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

By

Akihiro GOTO

京都大学　数理解析研究所

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

Akihiro GOTO

Abstract

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

Contents

Introduction

There is a classical theorem as follows:

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

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

where B_n and E_n are the n-th Bernoulli and Euler numbers respectively, i.e., $\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$, $\frac{2}{e^t+e^{-t}} = \sum_{n=0}^{\infty} E_n \frac{t^n}{n!}$.

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

$$\#\mathrm{III}(E_\lambda/\mathbb{Q}(i)) \underset{\mathrm{mod}\,\ell}{\equiv} \text{Hurwitz-type number}$$

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

In this paper, we prove an analogue of Onishi's result for the Eisenstein integer ring $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$. To explain the main results of this paper precisely, we first introduce some notation and definitions: let $\rho := e^{\frac{2\pi i}{3}}$, $\varpi_1 := \int_0^1 \frac{dt}{\sqrt[3]{(1-t^3)^2}}$ (the real period of the elliptic curve $y^2 = 4x^3 - 27$; see Lemma 1.2 (3)), and $\varphi(u) := \frac{6\wp(\varpi_1 u)}{9+\wp'(\varpi_1 u)}$, $\mathrm{Sl}(u) := \varphi\left(\frac{u}{-3\varpi_1}\right)$, where $\wp$ is the Weierstrass $\wp$ function with the period lattice $\varpi_1\mathbb{Z}[\rho]$. We define the rational numbers C_n, D_n as

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

(C_{3n+1}, D_{3n+2} have easy recurrence relations, respectively; see the proof of Lemma 1.9 and Remark 1.10.) The rational numbers C_{3n+1}, D_{3n+2} of elliptic functions (with the period lattice $\mathbb{Z}[\rho]$) are analogues of the Bernoulli numbers or the Euler numbers and we call them **Bernoulli-Hurwitz-type numbers**, named after Katz' paper [Ka]. Let ℓ be a rational prime number such that $\ell \equiv 1 \bmod 3$, $\lambda \in \mathbb{Z}[\rho]$ a prime element such that $\ell = \lambda\bar{\lambda}$ and $\lambda \equiv 1 \bmod 3$. We denote by χ_λ the cubic residue character over $(\mathbb{Z}[\rho]/(\lambda))^\times \simeq \mathbb{F}_\ell^\times$ and set $\widetilde{\lambda} := \prod_{\chi_\lambda(\nu)=1} \varphi\left(\frac{\nu}{\lambda}\right)$. (Then $\widetilde{\lambda}^3 = \lambda$ holds; see Lemma 1.15 (2).) Let

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

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

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

The number α_λ is called the **coefficient of the elliptic Gauss sum**. (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 2.3.) The following two theorems are the main results of this paper:

Theorem. (Theorem 2.5) The denominator of $C_{\frac{2}{3}(\ell-1)}$ (resp. $D_{\frac{2}{3}(\ell-1)}$) cannot be divided by ℓ when $\ell \equiv 7 \bmod 9$ (resp. $\ell \equiv 4 \bmod 9$). We have

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

---

[1]By using [R], the main result of [O] can be easily improved in this form.

Theorem. (Theorem 3.6 and Corollary 3.8) We write $\lambda = 3m + 1 + 3n\rho$, $m, n \in \mathbb{Z}$. Then, for the elliptic curve $\mathscr{E}_\lambda : y^2 = x^3 + \frac{\lambda^2}{4}$, we have

$$\#\mathrm{III}(\mathscr{E}_\lambda/\mathbb{Q}(\rho)) = \begin{cases} |\alpha_\lambda|^2/4 & \underset{\mathrm{mod}\ \ell}{\equiv} \left(3^{\frac{\ell-4}{3}} D_{\frac{2(\ell-1)}{3}}\right)^2/4 & \ell \equiv 4 \bmod 9 \text{ and } n \equiv 0 \bmod 3, \\ |\alpha_\lambda|^2 & \underset{\mathrm{mod}\ \ell}{\equiv} \left(3^{\frac{\ell-4}{3}} D_{\frac{2(\ell-1)}{3}}\right)^2 & \ell \equiv 4 \bmod 9 \text{ and } n \equiv \pm 1 \bmod 3, \\ |\alpha_\lambda|^2 & \underset{\mathrm{mod}\ \ell}{\equiv} \left(3^{\frac{\ell-7}{6}} C_{\frac{2(\ell-1)}{3}}\right)^2 & \ell \equiv 7 \bmod 9, \end{cases} \qquad (0.1)$$

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

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

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

$$\text{Bernoulli-Hurwitz-type number} \underset{(1)}{\longleftrightarrow} \text{Elliptic Gauss sum} \underset{(2)}{\longleftrightarrow} \text{Hecke } L\text{-value} \underset{(3)}{\longleftrightarrow} \text{Elliptic } L\text{-value}$$
$$\underset{(4)}{\updownarrow}$$
$$\#\mathrm{III}$$

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

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

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

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

Acknowledgments

1 Elliptic functions

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

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

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

We denote by ϖ_1 (See [A, §1.1.1.]) the real period given by

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

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

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

Lemma 1.1. (The real period and the beta function) $\varpi_1 = \frac{1}{3}B\left(\frac{1}{3}, \frac{1}{3}\right) = \frac{1}{2\pi\sqrt{3}}\Gamma\left(\frac{1}{3}\right)^3 = \frac{2^{\frac{1}{3}}}{3\sqrt{3}}B(\frac{1}{6}, \frac{1}{2})$, where B and Γ denote the beta and gamma functions respectively.

Proof. Let g denote $\Gamma(\frac{1}{3})$. Then we have $\Gamma(\frac{2}{3}) = \frac{2\pi}{\sqrt{3}g}$ by the formula $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$. We also have $\Gamma(\frac{1}{6}) = \frac{\sqrt{3}}{\sqrt{\pi}2^{\frac{1}{3}}}g^2$, since $\Gamma(\frac{1}{6}) = \frac{2\sqrt{\pi}}{2^{\frac{1}{3}}}\frac{\Gamma(\frac{1}{3})}{\Gamma(\frac{2}{3})} = \frac{2\sqrt{\pi}}{2^{\frac{1}{3}}}\frac{g}{2\pi/\sqrt{3}g} = \frac{\sqrt{3}}{\sqrt{\pi}2^{\frac{1}{3}}}g^2$ by putting $s = \frac{1}{6}$ in the formula $\Gamma(s)\Gamma(s+\frac{1}{2}) = \frac{2\sqrt{\pi}}{2^{2s}}\Gamma(2s)$. Then, $B(\frac{1}{6}, \frac{1}{2}) = \frac{\Gamma(\frac{1}{6})\Gamma(\frac{1}{2})}{\Gamma(\frac{2}{3})} = \frac{(\sqrt{3}/\sqrt{\pi}2^{\frac{1}{3}})g^2\sqrt{\pi}}{2\pi/\sqrt{3}g} = \frac{3}{2^{\frac{4}{3}}\pi}g^3$, by the formula $\Gamma(\frac{1}{2}) = \sqrt{\pi}$. By definition and the formula $B(s,t) = \frac{\Gamma(s)\Gamma(t)}{\Gamma(s+t)}$,

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

where $x = t^3$. $\qquad\square$

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

(1) $\wp(\rho u) = \rho\wp(u), \wp(-u) = \wp(u), \wp'(\rho u) = \wp'(u), \wp'(-u) = -\wp'(u)$,

(2) $\wp(\overline{u}) = \overline{\wp(u)}, \wp'(\overline{u}) = \overline{\wp'(u)}$, thus if $u \in \mathbb{R}$, $\wp(u), \wp'(u) \in \mathbb{R}$,

(3) The function $\wp$ satisfies $\wp'^2 = 4\wp^3 - 27$,

(4) $\wp\left(\frac{\varpi_1}{3}\right) = 3, \ \wp\left(\frac{\rho}{3}\varpi_1\right) = 3\rho, \ \wp\left(\frac{\overline{\rho}}{3}\varpi_1\right) = 3\overline{\rho}, \ \wp\left(\frac{1-\rho}{3}\varpi_1\right) = 0$,

(5) $\wp'\left(\frac{\varpi_1}{3}\right) = \wp'\left(\frac{\rho}{3}\varpi_1\right) = \wp'\left(\frac{\overline{\rho}}{3}\varpi_1\right) = -9, \ \wp'\left(\frac{1-\rho}{3}\varpi_1\right) = -3\sqrt{-3}$.

Proof. (1) Since $\wp(u) = \frac{1}{u^2} + \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right)$ and $\rho, -1 \in (\mathbb{Z}[\rho])^\times$,

$$\wp(\rho u) = \frac{1}{(\rho u)^2} + \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \left(\frac{1}{(\rho u - \rho \omega)^2} - \frac{1}{(\rho \omega)^2} \right) = \frac{1}{\rho^2} \left(\frac{1}{u^2} + \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right) \right) = \frac{1}{\rho^2} \wp(u) = \rho \wp(u),$$

$$\wp(-u) = \frac{1}{(-u)^2} + \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \left(\frac{1}{(-u-(-\omega))^2} - \frac{1}{(-\omega)^2} \right) = \frac{1}{u^2} + \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right) = \wp(u).$$

Differentiating both hand sides of $\wp(\rho u) = \rho \wp(u), \wp(-u) = \wp(u)$, we also get $\wp'(\rho u) = \wp'(u), \wp'(-u) = -\wp'(u)$ respectively.

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

(3) $\wp'^2 = 4\wp^3 - 60G_4 \wp - 140G_6$, where $G_6 := \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \frac{1}{\omega^6}$, and

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

Thus, $G_4 = 0$ and $\wp'^2 = 4\wp^3 - 140G_6 = 4(\wp - \wp(\frac{1}{2}\varpi_1))(\wp - \wp(\frac{\rho}{2}\varpi_1))(\wp - \wp(\frac{1+\rho}{2}\varpi_1))$. We denote $e := \wp(\frac{\varpi_1}{2})$. Then, since $\rho e = \wp(\frac{\rho}{2}\varpi_1)$, $\overline{\rho}e = \wp(\frac{\overline{\rho}}{2}\varpi_1) = \wp(-\frac{1+\rho}{2}\varpi_1) = \wp(\frac{1+\rho}{2}\varpi_1)$ by (1), we have $4e^3 = 4\wp(\frac{\varpi_1}{2})\wp(\frac{\rho}{2}\varpi_1)\wp(\frac{1+\rho}{2}\varpi_1) = 140G_6$. We also have, by Lemma 1.1,

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

where $y = x^{-3}$. Hence $4e^3 = 27$.

