

Arithmetic over the Gaussian Number Field on a Certain Family of Elliptic Curves with Complex Multiplication

Dedicated to Professor Tetsuya Asai on the occasion of his eightieth birthday

By

Yoshihiro ÔNISHI* and Fumio SAIRAIJI**

Abstract

This work is a sequel of a previous work of one of the authors (Y.Ô), which treated certain congruence relation between an elliptic Gauss sum and a coefficient of power series expansion at the origin of the lemniscate sine function. We extend the previous result (in [O]) which concerned only for non-vanishing elliptic Gauss sums. We give new congruence relations between power series coefficients of the lemniscate cosine function, which hold if and only if the corresponding elliptic Gauss sum vanishes.

Introduction

In the paper [H1], Hurwitz gave the following result :

Theorem 0.1. *Let $p > 3$ be a rational prime, and let $h(-p)$ be the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$. Then we have*

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

Here B_n is the n -th Bernoulli number, and E_n is the n -th Euler number¹. Moreover, the absolutely smallest residue of the right hand side exactly equals to $h(-p)$.

Each of these congruences in is proved by expressing the value at $s = 1$ of the Dirichlet L -series $L(s, \left(\frac{\cdot}{p}\right))$ as a trigonometric Gauss sums, which is defined by a sort of Gauss sum using suitable trigonometric function instead of the exponential function

Received May 9, 2020. Revised April 8, 2023.

2010 Mathematics Subject Classification(s): 11G05, 11G40.

Key Words: elliptic Gauss sums, elliptic curves, Hecke L -series, formal group, Birch and Swinnerton-Dyer conjecture.

This work was supported by the RIMS.

*Faculty of Science and Technology, Meijo University, Nagoya 468-8502, Japan.

e-mail: yonishi@meijo-u.ac.jp

**Faculty of Pharmaceutical Sciences, Hiroshima International University, Hiroshima 737-0112, Japan.

e-mail: sairaiji@hirokoku-u.ac.jp

¹ We define E_n by $\operatorname{sech}(u) = \sum_{n=1}^{\infty} (E_n/n!)u^n$. So that, $E_2 = -1$, $E_4 = 5$, $E_6 = -61$, \dots .

in the classical Gauss sum. Under the Birch Swinnerton-Dyer (BSD) conjecture, one of the authors gave in [O] an analogue of Theorem 0.1 by replacing Dirichlet L -series and the trigonometric Gauss sum by Hecke's L -series and an elliptic Gauss sum, respectively, in which the class number is replaced by a square root of the conjectural order of the Tate-Shafarevich group, and the Bernoulli number or Euler number is done by certain coefficient of the power series expansion at the origin of the lemniscate sine function.

Elliptic Gauss sums were used, in order to compute numerically the L -series attached to some elliptic curves over \mathbf{Q} , in the famous original paper [BSD] by Birch and Swinnerton-Dyer. We wish to use them for investigation of L -series attached to some elliptic curves defined over $\mathbf{Q}(i)$, where $i = \sqrt{-1}$ is the imaginary unit.

The paper [O] is written about such investigation only for the case where the associated prime ℓ is congruent to 5 or 13 modulo 16, since the treated elliptic Gauss sum for that case does not vanish and it is directly relates the order of Tate-Shafarevich group. In this paper, we extend the result [O] to all the cases on modulo 16 of the primes ℓ congruent to 1 modulo 4. The remarkable point is that, in the cases which were not treated in [O], the corresponding elliptic Gauss sums indeed vanish often, which means the associated Hecke L -series vanish as well. We verify such vanishing phenomenon by the tables in [A]. So that, the corresponding elliptic curve, which is defined over the Gaussian number field, is expected to be of positive Mordell-Weil rank.

We present certain Kummer type congruences (Theorem 7.1) on power series coefficients of the lemniscate cosine function which are valid if and only if the corresponding elliptic Gauss sum (hence the value at 1 of the corresponding Hecke L series) vanishes.

The corresponding elliptic curve (see the defining equations (3.4), (4.4), and (5.5)) is additive reduction modulo λ and our Kummer-type congruence is quite resemble to the Kummer congruence which guarantees the existence of the Kubota-Leopoldt p -adic L -function. So the authors hope that our result gives a hint for a construction of p -adic L -functions for an elliptic curve which is additive reduction modulo p .

This paper is organized as follows. We setup fundamental background in §1 and §2. From §3 to §4, we review the results in [A] and [O]. In §5, we review the result for the rest cases which are omitted in [O]. In §6, we discuss some structure of the Mordell-Weil group of the curve and how our theory relates to BSD conjecture. From §7 to §12, we give the main result (Theorem 7.1) and its proof.

Acknowledgment: The authors thank Prof. G. Yamashita who informed them of Hurwitz' paper [H1], which looks the earliest literature in which Theorem 0.1 appeared. They also thank Prof. S. Yasuda to whose advice they owe §11. We have special thanks to A. Goto who pointed out some crucial misunderstanding of the authors.

Contents

1	The lemniscate sine and cosine function	3
2	The ray class field	4
3	Asai's theory	4
4	Some congruence on the coefficients of elliptic Gauss sums	5
5	The foregoing researches in the case of $\ell \equiv 1 \pmod{8}$	6
6	An analogue of the congruent numbers	7
7	Vanishing EGS and Kummer-type congruence	10
8	ℓ -Adic explicit formula of an elliptic Gauss sum	11
9	Application of the Hochschild formula	14
10	Proof of the main theorem	15
11	Central value of the Hecke L -function	17
12	Estimate of the coefficients of elliptic Gauss sums	20
	References	21

1 The lemniscate sine and cosine function

The inverse function $u \mapsto t$ of

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

is called the *lemniscate sine function*, which is denoted by $t = \text{sl}(u)$ and is expanded as

$$(1.1) \quad \text{sl}(u) = u - \frac{1}{10}u^5 + \frac{1}{120}u^9 - \frac{11}{15600}u^{13} + \dots = \sum_{n=0}^{\infty} C_n u^n$$

with C_n in \mathbf{Q} . Then we have $C_n = 0$ if $n \not\equiv 1 \pmod{4}$ and $n!C_n$ belongs to \mathbf{Z} . It is an elliptic function whose period lattice is $\Omega = (1 - i)\varpi \mathbf{Z}[i]$, where

$$\varpi = 2 \int_0^1 \frac{dt}{\sqrt{1-t^4}} = \int_1^{\infty} \frac{dx}{2\sqrt{x^3-x}} = 2.62205\dots$$

The divisor of $\text{sl}(u)$ modulo Ω is given by

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

Throughout this paper, we denote

$$\varphi(u) = \text{sl}((1-i)\varpi u).$$

The lemniscate cosine $\text{cl}(u)$ is defined by

$$\text{cl}(u) = \text{sl}\left(u + \frac{\varpi}{2}\right).$$

Moreover, we use the notation

$$\psi(u) = \text{cl}((1-i)\varpi u).$$

Then both of functions $\varphi(u)$ and $\psi(u)$ have period lattice $\mathbf{Z}[i]$ of \mathbf{C} . We define the D_n 's by the expansion of $\text{cl}(u)$ as

$$(1.2) \quad \text{cl}(u) = \sum_{n=0}^{\infty} D_n u^n = 1 - u^2 + \frac{1}{2}u^4 - \frac{3}{10}u^6 + \frac{7}{40}u^8 - \dots$$

Then, $D_n = 0$ for odd n and $n!D_n$ is in \mathbf{Z} .

2 The ray class field

We take a rational prime $\ell \equiv 1 \pmod{4}$, and we fix its decomposition $\ell = \lambda \bar{\lambda}$ in $\mathbf{Z}[i]$ with $\lambda \equiv 1 \pmod{(1+i)^3}$. We fix a subset S of $\mathbf{Z}[i]$ (sometimes called a 1/4-set) such that $(\mathbf{Z}[i]/(\lambda))^\times \simeq S \cup -S \cup iS \cup -iS$, $|S| = (\ell - 1)/4$. Moreover we define

$$(2.1) \quad \begin{aligned} \Lambda &= \varphi\left(\frac{1}{\lambda}\right), \quad \mathcal{O}_\lambda = \text{“the ring of integers in } \mathbf{Q}(i, \Lambda)\text{”}, \\ \tilde{\lambda} &= \gamma(S)^{-1} \prod_{r \in S} \varphi\left(\frac{r}{\lambda}\right), \\ \text{where } &\begin{cases} \{\pm 1, \pm i\} \ni \gamma(S) \equiv \prod_{r \in S} r \pmod{\lambda} & \text{if } \ell \equiv 5 \pmod{8}, \\ \{\pm i\} \ni \gamma(S)^2 \equiv \prod_{r \in S} r^2 \pmod{\lambda} & \text{if } \ell \equiv 1 \pmod{8}. \end{cases} \end{aligned}$$

Here, we have \pm sign ambiguity of $\gamma(S)$ in the case of $\ell \equiv 1 \pmod{8}$. In any case, we know (see for example p.106 of [A] or Lemma 1.11 in [O]) that

$$(2.2) \quad \Lambda \in \mathcal{O}_\lambda, \quad (\Lambda)^{\ell-1} = (\lambda), \quad \tilde{\lambda}^4 = -\lambda.$$

Note that $\mathbf{Q}(i, \Lambda)$ is the ray class field over $\mathbf{Q}(i)$ of conductor $((1+i)^3\lambda)$ (see Takagi [T], §32, for instance).

Throughout this paper, we fix the identification

$$(2.3) \quad \mathbf{Z}[i]_\lambda \simeq \mathbf{Z}_\ell,$$

where the left hand side is the λ -adic completion of $\mathbf{Z}[i]$. Moreover, we consider they are subrings of the algebraic closure $\overline{\mathbf{Q}_\ell}$ of \mathbf{Q}_ℓ . We use the following notation. For any element α in the integer ring $\overline{\mathbf{Z}_\ell}$ of $\overline{\mathbf{Q}_\ell}$, we denote the ℓ -adic order by ord . For example, for α in $\mathbf{Z}[i]_\lambda$, $\text{ord}(\alpha) = n$ if and only if λ^n divides α but λ^{n+1} does not.

