ACTA ARITHMETICA
125.1 (2006)

On some equalities for the Weierstrass modular units of level p

by

HEIMA HAYASHI (Kumamoto)

1. Terminology and statement of results. Let $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ and $\mathbb{Z}$ be respectively the fields of complex, real and rational numbers and the ring of rational integers. For each algebraic number field F, we denote the ring of integers in F by $\mathfrak{o}_F$. For two numbers (or ideals) A and B in some algebraic number field, let the relation $A \sim B$ mean that $A\mathfrak{o}_F = B\mathfrak{o}_F$ as an ideal in a sufficiently large algebraic number field F. By a $\mathbb{C}$-*lattice* we mean a free $\mathbb{Z}$-module in $\mathbb{C}$ of rank 2 which spans $\mathbb{C}$ over $\mathbb{R}$. In any $\mathbb{C}$-lattice a basis $\{\omega_1, \omega_2\}$ can be chosen so that $\mathrm{Im}(\omega_1/\omega_2) > 0$. Hereafter we denote the $\mathbb{C}$-lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ simply by $[\omega_1, \omega_2]$.

Let Ω be a $\mathbb{C}$-lattice. The *Weierstrass* $\wp$*-function* $\wp_\Omega(z)$ attached to Ω is defined by

$$\wp_\Omega(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega \setminus \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right].$$

As usual let $g_2(\Omega)$, $g_3(\Omega)$ and $\Delta(\Omega)$ be the lattice functions respectively defined by

$$g_2(\Omega) = 60 \sum_{\omega \in \Omega \setminus \{0\}} \frac{1}{\omega^4}, \qquad g_3(\Omega) = 140 \sum_{\omega \in \Omega \setminus \{0\}} \frac{1}{\omega^6}$$

and

$$\Delta(\Omega) = g_2^3(\Omega) - 27 g_3^2(\Omega).$$

Let τ be in the complex upper half plane $\mathfrak{H}$, and let $\Omega_\tau = [\tau, 1]$. We write $g_2(\tau)$, $g_3(\tau)$ and $\Delta(\tau)$ respectively for $g_2(\Omega_\tau)$, $g_3(\Omega_\tau)$ and $\Delta(\Omega_\tau)$. Let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. For a prime number p, let $\Gamma(p)$ and $\Gamma_0(p)$ be the subgroups

---

2000 *Mathematics Subject Classification*: Primary 11G15, 11G16.

of Γ given by

$$\Gamma(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,\middle|\, a \equiv d \equiv 1,\, b \equiv c \equiv 0 \pmod{p} \right\},$$
$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \,\middle|\, c \equiv 0 \pmod{p} \right\}.$$

As is well known, $[\Gamma_0(p) : \Gamma(p)] = p(p-1)$ (cf. [1], [7]). More precisely the map $\Gamma_0(p) \to (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a, b) \pmod{p}$$

induces an injective map from the factor group $\Gamma(p)\backslash\Gamma_0(p)$ onto $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})$.

We define a function λ_p on $\mathfrak{H}$ by

$$\lambda_p(\tau) := \frac{\wp_{\Omega_\tau}\left(\dfrac{1}{p}\right) - \wp_{\Omega_\tau}\left(\dfrac{\tau+1}{p}\right)}{\wp_{\Omega_\tau}\left(\dfrac{\tau}{p}\right) - \wp_{\Omega_\tau}\left(\dfrac{\tau+1}{p}\right)}. \tag{1.1}$$

It is called a *Weierstrass modular unit* (cf. Kubert–Lang [8]). Especially λ_2 is well known as a function which appears in the Legendre model of elliptic curves (cf. [4], [5]). By the properties of the $\wp$-function, we see that λ_p is a modular function for $\Gamma(p)$ which is holomorphic and non-zero on $\mathfrak{H}$. Hereafter, when the subscript Ω_τ is clear from the context, we often write $\wp(z)$ in place of $\wp_{\Omega_\tau}(z)$, that is,

$$\lambda_p(\tau) = \frac{\wp\left(\dfrac{1}{p}\right) - \wp\left(\dfrac{\tau+1}{p}\right)}{\wp\left(\dfrac{\tau}{p}\right) - \wp\left(\dfrac{\tau+1}{p}\right)}.$$

