Vanishing Elliptic Gauss Sums and Bernoulli-Hurwitz Type Numbers

(joint work with Fumio Sairaiji)

by Yoshihiro Ônishi at Meijo Univ.

RIMS 研究集会「代数的整数論とその周辺」

9th December, 2019

Contents

Main references

- Asai, T. : *Elliptic Gauss sums and Hecke L-values at $s = 1$*, RIMS Kôkyũroku Bessatsu, **4**(2007). [Asai]
- Birch,B.J. and Swinnerton-Dyer,H.P.F. : *Notes on elliptic curves II*, Crelle, **218**(1965). [BSD]
- Ônishi, Y. : *Congruence relations connecting Tate-Shafarevich groups with Hurwitz numbers*, Interdisciplinary Information Sciences, **16**(2010). [Ô]
- 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).
- Hurwitz, A. : *Über die Anzahl der Klassen binärer quadratischer Formen von negativer Determinante*, Acta Math., **19**(1985). [H]

  (The last reference was informed by G. Yamashita after the talk.)

Introduction

Theorem. (Hurwitz [H]) 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 absolutely smallest 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.

We give an analogy for Tate-Shafarevich groups of this theorem.

Elliptic Gauss sums were already used, in order to compute numerically the L-series attached to some elliptic curves over $\mathbf{Q}$, in the famuous original paper [BSD] by Birch and Swinnerton-Dyer themselves. We wish to use them for investigation of L-series attached to some elliptic curves defined over $\mathbf{Q}(i)$.

The lemniscatic sine function

The inverse function $u \mapsto t$ of

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

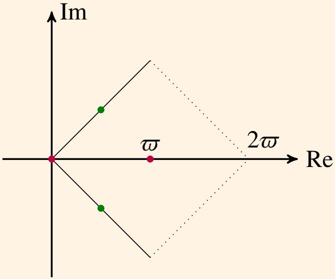
is the lemniscatic sine function, which is denoted by $t = \mathrm{sl}(u)$.

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

$\mathrm{sl}(u)$ is an elliptic function whose period lattice is $\Omega = (1-\boldsymbol{i})\,\varpi\,\mathbf{Z}[\boldsymbol{i}]$

and its divisor modulo Ω is

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



It is expanded as

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

The ray class field

Through out this talk, we denote $\varphi(u) = \mathrm{sl}\,(\,(1-\boldsymbol{i})\,\varpi\,u\,)$.

(The period lattice of this function is $\mathbf{Z}[\boldsymbol{i}]$.)

Take a prime $\ell \equiv 1 \bmod 4, \in \mathbf{Z}$. $\ell = \lambda\bar{\lambda}$ with $\lambda \equiv 1 \bmod (1+\boldsymbol{i})^3$.

Let $S \subset \mathbf{Z}[\boldsymbol{i}]$ be a fixed set such that

$(\mathbf{Z}[\boldsymbol{i}]/(\lambda))^\times \simeq S \cup -S \cup \boldsymbol{i}S \cup -\boldsymbol{i}S$, $|S| = \frac{\ell-1}{4}$. Moreover we define

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

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

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

Then, we have

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

Note that $\mathbf{Q}(\boldsymbol{i}, \Lambda)$ is the ray class field over $\mathbf{Q}(\boldsymbol{i})$ of conductor $(1+\boldsymbol{i})^3(\lambda)$.

(T. Takagi [1920], §32) (Remind that $\left(\mathbf{Z}[\boldsymbol{i}]/(1+\boldsymbol{i})^3\right)^\times \simeq \{\pm 1, \pm\boldsymbol{i}\}$.)

Asai's theorem for $\ell \equiv 13 \bmod 16$ (Typical case)

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

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

Since the terms of this summation are alg. integers, $\mathrm{egs}(\lambda)$ is an alg. integer.

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

$$\mathrm{egs}(\lambda) = A_\lambda\,\tilde{\lambda}^3, \qquad \left(\tilde{\lambda} = \gamma(S)^{-1}\prod_{r\in S}\varphi\left(\tfrac{r}{\lambda}\right)\right).$$

In particular, $\mathrm{egs}(\lambda) \neq 0$.

Proof. Use the functional equation for the Hecke L-series corresponding to χ_λ and the formula of Cassels-Matthews for classical quartic Gauss sum. □

—. Note that BSD $\Longrightarrow$ Rationality of EGS $\Longrightarrow$ Cassels-Matthews.