3 Asai's theory

In this section we recall the results from [A] in order to go to the rest cases smoothly. We assume here $\ell \equiv 13 \pmod{16}$ for simplicity. For the other cases, see [A]. We put $\chi_\lambda(r) = \left(\frac{r}{\lambda}\right)_4$. In this case, the *elliptic Gauss sum* is defined by

$$\text{egs}(\lambda) = \sum_{r \in S} \chi_\lambda(r) \varphi\left(\frac{r}{\lambda}\right).$$

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

Theorem 3.1. ([A]) *There exists an odd A_λ in \mathbf{Z} such that*

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

where $\tilde{\lambda}$ is defined by (2.1). In particular, $\text{egs}(\lambda) \neq 0$.

Remark 3.2. (1) This theorem is proved by using the functional equation for the Hecke L -series corresponding to the suitable Hecke character associated to χ_λ and

the formula of Cassels-Matthews (see [M]) for the classical quartic Gauss sum which appears as the root number of the functional equation. It is expected to have another proof of the formula of Cassels-Matthews if we get a part of BSD conjecture including the parity of the order of the corresponding Tate-Shafarevich group.

(2) We call A_λ the *coefficient* of $\text{egs}(\lambda)$ according to [A].

We recall the corresponding Hecke L -series. Still we are assuming $\ell \equiv 13 \pmod{16}$. Taking $\{1, \mathbf{i}\}$ as a set of complete representatives of $(\mathbf{Z}[\mathbf{i}] / (1 + \mathbf{i})^2)^\times$, we define

$$\chi_0(\alpha) = \varepsilon^2 \quad \text{for } \alpha \equiv \varepsilon \pmod{(1 + \mathbf{i})^2}, \quad \varepsilon \in \{1, \mathbf{i}\}, \quad \tilde{\chi}(\alpha) = \chi_\lambda(\alpha) \chi_0(\alpha) \bar{\alpha}.$$

Then $\tilde{\chi}$ is a Hecke character of conductor $((1 + \mathbf{i})^2 \lambda)$. Now we have the following expression given by Asai [A] for the central value of the corresponding Hecke L -series.

Theorem 3.3. *We have $L(1, \tilde{\chi}) = -\varpi (1 - \mathbf{i})^{-1} \chi_\lambda(2) \lambda^{-1} \text{egs}(\lambda)$.*

Searching an elliptic curve whose conductor is the square of that of $\tilde{\chi}$ (see [ST], Theorem 12), we see that the elliptic curve corresponding to $L(s, \tilde{\chi})$ is

$$(3.4) \quad \mathcal{E}_{-\lambda} : y^2 = x^3 + \lambda x, \quad (\lambda \bar{\lambda} = \ell \equiv 13 \pmod{16}).$$

Deuring [D] showed that

$$(3.5) \quad L_{\mathcal{E}_{-\lambda}/\mathbf{Q}(\mathbf{i})}(s) = L(s, \tilde{\chi}) L(s, \bar{\tilde{\chi}}).$$

Especially, if $\ell \equiv 13 \pmod{16}$, then $\text{rank } \mathcal{E}_{-\lambda}(\mathbf{Q}(\mathbf{i})) = 0$, which is shown by Theorems 3.1, 3.3, and Coates-Wiles theorem in [CW]. Moreover, we recall the following result from [O].

Proposition 3.6. *If the full statement of BSD conjecture for the curve $\mathcal{E}_{-\lambda}$ is true, then $\#\text{III}(\mathcal{E}_{-\lambda}/\mathbf{Q}(\mathbf{i})) = A_\lambda^2$.*

4 Some congruence on the coefficients of elliptic Gauss sums

The former part of the following theorem is proved in [O] and reproved a sophisticated method as Lemma 8.4 later. Let C_n be the coefficient of u^n defined by (1.1). Since $(\frac{3}{4}(\ell - 1))! C_{\frac{3}{4}(\ell - 1)}$ is in \mathbf{Z} , $-\frac{1}{4} C_{\frac{3}{4}(\ell - 1)}$ is in \mathbf{Z}_ℓ .

Theorem 4.1. ([O]) *Assuming $\ell \equiv 13 \pmod{16}$, we have $A_\lambda \equiv -\frac{1}{4} C_{\frac{3}{4}(\ell - 1)} \pmod{\ell}$. The absolutely minimal residue of the right hand side is exactly equal to A_λ .*

The latter part of Theorem 4.1 follows from the former part and the following lemma which is proved in §12.

Lemma 4.2. *For any $\ell = \lambda \bar{\lambda} \equiv 1 \pmod{4}$, we have $|A_\lambda| < \frac{1}{2} \ell$.*

Remark 4.3. Observing Kanou's manmouh table, the behavior of $|\text{egs}(\lambda)|$ with respect to $\ell \rightarrow \infty$ is quite small. Indeed, the estimation $|A_\lambda| < \ell^{1/4}$ is hopeful.

Joining Proposition 3.6 and Theorem 4.1 together, we have a natural generalization of Hurwitz' congruence in Theorem 0.1.

For the case of $\ell \equiv 5 \pmod{16}$, we have a similar story which is described in [A] and [O]. The corresponding elliptic curve for this case is

$$(4.4) \quad \mathcal{E}_{\frac{1}{4}\lambda} : y^2 = x^3 - \frac{1}{4}\lambda x, \quad (\lambda\bar{\lambda} = \ell \equiv 5 \pmod{16}),$$

for which we have $\text{rank } \mathcal{E}_{\frac{1}{4}\lambda}(\mathbf{Q}(\mathbf{i})) = 0$, and the corresponding congruence as (4.1). So, from the next section, we proceed to the remaining case of $\ell \equiv 1 \pmod{8}$.

5 The foregoing researches in the case of $\ell \equiv 1 \pmod{8}$

From now on, we denote by ℓ a prime number satisfying $\ell \equiv 1 \pmod{8}$, and write $\ell = \lambda\bar{\lambda}$ with $\lambda \equiv 1 \pmod{(1+\mathbf{i})^3}$. We define $\chi_\lambda(\nu) = \left(\frac{\nu}{\lambda}\right)_4$. Then we see $\chi_\lambda(\mathbf{i}) = \mathbf{i}^{\frac{\ell-1}{4}} = (-1)^{\frac{\ell-1}{8}}$. Using $\psi(u) = \text{cl}((1-\mathbf{i})\varpi u)$, the elliptic Gauss sum in this case is defined by

$$\text{egs}(\lambda) = \sum_{\nu \in S\mathbf{U}\mathbf{i}S} \chi_\lambda(\nu) \psi\left(\frac{\nu}{\lambda}\right).$$

Remark 5.1. For the elliptic Gauss sum $\text{egs}(\lambda)$ in this case which is defined in the next section, Asai observed for examples in his Table (see Remark in p.115 of [A]) that $\text{egs}(\lambda) = 0$, only if $\ell \equiv 1 \pmod{16}$ and $\chi_\lambda(1+\mathbf{i}) = 1$, or $\ell \equiv 9 \pmod{16}$ and $\chi_\lambda(1+\mathbf{i}) = -\mathbf{i}$. About 76% in the former case, and about 70% in the later case, of examples in Table of [A], we have, indeed, $\text{egs}(\lambda) = 0$.

In this paper ε always denotes any element in $\boldsymbol{\mu}_4 = \{1, -1, \mathbf{i}, -\mathbf{i}\}$. Recalling the canonical isomorphism $\boldsymbol{\mu}_4 \xrightarrow{\sim} (\mathbf{Z}[\mathbf{i}]/(1+\mathbf{i})^3)^\times$, we define the character χ_0 by

$$\chi_0(\alpha) = \varepsilon \quad \text{if } \alpha \equiv \varepsilon \pmod{(1+\mathbf{i})^3} \quad (\alpha \in \mathbf{Z}[\mathbf{i}], (1+\mathbf{i}) \nmid \alpha).$$

(Case 1) If $\ell \equiv 1 \pmod{16}$, $\chi_\lambda(\mathbf{i}) = 1$, we define $\chi_1 = \chi_\lambda \chi_0$ and $\tilde{\chi}((\alpha)) = \chi_1(\alpha)\bar{\alpha}$.

(Case 2) If $\ell \equiv 9 \pmod{16}$, $\chi_\lambda(\mathbf{i}) = -1$, we define $\chi_1 = \chi_\lambda \bar{\chi}_0$ and $\tilde{\chi}((\alpha)) = \chi_1(\alpha)\bar{\alpha}$.

In any case, we see $\tilde{\chi}$ is a Hecke character of conductor $((1+\mathbf{i})^3\lambda)$. Then, as in [A], we have the following expression :

$$(5.2) \quad L(1, \tilde{\chi}) = (-1)^{\frac{1}{8}(\ell-1)} \varpi \overline{\chi_\lambda(1+\mathbf{i})} 2^{-1} \lambda^{-1} \text{egs}(\lambda).$$

Theorem 5.3. ([A]) Let $\zeta_8 = \exp(2\pi\mathbf{i}/8)$. There exists A_λ in $\mathbf{Z}[\zeta_8]$ such that

$$(5.4) \quad \text{egs}(\lambda) = A_\lambda \tilde{\lambda}^3.$$

Here, A_λ is given by the table (5.6) below with some a_λ in \mathbf{Z} .

This theorem is also proved by using the formula of Cassels-Matthew and the functional equation of $L(s, \tilde{\chi})$. In [A], it is observed by Asai that a_λ is in $2\mathbf{Z}$, but any proof of this is not known yet.

