SPECIAL VALUES OF j-FUNCTION WHICH ARE ALGEBRAIC

KIM, SUNGJIN

1. Introduction

Let $E_k(z) = \frac{1}{2}\sum_{(c,d)=1}(cz+d)^{-k}$ be the Eisenstein series of weight $k > 2$. The j-function on the upper half plane is defined by $j(z) = \frac{E_4^3}{\Delta}$ where $\Delta(z) = \frac{1}{1728}(E_4^3 - E_6^2)$. For a primitive positive definite quadratic form $Q(x,y) = ax^2 + bxy + cy^2$, and $z_Q = \frac{-b+\sqrt{D}}{2a}$ with $D = b^2 - 4ac < 0$, it is known that $j(z_Q)$ is an algebraic integer of degree $h(D)$ by Kronecker and Weber. Here, we show a weaker result that $j(z_Q)$ is an algebraic number of degree at most the class number $h(D)$ using the j-invariant of a complex lattice, orders in an imaginary quadratic field, and complex multiplication.

Theorem 1.1. *For a primitive positive definite quadratic form $Q(x,y) = ax^2 + bxy + cy^2$, and $z_Q = \frac{-b+\sqrt{D}}{2a}$ with $D = b^2 - 4ac < 0$, $j(z_Q)$ is an algebraic number of degree at most the class number $h(D)$.*

2. j-invariant of a complex lattice

Definition 2.1. A subgroup L of $\mathbb{C}$ is called a *complex lattice* if $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ with $\omega_1, \omega_2 \in \mathbb{C}$ being linearly independent over $\mathbb{R}$. We simply write $L = [\omega_1, \omega_2]$. We say that two lattices L and L' are *homothetic* if there is a nonzero complex number λ such that $L' = \lambda L$. Note that homothety is an equivalence relation.

Definition 2.2. *Weierstrass $\wp$-function* associated to a complex lattice $L = [\omega_1, \omega_2]$ is defined by:

$$\wp(z;L) = \frac{1}{z^2} + \sum_{w \in L-\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right). \tag{2.1}$$

We simply write $\wp(z) = \wp(z;L)$. Note that $\wp(z+w) = \wp(z)$ for all $w \in L$.

Lemma 2.1. *Let $G_k(L) = \sum_{w\in L-\{0\}} w^{-k}$ for $k > 2$. Then, Weierstrass $\wp$-function for a lattice L has Laurent expansion*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(L)z^{2n}. \tag{2.2}$$

Proof. We have the series expansion

$$\frac{1}{(1-x)^2} = 1 + \sum_{n=1}^{\infty}(n+1)x^n$$

for $|x| < 1$. Thus, if $|z| < |w|$, we have

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \sum_{n=1}^{\infty} \frac{n+1}{w^{n+2}} z^n.$$

Summing over w, we obtain

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}(L)z^n.$$

Since $\wp$ is an even function, the odd coefficients must vanish and (2) follows. □

Lemma 2.2. $\wp$-function for a lattice L satisfies the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 \tag{2.3}$$

where $g_2 = 60G_4$, and $g_3 = 140G_6$.

Proof. Let $F(z) = \wp'(z)^2 - 4\wp(z)^3 + g_2\wp(z) + g_3$, then F has possible poles at $z = w \in L$, is holomorphic on $\mathbb{C} - L$, and $F(z+w) = F(z)$ for all $w \in L$. But, Laurent series expansions (followed from Lemma2.1)

$$\wp(z)^3 = \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + O(z)$$

, and

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + O(z)$$

imply that F is holomorphic at 0, and $F(0) = 0$. By Liouville's theorem, we have $F(z) = 0$ for all $z \in \mathbb{C}$. □

Corollary 2.1. $\wp'(z)^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$ where $e_1 = \wp(\omega_1/2)$, $e_2 = \wp(\omega_2/2)$, and $e_3 = \wp((\omega_1 + \omega_2)/2)$. Furthermore,

$$\Delta(L) = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 = g_2^3 - 27g_3^2 \neq 0.$$

Definition 2.3. The *j-invariant* $j(L)$ of a lattice L is defined to be the complex number

$$j(L) = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2} = 1728\frac{g_2(L)^3}{\Delta(L)}. \tag{2.4}$$

The remarkable fact is that the j-invariant $j(L)$ characterizes the lattice L up to homothety:

Proposition 2.1. If L and L' are lattices in $\mathbb{C}$, then $j(L) = j(L')$ if and only if L and L' are homothetic.

