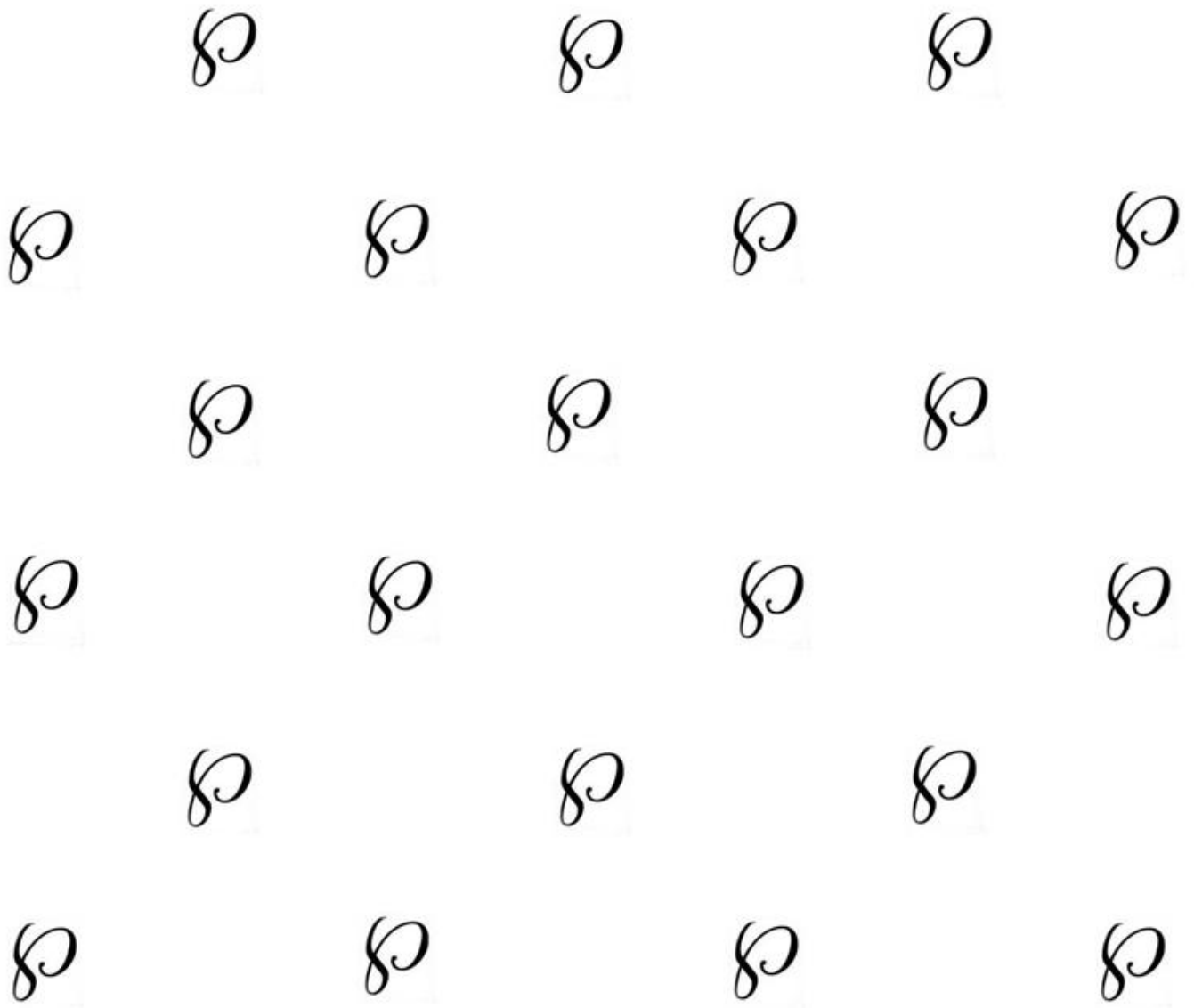
Elliptic divisibility sequences

Rutger de Looij

28 May 2010



Master's thesis, Mathematical Sciences, Universiteit Utrecht,
written under the supervision of prof. dr. Gunther Cornelissen

Καὶ μὴν ἀριθμὸν, ἔξοχον σοφισμάτων, ἐξηῦρον αὐτοῖς.
And I found number for them, chief devise of all.

(PROMETHEUS in Aischylos' *Prometheus bound*, v. 475)

Contents

List of notation

$m \mid n$	m divides n
$m^k \mid\mid n$	m^k is the exact power of m dividing n
(m,n)	the greatest common divisor of m and n
$[x]$	Floor(x), i.e. the greatest integer k such that $k \leqslant x$
Δ	discriminant of an elliptic sequence
g_2, g_3	modular invariants associated with the lattice L
L	a lattice in the complex plane
O	the unity element of the group of rational points of an elliptic curve
$\wp(z)$	the doubly periodic Weierstraß $\wp$-function associated with the lattice L
ρ	the smallest rank of apparition of a prime p
$\sigma(z)$	the Weierstraß sigma function associated with the lattice L
$\psi_n(z)$	the elliptic function $\sigma(nz)/\sigma(z)^{n^2}$
$\Psi_n(X,Y)$	the n-th division polynomial evaluated at the point (X,Y)
u	a complex constant
z	a complex variable
$\boxtimes$	end of a proof
$\lozenge$	end of a definition or example

Introduction

In 1948 Morgan Ward introduced the topic of elliptic divisibility sequences. An elliptic divisibility sequence (EDS) is a sequence of integers (h) satisfying the recursive relation

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \qquad m \geqslant n \geqslant 0,$$

and such that h_n divides h_m whenever n divides m. This recursive relation, that Ward imposed on rational integers, is the fundamental relation on which the multiplication theory of elliptic functions rests. The sequences that are of arithmetical interest turn out to be those in which $h_0 = 0$, $h_1 = 1$ and not both h_2 and h_3 vanish: the so-called *general* elliptic divisibility sequences.

This thesis is centered around Ward's article *Memoir on elliptic divisibility sequences*. In part I we will see that the recursive relation, which Ward took as a starting point, originates from a certain elliptic function. In part II we work out the details of Ward's article and touch on the connection between elliptic divisibility sequences and elliptic curves.

The main results of Ward's *Memoir* are as follows. A sequence (h) satisfying the recursive relation is an elliptic divisibility sequence if and only if $h_2,\ h_3,\ h_4$ are integers and h_2 divides h_4. Every such solution is uniquely determined by the initial values of $h_2,\ h_3$ and h_4 and may be parameterized by elliptic functions provided that h_2 and h_3 are not zero.[1] The invariants g_2 and g_3 of the associated Weierstraß $\wp$-function are rational functions of h_2, h_3 and h_4.

Furthermore, we define an equivalence relation $\sim$ on elliptic divisibility sequences and show that there are essentially four types – i.e. equivalence classes – of elliptic divisibility sequences. A rational solution of the recursive relation, which is called an *elliptic sequence*, is shown to be equivalent to an EDS.

A prime p is said to be a divisor of (h) if it divides some term h_k with $k > 0$. If p divides h_k but does not divide h_l when l divides k, then k is called a rank of apparition of p in (h). Every prime p which does not divide both h_3 and h_4 has precisely one rank of apparition ρ, and (h) is periodic modulo p with period $\rho\tau$ where τ is a certain arithmetical function of p and (h) which can be exactly determined. If we calculate the least positive residues modulo p of the succesive values $h_0,\ h_1,\ h_2, \ldots$ of a general EDS, the pattern of residues exhibits interesting symmetries.

[1] If h_2 or h_3 is zero, h_n is trivially a product of powers of $\pm h_3$ or $\pm h_2$ and h_4. This case is discussed in chapter 7.

Part I
Elliptic function theory

1 Prerequisites

In this chapter we state results from elliptic function theory we shall need throughout this thesis. They can be found in Lang [5], unless stated otherwise. We always assume L to be a lattice in the complex plane: $L = \{m_1\lambda_1 + m_2\lambda_2 : \ m_1, m_2 \in \mathbb{Z}\}$, where λ_1, λ_2 are complex numbers such that $\mathrm{Im}(\lambda_1/\lambda_2) \neq 0$.

Definition 1.1. The Weierstraß $\wp$-function is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L^*} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right],$$

where $L^* = L \backslash \{0\}$, the set of non-zero periods. Its derivative $\wp'$ is given by

$$\wp'(z) = -\frac{2}{z^3} - \sum_{\omega \in L^*} \frac{1}{(z-\omega)^3} = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3}. \tag{1}$$

Theorem 1.2. (Addition theorem) For $z_1 \neq z_2$ one has

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \tfrac{1}{4} \left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)} \right)^2.$$

Theorem 1.3. (Duplication formula) It holds that

$$\wp(2z) = -2\wp(z) + \tfrac{1}{4} \left(\frac{\wp''(z)}{\wp'(z)} \right)^2.$$

Theorem 1.4. The Weierstraß $\wp$-function and its derivative $\wp'$ satisfy the relation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Taking the derivative of the above identity yields the following result.

