APPARITION AND PERIODICITY PROPERTIES OF EQUIANHARMONIC DIVISIBILITY SEQUENCES

Thesis by

Lincoln Kearney Durst

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1952

That the author of this thesis owes a debt to Professor Morgan Ward will be apparent to anyone who reads beyond this page. The size of that debt may not be as apparent, however, for it must be reckoned in terms of the very generous guidance and continual encouragement he has given since the study was undertaken.

ABSTRACT

Elliptic divisibility sequences were first studied by Morgan Ward, who proved that they admit every prime p as a divisor and gave the upper bound $2p+1$ for the smallest place of apparition of p. He also proved that, except for a few special primes, the sequences are numerically periodic modulo p.

This thesis contains a discussion of equianharmonic divisibility sequences and mappings. These sequences are the special elliptic sequences which occur when the elliptic functions involved degenerate into equianharmonic functions, and the divisibility mappings are an extension of the notion of a sequence to a function over a certain ring of quadratic integers.

For equianharmonic divisibility sequences and mappings an arithmetical relation between any rational prime of the form $3k+2$ and its rank of apparition is found.

It is also shown that, except for a few special prime ideals, equianharmonic divisibility mappings are numerically doubly periodic to prime ideal moduli.

CONTENTS

SECTION ONE

Introduction

In the first volume of the American Journal of Mathematics, Edouard Lucas [I] published his theory of the functions

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad V_n = \alpha^n + \beta^n ,$$

where α and β are the roots of $x^2 - Px + Q = 0$, P and Q rational integers. These functions satisfy the linear recursions

$$U_{n+2} = PU_{n+1} - QU_n$$

$$V_{n+2} = PV_{n+1} - QV_n .$$

Lucas also showed that U_n satisfies the difference equation

$$Q^{n-1} U_{m+n} U_{m-n} = U_{m+1} U_{m-1} U_m^2 - U_{n+1} U_{n-1} U_m^2 ,$$

and stated that this formula was fundamental to the theory of "doubly periodic numerical functions" [I, p. 203]. No explanation was given as to what he meant by double periodicity. Although he published nothing on the subject of such functions, he stated elsewhere [cf. II] that the proof of the last theorem of Fermat could be reduced to the proof of the fact that the solutions of this difference equation are at most "doubly periodic." No account of this reduction has been preserved.

The difference equation occurs in the theories of the real multiplication and the complex multiplication of elliptic functions. Morgan Ward has made a study of the solutions of this recursion

arising in the theory of the real multiplication of elliptic functions [III]; and he found that the solutions are simply periodic when taken modulo p, p a rational prime. It is shown here that in one case of complex multiplication (the equianharmonic case) a species of double periodicity occurs. Similar results hold in the lemniscate case [IV].

The remainder of this section contains results from analysis and arithmetic, collected here for convenient reference.

The Weierstrass functions $\sigma(u)$, $\zeta(u)$, $\wp(u)$, $\wp'(u)$, defined for the fundamental parallelogram

$$0, \quad 2\omega_1, \quad 2\omega_2, \quad 2\omega_1 + 2\omega_2,$$

where $\mathrm{Im}(\omega_2/\omega_1) > 0$, have the following expansions:

$$\sigma(u) = u \prod_{m,n}{}' \left\{ \left(1 - \frac{u}{2m\omega_1 + 2n\omega_2}\right) \exp\left(\frac{u}{2m\omega_1 + 2n\omega_2} + \tfrac{1}{2} \frac{u^2}{(2m\omega_1 + 2n\omega_2)^2} \right) \right\}$$

$$\zeta(u) = \frac{\sigma'(u)}{\sigma(u)} = \frac{1}{u} + \sum_{m,n}{}' \left\{ \frac{1}{u - 2m\omega_1 - 2n\omega_2} + \frac{1}{2m\omega_1 + 2n\omega_2} + \frac{u}{(2m\omega_1 + 2n\omega_2)^2} \right\}$$

$$\wp(u) = -\zeta'(u) = \frac{1}{u^2} + \sum_{m,n}{}' \left\{ \frac{1}{(u - 2m\omega_1 - 2n\omega_2)^2} - \frac{1}{(2m\omega_1 + 2n\omega_2)^2} \right\}$$

$$\wp'(u) = -2 \sum_{m,n} \frac{1}{(u - 2m\omega_1 - 2n\omega_2)^3} \quad ,$$

where the indices m, n run from $-\infty$ to $+\infty$, and the accents on $\prod$ and $\sum$ mean, as usual, that m and n do not vanish together.

The invariants g_2 and g_3 are given by

$$g_2 = 60 \sum_{m,n}{}' \frac{1}{(2m\omega_1 + 2n\omega_2)^4}, \qquad g_3 = 140 \sum_{m,n}{}' \frac{1}{(2m\omega_1 + 2n\omega_2)^6},$$

where the indices m, n have the same range as before.

In terms of u, ω_1, ω_2, the homogeneity properties of the Weierstrass functions are given by

$$\sigma(\lambda u, \lambda\omega_1, \lambda\omega_2) = \lambda\,\sigma(u, \omega_1, \omega_2)$$
$$\zeta(\lambda u, \lambda\omega_1, \lambda\omega_2) = \lambda^{-1}\zeta(u, \omega_1, \omega_2)$$
$$\wp(\lambda u, \lambda\omega_1, \lambda\omega_2) = \lambda^{-2}\wp(u, \omega_1, \omega_2)$$
$$\wp'(\lambda u, \lambda\omega_1, \lambda\omega_2) = \lambda^{-3}\wp'(u, \omega_1, \omega_2) \quad ;$$

and, in terms of u, g_2, g_3, the homogeneity properties are

$$\sigma(\lambda u; \lambda^{-4}g_2, \lambda^{-6}g_3) = \lambda\sigma(u; g_2, g_3)$$
$$\zeta(\lambda u; \lambda^{-4}g_2, \lambda^{-6}g_3) = \lambda^{-1}\zeta(u; g_2, g_3)$$
$$\wp(\lambda u; \lambda^{-4}g_2, \lambda^{-6}g_3) = \lambda^{-2}\wp(u; g_2, g_3)$$
$$\wp'(\lambda u; \lambda^{-4}g_2, \lambda^{-6}g_3) = \lambda^{-3}\wp'(u; g_2, g_3).$$

The functions $\wp(u)$, $\wp'(u)$ are doubly periodic with periods $2\omega_1$, $2\omega_2$. The pseudo-periodicity of $\sigma(u)$ is given by $\sigma(u+2r\omega_1+2s\omega_2) = (-1)^{rs+r+s}\, e^{2(r\eta_1+s\eta_2)(u+r\omega_1+s\omega_2)}\sigma(u)$, where $\eta_1 = \zeta(\omega_1)$, $\eta_2 = \zeta(\omega_2)$.

The function $\sigma(u)$ further satisfies the three-term sigma formula:

$$\sigma(u+u_1)\,\sigma(u-u_1)\,\sigma(u_2+u_3)\,\sigma(u_2-u_3)$$
$$+\,\sigma(u+u_2)\,\sigma(u-u_2)\,\sigma(u_3+u_1)\,\sigma(u_3-u_1)$$
$$+\,\sigma(u+u_3)\,\sigma(u-u_3)\,\sigma(u_1+u_2)\,\sigma(u_1-u_2) = 0.$$

These formulas may all be found in any treatise on elliptic functions; for example, Tannery et Molk [V, vol. 2, pp. 234-236].

The ring E of the Eisenstein integers consists of the numbers $a+b\rho$, a and b rational integers and $\rho = \exp(2\pi i/3)$. Since $\rho^2+\rho+1 = 0$, the conjugate and

norm in this ring are

$$\overline{a+b\rho} = a+b\rho^2 ,$$

$$N(a+b\rho) = a^2 - ab + b^2 .$$

The ring has six units ϵ, for which $N\epsilon = 1$:

$$\pm 1, \quad \pm\rho, \quad \pm\rho^2 = \mp(1+\rho);$$

and the smallest twenty-one values of $N\mu$, for μ in E, are

0, 1, 3, 4, 7, 9, 12,

13, 16, 19, 21, 25, 27, 28,

31, 36, 37, 39, 43, 48, 49.

The parity, modulo 2, of $N\mu$ is simply:

$N(a+b\rho) \equiv 0 \pmod 2$ if and only if $a \equiv b \equiv 0 \pmod 2$.

Since E is a principal ideal ring, the Möbius function $M(m)$ of the ideals of E may be defined by

$M(\epsilon) = 1$ if $N\epsilon = 1$

$M(\mu) = (-1)^r$ if (μ) is a product of r distinct prime ideals

$M(\mu) = 0$ if (μ) is divisible by the square of a prime ideal.

A discussion of the ring E is given by Hardy and Wright [VI, sections 12.9 and 15.3].

The equianharmonic case of the Weierstrass functions occurs when the period ratio ω_2/ω_1 is ρ. [VII, vol. 1, p. 136] In this case the expansions for $\sigma(u)$, $\zeta(u)$, $\wp(u)$ and $\wp'(u)$ may be written

$$\sigma(u) = u \prod_{\mu \text{ in } E}^{\mu \neq 0} \left\{ \left(1 - \frac{u}{2\mu\omega_1}\right) \exp\left(\frac{u}{2\mu\omega_1} + \tfrac{1}{2} \frac{u^2}{(2\mu\omega_1)^2} \right) \right\}$$

$$\zeta(u) = \frac{1}{u} + \sum_{\mu \text{ in } E}^{\mu \neq 0} \left\{ \frac{1}{u - 2\mu\omega_1} + \frac{1}{2\mu\omega_1} + \frac{u}{(2\mu\omega_1)^2} \right\}$$

$$\wp(u) = \frac{1}{u} - \sum_{\mu \text{ in } E}^{\mu \neq 0} \left\{ \frac{1}{(u - 2\mu\omega_1)^2} - \frac{1}{(2\mu\omega_1)^2} \right\}$$

$$\wp'(u) = -2 \sum_{\mu \text{ in } E} \frac{1}{(u - 2\mu\omega_1)^3} ,$$

where the index μ runs through E. Hence, if $N\epsilon = 1$, the homogeneity relations imply

$$\sigma(\epsilon u, \omega_1, \rho\omega_1) = \epsilon\, \sigma(u, \omega_1, \rho\omega_1)$$

$$\zeta(\epsilon u, \omega_1, \rho\omega_1) = \epsilon^{-1} \zeta(u, \omega_1, \rho\omega_1)$$

$$\wp(\epsilon u, \omega_1, \rho\omega_1) = \epsilon^{-2} \wp(u, \omega_1, \rho\omega_1)$$

$$\wp'(\epsilon u, \omega_1, \rho\omega_1) = \epsilon^{-3} \wp'(u, \omega_1, \rho\omega_1) .$$

When $\omega_2 = \rho\omega_1$ the pseudo-periodicity of $\sigma(u)$ takes the form

$$\sigma(u + 2\mu\omega_1) = (-1)^{N\mu}\, e^{2\bar{\mu}\eta_1 (u + \mu\omega_1)}\, \sigma(u) , \qquad \mu \text{ in } E,$$

since $\eta_2 = \zeta(\omega_2) = \rho^2 \zeta(\omega_1) = \rho^2 \eta_1$.

