Congruence Relations Connecting Tate-Shafarevich Groups with Bernoulli-Hurwitz Numbers by Elliptic Gauss Sums in Eisenstein Integers Case

Akihiro GOTO

Abstract

There are classical congruences between the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ for a rational prime $p > 3$ and a Bernoulli number or an Euler number. Under the BSD conjecture on the 2-parts of the leading term, Onishi obtained an elliptic generalization of these congruences, which gives congruences between the order of the Tate-Shafarevich group of certain elliptic curves with complex multiplication by the Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ and Mordell-Weil rank 0, and a coefficient of power series expansion of an elliptic function associated to $\mathbb{Z}[\sqrt{-1}]$. In this paper, we provide Onishi’s type congruences for the Eisenstein integers $\mathbb{Z}[\sqrt{1-3}]$.

Contents

Introduction 1

1 Elliptic functions 4
  1.1 The basic properties of elliptic functions in the case of Eisenstein integers 4
  1.2 Power series expansions in terms of $\text{Sl}$ 4
  1.3 Bernoulli-Hurwitz-type numbers for the Eisenstein integers 11
  1.4 Eisenstein’s product formula 11

2 Elliptic Gauss sums 13
  2.1 Elliptic Gauss sums and their coefficients 13
  2.2 The main congruences 13

3 Elliptic Gauss sums and associated elliptic curves 17
  3.1 Hecke $L$-series 17
  3.2 $L$-functions of elliptic curves 17
  3.3 Elliptic Gauss sums and Tate-Shafarevich groups 23

A Appendix 24
  A.1 On the denominator of $d_n$ 25
  A.2 On the signs and the non-vanishing of $C_n, D_n,$ and $G_n$ 27
  A.3 Numerical tables of $c_n, d_n, G_6n,$ and $BH_6n$ 30

Introduction

There is a classical theorem as follows:

**Theorem 0.1.** (H) Let $p > 3$ be a rational prime, $h(-p)$ the class number of $\mathbb{Q}(\sqrt{-p})$, then

$$h(-p) \equiv \begin{cases} -2B_{(p+1)/2} \mod p & \text{if } p \equiv 3 \mod 4, \\ 2^{-1}E_{(p-1)/2} \mod p & \text{if } p \equiv 1 \mod 4, \end{cases}$$
where \( B_n \) and \( E_n \) are the \( n \)-th Bernoulli and Euler numbers respectively, i.e., \( \frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n t^n \), \( \frac{2}{e^t + 1} = \sum_{n=0}^{\infty} E_n t^n \).

As an elliptic generalization of these congruences, based on Asai’s previous research of elliptic Gauss sums \( \mathcal{A} \). Onishi studied a certain family \( \{ E_\lambda \} \) of elliptic curves over \( \mathbb{Q}(i) \), with complex multiplication by \( \mathbb{Z}[i] \) and Mordell-Weil rank 0, parametrized by degree one primes \( \lambda \in \mathbb{Z}[i] \), and showed\(^1\)\(^2\) that the congruence relation

\[
\# \text{III}(E_\lambda / \mathbb{Q}(i)) \equiv \mod \ell \ 	ext{Hurwitz-type number}
\]

up to multiplication by powers of 2, where \( \ell \) is the norm prime of \( \lambda \) satisfying \( \ell \equiv 5 \mod 8 \), holds by proving the congruences between the coefficients of elliptic Gauss sums and Hurwitz-type numbers (defined as power series coefficients of certain elliptic functions), and that, moreover, under the BSD conjecture on the 2-part of the leading term for the elliptic curve \( E_\lambda \), the congruence above for \( E_\lambda \) holds without ambiguity of multiplication by powers of 2. Here, \( \text{III}(E_\lambda / \mathbb{Q}(i)) \) is the Tate-Shafarevich group of the elliptic curve \( E_\lambda / \mathbb{Q}(i) \). The Hurwitz-type number of an elliptic function (with the period lattice \( \mathbb{Z}[i] \)) is an analogue of the Bernoulli number or the Euler number.

In this paper, we prove an analogue of Onishi’s result for the Eisenstein integer ring \( \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] \). To explain the main results of this paper precisely, we first introduce some notation and definitions: let \( \rho := e^{2\pi i} \), \( \varpi_1 := \int_0^1 \frac{dt}{\sqrt{(1-t^2)^2}} \) (the real period of the elliptic curve \( y^2 = 4x^3 - 27 \); see Lemma \( 12 \)), and \( \varphi(u) := \frac{6u}{u^3+1} \), \( \text{Sl}(u) := \varphi\left(\frac{u}{\sqrt{1-u^2}}\right) \), where \( \varphi \) is the Weierstrass \( \varphi \) function with the period lattice \( \varpi_1 \mathbb{Z}[\rho] \).

We define the rational numbers \( C_n, D_n \) as

\[
\text{Sl}(u) =: \sum_{n=0}^{\infty} C_{3n+1} u^{3n+1}, \quad \text{Sl}(u)^{-1} =: \frac{1}{u} + \sum_{n=0}^{\infty} D_{3n+2} u^{3n+2}.
\]

\((C_{3n+1}, D_{3n+2}) \) have easy recurrence relations, respectively; see the proof of Lemma \( 15 \) and Remark \( 19 \).

The rational numbers \( C_{3n+1}, D_{3n+2} \) of elliptic functions (with the period lattice \( \mathbb{Z}[\rho] \)) are analogues of the Bernoulli numbers or the Euler numbers and we call them \textbf{Bernoulli-Hurwitz-type numbers}, named after Katz’ paper \( K_a \). Let \( \ell \) be a rational prime number such that \( \ell \equiv 1 \mod 3 \), \( \lambda \in \mathbb{Z}[\rho] \) a prime element such that \( \ell = \lambda \ell \) and \( \lambda \equiv 1 \mod 3 \). We denote by \( \chi_\lambda \) the cubic residue character over \( (\mathbb{Z}[\rho]/(\lambda))^\times \simeq \mathbb{F}_\ell^* \) and set \( \lambda := \prod_{\chi_\lambda = 1} \varphi\left(\frac{\lambda}{\ell}\right) \). (Then \( \lambda^3 = \lambda \) holds; see Lemma \( 15 \)) Let

\[
G_\lambda(\chi_\lambda, \varphi) := \frac{1}{3} \sum_{\nu \in (\mathbb{Z}[\rho]/(\lambda))^\times} \chi_\lambda(\nu) \varphi\left(\frac{\nu}{\lambda}\right), \quad G_\lambda(\chi_\lambda, \varphi^{-1}) := \frac{1}{3} \sum_{\nu \in (\mathbb{Z}[\rho]/(\lambda))^\times} \chi_\lambda(\nu) \varphi\left(\frac{\nu}{\lambda}\right)^{-1}.
\]

\( G_\lambda(\chi_\lambda, \varphi) \) (resp. \( G_\lambda(\chi_\lambda, \varphi^{-1}) \)) is called the \textbf{elliptic Gauss sum} associated to \( \chi_\lambda \) and \( \varphi \) (resp. \( \varphi^{-1} \)). We define

\[
\alpha_\lambda := \left\{ \begin{array}{ll}
G_\lambda(\chi_\lambda, \varphi)/\lambda^2 & \ell \equiv 7 \mod 9, \\
G_\lambda(\chi_\lambda, \varphi^{-1})/\lambda^2 & \ell \equiv 4 \mod 9.
\end{array} \right.
\]

The number \( \alpha_\lambda \) is called the \textbf{coefficient of the elliptic Gauss sum}. (Then, \( \alpha_\lambda \in \chi_\lambda(3)(1+3\mathbb{Z}) \) or \( \alpha_\lambda \in \chi_\lambda(3)(-1+3\mathbb{Z}) \) hold; see Theorem \( 23 \)) The following two theorems are the main results of this paper:

\textbf{Theorem.} (Theorem \( 26 \)) The denominator of \( C_{\frac{3}{2}(\ell-1)} \) (resp. \( D_{\frac{3}{2}(\ell-1)} \)) cannot be divided by \( \ell \) when \( \ell \equiv 7 \mod 9 \) (resp. \( \ell \equiv 4 \mod 9 \)). We have

\[
\alpha_\lambda \equiv \mod \lambda \left\{ \begin{array}{ll}
-\frac{1}{3} C_{\frac{3}{2}(\ell-1)} & \ell \equiv 7 \mod 9, \\
-\frac{1}{3} D_{\frac{3}{2}(\ell-1)} & \ell \equiv 4 \mod 9.
\end{array} \right.
\]

\textsuperscript{1}By using \( \mathcal{R} \), the main result of \( \mathcal{O} \) can be easily improved in this form.
Theorem. (Theorem 3.6 and Corollary 3.8) We write \( \lambda = 3m + 1 + 3np, \ m, n \in \mathbb{Z} \). Then, for the elliptic curve \( \mathcal{E}_\lambda : y^2 = x^3 + \frac{3n}{\lambda} \), we have

\[
\# \mathcal{III}(\mathcal{E}_\lambda / \mathbb{Q}(\rho)) = \begin{cases} 
|\alpha_\lambda|^2/4 & \equiv_{\text{mod } \ell} \left(3 \frac{\ell}{2(\ell - 1)} \right)^2 /4 \ \ell \equiv 4 \text{ mod } 9 \text{ and } n \equiv 0 \text{ mod } 3, \\
|\alpha_\lambda|^2 & \equiv_{\text{mod } \ell} \left(3 \frac{\ell}{2(\ell - 1)} \right)^2 \ \ell \equiv 4 \text{ mod } 9 \text{ and } n \equiv \pm 1 \text{ mod } 3, \\
|\alpha_\lambda|^2 & \equiv_{\text{mod } \ell} \left(3 \frac{\ell}{2(\ell - 1)} \right)^2 \ \ell \equiv 7 \text{ mod } 9,
\end{cases}
\]

(0.1)

up to multiplication by powers of 2, 3. Moreover, for \( p = 2, 3 \), under the BSD conjecture on the \( p \)-part of the leading term for the elliptic curve \( \mathcal{E}_\lambda \), the congruence (0.1) holds without the ambiguity of multiplication by powers of \( p \).

Note that \( \mathcal{E}_\lambda \) is an elliptic curve over \( \mathbb{Q}(\rho) \) with complex multiplication by \( \mathbb{Z}[\rho] \) and Mordell-Weil rank 0, by [CW] and the non-vanishing of \( L(\mathcal{E}_\lambda / \mathbb{Q}(\rho), 1) \) (due to [A]), where \( L(\mathcal{E}_\lambda / \mathbb{Q}(\rho), s) \) is the \( L \)-function of the elliptic curve \( \mathcal{E}_\lambda / \mathbb{Q}(\rho) \) (see the proof of Theorem 3.6).

We explain the outline of the proof of the main results roughly. Corollary 3.8 is proved by verifying the following relationship:

Bernoulli-Hurwitz-type number \( \longrightarrow \) Elliptic Gauss sum \( \longrightarrow \) Hecke \( L \)-value \( \longrightarrow \) Elliptic \( L \)-value \( \longrightarrow \) \# III

The relationship (1) is the content of Theorem 2.5 which is proved by taking \( \varphi \left( \frac{1}{3} \right) \)-adic expansions of \( \varphi \left( \frac{1}{3} \right)^{s+1} \) and the elliptic Gauss sums and taking mod \( \varphi \left( \frac{1}{3} \right)^{s+1} \). The relationship (2) is due to Asai [A]. The relationship (3) is the equality \( L(s, \overline{\chi})L(s, \overline{\chi^3}) = L(\mathcal{E}_\lambda / \mathbb{Q}(\rho), s) \) given in Proposition 3.4 which is directly proved by the cubic reciprocity law and expressing the local \( L \)-factors of \( L(\mathcal{E}_\lambda / \mathbb{Q}(\rho), s) \) in terms of Jacobi sums, where \( \overline{\chi} \) is the Hecke character associated to \( \chi \), and \( L(s, \overline{\chi^3}) \) is the Hecke \( L \)-series associated to \( \overline{\chi^3} \). The relationship (4) is the content of Theorem 3.6 which is shown by using Rubin’s result [R] and calculations of the real period of \( \mathcal{E}_\lambda \), local Tamagawa numbers, and \( \# \mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}} \).

The proofs of these results are similar to the ones of the main results of [O], approximately. But there are some differences of the proofs, the phenomena and the outputs between this paper and [O]. First, the denominator of \( d_{6n+2} \), which appears in Theorem 2.5 is easy, i.e., a power of 3 (see Lemma 1.12), although the denominator of \( H_{4n} \) in [O] is more arithmetical (see [Ka]). Next, Theorem 3.6 implies \( |\alpha_\lambda|^2 \) is divisible by 4 for \( \ell \equiv 4 \text{ mod } 9 \) and \( n \equiv 0 \text{ mod } 3 \), while Proposition 3.9 of [O] in the Gaussian case does not imply such divisibility.

Note that the results of [O] and this paper are studied only over the Gaussian and Eisenstein integers. Since the fields \( \mathbb{Q}(i) \) and \( \mathbb{Q}(\rho) \) are imaginary quadratic fields and cyclotomic fields at once, we think that the situation is easy. To extend the results to the imaginary quadratic field \( \mathbb{Q}(\sqrt{-p}) \) for a rational prime \( p > 3 \), we may have to consider the inclusion \( \mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p) \) if \( p \equiv 3 \text{ mod } 4 \), \( \mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_{4p}) \) if \( p \equiv 1 \text{ mod } 4 \) at some point.

Finally, we explain the organization of this paper. In Chapter 1, we study properties of certain elliptic functions whose period lattice is the Eisenstein integers. We use these properties to define the elliptic Gauss sums and their coefficients. In Chapter 2, we introduce the elliptic Gauss sums and show the main congruences (Theorem 2.5) between the Bernoulli-Hurwitz-type numbers and the coefficients of the elliptic Gauss sums. In Chapter 3, we study certain Hecke characters, the Hecke \( L \)-series associated to them, certain elliptic curves \( \mathcal{E}_\lambda \) for \( \lambda \), and their \( L \)-functions relevant to our elliptic Gauss sums. Moreover, we show the main results (Theorem 3.6 and Corollary 3.8). In Appendix, we show some lemmas, formulae and tables of \( C_n, D_n \), etc. which are not used in the proofs of the main results of this paper but are of independent interest.
Acknowledgments

The author would like to express his great gratitude to his advisors Professors Akio Tamagawa and Go Yamashita for their careful and constant advice for the study of this paper. Especially, Professor Yamashita suggested the research of elliptic Gauss sums to the author and corrected many errors of the draft. Moreover, the author is very thankful to them for guiding the author in the master seminar.

1 Elliptic functions

In Chapter 1, we study properties of certain elliptic functions whose period lattice is the Eisenstein integers (or its constant multiple). In §1.1, we introduce elliptic functions $\text{Sl}(\rho)$, $\text{Cl}(\varphi)$, and $\psi$, and their function-theoretic properties. In §1.2, we study power series expansions of $\text{Sl}(ru), \text{Sl}(ru)^{-1}(r \in \mathbb{Z} \setminus \{0\})$ in terms of $\text{Sl}(u)$, which will be used to show the main congruences in Chapter 2. In §1.3, we introduce Bernoulli-Hurwitz-type numbers, which will also be used to show the main congruences in Chapter 2. In §1.4, we study some arithmetic properties of the values of $\text{Sl}(u)$ at division points.

Let $\rho$ be the cubic root $e^{2\pi i/3} = -\frac{1 + \sqrt{-3}}{2}$ of unity, where the imaginary part of $\sqrt{-3}$ is $> 0$.

1.1 The basic properties of elliptic functions in the case of Eisenstein integers

We denote by $\varpi_1$ (See [A] §1.1.1) the real period given by

$$\varpi_1 = \int_0^1 \frac{dt}{\sqrt{(1 - t^3)^2}} = 1.76663875 \cdots ,$$

and let $\varphi(u)$ denote Weierstrass' $\varphi$ function with the period lattice $\varpi_1 \mathbb{Z} \rho$, so that $\varphi^2 = 4\varphi^3 - 27$ (See Lemma 1.2). In this paper, $(\cdot)$ denotes the complex conjugate. We write

$$W := \{ \pm 1, \pm \rho, \pm \overline{\rho} \}, \quad W' := \{ 1, \rho, \overline{\rho} \}.$$

**Lemma 1.1.** (The real period and the beta function) $\varpi_1 = \frac{1}{2} B \left( \frac{1}{3}, \frac{1}{3} \right) = \frac{1}{2\pi^3} \Gamma \left( \frac{1}{3} \right)^3 = \frac{2}{3\pi} B \left( \frac{1}{3}, \frac{1}{3} \right)$, where $B$ and $\Gamma$ denote the beta and gamma functions respectively.

**Proof.** Let $g$ denote $\Gamma \left( \frac{1}{3} \right)$. Then we have $\frac{\varpi_1}{\sqrt{3}} = \frac{2\sqrt{3\pi}}{\sqrt{2\pi}} g^2$ by the formula $\Gamma(s)\Gamma(1 - s) = \frac{\pi}{\sin(\pi s)}$. We also have $\frac{\varpi_1}{\sqrt{3}} = \frac{2\sqrt{3\pi}}{\sqrt{2\pi}} g^2$, since $\frac{\varpi_1}{\sqrt{3}} = \frac{2\sqrt{3\pi}}{\sqrt{2\pi}} g^2$ by putting $s = \frac{1}{3}$ in the formula $\Gamma(s)\Gamma(1 - s) = \frac{2\sqrt{3\pi}}{\sqrt{2\pi}} g^2$. Then, $B \left( \frac{1}{3}, \frac{1}{3} \right) = \frac{\Gamma(\frac{1}{3})\Gamma(\frac{1}{3})}{\Gamma(\frac{1}{3})} = \frac{\sqrt{3\sqrt{2\pi}} g^2}{2\pi g^2} = \frac{3}{2\pi} g^2$, by the formula $\Gamma \left( \frac{1}{3} \right) = \sqrt{\pi}$. By definition and the formula $B(s, t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s + t)}$, we obtain

$$\varpi_1 = \int_0^1 \frac{dt}{\sqrt{(1 - t^3)^2}} = \frac{1}{3} \int_0^1 x^{-\frac{1}{3}} (1 - x)^{-\frac{2}{3}} dx = \frac{1}{3} B \left( \frac{1}{3}, \frac{1}{3} \right) = \frac{1}{3} \frac{g^2}{2\pi \sqrt{3}} = \frac{g^3}{3\sqrt{3}} = \frac{2+}{3\sqrt{3}} B \left( \frac{1}{6}, \frac{1}{2} \right),$$

where $x = t^3$.

**Lemma 1.2.** (Elementary properties of $\varphi$-function with the period lattice $\varpi_1 \mathbb{Z} \rho$) We have

1. $\varphi(\rho u) = \rho \varphi(u), \varphi(-u) = \varphi(u), \varphi'(\rho u) = \varphi'(u), \varphi'(-u) = -\varphi'(u)$,
2. $\varphi(\overline{u}) = \overline{\varphi(u)}, \varphi'(\overline{u}) = \overline{\varphi'(u)}$, thus if $u \in \mathbb{R}$, $\varphi(u), \varphi'(u) \in \mathbb{R}$,
3. The function $\varphi$ satisfies $\varphi^2 = 4\varphi^3 - 27$,
4. $\varphi \left( \frac{\varpi_1}{3} \right) = 3, \varphi \left( \frac{4}{3} \varpi_1 \right) = 3\rho, \varphi \left( \frac{\varpi_1}{3} \right) = 3\overline{\rho}, \varphi \left( \frac{1 + \rho}{3} \varpi_1 \right) = 0$,
5. $\varphi' \left( \frac{\varpi_1}{3} \right) = \varphi' \left( \frac{4}{3} \varpi_1 \right) = \varphi' \left( \frac{\varpi_1}{3} \right) = -9, \varphi' \left( \frac{1 + \rho}{3} \varpi_1 \right) = -3\sqrt{3}$. 