—. We call A_λ the coefficient of $\mathrm{egs}(\lambda)$. (Asai)

—. In the definition of $\mathrm{egs}(\lambda)$, if we replace χ_λ by another character χ such that $\chi(\boldsymbol{i}) = \boldsymbol{i}$, then the sum trivially vanishes.
Each character χ "knows" which elliptic function corresponds to itself.

The corresponding Hecke L-series

$\ell \equiv 13 \bmod 16$ Keeping in mind that $\left(\mathbf{Z}[\boldsymbol{i}]/(1+\boldsymbol{i})^2\right)^\times \simeq \{1,\ \boldsymbol{i}\}$, we define

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

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

This is a Hecke character of conductor $\left(\lambda(1+\boldsymbol{i})^2\right)$.

Theorem. ([Asai])

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

The elliptic curve corresponding to $L(s, \tilde{\chi})$ is $\mathscr{E}_{-\lambda} : y^2 = x^3 + \lambda x$.

Deuring showed that

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

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

Some Congruence on the Coefficients of EGS

We define $C_j \in \mathbf{Q}$ by the expansion of $u \mapsto \mathrm{sl}(u)$ as follows:

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

Theorem. ([Ô]) Assuming $\ell \equiv 13 \mod 16,$ we have

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

The absolutely minimal residue of the RHS is exactly the LHS. (?)

This is a generalization of the following :

Theorem. (revisited) For any prime $p > 3$, we have

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

Summary up to here

$\boxed{\ell \equiv 13 \bmod 16}$ The corresponding elliptic curve is

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

and $L(1, \tilde{\chi}) \neq 0$. Coates-Wiles' theorem implies that

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

$\boxed{\ell \equiv 5 \bmod 16}$ We have a similar story.
The corresponding ellipitic curve is

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

and, similarly, it has $\operatorname{rank} \mathcal{E}_{\frac{1}{4}\lambda}\left(\mathbf{Q}(\boldsymbol{i})\right) = 0$.

We proceed to the other case :

$\boxed{\ell \equiv 1 \bmod 8}$. About 18% of the 172 examples of this case in [Asai],

$$\operatorname{egs}(\lambda) = 0.$$

$\ell \equiv 1 \bmod 8$ case

ε always denotes an element in $\{\pm 1, \pm \boldsymbol{i}\}$.

Define χ_0 by

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

$\ell \equiv 1 \bmod 16$ Since $\chi_\lambda(\boldsymbol{i}) = 1$, we define $\chi_1 = \chi_\lambda \chi_0$.

Then $\tilde{\chi}((\alpha)) = \chi_1(\alpha)\,\overline{\alpha}$ is a Hecke character of conductor $(\lambda(1+\boldsymbol{i})^3)$.

We have

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

Here, $\operatorname{egs}(\lambda)$ is defined in the next page.

$\ell \equiv 9 \bmod 16$ Since $\chi_\lambda(\boldsymbol{i}) = -1$, we define $\chi_1 = \chi_\lambda \overline{\chi_0}$.

Then $\tilde{\chi}((\alpha)) = \chi_1(\alpha)\,\overline{\alpha}$ is a Hecke character of conductor $(\lambda(1+\boldsymbol{i})^3)$.

We have

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

Here $\operatorname{egs}(\lambda)$ is defined in the next page.

The elliptic Gauss sum

Our situation: $\ell \equiv 1 \bmod 8$ is a prime, and

$$\ell = \lambda\bar{\lambda}, \quad \lambda \equiv 1 \bmod (1+\boldsymbol{i})^3, \ \chi_\lambda(\nu) = \left(\frac{\nu}{\lambda}\right)_4, \ \chi_\lambda(\boldsymbol{i}) = \boldsymbol{i}^{\frac{\ell-1}{4}} = \pm 1.$$

Using $\mathrm{cl}(u) = \mathrm{sl}\left(u + \frac{\varpi}{2}\right)$, we define $\psi(u) = \mathrm{cl}\left((1-\boldsymbol{i})\,\varpi u\right)$ and the elliptic Gauss sum by

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

Then we have (revisited)

Proposition. ([Asai])

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

The coefficients of EGS

For the coefficients, we recall the following

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

ℓ mod 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	$\boldsymbol{i}\zeta_8 \cdot a_\lambda$	$\zeta_8 \cdot a_\lambda$	$\boldsymbol{i}\sqrt{2} \cdot a_\lambda$	$\sqrt{2} \cdot a_\lambda$

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

Proof.