Proof. It is easy to see that homothetic lattices have the same j-invariant. Namely, if $\lambda \in \mathbb{C}^*$, then the definition of g_2 and g_3 implies that

$$g_2(\lambda L) = \lambda^{-4}g_2(L)$$

$$g_3(\lambda L) = \lambda^{-6}g_3(L), \tag{2.5}$$

and $j(\lambda L) = j(L)$ follows easily.

For any lattice $L = [\omega_1, \omega_2]$, we can assume that $z = \frac{\omega_2}{\omega_1} \in H = \{z \in \mathbb{C} | \text{Im } z > 0\}$ without loss of generality. Then, L and $[1, z]$ become homothetic lattices. Now, we have the connection from j-invariant a lattice L and j-function on the upper half plane:

$$j(L) = j([1, z]) = j(z) = \frac{E_4(z)^3}{\Delta(z)}.$$

Suppose that L and L' have the same j-invariant. We first find $z, z' \in H$ such that L is homothetic to $[1, z]$, and L' is homothetic to $[1, z']$. Then, we have $j(z) =$

$j(z')$. By the valence formula(See [2] p16, Theorem1.3), we obtain $z' \equiv z \pmod{\Gamma = SL(2,\mathbb{Z})}$, since j has a simple pole at $i\infty$. This implies that $[1, z'] = [1, z]$. Hence L and L' are homothetic. □

Lemma 2.3. Let $\wp(z)$ be the $\wp$-function for the lattice L, and as in Lemma 2.1, let

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(L)z^{2n}. \tag{2.6}$$

be its Laurent expansion. Then for $n \geq 1$, the coefficient $(2n+1)G_{2n+2}(L)$ of z^{2n} is a polynomial with rational coefficients, independent of L, in $g_2(L)$ and $g_3(L)$.

Proof. We differentiate $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ to obtain

$$\wp''(z) = 6\wp(z)^2 - \frac{1}{2}g_2.$$

Let $a_n = (2n+1)G_{2n+2}(L)$. By substituting in the Laurent expansion for $\wp(z)$ and comparing the coefficients of z^{2n-2}, one easily sees that for $n \geq 3$,

$$2n(2n-1)a_n = 6\left(2a_n + \sum_{i=1}^{n-2} a_i a_{n-1-i}\right),$$

and hence

$$(2n+3)(n-2)a_n = 3\sum_{i=1}^{n-2} a_i a_{n-1-i}.$$

Since $g_2(L) = 20a_1$ and $g_3(L) = 28a_2$, induction shows that a_n is a polynomial with rational coefficients in $g_2(L)$ and $g_3(L)$. □

3. Orders in quadratic fields

Definition 3.1. An *order* $\mathcal{O}$ in a quadratic field K is a subset $\mathcal{O} \subset K$ such that
(i) $\mathcal{O}$ is a subring of K containing 1.
(ii) $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module.
(iii) $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.

The ring $\mathcal{O}_K$ of integers in K is always an order in K. More importantly, (i) and (ii) imply that for any order $\mathcal{O}$ of K, we have $\mathcal{O} \subset \mathcal{O}_K$, so that $\mathcal{O}_K$ is the maximal order of K. Note that the maximal order $\mathcal{O}_K$ can be written as:

$$\mathcal{O}_K = [1, w_K],\ w_K = \frac{d_K + \sqrt{d_K}}{2}, \tag{3.1}$$

where d_K is the discriminant of K. We can now describe all orders in quadratic fields:

