Integrality of Coefficients of Division Polynomials for Elliptic Functions

Yoshihiro Ônishi

Introduction

By this paper we show that the coefficients of the denominator (hence the numerator) of λ-plication formula, where $\lambda \in \mathbf{Z}[\boldsymbol{i}]$, for the Weierstrass $\wp$-function associated to the leminiscate $y^2 = x^3 - x$ belong to $\lambda \in \mathbf{Z}[\boldsymbol{i}]$. When almost every student who started complex multiplication of elliptic function faces this fact, he/she may troubles that description of Eisenstein's original paper is too deep for beginners and there are no other references which provides a precise proof of this. So the author think this paper might be useful.

Our method hardly use the Weierstrass sigma function. The first part treats any elliptic curve. The second part is restricted to the lemniscate. The method of this paper is applicable for equianhormonic case, that is for the curve $y^2 = x^3 - 1$.

1 General Theory

1.1 Notations

Let consider the most general elliptic curve, say C, which is defined by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4 + a_6. \tag{1.1}$$

This is proper curve with unique point ∞ at infinity. Let

$$\omega = \frac{dx}{2y + a_1x + a_3}, \quad \eta = \frac{xdx}{2y + a_1x + a_3} \tag{1.2}$$

are canonical differential form of the 1st kind and of the 2nd kind. We denote by Λ the lattice in the complex plane $\mathbb{C}$ consists of all the periods of ω:

$$\Lambda = \Big\{ \oint \omega \ ; \text{ for all closed paths of integral} \Big\}. \tag{1.3}$$

We fix a symplectic base α_1, β_1 of 1-dimensional homology group over $\mathbf{Z}$. Let

$$\begin{cases} \omega' = \int_{\alpha_1} \omega \ \ \Big(= \int_{\alpha_1} \frac{dx}{2y+a_1x+a_3} \Big), \\ \omega'' = \int_{\beta_1} \omega \ \ \Big(= \int_{\beta_1} \frac{dx}{2y+a_1x+a_3} \Big) \end{cases} \tag{1.4}$$

and

$$\begin{cases} \eta' = \int_{\alpha_1} \eta \ \ \Big(= \int_{\alpha_1} \frac{xdx}{2y+a_1x+a_3} \Big), \\ \eta'' = \int_{\alpha_1} \eta \ \ \Big(= \int_{\beta_2} \frac{xdx}{2y+a_1x+a_3} \Big). \end{cases} \tag{1.5}$$

For each $v \in \mathbf{C}$, we denote by v', $v'' \in \mathbf{R}$ the elements such that

$$v = v'\omega_1 + v''\omega_2. \tag{1.6}$$

Then, for instance, $\ell \in \Lambda$ is written as

$$\ell = \ell'\omega_1 + \ell''\omega_2 \tag{1.7}$$

for ℓ', $\ell' \in \mathbf{Z}$. We define

$$L(u, v) = u(v'\eta_1 + v''\eta_2). \tag{1.8}$$

1.2 Basic facts

The *sigma function* of the curve C is an entire function and has the following properties:

$$\begin{aligned} &\sigma(u) = u + \text{“higher terms with respect to } u\text{”}, \\ &\sigma(u) = 0 \iff u \in \Lambda, \\ &\sigma(u+\ell) = \chi(\ell)\sigma(u)\exp L(u+\tfrac{1}{2}\ell, \ell) \ \text{ for all } \ell \in \Lambda \text{ and } u \in \mathbf{C}. \end{aligned} \tag{1.9}$$

For the definition of the sigma functions and its properties, see [Ô]. Let

$$E(u,v) = L(u,v) - L(v,u). \tag{1.10}$$

This is the *Riemann form* associated to C.