The expansion for $\sigma(u)$ shows that $\sigma(u) = 0$ if and only if

$$u = 2\mu\omega_1 , \qquad \mu \text{ in } E.$$

The differential equation satisfied by $\wp(u)$,

$$\wp'(u)^2 = 4\wp(u)^3 - g_2 \wp(u) - g_3 ,$$

is simplified by the fact that $g_2 = 0$; for

$$\wp'(\rho u)^2 = 4\wp(\rho u)^3 - g_2 \wp(\rho u) - g_3$$

or

$$\wp'(u)^2 = 4\wp(u)^3 - \rho\, g_2 \wp(u) - g_3 ,$$

hence $g_2 = 0$ and

$$\wp'(u)^2 = 4\,\wp(u)^3 - g_3 .$$

SECTION TWO

Equianharmonic Divisibility Mappings

This section contains a discussion of the properties of the function $\psi_n(u)$, which Morgan Ward used in his theory of elliptic divisibility sequences [III], for the case in which the Weierstrass functions on which it is based degenerate into equianharmonic functions. The notion of a divisibility sequence, as a mapping of the set of natural numbers into the ring of rational integers preserving division, is generalized for this case into that of a division-preserving mapping of the ring E into itself. This generalization is the key to the arithmetical structure of such sequences. The argument relies constantly on the fact that the equianharmonic functions admit a complex multiplication, which fact may be expressed in this case by the equation $\wp(\rho u) = \rho\,\wp(u)$.

Since $\sigma(u)$ is an entire function of u, the function

$$\psi_\mu(u) = \frac{\sigma(\mu u, \omega_1, \rho\omega_1)}{\sigma(u, \omega_1, \rho\omega_1)^{N\mu}}, \qquad \mu \text{ in } E,$$

is a meromorphic function of u. Furthermore it is an elliptic function since it has the periods $2\omega_1$ and $2\rho\omega_1$:

$$\begin{aligned}\psi_\mu(u+2\omega_1) &= \frac{\sigma(\mu u + 2\mu\omega_1)}{\sigma(u+2\omega_1)^{N\mu}} \\ &= \frac{(-1)^{N\mu}\, e^{2\bar{\mu}\eta_1(\mu u+\mu\omega_1)}\,\sigma(\mu u)}{\left\{-e^{2\eta_1(u+\omega_1)}\,\sigma(u)\right\}^{N\mu}} \\ &= \psi_\mu(u),\end{aligned}$$

from the pseudo-periodicity of $\sigma(u)$. Likewise

$$\psi_\mu(u+2\rho\omega_1) = \frac{\sigma(\mu u+2\mu\rho\omega_1)}{\sigma(u+2\rho\omega_1)^{N\mu}}$$

$$= \frac{(-1)^{N(\mu\rho)}\, e^{2\bar{\mu}\bar{\rho}\,\eta_1(\mu u+\mu\rho\omega_1)}\,\sigma(\mu u)}{\{-e^{2\bar{\rho}\,\eta_1(u+\rho\omega_1)}\sigma(u)\}^{N\mu}}$$

$$= \psi_\mu(u) .$$

Theorem 1. $\psi_\mu(u)$ satisfies the recursion

$$\epsilon^2\,\psi_{\mu+\nu}(u)\,\psi_{\mu-\nu}(u) = \psi_{\mu+\epsilon}(u)\,\psi_{\mu-\epsilon}(u)\,\psi_\nu^2(u) - \psi_{\nu+\epsilon}(u)\,\psi_{\nu-\epsilon}(u)\,\psi_\mu^2(u) ,$$

for μ, ν and ϵ in E, where $N\epsilon = 1$.

Proof. Replacing u, u_1, u_2, u_3 in the three-term sigma formula by 0, ϵu, μu, νu, respectively, yields

$$\epsilon^2\sigma^2(u)\,\sigma\big((\mu+\nu)u\big)\,\sigma\big((\mu-\nu)u\big) = \sigma\big((\mu+\epsilon)u\big)\,\sigma\big((\mu-\epsilon)u\big)\,\sigma^2(\nu u) - \sigma\big((\nu+\epsilon)u\big)\,\sigma\big((\nu-\epsilon)u\big)\,\sigma^2(\mu u) .$$

Since

$$2+N(\mu+\nu)+N(\mu-\nu) = N(\mu+\epsilon)+N(\mu-\epsilon)+2N\nu = N(\nu+\epsilon)+N(\nu-\epsilon)+2N\mu ,$$

division by

$$\sigma(u)^{2+N(\mu+\nu)+N(\mu-\nu)}$$

gives

$$\epsilon^2\,\psi_{\mu+\nu}(u)\,\psi_{\mu-\nu}(u) = \psi_{\mu+\epsilon}(u)\,\psi_{\mu-\epsilon}(u)\,\psi_\nu^2(u) - \psi_{\nu+\epsilon}(u)\,\psi_{\nu-\epsilon}(u)\,\psi_\mu^2(u) ,$$

which proves the theorem.

Theorem 2. Using $\psi_{\epsilon\mu}(u) = \epsilon\,\psi_{\mu}(u)$, $N\epsilon = 1$, and the recursion of theorem 1, every value of $\psi_{\mu}(u)$ may be computed from the initial values

$$\psi_0(u) = 0, \quad \psi_1(u) = 1, \quad \psi_{1-\rho}(u), \quad \psi_2(u).$$

Lemma 1. If $N\mu > 12$, $N\mu$ even,

$N\mu > 20$, $N\mu$ odd,

then $\psi_{\mu}(u)$ may be computed from the recursion if the values of $\psi_{\nu}(u)$, $N\nu < N\mu$, are known.

Proof of the lemma. Since, for any μ in E, $N\mu \equiv 0 \pmod 2$ if and only if $\mu \equiv 0 \pmod 2$, just one of the four possibilities

$$\mu \equiv 0 \pmod 2$$
$$\mu \equiv 1 \pmod 2$$
$$\mu \equiv \rho \pmod 2$$
$$\mu \equiv \rho^2 \pmod 2$$

must hold. Replacing μ, ν, ϵ in the recursion by

$$\nu+\rho,\ \nu-\rho,\ 1$$
$$\nu+1,\ \nu,\ \rho$$
$$\nu+\rho,\ \nu,\ 1$$
$$\nu+\rho^2,\ \nu,\ 1$$

yield, respectively,

$$\rho\,\psi_{2\nu}\,\psi_2 = \psi_{\nu+1+\rho}\,\psi_{\nu-1+\rho}\,\psi_{\nu-\rho}^2 - \psi_{\nu+1-\rho}\,\psi_{\nu-1-\rho}\,\psi_{\nu+\rho}^2$$
$$\rho^2\,\psi_{2\nu+1} = \psi_{\nu+1+\rho}\,\psi_{\nu+1-\rho}\,\psi_{\nu}^2 - \psi_{\nu+\rho}\,\psi_{\nu-\rho}\,\psi_{\nu+1}^2$$
$$\rho\,\psi_{2\nu+\rho} = \psi_{\nu+1+\rho}\,\psi_{\nu-1+\rho}\,\psi_{\nu}^2 - \psi_{\nu+1}\,\psi_{\nu-1}\,\psi_{\nu+\rho}^2$$
$$\rho^2\,\psi_{2\nu+\rho^2} = \psi_{\nu+1+\rho^2}\,\psi_{\nu-1+\rho^2}\,\psi_{\nu}^2 - \psi_{\nu+1}\,\psi_{\nu-1}\,\psi_{\nu+\rho^2}^2.$$

Since $N(1-\rho) = N(1-\rho^2) = 3$, every subscript appearing on the right side of any of these equations lies in or on the circle of radius $\sqrt{3}$ and center ν.

Case 1. μ even. If $N\mu > 12$ or $|\mu| > 2\sqrt{3}$,

$$|\mu| - \tfrac{1}{2}|\mu| = \tfrac{1}{2}|\mu| > \sqrt{3}$$

so that μ lies farther from the origin than any point in or on the circle of radius $\sqrt{3}$ and center $\frac{1}{2}\mu$.

Case 2. $\mu \equiv \epsilon \pmod 2$, $N\epsilon = 1$. If $N\mu > 20$, or $|\mu| > 2\sqrt{5}$,

$$\begin{aligned} |\mu| - \tfrac{1}{2}|\mu-\epsilon| &\geqslant |\mu| - \tfrac{1}{2}(|\mu|+1) \\ &\geqslant \tfrac{1}{2}|\mu| - \tfrac{1}{2} \\ &> \sqrt{5} - \tfrac{1}{2} > \sqrt{3}, \end{aligned}$$

and μ lies farther from the origin than any point in or on the circle of radius $\sqrt{3}$ and center $\frac{1}{2}(\mu-\epsilon)$. The lemma is proved.

Proof of the theorem. For $n = 7, 9, 12, 13, 19$ the equations $N\mu = n$ have the following solutions:

$N\mu = 7$ $\quad \mu = (1-2\rho)\epsilon\ ,\ (3+2\rho)\epsilon$

$N\mu = 9$ $\quad \mu = 3\epsilon$

$N\mu = 12$ $\quad \mu = (4+2\rho)\epsilon$

$N\mu = 13$ $\quad \mu = (1+4\rho)\epsilon\ ,\ (3+4\rho)\epsilon$

$N\mu = 19$ $\quad \mu = (3-2\rho)\epsilon\ ,\ (5+2\rho)\epsilon$.

