



**CONGRUENCE RELATIONS CONNECTING
TATE–SHAFAREVICH GROUPS WITH BERNOULLI–HURWITZ
NUMBERS BY ELLIPTIC GAUSS SUMS IN THE EISENSTEIN
INTEGERS CASE**

Akihiro Goto

Faculty of Mathematics, Kyushu University, Motoooka, Fukuoka, Japan
akihiro.gotoh64@gmail.com

Received: 5/14/24, Revised: 11/26/25, Accepted: 8/20/26, Published: 10/7/26

Abstract

We prove a congruence relation between the order of the Tate–Shafarevich groups of certain elliptic curves with complex multiplication (CM) by the Eisenstein integers and Mordell–Weil rank 0, and a coefficient in the power series expansion of an elliptic function associated with the Eisenstein integers. A similar result in the case of elliptic curves with CM by the Gaussian integers was formerly proved by Onishi. These congruences can be viewed as generalizations of the classical congruence between class numbers of imaginary quadratic fields and Bernoulli numbers or Euler numbers.

1. Introduction

The following congruence is classically well-known.

Theorem 1 ([5]). *Let $p > 3$ be a prime number, and let $h(-p)$ be the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Then the congruence*

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

holds. Here, B_n and E_n are the n -th Bernoulli and Euler numbers, respectively, defined by the generating series $\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$ and $\frac{2}{e^t+e^{-t}} = \sum_{n=0}^{\infty} E_n \frac{t^n}{n!}$.

As an elliptic generalization of this, based on Asai’s previous work on elliptic Gauss sums [1], Onishi studied a certain family $\{E_\lambda\}$ of elliptic curves over $\mathbb{Q}(i)$ with complex multiplication (CM) by the ring of Gaussian integers $\mathbb{Z}[i]$, parametrized by primary primes $\lambda \in \mathbb{Z}[i]$, that is, $\lambda \equiv 1 \pmod{(2+2i)}$ lying above prime numbers $\ell \equiv 5 \pmod{8}$, and obtained the following theorem.

Theorem 2 ([10]). *For a primary prime $\lambda \in \mathbb{Z}[i]$, there exists an integer $n \in \mathbb{Z}$ such that*

$$\#\text{III}(E_\lambda/\mathbb{Q}(i)) \equiv_{\text{mod } \ell} 2^n C_{3(\ell-1)/4},$$

where ℓ is the norm prime of λ satisfying $\ell \equiv 5 \pmod{8}$, $\text{III}(E_\lambda/\mathbb{Q}(i))$ is the Tate–Shafarevich group of the elliptic curve $E_\lambda/\mathbb{Q}(i)$, and $C_{3(\ell-1)/4}$ is the Hurwitz-type number which is defined as a coefficient in the power series expansion of the lemniscatic sine or cosine function.

Note that this theorem is obtained by combining Theorem 2.4 and Proposition 3.9 in [10]. The author of [10] showed this result by proving congruences between the coefficients of elliptic Gauss sums and Hurwitz-type numbers (defined as power series coefficients of certain elliptic functions). Note that the above n is always 0 because of a recent result of Burungale and Flach [3], which establishes the Birch–Swinnerton–Dyer conjecture on the leading term of the Hasse–Weil L -function (see [12, Section 10 of Chap. II]) for an elliptic curve E over a number field F with CM by an imaginary quadratic field K and with analytic rank 0 under the assumption that $F(E_{\text{tors}})/K$ is abelian. For the statement of the Birch–Swinnerton–Dyer conjecture, see Conjecture 1.

In this paper, we prove an analogue of Onishi’s result for the ring $\mathbb{Z}[\frac{-1+i\sqrt{3}}{2}]$ of Eisenstein integers (see Corollary 2). To state the main results of this paper precisely, we first introduce some notation and definitions. Let $\rho := e^{\frac{2\pi i}{3}}$, $\varpi_1 := \int_0^1 \frac{dt}{\sqrt[3]{(1-t^3)^2}}$ (the real period of the elliptic curve $y^2 = 4x^3 - 27$; see Lemma 2 (c)), $\varphi(u) := \frac{6\wp(\varpi_1 u)}{9+\wp'(\varpi_1 u)}$, and $\text{Sl}(u) := \varphi\left(\frac{u}{-3\varpi_1}\right)$, where $\wp$ is the Weierstrass $\wp$ function with the period lattice $\varpi_1\mathbb{Z}[\rho]$. We define the rational numbers C_n and D_n as the coefficients of Taylor expansions of $\text{Sl}(u)$ and $\text{Sl}(u)^{-1}$, respectively, that is,

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

(The numbers C_{3n+1} and D_{3n+2} satisfy certain recurrence relations; see the proof of Lemma 7 and Remark 1.) The rational numbers C_{3n+1} and D_{3n+2} are analogues of the Bernoulli numbers or the Euler numbers, which we call *Bernoulli–Hurwitz-type numbers*, following Katz [7]. Let ℓ be a prime number such that $\ell \equiv 1 \pmod{3}$ and let $\lambda \in \mathbb{Z}[\rho]$ be a prime element such that $\ell = \lambda\bar{\lambda}$ and $\lambda \equiv 1 \pmod{3}$. We denote by χ_λ the cubic residue character over $(\mathbb{Z}[\rho]/(\lambda))^\times \simeq \mathbb{F}_\ell^\times$ and set $\tilde{\lambda} := \prod_{\chi_\lambda(\nu)=1} \varphi\left(\frac{\nu}{\lambda}\right)$. (Then $\tilde{\lambda}^3 = \lambda$ holds; see Lemma 9 (b).)

The *elliptic Gauss sum* associated with χ_λ and $f \in \{\varphi, \varphi^{-1}\}$ is defined by

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

We define the *coefficient of the elliptic Gauss sum* by

$$\alpha_\lambda := \begin{cases} G_\lambda(\chi_\lambda, \varphi)/\tilde{\lambda}^2 & \ell \equiv 7 \pmod{9} \\ G_\lambda(\chi_\lambda, \varphi^{-1})/\tilde{\lambda}^2 & \ell \equiv 4 \pmod{9}. \end{cases}$$

(Then, $\alpha_\lambda \in \chi_\lambda(3)(1 + 3\mathbb{Z})$ or $\alpha_\lambda \in \overline{\chi_\lambda}(3)(-1 + 3\mathbb{Z})$ hold; see Theorem 5.) The reason why we do not consider the case $\ell \equiv 1 \pmod{9}$ is explained in Subsection 3.1. The following two theorems are the main results of this paper.

Theorem 3. *The denominators of $C_{\frac{2}{3}(\ell-1)}$ and $D_{\frac{2}{3}(\ell-1)}$ are not divisible by ℓ when $\ell \equiv 7 \pmod{9}$ and $\ell \equiv 4 \pmod{9}$, respectively. We have*

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

We note the right-hand side of the above congruences. By the universal property of ring localization, the natural ring homomorphism $\mathbb{Z}_{(\ell)} \rightarrow \mathbb{F}_\ell$ is induced by the canonical projection $\mathbb{Z} \rightarrow \mathbb{F}_\ell$, where $\mathbb{Z}_{(\ell)}$ denotes the localization of $\mathbb{Z}$ at the prime ideal (ℓ) . The rational numbers $-\frac{1}{3}C_{\frac{2}{3}(\ell-1)}$ and $-\frac{1}{3}D_{\frac{2}{3}(\ell-1)}$ belong to $\mathbb{Z}_{(\ell)}$. In the above congruences, we regard $-\frac{1}{3}C_{\frac{2}{3}(\ell-1)}$ and $-\frac{1}{3}D_{\frac{2}{3}(\ell-1)}$ as elements of $\mathbb{Z}[\rho]/(\lambda)$ via the homomorphism $\mathbb{Z}_{(\ell)} \rightarrow \mathbb{F}_\ell$ and the natural isomorphism $\mathbb{F}_\ell \simeq \mathbb{Z}[\rho]/(\lambda)$.

Theorem 4. *Let $\lambda = 3m + 1 + 3n\rho$ with $m, n \in \mathbb{Z}$. Then, for the elliptic curve $\mathcal{E}_\lambda : y^2 = x^3 + \frac{\lambda^2}{4}$, the Tate–Shafarevich group $\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho))$ of $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$ is finite and we have*

$$\#\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho)) = \begin{cases} |\alpha_\lambda|^2/4 & \ell \equiv 4 \pmod{9} \text{ and } n \equiv 0 \pmod{3} \\ |\alpha_\lambda|^2 & \text{otherwise.} \end{cases}$$

We will briefly explain the outline of the proof of the main results. First, Theorem 3 is proved by taking $\varphi\left(\frac{1}{\lambda}\right)$ -adic expansions of the elliptic Gauss sums. Theorem 4 is proved by verifying each of the following relationships:

$$\alpha_\lambda \xleftrightarrow[\text{(i)}]{\text{Hecke } L\text{-value at } s=1} \xleftrightarrow[\text{(ii)}]{\text{Elliptic } L\text{-value at } s=1} \xleftrightarrow[\text{(iii)}]{\# \text{III}}$$

Asai [1] has shown that the elliptic Gauss sum appears in the value of the Hecke L -series $L(\widetilde{\chi}_\lambda, s)$ at $s = 1$ (see Theorem 5), which is the relationship (i) in the above diagram. The relationship (ii) in the above diagram is the equality $L(\widetilde{\chi}_\lambda, s)L(\overline{\widetilde{\chi}_\lambda}, s) = L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s)$ given in Proposition 1. This equality is established directly by applying 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 $\widetilde{\chi}_\lambda$ is the Hecke character arising from χ_λ (see Subsection 4.1), $L(\widetilde{\chi}_\lambda, s)$ is the Hecke L -series associated with $\widetilde{\chi}_\lambda$, and $L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s)$ is the Hasse–Weil L -function for $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$. It follows that the relationship (iii) in the above diagram is a consequence of the Birch–Swinnerton–Dyer conjecture on the

leading term of $L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s)$. Here we emphasize that, since the analytic rank of $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$ is zero, the result of [3] shows that the Birch–Swinnerton–Dyer conjecture for the leading term of $L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s)$ is known to hold.

The proofs of these results are similar to those of the main results of [10]. However, several new phenomena arise, requiring modifications to our arguments. For example, while the denominator of H_{4n} in [10] cannot be explicitly determined and necessitates a reference to Katz [7] to consider congruences modulo ℓ , it can be shown that the denominator of d_{6n+2} , which appears in Theorem 3 of this paper, divides an integer of the form $2 \cdot 3^m$ for some non-negative integer m (see Lemma 8). Furthermore, Theorem 4 implies that $|\alpha_\lambda|^2$ is divisible by 4 when $\ell \equiv 4 \pmod{9}$ and $n \equiv 0 \pmod{3}$, whereas Proposition 3.9 of [10], in the Gaussian integers case, does not imply such divisibility.

Note that the results of [10] and this paper are considered only over the Gaussian and Eisenstein integers. Since the fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\rho)$ are both imaginary quadratic fields and cyclotomic fields, we believe this case to be more tractable. To extend the results to the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ for a prime number $p > 3$, at some point, it may be necessary to consider the inclusions $\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_p)$ if $p \equiv 3 \pmod{4}$, and $\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_{4p})$ if $p \equiv 1 \pmod{4}$.

Finally, we outline the organization of this paper. In Section 2, we study properties of certain elliptic functions whose period lattice consists of Eisenstein integers. We use these properties in defining the elliptic Gauss sums and their coefficients. In Section 3, we introduce the elliptic Gauss sums and establish the main congruences (Theorem 3) between the Bernoulli–Hurwitz-type numbers and the coefficients of the elliptic Gauss sums. In Section 4, we prove Theorem 4 after providing some preparatory material on certain Hecke characters, the Hecke L -series associated with them, certain elliptic curves $\mathcal{E}_\lambda$ for λ , and their L -functions. In the Appendix, we provide some lemmas, formulae, and tables of C_n , D_n , and related quantities, which are not directly used in proving the main results of this paper but are of independent interest.

For basic terms related to the theory of elliptic curves used in this paper, please refer to [12] and [13].

2. Elliptic Functions

This section is devoted to the study of certain elliptic functions whose period lattice is generated by the Eisenstein integers (or their constant multiples). In Subsection 2.1, we introduce elliptic functions Sl , Cl , φ , and ψ and show their function-theoretic properties. In Subsection 2.2, we investigate the power series expansions of $\text{Sl}(ru)$ and $\text{Sl}(ru)^{-1}$ (for $r \in \mathbb{Z} \setminus \{0\}$) in terms of $\text{Sl}(u)$. These expansions will be used to establish the main congruences of Theorem 3. In Subsection 2.3, we introduce

Bernoulli–Hurwitz-type numbers. In Subsection 2.4, we explore certain arithmetic properties of the values of $\text{Sl}(u)$ at division points.

2.1. Basic Properties of Elliptic Functions with Eisenstein Integer Periods

We denote by ϖ_1 (see [1, Section 1.1.1.]) the real period given by

$$\varpi_1 = \int_0^1 \frac{dt}{\sqrt[3]{(1-t^3)^2}} = 1.76663875 \dots$$

Let $\wp(u)$ denote the Weierstrass $\wp$ -function with period lattice $\varpi_1\mathbb{Z}[\rho]$, so that $\wp'^2 = 4\wp^3 - 27$ (see Lemma 2). Throughout this paper, $\overline{(\cdot)}$ denotes complex conjugation. We write

$$W := \{\pm 1, \pm \rho, \pm \bar{\rho}\} \text{ and } W' := \{1, \rho, \bar{\rho}\}.$$

Lemma 1. *We have*

$$\varpi_1 = \frac{1}{3}B\left(\frac{1}{3}, \frac{1}{3}\right) = \frac{1}{2\pi\sqrt{3}}\Gamma\left(\frac{1}{3}\right)^3 = \frac{2^{\frac{1}{3}}}{3\sqrt{3}}B\left(\frac{1}{6}, \frac{1}{2}\right),$$

where B and Γ denote the beta and gamma functions, respectively.

Proof. This follows from the following identities:

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}, \quad \Gamma(s)\Gamma\left(s + \frac{1}{2}\right) = \frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s), \text{ and } B(s, t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}.$$

□

Lemma 2. *The Weierstrass $\wp$ -function with period lattice $\varpi_1\mathbb{Z}[\rho]$ satisfies the following properties:*

- (a) $\wp(\rho u) = \rho\wp(u)$, $\wp(-u) = \wp(u)$, $\wp'(\rho u) = \wp'(u)$, $\wp'(-u) = -\wp'(u)$;
- (b) $\wp(\bar{u}) = \overline{\wp(u)}$, $\wp'(\bar{u}) = \overline{\wp'(u)}$, thus if $u \in \mathbb{R}$, $\wp(u), \wp'(u) \in \mathbb{R}$;
- (c) $\wp'^2 = 4\wp^3 - 27$;
- (d) $\wp(\varpi_1/3) = 3$, $\wp((1-\rho)\varpi_1/3) = 0$;
- (e) $\wp'(\varpi_1/3) = -9$, and $\wp'((1-\rho)\varpi_1/3) = -3\sqrt{3}i$.