(4) By (1) and the periodicity of $\wp$, we have $\wp(\frac{1-\rho}{3}\varpi_1) = \wp(\frac{1+2\rho}{3}\varpi_1) = \wp(\frac{(1+\rho)+\rho}{3}\varpi_1) = \wp(\frac{-\rho^2+\rho}{3}\varpi_1) = \rho\wp(\frac{-\rho+1}{3}\varpi_1)$. Hence,

$$\wp\left(\frac{1-\rho}{3}\varpi_1 \right) = 0. \tag{1.1}$$

By $\wp'^2 = 4\wp^3 - 27$, we have

$$\wp'\left(\frac{1-\rho}{3}\varpi_1 \right)^2 = -27. \tag{1.2}$$

In particular, we have

$$\wp'\left(\frac{1-\rho}{3}\varpi_1 \right) \in i\mathbb{R}. \tag{1.3}$$

By putting $u_1 = \frac{1-\rho}{3}\varpi_1$ and $u_2 = \frac{\rho}{3}\varpi_1$ in the addition formula (see, for example, [WW, Chap. XX, 20.3])

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

(1) and (1.1), we have

$$\wp\left(\frac{\varpi_1}{3} \right) = -\wp\left(\frac{1-\rho}{3}\varpi_1 \right) - \wp\left(\frac{\rho}{3}\varpi_1 \right) + \frac{1}{4}\left(\frac{\wp'\left(\frac{1-\rho}{3}\varpi_1 \right) - \wp'\left(\frac{\rho}{3}\varpi_1 \right)}{\wp\left(\frac{1-\rho}{3}\varpi_1 \right) - \wp\left(\frac{\rho}{3}\varpi_1 \right)} \right)^2$$
$$= -\rho\wp\left(\frac{\varpi_1}{3} \right) + \frac{1}{4}\left(\frac{\wp'\left(\frac{1-\rho}{3}\varpi_1 \right) - \wp'\left(\frac{\varpi_1}{3} \right)}{-\rho\wp\left(\frac{\varpi_1}{3} \right)} \right)^2,$$

5

thus, by (1.2),

$$-4\rho\wp\left(\frac{\varpi_1}{3}\right)^3 = (1+\rho)\wp\left(\frac{\varpi_1}{3}\right)4\left(-\rho\wp\left(\frac{\varpi_1}{3}\right)\right)^2 = \left(\wp'\left(\frac{1-\rho}{3}\varpi_1\right) - \wp'\left(\frac{\varpi_1}{3}\right)\right)^2$$

$$= -27 + \wp'\left(\frac{\varpi_1}{3}\right)^2 - 2\wp'\left(\frac{1-\rho}{3}\varpi_1\right)\wp'\left(\frac{\varpi_1}{3}\right). \tag{1.4}$$

By taking the real part of the equation (1.4), we get

$$2\wp\left(\frac{\varpi_1}{3}\right)^3 = -27 + \wp'\left(\frac{\varpi_1}{3}\right)^2 = -27 + 4\wp\left(\frac{\varpi_1}{3}\right)^3 - 27,$$

since (3) and (1.3) and $\wp(\frac{\varpi_1}{3}), \wp'(\frac{\varpi_1}{3}) \in \mathbb{R}$ by (2). Hence we have $\wp(\frac{\varpi_1}{3})^3 = 27$. Since $\wp(\frac{\varpi_1}{3}) \in \mathbb{R}$, we obtain $\wp(\frac{\varpi_1}{3}) = 3$. From $\wp(\frac{\varpi_1}{3}) = 3$ and (1), we get also $\wp\left(\frac{\rho}{3}\varpi_1\right) = 3\rho$ and $\wp\left(\frac{\bar{\rho}}{3}\varpi_1\right) = 3\bar{\rho}$.

(5) The divisor of $\wp'(u)$ is $-3(0) + (\frac{\varpi_1}{2}) + (\frac{\rho\varpi_1}{2}) + (\frac{(1+\rho)\varpi_1}{2}) \pmod{\varpi_1\mathbb{Z}[\rho]}$. Then, the function $(0, \varpi_1) \to \mathbb{R}$, $x \mapsto \wp'(x)$ has a unique zero at $x = \frac{\varpi_1}{2}$, where $(0, \varpi_1)$ is an open interval. Since $\lim_{x \to +0} \wp'(x) = -\infty$ from $\wp'(u) = -\frac{1}{u^3} + \cdots$ around $u = 0$, it holds $\wp'(x) < 0$ for $x \in (0, \frac{\varpi_1}{2})$. Especially $\wp'(\frac{\varpi_1}{3}) < 0$. Since $\wp(\frac{\varpi_1}{3}) = 3$ (by (4)) and $\wp'^2 = 4\wp^3 - 27$ (by (3)), we get $\wp'(\frac{\varpi_1}{3})^2 = 81$. Then, we get $\wp'(\frac{\varpi_1}{3}) = -9$. By (1), we also get $\wp'(\frac{\varpi_1}{3}) = \wp'(\frac{\rho}{3}\varpi_1) = \wp'(\frac{\bar{\rho}}{3}\varpi_1) = -9$. By (1.4) and (4), we get

$$-4\rho\cdot 27 = -4\rho\wp\left(\frac{\varpi_1}{3}\right)^3 = -27 + \wp'\left(\frac{\varpi_1}{3}\right)^2 - 2\wp'\left(\frac{1-\rho}{3}\varpi_1\right)\wp'\left(\frac{\varpi_1}{3}\right) = -27 + (-9)^2 - 2\wp'\left(\frac{1-\rho}{3}\varpi_1\right)(-9).$$

Hence we have $\wp'(\frac{1-\rho}{3}\varpi_1) = \frac{-4\rho\cdot 27 + 27 - (-9)^2}{18} = -3(2\rho + 1) = -3\sqrt{-3}$.

$\square$

Definition 1.3. ([A, Difinition1.1, 1.2] for $\mathsf{Z}, \varphi, \psi$) Let $\zeta(u)$ denote Weierstrass' ζ function associated to the lattice $\varpi_1\mathbb{Z}[\rho]$. We define

$$\mathsf{Z}(u) := \zeta(\varpi_1 u) - \frac{2\pi}{\sqrt{3}\varpi_1}\bar{u},$$

$$\varphi(u) := \frac{1}{3}\left\{\mathsf{Z}\left(u - \frac{1}{3}\right) + \bar{\rho}\mathsf{Z}\left(u - \frac{\rho}{3}\right) + \rho\mathsf{Z}\left(u - \frac{\bar{\rho}}{3}\right)\right\},$$

$$\psi(u) := -\frac{1}{3}\left\{\mathsf{Z}\left(u - \frac{1}{3}\right) + \rho\mathsf{Z}\left(u - \frac{\rho}{3}\right) + \bar{\rho}\mathsf{Z}\left(u - \frac{\bar{\rho}}{3}\right)\right\},$$

$$\mathrm{Sl}(u) := \varphi\left(\frac{u}{-3\varpi_1}\right), \quad \mathrm{Cl}(u) := \psi\left(\frac{u}{-3\varpi_1}\right).$$

Note also that

$$\mathsf{Z}(u + v) = \mathsf{Z}(u) + \mathsf{Z}(v) + \frac{1}{2}\frac{\wp'(\varpi_1 u) - \wp'(\varpi_1 v)}{\wp(\varpi_1 u) - \wp(\varpi_1 v)}, \tag{1.5}$$

which follows from the addition formula (see, for example, [WW, Chap. XX, 20.53, example 2])

$$\zeta(u + v) = \zeta(u) + \zeta(v) + \frac{1}{2}\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}. \tag{1.6}$$

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

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

(1) $\zeta(\rho u) = \bar{\rho}\zeta(u)$, $\zeta(-u) = -\zeta(u)$, $\zeta\left(\frac{\varpi_1}{2}\right) = \frac{\pi}{\sqrt{3}\varpi_1}$, $\zeta\left(\frac{\rho}{2}\varpi_1\right) = \frac{\pi}{\sqrt{3}\varpi_1}\bar{\rho}$.

(2) The function Z is a non-holomorphic periodic function with the period lattice $\mathbb{Z}[\rho]$, and satisfies $\mathsf{Z}(\rho u) = \bar{\rho}\mathsf{Z}(u)$, $\mathsf{Z}(-u) = -\mathsf{Z}(u)$, $\mathsf{Z}\left(\frac{1}{3}\right) = 1$, $\mathsf{Z}\left(\frac{1-\rho}{3}\right) = 0$.

6

(3) $\varphi(u) = \dfrac{6\wp(\varpi_1 u)}{9 + \wp'(\varpi_1 u)}, \psi(u) = \dfrac{-9 + \wp'(\varpi_1 u)}{9 + \wp'(\varpi_1 u)}$. Thus, φ, ψ are elliptic functions with the period lattice $\mathbb{Z}[\rho]$, and $\mathrm{Sl}(u), \mathrm{Cl}(u)$ are elliptic functions with the period lattice $3\varpi_1 \mathbb{Z}[\rho]$.

(4) $\wp(\varpi_1 u) = \dfrac{3\varphi(u)}{1 - \psi(u)}, \wp'(\varpi_1 u) = 9\dfrac{1 + \psi(u)}{1 - \psi(u)}$.

(5) $\varphi(\rho u) = \rho \varphi(u), \mathrm{Sl}(\rho u) = \rho\, \mathrm{Sl}(u), \psi(\rho u) = \psi(u), \mathrm{Cl}(\rho u) = \mathrm{Cl}(u)$.
$\varphi(\overline{u}) = \overline{\varphi(u)}, \mathrm{Sl}(\overline{u}) = \overline{\mathrm{Sl}(u)}, \psi(\overline{u}) = \overline{\psi(u)}, \mathrm{Cl}(\overline{u}) = \overline{\mathrm{Cl}(u)}$, thus, $\varphi(u), \mathrm{Sl}(u), \psi(u), \mathrm{Cl}(u) \in \mathbb{R}$ for $u \in \mathbb{R}$.

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

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

(8) $\varphi(-u) = -\dfrac{\varphi(u)}{\psi(u)}, \; \mathrm{Sl}(-u) = -\dfrac{\mathrm{Sl}(u)}{\mathrm{Cl}(u)}, \; \psi(-u) = \dfrac{1}{\psi(u)}, \; \mathrm{Cl}(-u) = \dfrac{1}{\mathrm{Cl}(u)}$.

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

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

Proof. (1) The claims $\zeta(\rho u) = \overline{\rho}\zeta(u), \; \zeta(-u) = -\zeta(u)$ are proved similarly as Lemma 1.2 (1). Thus it suffices to show that $\zeta\left(\frac{\varpi_1}{2}\right) = \frac{\pi}{\sqrt{3}\varpi_1}$. This is proved by Legendre's relation (see, for example, [WW, Chap.XX, 20.411])
$$\frac{\rho \varpi_1}{2}\zeta\left(\frac{\varpi_1}{2}\right) - \frac{\varpi_1}{2}\zeta\left(\frac{\rho \varpi_1}{2}\right) = \frac{\pi i}{2}.$$

(2) The calims $\mathsf{Z}(\rho u) = \overline{\rho}\mathsf{Z}(u), \; \mathsf{Z}(-u) = -\mathsf{Z}(u)$ are trivial by the definition and (1). By the quasi-periodicity (see, for example, [WW, Chap.XX 20.41])
$$\zeta(\varpi_1(u+1)) = \zeta(\varpi_1 u) + 2\zeta\left(\frac{\varpi_1}{2}\right),$$
we have
$$\mathsf{Z}(u+1) - \mathsf{Z}(u) = \zeta(\varpi_1(u+1)) - \zeta(\varpi_1 u) - \frac{2\pi}{\sqrt{3}\varpi_1} = 2\zeta\left(\frac{\varpi_1}{2}\right) - \frac{2\pi}{\sqrt{3}\varpi_1} = 0.$$
Then, we also have $\mathsf{Z}(u + \rho) - \mathsf{Z}(u) = \mathsf{Z}(\rho(\overline{\rho}u + 1)) - \mathsf{Z}(\rho \cdot \overline{\rho}u) = \overline{\rho}(\mathsf{Z}(\overline{\rho}u + 1) - \mathsf{Z}(\overline{\rho}u)) = 0$. Thus, it is proved that Z is periodic with the period lattice $\mathbb{Z}[\rho]$. The claim $\mathsf{Z}\left(\frac{1-\rho}{3}\right) = 0$ is similarly proved as $\wp\left(\frac{1-\rho}{3}\varpi_1\right)$ in Lemma 1.2 (4). The claim $\mathsf{Z}\left(\frac{1}{3}\right) = 1$ is proved by putting $u = \frac{1-\rho}{3}, v = \frac{\rho}{3}$ in (1.5), $\mathsf{Z}\left(\frac{1-\rho}{3}\right) = 0, \mathsf{Z}(\rho u) = \overline{\rho}\mathsf{Z}(u)$, and Lemma 1.2 (4) and (5).

