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

1 Main references
2 Introduction
3 Review of Elliptic Gauss Sums
4 The lemniscatic sine function
5 The ray class field
6 Asai’s theorem for $\ell \equiv 13 \mod 16$
7 The corresponding Hecke $L$-series
8 Some Congruence on the Coefficients of EGS
9 Summary up to Here
10 $\ell \equiv 1 \mod 8$ case
11 The elliptic Gauss sum for $\ell \equiv 1 \mod 8$
12 The coefficients of EGS
13 Arithmetic on the elliptic curve associated to the EGS for $\ell \equiv 1 \mod 8$
14 The Congruence
15 An analogue of the congruence numbers
16 BSD Conjecture and EGS
17 An example
18 Vanishing EGS and Kummer-type congruence
19 EGS and Kummer-type congruences
20 Idea of the proof
21 Sketch of the proof
22 Some Observation
Main references

- Ônishi, Y. : *Congruence relations connecting Tate-Shafarevich groups with Hurwitz numbers*, Interdisciplinary Information Sciences, 16(2010).  [Ô]

( 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 $\mathbb{Q}(\sqrt{-p})$. 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 $\mathbb{Q}$, in the famous 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 $\mathbb{Q}(i)$. 
The lemniscatic sine function

The inverse function \( u \mapsto t \) of

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

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

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

\( \text{sl}(u) \) is an elliptic function whose period lattice is \( \Omega = (1 - i) \wp \mathbb{Z}[i] \) and its divisor modulo \( \Omega \) is

\[
    \text{div}(\text{sl}) = (0) + (\wp) - \left(\frac{\wp}{1 - i}\right) - \left(\frac{i\wp}{1 - i}\right).
\]

It is expanded as

\[
    \text{sl}(u) = u - \frac{1}{10} u^5 + \frac{1}{120} u^9 - \frac{11}{15600} u^{13} + \cdots
\]

\[
    = \sum_{m=0}^{\infty} C_{4m+1} u^{4m+1}.
\]
The ray class field

Throughout this talk, we denote $\varphi(u) = s1((1 - i) \bar{\varphi} u)$. (The period lattice of this function is $\mathbb{Z}[i]$.)

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

Let $S \subset \mathbb{Z}[i]$ be a fixed set such that $(\mathbb{Z}[i]/(\lambda))^\times \simeq S \cup -S \cup iS \cup -iS$, $|S| = \frac{\ell - 1}{4}$. Moreover we define

$$\Lambda = \varphi\left(\frac{1}{\lambda}\right), \quad \mathcal{O}_\lambda = "the\ ring\ of\ integers\ in\ \mathbb{Q}(i, \Lambda)", \quad \bar{\lambda} = \gamma(S)^{-1} \prod_{r \in S} \varphi\left(\frac{r}{\lambda}\right),$$

where

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

Then, we have

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

Note that $\mathbb{Q}(i, \Lambda)$ is the ray class field over $\mathbb{Q}(i)$ of conductor $(1 + i)^3(\lambda)$. (T. Takagi [1920], §32) (Remind that $(\mathbb{Z}[i]/(1 + i)^3)^\times \simeq \{\pm 1, \pm i\}$.)
Asai’s theorem for $\ell \equiv 13 \text{ mod } 16$ (Typical case)

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

\[
\text{egs}(\lambda) = \frac{1}{4} \sum_{r=1}^{\ell-1} \chi_\lambda(r) \text{ sl} \left( (1 - i) \overline{\omega} \frac{r}{\lambda} \right).
\]

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

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

\[
\text{egs}(\lambda) = A_\lambda \overline{\lambda}^3, \quad \left( \overline{\lambda} = \gamma(S)^{-1} \prod_{r \in S} \varphi \left( \frac{r}{\lambda} \right) \right).
\]

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

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

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

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

—. In the definition of $\text{egs}(\lambda)$, if we replace $\chi_\lambda$ by another character $\chi$ such that $\chi(i) = i$, then the sum trivially vanishes.

Each character $\chi$ “knows” which elliptic function corresponds to itself.
The corresponding Hecke $L$-series

Keeping in mind that $\left(\mathbb{Z}[i]/(1+i)^2\right) \simeq \{1, i\}$, we define

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

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

This is a Hecke character of conductor $(\lambda(1+i)^2)$.