Proof. Parts (a) and (b) follow immediately from the symmetry and homogeneity properties of the $\wp$ -function. To prove (c), recall the classical identity:

$$\wp'^2 = 4\wp^3 - 60G_4\wp - 140G_6,$$

where $G_6 := \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \omega^{-6}$ and $G_4 := \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \omega^{-4}$. We compute

$$G_4 = \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \frac{1}{(\rho\omega)^4} = \frac{1}{\rho^4} \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \frac{1}{\omega^4} = \bar{\rho} \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \frac{1}{\omega^4} = \bar{\rho} G_4,$$

which implies $G_4 = 0$. Hence,

$$\wp'^2 = 4\wp^3 - 140G_6 = 4(\wp - \wp(\varpi_1/2))(\wp - \wp(\rho\varpi_1/2))(\wp - \wp((1+\rho)\varpi_1/2)).$$

Let $e := \wp(\varpi_1/2)$. Then, using the symmetry properties in (a) and the identity $1 + \rho + \bar{\rho} = 0$, we find

$$140G_6 = 4\wp\left(\frac{\varpi_1}{2}\right)\wp\left(\frac{\rho}{2}\varpi_1\right)\wp\left(\frac{1+\rho}{2}\varpi_1\right) = 4e^3.$$

From Lemma 1, we also obtain

$$\begin{aligned} \frac{\varpi_1}{2} &= \int_0^{\frac{\varpi_1}{2}} du = \int_{\infty}^e \frac{d(\wp(u))}{\wp'(u)} = \int_e^{\infty} \frac{dx}{\sqrt{4x^3 - 4e^3}} = \frac{1}{2e^{\frac{1}{2}}} \int_1^{\infty} \frac{dx}{\sqrt{x^3 - 1}} \\ &= \frac{1}{2e^{\frac{1}{2}}} \frac{1}{3} \int_0^1 y^{-\frac{5}{6}} (1-y)^{-\frac{1}{2}} dy = \frac{1}{2e^{\frac{1}{2}}} \frac{1}{3} B\left(\frac{1}{6}, \frac{1}{2}\right) = \frac{1}{e^{\frac{1}{2}}} \frac{\sqrt{3}}{2^{\frac{4}{3}}} \varpi_1, \end{aligned}$$

where we used the substitution $y = x^{-3}$. Solving, we obtain $4e^3 = 27$.

To prove (d) and (e), observe that the periodicity of $\wp$ and part (a) yield

$$\wp((1-\rho)\varpi_1/3) = 0.$$

Using the addition formula:

$$\wp(u_1 + u_2) = -\wp(u_1) - \wp(u_2) + \frac{1}{4} \left(\frac{\wp'(u_1) - \wp'(u_2)}{\wp(u_1) - \wp(u_2)} \right)^2$$

(see, for example, [16, Chap. XX, 20.3]) together with (c), we deduce $\wp(\varpi_1/3) = 3$ and

$$\wp'\left(\frac{1-\rho}{3}\varpi_1\right)\wp'\left(\frac{\varpi_1}{3}\right) = 27\sqrt{3}i. \quad (1)$$

Since $\wp'\left(\frac{1-\rho}{3}\varpi_1\right)^2 = -27$, we have $\wp'((1-\rho)\varpi_1/3) \in i\mathbb{R}$ and by (b), $\wp'\left(\frac{\varpi_1}{3}\right) \in \mathbb{R}$

Now, recall that the divisor of $\wp'$ is

$$-3(0) + (\varpi_1/2) + (\rho\varpi_1/2) + ((1+\rho)\varpi_1/2) \pmod{\varpi_1 \mathbb{Z}[\rho]}.$$

Thus, $\wp'(x)$ is a real-valued function on the open interval $(0, \varpi_1)$ with a unique zero at $x = \varpi_1/2$. Since $\wp'(u) = -2u^{-3} + \dots$ around $u = 0$, we find

$$\lim_{x \rightarrow +0} \wp'(x) = -\infty,$$

and hence $\wp'(x) < 0$ for $x \in (0, \varpi_1/2)$. In particular, $\wp'(\varpi_1/3) < 0$. Since $\wp(\varpi_1/3) = 3$ and $\wp'^2 = 4\wp^3 - 27$, we conclude

$$\wp'(\varpi_1/3) = -9.$$

Substituting this into Equation (1) yields

$$\wp'((1 - \rho)\varpi_1/3) = -3\sqrt{3}i,$$

as desired. $\square$

Definition 1 (Definition 1.1 and 1.2 in [1] for Z, φ , and ψ). Let $\zeta(u)$ denote Weierstrass' ζ function associated with the lattice $\varpi_1\mathbb{Z}[\rho]$. We define

$$\begin{aligned} Z(u) &:= \zeta(\varpi_1 u) - \frac{2\pi}{\sqrt{3}\varpi_1} \bar{u}, \\ \varphi(u) &:= \frac{1}{3} \left\{ Z\left(u - \frac{1}{3}\right) + \bar{\rho}Z\left(u - \frac{\rho}{3}\right) + \rho Z\left(u - \frac{\bar{\rho}}{3}\right) \right\}, \\ \psi(u) &:= -\frac{1}{3} \left\{ Z\left(u - \frac{1}{3}\right) + \rho Z\left(u - \frac{\rho}{3}\right) + \bar{\rho}Z\left(u - \frac{\bar{\rho}}{3}\right) \right\}, \\ \text{Sl}(u) &:= \varphi\left(\frac{u}{-3\varpi_1}\right), \text{ and } \text{Cl}(u) := \psi\left(\frac{u}{-3\varpi_1}\right). \end{aligned}$$

Note that

$$Z(u + v) = Z(u) + Z(v) + \frac{1}{2} \frac{\wp'(\varpi_1 u) - \wp'(\varpi_1 v)}{\wp(\varpi_1 u) - \wp(\varpi_1 v)}, \quad (2)$$

which follows from the addition formula:

$$\zeta(u + v) = \zeta(u) + \zeta(v) + \frac{1}{2} \frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)} \quad (3)$$

(see, for example, [16, Chap. XX, 20.53, Example 2]).

We recall the basic properties of these functions stated in [1], without proof.

Lemma 3 ([1]). *The following hold:*

- (a) $\zeta(\rho u) = \bar{\rho}\zeta(u)$, $\zeta(-u) = -\zeta(u)$, and $\zeta(\varpi_1/2) = \pi/(\sqrt{3}\varpi_1)$;
- (b) The function Z is a non-holomorphic periodic function with the period lattice $\mathbb{Z}[\rho]$. It satisfies the following properties: $Z(\rho u) = \bar{\rho}Z(u)$, $Z(-u) = -Z(u)$, $Z(1/3) = 1$, $Z((1 - \rho)/3) = 0$;
- (c) We have

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

Thus, φ and ψ are elliptic functions with the period lattice $\mathbb{Z}[\rho]$;

(d) $\varphi(\rho u) = \rho\varphi(u)$ and $\psi(\rho u) = \psi(u)$. We also have $\varphi(\bar{u}) = \overline{\varphi(u)}$ and $\psi(\bar{u}) = \overline{\psi(u)}$.

Therefore, $\varphi(u)$ and $\psi(u)$ are real if u is real;

(e) $\varphi'(u) = -3\varpi_1\psi(u)^2$ and $\psi'(u) = 3\varpi_1\varphi(u)^2$;

(f) $\varphi(u)^3 + \psi(u)^3 = 1$, $\varphi(0) = 0$, and $\psi(0) = 1$;

(g) $\varphi(-u) = -\varphi(u)\psi(u)^{-1}$, $\psi(-u) = \psi(u)^{-1}$, and $\varphi(u)^{-1} + \varphi(-u)^{-1} = 3\wp(\varpi_1 u)^{-1}$;

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

Proof. The identities $\zeta(\rho u) = \bar{\rho}\zeta(u)$ and $\zeta(-u) = -\zeta(u)$ in (a) follow immediately. The third identity follows from Legendre's relation (see, for example, [16, Chap. XX, 20.411])

$$\frac{\rho\varpi_1}{2}\zeta\left(\frac{\varpi_1}{2}\right) - \frac{\varpi_1}{2}\zeta\left(\frac{\rho\varpi_1}{2}\right) = \frac{\pi i}{2}.$$

The identities $Z(\rho u) = \bar{\rho}Z(u)$ and $Z(-u) = -Z(u)$ in (b) are direct consequences of the definition and (a). By the quasi-periodicity (see, for example, [16, Chap. XX 20.41])

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

we find that $Z(u+1) = Z(u)$ and $Z(u+\rho) = Z(u)$. Due to the periodicity of Z and the identity $Z(\rho u) = \bar{\rho}Z(u)$, we deduce that $Z((1-\rho)/3) = 0$. The identity $Z(1/3) = 1$ is shown by setting $u = (1-\rho)/3$ and $v = \rho/3$ in Equation (2).

The identities in (c) follow from Equation (2), Lemma 2, and the following formulas:

$$\sum_{w \in W'} \frac{\bar{w}}{x-w} = \frac{3x}{x^3-1}, \quad \sum_{w \in W'} \frac{w}{x-w} = \frac{3}{x^3-1},$$

for $w \in \{1, \rho, \bar{\rho}\} = W'$. Then, (d) follows directly from (c) and Lemma 2. Differentiating the expressions in (c), and using $\wp'^2 = 4\wp^3 - 27$ and $\wp'' = 6\wp^2$, yields (e).

From (e), we find that $(\varphi^3 + \psi^3)' = 0$, so $\varphi^3 + \psi^3$ is constant. Evaluating at $u = 0$, we find $\varphi(0) = 0$ and $\psi(0) = 1$ by (c) and the fact that $\wp(u)$ and $\wp'(u)$ have poles of order 2 and 3 at $u = 0$, respectively. Hence, (f) follows. The identities in (g) can be verified using (c) and Lemma 2.

Substituting $u := \varpi_1 u$ and $v := -\rho\varpi_1 u$ into Equation (3), we get

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

On the other hand, using (c), we have

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

Combining these gives the desired identity in (h). $\square$

2.2. The Power Series Expansions in Terms of Sl

Let us consider the power series expansions in terms of the function $\text{Sl}(u)$ in this subsection, which will be used to show the main congruences (Theorem 3).

We note that $\mathbb{Q}[[\text{Sl}(u)]]$ is isomorphic to the ring of formal power series over $\mathbb{Q}$. Indeed, since $\text{Sl}(u)$ is an elliptic function which is holomorphic at $u = 0$, $\text{Sl}(u)$ has infinitely many values around $u = 0$. Thus, $\text{Sl}(u) \in \mathbb{Q}[[u]]$ is transcendental over $\mathbb{Q}$.

First, we will prove the following lemma.

Lemma 4 ([1, page 97]). *We have*

$$\text{Sl}(u+v) = \frac{\text{Sl}(u)^2 \text{Cl}(v) - \text{Sl}(v)^2 \text{Cl}(u)}{\text{Sl}(u) \text{Cl}(v)^2 - \text{Sl}(v) \text{Cl}(u)^2}$$

and

$$\text{Sl}(u+v) \in \text{Sl}(u) + \text{Sl}(v) + (\text{Sl}(u), \text{Sl}(v))^4 \mathbb{Z}[\frac{1}{3}][[\text{Sl}(u), \text{Sl}(v)]] \subset \mathbb{Q}[[u, v]].$$

Proof. Let us set $\alpha := (u+v)/2$ and $\beta := (u-v)/2$. Define the function

$$f(\alpha, \beta) := \frac{\text{Sl}(u)^2 \text{Cl}(v) - \text{Sl}(v)^2 \text{Cl}(u)}{\text{Sl}(u) \text{Cl}(v)^2 - \text{Sl}(v) \text{Cl}(u)^2}.$$

Then, it can be verified that the partial derivative of f with respect to β is zero. Hence, f is independent of β , that is, it is constant with respect to β . Therefore, $f(\alpha, \beta) = f(\alpha, \alpha) = \text{Sl}(2\alpha) = \text{Sl}(u+v)$, where the last equality follows from the identities in Lemma 3 (f). This proves the identity.

It remains to show that $\text{Sl}(u+v) \in \text{Sl}(u) + \text{Sl}(v) + (\text{Sl}(u), \text{Sl}(v))^4 \mathbb{Z}[\frac{1}{3}][[\text{Sl}(u), \text{Sl}(v)]]$. By Lemma 3 (f), we have the following expansions:

$$\text{Cl}(u) = 1 + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{3}}{n} \text{Sl}(u)^{3n}, \quad \text{Cl}(u)^2 = 1 + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{2}{3}}{n} \text{Sl}(u)^{3n}, \quad (4)$$

which hold for $u \in \mathbb{R}$ around $u = 0$. By analytic continuation, these expressions also hold for $u \in \mathbb{C}$ around $u = 0$. Set $x := \text{Sl}(u)$ and $y := \text{Sl}(v)$. Then, using Equation (4), we have

$$\begin{aligned} \text{Sl}(u+v) &= \frac{x^2 - y^2 + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{3}}{n} (x^2 y^{3n} - y^2 x^{3n})}{x - y + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{2}{3}}{n} (xy^{3n} - yx^{3n})} \\ &= \frac{x + y - x^2 y^2 \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{3}}{n} (x^{3n-3} + \dots + y^{3n-3})}{1 - xy \sum_{n=1}^{\infty} (-1)^n \binom{\frac{2}{3}}{n} (x^{3n-2} + \dots + y^{3n-2})} \\ &\in x + y + (x, y)^4 \mathbb{Z}[\frac{1}{3}][[x, y]]. \end{aligned}$$

Here, note that the reciprocal of the denominator lies in

$$\begin{aligned} \left(1 - xy \sum_{n=1}^{\infty} (-1)^n \binom{\frac{2}{3}}{n} (x^{3n-2} + \dots + y^{3n-2})\right)^{-1} &\in 1 + (xy)\mathbb{Z}\left[\frac{1}{3}\right][[x, y]] \\ &\subset \left(\mathbb{Z}\left[\frac{1}{3}\right][[x, y]]\right)^{\times}, \end{aligned}$$

and also that $\left(\frac{1}{3}\right), \left(\frac{2}{3}\right) \in \mathbb{Z}\left[\frac{1}{3}\right]$ (see p.52 of [15]). $\square$

Lemma 5. *For any integer r , the following holds*

$$\text{Sl}(ru) \in r \text{Sl}(u) + \text{Sl}(u)^4 \mathbb{Z}\left[\frac{1}{3}\right][[\text{Sl}(u)^3]] \subset \mathbb{Q}[[u]]. \quad (5)$$

Moreover, if $r \neq 0$, then

$$\text{Sl}(ru)^{-1} \in \frac{1}{r \text{Sl}(u)} + \text{Sl}(u)^2 \mathbb{Z}\left[\frac{1}{r}, \frac{1}{3}\right][[\text{Sl}(u)^3]] \subset \frac{1}{u} \mathbb{Q}[[u]]. \quad (6)$$

Proof. From Lemma 4, there exists a formal power series $f(x, y) \in (x, y)^4 \mathbb{Z}[1/3][[x, y]]$ such that

$$\text{Sl}(u + v) = \text{Sl}(u) + \text{Sl}(v) + f(\text{Sl}(u), \text{Sl}(v)).$$

We first prove Equation (5) for all non-negative integers r by induction on r . The case $r = 0$ is trivial. Assume that Equation (5) holds for some $r \geq 0$, that is,

$$\text{Sl}(ru) = r \text{Sl}(u) + \text{Sl}(u)^4 f_r(\text{Sl}(u)^3)$$

for some $f_r(t) \in \mathbb{Z}\left[\frac{1}{3}\right][[t]]$, where t is a formal variable. Then, by the addition formula, we have

$$\begin{aligned} \text{Sl}((r+1)u) &= \text{Sl}(u) + \text{Sl}(ru) + f(\text{Sl}(u), \text{Sl}(ru)) \\ &\in (r+1) \text{Sl}(u) + \text{Sl}(u)^4 \mathbb{Z}\left[\frac{1}{3}\right][[\text{Sl}(u)^3]], \end{aligned}$$

since f has no terms of degree less than 4. Thus, Equation (5) holds for any $r \geq 0$. We now consider the case of negative integers. It is easy to get the identity

$$\text{Cl}(u)^{-1} = 1 + \sum_{n=1}^{\infty} (-1)^n \binom{-\frac{1}{3}}{n} \text{Sl}(u)^{3n} \in 1 + \text{Sl}(u)^3 \mathbb{Z}[1/3][[\text{Sl}(u)^3]] \subset (\mathbb{Z}[1/3][[\text{Sl}(u)^3]])^{\times}$$

from Lemma 3 (f). Then we have

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

Using the same inductive structure as for the positive case, it follows that for any $r > 0$,

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

Hence, Equation (5) holds for all $r \in \mathbb{Z}$.

