell \frac{G_{\frac{3}{4}(\ell-1)}}{\frac{3}{4}(\ell-1)} - \frac{G_{\frac{7}{4}(\ell-1)}}{\frac{7}{4}(\ell-1)} \equiv 0 \mod \ell.$$

(7) (6) を大袈裟にして (つまり (6) は次式の $a=1$ の場合), ある自然数 $a < \frac{3}{4}(p-1)$ に対して

$$\sum_{r=0}^{a} \binom{a}{r} (-A_\ell)^{a-r} \frac{G_{\frac{3}{4}(\ell-1)+r(\ell-1)}}{\frac{3}{4}(\ell-1)+r(\ell-1)} \equiv 0 \mod \ell^a.$$

(8) 任意の自然数 $a < \frac{3}{4}(p-1)$ について (7) の式が成り立つ．

((7) と (8) については講演後の西来路氏にご指摘いただき修正.)

Some observation

ζ を 1 の原始 $\ell-1$ 乗根 $(\in \mathbf{Z}_\ell)$ とし,

$$\mathrm{Cl}(\ell,u)=\sum_{j=0}^{\ell-1}\chi_\lambda(\zeta^j)\mathrm{cl}(\zeta^j u)$$

とおく. $\chi_\lambda(\zeta)=\zeta^{-\frac{3}{4}(\ell-1)}\in\{\pm 1,\ \pm \boldsymbol{i}\}$ であることに注意. このとき

$$\mathrm{Cl}(\ell,u)=\ell\sum_{a=0}^{\infty}G_{\frac{3}{4}(\ell-1)+a(\ell-1)}\frac{u^{\frac{3}{4}(\ell-1)+a(\ell-1)}}{\left(\frac{3}{4}(\ell-1)+a(\ell-1)\right)!}$$

となる. これを使ふと, 次の言ひ換へができるが, …

$$\mathrm{egs}(\lambda)=0 \iff \left(\left(\frac{\partial}{\partial u}\right)^{\ell}-A_\ell\frac{\partial}{\partial u}\right)^{a}\left(\frac{\mathrm{Cl}(\ell,u)}{u}\right)\equiv 0 \bmod \ell^{a+1}.$$

しかし $\dfrac{\mathrm{Cl}(\ell,u)}{u}$ には違和感を感じる.

[Ô] : Generalized Bernoulli-Hurwitz numbers and the universal Bernoulli numbers, Russian Math. Surveys 66(2011)871-932