Searching the elliptic curve whose conductor is $((1+i)^3\lambda)^2$, which is square of that of $\tilde{\chi}$ ([ST], Theorem 12), we see the Hecke L -series associated to $\text{egs}(\lambda)$ is a factor of the L -series of the elliptic curve

$$(5.5) \quad \mathcal{E}_\lambda : y^2 = x^3 - \lambda x, \quad (\lambda\bar{\lambda} = \ell \equiv 1 \pmod{8}).$$

We have the same equation as (3.5) for this case as well. The reduction type at $(1+i)$ is of type III, and one at λ is of type I_2^* . Each Tamagawa number τ_p and the coefficients A_λ of $\text{egs}(\lambda)$ is given as follows:

$$(5.6) \quad \begin{array}{c|cc|cccc} & \chi_\lambda(1+i) & & 1 & -1 & i & -i \\ \hline & A_\lambda & & \mathbf{i}\sqrt{2} \cdot a_\lambda & \sqrt{2} \cdot a_\lambda & \zeta_8 \cdot a_\lambda & \mathbf{i}\zeta_8 \cdot a_\lambda \\ \ell \equiv 1 \pmod{16} & \tau_{(\lambda)} & & 2 & 2 & 2 & 2 \\ & \tau_{(1+i)} & & 4 & 4 & 2 & 2 \\ \hline & A_\lambda & & \mathbf{i}\zeta_8 \cdot a_\lambda & \zeta_8 \cdot a_\lambda & \mathbf{i}\sqrt{2} \cdot a_\lambda & \sqrt{2} \cdot a_\lambda \\ \ell \equiv 9 \pmod{16} & \tau_{(\lambda)} & & 2 & 2 & 2 & 2 \\ & \tau_{(1+i)} & & 2 & 2 & 4 & 4 \end{array}$$

Remark 5.7. Assume $a_\lambda \neq 0$ and the full statement of BSD conjecture true. Then we have $a_\lambda \in 2\mathbf{Z}$ and $(\frac{1}{2}a_\lambda)^2 = \#\text{III}(\mathcal{E}_\lambda)$

Recall the numbers D_n defined in (1.2). Since $(\frac{3}{4}(\ell-1))!D_{\frac{3}{4}(\ell-1)}$ is in \mathbf{Z} , $-\frac{1}{2}D_{\frac{3}{4}(\ell-1)}$ is in \mathbf{Z}_ℓ . We keep in mind that $\mathbf{Z}[\zeta_8]$ is an Euclidean ring. Using the method of [O] and Lemma 4.2, the following is shown.

Theorem 5.8. Let $\tilde{\lambda}_0$ be a prime lying above λ in $\mathbf{Q}(\zeta_8)$ such that $\gamma(S) \equiv \prod_{r \in S} r \pmod{\tilde{\lambda}_0}$. We have

$$A_\lambda \equiv -\frac{1}{2} D_{\frac{3}{4}(\ell-1)} \pmod{\tilde{\lambda}_0},$$

where A_λ is given by the table (5.6). Furthermore, A_λ is the minimal residue in $\zeta_8 \mathbf{Z}[\mathbf{i}]$ of the right hand side with respect to the absolute norm.

6 An analogue of the congruent numbers

The following is well-known (see, for example, Koblitz' book [K]).

Proposition 6.1. Let n be a rational integer. For the elliptic curve $\mathcal{E}_{n^2} : y^2 = x^3 - n^2x$, the following three are equivalent each other:

- (1) There exist u, v in \mathbf{Q} such that $n^2 = u^4 - v^2$;
- (2) n is a congruent number;
- (3) $\text{rank } \mathcal{E}_{n^2}(\mathbf{Q}) > 0$.

The claim (1) is just a rewording of the definition of congruent number for n . The equivalence of (2) and (3) is described as Proposition 18 in [K].

Lemma 6.2. *Let A be a square-free integer in $\mathbf{Z}[\mathbf{i}]$ not equal to $1 \pm 2\mathbf{i}$. Then there are only two torsion points $(0,0)$ and ∞ in the group of $\mathbf{Q}(\mathbf{i})$ -rational points on the elliptic curve $\mathcal{E}_A : y^2 = x^3 - Ax$.*

Proof. This proof is a slight modification of the argument in [N]. Since A is square-free, the equation $x^3 - Ax = 0$ has only root $x = 0$ in $\mathbf{Q}(\mathbf{i})$. Thus the 2-torsion subgroup of $\mathbf{Q}(\mathbf{i})$ -rational points of \mathcal{E}_A is generated by $(0,0)$. Let (a,b) be a $\mathbf{Q}(\mathbf{i})$ -rational point of \mathcal{E}_A . The x -coordinate of $[1 + \mathbf{i}](a,b)$ is $x_{1+\mathbf{i}} = \left(\frac{b}{(1+\mathbf{i})a}\right)^2$. Therefore, x -coordinate of any point in $[1 + \mathbf{i}]\mathcal{E}_A(\mathbf{Q}(\mathbf{i}))$ is square. Assume (a,b) is of finite order. Then a and b belong to $\mathbf{Z}[\mathbf{i}]$ (see [N], p.14, Theorem 2 or [C], §11 and §12). If (a,b) satisfies $[2](a,b) = (0,0)$, we have $\left(\frac{a^2+A}{2b}\right)^2 = 0$ on the x -coordinate, and hence $a^2 = -A$. It does not occur because A is square-free. Hence there does not exist any $\mathbf{Q}(\mathbf{i})$ -rational point of order divided by 4. Assume that (a,b) is a $\mathbf{Q}(\mathbf{i})$ -rational point of odd order. Since $\mathcal{E}_A(\mathbf{Q}(\mathbf{i}))/[1 + \mathbf{i}]\mathcal{E}_A(\mathbf{Q}(\mathbf{i}))$ is an abelian group of exponent two, (a,b) is in $[1 + \mathbf{i}]\mathcal{E}_A(\mathbf{Q}(\mathbf{i}))$. Thus a is square in $\mathbf{Z}[\mathbf{i}]$. Since $[1 + \mathbf{i}](a,b)$ is of odd order and $x_{1+\mathbf{i}}$ is in $\mathbf{Z}[\mathbf{i}]$, we have $a|b$ and $1 + \mathbf{i}|b$. As a is square and $b^2 = a(a^2 - A)$, we have $a = f^2$, $b = f^2g$, $a^2 - A = f^2g^2$ for some f, g in $\mathbf{Z}[\mathbf{i}]$. Since $-A = f^2(g^2 - f^2)$ and A is square-free, f^2 is unit. Thus we have $f^2 = \pm 1$. Furthermore, $[2](a,b)$ is of odd order and x_2 is in $\mathbf{Z}[\mathbf{i}]$, we have $2b|a^2 + A$. Since f^2 is unit, we have $2g|2f^2 - g^2$. Thus we have $1 + \mathbf{i}|g$ and $\frac{g}{1+\mathbf{i}}|f^2$. Since f^2 is a unit, g is equal to $1 + \mathbf{i}$ up to unit. Therefore we have $A = 1 \pm 2\mathbf{i}$, the exceptions of this lemma. This completes the proof. \square

Remark 6.3. In the exceptional two cases of $A = 1 \pm 2\mathbf{i}$ of 6.2, we see the groups of $\mathbf{Q}(\mathbf{i})$ -rational points of the curves are of rank 0 because the L -functions do not vanish at 1 (see the proof of Lemma 2.11 (b), p.105, [A]). So that they are finite groups due to [CW]. MAGMA says that the groups are of order 10 generated by $(1 \pm 2\mathbf{i}, -1 \pm 3\mathbf{i})$ for each values $A = 1 \pm 2\mathbf{i}$, respectively.

We prove the following analogue of Proposition 6.1.

Proposition 6.4. *Let λ be any Gaussian prime of degree 1 satisfying $\lambda \equiv 1 \pmod{(1 + \mathbf{i})^3}$. The following three statements are equivalent:*

- (1) *There are infinitely many $\mathbf{Q}(\mathbf{i})$ -rational points on \mathcal{E}_λ , namely, $\text{rank } \mathcal{E}_\lambda(\mathbf{Q}(\mathbf{i})) > 0$;*
- (2) *The prime λ is of the form $-\alpha^4 + \beta^2\mathbf{i}$ with $\alpha, \beta \in \mathbf{Q}(\mathbf{i})$;*
- (3) *The prime λ is of the form $u^4 - v^2$ with $u, v \in \mathbf{Q}(\mathbf{i})$.*

Proof. (2) \Rightarrow (1). For the given expression $\lambda = -\alpha^4 + \beta^2\mathbf{i}$, we see $(\alpha^2\mathbf{i}, \alpha\beta)$ is a $\mathbf{Q}(\mathbf{i})$ -rational point of infinite order on the curve \mathcal{E}_λ because of Lemma 6.2 and

$$(\alpha^2\mathbf{i})^3 - \lambda(\alpha^2\mathbf{i}) = (\alpha^2\mathbf{i})^3 - (-\alpha^4 + \beta^2\mathbf{i})\alpha^2\mathbf{i} = (\alpha\beta)^2.$$

(3) \Rightarrow (1). This is proved similarly. Indeed, if $\lambda = u^4 - v^2$, then $(x,y) = (u^2, uv)$ is a point of infinite order on $\mathcal{E}_\lambda(\mathbf{Q}(\mathbf{i}))$ because of $x^3 - \lambda x = u^6 - (u^4 - v^2)u^2 = (uv)^2 = y^2$. (1) \Rightarrow (3). Lemma 6.2 implies that the set of torsion points of $\mathcal{E}_\lambda(\mathbf{Q}(\mathbf{i}))$ is $\{(0,0), \infty\}$.

We note that $\lambda \neq 1 \pm 2i$, i.e. not an exceptional prime, since $1 \pm 2i \not\equiv 1 \pmod{(1+i)^3}$. So we assume there exists a non-torsion point (a, b) , namely $b^2 = a^3 - \lambda a$, with a, b in $\mathbf{Q}(i)$. The duplication $[2](a, b)$ is given by

$$\left(\frac{(a^2 + \lambda)^2}{4b^2}, \frac{a^6 - 5\lambda a^4 - 5\lambda^2 a^2 + \lambda^3}{8b^3} \right).$$

We define $u = \frac{a^2 + \lambda}{2b} (\neq 0)$, $v = \frac{a^4 - 6\lambda a^2 + \lambda^2}{4b^2}$. Then the point (u^2, uv) is on the curve, and $\lambda = u^4 - v^2$.