Proof. Since \( \varphi(u) = e^{1_{\frac{u}{\text{u}}}} + \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \left( \frac{1}{u - \omega\rho} - \frac{1}{\omega^2} \right) \) and \( \rho, -1 \in (\mathbb{Z}[\rho])^\times \),

\[
\varphi'(\rho u) = \frac{1}{(\rho u)^2} + \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \left( \frac{1}{(\rho u - \rho\omega)^2} - \frac{1}{(\rho\omega)^2} \right) = \frac{1}{\rho^2} \left( \frac{1}{u^2} + \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \left( \frac{1}{(u - \omega)^2} - \frac{1}{\omega^2} \right) \right) = \frac{1}{\rho^2} \varphi(u) = \rho \varphi(u),
\]

\[
\varphi'(-u) = \frac{1}{(-u)^2} + \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \left( \frac{1}{(-u - (-\omega))^2} - \frac{1}{(-\omega)^2} \right) = \frac{1}{u^2} + \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \left( \frac{1}{(u - \omega)^2} - \frac{1}{\omega^2} \right) = \varphi(u).
\]

Differentiating both hands of \( \varphi'(\rho u) = \rho \varphi(u), \varphi'(-u) = \varphi(u) \), we also get \( \varphi'(\rho u) = \varphi'(u), \varphi'(-u) = -\varphi'(u) \) respectively.

2 It is obvious, since \( \mathbb{Z}[\rho] = \mathbb{Z}[\rho] \).

3 Then, \( \varphi' = 4\varphi^2 - 60G_4 \varphi - 140G_6 \), where \( G_6 := \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \frac{1}{\omega^6} \), and

\[
G_4 := \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \frac{1}{\omega^4} = \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \frac{1}{(\rho\omega)^4} = \frac{1}{\rho^4} \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \frac{1}{\omega^4} = \frac{1}{\rho^4} \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \frac{1}{\omega^4} = \rho G_4.
\]

Thus, \( G_4 = 0 \) and \( \varphi^2 = 4\varphi^3 - 140G_6 = 4(\varphi - \varphi(\frac{2}{3} \varphi))((\varphi - \varphi(\frac{2}{3} \varphi))((\varphi - \varphi(\frac{4}{3} \varphi))) \). We denote \( e := \varphi(\frac{2}{3}) \).

Then, since \( \rho e = \varphi(\frac{2}{3} \varphi), \rho E = \varphi(\frac{2}{3} \varphi) = \varphi(-\frac{1}{3} \rho \varphi = \varphi(\frac{1}{3} + \rho \varphi(\frac{2}{3} \varphi)) \) by 1, we have \( 4e^3 = 4\varphi(\frac{2}{3} \varphi) \varphi(\frac{2}{3} \varphi) \varphi(\frac{1}{3} + \rho \varphi(\frac{2}{3} \varphi)) = 140G_6 \). We also have, by Lemma 1.1

\[
\frac{\varphi_1}{2} = \int_0^{\frac{1}{2}} du = \int_0^\infty d(\varphi(u)) = \int_0^\infty \left( \frac{dx}{\sqrt{4x^3 - 4e^3}} \right) = \frac{1}{2e^2} \int_0^\infty \left( \frac{dx}{\sqrt{x^3 - 1}} \right) = \frac{1}{2e^2} \int_0^1 y^{-\frac{8}{3}} (1-y)^{-\frac{1}{2}} dy = \frac{1}{2e^2} \left( \frac{1}{6} \right) = \frac{1}{2e^2} \varphi_1.
\]

where \( y = x^{-3} \). Hence \( 4e^3 = 27 \).

4 By 1 and the periodicity of \( \varphi \), we have \( \varphi(\frac{1}{3} - \rho \varphi(\frac{2}{3} \varphi) = \varphi(1 + \frac{2}{3} \varphi) = \varphi(\frac{1}{3} + \rho \varphi(\frac{2}{3} \varphi) = \varphi(\frac{1}{3} + \rho \varphi(\frac{2}{3} \varphi) = \rho \varphi(-\frac{1}{3} + \rho \varphi(\frac{2}{3} \varphi) \). Hence,

\[
\varphi\left(\frac{1}{3} - \rho \varphi(\frac{2}{3} \varphi) = 0 \quad (1.1)
\]

By \( \varphi^2 = 4\varphi^3 - 27 \), we have

\[
\varphi^2\left(\frac{1}{3} - \rho \varphi(\frac{2}{3} \varphi) = -27 \quad (1.2)
\]

In particular, we have

\[
\varphi^2\left(\frac{1}{3} - \rho \varphi(\frac{2}{3} \varphi) \in i\mathbb{R}. \quad (1.3)
\]

By putting \( u_1 = \frac{1}{3} - \rho \varphi(\frac{2}{3} \varphi) \) and \( u_2 = \varphi(\frac{2}{3} \varphi) \) in the addition formula (see, for example, WW Chap. XX, 20.3)

\[
\varphi(u_1 + u_2) = -\varphi(u_1) - \varphi(u_2) + \frac{1}{4} \left( \frac{\varphi'(u_1) - \varphi'(u_2)}{\varphi(u_1) - \varphi(u_2)} \right)^2,
\]

1 and (1.1), we have

\[
\varphi\left(\frac{1}{3} \varphi(\frac{2}{3} \varphi) = -\varphi\left(\frac{1}{3} \varphi(\frac{2}{3} \varphi) = \frac{1}{4} \left( \varphi'(\frac{1}{3} \varphi(\frac{2}{3} \varphi) - \varphi'(\frac{2}{3} \varphi) \right)^2,
\]

5
thus, by (1.2),
\[-4\rho \wp \left( \frac{\wp_1}{3} \right)^3 = (1 + \rho) \wp \left( \frac{\wp_1}{3} \right) 4 \left( -\rho \wp \left( \frac{\wp_1}{3} \right) \right)^2 = \left( \wp' \left( \frac{1 - \rho}{3} \wp_1 \right) - \wp' \left( \frac{\wp_1}{3} \right) \right)^2 \]
\[= -27 + \wp' \left( \frac{\wp_1}{3} \right)^2 - 2 \wp' \left( \frac{1 - \rho}{3} \wp_1 \right) \wp' \left( \frac{\wp_1}{3} \right). \tag{1.4} \]
By taking the real part of the equation (1.4), we get
\[2 \wp' \left( \frac{\wp_1}{3} \right)^3 = -27 + \wp' \left( \frac{\wp_1}{3} \right)^2 = -27 + 4 \wp \left( \frac{\wp_1}{3} \right)^3 - 27,
\]
since (3) and (1.3) and \(\wp (\frac{\wp_1}{3}), \wp' (\frac{\wp_1}{3}) \in \mathbb{R} \) by (2). Hence we have \(\wp (\frac{\wp_1}{3})^3 = 27\). Since \(\wp (\frac{\wp_1}{3}) \in \mathbb{R}\), we obtain \(\wp (\frac{\wp_1}{3}) = 3\). From \(\wp (\frac{\wp_1}{3}) = 3\) and (11), we get also \(\wp \left( \frac{\wp}{3} \wp_1 \right) = 3\rho\) and \(\wp \left( \frac{\pi}{3} \wp_1 \right) = 3\pi\).

(3) The divisor of \(\wp'(u)\) is \(-3(0) + (\frac{\wp_1}{3}) + (\frac{\wp_1}{3}) + (\frac{(1 + \rho)\wp_1}{2}) \pmod{\wp_1 \mathbb{Z}[\rho]}\). Then, the function \((0, \wp_1) \to \mathbb{R}, u \mapsto \wp'(x)\) has a unique zero at \(x = \frac{\wp_1}{2}\), where \((0, \wp_1)\) is an open interval. Since \(\lim_{x \to +0} \wp'(x) = -\infty\) from \(\wp'(u) = -\frac{1}{u} + \cdots\) among \(u = 0\), it holds \(\wp'(x) < 0\) for \(x \in (0, \frac{\wp_1}{2})\). Especially \(\wp' (\frac{\wp_1}{3}) < 0\). Since \(\wp (\frac{\wp_1}{3}) = 3\) (by (3)) and \(\wp'^2 = 4\wp^3 - 27\) (by (3)), we get \(\wp' (\frac{\wp_1}{3})^2 = 81\). Then, we get \(\wp' (\frac{\wp_1}{3}) = -9\). By (11), we also get \(\wp' (\frac{\wp_1}{3}) = \wp' (\frac{\pi}{3} \wp_1) = \wp' (\frac{\pi}{3} \wp_1) = 9\). By (1.4) and (11), we get
\[-4 \rho \cdot 27 = -4\rho \wp \left( \frac{\wp_1}{3} \right)^3 = -27 + \wp' \left( \frac{\wp_1}{3} \right)^2 - 2 \wp' \left( \frac{1 - \rho}{3} \wp_1 \right) \wp' \left( \frac{\wp_1}{3} \right) = -27 + (9)^2 - 2 \wp' \left( \frac{1 - \rho}{3} \wp_1 \right) (-9).
\]
Hence we have \(\wp' \left( \frac{1 - \rho}{3} \wp_1 \right) = \frac{-4\rho \cdot 27 + 27 - (9)^2}{18} = -3(2\rho + 1) = -3\sqrt{-3}.\]

**Definition 1.3.** ([A] Definition 1.1, 1.2) Let \(\zeta(u)\) denote Weierstrass’ \(\zeta\) function associated to the lattice \(\wp_1 \mathbb{Z}[\rho]\). We define
\[
\begin{align*}
Z(u) & := \zeta(\wp_1 u) - \frac{2\pi}{\sqrt{3}\wp_1},  \\
\varphi(u) & := \frac{1}{3} \left\{ 2\zeta \left( u - \frac{1}{3} \right) + \frac{2}{3} \varphi \left( u - \frac{1}{3} \right) + \frac{1}{3} \varphi \left( u - \frac{1}{3} \right) \right\},  \\
\psi(u) & := -\frac{1}{3} \left\{ 2\zeta \left( u - \frac{1}{3} \right) + \frac{2}{3} \varphi \left( u - \frac{1}{3} \right) + \frac{1}{3} \varphi \left( u - \frac{1}{3} \right) \right\},  \\
\text{Sl}(u) & := \varphi \left( \frac{u}{-3\wp_1} \right),  \\
\text{Cl}(u) & := \psi \left( \frac{u}{-3\wp_1} \right).
\end{align*}
\]

Note also that
\[
Z(u + v) = Z(u) + Z(v) + \frac{1}{2} \frac{\wp'(u)}{\wp(u)} \varphi'(v),
\]
which follows from the addition formula (see, for example, [WWW] Chap. XX, 20.53, example 2])
\[
\zeta(u + v) = \zeta(u) + \zeta(v) + \frac{1}{2} \frac{\wp'(u)}{\wp(u)} \varphi'(v).
\tag{1.6}
\]

We recall the basic properties of these functions stated in [A] without proofs:

**Lemma 1.4.** (Elementary properties of \(\zeta, Z, \varphi, \psi, \text{Sl}, \text{Cl}\))(cf. [A] §1.1.1) for (3) and (5–10) The following hold:

1. \(\zeta(\rho u) = \sqrt{3} \varphi(u)\), \(\zeta(-u) = -\zeta(u)\), \(\zeta \left( \frac{\wp_1}{2} \right) = \frac{\pi}{\sqrt{3} \wp_1}\), \(\zeta \left( \frac{\pi}{3} \wp_1 \right) = \frac{\pi}{\sqrt{3} \wp_1}\).

2. The function \(Z\) is a non-holomorphic periodic function with the period lattice \(\mathbb{Z}[\rho]\), and satisfies \(Z(\rho u) = \wp Z(u), Z(-u) = -Z(u), Z \left( \frac{1}{3} \right) = 1, Z \left( \frac{1 - \rho}{3} \right) = 0.\)
(3) \( \varphi(u) = \frac{6\varphi(\varpi_1 u)}{9 + \varphi'((\varpi_1 u)^2)}, \psi(u) = \frac{-9 + \varphi'((\varpi_1 u)^2)}{9 + \varphi'(\varpi_1 u)}. \) Thus, \( \varphi, \psi \) are elliptic functions with the period lattice \( \mathbb{Z}[\rho] \), and \( \text{Sl}(u), \text{Cl}(u) \) are elliptic functions with the period lattice \( 3\varpi_1 \mathbb{Z}[\rho] \).

(4) \( \varphi(\varpi_1 u) = \frac{3\varphi(u)}{1 - \psi(u)}, \varphi'(\varpi_1 u) = \frac{1 + \psi(u)}{1 - \psi(u)}. \)

(5) \( \varphi(\rho u) = \rho \varphi(u), \text{Sl}(\rho u) = \rho \text{Sl}(u), \psi(\rho u) = \psi(u), \text{Cl}(\rho u) = \text{Cl}(u). \)

(6) \( \varphi'(u) = -3\varpi_1 \psi(u)^2, \psi'(u) = 3\varpi_1 \varphi(u)^2, \text{Sl}'(u) = \text{Cl}(u)^2, \text{Cl}'(u) = -\text{Sl}(u)^2. \)

(7) \( \varphi(u)^3 + \psi(u)^3 = 1, \text{Sl}(u)^3 + \text{Cl}(u)^3 = 1, \varphi(0) = 0, \psi(0) = 1, \text{Sl}(0) = 0, \text{Cl}(0) = 1. \)

(8) \( \varphi(-u) = -\frac{\varphi(u)}{\psi(u)} = -\frac{\text{Sl}(u)}{\text{Cl}(u)}, \psi(-u) = \frac{1}{\psi(u)}, \text{Cl}(-u) = \frac{1}{\text{Cl}(u)}. \)

(9) \( \text{Sl}(-3\varpi_1 u)^{-1} + \text{Sl}(3\varpi_1 u)^{-1} = \varphi(u)^{-1} + \varphi(-u)^{-1} = 3\varphi(\varpi_1 u)^{-1}. \)

(10) \( \zeta((1 - \rho)\varpi_1 u) = (1 - \rho)\zeta(\varpi_1 u) + (1 - \rho)(\varphi(u)^{-1} - \varphi(-u)^{-1}). \)

**Proof.** (1) The claims \( \zeta((\rho u) \varpi_1 u) = \varphi(u) \zeta(u), \zeta(-u) = -\zeta(u) \) are proved similarly as Lemma \( \text{L2} \). Thus, it suffices to show that \( \zeta(\varpi_1 u) = \frac{2\pi i}{3\varpi_1}. \) This is proved by Legendre’s relation (see, for example, \([\text{WW}, \text{Chap.XX}, 20.411]\) )

\[
\frac{\rho \varpi_1}{2} \zeta\left(\frac{\varpi_1 u}{2}\right) = \frac{2\pi i}{3\varpi_1}.
\]

(2) The claims \( Z(\rho u) = \varpi_1 Z(u), \ Z(-u) = -Z(u) \) are trivial by the definition and \( \text{L1} \). By the quasi-periodicity (see, for example, \([\text{WW}, \text{Chap.XX}, 20.411]\) )

\[
\zeta\left(\varpi_1 u + 1\right) = \zeta(\varpi_1 u) + 2\zeta\left(\frac{\varpi_1 u}{2}\right),
\]

we have

\[
Z(u + 1) - Z(u) = \zeta(\varpi_1 u + 1) - \zeta(\varpi_1 u) - \frac{2\pi}{\sqrt{3}\varpi_1} = 2\zeta\left(\frac{\varpi_1 u}{2}\right) - \frac{2\pi}{\sqrt{3}\varpi_1} = 0.
\]

Then, we also have \( Z(u + \rho) - Z(u) = Z(\rho(\varpi_1 u + 1)) - Z(\rho \cdot \varpi_1 u) = \varpi_1 Z(\varpi_1 u + 1) - Z(\varpi_1 u) = 0. \) Thus, it is proved that \( Z \) is periodic with the period lattice \( \mathbb{Z}[\rho] \). The claim \( Z\left(\frac{\varpi_1 u}{2}\right) = 0 \) is similarly proved as \( \varphi\left(\frac{\varpi_1 u}{2}\right) \) in Lemma \( \text{L2} \). The claim \( Z\left(\frac{u}{2}\right) = 0 \) is proved by putting \( u = \frac{1}{\varpi_1}, \nu = \frac{3}{3\varpi_1} \) in \( \text{L3} \), \( Z\left(\frac{1}{2}\right) = 0, \ Z(\rho u) = \varpi_1 Z(u) \), and Lemma \( \text{L2} \). (4) and (5).

(3) For \( w \in \{1, 2, 3\}, \) \( W' \) by putting \( v = \frac{w}{3} \) in \( \text{L4} \),

\[
Z\left(u - \frac{w}{3}\right) = Z(u) + Z\left(-\frac{w}{3}\right) - \frac{1}{2} \frac{\varphi'(\varpi_1 u) - \varphi'\left(-\frac{w}{3}\varpi_1 u\right)}{\varphi(\varpi_1 u) - \varphi(-\frac{w}{3}\varpi_1 u)} = Z(u) - \frac{w}{3} + \frac{1}{2} \frac{\varphi'(\varpi_1 u) - 9}{\varphi'(\varpi_1 u) - 3w},
\]

by \( \text{L2} \), and Lemma \( \text{L2} \). (4) and (5). Then, by the definition of \( \varphi \), the facts that \( \sum_{w \in W', w} = 0, \sum_{w \in W', w} w = \sum_{w \in W'} w, \varpi = 0, \sum_{w \in W', w} w = \frac{3w}{3\varpi - 1} \), and Lemma \( \text{L2}, \text{L3} \), we have

\[
3\varphi(u) = \sum_{w \in W'} w Z\left(u - \frac{w}{3}\right) = \sum_{w \in W'} w Z(u) - \sum_{w \in W'} w + \frac{\varphi'(\varpi_1 u) - 9}{2 \varphi'(\varpi_1 u) - 3w} \sum_{w \in W'} \varpi = \frac{\varphi'(\varpi_1 u) - 9}{2 \varphi'(\varpi_1 u) - 3w},
\]

Thus \( \varphi(u) = \frac{6\varphi(\varpi_1 u)}{\varphi'(\varpi_1 u) + 9}. \) Similarly, by \( \sum_{w \in W'} \frac{w}{3 - \varpi} = \frac{3w}{3\varpi - 1} \), we have

\[
-3\psi(u) = \sum_{w \in W'} w Z\left(u - \frac{w}{3}\right) = \sum_{w \in W'} w Z(u) - \sum_{w \in W'} 1 + \frac{\varphi'(\varpi_1 u) - 9}{2 \varphi'(\varpi_1 u) - 3w} \sum_{w \in W'} w = -3 + \frac{\varphi'(\varpi_1 u) - 9}{2 \varphi'(\varpi_1 u) - 3w} = -3 + \frac{54}{\varphi'(\varpi_1 u) + 9}. 
\]
Thus $\psi(u) = 1 - \frac{18}{\varphi(\varpi_1 u) + \varpi} = \frac{\psi(\varpi_1 u) - \varpi}{\varphi(\varpi_1 u) + \varpi}$.

This is proved by solving two equations of 3 in terms of $\varphi(\varpi_1 u)$ and $\psi(\varpi_1 u)$.

It is trivial, since Lemma 1.2 (1), (2), and (3).

This is proved by differentiating two equations of 3 and the facts that $\psi'^2 = 4\psi^3 - 27$ and $\psi'' = 6\psi^2$.