Corollary 1.5. The functions $\wp(z)$ and $\wp''(z)$ satisfy the relation

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

Definition 1.6. The Weierstraß σ-function , which has zeroes of order 1 at all lattice points, is given by

$$\sigma(z) = z \prod_{\omega \in L^*} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2}. \tag{2}$$

Theorem 1.7. (Quasi-periodicity of the sigma function) Let $\omega \in L$. The function σ is a theta function, and in fact

$$\sigma(z+\omega) = \delta(\omega) e^{\eta(\omega)(z+\omega/2)} \sigma(z) \tag{3}$$

where

$$\delta(\omega) = \begin{cases} 1 & \text{if } \omega/2 \in L \\ -1 & \text{if } \omega/2 \notin L. \end{cases}$$

Theorem 1.8. For any $a \in \mathbb{C}$ not in L, we have

$$\wp(z) - \wp(a) = -\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2\sigma(a)^2}. \tag{4}$$

Theorem 1.9. For any $z \in \mathbb{C}$ not in L, we have[2]

$$\wp'(z) = -\frac{\sigma(2z)}{\sigma(z)^4}. \tag{5}$$

Theorem 1.10. The Weierstraß σ-function has a power series expansion[3]

$$\sigma(z) = \sum_{m,n=0}^{\infty} a_{m,n} \left(\tfrac{1}{2}g_2\right)^m (2g_3)^n \frac{z^{4m+6n+1}}{(4m+6n+1)!}$$

where $a_{0,0} = 1$ and

$$a_{m,n} = 3(m+1)a_{m+1,n-1} + \tfrac{16}{3}(n+1)a_{m-2,n+1} - \tfrac{1}{3}(2m+3n-1)(4m+6n-1)a_{m-1,n},$$

it being understood that $a_{m,n} = 0$ if either subscript is negative. In particular, the first terms of the expansion of $\sigma(z)$ are given by

$$\sigma(z) = z - \tfrac{1}{240}g_2 z^5 - \tfrac{1}{840}g_3 z^7 - \tfrac{1}{161280}g_2^2 z^9 - \dots$$

[2]Confer Silverman's *The arithmetic of elliptic curves*, 2nd edition (2009), exercise 6.3

[3]Formula 18.5.6 from the *Handbook of mathematical functions* by Abramowitz and Stegun.

2 Multiplication of the function $\wp(z)$

In this chapter we will see how the recursive relation Ward imposed on integers, arises from a certain elliptic function.

2.1 The function $\psi_n(z)$

We consider the doubly periodic function $\wp(nz)-\wp(z)$, n being an integer >0. Using the definition of the $\wp$-function, we see that

$$\wp(nz)-\wp(z)=\frac{1-n^2}{n^2z^2}+\sum_{\omega\in L^*}\left[\frac{1}{(nz-\omega)^2}-\frac{1}{(z-\omega)^2}\right], \tag{6}$$

so that it has a pole of order two at $z=0$. Furthermore, it has poles of order two at those values z_0 of z for which $nz_0\equiv 0 \pmod L$, i.e.

$$z_0=\frac{\nu_1\omega_1+\nu_2\omega_2}{n}, \tag{7}$$

$\nu_1,\nu_2\in\mathbb{Z}$. We obtain all incongruent values of z_0 by letting ν_1 and ν_2 run over $\mathbb{Z}/n\mathbb{Z}$.

The function $\wp(nz)-\wp(z)$ vanishes for those values z_1 of z for which $\wp(nz_1)=\wp(z_1)$, i.e. for which the congruence $nz_1\equiv\pm z_1 \pmod L$ holds. This follows from the periodicity of the $\wp$-function and the fact that $\wp$ is an even function. As a consequence, $nz_1\pm z_1=(n\pm 1)z_1\equiv 0 \pmod L$. This implies that z_1 is of the form

$$z_1=\frac{\nu_1\omega_1+\nu_2\omega_2}{n\pm 1}, \tag{8}$$

$\nu_1,\nu_2\in\mathbb{Z}$. The zeroes of $\wp(nz)-\wp(z)$ have order one.

We now introduce a function $\psi_n(z)$, which will turn out to have exactly the same poles and zeroes (counting multiplicity) as $\wp(nz)-\wp(z)$. For $n\geqslant 2$ we define

$$\psi_n(z)^2=n^2\prod_{\nu_1,\nu_2}\left[\wp(z)-\wp\left(\tfrac{\nu_1\omega_1+\nu_2\omega_2}{n}\right)\right], \tag{9}$$

where (ν_1,ν_2) runs over $(\mathbb{Z}/n\mathbb{Z})^2\backslash\{(0,0)\}:=A$, and put $\psi_1=1$. If n is odd, say $n=2m+1$, we can write $\mathbb{Z}/n\mathbb{Z}=\{-m,-m+1,\ldots,-1,0,1,\ldots,m-1,m\}$, so that $(\nu_1,\nu_2)\in A$ implies $-(\nu_1,\nu_2)=(-\nu_1,-\nu_2)\in A$ and $(\nu_1,\nu_2)\neq-(\nu_1,\nu_2)$. Since $\wp$ is an even function, one has $\wp(\frac{\nu_1\omega_1+\nu_2\omega_2}{n})=\wp(\frac{-\nu_1\omega_1-\nu_2\omega_2}{n})$, which means that every linear term in the product (9) appears twice. As $\#A=n^2-1$, we see that $\psi_n=P_n$, where P_n is a polynomial in $\wp(z)$ with highest term $\pm n\wp(z)^{(n^2-1)/2}$.

If n is even, say $n=2m$, we can write $\mathbb{Z}/n\mathbb{Z}=\{-m+1,-m+2,\ldots,-1,0,1,\ldots,m-1,m\}$. We have $-m\equiv m \pmod n$, so that $(\nu_1,\nu_2)\in A$ implies $(-\nu_1,-\nu_2)\in A$ and furthermore $(\nu_1,\nu_2)\neq(-\nu_1,-\nu_2)$ unless both ν_1 and ν_2 are in $\{0,m\}$. This means that every linear term in (9) appears twice, except for the terms corresponding to $(m,0)$, $(0,m)$ and (m,m), which appear only once. The product of these three terms is

$$\left(\wp(z)-\wp(\tfrac{\omega_1}{2})\right)\left(\wp(z)-\wp(\tfrac{\omega_2}{2})\right)\left(\wp(z)-\wp(\tfrac{\omega_1+\omega_2}{2})\right),$$

which we by theorem 1.4 know to be equal to $\frac{1}{4}\wp'(z)^2$. We therefore conclude that $\psi_n=\wp'\cdot P_n$, where P_n is a polynomial in $\wp(z)$ with highest term $\pm\frac{n}{2}\wp(z)^{(n^2-4)/2}$.

After choosing the sign of the highest term to be positive in case n is odd and negative in case n is even, one has in short:

$$\psi_n=\begin{cases}P_n & \text{if } n \text{ is odd,} \quad \text{highest term of } P_n \text{ is } n\wp(z)^{\frac{n^2-1}{2}};\\ \wp' P_n & \text{if } n \text{ is even,} \quad \text{highest term of } P_n \text{ is } -\frac{n}{2}\wp(z)^{\frac{n^2-4}{2}}.\end{cases} \tag{10}$$

We will see shortly that the coefficients of P_n are made up of rational functions of g_2 and g_3 and elements of $\mathbb{Q}$ (corollary 2.6).

Next we will prove the following lemma, which will turn out te be very useful. Note that by 'first term' of a power series expansion we mean the term of lowest degree.

Lemma 2.1. The first term in the power series expansion of $\psi_n(z)$ is given by

$$\frac{n}{z^{n^2-1}}.$$

PROOF. We use the expansions of $\wp(z)$ and $\wp'(z)$ in powers of z:[4]

$$\wp(z) = \tfrac{1}{z^2} + a_0 + a_1 z^2 + a_2 z^4 + a_3 z^6 + \cdots,$$

$$\wp'(z) = \tfrac{-2}{z^3} + 2a_1 z + 4a_2 z^3 + 6a_3 z^5 + \ldots$$

For odd n one has as first term of $\psi_n(z)$ the expression

$$n\left(\frac{1}{z^2}\right)^{\frac{n^2-1}{2}} = \frac{n}{z^{n^2-1}}.$$

For even n the first term of ψ_n equals

$$-\frac{n}{2}\cdot -\frac{2}{z^3}\cdot\left(\frac{1}{z^2}\right)^{\frac{n^2-4}{2}} = \frac{n}{z^{n^2-1}}.\boxtimes$$

Notice that by (7) the poles of $\wp(nz)-\wp(z)$ coincide with the zeroes of $\psi_n(z)$ and that by (8) the zeroes of $\wp(nz)-\wp(z)$ coincide with the zeroes of $\psi_{n\pm1}(z)$. Since the poles of $\wp(nz)-\wp(z)$ have order two, the quotient

$$\frac{\psi_n(z)^2\left[\wp(nz)-\wp(z)\right]}{\psi_{n+1}(z)\psi_{n-1}(z)} \tag{11}$$

is an elliptic function without zero or pole, hence a constant $c \in \mathbb{C}$. This constant is exactly the ratio of the first terms of the expansion in powers of z of the numerator and denominator respectively. On using (6) one derives that

$$c = \frac{\frac{n^2}{z^{2n^2-2}}\cdot\frac{1-n^2}{n^2z^2}}{\frac{n+1}{z^{(n+1)^2-1}}\cdot\frac{n-1}{z^{(n-1)^2-1}}} = \frac{\frac{1-n^2}{z^{2n^2}}}{\frac{n^2-1}{z^{2n^2}}} = \frac{-(n^2-1)}{n^2-1} = -1.$$

Thus, we have established a formula for $\wp(nz)$ in terms of $\wp(z)$, $\psi_n(z)$ and $\psi_{n\pm1}(z)$, which whe state in a theorem.