For $\sigma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\Gamma_0(p)$, we have

$$\lambda_p(\sigma(\tau)) = \frac{\wp\left(\dfrac{d}{p}\right) - \wp\left(\dfrac{a\tau+b+d}{p}\right)}{\wp\left(\dfrac{a\tau+b}{p}\right) - \wp\left(\dfrac{a\tau+b+d}{p}\right)} \quad \text{with} \quad \sigma(\tau) = \frac{a\tau+b}{c\tau+d}.$$

We consider the function on $\mathfrak{H}$ defined by

$$\Lambda_p(\tau) := \prod_{\substack{\sigma \bmod \Gamma(p) \\ \sigma \in \Gamma_0(p)}} \lambda_p(\sigma(\tau)) \tag{1.2}$$

$$= \prod_{a=1}^{p-1} \prod_{b=0}^{p-1} \frac{\wp\left(\frac{d}{p}\right) - \wp\left(\frac{a\tau + b + d}{p}\right)}{\wp\left(\frac{a\tau + b}{p}\right) - \wp\left(\frac{a\tau + b + d}{p}\right)}.$$

In each factor of the expression (1.2), d is determined modulo p so that $ad \equiv 1 \pmod{p}$. It is easy to see that $\Lambda_p(\tau)$ is a modular function for $\Gamma_0(p)$ which is holomorphic and non-zero on $\mathfrak{H}$.

For example, for $p = 2$,

$$\Lambda_2(\tau) = \frac{\wp\left(\frac{1}{2}\right) - \wp\left(\frac{\tau+1}{2}\right)}{\wp\left(\frac{\tau}{2}\right) - \wp\left(\frac{\tau+1}{2}\right)} \cdot \frac{\wp\left(\frac{1}{2}\right) - \wp\left(\frac{\tau}{2}\right)}{\wp\left(\frac{\tau+1}{2}\right) - \wp\left(\frac{\tau}{2}\right)}$$
$$= \lambda_2(\tau)(1 - \lambda_2(\tau)).$$

Cougnard gave the following equality:

$$\Lambda_2(\tau) \cdot \left(2^{12} \frac{\Delta(2\tau)}{\Delta(\tau)}\right) = -2^4 \tag{1.3}$$

([4, Theorem 7]). Also if p is an odd prime number, an equality analogous to (1.3) should be expected. Our first aim is to prove the following

Theorem 1. *For any odd prime number* p,

$$\Lambda_p^2(\tau) \cdot \left(p^{12} \frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{(p+1)/2} = p^6.$$

In particular, *if* $p \equiv 3 \pmod{4}$, *then*

$$\Lambda_p(\tau) \cdot \left(p^{12} \frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{(p+1)/4} = -p^3.$$

Section 2 is devoted to proving Theorem 1. In Section 3 we consider a few applications of Theorem 1. First we compute the equation relating the function Λ_p and the modular invariant j (see Proposition 2). Next we apply Theorem 1 to the complex multiplication case. In the expressions (1.1) and (1.2), we can replace $\wp(*) = \wp_{\Omega_\tau}(*)$ by the Weber function

$$h(*) := h_{\Omega_\tau}(*) := \frac{-2^7 \cdot 3^5 \cdot g_2(\tau) \cdot g_3(\tau)}{\Delta(\tau)} \wp_{\Omega_\tau}(*).$$

Namely we may write

$$\lambda_p(\tau) := \frac{h\left(\dfrac{1}{p}\right) - h\left(\dfrac{\tau+1}{p}\right)}{h\left(\dfrac{\tau}{p}\right) - h\left(\dfrac{\tau+1}{p}\right)},$$

$$\Lambda_p(\tau) = \prod_{a=1}^{p-1}\prod_{b=0}^{p-1} \frac{h\left(\dfrac{d}{p}\right) - h\left(\dfrac{a\tau+b+d}{p}\right)}{h\left(\dfrac{a\tau+b}{p}\right) - h\left(\dfrac{a\tau+b+d}{p}\right)}.$$