The cases $N\mu = 19$ and $N\mu = 13$. Taking $\mu = \nu+1$ and $\epsilon = 1$ in the recursion gives

$$\psi_{2\nu+1} = \psi_{\nu+2}\,\psi_\nu^3 - \psi_{\nu-1}\,\psi_{\nu+1}^3$$

ν	$2\nu+1$	$N(2\nu+1)$	$N(\nu+2)$	$N\nu$	$N(\nu-1)$	$N(\nu+1)$
$-2+\rho$	$-3+2\rho$	19	3	7	13	3
$-3-\rho$	$-5-2\rho$	19	3	7	13	3
2ρ	$1+4\rho$	13	4	4	7	3
$-2-2\rho$	$-3-4\rho$	13	4	4	7	3

Thus $\psi_{-3+2\rho}$, $\psi_{-5-2\rho}$, $\psi_{1+4\rho}$, $\psi_{-3-4\rho}$ may each be computed from values with indices of smaller norm. The other ten ψ_μ for $N\mu = 19$ and for $N\mu = 13$ are unit multiples of these. The case $N\mu = 12$. Although μ lies on the circle of radius $\sqrt{3}$ and center $\frac{1}{2}\mu$, the first formula employed in proving the lemma may be used to compute $\psi_{4+2\rho}$. For, if $\nu = 2+\rho$,

$$\begin{aligned} N(\nu-\rho) &= 4 & N(\nu+\rho) &= 4 \\ N(\nu+1+\rho) &= 7 & N(\nu+1-\rho) &= 9 \\ N(\nu-1+\rho) &= 3 & N(\nu-1-\rho) &= 1. \end{aligned}$$

The other five ψ_μ, $N\mu = 12$, are unit multiples of $\psi_{4+2\rho}$. The case $N\mu = 9$. ψ_3 may be computed from the second formula used to prove the lemma, for, if $\mu = 3$,

$$|\mu| - \tfrac{1}{2}|\mu-1| = 2 > \sqrt{3};$$

and the other five ψ_μ, $N\mu = 9$, are unit multiples of ψ_3. The case $N\mu = 7$. Taking $\mu = \nu + 1$ and $\epsilon = \rho^2 = -1-\rho$ in the recursion gives

$$\rho\,\psi_{2\nu+1} = \psi_{\nu+2+\rho}\,\psi_{\nu-\rho}\,\psi_\nu^2 - \psi_{\nu+1+\rho}\,\psi_{\nu-1-\rho}\,\psi_{\nu+1}^2,$$

and if $\nu = -\rho$, then $2\nu+1 = 1-2\rho$ and

$$\begin{aligned} N(\nu+2+\rho) &= 4 & N(\nu+1+\rho) &= 1 \\ N(\nu-\rho) &= 4 & N(\nu-1-\rho) &= 3 \\ N\nu &= 1 & N(\nu+1) &= 3, \end{aligned}$$

which exhibits a method of computing $\psi_{1-2\rho}$. The second formula in the lemma proof suffices for $\psi_{3+2\rho}$, since if $\nu = 1+\rho$, then $2\nu+1 = 3+2\rho$ and

$$\begin{aligned} N(\nu+1+\rho) &= 4 & N(\nu+\rho) &= 3 \\ N(\nu+1-\rho) &= 4 & N(\nu-\rho) &= 1 \\ N\nu &= 1 & N(\nu+1) &= 3. \end{aligned}$$

The other ten are unit multiples of these two.

The equations

$$N\mu = 1,\ 3,\ 4, \qquad \mu \text{ in } E,$$

have the six solutions

$$\epsilon\ ,\quad (1-\rho)\epsilon\ ,\quad 2\epsilon\ ,\quad N\epsilon = 1,$$

respectively. Therefore every value of ψ_μ , $N\mu \leq 4$, is a unit multiple of one of ψ_0 , ψ_1 , $\psi_{1-\rho}$, ψ_2 . But every ψ_μ may be computed from various ψ_ν , $N\nu \leq 4$; hence the theorem is proved.

If $N\mu > 0$ and $N\nu > 0$, the two elliptic functions

$$\frac{\psi_{\mu+\nu}(u)\ \psi_{\mu-\nu}(u)}{\psi_\mu^2(u)\ \psi_\nu^2(u)} = \frac{\sigma((\mu+\nu)u)\,\sigma((\mu-\nu)u)}{\sigma^2(\mu u)\,\sigma^2(\nu u)} \quad \text{and}$$

$\wp(\nu u) - \wp(\mu u)$ have the same poles, whose orders and principal parts are equal. Hence

$$\frac{\psi_{\mu+\nu}(u)\ \psi_{\mu-\nu}(u)}{\psi_\mu^2(u)\ \psi_\nu^2(u)} = \wp(\nu u) - \wp(\mu u).$$

Taking $\mu = 1$ and $\nu = \rho$,

$$\frac{\psi_{1+\rho}(u)\ \psi_{1-\rho}(u)}{\psi_1^2(u)\ \psi_\rho^2(u)} = \wp(\rho u) - \wp(u),$$

and since $\wp(\rho u) = \rho\,\wp(u)$ and $\psi_\epsilon(u) = \epsilon$, for $N\epsilon = 1$,

$$\psi_{1-\rho}(u) = (1-\rho)\,\wp(u).$$

The other initial value

$$\psi_2(u) = -\wp'(u)$$

may be found in Tannery et Molk [V, vol. 4, p. 98].

Theorem 3. $\psi_\mu(u) = P_\mu(z, g_3)$, $N\mu$ odd,

$\psi_\mu(u) = \wp'(u) P_\mu(z, g_3)$, $N\mu$ even,

where $z = \wp(u)$ and $P_\mu(z, g_3)$ is a polynomial in z and g_3 over E.

Proof by induction. The theorem holds for the initial values

$$\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_{1-\rho} = (1-\rho)z, \quad \psi_2 = -\wp'(u)$$

and for any unit multiple of them. Since $g_2 = 0$,

$$\wp'(u)^2 = 4\wp(u)^3 - g_3 = 4z^3 - g_3.$$

Case 1. $N\mu$ odd. If $\mu = 2\nu + \epsilon_1$, $N\epsilon_1 = 1$, taking $\mu = \nu + \epsilon_1$ in the recursion gives

$$\epsilon^2 \psi_{2\nu+\epsilon_1} \psi_{\epsilon_1} = \psi_{\nu+\epsilon_1+\epsilon} \psi_{\nu+\epsilon_1-\epsilon} \psi_\nu^2 - \psi_{\nu+\epsilon} \psi_{\nu-\epsilon} \psi_{\nu+\epsilon_1}^2$$

or

$$\psi_{2\nu+\epsilon_1} = \epsilon^{-2}\epsilon_1^{-1}\left\{\psi_{\nu+\epsilon_1+\epsilon} \psi_{\nu+\epsilon_1-\epsilon} \psi_\nu^2 - \psi_{\nu+\epsilon} \psi_{\nu-\epsilon} \psi_{\nu+\epsilon_1}^2\right\}.$$

The formulas used to compute ψ_μ, $N\mu = 13, 19$, are special cases of this expression for which $\epsilon = \epsilon_1$; all the other formulas used in the proofs of lemma 1 and theorem 2 for $N\mu$ odd are special cases for which $\epsilon \neq \epsilon_1$. Since (in either case)

$$\nu + \epsilon_1 + \epsilon \equiv \nu + \epsilon_1 - \epsilon \pmod 2$$

and

$$\nu + \epsilon \equiv \nu - \epsilon \pmod 2,$$

wherever $\wp'(u)$ may occur in this expression for $\psi_{2\nu+\epsilon_1}$ (if it occurs at all), it does so to the second power. Case 1 is therefore proved by induction on $N\mu$.

Case 2. $\mu = 2\nu$, $\nu \equiv \epsilon \pmod 2$. Replacing μ and ν in the recursion by $\nu+\epsilon$ and $\nu-\epsilon$, respectively, gives

$$\psi_{2\nu} \psi_{2\epsilon} = \psi_\nu \left(\psi_{\nu+2\epsilon} \psi_{\nu-\epsilon}^2 - \psi_{\nu-2\epsilon} \psi_{\nu+\epsilon}^2\right).$$

Suppose that $N\mu > 4$, and that if $N(2K) < N\mu$, ψ_{2K} is $\wp'(u)$ times a polynomial in z, g_3 over E. Since

$$N\mu = N(2\nu) > 4, \quad |\nu| > 1 \qquad \text{and}$$

$$2|\nu| \geq |\nu| + 1 \geq |\nu \pm \epsilon|,$$

or

$$N(2\nu) > N(\nu \pm \epsilon).$$

Because

$$\nu - \epsilon \equiv \nu + \epsilon \equiv 0 \pmod 2$$

but $\nu \equiv \nu + 2\epsilon \equiv \nu - 2\epsilon \not\equiv 0 \pmod 2$,

$\wp'(u)$ occurs on the right side to the second power; and since $\psi_{2\epsilon} = -\epsilon\, \wp'(u)$, $\psi_{2\nu}$ is $\wp'(u)$ times a polynomial in z, g_3 over E.

Case 3. $\mu = 2\nu$, $\nu \equiv 0 \pmod 2$. Direct computation shows that

$$\psi_4(u) = -\wp'(u)\left\{2z^6 - 10g_3 z^3 - g_3^2\right\}.$$

Suppose that $N\mu > 16$ and that if $N(2\kappa) < N\mu$, $\psi_{2\kappa}$ is $\wp'(u)$ times a polynomial in z, g_3 over E. Since

$$N\mu = N(2\nu) > 16, \quad |\nu| > 2 \qquad \text{and}$$

$$2|\nu| > |\nu| + 2 \geq |\nu \pm 2\epsilon|$$

or $$N\mu > N\nu,\ N(\nu \pm 2\epsilon).$$

But $\nu \equiv \nu \pm 2\epsilon \equiv 0 \pmod 2$

and $\nu + \epsilon \equiv \nu - \epsilon \not\equiv 0 \pmod 2$;

so $\wp'(u)$ occurs on the right-hand side of

$$\psi_{2\nu}\,\psi_{2\epsilon} = \psi_\nu\left(\psi_{\nu+2\epsilon}\,\psi_{\nu-\epsilon}^2 - \psi_{\nu-2\epsilon}\,\psi_{\nu+\epsilon}^2\right)$$

to the second power, and the theorem follows by induction on $N\mu$.

The nature of the pole at $u = 0$ gives an immediate corollary to theorem 3: considered as a polynomial in z, the leading coefficient of $P_\mu(z, g_3)$ is

$$\begin{cases} \mu & \text{if } N\mu \text{ odd} \\ -\frac{1}{2}\mu & \text{if } N\mu \text{ even,} \end{cases}$$

and the degree of $P_\mu(z, g_3)$ in z is

$$\begin{cases} \frac{1}{2}(N\mu - 1) & \text{if } N\mu \text{ odd} \\ \frac{1}{2}(N\mu - 4) & \text{if } N\mu \text{ even.} \end{cases}$$

Theorem 4. If $N\mu \equiv 0 \pmod 3$,

$$P_\mu(z,g_3) = \sum_{r=0}^{\frac{1}{3}(D\mu-1)} \kappa_r g_3^r z^{D\mu-3r}, \qquad \kappa_r \text{ in } E,$$

and if $N\mu \equiv 1 \pmod 3$,

$$P_\mu(z,g_3) = \sum_{r=0}^{\frac{1}{3}D\mu} \kappa_r g_3^r z^{D\mu-3r}, \qquad \kappa_r \text{ in } E,$$

where $D\mu$ is the degree of $P_\mu(z,g_3)$ in z.