By 9, we have

$$(\varphi^3 + \psi^3)' = 3(\varphi^2 \psi' + \psi^2 \varphi') = 9\varpi_1 (-\varphi^2 \psi^2 + \psi^2 \varphi^2) = 0.$$ 

Thus, $\varphi^3 + \psi^3$ is constant. On the other hand, $\varphi(0) = 0, \psi(0) = 1$, since 3, and the fact $\varphi(u), \psi(u)$ have poles of order 2, 3 at $u = 0$ respectively. Therefore, we have $\varphi^3 + \psi^3 = 1$. By definitions of $\varphi$ and $\psi$, we also have $\varphi^3 + \psi^3 = 1$ and $\varphi(0) = 0, \psi(0) = 1$.

By 3 and Lemma 1.2 (1), it follows that

$$\varphi(-u) = \frac{6 \varphi(-\varpi_1 u)}{9 + \varphi'(-\varpi_1 u)} = \frac{6 \varphi(\varpi_1 u)}{9 - \varphi'(\varpi_1 u)} = \frac{9 + \varphi'(\varpi_1 u)}{9 - \varphi'(\varpi_1 u)} = \varphi(u).$$

By definitions of $\varphi$ and $\psi$, we also have $\varphi(-u) = \frac{\varphi(\varpi_1 u)}{\varphi(\varpi_1 u)}$.

This is obvious from 3.

By substituting $u := \varpi_1 u, v := -\varpi_1 u$ in 1.6, 1, and Lemma 1.2 (1), we have

$$\zeta((1 - \rho)\varpi_1 u) = (1 - \varpi)\zeta(\varpi_1 u) + \frac{1}{1 - \rho} \frac{\varphi'(\varpi_1 u)}{\varphi(\varpi_1 u)}.$$ 

On the other hand, by 3 and Lemma 1.2 (1), we also have

$$\varphi(u)^{-1} - \varphi(-u)^{-1} = \frac{1}{3} \frac{
abla}{\varphi(\varpi_1 u)}.$$ 

Thus, 10 follows from these two equalities.

\[ \square \]

1.2 Power series expansions in terms of $\varphi$

Let us consider power series expansions in terms of the function $\varphi(u)$ in this section, which will be used to show the main congruences (Theorem 2.3).

We note that $\mathbb{Q}[\varphi(u)]$ is isomorphic to a formal power series ring over $\mathbb{Q}$. Indeed, since $\varphi(u)$ is an elliptic function which is holomorphic at $u = 0$. $\varphi(u)$ has infinitely many values around $u = 0$. Thus, $\varphi(u) \in \mathbb{Q}[u]$ is a transcendental element. First, we will show the following:

Lemma 1.5 (Addition formula of $\varphi(u)$). (cf. A § 1. Appendix 1. Addition Formula (i))

We have

$$\varphi(u + v) = \frac{\varphi(u)^2 \varphi(v) - \varphi(v)^2 \varphi(u)}{\varphi(u)^2 \varphi(v)^2 - \varphi(v)^2 \varphi(u)^2} \in \varphi(u) + \varphi(v) + (\varphi(u), \varphi(v))^{2}[1/3] [[\varphi(u), \varphi(v)]] \subset \mathbb{Q}[\varphi(u), \varphi(v)].$$

Proof. After putting $\alpha := (u + v)/2, \beta := (u - v)/2$, we can see that the partial derivative as $\beta$ of $f(\alpha, \beta) := \varphi(u)^2 \varphi(v) - \varphi(v)^2 \varphi(u)$ is zero. Hence, $f$ is a constant function of $\beta$. Therefore $f(\alpha, \beta) = f(\alpha, 0) = \varphi(u + v)$, by the last two equations of Lemma 1.4 (7). The equality of Lemma is proved.

It remains to show that $\varphi(u + v) \in \varphi(u) + \varphi(v) + (\varphi(u), \varphi(v))^{2}[1/3] [[\varphi(u), \varphi(v)]]$. Since Lemma 1.3 (7) and 9,

$$\varphi(u) = \sum_{n=0}^{\infty} (-1)^n \frac{(\frac{3}{n})}{\varphi(u)^{3n}} = 1 + \sum_{n=1}^{\infty} (-1)^n \frac{(\frac{3}{n})}{\varphi(u)^{3n}},$$

\[ \square \]
\[
\mathrm{Cl}(u)^2 = \sqrt[3]{(1 - \mathrm{Sl}(u)^3)^2} = \sum_{n=0}^{\infty} (-1)^n \left(\frac{2}{3} \right)^n \mathrm{Sl}(u)^{3n} = 1 + \sum_{n=1}^{\infty} (-1)^n \left(\frac{2}{3} \right)^n \mathrm{Sl}(u)^{3n}
\]

hold for \( u \in \mathbb{R} \) around \( u = 0 \). By the analytic continuations,

\[
\mathrm{Cl}(u) = 1 + \sum_{n=1}^{\infty} (-1)^n \left(\frac{1}{3} \right)^n \mathrm{Sl}(u)^{3n}, \quad \mathrm{Cl}(u)^2 = 1 + \sum_{n=1}^{\infty} (-1)^n \left(\frac{2}{3} \right)^n \mathrm{Sl}(u)^{3n}
\]

(1.7) hold for \( u \in \mathbb{C} \) around \( u = 0 \). Write \( x = \mathrm{Sl}(u), y = \mathrm{Sl}(v) \). Then, since (1.7),

\[
\mathrm{Sl}(u + v) = \frac{x^2 - y^2 + \sum_{n=1}^{\infty} (-1)^n \left(\frac{4}{3} \right)^n (x^2 y^{3n} - y^2 x^{3n})}{x - y + \sum_{n=1}^{\infty} (-1)^n \left(\frac{4}{3} \right)^n (xy^{3n} - yx^{3n})} = \frac{x + y - x^2 y^2 \sum_{n=1}^{\infty} (-1)^n \left(\frac{4}{3} \right)^n (x^{3n-3} + \cdots + y^{3n-3})}{1 - xy \sum_{n=1}^{\infty} (-1)^n \left(\frac{2}{3} \right)^n (x^{3n-2} + \cdots + y^{3n-2})} \in x + y + (x, y)^2 \mathbb{Z} \left[\frac{1}{3}\right][[x, y]].
\]

(1.8)

Here, we note that \( \left(1 - xy \sum_{n=1}^{\infty} (-1)^n \left(\frac{2}{3} \right)^n (x^{3n-2} + \cdots + y^{3n-2})\right)^{-1} \in 1 + (xy)\mathbb{Z} \left[\frac{1}{3}\right][[x, y]] \subset (\mathbb{Z} \left[\frac{1}{3}\right][[x, y]])^\times \), and \( \left(\frac{1}{3} \right), \left(\frac{2}{3} \right) \in \mathbb{Z} \left[\frac{1}{3}\right] \) (See p.52 of [W]).

Lemma 1.6. (Power series expansion of \( \mathrm{Sl}(ru) \) and \( \mathrm{Sl}(ru)^{-1} \) in terms of \( \mathrm{Sl}(u) \)) For any integer \( r \), we have

\[
\mathrm{Sl}(ru) \in r \mathrm{Sl}(u) + \mathrm{Sl}(u)^4 \mathbb{Z} \left[\frac{1}{3}\right][[\mathrm{Sl}(u)^3]] (\subset \mathbb{Q}[u]).
\]

We also have, if \( r \neq 0 \),

\[
\mathrm{Sl}(ru)^{-1} \in \frac{1}{r \mathrm{Sl}(u)} + \mathrm{Sl}(u)^2 \mathbb{Z} \left[\frac{1}{3}\right][[\mathrm{Sl}(u)^3]] \left(\subset \frac{1}{u} \mathbb{Q}[u]\right).
\]

Proof. There exists \( f(x, y) \in (x, y)^2 \mathbb{Z} \left[\frac{1}{3}\right][[x, y]] \) such that

\[
\mathrm{Sl}(u + v) = \mathrm{Sl}(u) + \mathrm{Sl}(v) + f(\mathrm{Sl}(u), \mathrm{Sl}(v))
\]

from Lemma 1.5. We will show that, for any \( r > 0 \), \( \mathrm{Sl}(ru) \in r \mathrm{Sl}(u) + \mathrm{Sl}(u)^4 \mathbb{Z} \left[\frac{1}{3}\right][[\mathrm{Sl}(u)^3]] \) by induction on \( r \). We assume that there exists \( r > 0 \) such that \( \mathrm{Sl}(ru) \in r \mathrm{Sl}(u) + \mathrm{Sl}(u)^4 \mathbb{Z} \left[\frac{1}{3}\right][[\mathrm{Sl}(u)^3]] \). Then, there exists \( f_r(t) \in \mathbb{Z} \left[\frac{1}{3}\right][[t]] \) such that \( \mathrm{Sl}(ru) = r \mathrm{Sl}(u) + \mathrm{Sl}(u)^4 f_r(\mathrm{Sl}(u)^3) \), where \( t \) is a variable. Then putting \( v := ru \), we have

\[
\mathrm{Sl}((r + 1)u) = \mathrm{Sl}(u) + \mathrm{Sl}(ru) + f(\mathrm{Sl}(u), \mathrm{Sl}(ru)) = \mathrm{Sl}(u) + (r \mathrm{Sl}(u) + \mathrm{Sl}(u)^4 f_r(\mathrm{Sl}(u)^3)) + f(\mathrm{Sl}(u), r \mathrm{Sl}(u) + \mathrm{Sl}(u)^4 f_r(\mathrm{Sl}(u)^3))
\]

\[
\in (r + 1) \mathrm{Sl}(u) + \mathrm{Sl}(u)^4 \mathbb{Z} \left[\frac{1}{3}\right][[\mathrm{Sl}(u)^3]],
\]

since \( f \) has no terms of degree 0 or 1, and the power series expansion of \( \mathrm{Sl}((r + 1)u) \) as \( \mathrm{Sl}(u) \) has only \( \mathrm{Sl}(u)^{3n+1} \) terms since \( \mathrm{Sl}(ru) = \rho \mathrm{Sl}(u) \). Therefore, \( \mathrm{Sl}(ru) \in r \mathrm{Sl}(u) + \mathrm{Sl}(u)^4 \mathbb{Z} \left[\frac{1}{3}\right][[\mathrm{Sl}(u)^3]] \) is proved for any \( r > 0 \).
Next, we will show that $\text{Sl}(-ru) \in -r\text{Sl}(u) + \text{Sl}(u)^4\mathbb{Z}\left[\frac{1}{3}\right] [[\text{Sl}(u)^3]]$ for any $r > 0$. Now, since $\text{Cl}(u)^{-1} = 
abla + \sum_{n=1}^{\infty}(-1)^n\left(\frac{1}{3} n\right) \text{Sl}(u)^{3n})^{-1} \in 1 + \text{Sl}(u)^4\mathbb{Z}\left[\frac{1}{3}\right] [[\text{Sl}(u)^3]] \subset (\mathbb{Z}\left[\frac{1}{3}\right] [[\text{Sl}(u)^3]])^\times$, and Lemma 1.4 (4) (5), by Lemma 1.4 (6), $(1 + \sum_{n=1}^{\infty}(-1)^n\left(\frac{1}{3} n\right) \text{Sl}(u)^{3n})^{-1} \in 1 + \text{Sl}(u)^4\mathbb{Z}\left[\frac{1}{3}\right] [[\text{Sl}(u)^3]]$

follows. Therefore, for any $r > 0$, $\text{Sl}(-ru) = r \text{Sl}(-u) + \text{Sl}(-u)^4f_r(\text{Sl}(-u)^3) \in -r\text{Sl}(u) + \text{Sl}(u)^4\mathbb{Z}\left[\frac{1}{3}\right] [[\text{Sl}(u)^3]]$

follows similarly to the former case. Thus, we have $\text{Sl}(ru) \in r\text{Sl}(u) + \text{Sl}(u)^4\mathbb{Z}\left[\frac{1}{3}\right] [[\text{Sl}(u)^3]]$ for any $r \in \mathbb{Z}$.

If $r \neq 0$, we write $\text{Sl}(ru) = r \text{Sl}(u) + \text{Sl}(u)^4f_r(\text{Sl}(u)^3)$, where $f_r(t) \in \mathbb{Z}\left[\frac{1}{3}\right] [t]$. Since $\left(1 + \frac{\text{Sl}(u)^3f_r(\text{Sl}(u)^3)}{r}\right)^{-1} = 1 + \sum_{n=1}^{\infty} \left(-\frac{\text{Sl}(u)^3f_r(\text{Sl}(u)^3)}{r}\right)^n \in 1 + \text{Sl}(u)^4\mathbb{Z}\left[\frac{1}{3}, \frac{1}{4}\right] [[\text{Sl}(u)^3]]$.

$$\text{Sl}(ru)^{-1} = \frac{1}{r \text{Sl}(u)} \left(1 + \frac{\text{Sl}(u)^3f_r(\text{Sl}(u)^3)}{r}\right)^{-1} \in \text{Sl}(u)^4\mathbb{Z}\left[\frac{1}{3}, \frac{1}{4}\right] [[\text{Sl}(u)^3]].$$

\[\square\]

**Lemma 1.7.** (An explicit power series expansion of the inverse of Sl) The function $\text{Sl} : [0, \varpi_1] \rightarrow [0, 1]$ is the inverse function of

$$\text{ArcSl} : \begin{array}{c c}
[0, 1] & \rightarrow & [0, \varpi_1] \\
\psi & \mapsto & \int_{0}^{\psi} \frac{dt}{\sqrt{1 - t^2}} \left( = \sum_{n=0}^{\infty} (-1)^n \left(\frac{-\frac{2}{3}}{n}\right) \tfrac{n+1}{3n+1} \right),
\end{array}$$

where we choose the branch of $\sqrt{\cdot}$ to be in $\mathbb{R}$.

**Proof.** Since $\frac{d}{d\psi}\text{ArcSl} = \frac{1}{\sqrt{1 - \psi^2}}$, ArcSl is monotone increasing. By the definitions of ArcSl and $\varpi_1$, $\text{ArcSl}(0) = 0$, $\text{ArcSl}(1) = \varpi_1$. Thus, the map $\text{ArcSl} : [0, 1] \rightarrow [0, \varpi_1]$ is bijective. On the other hand, the facts that

$$\text{Sl}(0) = 0, \quad \text{Sl}(\varpi_1) = \varphi\left(-\frac{1}{3}\right) = \frac{6\varphi\left(-\frac{\varpi_1}{3}\right)}{9 + \varphi'\left(-\frac{\varpi_1}{3}\right)} = 1$$

follow by Lemma 1.4 (3) and Lemma 1.2 (4) (5). By Lemma 1.4 (6), Sl is monotone increasing over $[0, \varpi_1]$. Thus, the map $\text{Sl} : [0, \varpi_1] \rightarrow [0, 1]$ is a bijection. Therefore, for $u_0 \in [0, \varpi_1]$, we write $t_0 := \text{Sl}(u_0)$, then

$$\text{ArcSl(\text{Sl}(u_0))} = \int_{0}^{t_0} \frac{dt}{\sqrt{1 - t^2}} = \int_{0}^{u_0} \frac{\text{Cl}(u)^2 du}{\sqrt{1 - \text{Sl}(u)^2}} = u_0,$$

where $t = \text{Sl}(u)$ and $dt = \text{Sl}'(u) du = \text{Cl}^2(u) du$, since Lemma 1.4 (10) and (17). Note that $\text{Sl}(u), \text{Cl}(u) \in \mathbb{R}$ for $u \in \mathbb{R}$ (Lemma 1.4 (5)). This means that the map $\text{Sl} : [0, \varpi_1] \rightarrow [0, 1]$ is the inverse function of the map $\text{ArcSl} : [0, 1] \rightarrow [0, \varpi_1]$.

From [Ko] Theorem 1.19 and $\text{Sl}'(0) = \text{Cl}^2(0) = 1 \neq 0$, we have $\text{Sl}(u)$ is bijective around $u = 0$ for $u \in \mathbb{C}$. Hence, by Lemma 1.2, the inverse function of $\text{Sl}(u)$ is the analytic continuation of the function $\text{ArcSl}(t)$ to a sufficiently small neighbourhood of $t = 0$, which is $\text{ArcSl}(t) = \sum_{n=0}^{\infty} (-1)^n \left(\frac{-\frac{2}{3}}{n}\right) \frac{\text{Sl}(u)^{n+1}}{3n+1}$. Thus, we have:

**Corollary 1.8.** $u = \sum_{n=0}^{\infty} (-1)^n \left(\frac{-\frac{2}{3}}{n}\right) \frac{\text{Sl}(u)^{n+1}}{3n+1}$.

Thus, we have $\mathbb{Q}[u] = \mathbb{Q}[\text{Sl}(u)]$. 

10
1.3 Bernoulli-Hurwitz-type numbers for the Eisenstein integers

In this section, we introduce Bernoulli-Hurwitz-type numbers for Eisenstein integers, and study their denominators for the proof of Theorem 2.3.

We denote the coefficients of the power series expansion of $\text{Sl}(u)$ around $u = 0$ as

$$\text{Sl}(u) = \sum_{m=0}^{\infty} C_{3m+1} u^{3m+1} = \sum_{m=0}^{\infty} c_{3m+1} \frac{u^{3m+1}}{(3m+1)!}. $$

(Note that, since $\text{Sl}(\rho u) = \rho \text{Sl}(u)$ by Lemma 1.4 (6) and (7), the coefficients of $u^n$ in $\text{Sl}(u)$ are zero unless $n$ is congruent 1 modulo 3.)

**Lemma 1.9.** (Integrality of $c_n$) We have $c_{3m+1} \in \mathbb{Z}$ for any $m \geq 0$.

*Proof.* We see that

$$\text{Sl}^{(3)} = 6 \text{Sl}^4 - 4 \text{Sl}$$

by Lemma 1.4 (6) and (7). Hence, by induction on $m$, we have $c_{3m+1} \in \mathbb{Z}$ for any $m \geq 0$. \qed

We denote the coefficients of the power series expansion of $\frac{1}{\text{Sl}(u)}$ around $u = 0$ as

$$\frac{1}{\text{Sl}(u)} = \frac{1}{u} + \sum_{n=0}^{\infty} D_{3n+2} u^{3n+2} = \frac{1}{u} + \sum_{n=0}^{\infty} \frac{d_{3n+2}}{(3n+2)!} u^{3n+2}. $$

(1.10)

We also put $D_{-1} := 1$, then we can express it as $\frac{1}{\text{Sl}(u)} = \sum_{n=0}^{\infty} D_{3n-1} u^{3n-1}$.

We call $C_{3m+1}$, $D_{3n+2}$ *Bernoulli-Hurwitz-type numbers* for the Eisenstein integers.

**Remark 1.10.** (Non-integrality of $d_n$) The function $f(u) = \frac{1}{\text{Sl}(u)}$ satisfies a differential equation $f^{(3)} = 4f - 6f^4$, hence $D_{3n+2} \in \mathbb{Q}$ for $m \geq 0$. We have $D_2 = \frac{1}{6}, D_5 = \frac{1}{360}, D_8 = -\frac{1}{4536}$. Therefore, $d_{3n+2} = (3n+2)! D_{3n+2}$ is not necessarily a rational integer. However, Lemma 1.12 below holds.

**Definition 1.11.** For a subring $R$ of $\mathbb{Q}$, we define

$$\mathcal{H}_R := \left\{ \sum_{n=0}^{\infty} \frac{a_n}{n!} t^n \in \mathbb{Q}[t] \mid a_n \in R \text{ for every } n \geq 0 \right\}. $$

It is easy to show that this is a subring of $\mathbb{Q}[t]$. We call $\mathcal{H}_R$’s elements *Hurwitz-R-integer series*.

