Interdisciplinary of Information Sciences, **16** (2010) 71-86,
"Proceedings of Japan-Korea Joint Seminar on Number Theory and Related Topics" 2008

Congruence Relations Connecting Tate-Shafarevich Groups with Hurwitz Numbers

Yoshihiro Ônishi

Faculty of Humanities and Social Sciences, Iwate University, Japan

Email : onishi@iwate-u.ac.jp

Abstract

Let $p > 3$ be a rational prime congruent to 3 modulo 4, and $h(-p)$ be the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$. Then $h(-p) \equiv -2\,B_{\frac{p+1}{2}} \mod p$, where B_n is the n-th Bernoulli number. This is a quite classical congruence. Under the full BSD conjecture, we provide an easy method to obtain the natural explicit generalization of this, which is a congruence between the conjectural order of the Tate-Shafarevich group for certain elliptic curve with Mordell-Weil rank 0 and a coefficient of power series expansion of an elliptic function associating the elliptic curve.

AMS subject classification : 11G05, 11R29, 11B68
Key words : Bernoulli-Hurwitz numbers, elliptic Gauss sums, Tate-Shafarevich groups

Introduction

Keeping in mind that the Tate-Shafarevich group of an elliptic curve is an analogy of the ideal class group of a number field, the purpose of this paper is to give quickly an explicit analogue of the following theorem, though the results themselves may be obtained by standard method from known results.

Theorem 0.1. *Let $p > 3$ be a prime and $h(-p)$ be the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$. One has*

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

where B_n is the n-th Bernoulli number and E_n is the n-th Euler number[1]*. Here the smallest residue modulo p in $\mathbf{Z}$ of the right hand side with respect to absolute value is just equal to the left hand side*[2]*.*

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

[2] There arises a question "Can we explain, without going through class numbers, why the smallest residue of the right hand side is quite smaller than p?" Similar question arises for Theorem 2.4, too.

The first congruence in Theorem 0.1 (the case of $p \equiv 3 \bmod 4$) is quite classical (e.g. [IR], p.238), and the second one (the case of $p \equiv 1 \bmod 4$) is given in [ZX] and [Yu], for example. Both congruences are easily derived from analytic property (Theorem 5.12 in [Wa] for instance) of p-adic Dirichlet L-function[3]. However, such implication of the congruences from the theory of L-function does not seem to be well-known extensively even for researchers. Indeed, every bibliography which mentions these congruences ignores such background.

Nowadays, we have direct and fruitful generalizations of the p-adic Dirichlet L-functions to p-adic Hecke L-functions, due to Coates-Wiles, Rubin, and others ([CW], [R], [K], [Ya], etcetera). If we have worked out a calculation by using the theory of p-adic Hecke L-function including the Birch and Swinnerton-Dyer conjecture, we should have congruences analogous to Theorem 0.1 which is a (conjectural) congruence connecting orders of Tate-Shafarevich groups and certain coefficients (called Hurwitz numbers) of power series expansion of a suitable elliptic function associated to an elliptic curve.

However, in this paper, we demonstrate a very simple method to obtain such congruences (under the full BSD conjecture). Moreover, in Appendix of this paper, both congruences in 0.1 also are derived unitedly by our method with combining Dirichlet's class number formula.

To explain the main results, let λ run through degree 1 primes in the ring $\mathbf{Z}[\boldsymbol{i}]$ of the Gauss integers. One of the main results of this paper concern certain family of elliptic curves $\{\mathscr{E}_{\lambda^*}\}$ parametrized by λ (for the exact definition, see (3.2)).

Assuming the full statement of the Birch and Swinnerton-Dyer conjecture for $\mathscr{E}_{\lambda^*}$, our result (see Corollary 2.16 and Proposition 3.9) shows that the order of the Tate-Shafarevich group for $\mathscr{E}_{\lambda^*}$ is congruent modulo the norm prime ℓ of λ to the square of suitable coefficient (Hurwitz-type number) of power series expansion of the lemniscate function $\mathrm{sl}(u)$ or Weierstrass function $\zeta(u)$. Since the order of the Tate-Shafarevich group above are expected to be smaller than $\sqrt{\ell}$, such congruence gives the order itself as in the latter part of 0.1.

Although there are many other congruences of this kind, only the case of elliptic curves with complex multiplication in Gauss's number field is treated in this paper.

Throughout this paper we treat mainly certain character sums called elliptic Gauss sums, which are associated with suitable elliptic functions. In the Appendix we consider character sums called trigonometric Gauss sums, which are associated with trigonometric functions.

We summarize objects which used in this paper as in the following table.

[3] T. Asai showed the author such the proof on this.

parameter prime	group	L-series	function f defining "f-tic" Gauss sum	power series coeff. of f
rational odd prime p	class group of $\mathbf{Q}(\sqrt{-p})$	Dirichlet L with a character associated to p	$\cot(u)$ and $\sec(u)$	Bernoulli and Euler numbers
degree one prime λ in $\mathbf{Z}[\boldsymbol{i}]$	Tate-Shafarevich group of $\mathscr{E}_{\lambda^*}$ over $\mathbf{Q}(\boldsymbol{i})$	Hecke L with a Grössen-character associated to λ	lemniscate function $\mathrm{sl}(u)$, etc.	Hurwitz-type numbers

This paper is closely related to Asai's recent work in [A]. In the paper [A], it is explained how each L-series in the third column corresponds to suitable f in the fourth column. Superficially, the statement of our result connect directly the second or third column of the table with the fifth.

In order to explain roughly our idea of avoiding complexity, we outline here the proof of the second case $p \equiv 1 \bmod 4$ in 0.1. A detailed proof is given in Appendix 4.1. Let us consider the sum

$$\frac{1}{2}\sum_{r \bmod p}\left(\frac{r}{p}\right)\sec\left(\frac{2\pi}{p}r\right), \tag{0.2}$$

where $(\frac{\cdot}{p})$ is the Legendre symbol. This should be called the *secant Gauss sum.* We compute this by two different methods: one is by using the infinite fractional expansion of $\sec(u)$ and expressing the secant Gauss sum as a special value of Dirichlet L-series at 1, which due to Dirichlet gives rise to the class number $h(-p)$; the other method uses power series expansion with respect to

$$\mathit{\Pi} = \tan\frac{\pi}{p},$$

in which the Euler numbers appears, and gives a congruence modulo p of certain term of the expansion. To read the Appendix 4.1 before the main body of this paper might be helpful for the reader to understand quickly the idea of our method.

If we consider similar sums by replacing $\sec(u)$ in (0.2) by, for example, the lemniscate function $\mathrm{sl}(u)$ and the Legendre symbol by the quartic-residue symbol, we have typical one of the *elliptic Gauss sums.* Then we have infinite fractional series expansion and power series expansion of such an elliptic Gauss sum with respect to certain division value of $\mathrm{sl}(u)$. Although this idea might be seen too naïve for the reader, the method works so nicely.

Our congruences are generalized also to the direction of the Appendix 4.2 that describes connection with the trigonometric Gauss sum associated to higher derivatives of $\cot(u)$, for instance, and special value at an integer other than 1 of Hecke L-series.

This paper is restricted to the case of Hecke character arising from the quartic-residue symbol with respect to a degree 1 prime in $\mathbf{Z}[\boldsymbol{i}]$ dividing $\ell \equiv 5 \bmod 8$. Moreover, as we mentioned before, we have similar results by replacing the base ring in the story of this paper by $\mathbf{Z}[\frac{-1+\sqrt{3}\boldsymbol{i}}{2}]$.

Finally, we mention on notation in this paper. We denote the imaginary unit by $\boldsymbol{i}$, which is a bold face letter.

Acknowledgement: The idea of this research has grown up in communication with Professor T. Asai on the elliptic Gauss sum. He encouraged constantly the author and corrected several errors of the draft. He pointed out our results are just the extension of congruences in 0.1 and explained how those congruences are derived from modern theory of p-adic L-functions. Moreover, one of the referees explained properly our results should be derived from the theory of p-adic Hecke L-functions. Dr. Naruo Kanou computed and showed the author so many numerical examples of elliptic Gauss sums. He taught kindly the author several things on `PARI/GP` on checking the results of this work. Dr. Masataka Chida kindly explained the connection with the Birch and Swinnerton-Dyer conjecture. The author is very thankful for their consideration. This work was supported by JSPS grant-in-aid for scientific researches, No.16540002 and No.19540002.

Contents

1 Elliptic functions

1.1 The lemniscate function

Let

$$\begin{aligned}\varpi = 2\int_1^\infty \frac{dx}{2\sqrt{x^3-x}} = 2\int_0^1 \frac{dt}{\sqrt{1-t^4}}\\ = 2.62205755429211981046483958989111\cdots\end{aligned}$$

be the positive minimal period of the canonical 1-form on the elliptic curve

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

Let us consider the function $t = \mathrm{sl}(u)$. This is the inverse function of

$$u = \int_0^t \frac{dt}{\sqrt{1-t^4}} \tag{1.1}$$

and has the period lattice $(1-\boldsymbol{i})\,\omega\,\mathbf{Z}[\boldsymbol{i}]$. This function has the property

$$\mathrm{sl}(\boldsymbol{i}u) = \boldsymbol{i}\,\mathrm{sl}(u). \tag{1.2}$$

We know that the power series expansion of (1.1) is given by

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

Here we note that the leading term is t, $\binom{-\frac{1}{2}}{n} \in \mathbf{Z}[\frac{1}{2}]$, and

$$\frac{du}{dt} = \frac{d}{dt}\mathrm{sl}^{-1}(t) \in \mathbf{Z}[\tfrac{1}{2}][[t]].$$

We denote the coefficients of power series expansion of $\mathrm{sl}(u)$ as

$$\begin{aligned}\mathrm{sl}(u) = &\quad u - \tfrac{1}{10}u^5 + \tfrac{1}{120}u^9 - \tfrac{11}{15600}u^{13} + \tfrac{211}{3536000}u^{17} - \tfrac{1607}{318240000}u^{21} + \cdots\\ = &\quad u - \tfrac{12}{5!}u^5 + \tfrac{3024}{9!}u^9 - \tfrac{4390848}{13!}u^{13} + \tfrac{21224560896}{17!}u^{17}\\ &\qquad\qquad\qquad\qquad\qquad - \tfrac{257991277243392}{21!}u^{21} + \cdots\\ = &\ C_1u + C_5u^5 + C_9u^9 + \cdots\\ = &\ \sum_{m=0}^\infty c_{4m+1}\frac{u^{4m+1}}{(4m+1)!}.\end{aligned}$$

Then, since

$$\frac{du}{dt} = \frac{1}{\sqrt{1-t^4}},$$

we see that $\frac{d^2t}{du^2} = -2t^3$, and

$$c_{4m+1} \in \mathbf{Z}. \tag{1.3}$$

We recall facts on addition formula of $\mathrm{sl}(u)$. For a proof of them, we refer the reader to [S1], pp.113-115, for instance.