Proof. First:

$D\mu \equiv 1 \pmod 3$ if and only if $N\mu \equiv 0 \pmod 3$

$D\mu \equiv 0 \pmod 3$ if and only if $N\mu \equiv 1 \pmod 3$,

but $N\mu$ is never congruent to 2 modulo 3. The homogeneity of $\sigma(u)$, $\wp(u)$, $\wp'(u)$ as functions of the invariants are given by

$$\sigma(\lambda u; \lambda^{-4}g_2, \lambda^{-6}g_3) = \lambda\,\sigma(u; g_2, g_3)$$

$$\wp(\lambda u; \lambda^{-4}g_2, \lambda^{-6}g_3) = \lambda^{-2}\wp(u; g_2, g_3)$$

$$\wp'(\lambda u; \lambda^{-4}g_2, \lambda^{-6}g_3) = \lambda^{-3}\wp'(u; g_2, g_3).$$

Hence

$$\sigma(u; 0, g_3) = g_3^{-\frac{1}{6}}\sigma(g_3^{\frac{1}{6}}u; 0, 1)$$

$$\wp(u; 0, g_3) = g_3^{\frac{1}{3}}\wp(g_3^{\frac{1}{6}}u; 0, 1)$$

$$\wp'(u; 0, g_3) = g_3^{\frac{1}{2}}\wp'(g_3^{\frac{1}{6}}u; 0, 1)$$

and

$$\psi_\mu(u; 0, g_3) = \frac{\sigma(\mu u; 0, g_3)}{\sigma(u; 0, g_3)^{N\mu}}$$

$$= \frac{g_3^{-\frac{1}{6}}\,\sigma(\mu g_3^{\frac{1}{6}}u; 0, 1)}{(g_3^{-\frac{1}{6}})^{N\mu}\,\sigma(g_3^{\frac{1}{6}}u; 0, 1)^{N\mu}}$$

$$= g_3^{\frac{N\mu-1}{6}} \psi_\mu(g_3^{\frac{1}{6}} u;\ 0,1)\ .$$

Let $y = \wp(g_3^{\frac{1}{6}} u;\ 0,1)$, then $y = z g_3^{-\frac{1}{3}}$. Writing

$$\psi_\mu(u;\ 0,g_3) = E_\mu(u)\ P_\mu(z,g_3),$$

where $E_\mu(u) = 1$ if $N\mu$ odd

$E_\mu(u) = \wp'(u)$ if $N\mu$ even;

$$\psi_\mu(g_3^{\frac{1}{6}} u;\ 0,1) = E_\mu(g_3^{\frac{1}{6}} u)\ P_\mu(y,1).$$

Hence, if $N\mu$ odd

$$\psi_\mu(u;\ 0,g_3) = g_3^{\frac{N\mu-1}{6}} P_\mu(y,1)$$
$$= g_3^{\frac{1}{3}D\mu} P_\mu(y,1)$$

and if $N\mu$ even,

$$\psi_\mu(u;\ o,g_3) = g_3^{\frac{N\mu-1}{6}} \wp'(g_3^{\frac{1}{6}} u;\ 0,1)\ P_\mu(y,1)$$
$$= g_3^{\frac{N\mu-4}{6}} g_3^{\frac{1}{2}} \wp'(g_3^{\frac{1}{6}} u;\ 0,1)\ P_\mu(y,1)$$
$$= g_3^{\frac{1}{3}D\mu} \wp'(u;\ 0,g_3)\ P_\mu(y,1).$$

Consequently, in either case,

$$P_\mu(z,g_3) = g_3^{\frac{1}{3}D\mu} P_\mu(y,1).$$

On the other hand,

$$\sigma(\rho u, \omega_1, \rho\omega_1) = \rho\,\sigma(u, \omega_1, \rho\omega_1),$$

hence

$$\psi_\mu(\rho u;\ 0,1) = \rho^{1-N\mu} \psi_\mu(u;\ 0,1)$$

and $$\psi_\mu(\rho^2 u;\ 0,1) = \rho^{2(1-N\mu)} \psi_\mu(u;\ 0,1).$$

But, by theorem 3 and its corollary,

$$P_\mu(y,1) = \sum_{s=0}^{D\mu} \lambda_s y^s, \qquad \lambda_s \text{ in } E,$$

therefore

$$P_\mu(\rho y,1) = \sum_{s=0}^{D\mu} \lambda_s \rho^s y^s = \rho^{1-N\mu} P_\mu(y,1).$$

$$P_\mu(\rho^2 y,1) = \sum_{s=0}^{D\mu} \lambda_s \rho^{2s} y^s = \rho^{2(1-N\mu)} P_\mu(y,1).$$

Now if $N\mu \equiv 1 \pmod 3$, $\rho^{1-N\mu} = \rho^{2(1-N\mu)} = 1$, so

$$P_\mu(y,1) = \sum_{s=0}^{D\mu} \lambda_s y^s = \sum_{s=0}^{D\mu} \lambda_s \rho^s y^s = \sum_{s=0}^{D\mu} \lambda_s \rho^{2s} y^s,$$

and, adding,

$$3P_\mu(y,1) = \sum_{s=0}^{D\mu} \lambda_s (1+\rho^s+\rho^{2s}) y^s.$$

But

$$1+\rho^s+\rho^{2s} = 3 \qquad \text{if } s \equiv 0 \pmod 3$$
$$1+\rho^s+\rho^{2s} = 0 \qquad \text{if } s \not\equiv 0 \pmod 3,$$

so

$$P_\mu(y,1) = \sum_{s=0}^{\frac{1}{3}D\mu} \lambda_{3s} y^{3s}$$

and

$$P_\mu(z,g_3) = g_3^{\frac{1}{3}D\mu} \sum_{s=0}^{\frac{1}{3}D\mu} \lambda_{3s} g_3^{-s} z^{3s}$$
$$= \sum_{\lambda=0}^{\frac{1}{3}D\mu} \kappa_\lambda g_3^\lambda z^{D\mu-3\lambda}.$$

But, if $N\mu \equiv 0 \pmod 3$, $\rho^{1-N\mu} = \rho$, $\rho^{2(1-N\mu)} = \rho^2$,

so

$$P_\mu(y,1) = \sum_{s=0}^{D\mu} \lambda_s y^s = \rho^2 \sum_{s=0}^{D\mu} \lambda_s \rho^s y^s = \rho \sum_{s=0}^{D\mu} \lambda_s \rho^{2s} y^s,$$

and, adding,

$$3P_\mu(y,1) = \sum_{s=0}^{D\mu} \lambda_s (1+\rho^{2+s}+\rho^{1+2s}) y^s.$$

But

$$1+\rho^{2+s}+\rho^{1+2s} = 3 \qquad \text{if } s \equiv 1 \pmod 3$$
$$1+\rho^{2+s}+\rho^{1+2s} = 0 \qquad \text{if } s \not\equiv 1 \pmod 3,$$

so

$$P_\mu(y,1) = \sum_{s=0}^{\frac{1}{3}(D\mu-1)} \lambda_{3s+1}\, y^{3s+1}$$

and

$$P_\mu(z,g_3) = g_3^{\frac{1}{3}D\mu} \sum_{s=0}^{\frac{1}{3}(D\mu-1)} \lambda_{3s+1}\, g_3^{-\frac{3s+1}{3}}\, z^{3s+1}$$

$$= \sum_{r=0}^{\frac{1}{3}(D\mu-1)} \kappa_r\, g_3^{r}\, z^{D\mu-3r}.$$

Theorem 5. If $\nu \mid \mu$ then $P_\nu(z,g_3) \mid P_\mu(z,g_3)$.

Proof. Let $\mu = \lambda\nu$. Then

$$\psi_\mu(u) = \psi_{\lambda\nu}(u) = \frac{\sigma(\lambda\nu\, u)}{\sigma(u)^{N(\lambda\nu)}} = \frac{\sigma(\lambda\nu\, u)}{\sigma(\nu u)^{N\lambda}} \left\{ \frac{\sigma(\nu u)}{\sigma(u)^{N\nu}} \right\}^{N\lambda}$$

$$= \psi_\lambda(\nu u)\, \psi_\nu(u)^{N\lambda}.$$

Hence, if $N\lambda$ and $N\nu$ are odd,

$$P_\mu(z,g_3) = P_\lambda\big(\wp(\nu u), g_3\big)\, P_\nu(z,g_3)^{N\lambda}.$$

But $D\lambda = \frac{1}{2}(N\lambda - 1)$ and

$$\wp(\nu u) = \wp(u) - \frac{\psi_{\nu-1}(u)\, \psi_{\nu+1}(u)}{P_\nu(z,g_3)^2}$$

$$= \frac{zP_\nu(z,g_3)^2 - \psi_{\nu-1}(u)\, \psi_{\nu+1}(u)}{P_\nu(z,g_3)^2}$$

so $$P_\mu(z,g_3) = P(z,g_3)\, P_\nu(z,g_3)$$

where

$$P(z,g_3) = P_\nu(z,g_3)^{N\lambda-1}\, P_\lambda\big(\wp(\nu u), g_3\big)$$

$$= \sum \kappa_r\, g_3^{r} \big(zP_\nu(z,g_3)^2 - \psi_{\nu-1}(u)\, \psi_{\nu+1}(u)\big)^{D\lambda-3r}\, P_\nu(z,g_3)^{6r}$$

is a polynomial in z and g_3 over E. The cases where one or

both of $N\lambda$, $N\nu$ are even may be carried out in a similar manner. This theorem may also be deduced directly from the recursion by an argument similar to the proof of theorem 4.1 of Ward's Memoir [III].

SECTION THREE

The Apparition of Prime Ideals

Fix z and g_3 in the ring of rational integers. Then the correspondence $\mu \rightarrow P_\mu(z,g_3)$ is a mapping of E into itself which preserves division (theorem 5). Let $\mathfrak{p}$ be a prime ideal of E. An integer λ of E is called a zero of $\mathfrak{p}$ if

$$P_\lambda(z,g_3) \equiv 0 \pmod{\mathfrak{p}}.$$

A zero α of $\mathfrak{p}$ with minimum positive norm is called a rank of apparition of $\mathfrak{p}$.

By an argument similar to the proof of theorem 5.1 of Ward's Memoir [III] it can be shown that every prime ideal appears somewhere. The object of this section is to find an arithmetical relationship between $\mathfrak{p}$ and α. For this purpose the prime ideals $\mathfrak{p}$ of E are divided into two classes according as $P_{1-\rho}(z)$ is or is not congruent to zero modulo $\mathfrak{p}$. The latter $\mathfrak{p}$ will be called regular prime ideals, and the former irregular.