Theorem. ([Asai])

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

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

Deuring showed that

$$L_{E_{-\lambda}/\mathbb{Q}(i)}(s) = L(s, \tilde{\chi}) \cdot L(s, \overline{\tilde{\chi}}).$$

Proposition. If the full statement of BSD conjecture for the curve $E_{-\lambda} : y^2 = x^3 + \lambda x$ is true, then $\# \text{III}(E_{-\lambda}/\mathbb{Q}(i)) = |A_{\lambda}|^2$. 
Some Congruence on the Coefficients of EGS

We define $C_j \in \mathbb{Q}$ by the expansion of $u \mapsto s\ell(u)$ as follows:

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

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

$$\pm \sqrt{\# \operatorname{III}(\mathcal{E}_-/\mathbb{Q}(i))} \equiv A_\lambda \equiv -\frac{1}{4} C_{\frac{3(\ell-1)}{4}} \mod \ell.$$ 

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

$$h(-p) \equiv \begin{cases} 
-2 \frac{B_{p+1}}{2} \pmod{p} & \text{if } p \equiv 3 \mod 4, \\
2^{-1} E_{\frac{p-1}{2}} \pmod{p} & \text{if } p \equiv 1 \mod 4.
\end{cases}$$
The corresponding elliptic curve is
\[ E_{-\lambda} : y^2 = x^3 + \lambda x \]
and \( L(1, \chi) \neq 0 \). Coates-Wiles’ theorem implies that
\[ \text{rank } E_{-\lambda}(\mathbb{Q}(i)) = 0. \]

We have a similar story.

The corresponding elliptic curve is
\[ E_{14\lambda} : y^2 = x^3 - \frac{1}{4}\lambda x \]
and, similarly, it has \( \text{rank } E_{14\lambda}(\mathbb{Q}(i)) = 0. \)

We proceed to the other case:

\( \ell \equiv 1 \mod 8 \). About 18% of the 172 examples of this case in [Asai],
\[ \text{egs}(\lambda) = 0. \]
ℓ \equiv 1 \mod 8 \text{ case}

\varepsilon \text{ always denotes an element in } \{ \pm 1, \pm i \}.

Define \( \chi_0 \) by

\[ \chi_0(\alpha) = \varepsilon \quad \text{if} \quad \alpha \equiv \varepsilon \mod (1 + i)^3 \quad (\alpha \neq 0 \in \mathbb{Z}[i]). \]

\[ \ell \equiv 1 \mod 16 \] Since \( \chi_\lambda(i) = 1 \), we define \( \chi_1 = \chi_\lambda \chi_0 \).

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

We have

\[ L(1, \tilde{\chi}) = \omega \chi_\lambda(1 + i) 2^{-1} \lambda^{-1} \text{egs}(\lambda). \]

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

\[ \ell \equiv 9 \mod 16 \] Since \( \chi_\lambda(i) = -1 \), we define \( \chi_1 = \chi_\lambda \overline{\chi_0} \).

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

We have

\[ L(1, \tilde{\chi}) = \omega \chi_\lambda(1 + i) 2^{-1} \lambda^{-1} \text{egs}(\lambda). \]

Here \( \text{egs}(\lambda) \) is defined in the next page.
The elliptic Gauss sum

Our situation: \( \ell \equiv 1 \mod 8 \) is a prime, and

\[
\ell = \lambda \overline{\lambda}, \quad \lambda \equiv 1 \mod (1 + i)^3, \quad \chi_\lambda(\nu) = \left( \frac{\nu}{\lambda} \right)_4, \quad \chi_\lambda(i) = i^{\frac{\ell-1}{4}} = \pm 1.
\]

Using \( \text{cl}(u) = s_1 \left( u + \frac{\varpi}{2} \right) \), we define \( \psi(u) = \text{cl}((1 - i) \varpi u) \) and the elliptic Gauss sum by

\[
\text{egs}(\lambda) = \sum_{\nu \in S \cup iS} \chi_\lambda(\nu) \psi\left( \frac{\nu}{\lambda} \right).
\]

Then we have (revisited)