Lemma 1.4. (Addition formula of $\mathrm{sl}(u)$) *The addition formula of* $\mathrm{sl}(u)$ *is given as follows*:

$$\begin{aligned}\mathrm{sl}(u+v) &= \frac{\mathrm{sl}^2(u)-\mathrm{sl}^2(v)}{\mathrm{sl}(u)\sqrt{1-\mathrm{sl}^4(v)}-\mathrm{sl}(v)\sqrt{1-\mathrm{sl}^4(u)}} \\ &\in \mathrm{sl}(u)+\mathrm{sl}(v)+\big(\mathrm{sl}^2(u),\mathrm{sl}(u)\mathrm{sl}(v),\mathrm{sl}^2(v)\big)\,\mathbf{Z}[\tfrac{1}{2}][[\mathrm{sl}(u),\mathrm{sl}(v)]].\end{aligned}$$

Using this formula, we have

$$\mathrm{sl}\big((1-\boldsymbol{i})u\big)=\frac{(1-\boldsymbol{i})\mathrm{sl}(u)}{\sqrt{1-\mathrm{sl}^4(u)}}.$$

The formula in Lemma 1.4 and (1.2) imply the following.

Lemma 1.5. *For any integer r,* $\mathrm{sl}(ru)$ *is expanded as a power series of* $\mathrm{sl}(u)$ *with coefficients in* $\mathbf{Z}[\frac{1}{2}]$:

$$\mathrm{sl}(ru)\in r\,\mathrm{sl}(u)+\mathrm{sl}(u)^5\,\mathbf{Z}[\tfrac{1}{2}][[\,\mathrm{sl}(u)^4\,]].$$

1.2 Weierstrass ζ-function

To avoid confusion, we use two complex variables. The first one is u and the second one is U. We assume that u and U relate as $U=u/(1-\boldsymbol{i})$. In addition to $\mathrm{sl}(u)$, we discuss on the function

$$\zeta^*(U)=\zeta(U)-\tfrac{\pi}{\varpi^2}\,\overline{U},$$

where $\zeta(U)$ is the Weierstrass zeta function associated to the elliptic curve $\mathscr{E}$, and $\overline{U}$ denotes the complex conjugate of U. Legendre relation implies that this function is periodic with respect to the lattice $\varpi\mathbf{Z}[\boldsymbol{i}]$ ($\subset\mathbf{C}$).

The Weierstrass elliptic function $\wp(U)$ for the elliptic curve above is given by

$$\wp(U)=1/\mathrm{sl}(U)^2$$

and satisfies $\wp'(U)^2=4\wp(U)^3-4\wp(U)$. In the sequel, we denote by $\mathbf{Z}[\,\boldsymbol{i}\,;\,\cdots,\frac{1}{r}]$ the ring

$$\mathbf{Z}\Big[\,\boldsymbol{i},\,\Big\{\frac{1}{a}\,;\,0\neq|a|\leqq|r|\Big\}\Big]$$

Lemma 1.6. *Let r be a non-zero element in $\mathbf{Z}[\boldsymbol{i}]$. We have*

$$\zeta(rU)-\overline{r}\zeta(U)-\frac{1-r\overline{r}}{r}\,\frac{1}{\mathrm{sl}(U)}\ \in\ \mathrm{sl}(U)^3\,\mathbf{Z}[\,\boldsymbol{i}\,;\,\cdots,\tfrac{1}{r}][[\mathrm{sl}(U)]].$$

Proof Using a well-known formula ([S1], pp.113-115, for instance), we see that

$$\begin{aligned}
\zeta(U+V) &= \zeta(U)+\zeta(V)+\frac{1}{2}\frac{\wp'(U)-\wp'(V)}{\wp(U)-\wp(V)}\\
&= \zeta(U)+\zeta(V)-\frac{\mathrm{sl}(U)^{-3}\mathrm{sl}'(U)-\mathrm{sl}(V)^{-3}\mathrm{sl}'(V)}{\mathrm{sl}(U)^{-2}-\mathrm{sl}(V)^{-2}}\\
&= \zeta(U)+\zeta(V)-\frac{\mathrm{sl}(U)^{-3}\sqrt{1-\mathrm{sl}(U)^4}-\mathrm{sl}(V)^{-3}\sqrt{1-\mathrm{sl}(V)^4}}{\mathrm{sl}(U)^{-2}-\mathrm{sl}(V)^{-2}}\\
&= \zeta(U)+\zeta(V)-\frac{\mathrm{sl}(V)^{3}\sqrt{1-\mathrm{sl}(U)^4}-\mathrm{sl}(U)^{3}\sqrt{1-\mathrm{sl}(V)^4}}{\mathrm{sl}(U)\mathrm{sl}(V)\big(\mathrm{sl}(U)^{2}-\mathrm{sl}(V)^{2}\big)}\\
&\in \zeta(U)+\zeta(V)-\frac{\mathrm{sl}(U)^2+\mathrm{sl}(U)\mathrm{sl}(V)+\mathrm{sl}(V)^2}{\mathrm{sl}(U)\mathrm{sl}(V)\big(\mathrm{sl}(U)+\mathrm{sl}(V)\big)}\\
&\qquad+\frac{1}{\mathrm{sl}(U)\mathrm{sl}(V)\big(\mathrm{sl}(U)+\mathrm{sl}(V)\big)}\big(\mathrm{sl}(U),\mathrm{sl}(V)\big)^6\,\mathbf{Z}[\tfrac{1}{2}]\big[\big[\mathrm{sl}(U)^4,\mathrm{sl}(V)^4\big]\big].
\end{aligned}$$

Since $\zeta(\pm\boldsymbol{i}U)=\mp\boldsymbol{i}\zeta(U)$, it is obvious that the claim is true for $r=\pm1$, $\pm\boldsymbol{i}$. Assume that the statement is true for any r whose absolute value is less than or equal to arbitrarily fixed $|r|$. We suppose that $|r|<|r+1|$ and consider the multiplication by $(r+1)$. Then

$$\begin{aligned}
\zeta((r+1)U) \ &\in\ \zeta(rU)+\zeta(U)-\frac{\mathrm{sl}(rU)^2+\mathrm{sl}(rU)\mathrm{sl}(U)+\mathrm{sl}(U)^2}{\mathrm{sl}(rU)\mathrm{sl}(U)\big(\mathrm{sl}(rU)+\mathrm{sl}(U)\big)}\\
&\qquad+\frac{1}{\mathrm{sl}(rU)\mathrm{sl}(U)\mathrm{sl}\big((rU)+\mathrm{sl}(U)\big)}\big(\mathrm{sl}(rU),\mathrm{sl}(U)\big)^6\,\mathbf{Z}[\tfrac{1}{2}]\big[\big[\mathrm{sl}(rU)^4,\mathrm{sl}(U)^4\big]\big]\\
&\subset (\overline{r}+1)\zeta(U)+\frac{1-r\overline{r}}{r}\,\frac{1}{\mathrm{sl}(U)}-\frac{r^2+r+1}{r(r+1)}\,\frac{1}{\mathrm{sl}(U)}\ +\mathrm{sl}(U)^3\,\mathbf{Z}[\,\boldsymbol{i}\,;\,\cdots,\tfrac{1}{r+1}]\big[\big[\mathrm{sl}(U)\big]\big]\\
&= (\overline{r}+1)\zeta(U)+\frac{1-(r+1)(\overline{r}+1)}{r+1}\,\frac{1}{\mathrm{sl}(U)}+\mathrm{sl}(U)^3\,\mathbf{Z}[\,\boldsymbol{i}\,;\,\cdots,\tfrac{1}{r+1}]\big[\big[\mathrm{sl}(U)\big]\big].
\end{aligned}$$

Therefore, the statement is true for multiplication by $(r+1)$. Similar argument shows that it is true for multiplications by $(r-1)$ and by $(r\pm\boldsymbol{i})$. We note here that, for the multiplications by $(r\pm\boldsymbol{i})$, we need $\zeta(\boldsymbol{i}U)=-\boldsymbol{i}\zeta(U)$. □

Usually the expansion of $\zeta^*(u)$ is written as

$$\begin{aligned}
\zeta^*(U) &= -\frac{\pi}{\varpi^2}\overline{U}+\frac{1}{U}+\sum_{n=1}^{\infty}\frac{-2^{4n}H_{4n}}{4n}\frac{U^{4n-1}}{(4n-1)!}\\
&= -\frac{\pi}{\varpi^2}\overline{U}+\frac{1}{U}-\frac{1}{15}U^3-\frac{1}{525}U^7-\frac{2}{52625}U^{11}-\frac{1}{1243125}U^{15}-\cdots,
\end{aligned}\tag{1.7}$$

and its coefficients $H_{4n}\in\mathbf{Q}$ are called the Hurwitz numbers. The denominator of H_{4n} was known by Hurwitz himself. We recall this in a rather weak form as follows (see [H]).

Lemma 1.8. *We have*

$$H_{4n}=\frac{1}{2}+\sum_{\substack{p\,:\,\mathrm{prime}\\ p\equiv1 \bmod 4\\ (p-1)|4n}}\frac{b_p}{p}+\text{“rational integer”},$$

where b_p are rational integer.