Lemma 1.11. For the Riemann form $E(\ ,\ )$, one has that
(1) $E(\boldsymbol{i}u, v) = E(\boldsymbol{i}v, u)$,
(2) $E(u,v) = 2\pi\boldsymbol{i}(u'v'' - u''v')$.
Especially, $E(\ ,\ )$ is $\boldsymbol{i}\mathbf{R}$-valued form and $2\pi\boldsymbol{i}\mathbf{Z}$-valued on $\Lambda \times \Lambda$.

Proof.

$$\begin{aligned} E(u,v) &= L(u,v) - L(v,u) \\ &= (u'\omega' + u''\omega'')\,(v'\eta' - v''\eta'') - (v'\omega' + v''\omega'')\,(u'\eta' - u''\eta'') \\ &= (\eta''\omega' - \eta'\omega'')\,(u'v'' - u''v') \end{aligned} \tag{1.12}$$

The Legendre relation $\eta''\omega' - \eta'\omega'' = 2\pi\boldsymbol{i}$ shows the assertion (2). In the equation

$$\begin{aligned} E(\boldsymbol{i}u, v) - E(\boldsymbol{i}v, u) &= L(\boldsymbol{i}u, v) - L(v, \boldsymbol{i}u) - L(\boldsymbol{i}v, u) + L(u, \boldsymbol{i}v) \\ &= \boldsymbol{i}L(u,v) + \boldsymbol{i}L(\boldsymbol{i}v, \boldsymbol{i}u) - \boldsymbol{i}L(v,u) + \boldsymbol{i}L(\boldsymbol{i}u, \boldsymbol{i}v) \\ &= \boldsymbol{i}\big(E(u,v) - E(\boldsymbol{i}u, \boldsymbol{i}v)\big) \end{aligned} \tag{1.13}$$

the first belongs $\boldsymbol{i}\mathbf{R}$ and the last belongs $\mathbf{R}$. Hence this must be 0. □

The function defined by

$$\wp(u) = \tfrac{\partial^2}{\partial u^2}\log\sigma(u) \tag{1.14}$$

is an Abelian function associated to the curve C. Namely, this is periodic with respect to Λ:

$$\wp(u+\ell) = \wp(u)$$

for all $u \in \mathbb{C}$ and for all $\ell \in \Lambda$. This coincides with the Weierstrass $\wp$-function if and only if ${a_1}^2 + 4a_2 = 0$. Let (x,y) be a variable point on C and let

$$u = \int_\infty^{(x,y)} \omega = \int_\infty^{(x,y)} \frac{dx}{2y + a_1 x + a_3}. \tag{1.15}$$

We consider the inverse functions $u \mapsto x(u)$, $u \mapsto y(u)$ determined by this equation. For these functions, we see easily that

$$\begin{aligned} &\wp(u) = x(u), \\ &\wp'(u) \ \big(= \tfrac{\partial}{\partial u}\wp(u) \big) \ = 2\, y(u) + a_1 x(u) + a_3. \end{aligned} \tag{1.16}$$

and have the relation which expresses $\wp'(u)^2$ as a cubic polynomial of $\wp(u)$. Now we state the *formula of Frobenius-Stickelberger*:

Proposition 1.17. *Assume $n \geqq 2$. Then one has*

$$\begin{aligned} &\frac{\sigma(u^{(1)} + \cdots + u^{(n)}) \prod_{i<j} \sigma(u^{(i)} - u^{(j)})}{\prod_j \sigma(u^{(j)})^n} \\ &= \begin{vmatrix} 1 & x(u^{(1)}) & y(u^{(1)}) & x^2(u^{(1)}) & yx(u^{(1)}) & x(u^{(1)})^3 & yx^2(u^{(1)}) & \cdots \\ 1 & x(u^{(2)}) & y(u^{(2)}) & x^2(u^{(2)}) & yx(u^{(2)}) & x(u^{(2)})^3 & yx^2(u^{(2)}) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\ 1 & x(u^{(n)}) & y(u^{(n)}) & x^2(u^{(n)}) & yx(u^{(n)}) & x(u^{(n)})^3 & yx^2(u^{(n)}) & \cdots \end{vmatrix} \end{aligned} \tag{1.18}$$

where the right hand side is an $n \times n$-matrix truncated by the n-th column, and, for instance, $xy(u)$ means the product $x(u)\, y(u)$.