Proposition. ([Asai])

\[
L(1, \tilde{\chi}) = \varpi \chi(1 + i) 2^{-1} \lambda^{-1} \text{egs}(\lambda).
\]
The coefficients of EGS

For the coefficients, we recall the following

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

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

where $A_\lambda$ is given by

<table>
<thead>
<tr>
<th>$\ell \mod 16$</th>
<th>$\chi_\lambda(1 + i) = 1$</th>
<th>$\chi_\lambda(1 + i) = -1$</th>
<th>$\chi_\lambda(1 + i) = i$</th>
<th>$\chi_\lambda(1 + i) = -i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$i\sqrt{2} \cdot a_\lambda$</td>
<td>$\sqrt{2} \cdot a_\lambda$</td>
<td>$\zeta_8 \cdot a_\lambda$</td>
<td>$i\zeta_8 \cdot a_\lambda$</td>
</tr>
<tr>
<td>9</td>
<td>$i\zeta_8 \cdot a_\lambda$</td>
<td>$\zeta_8 \cdot a_\lambda$</td>
<td>$i\sqrt{2} \cdot a_\lambda$</td>
<td>$\sqrt{2} \cdot a_\lambda$</td>
</tr>
</tbody>
</table>

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

**Proof.**

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

**Remark.** Asai observed that $a_\lambda \in 2\mathbb{Z}$. 
Arithmetic on the elliptic curve associated to the EGS for $\ell \equiv 1 \mod 8$

The Hecke $L$-series associated to $\text{egs}(\lambda)$ is a factor of the $L$-series of the elliptic curve

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

The conductor of this is $(1 + i)^3\lambda^2$ (See [Serre-Tate], Thm.12), and the reduction type at $(1 + i)$ is of type III, and that at $\lambda$ is of type $I_{2}^*$. Each Tamagawa number $\tau_p$ and $A_\lambda = \text{“the coeff. of eg}_s(\lambda)\text{”}$ are as follows:

<table>
<thead>
<tr>
<th>$\ell \mod 16$</th>
<th>Invariants</th>
<th>$\chi_\lambda(1 + i) = 1$</th>
<th>$\chi_\lambda(1 + i) = -1$</th>
<th>$\chi_\lambda(1 + i) = i$</th>
<th>$\chi_\lambda(1 + i) = -i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$A_\lambda$</td>
<td>$i\sqrt{2} \cdot a_\lambda$</td>
<td>$\sqrt{2} \cdot a_\lambda$</td>
<td>$\zeta_8 \cdot a_\lambda$</td>
<td>$i\zeta_8 \cdot a_\lambda$</td>
</tr>
<tr>
<td></td>
<td>$\tau(\lambda)$</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>$\tau(1+i)$</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>$A_\lambda$</td>
<td>$i\zeta_8 \cdot a_\lambda$</td>
<td>$\zeta_8 \cdot a_\lambda$</td>
<td>$i\sqrt{2} \cdot a_\lambda$</td>
<td>$\sqrt{2} \cdot a_\lambda$</td>
</tr>
<tr>
<td></td>
<td>$\tau(\lambda)$</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>$\tau(1+i)$</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

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

It is quite certain that $\left(\frac{1}{2} a_\lambda\right)^2 = \# III(\mathcal{E}_\lambda)$ if $a_\lambda \neq 0$. 

14 / 28
The congruence for $\ell \equiv 1 \mod 8$

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

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

For the sake of simplicity, we restrict the case $\ell \equiv 1 \mod 16$, and assume, as before, that $\ell = \lambda \bar{\lambda}$, $\lambda \equiv 1 \mod (1 + i)^3$.

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

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

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

$\text{egs}(\lambda) := \sum_{\nu \in S \cup iS} \chi_{\lambda}(\nu) \psi\left(\frac{\nu}{\lambda}\right) = A_{\lambda} \bar{\lambda}^3$ with $A_{\lambda} \in \mathbb{Z}[\zeta_8]$.