Let $k = \mathbb{Q}(\sqrt{-d})$ with a square free positive integer d. For simplicity we assume that $d \neq 1, 3$. Let τ $(\in \mathfrak{H})$ be in k and assume that $\Omega_\tau = [\tau, 1]$ is an $\mathfrak{o}_k$-ideal. For $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ such that $(a, b) \not\equiv (0, 0) \pmod p$, $(a\tau + b)/p$ represents a non-zero p-division point of $\mathbb{C}/[\tau, 1]$, and hence by the classical theory of complex multiplication (cf. Cassou-Noguès and Taylor [3], Deuring [6]), $h((a\tau + b)/p)$ is an integer belonging to the ray class field $k(p\mathfrak{o}_k)$ over k with conductor $p\mathfrak{o}_k$. Therefore $\lambda_p(\tau)$ and $\Lambda_p(\tau)$ also belong to $k(p\mathfrak{o}_k)$. Using the equality in Theorem 1, we shall show some arithmetic properties of $\Lambda_p(\tau)$ (see Theorem 4). In Section 4, we shall treat the arithmetic of $\lambda_p(\tau)$. Therein we first show how to compute the equation relating $\lambda_p(\tau)$ and the modular invariant j, and give a numerical example (Theorem 5). Next we consider the algebraic properties of $\lambda_p(\tau)$ in the case of complex multiplication (see Theorem 6).

2. Proof of Theorem 1.

We put

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

As is well known, $[\Gamma : \Gamma_0(p)] = p + 1$, and the following is a complete set of left coset representatives for $\Gamma_0(p)$ in Γ:

$$\alpha_0 = I \quad \text{and} \quad \alpha_i = ST^{i-1} \qquad (i = 1, \ldots, p)$$

(cf. [1], [7]). Of course $\{\alpha_i^{-1}\}_{0\le i\le p}$ represents all right cosets of $\Gamma/\Gamma_0(p)$. The set of cusps of $\Gamma_0(p)$ is $\{0, \infty\}$, because $\alpha_0(\infty) = \infty$ and $\alpha_i(\infty) = 0$ $(1 \le i \le p)$. Now we know that both $\Lambda_p(\tau)$ and $\Delta(p\tau)/\Delta(\tau)$ are modular functions for $\Gamma_0(p)$ which are non-zero and holomorphic on $\mathfrak{H}$. We compare their q-expansions at the cusps of $\Gamma_0(p)$. Using the well known formula

$$(2\pi i)^{-12}\Delta(\tau) = q\prod_{n=1}^{\infty}(1 - q^n)^{24} \quad \text{with } q = e^{2\pi i\tau} \tag{2.1}$$

(cf. [9]), we have

$$\frac{\Delta(p\tau)}{\Delta(\tau)} = q^{p-1}(1+qR_0(q))$$

where $R_0(X)$ is a power series in X with coefficients in $\mathbb{Z}$. On the other hand, by making use of Proposition A-1 in the Appendix, we can describe the q-expansion of each factor on the right hand side of (1.2). Moreover, by applying Lemma A-2, we can deduce that

$$\Lambda_p(\tau) = (-1)^{(p-1)/2} p^{-3p} q^{-(p^2-1)/4} \cdot (1 + q^{1/p} R_1(q^{1/p})),$$

where $R_1(X)$ is a power series in X with coefficients in $\mathbb{Z}[\zeta_p]$ and $\zeta_p = e^{2\pi i/p}$. Hence the q-expansion of

$$\Lambda_p^2(\tau) \cdot \left(p^{12}\,\frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{(p+1)/2} \tag{2.2}$$

at ∞ starts with the constant term p^6, and this also means that (2.2) is holomorphic at ∞. It is also clear that if $p \equiv 3 \pmod 4$ the leading term of the q-expansion of

$$\Lambda_p(\tau) \cdot \left(p^{12}\,\frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{(p+1)/4}$$

at ∞ is equal to $-p^3$. Next we consider the q-expansion at the cusp $0 = S(\infty)$. Since