Now we prove Equation (6). If $r \neq 0$, we write

$$\text{Sl}(ru) = r \text{Sl}(u) + \text{Sl}(u)^4 f_r(\text{Sl}(u)^3), \quad f_r(t) \in \mathbb{Z}[1/3][[t]].$$

Then,

$$\begin{aligned} \left(1 + \frac{\text{Sl}(u)^3 f_r(\text{Sl}(u)^3)}{r}\right)^{-1} &= 1 + \sum_{n=1}^{\infty} \left(-\frac{\text{Sl}(u)^3 f_r(\text{Sl}(u)^3)}{r}\right)^n \\ &\in 1 + \text{Sl}(u)^3 \mathbb{Z}[1/r, 1/3][[\text{Sl}(u)^3]]. \end{aligned}$$

Therefore, we have

$$\text{Sl}(ru)^{-1} = \frac{1}{r \text{Sl}(u)} \left(1 + \frac{\text{Sl}(u)^3 f_r(\text{Sl}(u)^3)}{r}\right)^{-1} \in \frac{1}{r \text{Sl}(u)} + \text{Sl}(u)^2 \mathbb{Z}\left[\frac{1}{r}, \frac{1}{3}\right][[\text{Sl}(u)^3]]$$

as claimed. $\square$

Lemma 6. *The function $\text{Sl} : [0, \varpi_1] \rightarrow [0, 1]$ is the inverse of the function*

$$\begin{aligned} \text{ArcSl} : \quad [0, 1] &\longrightarrow [0, \varpi_1] \\ \downarrow &\quad \downarrow \\ t &\longmapsto \int_0^t \frac{dt}{\sqrt[3]{(1-t^3)^2}} \quad \left(= \sum_{n=0}^{\infty} (-1)^n \binom{-\frac{2}{3}}{n} \frac{t^{3n+1}}{3n+1} \right), \end{aligned}$$

where we choose the branch of $\sqrt[3]{(-)}$ to be a real number.

Proof. Since $\frac{d}{dt} \text{ArcSl} = 1/\sqrt[3]{(1-t^3)^2}$, the function ArcSl is strictly increasing. By the definitions of ArcSl and ϖ_1 , we have $\text{ArcSl}(0) = 0$ and $\text{ArcSl}(1) = \varpi_1$. Hence, the map $\text{ArcSl} : [0, 1] \rightarrow [0, \varpi_1]$ is bijective. On the other hand, from Lemmas 2 and 3, we have $\text{Sl}(0) = 0$ and $\text{Sl}(\varpi_1) = 1$. By Lemma 3 (e), the function Sl is strictly increasing on $[0, \varpi_1]$, and hence the map $\text{Sl} : [0, \varpi_1] \rightarrow [0, 1]$ is also bijective. Now, take any $u_0 \in [0, \varpi_1]$, and set $t_0 := \text{Sl}(u_0)$. Then,

$$\text{ArcSl}(\text{Sl}(u_0)) = \int_0^{t_0} \frac{dt}{\sqrt[3]{(1-t^3)^2}} = \int_0^{u_0} \frac{\text{Cl}(u)^2 du}{\sqrt[3]{(1-\text{Sl}(u)^3)^2}} = u_0,$$

where we used the substitution $t = \text{Sl}(u)$ and $dt = \text{Sl}'(u)du = \text{Cl}^2(u)du$ (by Lemma 3 (e) and (f)). Note that both $\text{Sl}(u)$ and $\text{Cl}(u)$ are real-valued for real u (by Lemma 3 (d)). This confirms that $\text{Sl} : [0, \varpi_1] \rightarrow [0, 1]$ is indeed the inverse of $\text{ArcSl} : [0, 1] \rightarrow [0, \varpi_1]$. $\square$

From [8, Theorem 1.19] and the fact that $\text{Sl}'(0) = \text{Cl}^2(0) = 1 \neq 0$, we have that $\text{Sl}(u)$ is bijective around $u = 0$ for $u \in \mathbb{C}$. Hence, by Lemma 6, the inverse function of $\text{Sl}(u)$ is the analytic continuation of the function $\text{ArcSl}(t)$ to a sufficiently small neighborhood of $t = 0$, which is $\text{ArcSl}(t) = \sum_{n=0}^{\infty} (-1)^n \binom{-\frac{2}{3}}{n} t^{3n+1} / (3n+1)$. Thus, we have the following corollary.

Corollary 1. *We have*

$$u = \sum_{n=0}^{\infty} (-1)^n \binom{-\frac{2}{3}}{n} \frac{\text{Sl}(u)^{3n+1}}{3n+1}$$

in $\mathbb{Q}[[u]]$, in particular, $\mathbb{Q}[[u]] = \mathbb{Q}[[\text{Sl}(u)]]$.

2.3. Bernoulli–Hurwitz-Type Numbers for the Eisenstein Integers

In this subsection, we introduce Bernoulli–Hurwitz-type numbers for the Eisenstein integers and investigate their denominators in connection with the proof of Theorem 3.

We write 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 3 (d), the coefficients of u^n in $\text{Sl}(u)$ vanishes unless $n \equiv 1 \pmod{3}$.)

Lemma 7. *We have $c_{3m+1} \in \mathbb{Z}$ for all $m \geq 0$.*

Proof. We have

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

by Lemma 3, parts (e) and (f). Hence, by induction on m , we have $c_{3m+1} \in \mathbb{Z}$ for any $m \geq 0$. $\square$

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

$$\frac{1}{\text{Sl}(u)} = \frac{1}{u} + \sum_{n=0}^{\infty} D_{3n+2} u^{3n+2} = \frac{1}{u} + \sum_{n=0}^{\infty} \frac{d_{3n+2}}{(3n+2)!} u^{3n+2}. \quad (7)$$

We define $D_{-1} := 1$, so that the expression may also be written as $\text{Sl}(u)^{-1} = \sum_{n=0}^{\infty} D_{3n-1} u^{3n-1}$.

We refer to the coefficients C_{3m+1} and D_{3n+2} as *Bernoulli–Hurwitz-type numbers*.

Remark 1. The function $f(u) = \text{Sl}(u)^{-1}$ satisfies a differential equation $f^{(3)} = 4f - 6f^4$, hence $D_{3m+2} \in \mathbb{Q}$ for $m \geq 0$. We have $D_2 = 1/6, D_5 = -1/252, D_8 = -1/4536$. Therefore, d_{3n+2} is not necessarily a rational integer. However, Lemma 8 below holds.

Definition 2. 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 7 implies $\text{Sl}(u) \in \mathcal{H}_{\mathbb{Z}}$.

Lemma 8. For all integers $m \geq 0$, we have

$$2d_{6m+2} \in \mathbb{Z}[\frac{1}{3}].$$

Proof. Let $f(u) := \text{Sl}(u)^{-1} + \text{Sl}(-u)^{-1}$. Then we have the power series expansion

$$f(u) = 2 \sum_{m=0}^{\infty} \frac{d_{6m+2}}{(6m+2)!} u^{6m+2}.$$

On the other hand, by Lemma 5, we can write

$$\text{Sl}(-u)^{-1} = -\text{Sl}(u)^{-1} + g(\text{Sl}(u)),$$

for some power series $g \in t^2\mathbb{Z}[1/3][[t^3]]$, where t is a formal variable. Hence, $f(u) = g(\text{Sl}(u))$. By Lemma 7, the function $\text{Sl}(u) = \sum_{n=0}^{\infty} c_{3n+1} u^{3n+1} / (3n+1)!$ belongs to $\mathcal{H}_{\mathbb{Z}}$. Hence, it follows that $f(u) \in \mathcal{H}_{\mathbb{Z}[1/3]}$. Therefore, by comparing the coefficients, we conclude that $2d_{6m+2} \in \mathbb{Z}[1/3]$ for all $m \geq 0$. $\square$

Remark 2. Moreover, we can show $d_{6m+2} \in \mathbb{Z}[1/3]$. See Lemma 18. For the denominators of d_{6m-1} , see Lemma 20. However, these facts are not used in the proof of the main congruences in Theorem 3.

2.4. Eisenstein's Product Formula

We recall arithmetic properties of Sl at division points.

Definition 3. For $a \in \mathbb{Z}[\rho]$, we call a *primary* if $a \equiv 1 \pmod{3}$.

This definition is slightly different from the ones in [9, Section 7.1] ($a \equiv \pm 1 \pmod{3}$) and [6, Section 3 of Chap. 9] ($a \equiv -1 \pmod{3}$).

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

$$\ell = \lambda \bar{\lambda} \text{ and } \lambda \equiv 1 \pmod{3}.$$

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

$$\chi_\lambda(\nu) := \left(\frac{\nu}{\lambda}\right)_3,$$

that is,

$$\chi_\lambda(\nu) \in \{1, \rho, \bar{\rho}\} (\subset \mathbb{C}) \text{ and } \chi_\lambda(\nu) \equiv \nu^{(\ell-1)/3} \pmod{\lambda} \quad (\nu \in (\mathbb{Z}[\rho]/(\lambda))^\times).$$

We write

$$\Lambda := \varphi\left(\frac{1}{\lambda}\right).$$

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

Lemma 9 ([1, Lemma 1.3, Definition 1.11, and (xi) of page 98]). *In the notation above, we have the following.*

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

(b) *(Eisenstein's product formula) Let $\tilde{\lambda} := \prod_{\chi_\lambda(r)=1} \varphi(r/\lambda)$. Then $\tilde{\lambda}^3 = \lambda$.*

Lemma 10. *We have the following congruence:*

$$\tilde{\lambda}^2 \equiv \Lambda^{\frac{2(\ell-1)}{3}} \pmod{\Lambda^{\frac{2(\ell-1)}{3}+1}}.$$

Proof. By Lemma 5, for $r \in \mathbb{Z}$, we can write

$$\varphi\left(\frac{r}{\lambda}\right) = r\Lambda + \Lambda^4 f_r(\Lambda^3) = r\Lambda \left(1 + \frac{1}{r}\Lambda^3 f_r(\Lambda^3)\right),$$

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

$$\tilde{\lambda} = \left(\prod_{j=1}^{\frac{\ell-1}{3}} g^{3j}\right) \Lambda^{\frac{\ell-1}{3}} \cdot \prod_{j=1}^{\frac{\ell-1}{3}} \left(1 + \frac{1}{g^{3j}} \Lambda^3 f_{g^{3j}}(\Lambda^3)\right). \quad (8)$$

Since g^{3j} is relatively prime to ℓ for any $j = 1, \dots, (\ell - 1)/3$,

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

is true. Hence, we have

$$\prod_{j=1}^{\frac{\ell-1}{3}} \left(1 + \frac{1}{g^{3j}} \Lambda^3 f_{g^{3j}}(\Lambda^3) \right) \in \mathcal{O}_{\lambda, \Lambda},$$

where $\mathcal{O}_{\lambda, \Lambda}$ is the completion of $\mathcal{O}_{\lambda}$ by Λ . Thus, by taking Equation (8) modulo $\Lambda^{\frac{\ell-1}{3}+1}$, we have

$$\tilde{\lambda} \equiv \left(\prod_{j=1}^{\frac{\ell-1}{3}} g^{3j} \right) \Lambda^{\frac{\ell-1}{3}} \equiv -\Lambda^{\frac{\ell-1}{3}} \pmod{\Lambda^{\frac{\ell-1}{3}+1}},$$

since $\prod_{j=1}^{\frac{\ell-1}{3}} g^{3j} = (g^{\frac{\ell-1}{2}})^{\frac{\ell+2}{3}} \equiv -1 \pmod{\ell}$. We note that $(\ell + 2)/3$ is odd because ℓ is an odd prime. Thus, there exists $a \in \mathcal{O}_{\lambda}$ such that $\tilde{\lambda} = -\Lambda^{\frac{\ell-1}{3}} + a\Lambda^{\frac{\ell-1}{3}+1} = -\Lambda^{\frac{\ell-1}{3}}(1 - a\Lambda)$. We have

$$\tilde{\lambda}^2 = \Lambda^{\frac{2}{3}(\ell-1)}(1 - a\Lambda)^2 \equiv \Lambda^{\frac{2}{3}(\ell-1)} \pmod{\Lambda^{\frac{2}{3}(\ell-1)+1}}.$$

□

3. Elliptic Gauss Sums

In this section, 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 Subsection 3.1, we introduce the elliptic Gauss sums and their coefficients due to Asai. In Subsection 3.2, we show the main congruences and give some examples.

Let $\ell, \lambda, \tilde{\lambda}, \chi_{\lambda}$, and Λ be as in Section 2.

3.1. Elliptic Gauss Sums and Their Coefficients

In this subsection, we introduce the elliptic Gauss sums and their coefficients. We put

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

In this paper, we do not treat the case where $\ell \equiv 1 \pmod{9}$ since the Hecke L -value $L(\widetilde{\chi_{\lambda}}, 1)$ which is described by an elliptic Gauss sum (cf. [1, Theorem 1.16]), can

vanish (cf. [1, Remark of Corollary 1.22]) in the case where $\ell \equiv 1 \pmod 9$. Note that, in the cases where $\ell \equiv 7, 4 \pmod 9$, the Hecke L -value $L(\widetilde{\chi}_\lambda, 1)$ does not vanish (cf. [1, Corollary 1.22]).

Definition 4 ([1, Definition 1.8]). We define

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

and call $G_\lambda(\chi_\lambda, f)$ the *elliptic Gauss sum* associated with χ_λ and f .