(3) For $w \in \{1, \rho, \overline{\rho}\} = W'$, by putting $v = -\frac{w}{3}$ in (1.5),
$$\mathsf{Z}\left(u - \frac{w}{3}\right) = \mathsf{Z}(u) + \mathsf{Z}\left(-\frac{w}{3}\right) + \frac{1}{2}\frac{\wp'(\varpi_1 u) - \wp'(-\frac{w}{3}\varpi_1)}{\wp(\varpi_1 u) - \wp(-\frac{w}{3}\varpi_1)} = \mathsf{Z}(u) - \overline{w} + \frac{1}{2}\frac{\wp'(\varpi_1 u) - 9}{\wp(\varpi_1 u) - 3w},$$
by (2), and Lemma 1.2 (4) and (5). Then, by the definition of φ, the facts that $\sum_{w \in W'} w = \sum_{w \in W'} \overline{w} = 0$, $\sum_{w \in W'} \frac{\overline{w}}{x - w} = \frac{3x}{x^3 - 1}$, and Lemma 1.2 (3), we have
$$3\varphi(u) = \sum_{w \in W'} \overline{w}\mathsf{Z}\left(u - \frac{w}{3}\right) = \sum_{w \in W'} \overline{w}\mathsf{Z}(u) - \sum_{w \in W'} w + \frac{\wp'(\varpi_1 u) - 9}{2}\sum_{w \in W'} \frac{\overline{w}}{\wp(\varpi_1 u) - 3w}$$
$$= \frac{\wp'(\varpi_1 u) - 9}{2}\sum_{w \in W'} \frac{\overline{w}}{\wp(\varpi_1 u) - 3w} = \frac{\wp'(\varpi_1 u) - 9}{2}\frac{9\wp(\varpi_1 u)}{\wp(\varpi_1 u)^3 - 27} = \frac{18\wp(\varpi_1 u)}{\wp'(\varpi_1 u) + 9}.$$

Thus $\varphi(u) = \frac{6\wp(\varpi_1 u)}{\wp'(\varpi_1 u) + 9}$. Similarly, by $\sum_{w \in W'} \frac{w}{x - w} = \frac{3}{x^3 - 1}$, we have
$$-3\psi(u) = \sum_{w \in W'} w\mathsf{Z}\left(u - \frac{w}{3}\right) = \sum_{w \in W'} w\mathsf{Z}(u) - \sum_{w \in W'} 1 + \frac{\wp'(\varpi_1 u) - 9}{2}\sum_{w \in W'} \frac{w}{\wp(\varpi_1 u) - 3w}$$
$$= -3 + \frac{\wp'(\varpi_1 u) - 9}{2}\sum_{w \in W'} \frac{w}{\wp(\varpi_1 u) - 3w} = -3 + \frac{\wp'(\varpi_1 u) - 9}{2}\frac{27}{\wp(\varpi_1 u)^3 - 27} = -3 + \frac{54}{\wp'(\varpi_1 u) + 9}.$$

Thus $\psi(u) = 1 - \frac{18}{\wp'(\varpi_1 u)+9} = \frac{\wp'(\varpi_1 u)-9}{\wp'(\varpi_1 u)+9}$.

(4) This is proved by solving two equations of (3) in terms of $\wp(\varpi_1 u)$ and $\wp'(\varpi_1 u)$.

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

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

(7) By (6), we have

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

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

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

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

By definitions of Sl and Cl, we also have $\mathrm{Sl}(-u) = -\frac{\mathrm{Sl}(u)}{\mathrm{Cl}(u)}$. By (3), it follows that $\psi(-u)\psi(u) = \frac{-9+\wp'(\varpi_1 u)}{9+\wp'(\varpi_1 u)} \cdot \frac{-9-\wp'(\varpi_1 u)}{9-\wp'(\varpi_1 u)} = 1$. By definition of Cl, we also have $\mathrm{Cl}(-u) = \frac{1}{\mathrm{Cl}(u)}$.

(9) This is obvious from (3).

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

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

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

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

Thus, (10) follows from these two equalities.

$\square$

1.2   Power series expansions in terms of Sl

Let us consider power series expansions in terms of the function $\mathrm{Sl}(u)$ in this section, which will be used to show the main congruences (Theorem 2.5).

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

Lemma 1.5 (Addition formula of $\mathrm{Sl}(u)$). (cf. [A, §1. Appendix. 1. Addition Formula (i)])
We have

$$\mathrm{Sl}(u+v) = \frac{\mathrm{Sl}(u)^2\,\mathrm{Cl}(v) - \mathrm{Sl}(v)^2\,\mathrm{Cl}(u)}{\mathrm{Sl}(u)\,\mathrm{Cl}(v)^2 - \mathrm{Sl}(v)\,\mathrm{Cl}(u)^2} \in \mathrm{Sl}(u) + \mathrm{Sl}(v) + (\mathrm{Sl}(u),\mathrm{Sl}(v))^2\mathbb{Z}\left[\frac{1}{3}\right][[\mathrm{Sl}(u),\mathrm{Sl}(v)]] \ (\subset \mathbb{Q}[[u,v]]).$$

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

It remains to show that $\mathrm{Sl}(u+v) \in \mathrm{Sl}(u) + \mathrm{Sl}(v) + (\mathrm{Sl}(u),\mathrm{Sl}(v))^2\mathbb{Z}\left[\frac{1}{3}\right][[\mathrm{Sl}(u),\mathrm{Sl}(v)]]$. Since Lemma 1.4 (7) and (5),

$$\mathrm{Cl}(u) = \sqrt[3]{1 - \mathrm{Sl}(u)^3} = \sum_{n=0}^{\infty}(-1)^n\binom{\frac{1}{3}}{n}\mathrm{Sl}(u)^{3n} = 1 + \sum_{n=1}^{\infty}(-1)^n\binom{\frac{1}{3}}{n}\mathrm{Sl}(u)^{3n},$$

8

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

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

$$\mathrm{Cl}(u) = 1 + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{3}}{n} \mathrm{Sl}(u)^{3n}, \quad \mathrm{Cl}(u)^2 = 1 + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{2}{3}}{n} \mathrm{Sl}(u)^{3n} \tag{1.7}$$

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

$$
\begin{aligned}
\mathrm{Sl}(u + v) &= \frac{x^2 - y^2 + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{3}}{n} (x^2 y^{3n} - y^2 x^{3n})}{x - y + \sum_{n=1}^{\infty} (-1)^n \binom{\frac{2}{3}}{n} (x y^{3n} - y x^{3n})} \\[2mm]
&= \frac{x + y - x^2 y^2 \sum_{n=1}^{\infty} (-1)^n \binom{\frac{1}{3}}{n} (x^{3n-3} + \cdots + y^{3n-3})}{1 - xy \sum_{n=1}^{\infty} (-1)^n \binom{\frac{2}{3}}{n} (x^{3n-2} + \cdots + y^{3n-2})} \in x + y + (x,y)^2 \mathbb{Z}\left[\tfrac{1}{3}\right][[x,y]].
\end{aligned}
\tag{1.8}
$$

Here, we note that $\left(1 - xy \sum_{n=1}^{\infty} (-1)^n \binom{\frac{2}{3}}{n} (x^{3n-2} + \cdots + y^{3n-2})\right)^{-1} \in 1 + (xy)\mathbb{Z}\left[\tfrac{1}{3}\right][[x,y]] \subset \left(\mathbb{Z}\left[\tfrac{1}{3}\right][[x,y]]\right)^{\times}$,

and $\binom{\frac{1}{3}}{n}, \binom{\frac{2}{3}}{n} \in \mathbb{Z}\left[\tfrac{1}{3}\right]$ (See p.52 of [W]). $\qquad\square$

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

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

We also have, if $r \neq 0$,

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

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

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

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

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

since f has no terms of degree 0 or 1, and the power series expansion of $\mathrm{Sl}((r+1)u)$ as $\mathrm{Sl}(u)$ has only $\mathrm{Sl}(u)^{3n+1}$ terms since $\mathrm{Sl}(\rho u) = \rho \, \mathrm{Sl}(u)$. Therefore, $\mathrm{Sl}(ru) \in r \, \mathrm{Sl}(u) + \mathrm{Sl}(u)^4 \mathbb{Z}\left[\tfrac{1}{3}\right][[\mathrm{Sl}(u)^3]]$ is proved for any $r > 0$.

Next, we will show that $\mathrm{Sl}(-ru) \in -r\,\mathrm{Sl}(u) + \mathrm{Sl}(u)^4 \mathbb{Z}\left[\frac{1}{3}\right][[\mathrm{Sl}(u)^3]]$ for any $r > 0$. Now, since $\mathrm{Cl}(u)^{-1} =$

$$\left(1 + \sum_{n=1}^{\infty}(-1)^n \binom{\frac{1}{3}}{n}\mathrm{Sl}(u)^{3n}\right)^{-1} \in 1 + \mathrm{Sl}(u)^3 \mathbb{Z}\left[\tfrac{1}{3}\right][[\mathrm{Sl}(u)^3]] \subset \left(\mathbb{Z}\left[\tfrac{1}{3}\right][[\mathrm{Sl}(u)^3]]\right)^{\times},\ \text{and Lemma 1.4 (8)},$$

$$\mathrm{Sl}(-u) = -\frac{\mathrm{Sl}(u)}{\mathrm{Cl}(u)} = -\frac{\mathrm{Sl}(u)}{1 + \sum_{n=1}^{\infty}(-1)^n \binom{\frac{1}{3}}{n}\mathrm{Sl}(u)^{3n}} = -\mathrm{Sl}(u) + \cdots \in -\mathrm{Sl}(u) + \mathrm{Sl}(u)^4 \mathbb{Z}\left[\frac{1}{3}\right][[\mathrm{Sl}(u)^3]]$$

follows. Therefore, for any $r > 0$, $\mathrm{Sl}(-ru) = r\,\mathrm{Sl}(-u)+\mathrm{Sl}(-u)^4 f_r(\mathrm{Sl}(-u)^3) \in -r\,\mathrm{Sl}(u)+\mathrm{Sl}(u)^4\mathbb{Z}\left[\frac{1}{3}\right][[\mathrm{Sl}(u)^3]]$ follows similarly to the former case. Thus, we have $\mathrm{Sl}(ru) \in r\,\mathrm{Sl}(u) + \mathrm{Sl}^4(u)\mathbb{Z}\left[\frac{1}{3}\right][[\mathrm{Sl}^3(u)]]$ for any $r \in \mathbb{Z}$.

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

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

$\square$

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

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

where we choose the branch of $\sqrt[3]{(-)}$ to be $\in \mathbb{R}$.