Lemma 3.1. Let $\mathcal{O}$ be an order in a quadratic field K of discriminant d_K. Then $\mathcal{O}$ has finite index in $\mathcal{O}_K$, and we set $f = [\mathcal{O}_K : \mathcal{O}]$, then

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1, fw_K]. \tag{3.2}$$

Proof. Since $\mathcal{O}$ and $\mathcal{O}_K$ are free $\mathbb{Z}$-modules of rank 2, it follows that $f = [\mathcal{O}_K : \mathcal{O}]$ is finite. Since $f\mathcal{O}_K \subset \mathcal{O}$, $\mathbb{Z} + f\mathcal{O}_K = [1, fw_K] \subset \mathcal{O}$ follows. Thus, $\mathcal{O} = [1, fw_K]$. □

Given an order $\mathcal{O}$ in a quadratic field K, *discriminant* is defined as follows. Let $\alpha \mapsto \alpha'$ be the nontrivial automorphism of K, and suppose $\mathcal{O} = [\alpha, \beta]$. Then the discriminant of $\mathcal{O}$ is the number

$$D = \mathrm{disc}[\alpha, \beta] = \left(\det \begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}\right)^2. \tag{3.3}$$

If $f = [\mathcal{O}_K : \mathcal{O}]$, then it follows that $D = f^2 d_K$ by Lemma 3.1.

Now consider ideals of an order $\mathcal{O}$. Since $\mathcal{O}$ may not be a Dedekind domain, we cannot assume that ideals have unique factorization. We introduce the concept of a *proper ideal* of an order.

Definition 3.2. A *fractional ideal* of $\mathcal{O}$ is a subset of K which is a nonzero finitely generated $\mathcal{O}$-module. Then, a fractional $\mathcal{O}$-ideal $\mathfrak{b}$ is *proper* provided that

$$\mathcal{O} = \{\beta \in K : \beta\mathfrak{b} \subset \mathfrak{b}\}. \tag{3.4}$$

Proposition 3.1. Let $\mathcal{O}$ be an order in a quadratic field K, and let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible.

Proof. If $\mathfrak{a}$ is invertible, then $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ for some fractional $\mathcal{O}$-ideal $\mathfrak{b}$. If $\beta \in K$ and $\beta\mathfrak{a} \subset \mathfrak{a}$, then we have

$$\beta\mathcal{O} = \beta(\mathfrak{a}\mathfrak{b}) = (\beta\mathfrak{a})\mathfrak{b} \subset \mathfrak{a}\mathfrak{b} = \mathcal{O},$$

and $\beta \in \mathcal{O}$ follows, proving that $\mathfrak{a}$ is proper. □

To prove the converse, we need the following lemma:

Lemma 3.2. Let $K = \mathbb{Q}(\tau)$ be a quadratic field, and let $ax^2 + bx + c$ be the minimal polynomial of τ, where a, b and c are relatively prime integers. Then $[1, \tau]$ is a proper fractional ideal for the order $[1, a\tau]$ of K.

Proof. First, $[1, a\tau]$ is an order since $a\tau$ is an algebraic integer. Then, given $\beta \in K$, note that $\beta[1, \tau] \subset [1, \tau]$ is equivalent to $\beta = m + n\tau$, $m, n \in \mathbb{Z}$, and $\beta\tau = m\tau + n\tau^2 = \frac{-cn}{a} + \left(\frac{-bn}{a} + m\right)\tau \in [1, \tau]$. But, this is also equivalent to $a|n$, since $(a, b, c) = 1$. Thus, $[1, \tau]$ is a proper fractional ideal for the order $[1, a\tau]$.