(1) \Rightarrow (2). This proof is given by 2-descent, which is a modification of the proof of Proposition 1.4 in Chapter X, [Si]. We put

$$T_\lambda = \{ b \in \mathbf{Q}(i)^\times / (\mathbf{Q}(i)^\times)^2 \mid \text{ord}_\pi(b) \equiv 0 \pmod{2} \text{ for all prime } \pi \nmid \lambda \}.$$

This is a subgroup of $\mathbf{Q}(i)^\times / (\mathbf{Q}(i)^\times)^2$ of order four generated by i and λ . There is a homomorphism

$$(6.5) \quad \mathcal{E}_\lambda(\mathbf{Q}(i)) \rightarrow T_\lambda \text{ defined by } (x, y) \mapsto \begin{cases} x & \text{if } x \neq 0, \\ \lambda & \text{if } x = 0, \\ 1 & \text{if } x = \infty. \end{cases}$$

Indeed, if we put $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ which is an addition on \mathcal{E}_λ , and

$$m = \begin{cases} (y_1 - y_2)/(x_1 - x_2) & \text{if } x_1 \neq x_2, \\ (3x_1^2 - \lambda)/(2y_1) & \text{if } x_1 = x_2, \end{cases}$$

we have $x_1 x_2 x_3 = (-m x_1 + y_1)^2$. Hence, $x_3 \in x_1 x_2 (\mathbf{Q}(i)^\times)^2$ if $x_1 x_2 \neq 0$. If $x_2 \neq 0$ and $x_1 = 0$, we have

$$x_3 = \left(\frac{y_2}{x_2} \right)^2 - x_2 = \frac{-\lambda x_2}{x_2^2} \in \lambda x_2 (\mathbf{Q}(i)^\times)^2$$

because of $m^2 = x_1 + x_2 + x_3$, so that (6.5) is a homomorphism. We show that the kernel of (6.5) is $[1+i]\mathcal{E}_\lambda(\mathbf{Q}(i))$. Let (x_1, y_1) be a point in $\mathcal{E}_\lambda(\mathbf{Q}(i))$ and $(x_2, y_2) = [i](x_1, y_1)$. Then the first coordinate of $(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = [1+i](x_1, y_1)$ is

$$x_3 = \left(\frac{y_1}{(1+i)x_1} \right)^2 \in (\mathbf{Q}(i)^\times)^2.$$

Therefore $[1+i]\mathcal{E}_\lambda(\mathbf{Q}(i))$ is contained in the kernel. Conversely, suppose $[1+i](x_1, y_1)$ is in $\mathcal{E}_\lambda(\mathbf{Q}(i))$ and its first coordinate $\left(\frac{y_1}{(1+i)x_1} \right)^2$ is in $(\mathbf{Q}(i)^\times)^2$. Then $m = y_1 / ((1+i)x_1)$ is in $\mathbf{Q}(i)^\times$. On the other hand, since the second coordinate

$$y_3 = -m^3 - \frac{1+i}{2} y_1$$

of $[1+i](x_1, y_1)$ is in $\mathbf{Q}(i)^\times$, y_1 belongs to $\mathbf{Q}(i)^\times$, and x_1 is also in $\mathbf{Q}(i)^\times$. Accordingly, the kernel is contained in $[1+i]\mathcal{E}_\lambda(\mathbf{Q}(i))$. Therefore the induced homomorphism

$$\mathcal{E}_\lambda(\mathbf{Q}(i)) / [1+i]\mathcal{E}_\lambda(\mathbf{Q}(i)) \longrightarrow T_\lambda$$

is injective, so that bijective. Summing up, for a $\mathbf{Q}(\mathbf{i})$ -rational point (x, y) different from $(0, 0)$ and ∞ , either x or the first coordinate of $(x, y) + (0, 0)$ is of the form $\alpha^2 \mathbf{i}$ with non-zero $\alpha \in \mathbf{Q}(\mathbf{i})$. We write one of the obtained points with such property as $(\alpha^2 \mathbf{i}, \alpha\beta)$. Then $\alpha^2 \beta^2 = -\alpha^6 \mathbf{i} - \lambda \alpha^2 \mathbf{i}$. This means $\lambda = -\alpha^4 + \beta^2 \mathbf{i}$ and the proof has been completed. \square

Remark 6.6. We shall give some remarks on Proposition 6.4.

- (1) A prime λ of the form in (2) or (3) of Proposition 6.4 should be called a *Gaussian congruent number*.
- (2) In the examples in [A] each one of the statements (1), (2), and (3) of Proposition 6.4 is satisfied if and only if $\text{egs}(\lambda) = 0$.
- (3) In the examples of [A] such that $\text{egs}(\lambda) = 0$, except $\lambda \bar{\lambda} = 4817 \equiv 1 \pmod{16}$, we can take α, β in the integer ring $\mathbf{Z}[\mathbf{i}]$. See Example 6.7 below.
- (4) We summarize the situation as follows:

$$\begin{array}{ccc} \lambda \text{ is of the form } -\alpha^4 + \beta^2 \mathbf{i} & \xleftrightarrow{\text{Prop. 6.4}} & \text{rank } \mathcal{E}_\lambda(\mathbf{Q}(\mathbf{i})) > 0 \\ \xleftarrow{\text{BSD}} \xrightarrow{\text{Coates-Wiles}} L(1, \tilde{\chi}) = 0 & \xleftrightarrow{\text{Asai}} & \text{egs}(\lambda) = 0. \end{array}$$

- (5) In the proof of (1) \Rightarrow (2), we show that $\mathcal{E}_\lambda(\mathbf{Q}(\mathbf{i}))/[1 + \mathbf{i}]\mathcal{E}_\lambda(\mathbf{Q}(\mathbf{i}))$ is generated by $(0, 0)$ and at most one non-torsion point. Thus the $\mathbf{Z}[\mathbf{i}]$ -rank of $\mathcal{E}_\lambda(\mathbf{Q}(\mathbf{i}))$ is at most one. If $\text{egs}(\lambda) = 0$, then $\mathcal{E}_\lambda(\mathbf{Q}(\mathbf{i}))$ has $\mathbf{Z}[\mathbf{i}]$ -rank one, that is, MW-rank two.

Example 6.7. Take $\lambda = 41 + 56 \mathbf{i}$, $\ell = \lambda \bar{\lambda} = 4817 \equiv 1 \pmod{16}$. Then for

$$u = \frac{-7\mathbf{i}(2 + \mathbf{i})(4 + \mathbf{i})}{3(1 + 2\mathbf{i})(2 + 3\mathbf{i})}, \quad v = \frac{-(1 + \mathbf{i})^5(3 + 2\mathbf{i})(7 + 8\mathbf{i})(6 + 11\mathbf{i})}{3^2(1 + 2\mathbf{i})^2(2 + 3\mathbf{i})^2},$$

we see $\lambda = u^4 - v^2$ and that $P = (u^2, uv)$ is a point of infinite order. This is given by using MAGMA. It also says that the Mordell-Weil rank of \mathcal{E}_λ is 2. We know another rational point by MAGMA as follows. Let

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

Then $\lambda = -\alpha^4 + \beta^2 \mathbf{i}$ and $Q = (\alpha^2 \mathbf{i}, \alpha\beta)$ is in $\mathcal{E}_\lambda(\mathbf{Q}(\mathbf{i}))$ and $P = [1 + \mathbf{i}]Q$. We do not know the point Q generates how much part of the MW-group.

7 Vanishing EGS and Kummer-type congruence

We rewrite the expansion (1.2) of $\text{cl}(u)$. Namely, we define G_n in \mathbf{Z} by

$$\text{cl}(u) = \sum_{n=0}^{\infty} G_n \frac{u^n}{n!} = 1 - 2 \frac{u^2}{2!} + 12 \frac{u^4}{4!} - 216 \frac{u^6}{6!} + 7056 \frac{u^8}{8!} - 368928 \frac{u^{10}}{10!} + \cdots.$$

Of course $G_n = n! D_n$. We denote by H_ℓ the *Hasse invariant* of $y^2 = x^3 - x$ at ℓ ($\equiv 1 \pmod{4}$), namely,

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

Our main result is the following theorem.

Theorem 7.1. *The following three statements are equivalent:*

- (1) $\text{egs}(\lambda) = 0$;
- (2) $\ell \mid G_{\frac{3}{4}(\ell-1)}$; (*This is a special case of (3).*)
- (3) *For any integers a and n satisfying $n > a \geq 0$, $n + a(\ell - 1) \leq \ell(\ell - 1)$, and $n \equiv \frac{3}{4}(\ell - 1) \pmod{\ell - 1}$, it holds that*

$$\sum_{r=0}^a \binom{a}{r} (-H_\ell)^{a-r} \frac{G_{n+r(\ell-1)}}{n+r(\ell-1)} \equiv 0 \pmod{\ell^{a+1}}.$$

Remark 7.2. The least ℓ with $\text{egs}(\lambda) = 0$ is 89. The authors checked that the congruence in 7.1(3) holds for the cases $\ell = 89$, $0 \leq a \leq \ell$, and $n = \frac{7}{4}(\ell - 1)$ by PARI/GP. It took over four months. Note in these examples that the cases $a = \ell - 1$, ℓ break the inequality $n + a(\ell - 1) \leq \ell(\ell - 1)$.

8 ℓ -Adic explicit formula of an elliptic Gauss sum

Recall our identification of $\mathbf{Z}[i]_\lambda$ and \mathbf{Z}_ℓ . As we treat a plenty of power series in $\overline{\mathbf{Z}}_\ell[[x]]$ in this paper, we summarize convention on notation here. Let $f(x)$ and $g(x)$ be power series in $\overline{\mathbf{Z}}_\ell[[x]]$. For a rational number a in \mathbf{Q} , we write

$$f(x) \equiv g(x) \pmod{\lambda^a}$$

if all the coefficients of the terms in $f(x) - g(x)$ have ℓ -adic order at least a . For a positive integer m , we write

$$f(x) \equiv g(x) \pmod{\deg m}$$

if $f(x) - g(x)$ belongs to $x^m \overline{\mathbf{Z}}_\ell[[x]]$. Moreover, we write

$$f(x) \equiv g(x) \pmod{\deg m, \text{ mod } \lambda^a}$$

if all the coefficients of the terms of degree less than m in $f(x) - g(x)$ have ℓ -adic order at least a . From now on, the number

$$d = \frac{3}{4}(\ell - 1)$$

appears frequently. Taking a primitive $(\ell - 1)$ -th root ζ of 1 in \mathbf{Z}_ℓ , we define

$$(8.1) \quad \text{Cl}(u) = \frac{1}{2} \sum_{j=0}^{\ell-2} \zeta^{-dj} \text{cl}(\zeta^j u).$$

Then we have

$$\text{Cl}(u) = \frac{\ell - 1}{2} \sum_{a=0}^{\infty} G_{d+a(\ell-1)} \frac{u^{d+a(\ell-1)}}{(d+a(\ell-1))!}.$$

Thus $G_{d+a(\ell-1)}/(d+a(\ell-1))!$ is the coefficient of the term $u^n/n!$ with $n = d+a(\ell-1)-1$ in the power series expansion of $\frac{2}{\ell-1} \text{Cl}(u)/u$.