Theorem 2.2. The following relation holds:

$$\wp(nz) = \wp(z) - \frac{\psi_{n+1}(z)\psi_{n-1}(z)}{\psi_n(z)^2}. \tag{12}$$

[4]Heinrich Weber, *Lehrbuch der Algebra* (1908), dritter Band, §56, p.185.

2.2 Explicit computation of $\psi_2(z)$, $\psi_3(z)$ and $\psi_4(z)$

We will now compute $\psi_2(z)$, $\psi_3(z)$ and $\psi_4(z)$ explicitly — expressions we shall need later on. We establish $\psi_2(z)$ right from (10): P_2 is a polynomial with highest term

$$-\tfrac{n}{2}\wp(z)^{\frac{n^2-4}{2}} = -\tfrac{2}{2}\wp(z)^0 = -1,$$

and therefore must be itself equal to -1. Hence, $\psi_2(z) = -\wp'(z)$. By the duplication formula one has

$$\wp(2z) = -2\wp(z) + \tfrac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2 = -2\wp(z) + \frac{\frac{1}{4}\left(6\wp(z)^2 - \frac{1}{2}g_2\right)^2}{4\wp(z)^3 - g_2\wp(z) - g_3} = \tag{13}$$

$$-2\wp(z) + \frac{9\wp(z)^4 - \frac{3}{2}g_2\wp(z)^2 + \frac{1}{16}g_2^2}{4\wp(z)^3 - g_2\wp(z) - g_3} =$$

$$-2\wp(z) + \frac{3\wp(z)\left[4\wp(z)^3 - g_2\wp(z) - g_3\right] - 3\wp(z)^4 + \frac{3}{2}g_2\wp(z)^2 + 3g_3\wp(z) + \frac{1}{16}g_2^2}{4\wp(z)^3 - g_2\wp(z) - g_3} =$$

$$\wp(z) - \frac{3\wp(z)^4 - \frac{3}{2}g_2\wp(z)^2 - 3g_3\wp(z) - \frac{1}{16}g_2^2}{\wp'(z)^2}.$$

By (12) this expression equals

$$\wp(z) - \frac{\psi_3(z)\psi_1(z)}{\psi_2(z)^2} = \wp(z) - \frac{\psi_3(z)}{\wp'(z)^2}.$$

We have thus derived that

$$\psi_3(z) = P_3 = 3\wp(z)^4 - \tfrac{3}{2}g_2\wp(z)^2 - 3g_3\wp(z) - \tfrac{1}{16}g_2^2. \tag{14}$$

In order to determine $\psi_4(z)$, we use the addition formula:

$$\wp(w+z) = -\wp(w) - \wp(z) + \tfrac{1}{4}\left(\frac{\wp'(w) - \wp'(z)}{\wp(w) - \wp(z)}\right)^2.$$

Furthermore, since $\wp$ is an even and $\wp'$ is an odd function, one has

$$\wp(w-z) = -\wp(w) - \wp(-z) + \tfrac{1}{4}\left(\frac{\wp'(w) - \wp'(-z)}{\wp(w) - \wp(-z)}\right)^2 = -\wp(w) - \wp(z) + \tfrac{1}{4}\left(\frac{\wp'(w) + \wp'(z)}{\wp(w) - \wp(z)}\right)^2.$$

Thus

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

On taking $w = 2z$ and applying (12) for $n = 3$ we now obtain

$$\wp(3z) - \wp(z) = -\frac{\wp'(2z)\wp'(z)}{\left(\wp(2z) - \wp(z)\right)^2} = -\frac{\psi_4(z)\psi_2(z)}{\psi_3(z)^2}.$$

Given that

$$\wp(2z) - \wp(z) = -\frac{\psi_3(z)}{\psi_2(z)^2} = -\frac{\psi_3(z)}{\wp'(z)^2},$$

we derive that

$$\wp(3z)-\wp(z)=-\frac{\wp'(2z)\wp'(z)}{(\wp(2z)-\wp(z))^2}=-\frac{\wp'(z)^5\wp'(2z)}{\psi_3(z)^2}=\frac{\psi_4(z)\wp'(z)}{\psi_3(z)^2}.$$

As a consequence,

$$\psi_4(z)=-\wp'(z)^4\wp'(2z).$$

We obtain the value of $\wp'(2z)$ by differentiating expression (13):

$$2\wp'(2z)=\wp'(z)-\frac{\wp'(z)^2\left[12\wp(z)^3\wp'(z)-3g_2\wp(z)\wp'(z)-3g_3\wp'(z)\right]}{\wp'(z)^4}$$

$$+\frac{2\wp'(z)\wp''(z)\left[3\wp(z)^4-\frac{3}{2}g_2\wp(z)^2-3g_3\wp(z)-\frac{1}{16}g_2^2\right]}{\wp'(z)^4}.$$

Therefore

$$\psi_4(z)=-\wp'(z)^4\wp'(2z)=-\tfrac{1}{2}\left(\wp'(z)^5-\wp'(z)^2\left[12\wp(z)^3\wp'(z)-3g_2\wp(z)\wp'(z)-3g_3\wp'(z)\right]\right)$$

$$-\tfrac{1}{2}2\wp'(z)\wp''(z)\left[3\wp(z)^4-\tfrac{3}{2}g_2\wp(z)^2-3g_3\wp(z)-\tfrac{1}{16}g_2^2\right]=$$

$$-\tfrac{1}{2}\wp'(z)\left(\wp'(z)^4-\wp'(z)^2\left[12\wp(z)^3-3g_2\wp(z)-3g_3\right]+2\wp''(z)\left[3\wp(z)^4-\tfrac{3}{2}g_2\wp(z)^2-3g_3\wp(z)-\tfrac{1}{16}g_2^2\right]\right).$$

Next, on using theorems 1.4 and 1.5 we conclude that

$$\psi_4(z)=-\tfrac{1}{2}\wp'(z)\left([4\wp(z)^3-g_2\wp(z)-g_3]^2-[4\wp(z)^3-g_2\wp(z)-g_3][12\wp(z)^3-3g_2\wp(z)-3g_3]\right)$$

$$-\tfrac{1}{2}\wp'(z)\cdot 2[6\wp(z)^2-\tfrac{1}{2}g_2][3\wp(z)^4-\tfrac{3}{2}g_2\wp(z)^2-3g_3\wp(z)-\tfrac{1}{16}g_2^2]=$$

$$-\tfrac{1}{2}\wp'(z)\left(4\wp(z)^6-5g_2\wp(z)^4-20g_3\wp(z)^3-\tfrac{5}{4}g_2^2\wp(z)^2-g_2g_3\wp(z)-2g_3^2+\tfrac{1}{16}g_2^3\right)=$$

$$\wp'(z)\left(-2\wp(z)^6+\tfrac{5}{2}g_2\wp(z)^4+10g_3\wp(z)^3+\tfrac{5}{8}g_2^2\wp(z)^2+\tfrac{1}{2}g_2g_3\wp(z)+g_3^2-\tfrac{1}{32}g_2^3\right).$$

In view of (10) it follows that

$$P_4=-2\wp(z)^6+\tfrac{5}{2}g_2\wp(z)^4+10g_3\wp(z)^3+\tfrac{5}{8}g_2^2\wp(z)^2+\tfrac{1}{2}g_2g_3\wp(z)+g_3^2-\tfrac{1}{32}g_2^3. \tag{15}$$

2.3 A general recursive formula for $\psi_n(z)$

Let us now apply formula (12) to the numbers m and n:

$$\wp(mz)-\wp(z)=\frac{\psi_{m+1}(z)\psi_{m-1}(z)}{\psi_m(z)^2},\qquad \wp(nz)-\wp(z)=\frac{\psi_{n+1}(z)\psi_{n-1}(z)}{\psi_n(z)^2}.$$

Because the left-hand sides are equal for those values z_0 of z for which $mz_0\equiv\pm nz_0 \pmod L$, i.e. $(m\pm n)z_0\equiv 0 \pmod L$, the right-hand sides must be equal too for $z=z_0$. But those values z_0 are precisely the zeroes of $\psi_{m\pm n}(z)$. Consequently, the functions

$$\psi_{m+1}(z)\psi_{m-1}(z)\psi_n(z)^2-\psi_{n+1}(z)\psi_{n-1}(z)\psi_m(z)^2,$$

$$\psi_{m+n}(z)\psi_{m-n}(z)$$

both vanish precisely at $z = z_0$. By (10) they are polynomials in $\wp(z)$ having exactly the same zeroes. Therefore their quotient must be a constant $c \in \mathbb{C}$. As before, we determine it by computing the ratio of the first term of the power expansion of $\psi_{m+1}(z)\psi_{m-1}(z)\psi_n(z)^2 - \psi_{n+1}(z)\psi_{n-1}(z)\psi_m(z)^2$ and that of $\psi_{m+n}(z)\psi_{m-n}(z)$:

$$c = \frac{\frac{m+1}{z^{(m+1)^2-1}} \cdot \frac{m-1}{z^{(m-1)^2-1}} \frac{n^2}{z^{2n^2-2}} - \frac{n+1}{z^{(n+1)^2-1}} \cdot \frac{n-1}{z^{(n-1)^2-1}} \frac{m^2}{z^{2m^2-2}}}{\frac{m+n}{z^{(m+n)^2-1}} \cdot \frac{m-n}{z^{(m-n)^2-1}}} =$$

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

We have established a recursive formula which we state in a theorem.