Lemma 11. *We have*

$$(a) \quad G_\lambda(\chi_\lambda, f) \in \mathcal{O}_\lambda;$$

$$(b) \quad G_\lambda(\chi_\lambda, f) = \sum_{r \in \ker(\chi_\lambda)} f(r/\lambda).$$

Proof. See [1, Lemma 1.9] for (a). To show (b), we can decompose as follows: $(\mathbb{Z}[\rho]/(\lambda))^\times = S \cup \rho S \cup \bar{\rho} S$ (disjoint union), where $S := \ker(\chi_\lambda)$. Then, (b) follows from the fact that

$$\chi_\lambda(\rho\nu)f(\rho\nu/\lambda) = \chi_\lambda(\nu)f(\nu/\lambda)$$

holds for $\nu \in (\mathbb{Z}[\rho]/(\lambda))^\times$ in both cases $\ell \equiv 7$ and $4 \pmod 9$. □

We shall recall Asai's results from Section 1 of [1].

Theorem 5 ([1, Theorem 1.19]). *We define*

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

Then α_λ is an element of $\mathbb{Z}[\rho]$, and we have

$$\alpha_\lambda \in \begin{cases} \chi_\lambda(3)(1 + 3\mathbb{Z}), & \ell \equiv 7 \pmod 9, \\ \overline{\chi}_\lambda(3)(-1 + 3\mathbb{Z}), & \ell \equiv 4 \pmod 9. \end{cases}$$

In particular, α_λ does not vanish.

Remark 3. In $\ell \equiv 1 \pmod 9$, it may happen that $\alpha_\lambda = 0$ (cf. [1, Remark of Corollary 1.22 and Table 1]).

The number α_λ is called the *coefficient of elliptic Gauss sum*, following [1, Definition 1.12].

3.2. The Proof of Theorem 3

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

Proof of Theorem 3. Let $t := \text{Sl}(u)$. By Corollary 1, for any $\nu \in \mathbb{Z}[\rho]$, we have

$$\begin{aligned} \text{Sl}(\nu u) & \left(= \sum_{m=0}^{\infty} C_{3m+1}(\nu u)^{3m+1} \right) \\ & = \sum_{m=0}^{\infty} C_{3m+1} \nu^{3m+1} \left(\sum_{n=0}^{\infty} (-1)^n \binom{-\frac{2}{3}}{n} \frac{t^{3n+1}}{3n+1} \right)^{3m+1} \end{aligned} \quad (9)$$

and

$$\begin{aligned} \frac{1}{\text{Sl}(\nu u)} + \frac{1}{\text{Sl}(-\nu u)} & \left(= 2 \sum_{m=0}^{\infty} D_{6m+2}(\nu u)^{6m+2} \right) \\ & = 2 \sum_{m=0}^{\infty} D_{6m+2} \nu^{6m+2} \left(\sum_{n=0}^{\infty} (-1)^n \binom{-\frac{2}{3}}{n} \frac{t^{3n+1}}{3n+1} \right)^{6m+2} \end{aligned} \quad (10)$$

as elements of $\mathbb{Q}[[u]] = \mathbb{Q}[[t]]$. By Theorem 5 and Lemma 10, we have

$$G_{\lambda}(\chi_{\lambda}, f) \equiv \alpha_{\lambda} \Lambda^{\frac{2(\ell-1)}{3}} \pmod{\Lambda^{\frac{2(\ell-1)}{3}+1}}, \quad (11)$$

where

$$f = \begin{cases} \varphi, & \ell \equiv 7 \pmod{9}, \\ \varphi^{-1}, & \ell \equiv 4 \pmod{9}. \end{cases}$$

We aim to prove that

$$G_{\lambda}(\chi_{\lambda}, f) \equiv \begin{cases} -\frac{1}{3} C_{\frac{2(\ell-1)}{3}} \cdot \Lambda^{\frac{2(\ell-1)}{3}}, & \ell \equiv 7 \pmod{9}, \\ -\frac{1}{3} D_{\frac{2(\ell-1)}{3}} \cdot \Lambda^{\frac{2(\ell-1)}{3}}, & \ell \equiv 4 \pmod{9} \end{cases} \pmod{\Lambda^{\frac{2(\ell-1)}{3}+1}}. \quad (12)$$

If Equation (12) holds, then we have

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

Recall that $\alpha_{\lambda} \in \mathbb{Z}[\rho]$ by Theorem 5. By Lemma 7 and Lemma 8, we have

$$C_{\frac{2(\ell-1)}{3}} \in \mathbb{Z}_{(\ell)}, \text{ if } \ell \equiv 7 \pmod{9}$$

and

$$D_{\frac{2(\ell-1)}{3}} \in \mathbb{Z}_{(\ell)}, \text{ if } \ell \equiv 4 \pmod{9}.$$

Therefore we may replace "mod Λ " with "mod λ " in the above congruences. To complete the proof of Theorem 3, it suffices to prove Equation (12). To establish Equation (12), we consider two cases.

Case 1: $\ell \equiv 7 \pmod 9$. Let $g \in \mathbb{Z}$ be a primitive root of 1 modulo ℓ , so that $g \pmod \ell$ generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$. Consider the sum

$$L_1(u) := \text{Sl}(g^3u) + \text{Sl}(g^6u) + \cdots + \text{Sl}(g^{\ell-1}u).$$

By Lemma 11 (b) and Equation (9), we obtain

$$G_\lambda(\chi_\lambda, \varphi) = \sum_{j=1}^{\frac{\ell-1}{3}} \text{Sl}\left(\frac{-3\varpi_1 g^{3j}}{\lambda}\right) = L_1\left(\frac{-3\varpi_1}{\lambda}\right)$$

and

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

respectively. By Lemma 5 and the definition of L_1 , the coefficients of this expansion lie in $\mathbb{Z}[\frac{1}{3}]$, in particular, in $\mathbb{Z}_{(\ell)}$. Substituting $t = \Lambda$ (corresponding to $u = \frac{-3\varpi_1}{\lambda}$), we see that $\text{Sl}(\nu u) \mapsto \text{Sl}\left(\frac{-3\varpi_1 \nu}{\lambda}\right)$ for $\nu \in \mathbb{Z}$, by Lemma 5. Therefore,

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

converges Λ -adically in $\mathcal{O}_{\lambda, \Lambda}$ and is equal to $G_\lambda(\chi_\lambda, \varphi)$. By noting that

$$(-1)^n \binom{-\frac{2}{3}}{n} \frac{1}{3n+1} \in \mathbb{Z}_{(\ell)}$$

for $n \leq \frac{2\ell-5}{9}$ (since $\binom{-\frac{2}{3}}{n} \in \mathbb{Z}[\frac{1}{3}]$ and $3n+1 \leq \frac{2\ell-2}{3} < \ell$) and the fact that $C_{3m+1} \in \mathbb{Z}_{(\ell)}$ for $m \leq \frac{2\ell-5}{9}$ (since $C_{3m+1} = \frac{c_{3m+1}}{(3m+1)!}$, $3m+1 < \ell$, and $c_{3m+1} \in \mathbb{Z}$ (Lemma 7)), and that the coefficients of this expansion in terms of Λ are in $\mathbb{Z}[\frac{1}{3}]$, we have

$$\begin{aligned} G_\lambda(\chi_\lambda, \varphi) &\equiv \sum_{m=0}^{\frac{2\ell-5}{9}} C_{3m+1} \left(\sum_{j=1}^{\frac{\ell-1}{3}} g^{3(3m+1)j} \right) \Lambda^{3m+1} \\ &\quad \times \left(\sum_{n=0}^{\frac{2\ell-5}{9}} (-1)^n \binom{-\frac{2}{3}}{n} \frac{\Lambda^{3n}}{3n+1} \right)^{3m+1} \pmod{\Lambda^{\frac{2(\ell-1)}{3}+1}}. \end{aligned}$$

We also have

$$\sum_{j=1}^{\frac{\ell-1}{3}} g^{3(3m+1)j} \equiv_{\text{mod } \ell} \begin{cases} 0 & \text{if } \ell-1 \nmid 3(3m+1) \\ \frac{\ell-1}{3} & \text{if } \ell-1 \mid 3(3m+1). \end{cases}$$

Since $0 \leq m \leq \frac{2\ell-5}{9}$ and $\ell \equiv 7 \pmod{9}$, we see that $\ell-1 \mid 3(3m+1)$ if and only if $3(3m+1) = 2(\ell-1)$. Thus, we have

$$G_{\lambda}(\chi_{\lambda}, \varphi) \equiv C_{\frac{2(\ell-1)}{3}} \cdot \frac{\ell-1}{3} \cdot \Lambda^{\frac{2(\ell-1)}{3}} = -\frac{1}{3} C_{\frac{2(\ell-1)}{3}} \cdot \Lambda^{\frac{2(\ell-1)}{3}} \pmod{\Lambda^{\frac{2(\ell-1)}{3}+1}}.$$

Case 2: $\ell \equiv 4 \pmod{9}$. Again, let $g \in \mathbb{Z}$ be a primitive root of 1 modulo ℓ . Consider the sum

$$\begin{aligned} L_2(u) &:= \text{Sl}(g^3 u)^{-1} + \text{Sl}(g^6 u)^{-1} + \cdots + \text{Sl}(g^{\frac{\ell-1}{2}} u)^{-1} \\ &\quad + \text{Sl}(-g^3 u)^{-1} + \text{Sl}(-g^6 u)^{-1} + \cdots + \text{Sl}(-g^{\frac{\ell-1}{2}} u)^{-1}. \end{aligned}$$

By noting that $g^{\frac{\ell-1}{2}} \equiv -1 \pmod{\ell}$, we have $\ker(\chi_{\lambda}) = \{g^{3j}, -g^{3j} \pmod{\ell} \mid j = 1, \dots, \frac{\ell-1}{6}\}$. By this fact and Lemma 11 (b), we have

$$G_{\lambda}(\chi_{\lambda}, \varphi^{-1}) = \sum_{j=1}^{\frac{\ell-1}{6}} \left(\text{Sl}\left(\frac{-3\varpi_1 g^{3j}}{\lambda}\right)^{-1} + \text{Sl}\left(\frac{3\varpi_1 g^{3j}}{\lambda}\right)^{-1} \right) = L_2\left(\frac{-3\varpi_1}{\lambda}\right).$$

By Equation (10),

$$L_2(u) = 2 \sum_{m=0}^{\infty} D_{6m+2} \left(\sum_{j=1}^{\frac{\ell-1}{6}} g^{3(6m+2)j} \right) t^{6m+2} \left(\sum_{n=0}^{\infty} (-1)^n \binom{-\frac{2}{3}}{n} \frac{t^{3n}}{3n+1} \right)^{6m+2}.$$

By Lemma 5 and the definition of L_2 , the coefficients of this expansion in terms of t belong to $\mathbb{Z}[\frac{1}{g^{3j}}, \frac{1}{3} : j = 1, \dots, \frac{\ell-1}{6}]$, in particular, to $\mathbb{Z}_{(\ell)}$. Here, we substitute Λ for t (which corresponds to the substitution of $\frac{-3\varpi_1}{\lambda}$ for u), then, $\text{Sl}(\nu u) \mapsto \text{Sl}(\frac{-3\varpi_1 \nu}{\lambda})$ for any $\nu \in \mathbb{Z}$, by Lemma 5. Therefore,

$$2 \sum_{m=0}^{\infty} D_{6m+2} \left(\sum_{j=1}^{\frac{\ell-1}{6}} g^{3(6m+2)j} \right) \Lambda^{6m+2} \left(\sum_{n=0}^{\infty} (-1)^n \binom{-\frac{2}{3}}{n} \frac{\Lambda^{3n}}{3n+1} \right)^{6m+2}$$

converges Λ -adically in $\mathcal{O}_{\lambda, \Lambda}$ and is equal to $G_{\lambda}(\chi_{\lambda}, \varphi^{-1})$. By noting that

$$(-1)^n \binom{-\frac{2}{3}}{n} \frac{1}{3n+1} \in \mathbb{Z}_{(\ell)}$$

for $n \leq \frac{2(\ell-4)}{9}$ (since $\binom{-\frac{2}{3}}{n} \in \mathbb{Z}[\frac{1}{3}]$ and $3n+1 \leq \frac{2\ell-3}{3} < \ell$) and the fact that $D_{6m+2} \in \mathbb{Z}_{(\ell)}$ for $m \leq \frac{\ell-4}{9}$ (since $D_{6m+2} = \frac{d_{6m+2}}{(6m+2)!}$, $6m+2 < \ell$, and $d_{6m+2} \in \mathbb{Z}_{(\ell)}$)

(Lemma 8)), and that the coefficients of this expansion in terms of Λ belong to $\mathbb{Z}[\frac{1}{3}]$, we have

$$G_\lambda(\chi_\lambda, \varphi^{-1}) \equiv 2 \sum_{m=0}^{\frac{\ell-4}{9}} D_{6m+2} \left(\sum_{j=1}^{\frac{\ell-1}{6}} g^{3(6m+2)j} \right) \Lambda^{6m+2} \\ \times \left(\sum_{n=0}^{\frac{2(\ell-4)}{9}} (-1)^n \binom{-\frac{2}{3}}{n} \frac{\Lambda^{3n}}{3n+1} \right)^{6m+2} \pmod{\Lambda^{\frac{2(\ell-1)}{3}+1}}.$$

We also have

$$\sum_{j=1}^{\frac{\ell-1}{6}} g^{3(6m+2)j} \equiv_{\pmod{\ell}} \begin{cases} 0 & \text{if } \ell-1 \nmid 3(6m+2) \\ \frac{\ell-1}{6} & \text{if } \ell-1 \mid 3(6m+2). \end{cases}$$

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

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

□

Example 1. (a) Let $\ell = 7$ and $\lambda = 1 + 3\rho$. By Table 1, we have $C_4 = -\frac{1}{6}$. Then,

$$-\frac{1}{3}C_{\frac{2(\ell-1)}{3}} = -\frac{1}{3}C_4 = \frac{1}{18} \equiv 2 \pmod{7}.$$

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 [1, Table 1, p. 117].

(b) $\ell = 13$ and $\lambda = 4 + 3\rho$. By Table 3, $D_8 = -\frac{1}{4536} \equiv 1 \pmod{13}$. Then,

$$-\frac{1}{3}D_{\frac{2(\ell-1)}{3}} = -\frac{1}{3}D_8 \equiv -\frac{1}{3} \equiv -3^2 \pmod{13}.$$

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

Lemma 12. *We have*

$$|\alpha_\lambda|^2 \equiv_{\pmod{\lambda}} \begin{cases} \left(\overline{\chi_\lambda(3)} C_{\frac{2(\ell-1)}{3}} \right)^2 / 9 & \text{if } \ell \equiv 7 \pmod{9} \\ \left(\chi_\lambda(3) D_{\frac{2(\ell-1)}{3}} \right)^2 / 9 & \text{if } \ell \equiv 4 \pmod{9}. \end{cases}$$

We also have

$$|\alpha_\lambda|^2 \equiv_{\pmod{\ell}} \begin{cases} \left(3^{\frac{\ell-7}{6}} C_{\frac{2(\ell-1)}{3}} \right)^2 & \text{if } \ell \equiv 7 \pmod{9}, \\ \left(3^{\frac{\ell-4}{3}} D_{\frac{2(\ell-1)}{3}} \right)^2 & \text{if } \ell \equiv 4 \pmod{9}. \end{cases}$$

Proof. Let $\ell \equiv 7 \pmod 9$. We have $\alpha_\lambda^2 \equiv \left(C_{\frac{2(\ell-1)}{3}}\right)^2 / 9 \pmod \lambda$ by Theorem 3. We can take $a_\lambda \in 1 + 3\mathbb{Z}$ as $\alpha_\lambda = \chi_\lambda(3)a_\lambda$ by Theorem 5. Then, $\alpha_\lambda^2 = \overline{\chi_\lambda(3)}a_\lambda^2$ and $|\alpha_\lambda|^2 = a_\lambda^2$ hold. Therefore, we have

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

Since $\overline{\chi_\lambda(3)}^2 = \chi_\lambda(3) \equiv 3^{\frac{\ell-1}{3}} = 9 \cdot (3^{\frac{\ell-7}{6}})^2 \pmod \lambda$ and the fact that both $|\alpha_\lambda|^2$ and $\left(3^{\frac{\ell-7}{6}}C_{\frac{2(\ell-1)}{3}}\right)^2$ belong to $\mathbb{Q}$, the second congruence in the case where $\ell \equiv 7 \pmod 9$ is proved.