Note that Lemma 1.9 says $\text{Sl}(u) \in \mathcal{H}_\mathbb{Z}$.

**Lemma 1.12.** (Integrality of $2d_{6m+2}$ outside 3) For $m \geq 0$, we have $2d_{6m+2} = 2(6m+2)! D_{6m+2} \in \mathbb{Z} \left[ \frac{1}{3} \right]$.

*Proof.* We write $f(u) := \frac{1}{\text{Sl}(u)} + \frac{1}{\text{Sl}(-u)}$. Then, $f(u) = 2 \sum_{n=0}^{\infty} D_{6m+2} u^{6m+2} = 2 \sum_{m=0}^{\infty} \frac{d_{6m+2}}{(6m+2)!} u^{6m+2}$ by (1.10).

On the other hand, by Lemma 1.6 we can write $\frac{1}{\text{Sl}(-u)} = -\frac{1}{\text{Sl}(u)} + g(\text{Sl}(u))$, where $g \in t^2 \mathbb{Z} \left[ \frac{1}{3} \right] [[t^3]]$ (t is a variable). Then, $f(u) = g(\text{Sl}(u))$. Here, by noting that $\text{Sl}(u) = \sum_{n=0}^{\infty} \frac{C_{3n+1}}{(3n+1)!} u^{3n+1} \in \mathcal{H}_2$ by Lemma 1.9 and that $\text{Sl}(u)$ does not have constant term as the expansion in terms of $u$, we have $f(u) \in \mathcal{H}_2[\frac{1}{3}]$.

Therefore, by comparing the coefficients, we have $2d_{6m+2} \in \mathbb{Z} \left[ \frac{1}{3} \right]$. \qed

**Remark 1.13.** (1) Moreover, we can show $d_{6m+2} \in \mathbb{Z} \left[ \frac{1}{3} \right]$. See Lemma A.5 (which is not used to show the main congruences in Theorem 2.3).

(2) For the denominators of $d_{6m-1}$, see Lemma A.7 (which is not used to show the main congruences in Theorem 2.3).
1.4 Eisenstein’s product formula

We recall that the arithmetic properties of $\mathbb{Z}[\rho]$ at division points.

**Definition 1.14.** (Primarity) For $a \in \mathbb{Z}[\rho]$, we call $a$ a primary if $a \equiv \pm 1 \mod 3$. This definition is slightly different from the ones in [L] §7.1 ($a \equiv \pm 1 \mod 3$) and [IR] §3 of Chap. 9 ($a \equiv -1 \mod 3$).

Note that, for a prime ideal $p$ ($3$), there uniquely exists a primary element $\mu$ such that $p = (\mu)$. Let $\ell$ be a rational prime number such that $\ell \equiv 1 \mod 3$ and fix $\lambda \in \mathbb{Z}[\rho]$ satisfying

$$\ell = \lambda \lambda'$$

and $\lambda \equiv 1 \mod 3$.

Note that there are precisely two choices of such $\lambda$, i.e., $\lambda$ and $\lambda'$. Then, there is a canonical isomorphism $\mathbb{Z}[\rho]/(\lambda) \simeq \mathbb{Z}/\ell \mathbb{Z}$. Let $\chi_{\lambda}$ be the cubic residue character to the modulus $\lambda$; the notation is fixed throughout this paper:

$$\chi_{\lambda}(\nu) := \left( \frac{\nu}{\lambda} \right)^3, \quad \chi_{\lambda}(\nu)^3 = 1, \quad \text{and} \quad \chi_{\lambda}(\nu) \equiv \nu^{(\ell-1)/3} \mod \lambda \quad (\nu \in (\mathbb{Z}[\rho]/(\lambda))^{\times}).$$

We write

$$\Lambda := \varphi \left( \frac{3}{\lambda} \right) = \text{Sl} \left( \frac{-3\varpi_1}{\lambda} \right).$$

Note that $\Lambda$ is algebraic and $[\mathbb{Q}(\rho, \Lambda) : \mathbb{Q}(\rho)] = \ell - 1$ (see [A] Lemma 1.3). Let $\mathcal{O}_{\Lambda}$ be the ring of integers of $\mathbb{Q}(\rho, \Lambda)$. We recall the properties of $\varphi (\frac{3}{\lambda})$'s from [A].

**Lemma 1.15.** (Arithmetic properties of $\varphi$ at division points) ([A] Lemma 1.3 of §1.1.2., Definition 1.11 of §1.3.2. with Remark, and Appendix of §1 3. (xi)) In the notation above, we have the following:

1. We have $\Lambda \in \mathcal{O}_{\Lambda}$. Moreover, $\Lambda$ is a prime element in $\mathcal{O}_{\Lambda}$ and has a property $(\Lambda) = (\Lambda)^{\ell - 1}$ as ideals of $\mathcal{O}_{\Lambda}$. For any $r \not\equiv 0 \mod \ell$, it holds that $(\varphi (\frac{3}{\lambda})) = (\Lambda)$ as ideals of $\mathcal{O}_{\Lambda}$.

2. (Eisenstein’s product formula) Let $\lambda := \prod_{\chi_{\lambda}(r) = 1} \varphi (\frac{3}{\lambda})$. Then $\lambda^3 = \Lambda$.

**Lemma 1.16.**

$$\lambda^2 \equiv \Lambda \frac{2\ell-1}{3} \mod \Lambda \frac{2\ell-1}{3} + 1.$$

**Proof.** By Lemma 1.16 for $r \in \mathbb{Z}$, we can write

$$\varphi \left( \frac{3}{\lambda} \right) = r\Lambda + \Lambda^3 f_r(\Lambda^3) = r\Lambda \left( 1 + \frac{1}{r} \Lambda^3 f_r(\Lambda^3) \right),$$

where $f_r(t) \in \mathbb{Z}[\frac{1}{3}][[t]]$, $(t$ is a variable). Let $g \in \mathbb{Z}$ be a primitive root of $1$ modulo $\ell$. Then, since $\ker(\chi_{\lambda}) = \{g^{3j} \mod \lambda : j = 1, \ldots, \frac{\ell-1}{3} \}$ (note that $(\mathbb{Z}[\rho]/(\lambda))^{\times} \simeq (\mathbb{Z}/\ell \mathbb{Z})^{\times}$), we have

$$\lambda = \left( \prod_{j=1}^{\frac{\ell-1}{3}} g^{3j} \right) \Lambda \frac{\ell-1}{3} \cdot \prod_{j=1}^{\frac{\ell-1}{3}} \left( 1 + \frac{1}{g^{3j}} \Lambda^3 f_r(\Lambda^3) \right). \quad (1.11)$$

Since $g^{3j}$ is relatively prime to $\ell$ for any $j = 1, \ldots, \frac{\ell-1}{3}$,

$$\prod_{j=1}^{\frac{\ell-1}{3}} \left( 1 + \frac{1}{g^{3j}} f_r(\Lambda^3) \right) \in 1 + t\mathbb{Z} \left[ \frac{1}{3} : \frac{1}{g^{3j}} : j = 1, \ldots, \frac{\ell-1}{3} \right] [[t]] \subseteq 1 + t\mathbb{Z}(t)[[t]],$$

hence,

$$\prod_{j=1}^{\frac{\ell-1}{3}} \left( 1 + \frac{1}{g^{3j}} \Lambda^3 f_r(\Lambda^3) \right) \in \mathcal{O}_{\lambda, \Lambda},$$
Lemma 2.2. \[(1) \quad \text{See } [A, Lemma 1.9]. \]

Proof. \[(1) \quad \text{We note that } \ell \text{ is odd because } \ell \text{ is odd prime. Thus, there exists } a \in \mathcal{O}_\lambda \text{ such that } \lambda = -\Lambda_{\ell+1}^2 + a\Lambda_{\ell+1}^2 = -\Lambda_{\ell+1}^2(1 - a\Lambda). \text{ We have} \]

\[
\overline{\lambda}^2 = \Lambda_{\frac{\ell-1}{2}}^2 (1 - a\Lambda)^2 \equiv \Lambda_{\frac{\ell-1}{2}}^2 (1 - \alpha\Lambda) \mod \Lambda_{\frac{\ell-1}{2}+1}.
\]

\[\Box\]

2 Elliptic Gauss sums

In this chapter, we introduce the elliptic Gauss sums and show the main congruences between the Bernoulli-Hurwitz-type numbers and the coefficients of the elliptic Gauss sums. In §2.1, we introduce the elliptic Gauss sums and their coefficients due to Asai. In §2.2, we show the main congruences and give some examples.

Let \(\ell, \lambda, \overline{\lambda}, \chi_\lambda\) and \(\Lambda\) be as in Chapter 1.

2.1 Elliptic Gauss sums and their coefficients

In this section, we introduce the elliptic Gauss sums and their coefficients.

We put

\[
f := \begin{cases} 
\varphi & \text{if } \ell \equiv 7 \mod 9, \\
\varphi^{-1} & \text{if } \ell \equiv 4 \mod 9.
\end{cases}
\]

In this paper, we do not treat the case where \(\ell \equiv 1 \mod 9\), since the Hecke \(L\)-value \(L(\overline{\lambda}, 1)\), which is described by an elliptic Gauss sum (cf. [A, Theorem 1.16]), can vanish (cf. [A, Remark of Corollary 1.22]) in the case where \(\ell \equiv 1 \mod 9\). Note that, in the cases where \(\ell \equiv 7, 4 \mod 9\), the Hecke \(L\)-value \(L(\overline{\lambda}, 1)\) does not vanish (cf. [A, Corollary 1.22]).

Definition 2.1. (Elliptic Gauss sum) [A] Definition 1.8 We define

\[
G_\lambda(\chi_\lambda, f) := \frac{1}{3} \sum_{r \in (\mathbb{Z}/(\lambda))^\times} \chi_\lambda(r) f \left( \frac{r}{\lambda} \right),
\]

and call \(G_\lambda(\chi_\lambda, f)\) the elliptic Gauss sum associated to \(\chi_\lambda\) and \(f\).

Lemma 2.2. (1) \(G_\lambda(\chi_\lambda, f) \in \mathcal{O}_\lambda\).

(2) \(G_\lambda(\chi_\lambda, f) = \sum_{r \in \ker(\chi_\lambda)} f \left( \frac{r}{\lambda} \right)\).

Proof. (1) See [A, Lemma 1.9].

(2) We have \((\mathbb{Z}/(\lambda))^\times = S \cup \rho S \cup \overline{\rho} S\) (disjoint union), where \(S := \ker(\chi_\lambda)\), if \(\ell \equiv 7, 4 \mod 9\). If \(\ell \equiv 7 \mod 9\) (resp. \(\ell \equiv 4 \mod 9\), then \(f = \varphi\) (resp. \(f = \varphi^{-1}\)), \(\varphi(pu) = \rho\varphi(u)\) (resp. \(\varphi(pu)^{-1} = \overline{\rho}\varphi(u)^{-1}\)) (by Lemma 1.4 [A]), and \(\chi_\lambda(\rho) = \rho\overline{\chi_\lambda} = \overline{\rho}\) (resp. \(\chi_\lambda(\rho) = \rho\overline{\chi_\lambda} = \overline{\rho}\)) (by the definition of \(\chi_\lambda\)). Hence, we have \(G_\lambda(\chi_\lambda, f) = \frac{1}{3} \sum_{r \in S} \left( f \left( \frac{r}{\lambda} \right) + \chi_\lambda(\rho) f \left( \frac{r}{\lambda} \right) + \chi_\lambda(\overline{\rho}) f \left( \frac{r}{\lambda} \right) \right) = \sum_{r \in S} f \left( \frac{r}{\lambda} \right)\). \[\Box\]

We shall recall Asai's results from §1 of [A]:

Theorem 2.3. (The descent of \(\chi_\lambda(3)^{-1} \alpha_\lambda\) or \(\overline{\chi_\lambda(3)^{-1}} \alpha_\lambda\) and the non-vanishing) [A] Definition 1.12 and Theorem 1.19

(1) If \(\ell \equiv 7 \mod 9\), then there exists \(\alpha_\lambda \in \chi_\lambda(3)(1 + 3\mathbb{Z})\) such that

\[
G_\lambda(\chi_\lambda, \varphi) = \alpha_\lambda \overline{\lambda}^2.
\]
(2) If $\ell \equiv 4 \mod 9$, then there exists $\alpha_\ell \in \mathbb{X}(3)(-1 + 3\mathbb{Z})$ such that

$$G_\ell(\chi_\ell, \varphi^{-1}) = \alpha_\ell \lambda^2.$$ 

In particular, $\alpha_\ell$ does not vanish in the cases of $\ell \equiv 7, 4 \mod 9$.

**Remark 2.4.** In $\ell \equiv 1 \mod 9$, it may happen $\alpha_\ell = 0$ (cf. [A] Remark of Corollary 1.22 of §1 and Table 1).

The number $\alpha_\ell$ is called the coefficient of elliptic Gauss sum in [A].

### 2.2 The main congruences

In this section, we show the main congruences and give some examples.

**Theorem 2.5.** (The congruences between the coefficients of elliptic Gauss sums and the Bernoulli-Hurwitz-type numbers) One has

$$\alpha_\ell = \begin{cases} \frac{-1}{3} C_{\frac{\ell-1}{2}} \pmod{\lambda} & \text{if } \ell \equiv 7 \mod 9, \\ \frac{-1}{3} D_{\frac{(\ell-1)}{2}} \pmod{\lambda} & \text{if } \ell \equiv 4 \mod 9. \end{cases}$$

**Proof.** Let $t := \text{Sl}(u)$. By Corollary [1.8] for any $\nu \in \mathbb{Z}[\rho]$, we have

$$\text{Sl}(\nu u) = \sum_{m=0}^{\infty} C_{3m+1}(\nu u)^{3m+1} = \sum_{m=0}^{\infty} C_{3m+1} \nu^{3m+1} \left( \sum_{n=0}^{\infty} (-1)^n \left(\frac{-2}{3} \right) \frac{t^{3n+1}}{3n+1} \right)^{3m+1}, \quad (2.2)$$

$$\frac{1}{\text{Sl}(\nu u)} + \frac{1}{\text{Sl}(-\nu u)} = 2 \sum_{m=0}^{\infty} D_{6m+2}(\nu u)^{6m+2} = 2 \sum_{m=0}^{\infty} D_{6m+2} \nu^{6m+2} \left( \sum_{n=0}^{\infty} (-1)^n \left(\frac{-2}{3} \right) \frac{t^{3n+1}}{3n+1} \right)^{6m+2}, \quad (2.3)$$

as elements of $\mathbb{Q}[\nu u] = \mathbb{Q}[t]$. The case $\ell \equiv 7 \mod 9$. Let $g \in \mathbb{Z}$ be a primitive root of 1 modulo $\ell$, i.e., $g \mod \ell$ generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$. We consider the sum

$$L_1(u) := \text{Sl}(g^7 u) + \text{Sl}(g^6 u) + \cdots + \text{Sl}(g^{\ell-1} u).$$

By Lemma [2.2] (2),

$$G_\ell(\chi_\ell, \varphi) = \sum_{j=1}^{\ell-1} \text{Sl} \left( \frac{-3\omega_1 g^{3j}}{\lambda} \right) = L_1 \left( \frac{-3\omega_1}{\lambda} \right).$$

By [2.2],

$$L_1(u) = \sum_{m=0}^{\infty} C_{3m+1} \left( \sum_{j=1}^{\ell-1} g^{3(3m+1)+j} \right) t^{3m+1} \left( \sum_{n=0}^{\infty} (-1)^n \left(\frac{-2}{3} \right) \frac{t^{3n}}{3n+1} \right)^{3m+1}.$$

Since Lemma [1.9] and the definition of $L_1$, the coefficients of this expansion in terms of $t$ are $\in \mathbb{Z} \left[ \frac{1}{\lambda} \right]$, especially $\in \mathbb{Z}(\ell)$. Here, we substitute $\Lambda$ for $t$ (which corresponds to the substitution of $\frac{-3\omega_1}{\lambda}$ for $u$), then, $\text{Sl}(\nu u) \mapsto \text{Sl} \left( \frac{-3\omega_1 \nu}{\lambda} \right)$ for any $\nu \in \mathbb{Z}$, since Lemma [1.9]. Therefore,

$$\sum_{m=0}^{\infty} C_{3m+1} \left( \sum_{j=1}^{\ell-1} g^{3(3m+1)+j} \right) \Lambda^{3m+1} \left( \sum_{n=0}^{\infty} (-1)^n \left(\frac{-2}{3} \right) \frac{\Lambda^{3n}}{3n+1} \right)^{3m+1}$$

converges $\Lambda$-adically in $\mathcal{O}_{\lambda, \Lambda}$ and is equal to $G_\ell(\chi_\ell, \varphi)$. By noting that $(-1)^n \left(\frac{-2}{3} \right) \frac{1}{3n+1} \in \mathbb{Z}(\ell)$ for $n \leq \frac{2\ell-5}{9}$ (since $C_{3m+1} \leq \frac{c_{3m+1}}{(3m+1)!}$),

$$\left(\frac{-2}{3} \right) \in \mathbb{Z} \left[ \frac{1}{\lambda} \right] \text{ and } 3n+1 \leq \frac{2\ell-2}{3} < \ell$$

and $C_{3m+1} \in \mathbb{Z}(\ell)$ for $m \leq \frac{2\ell-5}{9}$ (since $C_{3m+1} \leq \frac{c_{3m+1}}{(3m+1)!}$),
Let Lemma 2.2 (2), we have \( L \). Since Lemma 1.6 and the definition of \( \ell \), we have \( 3 \mod 9 \). Since \( \ell \mod 3(3m + 1) \) if and only if \( 3(3m + 1) = 2(\ell - 1) \). Then, we have
\[
G_\lambda(\chi, \varphi) = \alpha_\lambda \Lambda^{2(\ell-1)} \mod \Lambda^{2(\ell-1)+1}.
\]

On the other hand, by Theorem 2.3 (1) and Lemma 1.16, we have
\[
G_\lambda(\chi, \varphi) = \alpha_\lambda \Lambda^{2(\ell-1)} \mod \Lambda^{2(\ell-1)+1}.
\]

Therefore,
\[
\alpha_\lambda \equiv -\frac{1}{3} C_{2(\ell-1)} \mod \Lambda
\]
holds. Since \( \alpha_\lambda \in \chi(3)(1 + 3Z) \subset Z[\rho] \), and \( C_{2(\ell-1)} = \frac{1}{3} C_{2(\ell-1)/(2(\ell-1))}! \in Z(\ell) \) by Theorem 2.3 (1) and Lemma 1.10, we have \( \alpha_\lambda \equiv -\frac{1}{3} C_{2(\ell-1)} \mod \Lambda \).