Theorem 2.3. The following formula holds:

$$\psi_{m+n}(z)\psi_{m-n}(z) = \psi_{m+1}(z)\psi_{m-1}(z)\psi_n(z)^2 - \psi_{n+1}(z)\psi_{n-1}(z)\psi_m(z)^2. \tag{16}$$

Taking $m = n+1,\ n = n$ and subsequently $m = n+1,\ n = n-1$ directly yields the following result.

Corollary 2.4. The following relations hold:

$$\psi_{2n+1}(z) = \psi_{n+2}(z)\psi_n(z)^3 - \psi_{n-1}(z)\psi_{n+1}(z)^3, \qquad n \geqslant 1, \tag{17}$$

$$\wp'(z)\psi_{2n}(z) = -\psi_n(z)\left[\psi_{n+2}(z)\psi_{n-1}(z)^2 - \psi_{n-2}(z)\psi_{n+1}(z)^2\right], \qquad n \geqslant 2.$$

In terms of the polynomials P_n, the corollary reads as follows.

Corollary 2.5. For $n \geqslant 2$ the following relations hold:

$$P_{2n+1} = \begin{cases} \wp'(z)^4 P_{n+2}P_n^3 - P_{n-1}P_{n+1}^3 & \text{for } n \text{ even}, \\ P_{n+2}P_n^3 - \wp'(z)^4 P_{n-1}P_{n+1}^3 & \text{for } n \text{ odd}, \end{cases}$$

$$P_{2n} = -P_n\left(P_{n+2}P_{n-1}^2 - P_{n-2}P_{n+1}^2\right).$$

Corollary 2.6. The coefficients of P_n are elements of $\mathbb{Z}[\frac{g_2}{4}, g_3]$, that is: $P_n \in \mathbb{Z}[\wp(z), \frac{g_2}{4}, g_3]$. In particular, the coefficients of P_n are elements of $\mathbb{Q}[g_2, g_3]$.

PROOF. As we have seen explicitly, P_1, P_2, P_3 and P_4 are elements of $\mathbb{Z}[\wp(z), \frac{g_2}{4}, g_3]$. By corollary 2.5, $P_n \in \mathbb{Z}[P_1, P_2, P_3, P_4, \wp'(z)^4] \subseteq \mathbb{Z}[\wp(z), \wp'(z)^4, \frac{g_2}{4}, g_3]$. Using the fact that $\wp'(z)^4 = (4\wp(z)^3 - g_2\wp(z) - g_3)^2$, we see that $\mathbb{Z}[\wp(z), \wp'(z)^4, \frac{g_2}{4}, g_3] \subseteq \mathbb{Z}[\wp(z), \frac{g_2}{4}, g_3]$. We conclude that $P_n \in \mathbb{Z}[\wp(z), \frac{g_2}{4}, g_3]$, which is equivalent to saying that the coefficients of P_n lie in $\mathbb{Z}[\frac{g_2}{4}, g_3]$. ⊠

2.4 A representation of $\psi_n(z)$ by means of the Weierstraß sigma function

This section is devoted to the proof of the following theorem, which gives a representation of our function $\psi_n(z)$ by means of the Weierstraß sigma function.

Theorem 2.7. Define

$$\phi_n(z) := \frac{\sigma(nz)}{\sigma(z)^{n^2}}.$$

It holds that:

(i) The function $\phi_n(z)$ is elliptic with lattice L, i.e. $\phi_n(z+\omega) = \phi_n(z)$ for $\omega \in L$.
(ii) $\phi_n(z) = \psi_n(z)$.

PROOF. (i) One has, on the basis of theorem 1.7,

$$\phi_n(z+\omega) = \frac{\sigma(nz+n\omega)}{(\sigma(z))^{n^2}} = \frac{\delta(n\omega)e^{\eta(n\omega)(nz+n\omega/2)}\sigma(nz)}{\left(\delta(\omega)e^{\eta(\omega)(z+\omega/2)}\sigma(z)\right)^{n^2}} =$$

$$\frac{\delta(n\omega)e^{n^2\eta(\omega)(z+\omega/2)}\sigma(nz)}{\delta(\omega)^{n^2}e^{n^2\eta(\omega)(z+\omega/2)}\sigma(z)^{n^2}} = \frac{\delta(n\omega)\sigma(nz)}{\delta(\omega)^{n^2}\sigma(z)^{n^2}}.$$

If n is even, $\frac{n}{2} \in \mathbb{Z}$ so that $\frac{n\omega}{2} \in L$. This means that $\delta(n\omega) = +1$. Furthermore, $\delta(\omega)^{n^2} = \left((\pm 1)^2\right)^{\frac{n}{2}} = +1$. If n is odd, we see that $\frac{\omega}{2} \in L$ if and only if $\frac{n\omega}{2} \in L$, so that $\delta(n\omega) = \delta(\omega) = \delta(\omega)^{n^2}$. In either case, whether n be even or odd, one has $\delta(n\omega) = \delta(\omega)^{n^2}$. Hence,

$$\phi_n(z+\omega) = \frac{\delta(n\omega)\sigma(nz)}{\delta(\omega)^{n^2}\sigma(z)^{n^2}} = \frac{\sigma(nz)}{\sigma(z)^{n^2}} = \phi_n(z).$$

(ii) The zeroes of $\psi_n(z)$ are the points in the complex plane that are of the form $\frac{\nu_1\omega_1+\nu_2\omega_2}{n}$ with $\nu_1, \nu_2 \in \mathbb{Z}$. They are of order one. It is easy to see that these are exactly the zeroes of $\phi_n(z)$, which are of order one as well.

As for the poles, from (10) it follows that $\psi_n(z)$ has poles of order n^2-1 at all the lattice points $\omega \in L$. The zeroes of the denominator of $\phi_n(z)$ are the lattice points $\omega \in L$ and have order n^2. Because the zeroes of the numerator of $\phi_n(z)$ are of the form $\frac{\nu_1\omega_1+\nu_2\omega_2}{n}$ with $\nu_1, \nu_2 \in \mathbb{Z}$, and are of order one, and because each lattice point particularly can be be written in this form, we conclude that $\phi_n(z)$ has poles at all the lattice points, of order n^2-1.

Seeing that $\psi_n(z)$ and $\phi_n(z)$ are elliptic functions having exactly the same zeroes and poles, their quotient must be a constant c. To determine it, we compute, as usual, the ratio of the first terms of the power series of $\psi_n(z)$ c.q. $\phi_n(z)$. By lemma 2.1, the first term of the power series of $\psi_n(z)$ is n/z^{n^2-1}. By theorem 1.10, the first term of the power series of $\sigma(z)$ is given by z. As a consequence, the first term of the power series of $1/\sigma(z)$ is given by $1/z$ and that of $\sigma(nz)$ by nz. We conclude that the first term of the power series of $\phi_n(z)$ is given by

$$\frac{nz}{z^{n^2}} = \frac{n}{z^{n^2-1}}.$$

Hence, the constant c must be 1 and the theorem follows. ☒

2.5 Multiplication by n of a rational point on an elliptic curve

The previous sections enable us to compute explicitly the coordinates of the n-multiple of a rational point on an elliptic curve. To avoid confusion we shall use capital letters to denote the equation for an elliptic curve in modern short Weierstraß form and small letters to denote the equation for an elliptic curve in classical short Weierstraß form — a notation we will stick to throughout this entire thesis.