$$p^{12}\,\frac{\Delta(pS^{-1}(\tau))}{\Delta(S^{-1}(\tau))} = p^{12}\,\frac{\Delta\left(\dfrac{-p}{\tau}\right)}{\Delta\left(\dfrac{-1}{\tau}\right)} = \frac{\Delta\left(\dfrac{\tau}{p}\right)}{\Delta(\tau)},$$

using (2.1), we see that the leading term of the q-expansion of $p^{12}\Delta(p\tau)/\Delta(\tau)$ at 0 is equal to $q^{-(p-1)/p}$. On the other hand, we have

$$\Lambda_p(S^{-1}(\tau)) = \prod_{a=1}^{p-1}\prod_{b=0}^{p-1} \frac{\wp\left(\dfrac{d\tau}{p}\right) - \wp\left(\dfrac{(b+d)\tau - a}{p}\right)}{\wp\left(\dfrac{b\tau - a}{p}\right) - \wp\left(\dfrac{(b+d)\tau - a}{p}\right)}. \tag{2.3}$$

Applying Lemma A-2, we can find the leading term of the q-expansion of each factor of (2.3). Then by a tedious check, we see that the q-expansion of $\Lambda_p(S^{-1}(\tau))$ at ∞ starts with $q^{\frac{1}{p}\cdot\frac{p^2-1}{4}}$, and hence the q-expansion of (2.2) at $0 = S(\infty)$ starts with the constant term. This means that (2.2) is also holomorphic at 0. Hence (2.2) is holomorphic on the compact Riemann surface $\Gamma_0(p)\backslash\mathfrak{H} \cup \{\text{cusps}\}$ and so must be a constant. Moreover since

$$\lim_{\tau\to i\infty} \Lambda_p^2(\tau) \cdot \left(p^{12}\,\frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{(p+1)/2} = p^6,$$

we have the first equality of Theorem 1. It is also clear that if $p \equiv 3 \pmod 4$, then

$$\Lambda_p(\tau) \cdot \left(p^{12} \frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{(p+1)/4} = -p^3.$$

3. Some arithmetic properties of $\Lambda_p(\tau)$. Let $\{\alpha_i\}$ be as in Section 2. We define

$$A_i(\tau) := \Lambda_p(\alpha_i(\tau)) \qquad (i = 0, 1, \ldots, p).$$

Then by Theorem 1, we have

$$A_0^2(\tau) \cdot \left(p^{12} \frac{\Delta(p\tau)}{\Delta(\tau)}\right)^{(p+1)/2} = p^6 \tag{3.1}$$

and for $1 \le i \le p$,

$$A_i^2(\tau) \cdot \left(\frac{\Delta\left(\frac{\tau+i-1}{p}\right)}{\Delta(\tau)}\right)^{(p+1)/2} = p^6. \tag{3.2}$$

As is well known,

$$\beta_0 = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \beta_i = \begin{pmatrix} 1 & i-1 \\ 0 & p \end{pmatrix} \qquad (1 \le i \le p)$$

constitute a complete system of representatives of the left cosets $\Gamma \backslash M_p$, where M_p is the set of integral matrices of determinant p. We define

$$B_0(\tau) := p^{12} \frac{\Delta(\beta_0(\tau))}{\Delta(\tau)} = p^{12} \frac{\Delta(p\tau)}{\Delta(\tau)}$$

and

$$B_i(\tau) := \frac{\Delta(\beta_i(\tau))}{\Delta(\tau)} = \frac{\Delta\left(\dfrac{\tau+i-1}{p}\right)}{\Delta(\tau)} \quad \text{for } 1 \le i \le p.$$

Then the equalities (3.1) and (3.2) can be restated as follows:

$$A_i^2(\tau) \cdot B_i(\tau)^{(p+1)/2} = p^6 \quad \text{for } i = 0, 1, \ldots, p. \tag{3.3}$$