Proof. Using the 3rd property in (1.9), we see the left hand side is completely periodic with respect to Λ. We prove the formula by induction on n. We regard the left hand side as a function function of $u^{(n)}$ on the Jacobian $\mathbb{C}/\Lambda$ of C. Using the 2nd property in (1.9), we see the divisor (in the sense of algebraic geometry) of left hand side. That is, it has pole only at 0 (modulo Λ) whose order is n, and has zeroes of order 1 at least at $u^{(1)}$, $\cdots$, $u^{(n-1)}$. On the other hand the right hand side has pole only at 0 (modulo Λ) whose order is n, and has zeroes of order 1 at least at $u^{(1)}$, $\cdots$, $u^{(n-1)}$ (modulo Λ). So, let α be the remaining zero. Then Abel-Jacobi theorem shows that

$$u^{(1)} + u^{(2)} + \cdots + u^{(n-1)} + \alpha \in \Lambda.$$

We denote

$$u^{(1)} + u^{(2)} + \cdots + u^{(n-1)} + \alpha = \ell.$$

Since

$$\sigma(u^{(1)} + \cdots + u^{(n-1)} + u^{(n)}) = \sigma(\ell - \alpha + u^{(n)}),$$

by the 3rd property in (1.9) again, we see this vanishes at $\alpha + \Lambda$ with 1st order. Hence the two sides have exactly the same divisor. Then, by looking at the leading coefficients of Laurent expansions of both sides with respect to $u^{(n)}$, we reduce this to the induction hypothesis. So we get the desired formula. □

We write down this formula. If $n = 2$, then

$$\frac{\sigma(u^{(1)} + u^{(2)})\sigma(u^{(1)} - u^{(2)})}{\sigma(u^{(1)})^2\, \sigma(u^{(2)})^2} = \begin{vmatrix} 1 & x(u^{(1)}) \\ 1 & x(u^{(2)}) \end{vmatrix}. \tag{1.19}$$

If $n = 3$, we have

$$\begin{aligned}&\frac{\sigma(u^{(1)}+u^{(2)}+u^{(3)})\,\sigma(u^{(1)}-u^{(2)})\,\sigma(u^{(1)}-u^{(3)})\,\sigma(u^{(2)}-u^{(3)})}{\sigma(u^{(1)})^3\,\sigma(u^{(2)})^3\,\sigma(u^{(3)})^3}\\ &= \begin{vmatrix} 1 & x(u^{(1)}) & y(u^{(1)}) \\ 1 & x(u^{(2)}) & y(u^{(2)}) \\ 1 & x(u^{(3)}) & y(u^{(3)}) \end{vmatrix}.\end{aligned} \tag{1.20}$$

From the formula

$$\lim_{u\to v}\frac{\sigma(u-v)}{u-v} = 1 \tag{1.21}$$

which is easily checked, we see by (1.19) that

$$\frac{\sigma(2u)}{\sigma(u)^4} = 2\,y(u), \tag{1.22}$$

though this is never used in this paper. Taking limit that all points $u^{(j)}$ approaching a point u with straightforward caluculation, we get the following:

Proposition 1.23. (Kiepert) *For any integer $n \geqq 1$, one has*

$$\frac{\sigma(nu)}{\sigma(u)^{n^2}} = \frac{1}{1!\,2!\cdots(n-1)!}\begin{vmatrix} x'(u) & y(u) & (x^2)'(u) & (yx)'(u) & \cdots \\ x''(u) & y'(u) & (x^2)''(u) & (yx)''(u) & \cdots \\ x'''(u) & y''(u) & (x^2)'''(u) & (yx)'''(u) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \\ x^{(n-1)}(u) & y^{(n-1)}(u) & (x^2)^{(n-1)} & (yx)^{(n-1)}(u) & \cdots \end{vmatrix}. \tag{1.24}$$