Now, we can prove that proper fractional ideals are invertible. First note that $\mathfrak{a}$ is a $\mathbb{Z}$-module of rank 2, so that $\mathfrak{a} = [\alpha, \beta]$ for some $\alpha, \beta \in K$. Then $\mathfrak{a} = \alpha[1, \tau]$, where $\tau = \beta/\alpha$. If $ax^2 + bx + c$, $(a, b, c) = 1$, is the minimal polynomial of τ, then Lemma 3.2 implies that $\mathcal{O} = [1, a\tau]$. Let $\beta \mapsto \beta'$ denote the nontrivial automorphism of K. Since τ' is the other root of $ax^2 + bx + c$, using Lemma 3.2 again shows $\mathfrak{a}' = \alpha'[1, \tau']$ is a fractional ideal for $[1, a\tau] = [1, a\tau'] = \mathcal{O}$. To see why $\mathfrak{a}$ is invertible, note that

$$a\mathfrak{a}\mathfrak{a}' = a\alpha\alpha'[1, \tau][1, \tau'] = N(\alpha)[a, a\tau, a\tau', a\tau\tau'].$$

Since $\tau + \tau' = -b/a$ and $\tau\tau' = c/a$, this becomes

$$a\mathfrak{a}\mathfrak{a}' = N(\alpha)[a, a\tau, -b, c] = N(\alpha)[1, a\tau] = N(\alpha)\mathcal{O}$$

since $(a, b, c) = 1$. This proves that $\mathfrak{a}$ is invertible. □

Definition 3.3. Given an order $\mathcal{O}$, let $I(\mathcal{O})$ denote the set of proper fractional $\mathcal{O}$-ideals. By Proposition2, $I(\mathcal{O})$ forms a group. The principal $\mathcal{O}$-ideals give a subgroup $P(\mathcal{O}) \subset I(\mathcal{O})$, and thus we can form the quotient

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}),$$

which is the *ideal class group* of the order $\mathcal{O}$.

Let $C(D)$ be the set of proper-equivalence classes of primitive quadratic forms with discriminant D. Denote $h(D) = |C(D)|$.

Theorem 3.1. Let $\mathcal{O}$ be the order of discriminant D in an imaginary quadratic field K.
(i) If $f(x, y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant D, then $[a, (-b + \sqrt{D})/2]$ is a proper ideal of $\mathcal{O}$.
(ii) The map sending $f(x, y)$ to $[a, (-b+\sqrt{D})/2]$ induces a bijection between $C(D)$ and the ideal class group $C(\mathcal{O})$. Remark that $h(D) = |C(D)| = |C(\mathcal{O})|$.

Proof. (i) Let $\tau = (-b + \sqrt{D})/2a$. Then $[a, (-b + \sqrt{D})/2] = [a, a\tau] = a[1, \tau]$. Note that by Lemma 3.2, $a[1, \tau]$ is a proper ideal for the order $[1, a\tau]$. However, if $f = [\mathcal{O}_K : \mathcal{O}]$, then $D = f^2 d_K$, and thus

$$a\tau = -\frac{b + f d_K}{2} + f w_K \in [1, f w_K].$$

It follows that $[1, a\tau] = [1, f w_K] = \mathcal{O}$ by Lemma 3.1. This proves that $a[1, \tau]$ is a proper $\mathcal{O}$-ideal.
(ii) Let $f(x, y)$ and $g(x, y)$ be forms of discriminant D, and let τ and τ' be their respective roots. We will prove:

$$\begin{aligned} &f(x, y),\ g(x, y) \text{ are properly equivalent} \\ \Longleftrightarrow &\tau' = \frac{p\tau + q}{r\tau + s},\ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL(2, \mathbb{Z}) \\ \Longleftrightarrow &[1, \tau] = \lambda[1, \tau'],\ \lambda \in K^*. \end{aligned}$$

To see the first equivalence, assume that $f(x, y) = g(px + qy, rx + sy)$, where $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL(2, \mathbb{Z})$. Then

$$0 = f(\tau, 1) = g(p\tau + q, r\tau + s) = (r\tau + t)^2 g\left(\frac{p\tau + q}{r\tau + s}, 1\right),$$

so that $g((p\tau + q)/(r\tau + s), 1) = 0$. However, if $\tau \in H$, then $(p\tau + q)/(r\tau + s) \in H$, thus $\tau' = (p\tau + q)/(r\tau + s)$. Conversely, if $\tau' = (p\tau + q)/(r\tau + s)$, then we have $f(x, y)$ and $g(px + qy, rx + sy)$ have the same root, hence they are equal.