For a point (X,Y) on $E:\ Y^2 = X^3 + AX + B$ a well-known result is the *duplication formula*:

$$2(X,Y) = \left(\frac{X^4 - 2AX^2 - 8BX + A^2}{4Y^2}, \frac{X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3}{8Y^3}\right). \quad (18)$$

Its classical counterpart for a point (x,y) on $E':\ y^2 = 4x^3 + ax + b$ is:

$$2(x,y) = \left(\frac{16x^4 - 8ax^2 - 32bx + a^2}{16y^2}, \frac{64x^6 + 80ax^4 + 320bx^3 - 20a^2x^2 - 16abx - 32b^2 - a^3}{32y^3}\right). \quad (19)$$

Let us consider the n-multiple of the point $Q=(x,y)\in E'(\mathbb{Q})$. The Weierstraß function $\wp(z;\,-a,-b)$ satisfies the equation for E' and it is known from elliptic function theory that there exists a complex constant u such that $(x,y)=(\wp(u),\wp'(u))$. In section section 2.1 we derived that $\wp(nu)=\wp(u)-\frac{\psi_{n+1}(u)\psi_{n-1}(u)}{\psi_n(u)^2}$. Therefore we have for the x-coordinate of nQ:

$$x(nQ)=\frac{\wp(u)\psi_n(u)^2-\psi_{n+1}(u)\psi_{n-1}(u)}{\psi_n(u)^2}=\frac{x\psi_n(u)^2-\psi_{n+1}(u)\psi_{n-1}(u)}{\psi_n(u)^2}.$$

We know that for odd n we have $\psi_n(u)=P_n$ and for even n we have $\psi_n(u)=\wp'(u)P_n=yP_n$. Since P_n is a polynomial in $\wp(u)=x$, we may write for odd n:

$$x(nQ)=\frac{xP_n(x)^2-y^2P_{n+1}(x)P_{n-1}(x)}{P_n(x)^2}=\frac{xP_n(x)^2-(4x^3+ax+b)P_{n+1}(x)P_{n-1}(x)}{P_n(x)^2}.$$

For even n we may write

$$x(nQ)=\frac{xy^2P_n(x)^2-P_{n+1}(x)P_{n-1}(x)}{y^2P_n(x)^2}=\frac{(4x^4+ax^2+bx)P_n(x)^2-P_{n+1}(x)P_{n-1}(x)}{(4x^3+ax+b)P_n(x)^2}.$$

Let us write $\phi_n(x)$ for the 'numerator' of $x(nQ)$:

$$\phi_n(x)=\begin{cases}xP_n(x)^2-(4x^3+ax+b)P_{n+1}(x)P_{n-1}(x) & \text{if } n \text{ is odd}\\ (4x^4+ax^2+bx)P_n(x)^2-P_{n+1}(x)P_{n-1}(x) & \text{if } n \text{ is even.}\end{cases}$$

Regardless of the parity of n, $\phi_n(x)$ is a polynomial in x of degree n^2. As the 'denominator' of $x(nQ)$, that is to say $\psi_n(u)^2$, is a polynomial in x of degree n^2-1, we may write $\psi_n(x)^2$ instead of $\psi_n(u)^2$. In short, we have

$$x(nQ)=\frac{\phi_n(x)}{\psi_n(x)^2}.$$

Example 2.8. On taking $n=2$ and using the expressions for P_1, P_2 and P_3 from section 2.2 and the fact that $g_2=-a$ and $g_3=-b$, we see that

$$x(2Q)=\frac{4x^4+ax^2+bx-(3x^4+\frac{3}{2}ax^2+3bx-\frac{1}{16}a^2)}{4x^3+ax+b}=$$

$$\frac{64x^4+16ax^2+16bx-48x^4-24ax^2-48bx+a^2}{16(4x^3+ax+b)}=\frac{16x^4-8ax^2-32bx+a^2}{16y^2},$$

in accordance with (19), of course.$\Diamond$

What about $y(nQ)$? It turns out that if we use the expression for $\psi_n(u)$ in terms of the sigma function that we established in section 2.4, calculations become fairly simple. From (5) we know that if $z\notin L$,

$$\wp'(z)=-\frac{\sigma(2z)}{\sigma(z)^4}.$$

Hence, plugging in nu for z yields

$$y(nP)=\wp'(nu)=-\frac{\sigma(2nu)}{\sigma(nu)^4}=-\frac{\sigma(2nu)}{\sigma(nu)^4}\,\frac{\sigma(u)^{4n^2}}{\sigma(u)^{4n^2}}=-\frac{\sigma(2nu)}{\sigma(u)^{4n^2}}\left(\frac{\sigma(u)^{n^2}}{\sigma(nu)}\right)^4=-\frac{\psi_{2n}(u)}{\psi_n(u)^4}=-\frac{\psi_{2n}(x,y)}{\psi_n(x,y)^4}.$$

We now state our results in a theorem.

Theorem 2.9. Let $Q = (x,y) =$ be a non-n-torsion point on the elliptic curve $E:\ y^2 = 4x^3 + ax + b$ with $a,b \in \mathbb{Z}$. If we write $\psi_n = \psi_n(x,y)$, then the coordinates of the point nP are given by

$$nQ = \left(\frac{x\psi_n^2 - \psi_{n+1}\psi_{n-1}}{\psi_n^2}, -\frac{\psi_{2n}}{\psi_n^4} \right).$$

Example 2.10. On taking $n = 2$ and using the expressions for ψ_2 and ψ_4 from section 2.2 and the fact that $g_2 = -a$ and $g_3 = -b$, we find that

$$y(2Q) = -\frac{\psi_4(x,y)}{\psi_2(x,y)^4} = -\frac{32}{32}\,\frac{y(-2x^6 - \frac{5}{2}ax^4 - 10bx^3 + \frac{5}{8}a^2x^2 + \frac{1}{2}abx + b^2 + \frac{1}{32}a^3)}{(-y)^4} =$$

$$\frac{64x^6 + 80ax^4 + 320bx^3 - 20a^2x^2 - 16abx - 32b^2 - a^3}{32y^3},$$

in accordance with (19), of course.$\Diamond$

To conclude this section, we will translate the above discussion to elliptic curves in *modern* short Weierstraß form. So let $E:\ Y^2 = X^3 + AX + B$ be an elliptic curve with coefficients in $\mathbb{Z}$. Multiplying the equation by 4 yields $(2Y)^2 = 4X^3 + 4AX + 4B$. By putting $x = X$, $y = -2Y$, $a = 4A$ and $b = 4B$ we obtain an equation in classical Weierstraß form[5]: $E':\ y^2 = 4x^3 + ax + b$. Now define $\Psi_n = \Psi_n(X,Y) := \psi_n(x,y) = \psi_n(X,-2Y)$. Then we have

$$\Psi_1 = 1,$$

$$\Psi_2 = \psi_2(x,y) = -y = 2Y,$$

$$\Psi_3 = \psi_3(x,y) = 3x^4 + \tfrac{3}{2}ax^2 + 3bx - \tfrac{1}{16}a^2 = 3X^4 + 6AX^2 + 12BX - A^2.$$

Moreover,

$$\Psi_4 = \psi_4(x,y) = y(-2x^6 - \tfrac{5}{2}ax^4 - 10bx^3 + \tfrac{5}{8}a^2x^2 + \tfrac{1}{2}abx + b^2 + \tfrac{1}{32}a^3) =$$

$$4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3).$$

By definition, $\Psi_n = \Psi_n(X,Y)$ satisfies the recursive relation (16). Thus, by corollary 2.4,

$$\Psi_{2n+1}(X,Y) = \Psi_{n+2}\Psi_n^3 - \Psi_{n-1}\Psi_{n+1}^3, \quad n \geqslant 2,$$

$$\Psi_{2n}(X,Y) = \frac{\Psi_n}{2Y}\left(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2\right), \quad n \geqslant 3.$$

The Ψ_n are in $\mathbb{Z}[X,Y,A,B]$ and are called *division polynomials*, since they satisfy the relation: if $n|m$, then $\Psi_n|\Psi_m$ as polynomials in $\mathbb{Z}[X,Y,A,B]$.

Now suppose we have a point $R = (X,Y)$ on E. R corresponds to the point $R' = (X,-2Y)$ on E'. By theorem 2.9, the coordinates of nR' are

$$\left(\frac{X\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, -\frac{\Psi_{2n}}{\Psi_n^4} \right).$$

Consequently, the coordinates of nR are

$$\left(\frac{X\Psi_n^2 - \Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{2n}}{2\Psi_n^4} \right).$$

[5]We choose $y = -2Y$ instead of $y = 2Y$ so that the results coincide with the common definition of division polynomials.

Part II
Elliptic divisibility sequences

3 Elementary properties of elliptic divisibility sequences

3.1 Divisibility sequences

Definition 3.1. (Divisibility sequence) By an integral *divisibility sequence* we mean a sequence of integers,

$$(h): \quad h_0, h_1, h_2, \ldots, h_n, \ldots$$

such that h_r divides h_s if r divides s.

REMARK. Since h_1 must divide every term of (h), we may *always* assume that $h_1 = 1$.

Example 3.2. The sequence given by $h_n = n$ for $n \in \mathbb{N}$ is a trivial example of a divisibility sequence.$\Diamond$

Example 3.3. The sequence (M) of *Mersenne* numbers

$$0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, \ldots$$

defined by $M_n = 2^n - 1$ for $n \geqslant 0$, is a divisibility sequence. Indeed, let m be a divisor of n, so that $n = mk$ for some k. We have

$$M_n = 2^n - 1 = 2^{mk} - 1 = (2^m - 1)(1 + 2^m + 2^{2m} + 2^{3m} + \ldots + 2^{(k-1)m}),$$

so that $M_m | M_n$. $\Diamond$

Example 3.4. The sequence (F) of Fibonacci numbers

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, \ldots$$

given by $F_0 = 0$, $F_1 = 1$ and $F_m = F_{m-1} + F_{m-2}$ for $m \geqslant 2$, is a divisibility sequence. To see this, we shall first prove that

$$F_{m+n} = F_{m-1}F_n + F_m F_{n+1} \tag{20}$$

by induction on n. For $n = 1$ this formula takes the form

$$F_{m+1} = F_{m-1}F_1 + F_m F_2 = F_{m-1} + F_m,$$

which is obviously true. For $n = 2$ the formula is also true, because

$$F_{m+2} = F_{m-1}F_2 + F_m F_3 = F_{m-1} + 2F_m = F_m + (F_{m-1} + F_m) = F_m + F_{m+1}.$$

Thus the basis of the induction is proved. Now suppose that (20) holds for $n = k$ and $n = k + 1$:

$$F_{m+k} = F_{m-1}F_k + F_m F_{k+1},$$

$$F_{m+k+1} = F_{m-1}F_{k+1} + F_m F_{k+2}.$$

We have to show that it holds for $n = k + 2$ also. Adding the last two equations term by term we obtain

$$F_{m+k+2} = F_{m-1}F_{k+2} + F_m F_{k+3},$$

and this was the desired result.