For a proof of Theorem 7.1, we give an ℓ -adic explicit formula of $\text{egs}(\lambda)$ by using the Lubin-Tate formal group.

Let $\mathbf{LT}(x, y)$ be the Lubin-Tate formal group over \mathbf{Z}_ℓ corresponding to the λ -plication $[\lambda]_{\mathbf{LT}}(x) = \lambda x + x^\ell$. Then non-zero points of the group $\mathbf{LT}[\lambda]$ of the λ -division points are roots of $\lambda + x^{\ell-1} = 0$. Let $f_0(x)$ be the formal logarithm of $\mathbf{LT}(x, y)$. It follows from $[\lambda]_{\mathbf{LT}}(x) = f_0^{-1}(\lambda f_0(x)) \equiv x^\ell \pmod{\lambda}$ that $\lambda f_0(x) \equiv f_0(x^\ell) \pmod{\lambda}$ by Lemma 4.2 of Honda [Ho]. Namely, $\mathbf{LT}(x, y)$ is of type $\lambda - T$. Let $\widehat{\mathbf{sl}}(x, y)$ be the formal group defined by

$$\widehat{\mathbf{sl}}(x, y) = \text{sl}(\text{sl}^{-1}(x) + \text{sl}^{-1}(y)).$$

By the definition of $\widehat{\mathbf{sl}}(x, y)$, the λ -plication $[\lambda]_{\widehat{\mathbf{sl}}}(x)$ satisfies

$$[\lambda]_{\widehat{\mathbf{sl}}} \circ \text{sl}(x) = \text{sl}(\lambda x).$$

Thus $[\lambda]_{\widehat{\mathbf{sl}}}(x)$ is equal to the λ -plication of $x = \text{sl}(u)$. We have

$$(8.2) \quad [\lambda]_{\widehat{\mathbf{sl}}}(x) = x \prod_{a=1}^{\ell-1} \left(x - \varphi\left(\frac{a}{\lambda}\right) \right) / \prod_{a=1}^{\ell-1} \left(1 - \varphi\left(\frac{a}{\lambda}\right)x \right),$$

which is Example 2.6 in [A], p.101. Especially, A is a point of the group $\widehat{\mathbf{sl}}[\lambda]$ of λ -division points. It is well-known (see for instance, Proposition 8.2 of [Le] or Theorem 1.28 in [O2] which gives another proof by using the relation $\wp(u) = \text{sl}(u)^{-2}$), but is shown also by using (8.2) that

$$[\lambda]_{\widehat{\mathbf{sl}}}(x) \equiv x^\ell \pmod{\lambda}.$$

Hence, the formal group $\widehat{\mathbf{sl}}(x, y)$ is of type $\lambda - T$ as well. Since the formal group $\mathbf{LT}(x, y)$ is of the same type $\lambda - T$, there exists the unique strong isomorphism ι over \mathbf{Z}_ℓ from $\mathbf{LT}(x, y)$ to $\widehat{\mathbf{sl}}(x, y)$. Namely, there uniquely exists $\iota(x)$ in $\mathbf{Z}_\ell[[x]]$ such that

$$\iota(\mathbf{LT}(x, y)) = \widehat{\mathbf{sl}}(\iota(x), \iota(y)), \quad \iota(x) \equiv x \pmod{\deg 2}.$$

Then there exists η of the group $\mathbf{LT}[\lambda]$ of λ -division points of $\mathbf{LT}(x, y)$ such that

$$A = \varphi(1/\lambda) = \iota(\eta).$$

We recall that $\eta^{\ell-1} = -\lambda$ (see (2.2)). Since

$$\text{cl}(u) = \phi \circ \text{sl}(u), \quad \text{where } \phi(x) = \sqrt{\frac{1-x^2}{1+x^2}},$$

we have

$$\psi(1/\lambda) = \phi \circ \iota(\eta).$$

We note that $\phi(x)$ is in $\mathbf{Z}_\ell[[x]]$.

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

$$\text{Sl}(u) = \frac{1}{4} \sum_{j=0}^{\ell-2} \zeta^{-dj} \text{sl}(\zeta^j u).$$

Then we have

$$\text{Sl}(u) = \frac{\ell-1}{4} \sum_{a=0}^{\infty} C_{d+a(\ell-1)} u^{d+a(\ell-1)}$$

as well as

$$\text{Cl}(u) = \frac{\ell-1}{2} \sum_{a=0}^{\infty} D_{d+a(\ell-1)} u^{d+a(\ell-1)}.$$

Lemma 8.3. (1) *If $\ell \equiv 5 \pmod{8}$, the equation $\text{egs}(\lambda) = (\text{Sl} \circ f_0)(\eta)$ holds.*
 (2) *If $\ell \equiv 1 \pmod{8}$, the equation $\text{egs}(\lambda) = (\text{Cl} \circ f_0)(\eta)$ holds.*

Proof. It follows from $[\zeta]_{\widehat{\text{sl}}}(x) = \text{sl}(\zeta \text{sl}^{-1}(x)) \in \mathbf{Z}_{\ell}[[x]]$ that $\text{Sl} \circ \text{sl}^{-1}(x)$ is in $\mathbf{Z}_{\ell}[[x]]$, and from $\text{sl}^{-1} \circ \iota(x) = f_0(x)$ that $\text{Sl} \circ f_0(x)$ is also in $\mathbf{Z}_{\ell}[[x]]$. Since $\text{cl}(u) = \phi \circ \text{sl}(u)$ and $\phi(x)$ is in $\mathbf{Z}_{\ell}[[x]]$, we see $\text{cl}(\zeta \text{sl}^{-1}(x)) = \phi \circ [\zeta]_{\widehat{\text{sl}}}(x)$ is in $\mathbf{Z}_{\ell}[[x]]$. Hence, $\text{Cl} \circ f_0(x)$ is in $\mathbf{Z}_{\ell}[[x]]$. For α in $\mathbf{Z}[i]$ coprime to λ , $\alpha \equiv \zeta^j \pmod{\lambda}$ for some j . Then $\varphi(\alpha/\lambda) = [\alpha]_{\widehat{\text{sl}}}(A) = [\zeta^j]_{\widehat{\text{sl}}}(A)$. Since $A = \iota(\eta)$ and $\text{sl}^{-1} \circ \iota(x) = f_0(x)$, we have $\varphi(\alpha/\lambda) = (\text{sl} \circ \zeta^j \text{sl}^{-1})(A) = (\text{sl} \circ \zeta^j f_0)(\eta)$. We also have $\psi(\alpha/\lambda) = (\text{cl} \circ \zeta^j f_0)(\eta)$. Since $\chi_{\lambda}(\alpha) = \chi_{\lambda}(\zeta^j) = \zeta^{-dj}$, we have

$$\text{egs}(\lambda) = \frac{1}{4} \sum_{\alpha=1}^{\ell-1} \chi_{\lambda}(\alpha) \varphi\left(\frac{\alpha}{\lambda}\right) = (\text{Sl} \circ f_0)(\eta)$$

in the case of $\ell \equiv 5 \pmod{8}$, and

$$\text{egs}(\lambda) = \frac{1}{2} \sum_{\alpha=1}^{\ell-1} \chi_{\lambda}(\alpha) \psi\left(\frac{\alpha}{\lambda}\right) = (\text{Cl} \circ f_0)(\eta)$$

in the case of $\ell \equiv 1 \pmod{8}$. This completes the proof of Lemma 8.3. \square

Lemma 8.4. (1) *If $\ell \equiv 5 \pmod{8}$, it holds that*

$$\text{egs}(\lambda) \equiv \frac{\ell-1}{4} C_d \eta^d \pmod{\eta^{\ell}}.$$

(2) *If $\ell \equiv 1 \pmod{8}$, it holds that*

$$\text{egs}(\lambda) \equiv \frac{\ell-1}{2} D_d \eta^d \pmod{\eta^{\ell}}.$$

Proof. Since $\lambda f_0(x) = f_0 \circ [\lambda]_{\text{LT}} = f_0(\lambda x + x^{\ell})$, we have $\lambda f_0(x) \equiv f_0(\lambda x) \pmod{\deg \ell}$. Thus we have $f_0(x) \equiv x \pmod{\deg \ell}$ and

$$\text{Sl} \circ f_0(x) \equiv \text{Sl}(x) \equiv \frac{\ell-1}{4} C_d x^d \pmod{\deg \ell}.$$

Similarly we have

$$\text{Cl} \circ f_0(x) \equiv \text{Cl}(x) \equiv \frac{\ell-1}{2} D_d x^d \pmod{\deg \ell}.$$

Since $\text{Sl} \circ f_0(x)$ and $\text{Cl} \circ f_0(x)$ belong to $\mathbf{Z}_{\ell}[[x]]$, the assertion follows. \square

Proof of Theorem 5.8. Because of $\tilde{\lambda} = \gamma(S)^{-1} \prod_{r \in S} \varphi(r/\lambda) \equiv \eta^{\frac{\ell-1}{4}} \pmod{\eta^{\frac{\ell-1}{4}+1}}$ and $\text{egs}(\lambda) = A_{\lambda} \tilde{\lambda}^3$, Lemma 8.4 implies

$$A_{\lambda} \equiv -\frac{1}{2} D_d \pmod{\eta^{\frac{\ell-1}{4}+1}}.$$

Since both sides belong to $\mathbf{Z}[\zeta_8]$, we have the assertion of Theorem 5.8. \square

9 Application of the Hochschild formula

In this section, we use the following formula known as the *Hochschild formula*. For a proof of this formula, see Matsumura [Ma], p.197, Theorem 25.5.