The Apparition of Irregular Prime Ideals

If $z \equiv 0 \pmod{\mathfrak{p}}$, then theorem 4 implies

$$P_\mu(z,g_3) \equiv 0 \pmod{\mathfrak{p}} \quad \text{if } N\mu \equiv 0 \pmod 3$$
$$\equiv \varkappa_\lambda g_3^{\frac{1}{3}\mathfrak{D}\mu} \pmod{\mathfrak{p}} \quad \text{if } N\mu \equiv 1 \pmod 3,$$

where $\varkappa_\lambda = P_\mu(0,1)$ is an integer of E.

Lemma 2. If $N\mu \equiv 1 \pmod 3$, then $P_\mu(0,1)$ is a unit of E.

Proof. For any μ in E, just one of the three possibilities

$$\mu \equiv 0 \pmod{1-\rho}$$
$$\mu \equiv 1 \pmod{1-\rho}$$
$$\mu \equiv -1 \pmod{1-\rho}$$

holds, and $N\mu \equiv 1 \pmod 3$ means $\mu \equiv \pm 1 \pmod{1-\rho}$. Replacing μ and ν in the recursion by $(1-\rho)\nu$ and $(1+\rho)\nu$, respectively, and taking $\epsilon = 1$, gives

$$\psi_{2\nu}\,\psi_{-2\rho\nu} = \psi_{(1-\rho)\nu+1}\,\psi_{(1-\rho)\nu-1}\,\psi^2_{(1+\rho)\nu} - \psi_{(1+\rho)\nu+1}\,\psi_{(1+\rho)\nu-1}\,\psi^2_{(1-\rho)\nu},$$

and when $z = 0$,

$$\psi_{(1-\rho)\nu} = 0 \quad \text{and} \quad \psi_{(1-\rho)\nu+1}\,\psi_{(1-\rho)\nu-1} = -\frac{\psi^2_{2\nu}}{\psi^2_\nu}.$$

Since

$$\wp(2u) = \tfrac{1}{4}\left\{\frac{\wp''(u)}{\wp'(u)}\right\}^2 - 2\wp(u), \qquad \wp''(u) = 6\wp(u)^2$$

[I, vol. 4, p. 97], $\wp(\mu) = 0$ implies $\wp(2u) = 0$, and hence taking $\mu = 2$, $z = 0$, $g_3 = 1$ in

$$\psi_{\mu\nu}(u) = \psi_\nu(\mu u)\,\psi_\mu(u)^{N\nu}$$

gives

$$\frac{\psi_{2\nu}}{\psi_\nu} = \psi_2^{N\nu} = (-i)^{N\nu}, \quad \text{at } z = 0.$$

Consequently

$$P_{(1-\rho)\nu+1}(0,1)\,P_{(1-\rho)\nu-1}(0,1) = (-1)^{N((1-\rho)\nu+1)}.$$

Therefore, both of the quantities $P_{(1-\rho)\nu+1}(0,1)$, $P_{(1-\rho)\nu-1}(0,1)$, being integers in E, are units in E.

Theorem 6. If $g_3 \not\equiv z \equiv 0 \pmod{\mathcal{P}}$, then $P_\mu(z,g_3) \equiv 0 \pmod{\mathcal{P}}$ if and only if $N\mu \equiv 0 \pmod 3$.

And if $g_3 \equiv z \equiv 0 \pmod{\mathcal{P}}$, then $P_\mu(z,g_3) \equiv 0 \pmod{\mathcal{P}}$ if and only if $N\mu \neq 1,4$.

In either case $\alpha = (1-\rho)\epsilon$.

Proof. The first part is a consequence of the lemma, and the second part is immediate for $D\mu = 0$ if and only if $N\mu = 1,4$.

Theorem 7. If $g_3 \not\equiv z^3 \pmod{1-\rho}$, then $P_\mu(z,g_3) \equiv 0 \pmod{1-\rho}$ if and only if $N\mu \equiv 0 \pmod 3$.

And if $g_3 \equiv z^3 \pmod{1-\rho}$, then $P_\mu(z,g_3) \equiv 0 \pmod{1-\rho}$ if and only if $N\mu \neq 1,4$.

In either case $\alpha = (1-\rho)\epsilon$.

Proof. Suppose $g_3 \not\equiv z^3 \pmod{1-\rho}$. Replacing μ and ν in the recursion by $(1-\rho)\nu$ and $(1+\rho)\nu$, respectively, and taking $\epsilon = 1$, gives

$$\begin{aligned}\psi_{2\nu}\,\psi_{-2\rho\nu} &= \psi_{(1-\rho)\nu+1}\,\psi_{(1-\rho)\nu-1}\,\psi^2_{(1+\rho)\nu} - \psi_{(1+\rho)\nu+1}\,\psi_{(1+\rho)\nu-1}\,\psi^2_{(1-\rho)\nu} \\ &\equiv \psi_{(1-\rho)\nu+1}\,\psi_{(1-\rho)\nu-1}\,\psi^2_{(1+\rho)\nu} \pmod{1-\rho},\end{aligned}$$

by theorem 5. But

$$\psi_{2\nu}(u) = \psi_\nu(2u)\,\psi_2(u)^{N\nu}$$

and

$$\begin{aligned}\wp(2u) &= \tfrac{1}{4}\left\{\frac{6\,\wp(u)^2}{4z^3 - g_3}\right\}^2 - 2\wp(u) \\ &\equiv \wp(u) \pmod{1-\rho}\end{aligned}$$

since $3 \equiv 0$, $2 \equiv -1$, $g_3 \not\equiv z^3 \pmod{1-\rho}$. Hence

$$\psi_{2\nu}(u) \equiv \psi_\nu(u)\,\psi_2(u)^{N\nu} \pmod{1-\rho},$$

and, consequently,

$$\psi_{(1-\rho)\nu-1}\,\psi_{(1-\rho)\nu+1} \equiv -\psi_2(u)^{2N\nu} \pmod{1-\rho}$$

$$\equiv -(z^3-g_3)^{N\nu} \pmod{1-\rho}.$$

So, if $g_3 \not\equiv z^3 \pmod{1-\rho}$, then

$$\psi_\mu(u) \equiv 0 \pmod{1-\rho} \text{ if and only if } N\mu \equiv 0 \pmod 3.$$

On the other hand, if $g_3 \equiv z^3 \pmod{1-\rho}$, then

$$P_\mu(z,g_3) \equiv z^{D\mu}\, P_\mu(1,1) \pmod{1-\rho}.$$

But $$\wp'(u)^2 = 4z^3 - g_3 \equiv 3z^3 \equiv 0 \pmod{1-\rho}$$

and

$$P_\epsilon(1,1) = \epsilon \qquad \text{if } N\epsilon = 1$$

$$P_{2\epsilon}(1,1) = -\epsilon$$

$$P_\mu(1,1) \equiv 0 \pmod{1-\rho} \qquad \text{if } N\mu \neq 1,4.$$

The Apparition of Regular Prime Ideals

Theorem 8. If $z \not\equiv 0 \pmod 2$, then the rank of apparition of 2 is

4ϵ	if	$g_3 \equiv 0 \pmod 2$
3ϵ	if	$g_3 \equiv 1 \pmod 2$
$(1-2\rho)\epsilon$	if	$g_3 \equiv \rho \pmod 2$
$(3+2\rho)\epsilon$	if	$g_3 \equiv \rho^2 \pmod 2$.

Proof. If $g_3 \equiv 0 \pmod 2$, then

$$P_\mu(z,g_3) \equiv \mu\, z^{D\mu} \pmod 2 \quad \text{if } N\mu \text{ odd}$$

$$P_\mu(z,g_3) \equiv -\tfrac{1}{2}\mu z^{D\mu} \pmod 2 \text{ if } N\mu \text{ even}.$$

On the other hand

$$\psi_0 \equiv 0, \quad \psi_1 \equiv 1, \quad \psi_{1-\rho} \equiv \rho^2 z, \quad \psi_2 \equiv \wp' \pmod 2,$$

where $\wp'^2 \equiv g_3 \pmod 2$, and direct computation shows that

$$\psi_{1-2\rho} \equiv 1 + \rho^2 g_3 \pmod 2$$
$$\psi_{3+2\rho} \equiv 1 + \rho\, g_3 \pmod 2$$
$$\psi_3 \equiv z(1+g_3) \pmod 2 .$$

Lemma 3. If $\mathfrak{p} = (\pi)$ is a prime ideal of E and $N\pi = p$, an odd rational prime, then

$$P_\pi(z, g_3) \equiv P_\pi(0, g_3) \pmod{\mathfrak{p}}, \quad \text{all } z.$$

(A result of this nature for Jacobi lemniscate functions may be found in Eisenstein's Works [VIII, p. 131].)

Proof. If $\pi = 1-\rho$, the lemma is trivial. Suppose $N\pi \equiv 1 \pmod 6$. Logarithmic differentiation of the definition of $\psi_\pi(u)$ gives

$$\frac{\psi_\pi'(u)}{\psi_\pi(u)} = \pi \frac{\sigma'(\pi u)}{\sigma(\pi u)} - N\pi \frac{\sigma'(u)}{\sigma(u)},$$

where the accents denote differentiation with respect to u. Differentiating again yields

$$\psi_\pi'(u)^2 - \psi_\pi(u)\psi_\pi''(u) = \psi_\pi(u)^2 \left\{ \pi^2 \wp(\pi u) - \wp(u) N\pi \right\} = \pi P(z),$$

where $P(z)$ is a polynomial in z over E, since

$$\wp(u) = -\frac{d}{du}\left\{\frac{\sigma'(u)}{\sigma(u)}\right\},$$
$$\wp(\pi u) = \wp(u) - \frac{\psi_{\pi-1}(u)\,\psi_{\pi+1}(u)}{\psi_\pi(u)^2}.$$

But since $N\pi$ is odd,

$$\psi_\pi(u) = P_\pi(z)$$

and

$$\psi_\pi'(u) = \wp'(u)\, P_\pi'(z)$$
$$\psi_\pi''(u) = \wp''(u)\, P_\pi'(z) + \wp'(u)^2\, P_\pi''(z),$$

where the accents on $\psi_\pi(u)$ and $\wp(u)$ denote differentiations

with respect to u, but the accents on $P_\pi(z)$ denote differentiations with respect to z. Hence

$$\psi_\pi'^{\,2} - \psi_\pi \psi_\pi'' = \wp'^{\,2}(P_\pi'^{\,2} - P_\pi P_\pi'') - \wp'' P_\pi P_\pi' \ .$$