From the classical theory of complex multiplication (cf. [2], [3], [6]), we know that the polynomial

$$\Phi_p^{(k)}(X) := \prod_{i=0}^{p} (X - B_i^k(\tau))$$

lies in $\mathbb{Z}[j, X]$, where j is the modular invariant defined by

$$j(\tau) = \frac{1728 g_2^3(\tau)}{\Delta(\tau)}.$$

Hence by using equation (1.3) and Theorem 1, it is possible to give the equation relating the functions Λ_p and j. For example, by numerical computations we obtain the following

Proposition 2. *Under the notations as above*,

(i) Λ_2 *satisfies*

$$\Lambda_2^3 + \frac{1}{2^8}(j-768)\Lambda_2^2 + 3\Lambda_2 - 1 = 0,$$

or equivalently

$$j = -2^8\,\frac{(\Lambda_2-1)^3}{\Lambda_2^2}.$$

(ii) Λ_3 *satisfies*

$$\Lambda_3^4 + \frac{1}{3^9}(j^2 - 1512j + 177876)\Lambda_3^3 + \frac{1}{3^4}(8j+2214)\Lambda_3^2 + 28\Lambda_3 + 1 = 0.$$

Remark. The second equality in (i) of Proposition 2 is nothing but the equality given in Lang [9, p. 256].

For any odd prime p, we know that

$$\prod_{i=0}^{p} B_i(\tau) = p^{12}\,\frac{\Delta(p\tau)}{\Delta(\tau)}\prod_{i=1}^{p}\frac{\Delta\left(\dfrac{\tau+i-1}{p}\right)}{\Delta(\tau)} = p^{12}.$$

Hence by (3.3), we have

$$\prod_{i=0}^{p} A_i^2(\tau) = 1. \tag{3.4}$$

In particular, if $p \equiv 3 \pmod 4$, we have

$$\prod_{i=0}^{p} A_i(\tau) = 1. \tag{3.5}$$

Hereafter in this section, let $\tau\ (\in \mathfrak{H})$ be in an imaginary quadratic number field $k\ (\neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}))$, and let $\Omega_\tau = [\tau, 1]$ be an $\mathfrak{o}_k$-ideal. The following is a fundamental result in the classical theory of complex multiplication (cf. [2], [3], [6], [10]).

Proposition 3. *Under the above notations*, $B_i(\tau)$ $(0 \le i \le p)$ *are algebraic integers and the following hold*:

(i) *If p splits in k with $p\mathfrak{o}_k = \mathfrak{p}\bar{\mathfrak{p}}$, then there exists a unique β_{i_1} (resp. β_{i_2}) such that $\beta_{i_1}(\tau)$ (resp. $\beta_{i_2}(\tau)$) is a basis quotient of $\bar{\mathfrak{p}}\Omega_\tau$ (resp. $\mathfrak{p}\Omega_\tau$). In this case $B_{i_1}(\tau)$ and $B_{i_2}(\tau)$ are contained in $\mathcal{H}_k$, the Hilbert class field of k, and*

$$B_{i_1}(\tau) \sim \mathfrak{p}^{12} \quad \text{and} \quad B_{i_2}(\tau) \sim \bar{\mathfrak{p}}^{12}.$$

Moreover, for any $i \neq i_1, i_2$, $B_i(\tau)$ is a unit.

(ii) *If p is ramified in k with $p\mathfrak{o}_k = \mathfrak{p}^2$, then there exists a unique β_{i_1} such that $\beta_{i_1}(\tau)$ is a basis quotient of $\mathfrak{p}\Omega_\tau$. In this case $B_{i_1}(\tau)$ is contained in $\mathcal{H}_k$ and*

$$B_{i_1}(\tau) \sim p^6, \qquad B_i(\tau) \sim p^{6/p} \qquad \text{for any } i \neq i_1.$$

(iii) *If p remains prime in k, then $B_i(\tau) \sim p^{12/(p+1)}$ for any i.*

Combining Theorem 1 and Proposition 3, we have the following

THEOREM 4. *Let the notations be as above. Then $\Lambda_p(\tau)$ is an algebraic number which is a unit outside the prime divisors of p. In particular, $\Lambda_p(\tau)$ is a unit if p remains prime in k.*