Next, if $\tau' = (p\tau + q)/(r\tau + s)$, let $\lambda = r\tau + s \in K^*$. Then

$$\begin{aligned} \lambda[1, \tau'] &= (r\tau + s)\left[1, \frac{p\tau + q}{r\tau + s}\right] \\ &= [r\tau + s, p\tau + q] = [1, \tau] \end{aligned}$$

since $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL(2, \mathbb{Z})$. Conversely, if $[1, \tau] = \lambda[1, \tau']$ for some $\lambda \in K^*$, then $[1, \tau] = [\lambda, \lambda\tau']$, which implies

$$\begin{aligned} \lambda\tau' &= p\tau + q \\ \lambda &= r\tau + s \end{aligned}$$

for some $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in GL(2, \mathbb{Z})$. This gives us $\tau' = \frac{p\tau+q}{r\tau+s}$. Since τ, τ' are both in H, we have $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL(2, \mathbb{Z})$.

These equivalences show that the map sending $f(x,y)$ to $a[1,\tau]$ induces an injection $C(D) \longrightarrow C(\mathcal{O})$.
To show that the map is surjective, let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. We write $\mathfrak{a} = [\alpha, \beta]$ for some $\alpha, \beta \in K$ with $\tau = \beta/\alpha$ lies in H. Let $ax^2 + bx + c$ be the minimal polynomial of τ. We may assume that $(a, b, c) = 1$ and $a > 0$. Then $f(x, y) = ax^2 + bxy + cy^2$ is positive definite of discriminant D, and maps to $a[1, \tau]$ which is in the class of $\mathfrak{a}$.

We thus have a bijection of sets

$$C(D) \longrightarrow C(\mathcal{O}). \tag{3.5}$$

□

4. Complex Multiplication

First, we observe that orders in imaginary quadratic fields give rise to a natural class of lattices. If $\mathcal{O}$ is an order in a quadratic field K and $\mathfrak{a} = [\alpha, \beta]$ is a proper fractional $\mathcal{O}$-ideal, then α and β are linearly independent over $\mathbb{R}$. Thus $\mathfrak{a} \subset \mathbb{C}$ is a lattice. Conversely, let $L \subset \mathbb{C}$ be a lattice which is contained in K. Then L is a proper fractional $\mathcal{O}$-ideal for some order $\mathcal{O}$ of K. As a consequence, we have that $\mathfrak{a}$ and $\mathfrak{b}$ determine the same class in the ideal class group $C(\mathcal{O})$ if and only if they are homothetic as lattices in $\mathbb{C}$. Moreover, this enables us to define $j(\mathfrak{a})$ for a proper fractional $\mathcal{O}$-ideal.

We defined $\wp$-function for a lattice $L \subset \mathbb{C}$. In fact, any elliptic function for L is a rational function of $\wp$ and $\wp'$.

Lemma 4.1. Any even elliptic function for L is a rational function in $\wp(z)$.

Proof. (a) Let $f(z)$ be an even elliptic function which is holomorphic on $\mathbb{C} - L$. Then there is a polynomial $A(x)$ such that the Laurent expansion of $f(z) - A(\wp(z))$ is holomorphic on $\mathbb{C}$. By Liouville's theorem, $f(z) - A(\wp(z))$ is a constant. Thus, $f(z)$ is a polynomial in $\wp(z)$.
(b) Let $f(z)$ be an even elliptic function that has a pole of order m at $w \in \mathbb{C} - L$. If $2w \notin L$, then $(\wp(z) - \wp(w))^m f(z)$ is holomorphic at w, since $(\wp(z) - \wp(w))$ has a zero at $z = w$. If $2w \in L$, then m is even, since the Laurent expansion for $f(z)$ and $f(2w - z)$ at $z = w$ must be equal. In this case, $(\wp(z) - \wp(w))^{m/2} f(z)$ is holomorphic at w, since $(\wp(z) - \wp(w))$ has double zero at $z = w$.
(c) Now we can show that for an even elliptic function $f(z)$, there is a polynomial $B(x)$ such that $B(\wp(z))f(z)$ is holomorphic on $\mathbb{C} - L$. Then the lemma follows by part (a). □