Proof. Since $\frac{d}{dt}\mathrm{ArcSl} = \frac{1}{\sqrt[3]{(1-t^3)^2}}$, ArcSl is monotone increasing. By the definitions of ArcSl and ϖ_1, $\mathrm{ArcSl}(0) = 0, \mathrm{ArcSl}(1) = \varpi_1$. Thus, the map $\mathrm{ArcSl}: [0,1] \to [0,\varpi_1]$ is bijective. On the other hand, the facts that

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

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

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

where $t = \mathrm{Sl}(u)$ and $dt = \mathrm{Sl}'(u)du = \mathrm{Cl}^2(u)du$, since Lemma 1.4 (6) and (7). Note that $\mathrm{Sl}(u), \mathrm{Cl}(u) \in \mathbb{R}$ for $u \in \mathbb{R}$ (Lemma 1.4 (5)). This means that the map $\mathrm{Sl}: [0, \varpi_1] \to [0,1]$ is the inverse function of the map $\mathrm{ArcSl}: [0,1] \to [0,\varpi_1]$. $\square$

From [Ko, Theorem 1.19] and $\mathrm{Sl}'(0) = \mathrm{Cl}^2(0) = 1 \neq 0$, we have $\mathrm{Sl}(u)$ is bijective around $u = 0$ for $u \in \mathbb{C}$. Hence, by Lemma 1.7, the inverse function of $\mathrm{Sl}(u)$ is the analytic continuation of the function $\mathrm{ArcSl}(t)$ to a sufficiently small nighbourhood of $t = 0$, which is $\mathrm{ArcSl}(t) = \sum_{n=0}^{\infty}(-1)^n \binom{-\frac{2}{3}}{n}\frac{t^{3n+1}}{3n+1}$. Thus, we have:

Corollary 1.8. $u = \sum_{n=0}^{\infty}(-1)^n \binom{-\frac{2}{3}}{n}\frac{\mathrm{Sl}(u)^{3n+1}}{3n+1}$.

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

1.3 Bernoulli-Hurwitz-type numbers for the Eisenstein integers

In this section, we introduce Bernoulli-Hurwitz-type numbers for Eisenstein integers, and study their denominators for the proof of Theorem 2.5.

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

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

(Note that, since $\mathrm{Sl}(\rho u) = \rho \, \mathrm{Sl}(u)$ by Lemma 1.4 (5), the coefficients of u^n in $\mathrm{Sl}(u)$ are zero unless n is congruent 1 modulo 3.)

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

Proof. We see that
$$\mathrm{Sl}^{(3)} = 6 \, \mathrm{Sl}^4 - 4 \, \mathrm{Sl} \tag{1.9}$$
by Lemma 1.4 (6) and (7). Hence, by induction on m, we have $c_{3m+1} \in \mathbb{Z}$ for any $m \geq 0$. $\qquad\square$

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

$$\frac{1}{\mathrm{Sl}(u)} = \frac{1}{u} + \sum_{n=0}^{\infty} D_{3n+2} u^{3n+2} = \frac{1}{u} + \sum_{n=0}^{\infty} \frac{d_{3n+2}}{(3n+2)!} u^{3n+2}. \tag{1.10}$$

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

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

Remark 1.10. (Non-integrality of d_n) The function $f(u) = \frac{1}{\mathrm{Sl}(u)}$ satisfies a differential equation $f^{(3)} = 4f - 6f^4$, hence $D_{3m+2} \in \mathbb{Q}$ for $m \geq 0$. We have $D_2 = \frac{1}{6}, D_5 = -\frac{1}{252}, D_8 = -\frac{1}{4536}$. Therefore, $d_{3n+2} = (3n+2)! D_{3n+2}$ is not necessarily a rational integer. However, Lemma 1.12 below holds.

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

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

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

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

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

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

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

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

Remark 1.13. (1) Moreover, we can show $d_{6m+2} \in \mathbb{Z}\left[\frac{1}{3}\right]$. See Lemma A.5 (which is not used to show the main congruences in Theorem 2.5).

(2) For the denominators of d_{6m-1}, see Lemma A.7 (which is not used to show the main congruences in Theorem 2.5).

1.4 Eisenstein's product formula

We recall that the arithmetic properties of Sl at division points.

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

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

$$\ell = \lambda \overline{\lambda} \ \text{ and } \lambda \equiv 1 \bmod 3.$$

Note that there are precisely two choices of such λ, i.e., λ and $\overline{\lambda}$. 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:

$$\chi_\lambda(\nu) := \left(\frac{\nu}{\lambda}\right)_3, \ \chi_\lambda(\nu)^3 = 1, \text{ and } \chi_\lambda(\nu) \equiv \nu^{(\ell-1)/3} \ \bmod \lambda \ \ (\nu \in (\mathbb{Z}[\rho]/(\lambda))^\times).$$

We write

$$\Lambda := \varphi\left(\frac{1}{\lambda}\right) = \mathrm{Sl}\left(\frac{-3\varpi_1}{\lambda}\right).$$

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

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

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

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

Lemma 1.16.
$$\widetilde{\lambda}^2 \equiv \Lambda^{\frac{2(\ell-1)}{3}} \bmod \Lambda^{\frac{2(\ell-1)}{3}+1}.$$

Proof. By Lemma 1.6, 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 $f_r(t) \in \mathbb{Z}[\frac{1}{3}][[t]]$, ($t$ is a variable). Let $g \in \mathbb{Z}$ be a primitive root of 1 modulo ℓ. Then, since $\ker(\chi_\lambda) = \{g^{3j} \bmod \lambda \mid j = 1, \ldots, \frac{\ell-1}{3}\}$ (note that $(\mathbb{Z}[\rho]/(\lambda))^\times \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$), we have

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

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

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

hence,

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

where $\mathscr{O}_{\lambda,\Lambda}$ is the completion of $\mathscr{O}_\lambda$ by Λ. Thus, by taking mod $\Lambda^{\frac{\ell-1}{3}+1}$ of (1.11), we have

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

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

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

$\square$

2 Elliptic Gauss sums

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

Let $\ell, \lambda, \widetilde{\lambda}, \chi_\lambda$ and Λ be as in Chapter 1.

2.1 Elliptic Gauss sums and their coefficients

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

We put

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

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

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

$$G_\lambda(\chi_\lambda, f) := \frac{1}{3}\sum_{r \in (\mathbb{Z}[\rho]/(\lambda))^\times} \chi_\lambda(r)f\left(\frac{r}{\lambda}\right), \tag{2.1}$$

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

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

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

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

(2) We have $(\mathbb{Z}[\rho]/(\lambda))^\times = S \cup \rho S \cup \overline{\rho}S$ (disjoint union), where $S := \ker(\chi_\lambda)$, if $\ell \equiv 7, 4 \bmod 9$. If $\ell \equiv 7 \bmod 9$ (resp. $\ell \equiv 4 \bmod 9$), then $f = \varphi$ (resp. $f = \varphi^{-1}$), $\varphi(\rho u) = \rho\varphi(u)$ (resp. $\varphi(\rho u)^{-1} = \overline{\rho}\varphi(u)^{-1}$) (by Lemma 1.4 (5)), and $\chi_\lambda(\rho) = \rho^{\frac{\ell-1}{3}} = \overline{\rho}$ (resp. $\chi_\lambda(\rho) = \rho^{\frac{\ell-1}{3}} = \rho$) (by the definition of χ_λ). Hence, we have $G_\lambda(\chi_\lambda, f) = \frac{1}{3}\sum_{r \in S}\left(f\left(\frac{r}{\lambda}\right) + \chi_\lambda(\rho)f\left(\frac{\rho r}{\lambda}\right) + \chi_\lambda(\overline{\rho})f\left(\frac{\overline{\rho} r}{\lambda}\right)\right) = \sum_{r \in S} f\left(\frac{r}{\lambda}\right)$. $\square$

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

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

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

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

(2) If $\ell \equiv 4 \bmod 9$, then there exists $\alpha_\lambda \in \overline{\chi_\lambda}(3)(-1 + 3\mathbb{Z})$ such that

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

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

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

The number α_λ is called the *coefficient of elliptic Gauss sum* in [A].

2.2 The main congruences

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

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

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

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

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

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

as elements of $\mathbb{Q}[[u]] = \mathbb{Q}[[t]]$.

<u>The case $\ell \equiv 7 \bmod 9$.</u> Let $g \in \mathbb{Z}$ be a primitive root of 1 modulo ℓ, i.e., $g \bmod \ell$ generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$. We consider the sum

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

By Lemma 2.2 (2),

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

By (2.2),

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

Since Lemma 1.6 and the definition of L_1, the coefficients of this expansion in terms of t are $\in \mathbb{Z}\left[\frac{1}{3}\right]$, especially $\in \mathbb{Z}_{(\ell)}$. Here, we substitute Λ for t (which corresponds to the substitution of $\frac{-3\varpi_1}{\lambda}$ for u), then, $\mathrm{Sl}(\nu u) \mapsto \mathrm{Sl}\left(\frac{-3\varpi_1\nu}{\lambda}\right)$ for any $\nu \in \mathbb{Z}$, since Lemma 1.6. 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 $\mathscr{O}_{\lambda,\Lambda}$ 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 $\binom{-\frac{2}{3}}{n} \in \mathbb{Z}\left[\frac{1}{3}\right]$ and $3n+1 \leq \frac{2\ell-2}{3} < \ell$) and $C_{3m+1} \in \mathbb{Z}_{(\ell)}$ for $m \leq \frac{2\ell-5}{9}$ (since $C_{3m+1} = \frac{c_{3m+1}}{(3m+1)!}$,

14

$3m + 1 < \ell$, and $c_{3m+1} \in \mathbb{Z}$ (Lemma 1.9)), and that the coefficients of this expansion in terms of Λ are $\in \mathbb{Z}\left[\frac{1}{3}\right]$, we have

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

We also have

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

Since $0 \le m \le \frac{2\ell-5}{9}$ and $\ell \equiv 7 \bmod 9$, we see that $\ell - 1 | 3(3m+1)$ if and only if $3(3m+1) = 2(\ell-1)$. Then, we have

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

On the other hand, by Theorem 2.3 (1) and Lemma 1.16, we have

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

Therefore,

$$\alpha_\lambda \equiv -\frac{1}{3} C_{\frac{2(\ell-1)}{3}} \ \mathrm{mod}\ \Lambda$$

holds. Since $\alpha_\lambda \in \chi_\lambda(3)(1 + 3\mathbb{Z}) \subset \mathbb{Z}[\rho]$, and $C_{\frac{2(\ell-1)}{3}} = c_{\frac{2(\ell-1)}{3}} / (\frac{2(\ell-1)}{3})! \in \mathbb{Z}_{(\ell)}$ by Theorem 2.3 (1) and Lemma 1.9, we have $\alpha_\lambda \equiv -\frac{1}{3} C_{\frac{2(\ell-1)}{3}} \bmod \lambda$.