Now we are able to prove that (F) is in fact a divisibility sequence, that is

$$m|n \qquad \Rightarrow \qquad F_m|F_n.$$

To that end, let n by divisible by m, i.e. let $n = km$. We shall carry out the proof by induction over k. If $k = 1$, then $m = n$ so that the conclusion of the implication is obvious. Now suppose the statement holds for $k = q$. We have to prove it holds for $k = q+1$ also, that is, that $F_m|F_{(q+1)m}$. By (20) we have

$$F_{(q+1)m} = F_{qm+m} = F_{qm-1}F_m + F_{qm}F_{m+1}.$$

It is obvious that the first term is divisible by F_m. By the induction hypothesis, $F_m|F_{qm}$. Hence the second term is divisible by F_m. Thus $F_m|F_{(q+1)m}$ and we have proven that (F) is a divisibility sequence.$\Diamond$

Definition 3.5. Let (h) be any sequence of integers. An integer m is said to be a *divisor* of the sequence (h) if it divides some term h_r with $r \geqslant 1$. If m divides h_r but does not divide h_d if d divides r, then m is called a *rank of apparition* of m in (h). We will mostly be concerned with the *smallest* rank of apparition in (h) of a given integer, which we often denote by ρ. By *the* rank of apparition we shall always mean 'smallest rank of apparition'.

We conclude this paragraph with an important theorem on divisibility sequences. We write (m,n) for the greatest common divisor of m and n. If m^k is the highest power of m that divides n, we shall write $m^k||n$.

Theorem 3.6. Let (h) be a divisibility sequence. Then the following statements are equivalent:

(i) $(h_m, h_n) = h_{(m,n)}$.

(ii) For every prime divisor p of (h) and every positive integer k, it holds that (I) $h_r \equiv 0 \pmod{p^k}$ if and only if (II) $r \equiv 0 \pmod{\rho_k}$, where ρ_k is the smallest rank of apparition of p^k in (h).

REMARK. Property (ii) means: every prime power p^k that is a divisor of (h) has a unique rank of apparition.

PROOF. "(i)⇒(ii)". For the implication (I)⇒(II), assume that p is any prime divisor of (h) and furthermore that $h_r \equiv 0 \pmod{p^k}$. Because of the latter assumption p^k is a divisor of (h), so that ρ_k truly exists. We have $h_r \equiv h_{\rho_k} \equiv 0 \pmod{p^k}$. Hence (h_r, h_{ρ_k}) contains p^k as factor, so that $(h_r, h_{\rho_k}) \equiv 0 \pmod{p^k}$. From (i) it follows that $h_{(r,\rho_k)} = (h_r, h_{\rho_k}) \equiv 0 \pmod{p^k}$. By minimality of ρ_k we see that $(r,\rho_k) \geqslant \rho_k$. On the other hand, since by the definition of greatest common divisor $(r,\rho_k)|\rho_k$, we have $(r,\rho_k) \leqslant \rho_k$. Therefore $(r,\rho_k) = \rho_k$, in other words $\rho_k|r$, i.e. $r \equiv 0 \pmod{\rho_k}$.

For the reverse implication (II)⇒(I), assume that $r \equiv 0 \pmod{\rho_k}$. We have implicitly assumed that ρ_k exists. By assumption, $\rho_k|r$. Since (h) is a divisibility sequence, it follows that $h_{\rho_k}|h_r$. By the definition of ρ_k we have that $p^k|h_{\rho_k}$, the result being that $p^k|h_r$, i.e. $h_r \equiv 0 \pmod{p^k}$. Note that for the proof of (II)⇒(I) we did not use the validity of (i).

"(ii)⇒(i)". Let h_m and h_n be any two terms of (h). We will prove successively that (III) $h_{(m,n)}|(h_m, h_n)$ and (IV) $(h_m, h_n)|h_{(m,n)}$, whereupon (i) shall be proven. For the proof of (III) we do not even have to assume the validity of (ii). Since $(m,n)|m$ and $(m,n)|n$, it holds that $h_{(m,n)}|h_m$ and $h_{(m,n)}|h_n$, for (h) is a divisibility sequence. Hence $h_{(m,n)}|(h_m, h_n)$.

In order to prove (IV), suppose first that h_m and h_n are coprime, i.e. $(h_m, h_n) = 1$. As we have just seen, it always holds that $h_{(m,n)}|(h_m, h_n)$. As $(h_m, h_n) = 1$, we must have $h_{(m,n)} = 1$ also. Hence (i) holds in case h_m and h_n are coprime.

For the rest of the proof we may assume that $(h_m, h_n) > 1$. Let p be any common prime divisor of

h_m and h_n. Let p^a and p^b be the highest powers of p that divide h_m and h_n respectively ($a,b \geqslant 1$). Equivalently put, $p^a \,||h_m$ and $p^b \,||h_n$. Let $c := \min\{a,b\}$. It suffices to show that $p^c|h_{(m,n)}$. Indeed, assume $p^c|h_{(m,n)}$ proven for every common prime divisor p of h_m and h_n. Then, since $p^c \,||(h_m,h_n)$, it follows that $(h_m,h_n)|h_{(m,n)}$.

It remains for us to show that $p^c|h_{(m,n)}$. Since $h_m \equiv 0 \pmod{p^a}$ and $h_n \equiv 0 \pmod{p^b}$, the numbers ρ_a and ρ_b – the smallest ranks of apparition of p^a and p^b respectively – truly exist. Without loss of generality we may assume that $a \geqslant b$, so that $c = b$. We therefore have $h_m \equiv h_n \equiv 0 \pmod{p^b}$. Since (ii) holds, it follows that $\rho_b|m$ and $\rho_b|n$, so that $\rho_b|(m,n)$. Because (h) is a divisibility sequence, we now have $h_{\rho_b}|h_{(m,n)}$. But by definition $p^b|h_{\rho_b}$ whence $p^c = p^b|h_{(m,n)}$, as desired. This completes the proof. ⊠

3.2 Elliptic divisibility sequences

Definition 3.7. (Elliptic divisibility sequence) By an *elliptic divisibility sequence* (EDS) we mean a sequence of integers (h) that is a divisibility sequence and that in addition satisfies the following relation:

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \qquad 1 \leqslant n \leqslant m. \tag{21}$$

REMARK. If (h) isn't a sequence of integers but of rational numbers satisfying (21), we call (h) an *elliptic sequence*. Although for the time being we shall be concerned only with elliptic divisibility sequences, we will come across elliptic sequences later on.♢

On taking first $m = n+1$, $n = n$ and then $m = n+1$, $n = n-1$ in (21) we obtain two important formulas.

Theorem 3.8. If (h) is a solution of (21), we have

$$h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3, \qquad n \geqslant 1, \tag{22}$$

$$h_{2n}h_2 = h_n\left(h_{n+2}h_{n-1}^2 - h_{n-2}h_{n+1}^2\right), \qquad n \geqslant 2. \tag{23}$$

Example 3.9. The sequence from before, given by $h_n = n$ for $n \in \mathbb{N}$, is also an *elliptic* divisibility sequence. Indeed, for every $m,n \in \mathbb{N}$ with $1 \leqslant n \leqslant m$ one has $h_{m+n}h_{m-n} = (m+n)(m-n) = m^2 - n^2$ so that

$$h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 = (m+1)(m-1)n^2 - (n+1)(n-1)m^2 =$$
$$(m^2-1)n^2 - (n^2-1)m^2 = m^2n^2 - n^2 - m^2n^2 + m^2 = m^2 - n^2 = h_{m+n}h_{m-n}.\diamondsuit$$

Example 3.10. The sequence of Fibonacci numbers itself is *not* an elliptic divisibility sequence, but the sequence (G) consisting of every other term in the Fibonacci sequence is. We have $G_m = F_{2m}$. First of all, since (F) is a divisibility sequence, (G) is too. It remains te be proven that (G) satisfies (21), in order for (G) to be an EDS. To this end, we first prove that the following formulas hold:

(i) $G_{m+1} = 3G_m - G_{m-1}$
(ii) $G_{m+n} = G_mG_{n+1} - G_{m-1}G_n$
(iii) $G_{m-n} = G_{m-1}G_n - G_mG_{n-1}$.