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

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

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

\[15 / 28\]
Proof of the congruence (in a few words) (1/2)

Recall

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

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

\( egs(\lambda) = \left. \sum_{j=0}^{\frac{\ell-3}{2}} \chi(g^j) \cl(g^ju) \right|_{u=(1-i)\omega^\frac{1}{4}} = \left. \sum_{j=0}^{\frac{\ell-3}{2}} \chi(g^j) \cl\left(g^j \sum_{n=0}^{\infty} (-1)^n \left(\frac{-1}{4n+1}\right) t^{4n+1} \right) \right|_{t=\Lambda} \)

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

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

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

\[ \equiv \left. \sum_{m=0}^{\frac{3(\ell-1)}{8}} \left( \sum_{j=0}^{\frac{\ell-3}{2}} \chi(g^j) g^{2jm} \right) C_{2m} \left( \sum_{n=0}^{\infty} (-1)^n \left(\frac{-1}{4n+1}\right) t^{4n+1} \right)^{2m} \right|_{t=\Lambda} \mod \left(\Lambda^\frac{3(\ell-1)}{4} + 1\right). \]

\[ \Downarrow \]

\[ = \sum_{j=0}^{\frac{\ell-3}{2}} g^{\frac{j(\ell-1)}{4}} g^{2jm} = \sum_{j=0}^{\frac{\ell-3}{2}} g^{\frac{j(\ell-1)}{4} + 2m} \]
Proof of the congruence (in a few words) (2/2)

Because of

\[ \sum_{j=0}^{\ell^2/2} \ell \cdot (\ell - 1) \cdot \left( \frac{j(\ell - 1)}{4} + 2m \right) \begin{cases} 0 & \text{if } (\ell - 1) \nmid \left( \frac{j(\ell - 1)}{4} + 2m \right), \\ \frac{\ell - 1}{2} & \text{if } (\ell - 1) \mid \left( \frac{j(\ell - 1)}{4} + 2m \right), \end{cases} \quad 0 \leq 2m \leq \frac{3(\ell - 1)}{4}, \]

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

\[ \equiv \frac{\ell - 1}{2} \cdot C_{\frac{3(\ell - 1)}{4}} \cdot \left( \sum_{n=0}^{\infty} (-1)^n \left( \frac{n}{4n + 1} \right) \right) \mod \left( \Lambda^{\frac{3(\ell - 1)}{4}} + 1 \right) \]

This implies

\[ \operatorname{egs}(\lambda) \equiv A_\lambda \cdot \Lambda^{\frac{3(\ell - 1)}{4}} \equiv \frac{\ell - 1}{2} \cdot C_{\frac{3(\ell - 1)}{4}} \cdot \Lambda^{\frac{3(\ell - 1)}{4}} \mod \left( \Lambda^{\frac{3(\ell - 1)}{4}} + 1 \right), \]

and, at last, we have:

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

The rationality of \( A_\lambda \) (Asai’s theorem) yields the congruence \( \mod \ell \).

The absolutely minimal residues of the RHS in numerical check coincide with the values in the table of [Asai].
The following is well-known: (see, for example, Koblitz’ GTM book)

**Theorem.** Let $n \in \mathbb{Z}$. For the elliptic curve $E_{n^2} : y^2 = x^3 - n^2 x$
the following three are equivalent each other:

1. $\exists u, \exists v \in \mathbb{Q}$ such that $n^2 = u^4 - v^2$,
2. $n$ is a congruence number,
3. $\text{rank } E_{n^2}(\mathbb{Q}) > 0$.
An analogue of the congruence numbers (2/2)

Some numerical calculation suggests the following analogue:

**Conjecture. (Gaussian congruence numbers)**

Let \( \lambda \) be a first degree Gaussian prime such that \( \lambda \equiv 1 \mod (1 + i)^3 \).

There exist \( \alpha, \beta \in \mathbb{Q}(i) \) satisfying

\[
(\star) \quad \lambda = -\alpha^4 + \beta^2 i,
\]

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

---

— All the examples in [Asai] satisfy this conjecture.
— In the examples of [Asai] such that \( \text{egs}(\lambda) = 0 \), except \( \lambda \lambda = 4817 \), we can take \( \alpha, \beta \in \mathbb{Z}[i] \).
— If \( \lambda = -\alpha^4 + \beta^2 i \), the point \( (x, y) = (\alpha^2 i, \pm \alpha \beta) \) is on \( \mathcal{E}_\lambda(\mathbb{Q}(i)) \). Indeed

\[
x^3 - \lambda x = -\alpha^6 i - (-\alpha^4 + \beta^2 i) \alpha^2 i = (\beta \alpha)^2 = y^2.
\]

This is a non-torsion point.