   The case $\ell \equiv 4 \bmod 9$. Let $g \in \mathbb{Z}$ be a primitive root of 1 modulo ℓ. We consider the sum

$$L_2(u) := \mathrm{Sl}(g^3 u)^{-1} + \mathrm{Sl}(g^6 u)^{-1} + \cdots + \mathrm{Sl}(g^{\frac{\ell-1}{2}} u)^{-1} + \mathrm{Sl}(-g^3 u)^{-1} + \mathrm{Sl}(-g^6 u)^{-1} + \cdots + \mathrm{Sl}(-g^{\frac{\ell-1}{2}} u)^{-1}. \quad (2.4)$$

By noting that $g^{\frac{\ell-1}{2}} \equiv -1 \bmod \ell$, we have $\ker(\chi_\lambda) = \{g^{3j}, -g^{3j} \bmod \ell \mid j = 1, \ldots, \frac{\ell-1}{6}\}$. By this fact and Lemma 2.2 (2), we have

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

By (2.3),

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

Since Lemma 1.6 and the definition of L_2, the coefficients of this expansion in terms of t are $\in \mathbb{Z}\left[\frac{1}{g^{3j}}, \frac{1}{3} : j = 1, \ldots, \frac{\ell-1}{6}\right]$, especially $\in \mathbb{Z}_{(\ell)}$. Here, we substitute Λ for t (which corresponds to the substitution of $\frac{-3\varpi_1}{\lambda}$ for u), then, $\mathrm{Sl}(\nu u) \mapsto \mathrm{Sl}\left(\frac{-3\varpi_1 \nu}{\lambda} \right)$ for any $\nu \in \mathbb{Z}$, since Lemma 1.6. 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 $\mathscr{O}_{\lambda,\Lambda}$ 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 $n \le \frac{2(\ell-4)}{9}$ (since $\binom{-\frac{2}{3}}{n} \in \mathbb{Z}\left[\frac{1}{3}\right]$ and $3n+1 \le \frac{2\ell-3}{3} < \ell$) and $D_{6m+2} \in \mathbb{Z}_{(\ell)}$ for $m \le \frac{\ell-4}{9}$ (since $D_{6m+2} = \frac{d_{6m+2}}{(6m+2)!}$,

15

$6m + 2 < \ell$, and $d_{6m+2} \in \mathbb{Z}_{(\ell)}$ (Lemma 1.12)), and that the coefficients of this expansion in terms of Λ are $\in \mathbb{Z}\left[\frac{1}{3}\right]$, we have

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

We also have

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

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

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

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

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

Therefore,

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

holds.

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

Example 2.6. (1) Let $\ell = 7$ and $\lambda = 1 + 3\rho$. By Table 1, we have $C_4 = -\frac{1}{6}$. Then,

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

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

(2) $\ell = 13$ and $\lambda = 4 + 3\rho$. By Table 2, $D_8 = -\frac{1}{4536} \equiv 1 \bmod 13$. Then,

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

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

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

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

We also have

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

16

Proof. Let $\ell \equiv 7 \bmod 9$. We have $\alpha_\lambda^2 \equiv \left(C_{\frac{2(\ell-1)}{3}}\right)^2 / 9 \bmod \lambda$ by Theorem 2.5. We can take $a_\lambda \in 1 + 3\mathbb{Z}$ as $\alpha_\lambda = \chi_\lambda(3) a_\lambda$ by Theorem 2.3 (1). Then, $\alpha_\lambda^2 = \overline{\chi_\lambda(3)} a_\lambda^2$, and $|\alpha_\lambda|^2 = a_\lambda^2$ hold. Therefore, we have

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

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

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

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

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

3 Elliptic Gauss sums and associated elliptic curves

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

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

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

3.1 Hecke L-series

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

We define, due to [A, §1.4.1],

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

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 choice of the generator ν of the ideal (ν). Hecke L-series associated to the Hecke character $\widetilde{\chi_\lambda}$ is

$$\begin{aligned}
L(s, \widetilde{\chi_\lambda}) &= \prod_{(\mu): \text{ prime ideal}} (1 - \widetilde{\chi_\lambda}((\mu))(\mu\overline{\mu})^{-s})^{-1} = \prod_{\substack{\mu: \text{ prime} \\ \mu \equiv 1 \bmod 3 \\ \text{or } \mu = 1-\rho}} (1 - \widetilde{\chi_\lambda}((\mu))(\mu\overline{\mu})^{-s})^{-1} \\
&= \prod_{\substack{\mu: \text{ primary prime} \\ \mu \neq \lambda, 1-\rho}} (1 - \chi_\lambda(\mu)\overline{\mu}(\mu\overline{\mu})^{-s})^{-1}
\end{aligned} \tag{3.1}$$

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

3.2 L-functions of elliptic curves

In this section, we introduce certain elliptic curves for λ, and show the properties of them such as their reduction types at prime ideals of $\mathbb{Z}[\rho]$, the numbers of the points of the reductions of the elliptic curves. We

also show that the Hecke L-series defined in §3.1 correspond to the L-functions of the elliptic curves defined in this section.

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

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

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

If ϕ is the quadratic residue character, χ is the cubic residue character, then

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

holds.

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

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

If ϕ has order 2 and χ has order 3, then
$$J_2(\phi, \chi) = q$$

holds.

(3) (Cubic Reciprocity Law) If λ_1, 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. (1) The first equality follows from [IR, Lemma in §3 of Chap. 18] and the second equality follows from [IR, Lemma 1 in §4 of Chap. 9]. (Note that $-\mu$ is primary in the definition of [IR, §3 of Chap. 9].)

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

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

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

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

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

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

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

(2) (Special Fibers) The special fiber of $\mathscr{E}_\lambda$ at (λ) is of Type IV, and the one at $(1 - \rho)$ is of Type IV if $\ell \equiv 7 \bmod 9$, of Type I_0^* if $\ell \equiv 4 \bmod 9$, in the notation of Kodaira symbols in the Kodaira-Néron classification of the special fibers of Néron models.

(3) (Local Tamagawa Numbers) For any prime ideal $\mathfrak{P} \subset \mathbb{Z}[\rho]$, let $\mathcal{E}/R_{\mathfrak{P}}$ be the Néron model of $\mathscr{E}_\lambda \times_{\mathbb{Q}(\rho)} K_{\mathfrak{P}}$, $\widetilde{\mathcal{E}}/k_{\mathfrak{P}} = \mathcal{E} \times_{R_{\mathfrak{P}}} k_{\mathfrak{P}}$ the special fiber of $\mathcal{E}$, $\widetilde{\mathcal{E}^0}/k_{\mathfrak{P}}$ the identity component of the group variety $\widetilde{\mathcal{E}}/k_{\mathfrak{P}}$, and $\tau_{\mathfrak{P}}$ the order of the group of components $\widetilde{\mathcal{E}}(k_{\mathfrak{P}})/\widetilde{\mathcal{E}^0}(k_{\mathfrak{P}})$. Then, we have

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

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

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

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

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

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

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

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

(6) (Global Rational Torsion Points)

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

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

Remark 3.3. On (6), we can show, moreover, $\mathscr{E}_\lambda(\mathbb{Q}(\rho)) = \mathscr{E}_\lambda(\mathbb{Q}(\rho))_{\mathrm{tors}}$ as follows: As we will see later, the L-function of $\mathscr{E}_\lambda$ does not vanish at $s = 1$. This fact follows from Lemma 3.5, which is proved without Lemma 3.2 (6). From [CW, Theorem 1], the rank of $\mathscr{E}_\lambda(\mathbb{Q}(\rho))$ is zero. Thus, $\mathscr{E}_\lambda(\mathbb{Q}(\rho)) = \mathscr{E}_\lambda(\mathbb{Q}(\rho))_{\mathrm{tors}}$.

Proof. (1) The substitution $y \mapsto y + \frac{\lambda}{2}$ to $y^2 = x^3 + \frac{\lambda^2}{4}$ gives an equation of the form

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

This equation has the discriminant $\Delta = -27\lambda^4$ and $c_4 = 0$, where c_4 is the one defined in [S1, Chap. III. 1]. Thus $(\Delta) = (1 - \rho)^6(\lambda)^4$ as ideals in $\mathbb{Z}[\rho]$. This is a global minimal Weierstrass equation of $\mathscr{E}_\lambda/\mathbb{Q}(\rho)$, since [S1, Chap. VII, Remark 1.1]. (Note that Weierstrass equation $y^2 = x^3 + \frac{\lambda^2}{4}$ is minimal at every prime except (2).) Hence, $\mathscr{E}_\lambda$ has only two bad primes $(\lambda), (1 - \rho)$, and it has additive reductions at these primes, since [S1, Chap. VII, Proposition 5.1(c)] (The fact that $\mathscr{E}_\lambda$ has additive reductions at $(\lambda), (1 - \rho)$ can be deduced in the following way as well: Since $\mathscr{E}_\lambda$ has complex multiplication, the j-invariant of $\mathscr{E}_\lambda$ is integral by [S2, Chap. II, Theorem 6.1]. Since [S1, Chap. VII, Proposition 5.5], $\mathscr{E}_\lambda$ has potential good reduction at every primes. By [S1, Chap. VII, Proposition 5.4 (b)], $\mathscr{E}_\lambda$ does not have multiplicative reductions.).

(2)-(3) In the following, we use the symbols (e.g., $a_1, b_2, a_{3,1}$ etc.) and the terminology (e.g., Step1 etc.) of [S2, Chap. IV, Tate's Algorithm 9.4]. Note that $a_1 = 0, a_3 = \lambda, a_2 = a_4 = a_6 = 0, b_2 = b_4 = 0, b_6 = \lambda^2, b_8 = 0$. First, we determine the reduction type at (λ) and $\tau_{(\lambda)}$. Note that $k_{(\lambda)} \simeq \mathbb{F}_\ell$, and choose λ as a uniformizer.

Step1: Since $\lambda | \Delta$, go to Step2.
Step2: Since $\lambda | a_3, a_4, a_6$ and b_2, go to Step3.
Step3: Since $\lambda^2 | a_6$, go to Step4.
Step4: Since $\lambda^3 | b_8$, go to Step5.
Step5: Since $\lambda^3 \nmid b_6 = \lambda^2$, $\mathscr{E}_\lambda$ is of Type IV at (λ). Let k' be the splitting field over $k_{(\lambda)}$ of $T^2 + a_{3,1}T - a_{6,2} = T^2 + T = 0$. Then, $k' = k_{(\lambda)}$. Thus, we have $\tau_{(\lambda)} = c = 3$.

Next, we determine the reduction type at $(1 - \rho)$ and $\tau_{(1-\rho)}$. Note that $k_{(1-\rho)} \simeq \mathbb{F}_3$, and choose $1 - \rho$ as a uniformizer.

Step1: Since $(1-\rho)|\Delta$, go to Step2.

Step2: $\mathscr{E}_\lambda \otimes k_{(1-\rho)}/k_{(1-\rho)} : y^2 + y = x^3$, since $\lambda \equiv 1 \mod 3$, especially, $\lambda \equiv 1 \mod (1-\rho)$. Here, $(x,y) = (-1,1)$ is the singular point. To make a change of variables to move the singular point to $(0,0)$, we substitute $(x,y) \mapsto (x-1, y+\lambda)$. Then, $\mathscr{E}_\lambda : y^2 + 3\lambda y = x^3 - 3x^2 + 3x - 1 - 2\lambda^2$. The new a_i's and b_i's are:

$$a_1 = 0,\ a_3 = 3\lambda,\ a_2 = -3,\ a_4 = 3,\ a_6 = -1 - 2\lambda^2,$$

$$b_2 = -12,\ b_4 = 6,\ b_6 = \lambda^2 - 4,\ b_8 = -3(\lambda^2 - 1).$$

Thus, $(1-\rho)|a_3, a_4, a_6$ and b_2, go to Step3.

Step3: Since $a_6 = -1 - 2\lambda^2 \equiv -1 - 2 \equiv 0 \mod 3$, $(3) = (1-\rho)^2|a_6$, go to Step4.