Lemma 9.1. *Let R be a commutative ring of characteristic ℓ . Let δ be a derivation over R . Then, for any element b in R , we have*

$$(b\delta)^\ell = b^\ell \delta^\ell + ((b\delta)^{\ell-1}(b)) \cdot \delta.$$

We put $u = f_0(x)$. By the definition of H_ℓ , we have $(\bar{\lambda} - T)(\lambda - T) = \ell - H_\ell T + T^2$. Since $\bar{\lambda} - T$ is a unit in $\mathbf{Z}_\ell[[T]]$, any formal group over \mathbf{Z}_ℓ of type $\lambda - T$ is also of type $\ell - H_\ell T + T^2$.

Lemma 9.2. *Let $\phi(x)$ be a power series in $\mathbf{Z}_\ell[[x]]$. Then*

$$(9.3) \quad \left(\left(\frac{d}{du} \right)^\ell - H_\ell \frac{d}{du} \right) \phi(x) \in \ell \mathbf{Z}_\ell[[x]].$$

Proof. Since $du/dx = f_0'(x)$ is in $\mathbf{Z}_\ell[[x]]^\times$, $\frac{d}{du} = \frac{dx}{du} \frac{d}{dx}$ is a derivation on $\mathbf{Z}_\ell[[x]]$. Since $\mathbf{LT}(x, y)$ is of type $\ell - H_\ell T + T^2$, there exists $h(x)$ in $\mathbf{Z}_\ell[[x]]$ such that

$$\ell f_0(x) - H_\ell f_0(x^\ell) + f_0(x^{\ell^2}) = \ell h(x).$$

This yields that

$$f_0'(x) - H_\ell f_0'(x^\ell) x^{\ell-1} \equiv h'(x) \pmod{\ell}.$$

Differentiating this $\ell - 1$ times by x , we have

$$f_0^{(\ell)}(x) - H_\ell f_0'(x^\ell) (\ell - 1)! \equiv h^{(\ell)}(x) \pmod{\ell}.$$

By $(\ell - 1)! \equiv -1 \pmod{\ell}$, $f_0'(x)$ in $\mathbf{Z}_\ell[[x]]$, and $h^{(\ell)}(x) \equiv 0 \pmod{\ell}$, we have

$$(9.4) \quad f_0^{(\ell)}(x) + H_\ell (f_0'(x))^\ell \equiv 0 \pmod{\ell}.$$

Let $\phi(x)$ be a power series in $\mathbf{Z}_\ell[[x]]$.

$$0 \equiv \left(\frac{d}{dx} \right)^\ell \phi(x) \equiv \left(\frac{du}{dx} \frac{d}{du} \right)^\ell \phi(x) \pmod{\ell}.$$

By using the Hochschild formula (Lemma 9.1), we have

$$0 \equiv \left(\frac{du}{dx} \right)^\ell \frac{d^\ell \phi}{du^\ell} + \left(\frac{du}{dx} \frac{d}{du} \right)^{\ell-1} \frac{du}{dx} \cdot \frac{d\phi}{du} \equiv \left(\frac{du}{dx} \right)^\ell \frac{d^\ell \phi}{du^\ell} + \frac{d^\ell u}{dx^\ell} \cdot \frac{d\phi}{du} \pmod{\ell}.$$

Thus we have

$$\frac{d^\ell \phi}{du^\ell} + \left(\frac{du}{dx} \right)^{-\ell} \frac{d^\ell u}{dx^\ell} \cdot \frac{d\phi}{du} \equiv 0 \pmod{\ell}.$$

By (9.4) we have

$$(9.5) \quad \frac{d^\ell \phi}{du^\ell} - H_\ell \frac{d\phi}{du} \equiv 0 \pmod{\ell \mathbf{Z}_\ell[[x]]}.$$

This completes the proof of Lemma 9.2. \square

Let c be a non-negative integer. Let $\phi(x)$ be any element in $\ell^c \mathbf{Z}_\ell[[x]]$. We define the expansion of $\phi \circ \text{sl}(u)$ by

$$\phi \circ \text{sl}(u) = \sum_{k \geq 0} \frac{b_k}{k!} u^k \quad (b_k \in \mathbf{Q}_\ell).$$

We denote

$$\Omega_\ell = \left(\frac{d}{du} \right)^\ell - H_\ell \frac{d}{du}.$$

For any non-negative integer a , we see $\Omega_\ell^a \phi(x)$ in $\ell^{a+c} \mathbf{Z}_\ell[[x]]$ by (9.5). Since

$$\Omega_\ell^a \left(\sum_{k \geq 0} \frac{b_k}{k!} u^k \right) = \sum_{k \geq 0} \left(\sum_{r=0}^a \binom{a}{r} (-H_\ell)^{a-r} b_{k+a+r(\ell-1)} \right) \frac{u^k}{k!} \in \ell^{a+c} \mathbf{Z}_\ell[[x]] \subset \ell^{a+c} \mathbf{Z}_\ell \langle\langle u \rangle\rangle,$$

we have

$$(9.6) \quad \sum_{r=0}^a \binom{a}{r} (-H_\ell)^{a-r} b_{k+a+r(\ell-1)} \equiv 0 \pmod{\ell^{a+c}}.$$

10 Proof of the main theorem

We prove the implications (1) \Rightarrow (3) \Rightarrow (2) in Theorem 7.1.

Proof of (3) \Rightarrow (2) of Theorem 7.1. Plugging $a = 0$ and $n = d$ in (3) of Theorem 7.1, we have

$$\frac{G_d}{d} \equiv 0 \pmod{\ell},$$

which is (2) in Theorem 7.1. \square

Lemma 10.1. *If $\text{egs}(\lambda) = 0$, then $(\text{Cl} \circ f_0)(x)/(\lambda x + x^\ell)$ is in $\mathbf{Z}_\ell[[x]]$.*

Proof. Assume $\text{egs}(\lambda) = 0$ and put $(\text{Cl} \circ f_0)(x) = \sum_{n=0}^{\infty} b_n x^n$ with b_n in \mathbf{Z}_ℓ . Then, $(\text{Cl} \circ f_0)(\eta) = \sum_{n=0}^{\infty} b_n \eta^n = 0$ by Lemma 8.3. Therefore,

$$(\text{Cl} \circ f_0)(x) = \sum_{n=0}^{\infty} b_n x^n - \sum_{n=0}^{\infty} b_n \eta^n = (x - \eta) \sum_{n=1}^{\infty} b_n \frac{x^n - \eta^n}{x - \eta} \in \mathbf{Z}_\ell[\eta][[x]]$$

because $x - \eta$ divides $x^n - \eta^n$. Similarly, any conjugate of $x - \eta$ divides $(\text{Cl} \circ f_0)(x)$ and x divides $(\text{Cl} \circ f_0)(x)$. Hence, the assertion follows. \square

The following two lemmas are formulated little stronger than for use in the proof of implication from (1) to (3) in Theorem 7.1.

Lemma 10.2. *Let ν be a positive integer. Assume $\text{egs}(\lambda) = 0$. If $n < \nu\ell(\ell-1)$, then the coefficient in $\lambda^{\nu-1}(\text{Cl} \circ f_0)(x)/f_0(x)$ of x^n belongs to $\ell \mathbf{Z}_\ell$.*

Proof. Since $f_0'(x)$ is in $\mathbf{Z}_\ell[[x]]$, it is seen that $\xi^{-1} f_0(\xi x)$ is in $\mathbf{Z}_\ell[\xi][[x]]$ for any ℓ -adic algebraic integer ξ with $\text{ord}(\xi) = 1/(\ell-1)$ by calculating the ℓ -adic order of each coefficients of its expansion. We put

$$g(x) = \frac{\lambda x + x^\ell}{\lambda f_0(x)} = \frac{\lambda x + x^\ell}{f_0(\lambda x + x^\ell)}.$$

Since $\text{ord}(\lambda\xi^{\frac{1}{\ell}-1}) = 1 - 1/\ell$ and $\xi^{-1}f_0(\xi x)/x$ is a unit in $\mathbf{Z}_\ell[\xi][[x]]$,

$$g(\xi^{\frac{1}{\ell}}x) = \frac{\xi(\lambda\xi^{\frac{1}{\ell}-1}x + x^\ell)}{f_0(\xi(\lambda\xi^{\frac{1}{\ell}-1}x + x^\ell))} \in \mathbf{Z}_\ell[\xi^{\frac{1}{\ell}}][[x]].$$

Thus the ℓ -adic order of the coefficient of x^n of $g(x)$ is greater than or equal to $-\lfloor \frac{n}{\ell(\ell-1)} \rfloor$. Therefore, we see

$$\lambda^\nu g(x) \equiv 0 \pmod{\deg \nu\ell(\ell-1), \text{ mod } \lambda}.$$

Thus, each coefficient of the terms of degree less than $\nu\ell(\ell-1)$ in

$$\lambda^{\nu-1} \frac{\text{Cl}(u)}{u} = \lambda^{\nu-1} \frac{\text{Cl} \circ f_0(x)}{f_0(x)} = \frac{\text{Cl} \circ f_0(x)}{\lambda x + x^\ell} \cdot \lambda^\nu g(x)$$

is in $\ell\mathbf{Z}_\ell$ by Lemma 10.1. \square

Lemma 10.3. *Assume that $\text{egs}(\lambda) = 0$. Let a , n , and ν be integers such that $n > a \geq \nu - 1 \geq 0$, $n + a(\ell - 1) \leq \nu\ell(\ell - 1)$ and $n \equiv d \pmod{\ell - 1}$. Then it holds that*

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

Proof. We denote by $\phi(x)$ the sum of the terms in $\frac{2}{\ell-1}\lambda^{\nu-1}(\text{Cl} \circ f_0(x))/f_0(x)$ of degree less than $\nu\ell(\ell-1)$ with respect to x . From Lemma 10.2, we see $\phi(x)$ in $\ell\mathbf{Z}_\ell[[x]]$. Then the coefficient b_k of $\frac{u^k}{k!}$ in the expansion of $\phi(x)$ with respect to u is given by

$$b_k = \begin{cases} \lambda^{\nu-1} \frac{G_{k+1}}{k+1} & \text{if } k+1 \equiv d \pmod{\ell-1} \text{ and } k < \nu\ell(\ell-1), \\ 0 & \text{if } k+1 \not\equiv d \pmod{\ell-1} \text{ and } k < \nu\ell(\ell-1), \end{cases}$$

whereas we do not concern the other b_k s. Now, the last argument in the previous section is applied for this $\phi(x)$ with $c = 1$. By using (9.6), for the integers a and n in the statement, we have

$$(10.4) \quad \lambda^{\nu-1} \sum_{r=0}^a \binom{a}{r} (-H_\ell)^{a-r} \frac{G_{n+r(\ell-1)}}{n+r(\ell-1)} \equiv 0 \pmod{\ell^{a+1}},$$

hence the desired congruence. \square

Proof of (1) \implies (3) of Theorem 7.1. Done by setting $\nu = 1$ in Lemma 10.3. \square