We denote the expansion (1.7) simply as

$$\zeta^*(U) = -\frac{\pi}{\varpi^2}\overline{U} + \frac{1}{U} + \sum_{n=1}^{\infty} D_{4n-1}U^{4n-1} \quad \Big(\text{i.e. } D_{4n-1} = \frac{-2^{4n}H_{4n}}{(4n)!}\Big).$$

By using another variable z, we further introduce the function

$$\mathsf{Z}(z) = \zeta^*(\varpi z).$$

More detailed properties on $\mathsf{Z}(z)$ is seen in [A].

1.3 Eisenstein's product formula

We introduce here some notations that we use through out this paper. We denote by $\ell \in \mathbf{Z}$ a rational prime number bigger than 5 such that $\ell \equiv 5 \bmod 8$ and fix $\lambda \in \mathbf{Z}[\boldsymbol{i}]$ satisfying

$$\ell = \lambda\overline{\lambda} \text{ and } \lambda \equiv 1 \bmod (2+2\boldsymbol{i}), \tag{1.9}$$

where $^-$ is the complex conjugation. The function defined by

$$\varphi(z) = \mathrm{sl}\big((1-\boldsymbol{i})\varpi z\big)$$

is used everywhere in this paper. Let

$$\varLambda = \varphi(\tfrac{1}{\lambda}),$$

and

$$\mathscr{O}_\lambda = \text{“the ring of integers of } \mathbf{Q}(\boldsymbol{i}, \varLambda)\text{”}.$$

We consider the quartic character

$$\chi_{\lambda}(r) = \Big(\frac{r}{\lambda}\Big)_4. \tag{1.10}$$

Lemma 1.11. *By the notation above, we have the following.*
(1) *We have $\varLambda \in \mathscr{O}_\lambda$. Moreover, $\varLambda$ is a prime element in $\mathscr{O}_\lambda$ and has a property $(\lambda) = (\varLambda)^{\ell-1}$ as ideals. Any $\varphi(\frac{r}{\lambda})$ for $r \not\equiv 0$ modulo ℓ is an associate of $\varLambda$ in $\mathscr{O}_\lambda$, namely, they generate the same prime ideal.*
(2) *Let $\widetilde{\lambda} = \prod_{\chi_\lambda(r)=1}\varphi\big(\frac{r}{\lambda}\big)$. Then $\widetilde{\lambda}^4 = -\lambda$.*
(3) *The $\widetilde{\lambda}$ in (2) belongs to $\varLambda^{(\ell-1)/4}(1+\varLambda^4\,\mathscr{O}_\lambda)$.*

Proof. The assertion (1) and (2) are classical and there are several proofs (see [O] for instance). The expansion Lemma 1.5 and (1) imply $\widetilde{\lambda} \in \varLambda^{(\ell-1)/4}(1+\varLambda^4\,(\mathscr{O}_\lambda)_{(\varLambda)})$, where $(\mathscr{O}_\lambda)_{(\varLambda)}$ is the localization of $\mathscr{O}_\lambda$ with respect to the prime ideal $(\varLambda)$. Adding the statement (1) with this, the assertion (3) follows. □

2 Elliptic Gauss sums

2.1 Definition of elliptic Gauss sums

To express the value at $s = 1$ of the Hecke L-series defined later by (3.1), we consider elliptic Gauss sums following [A]. For ℓ, λ in (1.9) and the character χ_{λ} in (1.10), let f be a function defined by

$$f = \begin{cases} \varphi & \text{if } \ell \equiv 13 \bmod 16, \\ \mathsf{Z} & \text{if } \ell \equiv 5 \bmod 16 \end{cases}$$

and

$$G_\lambda(\chi_{\lambda}, f) = \frac{1}{4} \sum_{r \bmod \lambda} \chi_{\lambda}(r) f(\tfrac{r}{\lambda}), \tag{2.1}$$

where $r \in \mathbf{Z}[\boldsymbol{i}]$ runs through residues modulo λ. It is known that

$$G_\lambda(\chi_{\lambda}, f) \in \mathscr{O}_\lambda$$

by Lemma 1.11. We call this the *elliptic Gauss sum* associated to χ_{λ} and f. We remark here that, actually, the function f above is chosen depending on the character χ_{λ}, and f is associated to the Hecke L-series (3.1) defined later (see [A]).

2.2 Integrality and rationality of the coefficients

We shall recall Asai's results from [A] for the lemniscate case. Here ℓ and λ are as before.

Theorem 2.2. (Asai) *We use the notation above.*
(1) *If* $\ell \equiv 13 \bmod 16$*, then there exists* $\alpha_\lambda \in 1 + 2\mathbf{Z}$ *such that*

$$G_\lambda(\chi_{\lambda}, \varphi) = \alpha_\lambda \widetilde{\lambda}^3.$$

(2) *If* $\ell \equiv 5 \bmod 16$ (*and* $\ell \neq 5$)*, then there exists* $\alpha_\lambda \in \chi_{\lambda}(1 + i) \cdot \big(1 + 2\mathbf{Z}\big)$ *such that*

$$G_\lambda(\chi_{\lambda}, \mathsf{Z}) = \alpha_\lambda \widetilde{\lambda}^3.$$

Remark 2.3. (1) The number α_λ is called the *coefficient* of $G_\lambda(\chi_{\lambda}, \varphi)$ in [A].
(2) In [A], the theorem above is proved by using the functional equations of the Hecke L-series defined in (3.1) below, which are associated to Hecke characters arising from χ_{λ}.
(3) The fact $\alpha_\lambda \in \mathbf{Z}[\boldsymbol{i}]$ is easily shown (Eisenstein, [E2], pp.234–236). However, the fact $\alpha_\lambda \in \mathbf{Z}$ or $\alpha_\lambda \in \chi_{\lambda}(1+\boldsymbol{i}) \cdot \mathbf{Z}$ is quite number theoretic, and is equivalent to the determination of the sign of the usual quartic Gauss sum (see [A]), namely, to Cassels-Matthews formula. We use Asai's result to lift congruences modulo λ to modulo ℓ. Actually, Theorem 2.2(1) is used in the proof of the first congruence in Theorem 2.4, and Theorem 2.2(2) is essential to show the congruence in Corollary 2.16 for the case $\ell \equiv 5 \bmod 16$.

(4) The absolute value of α_λ is quite small. It would be expected by a lot of numerical examples by N. Kanou that

$$|\alpha_\lambda| < \sqrt{\ell},$$

and the growth order seems to be of $\ell^{1/4}$.

2.3 The congruences, main results

The first main result of this paper is the following congruence.

Theorem 2.4. *Under the notation in* 2.2, *one has*

$$\alpha_\lambda \equiv \begin{cases} -\frac{1}{4}\, C_{\frac{3(\ell-1)}{4}} \mod \ell & \text{if } \ell \equiv 13 \mod 16, \\ -\frac{1}{4}\, \chi_\lambda(1-\boldsymbol{i})\, D_{\frac{3(\ell-1)}{4}} \mod \lambda & \text{if } \ell \equiv 5 \mod 16. \end{cases}$$

Remark 2.5. On the second case, the modulus λ can not be replaced by ℓ.

Proof of Theorem 2.4. Let $t = \mathrm{sl}(u)$. For any $\nu \in \mathbf{Z}[\boldsymbol{i}]$, we have

$$\begin{aligned} \mathrm{sl}(\nu u) &= \mathrm{sl}\Big(\nu \sum_{n=0}^{\infty}(-1)^n \binom{-\frac{1}{2}}{n} \frac{t^{4n+1}}{4n+1}\Big) \\ &= \sum_{m=0}^{\infty} C_{4m+1}\Big(\nu \sum_{n=0}^{\infty}(-1)^n \binom{-\frac{1}{2}}{n} \frac{t^{4n+1}}{4n+1}\Big)^{4m+1} \\ &= \sum_{m=0}^{\infty} C_{4m+1}\,\nu^{4m+1}\Big(\sum_{n=0}^{\infty}(-1)^n \binom{-\frac{1}{2}}{n} \frac{t^{4n+1}}{4n+1}\Big)^{4m+1}. \end{aligned}$$

Let $\ell \equiv 13 \bmod 16$ and g be a primitive root of 1 modulo ℓ. We consider the sum

$$L(u) = \mathrm{sl}(u) + \mathrm{sl}(g^4 u) + \cdots + \mathrm{sl}(g^{\ell-5}u). \tag{2.6}$$

The elliptic Gauss sum (2.1) is given by

$$G_\lambda(\chi_\lambda, \varphi) = L\Big(\frac{(1-\boldsymbol{i})\varpi}{\lambda}\Big). \tag{2.7}$$

On the other hand, the function $L(u)$ is expanded as

$$\begin{aligned} L(u) &= \sum_{j=1}^{\frac{\ell-1}{4}} \mathrm{sl}\Big(g^{4j} \sum_{n=0}^{\infty}(-1)^n \binom{-\frac{1}{2}}{n} \frac{t^{4n+1}}{4n+1}\Big) \\ &= \sum_{j=1}^{\frac{\ell-1}{4}} \sum_{m=0}^{\infty} C_{4m+1}\Big(g^{4j} \sum_{n=0}^{\infty}(-1)^n \binom{-\frac{1}{2}}{n} \frac{t^{4n+1}}{4n+1}\Big)^{4m+1} \\ &= \sum_{m=0}^{\infty} C_{4m+1}\Big(\sum_{j=1}^{\frac{\ell-1}{4}} g^{4(4m+1)j}\Big)\Big(\sum_{n=0}^{\infty}(-1)^n \binom{-\frac{1}{2}}{n} \frac{t^{4n+1}}{4n+1}\Big)^{4m+1} \\ &= \sum_{m=0}^{\infty} C_{4m+1}\Big(\sum_{j=1}^{\frac{\ell-1}{4}} g^{4(4m+1)j}\Big)\big(t^{4m+1} + \text{“higher terms on } t\text{”}\big). \end{aligned} \tag{2.8}$$