1.3 The integrality theorem

Lemma 1.25. *Let $m \geqq 0$ and $k \geqq 0$ are integers. Then for the k-th derivatives, one has*

$$\tfrac{1}{k!}\big(yx^m(u)\big)^{(k)},\quad \tfrac{1}{k!}\big(x^m(u)\big)^{(k)} \;\in\; \mathbf{Z}[x(u)] + y(u)\,\mathbf{Z}[x(u)]. \tag{1.26}$$

Proof. By the definition of (1.15) of u, we have $du = dx/(2y + a_1x + a_3)$. Hence, $x'(u) = 2y(u) + a_1x(u) + a_3$. Since $(2y + a_1x + a_3)\,dy/dx = 3x^2 + a_2x + a_4$ by the defining equation of C, we see $y'(u) = -a_1y(u) + 3x(u)^2 + a_2x^2 + a_4x + a_6$. Using Leibniz rule, we see the statement. □

For any integer n, let

$$\psi_n(u) = \frac{\sigma(nu)}{\sigma(u)^{n^2}}. \tag{1.27}$$

This is a periodic function with respect to Λ because of the 3rd property of (1.9), and is a polynomial of $x(u)$ and $y(u)$ because of the 2nd property of (1.9. Since $\psi(u) = 0$ for $u \notin \Lambda$ if and only if $nu \in \Lambda$, this is called the *n-division polynomial* of the function $u \mapsto x(u)$.

We consider *n-plication formula* for $\wp(u)(=x(u))$:

$$\wp(nu) = \frac{\sigma'(nu)^2 - \sigma''(nu)\sigma(nu)}{\sigma(nu)^2} = \frac{\frac{\sigma'(nu)^2-\sigma''(nu)\sigma(nu)}{\sigma(u)^{n^2}}}{\left(\frac{\sigma(nu)}{\sigma(u)^{n^2}}\right)^2},$$

where σ' and σ'' are the 1st and 2nd derivatives of the function σ, respectively.

Theorem 1.28. (Eisenstein) *The n-division polynomial $\psi_n(u)$ is expressed as*

$$\psi_n(u) = \begin{cases} n\,x(u)^{(n^2-1)/2} + \cdots + 1 \ \in \mathbf{Z}[x(u)] & \text{if } n \text{ is odd,} \\ \frac{1}{2}\,x'(u)\big(n\,x(u)^{(n^2-1)/2} + \cdots + 1\big) \ \in x'(u)\mathbf{Z}[x(u)] & \text{if } n \text{ is even.} \end{cases} \tag{1.29}$$

Namely, this is a polynomial of $x(u)$ over $\mathbf{Z}$ of degree $\frac{1}{2}(n^2-1)$ with the coefficient of the highest term n and the constant term 1 or it times $x'(u)$. Moreover, the denominator $x(nu)\psi_n(u)^2$ of $x(nu)$ is also belongs to $\mathbf{Z}[\,x(u)]$.

Proof. From 1.25 and 1.23, it is obvious that $\psi_n(u) \in \mathbf{Z}[x(u)]$ or $\in x'(u)\mathbf{Z}[x(u)]$ according to n is odd or even. The coefficient of the highest term is n because

$$\begin{aligned} \psi_n(u) &= \frac{\sigma(nu)}{\sigma(u)^{n^2}} \\ &= \frac{nu + \cdots}{u^{n^2}} + \cdots \\ &= n\,\frac{1}{u^{n^2-1}} + \cdots \\ &= n\,\wp(u)^{(n^2-1)/2} + \cdots, \end{aligned} \tag{1.30}$$

and the constant term is 1 because

$$\begin{aligned} \psi_n(v+u_0) &= \frac{\sigma(n(v+u_0))}{\sigma(v+u_0)^{n^2}} \\ &= \frac{\chi((n-1)u_0)\sigma(u_0)^{n^2-1}\sigma(nv+u_0)}{\sigma(v+u_0)^{n^2-1}\sigma(v+u_0)} + \cdots \quad \text{(by (2.23))} \\ &= \frac{\sigma(nv+u_0)}{\sigma(v+u_0)} + \cdots \\ &= 1 + (d^\circ \geqq 1) \quad (\text{ since } \sigma(u_0) \neq 0\ ). \end{aligned} \tag{1.31}$$