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

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

$$(1-\rho)|(\alpha+\beta\rho) \Longleftrightarrow \alpha + \beta \equiv 0 \mod 3. \tag{3.2}$$

Note also that $a_6 = -1 - 2\lambda^2 = -1 - 2(3m+1+3n\rho)^2 \equiv -3(1+m+n\rho) \mod 9$.

<u>We assume that $\ell \equiv 7 \mod 9$.</u> We will show that $(1-\rho)^3 \nmid b_6$. Note that $b_6 = (\lambda+2)(\lambda-2)$. Since $\lambda - 2 \equiv -1 \mod 3$, $(1-\rho) \nmid (\lambda-2)$. Thus, it suffices to show that $(1-\rho)^3 \nmid \lambda + 2$. Therefore, it suffices to show that $(1-\rho) \nmid m + 1 + n\rho$. Now, $7 \equiv \ell \equiv 6m + 1 - 3n \mod 9$, thus, $-3 \equiv -3(m+n) \mod 9$. Hence, we have $1 \equiv m + n \mod 3$. Since $m + n + 1 \equiv 2 \mod 3$ and (3.2), we have $(1-\rho) \nmid m + 1 + n\rho$. Therefore, we proved $(1-\rho)^3 \nmid b_6$. Thus, $\mathscr{E}_\lambda$ is of Type IV at $(1-\rho)$. We have $a_{6,2} = \frac{a_6}{(1-\rho)^2} \equiv \bar{\rho}(1+m+n\rho) \equiv 1 + m + n \equiv -1 \mod (1-\rho)$ (note that $(1-\rho)^2 = -3\rho$). Let k' be the splitting field over $k_{(1-\rho)}$ of $T^2 + a_{3,1}T - a_{6,2} = T^2 + 1 \in k_{(1-\rho)}[T]$. Then, $k' \neq k_{(1-\rho)}$. Thus, we have $\tau_{(1-\rho)} = c = 1$.

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

Step6: Already, $(1-\rho)|a_1, a_2$; $(1-\rho)^2|a_3, a_4$; and $(1-\rho)^3|a_6$ are satified. Since $a_{6,3} = \frac{a_6}{(1-\rho)^3} \equiv \frac{1+m+n\rho}{\rho(1-\rho)} = \rho^2 \frac{1+m+n}{1-\rho} - \rho^2 n \equiv -n \mod 1 - \rho$. We consider $P(T) = T^3 + a_{2,1}T^2 + a_{4,2}T + a_{6,3} = T^3 - T - n \in k_{(1-\rho)}[T]$. Since $P'(T) = -1$, the polynomial $P(T)$ has distinct roots in an algebraic closure of $k_{(1-\rho)}$. Thus, $\mathscr{E}_\lambda$ is of Type I_0^* at $(1-\rho)$. We have

$$\tau_{(1-\rho)} = c = 1 + \#\{\alpha \in k_{(1-\rho)} \mid P(\alpha) = 0\} = \begin{cases} 4 & \text{if } n \equiv 0 \mod 3, \\ 1 & \text{if otherwise,} \end{cases}$$

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

(4) $y^2 = x^3 + \frac{\lambda^2}{4}$ is the minimal Weierstrass equation at the prime ideal (μ). Let $\phi : \mathbb{F}_p^\times \to \{\pm 1\}$ be the quadratic residue symbol, and $\chi : \mathbb{F}_p^\times \to W'$ 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 $D_1 \neq 0, \phi(D_1) = 1, \chi(-1) = 1$. Then, we have

$$\#(\mathscr{E}_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = 1 + \#\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + D_1\} = 1 + \sum_{\substack{u,v \in \mathbb{F}_p \\ u+v=D_1}} \#\{y \in \mathbb{F}_p \mid y^2 = u\} \cdot \#\{x \in \mathbb{F}_p \mid x^3 = -v\}$$

$$= 1 + \sum_{\substack{u,v \in \mathbb{F}_p \\ u+v=D_1}} (1+\phi(u))(1 + \chi(-v) + \overline{\chi(-v)}) = p + 1 + \sum_{\substack{u,v \in \mathbb{F}_p \\ u+v=D_1}} \phi(u)(\chi(-v) + \overline{\chi(-v)})$$

$$= p + 1 + \phi(D_1)\chi(D_1) \sum_{\substack{u,v \in \mathbb{F}_p \\ u+v=1}} \phi(u)\chi(v) + \phi(D_1)\overline{\chi(D_1)} \sum_{\substack{u,v \in \mathbb{F}_p \\ u+v=1}} \phi(u)\overline{\chi(v)}$$

$$= p + 1 + \chi(D_1)J(\phi,\chi) + \overline{\chi(D_1)J(\phi,\chi)}.$$

By Lemma 3.1 (1), we have $\#(\mathscr{E}_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = p + 1 - (\chi(D_1)\chi(4)\mu + \overline{\chi(D_1)\chi(4)\mu})$. 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 3.1 (3)), we have $\chi(4D_1) = \left(\frac{\lambda}{\mu}\right)_3^2 = \overline{\left(\frac{\lambda}{\mu}\right)_3} = \overline{\chi_\lambda(\mu)}$. Thus, $\#(\mathscr{E}_\lambda \otimes \mathbb{F}_p)(\mathbb{F}_p) = p + 1 - (\overline{\chi_\lambda(\mu)}\mu + \chi_\lambda(\mu)\bar{\mu})$ holds.

(5) For $q \neq 2$, $y^2 = x^3 + \frac{\lambda^2}{4}$ is the minimal Weierstrass equation at the prime ideal $(-q)$. Let $\phi : \mathbb{F}_{q^2}^{\times} \to \{\pm 1\}$ be the quadratic residue symbol, and $\chi : \mathbb{F}_{q^2}^{\times} \to W'$ 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 $D_2 \neq 0, \phi(D_2) = 1, \chi(-1) = 1$. Then, we have

$$\#(\mathscr{E}_\lambda \otimes \mathbb{F}_{q^2})(\mathbb{F}_{q^2}) = 1 + \#\{(x,y) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2} \mid y^2 = x^3 + D_2\} = 1 + \sum_{\substack{u,v \in \mathbb{F}_{q^2} \\ u+v = D_2}} \#\{y \in \mathbb{F}_{q^2} \mid y^2 = u\} \cdot \#\{x \in \mathbb{F}_{q^2} \mid x^3 = -v\}$$

$$= 1 + \sum_{\substack{u,v \in \mathbb{F}_{q^2} \\ u+v = D_2}} (1 + \phi(u))(1 + \chi(-v) + \overline{\chi(-v)}) = q^2 + 1 + \sum_{\substack{u,v \in \mathbb{F}_{q^2} \\ u+v = D_2}} \phi(u)(\chi(-v) + \overline{\chi(-v)})$$

$$= q^2 + 1 + \phi(D_2)\chi(D_2) \sum_{\substack{u,v \in \mathbb{F}_{q^2} \\ u+v=1}} \phi(u)\chi(v) + \phi(D_2)\overline{\chi(D_2)} \overline{\sum_{\substack{u,v \in \mathbb{F}_{q^2} \\ u+v=1}} \phi(u)\chi(v)}$$

$$= q^2 + 1 + \chi(D_2)J_2(\phi,\chi) + \overline{\chi(D_2)J_2(\phi,\chi)}.$$

By Lemma 3.1 (2), we have $\#(\mathscr{E}_\lambda \otimes \mathbb{F}_{q^2})(\mathbb{F}_{q^2}) = q^2 + 1 + q(\chi(D_2) + \overline{\chi(D_2)})$. By noting that $\left(\frac{\cdot}{-q}\right)_3 : (\mathbb{Z}[\rho]/(-q))^{\times} \simeq \mathbb{F}_{q^2}^{\times} \xrightarrow{\chi} W'$, $\left(\frac{-2}{-q}\right)_3 = \left(\frac{-q}{-2}\right)_3 = 1$, and $\left(\frac{\lambda}{-q}\right)_3 = \left(\frac{-q}{\lambda}\right)_3 = \chi_\lambda(-q) = \chi_\lambda(q)$ (Lemma 3.1 (3)), we have $\chi(D_2) = \left(\frac{\lambda}{-q}\right)_3^2 = \overline{\left(\frac{\lambda}{-q}\right)_3} = \overline{\chi_\lambda(q)}$. Thus, $\#(\mathscr{E}_\lambda \otimes \mathbb{F}_{q^2})(\mathbb{F}_{q^2}) = q^2 + 1 + q(\chi_\lambda(q) + \overline{\chi_\lambda(q)})$ 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 $D_3 \neq 0$ and $y^2 + \lambda y = x^3$ is the minimal Weierstrass equation at the prime ideal (-2). For $y \in \mathbb{F}_4$, we show that $y^2 + D_3 y = 1$ if and only if $(D_3 + 1)y = 0$, $y \neq 0, 1$. Indeed, for $y \in \mathbb{F}_4$ with $y^2 + D_3 y = 1$, we have $y \neq 0, 1$, since $D_3 \neq 0$. Thus, $y^2 = y + 1$ holds, since $0 = y^3 - 1 = (y-1)(y^2 + y + 1)$ and $y \neq 1$. Thus, we have $(D_3 + 1)y = 0$ from $y^2 + D_3 y = 1$. For $(D_3 + 1)y = 0$, $y \neq 0, 1$, since $y^2 = y + 1$, we have $y^2 + D_3 y = y + 1 + D_3 y = 1$. Therefore,

$$\#\{(x,y) \in \mathbb{F}_4^{\times} \times \mathbb{F}_4 \mid y^2 + D_3 y = 1\} = 3\#\{y \in \mathbb{F}_4 \mid y^2 + D_3 y = 1\} = 3\#\{y \in \mathbb{F}_4 \mid (D_3+1)y = 0, y \neq 0, 1\}$$

$$= \begin{cases} 6 & \text{if } D_3 = 1, \\ 0 & \text{if } D_3 \neq 1 \end{cases}$$

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

$$\#(\mathscr{E}_\lambda \otimes \mathbb{F}_4)(\mathbb{F}_4) = 1 + \#\{(x,y) \in \mathbb{F}_4 \times \mathbb{F}_4 \mid y^2 + D_3 y = x^3\}$$

$$= 1 + \#\{(x,y) \in \mathbb{F}_4^{\times} \times \mathbb{F}_4 \mid y^2 + D_3 y = 1\} + \#\{y \in \mathbb{F}_4 \mid y^2 + D_3 y = 0\}$$

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

On the other hand, by Lemma 3.1 (3), we have

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

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

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

holds. Since $\lambda \equiv 1 \bmod 2 \iff D_3 = 1$, we have $\#(\mathscr{E}_\lambda \otimes \mathbb{F}_{q^2})(\mathbb{F}_{q^2}) = q^2 + 1 + q(\chi_\lambda(q) + \overline{\chi_\lambda(q)})$ for $q = 2$.