The case where $\ell \equiv 4 \pmod 9$ is proved similarly to the case where $\ell \equiv 7 \pmod 9$. $\square$

Remark 4. It seems that the statement of [10, Corollary 2.16], which is the counterpart of Lemma 12 for the Gaussian integers case, should be written as

$$|\alpha_\lambda|^2 \equiv_{\pmod \ell} \begin{cases} \left(\frac{1}{4}C_{\frac{3(\ell-1)}{4}}\right)^2 & \ell \equiv 13 \pmod{16}, \\ -\left(\frac{1}{4}D_{\frac{3(\ell-1)}{4}}\right)^2 & \ell \equiv 5 \pmod{16}. \end{cases}$$

4. Elliptic Gauss Sums and Elliptic Curves Associated with Them

In this section, we study certain Hecke characters, Hecke L -series associated with them, certain elliptic curves $\mathcal{E}_\lambda$ for λ , and their L -functions relevant to our elliptic Gauss sums.

In Subsection 4.1, we define appropriate Hecke characters and the Hecke L -series associated with them. In Subsection 4.2, we introduce certain elliptic curves $\mathcal{E}_\lambda$ for λ and show that their L -functions correspond to the Hecke L -series defined in Subsection 4.1. In Subsection 4.3, by using the coefficient of the elliptic Gauss sum, we show that the order of the Tate–Shafarevich group of $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$ is congruent to the Bernoulli–Hurwitz-type number modulo ℓ . We also obtain unconditional results.

Let $\ell, \lambda, \tilde{\lambda}, \chi_\lambda, W$, and W' be as in Section 2.

4.1. Hecke L -series

We introduce appropriate Hecke characters and the Hecke L -series associated with them.

Following [1, Section 1.4.1], we define

$$\widetilde{\chi_\lambda}((\nu)) := \chi_1(\nu)\overline{\nu}, \quad \chi_1 := \begin{cases} \chi_\lambda \cdot \overline{\chi_0} & \text{for } \ell \equiv 7 \pmod 9, \\ \chi_\lambda \cdot \chi'_0 & \text{for } \ell \equiv 4 \pmod 9, \end{cases}$$

where $\chi_0 : (\mathbb{Z}[\rho]/(3))^\times \xrightarrow{\sim} W$ and $\chi'_0 : (\mathbb{Z}[\rho]/(\sqrt{-3}))^\times \xrightarrow{\sim} \{\pm 1\}$ are natural isomorphisms. Note that $\widetilde{\chi}_\lambda((\nu))$ is independent of the choice of a generator ν of the ideal (ν) . The Hecke L -series associated with the Hecke character $\widetilde{\chi}_\lambda$ is

$$L(\widetilde{\chi}_\lambda, s) = \prod_{(\mu): \text{ prime ideal}} (1 - \widetilde{\chi}_\lambda((\mu))(\mu\bar{\mu})^{-s})^{-1}$$

for $\ell \equiv 7, 4 \pmod{9}$. Since $\chi_\lambda(\lambda) = 0$ and $\chi_0(1 - \rho) = \chi'_0(1 - \rho) = 0$, we may write this as

$$L(\widetilde{\chi}_\lambda, s) = \prod_{\substack{\mu: \text{ primary prime} \\ \mu \neq \lambda, 1-\rho}} (1 - \chi_\lambda(\mu)\bar{\mu}(\mu\bar{\mu})^{-s})^{-1} \quad (13)$$

4.2. L -functions of Elliptic Curves

In this subsection, we introduce certain elliptic curves for λ and give some of their properties, such as their reduction types at prime ideals of $\mathbb{Z}[\rho]$ and the number of the points of the reductions of the elliptic curves. We also show that the Hecke L -series defined in Subsection 4.1 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 the number of rational points of an elliptic curve over a finite field. In this paper, we consider only Jacobi sums of the following form:

- (i) For any primary prime $\mu \in \mathbb{Z}[\rho]$ such that $p = \mu\bar{\mu} \equiv 1 \pmod{3}$ is a prime number and any characters ϕ and χ of $\mathbb{F}_p^\times$, we define the *Jacobi sum* associated with ϕ and χ to be

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

- (ii) For any primary prime $-q \in \mathbb{Z}[\rho]$ such that q is a prime number (automatically satisfying $q \equiv 2 \pmod{3}$) and any characters ϕ and χ of $\mathbb{F}_{q^2}^\times$, we define the *Jacobi sum* associated with ϕ and χ to be

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

Lemma 13. (a) Under the setting of (i) above,

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

holds;

- (b) Under the setting of (ii) above,

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

holds;

(c) If λ_1 and λ_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. For (a), the first equality follows from [6, Lemma in Section 3 of Chap. 18] and the second equality follows from [6, Lemma 1 in Section 4 of Chap. 9]. Note that $-\mu$ is primary in the definition of [6, Section 3 of Chap. 9].

See Theorem 2.3 and Theorem 2.14 in [2] for (b). Also see [9, Theorem 7.8] for (c). Note that, the primarity in Definition 3 implies the primarity in [9, Section 7.1]. $\square$

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 14. For any prime ideal $0 \neq \mathfrak{P} \subset \mathbb{Z}[\rho]$, 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 $K_{\mathfrak{P}}$.

- (a) The elliptic curve $\mathcal{E}_\lambda$ has exactly two bad primes, namely (λ) and $(1 - \rho)$, moreover, $\mathcal{E}_\lambda$ has additive reduction at these primes;
- (b) The special fiber of $\mathcal{E}_\lambda$ at (λ) is of Type IV. The one at $(1 - \rho)$ is of Type IV if $\ell \equiv 7 \pmod{9}$ and, of Type I_0^* if $\ell \equiv 4 \pmod{9}$, in the notation of Kodaira symbols in the Kodaira–Néron classification of the special fibers of Néron models;
- (c) For any prime ideal $0 \neq \mathfrak{P} \subset \mathbb{Z}[\rho]$, let $\mathcal{E}/R_{\mathfrak{P}}$ be the Néron model of $\mathcal{E}_\lambda \times_{\mathbb{Q}(\rho)} K_{\mathfrak{P}}$, $\tilde{\mathcal{E}}/k_{\mathfrak{P}} = \mathcal{E} \times_{R_{\mathfrak{P}}} k_{\mathfrak{P}}$ the special fiber of $\mathcal{E}$, $\tilde{\mathcal{E}}^0/k_{\mathfrak{P}}$ be the identity component of the group variety $\tilde{\mathcal{E}}/k_{\mathfrak{P}}$, and $\tau_{\mathfrak{P}}$ be the order of the group of components $\tilde{\mathcal{E}}(k_{\mathfrak{P}})/\tilde{\mathcal{E}}^0(k_{\mathfrak{P}})$. Then, we have

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

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

- (d) For a primary prime $\mu \in \mathbb{Z}[\rho]$ such that $p = \mu\bar{\mu}$ is a prime number with $\mu \neq \lambda$, we have

$$\#(\mathcal{E}_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = p + 1 - (\chi_\lambda(\mu)\bar{\mu} + \overline{\chi_\lambda(\mu)}\mu),$$

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

(e) For a prime number $q \equiv 2 \pmod{3}$, 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 $R_{(-q)}$;

(f) We have

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

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

Remark 5. For (f), we can show, moreover, that $\mathcal{E}_\lambda(\mathbb{Q}(\rho)) = \mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}}$ 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 15, which is proved without Lemma 14 (f). From [4, 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 of Lemma 14. To show that (a) holds, we see that applying 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 elliptic curve has discriminant $\Delta = -27\lambda^4$ and invariant $c_4 = 0$. Here c_4 is the invariant of an elliptic curve defined as follows (See [13, Chap. III. 1]). For an elliptic curve in Weierstrass form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

define

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3,$$

Then c_4 is defined by

$$c_4 = b_2^2 - 24b_4.$$

Thus $(\Delta) = (1 - \rho)^6(\lambda)^4$ as ideals in $\mathbb{Z}[\rho]$. This is a global minimal Weierstrass equation of $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$, by [13, Chap. VII, Remark 1.1]. Note that the Weierstrass equation $y^2 = x^3 + \frac{\lambda^2}{4}$ is minimal at every prime except (2). Hence, $\mathcal{E}_\lambda$ has exactly two bad primes, namely (λ) and $(1 - \rho)$, and it has additive reduction at these primes, by [13, 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 [12, Chap. II, Theorem 6.1]. By [13, Chap. VII, Proposition 5.5], $\mathcal{E}_\lambda$ has potential good reduction at every prime. By [13, Chap. VII, Proposition 5.4 (b)], $\mathcal{E}_\lambda$ does not have multiplicative reductions. Parts (b) and (c) hold by the calculations in [12, Chap. IV, Tate's Algorithm 9.4].

We will show that (d) holds. The equation $y^2 = x^3 + \frac{\lambda^2}{4}$ is the minimal Weierstrass equation at the prime ideal (μ) . Let $\phi : \mathbb{F}_p^\times \rightarrow \{\pm 1\}$ be the quadratic residue symbol and $\chi : \mathbb{F}_p^\times \rightarrow W'$ be the cubic residue symbol. Let $D_1 \in \mathbb{F}_p$ be the image of $\frac{\lambda^2}{4}$ in $\mathbb{Z}[\rho]/(\mu) \simeq \mathbb{F}_p$. Note that $D_1 \neq 0$, $\phi(D_1) = 1$, and $\chi(-1) = 1$. Then, we have

$$\begin{aligned} \#(\mathcal{E}_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) &= 1 + \#\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + D_1\} \\ &= 1 + \sum_{\substack{u, v \in \mathbb{F}_p \\ u+v=D_1}} \#\{y \in \mathbb{F}_p \mid y^2 = u\} \cdot \#\{x \in \mathbb{F}_p \mid x^3 = -v\} \\ &= 1 + \sum_{\substack{u, v \in \mathbb{F}_p \\ u+v=D_1}} (1 + \phi(u))(1 + \chi(-v) + \overline{\chi(-v)}) \\ &= p + 1 + \sum_{\substack{u, v \in \mathbb{F}_p \\ u+v=D_1}} \phi(u)(\chi(-v) + \overline{\chi(-v)}) \\ &= p + 1 \\ &\quad + \phi(D_1)\chi(D_1) \sum_{\substack{u, v \in \mathbb{F}_p \\ u+v=1}} \phi(u)\chi(v) + \phi(D_1)\overline{\chi(D_1)} \sum_{\substack{u, v \in \mathbb{F}_p \\ u+v=1}} \phi(u)\chi(v) \\ &= p + 1 + \chi(D_1)J(\phi, \chi) + \overline{\chi(D_1)J(\phi, \chi)}. \end{aligned}$$

By Lemma 13 (a), we have $\#(\mathcal{E}_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = p + 1 - (\chi(D_1)\chi(4)\mu + \overline{\chi(D_1)\chi(4)\mu})$. By noting that $\left(\frac{\cdot}{\mu}\right)_3 : (\mathbb{Z}[\rho]/(\mu))^\times \simeq \mathbb{F}_p^\times \xrightarrow{\chi} W'$ and $\left(\frac{\lambda}{\mu}\right)_3 = \left(\frac{\mu}{\lambda}\right)_3 = \chi_\lambda(\mu)$ (Lemma 13 (c)), we have $\chi(4D_1) = \left(\frac{\lambda}{\mu}\right)_3^2 = \overline{\left(\frac{\lambda}{\mu}\right)_3} = \overline{\chi_\lambda(\mu)}$. Thus, $\#(\mathcal{E}_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = p + 1 - (\overline{\chi_\lambda(\mu)}\mu + \chi_\lambda(\mu)\overline{\mu})$ holds.

To show that (e) holds, for $q \neq 2$, we can see that the equation $y^2 = x^3 + \frac{\lambda^2}{4}$ is the minimal Weierstrass equation at the prime ideal $(-q)$. Let $\phi : \mathbb{F}_{q^2}^\times \rightarrow \{\pm 1\}$ be the quadratic residue symbol and $\chi : \mathbb{F}_{q^2}^\times \rightarrow W'$ be the cubic residue symbol. Let $D_2 \in \mathbb{F}_{q^2}$ be the image of $\frac{\lambda^2}{4}$ in $\mathbb{Z}[\rho]/(-q) \simeq \mathbb{F}_{q^2}$. Note that $D_2 \neq 0$, $\phi(D_2) = 1$, and $\chi(-1) = 1$. Then, we have

$$\begin{aligned} \#(\mathcal{E}_\lambda \otimes \mathbb{F}_{q^2})(\mathbb{F}_{q^2}) &= 1 + \#\{(x, y) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \mid y^2 = x^3 + D_2\} \\ &= 1 + \sum_{\substack{u, v \in \mathbb{F}_{q^2} \\ u+v=D_2}} \#\{y \in \mathbb{F}_{q^2} \mid y^2 = u\} \cdot \#\{x \in \mathbb{F}_{q^2} \mid x^3 = -v\} \\ &= 1 + \sum_{\substack{u, v \in \mathbb{F}_{q^2} \\ u+v=D_2}} (1 + \phi(u))(1 + \chi(-v) + \overline{\chi(-v)}) \\ &= q^2 + 1 + \sum_{\substack{u, v \in \mathbb{F}_{q^2} \\ u+v=D_2}} \phi(u)(\chi(-v) + \overline{\chi(-v)}) \end{aligned}$$

$$\begin{aligned}
 &= q^2 + 1 + \phi(D_2) \left(\chi(D_2) \sum_{\substack{u, v \in \mathbb{F}_{q^2} \\ u+v=1}} \phi(u)\chi(v) + \overline{\chi(D_2)} \overline{\sum_{\substack{u, v \in \mathbb{F}_{q^2} \\ u+v=1}} \phi(u)\chi(v)} \right) \\
 &= q^2 + 1 + \chi(D_2)J_2(\phi, \chi) + \overline{\chi(D_2)J_2(\phi, \chi)}.
 \end{aligned}$$

By Lemma 13 (b), we have $\#(\mathcal{E}_\lambda \otimes \mathbb{F}_{q^2})(\mathbb{F}_{q^2}) = q^2 + 1 + q(\chi(D_2) + \overline{\chi(D_2)})$. By noting that $\left(\frac{-}{-q}\right)_3 : (\mathbb{Z}[\rho]/(-q))^\times \simeq \mathbb{F}_{q^2}^\times \xrightarrow{\chi} W'$, $\left(\frac{-2}{-q}\right)_3 = \left(\frac{-q}{-2}\right)_3 = 1$, and $\left(\frac{\lambda}{-q}\right)_3 = \left(\frac{-q}{\lambda}\right)_3 = \chi_\lambda(-q) = \chi_\lambda(q)$ (Lemma 13 (c)), we have $\chi(D_2) = \left(\frac{\lambda}{-q}\right)_3^2 = \overline{\left(\frac{\lambda}{-q}\right)_3} = \overline{\chi_\lambda(q)}$. Thus, $\#(\mathcal{E}_\lambda \otimes \mathbb{F}_{q^2})(\mathbb{F}_{q^2}) = q^2 + 1 + q(\chi_\lambda(q) + \overline{\chi_\lambda(q)})$ holds.

