THE APPARITION PROBLEM FOR EQUIANHARMONIC DIVISIBILITY SEQUENCES

By L. K. Durst

The Rice Institute, Houston

Communicated by E. T. Bell, February 27, 1952

The apparition problem consists in finding an arithmetical relation between a rational prime p and its rank of apparition in an elliptic divisibility sequence.[1] In this report the elliptic divisibility sequences parameterized by equianharmonic functions are investigated, and a partial answer to the apparition problem for such sequences is given (Theorem 2).

If $\omega_2/\omega_1 = \rho = {}^1/_2(-1 + \sqrt{-3})$, the Weierstrass functions for the parallelogram 0, $2\omega_1$ $2\omega_2$, $2\omega_1 + 2\omega_2$ are called equianharmonic functions and have the following expansions:

$$
\begin{aligned}
\sigma(u) &= u \prod_{\mu \text{ in } E}^{\mu \neq 0} \left\{\left(1 - \frac{u}{2\mu\omega_1}\right) \exp\left(\frac{u}{2\mu\omega_1} + \frac{1}{2}\frac{u^2}{(2\mu\omega_1)^2}\right)\right\} \\
\zeta(u) &= \frac{1}{u} + \sum_{\mu \text{ in } E}^{\mu \neq 0} \left\{\frac{1}{u - 2\mu\omega_1} + \frac{1}{2\mu\omega_1} + \frac{u}{(2\mu\omega_1)^2}\right\} \\
\wp(u) &= \frac{1}{u^2} + \sum_{\mu \text{ in } E}^{\mu \neq 0} \left\{\frac{1}{(u - 2\mu\omega_1)^2} - \frac{1}{(2\mu\omega_1)^2}\right\} \\
\wp'(u) &= -2 \sum_{\mu \text{ in } E} \frac{1}{(u - 2\mu\omega_1)^3}
\end{aligned}
\tag{1}
$$

where the index μ runs through the ring E of the quadratic integers $\mu = a + b\rho$, a and b rational integers. The norm in E is given by $N\mu = N(a + b\rho) = a^2 - ab + b^2$, and the units in E are $\epsilon = \pm 1, \pm\rho, \pm\rho^2 = \mp(1 + \rho)$. Equations (1) imply

$$
\begin{aligned}
\sigma(\epsilon u, \omega_1, \rho\omega_1) &= \epsilon\, \sigma(u, \omega_1, \rho\omega_1) \\
\zeta(\epsilon u, \omega_1, \rho\omega_1) &= \epsilon^{-1}\zeta(u, \omega_1, \rho\omega_1) \\
\wp(\epsilon u, \omega_1, \rho\omega_1) &= \epsilon^{-2}\wp(u, \omega_1, \rho\omega_1) \\
\wp'(\epsilon u, \omega_1, \rho\omega_1) &= \epsilon^{-3}\wp'(u, \omega_1, \rho\omega_1)
\end{aligned}
\tag{2}
$$

where $N\epsilon = 1$. The function $\sigma(u)$ is a doubly periodic function of the third kind:

$$\sigma(u + 2\mu\omega_1) = (-1)^{N\mu}\, e^{2\bar{\mu}\eta_1(u + \mu\omega_1)}\, \sigma(u), \mu \text{ in } E, \tag{3}$$

$\bar{\mu}$ being the conjugate at μ, and $\eta_1 = \zeta(\omega_1)$. Furthermore (2) implies $g_2 = 0$ and hence

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

Equianharmonic functions afford one of the simpler examples of elliptic functions admitting complex multiplication.[2]

If $\psi_\mu(u) = \sigma(\mu u, \omega_1, \rho\omega_1)\, \sigma(u, \omega_1, \rho\omega_1)^{-N\mu}$, for μ in E, then (1) and (3) imply that $\psi_\mu(u)$ is an elliptic function of u with periods $2\omega_1$ and $2\rho\omega_1$. The three-term sigma formula[3] implies

$$\epsilon^2\psi_{\mu+\nu}(u)\psi_{\mu-\nu}(u) = \psi_{\mu+\epsilon}(u)\psi_{\mu-\epsilon}(u)\psi_\nu^2(u) - \psi_{\nu+\epsilon}(u)\psi_{\nu-\epsilon}(u)\psi_\mu^2(u), \tag{4}$$

for any μ, ν, ϵ in E, provided $N\epsilon = 1$.

1°. Using $\psi_{\epsilon\mu}(u) = \epsilon\psi_\mu(u)$, $N\epsilon = 1$, and the recursion (4), every value of $\psi_\mu(u)$ may be computed from the initial values

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

2°. If $N\mu$ is an odd rational integer,

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

and if $N\mu$ is even,

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

where $z = \wp(u)$ and $P_\mu(z, g_3)$ is a polynomial in z over the polynomial ring $E[g_3]$ of degree $^1/_2(N\mu - 1)$ if $N\mu$ odd, and $^1/_2(N\mu - 4)$ if $N\mu$ even.

Proofs of 1° and 2° may be given by inductions on $N\mu$.

3°. If $\nu|\mu$ in the ring E, then $P_\nu(z, g_3)\,|\,P_\mu(z, g_3)$ in the ring $E[z, g_3]$.

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

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

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

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

But

$$\wp(\nu u) = \wp(u) - \psi_{\nu-1}(u)\psi_{\nu+1}(u)\psi_\nu(u)^{-2}, \tag{5}$$

so $P_\lambda(\wp(\nu u), g_3)P_\nu(z, g_3)^{N\lambda - 1}$ is a polynomial in $E[z, g_3]$. The details of the proof of 3° are similar if one or both of $N\lambda$, $N\nu$ are even.