And since

$$N\pi \equiv 1 \pmod 3 \ ,$$

$$P_\pi(z) = \sum_{\lambda=0}^{\frac{1}{3}D\pi} \kappa_\lambda \, g_3^{\lambda} \, z^{D\pi - 3\lambda} \ .$$

By the corollary to theorem 3, $\kappa_0 = \pi$ since $N\pi$ is odd. If $g_3 \equiv 0 \pmod \pi$, there is nothing to prove. Suppose

$$\kappa_s \not\equiv \kappa_{s-1} \equiv \cdots \equiv \kappa_1 \equiv \kappa_0 \equiv 0 \not\equiv g_3 \pmod \pi .$$

Then

$$\left.\begin{aligned} P_\pi(z) &= \sum_{\lambda=s}^{\frac{1}{3}D\pi} \kappa_\lambda \, g_3^{\lambda} \, z^{D\pi-3\lambda} \\ P_\pi'(z) &= \sum_{\lambda=s}^{\frac{1}{3}D\pi} (D\pi - 3r)\kappa_\lambda \, g_3^{\lambda} \, z^{D\pi-3\lambda-1} \\ P_\pi''(z) &= \sum_{\lambda=s}^{\frac{1}{3}D\pi} (D\pi - 3r)(D\pi - 3r - 1)\kappa_\lambda \, g_3^{\lambda} \, z^{D\pi-3\lambda-2} \end{aligned}\right\} \pmod \pi ,$$

and since $\wp'^{\,2} = 4z^3 - g_3$, $\wp'' = 6z$,

$$\begin{aligned} 0 \equiv \psi_\pi'^{\,2} - \psi_\pi \psi_\pi'' \pmod \pi, \text{ all } z \\ &\equiv 4z^3(D\pi - 3s)^2 \kappa_s^2 \, g_3^{2s} \, z^{2(D\pi-3s-1)} + \cdots \\ &\quad -4z^3(D\pi-3s)(D\pi-3s-1)\kappa_s^2 \, g_3^{2s} \, z^{2(D\pi-3s)-2} + \cdots \\ &\quad -6z^2(D\pi-3s)\kappa_s^2 \, g_3^{2s} \, z^{2(D\pi-3s)-1} + \cdots \pmod \pi, \text{ all } z \\ &\equiv -2(D\pi-3s)\kappa_s^2 \, g_3^{2s} \, z^{2(D\pi-3s)+1} + \cdots \pmod \pi, \text{ all } z, \end{aligned}$$

where all the terms omitted contain lower powers of z. When $N\pi = p \equiv 1 \pmod 3$, $(\pi, \bar{\pi}) = 1$ by lemma 7, page 31. And when $p \equiv 1 \pmod 6$, $D\pi = \frac{1}{2}(p-1)$ so that $(D\pi - 3s, \pi) = 1$

if $0 \leq s < \frac{1}{3}D\pi$. Hence $\kappa_s \equiv 0 \pmod{\pi}$ if $0 \leq s < \frac{1}{3}D\pi$.

Theorem 9. If $\mathfrak{p} = (\pi)$ is regular and $N\pi = p$, an odd rational prime, then $\alpha = \pi\epsilon$ if and only if $g_3 \equiv 0 \pmod{\mathfrak{p}}$.

Proof. Immediate from lemmas 2 and 3.

The notation

$$P_\mu(z) = P_\mu(z, g_3)$$

will be used to indicate that g_3 is a rational integer, but that z is an indeterminate.

By theorem 5,

$$Q_\mu(z) = \prod_{(\delta)|(\mu)} P_{\mu/\delta}(z)^{M(\delta)}$$

(here (δ) runs through the divisors of (μ), and $M(\delta)$ is the Möbius function for the ideals of E) is a polynomial in z over E. By the inversion formula of Dedekind,

$$P_\mu(z) = \prod_{(\delta)|(\mu)} Q_\delta(z)$$

up to a unit factor in E. In particular, if (μ) is a prime ideal,

$$Q_\mu(z) = P_\mu(z).$$

Since $\sigma(u) = 0$ if and only if $u = 2\nu\omega_1$, ν in E, the roots of $Q_\mu(z) = 0$ are

$$z_\nu = \wp\left(\frac{2\nu\omega_1}{\mu}\right), \quad (\nu, \mu) = 1.$$

And since $\wp(u)$ is even and of order two,

$$\wp\left(\frac{2\nu_1\omega_1}{\mu}\right) = \wp\left(\frac{2\nu_2\omega_1}{\mu}\right) \quad \text{if and only if } \nu_1^2 \equiv \nu_2^2 \pmod{\mu}.$$

If $\mathfrak{p}$ are distinct prime ideals of E and

$$(\mu) = \prod \mathfrak{p}^a,$$

then the degree of $Q_\mu(z)$ is $\frac{1}{2}\Phi(\mu)$, where $\Phi(\mu)$ is the

Euler ϕ-function for the ring E:

$$\Phi(\mu) = \prod_{\eta|(\mu)} N\eta^{a-1}(N\eta - 1).$$

Let R be the field of rational numbers; and let G_μ be the galois group of $Q_\mu(z) = 0$ over $R(\rho)$, its coefficient field.

Theorem 10. G_μ is transitive and abelian.

Proof. Let S_κ be the substitution

$$z_{\kappa\nu} = S_\kappa z_\nu .$$

For any two ν_1, ν_2 in E, $(\nu_1, \mu) = (\nu_2, \mu) = 1$, there exists an S_κ, $(\kappa, \mu) = 1$, so that

$$z_{\nu_1} = S_\kappa z_{\nu_2}$$

because the congruence

$$\kappa\nu_2 \equiv \nu_1 \pmod{\mu}$$

has a unique solution κ prime to μ. Hence the group is transitive. Since

$$S_{\nu_1} S_{\nu_2} z_\nu = S_{\nu_1} z_{\nu_2\nu} = z_{\nu_1\nu_2\nu} = S_{\nu_2} S_{\nu_1} z_\nu = S_{\nu_1\nu_2} z_\nu ,$$

the group is abelian; and, indeed, it may be represented by the multiplicative group of the quadratic residues of μ, for $S_{\nu_1} = S_{\nu_2}$ implies $z_{\nu_1} = z_{\nu_2}$ or $\nu_1^2 \equiv \nu_2^2 \pmod{\mu}$.

Theorem 11. If α is a rank of apparition of $\mathfrak{p}$, then $Q_\alpha(z)$ and $P_\alpha(z)$ split into linear factors in $E/\mathfrak{p}$.

Proof. By the definition of α,

$$P_\alpha(z, g_3) \equiv 0 \pmod{\mathfrak{p}}$$

but

$$P_\delta(z, g_3) \not\equiv 0 \pmod{\mathfrak{p}},$$

for the same rational integers z and g_3, when $N\delta < N\alpha$.

Hence if

$$P_\alpha(z_0) = \prod_{(\delta)|(\alpha)} Q_\delta(z_0) \equiv 0 \pmod{\mathfrak{p}},$$

z_0 a rational integer, then

$$Q_\alpha(z_0) \equiv 0 \pmod{\mathfrak{p}};$$

for, otherwise,

$$Q_\delta(z_0) \equiv 0 \pmod{\mathfrak{p}}, \quad N\delta < N\alpha,$$

and

$$P_\delta(z_0) \equiv 0 \pmod{\mathfrak{p}}, \quad N\delta < N\alpha.$$

But, since

$$Q_\alpha(z_0) \equiv 0 \pmod{\mathfrak{p}},$$

z_0 lies in $E/\mathfrak{p}$. Let

$$z_0 = \wp\left(\frac{2\kappa\omega_1}{\alpha}\right), \quad (\kappa, \alpha) = 1.$$

Since $(\kappa, \alpha) = 1$, the congruence

$$\nu\kappa \equiv \lambda \pmod{\alpha}$$

has solutions ν for any λ in E. When $\lambda \not\equiv 0 \pmod{\alpha}$ ν may be taken so that $0 < N\nu < N\alpha$. Hence

$$\wp\left(\frac{2\lambda\omega_1}{\alpha}\right) = \wp\left(\frac{2\kappa\omega_1}{\alpha}\right) - \frac{\psi_{\nu-1}\left(\frac{2\kappa\omega_1}{\alpha}\right)\psi_{\nu+1}\left(\frac{2\kappa\omega_1}{\alpha}\right)}{\psi_\nu\left(\frac{2\kappa\omega_1}{\alpha}\right)^2},$$

$\lambda \not\equiv 0 \pmod{\alpha}$, all lie in $E/\mathfrak{p}$, since the denominator is not divisible by $\mathfrak{p}$. Therefore $Q_\alpha(z)$ and $P_\alpha(z)$ split into linear factors in $E/\mathfrak{p}$.

Let F_μ be the root field of $Q_\mu(z) = 0$, and let $C_n(x) = 0$ be the equation, irreducible over R, satisfied by the primitive n-th roots of unity. If $n \neq 3$, $C_n(x)$ is irreducible over $R(\rho)$.

Lemma 4. If $C_n(x)$ splits in F_μ, it splits into factors of equal degree.

Proof. Suppose

$$C_n(x) = f(x)g(x)h(x) \ldots$$

is the decomposition of $C_n(x)$ into irreducible factors in F_μ. Let H_μ be the subgroup of G_μ which leaves $f(x)$ fixed, and let

$$f_1(x), \quad f_2(x), \quad \ldots, \quad f_k(x)$$

be the values of

$$Sf(x) , \qquad S \text{ in } G_\mu / H_\mu .$$

Then

$$C_n(x) = f_1(x)\, f_2(x) \ldots f_k(x) ,$$

where all of the $f_i(x)$ have the same degree

$$d = \frac{\phi(n)}{k} .$$

Lemma 5. If n is an odd rational integer, then $C_n(x)$ splits into at least two factors in F_n.