( From Nagell-Lutz argument, we see the torsion part of \( \mathcal{E}_\lambda(\mathbb{Q}(i)) \) is \( \{(0, 0), \infty\} \). )
BSD Conjecture and EGS

We summarize the result up to here:

\[ \lambda \text{ is of the form } -\alpha^4 + \beta^2 i \iff \text{rank } E_\lambda (\mathbb{Q}(i)) > 0 \]

\[ \iff L(1, \tilde{\chi}) = 0 \]

\[ \iff \text{egs}(\lambda) = 0. \]
An example

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

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

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

MAGMA says that the Mordell-Weil rank of $E_{\lambda}$ is 2.

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

Remark. Since

$$L(s, \tilde{\chi}) L(s, \overline{\tilde{\chi}}) = L_{E_{\lambda}/\mathbb{Q}(i)}(s),$$

the analytic rank of $E_{\lambda}/\mathbb{Q}(i)$ is even.

This is consistent with that the MW-group of $E_{\lambda}$ over $\mathbb{Q}(i)$ is a $\mathbb{Z}[i]$-module.

MAGMA says that all cases in the table in [Asai] are of MW-rank two.
Vanishing EGS and Kummer-type congruence

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

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

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

We denote by $H_\ell$ the Hasse invariant of $y^2 = x^3 - x$ at $\ell \equiv 1 \mod 4$:

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

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

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

if the behavior of $|\text{egs}(\lambda)|$ 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.)
The following theorem was proved by Fumio Sairaiji, which had been a conjecture until 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. $\text{egs}(\lambda) = 0$;
2. $\ell \mid G_{\frac{3}{4}(\ell-1)}$;
3. For any $0 \leq a < \ell$, we have
   \[
   \sum_{r=0}^{a} \binom{a}{r}(-H_\ell)^{a-r} \frac{G_{\frac{3}{4}(\ell-1)+r(\ell-1)}}{\frac{3}{4}(\ell - 1) + r(\ell - 1)} \equiv 0 \mod \ell^{a+1}.
   \]

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

4. \[
   \sum_{r=0}^{a} \binom{a}{r}(-H_\ell)^{a-r} \frac{G_{\frac{3}{4}(\ell-1)+r(\ell-1)}}{\frac{3}{4}(\ell - 1) + r(\ell - 1)} \equiv 0 \mod \ell^{a-\nu+2}
   \]
   if and only if $\text{egs}(\lambda) = 0$. 

Idea of the proof

Taking an \((\ell - 1)\)th root \(\zeta\) of 1 in \(\mathbb{Z}_\ell\), we define

\[
\text{Cl}(u) = \sum_{j=0}^{\ell-1} \chi_\lambda(\zeta^j) \text{cl}(\zeta^j u).
\]

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

Then we have \(\text{Cl}(s\ell^{-1}(\Lambda)) = \text{egs}(\lambda)\) and

\[
\text{Cl}(u) = (\ell - 1) \sum_{a=0}^{\infty} G_{\frac{3}{4}(\ell-1)+a(\ell-1)} \frac{u^{\frac{3}{4}(\ell-1)+a(\ell-1)}}{\left(\frac{3}{4}(\ell - 1) + a(\ell - 1)\right)!}.
\]

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

\[
\left(\left(\frac{\partial}{\partial u}\right)^{\ell-1} - H_\ell\right)^a \left(\frac{\text{Cl}(u)}{u}\right)
\]

belongs to \(\ell^{a+1} \mathbb{Z}_\ell\).
Sketch of the proof

We show (1) \implies (3) (and (4)), which is the most difficult part of the proof.
So, we assume \( \text{egs}(\lambda) = 0 \).

We identify the completion \( \mathbb{Z}[i]_{\lambda} \) with \( \mathbb{Z}_{\ell} \).

**LT** : Lubin-Tate formal group over \( \mathbb{Z}_{\ell} \) corresponding to \( \lambda \)-plication \( x \mapsto \lambda x + x^\ell \).