The case \( \ell \equiv 4 \mod 9 \). Let \( g \in Z \) be a primitive root of 1 modulo \( \ell \). We consider the sum
\[
L_2(u) := \text{Sl}(g^3u)^{-1} + \text{Sl}(g^6u)^{-1} + \cdots + \text{Sl}(g^{\frac{\ell-1}{6}}u)^{-1} + \text{Sl}(-g^3u)^{-1} + \text{Sl}(-g^6u)^{-1} + \cdots + \text{Sl}(-g^{\frac{\ell-1}{6}}u)^{-1}.
\]

By noting that \( g^{\frac{\ell-1}{6}} \equiv -1 \mod \ell \), we have \( \ker(\chi_\lambda) = \{ g^{3j}, -g^{3j} \mod \ell \mid j = 1, \ldots, \frac{\ell-1}{6} \} \). By this fact and Lemma 2.2 (2), we have
\[
G_\lambda(\chi, \varphi^{-1}) = \sum_{j=1}^{\frac{\ell-1}{6}} \left( \text{Sl} \left( \frac{-3\zeta_1 g^{3j}}{\Lambda} \right)^{-1} + \text{Sl} \left( \frac{3\zeta_1 g^{3j}}{\Lambda} \right)^{-1} \right) = L_2 \left( \frac{-3\zeta_1}{\Lambda} \right).
\]

By 2.3,
\[
L_2(u) = 2 \sum_{m=0}^{\infty} D_{6m+2} \left( \sum_{j=1}^{\frac{\ell-1}{6}} g^{3(6m+2)j} \right) t^{6m+2} \left( \sum_{n=0}^{\infty} (-1)^n \frac{-2}{3} \frac{\Lambda^{3n}}{3n+1} \right) \phi(\Lambda^{3m+1}) \cdot \Lambda^{6m+2} \phi(\Lambda^{3m+1})
\]
converges \( \Lambda \)-adically in \( G_{\lambda, \Lambda} \) and is equal to \( G_\lambda(\chi, \varphi^{-1}) \). By noting that \( (-1)^n \left( \frac{-2}{3} \right)^{3n+1} \in Z(\ell) \) for \( n \leq \frac{2(\ell-1)}{9} \) (since \( \left( \frac{-2}{3} \right) \in Z \left( \frac{1}{9} \right) \) and \( 3n + 1 \leq \frac{2(\ell-1)}{9} \leq \ell \)) and \( D_{6m+2} \in Z(\ell) \) for \( m \leq \frac{\ell-1}{9} \) (since \( D_{6m+2} = \frac{4(6m+2)!}{(6m+2)!} \)).
6m + 2 < ℓ, and \(d_{6m+2} \in \mathbb{Z}_\ell\) (Lemma 1.12), and that the coefficients of this expansion in terms of \(\Lambda\) are \(\in \mathbb{Z}\left[\frac{1}{3}\right]\), we have

\[
G_\Lambda(\chi_\lambda, \varphi^{-1}) = 2 \sum_{m=0}^{\frac{\ell-4}{6}} \sum_{j=1}^{\frac{\ell-1}{6}} g^{3(6m+2)j} \Lambda^{6m+2} \sum_{n=0}^{\frac{2(\ell-4)}{3}} (-\frac{2}{n}) \Lambda^{3n+1} \mod \Lambda^{\frac{2(\ell-1)}{3}+1}.
\]

We also have

\[
\sum_{j=1}^{\frac{\ell-1}{6}} g^{3(6m+2)j} = \begin{cases} 0 & \text{mod } \ell \text{ if } \ell - 1 \not\equiv 3(6m + 2), \\ \ell - 1 & \text{mod } \ell \text{ if } \ell - 1 \equiv 3(6m + 2). \end{cases}
\]

Since \(0 \leq m \leq \frac{\ell-4}{6}\) and \(\ell \equiv 4 \mod 9\), we see that \(\ell - 1 \equiv 3(6m + 2)\) if and only if \(3(6m + 2) = 2(\ell - 1)\). Then, we have

\[
G_\Lambda(\chi_\lambda, \varphi^{-1}) = 2D_{2(\ell-1)} \cdot \frac{\ell - 1}{6} \cdot \Lambda^{\frac{2(\ell-1)}{3}} = -\frac{1}{3}D_{2(\ell-1)} \Lambda^{\frac{2(\ell-1)}{3}} \mod \Lambda^{\frac{2(\ell-1)}{3}+1}.
\]

On the other hand, by Theorem 2.3 (2) and Lemma 1.16, we have

\[
G_\Lambda(\chi_\lambda, \varphi^{-1}) = \alpha_\lambda \Lambda^2 \equiv \alpha_\lambda \Lambda^{\frac{2(\ell-1)}{3}} \mod \Lambda^{\frac{2(\ell-1)}{3}+1}.
\]

Therefore,

\[
\alpha_\lambda \equiv -\frac{1}{3}D_{2(\ell-1)} \mod \Lambda
\]

holds.

Since \(\alpha_\lambda \in \mathbb{Z}(3)(-1 + 3\mathbb{Z}) \subset \mathbb{Z}[\rho]\), and \(D_{2(\ell-1)} = d_{2(\ell-1)}/(2(\ell-1))! \in \mathbb{Z}_\ell\) by Theorem 2.3 (2) and Lemma 1.12, we have \(\alpha_\lambda \equiv -\frac{1}{3}D_{2(\ell-1)} \mod \lambda\).

**Example 2.6.** (1) Let \(\ell = 7\) and \(\lambda = 1 + 3\rho,\) By Table 1 we have \(C_4 = -\frac{1}{5}\). Then,

\[
-\frac{1}{3}C_{2(\ell-1)} = -\frac{1}{3}C_4 = \frac{1}{18} \equiv 2 \mod 7.
\]

By noting that \(\mathbb{Z}[\rho]/(\lambda) \simeq \mathbb{Z}/\ell\mathbb{Z} : \rho \mapsto 2\), this coincides with the value \(\alpha_\lambda = 1 \cdot \rho \) in the table at [A] Table 1. in p.117.

(2) \(\ell = 13\) and \(\lambda = 4 + 3\rho\). By Table 2 \(D_8 = -\frac{1}{4356} \equiv 1 \mod 13\). Then,

\[
-\frac{1}{3}D_{2(\ell-1)} = -\frac{1}{3}D_8 \equiv -\frac{1}{3} \equiv -3^2 \mod 13.
\]

By noting that \(\mathbb{Z}[\rho]/(\lambda) \simeq \mathbb{Z}/\ell\mathbb{Z} : \rho \mapsto 3\), this coincides with the value \(\alpha_\lambda = -1 \cdot \rho\) in the table at [A] Table 1. in p.117.

**Lemma 2.7.** (The congruences between the square of the absolute value of the coefficients of the elliptic Gauss sums and the Bernoulli-Hurwitz-type numbers) We have

\[
|\alpha_\lambda|^2 \equiv \begin{cases} \chi_\lambda(3)C_{2(\ell-1)}^2 / 9 & \text{if } \ell \equiv 7 \mod 9, \\ \chi_\lambda(3)D_{2(\ell-1)}^2 / 9 & \text{if } \ell \equiv 4 \mod 9. \end{cases}
\]

We also have

\[
|\alpha_\lambda|^2 \equiv \begin{cases} \left(3\ell^{\ell-7}C_{2(\ell-1)}^2 / 9 & \text{if } \ell \equiv 7 \mod 9, \\ \left(3\ell^{\ell-4}D_{2(\ell-1)}^2 / 9 & \text{if } \ell \equiv 4 \mod 9. \end{cases}
\]
Proof. Let $\ell \equiv 7 \mod 9$. We have $\alpha_\lambda^2 \equiv \left( C_{2(\ell-1)} \right)^2 / 9 \mod \lambda$ by Theorem 2.3. We can take $a_\lambda \in 1 + 3\mathbb{Z}$ as $\alpha_\lambda = \chi_\lambda(3)a_\lambda$ by Theorem 2.3. Then, $\alpha_\lambda^2 = \chi_\lambda(3)a_\lambda^2$, and $|\alpha_\lambda|^2 = a_\lambda^2$ hold. Therefore, we have

$$|\alpha_\lambda|^2 = a_\lambda^2 = \chi_\lambda(3)a_\lambda^2 = \left( \chi_\lambda(3)C_{2(\ell-1)} \right)^2 / 9 \mod \lambda.$$ 

Since $\chi_\lambda(3)^2 = \chi_\lambda(3) \equiv 3 \sqrt{3} = 9 \cdot \left( 3 \sqrt{3} \right)^2 \mod \lambda$ and $|\alpha_\lambda|^2, \left( 3 \sqrt{3} \right)^2 C_{2(\ell-1)}^2 \in \mathbb{Q}$, the second congruence in the case where $\ell \equiv 7 \mod 9$ is proved.

The case where $\ell \equiv 4 \mod 9$ is proved similarly to the case where $\ell \equiv 7 \mod 9$. \hfill \qed

Remark 2.8. It seems that the statement of [O, Corollary 2.16], which is the counterpart of Lemma 2.7 for Gaussian integers case, is a typo of

$$|\alpha_\lambda|^2 \equiv \begin{cases} \left( \frac{\sqrt{3} C_{3(\ell-1)}}{\ell} \right)^2 & \ell \equiv 13 \mod 16, \\ - \left( \frac{\sqrt{3} D_{3(\ell-1)}}{\ell} \right)^2 & \ell \equiv 5 \mod 16. \end{cases}$$

3 Elliptic Gauss sums and associated elliptic curves

In this chapter, we study certain Hecke characters, Hecke $L$-series associated to them, certain elliptic curves $E_\lambda$ for $\lambda$, and their $L$-functions relevant to our elliptic Gauss sums.

In §3.1, we define appropriate Hecke characters and the Hecke $L$-series associated to them. In §3.2, we introduce certain elliptic curves $E_\lambda$ for $\lambda$ and show that their $L$-functions correspond to the Hecke $L$-series defined in §3.1. In §3.3, by using the coefficient of the elliptic Gauss sum, we show that the order of the Tate-Shafarevich group of $E_\lambda / \mathbb{Q}(\rho)$ is congruent to the Bernoulli-Hurwitz-type number modulo $\ell$ under the BSD conjecture on the 2,3-parts of the leading term. We also obtain unconditional results.

Let $\ell, \lambda, \lambda, \chi_\lambda, W$, and $W'$ be as in Chapter 1.

3.1 Hecke $L$-series

In this section, we introduce appropriate Hecke characters and the Hecke $L$-series associated to them.

We define, due to [A] §1.4.1,

$$\chi_\lambda((\nu)) := \chi_1((\nu)\mathfrak{m}), \quad \chi_1 := \begin{cases} \chi_\lambda \cdot \chi_0 & \text{for } \ell = \lambda \overline{\lambda} \equiv 7 \mod 9, \\ \chi_\lambda \cdot \chi_0' & \text{for } \ell = \lambda \overline{\lambda} \equiv 4 \mod 9, \end{cases}$$

where $\chi_0 : (\mathbb{Z}[\rho]/(3)) \xrightarrow{\sim} W$ and $\chi_0' : (\mathbb{Z}[\rho]/(\sqrt{3} \mathbb{Z})) \xrightarrow{\sim} \{ \pm 1 \}$ are natural isomorphisms. Note that $\chi_\lambda((\nu))$ is independent of choice of the generator $\nu$ of the ideal $(\nu)$. Hecke $L$-series associated to the Hecke character $\chi_\lambda$ is

$$L(s, \chi_\lambda) = \prod_{(\mu) \text{ prime ideal}} (1 - \chi_\lambda((\mu)(\mu\mathfrak{m})^{-s})^{-1} = \prod_{\mu \text{ prime, } \mu \equiv 1 \mod 3 \text{ or } \mu = 1 - \rho} (1 - \chi_\lambda((\mu)(\mu\mathfrak{m})^{-s})^{-1}$$

$$= \prod_{\mu \text{ primary prime}} (1 - \chi_\lambda((\mu)(\mu\mathfrak{m})^{-s})^{-1}$$

(3.1)

for $\ell \equiv 7, 4 \mod 9$, since $\chi_\lambda(\lambda) = 0, \chi_0(1 - \rho) = \chi_0'(1 - \rho) = 0$.

3.2 $L$-functions of elliptic curves

In this section, we introduce certain elliptic curves for $\lambda$, and show the properties of them such as their reduction types at prime ideals of $\mathbb{Z}[\rho]$, the numbers of the points of the reductions of the elliptic curves. We
also show that the Hecke $L$-series defined in §3.1 correspond to the $L$-functions of the elliptic curves defined in this section.

First, we recall the properties of Jacobi sums and the cubic reciprocity law which will be used to count points of elliptic curve over a finite field.

**Lemma 3.1.** (1) (Jacobi sums over $\mathbb{F}_p$) For any primary prime $\mu \in \mathbb{Z}[\rho]$ such that $p = \mu \equiv 1 \mod 3$ is a rational prime number, and any characters $\phi, \chi$ of $\mathbb{F}_p^\times$, we define the Jacobi sum associated to $\phi, \chi$ to be

$$J(\phi, \chi) := \sum_{t \in \mathbb{F}_p} \phi(t)\chi(1-t).$$

If $\phi$ is the quadratic residue character, $\chi$ is the cubic residue character, then

$$J(\phi, \chi) = \chi(4)J(\chi, \chi) = -\chi(4)\mu$$

holds.

(2) (Jacobi sums over $\mathbb{F}_{q^2}$) For any primary prime $-q \in \mathbb{Z}[\rho]$ such that $q$ is a rational prime number (automatically satisfying $q \equiv 2 \mod 3$), and any characters $\phi, \chi$ of $\mathbb{F}_{q^2}^\times$, we define

$$J_2(\phi, \chi) := \sum_{t \in \mathbb{F}_{q^2}} \phi(t)\chi(1-t).$$

If $\phi$ has order 2 and $\chi$ has order 3, then

$$J_2(\phi, \chi) = q$$

holds.

(3) (Cubic Reciprocity Law) If $\lambda_1, \lambda_2$ are primary primes in $\mathbb{Z}[\rho]$, then

$$\left( \frac{\lambda_1}{\lambda_2} \right)_3 = \left( \frac{\lambda_2}{\lambda_1} \right)_3.$$  

**Proof.** (1) The first equality follows from [IR] Lemma in §3 of Chap. 18 and the second equality follows from [IR] Lemma 1 in §4 of Chap. 9. (Note that $-\mu$ is primary in the definition of [IR] §3 of Chap. 9.)

(2) See Theorem 2.3 and Theorem 2.14 in [BE].

(3) See [L, Theorem 7.8]. (Note that, the primarity in Definition 1.14 implies the primarity in [L, §7.1].)

Let

$$\mathcal{E}_\lambda : y^2 = x^3 + \frac{\lambda^2}{4}$$

be an elliptic curve over $\mathbb{Q}(\rho)$, which is a twist of the elliptic curve $y^2 = 4x^3 - 27$. This has an automorphism $(x, y) \mapsto (\rho x, -y)$, and we see that

$$\text{End}(\mathcal{E}_\lambda) \simeq \mathbb{Z}[\rho].$$

**Lemma 3.2.** For any prime ideal $\mathfrak{p} \subset \mathbb{Z}[\rho]$, let $R_\mathfrak{p}$ be the completion of $\mathbb{Z}[\rho]$ by $\mathfrak{p}$, $K_\mathfrak{p}$ the fraction field of $R_\mathfrak{p}$, and $k_\mathfrak{p} (= \mathbb{Z}[\rho]/\mathfrak{p})$ the residue field of $K_\mathfrak{p}$.

(1) (Reductions) The elliptic curve $\mathcal{E}_\lambda$ has bad reductions only at $(\lambda), (1 - \rho)$, moreover, $\mathcal{E}_\lambda$ has additive reductions at $(\lambda), (1 - \rho)$.

(2) (Special Fibers) The special fiber of $\mathcal{E}_\lambda$ at $(\lambda)$ is of Type IV, and the one at $(1 - \rho)$ is of Type IV if $\ell \equiv 7 \mod 9$, of Type $I^*_9$ if $\ell \equiv 4 \mod 9$, in the notation of Kodaira symbols in the Kodaira-Néron classification of the special fibers of Néron models.
(3) (Local Tamagawa Numbers) For any prime ideal $\mathfrak{P} \subset \mathbb{Z}[\rho]$, let $\mathcal{E}/R_{\mathfrak{P}}$ be the Néron model of $\mathcal{E}_\mathfrak{P} \times_{\mathbb{Q}(\rho)} K_{\mathfrak{P}}$, $\mathcal{E}/k_{\mathfrak{P}} = \mathcal{E} \times_{R_{\mathfrak{P}}} k_{\mathfrak{P}}$ the special fiber of $\mathcal{E}$, $\mathcal{E}_0/k_{\mathfrak{P}}$ the identity component of the group variety $\mathcal{E}/k_{\mathfrak{P}}$, and $\tau_{\mathfrak{P}}$ the order of the group of components $\mathcal{E}_0(k_{\mathfrak{P}})/\mathcal{E}_0(k_{\mathfrak{P}})$. Then, we have

$$\tau(\lambda) = 3, \quad \tau(1-\rho) = \begin{cases} 4 & \text{if } n \equiv 0 \mod 3, \\ 1 & \text{if otherwise}, \end{cases}$$

where $\lambda = 3m + 1 + 3n\rho, m, n \in \mathbb{Z}$.

(4) (Point Counting at Good Ordinary Reductions) For a prime number $p \in \mathbb{Z}[\rho]$ such that $p = \mu\mathfrak{P}$ is a rational prime number and $\mu \neq \lambda$, we have

$$\#(\mathcal{E}_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = p + 1 - (\chi\lambda(\mu)\mathfrak{P} + \overline{\chi\lambda(\mu)/\mu}),$$

where $\mathcal{E}_\lambda \otimes \mathbb{F}_p$ is the special fiber of the minimal Weierstrass model of $\mathcal{E}_\lambda$ over $R(\mu)$.

(5) (Point Counting at Good Supersingular Reductions) For a rational prime number $q \equiv 2 \mod 3$, we have

$$\#(\mathcal{E}_\lambda \otimes \mathbb{F}_{q^2})(\mathbb{F}_{q^2}) = q^2 + 1 + q(\chi\lambda(q) + \overline{\chi\lambda(q)}),$$

where $\mathcal{E}_\lambda \otimes \mathbb{F}_{q^2}$ is the minimal Weierstrass model of $\mathcal{E}_\lambda$ over $R(-q)$.

(6) (Global Rational Torsion Points)

$$\mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}} = \mathcal{E}_\lambda(\mathbb{Q}(\rho))[3] = \{ \infty, (0, \frac{\lambda}{2}) \},$$

thus $\#\mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}} = 3$. Here, $\mathcal{E}_\lambda(\mathbb{Q}(\rho))[m], \mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}}$ are the $m$-torsion subgroup and the torsion subgroup of $\mathcal{E}_\lambda(\mathbb{Q}(\rho))$, respectively.

**Remark 3.3.** On [6], we can show, moreover, $\mathcal{E}_\lambda(\mathbb{Q}(\rho)) = \mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}}$ as follows: As we will see later, the $L$-function of $\mathcal{E}_\lambda$ does not vanish at $s = 1$. This fact follows from Lemma 3.2 which is proved without Lemma 3.2 [6]. From [CW Theorem 1], the rank of $\mathcal{E}_\lambda(\mathbb{Q}(\rho))$ is zero. Thus, $\mathcal{E}_\lambda(\mathbb{Q}(\rho)) = \mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}}$.

**Proof.** The substitution $y \mapsto y + \frac{\lambda}{2}$ to $y^2 = x^3 + \frac{\lambda^2}{4}$ gives an equation of the form

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

This equation has the discriminant $\Delta = -27\lambda^4$ and $c_4 = 0$, where $c_4$ is the one defined in [51 Chap. III. 1]. Thus $(\Delta) = (1 - \rho)^6(\lambda)^4$ as ideals in $\mathbb{Z}[\rho]$. This is a global minimal Weierstrass equation of $\mathcal{E}_\lambda(\mathbb{Q}(\rho))$, since [51 Chap. VII, Remark 1.1]. (Note that Weierstrass equation $y^2 = x^3 + \lambda^2$ is minimal at every prime except (2).) Hence, $\mathcal{E}_\lambda$ has only two bad primes $(\lambda), (1 - \rho)$, and it has additive reductions at these primes, since [51 Chap. VII, Proposition 5.1(c)] (The fact that $\mathcal{E}_\lambda$ has additive reductions at $(\lambda), (1 - \rho)$ can be deduced in the following way as well: Since $\mathcal{E}_\lambda$ has complex multiplication, the $j$-invariant of $\mathcal{E}_\lambda$ is integral by [52 Chap. II, Theorem 6.1]. Since [51 Chap. VII, Proposition 5.5], $\mathcal{E}_\lambda$ has potential good reduction at every primes. By [51 Chap. VII, Proposition 5.4 (b)], $\mathcal{E}_\lambda$ does not have multiplicative reductions.).