Remark 10.5. (1) On the classical Bernoulli numbers, if $b \leq d$, then

$$\frac{B_d}{d} \equiv \frac{B_{d+mp^{b-1}(p-1)}}{d+mp^{b-1}(p-1)} \pmod{p^b}.$$

Here the condition $b \leq d$ is essential. However, for any b , d , and m , it is known that

$$(10.6) \quad (1-p^{d-1})\frac{B_d}{d} \equiv (1-p^{d+mp^{b-1}(p-1)-1})\frac{B_{d+mp^{b-1}(p-1)}}{d+mp^{b-1}(p-1)} \pmod{p^b}.$$

Of course, the extra factors are no other than Euler p -factors of the Riemann ζ -function. From this consideration we are interested in the following problem. Assuming $\text{egs}(\lambda) = 0$, does the congruence

$$(10.7) \quad \frac{G_{e+m\ell^b(\ell-1)}}{e+m\ell^b(\ell-1)} \equiv H_\ell^{m\ell^b} \cdot \frac{G_e}{e} \pmod{\ell^{b+2}}$$

hold for any non-negative integers m , b , and e with $e \equiv d \pmod{\ell-1}$ or not? Namely, there might be required no additional condition on b and e , which is suggested by the fact that the Euler λ -factor of the Hecke L -function for $\mathcal{E}_{\pm\lambda}$ is 1.

(2) On Kubota-Leopoldt p -adic L -function, it is fundamental that the special values of the corresponding complex L -function is given by (generalized) Bernoulli numbers and they satisfy (10.6) involving Euler p -factor of the complex L -series. However the congruence (10.7) is a relation on the numbers which are not exactly the special values but only their residues modulo some power of ℓ .

11 Central value of the Hecke L -function

In this section we refer to Koblitz [K]. We modify §5 and §6 of Chapter 2 in [K].

Put $\mathcal{O} = \mathbf{Z}[i]$ and take β in \mathcal{O} . Let $\tilde{\chi}$ be a Hecke character of modulus (β) of weight one. Namely, $\tilde{\chi}((\nu)) = \chi_1(\nu)\bar{\nu}$, where χ_1 is a character form $(\mathcal{O}/(\beta))^\times$ to \mathbf{C}^\times satisfying $\chi_1(i) = i$. We define the Hecke L -function by

$$\begin{aligned} L(s, \tilde{\chi}) &= \sum_{\mathfrak{a}} \frac{\tilde{\chi}(\mathfrak{a})}{N\mathfrak{a}^s} = \frac{1}{4} \sum_{\nu \in \mathcal{O}} \frac{\chi_1(\nu)\bar{\nu}}{|\nu|^{2s}} \\ &= \frac{1}{4} \sum_{\gamma \pmod{\beta}} \chi_1(\gamma) \sum_{\alpha \in \mathcal{O}} \frac{\overline{\gamma + \alpha\beta}}{|\gamma + \alpha\beta|^{2s}}, \end{aligned}$$

where \mathfrak{a} runs over the non-zero integral ideals of \mathcal{O} and $N\mathfrak{a} = \# \mathcal{O}/\mathfrak{a}$ is the norm of \mathfrak{a} .

We use a method which obtains the following classically known fact.

Theorem 11.1. *The function defined by*

$$\Lambda(s, \tilde{\chi}) = \left(\frac{2\pi}{\sqrt{4N(\beta)}} \right)^{-s} \Gamma(s) L(s, \tilde{\chi})$$

satisfies

$$\Lambda(s, \tilde{\chi}) = C(\tilde{\chi}) \Lambda(2-s, \bar{\tilde{\chi}}),$$

where $C(\tilde{\chi}) = -i\beta^{-1} \sum_{\lambda \pmod{\beta}} \chi_1(\lambda) e^{2\pi i \text{Re}(\lambda/\beta)}$.

We do not need the result above itself but the following bi-product of its proof.

Lemma 11.2. *We have the estimation*

$$|L(1, \tilde{\chi})| < \frac{4}{e^{\pi/|\beta|} - 1}.$$

Proof. First of all, we note that $(2\pi/\sqrt{4N(\beta)})^{-s} = |\beta|^s \pi^{-s}$ because of $|\beta| = \sqrt{N(\beta)}$. We give an outline of proof which is divided into four steps.

(Step 1) We define

$$F(t, \tilde{\chi}) = \frac{1}{4} \sum_{\nu \in \mathcal{O}} \chi_1(\nu) \bar{\nu} e^{-\pi t |\nu|^2}.$$

Then, by using $\int_0^\infty e^{-ct} t^s \frac{dt}{t} = c^{-s} \Gamma(s)$, we have

$$(11.3) \quad \pi^{-s} \Gamma(s) L(s, \tilde{\chi}) = \int_0^\infty F(t, \tilde{\chi}) t^s \frac{dt}{t}.$$

(Step 2) The function $F(t, \tilde{\chi})$ is rewritten

$$\begin{aligned} F(t, \tilde{\chi}) &= \frac{1}{4} \sum_{\gamma \bmod \beta} \chi_1(\gamma) \sum_{\alpha \in \mathcal{O}} \overline{\beta\alpha + \gamma} e^{-\pi t |\beta\alpha + \gamma|^2} \\ &= \frac{\bar{\beta}}{4} \sum_{\gamma \bmod \beta} \chi_1(\gamma) \sum_{\alpha \in \mathcal{O}} \overline{\alpha + \frac{\gamma}{\beta}} e^{-\pi t |\beta|^2 |\alpha + \frac{\gamma}{\beta}|^2} \end{aligned}$$

By using a vector in \mathbf{R}^2 , we write the inner sum. For a given γ , we put $\frac{\gamma}{\beta} = u_1 + u_2 i$ with $u = (u_1, u_2)$ in \mathbf{Q}^2 , $\alpha = m_1 + m_2 i$ with $m = (m_1, m_2)$ in \mathbf{Z}^2 . Then we have

$$\begin{aligned} \sum_{\alpha \in \mathcal{O}} \overline{\alpha + \frac{\gamma}{\beta}} e^{-\pi t |\beta|^2 |\alpha + \frac{\gamma}{\beta}|^2} &= \sum_{m \in \mathbf{Z}^2} \overline{(m+u) \cdot (1, i)} e^{-\pi t |\beta|^2 |m+u|^2} \\ &= \sum_{m \in \mathbf{Z}^2} (m+u) \cdot (1, -i) e^{-\pi t |\beta|^2 |m+u|^2}, \end{aligned}$$

where \cdot stands for the inner product. For u in \mathbf{R}^2 and w in \mathbf{C}^2 , we define

$$\theta_u(t) = \sum_{m \in \mathbf{Z}^2} (m+u) \cdot w e^{-\pi t |m+u|^2}.$$

Setting $w = (1, -i)$, we have, for $u = (u_1, u_2) \in \mathbf{Q}^2$ defined before depending on γ ,

$$F(t, \tilde{\chi}) = \frac{\bar{\beta}}{4} \sum_{\gamma \bmod \beta} \chi_1(\gamma) \theta_u(|\beta|^2 t).$$

(Step 3) For u in \mathbf{R}^2 and w in \mathbf{C}^2 , we define

$$\theta^u(t) = \sum_{m \in \mathbf{Z}^2} m \cdot w e^{2\pi i m \cdot u} e^{-\pi t |m|^2}.$$

Then, we have (cf. [K], p.85, (5.16))

$$(11.4) \quad \theta_u(t) = -\frac{i}{t^2} \theta^u\left(\frac{1}{t}\right).$$

By using the functional equation (11.4), we prove that of $F(t, \tilde{\chi})$.

$$F\left(\frac{1}{|\beta|^2 t}, \tilde{\chi}\right) = \frac{\bar{\beta}}{4} \sum_{\gamma \bmod \beta} \chi_1(\gamma) \theta_u\left(\frac{1}{t}\right) = \frac{\bar{\beta}}{4} \sum_{\gamma \bmod \beta} \chi_1(\gamma) (-it^2) \theta^u(t).$$

By the definition of $\theta^u(t)$, we calculate the right hand side.

$$\begin{aligned} F\left(\frac{1}{|\beta|^2 t}, \tilde{\chi}\right) &= \frac{\bar{\beta}}{4} \sum_{\gamma \bmod \beta} \chi_1(\gamma) (-it^2) \sum_{m \in \mathbf{Z}^2} m \cdot (1, -i) e^{2\pi i m \cdot u} e^{-\pi t |m|^2} \\ &= \frac{\bar{\beta}}{4} (-it^2) \sum_{m \in \mathbf{Z}^2} m \cdot (1, -i) e^{-\pi t |m|^2} \sum_{\gamma \bmod \beta} \chi_1(\gamma) e^{2\pi i m \cdot u}. \end{aligned}$$

It follows from $m \cdot u = m_1 u_1 + m_2 u_2 = \operatorname{Re}((m_1 - m_2 i)(u_1 + u_2 i)) = \operatorname{Re}(\bar{\alpha} \frac{\gamma}{\beta})$ that the sum inside is essentially Gauss sum and

$$\begin{aligned} \sum_{\gamma \bmod \beta} \chi_1(\gamma) e^{2\pi i m \cdot u} &= \overline{\chi_1(\bar{\alpha})} \sum_{\gamma \bmod \beta} \chi_1(\bar{\alpha} \gamma) e^{2\pi i \operatorname{Re}(\bar{\alpha} \gamma / \beta)} \\ &= \overline{\chi_1(\bar{\alpha})} \sum_{\gamma \bmod \beta} \chi_1(\gamma) e^{2\pi i \operatorname{Re}(\gamma / \beta)} = \overline{\chi_1(\bar{\alpha})} i \beta C(\tilde{\chi}). \end{aligned}$$