In this situation, we note that the ring $\mathbf{Q}[[t]]$ is isomorphic to a formal power series ring over $\mathbf{Q}$. If we gather the similar terms for every order in (2.8), then such the t-adic expansion must coincide with the expression of $L(u)$ coming from power series expansion of the addition formula (i.e. Lemma 1.4) and (2.6), which expansion has coefficients in $\mathbf{Z}[\frac{1}{2}]$ by Lemma 1.5. Recall (1.3), that is

$$\varLambda = \varphi\big(\tfrac{1}{\lambda}\big) = \mathrm{sl}\Big(\frac{(1-\boldsymbol{i})\varpi}{\lambda}\Big).$$

Then, by (2.8) and (2.7),

$$G_\lambda(\chi_{{}_\lambda},\,\varphi) = \sum_{m=0}^{\infty} C_{4m+1}\bigg(\sum_{j=1}^{\frac{\ell-1}{4}} g^{4(4m+1)j}\bigg)\Big(\varLambda^{4m+1} + \text{“higher terms on } \varLambda\text{”}\Big), \tag{2.9}$$

and this expansion converges $\varLambda$-adically. Since we are interested in (2.9) modulo $\varLambda^{\frac{3(\ell-1)}{4}+1}$, we may ignore the terms higher than $\varLambda^{\frac{3(\ell-1)}{4}}$. Now, Lemma 1.5 and (1.3) implies that the denominators of the coefficients C_{4m+1} for $4m+1 \leqq \frac{3(\ell-1)}{4}$ do not contain ℓ. Anyway, (2.9) is

$$\equiv \sum_{m=0}^{\frac{3\ell-7}{16}} C_{4m+1}\,\bigg(\sum_{j=1}^{\frac{\ell-1}{4}} g^{4(4m+1)j}\bigg)\varLambda^{4m+1} \bmod \varLambda^{\frac{3(\ell-1)}{4}+1}.$$

Now Fermat's theorem shows that

$$\sum_{j=1}^{\frac{\ell-1}{4}} g^{4(4m+1)j} \equiv \begin{cases} 0 & \bmod \ell \ \text{ if } \ (\ell-1)\not|\,4(4m+1), \\ \frac{\ell-1}{4} & \bmod \ell \ \text{ if } \ (\ell-1)\,|\,4(4m+1). \end{cases}$$

For $1 \leqq 4m{+}1 \leqq 3(\ell{-}1)/4$, we see that $\ell{-}1$ divides $4(4m{+}1)$ if and only if $4(4m{+}1) = \ell{-}1$, $2(\ell-1)$, or $3(\ell-1)$, namely, $4m+1 = \frac{\ell-1}{4}, \frac{2(\ell-1)}{4}, \frac{3(\ell-1)}{4}$. The former two cases are impossible since $\ell \equiv 13 \mod 16$, and only the last case is possible. Therefore we may compute only the term of $\varLambda^{3\frac{(\ell-1)}{4}}$, that is

$$C_{\frac{3(\ell-1)}{4}}\,\bigg(\sum_{j=1}^{\frac{\ell-1}{4}} g^{3(\ell-1)j}\bigg)\varLambda^{\frac{3(\ell-1)}{4}}$$

in the expansion (2.9), which is

$$\equiv C_{\frac{3(\ell-1)}{4}} \cdot \tfrac{\ell-1}{4} \cdot \varLambda^{\frac{3(\ell-1)}{4}} \bmod \varLambda^{\frac{3(\ell-1)}{4}+1}.$$

By Lemma 1.11(2) and Lemma 1.4 we see that

$$\begin{aligned} \widetilde{\lambda} &\equiv \Big(\prod_{\chi_\lambda(r)=1} r\Big)\,\varphi\big(\tfrac{1}{\lambda}\big)^{\frac{\ell-1}{4}} \equiv \Big(\prod_{j=1}^{\frac{(\ell-1)}{4}} g^{4j}\Big)\,\varLambda^{\frac{(\ell-1)}{4}} \mod \varLambda^{\frac{(\ell-1)}{4}+1} \\ &\equiv g^{\frac{(\ell-1)(\ell+3)}{4}}\varLambda^{\frac{(\ell-1)}{4}} \mod \varLambda^{\frac{(\ell-1)}{4}+1} \\ &\equiv \varLambda^{\frac{(\ell-1)}{4}} \mod \varLambda^{\frac{(\ell-1)}{4}+1}. \end{aligned}$$

Summing up, we have

$$G_\chi(\chi_{\lambda}, \varphi) = \alpha_\lambda \widetilde{\lambda}^3 \equiv \tfrac{\ell-1}{4} \cdot C_{\frac{3(\ell-1)}{4}}\, \widetilde{\lambda}^3 \quad \mathrm{mod}\ \widetilde{\lambda}^4.$$

So that, by (1.3),

$$\alpha_\lambda \equiv -\tfrac{1}{4}\, C_{\frac{3(\ell-1)}{4}} \quad \mathrm{mod}\ \widetilde{\lambda}.$$

Since both sides are rationals (see Theorem 2.2), we have the desired congruence.

We are going to prove the second case. Because $\ell > 5$, we can choose a quarter set

$$S = \text{“a set of representatives } \{r \,|\, \chi_{\lambda}(r){=}1\} \text{ mod } \ell \text{ with } 0 < r < \ell{-}1\text{”} \quad (\subset \mathbf{Z}) \tag{2.10}$$

such that *the sum of these elements is exactly* 0. Let us consider the sum

$$M(U) = \sum_{r \in S} \zeta^*(rU) = \sum_{r \in S} \zeta^*\big(\tfrac{r}{1-\boldsymbol{i}}\, u\big).$$

This has the same periods as $\mathrm{sl}(u)$ and we see that

$$G_\lambda(\chi_{\lambda},\, \mathsf{Z}) = M\Big(\frac{\varpi}{\lambda}\Big). \tag{2.11}$$

Let $U = \frac{u}{1-\boldsymbol{i}} = \frac{1}{1-\boldsymbol{i}}\, \mathrm{sl}^{-1}(t)$ as before. By Lemma 1.6 and the choice in (2.10),

$$\begin{aligned} M(U) &= \sum_{r \in S} \zeta(rU) \\ &\in \sum_{r \in S} \overline{r}\zeta(U) + \Big(\sum_{r \in S} \frac{1 - r\overline{r}}{r}\Big) \frac{1-\boldsymbol{i}}{\mathrm{sl}(u)} + \mathrm{sl}(u)^3\, \mathbf{Z}[\,\boldsymbol{i}\,; \cdots, \tfrac{1}{\ell-1}][[\mathrm{sl}(u)]] \\ &= \Big(\sum_{r \in S} \frac{1}{r}\Big) \frac{1-\boldsymbol{i}}{\mathrm{sl}(u)} + \mathrm{sl}(u)^3\, \mathbf{Z}[\,\boldsymbol{i}\,; \cdots, \tfrac{1}{\ell-1}][[\mathrm{sl}(u)]]. \end{aligned} \tag{2.12}$$

Now we set $U = \varpi/\lambda$. Because

$$\Big(\sum_{r \in S} \frac{1}{r}\Big) \frac{1-\boldsymbol{i}}{\mathit{\Lambda}} \equiv 0 \ \mathrm{mod}\ \mathit{\Lambda}^{(\ell-2)},$$

we see that (2.12) is expanded as a power series of $\mathit{\Lambda} = \mathrm{sl}((1-\boldsymbol{i})\varpi/\lambda)$ with $\mathit{\Lambda}$-adic integer coefficients. Especially, it is $\mathit{\Lambda}$-adically convergent. We are interested in (2.11) modulo

$\Lambda^{\frac{3(\ell-1)}{4}+1}$ as in the first case. Paying attention to Lemma 1.8, we have

$$\begin{aligned}
G_\lambda(\chi_\lambda,\, \mathsf{Z}) &= M\Big(\frac{\varpi}{\lambda}\Big)\\
&= \Big\{\sum_{r\in S}\frac{1}{rU} + \sum_{r\in S}\sum_{m=1}^{\infty} D_{4m-1}\,(rU)^{4m-1}\Big\}\Big|_{U=\varpi/\lambda}\\
&= \Big\{\sum_{r\in S}\frac{1-\boldsymbol{i}}{r}\frac{1}{t}\Big(1+\sum_{n=1}^{\infty}(-1)^n\binom{-\frac{1}{2}}{n}\frac{t^{4n}}{4n+1}\Big)^{-1}\\
&\qquad + \sum_{r\in S}\sum_{m=1}^{\infty} D_{4m-1}\Big(\frac{r}{1-\boldsymbol{i}}\sum_{n=0}^{\infty}(-1)^n\binom{-\frac{1}{2}}{n}\frac{t^{4n+1}}{4n+1}\Big)^{4m-1}\Big\}\Big|_{U=\varpi/\lambda} \qquad (2.13)\\
&\equiv \sum_{r\in S}\frac{1-\boldsymbol{i}}{r}\frac{1}{\Lambda}\Big(1+\sum_{n=1}^{\frac{3(\ell-1)}{4}}(-1)^n\binom{-\frac{1}{2}}{n}\frac{\Lambda^{4n}}{4n+1}\Big)^{-1}\\
&\qquad + \sum_{r\in S}\sum_{m=1}^{\frac{3\ell+1}{16}} D_{4m-1}\Big(\frac{r}{1-\boldsymbol{i}}\sum_{n=0}^{\frac{3(\ell-1)}{4}}(-1)^n\binom{-\frac{1}{2}}{n}\frac{\Lambda^{4n+1}}{4n+1}\Big)^{4m-1} \mod \Lambda^{\frac{3(\ell-1)}{4}+1}.
\end{aligned}$$