**\( f_0(x) \)** : the formal log of \( \text{LT} \).

**\( \widehat{sl} \)** : the formal group defined by \( t_1 + t_2 = \text{sl} \left( \text{sl}^{-1}(t_1) + \text{sl}^{-1}(t_2) \right) \) over \( \mathbb{Z}_{\ell} \).

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

\[
\iota : \text{LT} \quad \xrightarrow{\iota} \quad \widehat{sl}
\]

\[
\begin{align*}
x & \xmapsto{\iota(x)} t = \varphi(u) \\
\exists \eta & \xmapsto{\iota(\eta)} \Lambda = \varphi \left( \frac{1}{\lambda} \right).
\end{align*}
\]

So that \( \eta^\ell = -\lambda \).

Since \( \text{Cl} \left( \text{sl}^{-1}(t) \right) \in \mathbb{Z}_{\ell}[[t]] \), \( \text{Cl} \left( f_0(x) \right) \in \mathbb{Z}_{\ell}[[x]] \).
We want to show the terms of degree up to $\ell(\ell - 1)$ of
\[
\frac{\text{Cl}(u)}{u} = \frac{\text{Cl}(\text{sl}^{-1}(t))}{\text{sl}^{-1}(t)}
\]
are in $\ell \mathbb{Z}_\ell$, because this and a theorem of Hochschild yield
\[
\begin{pmatrix}
\frac{3}{4}(\ell - 1) \\
\end{pmatrix}
\text{in } t\text{-expansion of }
\left(\left(\frac{d}{du}\right)^{\ell - 1} - H_\ell\right)^a \frac{\text{Cl}(u)}{u}
\in \ell^{a+1}\mathbb{Z}_\ell[[t]] \subset \ell^{a+1}\mathbb{Z}_\ell\langle u \rangle
\]
provided $\frac{3}{4}(\ell - 1) + a(\ell - 1) < \ell(\ell - 1)$.

However, since $\widehat{\mathfrak{sl}}$ is strongly isomorphic to $\mathbf{LT}$, it is sufficient to check leading terms of
\[
\frac{\text{Cl}(f_0(x))}{f_0(x)}.
\]
Since $0 = \text{egs}(\lambda) = \text{Cl}(\text{sl}^{-1}(\Lambda))$ and then, $\text{Cl}(f_0(\zeta^j \eta)) = 0$ for $1 \leq j \leq \ell - 1$ as well, we have $0 = \text{Cl}(f_0(\zeta^j \eta))$ and then, $\text{Cl}(f_0(x))$ is divisible by $\lambda x + x^\ell = x \prod_{j=1}^{\ell-1} (x - \zeta^j \eta)$.

Hence we shall check leading terms of
\[
\frac{\text{Cl}(u)}{u} = \frac{\text{Cl}(f_0(x))/(\lambda x + x^\ell)}{f_0(x)/(\lambda x + x^\ell)} = \lambda \frac{\text{Cl}(f_0(x))}{f_0(x)} \cdot \frac{\lambda x + x^\ell}{\lambda f_0(x)}, \text{ namely, of } \frac{\lambda x + x^\ell}{\lambda f_0(x)}.
\]
To get (4), we take a $n \in \mathbb{N}$ and fix it. Thanks to $f_0(\zeta x) = \zeta f_0(x)$, we shall let

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

It is shown $b_\ell \in (\mathbb{Z}_\ell)^\times$.

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

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

Hence

$$\frac{\text{Cl}(f_0(x))}{\lambda x + x^\ell} \cdot \frac{\lambda x + x^\ell}{\lambda f_0(x)}$$

has the same property.

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

$$\frac{\text{Cl}(u)}{u} = \frac{\text{Cl}(f_0(x))}{f_0(x)} \cdot \frac{(\lambda x + x^\ell)}{(\lambda x + x^\ell)} = \lambda \frac{\text{Cl}(f_0(x))}{f_0(x)} \cdot \frac{\lambda x + x^\ell}{\lambda f_0(x)}$$

belongs to $\frac{1}{\ell^{\nu-2}} \mathbb{Z}_\ell$.

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 $\frac{3}{4}(\ell - 1) + a(\ell - 1) < \nu(\ell - 1)$, 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)

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

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 \( L\left( 1 + j(\ell - 1), \tilde{\chi}^{1+j(\ell-1)} \right) \) \((j = 1, \cdots)\), via

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