Since

$$\sum_{m \in \mathbf{Z}^2} m \cdot (1, -i) e^{-\pi t |m|^2} = \sum_{\alpha \in \mathcal{O}} \bar{\alpha} e^{-\pi t |\bar{\alpha}|^2} = \sum_{\alpha \in \mathcal{O}} \alpha e^{-\pi t |\alpha|^2}$$

and $\tilde{\chi}(\nu) = \overline{\chi_1(\nu)} \nu$,

$$(11.5) \quad F\left(\frac{1}{|\beta|^2 t}, \tilde{\chi}\right) = \frac{\bar{\beta} \beta}{4} t^2 C(\tilde{\chi}) \sum_{\alpha \in \mathcal{O}} \overline{\chi_1(\bar{\alpha})} \alpha e^{-\pi t |\alpha|^2} = |\beta|^2 t^2 C(\tilde{\chi}) F(t, \tilde{\chi}).$$

(Step 4) From (11.3) we have

$$\begin{aligned} \pi^{-s} \Gamma(s) L(s, \tilde{\chi}) &= \int_0^\infty t^s F(t, \tilde{\chi}) \frac{dt}{t} \\ &= \int_0^{\frac{1}{|\beta|}} t^s F(t, \tilde{\chi}) \frac{dt}{t} + \int_{\frac{1}{|\beta|}}^\infty t^s F(t, \tilde{\chi}) \frac{dt}{t}, \end{aligned}$$

in which the former integration is rewritten as

$$\begin{aligned} \int_0^{\frac{1}{|\beta|}} t^s F(t, \tilde{\chi}) \frac{dt}{t} &= |\beta|^{-2s} \int_{\frac{1}{|\beta|}}^\infty v^{-s} F\left(\frac{1}{|\beta|^2 v}, \tilde{\chi}\right) \frac{dv}{v} \\ &= |\beta|^{2-2s} C(\tilde{\chi}) \int_{\frac{1}{|\beta|}}^\infty v^{2-s} F(v, \tilde{\chi}) \frac{dv}{v} \end{aligned}$$

by replacing $t = \frac{1}{|\beta|^2 v}$ and $\frac{dt}{t} = -\frac{dv}{v}$. In the case of $s = 1$, we have

$$\pi^{-1} L(1, \tilde{\chi}) = C(\tilde{\chi}) \int_{\frac{1}{|\beta|}}^\infty F(t, \tilde{\chi}) dt + \int_{\frac{1}{|\beta|}}^\infty F(t, \tilde{\chi}) dt.$$

We put

$$L(s, \tilde{\chi}) = \sum_{m=1}^\infty \frac{b_m}{m^s} \quad (b_m \in \mathcal{O}).$$

Then we have

$$\begin{aligned} L(s, \tilde{\chi}) &= \sum_{m=1}^{\infty} \frac{\overline{b_m}}{m^s}, \\ F(t, \tilde{\chi}) &= \sum_{m=1}^{\infty} b_m e^{-\pi m t}, \\ F(t, \overline{\tilde{\chi}}) &= \sum_{m=1}^{\infty} \overline{b_m} e^{-\pi m t}. \end{aligned}$$

It follows from $|\overline{b_m}| = |b_m|$ that

$$|F(t, \tilde{\chi})| \leq \sum_{m=1}^{\infty} |b_m| e^{-\pi m t}, \quad |F(t, \overline{\tilde{\chi}})| \leq \sum_{m=1}^{\infty} |b_m| e^{-\pi m t}.$$

As $|C(\tilde{\chi})| = 1$, we see

$$\pi^{-1} |L(1, \tilde{\chi})| \leq 2 \int_{\frac{1}{|\beta|}}^{\infty} \sum_{m=1}^{\infty} |b_m| e^{-\pi m t} dt = 2 \sum_{m=1}^{\infty} \frac{|b_m|}{\pi m} e^{-\pi m / |\beta|}.$$

Multiplying by π on both sides and by using $|b_m| \leq \sigma_0(m) \sqrt{m} \leq 2m$, where $\sigma_0(m)$ denotes the number of positive divisors of m (cf. [K], p. 96, Prob. 4 of p. 97), we have

$$|L(1, \tilde{\chi})| \leq 4 \sum_{m=1}^{\infty} e^{-\pi m / |\beta|} = \frac{4e^{-\pi / |\beta|}}{1 - e^{-\pi / |\beta|}} = \frac{4}{e^{\pi / |\beta|} - 1}$$

as desired. \square

12 Estimate of the coefficients of elliptic Gauss sums

In this section we show (2) implies (1) in Theorem 7.1. At first we prove Lemma 4.2 whose proof has been reserved.

Proof of Lemma 4.2. Since $1/(e^{\pi / |\beta|} - 1) < |\beta|/\pi$, we have $|L(1, \tilde{\chi})| < 4 \times |\beta|/\pi$. For $\ell \equiv 1 \pmod{8}$ and the conductor $(\beta) = ((1 + i)^3 \lambda)$, we see

$$4 \cdot \frac{2\sqrt{2} \cdot |\lambda|}{\pi} > |L(1, \tilde{\chi})| = \varpi \frac{1}{2} |A_\lambda| |\lambda|^{-1} |\lambda|^{\frac{3}{4}} = \varpi \frac{1}{2} |A_\lambda| |\lambda|^{-\frac{1}{4}}$$

from Theorem 5.3, (5.2), and Lemma 11.2. So that we have $|A_\lambda| < (16\sqrt{2}/\pi \varpi) |\lambda|^{\frac{5}{4}}$. The right hand side is smaller than $\frac{1}{2} \ell$ for $\ell \geq 97$ because $97^{\frac{3}{8}} = 5.55 \dots > \frac{32\sqrt{2}}{\pi \varpi} = 5.49 \dots$. For $\ell < 97$, the inequality $|A_\lambda| < \ell/2$ actually holds by the tables in [A]. \square

Proof of (2) \Rightarrow (1) of Theorem 7.1. Assume that $\ell | G_d$. Then by Lemma 8.4 we have $\ell | \text{egs}(\lambda)$. By Theorem 5.2, we have $\tilde{\lambda}_0 | A_\lambda$, where $\tilde{\lambda}_0$ is the prime defined in Theorem 5.8, and we see $\ell | a_\lambda$. On the other hand, by Theorem 5.3 and Lemma 4.2, we have $|a_\lambda| \leq |A_\lambda| \leq \ell/2$. Thus we have $a_\lambda = A_\lambda = 0$ and $\text{egs}(\lambda) = 0$. \square

References

- [A] Asai, T., Elliptic Gauss sums and Hecke L -values at $s = 1$, *RIMS Kôkyûroku Bessatsu*, **4**(2007) 79-121.
- [BSD] Birch, B.J. and Swinnerton-Dyer, H.P.F., Notes on elliptic curves II, *J. reine und angew. Math.*, **218**(1965) 79-108.
- [CW] Coates, J. and Wiles, A., On the conjecture of Birch and Swinnerton-Dyer, *Invent. math.*, **39**(1977) 223-251.
- [C] Cassels, J.W.S., Lectures on elliptic curves, London Math. Soc. Student Texts **24**, Cambridge Univ. Press, 1991.
- [D] Deuring, M. : Die Zetafunktionen einer algebraischen Kurve vom Geschlechte Eins (III), *Nachr. Acad. Wiss. Göttingen*, (1956)37-76
- [Di] Dickson, L.E., History of the theory of numbers I, Carnegie Institution of Washington 1919.
- [Ha] Hazewinkel, T., Formal groups and applications, Academic Press, 1978, reprinted by A.M.S. Chelsea publishing, 2012.
- [Ho] Honda, T., On the theory of commutative formal groups, *J. Math. Soc. Japan*, **22** (1970), 213-246.
- [H1] Hurwitz, A., Über die Anzahl der Klassen binärer quadratischer Formen von negativer Determinante, *Acta Math.*, **19**(1895) 351-384.
- [H2] Hurwitz, A., Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, *Nachr. Acad. Wiss. Göttingen*, (1897)273-276, (Werke, Bd.II, pp.338–341).
- [H3] Hurwitz, A., Über die Entwicklungskoeffizienten der lemniskatischen Funktionen, *Math. Ann.*, **51** (1899) 196–226, (Werke, Bd.II, pp.342–373).
- [K] Koblitz, N., Introduction to elliptic curves and modular forms (2nd ed.), G.T.M. **97**, 1993.
- [Le] Lemmermeyer, F., Reciprocity laws, Springer-Verlag Berlin Heiderberg 2010.
- [L] Lutz, E., Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps \mathfrak{p} -adiques, *J. reine und angew. Math.*, **177**(1937) 238-247.
- [Ma] Matsumura, H., Commutative ring theory, Cambridge studies in advanced mathematics **8**, Cambridge Univ. Press 1986.
- [M] Matthews, C.R., Gauss sums and elliptic functions, II The quartic sum, *Invent. math.*, **54**(1979) 23-52.
- [N] Nagell, T., Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre, *Skifter utg. av det Norske Vidensk.-Akad. i Oslo, Mat.-Naturv. Kl.* (1935), No.1, 1-25.
- [O] Ônishi, Y., Congruence relations connecting Tate-Shafarevich groups with Hurwitz numbers, *Interdisciplinary Information Sciences*, **16**(2010)71-86.
- [O2] Ônishi, Y., Integrality of coefficients of division polynomials for elliptic Functions, <http://www2.meijo-u.ac.jp/~yonishi/index.html#publications>, (2011)
- [ST] Serre, J.-P. and Tate, J., Good reduction of Abelian varieties, *Ann. of Math.*, 2nd Ser., **88**(1968) 492-517 (= J.-P. Serre: Oeuvres, Tom 2, 1986, Springer-Verlag, pp.472-497) (= Collected Works of John Tate, Part 1, AMS 2010, pp.377-402)
- [Si] Silverman, J., The arithmetic of elliptic curves (2nd ed.), G.T.M. **106**, Springer-Verlag. 2009
- [T] Takagi, T., Über eine Theorie des relative Abel'schen Zahlkörpers, *J. College of Science, Imperial Univ. of Tokyo* **41**(1920) 1-133, (Especially §32). (= Collected Papers, Iwanami Shoten 1973, pp.73-167).