**Step 1-3** In the following, we use the symbols (e.g., $a_1, b_2, a_{3,1}$ etc.) and the terminology (e.g., Step1 etc.) of [52 Chap. IV, Tate’s Algorithm 9.4]. Note that $a_1 = 0$, $a_3 = \lambda$, $a_4 = a_6 = 0$, $b_2 = b_4 = 0$, $b_5 = \lambda^2, b_8 = 0$. First, we determine the reduction type at $(\lambda)$ and $\tau(\lambda)$. Note that $k(\lambda) \simeq \mathbb{F}_\ell$, and choose $\lambda$ as a uniformizer.

**Step1:** Since $\lambda | \Delta$, go to Step2.

**Step2:** Since $\lambda | a_3, a_4, a_6$ and $b_2$, go to Step3.

**Step3:** Since $\lambda^2 | a_6$, go to Step4.

**Step4:** Since $\lambda^3 | b_8$, go to Step5.

**Step5:** Since $\lambda^3 \not| b_4 = \lambda^2$, $\mathcal{E}_\lambda$ is of Type IV at $(\lambda)$. Let $k'$ be the splitting field over $k(\lambda)$ of $T^2 + a_{3,1} T - a_{6,2} = T^2 + T = 0$. Then, $k' = k(\lambda)$, Thus, we have $\tau(\lambda) = c = 3$.

Next, we determine the reduction type at $(1 - \rho)$ and $\tau(1 - \rho)$. Note that $k(1 - \rho) \simeq \mathbb{F}_3$, and choose $1 - \rho$ as a uniformizer.
We will show that $\chi(1) = 0$, since $\lambda \equiv 1 \mod 3$, especially $\lambda \equiv 1 \mod (1 - \rho)$. Here, $(x, y) = (0, 1)$ is the singular point. To make a change of variables to move the singular point to $(0, 0)$, we substitute $(x, y) \mapsto (x - 1, y + \lambda)$. Then, $\delta_\lambda : y^2 + 3\lambda y = x^3 - 3x^2 + 3x - 1 - 2\lambda^2$. The new $a_i$'s and $b_i$'s are:
\[a_1 = 0, a_3 = 3\lambda, a_2 = -3, a_4 = 3, a_6 = -1 - 2\lambda^2,\]
\[b_2 = -12, b_4 = 6, b_6 = \lambda^2 - 4, b_8 = -3(\lambda^2 - 1).\]
Thus, $(1 - \rho)(a_1, a_4, a_6)$ and $b_2$, go to Step3.

Step3: Since $a_9 = -1 - 2\lambda^2 \equiv -1 - 2 \equiv 0 \mod 3$, $(3) = (1 - \rho)^2 | a_9$, go to Step4.

Step4: Since $\lambda^2 - 1 \equiv 0 \mod 3$, $(3)^2 | b_9$. Especially $(1 - \rho)^3 | b_8$, go to Step5.

Step5: We write $\lambda = a + bp, a, b \in \mathbb{Z}$. Since $\lambda$ is primary, we can write $a = 3m + 1, b = 3n, m, n \in \mathbb{Z}$. Then, $\lambda + 2 = 3(m + 1) + 3n = 3(m + 1 + n)\rho$, and $\ell = \lambda = a^2 - ab + b^2 = (3m + 1)^2 - (3m + 1)3 + 9n = 6m + 1 - 3n \mod 9$. We note that, for $\alpha, \beta \in \mathbb{Z}[\rho]$,
\[(1 - \rho)(\alpha + \beta) \iff \alpha + \beta \equiv 0 \mod 3.\]
Note also that $a_6 = -1 - 2\lambda^2 = -1 - 2(3m + 1 + 3n)\rho \equiv -3(1 + m + n) \mod 9.\]

We assume that $\ell \equiv 7 \mod 9$. We will show that $(1 - \rho)^3 \not| b_9$. That $b_9 = (\lambda + 2)(\lambda - 2)$. Since $\lambda - 2 \equiv -1 \mod 3, (1 - \rho) \not| \lambda - 2$. Thus, it suffices to show that $(1 - \rho)^3 \not| \lambda + 2$. Therefore, it suffices to show that $(1 - \rho) \not| \ell + 1 + 1 \mod 9$. Now, $7 \equiv \ell \equiv 6m + 1 - 3n \mod 9$, thus, $-3 \equiv -3(m + n) \mod 9$. Hence, we have $1 \equiv m + n \mod 3$. Since $m + n + 1 \equiv 2 \mod 3 \text{ and } (3.2)$, we have $(1 - \rho) \not| m + 1 + n$. Therefore, we proved $(1 - \rho)^3 \not| b_9$. Thus, $\delta_\lambda$ is of Type IV at $(1 - \rho)$. We have $a_{6,2} = \frac{a_9}{(1 - \rho)^2} = \frac{1}{\mathbb{F}(1 + m + n) \equiv 1 + m + n \equiv -1 \mod (1 - \rho)}$ (note that $(1 - \rho)^2 = 3\rho$). Let $k'$ be the splitting field over $k_{1(\rho)- \rho}$ of $T^2 + 3a_1 T - a_{6,2} = T^2 + 1 \in k_{1(\rho)}[T]$. Then, $k' \neq k_{1(\rho)}$. Thus, we have $\tau_{1(\rho)} = c = 1$.

We assume that $\ell \equiv 4 \mod 9$. Then, $4 \equiv \ell \equiv 6m + 1 - 3n \mod 9$, we have $m + n \equiv -1 \mod 3$. Thus, $(1 - \rho)(m + 1 + n) \equiv \mathbb{F}(3.2)$. Hence, $\ell \equiv 3(m + 1 + n) \equiv \lambda + 2$. Since $(1 - \rho)^3 | (\lambda ^2 + 2) = b_6$, go to Step6.

Step6: Already, $(1 - \rho)|a_1, a_2, (1 - \rho)^2|a_3, a_4$; and $(1 - \rho)^3|a_6$ are satisfied. Since $a_{6,3} = \frac{a_9}{(1 - \rho)^2} = \frac{1 + m + n}{\rho(1 - \rho)} = \rho^2 + m + n = \rho^2 n = \rho n \equiv -n \mod 1 - \rho$. We consider $P(T) = T^3 + a_{2,1} T^2 + a_{4,2} T + a_{6,3} = T^3 - T - n \in k_{1(\rho)}[T]$.

Since $P'(T) = -1$, the polynomial $P(T)$ has distinct roots in an algebraic closure of $k_{1(\rho)}$. Thus, $\delta_\lambda$ is of Type $I_0^3$ at $(1 - \rho)$. We have
\[\tau_{1(\rho)} = c = 1 + \#\{\alpha \in k_{1(\rho)} \mid P(\alpha) = 0\} = \begin{cases} 4 & \text{if } n \equiv 0 \mod 3, \\ 1 & \text{if otherwise}, \end{cases}\]

since $t^3 - t = 0$ for any $t \in k_{1(\rho)} \simeq \mathbb{F}_3$.

(y^2 = x^3 + \frac{a_7}{4}$ is the minimal Weierstrass equation at the prime ideal $(\mu)$. Let $\phi : \mathbb{F}_3^\times \rightarrow \{\pm 1\}$ be the quadratic residue symbol, and $\chi : \mathbb{F}_3^\times \rightarrow W'$ be the cubic residue symbol. Let $D_1 \in \mathbb{F}_p$ be the image of $\lambda^2$ in $\mathbb{Z}[\rho]/(\mu) \simeq \mathbb{F}_p$. Note that $D_1 \neq 0, (\phi(D_1)) = 1, \chi(-1) = 1$. Then, we have
\[\#(\delta_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = 1 + \#\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + D_1\} = 1 + \sum_{u+v=D_1} \#\{y \in \mathbb{F}_p \mid y^2 = u\} \cdot \#\{x \in \mathbb{F}_p \mid x^3 = -v\} \]
\[= 1 + \sum_{u+v=D_1} (1 + \phi(u))(1 + \chi(-v) + \chi(-v)) = p + 1 + \sum_{u+v=D_1} \phi(u)(\chi(-v) + \chi(-v)) \]
\[= p + 1 + \phi(D_1) \chi(D_1) \sum_{u+v=D_1} \phi(u) \chi(v) + \phi(D_1) \chi(D_1) \sum_{u+v=D_1} \phi(u) \chi(v) \]
\[= p + 1 + \chi(D_1) \lambda(D_1) \sum_{u+v=D_1} \phi(u) \chi(v) \]
By Lemma 33.1 [4], we have $\#(\delta_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = p + 1 - (\chi(D_1) \lambda(4) \mu) + \chi(D_1) \lambda(4) \mu)$. By noting that $\left(\frac{\mu}{3}\right) = \chi(\lambda(\mu))$ and $\left(\frac{\mu}{3}\right) = \chi(\lambda(\mu))$ (Lemma 33.1 [3]), we have $\chi(4D_1) = \left(\frac{\mu}{3}\right) = \left(\frac{\mu}{3}\right) = \chi(\lambda(\mu))$. Thus, $\#(\delta_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = p + 1 - (\chi(\lambda(\mu)) - \chi(\lambda(\mu)))$ holds.
For \( q \neq 2 \), \( y^2 = x^3 + \frac{a^2}{x^2} \) is the minimal Weierstrass equation at the prime ideal \((-q)\). Let \( \phi : F_q^2 \rightarrow \{ \pm 1 \} \) be the quadratic residue symbol, and \( \chi : F_q^\times \rightarrow W^l \) be the cubic residue symbol. Let \( D_2 \in F_q^2 \) be the image of \( \frac{4}{x^2} \) in \( \mathbb{Z}[\rho]/(-q) \cong F_{q^2} \). Note that \( D_2 \neq 0 \), \( \phi(D_2) = 1 \), \( \chi(-1) = 1 \). Then, we have
\[
\#(\mathcal{E}_\chi \otimes F_q^2)(F_{q^2}) = 1 + \#\{(x, y) \in F_{q^2} \times F_{q^2} \mid y^2 = x^3 + D_2\} = 1 + \sum_{u, v \in F_{q^2}} \sum_{u + v = D_2} \phi(u)(\phi(v) + \chi(-v)) = q^2 + 1 + \phi(D_2) \sum_{u, v \in F_{q^2}} \phi(u)(\phi(v) + \chi(-v))
\]
\[
= q^2 + 1 + \phi(D_2) \sum_{u, v \in F_{q^2}} \phi(u)(\phi(v) + \chi(-v)) = q^2 + 1 + \chi(D_2) \sum_{u, v \in F_{q^2}} \phi(u)(\phi(v) + \chi(-v))
\]
By Lemma 3.41 [2], we have \( \#(\mathcal{E}_\chi \otimes F_q^2)(F_{q^2}) = q^2 + 1 + \phi(D_2) = 1 + \chi(D_2) \). By noting that \( \lambda \) is the image of \( \lambda \) in \( \mathbb{Z}[\rho]/(-2) \cong F_4 \). Note that \( D_2 \neq 0 \) and \( y^2 + \lambda y = x^3 \) is the minimal Weierstrass equation at the prime ideal \((-2)\). For \( y \in F_4 \), we show that \( y^2 + D_3y = 1 \) if and only if \( (D_3 + 1)y = 0 \).\( y \neq 0, 1 \). Indeed, for \( y \in F_4 \), we have \( y^2 + D_3y = 1 \) if and only if \( D_3 \neq 0 \). Thus, \( y^2 = y + 1 \) holds, so \( y^2 - y + 1 = (y - 1)(y + 1) \) and \( y \neq 1 \). Thus, we have \( D_3 = 0 \) if and only if \( y^2 + D_3y = 1 \). For \( D_3 + 1 = 0 \), we have \( y^2 + D_3y = 1 \). Therefore,
\[
\#\{(x, y) \in F_4 \times F_4 \mid y^2 + D_3y = 1\} = 3\#\{y \in F_4 \mid y^2 + D_3y = 1\} = 3\#\{y \in F_4 \mid (D_3 + 1)y = 0 \neq 0, 0\} = 0 \quad \text{if} \quad D_3 \neq 1
\]
holds. Then, by noting that \( \#\{y \in F_4 \mid y^2 + D_3y = 0\} = 0 \), we have
\[
\#(\mathcal{E}_\chi \otimes F_4)(F_4) = 1 + \#\{(x, y) \in F_4 \times F_4 \mid y^2 + D_3y = x^3\}
\]
\[
= 1 + \#\{(x, y) \in F_4 \times F_4 \mid y^2 + D_3y = 1\} = 3 \quad \text{if} \quad D_3 \neq 1
\]
On the other hand, by Lemma 3.41 [2], we have
\[
\chi(2) = \chi(-2) = \left( \frac{-2}{\lambda} \right) = \left\{ \begin{array}{ll}
1 & \text{if} \ \lambda \equiv 1 \mod 2,
\rho \text{ or } \overline{\rho} \mod 2
\end{array} \right.
\]
By noting that \( \rho + \overline{\rho} = -1 \),
\[
q^2 + 1 + q(\chi(q) + \overline{\chi(q)}) = 5 + 2(\chi(2) + \overline{\chi(2)}) = \left\{ \begin{array}{ll}
9 & \text{if} \ \lambda \equiv 1 \mod 2,
3 & \text{if} \ \lambda \equiv \rho \text{ or } \overline{\rho} \mod 2
\end{array} \right.
\]
holds. Since \( \lambda \equiv 1 \mod 2 \iff D_3 = 1 \), we have \#(\mathcal{E}_\chi \otimes F_4)(F_q^2) = q^2 + 1 + q(\chi(q) + \overline{\chi(q)}) \) for \( q = 2 \).

If \( \infty \neq (x, y) \in \mathcal{E}_\chi(Q(\rho))[2] \), then, \( y = 0 \). Then, \( x^3 = -\lambda^2 \) and \( x \in Q(\rho) \). This is a contradiction. Thus, we have \#(\mathcal{E}_\chi(Q(\rho))[2] = \{ \infty \}.

Let \( m \geq 1 \) be an integer that is relatively prime to 5. Then, \( \mathcal{E}_\chi(Q(\rho))[m] \) has injective homomorphisms to \( \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \) and \( (\mathcal{E}_\chi \otimes F_{25})(F_{25}) \) by [51] Chap. VII, Proposition 3.1 (b). On the other hand, \#(\mathcal{E}_\chi \otimes F_{25})(F_{25}) = 26 + 5(\chi(5) + \overline{\chi(5)}) = 36 \), or 21 by [41]. Thus, for \( m \) relatively prime to 2, 3, 5, 7, we have \#(\mathcal{E}_\chi(Q(\rho))[m] = 1 \). We also have that \#(\mathcal{E}_\chi(Q(\rho))[m] has injective homomorphisms to \( \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \) and
(δλ ⊗ F_{121})(F_{121}) for m relatively prime to 11 by loc. cit. On the other hand, #(δλ ⊗ F_{121})(F_{121}) = 122 + 11(χλ(11) + χλ(11)) = 144, or 111 by [5]. Thus, for m relatively prime to 2, 3, 11, 37, we have #δλ(Q)(m) = 1.

Therefore, we have δλ(Qρ)|_{tors} = δλ(Qρ)|[3]. Let ∞ ≠ P = (x, y) ∈ δλ(Qρ)|[3]. If y = 0, we have P ∈ δλ(Qρ)|[3] ∩ δλ(Qρ)|[2] = {∞}. This is a contradiction. Thus, we have y ≠ 0, equivalently, 4x^3 + λ^2 ≠ 0. For Q ∈ δλ, we denote the x-coordinate of Q by x(Q). Then, x(2P) = \frac{x^3 - 2λ^2}{4x^3 + λ^2}, x(-P) = x. Since 2P = -P, we have x^3 - 2λ^2 = x. Thus, x = 0 or x^3 = -λ^2. Since x ∈ Qρ, we have x^3 ≠ -λ^2. Therefore, x = 0. By P ∈ δλ : y^2 = x^3 + \frac{λ^2}{4}, we have y = ±\frac{λ}{2}. Thus, we proved δλ(Qρ)|_{tors} = δλ(Qρ)|[3] = {∞, (0, ±2)}. □

**Proposition 3.4.** (Correspondence between the Hecke L-series and the L-function of the elliptic curve) Let L(δλ/Qρ, s) be the L-function of the elliptic curve δλ : y^2 = x^3 + \frac{λ^2}{4} over Qρ (see [2], §10 of Chap. II). The Hecke L-series defined by (3.1) corresponds to the L-function of the elliptic curve δλ, i.e., one has

\[ L(s, \overline{\lambda})L(s, \overline{\lambda}) = L(\delta_{\lambda}/\mathbb{Q}(\rho), s). \]

**Proof.** We recall the definition of L(δλ/Qρ, s) : L(δλ/Qρ, s) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(\delta_{\lambda}/\mathbb{Q}(\rho), q_{\mathfrak{p}}^{-s})^{-1}, where L_{\mathfrak{p}}(\delta_{\lambda}/\mathbb{Q}(\rho), T) is the local L-factor of δλ/Qρ at \mathfrak{p} defined as follows: Let q_{\mathfrak{p}} := #k_{\mathfrak{p}}, a_{\mathfrak{p}} := q_{\mathfrak{p}} + 1 - #(\delta_{\lambda} \otimes k_{\mathfrak{p}})(k_{\mathfrak{p}}), if \delta_{\lambda} has good reduction at \mathfrak{p}. Then,

\[ L_{\mathfrak{p}}(\delta_{\lambda}/\mathbb{Q}(\rho), T) := 1 - a_{\mathfrak{p}} T + q_{\mathfrak{p}} T^2. \]

If δλ has bad reduction at \mathfrak{p}, we define

\[ L_{\mathfrak{p}}(\delta_{\lambda}/\mathbb{Q}(\rho), T) := \begin{cases} 1 - T & \text{if } \delta_{\lambda} \text{ has split multiplicative reduction at } \mathfrak{p}, \\ 1 + T & \text{if } \delta_{\lambda} \text{ has non-split multiplicative reduction at } \mathfrak{p}, \\ 1 & \text{if } \delta_{\lambda} \text{ has additive reduction at } \mathfrak{p}. \end{cases} \]

If \mathfrak{p} = (\mu), where \mu ∈ Z[\rho] is a primary prime ≠ λ such that p = \mu \mathfrak{p} is a rational prime, then k_{\mathfrak{p}} ∼ F_{p}, q_{\mathfrak{p}} = p, a_{\mathfrak{p}} = χλ(\mu)\mathfrak{p} + \overline{\chiλ}(\mu)\mu hold by Lemma [5.2] [4]. Thus,

\[ L_{\mathfrak{p}}(\delta_{\lambda}/\mathbb{Q}(\rho), q_{\mathfrak{p}}^{-s}) = 1 - (\chiλ(\mu)\mathfrak{p} + \overline{\chiλ}(\mu)\mu)p^{-s} + p^{1-2s}. \]

On the other hand, the local L-factor of L(s, \overline{\lambda})L(s, \overline{\lambda}) at \mathfrak{p} is

\[ (1 - \chiλ(\mu)\mathfrak{p}(\mu\mathfrak{p})^{-s})(1 - \overline{\chiλ}(\mu)\mu(\mu\mathfrak{p})^{-s}) = 1 - (\chiλ(\mu)\mathfrak{p} + \overline{\chiλ}(\mu)\mu)p^{-s} + p^{1-2s} \]

by (3.1). Therefore, the local L-factor of L(s, \overline{\lambda})L(s, \overline{\lambda}) at \mathfrak{p} coincides with the one of L(δλ/Qρ, s) at \mathfrak{p}.