□

1.4 Hermitian property of the form $L(\ ,\ )$

We shall explain a fact that the sigma function $\sigma(u)$ associated to an elliptic curve with "big" (geometric) automorphism group is a *normalized theta function*.

Lemma 1.32. *For the bilinear form $L(u,v)$ defined in (1.8),*

$$L(u,v) = \frac{1}{2\boldsymbol{i}}[E(\boldsymbol{i}u,v) + \boldsymbol{i}E(u,v)] \tag{1.33}$$

for any $u,\ v \in \mathbf{C}$ if and only if $L(u,v)$ is a skew hermitian form. So that, (1.33) is equivalent to $L(v,u) = -\overline{L(u,v)}$, where $\bar{}$ means the complex conjugation.

If $L(u,v)$ is a skew hermitian form, the function $\sigma(u)$ is a *normalized theta function* in G. Shimura's sense.

Lemma 1.34. *If the periods ω', ω'', η', and η'' defined in (1.2) satisfies ${\omega'}^{-1}\eta'' = \overline{{\omega'}^{-1}\omega''}$, then $L(u,v)$ is a hermitian form.*

Proof. Let $Z = {\omega'}^{-1}\omega''$. By the definition of $L(\ ,\ )$, we see $L(\boldsymbol{i}u, v) = \boldsymbol{i}L(u,v)$. Firstly, we show $L(u, \boldsymbol{i}v) = -\boldsymbol{i}L(u,v)$. For a given v, we define w', $w'' \in \mathbf{R}$ by $\boldsymbol{i}{\omega'}^{-1}v = w' + Zw''$. Then $-\boldsymbol{i}\,\overline{{\omega'}^{-1}v} = w' + \overline{Z}w''$. Since ${\omega'}^{-1}v = v' + Zv''$ and $\overline{{\omega'}^{-1}v} = v' + \overline{Z}v''$, we have

$$
\begin{aligned}
L(u, \boldsymbol{i}v) &= u(\eta' w' + \eta'' w'') \\
&= u\eta'(w' + \overline{Z}w'') \\
&= u\eta'(-\boldsymbol{i}\,\overline{{\omega'}^{-1}v}) \\
&= u\eta'(-\boldsymbol{i})(v' + \overline{Z}v'') \\
&= -\boldsymbol{i}u(\eta' v' + \eta'' v'') \\
&= -\boldsymbol{i}L(u,v).
\end{aligned} \tag{1.35}
$$

Therefore,

$$
E(\boldsymbol{i}u, v) = L(\boldsymbol{i}u, v) - L(v, \boldsymbol{i}u) = \boldsymbol{i}L(u,v) - L(v, \boldsymbol{i}u) = \boldsymbol{i}L(u,v) + \boldsymbol{i}L(v,u). \tag{1.36}
$$

On the other hand, by the definition, we see

$$
\boldsymbol{i}E(u,v) = \boldsymbol{i}L(u,v) - \boldsymbol{i}L(v,u). \tag{1.37}
$$

By adding this to 1.11 (1), we get (1.33). □

2 The case of leminiscate

2.1 Basics

The rest of this paper we assume C is the lemniscate

$$y^2 = x^3 - x. \tag{2.1}$$

Thus,

$$\wp'(u)^2 = 4\wp(u)^3 - 4\wp(u). \tag{2.2}$$

In this case, we have

$$\omega = \frac{dx}{2y}, \quad \eta = \frac{xdx}{2y}, \tag{2.3}$$

and take α and β satisfying

$$\boldsymbol{i}\omega' = \omega'', \quad -\boldsymbol{i}\eta' = \eta''. \tag{2.4}$$

Then $\eta'^{-1}\eta'' = \boldsymbol{i} = \overline{\omega'^{-1}\omega''}$. By 1.34, the associating $\sigma(u)$ is normalized.