Let g be a primitive root of 1 modulo ℓ as above. Since

$$\begin{aligned}
\sum_{r\in S}\frac{1}{\frac{r}{\lambda}} &\equiv \lambda\sum_{j=0}^{\frac{\ell-5}{4}}\frac{1}{g^{4j}} \mod \lambda\ell\\
&\equiv \lambda\cdot(1+g^4+\cdots+g^{\ell-5}) \mod \lambda\ell\\
&\equiv 0 \mod \lambda\ell,
\end{aligned}$$

the first sum of the last expression in (2.13) is congruent to 0 modulo $\lambda\ell$. Hence, we have

$$\begin{aligned}
&G_\lambda(\chi_\lambda,\, \mathsf{Z})\\
&\equiv \sum_{j=0}^{\frac{\ell-5}{4}}\sum_{m=1}^{\frac{3\ell+1}{16}} D_{4m-1}\Big(\frac{g^{4j}}{1-\boldsymbol{i}}\sum_{n=0}^{\frac{3(\ell-1)}{4}}(-1)^n\binom{-\frac{1}{2}}{n}\frac{\Lambda^{4n+1}}{4n+1}\Big)^{4m-1} \mod \Lambda^{\frac{3(\ell-1)}{4}+1}\\
&= \sum_{m=1}^{\frac{3\ell+1}{16}}\Big(\sum_{j=0}^{\frac{\ell-5}{4}} g^{4j(4m-1)}\Big) D_{4m-1}\Big(\frac{1}{1-\boldsymbol{i}}\sum_{n=0}^{\frac{3(\ell-1)}{4}}(-1)^n\binom{-\frac{1}{2}}{n}\frac{\Lambda^{4n+1}}{4n+1}\Big)^{4m-1}\\
&\equiv \sum_{m=1}^{\frac{3\ell+1}{16}}\Big(\sum_{j=0}^{\frac{\ell-5}{4}} g^{4j(4m-1)}\Big) D_{4m-1}\,\frac{1}{(1-\boldsymbol{i})^{4m-1}}\,\Lambda^{4m-1} \mod \Lambda^{\frac{3(\ell-1)}{4}+1}.
\end{aligned}$$

Now, as in the first case, Fermat's theorem yields that

$$\begin{aligned}
&\equiv \frac{1}{(1-\boldsymbol{i})^{\frac{3(\ell-1)}{4}}}\,\frac{\ell-1}{4}\,D_{\frac{3(\ell-1)}{4}}\,\Lambda^{\frac{3(\ell-1)}{4}} \mod \Lambda^{\frac{3(\ell-1)}{4}+1}\\
&\equiv (1-\boldsymbol{i})^{\frac{(\ell-1)}{4}}\,\frac{\ell-1}{4}\,D_{\frac{3(\ell-1)}{4}}\,\Lambda^{\frac{3(\ell-1)}{4}} \mod \Lambda^{\frac{3(\ell-1)}{4}+1}\\
&\equiv \chi(1-\boldsymbol{i})\,\frac{\ell-1}{4}\,D_{\frac{3(\ell-1)}{4}}\,\Lambda^{\frac{3(\ell-1)}{4}} \mod \Lambda^{\frac{3(\ell-1)}{4}+1}.
\end{aligned}$$

Using Lemma 1.11 again and Theorem 2.2(2), we have arrived at the congruence

$$\alpha_\lambda \equiv -\tfrac{1}{4}\,\chi_{_\lambda}(1{-}\boldsymbol{i})\,D_{\frac{3(\ell-1)}{4}} \quad \bmod \Lambda,$$

and the claimed one because both sides belong to $\mathbf{Q}(\boldsymbol{i})$. □

Since Hurwitz numbers H_n are computed recursively and

$$\chi_{_\lambda}(1{+}\boldsymbol{i})\,(-\boldsymbol{i}) = \chi_{_\lambda}\big((1{+}\boldsymbol{i})(-\boldsymbol{i})\big) = \chi_{_\lambda}(1{-}\boldsymbol{i}),$$

we can check that this coincides with our result and the numerical examples in [A].

Example 2.14. (a) Let $\ell = 13$ and $\lambda = 3 + 2\boldsymbol{i}$. Then

$$-\tfrac{1}{4}C_{\frac{3(\ell-1)}{4}} = -\tfrac{1}{4}C_9 = -\tfrac{1}{4}\cdot\tfrac{1}{12} \equiv 1 \quad \bmod 13.$$

This coincides with §2.3, Example 2.17 in [A] that states $\alpha_\lambda = 1$.
(b) Let $\ell = 29$ and $\lambda = -5 + 2i$. Then

$$-\tfrac{1}{4}C_{\frac{3(\ell-1)}{4}} = -\tfrac{1}{4}C_{21} = -\tfrac{1}{4}\cdot\tfrac{1607}{318240000} \equiv 1 \quad \bmod 29. \tag{2.15}$$

This coincides with the value $\alpha_\lambda = 1$ in the table at the end of [A].

We shall mention the "squared" form of Theorem 2.4 which is helpful to describe the connection of Theorem 2.4 and Tate-Shafarevich groups later.

Corollary 2.16. *For the number α_λ defined in* (2.2)*, one has*

$$|\alpha_\lambda|^2 \equiv \big(\tfrac{1}{4}\,D_{\frac{3(\ell-1)}{4}}\big)^2 \quad \bmod \ell.$$

Of course, if $\ell \equiv 13 \bmod 16$, we can replace $|\alpha_\lambda|^2$ by ${\alpha_\lambda}^2$ and this is trivial.

Proof. It is sufficient to prove only in the case $\ell \equiv 5 \bmod 16$. Because of Theorem 2.2(2) and $\chi_{_\lambda}(1{-}\boldsymbol{i}) = -\boldsymbol{i}\,\chi_{_\lambda}(1{+}\boldsymbol{i})$, taking product of the congruence

$$\alpha_\lambda - \tfrac{1}{4}\chi_{_\lambda}(1{-}\boldsymbol{i})D_{\frac{3(\ell-1)}{4}} \equiv 0 \bmod \lambda$$

given by Theorem 2.4 with its complex conjugation

$$\overline{\chi_{_\lambda}(1{+}\boldsymbol{i})}\chi_{_\lambda}(1{+}\boldsymbol{i})^{-1}\,\alpha_\lambda - \tfrac{1}{4}\,\overline{\chi_{_\lambda}(1{-}\boldsymbol{i})}\,D_{\frac{3(\ell-1)}{4}} \equiv 0 \bmod \overline{\lambda}$$

implies that

$$|\alpha_\lambda|^2 - \big(\tfrac{1}{4}\,D_{\frac{3(\ell-1)}{4}}\big)^2 \equiv 0 \bmod \ell,$$

and the proof is completed. □

3 Elliptic Gauss sums and associated elliptic curves

In this Section, we summarize a relation between special values of Hecke L-series, elliptic Gauss sum, and Tate-Shafarevich group of the corresponding elliptic curve. Main references are [D], §10 in Chapter II of [S2], [G], and [C]. Here we still use notations ℓ and λ as before.

3.1 Hecke L-series

The simplest Hecke character arising from χ_λ is constructed as follows. According to Lemma 1.11(2), suppose

$$\ell \equiv 5 \bmod 8$$

for simplicity. Using another character

$$\chi'_0(\nu) = \delta^2 \text{ for } \nu \equiv \delta \bmod (1+\boldsymbol{i})^2,\ \ \delta \in \{1, \boldsymbol{i}\},$$

we define for each $\mu \in \mathbf{Z}[\boldsymbol{i}]$,

$$\widetilde{\chi}_\lambda\big((\mu)\big) = \begin{cases} \chi_\lambda(\mu)\chi'_0(\mu)\,\overline{\mu} & \text{if } \ell \equiv 13 \mod 16, \\ \chi_\lambda(\mu)\,\overline{\mu} & \text{if } \ell \equiv 5 \mod 16. \end{cases}$$

Then $\widetilde{\chi}_\lambda$ is a Hecke character whose conductor is

$$\begin{cases} \big((1+\boldsymbol{i})^2\,\lambda\big) & \text{if } \ \ell \equiv 13 \mod 16, \\ \quad (\lambda) & \text{if } \ \ell \equiv 5 \mod 16. \end{cases}$$

There is a quite explicit description on this fact in [A]. We assume here that

$$\widetilde{\chi}_\lambda\big((\lambda)\big) = \chi_\lambda(\lambda) = 0,$$

and if $\ell \equiv 13 \mod 16$, then

$$\widetilde{\chi}_\lambda\big((1+\boldsymbol{i})\big) = \chi_\lambda(1+\boldsymbol{i}) = 0.$$

Hecke L-series associated to the character $\widetilde{\chi}_\lambda$ is

$$\begin{aligned} L(s, \widetilde{\chi}_\lambda) &= \prod_{(\mu)\,:\,\text{prime ideal}} \big(1 \,-\, \widetilde{\chi}_\lambda\big((\mu)\big)(\mu\overline{\mu})^{-s}\big)^{-1} \\ &= \prod_{\substack{\mu\,:\,\text{prime} \\ \mu\equiv 1 \bmod (1+\boldsymbol{i})^3 \\ \text{or } \mu = 1+\boldsymbol{i}}} \big(1 \,-\, \chi_\lambda(\mu)\,\overline{\mu}\,(\mu\overline{\mu})^{-s}\big)^{-1}. \end{aligned} \tag{3.1}$$

3.2 L-functions of elliptic curves

For $D \in \mathbf{Q}(\boldsymbol{i})$, we denote by $\mathscr{E}_D$ the twisted elliptic curve

$$\mathscr{E}_D : y^2 = x^3 - Dx$$

of $\mathscr{E}$. Since this has an automorphism $[(x,y) \mapsto (-x, \boldsymbol{i}y)]$, we see that

$$\mathrm{End}(\mathscr{E}_D) \simeq \mathbf{Z}[\boldsymbol{i}].$$

Let $L(\mathscr{E}_D/\mathbf{Q}(i), s)$ be the L-function of the elliptic curve $\mathscr{E}_D$ over $\mathbf{Q}(\boldsymbol{i})$ (see [S2], p.172). For simplicity we let

$$\lambda^* = \begin{cases} -\lambda & \text{if } \ell \equiv 13 \bmod 16, \\ \frac{\lambda}{4} & \text{if } \ell \equiv 5 \bmod 16. \end{cases}$$

The Hecke L-series defined by (3.1) corresponds to the twisted elliptic curve

$$\mathscr{E}_{\lambda^*} = \begin{cases} \mathscr{E}_{-\lambda} : y^2 = x^3 + \lambda x & \text{if } \ell \equiv 13 \bmod 16, \\ \mathscr{E}_{\frac{\lambda}{4}} : y^2 = x^3 - \frac{\lambda}{4}x & \text{if } \ell \equiv 5 \bmod 16. \end{cases} \tag{3.2}$$

Proposition 3.3. *One has*

$$L(s, \widetilde{\chi}_\lambda)\, L(s, \overline{\widetilde{\chi}_\lambda}) = L(\mathscr{E}_{\lambda^*}/\mathbf{Q}(\boldsymbol{i}), s). \tag{3.4}$$

Although this formula is a special case of Deuring's theorem ([D], see also [S2], p.175), we demonstrate this by explicit computation as follows. Doing so, we might deeply appreciate general theories described in [S2].