Use the formula of Cassels-Matthew and the functional equation of $L(s, \tilde{\chi})$. □

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

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

$\boxed{\ell = 8n + 1 = \lambda\bar{\lambda}}$ The Hecke L-series associated to $\mathrm{egs}(\lambda)$ is a factor of the L-series of the elliptic curve

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

The conductor of this is $\left((1+\boldsymbol{i})^3\lambda\right)^2$ (See [Serre-Tate], Thm.12),
and the reduction type at $(1+\boldsymbol{i})$ is of type III,
and that at λ is of type $\mathrm{I}_2{}^*$.
Each Tamagawa number $\tau_{\mathfrak{p}}$ and $A_\lambda =$ "the coeff. of $\mathrm{egs}(\lambda)$" are as follows :

ℓ mod 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 $a_\lambda \in 2\,\mathbf{Z}$.

It is quite certain that $\left(\frac{1}{2}\,a_\lambda\right)^2 = \sharp\,\text{Ш}(\mathscr{E}_\lambda)$ if $a_\lambda \neq 0$.

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

We define the C_{2j}s by the expansion of the lemniscateic cosine $u \mapsto \mathrm{cl(u)}$ as

$$\mathrm{cl}(u) = 1 + \sum_{j=2}^{\infty} C_{2j} u^{2j} = 1 - u^2 + \frac{1}{2}u^4 - \frac{3}{10}u^6 + \frac{7}{40}u^8 - \cdots .$$

For the sake of simplicity, we restrict the case $\ell \equiv 1 \bmod 16$, and assume, as before, that

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

Take a set S such that $(\mathbf{Z}[\boldsymbol{i}]/(\lambda))^{\times} = S \cup -S \cup \boldsymbol{i}S \cup -\boldsymbol{i}S$ and $|S| = \frac{\ell-1}{4}$.

Since $\chi_{\lambda}(\nu) \equiv \nu^{\frac{\ell-1}{4}} \bmod \ell$, we see $\chi(\boldsymbol{i}) = 1$.

Define $\psi(u) = \mathrm{cl}((1-\boldsymbol{i})\varpi u)$. According to [Asai],

$$\mathrm{egs}(\lambda) := \sum_{\nu \in S \cup \boldsymbol{i}S} \chi_{\lambda}(\nu)\, \psi\left(\frac{\nu}{\lambda}\right) = A_{\lambda}\, \tilde{\lambda}^3 \quad \text{with } A_{\lambda} \in \mathbf{Z}[\zeta_8].$$

Theorem. (alternative of [Ô]) In $\mathbf{Z}[\zeta_8]$, we have

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

Remark. $\mathbf{Z}[\zeta_8]$ is Euclidian. It is quite prospective that the absolute minimal residue of the RHS gives the exact value of A_{λ}.

Proof of the congruence (in a few words) (1/2)

Recall

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

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

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

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

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

Concerning $\bmod \Lambda^{\frac{3(\ell-1)}{4}+1}$, we see

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

$$\searrow \quad = \sum_{j=0}^{\frac{\ell-3}{2}} g^{\frac{j(\ell-1)}{4}}\, g^{2jm} = \sum_{j=0}^{\frac{\ell-3}{2}} g^{\,j\left(\frac{\ell-1}{4}+2m\right)}$$

Proof of the congruence (in a few words) (2/2)

Because of

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

the terms in the previous page vanish unless $2m = \frac{3(\ell-1)}{4}$. Therefore,

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

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

This implies

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

and, at last, we have :

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

The rationality of A_λ (Asai's theorem) yields the congruence $\bmod\ \ell$.

The absolutely minimal residues of the RHS in numerical check coincide with the values in the table of [Asai].

An analogue of the congruence numbers (1/2)

The following is well-known : (see, for example, Koblitz' GTM book)

Theorem. Let $n \in \mathbf{Z}$. For the elliptic curve $\mathscr{E}_{n^2} : y^2 = x^3 - n^2 x$

the following three are equivalent each other:

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

(2) n is a conguence number,

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

Some numerical calculation suggests the following analogue:

Conjecture. (Gaussian congruence numbers)

Let λ be a first degree Gaussian prime such that $\lambda \equiv 1 \bmod (1+\boldsymbol{i})^3$.