Proof. The abelian relations assert that if n is an odd rational integer, then

$$\sum_{s=0}^{n-1} \theta^{2rs} \frac{1}{\wp'\left(\frac{2\omega_1}{n}(r+s\rho)\right)} = 0$$

$$\sum_{s=0}^{n-1} \theta^{2rs} \frac{\wp\left(\frac{2\omega_1}{n}(r+s\rho)\right)}{\wp'\left(\frac{2\omega_1}{n}(r+s\rho)\right)} = 0 ,$$

where $\theta = \exp(2\pi i/n)$ and $r = 0,1,\ldots,n-1$ [VII, vol. 2, p. 242]. Since $\wp'(u)$ is odd and $\wp(u)$ even, the equations for $r = 0$ are trivial and the equations for $n-r$ merely duplicate those for r. Consequently, r may be restricted to the range $1, 2, \ldots, \frac{1}{2}(n-1)$. Now, differentiating

$$\wp(\mu u) = \wp(u) - \frac{\psi_{\mu-1}(u)\, \psi_{\mu+1}(u)}{\psi_\mu(u)^2} = A_\mu\left(\wp(u)\right),$$

which expresses $\wp(\mu u)$ as a rational function of $\wp(u)$, shows that

$$\frac{\wp'\left(\frac{2\mu\omega_1}{n}\right)}{\wp'\left(\frac{2\omega_1}{n}\right)} = \mu^{-1} A_\mu'\left(\wp\left(\frac{2\omega_1}{n}\right)\right)$$

is in F_n. Therefore, if d is any divisor of n, removing a factor $\wp'\left(\frac{2\omega_1}{n}\right)$ from each of the equations

$$\sum_{s=0}^{d-1} \theta^{2rsd'} \frac{1}{\wp'\left(\frac{2\omega_1}{d}\ (r+s\rho)\right)} = 0$$

$$\sum_{s=0}^{d-1} \theta^{2rsd'} \frac{\wp\left(\frac{2\omega_1}{d}\ (r+s\rho)\right)}{\wp'\left(\frac{2\omega_1}{d}\ (r+s\rho)\right)} = 0$$

where $\theta = \exp(2\pi i/n)$

$r = 1,2,\ldots,\frac{1}{2}(d-1)$

$n = dd'$,

yields a set of polynomials over F_n satisfied by θ. There are $\frac{1}{2}\sum_{d/n}(d-1)$ pair of equations, each of degree at most $n-1$. Now $d > \phi(d)$ if $d>1$ and $n = \sum_{d/n} \phi(d)$, hence if $n>1$,

$$\sum_{d/n}^{d<n} d \geqslant \sum_{d/n}^{d<n} \phi(d) \quad \text{and} \quad n > \sum_{d/n}^{d<n} \phi(d)\ ;$$

adding,

$$\sum_{d/n} d > 2\sum_{d/n}^{d<n} \phi(d) = 2\left(n-\phi(n)\right) \geqslant n-\phi(n)+\sum_{d/n}^{d>1} 1 = n-1-\phi(n)+\sum_{d/n} 1,$$

for $n-\phi(n) \geqslant \sum_{d/n}^{d>1} 1$, so

$$\phi(n)+\sum_{d/n}(d-1) > n-1\ .$$

Therefore systematic elimination of the highest powers of θ leads to an equation over F_n, of degree less than $\phi(n)$, satisfied by θ.

Lemma 6. If α is a rank of apparition of $\mathfrak{P}$, then $\overline{\alpha}$ is a rank of apparition of $\overline{\mathfrak{P}}$.

Proof. This lemma is an immediate consequence of the relation

$$P_{\overline{\mu}}(z,g_3) = \overline{P_{\mu}(z,g_3)},$$

which follows from theorem 2 by an induction on $N\mu$.

Lemma 7. If $\alpha = \overline{\alpha}\epsilon_1$, then $\alpha = a\epsilon$ or $\alpha = a(1-\rho)\epsilon$, where a is a rational integer.

Proof. If $a+b\rho = \rho(a+b\rho^2) = a\rho + b$,

then $a+b\rho = a(1+\rho)$;

and if $a+b\rho = -\rho(a+b\rho^2) = -a\rho - b$,

then $a+b\rho = a(1-\rho)$.

The four remaining cases are omitted since these two are typical.

Theorem 12. If $p \equiv 2 \pmod 3$, α is a rank of apparition of p, and $\alpha \not\equiv 0 \pmod p$, then

$$\alpha = 2^c b\epsilon \quad \text{or} \quad \alpha = 2^c b(1-\rho)\epsilon,$$

where b is 1, 3, or an odd divisor of $p^e - 1$ and c and e are rational integers, $c \geqslant 0$ and $e < \phi(b)$.

Proof. If $p \equiv 2 \pmod 3$, then (p) is a prime ideal of E, say $\mathfrak{P}$ [VI, p. 221]. Since p is rational, $\overline{\mathfrak{P}} = \mathfrak{P}$, and so $\alpha = \overline{\alpha}\epsilon_1$, by lemma 6. And by lemma 7, either

$$\alpha = a\epsilon \quad \text{or} \quad \alpha = a(1-\rho)\epsilon.$$

Suppose $a = 2^c b$, b odd. Since $b \mid \alpha$,

$$F_\alpha \supseteq F_b \supseteq R(\rho), \quad \text{if} \quad b > 1.$$

By lemma 5, $C_b(x)$ definitely splits into two or more factors in F_b, and by theorem 11

$$F_\alpha/p = F_\beta/p = E/p \ ;$$

therefore $C_\beta(x)$ splits in E/p. Hence, if $b \neq 3$, then $p^e \equiv 1 \pmod{b}$, where e is the common degree of the irreducible factors of $C_\beta(x)$ in E/p.

If $p \equiv 1 \pmod{3}$, then $p = N\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of E [VI, p. 221]. In this case the apparition problem is an open question.

SECTION FOUR

Numerical Periodicity Modulo Prime Ideals

Let $\mathfrak{p}$ be a regular prime ideal of E. This section contains a study of the periodicity modulo $\mathfrak{p}$ of the divisibility mapping $\mu \to P(z, g_3)$, z and g_3 in E.

Lemma 8. If $\psi_\mu(u) = \psi_{\mu+\delta}(u) = 0$ and $N\delta \neq 1$, then $\psi_\delta(u) = 0$.

Proof. If $\delta = 0$, there is nothing to prove. If $N\delta = 1$, then $\psi_\delta(u) = \delta$ is never zero. Suppose $N\delta > 1$. Since $u = 2\nu\omega_1$, ν in E, is a pole of $\psi_\mu(u)$ and

$$u = \frac{2\nu\omega_1}{\mu}, \qquad \mu \nmid \nu$$

are the zeros of $\psi_\mu(u)$, the hypotheses imply

$$\mu u = 2\nu_1\omega_1, \quad \mu \nmid \nu_1,$$

$$(\mu+\delta)u = 2\nu_2\omega_1, \quad \mu+\delta \nmid \nu_2.$$

But $N\delta > 0$ implies $\nu_2 \neq \nu_1$, so

$$\delta u = 2(\nu_2 - \nu_1)\omega_1 \neq 0.$$

Furthermore $\delta \nmid \nu_2 - \nu_1$, for otherwise u would be a pole of $\psi_\mu(u)$. (In particular, this excludes the case $N\delta = 1$.) Hence $\psi_\delta(u) = 0$.

Theorem 13. If $\mathfrak{p}$ is a regular prime ideal, then the zeros of $\mathfrak{p}$ form an ideal $\mathfrak{o}$ of E. If α is a rank of apparition of $\mathfrak{p}$, then $\mathfrak{o} = (\alpha)$.

Proof. First $\psi_\mu(u) \equiv 0 \pmod{\mathfrak{p}}$ implies $\psi_{\mu\nu}(u) \equiv 0 \pmod{\mathfrak{p}}$ by theorem 5. If

$$\psi_\mu(u) \equiv \psi_\nu(u) \equiv 0 \pmod{\mathfrak{p}}$$

then (from the recursion)

$$\psi_{\mu+\nu}(u)\,\psi_{\mu-\nu}(u) \equiv 0 \pmod{\mathfrak{p}}.$$

Replacing μ and ν in the recursion by $\mu+\nu$ and $\mu-\nu$, respectively, gives

$$\epsilon^2 \psi_{2\mu}\,\psi_{2\nu} = \psi_{\mu+\nu+\epsilon}\,\psi_{\mu+\nu-\epsilon}\,\psi_{\mu-\nu}^2 - \psi_{\mu-\nu+\epsilon}\,\psi_{\mu-\nu-\epsilon}\,\psi_{\mu+\nu}^2.$$

Consequently, if $\psi_{\mu-\nu}(u) \not\equiv 0 \pmod{\mathfrak{p}}$, then $\psi_{\mu+\nu} \equiv 0$,

$$\psi_{\mu+\nu+\epsilon}\,\psi_{\mu+\nu-\epsilon} \equiv 0 \pmod{\mathfrak{p}}$$

for all ϵ, $N\epsilon = 1$. But the norm of a sum or difference of two units is 1 or 3, hence by the lemma $\psi_\delta(u) \equiv 0 \pmod{\mathfrak{p}}$, $N\delta = 3$, contradicting the hypothesis on $\mathfrak{p}$. Therefore $\psi_{\mu-\nu}(u) \equiv 0 \pmod{\mathfrak{p}}$ and the zeros of $\mathfrak{p}$ form an ideal. The ideal $\mathfrak{a}$ is non-void by an argument similar to the proof of theorem 5.1 of Ward's Memoir [III]. Since E is a principal ideal ring $\mathfrak{a} = (\alpha)$, where α is a rank of apparition of $\mathfrak{p}$.

An integer δ of E is called a period of $\mathfrak{p}$ if

$$\psi_{\mu+\delta}(u) \equiv \psi_\mu(u) \pmod{\mathfrak{p}}, \quad N\delta > 0,$$

for all μ in E. The existence of periods follows from the conditions stated in lemma 11.

Lemma 9. The periods of $\mathfrak{p}$ form a module $\mathfrak{M}$ which is contained in $\mathfrak{a}$.

Proof. If

$$\psi_{\mu+\delta}(u) \equiv \psi_\mu(u) \pmod{\mathfrak{p}}, \quad \text{all } \mu \text{ in E}$$

then

$$\psi_{\mu-\delta}(u) \equiv \psi_\mu(u) \pmod{\mathfrak{p}}, \quad \text{all } \mu \text{ in E}$$

since $\psi_\mu(u)$ is an odd function of μ. Furthermore if

$$\psi_{\mu+\delta_1}(u) \equiv \psi_{\mu+\delta_2}(u) \equiv \psi_\mu(u) \pmod{\wp},$$ all μ in E

then $\psi_{\mu+\delta_1+\delta_2}(u) \equiv \psi_{\mu+\delta_1}(u) \equiv \psi_\mu(u) \pmod{\wp}$, all μ in E. Taking $\mu = 0$,

$$\psi_\delta(u) \equiv \psi_0(u) \equiv 0 \pmod{\wp}$$

so δ is in $\mathfrak{a}$. Since $\mathfrak{a} = (\alpha)$, there exists an integer β in E so that $\delta = \alpha\beta$.

Lemma 10. If $\mu = m+n\rho$ and $\beta = b+c\rho$, there exist integers κ_1, κ_2, κ_3, κ_4 in E so that

$$\psi_{\mu+\alpha\beta}(u) \equiv \kappa_1^{N\beta} (\kappa_2^b \kappa_3^c)^m (\kappa_2^c \kappa_4^b)^n \psi_\mu(u) \pmod{\wp}$$

where α is a rank of apparition of $\wp$.