PROOF. (i) Using the fact that $F_m = F_{m+1} - F_{m-1}$, we see that

$$G_{m+1} = F_{2m+2} = F_{2m+1} + F_{2m} = (F_{2m} + F_{2m-1}) + F_{2m} = 2F_m + F_{2m-1} =$$
$$2F_{2m} + (F_{2m-2} - F_{2m}) = 3F_{2m} - F_{2m-2} = 3G_m - G_{m-1}.$$

(ii) We have

$$G_{m+n} = F_{2m+2n} = F_{2m-1}F_{2n} + F_{2m}F_{2n+1} = (F_{2m} - F_{2m-2})F_{2n} + F_{2m}(F_{2n+2} - F_{2n}) =$$

$$(G_m - G_{m-1})G_n + G_m(G_{n+1} - G_n) = G_m G_{n+1} - G_{m-1}G_n.$$

(iii) Using the recurrence relation, the Fibonacci sequence can be extended to negative index:

$$\ldots, -144, 89, -55, 34, -21, 13, -8, 5, -3, 2, -1, 1, 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$$

Thus we have $F_{-m} = (-1)^{m+1}F_m$. Hence

$$G_{-m} = F_{-2m} = (-1)^{2m+1}F_{2m} = -F_{2m} = -G_m.$$

Since the formula for G_{m+n} of part (ii) was completely based on the recurrence relation, it holds for negative indices also. Therefore we have

$$G_{m-n} = G_m G_{-(n-1)} - G_{m-1}G_{-n} = G_{m-1}G_n - G_m G_{n-1}.$$

With these three formulas we can now show that (G) indeed satisfies (21). We have

$$G_{m+n}G_{m-n} = (G_m G_{n+1} - G_{m-1}G_n)(G_{m-1}G_n - G_m G_{n-1}) =$$

$$G_{m-1}G_m G_n G_{n+1} - G_m^2 G_{n-1}G_{n+1} - G_{m-1}^2 G_n^2 + G_{m-1}G_m G_{n-1}G_n.$$

Now that (i), (ii) and three (iii) have been shown, we can prove that (G) actually satisfies (21). The second term on the right-hand side in the last expression looks like half of the required result, so let us look at the first, third and fourth term. On substituting $3G_n - G_{n-1}$ for G_{n+1} we obtain

$$G_{m-1}G_m G_n G_{n+1} - G_{m-1}^2 G_n^2 + G_{m-1}G_m G_{n-1}G_n =$$

$$G_{m-1}G_m G_n(3G_n - G_{n-1}) - G_{m-1}^2 G_n^2 + G_{m-1}G_m G_{n-1}G_n =$$

$$3G_{m-1}G_m G_n^2 - G_{m-1}^2 G_n^2 = (3G_m - G_{m-1})G_{m-1}G_n^2 = G_{m+1}G_{m-1}G_n^2.$$

Hence

$$G_{m+n}G_{m-n} = G_{m+1}G_{m-1}G_n^2 - G_{n+1}G_{n-1}G_m^2. \ \Diamond$$

Example 3.11. Let a be any integer and let p be an odd prime. The *Legendre symbol* (a/p) is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \not\equiv 0 \pmod{p} \text{ and there exists an integer } x \text{ such that } x^2 \equiv a \pmod{p} \\ -1 & \text{otherwise.} \end{cases}$$

The sequence defined by $h_n = (n/3)$ is an elliptic divisibility sequence. Note that (h) is just the sequence $0, 1, -1, 0, 1, -1, 0, 1, -1, \ldots$ It is obvious that (h) is a divisibility sequence. We still have to show that $h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$. As (h) is periodic with period 3, we do this by direct computation.

$m \pmod 3$	$n \pmod 3$	h_m	h_n	h_{m+n}	h_{m-n}	h_{m+1}	h_{m-1}	h_{n+1}	h_{n-1}	$h_{m+n}h_{m-n}$	$h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$
0	0	0	0	0	0	1	−1	1	−1	0	0
0	1	0	1	1	−1	1	−1	−1	0	−1	−1
0	2	0	−1	−1	1	1	−1	0	1	−1	−1
1	0	1	0	1	1	−1	0	1	−1	1	1
1	1	1	1	−1	0	−1	0	−1	0	0	0
1	2	1	−1	0	−1	−1	0	0	1	0	0
2	0	−1	0	−1	−1	0	1	1	−1	1	1
2	1	−1	1	0	1	0	1	−1	0	0	0
2	2	−1	−1	1	0	0	1	0	1	0	0

Thus we see that (h) satisfies (21).

Note that the sequence given by the Legendre symbol (n/p) generally is not an elliptic divisibility sequence. For example, let $p = 7$ and define $u_n = (n/7)$. On taking $m = 3$ and $n = 2$, we see that $u_{m+n}u_{m-n} = u_5u_1 = -1$, whereas $u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2 = u_4u_2^3 - u_1u_3^3 = 1 - -1 = 2$. Therefore, (u) does not satisfy (21). $\Diamond$

3.3 Elementary properties of elliptic divisibility sequences

The name *elliptic divisibility sequence* comes from division polynomials on elliptic curves. We shall confine ourselves in this chapter to sequences (h) for which $h_0 = 0$ and $h_1 = 1$. If in addition neither h_2 nor h_3 vanishes, we call the sequence (h) *general*. If one or more of these restrictions is violated, (h) is called a *special* sequence. The special sequences shall be taken care of in chapter 7. It turns out that the only sequences (h) which have any arithmetical interest satisfy the following conditions:

$$h_0 = 0, \;\; h_1 = 1; \;\; \text{not both } h_2 \text{ and } h_3 \text{ zero.}$$

We call such sequences *proper*. There are three types of proper sequences: (i) general sequences, (ii) sequences with $h_2 = 0$, $h_3 \neq 0$ and (iii) sequences with $h_2 \neq 0$, $h_3 = 0$. We begin by proving the following lemma.

Lemma 3.12. Let (h) be any solution whatever of (21) with initial values $h_0 = 0$, $h_1 = 1$ and not both h_2 and h_3 zero. Then if two consecutive terms of (h) vanish, all terms of (h) vanish beyond the third.

PROOF. If two consecutive terms of (h) vanish, then two consecutive terms of smallest index vanish; let them be h_r and h_{r+1}. Then $r \geqslant 3$, and in the interval $0 < n < r$, not both h_n and h_{n+1} are zero. More than that, we claim the following:

$$h_n \neq 0 \quad \text{for} \quad 0 < n < r.$$

The claim is true for $r = 3$. Indeed, $h_1 = 1$, and $h_2 = 0$ would contradict the assumption that not both h_2 and h_3 are zero.

We may now assume that $r > 3$. We suppose that $h_n = 0$ for some $0 < n < r$ and derive that for some $k < r$, $h_k = h_{k+1} = 0$, contradicting the minimality of r. Thus, let $h_n = 0$. One has $2 \leqslant n \leqslant r-2$. Because of the minimality of r, h_{n+1} and h_{n-1} must be different from zero:

$$h_{n+1}h_{n-1} \neq 0. \tag{24}$$

We distinguish three cases: (i) $n < r/2$, (ii) $n = r/2$ and (iii) $n > r/2$.

(i) If $n < r/2$, choose k such that $k + n = r$ and take $m = k$ and $n = n$ in (21):

$$h_{k+n}h_{k-n} = h_{k+1}h_{k-1}h_n^2 - h_{n+1}h_{n-1}h_k^2. \tag{25}$$

Since $k > n$ and $n \geqslant 2$, this is a valid expression, i.e. the indices are non-negative integers. Recalling that $h_n = h_r = 0$, we obtain $-h_{n+1}h_{n-1}h_k^2 = 0$. As $h_{n+1}h_{n-1} \neq 0$, h_k must be zero. Now replace k in (25) by $k+1$:

$$h_{r+1}h_{k+1-n} = h_{k+2}h_k h_n^2 - h_{n+1}h_{n-1}h_{k+1}^2.$$

Recalling that $h_{r+1} = h_n = h_k = 0$, we obtain $-h_{n+1}h_{n-1}h_{k+1}^2 = 0$. As $h_{n+1}h_{n-1} \neq 0$, h_{k+1} must be zero. But $h_k = h_{k+1} = 0$ contradicts the minimality of r. Therefore the assumption that $h_n = 0$ for some $0 < n < r/2$ must be false.

(ii) If $n = r/2$, the preceding holds for $k = n$. We conclude that $h_{n+1} = 0$, contrary to (24).

(iii) If $n > r/2$, we can repeat part (i) by again choosing k such that $k+n = r$ but now taking $m = n$ and $n = k$ in formula (21).

Let us summarize what we have proven thusfar:

$$h_r = 0, \quad h_{r+1} = 0; \quad h_n \neq 0 \quad \text{for} \quad 0 < n < r. \tag{26}$$

We claim that $r = 3$. For if $r > 3$, $h_3 \neq 0$ by (26). Hence on taking $m+n = 2r-3$ and $m-n = 3$ in (21), i.e. $m = r$ and $n = r-3$, we obtain the relation

$$h_{2r-3}h_3 = h_{r+1}h_{r-1}h_{r-3}^2 - h_{r-2}h_{r-4}h_r^2,$$

where all the indices are $\geqslant 0$. Hence by (26), $h_{2n-3} = 0$. But by taking $n = r-2$ in (22), we see that

$$0 = h_{2r-3} = h_r h_{r-2}^3 - h_{r-3}h_{r-1}^3 = -h_{r-3}h_{r-1}^3.$$

Hence either h_{r-3} or h_{r-1} is zero, contradicting (26).