Next, if \mathfrak{p} = (-q), where q is a rational prime such that q ≡ 2 mod 3, then k_{\mathfrak{p}} ∼ F_{q^2}, q_{\mathfrak{p}} = q^2, a_{\mathfrak{p}} = -q(\chiλ(q) + \overline{\chiλ}(q)) hold by Lemma [5.2] [3]. Thus,

\[ L_{\mathfrak{p}}(\delta_{\lambda}/\mathbb{Q}(\rho), q_{\mathfrak{p}}^{-s}) = 1 + (\chiλ(q) + \overline{\chiλ}(q))q^{1-2s} + q^{2-4s}. \]

On the other hand, the local L-factor of L(s, \overline{\lambda})L(s, \overline{\lambda}) at \mathfrak{p} is

\[ (1 - \chiλ(-q)(\overline{\chiλ})^{-2s})(1 - \overline{\chiλ}(-q)(\overline{\chiλ})^{-2s}) = 1 + (\chiλ(q) + \overline{\chiλ}(q))q^{1-2s} + q^{2-4s} \]

by (3.1). Therefore, the local L-factors of L(s, \overline{\lambda})L(s, \overline{\lambda}) at \mathfrak{p} coincides with the one of L(δλ/Qρ, s) at \mathfrak{p}. If \mathfrak{p} = (λ), (1 - ρ), then, δλ has additive reduction at \mathfrak{p} by Lemma [5.2] [1]. Then, both of the local L-factors of L(s, \overline{\lambda})L(s, \overline{\lambda}) and L(δλ/Qρ, s) are equal to 1. □
Chapter 3.3 Elliptic Gauss sums and Tate-Shafarevich groups

In this section, we show that the order of the Tate-Shafarevich group of the elliptic curve $E/\mathbb{Q}(\rho)$ is equal to the square of the absolute value of the coefficient $a_\lambda$ of the relevant elliptic Gauss sum or its quarter under the BSD conjecture on the $2, 3$-parts of the leading term for $E/\mathbb{Q}(\rho)$. By combining this and Theorem 2.3, we obtain that the order of the Tate-Shafarevich group of $E/\mathbb{Q}(\rho)$ is congruent to the square of Bernoulli-Hurwitz-type numbers $C_n, D_n$ times $1/9$ or $1/36$ modulo $\ell$ under the BSD conjecture on the $2, 3$-parts of the leading term. Unconditionally, we have such congruences up to the multiplications of powers of $2, 3$.

**Lemma 3.5.** (Hecke $L$-value and elliptic Gauss sum)

$$L(1, \tilde{\chi}_\lambda) = \begin{cases} \frac{-\varpi_1 \chi_\lambda(3) G_\lambda(\chi_\lambda, \varphi)}{\lambda} & \text{if } \ell \equiv 4 \text{ mod } 9 \text{ and } n \equiv 0 \text{ mod } 3 \text{ (where } \lambda = 3m + 1 + 3n\rho, \ m, n \in \mathbb{Z}), \\ \frac{-\varpi_1 \chi_\lambda(3) G_\lambda(\chi_\lambda, \varphi^{-1})}{\lambda} & \text{otherwise,} \end{cases}$$

up to the multiplications of powers of $2, 3$. Moreover, for $p = 2, 3$, under the BSD conjecture on the $p$-part of the leading term for the elliptic curve $\mathcal{E}_\lambda$, the above equality holds at powers of $p$ as well.

**Proof.** The lemma follows from [A, Theorem 1.16 of §1.4] and Theorem 2.3.

**Theorem 3.6.** (The Tate-Shafarevich groups and the coefficients of elliptic Gauss sums) For the number $a_\lambda$ defined in Theorem 2.3, one has

$$\#\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho)) = \begin{cases} \frac{|a_\lambda|^2}{4} & \text{if } \ell \equiv 4 \text{ mod } 9 \text{ and } n \equiv 0 \text{ mod } 3 \text{ (where } \lambda = 3m + 1 + 3n\rho, \ m, n \in \mathbb{Z}), \\ \frac{|a_\lambda|^2}{2} & \text{otherwise,} \end{cases}$$

up to the multiplications of powers of $2, 3$. Moreover, for $p = 2, 3$, under the BSD conjecture on the $p$-part of the leading term for the elliptic curve $\mathcal{E}_\lambda$, the above equality holds at powers of $p$ as well.

**Proof.** Let $\tau_\infty := \varpi_\lambda \varpi_\lambda$, where $\varpi_\lambda$ is a generator, as $\mathbb{Z}[\rho]$-modules, over $\mathbb{Z}[\rho]$ of the period lattice, in $\mathbb{C}$, of $\mathcal{E}_\lambda$. (Note that $\varpi_\lambda$ is not unique, however, $\tau_\infty$ is well-defined). The substitution $y \mapsto \frac{y}{2}$ gives an equation of the form

$$\mathcal{E}_\lambda : y^2 = 4x^3 + \lambda^2.$$

From this equation, we have $g_\lambda := \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \frac{1}{\varpi_\lambda} = -\frac{\lambda^2}{144}$ by [S1, Theorem 3.5 (b) of Chap. VI]. On the other hand, by Lemma 1.2, $g_1 := \sum_{0 \neq \omega \in \mathbb{Z}[\rho]} \frac{1}{\varpi_1} = \frac{27}{144}$ by loc. cit. Thus, we have $\frac{\varpi_6}{\varpi_1} = \frac{g_1}{g_\lambda} = -\frac{27}{\lambda^2}$. By taking the absolute values, $\tau_\infty^3 = \frac{3\varpi_6^2}{\varpi_1^2}$ since $\ell = \lambda^2 = |\lambda|^2$. Then, we have

$$\tau_\infty = \frac{3\varpi_6^2}{\ell^2}.$$

We recall that

$$
\tau(\lambda) = 3, \quad \#\mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}} = 3
$$

by Lemma 3.2, respectively. If $s \in \mathbb{R}$, $L(s, \tilde{\chi}_\lambda) = L(s, \overline{\chi}_\lambda)$. Thus, $L(1, \tilde{\chi}_\lambda)L(1, \chi_\lambda) = |L(1, \tilde{\chi}_\lambda)|^2$. Therefore,

$$L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), 1) = L(1, \tilde{\chi}_\lambda)L(1, \chi_\lambda) = \frac{|a_\lambda|^2}{\ell^2} \varpi_1^2$$

by Proposition 3.4 and Lemma 3.5 (note that $\tilde{\lambda} = \lambda$, $(\tilde{\lambda})^2 = |\lambda|^2 = \ell$). Thus, $L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), 1) \neq 0$ holds since Lemma 3.5. Hence, by [R, Theorem (i)], we have $\#\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho)) < \infty$ and

$$L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), 1) = \tau_\infty \tau(1-\rho) \frac{\#\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho))}{\#\mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}}} \frac{\#\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho))}{\#\mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}}},$$

(3.3)

up to the multiplications of powers of $2, 3$. If $\ell \equiv 4 \text{ mod } 9 \text{ and } n \equiv 0 \text{ mod } 3$, then $\tau(1-\rho) = 4$ by Lemma 3.2. Thus,

$$\frac{|a_\lambda|^2}{\ell^2} \varpi_1^2 = 3\varpi_6^2 \frac{4 \cdot 3 \cdot \#\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho))}{3^2},$$

23
up to the multiplications of powers of 2, 3. Therefore, we have \( \# \text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho)) = \frac{|\alpha_\lambda|^2}{3^2} \) up to the multiplications of powers of 2, 3.

Otherwise, \( t_{(1-p)} = 1 \), we have

\[
\frac{|\alpha_\lambda|^2}{\ell^+} = \frac{3\pi^2}{\ell^+} \cdot 1 \cdot 3 \cdot \frac{\# \text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho))}{3^2},
\]

up to the multiplications of powers of 2, 3. Therefore, we have \( \# \text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho)) = |\alpha_\lambda|^2 \) up to the multiplications of powers of 2, 3.

Finally, for \( p = 2, 3 \), under the BSD conjecture on the \( p \)-part of the leading term for the elliptic curve \( \mathcal{E}_\lambda \), the equality \( \ref{equation:3.3} \) holds at powers of \( p \) as well. Hence the final claim of the theorem follows.

**Remark 3.7.** By the second supplementary law of the cubic reciprocity law, \( n \equiv 0 \mod 3 \iff \chi_\lambda(3) = 1 \) holds, since \( \chi_\lambda(3) = p^n \) by \( \ref{equation:3.6} \) the last formula in Theorem 7.8 of Chap. 7, where \( n \) is as in Theorem \( \ref{equation:3.6} \) (Note that the definition of primarity in \( \ref{equation:3.1} \) is slightly different from the one in this paper, however, it does not affect the above equivalence.) Hence, if \( \ell \equiv 7, 4 \mod 9 \) and \( n \equiv 0 \mod 3 \), we have \( \alpha_\lambda \in \mathbb{Z} \) by Theorem \( \ref{equation:2.7} \). Under the BSD conjecture on the 2-part of the leading term for the elliptic curve \( \mathcal{E}_\lambda \), we have

\[
n \equiv 0 \mod 3 \implies 2|\alpha_\lambda
\]

(3.4)
since Theorem \( \ref{equation:3.3} \) As long as the center of the table at \( \ref{equation:3.4} \), \( n \) is plausible. However, by the case of \( p = 139 \) in Asai’s table, we cannot replace “ \( \implies \) ” with “ \( \iff \) ” in \( \ref{equation:3.4} \).

**Corollary 3.8.** (The Tate-Shafarevich groups and the Bernoulli-Hurwitz-type numbers) We write \( \lambda = 3m + 1 + 3n\rho \), \( m, n \in \mathbb{Z} \), then we have

\[
\# \text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho)) \equiv_{\text{mod} \lambda} \begin{cases} 
\left(\frac{\chi_\lambda(3)D_{2(\ell-1)}}{\ell^+}\right)^2 / 36 & \text{if } \ell \equiv 4 \mod 9 \text{ and } n \equiv 0 \mod 3, \\
\left(\frac{\chi_\lambda(3)D_{2(\ell-1)}}{\ell^+}\right)^2 / 9 & \text{if } \ell \equiv 4 \mod 9 \text{ and } n \equiv \pm 1 \mod 3, \\
\left(\frac{\chi_\lambda(3)C_{2(\ell-1)}}{\ell^+}\right)^2 / 9 & \text{if } \ell \equiv 7 \mod 9,
\end{cases}
\]

(3.5)

\[
\# \text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho)) \equiv_{\text{mod} \ell} \begin{cases} 
\left(\frac{3^{\frac{\ell-7}{3}}D_{2(\ell-1)}}{\ell^+}\right)^2 / 4 & \text{if } \ell \equiv 4 \mod 9 \text{ and } n \equiv 0 \mod 3, \\
\left(\frac{3^{\frac{\ell-7}{3}}D_{2(\ell-1)}}{\ell^+}\right)^2 & \text{if } \ell \equiv 4 \mod 9 \text{ and } n \equiv \pm 1 \mod 3, \\
\left(\frac{3^{\frac{\ell-7}{3}}C_{2(\ell-1)}}{\ell^+}\right)^2 & \text{if } \ell \equiv 7 \mod 9,
\end{cases}
\]

up to the multiplications of powers of 2, 3. Moreover, for \( p = 2, 3 \), under the BSD conjecture on the \( p \)-part of the leading term for the elliptic curve \( \mathcal{E}_\lambda \), the congruence \( \ref{equation:3.3} \) holds without the ambiguity of the multiplications of powers of \( p \).

**Proof.** These congruences hold from Theorem \( \ref{equation:2.5} \), Theorem \( \ref{equation:3.6} \) and Lemma \( \ref{equation:2.4} \). 

**Remark 3.9.** There exist infinitely many rational primes \( \ell \) such that \( \ell \equiv 7, 4 \mod 9 \) and \( \mathbb{F}_\ell^\times/(2, 3 \mod \ell) \) is not trivial, by Chebotarev’s density theorem, where \( (2, 3 \mod \ell) \) is the subgroup generated by 2, 3 mod \( \ell \) of \( \mathbb{F}_\ell^\times \).

**A Appendix**

In this chapter, we show some lemmas and formulae which are very interesting, although they are not used in the proofs of the main results in this paper. In §A.1, we show lemmas on rational primes dividing the denominator of \( d_n \). In §A.2, we determine the signs and the non-vanishing of \( C_n, D_n \) (excluding \( D_{6n+2} \)), and the Eisenstein series \( G_n \) associated to the lattice \( \mathcal{w}_1[\mathbb{Z}] \rho \) (see Lemma \( \ref{equation:A.1} \)) by using new recurrence relations of them arising from new formulae of \( S_l \). In §A.3, we give numerical tables of \( e_n, d_n, G_n, \) and \( BH_n \).
A.1 On the denominator of $d_n$

First, we show a recurrence relation including $G_{6n}$ and $D_n$.

**Lemma A.1.** (Relations between $G_n$ and $D_n$) Let

$$G_n := \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \frac{1}{\omega^n}$$

for $n \geq 1$ (Eisenstein series associated to the lattice $\varpi_1 \mathbb{Z}[\rho]$). Then, for $m \geq 1$, we have

$$\sum_{k=0}^{m} D_{6k+2}(6m - 6k - 1)G_{6(m-k)}3^{6k} = 0, \quad D_{6m-1} = (-1)^{m}3^{3m-1} - 1 \frac{G_{6m}}{2 \cdot 3^{6m-1}}. \tag{A.1}$$

The second equality of (A.1) holds for $m = 0$ as well, where $G_0 := -1$.

**Proof.** First, we note that $G_{6n} \in \mathbb{Q}$ for $n \geq 0$, since $\varphi(u) = \frac{1}{6u} + \sum_{n=1}^{\infty} (6n-1)G_{6n}u^{6n-2}$ around $u = 0$ (note that $G_n = 0$ unless $n$ is congruent to 0 modulo 6) and $\varphi'' = 6\varphi^2$. We prove the first equality of (A.1). Since Lemma [A.4][4], we have

$$\left(\frac{1}{\text{Sl}(-3u)} + \frac{1}{\text{Sl}(3u)}\right) \varphi(u) = 3.$$

Around $u = 0$, we have $\varphi(u) = \sum_{n=0}^{\infty} (6n-1)G_{6n}u^{6n-2}$ and $\sum_{n=0}^{\infty} (6n-1)G_{6n}u^{6n} = \frac{1}{\text{Sl}(3u)}$ by the definitions. Thus, $18 \sum_{n=0}^{\infty} D_{6n+2}3^{6n}u^{6n+2}$ follows. By comparing the coefficients of $u^6$ of this equality for $m \geq 1$, the first equality of (A.1) follows.

We prove the second equality of (A.1). Since Lemma [A.4][10] and $3 = (1 - \rho)(1 - \overline{\rho})$, we have

$$3 \left(\frac{1}{\text{Sl}(-3u)} - \frac{1}{\text{Sl}(3u)}\right) = (1 - \rho)(1 - \overline{\rho}) - 3\zeta(u).$$

Around $u = 0$, $\zeta(u) = -\sum_{n=0}^{\infty} G_{6n}u^{6n-1}$, and $3 \left(\frac{1}{\text{Sl}(-3u)} - \frac{1}{\text{Sl}(3u)}\right) = -2 \sum_{n=0}^{\infty} D_{6n-1}3^{6n}u^{6n-1}$ by the definitions. Thus,

$$-2 \sum_{n=0}^{\infty} D_{6n-1}3^{6n}u^{6n-1} = -2 \sum_{n=0}^{\infty} G_{6n}\{(1 - \rho)6n - 3\}u^{6n-1} = -2 \sum_{n=0}^{\infty} G_{6n}\{-1\cdot 3^{3n} - 3\}u^{6n-1}$$

follows, since $(1 - \rho)^6 = (-1)^n3^{3n}$. By comparing the coefficients of $u^6$ of this equality for $n \geq 0$, the second equality of (A.1) is proved.

**Definition A.2.** (The Bernoulli-Hurwitz number for the period lattice $\varpi_1 \mathbb{Z}[\rho]$) Set $BH_{6m} := (6m)!G_{6m}$ for $m \geq 1$. (Note that $BH_{6m}$ is the Bernoulli-Hurwitz number for the elliptic curve $y^2 = 4x^3 - 27$ defined in [Ka].)

**Lemma A.3.** (The denominator of $D_{6m+2}$) For a rational prime $\ell \equiv 1 \mod 3$ and $m \geq 0$, we define

$$t(\ell, m) := \left\lfloor \frac{6m}{\ell - 1} \right\rfloor,$$

where $[\cdot]$ denotes the floor function. Then,

$$\prod_{\ell: \text{rational prime}} \ell^{t(\ell, m)} \cdot 2(6m)!D_{6m+2} \in \mathbb{Z} \left[\frac{1}{3}\right].$$

Note that the product on the left hand side is a finite product.
Proof. We write 

\[ h_m := \prod_{\ell \text{ rational prime} \atop \ell \equiv 1 \mod 3} \ell^{(\ell, m)} \cdot 2(6m)D_{6m+2} \] 

for \( m \geq 0 \). Since \( h_0 = 2D_2 = \frac{1}{3} \) (see Table 2), the lemma holds for \( m = 0 \). For \( m \geq 1 \), we assume that \( h_k \in \mathbb{Z} \left[ \frac{1}{3} \right] \) for \( k = 0, \ldots, m-1 \). By the first equality of (A.1), we have

\[ h_m 3^{6m} = - \sum_{k=0}^{m-1} h_k (6m - 6k - 1) \left( \prod_{\ell \text{ rational prime} \atop \ell \equiv 1 \mod 3} \ell^{(\ell, m)-t(\ell, k)} \right) BH_{6(m-k)} \frac{(6m)}{6k} 3^{6k}. \quad (A.2) \]

Since the elliptic curve \( y^2 = 4x^3 - 27 \) has good reduction (resp. good ordinary reduction) at \( \ell \) if and only if \( \ell \equiv 3 \) (cf. the proof of Lemma 3.2 [11] (resp. \( \ell \equiv 1 \mod 3 \) (see [52] Chap II, exer. 2.30))), it holds that \( \left( \prod_{\ell \text{ is rational prime}} \ell \right) BH_{6m} \in \mathbb{Z} \left[ \frac{1}{3} \right] \) by [53], Theorem. In terms of \( m \), \( t(\ell, m) \) is nondecreasing. For \( k = 0, \ldots, m-1 \) and a rational prime \( \ell \equiv 1 \mod 3 \), if \( \ell - 1 \) divides \( 6(m - k) \), we have \( t(\ell, m) > t(\ell, k) \), since \( t(\ell, m) = \left\lfloor \frac{6m}{\ell - 1} \right\rfloor = \frac{6(m-k)}{\ell-1} + \frac{6k}{\ell-1} > t(\ell, k) \). Therefore, the right hand side of (A.2) is in \( \mathbb{Z} \left[ \frac{1}{3} \right] \).