For any elliptic function $f(z)$ for L, we have

$$f(z) = \frac{f(z) + f(-z)}{2} + \left(\frac{f(z) - f(-z)}{2\wp'(z)}\right)\wp'(z).$$

Hence, any elliptic function for L is a rational function of $\wp$ and $\wp'$. We turn into an important proposition about complex multiplication:

Proposition 4.1. Let L be a lattice, and let $\wp(z)$ be the $\wp$-function for L. Then, for a number $\alpha \in \mathbb{C} - \mathbb{Z}$, the following statements are equivalent:
(i) $\wp(\alpha z)$ is a rational function in $\wp(z)$.
(ii) $\alpha L \subset L$.
(iii) There is an order $\mathcal{O}$ in an imaginary quadratic field K such that $\alpha \in \mathcal{O}$ and L

is homothetic to a proper fractional $\mathcal{O}$-ideal.
Furthermore, if these conditions are satisfied, then $\wp(\alpha z)$ can be written in the form

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))} \tag{4.1}$$

where $A(x)$ and $B(x)$ are relatively prime polynomials such that

$$\deg(A(x)) = \deg(B(x)) + 1 = [L : \alpha L] = N(\alpha).$$

Proof. (i)⇒(ii). If $\wp(\alpha z)$ is a rational function in $\wp(z)$, then there are polynomials $A(x)$ and $B(x)$ such that

$$B(\wp(z))\wp(\alpha z) = A(\wp(z)).$$

Comparing the order or pole at $z = 0$, we have

$$\deg(A(x)) = \deg(B(x)) + 1.$$

Now, let $\omega \in L$. Then the above show that $\wp(\alpha z)$ has a pole at ω, which means that $\wp(z)$ has a pole at $\alpha\omega$. Since the poles of $\wp(z)$ are exactly at members in L, this implies $\alpha\omega \in L$, and $\alpha L \subset L$ follows.
(ii)⇒(i). If $\alpha L \subset L$, it follows that $\wp(\alpha z)$ is meromorphic and has L as a lattice of periods. Furthermore, $\wp(\alpha z)$ is an even function. By Lemma 4.1, we have $\wp(\alpha z)$ is a rational function in $\wp(z)$.
(ii)⇒(iii). Suppose that $\alpha L \subset L$. Replacing L by λL for suitable λ, we can assume that $L = [1, \tau]$ for some $\tau \in \mathbb{C} - \mathbb{R}$. Then $\alpha L \subset L$ means that $\alpha = a + b\tau$ and $\alpha\tau = c + d\tau$ for some integers a, b, c and d. Then we obtain,

$$\tau = \frac{c + d\tau}{a + b\tau},$$

which implies $b\tau^2 + (a - d)\tau - c = 0$. Since τ is not real, we have $b \neq 0$, and $K = \mathbb{Q}(\tau)$ is an imaginary quadratic field. Thus,

$$\mathcal{O} = \{\beta \in K | \beta L \subset L\} = \{\beta \in K | \beta[1, \tau] \subset [1, \tau]\} = [1, b\tau]$$

is an order of K for which L is a proper fractional $\mathcal{O}$-ideal(by Lemma 3.2), and since α is obviously in $\mathcal{O}$, we are done.
(iii)⇒(ii) is trivial.
Suppose $\alpha L \subset L = [1, \tau]$. From the definition of discriminant (3.3), we obtain

$$N(\alpha)^2 \mathrm{disc}[1, \tau] = \mathrm{disc}[\alpha, \alpha\tau] = [L : \alpha L]^2 \mathrm{disc}[1, \tau].$$

Thus, $[L : \alpha L] = N(\alpha)$. It remains to prove that degree of $A(x)$ is the index $[L : \alpha L]$.