Let $q = 2$ and $D_3 \in \mathbb{F}_4$ be the image of λ in $\mathbb{Z}[\rho]/(-2) \simeq \mathbb{F}_4$. Note that $y^2 + \lambda y = x^3$ is the minimal Weierstrass equation at the prime ideal (-2) and $D_3 \neq 0$. For $y \in \mathbb{F}_4$, we have that $y^2 + D_3 y = 1$ if and only if $(D_3 + 1)y = 0$ and $y \neq 0, 1$. Therefore,

$$\begin{aligned}
 \#\{(x, y) \in \mathbb{F}_4^\times \times \mathbb{F}_4 \mid y^2 + D_3 y = 1\} &= 3\#\{y \in \mathbb{F}_4 \mid y^2 + D_3 y = 1\} \\
 &= 3\#\{y \in \mathbb{F}_4 \mid (D_3 + 1)y = 0 \text{ and } y \neq 0, 1\} \\
 &= \begin{cases} 6 & \text{if } D_3 = 1, \\ 0 & \text{if } D_3 \neq 1 \end{cases}
 \end{aligned}$$

holds. Then, by noting that $\#\{y \in \mathbb{F}_4 \mid y^2 + D_3 y = 0\} = \#\{0, -D_3\} = 2$, we have

$$\begin{aligned}
 \#(\mathcal{E}_\lambda \otimes \mathbb{F}_4)(\mathbb{F}_4) &= 1 + \#\{(x, y) \in \mathbb{F}_4 \times \mathbb{F}_4 \mid y^2 + D_3 y = x^3\} \\
 &= 1 + \#\{(x, y) \in \mathbb{F}_4^\times \times \mathbb{F}_4 \mid y^2 + D_3 y = 1\} \\
 &\quad + \#\{y \in \mathbb{F}_4 \mid y^2 + D_3 y = 0\} \\
 &= 3 + \#\{(x, y) \in \mathbb{F}_4^\times \times \mathbb{F}_4 \mid y^2 + D_3 y = 1\} \\
 &= \begin{cases} 9 & \text{if } D_3 = 1, \\ 3 & \text{if } D_3 \neq 1. \end{cases}
 \end{aligned}$$

On the other hand, by Lemma 13 (c), we have

$$\chi_\lambda(2) = \chi_\lambda(-2) = \left(\frac{\lambda}{-2}\right)_3 = \begin{cases} 1 & \text{if } \lambda \equiv 1 \pmod{2}, \\ \rho \text{ or } \bar{\rho} & \text{if } \lambda \equiv \rho \text{ or } \bar{\rho} \pmod{2}. \end{cases}$$

By noting that $\rho + \bar{\rho} = -1$,

$$q^2 + 1 + q(\chi_\lambda(q) + \overline{\chi_\lambda(q)}) = 5 + 2(\chi_\lambda(2) + \overline{\chi_\lambda(2)}) = \begin{cases} 9 & \text{if } \lambda \equiv 1 \pmod{2}, \\ 3 & \text{if } \lambda \equiv \rho \text{ or } \bar{\rho} \pmod{2} \end{cases}$$

holds. Since we have that $\lambda \equiv 1 \pmod{2}$ if and only if $D_3 = 1$, we conclude

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

for $q = 2$.

Finally, we will prove (f). If $\infty \neq (x, y) \in \mathcal{E}_\lambda(\mathbb{Q}(\rho))[2]$, then, $y = 0$. Then, $x^3 = -\lambda^2/4$ and $x \in \mathbb{Q}(\rho)$. This is a contradiction. Thus, we have $\mathcal{E}_\lambda(\mathbb{Q}(\rho))[2] = \{\infty\}$.

Let $m \geq 1$ be an integer relatively prime to 5. Then, $\mathcal{E}_\lambda(\mathbb{Q}(\rho))[m]$ has injective homomorphisms to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $(\mathcal{E}_\lambda \otimes \mathbb{F}_{25})(\mathbb{F}_{25})$ by [13, Chap. VII, Proposition 3.1 (b)]. On the other hand, $\#(\mathcal{E}_\lambda \otimes \mathbb{F}_{25})(\mathbb{F}_{25}) = 26 + 5(\chi_\lambda(5) + \overline{\chi_\lambda}(5)) = 36$, or 21 by (e). Thus, for m relatively prime to 2, 3, 5, and 7, we have $\#\mathcal{E}_\lambda(\mathbb{Q}(\rho))[m] = 1$. We also have that $\mathcal{E}_\lambda(\mathbb{Q}(\rho))[m]$ has injective homomorphisms to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $(\mathcal{E}_\lambda \otimes \mathbb{F}_{121})(\mathbb{F}_{121})$ for m relatively prime to 11 by [13, Chap. VII, Proposition 3.1 (b)]. On the other hand, $\#(\mathcal{E}_\lambda \otimes \mathbb{F}_{121})(\mathbb{F}_{121}) = 122 + 11(\chi_\lambda(11) + \overline{\chi_\lambda}(11)) = 144$, or 111 by (e). Thus, for m relatively prime to 2, 3, 11, 37, we have $\#\mathcal{E}_\lambda(\mathbb{Q}(\rho))[m] = 1$.

Therefore, we have $\mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}} = \mathcal{E}_\lambda(\mathbb{Q}(\rho))[3]$. Let $P \in \mathcal{E}_\lambda(\mathbb{Q}(\rho))[3]$ and let $\infty \neq P = (x, y)$. If $y = 0$, we have $P \in \mathcal{E}_\lambda(\mathbb{Q}(\rho))[3] \cap \mathcal{E}_\lambda(\mathbb{Q}(\rho))[2] = \{\infty\}$. This is a contradiction. Thus, we have $y \neq 0$, equivalently, $4x^3 + \lambda^2 \neq 0$. For $Q \in \mathcal{E}_\lambda$, we denote the x -coordinate of Q by $x(Q)$. Then, $x(2P) = \frac{x^4 - 2\lambda^2 x}{4x^3 + \lambda^2}$ and $x(-P) = x$. Since $2P = -P$, we have $\frac{x^4 - 2\lambda^2 x}{4x^3 + \lambda^2} = x$. Thus, $x = 0$ or $x^3 = -\lambda^2$. Since $x \in \mathbb{Q}(\rho)$, we have $x^3 \neq -\lambda^2$. Therefore, $x = 0$. By $P \in \mathcal{E}_\lambda : y^2 = x^3 + \frac{\lambda^2}{4}$, we have $y = \pm \frac{\lambda}{2}$. Thus, we proved $\mathcal{E}_\lambda(\mathbb{Q}(\rho))_{\text{tors}} = \mathcal{E}_\lambda(\mathbb{Q}(\rho))[3] = \{\infty, (0, \pm \frac{\lambda}{2})\}$. $\square$

Proposition 1. *Let $L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s)$ be the Hasse–Weil L -function of the elliptic curve $\mathcal{E}_\lambda : y^2 = x^3 + \frac{\lambda^2}{4}$ over $\mathbb{Q}(\rho)$. The Hecke L -series defined by Equation (13) corresponds to the L -function of the elliptic curve $\mathcal{E}_\lambda$, that is, one has*

$$L(\widetilde{\chi}_\lambda, s)L(\overline{\widetilde{\chi}_\lambda}, s) = L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s). \quad (14)$$

Proof. We recall the Hasse–Weil L -function of the elliptic curve $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$. We define

$$L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s) := \prod_{\mathfrak{P}:\text{prime ideal}} L_{\mathfrak{P}}(\mathcal{E}_\lambda/\mathbb{Q}(\rho), q_{\mathfrak{P}}^{-s})^{-1},$$

where $L_{\mathfrak{P}}(\mathcal{E}_\lambda/\mathbb{Q}(\rho), T)$ is the local L -factor of $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$ at $\mathfrak{P}$ defined as follows. Let $q_{\mathfrak{P}} := \#k_{\mathfrak{P}}$, $a_{\mathfrak{P}} := q_{\mathfrak{P}} + 1 - \#(\mathcal{E}_\lambda \otimes k_{\mathfrak{P}})(k_{\mathfrak{P}})$, if $\mathcal{E}_\lambda$ has good reduction at $\mathfrak{P}$. Then,

$$L_{\mathfrak{P}}(\mathcal{E}_\lambda/\mathbb{Q}(\rho), T) := 1 - a_{\mathfrak{P}}T + q_{\mathfrak{P}}T^2.$$

If $\mathcal{E}_\lambda$ has bad reduction at $\mathfrak{P}$, we define

$$L_{\mathfrak{P}}(\mathcal{E}_\lambda/\mathbb{Q}(\rho), T) := \begin{cases} 1 - T & \text{if } \mathcal{E}_\lambda \text{ has split multiplicative reduction at } \mathfrak{P}, \\ 1 + T & \text{if } \mathcal{E}_\lambda \text{ has non-split multiplicative reduction at } \mathfrak{P}, \\ 1 & \text{if } \mathcal{E}_\lambda \text{ has additive reduction at } \mathfrak{P}. \end{cases}$$

If $\mathfrak{P} = (\mu)$, where $\mu \in \mathbb{Z}[\rho]$ is a primary prime unequal to λ such that $p = \mu\overline{\mu}$ is a prime number, then $k_{\mathfrak{P}} \simeq \mathbb{F}_p$, $q_{\mathfrak{P}} = p$, and $a_{\mathfrak{P}} = \chi_\lambda(\mu)\overline{\mu} + \overline{\chi_\lambda}(\mu)\mu$ hold by Lemma 14 (d). Thus,

$$L_{\mathfrak{P}}(\mathcal{E}_\lambda/\mathbb{Q}(\rho), q_{\mathfrak{P}}^{-s}) = 1 - (\chi_\lambda(\mu)\overline{\mu} + \overline{\chi_\lambda}(\mu)\mu)p^{-s} + p^{1-2s}.$$

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

$$(1 - \chi_\lambda(\mu)\overline{\mu}(\mu\overline{\mu})^{-s})(1 - \overline{\chi_\lambda}(\mu)\mu(\mu\overline{\mu})^{-s}) = 1 - (\chi_\lambda(\mu)\overline{\mu} + \overline{\chi_\lambda}(\mu)\mu)p^{-s} + p^{1-2s}$$

by Equation (13). Therefore, the local L -factor of $L(\widetilde{\chi_\lambda}, s)L(\overline{\widetilde{\chi_\lambda}}, s)$ at $\mathfrak{P}$ coincides with that of $L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s)$ at $\mathfrak{P}$.

Next, if $\mathfrak{P} = (-q)$, where q is a prime number such that $q \equiv 2 \pmod{3}$, then $k_{\mathfrak{P}} \simeq \mathbb{F}_{q^2}$, $q_{\mathfrak{P}} = q^2$, and $a_{\mathfrak{P}} = -q(\chi_\lambda(q) + \overline{\chi_\lambda}(q))$ hold by Lemma 14 (e). Thus,

$$L_{\mathfrak{P}}(\mathcal{E}_\lambda/\mathbb{Q}(\rho), q_{\mathfrak{P}}^{-s}) = 1 + (\chi_\lambda(q) + \overline{\chi_\lambda}(q))q^{1-2s} + q^{2-4s}.$$

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

$$(1 - \chi_\lambda(-q)(\overline{-q})q^{-2s})(1 - \overline{\chi_\lambda}(-q)(-q)q^{-2s}) = 1 + (\chi_\lambda(q) + \overline{\chi_\lambda}(q))q^{1-2s} + q^{2-4s}$$

by Equation (13). Therefore, the local L -factor of $L(\widetilde{\chi_\lambda}, s)L(\overline{\widetilde{\chi_\lambda}}, s)$ at $\mathfrak{P}$ coincides with that of $L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s)$ at $\mathfrak{P}$.

If $\mathfrak{P} = (\lambda)$ or $(1 - \rho)$, then, $\mathcal{E}_\lambda$ has additive reduction at $\mathfrak{P}$ by Lemma 14 (a). Then, both of the local L -factors of $L(\widetilde{\chi_\lambda}, s)L(\overline{\widetilde{\chi_\lambda}}, s)$ and $L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), s)$ are equal to 1. $\square$

4.3. Elliptic Gauss Sums and Tate–Shafarevich Groups

In this subsection, we show that the order of the Tate–Shafarevich group of the elliptic curve $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$ is equal to the square of the absolute value of the coefficient α_λ of the relevant elliptic Gauss sum or its quarter. By combining this and Theorem 3, we obtain that the order of the Tate–Shafarevich group of $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$ is congruent to the square of Bernoulli–Hurwitz-type numbers C_n, D_n times $1/9$ or $1/36$ modulo ℓ .

Lemma 15. *We have*

$$L(\widetilde{\chi_\lambda}, 1) = \begin{cases} -\frac{\varpi_1 \chi_\lambda(3) G_\lambda(\chi_\lambda, \varphi)}{\lambda} = -\frac{\varpi_1 \chi_\lambda(3)}{\widetilde{\lambda}} \alpha_\lambda & \text{if } \ell \equiv 7 \pmod{9}, \\ -\frac{\varpi_1 \overline{\chi_\lambda}(3) G_\lambda(\chi_\lambda, \varphi^{-1})}{\lambda} = -\frac{\varpi_1 \overline{\chi_\lambda}(3)}{\widetilde{\lambda}} \alpha_\lambda & \text{if } \ell \equiv 4 \pmod{9}. \end{cases}$$

Moreover, we have $L(\widetilde{\chi_\lambda}, 1) \neq 0$.

Proof. The lemma follows from [1, Theorem 1.16] and Theorem 5. $\square$

Since we have $\overline{L(\widetilde{\chi_\lambda}, s)} = L(\overline{\widetilde{\chi_\lambda}}, s)$ for $s \in \mathbb{R}$, we have

$$L(\widetilde{\chi_\lambda}, 1)L(\overline{\widetilde{\chi_\lambda}}, 1) = |L(\widetilde{\chi_\lambda}, 1)|^2.$$

Substituting $s = 1$ in Equation (14) and using Lemma 15, we can write

$$L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), 1) = \frac{|\alpha_\lambda|^2}{\ell^{\frac{1}{3}}} \varpi_1^2$$

(note that $\tilde{\lambda}^3 = \lambda$, $(|\tilde{\lambda}|^2)^3 = |\lambda|^2 = \ell$). In particular, $L(\mathcal{E}_\lambda/\mathbb{Q}(\rho), 1) \neq 0$ holds. Hence, by [11, Theorem (i)], we have $\#\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho)) < \infty$. Therefore, by [3], one has the Birch–Swinnerton–Dyer conjecture (b) below on the leading term of the Hasse–Weil L -function for $\mathcal{E}_\lambda/\mathbb{Q}(\rho)$.