Proof. First of all we recall that, for any prime in $\mathbf{Z}[\boldsymbol{i}]$ which is congruent to 1 modulo $(1+\boldsymbol{i})^3$,

$$\chi_\lambda(\mu) = \left(\frac{\mu}{\lambda}\right)_4 = \left(\frac{-\lambda}{\mu}\right)_4. \tag{3.5}$$

<u>The case $\ell \equiv 13 \bmod 16$.</u> (i) The curve $\mathscr{E}_{-\lambda}$ has only two bad primes $\mathfrak{l} = (\lambda)$ and $\mathfrak{l} = (1+\boldsymbol{i})$. We can check by using Tate's algorithm that reduction modulo (λ) of the minimal proper regular model[4] of $\mathscr{E}_{-\lambda}$ is of type III in the symbols of Kodaira, which is additive reduction; and the reduction modulo $(1+\boldsymbol{i})$ is of type II*, which is also additive.
(ii) Let $q \equiv 3 \bmod 4$ be a rational prime. Then $-q \equiv 1 \bmod (1+\boldsymbol{i})^3$. We fix an identification $\mathbf{Z}[\boldsymbol{i}]/(q) \simeq \mathbf{F}_{q^2}$. We can show by a similar argument as in p.307 of [IR] with the result of determination of associated Jacobi sum (Theorems 2.3 and 2.14 in [BE]) that

$$\begin{aligned} \sharp\,(\mathscr{E}_{-\lambda} \otimes \mathbf{F}_{q^2})(\mathbf{F}_{q^2}) &= q^2 + 1 + \overline{\left(\frac{-\lambda}{q}\right)_4} q + \left(\frac{-\lambda}{q}\right)_4 q \\ &= q^2 + 1 - \overline{\left(\frac{-q}{\lambda}\right)_4}(-q) - \left(\frac{-q}{\lambda}\right)_4 (-q). \end{aligned} \tag{3.6}$$

[4] Its largest smooth subscheme over $\mathbf{Z}[\boldsymbol{i}]$ is known as the Néron model of $\mathscr{E}_{-\lambda}$.

Here we have used (3.5). Hence, the (q)-Euler factors in the two sides of (3.4) coincide.
(iii) For degree 1 prime ideals (μ) not dividing $((1+\boldsymbol{i})\lambda)$, the coincidence of the (μ)-Euler factors are similarly checked (see [IR]).
<u>The case $\ell \equiv 5 \bmod 16$.</u> (i) For the curve $\mathscr{E}_{\frac{\lambda}{4}}$, the reduction modulo (λ) of the minimal proper regular model of $\mathscr{E}_{\frac{\lambda}{4}}$ is also of type III.
(ii) The (q)-Euler factors for any rational prime $q \equiv 3 \bmod 4$ coincides as same as above, and the (μ)-Euler factors for degree 1 prime ideals $(\mu) \neq (\lambda)$.
(iii) The curve $\mathscr{E}_{\frac{\lambda}{4}}$ is good reduction modulo $(1+\boldsymbol{i})$ in this case as checked in the below. We shall give the explicit equation of the fibre at $(1+\boldsymbol{i})$ of the minimal proper regular model over $\mathbf{Z}[\boldsymbol{i}]$ based on [D], p.53. First of all, we note that the following. When $\ell \equiv 5 \bmod 16$, let us write the primary prime λ as

$$\lambda = -1 + 2A\boldsymbol{i}, \quad A \in \mathbf{Z}[\boldsymbol{i}].$$

Then we see

$$A \equiv 1 \text{ or } \ 3 \bmod 4.$$

Indeed, if $\ell = a^2 + b^2$ with odd a and even b, then we may suppose $a \equiv 1 \bmod 4$, $b \equiv 2 \bmod 4$. Now, letting

$$\lambda_0 = a + b\boldsymbol{i} = (1 + 4a') + (2 + 4b')\boldsymbol{i},$$

$-\lambda_0$ is primary prime and a' is even. Then the claim is checked by writing down A by a' and b'. Suppose $A \equiv 1 \bmod 4$ and denote $A = 1 + 4B$. Then by putting

$$y = v + \tfrac{1+\boldsymbol{i}}{2}\,u + \tfrac{1}{2}, \qquad x = u + \tfrac{\boldsymbol{i}A}{2}$$

into the equation (3.2) gives

$$\begin{aligned} v^2 + (1+\boldsymbol{i})uv + v &= u^3 + (6\boldsymbol{i}B + \boldsymbol{i})u^2 \\ &\quad - \big(12B^2 + (6+2\boldsymbol{i})B + 1 + \boldsymbol{i}\big)u + \big(-8\boldsymbol{i}B^3 + (4-6\boldsymbol{i})B^2 + (2-\boldsymbol{i})B\big). \end{aligned}$$

Reduction modulo $(1+\boldsymbol{i})$ of this gives

$$v^2 + v = u^3 + u^2 + B,$$

and this is good reduction.

Now suppose $A \equiv 3 \bmod 4$ and write $A = 3 + 4C$. Putting

$$y = v + \tfrac{1+\boldsymbol{i}}{2}\,u + \tfrac{\boldsymbol{i}}{2}, \qquad x = u - \tfrac{\boldsymbol{i}A}{2}$$

into the equation (3.2) gives

$$\begin{aligned} v^2 + (1+\boldsymbol{i})uv + \boldsymbol{i}v &= u^3 - (6\boldsymbol{i}C + 5\boldsymbol{i})u^2 - \big(12C^2 + (18+2\boldsymbol{i})C + 6 + 2\boldsymbol{i}\big)u \\ &\quad + (8\boldsymbol{i}C^3 - (4-18\boldsymbol{i})C^2 - (6-13\boldsymbol{i})C - (2-3\boldsymbol{i})). \end{aligned}$$

Reduction modulo $(1+\boldsymbol{i})$ of this is

$$v^2 + v = u^3 + u^2 + C + 1.$$

So that this is also good reduction. We can check the number of the rational points of each curve coincides to

$$2 + 1 - \chi_\lambda(1+\boldsymbol{i})\,(1-\boldsymbol{i}) - \chi_\lambda(1-\boldsymbol{i})\,(1+\boldsymbol{i}).$$

Now we have completely checked the equality of the claimed formula. □

3.3 Elliptic Gauss sums and Tate-Shafarevich groups

Assume that the prime ℓ satisfies $\ell \equiv 5 \bmod 8$. Let λ be as before. We explain a connection between $L(1, \widetilde{\chi}_\lambda)$ and suitable elliptic Gauss sum. Let χ_λ be the character defined by (1.10). Using the expression of $\mathrm{sl}(u)$ by infinite sum of fractions and the quartic reciprocity adding to Theorem 2.2, we have (see [A])

$$(3.7) \qquad L(1, \widetilde{\chi}_\lambda) = \begin{cases} \dfrac{(1+\boldsymbol{i})\chi_\lambda(2)\varpi}{2\widetilde{\lambda}}\,\alpha_\lambda & (\ell \equiv 13 \bmod 16), \\ -\dfrac{\varpi}{\widetilde{\lambda}}\,\alpha_\lambda & (\ell \equiv 5 \bmod 16). \end{cases}$$

Especially, by Theorem 2.2,

$$L(1, \widetilde{\chi}_\lambda) \neq 0.$$

If $s \in \mathbf{R}$, then

$$L(s, \overline{\widetilde{\chi}_\lambda}) = \overline{L(s, \widetilde{\chi}_\lambda)}.$$

Therefore,

$$(3.8) \qquad L(1, \widetilde{\chi}_\lambda)\,\overline{L(1, \widetilde{\chi}_\lambda)} = |L(1, \widetilde{\chi}_\lambda)|^2.$$

Then, as a corollary to Theorem 2.4, we have the following relation for the Tate-Shafarevich group $Ш\big(\mathscr{E}_{\lambda^*}/\mathbf{Q}(\boldsymbol{i})\big)$ of $\mathscr{E}_{\lambda^*}$ over $\mathbf{Q}(\boldsymbol{i})$:

Proposition 3.9. *For the number α_λ defined in* (2.2)*, one has*

$$\sharp\, Ш\big(\mathscr{E}_{\lambda^*}/\mathbf{Q}(\boldsymbol{i})\big) = |\alpha_\lambda|^2$$

if the full statement of the Birch and Swinnerton-Dyer conjecture holds for the corresponding elliptic curve. Especially, if $\ell \equiv 13 \bmod 16$, we can replace $|\alpha_\lambda|^2$ by ${\alpha_\lambda}^2$.