Fix $z \in \mathbb{C}$ such that $2z \notin (1/\alpha)L$, and consider the polynomial $A(x) - \wp(\alpha z)B(x)$. This polynomial has the same degree as $A(x)$, and z can be chosen so that it has distinct roots(multiple root of $A(x) - \wp(\alpha z)B(x)$ is a root of $A(x)B'(x) - A'(x)B(x)$.) Then consider the lattice $L \subset (1/\alpha)L$, and let $\{w_i\}$ be coset representatives of L in $(1/\alpha)L$. Our assumption on z implies that $\wp(z + w_i)$ are distinct. From (4.1), we see that $A(\wp(z + w_i)) = \wp(\alpha(z + w_i))B(\wp(z + w_i))$. But $\alpha w_i \in L$, hence $\wp(\alpha(z + w_i)) = \wp(\alpha z)$. This shows that $\wp(z + w_i)$ are distinct roots of $A(x) - \wp(\alpha z)B(x)$. Let u be another root. Then we see that $u = \wp(w)$ for some complex number w. Then, $\wp(\alpha z) = \wp(\alpha w)$, and $w \equiv z + w_i \bmod L$ for some i. Hence $\wp(z + w_i)$ are all roots of $A(x) - \wp(\alpha z)B(x)$, giving that $\deg A(x) = [(1/\alpha)L : L] = [L : \alpha L]$. □

Together with Laurent series of $\wp(z)$, this theorem allows us to compute some special values of j-function for example:

$$j(\sqrt{-2}) = 8000 \text{ and } j\left(\frac{1+\sqrt{-7}}{2}\right) = -3375.$$

To complete the proof of Theorem1.1, we need a lemma involving the invariants $g_2(L)$ and $g_3(L)$.

Lemma 4.2. Let g_2 and g_3 be given complex numbers satisfying $g_2^3 - 27g_3^2 \neq 0$. Then there is a unique lattice $L \subset \mathbb{C}$ such that $g_2(L) = g_2$ and $g_3(L) = g_3$.

Proof. We can find $z \in H$ such that $j(z) = E_4(z)^3/\Delta(z) = 1728g_2^3/(g_2^3 - 27g_3^2)$. By valence formula, this z is uniquely determined modulo Γ. If $g_2 \neq 0$, then we find $w_1 \in \mathbb{C}$ such that

$$g_2 = \frac{4\pi^4}{3w_1^4}E_4(z). \tag{4.2}$$

Using $-w_1$ if necessary, we obtain

$$g_3 = \frac{8\pi^6}{27w_1^6}E_6(z). \tag{4.3}$$

If $g_2 = 0$, then we have $g_3 \neq 0$ and we find $w_1 \in \mathbb{C}$ using (4.3). Let $w_2 = zw_1$, then $L = [w_1, w_2]$ is the desired lattice.

Suppose we have two lattices L and L' with $g_2(L) = g_2(L')$ and $g_3(L) = g_3(L')$. Then, $j(L) = j(L')$ implies that there exists $\lambda \in \mathbb{C} - \{0\}$ such that $L' = \lambda L$ by Proposition2.1. If $g_2(L) \neq 0$ and $g_3(L) \neq 0$, then (2.5) give $\lambda^2 = 1$. Thus, $L = L'$.
If $g_2(L) = 0$, then $L = \lambda_1[1, w]$ and $L' = \lambda_2[1, w]$ for some $\lambda_1, \lambda_2 \in \mathbb{C} - \{0\}$ with $w = \exp(2\pi i/3)$. But, (2,5) gives $\lambda_1^6 = \lambda_2^6$. Thus, $L = L'$
If $g_3(L) = 0$, then $L = \lambda_1[1, i]$ and $L' = \lambda_2[1, i]$ for some $\lambda_1, \lambda_2 \in \mathbb{C} - \{0\}$. In this case, (2.5) gives $\lambda_1^4 = \lambda_2^4$. Hence, $L = L'$. □

Now, we are ready to prove Theorem1.1. In fact, the following theorem will imply Theorem1.1.