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

Let $m \geq 1$ be an integer that is relatively prime to 5. Then, $\mathscr{E}_\lambda(\mathbb{Q}(\rho))[m]$ has injective homomorphisms to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and $(\mathscr{E}_\lambda \otimes \mathbb{F}_{25})(\mathbb{F}_{25})$ by [S1, Chap. VII, Proposition 3.1 (b)]. On the other hand, $\#(\mathscr{E}_\lambda \otimes \mathbb{F}_{25})(\mathbb{F}_{25}) = 26 + 5(\chi_\lambda(5) + \overline{\chi_\lambda(5)}) = 36$, or 21 by (5). Thus, for m relatively prime to $2, 3, 5, 7$, we have $\#\mathscr{E}_\lambda(\mathbb{Q}(\rho))[m] = 1$. We also have that $\mathscr{E}_\lambda(\mathbb{Q}(\rho))[m]$ has injective homomorphisms to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and

21

$(\mathscr{E}_\lambda \otimes \mathbb{F}_{121})(\mathbb{F}_{121})$ for m relatively prime to 11 by loc. cit. On the other hand, $\#(\mathscr{E}_\lambda \otimes \mathbb{F}_{121})(\mathbb{F}_{121}) = 122 + 11(\chi_\lambda(11) + \overline{\chi_\lambda(11)}) = 144$, or 111 by (5). Thus, for m relatively prime to $2, 3, 11, 37$, we have $\#\mathscr{E}_\lambda(\mathbb{Q}(\rho))[m] = 1$.

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

Proposition 3.4. (Correspondence between the Hecke L-series and the L-function of the elliptic curve) Let $L(\mathscr{E}_\lambda/\mathbb{Q}(\rho), s)$ be the L-function of the elliptic curve $\mathscr{E}_\lambda : y^2 = x^3 + \frac{\lambda^2}{4}$ over $\mathbb{Q}(\rho)$ (see [S2, §10 of Chap. II]). The Hecke L-series defined by (3.1) corresponds to the L-function of the elliptic curve $\mathscr{E}_\lambda$, i.e., one has

$$L(s, \widetilde{\chi_\lambda})L(s, \overline{\widetilde{\chi_\lambda}}) = L(\mathscr{E}_\lambda/\mathbb{Q}(\rho), s).$$

Proof. We recall the definition of $L(\mathscr{E}_\lambda/\mathbb{Q}(\rho), s)$: $L(\mathscr{E}_\lambda/\mathbb{Q}(\rho), s) := \prod_{\mathfrak{P}:\text{prime ideal}} L_{\mathfrak{P}}(\mathscr{E}_\lambda/\mathbb{Q}(\rho), q_{\mathfrak{P}}^{-s})^{-1}$, where $L_{\mathfrak{P}}(\mathscr{E}_\lambda/\mathbb{Q}(\rho), T)$ is the local L-factor of $\mathscr{E}_\lambda/\mathbb{Q}(\rho)$ at $\mathfrak{P}$ defined as follows: Let $q_{\mathfrak{P}} := \#k_{\mathfrak{P}}$, $a_{\mathfrak{P}} := q_{\mathfrak{P}} + 1 - \#(\mathscr{E}_\lambda \otimes k_{\mathfrak{P}})(k_{\mathfrak{P}})$, if $\mathscr{E}_\lambda$ has good reduction at $\mathfrak{P}$. Then,

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

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

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

If $\mathfrak{P} = (\mu)$, where $\mu \in \mathbb{Z}[\rho]$ is a primary prime $\neq \lambda$ such that $p = \mu\overline{\mu}$ is a rational prime, then $k_{\mathfrak{P}} \simeq \mathbb{F}_p$, $q_{\mathfrak{P}} = p$, $a_{\mathfrak{P}} = \chi_\lambda(\mu)\overline{\mu} + \overline{\chi_\lambda}(\mu)\mu$ hold by Lemma 3.2 (4). Thus,

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

On the other hand, the local L-factor of $L(s, \widetilde{\chi_\lambda})L(s, \overline{\widetilde{\chi_\lambda}})$ 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 (3.1). Therefore, the local L-factor of $L(s, \widetilde{\chi_\lambda})L(s, \overline{\widetilde{\chi_\lambda}})$ at $\mathfrak{P}$ coinsides with the one of $L(\mathscr{E}_\lambda/\mathbb{Q}(\rho), s)$ at $\mathfrak{P}$.

Next, if $\mathfrak{P} = (-q)$, where q is a rational prime such that $q \equiv 2 \bmod 3$, then $k_{\mathfrak{P}} \simeq \mathbb{F}_{q^2}$, $q_{\mathfrak{P}} = q^2$, $a_{\mathfrak{P}} = -q(\chi_\lambda(q) + \overline{\chi_\lambda}(q))$ hold by Lemma 3.2 (5). Thus,

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

On the other hand, the local L-factor of $L(s, \widetilde{\chi_\lambda})L(s, \overline{\widetilde{\chi_\lambda}})$ 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 (3.1). Therefore, the local L-factors of $L(s, \widetilde{\chi_\lambda})L(s, \overline{\widetilde{\chi_\lambda}})$ at $\mathfrak{P}$ coinsides with the one of $L(\mathscr{E}_\lambda/\mathbb{Q}(\rho), s)$ at $\mathfrak{P}$.

If $\mathfrak{P} = (\lambda), (1 - \rho)$, then, $\mathscr{E}_\lambda$ has additive reduction at $\mathfrak{P}$ by Lemma 3.2 (1). Then, both of the local L-factors of $L(s, \widetilde{\chi_\lambda})L(s, \overline{\widetilde{\chi_\lambda}})$ and $L(\mathscr{E}_\lambda/\mathbb{Q}(\rho), s)$ are equal to 1. $\qquad\square$

3.3 Elliptic Gauss sums and Tate-Shafarevich groups

In this section, we show that the order of the Tate-Shafarevich group of the elliptic curve $\mathscr{E}_\lambda/\mathbb{Q}(\rho)$ is equal to the square of the absolute value of the coefficient α_λ of the relevant elliptic Gauss sum or its quarter under the BSD conjecture on the $2, 3$-parts of the leading term for $\mathscr{E}_\lambda/\mathbb{Q}(\rho)$. By combining this and Theorem 2.5, we obtain that the order of the Tate-Shafarevich group of $\mathscr{E}_\lambda/\mathbb{Q}(\rho)$ is congruent to the square of Bernoulli-Hurwitz-type numbers C_n, D_n times $1/9$ or $1/36$ modulo ℓ under the BSD conjecture on the $2, 3$-parts of the leading term. Unconditionally, we have such congruences up to the multiplications of powers of $2, 3$.

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

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

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

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

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

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

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

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

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

From this equation, we have $g_\lambda := \sum_{0 \neq \omega \in \varpi_\lambda \mathbb{Z}[\rho]} \frac{1}{\omega^6} = -\frac{\lambda^2}{140}$ by [S1, Theorem 3.5 (b) of Chap. VI]. On the other hand, by Lemma 1.2 (3), $g_1 := \sum_{0 \neq \omega \in \varpi_1 \mathbb{Z}[\rho]} \frac{1}{\omega^6} = \frac{27}{140}$ by loc. cit. Thus, we have $\frac{\varpi_\lambda^6}{\varpi_1^6} = \frac{g_1}{g_\lambda} = -\frac{27}{\lambda^2}$. By taking the absolute values, $\tau_\infty^3 = \frac{3^3}{\ell} \varpi_1^6$ since $\ell = \lambda \overline{\lambda} = |\lambda|^2$. Then, we have

$$\tau_\infty = \frac{3\varpi_1^2}{\ell^{\frac{1}{3}}}.$$

We recall that

$$\tau_{(\lambda)} = 3, \ \#\mathscr{E}_\lambda(\mathbb{Q}(\rho))_{\mathrm{tors}} = 3$$

by Lemma 3.2 (3), (6), respectively. If $s \in \mathbb{R}$, $\overline{L(s, \widetilde{\chi_\lambda})} = L(s, \overline{\widetilde{\chi_\lambda}})$. Thus, $L(1, \widetilde{\chi_\lambda}) \overline{L(1, \widetilde{\chi_\lambda})} = |L(1, \widetilde{\chi_\lambda})|^2$. Therefore,

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

by Proposition 3.4 and Lemma 3.5 (note that $\widetilde{\lambda}^3 = \lambda$, $(|\widetilde{\lambda}|^2)^3 = |\lambda|^2 = \ell$). Thus, $L(\mathscr{E}_\lambda/\mathbb{Q}(\rho), 1) \neq 0$ holds since Lemma 3.5. Hence, by [R, Theorem (i)], we have $\#\mathrm{III}(\mathscr{E}_\lambda/\mathbb{Q}(\rho)) < \infty$ and

$$L(\mathscr{E}_\lambda/\mathbb{Q}(\rho), 1) = \tau_\infty \tau_{(1-\rho)} \tau_{(\lambda)} \frac{\#\mathrm{III}(\mathscr{E}_\lambda/\mathbb{Q}(\rho))}{\#\mathscr{E}_\lambda(\mathbb{Q}(\rho))_{\mathrm{tors}}^2}, \tag{3.3}$$

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

$$\frac{|\alpha_\lambda|^2}{\ell^{\frac{1}{3}}} \varpi_1^2 = \frac{3\varpi_1^2}{\ell^{\frac{1}{3}}} \cdot 4 \cdot 3 \cdot \frac{\#\mathrm{III}(\mathscr{E}_\lambda/\mathbb{Q}(\rho))}{3^2},$$

up to the multiplications of powers of $2, 3$. Therefore, we have $\#\mathrm{III}(\mathscr{E}_\lambda/\mathbb{Q}(\rho)) = \frac{|\alpha_\lambda|^2}{4}$ up to the multiplications of powers of $2, 3$.

Otherwise, $\tau_{(1-\rho)} = 1$, we have

$$\frac{|\alpha_\lambda|^2}{\ell^{\frac{1}{3}}}\varpi_1^2 = \frac{3\varpi_1^2}{\ell^{\frac{1}{3}}} \cdot 1 \cdot 3 \cdot \frac{\#\mathrm{III}(\mathscr{E}_\lambda/\mathbb{Q}(\rho))}{3^2},$$

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

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

Remark 3.7. By the second supplementary law of the cubic reciprocity law, $n \equiv 0 \bmod 3 \iff \chi_\lambda(3) = 1$ holds, since $\chi_\lambda(3) = \rho^n$ by [L, the last formula in Theorem 7.8 of Chap. 7], where n is as in Theorem 3.6. (Note that the definition of primarity in [L, §7.1] is slightly different from the one in this paper, however, it does not effect the above equivalence.) Hence, if $\ell \equiv 7, 4 \bmod 9$ and $n \equiv 0 \bmod 3$, we have $\alpha_\lambda \in \mathbb{Z}$ by Theorem 2.3. Under the BSD conjecture on the 2-part of the leading term for the elliptic curve $\mathscr{E}_\lambda$, we have

$$n \equiv 0 \bmod 3 \implies 2|\alpha_\lambda \tag{3.4}$$

since Theorem 3.6. As long as the center of the table at [A, Table 1. in p.117], (3.4) is plausible. However, by the case of $p = 139$ in Asai's table, we cannot replace " $\implies$ " with " $\iff$ " in (3.4).

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

$$\#\mathrm{III}(\mathscr{E}_\lambda/\mathbb{Q}(\rho)) \underset{\bmod \lambda}{\equiv} \begin{cases} \left(\chi_\lambda(3)D_{\frac{2(\ell-1)}{3}}\right)^2/36 & \text{if } \ell \equiv 4 \bmod 9 \text{ and } n \equiv 0 \bmod 3, \\ \left(\chi_\lambda(3)D_{\frac{2(\ell-1)}{3}}\right)^2/9 & \text{if } \ell \equiv 4 \bmod 9 \text{ and } n \equiv \pm 1 \bmod 3, \\ \left(\overline{\chi_\lambda(3)}C_{\frac{2(\ell-1)}{3}}\right)^2/9 & \text{if } \ell \equiv 7 \bmod 9, \end{cases} \tag{3.5}$$

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

up to the multiplications of powers of $2, 3$. Moreover, for $p = 2, 3$, under the BSD conjecture on the p-part of the leading term for the elliptic curve $\mathscr{E}_\lambda$, the congruence (3.5) holds without the ambiguity of the multiplications of powers of p.