If z and g_3 are fixed in the ring I of rational integers, then the correspondence $\mu \to P_\mu(z, g_3)$ is a mapping of E into itself preserving division. Let $\mathfrak{p}$ be a prime ideal of E. An integer λ of E will be called a *zero* of $\mathfrak{p}$ if

$$P_\lambda(z, g_3) \equiv 0 \pmod{\mathfrak{p}}, \qquad z,\ g_3 \text{ fixed in } I.$$

A zero α of $\mathfrak{p}$ with minimum positive norm will be called a *rank of apparition* of $\mathfrak{p}$. That every $\mathfrak{p}$ of E has a rank of apparition for each z, g_3 of I, may be shown by an argument similar to the proof of Theorem 5.1 of Ward's Memoir.[1]

Write $P_\mu(z) = P_\mu(z, g_3)$ for g_3 fixed in I. If $M(\delta)$ is the Möbius function of the principal ideal ring E, defined by

$$\begin{aligned} M(\epsilon) &= 1 \text{ if } N\epsilon = 1 \\ M(\delta) &= (-1)^r \text{ if } (\delta) \text{ is a product of } r \text{ distinct prime ideals} \\ M(\delta) &= 0 \text{ if } (\delta) \text{ is divisible by the square of a prime ideal,} \end{aligned}$$

then

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

is in $E[z]$; and by the inversion formula of Dedekind,

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

up to a unit factor in E. Since $\sigma(u) = 0$ if and only if $u = 2\nu\omega_1$, ν in E, the roots of $Q_\mu(z) = 0$ are the distinct values of $\wp(2\nu\omega_1/\mu)$, $(\nu, \mu) = 1$.

4°. If α is a rank of apparition of $\mathfrak{p}$, then $Q_\alpha(z)$ and $P_\alpha(z)$ split into linear factors in $E/\mathfrak{p}$.

4° follows from (5).

Let R be the field of rationals and let F_μ be the root field of $Q_\mu(z)$. If $\nu|\mu$, $N\nu > 1$, then $F_\mu \supseteq F_\nu \supseteq R(\rho)$, unless $N\nu = 4$. Let $C_n(x) = 0$ be the equation, irreducible over R, satisfied by the primitive nth roots of unity. If $n \neq 3$, $C_n(x)$ is irreducible over $R(\rho)$.

THEOREM 1. *If n is an odd rational integer, then $C_n(x)$ is reducible in F_n.*

For if $\theta = \exp(2\pi i/n)$ and $n = d\,d'$, then

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

$$\sum_{s=0}^{d-1} \theta^{2rsd'} \wp(2\omega_1(r + s\rho)/d)\wp'(2\omega_1(r + s\rho)/d)^{-1} = 0 \qquad (6)$$

where $r = 1, 2, \ldots, {}^1/_2(d - 1)$.[4] It follows from (5) that multiplication of equations (6) by $\wp'(2\omega_1/n)$ yields $\sum_{d|n} (d - 1)$ equations over F_n, of degree at most $n - 1$, each of which has θ as a root. Since

$$\phi(n) > n - 1 - \sum_{d|n} (d - 1),$$

$C_n(x)$ factors in F_n.

It is now possible to formulate an answer to the apparition problem for all rational primes that do not split in E.

THEOREM 2. *If $p \equiv 2 \pmod 3$ and α is a rank of apparition of p, then*

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

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

By hypothesis $(p) = \mathfrak{p}$, a prime ideal of E. But $\alpha = \bar{\alpha}\epsilon$ since $\mathfrak{p} = \bar{\mathfrak{p}}$, so that

$$\alpha = a \qquad \text{or} \qquad \alpha = a(1 - \rho),$$

where a is a rational integer. Let $a = 2^c b$, b odd. Since $b \mid \alpha$,

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

Hence by 4° and Theorem 1, $C_b(x)$ is reducible in E/p; and if $b \neq 3$, $p^e \equiv 1 \pmod b$, where e is the common degree of the irreducible factors of $C_b(x)$ in E/p.

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

[1] Ward, Morgan, "Memoir on Elliptic Divisibility Sequences," *Am. J. Math.*, **70**, 31–74 (1948).

[2] Ward, Morgan, "Arithmetical Properties of Polynomials Associated with the Lemniscate Elliptic Functions," PROC. NATL. ACAD. SCI., **36**, 359–362 (1950).

[3] For the three-term sigma formula, and all of the formulas of the previous paragraph, cf. Tannery and Molk, *Éléments de la théorie des fonctions elliptiques*, Vol. 2, pp. 234–236.

[4] For these "Abelian Relations," cf. Fricke, *Die elliptischen Funktionen und ihre Anwendungen*, Vol. 2, p. 242.

SOME THEOREMS ON PIECEWISE LINEAR EMBEDDING

BY V. K. A. M. GUGENHEIM

MAGDALEN COLLEGE, OXFORD

Communicated by S. Lefschetz, January 30, 1952

1. We call two (Euclidean) polyhedra equivalent if they have isomorphic simplicial subdivisions; the homeomorphism which maps each simplex of such a subdivision linearly onto its correlate in an isomorphic subdivision is called a piecewise linear homeomorphism onto, abbreviated *PLO*.

A polyhedron is called finite if it has a subdivision consisting of a finite number of simplices; a polyhedron equivalent to a q-simplex is called a q-element, one equivalent to the boundary of a q-simplex, a $(q - 1)$-sphere. A polyhedron for which the star of every vertex of a given subdivision is a q-element is called a q-manifold: but in what follows "q-manifold" will mean "connected q-manifold." If M^q is an orientable q-manifold, we denote by $\mathbf{M}^q$ the oriented manifold obtained by orienting