There exist $\alpha,\ \beta \in \mathbf{Q}(\boldsymbol{i})$ satisfying

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

if and only if $\mathrm{egs}(\lambda) = 0$.

—. All the examples in [Asai] satisfy this conjecture.

—. In the examples of [Asai] such that $\mathrm{egs}(\lambda) = 0$, except $\lambda\overline{\lambda} = 4817$, we can take $\alpha,\ \beta \in \mathbf{Z}[\boldsymbol{i}]$.

—. If $\lambda = -\alpha^4 + \beta^2\, \boldsymbol{i}$, the point $(x, y) = (\alpha^2\, \boldsymbol{i},\ \pm\alpha\beta)$ is on $\mathscr{E}_\lambda(\mathbf{Q}(\boldsymbol{i}))$. Indeed

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

This is a non-torsion point.

(From Nagell-Lutz argumant, we see the torsion part of $\mathscr{E}_\lambda(\mathbf{Q}(\boldsymbol{i}))$ is $\{(0,0), \infty\}$.)

BSD Conjecture and EGS

We summerize the result up to here :

$$\lambda \text{ is of the form } -\alpha^4 + \beta^2 \boldsymbol{i} \iff \operatorname{rank} \mathscr{E}_\lambda(\mathbf{Q}(\boldsymbol{i})) > 0$$

$$\overset{?}{\iff} L(1, \tilde{\chi}) = 0$$

$$\iff \operatorname{egs}(\lambda) = 0.$$

An example

Example. Take $\lambda = 41 + 56\,\boldsymbol{i}$, $\ell = \lambda\bar{\lambda} = 4817$.

Then $\lambda = -\alpha^4 + \beta^2\boldsymbol{i}$, where

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

`MAGMA` says that the Mordell-Weil rank of $\mathscr{E}_\lambda$ is 2.

The Mordell-Weil group is probably a rank one $\mathbf{Z}[\boldsymbol{i}]$-module generated by $(\alpha^2,\ \pm\alpha\beta)$.

Remark. Since

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

the analytic rank of $\mathscr{E}_\lambda/\mathbf{Q}(\boldsymbol{i})$ is even.

This is consistent with that the MW-group of $\mathscr{E}_\lambda$ over $\mathbf{Q}(\boldsymbol{i})$ is a $\mathbf{Z}[\boldsymbol{i}]$-module.

`MAGMA` says that all cases in the table in [Asai] are of MW-rank two.

Vanishing EGS and Kummer-type congruence

We define $G_{2j} \in \mathbf{Z}$ by

$$\mathrm{cl}(u) = 1 + \sum_{j=2}^{\infty} G_{2j} \frac{u^{2j}}{(2j)!} \quad (\text{ Hurwitz coefficients of } \mathrm{cl}(u) \text{ })$$

$$= 1 - u^2 + 6\frac{u^4}{4!} - 216\frac{u^6}{6!} + 882\frac{u^8}{8!} - 368928\frac{u^{10}}{10!} + \cdots .$$

We denote by H_ℓ the Hasse invarinat of $y^2 = x^3 - x$ at $\ell\ (\equiv 1 \bmod 4)$:

$$H_\ell = (-1)^{(\ell-1)/4} \binom{\frac{\ell-1}{2}}{\frac{\ell-1}{4}} = \lambda + \overline{\lambda}.$$

We see $\mathrm{egs}(\lambda) = 0$ is equivalent to

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

if the behavior of $|\mathrm{egs}(\lambda)|$ w.r.t. $\ell \to \infty$ is quite small.

Indeed, the estimation for the egs coefficient $|A_\lambda| < \ell^{1/4}$ is hopeful.

(This last sentence and the next page included typos pointed out by Sairaiji after the talk and now are corrected.)

EGS and Kummer-type congruences

The following theorem was proved by Fumio Sairaiji, which had been a conjecture untill a few months ago.

Theorem. (EGS and congruences of Kummer-type)

Assume that the expected estimation $|A_\lambda| < \ell^{1/4}$ holds.

The following three are equivalent:

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

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

(3) For any $0 \le a < \ell$, we have

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

Moreover, under the same assumption, we can show that for $0 \le a < \nu\ell$

(4)
$$\sum_{r=0}^{a} \binom{a}{r} (-H_\ell)^{a-r} \frac{G_{\frac{3}{4}(\ell-1)+r(\ell-1)}}{\frac{3}{4}(\ell-1)+r(\ell-1)} \equiv 0 \bmod \ell^{\,a-\nu+2}$$

if and only if $\mathrm{egs}(\lambda) = 0$.