Proof. These congruences hold from Theorem 2.5, Theorem 3.6 and Lemma 2.7. $\qquad\square$

Remark 3.9. There exist infinitely many rational primes ℓ such that $\ell \equiv 7, 4 \bmod 9$ and $\mathbb{F}_\ell^\times/\langle 2, 3 \bmod \ell\rangle$ is not trivial, by Chebotarev's density theorem, where $\langle 2, 3 \bmod \ell\rangle$ is the subgroup generated by $2, 3 \bmod \ell$ of $\mathbb{F}_\ell^\times$.

A   Appendix

In this chapter, we show some lemmas and formulae which are very interesting, although they are not used in the proofs of the main results in this paper. In §A.1, we show lemmas on rational primes dividing the denominator of d_n. In §A.2, we determine the signs and the non-vanishing of C_n, D_n (excluding D_{6n+2}), and the Eisenstein series G_n associated to the lattice $\varpi_1\mathbb{Z}[\rho]$ (see Lemma A.1) by using new recurrence relations of them arising from new formulae of Sl. In §A.3, we give numerical tables of c_n, d_n, G_n, and BH_n.

A.1　On the denominator of d_n

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

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

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

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

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

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

Proof. First, we note that $G_{6n} \in \mathbb{Q}$ for $n \geq 0$, since $\wp(u) = \frac{1}{u^2} + \sum_{n=1}^{\infty}(6n-1)G_{6n}u^{6n-2}$ around $u = 0$ (note that $G_n = 0$ unless n is congruent to 0 modulo 6) and $\wp'' = 6\wp^2$. We prove the first equality of (A.1). Since Lemma 1.4 (9), we have

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

Around $u = 0$, we have $\wp(u) = \sum_{n=0}^{\infty}(6n-1)G_{6n}u^{6n-2}$, and $\frac{1}{\mathrm{Sl}(-3u)} + \frac{1}{\mathrm{Sl}(3u)} = 18\sum_{n=0}^{\infty}D_{6n+2}3^{6n}u^{6n+2}$ by the definitions. 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 (A.1) follows.

We prove the second equality of (A.1). Since Lemma 1.4 (10) and $3 = (1-\rho)(1-\overline{\rho})$, we have

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

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

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

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 (A.1) is proved. □

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

Lemma A.3. (The denominator of D_{6m+2}) For a rational prime $\ell \equiv 1 \bmod 3$ 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,

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

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

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

$$h_m 3^{6m} = -\sum_{k=0}^{m-1} h_k(6m-6k-1)\left(\prod_{\substack{\ell:\text{rational prime}\\ \ell\equiv 1 \bmod 3}} \ell^{t(\ell,m)-t(\ell,k)}\right) BH_{6(m-k)}\binom{6m}{6k}3^{6k}. \tag{A.2}$$

Since the elliptic curve $y^2 = 4x^3 - 27$ has good reduction (resp. good ordinary reduction) at ℓ if and only if $\ell \neq 3$ (cf. the proof of Lemma 3.2 (1)) (resp. $\ell \equiv 1 \bmod 3$ (see [S2, Chap II, exer. 2.30])), it holds that $\left(\prod_{\substack{\ell \text{ is rational prime}\\ \ell-1|6m\\ \ell\equiv 1 \bmod 3}} \ell\right) BH_{6m} \in \mathbb{Z}[\frac{1}{3}]$ by [Ka, Theorem]. In terms of m, $t(\ell,m)$ is nondecreasing. For $k = 0, \ldots, m-1$ and a rational prime $\ell \equiv 1 \bmod 3$, 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 (A.2) is $\in \mathbb{Z}\left[\frac{1}{3}\right]$. $\square$

Remark A.4. 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 3). If this is true, then the same proof of lemma also shows that

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

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

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

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

Lemma A.6. (1)

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

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

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

Proof. (1) We have

$$\frac{1}{\mathrm{Sl}(\sqrt{-3}u)} = \frac{1 + \overline{\rho}\,\mathrm{Sl}(u)^3}{\sqrt{-3}\,\mathrm{Sl}(u)\,\mathrm{Cl}(u)}$$

by [A, 2. (viii) of Appendix] or putting $u := \rho u$ and $v := -\overline{\rho}u$ of the addition formula of Sl (Lemma 1.5). By $\mathrm{Sl}(-u) = -\frac{\mathrm{Sl}(u)}{\mathrm{Cl}(u)}$ and $\mathrm{Cl}(-u) = \frac{1}{\mathrm{Cl}(u)}$ (Lemma 1.4 (8)), we have

$$\frac{1}{\mathrm{Sl}(-\sqrt{-3}u)} = \frac{-1 - \rho\,\mathrm{Sl}(u)^3}{\sqrt{-3}\,\mathrm{Sl}(u)\,\mathrm{Cl}(u)}.$$

Then, by two equalities and noting that $\rho - \overline{\rho} = \sqrt{-3}$, the first equality of (1) is proved. The second equality of (1) also follows from $\mathrm{Sl}(-u) = -\frac{\mathrm{Sl}(u)}{\mathrm{Cl}(u)}$ (Lemma 1.4 (8)). By lemma 1.9, $\mathrm{Sl}(u), \mathrm{Sl}(-u) \in \mathcal{H}_{\mathbb{Z}}$. Thus, $\mathrm{Sl}(u)\,\mathrm{Sl}(-u) \in \mathcal{H}_{\mathbb{Z}}$.

(2) By the definition, we have $\frac{1}{\mathrm{Sl}(\sqrt{-3}u)} + \frac{1}{\mathrm{Sl}(-\sqrt{-3}u)} = 2\sum_{n=0}^{\infty} d_{6n+2}(-3)^{3n+1}\frac{u^{6n+2}}{(6n+2)!}$. By (1), we have $2d_{6n+2}(-3)^{3n+1} \in \mathbb{Z}$. By Lemma A.5, $d_{6n+2}(-3)^{3n+1} \in \mathbb{Z}$.

$\square$

Lemma A.7. (The denominator of d_{6m-1}) For $m \geq 1$, we have

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

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

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

Since $(-1)^m 3^{3m-1} - 1 \equiv 2 \bmod 4$, $\frac{(-1)^m 3^{3m-1}-1}{2} \in \mathbb{Z}$. From [Ka, Theorem], $\left(\prod_{\substack{\ell \text{ is rational prime} \\ \ell-1|6m \\ \ell \equiv 1 \bmod 3}} \ell \right) BH_{6m} \in$

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

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

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

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

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

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

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

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

here, note that $G_0 = -1$. Then, we have the equality (A.3). By the proof of Lemma 1.2 (3), we have $G_6 = \frac{27}{140} > 0$. The positivity of G_{6n} for $n \geq 1$ follows by induction on n, (A.3) and $G_6 > 0$. Then, by the second equality of (A.1), we have

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

for $m \geq 1$. $\qquad \square$

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

Lemma A.10. (1) We have

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

27

for $n \geq 1$.

$$2 \cdot 3^{6n} c_{6n+4} = -(6n+4)(2n+1)(6n+2)3^{6n} c_{6n+1} + \sum_{k=1}^{n} c_{6(n-k)+4} BH_{6k}(6k-1)(6k-2)3^{6(n-k)} \binom{6n+4}{6k}$$

for $n \geq 1$.

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

(3) (The sign and the non-vanishing of e_n) We put $\mathrm{Cl}(u) =: \sum_{n=0}^{\infty} \frac{e_{3n}}{(3n)!} u^{3n}$, 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. (1) By $\mathrm{Sl}(u) = \varphi\left(\frac{u}{-3\varpi_1}\right) = \frac{6\wp\left(\frac{u}{3}\right)}{9 - \wp'\left(\frac{u}{3}\right)}$ (Lemma 1.4 (3)), $\mathrm{Sl}(u) = \sum_{n=0}^{\infty} C_{3n+1} u^{3n+1} = \sum_{n=0}^{\infty} C_{6n+1} u^{6n+1} + \sum_{n=0}^{\infty} C_{6n+4} u^{6n+4}$, $\wp(u) = \sum_{n=0}^{\infty} G_{6n}(6n-1) u^{6n-2}$ and $\wp'(u) = \sum_{n=0}^{\infty} G_{6n}(6n-1)(6n-2) u^{6n-3}$, we have

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

Taking the even part of (A.4),

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

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

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

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

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

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

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

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

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

Therefore,

$$(6n+4)(2n+1)(6n+2)3^{6n} c_{6n+1} = -2 \cdot 3^{6n} c_{6n+4} + \sum_{k=1}^{n} c_{6(n-k)+4} BH_{6k}(6k-1)(6k-2)3^{6(n-k)} \binom{6n+4}{6k}$$

follows. This is the second equality of (1).

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

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

$\square$

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

A.3 Numerical tables of c_n, d_n, G_{6n}, and BH_{6n}

Table 1: c_n

n	c_n
1	1
4	-4
7	160
10	-20800
13	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	$-18474617726618802329201889210788021182113749879750656000000000000$
61	723544590939960717069350289218516137325917930092538888192000000000000
64	$-3280456305171371413525294691303861562668456710283801034489856000000000000$
67	17101062556199045349300255723604273974290886339141262190021548441600000000000000

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	$5835679909517861675008000000/575757$
	$= 2^{20} \cdot 5^7 \cdot 11^3 \cdot 17^2 \cdot 23 \cdot 29 \cdot 43 \cdot 1871 \cdot 34511/3^2 \cdot 7 \cdot 13 \cdot 19 \cdot 37$
38	$9304580611314692915200000000/3$
	$= 2^{24} \cdot 5^7 \cdot 11^3 \cdot 17^2 \cdot 23 \cdot 29 \cdot 701 \cdot 3947/3$
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	$102789613347709769146353217699840000000/273$
	$= 2^{26} \cdot 5^8 \cdot 11^4 \cdot 17^2 \cdot 23^2 \cdot 29 \cdot 41 \cdot 47 \cdot 313 \cdot 1001523179/3 \cdot 7 \cdot 13$
50	$8030649112422447620287537086464000000000/3$
	$= 2^{32} \cdot 5^{10} \cdot 11^5 \cdot 17^2 \cdot 23^2 \cdot 29 \cdot 41 \cdot 47 \cdot 61 \cdot 2029 \cdot 11243/3$
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	$-22871478427768693526299780079937388544000000000000/3$
	$= -2^{36} \cdot 5^{11} \cdot 11^5 \cdot 17^3 \cdot 23^2 \cdot 29 \cdot 41 \cdot 47 \cdot 53 \cdot 137 \cdot 4013306567/3$

Table 3: G_{6n}, and BH_{6n}

n	G_n	BH_n
6	27/140	972/7
12	729/112112	283435200/91
18	19683/184352896	90914674752000/133
24	9034497/2269709478400	2247402032060663808000/91
30	961376769/9936195998310400	55692060030763170322176000000/217
36	45251875376667/15343234021377167360000	491303185206504946068649519911075840000/447811
42	340935337980693/43280194527500713689088000	3331405704064326374257129065333532262400000/301

References

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

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

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

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

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

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

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

[L]   Lemmermeyer, F., "Reciprocity Laws : From Euler to Eisenstein", Springer-Verlag (2000).

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

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

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

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

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

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