Proof Let $\mathscr{M}_{\lambda^*}$ be the minimal regular model of $\mathscr{E}_{\lambda^*}$ over $\mathbf{Z}[\boldsymbol{i}]$, and, for any prime ideal $\mathfrak{p}$ of $\mathbf{Z}[\boldsymbol{i}]$, let

$$\tau_\mathfrak{p} = \sharp\,[\mathscr{M}_{\lambda^*}(\mathbf{Q}(\boldsymbol{i})_\mathfrak{p})/\mathscr{M}^\circ_{\lambda^*}(\mathbf{Q}(\boldsymbol{i})_\mathfrak{p})]$$

where $\mathscr{M}^{\circ}_{\lambda^*}$ means the connected component including the origin.
First of all, we note that $\alpha_\lambda \neq 0$ in the Theorem 2.2, and so that

$$L(\mathscr{E}_{\lambda^*}/\mathbf{Q}(\boldsymbol{i}), 1) \neq 0.$$

Hence, Rubin's result (Theorem A in [R]) shows that the Tate-Shafarevich group is finite. Let

$$\tau_\infty = \varpi_\lambda \overline{\varpi_\lambda},$$

where ϖ_λ is a generator over $\mathbf{Z}[\boldsymbol{i}]$ of the period lattice, in $\mathbf{C}$, of $\mathscr{E}_{\lambda^*}$. The full statement of the Birch and Swinnerton-Dyer conjecture claims[5] that

$$\begin{aligned} &L(\mathscr{E}_{\lambda^*}/\mathbf{Q}(\boldsymbol{i}), 1) = \tau_\infty \tau_{(1+\boldsymbol{i})} \tau_{(\lambda)} \cdot \frac{\sharp\,\text{Ш}(\mathscr{E}_{-\lambda}/\mathbf{Q}(\boldsymbol{i}))}{\sharp\,\mathscr{E}_{-\lambda}(\mathbf{Q}(\boldsymbol{i}))^2} \quad \text{for } \ell \equiv 13 \bmod 16 \\ &\Big(\text{resp. } L(\mathscr{E}_{\frac{\lambda}{4}}/\mathbf{Q}(\boldsymbol{i}), 1) = \tau_\infty \tau_{(\lambda)} \cdot \frac{\sharp\,\text{Ш}(\mathscr{E}_{\frac{\lambda}{4}}/\mathbf{Q}(\boldsymbol{i}))}{\sharp\,\mathscr{E}_{\frac{\lambda}{4}}(\mathbf{Q}(\boldsymbol{i}))^2} \quad \text{for } \ell \equiv 5 \bmod 16\Big). \end{aligned} \tag{3.10}$$

In this formula, we compute each of the factors of the right hand side.
<u>The case $\ell \equiv 13 \bmod 16$.</u> By considering several q's in (3.6), we see $\sharp\,\mathscr{E}_{-\lambda}(\mathbf{Q}(\boldsymbol{i})) = 2$. Indeed,

$$\mathscr{E}_{-\lambda}(\mathbf{Q}(\boldsymbol{i})) = \{(0,0),\ \infty\},$$

where ∞ is the point at infinity. We have $\tau_{(1+\boldsymbol{i})} = 1$ and $\tau_{(\lambda)} = 2$ since the corresponding reductions are of type II* and III, respectively, as seen in the proof of Proposition 3.3. The number τ_∞ is given by

$$\tau_\infty = \left| \int_\infty^{(\boldsymbol{i}\sqrt{\lambda},0)} \frac{dx}{2\sqrt{x^3+\lambda x}} \right|^2 = \frac{\varpi^2}{\ell^{\frac{1}{4}}}.$$

Therefore (3.10) is written as

$$L(\mathscr{E}_{-\lambda}/\mathbf{Q}(\boldsymbol{i}), 1) = \frac{\varpi^2}{\ell^{\frac{1}{4}}} \cdot 1 \cdot 2 \cdot \frac{\sharp\,\text{Ш}(\mathscr{E}_{-\lambda}/\mathbf{Q}(\boldsymbol{i}))}{2^2} \qquad (\ell \equiv 13 \bmod 16).$$

Under this formula, we see that $\sharp\,\text{Ш}(\mathscr{E}_{-\lambda}/\mathbf{Q}(\boldsymbol{i})) = {\alpha_\lambda}^2$ by (3.8), (3.7).
<u>The case $\ell \equiv 5 \bmod 16$.</u> As we proved in the proof of Proposition 3.3, $\mathscr{E}_{\frac{\lambda}{4}}$ is bad reduction only at (λ), at which it is reduction of type III. Therefore $\tau_{(\lambda)} = 2$. Since

$$\tau_\infty = \left| \int_\infty^{(\sqrt{\lambda}/2,0)} \frac{dx}{2\sqrt{x^3 - \frac{\lambda}{4}x}} \right|^2 = \frac{2\varpi^2}{\ell^{\frac{1}{4}}}$$

the equality (3.10) is written as

$$L(\mathscr{E}_{\frac{\lambda}{4}}/\mathbf{Q}(\boldsymbol{i}), 1) = \frac{2\varpi^2}{\ell^{\frac{1}{4}}} \cdot 2 \cdot \frac{\sharp\,\text{Ш}(\mathscr{E}_{\frac{\lambda}{4}}/\mathbf{Q}(\boldsymbol{i}))}{2^2} \qquad (\ell \equiv 5 \bmod 16)$$

and $\sharp\,\text{Ш}(\mathscr{E}_{\frac{\lambda}{4}}/\mathbf{Q}(\boldsymbol{i})) = |\alpha_\lambda|^2$. □

[5] See [C]. $\mathscr{E}_{\lambda^*}$ is regarded as a Weil restriction with respect to trivial extension $\mathbf{Q}(\boldsymbol{i})/\mathbf{Q}(\boldsymbol{i})$.

Remark 3.11. (1) If our observation on the growth on α_λ stated in 2.3 (4) would be true, then the norm with respect to $\mathbf{Q}(\boldsymbol{i})$ over $\mathbf{Q}$ of the smallest residue in $\mathbf{Z}[\boldsymbol{i}]$ (with respect to absolute value) of

$$\begin{cases} \frac{1}{4}\, C_{\frac{3(\ell-1)}{4}} \bmod \ell & \text{if} \quad \ell \equiv 13 \bmod 16, \\ \frac{1}{4}\, D_{\frac{3(\ell-1)}{4}} \bmod \lambda & \text{if} \quad \ell \equiv 5 \bmod 16 \end{cases}$$

just gives the order of the Tate-Shafarevich group of the elliptic curve $\mathscr{E}_{\lambda^*}$.
(2) The sign of α_λ in (2.2) seems to be equidistributed from Kanou's mammoth table of examples. It is interesting for us whether this sign reflects some property of the corresponding elliptic curve.

4 Appendix: Applications of trigonometric Gauss sums

4.1 Class numbers of imaginary quadratic fields

For an odd prime p, we denote by $h(-p)$ the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$. We prove here the following (known) congruence:

Theorem 4.1. *For a prime* $p \equiv 1 \bmod 4$*, one has*

$$h(-p) \equiv 2^{-1}\, E_{\frac{p-1}{2}} \bmod p,$$

where E_n is the n-th Euler number. Moreover, the minimal residue with respect to absolute value modulo p of the right hand side gives exactly the left hand side.

Historically, this result was a byproduct from our main results Theorem 2.4. In the sequel, we denote for the p above that

$$\Pi = \tan \tfrac{\pi}{p}.$$

This is an algebraic integer. We need the following well-known fact.

Lemma 4.2. *Let p be an odd prime. Then*

$$\sqrt{p} = \prod_{r=1}^{(p-1)/2} \tan\left(\tfrac{r\pi}{p}\right) \equiv \left(\tfrac{p-1}{2}\right)!\, \Pi^{(p-1)/2} \mod \Pi^{(p+1)/2}$$

in the localization of the ring of integers in $\mathbf{Q}(\boldsymbol{i})$ *at the prime* (Π).

Proof of Theorem 4.1. For an integer r, we consider the power series expansion of $\sec(ru)$ with respect to $\tan(\frac{u}{2})$:

$$\sec(u) = \frac{1+\tan^2(\frac{u}{2})}{1-\tan^2(\frac{u}{2})} = 1 + 2\tan^2(\tfrac{u}{2}) + 2\tan^4(\tfrac{u}{2}) + \cdots \quad \in \mathbf{Z}[[\tan(\tfrac{u}{2})]].$$

The addition of $\sec(u)$ is also given as an power series over $\mathbf{Z}$:

$$\sec(u+v) \in \mathbf{Z}[[\tan(\tfrac{u}{2}), \tan(\tfrac{v}{2})]], \quad \sec(ru) \in \mathbf{Z}[[\tan(\tfrac{u}{2})]] \quad (r \in \mathbf{Z}). \tag{4.3}$$

On the other hand, Euler number is defined as

$$\sec(u) = 1 - \frac{E_2}{2!}u^2 + \frac{E_4}{4!}u^4 - \cdots . \tag{4.4}$$

For the variable u above, the inverse function of $x = \tan(\frac{u}{2})$ is expanded as

$$\begin{aligned} u &= 2\tan^{-1}(x) = 2\int_0^x \frac{1}{1+x^2}dx \\ &= 2x - \frac{2}{3}\,x^3 + \frac{2}{5}\,x^5 - \cdots . \end{aligned} \tag{4.5}$$

Let g be a primitive root of unity modulo p. We consider

$$\begin{aligned} S(u) = \tfrac{1}{2}\big\{ &\sec(u) + \sec(g^2u) + \cdots + \sec(g^{(p-1)/2}u) \\ &- \sec(gu) - \sec(gg^2u) - \cdots - \sec(gg^{(p-1)/2}u)\big\}. \end{aligned} \tag{4.6}$$

Then

$$S(2\pi/p) = \frac{1}{2}\sum_{r \bmod p} \left(\frac{r}{p}\right) \sec\left(\frac{2\pi}{p}r\right) \qquad (\pi = 3.1415926535\cdots).$$

This is called the *secant Gauss sum* which attains the special value at 1 of the Dirichlet L-series associated to the character $(\frac{r}{p})$ by using the expansion of $\sec(u)$ to infinite sum of fractions. Namely, we have

$$S(2\pi/p) = h(-p)\sqrt{p}. \tag{4.7}$$

By (4.6), (4.4), and (4.5), we have

$$\begin{aligned} S(u) = \frac{1}{2}\sum_{j=0}^{(p-3)/2} \Big[&1 - \frac{E_2}{2!}\Big\{g^{2j}\Big(2x - \frac{2}{3}\,x^3 + \frac{2}{5}\,x^5 - \cdots\Big)\Big\}^2 \\ &+ \frac{E_4}{4!}\Big\{g^{2j}\Big(2x - \frac{2}{3}\,x^3 + \frac{2}{5}\,x^5 - \cdots\Big)\Big\}^4 - \cdots\Big] \\ - \frac{1}{2}\sum_{j=1}^{(p-1)/2} \Big[&1 - \frac{E_2}{2!}\Big\{g^{2j-1}\Big(2x - \frac{2}{3}\,x^3 + \frac{2}{5}\,x^5 - \cdots\Big)\Big\}^2 \\ &+ \frac{E_4}{4!}\Big\{g^{2j-1}\Big(2x - \frac{2}{3}\,x^3 + \frac{2}{5}\,x^5 - \cdots\Big)\Big\}^4 - \cdots\Big]. \end{aligned}$$