Idea of the proof

Taking an $(\ell-1)$th root ζ of 1 in $\mathbf{Z}_\ell$, we define

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

Note that $\chi_\lambda(\zeta) = \zeta^{-\frac{3}{4}(\ell-1)} \leftrightarrow \{\pm 1, \pm \boldsymbol{i}\}$.

Then we have $\mathrm{Cl}\left(\mathrm{sl}^{-1}(\Lambda)\right) = \mathrm{egs}(\lambda)$ and

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

We see that the last statement (3) of the theorem is equivalent to the Hurwitz coefficient of degree $\frac{3}{4}(\ell-1)$ of

$$\left(\left(\frac{\partial}{\partial u}\right)^{\ell-1} - H_\ell\right)^a \left(\frac{\mathrm{Cl}(u)}{u}\right)$$

belongs to $\ell^{a+1}\,\mathbf{Z}_\ell$.

Sketch of the proof

We show (1) $\Longrightarrow$ (3) (and (4)), which is the most difficult part of the proof.

So, we assume $\mathrm{egs}(\lambda) = 0$.

We identify the completion $\mathbf{Z}[\boldsymbol{i}]_\lambda$ with $\mathbf{Z}_\ell$.

$\mathbf{LT}$: Lubin-Tate formal group over $\mathbf{Z}_\ell$ corresponding to λ-plication $x \mapsto \lambda x + x^\ell$.

$f_0(x)$: the formal log of $\mathbf{LT}$.

$\widehat{\mathbf{sl}}$: the formal group defined by $t_1 \dotplus t_2 = \mathrm{sl}\left(\mathrm{sl}^{-1}(t_1) + \mathrm{sl}^{-1}(t_2)\right)$ over $\mathbf{Z}_\ell$.

Since $\ell - H_\ell T + T^2 = (\lambda - T)(\overline{\lambda} - T)$ is a special element of $\widehat{\mathbf{sl}}$,

we have a strong isomorphism

$$\begin{array}{rcl} \iota : \mathbf{LT} & \longrightarrow & \widehat{\mathbf{sl}} \\ x & \longmapsto & \iota(x) = t = \varphi(u) \\ \exists\, \eta & \longmapsto & \iota(\eta) = \Lambda = \varphi\left(\dfrac{1}{\lambda}\right). \end{array}$$

So that $\eta^\ell = -\lambda$.

Since $\mathrm{Cl}\left(\mathrm{sl}^{-1}(t)\right) \in \mathbf{Z}_\ell[[t]]$, $\mathrm{Cl}\,(f_0(x)) \in \mathbf{Z}_\ell[[x]]$.

(continuation)

We want to show the terms of degree up to $\ell(\ell-1)$ of

$$\frac{\mathrm{Cl}(u)}{u} = \frac{\mathrm{Cl}(\mathrm{sl}^{-1}(t))}{\mathrm{sl}^{-1}(t)}$$

are in $\ell\,\mathbf{Z}_\ell$, because this and a theorem of Hochschild yield

$$\left(\begin{array}{l} \text{The term(s) of degree (less than or equal to)} \\ \frac{3}{4}(\ell-1) \text{ in } t\text{-expansion of } \left(\left(\frac{d}{du}\right)^{\ell-1} - H_\ell \right)^a \frac{\mathrm{Cl}(u)}{u} \end{array} \right) \in \ell^{a+1}\mathbf{Z}_\ell[[t]] \subset \ell^{a+1}\mathbf{Z}_\ell\langle\!\langle u \rangle\!\rangle$$

provided $\frac{3}{4}(\ell-1) + a(\ell-1) < \ell(\ell-1)$.

However, since $\widehat{\mathbf{sl}}$ is strongly isomorphic to $\mathbf{LT}$, it is sufficient to check leading terms of

$$\frac{\mathrm{Cl}(f_0(x))}{f_0(x)}.$$

Since $0 = \mathrm{egs}(\lambda) = \mathrm{Cl}(\mathrm{sl}^{-1}(\Lambda))$ and then, $\mathrm{Cl}(f_0(\zeta^j\eta)) = 0$ for $1 \le j \le \ell-1$ as well,

we have $0 = \mathrm{Cl}(f_0(\zeta^j\eta))$ and then, $\mathrm{Cl}(f_0(x))$ is divisible by $\lambda x + x^\ell = x\prod_{j=1}^{\ell-1}(x - \zeta^j\eta)$.