2.2 Riemann forms

For our C of (2.1), the endomorphism ring of its Jacobian variety is canonically isomorphic to the ring $\mathbf{Z}[i]$. We take and fix a point u_0 of $\mathbf{C}$ that corresponds to the point $0,\ 1$ of C:

$$\text{mod } \Lambda \text{ map } :\ \mathbf{C} \ni u_0 \mapsto (0,1) \in C. \tag{2.5}$$

Explicitly, by a suitable path of the integral, we have

$$u_0 = \tfrac{(\boldsymbol{i}-1)\omega}{2} = -\tfrac{1}{2}\,\omega' + \tfrac{1}{2}\,\omega''. \tag{2.6}$$

Lemma 2.7. *For $\lambda \in \mathbf{Z}[\boldsymbol{i}]$, one has $E(\lambda u, v) = E(u, \overline{\lambda} v)$.*

Proof. This fact comes from that the endomorphism ring of the Jacobian variety of C is generated over $\mathbf{Z}$ by the (geometric) automorphismrphisms of C. For any integer j, there exists a matrix $M(\boldsymbol{i}^j)$ such that

$$\boldsymbol{i}^j u = [\omega' \ \ \omega'']M(\boldsymbol{i}^j)\begin{bmatrix} u' \\ u'' \end{bmatrix}. \tag{2.8}$$

Since the multiplication by $\boldsymbol{i}$ corresponds to the automorphism $(x, y) \mapsto (\boldsymbol{i}x, -y)$ of C, it induces an automorphism of the fundamental group of C. Hence, ${}^tM(\boldsymbol{i}^j)JM(\boldsymbol{i}^j) = J$, where $J = \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}$. For a given u, we define U' and $U'' \in \mathbb{R}$ by

$$\boldsymbol{i}^j U = U'\omega' + U''\omega'', \tag{2.9}$$

namely, by

$$\begin{bmatrix} U' \\ U'' \end{bmatrix} = M(\boldsymbol{i}^j) \begin{bmatrix} u' \\ u'' \end{bmatrix}, \tag{2.10}$$

and for a given v, we define V' と $V'' \in \mathbb{R}$ by

$$\begin{bmatrix} V' \\ V'' \end{bmatrix} = M(\boldsymbol{i}^j) \begin{bmatrix} v' \\ v'' \end{bmatrix}. \tag{2.11}$$

Then, we have

$$\begin{aligned} E(\boldsymbol{i}^j u, v) &= 2\pi\boldsymbol{i}({}^tU'v'' - {}^tU''v') \\ &= 2\pi\boldsymbol{i}[{}^tU \ {}^tU''] J \begin{bmatrix} v' \\ v'' \end{bmatrix} \\ &= 2\pi\boldsymbol{i}[{}^tu \ {}^tu''] {}^tM(\boldsymbol{i}^j) J \begin{bmatrix} v' \\ v'' \end{bmatrix} \\ &= 2\pi\boldsymbol{i}[{}^tu \ {}^tu''] M(\boldsymbol{i}^{-j}) J \begin{bmatrix} v' \\ v'' \end{bmatrix} \\ &= 2\pi\boldsymbol{i}[{}^tu \ {}^tu''] J \begin{bmatrix} V' \\ V'' \end{bmatrix} \\ &= 2\pi\boldsymbol{i}({}^tu'V'' - {}^tu''V') \\ &= E(u, \overline{\boldsymbol{i}^j} v). \end{aligned} \tag{2.12}$$