We now recall the Birch–Swinnerton–Dyer conjecture.

Conjecture 1 ([14]). Let K be a number field, and let E be an elliptic curve over K . As usual, let r denote the analytic rank of E/K . Then, the Birch–Swinnerton–Dyer conjecture asserts the following:

- (a) The Hasse–Weil L -function $L(E/K, s)$ has a zero at $s = 1$ of order r ;
- (b) The Tate–Shafarevich group $\text{III}(E/K)$ is finite and we have

$$\lim_{s \rightarrow 1} L(E/K, s)(s-1)^{-r} = \Omega_{E/K} \cdot |\Delta_K|^{-1/2} \cdot \frac{\#\text{III}(E/K)R(E/K)}{\#E(K)_{\text{tors}}^2} \cdot \prod_{\mathfrak{p}} \tau_{\mathfrak{p}}, \quad (15)$$

where $\Omega_{E/K}$ is the global period of E/K , Δ_K is the discriminant of K over $\mathbb{Q}$, $R(E/K)$ is the regulator of E/K , and $\tau_{\mathfrak{p}}$ is the local Tamagawa number at a prime $\mathfrak{p}$ of K .

We have seen that for the elliptic curve $E/K = \mathcal{E}_\lambda/\mathbb{Q}(\rho)$, the analytic rank r is equal to 0. Furthermore, we have computed all local Tamagawa numbers $\tau_{\mathfrak{p}}$ and the torsion subgroup $E(K)_{\text{tors}}$. Since $r = 0$, the regulator $R(E/K)$ is defined to be 1. Therefore, it remains to compute the period $\Omega_{E/K}$, after which the order of the Tate–Shafarevich group $\#\text{III}(E/K)$ can be expressed in terms of α_λ .

Proof of Theorem 4. Let us begin by computing $\Omega_{\mathcal{E}_\lambda/\mathbb{Q}(\rho)}$. In general, when K is an imaginary quadratic field, for an elliptic curve E/K , consider a corresponding period lattice in $\mathbb{C}$ of E given by $\omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subset \mathbb{C}$, where we assume that $\text{Im}(\omega_2/\omega_1) > 0$. Then, the period $\Omega_{E/K}$ is given by $\Omega_{E/K} = 2\text{Im}(\overline{\omega_1}\omega_2)$. Thus, we can write $\Omega_{\mathcal{E}_\lambda/\mathbb{Q}(\rho)} = \varpi_\lambda \overline{\varpi_\lambda} \sqrt{3}$. Here, ϖ_λ is a generator of the period lattice in $\mathbb{C}$ of $\mathcal{E}_\lambda$ as a $\mathbb{Z}[\rho]$ -module over $\mathbb{Z}[\rho]$. This does not depend on the choice of ϖ_λ . We put $\tau_\infty := \varpi_\lambda \overline{\varpi_\lambda}$. The substitution $y \mapsto y/2$ gives an equation of the form

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

From this equation, we have $g_\lambda := \sum_{0 \neq \omega \in \varpi_\lambda \mathbb{Z}[\rho]} 1/\omega^6 = -\lambda^2/140$ by [13, Theorem 3.5 (b) of Chap. VI]. On the other hand, by Lemma 2 (c), $g_1 := \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} 1/\omega^6 = 27/140$ by [13, Theorem 3.5 (b) of Chap. VI]. Thus, we have $\varpi_\lambda^6/\varpi_1^6 = g_1/g_\lambda = -27/\lambda^2$. By taking the absolute values, $\tau_\infty^3 = 3^3 \ell^{-1} \varpi_1^6$ since $\ell = \lambda \overline{\lambda} = |\lambda|^2$. Then, we have

$$\Omega_{\mathcal{E}_\lambda/\mathbb{Q}(\rho)} = \tau_\infty \sqrt{3} = 3\sqrt{3} \varpi_1^2 \ell^{-1/3}.$$

Since the discriminant of $\mathbb{Q}(\rho)$ is -3 , all terms in Equation (15) other than

$$\#\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho))$$

have now been computed. It follows that the claim of the theorem holds. $\square$

Remark 6. The condition $n \equiv 0 \pmod{3}$ is equivalent to $\chi_\lambda(3) = 1$, by the second supplementary law of the cubic reciprocity law and $\chi_\lambda(3) = \rho^n$ by the last formula in [9, Chap. 7, Theorem 7.8], where n is as in Theorem 4. Note that the definition of primarity in [9, Section 7.1] is slightly different from the one in this paper, however, it does not affect the above equivalence. Hence, if $\ell \equiv 7, 4 \pmod{9}$ and $n \equiv 0 \pmod{3}$, we have $\alpha_\lambda \in \mathbb{Z}$ by Theorem 5. We have $2 \mid \alpha_\lambda$ if $\ell \equiv 4 \pmod{9}$ and $n \equiv 0 \pmod{3}$ by Theorem 4. However, by the case of $p = 139$ in Asai's table [1, Table 1. in p.117], we cannot replace “if” with “if and only if”.

Corollary 2. Let $\lambda = 3m + 1 + 3n\rho$ with $m, n \in \mathbb{Z}$ as in Theorem 4. Then we have

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

or

$$\#\text{III}(\mathcal{E}_\lambda/\mathbb{Q}(\rho)) \equiv_{\text{mod } \ell} \begin{cases} \left(3^{\frac{\ell-4}{3}} D_{\frac{2(\ell-1)}{3}} \right)^2 / 4 & \text{if } \ell \equiv 4 \pmod{9} \text{ and } n \equiv 0 \pmod{3} \\ \left(3^{\frac{\ell-4}{3}} D_{\frac{2(\ell-1)}{3}} \right)^2 & \text{if } \ell \equiv 4 \pmod{9} \text{ and } n \equiv \pm 1 \pmod{3} \\ \left(3^{\frac{\ell-7}{6}} C_{\frac{2(\ell-1)}{3}} \right)^2 & \text{if } \ell \equiv 7 \pmod{9}. \end{cases}$$

Proof. These congruences hold from Theorem 3, Theorem 4, and Lemma 12. $\square$

Acknowledgment. The author would like to express his great gratitude to his advisors, Professors Akio Tamagawa and Go Yamashita, during his master's course for their careful and constant advice for the study of this paper. In particular, 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.

References

- [1] T. Asai, Elliptic Gauss sums and Hecke L -values at $s = 1$, in *Proceedings of the Symposium on Algebraic Number Theory and Related Topics*, vol. B4 of *RIMS Kôkyûroku Bessatsu*, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007, 79-121.

- [2] B. C. Berndt and R. J. Evans, Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer, *Illinois J. Math.* **23** (3) (1979), 374-437.
- [3] A. Burungale and M. Flach, The conjecture of Birch and Swinnerton-Dyer for certain elliptic curves with complex multiplication, *Camb. J. Math.* **12** (2) (2024), 357-415.
- [4] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **39** (3) (1977), 223dd-251.
- [5] A. Hurwitz, Über die Anzahl der Classen binärer quadratischer formen von negativer Determinante, *Acta Math.* **19** (1) (1895), 351-384.
- [6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1990.
- [7] N. M. Katz, The congruences of Clausen-von Staudt and Kummer for Bernoulli-Hurwitz numbers, *Math. Ann.* **216** (1975), 1-4.
- [8] K. Kodaira, *Complex Manifolds and Deformation of Complex Structures*, Springer-Verlag, Berlin, 2005.
- [9] F. Lemmermeyer, *Reciprocity laws*, Springer-Verlag, Berlin, 2000.
- [10] Y. Ônishi, Congruence relations connecting Tate-Shafarevich groups with Hurwitz numbers, *Interdiscip. Inform. Sci.* **16** (1) (2010), 71-86.
- [11] K. Rubin, The “main conjectures” of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** (1) (1991), 25-68.
- [12] *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.
- [13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Dordrecht, 2009.
- [14] J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, in *Séminaire Bourbaki, Vol. 9*, Soc. Math. France, Paris, 1995, 415-440.
- [15] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, 1997.
- [16] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, Cambridge University Press, Cambridge, 1996.

Appendix

In this section, 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 Subsection A1, we show lemmas on prime numbers dividing the denominator of d_n . In Subsection A2, we determine the signs and the nonvanishing of C_n , D_n (excluding D_{6n+2}), and the Eisenstein series G_n associated with the lattice $\varpi_1\mathbb{Z}[\rho]$ (see Lemma 16) by using new recurrence relations arising from new formulae of Sl. In Subsection A3, we give numerical tables of c_n , d_n , G_n , and BH_n .

A1. On the Denominator of d_n

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

Lemma 16. *Let*

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

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

$$\sum_{k=0}^m D_{6k+2}(6m-6k-1)G_{6(m-k)}3^{6k} = 0 \text{ and } D_{6m-1} = \frac{(-1)^m 3^{3m-1} - 1}{2 \cdot 3^{6m-1}} G_{6m}. \quad (16)$$

The second equality of Equation (16) holds for $m = 0$ as well, where $G_0 := -1$.

Proof. First, we note that $G_{6n} \in \mathbb{Q}$ for $n \geq 0$, by the fact that $\wp(u) = \frac{1}{u^2} + \sum_{n=1}^{\infty} (6n-1)G_{6n}u^{6n-2}$ around $u = 0$ (note that $G_n = 0$ unless n is congruent to 0 modulo 6) and $\wp'' = 6\wp^2$. Next, we prove the first equation in (16). By Lemma 3 (g), we have

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

Around $u = 0$, we have

$$\wp(u) = \sum_{n=0}^{\infty} (6n-1)G_{6n}u^{6n-2}$$

by the fact that $G_0 = -1$. By Equation (7), we have

$$\frac{1}{\text{Sl}(-3u)} + \frac{1}{\text{Sl}(3u)} = 18 \sum_{n=0}^{\infty} D_{6n+2} 3^{6n} u^{6n+2}.$$

Thus, $18 \sum_{n=0}^{\infty} D_{6n+2} 3^{6n} u^{6n} \sum_{n=0}^{\infty} (6n-1)G_{6n}u^{6n} = 3$ follows. By comparing the coefficients of u^{6m} of this equality for $m \geq 1$, the first equality of Equation (16) follows.

Finally, we prove the second equation in (16). By Lemma 3 (h) and the fact that $3 = (1-\rho)(1-\bar{\rho})$, we have

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

Around $u = 0$, we have

$$\zeta(u) = - \sum_{n=0}^{\infty} G_{6n} u^{6n-1}$$

since we write $G_0 = -1$, 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 Equation (7). Thus,

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

follows, since $(1-\rho)^{6n} = (-1)^n 3^{3n}$. By comparing the coefficients of u^{6n-1} of this equality for $n \geq 0$, the second equality of Equation (16) is proved. $\square$

Definition 5. 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 [7].

Lemma 17. For a prime number $\ell \equiv 1 \pmod{3}$ and $m \geq 0$, we define

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

where $\lfloor \cdot \rfloor$ denotes the floor function. Then,

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

Note that the product on the left-hand side is a finite product.

Proof. We write $h_m := \prod_{\substack{\ell: \text{prime} \\ \ell \equiv 1 \pmod{3}}} \ell^{t(\ell, m)} \cdot 2(6m)!D_{6m+2}$ for $m \geq 0$. Since $h_0 = 2D_2 = \frac{1}{3}$ (see Table 3), the lemma holds for $m = 0$. For $m \geq 1$, we assume that $h_k \in \mathbb{Z}[\frac{1}{3}]$ for $k = 0, \dots, m-1$. By the first equality of Equation (16), we have

$$h_m 3^{6m} = - \sum_{k=0}^{m-1} h_k (6m - 6k - 1) \left(\prod_{\substack{\ell: \text{prime} \\ \ell \equiv 1 \pmod{3}}} \ell^{t(\ell, m) - t(\ell, k)} \right) BH_{6(m-k)} \binom{6m}{6k} 3^{6k}. \quad (17)$$

Since the elliptic curve $y^2 = 4x^3 - 27$ has good reduction at ℓ if and only if $\ell \neq 3$ (cf. the proof of Lemma 14 (a)), and has good ordinary reduction at ℓ if and only if

$\ell \equiv 1 \pmod{3}$ (see [12, Chap II, exer. 2.30]), it follows that $\left(\prod_{\substack{\ell: \text{prime} \\ \ell-1|6m \\ \ell \equiv 1 \pmod{3}}} \ell \right) BH_{6m} \in$

$\mathbb{Z}[\frac{1}{3}]$ by [7, Theorem]. In terms of m , $t(\ell, m)$ is nondecreasing. For $k = 0, \dots, m-1$ and a prime number $\ell \equiv 1 \pmod{3}$, if $\ell-1$ divides $6(m-k)$, we have $t(\ell, m) > t(\ell, k)$, since $t(\ell, m) = \left\lfloor \frac{6m}{\ell-1} \right\rfloor = \frac{6(m-k)}{\ell-1} + \left\lfloor \frac{6k}{\ell-1} \right\rfloor > t(\ell, k)$. Therefore, the right hand side of Equation (17) is an element of $\mathbb{Z}[\frac{1}{3}]$. $\square$

Remark 7. Numerically, we guess that

$$BH_{6m} \in \mathbb{Z}_{(3)},$$

where $\mathbb{Z}_{(3)}$ is the localization of $\mathbb{Z}$ by the prime ideal $3\mathbb{Z}$ (see Table 2). If this is true, then a proof similar to that of Lemma 17 implies that

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

where let $L(m) := \prod_{\substack{\ell: \text{prime} \\ \ell \equiv 1 \pmod{3}}} \ell^{t(\ell, m)}$.

Lemma 18. For $m \geq 0$, we have $d_{6m+2} \in \mathbb{Z}[\frac{1}{3}]$.