4. Some arithmetic properties of $\lambda_p(\tau)$. As is well known, $[\Gamma : \Gamma(p)] = p(p^2-1)$ (cf. [1], [7]). Let $\{\gamma_i\}$ be a complete set of left coset representatives for $\pm\Gamma(p)$ in Γ. We consider the polynomial G_p given by

$$\begin{aligned} G_p(X) &:= \prod_{i=0}^{m-1} (X - \lambda_p(\gamma_i(\tau))) \\ &= X^m + C_{m-1}(\tau)X^{m-1} + \cdots + C_1(\tau)X + C_0(\tau), \end{aligned}$$

where $m = \frac{1}{2}p(p^2-1)$. It is easy to verify that all coefficients $C_i(\tau)$ of $G_p(X)$ are modular functions for Γ and holomorphic on $\mathfrak{H}$. Moreover by applying Proposition A-1 and Lemma A-2 of the Appendix, we can verify that the q-expansions of $C_i(\tau)$ all lie in $\mathbb{Z}[1/p, \zeta_p]((q))$, the ring of formal Laurent series in q with coefficients in $\mathbb{Z}[1/p, \zeta_p]$, where $\zeta_p = e^{2\pi i/p}$. Then from the q-expansion principle (cf. [3, Ch. 7]), we can deduce that $C_i(\tau)$ are all contained in $\mathbb{Z}[1/p, \zeta_p][j]$, the ring of polynomials in j with coefficients in $\mathbb{Z}[1/p, \zeta_p]$.

To get an explicit expression of $C_i(\tau)$ as a polynomial in j, for example, we only have to interpolate the q-expansion of $C_i(\tau)$ by

$$\begin{aligned} j &= \frac{1}{q}(1 + 744q + 196884q^2 + 21493760q^3 + \cdots), \\ j^2 &= \frac{1}{q^2}(1 + 1488q + 947304q^2 + 335950912q^3 + \cdots), \ \ldots. \end{aligned}$$

In particular, by (3.4) and (3.5), we always have

$$C_0^2(\tau) = \pm 1. \tag{4.1}$$

The following theorem is due to a numerical computation.

THEOREM 5. *λ_3 satisfies the monic equation*

$$\begin{aligned}&\lambda_3^{12} - 4(\zeta_3+2)\lambda_3^{11} + 22(\zeta_3+1)\lambda_3^{10} + \frac{1}{3^5}(2\zeta_3+1)(j-6588)\lambda_3^9\\ &\quad - \frac{1}{3^3}\zeta_3(j-2133)\lambda_3^8 + \frac{4}{3^4}(\zeta_3-1)(j-1242)\lambda_3^7 + \frac{1}{3^2}(j-1044)\lambda_3^6\\ &\quad + \frac{4}{3^4}(\zeta_3^2-1)(j-1242)\lambda_3^5 - \frac{1}{3^3}\zeta_3^2(j-2133)\lambda_3^4\\ &\quad + \frac{1}{3^5}(2\zeta_3^2+1)(j-6588)\lambda_3^3 + 22(\zeta_3^2+1)\lambda_3^2 - 4(\zeta_3^2+2)\lambda_3 + 1 = 0.\end{aligned}$$

Until the end of this section, let τ $(\in \mathfrak{H})$ be again in an imaginary quadratic number field k $(\neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}))$, and let $\Omega_\tau = [\tau, 1]$ be an $\mathfrak{o}_k$-ideal. Then from the above considerations, we see that the value $\lambda_p(\tau)$ is a unit outside the prime divisors of p. We conjecture that $\lambda_p(\tau)$ is a unit if and only if p remains prime in k.

Here we consider the case where 3 remains prime in k. From Theorem 4, $\Lambda_3(\tau)$ is a unit. Hence the equation in (ii) of Proposition 2 shows that

$$j^2 - 1512j + 177876 \equiv 0 \pmod{3^9} \quad \text{and} \quad 8j + 2214 \equiv 0 \pmod{3^4}.$$

This means that $j = 3^3 + 3^4\theta$ with an integer θ in $\mathcal{H}_k$, the Hilbert class field of k, such that $\theta^2 \equiv 0 \pmod 3$. Hence the coefficients of the equation in Theorem 5 are all in $\mathbb{Z}[\zeta_3, j]$. Thus we have the following

THEOREM 6. *Under the above notations*, $\lambda_3(\tau)$ *is a unit if and only if* 3 *remains prime in k.*

Appendix. In the proof of Theorem 1 and in the computation for the numerical example (Theorem 5), we used the following expansion formula for the Weierstrass $\wp$-function.