By the linearity, the statement follows. □

Lemma 2.13. *Let c be a rational number, and λ be an element of $\mathbf{Z}[\boldsymbol{i}]$. Suppose $\overline{\lambda} \equiv \lambda \bmod c^2$. Let $v_0 \in \mathbf{C}$ be a point such that $cv_0 \in \Lambda$. Then*

$$L(\lambda v_0, v_0) \equiv L(v_0, \lambda v_0) \bmod 2\pi\boldsymbol{i}\mathbf{Z}. \tag{2.14}$$

Proof. Because of $\overline{\lambda} - \lambda \equiv 0 \bmod c^2$, we have $\overline{\lambda} - \lambda = ac^2$ for some $a \in \mathbf{Z}[\boldsymbol{i}]$. Then $cv_0 \in \Lambda$. So that, by (1.11), we have

$$E(v_0, (\overline{\lambda} - \lambda)v_0) = E(\overline{c}v_0, acv_0) = E(cv_0, acv_0) \in 2\pi\boldsymbol{i}\mathbf{Z}. \tag{2.15}$$

This and (2.7) yield that

$$\begin{aligned} E(\lambda v_0, v_0) &= E(v_0, \overline{\lambda} v_0) \\ &= E(v_0, (\overline{\lambda} - \lambda)v_0 + \lambda v_0) \\ &= E(v_0, (\overline{\lambda} - \lambda)v_0) + E(v_0, \lambda v_0) \\ &\equiv E(v_0, \lambda v_0) \bmod 2\pi\boldsymbol{i}\mathbf{Z}. \end{aligned} \tag{2.16}$$

Since

$$E(\boldsymbol{i}\lambda v_0, v_0) = E(\boldsymbol{i}v_0, \lambda v_0) \tag{2.17}$$

by 1.11(1), we see from 1.33 that

$$L(\lambda v_0, v_0) = \tfrac{1}{2\boldsymbol{i}}\big(E(\boldsymbol{i}\lambda v_0, v_0) + \boldsymbol{i}E(\lambda v_0, v_0)\big) \equiv L(v_0, \lambda v_0) \bmod 2\pi\boldsymbol{i}\mathbf{Z}. \tag{2.18}$$

□

2.3 Power series expansion of $\sigma(u)$

Proposition 2.19. $\sigma(u_0)^4 = \exp[2L(u_0, u_0)]$.

Proof. Derivating the equation

$$\sigma(2u) = 2y(u)\sigma(u)^4 \tag{2.20}$$

implies

$$2\,\sigma'(2u) = 2\tfrac{dx}{du}\tfrac{dy}{dx}\sigma(u)^4 = y(u)\tfrac{3x^2-1}{2y}(u)\sigma(u)^4. \tag{2.21}$$

Substituting $u = u_0$ shows that $-2\sigma(u_0)^4 = 2\sigma'(2u_0)$. On the other hand, by using $\sigma'(0) = 1$ and $\sigma(0) = 0$, after derivating

$$\sigma(u + 2u_0) = \chi(2u_0)\sigma(u)\exp[L(u + u_0, 2u_0)] \ \text{ from (1.9)} \tag{2.22}$$

by substituting $u = 0$ shows that $\sigma'(2u_0) = -\exp(2L(u_0, u_0))$. Here, $\chi(2u_0) = -1$ is easily checked by its definition. Summing up, we have arrived that $\sigma(u_0)^4 = \exp[2L(u_0, u_0)]$. □

Lemma 2.23. *Let λ be an element in $\mathbf{Z}[\boldsymbol{i}]$. If $\lambda \equiv 1 \bmod 4$, then*

$$\sigma(\lambda(v + u_0)) = \chi((\lambda - 1)u_0)\sigma(u_0)^{\mathrm{N}\lambda-1}\sigma(\lambda v + u_0)(1 + O(u)). \tag{2.24}$$