Remark A.4. Numerically, we guess that

\[ BH_{6m} \in \mathbb{Z} \left[ \frac{1}{3} \right], \]

where \( \mathbb{Z} \left[ \frac{1}{3} \right] \) is the localization of \( \mathbb{Z} \) by the prime ideal \( 3\mathbb{Z} \) (see Table 3). If this is true, then the same proof of lemma also shows that

\[ 2 \cdot 3^{6m+1}(6m)!L(m) \cdot D_{6m+2} \in \mathbb{Z}, \]

where let \( L(m) := \prod_{\ell \text{ rational prime}} \ell^{(\ell, m)} \).

Lemma A.5. (Integrality of \( d_{6m+2} \) outside 3) For \( m \geq 0 \), we have \( d_{6m+2} \in \mathbb{Z} \left[ \frac{1}{3} \right] \).

Proof. By Lemma 1.12 we can write \( 2d_{6m+2} = \frac{N_m}{3^{6m+1}} \cdot r(m) \geq 0 \), \( N_m \in \mathbb{Z} \). By Lemma A.3 we have \( 2L(m) \cdot \frac{d_{6m+2}}{(6m+1)(6m+2)} \in \mathbb{Z} \left[ \frac{1}{3} \right] \). Thus, \( L(m) \cdot \frac{N_m}{(6m+1)(6m+2)} \cdot \frac{1}{3^{6m+1}} \in \mathbb{Z} \left[ \frac{1}{3} \right] \) holds. Then, we have \( (6m+1)(6m+2) \mid L(m) \cdot N_m \), since \( 6m+1 \) and \( 6m+2 \) are relatively prime to 3. Especially, we have \( 2 \mid N_m \), since 2 does not divide \( L(m) \). Therefore, the lemma is proved.

Lemma A.6. (1) \[ \frac{1}{\text{Sl}(\sqrt{-3}u)} + \frac{1}{\text{Sl}(-\sqrt{-3}u)} = -\frac{\text{Sl}(u^2)}{\text{Cl}(u)} = \text{Sl}(-u) \text{Sl}(u) \in \mathcal{H}_{\mathbb{Z}}. \]

(2) \( \text{The denominator of } d_{6m+2} \)

\[ d_{6n+2}3^{3n+1} \in \mathbb{Z}. \]

Proof. \( \Box \) We have

\[ \frac{1}{\text{Sl}(\sqrt{-3}u)} = \frac{1 + 7\text{Sl}(u)^3}{\sqrt{-3}\text{Sl}(u)\text{Cl}(u)}. \]

by A. 2. (viii) of Appendix or putting \( u := \rho u \) and \( v := -\rho u \) of the addition formula of \( \text{Sl} \) (Lemma 1.60). By \( \text{Sl}(-u) = -\frac{\text{Sl}(u)}{\text{Cl}(u)} \) and \( \text{Cl}(-u) = \frac{1}{\text{Cl}(u)} \) (Lemma 1.3 [11]), we have

\[ \frac{1}{\text{Sl}(-\sqrt{-3}u)} = \frac{-1 - \rho \text{Sl}(u)^3}{\sqrt{-3}\text{Sl}(u)\text{Cl}(u)}. \]

Then, by two equalities and noting that \( \rho - 7 = \sqrt{-3} \), the first equality of (1) is proved. The second equality of (1) also follows from \( \text{Sl}(-u) = -\frac{\text{Sl}(u)}{\text{Cl}(u)} \) (Lemma 1.63 [11]). By lemma 1.19 \( \text{Sl}(u), \text{Sl}(-u) \in \mathcal{H}_{\mathbb{Z}} \). Thus, \( \text{Sl}(u) \text{Sl}(-u) \in \mathcal{H}_{\mathbb{Z}} \).

(2) By the definition, we have \( \frac{1}{\text{Sl}(\sqrt{-3}u)} + \frac{1}{\text{Sl}(-\sqrt{-3}u)} = 2 \sum_{n=0}^{\infty} d_{6n+2}(-3)^{3n+1} \frac{3^{6n+2}}{(6n+2)!} \). By (1), we have \( 2d_{6n+2}(-3)^{3n+1} \in \mathbb{Z}. \) By Lemma A.3 \( d_{6n+2}(-3)^{3n+1} \in \mathbb{Z}. \)
Lemma A.7. (The denominator of \(d_{6m-1}\)) For \(m \geq 1\), we have

\[
d_{6m-1} = \left(\prod_{\ell \text{ is a rational prime } \ell \equiv 1 \mod 3} \ell\right)^2 \in \mathbb{Z}\left[\frac{1}{3}\right].
\]

Proof. From the second equality of (A.1), for \(m \geq 1\), we have

\[
d_{6m-1} = \frac{(-1)^m 3^{3m-1} - 1}{2 \cdot 3^{6m-1}} BH_{6m} = \frac{(-1)^m 3^{3m-1} - 1}{2} \cdot BH_{6m} - \frac{1}{2m} \cdot \frac{1}{3^{6m}}.
\]

Since \((-1)^m 3^{3m-1} - 1 \equiv 2 \mod 4\), \((\frac{-1)^m 3^{3m-1} - 1}{2} \in \mathbb{Z}\). From [K] Theorem, \(\prod_{\ell \text{ is a rational prime } \ell \equiv 1 \mod 3} \ell \) holds.

A.2 On the signs and the non-vanishing of \(C_n, D_n, \) and \(G_n\)

In this section, we determine the signs of \(C_n, D_n\) (excluding \(D_{6n+2}\)), and \(G_n\). Moreover, it is proved that \(C_{3n+1}, D_{6n-1}, G_{6n}, \) and \(BH_{6n}\) do not vanish. First, we determine the signs and the non-vanishing of \(G_n, BH_{6n}, \) and \(D_{6n-1}\).

Lemma A.8 (The signs and the non-vanishing of \(G_n, BH_{6n}, \) and \(D_{6n-1}\)). For \(n \geq 2\), we have

\[
(6n-1)(6n-2)(6n-3) - 12)G_{6n} = 6 \sum_{k=1}^{n-1} (6k-1)(6n-6k-1)G_{6k}G_{6(n-k)}, \quad (A.3)
\]

and for \(n \geq 1\), \(G_{6n} > 0\), hence \(BH_{6n} > 0\). Moreover, \((-1)^m D_{6m-1} > 0\) holds for \(m \geq 1\). In particular, \(G_{6n}, BH_{6n}, \) and \(D_{6n-1}\) are non-zero.

Proof. Since \(\varphi'' = 6\varphi^2\) and \(\varphi(u) = \sum_{n=0}^{\infty} (6n-1)G_{6n}u^{6n-2}\), for \(n \geq 1\), we have

\[
(6n-1)(6n-2)(6n-3)G_{6n} = 6 \sum_{m+k=n} G_{6k}(6k-1)G_{6m}(6m-1) = 6 \sum_{k=1}^{n-1} (6k-1)(6n-6k-1)G_{6k}G_{6(n-k)} + 12G_{6n}(6n-1),
\]

here, note that \(G_0 = -1\). Then, we have the equality (A.3). By the proof of Lemma A.2, we have \(G_6 = \frac{27}{140} > 0\). The positivity of \(G_{6n}\) for \(n \geq 1\) follows by induction on \(n\), (A.3) and \(G_6 > 0\). Then, by the second equality of (A.1), we have

\[
(-1)^m D_{6m-1} = (-1)^m \frac{3^{3m-1} - 1}{2 \cdot 3^{6m-1}} G_{6m} = \frac{3^{3m-1} - (-1)^m}{2 \cdot 3^{6m-1}} G_{6m} > 0
\]

for \(m \geq 1\).

Definition A.9 (Hurwitz coefficient). For a formal power series \(F(u) = \sum_{n=0}^{\infty} \frac{a_n}{n!} u^n \in \mathbb{Q}[[u]]\) in terms of \(u\), we call \(a_n\) the Hurwitz coefficient for \(F(u)\) of \(u^n\).

Lemma A.10. (1) We have

\[
2 \cdot 3^{6n} c_{6n+1} = 2BH_{6n}(6n+1)(6n-1) - 3^{6n}(6n+1)2n(6n-1)c_{6n-2} + \sum_{k=1}^{n} c_{6(n-k)+1} BH_{6k}(6k-1)(6k-2)3^{6(n-k)} \left(\frac{6n+1}{6k}\right)
\]
for \( n \geq 1 \).

\[
2 \cdot 3^{6n} c_{6n+4} = -(6n+4)(2n+1)(6n+2)3^{6n} c_{6n+1} + \sum_{k=1}^{n} c_{6(n-k)+4} BH_{6k}(6k-1)(6k-2)3^{6(n-k)} \left( \frac{6n+4}{6k} \right)
\]

for \( n \geq 1 \).

(2) (The sign and the non-vanishing of \( c_n \)) We have \((-1)^{k+1} c_k > 0\) for \( k \geq 1 \), i.e., \( c_{6n+1} > 0 \), \( c_{6n+4} < 0 \) for \( n \geq 0 \). In other words, all the Hurwitz coefficients for \(-\text{Sl}(\mathbf{u})\) are \( > 0 \). In particular, \( c_{3n+1} \) does not vanish.

(3) (The sign and the non-vanishing of \( e_n \)) We put \( \text{Cl}(\mathbf{u}) =: \sum_{n=0}^{\infty} \frac{c_n}{16^n} u^{3n} \), then \((-1)^n c_{3n} > 0\) for \( n \geq 0 \).

Equivalently, \( e_{6n} > 0 \), \( e_{6n+3} < 0 \) for \( n \geq 0 \). In particular, \( e_{3n} \) does not vanish.

**Proof.** By \( \text{Sl}(\mathbf{u}) = \varphi \left( \frac{u}{-3^{\frac{k}{2}}} \right) \) (Lemma 12.4 [1]), \( \text{Sl}(\mathbf{u}) = \sum_{n=0}^{\infty} C_{6n+1} u^{3n+1} = \sum_{n=0}^{\infty} c_{6n+1} u^{6n+1} + \sum_{n=0}^{\infty} C_{6n+4} u^{6n+4} \), \( \varphi'(u) = \sum_{n=0}^{\infty} G_{6n}(6n-1) u^{6n-2} \) and \( \varphi''(u) = \sum_{n=0}^{\infty} G_{6n}(6n-1)(6n-2) u^{6n-3} \), we have

\[
\left( \sum_{n=0}^{\infty} C_{6n+1} u^{6n} + \sum_{n=0}^{\infty} C_{6n+4} u^{6n+3} \right) \left( u^3 - \sum_{n=0}^{\infty} G_{6n}(6n-1)(6n-2) \frac{u^{6n}}{3^{6n-1}} \right) = 6 \sum_{n=0}^{\infty} G_{6n}(6n-1) \frac{u^{6n}}{3^{6n}}.
\]

(A.4)

Taking the even part of \( \text{A.4} \),

\[
\sum_{n=0}^{\infty} C_{6n+1} u^{6n} \left( G_{6n}(6n-1)(6n-2) \frac{u^{6n}}{3^{6n-1}} \right) + \sum_{n=0}^{\infty} C_{6n+4} u^{6n+3} \cdot u^3 = 6 \sum_{n=0}^{\infty} G_{6n}(6n-1) \frac{u^{6n}}{3^{6n}}
\]

holds. By comparing the coefficients of \( u^{6n} \), we have

\[
3^{6n-1} C_{6n-2} = 2G_{6n}(6n-1) - 2 \cdot 3^{6n} C_{6n+1} + \sum_{k=1}^{n} C_{6(n-k)+1} G_{6k}(6k-1)(6k-2)3^{6(n-k)}
\]

for \( n \geq 1 \). Since \( C_k = \frac{1}{k!} \), \( G_{6k} = \frac{BH_{6k}(6k)!}{(6k)!} \), we also have

\[
3^{6n}(6n+1)2n(6n-1)c_{6n-2} = 2BH_{6n}(6n+1)(6n-1) - 2 \cdot 3^{6n} c_{6n+1} + \sum_{k=1}^{n} C_{6(n-k)+1} BH_{6k}(6k-1)(6k-2)3^{6(n-k)} \left( \frac{6n+1}{6k} \right)
\]

for \( n \geq 1 \). This is the first equality of \( \Box \). Taking the odd part of \( \text{A.4} \),

\[
\sum_{n=0}^{\infty} C_{6n+1} u^{6n} \cdot u^3 + \sum_{n=0}^{\infty} C_{6n+4} u^{6n+3} \left( - \sum_{n=0}^{\infty} G_{6n}(6n-1)(6n-2) \frac{u^{6n}}{3^{6n-1}} \right) = 0.
\]

By comparing the coefficients of \( u^{6n+3} \), we have

\[
C_{6n+1} = -6C_{6n+4} + \sum_{k=1}^{n} C_{6(n-k)+4} G_{6k}(6k-1)(6k-2) \frac{1}{3^{6k-1}}.
\]

Therefore,

\[
(6n+4)(2n+1)(6n+2)3^{6n} c_{6n+1} = -2 \cdot 3^{6n} c_{6n+4} + \sum_{k=1}^{n} c_{6(n-k)+4} BH_{6k}(6k-1)(6k-2)3^{6(n-k)} \left( \frac{6n+4}{6k} \right)
\]

follows. This is the second equality of \( \Box \).
2. From Table 1, $c_1 = 1 > 0$, $c_4 = -4 < 0$. We assume that $c_1, c_7, \ldots, c_{6(n-1)+1} > 0$ and $c_4, c_{10}, \ldots, c_{6(n-1)+4} < 0$ for some $n \geq 1$. Then, since the first equality of (1) and $BH_{6n} > 0$ ($n \geq 1$) (by Lemma A.8), we have $c_{6n+1} > 0$. We also have $c_{6n+4} < 0$, since the second equality of (1). By induction on $n$, 2 is proved.

3. By 2, for all $n \geq 0$, the Hurwitz coefficient for $-\text{Sl}(-u)$ of $u^{3n+1}$ is $> 0$. Since $\text{Cl}(-u) = -(-\text{Sl}(-u))^2$ for all $n \geq 1$, the Hurwitz coefficient for $\text{Cl}'(-u) = \sum_{n=1}^{\infty} e_{3n} (-1)^{3n-1} e_{3n-1}^{3n-1} (3n-1)!$ is $< 0$. Therefore, we have $(-1)^{3n} e_{3n} > 0$. Since $\text{Cl}(0) = 1$, $e_0 = 1$. Thus, $(-1)^n e_{3n} > 0$ holds for $n \geq 0$.

Remark A.11. On the sign of $D_{6n+2}$ for $n \geq 0$, it is conjectured that $(-1)^n D_{6n+2} > 0$, which is still open. To prove this, we may have to relate it to some $L$-value to determine the sign of $D_{6n+2}$.
### A.3 Numerical tables of $c_n, d_n, G_{6n},$ and $BH_{6n}$

Table 1: $c_n$

| $n$ | $c_n$ |
|-----|-------|
| 1   | 1     |
| 4   | -4    |
| 7   | 160   |
| 10  | -20800|
| 13  | 647680|
| 16  | -3946624000 |
| 19  | 4161608704000 |
| 22  | -6974121256960000 |
| 25  | 1745522222028800000 |
| 28  | -622267704323448320000 |
| 31  | 30437918678165359820800000 |
| 34  | -198204965707722312916480000000 |
| 37  | 16758824127564135479341219840000000 |
| 40  | -18018078892547110999024290611200000000 |
| 43  | 241972954728067026275815933786193920000000000 |
| 46  | -399711453549126843327490319908738170880000000000 |
| 49  | 8013800222299278632180644288254182214860800000000000 |
| 52  | -19272532158166604513119104829337619755759042560000000000000 |
| 55  | 5502091915585466726498093137306896664233747415040000000000000000 |
| 58  | -1847461772661880232920188921078802118211374987978956500000000000000000 |
| 61  | 72354459099399071070935028921851613732359179300925398888192000000000000 |
| 64  | -3280456305171371413525294691303861562668456710283810344898560000000000000000 |
| 67  | 171010625561990453493002557236042739742908863391412621902154844160000000000000000 |


Table 2: $d_n$

| $n$ | $d_n$ |
|-----|-------|
| 2   | 1/3   |
| 5   | $-10/21$ |
| 8   | $-2 \cdot 5/3 \cdot 7$ |
| 11  | $48400/273$ |
| 14  | $70400/3$ |
| 17  | $-230982400/1197$ |
| 20  | $-2393600000/3$ |
| 23  | $46641833216000/273$ |
| 26  | $43504924672000000/27$ |
| 29  | $-4634596783616000000/651$ |
| 32  | $-384236269846528000000/3$ |
| 35  | $5835679905178616750080000000/57757$ |
| 38  | $9304580611314692915200000000/3$ |
| 41  | $-25268765638101190566608896000000000/6321$ |
| 44  | $-17284095511545036218564608000000000/9$ |
| 47  | $1027896133477097691463521769984000000000/273$ |
| 50  | $8030649112422447620287530780864000000000000/3$ |
| 53  | $-272275412126083890645192892507963392000000000000/3591$ |
| 56  | $-22871478427768693526299780079937838544000000000000/3$ |

31
Table 3: $G_n$, and $BH_n$

| $n$ | $G_n$ | $BH_n$ |
|-----|-------|--------|
| 6   | 27/140| 972/7  |
| 12  | 729/112112 | 283435200/91 |
| 18  | 19683/184352896 | 90914674752000/133 |
| 24  | 9034497/2269709478400 | 2247402096066380800/91 |
| 30  | 961376769/9936195998310400 | 5569206003076317032217600000/217 |
| 36  | 45251875376667/15343234021377167360000 | 4913031852065049466068649519911075840000/447811 |
| 42  | 3409353379806993/43280194527500713689088000 | 33314057040643263742571290653335322624000000/301 |

References

[A] Asai, T., “Elliptic Gauss sums and Hecke $L$-values at $s = 1$”, *RIMS Kokyuroku Bessatu*, 4, 79–121, Kyoto University (2007).

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

[CW] Coates, J., Wiles, A., “On the Conjecture of Birch and Swinnerton-Dyer”, *Inventiones math.*, 39, 223–251 (1977).

[H] Hurwitz, A., “Über die Anzahl der Klassen binärer quadratischer Formen von negativer Determinante”, *Acta Math.*, 19, 351–384 (1895).

[IR] Ireland, K., Rosen, M., “A Classical Introduction to Modern Number Theory”, 2nd ed., *G.T.M.*, 84, Springer-Verlag (1990).

[Ka] Katz, N. M., “The Congruences of Clausen-von Staudt and Kummer for Bernoulli-Hurwitz Numbers”, *Math. Ann.*, 216, 1–4 (1975).

[Ko] Kodaira, K., “Complex Manifolds and Deformation of Complex Structures”, *Classics in Mathematics*, Springer (2005).

[L] Lemmermeyer, F., “Reciprocities Laws : From Euler to Eisenstein”, Springer-Verlag (2000).

[O] Onishi, Y., “Congruence Relations Connecting Tate-Shafarevich Groups with Hurwitz Numbers”, *Interdisciplinary Information Sciences*, 16, No. 1, 71–86 (2010).

[R] Rubin, K., “The “main conjectures” of Iwasawa theory for imaginary quadratic fields”, *Inventiones math.*, 103, 25–68 (1991).

[S1] Silverman, J. H., “The Arithmetic of Elliptic Curves”, 2nd ed., *G.T.M.*, 106, Springer-Verlag (2009).

[S2] Silverman, J. H., “Advanced Topics in the Arithmetic of Elliptic Curves”, *G.T.M.*, 151, Springer-Verlag (1994).

[W] Washington, L. C., “Introduction to Cyclotomic Fields”, 2nd ed., *G.T.M.*, 83, Springer-Verlag (1997).

[WW] Whittaker, E. T., Watson, G. N., “A Course of Modern Analysis”, Cambridge University Press (1996)