PROPOSITION A-1 (cf. [9, Ch. 4]). *Let $\Omega = [\tau, 1]$ with τ in $\mathfrak{H}$. Then for $z \in \mathbb{C}$ we have*

$$\frac{1}{(2\pi i)^2}\wp_\Omega(z) = \frac{1}{12} + \sum_{m\in\mathbb{Z}} \frac{q^m q_z}{(1-q^m q_z)^2} - 2\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n},$$

where $q = e^{2\pi i\tau}$ and $q_z = e^{2\pi i z}$.

Let p be an odd prime number. We apply Proposition A-1 for z which represents a non-zero p-division point of $\mathbb{C}/[\tau, 1]$. We may write $z = (a\tau + b)/p$ where $0 \le a, b \le p-1$ and $(a, b) \neq (0, 0)$. From Proposition A-1, it is easy to deduce that

$$\frac{1}{(2\pi i)^2}\wp_{\Omega_\tau}\left(\frac{a\tau+b}{p}\right) - \frac{1}{12} = R(q^{1/p}),$$

where $q^{1/p} = e^{2\pi\tau/p}$ and $R(X)$ is a power series in X whose coefficients belong to $\mathbb{Z}[\zeta_p]$ with $\zeta_p = e^{2\pi i/p}$. In order to determine the leading term of the q-expansion of $\Lambda_p(\tau)$ at ∞, we used the following

LEMMA A-2 (cf. [3, Ch. 8]). *Under the above notations,*

$$\frac{1}{(2\pi i)^2}\wp_{\Omega_\tau}\left(\frac{a\tau+b}{p}\right) - \frac{1}{12}$$

has q-expansion at ∞ in $\mathbb{Z}[\zeta_p][[q^{1/p}]]$ with leading term

$$\begin{cases} \zeta_p^b/(1-\zeta_p^b)^2 & \text{if } a=0,\\ \zeta_p^b q^{a/p} & \text{if } 0<a<p/2,\\ \zeta_p^{-b} q^{(p-a)/p} & \text{if } p/2<a<p. \end{cases}$$

References

[1] T. M. Apostol, *Modular Functions and Dirichlet Series in Number Theory*, Grad. Texts in Math. 41, Springer, 1976.

[2] A. Borel, S. Chowla, C. S. Herz, K. Iwasawa and J.-P. Serre, *Seminar on Complex Multiplication*, Lecture Notes in Math. 21, Springer, 1966.

[3] Ph. Cassou-Noguès and M. J. Taylor, *Elliptic Functions and Ring of Integers*, Progr. Math. 66, Birkhäuser, Basel, 1987.

[4] J. Cougnard, *Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers*, Acta Arith. 54 (1990), 191–212.

[5] J. Cougnard et V. Fleckinger, *Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers II*, ibid. 55 (1990), 75–81.

[6] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzykl. d. Math. Wiss., Bd. 1/2, Heft 10, Teil II, Stuttgart, 1958.

[7] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd ed., Grad. Texts in Math. 97, Springer, 1993.

[8] D. Kubert and S. Lang, *Modular Units*, Grundlehren Math. Wiss. 244, Springer, 1973.

[9] S. Lang, *Elliptic Functions*, Addison-Wesley, 1973.

[10] R. Schertz, *Zur Theorie der Ringklassenkörper über imaginär quadratischen Zahlkörpern*, J. Number Theory 10 (1978), 70–82.

Department of Mathematics
Kyushu-Tokai University
9-1-1 Toroku
Kumamoto 862-8652, Japan
E-mail: hhayashi@ktmail.ktokai-u.ac.jp

Received on 3.8.2005
and in revised form on 25.7.2006 (5044)