Proof. Since $\lambda \equiv 1 \bmod 4$, we have $\mathrm{N}\lambda \equiv 1 \bmod 4$. The statement follows from 4.2.8(1) and

$$\exp[\tfrac{1}{2}(\lambda\overline{\lambda} - 1)L(u_0, u_0)] = \sigma(u_0)^{\mathrm{N}\lambda-1} \tag{2.25}$$

which is given by 5.2.1. □

In our case, Lemma 1.25 is rewritten as follows:

Lemma 2.26. *Let $m \geqq 0$ and $k \geqq 0$ be integers. Then for k-th order derivatives, one has*

$$\tfrac{1}{k!}\big(yx^m(u)\big)^{(k)},\ \ \tfrac{1}{k!}\big(x^m(u)\big)^{(k)} \ \in\ \mathbf{Z}[x(u)] \ \text{ または } \ y(u)\,\mathbf{Z}[x(u)]. \tag{2.27}$$

Proof. These are easily shown by $y'(u) = 3x(u)^2 - 1$ and the Leibniz rule inductively. □

Theorem 2.28. (Eisenstein) *Suppose that $\lambda \in \mathbf{Z}[i]$ satisfies $\lambda \equiv 1 \bmod 4$. Then*

$$\psi_\lambda(u) = \frac{\sigma(\lambda u)}{\sigma(u)^{\mathrm{N}\lambda}} \tag{2.29}$$

is of the form

$$\psi_\lambda(u) = \lambda\, x(u)^{(\mathrm{N}\lambda-1)/2} + \cdots + 1 \ \in \mathbf{Z}[\boldsymbol{i},\, x(u)]. \tag{2.30}$$

Namely, it is a polynomial of $x(u)$ over $\mathbf{Z}[\boldsymbol{i}]$ of degree $\frac{1}{2}(\mathrm{N}\lambda - 1)$ with the coefficient of the highest term λ, and the constant term 1. Moreover, $u \mapsto x(\lambda u)\psi_\lambda(u)^2 \in \mathbf{Z}[\boldsymbol{i},\, x(u)]$ and the sequence of its coefficients are just the reverse order of them of $\psi_\lambda(u)$ with respect to $x(u)$.

Proof. Calculation by taking limit as we derived 1.23 from 1.17, we have easily seen by 2.26 and 1.17 that $\psi_\lambda(u) \in \mathbf{Z}[\boldsymbol{i}, x(u)]$ for $\lambda \in \mathbf{Z}$. The coefficient of the highest term is λ because

$$\begin{aligned} \psi_\lambda(u) &= \frac{\sigma(\lambda u)}{\sigma(u)^{\mathrm{N}\lambda}} \\ &= \frac{\lambda u + \cdots}{u^{\mathbf{N}\lambda} + \cdots} \\ &= \lambda \frac{1}{u^{\mathbf{N}\lambda - 1}} + \cdots \\ &= \lambda\, \wp(u)^{(\mathbf{N}\lambda-1)/2} + \cdots , \end{aligned} \tag{2.31}$$

and the constant term is 1 because

$$\begin{aligned} \psi_\lambda(v + u_0) &= \frac{\sigma(\lambda(v+u_0))}{\sigma(v+u_0)^{\mathrm{N}b}} \\ &= \frac{\chi((\lambda-1)u_0)\sigma(u_0)^{\mathrm{N}\lambda-1}\sigma(\lambda v + u_0)}{\sigma(v+u_0)^{\mathrm{N}\lambda-1}\sigma(v+u_0)} + \cdots \quad \text{(by (2.23))} \\ &= \frac{\sigma(\lambda v + u_0)}{\sigma(v+u_0)} + \cdots \\ &= 1 + (d^\circ \geqq 1) \quad (\text{ since } \sigma(u_0) \neq 0\ ). \end{aligned} \tag{2.32}$$

Hence, our Theorem has been proved. □

References

[Ô] Y. Ônishi: Universal elliptic functions, `http://arxiv.org/abs/1003.2927`