Theorem 4.1. Let $\mathcal{O}$ be an order in an imaginary quadratic field, and let $\mathfrak{a}$ be a proper fractional $\mathcal{O}$-ideal. Then $j(\mathfrak{a})$ is an algebraic number of degree at most $h(\mathcal{O})$.

Proof. By Lemma2.3, we can write the Laurent expansion of $\wp(z)$ for the lattice $\mathfrak{a}$ as

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} a_n(g_2, g_3)z^{2n},$$

where a_n is a polynomial in g_2 and g_3 with rational coefficients. To emphasize the dependence on g_2 and g_3, we write $\wp(z)$ as $\wp(z; g_2, g_3)$.

By assumption, for any $\alpha \in \mathcal{O}$, we have $\alpha\mathfrak{a} \subset \mathfrak{a}$. Thus, by Proposition4.1, $\wp(\alpha z)$ is a rational function in $\wp(z)$.

$$\begin{aligned}\wp(\alpha z; g_2, g_3) &= \frac{1}{\alpha^2 z^2} + \sum_{n=1}^{\infty} a_n(g_2, g_3)\alpha^{2n}z^{2n} \\ &= \frac{A(\wp(z; g_2, g_3))}{B(\wp(z; g_2, g_3))}\end{aligned}$$

for some polynomials $A(x)$ and $B(x)$. We can regard this as an identity in the field of meromorphic Laurent series $\mathbb{C}((z))$.

Now let σ be any automorphism of $\mathbb{C}$. Then σ induces an automorphism of $\mathbb{C}((z))$. Applying σ, we obtain

$$\wp(\sigma(\alpha)z;\sigma(g_2),\sigma(g_3)) = \frac{A^\sigma(\wp(z;\sigma(g_2),\sigma(g_3)))}{B^\sigma(\wp(z;\sigma(g_2),\sigma(g_3)))}. \tag{4.4}$$

We observe that $g_2^3 - 27g_3^2 \neq 0$ implies $\sigma(g_2)^3 - 27\sigma(g_3)^2 \neq 0$. By Lemma4.2, there exists a lattice L such that

$$g_2(L) = \sigma(g_2)$$
$$g_3(L) = \sigma(g_3).$$

Since $\wp(z;\sigma(g_2),\sigma(g_3)) = \wp(z;L)$, (4.4) implies that $\wp(z;L)$ has complex multiplication by $\sigma(\alpha)$. Let $\mathcal{O}'$ be the ring of all complex multiplications of L, then we have proved that

$$\mathcal{O} = \sigma(\mathcal{O}) \subset \mathcal{O}'.$$

Applying σ^{-1} and we interchange $\mathfrak{a}$ and L, then above argument shows $\mathcal{O}' \subset \mathcal{O}$, which shows that $\mathcal{O}$ is the ring of all complex multiplications of both $\mathfrak{a}$ and L.

Now consider j-invariants. Above formulas for $g_2(L)$ and $g_3(L)$ imply that

$$j(L) = \sigma(j(\mathfrak{a})).$$

Since L has $\mathcal{O}$ as its ring of complex multiplications, there are only $h(\mathcal{O})$ possibilities for $j(L)$. It follows that $j(\mathfrak{a})$ must be an algebraic number, and the degree is at most $h(\mathcal{O})$. □

Suppose that $\mathcal{O}$ is an order of discriminant D in an imaginary quadratic field, and $ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form with discriminant D. Then, for $z_Q = \frac{-b+\sqrt{D}}{2a}$, $\mathfrak{a} = [1, z_Q]$ is a proper fractional ideal in $\mathcal{O}$ by Lemma3.2. Now, Theorem4.1 implies that $j(\mathfrak{a}) = j([1, z_Q]) = j(z_Q)$ is an algebraic number of degree at most $h(\mathcal{O}) = h(D)$ (by Theorem3.1). This completes the proof of Theorem1.1.

References

1. D. Cox, Prines of the Form $x^2 + ny^2$, John Wiley & Sons. Inc.
2. H. Iwaniec, Topics in Classical Automorphic Forms, AMS Providence, Rhode Island.