Substituting $u = 2\pi/p$, we have

$$\begin{aligned} S\left(\tfrac{2\pi}{p}\right) = \frac{1}{2}\sum_{j=0}^{(p-3)/2} \Bigg[1 &- \frac{E_2}{2!}\Big\{ g^{2j}\Big(2\varPi - \frac{2}{3}\,\varPi^3 + \frac{2}{5}\,\varPi^5 - \cdots\Big)\Big\}^2 \\ &+ \frac{E_4}{4!}\Big\{ g^{2j}\Big(2\varPi - \frac{2}{3}\,\varPi^3 + \frac{2}{5}\,\varPi^5 - \cdots\Big)\Big\}^4 - \cdots \Bigg] \\ - \frac{1}{2}\sum_{j=1}^{(p-1)/2} \Bigg[1 &- \frac{E_2}{2!}\Big\{ g^{2j-1}\Big(2\varPi - \frac{2}{3}\,\varPi^3 + \frac{2}{5}\,\varPi^5 - \cdots\Big)\Big\}^2 \\ &+ \frac{E_4}{4!}\Big\{ g^{2j-1}\Big(2\varPi - \frac{2}{3}\,\varPi^3 + \frac{2}{5}\,\varPi^5 - \cdots\Big)\Big\}^4 - \cdots \Bigg]. \end{aligned} \tag{4.8}$$

Although it is unclear if this series converges $\varPi$-adically, (4.6) and (4.3) shows that, in fact, it converges $\varPi$-adically. To show the desired congruence, we will calculate (4.8) modulo $\varPi^{1+(p-1)/2}$, so that we shall omit the terms of degree higher that $\varPi^{(p-1)/2}$. Since $E_n \in \mathbf{Z}$ the denominators of coefficients of the terms of degree lower than or equal to $\varPi^{(p-1)/2}$ do not contain p in the expression of (4.8). Now, by using

$$1 + g^{2k} + g^{4k} + \cdots + g^{(p-3)k} \equiv \begin{cases} 0 & \text{if } \frac{p-1}{2} \not|\, k, \\ \frac{p-1}{2} & \text{if } \frac{p-1}{2} \,\big|\, k, \end{cases}$$

we see that

$$\begin{aligned} S(2\pi/p) &\equiv \text{“ the term of } \varPi^{(p-1)/2} \text{ ”} \quad \bmod \varPi^{(p+1)/2} \\ &\equiv \frac{1}{2}\cdot(-1)^{(p-1)/4}\cdot\frac{E_{(p-1)/2}}{\big((p-1)/2\big)!}\big\{(g^{(p-1)} + g^{2(p-1)} + \cdots + g^{(p-1)^2/2}) \\ &\quad - (g^{(p-1)/2} + g^{3(p-1)/2} + \cdots + g^{(p-3)(p-1)/2})\big\}\,(2\varPi)^{(p-1)/2} \bmod \varPi^{(p+1)/2}. \end{aligned}$$

Because of $g^{(p-1)/2} \equiv -1 \bmod p$ and Lemma 4.2, this is

$$\begin{aligned} &\equiv \tfrac{1}{2}\,(-1)^{(p-1)/4}\,E_{(p-1)/2}\,\left(\tfrac{p-1}{2}\right)!^{-2}(p-1)\,2^{(p-1)/2}\sqrt{p} \quad \bmod \varPi^{(p+1)/2} \\ &\equiv \tfrac{1}{2}\,(-1)^{(p-1)/4}\,E_{(p-1)/2}\,(-1)(-1)^{(p-1)/2}(-1)2^{(p-1)/2}\,\sqrt{p} \bmod \varPi^{(p+1)/2} \\ &\equiv \tfrac{1}{2}\,(-1)^{(p-1)/4}\,E_{(p-1)/2}\,\left(\tfrac{2}{p}\right)\sqrt{p} \quad \bmod \varPi^{(p+1)/2}. \end{aligned}$$

Here we have used Wilson's theorem. Since

$$\left(\tfrac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{(p-1)/4},$$

for $p \equiv 1 \bmod 4$, we see, by (4.7), that

$$h(-p) \equiv \frac{1}{2}\cdot E_{(p-1)/2} \quad \bmod \varPi.$$

As both sides are rational, one has

$$h(-p) \equiv \frac{1}{2}\cdot E_{(p-1)/2} \quad \bmod p.$$

Finally, the well-known estimate

$$h(-p) \leqq \tfrac{p-1}{2}.$$

shows that the minimal residue of the right hand side gives the left hand side. □

The case for $p \equiv 3 \bmod 4$ in Theorem 0.1 in the Introduction is proved similarly by replacing $\sec(u)$ by $\cot(u)$.

In the case of elliptic Gauss sums, the product formula in Lemma 4.2 corresponds to Eisenstein's product formula in Lemma 1.11(2), and the function $\sec(u)$ corresponds to the lemniscate function or the Weierstrass ζ-function.

4.2 Kummer-type congruence

We shall go in another direction for congruences on trigonometric (and elliptic) Gauss sums. The following is an example in the case of trigonometric Gauss sums with a prime $p \equiv 3 \bmod 4$. Our method having proved Theorem 4.1 shows the following.

Theorem 4.9. *Let $p \equiv 3 \bmod 4$ be a prime and $m > 0$ be an odd integer. For the trigonometric Gauss sum for the $(m-1)$-st derivative of* $\cot$, *one has*

$$\frac{1}{\sqrt{p}}\left[\frac{1}{2}\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\cot^{(m-1)}\left(\frac{\pi k}{p}\right)\right] \equiv -(-1)^{\frac{m-1}{2}}2^m\frac{B_{m+(p-1)/2}}{2m-1} \mod p.$$

By using the infinite fractional expansion of $\cot(u)$, we can rewrite the left hand side of the congruence above in terms of special value of Dirichlet L-series.

Proposition 4.10. *Let $m > 0$ be an odd integer and $B_{m,(\frac{\cdot}{p})}$ be the m-th generalized-Bernoulli number associated to $\left(\frac{\cdot}{p}\right)$. Then*

$$\frac{1}{2}\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\cot^{(m-1)}\left(\frac{\pi k}{p}\right) = p^m\pi^{-m}(m-1)!\,L(m,\left(\frac{\cdot}{p}\right)) = \frac{\boldsymbol{i}^{m+1}2^{m-1}\sqrt{p}}{m}B_{m,(\frac{\cdot}{p})}.$$

Here, we refer to the reader [Wa], p.61 for the second equality above. These two results above imply the following well-known congruence.

Proposition 4.11. *Suppose $p \equiv 3 \bmod 4$ and $m > 0$ be an odd number. Then*

$$\frac{B_{m,(\frac{\cdot}{p})}}{m} \equiv \frac{B_{m+(p-1)/2}}{m+(p-1)/2} \mod p.$$

Similar argument shows many congruences evaluating special values of L-series of Dirichlet and Hecke. The author hopes for a further discussion on these topics in another occasion.

References

[A] Asai, T.: Elliptic Gauss sums and Hecke L-values at $s = 1$. RIMS Kôkyũroku Bessatsu, **4**(2008)79–122, Kyoto university

[BE] Berndt, B.C. and Evans, R.J. : Sums of Gauss, Eisenstein, Jacobi, Jacobsthal and Brewer. Illinois J. Math., **23**(1979)374–437

[BS] Birch, B.J. and Swinnerton-Dyer, H.P. : Notes on elliptic curves II. J. reine 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] Colwell, J. : The Conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication by a nonmaximal order. Ph.D. Dissertation, `http://etd.caltech.edu/etd/available/etd-04012004-151307/`

[D] Deuring, M. : Die Zetafunktionen einer algebraischen Kurve vom Geschlechte Eins (III). Nachr. Acad. Wiss. Gëttingen, (1956)37-76

[E1] Eisenstein, G. : Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen lemniscate abhängt. J. reine angew. Math., **39**(1850)160–179

[E2] Eisenstein, G. : Über einige allgemeine Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt, nebst Anwendungen derselben auf die Zahlentheorie. J. reine angew. Math., **39**(1850)224–287

[G] Gross, B.H. : On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication. Progr. Math., **26**(1982)219–236, Birkhäuser

[H] Hurwitz, H. : Über die Entwicklungskoeffizienten der lemniskatishen Funktionen. Math. Ann., **51**(1899)196-226, (Werke, Bd.II, pp.342–373).

[IR] Ireland, K. and Rosen, M. : *A classical introduction to modern number theory.* G.T.M. **84**, Springer-Verlag, 1982

[K] Katz, N. : p-adic interpolation of real analytic Eisenstein series. Ann. of Math., **104**(1976)459–571

[O] Ônishi, Y. : Integrality of coefficients of division polynomials for elliptic functions. `http://web.cc.iwate-u.ac.jp/~onishi/`

[R] Rubin, K. : Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. Invent. math., **89**(1987)527-560

[S1] Silverman, J.H. : *The arithmetic of elliptic curves.* G.T.M. **106**, Springer-Verlag, 1986

[S2] Silverman, J.H. : *Advanced topics in the arithmetic of elliptic curves.* G.T.M. **151**, Springer-Verlag, 1991

[Wa] Washington, L.C. : *Introduction to cyclotomic fields* (2nd ed.), G.T.M. **83**, Springer-Verlag, 1991

[We] Weil, A. : *Elliptic functions according to Eisenstein and Kronecker.* Springer-Verlag, 1976

[Ya] Yager, R. : On two variable p-adic L-functions. Ann. of Math., **115**(1982)411–449

[Yu] Yuan, P. : A conjecture on Euler numbers. Proc. Japan Acad., **80** Ser.A (2004)180–181

[ZX] Zhang, W. and Xu, Z. : On a conjecture of the Euler numbers. J. Number Theory, **127**(2007)283–291