Hence we shall check leading terms of

$$\frac{\mathrm{Cl}(u)}{u} = \frac{\mathrm{Cl}(f_0(x))/(\lambda x + x^\ell)}{f_0(x)/(\lambda x + x^\ell)} = \lambda\,\frac{\mathrm{Cl}(f_0(x))}{f_0(x)} \cdot \frac{\lambda x + x^\ell}{\lambda\, f_0(x)}, \quad \text{namely, of } \frac{\lambda x + x^\ell}{\lambda\, f_0(x)}.$$

(continuation)

To get (4), we take a $\nu \in \mathbf{N}$ and fix it. Thanks to $f_0(\zeta x) = \zeta f_0(x)$, we shall let

$$f_0(x) = \sum_{j=0}^{\infty} \frac{b_{1+j(\ell-1)}}{1+j(\ell-1)} x^{1+j(\ell-1)} = x + \frac{b_\ell}{\ell} x^\ell + \cdots \quad (b_{1+j(\ell-1)} \in \mathbf{Z}_\ell).$$ It is shown $b_\ell \in (\mathbf{Z}_\ell)^\times$.

There exists a polynomial $h(x) \in \mathbf{Z}_\ell[x]$ such that

$$\frac{\lambda x + x^\ell}{\lambda f_0(x)} \equiv 1 + \left(\frac{b_\ell}{\ell}\right)^\nu x^{\nu\ell(\ell-1)} + \frac{1}{\ell^{\nu-1}} h(x) \ \text{mod.deg}\ (\nu\ell(\ell-1)+1).$$

Hence $\dfrac{\mathrm{Cl}(f_0(x))}{\lambda x + x^\ell} \cdot \dfrac{\lambda x + x^\ell}{\lambda f_0(x)}$ has the same property.

So that, any coefficients of terms of degree $< \nu\ell(\ell-1)$ of

$$\frac{\mathrm{Cl}(u)}{u} = \frac{\mathrm{Cl}(f_0(x))/(\lambda x + x^\ell)}{f_0(x)/(\lambda x + x^\ell)} = \lambda \frac{\mathrm{Cl}(f_0(x))}{f_0(x)} \cdot \frac{\lambda x + x^\ell}{\lambda f_0(x)}$$ belongs to $\dfrac{1}{\ell^{\nu-2}} \mathbf{Z}_\ell$.

We finally have

$$\ell^{\nu-2} \sum_{r=0}^{a} \binom{a}{r} (-H_\ell)^{a-r} \frac{G_{\frac{3}{4}(\ell-1)+r(\ell-1)}}{\frac{3}{4}(\ell-1)+r(\ell-1)} \equiv 0 \mod \ell^a$$

for any $a > 0$ satisfying $\frac{3}{4}(\ell-1) + a(\ell-1) < \nu\ell(\ell-1)$, namely, for $0 < a < \nu\ell$.

Therefore,

$$\sum_{r=0}^{a} \binom{a}{k} (-H_\ell)^{a-r} \frac{G_{\frac{3}{4}(\ell-1)+r(\ell-1)}}{\frac{3}{4}(\ell-1)+r(\ell-1)} \equiv 0 \mod \ell^{a-\nu+2}.$$

Some Observation

(the last formula)

$$\sum_{r=0}^{a} \binom{a}{r} (-H_\ell)^{a-r} \frac{G_{\frac{3}{4}(\ell-1)+r(\ell-1)}}{\frac{3}{4}(\ell-1)+r(\ell-1)} \equiv 0 \mod \ell^{a-\nu+2}$$

implies, for example,

$$\frac{G_{\frac{3}{4}(\ell-1)}}{\frac{3}{4}(\ell-1)} \equiv (-H_\ell)^{k\,\ell^{b-1}} \cdot \frac{G_{\frac{3}{4}(\ell-1)+k\,\ell^{b-1}(\ell-1)}}{\frac{3}{4}(\ell-1)+k\,\ell^{b-1}(\ell-1)} \mod \ell^{b}.$$

They look like interpolating $L\Big(1+j(\ell-1),\ \tilde{\chi}^{1+j(\ell-1)}\Big)$ $(j=1,\cdots)$, via

$$\left(\frac{d}{du}\right)^{j(\ell-1)} \mathrm{Cl}(u)$$ (“higher derivative of the elliptic Gauss sum”)