Proof. By Lemma 8, we can write $2d_{6m+2} = \frac{N_m}{3^{r(m)}}$, $r(m) \geq 0$, $N_m \in \mathbb{Z}$. By Lemma 17, we have $2L(m) \cdot \frac{d_{6m+2}}{(6m+1)(6m+2)} \in \mathbb{Z}[\frac{1}{3}]$. Thus, $L(m) \cdot \frac{N_m}{(6m+1)(6m+2)} \cdot \frac{1}{3^{r(m)}} \in \mathbb{Z}[\frac{1}{3}]$ holds. Then, we have $(6m+1)(6m+2)|L(m) \cdot N_m$, since $6m+1$ and $6m+2$ are relatively prime to 3. In particular, we have $2|N_m$, since 2 does not divide $L(m)$. Therefore, the lemma is proved. $\square$

Lemma 19. (a) We have

$$\frac{1}{\text{Sl}(\sqrt{-3}u)} + \frac{1}{\text{Sl}(-\sqrt{-3}u)} = -\frac{\text{Sl}(u)^2}{\text{Cl}(u)} = \text{Sl}(-u) \text{Sl}(u) \in \mathcal{H}_{\mathbb{Z}};$$

(b) The rational number d_{6n+2} satisfies

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

Proof. We have

$$\frac{1}{\text{Sl}(\sqrt{-3}u)} = \frac{1 + \bar{\rho} \text{Sl}(u)^3}{\sqrt{-3} \text{Sl}(u) \text{Cl}(u)}$$

by [1, 2.(viii) of Appendix] or putting $u := \rho u$ and $v := -\bar{\rho}u$ of the addition formula of Sl (Lemma 4). By $\text{Sl}(-u) = -\frac{\text{Sl}(u)}{\text{Cl}(u)}$ and $\text{Cl}(-u) = \frac{1}{\text{Cl}(u)}$ (Lemma 3 (g)), 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 $\rho - \bar{\rho} = \sqrt{-3}$, the first equality of (a) is proved. The second equality of (a) also follows from $\text{Sl}(-u) = -\frac{\text{Sl}(u)}{\text{Cl}(u)}$ (Lemma 3 (g)). By Lemma 7, $\text{Sl}(u), \text{Sl}(-u) \in \mathcal{H}_{\mathbb{Z}}$. Thus, $\text{Sl}(u) \text{Sl}(-u) \in \mathcal{H}_{\mathbb{Z}}$.

By Equation (7), we have

$$\frac{1}{\text{Sl}(\sqrt{-3}u)} + \frac{1}{\text{Sl}(-\sqrt{-3}u)} = 2 \sum_{n=0}^{\infty} d_{6n+2}(-3)^{3n+1} \frac{u^{6n+2}}{(6n+2)!}.$$

By (a), we have $2d_{6n+2}(-3)^{3n+1} \in \mathbb{Z}$. By Lemma 18, $d_{6n+2}(-3)^{3n+1} \in \mathbb{Z}$. Thus, we also have (b). $\square$

Lemma 20. *For $m \geq 1$, we have*

$$2m \left(\prod_{\substack{\ell: \text{prime} \\ \ell-1|6m \\ \ell \equiv 1 \pmod{3}}} \ell \right) d_{6m-1} \in \mathbb{Z}[\frac{1}{3}].$$

Proof. From the second equation in (16), for $m \geq 1$, we have

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

Since $(-1)^m 3^{3m-1} - 1 \equiv 2 \pmod{4}$, we have $\frac{(-1)^m 3^{3m-1} - 1}{2} \in \mathbb{Z}$. From [7, Theorem],

$$\left(\prod_{\substack{\ell: \text{prime} \\ \ell-1|6m \\ \ell \equiv 1 \pmod{3}}} \ell \right) BH_{6m} \in \mathbb{Z}[\frac{1}{3}].$$

Then, $2m \left(\prod_{\substack{\ell: \text{prime} \\ \ell-1|6m \\ \ell \equiv 1 \pmod{3}}} \ell \right) d_{6m-1} \in \mathbb{Z}[\frac{1}{3}]$ holds. $\square$

A2. On the Signs and the Nonvanishing of C_n, D_n , and G_n

In this subsection, 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 nonvanishing of G_n, BH_{6n} , and D_{6n-1} .

Lemma 21. *For $n \geq 2$, we have*

$$(6n-1)\{(6n-2)(6n-3)-12\}G_{6n} = 6 \sum_{k=1}^{n-1} (6k-1)(6n-6k-1)G_{6k}G_{6(n-k)} \quad (18)$$

and $G_{6n} > 0$; hence $BH_{6n} > 0$ for $n \geq 1$. 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 $\wp'' = 6\wp^2$ and $\wp(u) = \sum_{n=0}^{\infty} (6n-1)G_{6n}u^{6n-2}$, for $n \geq 1$, we have

$$\begin{aligned} (6n-1)(6n-2)(6n-3)G_{6n} &= 6 \sum_{\substack{m+k=n \\ k,m \geq 0}} G_{6k}(6k-1)G_{6m}(6m-1) \\ &= 6 \sum_{k=1}^{n-1} (6k-1)(6n-6k-1)G_{6k}G_{6(n-k)} \\ &\quad + 12G_{6n}(6n-1). \end{aligned}$$

Here, note that $G_0 = -1$. Thus, we have Equation (18). By the proof of Lemma 2 (c), we have $G_6 = \frac{27}{140} > 0$. The positivity of G_{6n} for $n \geq 1$ follows by induction on n , Equation (18), and the fact that $G_6 > 0$. Then, by the second equation in (16), we have

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

for $m \geq 1$. By the definition of BH_{6m} , we have $BH_{6m} > 0$ for any $m \geq 1$. $\square$

Definition 6. 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 22. (a) For $n \geq 1$,

$$\begin{aligned} 2 \cdot 3^{6n} c_{6n+1} &= 2BH_{6n}(6n+1)(6n-1) - 3^{6n}(6n+1)2n(6n-1)c_{6n-2} \\ &\quad + \sum_{k=1}^n c_{6(n-k)+1} BH_{6k}(6k-1)(6k-2)3^{6(n-k)} \binom{6n+1}{6k} \end{aligned}$$

and

$$\begin{aligned} 2 \cdot 3^{6n} c_{6n+4} &= -(6n+4)(2n+1)(6n+2)3^{6n} c_{6n+1} \\ &\quad + \sum_{k=1}^n c_{6(n-k)+4} BH_{6k}(6k-1)(6k-2)3^{6(n-k)} \binom{6n+4}{6k}; \end{aligned}$$

(b) We have $(-1)^{k+1} c_k > 0$ for $k \geq 1$, that is, $c_{6n+1} > 0$, $c_{6n+4} < 0$ for $n \geq 0$. In other words, all the Hurwitz coefficients for $-\text{Sl}(-u)$ are > 0 . In particular, c_{3n+1} does not vanish;

(c) We set

$$\text{Cl}(u) =: \sum_{n=0}^{\infty} \frac{e_{3n}}{(3n)!} u^{3n}.$$

Then $(-1)^n e_{3n} > 0$ 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 the facts that

$$\text{Sl}(u) = \varphi\left(\frac{u}{-3\varpi_1}\right) = \frac{6\wp\left(\frac{u}{3}\right)}{9 - \wp'\left(\frac{u}{3}\right)}$$

(Lemma 3 (c)) and

$$\wp(u) = \sum_{n=0}^{\infty} G_{6n}(6n-1)u^{6n-2},$$

we have

$$\frac{\text{Sl}(u)}{u} \cdot \left(u^3 - \frac{u^3}{9}\wp'\left(\frac{u}{3}\right)\right) = \left(\frac{u}{3}\right)^2 \cdot 6\wp\left(\frac{u}{3}\right). \quad (19)$$

By also using

$$\frac{\text{Sl}(u)}{u} = \sum_{n=0}^{\infty} C_{3n+1}u^{3n} = \sum_{n=0}^{\infty} C_{6n+1}u^{6n} + \sum_{n=0}^{\infty} C_{6n+4}u^{6n+3}$$

and

$$\wp'(u) = \sum_{n=0}^{\infty} G_{6n}(6n-1)(6n-2)u^{6n-3},$$

we have

$$\begin{aligned} & \left(\sum_{n=0}^{\infty} C_{6n+1}u^{6n} + \sum_{n=0}^{\infty} C_{6n+4}u^{6n+3}\right) \left(u^3 - \sum_{n=0}^{\infty} G_{6n}(6n-1)(6n-2)\frac{u^{6n}}{3^{6n-1}}\right) \\ &= 6 \sum_{n=0}^{\infty} G_{6n}(6n-1)\frac{u^{6n}}{3^{6n}}. \end{aligned} \quad (20)$$

Taking the even part of Equation (20),

$$\begin{aligned} \sum_{n=0}^{\infty} C_{6n+1}u^{6n} \left(-\sum_{n=0}^{\infty} G_{6n}(6n-1)(6n-2)\frac{u^{6n}}{3^{6n-1}}\right) &+ \sum_{n=0}^{\infty} C_{6n+4}u^{6n+3} \cdot u^3 \\ &= 6 \sum_{n=0}^{\infty} G_{6n}(6n-1)\frac{u^{6n}}{3^{6n}} \end{aligned}$$

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 $C_k = c_k/k!$ and $G_{6k} = BH_{6k}/(6k)!$, we also have

$$\begin{aligned} 3^{6n}(6n+1)2n(6n-1)c_{6n-2} &= 2BH_{6n}(6n+1)(6n-1) - 2 \cdot 3^{6n}c_{6n+1} \\ &+ \sum_{k=1}^n c_{6(n-k)+1}BH_{6k}(6k-1)(6k-2)3^{6(n-k)}\binom{6n+1}{6k} \end{aligned}$$

for $n \geq 1$. This is the first equality of (a). Taking the odd part of Equation (20),

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

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,

$$\begin{aligned} (6n+4)(2n+1)(6n+2)3^{6n}c_{6n+1} &= -2 \cdot 3^{6n}c_{6n+4} + \sum_{k=1}^n c_{6(n-k)+4} BH_{6k} \\ &\quad \times (6k-1)(6k-2)3^{6(n-k)} \binom{6n+4}{6k} \end{aligned}$$

follows. This is the second equality of (a).

From Table 1, $c_1 = 1 > 0$ and $c_4 = -4 < 0$. We assume that

$$c_1, c_7, \dots, c_{6(n-1)+1} > 0$$

and

$$c_4, c_{10}, \dots, c_{6(n-1)+4} < 0$$

for some $n \geq 1$. Using the first equality of (a) and $BH_{6n} > 0$ ($n \geq 1$) (by Lemma 21), we have $c_{6n+1} > 0$. We also have $c_{6n+4} < 0$, by the second equality of (a). By induction on n , (b) is proved.

By (b), for all $n \geq 0$, the Hurwitz coefficient for $-\text{Sl}(-u)$ of u^{3n+1} is strictly greater than 0. Since $\text{Cl}'(-u) = -(-\text{Sl}(-u))^2$ for all $n \geq 1$, the Hurwitz coefficient for $\text{Cl}'(-u) = \sum_{n=1}^{\infty} e_{3n}(-1)^{3n-1}u^{3n-1}/(3n-1)!$ is strictly less than 0. Therefore, we have $(-1)^{3n}e_{3n} > 0$. Since $\text{Cl}(0) = 1$, $(-1)^ne_{3n} > 0$ holds for $n \geq 0$. $\square$

Remark 8. 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} .

A3. Numerical Tables of c_n , BH_{6n} , and d_n

n	c_n
1	1
4	-4
7	160
10	-20800
13	6476800
16	-3946624000
19	4161608704000
22	-6974121256960000
25	17455222222028800000
28	-62226770432344883200000
31	304379186781653598208000000
34	-1982049657077223312916480000000
37	16758824127564135479341219840000000
40	-180180787889254711099024290611200000000
43	2419729547280670262758159337861939200000000
46	-39971145354912684332749031990873817088000000000
49	801380022229927863218064428825418221486080000000000
52	-19272532158166604513119104829337619755759042560000000000
55	550209191558546672649809313730688966642337474150400000000000
58	-18474617726618802329201889210788021182113749879750656000000000000

Table 1: c_n

n	BH_n
6	972/7
12	283435200/91
18	90914674752000/133
24	224740203206066380800/91
30	5569206003076317032217600000/217
36	491303185206504946068649519911075840000/447811
42	33314057040643263742571290653335322624000000/301

Table 2: BH_{6n}

n	d_n
2	$1/3$ $= 1/3$
5	$-10/21$ $= -2 \cdot 5/3 \cdot 7$
8	$-80/9$ $= -2^4 \cdot 5/3^2$
11	$48400/273$ $= 2^4 \cdot 5^2 \cdot 11^2/3 \cdot 7 \cdot 13$
14	$70400/3$ $= 2^8 \cdot 5^2 \cdot 11/3$
17	$-2309824000/1197$ $= -2^9 \cdot 5^3 \cdot 11 \cdot 17 \cdot 193/3^2 \cdot 7 \cdot 19$
20	$-2393600000/3$ $= -2^{12} \cdot 5^5 \cdot 11 \cdot 17/3$
23	$46641833216000/273$ $= 2^{11} \cdot 5^3 \cdot 11^2 \cdot 17 \cdot 23 \cdot 3851/3 \cdot 7 \cdot 13$
26	$4350492467200000/27$ $= 2^{16} \cdot 5^5 \cdot 11^2 \cdot 17 \cdot 23 \cdot 449/3^3$
29	$-46343596783616000000/651$ $= -2^{17} \cdot 5^6 \cdot 11^2 \cdot 17 \cdot 23 \cdot 29 \cdot 16493/3 \cdot 7 \cdot 31$
32	$-384236269846528000000/3$ $= -2^{20} \cdot 5^6 \cdot 11^2 \cdot 17 \cdot 23 \cdot 29 \cdot 17093/3$
35	$58356799095178616750080000000/575757$ $= 2^{20} \cdot 5^7 \cdot 11^3 \cdot 17^2 \cdot 23 \cdot 29 \cdot 43 \cdot 1871 \cdot 34511/3^2 \cdot 7 \cdot 13 \cdot 19 \cdot 37$
38	$930458061131469291520000000/3$ $= 2^{24} \cdot 5^7 \cdot 11^3 \cdot 17^2 \cdot 23 \cdot 29 \cdot 701 \cdot 3947/3$
41	$-2526876563810119056660889600000000/6321$ $= -2^{25} \cdot 5^8 \cdot 11^3 \cdot 17^2 \cdot 23 \cdot 29 \cdot 41 \cdot 431 \cdot 42521761/3 \cdot 7^2 \cdot 43$
44	$-17284095511545036218564608000000000/9$ $= -2^{28} \cdot 5^9 \cdot 11^4 \cdot 17^2 \cdot 23 \cdot 29 \cdot 41 \cdot 331 \cdot 881 \cdot 977/3^2$
47	$1027896133477097691463532176998400000000/273$ $= 2^{26} \cdot 5^8 \cdot 11^4 \cdot 17^2 \cdot 23^2 \cdot 29 \cdot 41 \cdot 47 \cdot 313 \cdot 1001523179/3 \cdot 7 \cdot 13$
50	$80306491124224476202875370864640000000000/3$ $= 2^{32} \cdot 5^{10} \cdot 11^5 \cdot 17^2 \cdot 23^2 \cdot 29 \cdot 41 \cdot 47 \cdot 61 \cdot 2029 \cdot 11243/3$
53	$-272275412126083890645192489250796339200000000000/3591$ $= -2^{33} \cdot 5^{11} \cdot 11^4 \cdot 17^3 \cdot 23^2 \cdot 29 \cdot 41 \cdot 47 \cdot 53 \cdot 1201 \cdot 4795973261/3^3 \cdot 7 \cdot 19$
56	$-2287147842776869352629978007993738854400000000000/3$ $= -2^{36} \cdot 5^{11} \cdot 11^5 \cdot 17^3 \cdot 23^2 \cdot 29 \cdot 41 \cdot 47 \cdot 53 \cdot 137 \cdot 4013306567/3$

Table 3: d_n