Proof. Since $\psi_\alpha(u) \equiv 0 \pmod{\wp}$,

$$\wp(u) \equiv \wp\left(\frac{2\nu\omega_1}{\alpha}\right) \pmod{\wp}$$

for some ν in E, and

$$\psi_\mu(u) \equiv \psi_\mu\left(\frac{2\nu\omega_1}{\alpha}\right) \pmod{\wp}$$

for any μ in E. In particular

$$\psi_{\mu+\alpha\beta}(u) \equiv \psi_{\mu+\alpha\beta}\left(\frac{2\nu\omega_1}{\alpha}\right) \pmod{\wp}.$$

But

$$\psi_{\mu+\alpha\beta}\left(\frac{2\nu\omega_1}{\alpha}\right) = \frac{\sigma\left(\frac{2\mu\nu\omega_1}{\alpha} + 2\beta\nu\omega_1\right)}{\sigma\left(\frac{2\nu\omega_1}{\alpha}\right)^{N(\mu+\alpha\beta)}}$$

$$= \frac{(-1)^{N(\beta\nu)}\, e^{2\beta\overline{\nu}\,\eta_1\left(\frac{2\mu\nu\omega_1}{\alpha} + \beta\nu\omega_1\right)}\, \sigma\left(\frac{2\mu\nu\omega_1}{\alpha}\right)}{\sigma\left(\frac{2\nu\omega_1}{\alpha}\right)^{N\mu + \mu\overline{\alpha\beta} + \overline{\mu}\alpha\beta + N(\alpha\beta)}}$$

$$= \frac{(-1)^{N(\beta\nu)}\, e^{2\eta_1\omega_1 N(\beta\nu)}\, e^{\mu\bar{\beta}\frac{4\eta_1\omega_1 N\nu}{\alpha}}}{\sigma\left(\frac{2\nu\omega_1}{\alpha}\right)^{N(\alpha\beta)} \quad \sigma\left(\frac{2\nu\omega_1}{\alpha}\right)^{\mu\bar{\beta}\bar{\alpha}+\bar{\mu}\beta\alpha}} \psi_\mu\left(\frac{2\nu\omega_1}{\alpha}\right)$$

$$= K_1^{N\beta}\, K_5^{\mu\bar{\beta}}\, K_6^{\bar{\mu}\beta}\, \psi_\mu\left(\frac{2\nu\omega_1}{\alpha}\right) ,$$

where $K_1 = (-1)^{N\nu}\, e^{2\eta_1\omega_1 N\nu}\, \sigma\left(\frac{2\nu\omega_1}{\alpha}\right)^{-N\alpha}$

$$K_5 = e^{\frac{4\eta_1\omega_1 N\nu}{\alpha}}\, \sigma\left(\frac{2\nu\omega_1}{\alpha}\right)^{-\bar{\alpha}}$$

$$K_6 = \sigma\left(\frac{2\nu\omega_1}{\alpha}\right)^{-\alpha}$$

are all independent of μ and β. If

$$M = mb - mc + nc , \quad L = nb - mc ,$$

then $\mu\bar{\beta} = M + \rho L$ and

$$K_5^{\mu\bar{\beta}}\, K_6^{\bar{\mu}\beta} = K_5^{M+\rho L}\, K_6^{M+\rho^2 L} = K_2^{M}\, K_4^{L} = K_2^{mb-mc+nc}\, K_4^{nb-mc}$$

$$= K_2^{mb+nc} K_3^{mc} K_4^{nb} = (K_2^{b} K_3^{c})^{m} (K_2^{c} K_4^{b})^{n}$$

where $K_2 = K_5 K_6$, $K_4 = K_5^{\rho} K_6^{\rho^2}$, and $K_3 = K_2^{-1} K_4^{-1}$.

Hence

$$\psi_{\mu+\alpha\beta}(u) \equiv K_1^{N\beta} (K_2^{b} K_3^{c})^{m} (K_2^{c} K_4^{b})^{n} \psi_\mu(u) \pmod{\wp}.$$

Taking

$$\mu = \beta = 1$$
$$\mu = 1, \quad \beta = 1 + \rho$$
$$\mu = 1, \quad \beta = \rho$$
$$\mu = \rho, \quad \beta = 1$$

gives, respectively,

$$\begin{aligned} \psi_{\alpha+1} &\equiv K_1 K_2 \\ \psi_{(1+\rho)\alpha+1} &\equiv K_1 K_2 K_3 \\ \psi_{\rho\alpha+1} &\equiv K_1 K_3 \\ \psi_{\alpha+\rho} &\equiv \rho K_1 K_4 \end{aligned} \pmod{\wp}$$

Hence $\kappa_1\kappa_2$, $\kappa_1\kappa_2\kappa_3$, $\kappa_1\kappa_3$, $\kappa_1\kappa_4$ are congruent modulo $\mathfrak{p}$ to integers of E. Therefore, so are κ_1 , κ_2 , κ_3 , κ_4.

Lemma 11. The conditions

$$\kappa_1^{N\beta} \equiv \kappa_2^{b}\kappa_3^{c} \equiv \kappa_2^{c}\kappa_4^{b} \equiv \kappa_3^{b}\kappa_4^{c} \equiv 1 \pmod{\mathfrak{p}}$$

are necessary and sufficient for

$$\psi_{\mu+\alpha\beta}(u) \equiv \psi_{\mu}(u) \pmod{\mathfrak{p}}, \quad \text{all } \mu \text{ in E.}$$

Proof. The sufficiency is evident. And so is the necessity, for if

$$\psi_{\mu+\alpha\beta}(u) \equiv \psi_{\mu}(u) \pmod{\mathfrak{p}}, \quad \text{all } \mu \text{ in E}$$

then $$\kappa_1^{N\beta}\,(\,\kappa_2^{b}\kappa_3^{c}\,)^{m}\,(\,\kappa_2^{c}\kappa_4^{b}\,)^{n} \equiv 1 \pmod{\mathfrak{p}}$$

for all m, n. In particular

$$(m = n = 1) \qquad \kappa_1^{N\beta}\kappa_2^{b}\kappa_3^{c}\kappa_2^{c}\kappa_4^{b} \equiv 1 \pmod{\mathfrak{p}}$$

$$(m = 1,\ n = 0) \qquad \kappa_1^{N\beta}\kappa_2^{b}\kappa_3^{c} \equiv 1 \pmod{\mathfrak{p}}$$

$$(m = 0,\ n = 1) \qquad \kappa_1^{N\beta}\kappa_2^{c}\kappa_4^{b} \equiv 1 \pmod{\mathfrak{p}}.$$

Hence $$\kappa_1^{N\beta} \equiv \kappa_2^{b}\kappa_3^{c} \equiv \kappa_2^{c}\kappa_4^{b} \equiv 1 \pmod{\mathfrak{p}}.$$

But $$\kappa_2\kappa_3\kappa_4 = 1$$

so $$\kappa_3^{c} \equiv \kappa_3^{b}\kappa_4^{b}\ , \qquad \kappa_4^{b} \equiv \kappa_3^{c}\kappa_4^{c} \pmod{\mathfrak{p}}$$

or $$\kappa_3^{b} \equiv \kappa_3^{c}\kappa_4^{-b}\ , \qquad \kappa_4^{c} \equiv \kappa_3^{-c}\kappa_4^{b} \pmod{\mathfrak{p}}$$

and $$\kappa_3^{b}\kappa_4^{c} \equiv 1 \pmod{\mathfrak{p}}.$$

Theorem 14. If $\alpha\beta$ is a period of $\mathfrak{p}$ and γ is any integer of E, then $\alpha\beta\gamma$ is a period of $\mathfrak{p}$. That is, the module $\mathfrak{m}$ is an ideal of E.

Proof. If $\beta = b + c\rho$ and $\gamma = d + f\rho$, then

$$\beta\gamma = bd - cf + (dc + bf - cf)\rho$$

and

$$\psi_{\mu+\alpha\beta}(u) \equiv \kappa_1^{N(\beta\gamma)} \left(\kappa_2^{bd-cf} \kappa_3^{dc+bf-cf}\right)^m \cdot \left(\kappa_2^{dc+bf-cf} \kappa_4^{bd-cf}\right)^n \psi_\mu(u)$$

$$\equiv \kappa_1^{N(\beta\gamma)} \left(\kappa_2^{b} \kappa_3^{c}\right)^{dm} \left(\kappa_4^{c} \kappa_3^{b}\right)^{fm} \cdot \left(\kappa_2^{c} \kappa_4^{b}\right)^{dm} \left(\kappa_3^{c} \kappa_2^{b}\right)^{fm} \psi_\mu(u)$$

$$\equiv \psi_\mu(u) \pmod{\mathfrak{p}}$$

since $\kappa_2 \kappa_3 \kappa_4 = 1$ and

$$\kappa_1^{N\beta} \equiv \kappa_2^{b}\kappa_3^{c} \equiv \kappa_2^{c}\kappa_4^{b} \equiv \kappa_3^{b}\kappa_4^{c} \equiv 1 \pmod{\mathfrak{p}}.$$

This theorem states that, modulo regular prime ideals, equianharmonic divisibility mappings are doubly periodic in the same sense that $\wp(u, \omega_1, \rho\omega_1)$ is doubly periodic. The function $\wp(u)$ has the fundamental period $2\omega_1$, every other period of $\wp(u)$ is a multiple $2\mu\omega_1$, any μ in E, of $2\omega_1$. Modulo $\mathfrak{p}$, $\psi_\mu(u)$ has a fundamental period $\alpha\beta$, where $\mathfrak{m} = (\alpha\beta)$, and every other period of $\psi_\mu(u)$ modulo $\mathfrak{p}$ is a multiple $\alpha\beta\gamma$, any γ in E, of $\alpha\beta$.

REFERENCES

I E. Lucas, Théorie des fonctions numériques simplement périodiques, American Journal of Mathematics, volume 1 (1878), pp. 184-240, 289-321.

II E. T. Bell, Analogies between the u_n, v_n of Lucas and elliptic functions, Bulletin of the American Mathematical Society, volume 29 (1923), pp. 401-406.

III Morgan Ward, Memoir on elliptic divisibility sequences, American Journal of Mathematics, volume 70 (1948), pp. 31-74.

IV Morgan Ward, Arithmetical properties of polynomials associated with the lemniscate elliptic functions, Proceedings of the National Academy of Sciences, volume 36 (1950), pp. 359-362.

V J. Tannery and J. Molk, Éléments de la théorie des fonctions elliptiques, Paris, 1893-1902.

VI G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Second edition, Oxford, 1945.

VII R. Fricke, Die elliptischen Funktionen und ihre Anwendungen, Leipzig and Berlin, 1916-1922.

VIII G. Eisenstein, Mathematische Abhandlungen, Berlin, 1847.