But if $r = 3$, $h_2 \neq 0$ and $h_3 = h_4 = 0$. By a brief induction from (22) and (23) we find that $h_n = 0$ for $n \geqslant 3$. This completes the proof. $\boxtimes$

We are now equipped to prove the following theorem.

Theorem 3.13. Let (h) be a proper sequence for which (21) holds. Then (h) is an EDS if and only if

$$h_2,\ h_3,\ h_4 \text{ are integers,}$$

$$h_2 \text{ divides } h_4.$$

Furthermore, the sequence (h) is uniquely determined by the three initial values h_2, h_3 and h_4.

REMARK. Although the theorem is true also for the special case $h_2 = 0$, $h_3 \neq 0$, we postpone the proof of this particular case to section 7.2. We therefore now assume $h_2 \neq 0$.

PROOF. The necessity of the conditions is evident from the definition of an EDS. For the sufficiency, assume that (h) is a proper solution of (21) for which the conditions hold. We subsequently prove, all by induction, the following claims:

(i) All terms of (h) are integers and h_2 divides h_{2n}.

(ii) (h) is a divisibility sequence.

(iii) For $n > 4$, h_n is uniquely determined if $h_0, h_1, \ldots, h_{n-1}$ are uniquely determined.

(i) The induction hypothesis reads as follows:

(I) $h_0, h_1, \ldots, h_{n-1}$ are integers;

(II) h_2 divides h_{2r} for $2r < n$; $n \geqslant 5$.

Assuming this we have to prove that h_n is an integer, and that for n even one has in addition $h_2|h_n$. If n is odd, say $n=2k+1$, we conclude from (I) and (22) with $n=k$ that h_n is an integer. If n is even, say $n=2k$, then $k\geqslant 3$ and (23) with $n=k$ gives

$$h_n h_2 = h_k\left(h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2\right). \tag{27}$$

Since $k+2<2k$ and the indices $k\pm 2$ and $k\mp 1$ are of opposite parity, $h_{k+2}h_{k-1}^2 - h_{k-2}h_{k+1}^2$ is an integer divisible by h_2. But if k is even, h_k is divisible by h_2, and if k is odd, h_{k+1}^2 and h_{k-1}^2 are divisible by h_2^2. Hence in either case the right-hand side of (27) is divisible by h_2^2, which implies that h_n is divisible by h_2.

(ii) Our induction hypothesis now reads:

$$h_r|h_s \text{ provided that } r|s \text{ for } r\leqslant s<n.$$

We observe that the hypothesis is true for $n\leqslant 5$. Hence we may assume that $n>5$. If n is a prime number, there is nothing to prove since $h_1=1|h_n$ and $h_n|h_n$ hold trivially. So let n be composite, and let $n=ab$ be a non-trivial factorization of n, i.e. $a,b\geqslant 2$. We wish to show that $h_a|h_{ab}$, whereupon the statement will follow by induction. We distinguish two cases: (III) $h_a\neq 0$ and (IV) $h_a=0$.

(III) If b is even, (23) gives, on taking $n=ab/2$,

$$h_{ab}h_2 = h_{ab/2}\left(h_{ab/2+2}h_{ab/2-1}^2 - h_{ab/2-2}h_{ab/2+1}^2\right).$$

As we've seen in part (i), the expression between parentheses is divisible by h_2. This implies that $h_{ab/2}|h_{ab}$. By hypothesis, $h_a|h_{ab/2}$, the result being that $h_a|h_{ab}=h_n$.

If b is odd, a and ab are of the same parity. Hence on taking $k+l=ab$ and $k-l=a$, i.e. $k=\frac{a(b+1)}{2}$ and $l=\frac{a(b-1)}{2}$ in (21) we obtain the relation

$$h_{ab}h_a = h_{k+1}h_{k-1}h_l^2 - h_{l+1}h_{l-1}h_k^2.$$

Since $a|k$ and $a|l$ and $k,l<n$, it follows by the induction hypothesis that the right-hand side is divisible by h_a^2. As $h_a\neq 0$, h_{ab} must be divisible by h_a.

(IV) Since $h_a=0$, $h_{a(b-1)}=0$ by the induction hypothesis. Then on taking $m=ab$ and $n=a$ in (21), we obtain

$$h_{a(b+1)}h_{a(b-1)} = h_{ab+1}h_{ab-1}h_a^2 - h_{a+1}h_{a-1}h_{ab}^2,$$

which implies $-h_{a+1}h_{a-1}h_{ab}=0$. Consequently, either $h_{ab}=0$ or $h_{a+1}h_{a-1}=0$. In the latter case two consecutive terms of (h) vanish. Then, by lemma 3.12, $h_3=h_4=\ldots=h_{ab}=0$. Hence in all cases h_a divides $h_{ab}=h_n$.

(iii) The statement follows directly from the formulas (22) and (23) by induction. ⊠

Theorem 3.14. An elliptic divisibility sequence admits every prime p a divisor. Furthermore, p has at least one rank of apparition smaller than $2p+2$.

PROOF. If none of $h_1,h_2,\ldots,h_{p+1},h_{p+2}$ is divisible by p, each of the p numbers

$$\frac{h_{r+1}h_{r-1}}{h_r^2}, \qquad (r=2,3,\ldots,p+1)$$

is congruent modulo p to one of the numbers $1,2,\ldots,p-1$. Hence at least two are congruent to one another, say

$$\frac{h_{n+1}h_{n-1}}{h_n^2} \equiv \frac{h_{m+1}h_{m-1}}{h_m^2} \equiv c \pmod{p}$$

when $2 \leqslant n < m \leqslant p+1$ and $c \in \mathbb{Z}/p\mathbb{Z}$. Consequently

$$h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \equiv 0 \pmod{p}.$$

As (h) satisfies (21), it follows that

$$h_{m+n}h_{m-n} \equiv 0 \pmod{p}.$$

Since p is prime, either $p|h_{m-n}$ or $p|h_{m+n}$. But $m-n < p+2$ and we assumed that $h_1, h_2, \ldots, h_{p+1}, h_{p+2}$ were not divisible by p. Hence p does not divide h_{m-n}, so that p divides h_{m+n}. So the smallest rank of apparition ρ of p is at most $m+n$ and hence less than or equal to $2p+1$. ⊠

REMARK. By using the theory of elliptic curves we shall improve this result in section 9.2.

Theorem 3.15. Let p be a prime divisor of an elliptic divisibility sequence (h), and let ρ be its smallest rank of apparition. Then

$$h_{\rho+1} \not\equiv 0 \pmod{p} \tag{28}$$

implies

$$h_n \equiv 0 \pmod{p} \qquad \text{if and only if} \qquad n \equiv 0 \pmod{\rho}.$$

In other words: if $h_{\rho+1}$ is not divisible by p, h_n is divisible by p precisely when n is a multiple of ρ.

PROOF. "⇐". Suppose $n \equiv 0 \pmod{\rho}$, i.e. $\rho|n$. Since (h) is a divisibility sequence, $h_\rho|h_n$. By the definition of ρ, $p|h_\rho$. Hence $p|h_n$, i.e. $h_n \equiv 0 \pmod{p}$.

"⇒". We prove the statement by mathematical induction. Assume that the implication

$$h_k \equiv 0 \pmod{p} \qquad \Rightarrow \qquad k \equiv 0 \pmod{\rho}$$

holds for $k < n$. We have to show that it holds for $k = n$ too. For that purpose, let $h_n \equiv 0 \pmod{p}$. We have to prove that $n \equiv 0 \pmod{\rho}$. Divide n by ρ and let the quotient be q and the remainder r:

$$n = q\rho + r, \qquad 0 \leqslant r < \rho.$$

We shall show that the assumption that $r > 0$ leads to a contradiction, whereupon we conclude that $n \equiv 0 \pmod{\rho}$. For that purpose, assume that $r > 0$. On taking $m = q\rho$ and $n = r$ in (21), we obtain the relation

$$h_{q\rho+r}h_{q\rho-r} = h_{q\rho+1}h_{q\rho-1}h_r^2 - h_{r+1}h_{r-1}h_{q\rho}^2.$$

Since $h_{q\rho+r} = h_n \equiv 0 \pmod{p}$ and $h_\rho|h_{q\rho}$ implies $h_{q\rho} \equiv 0 \pmod{p}$, we get the congruence

$$h_{q\rho+1}h_{q\rho-1}h_r^2 \equiv 0 \pmod{p}.$$

Since $q\rho - 1 < n$, by the induction hypothesis $h_{q\rho-1} \equiv 0 \pmod{p}$ would imply that ρ divides $q\rho - 1$, which is absurd. Hence $h_{q\rho-1} \not\equiv 0 \pmod{p}$.

By the definition of ρ,

$$h_\rho \equiv 0 \pmod{p}, \qquad h_s \not\equiv 0 \pmod{\rho}, \qquad 0 < s < \rho. \tag{29}$$

Hence $h_r \not\equiv 0 \pmod{p}$, for we assumed $r > 0$. Because p is a prime number, $\mathbb{Z}/p\mathbb{Z}$ is a domain. Hence

$$h_{q\rho+1} \equiv 0 \pmod{p}. \tag{30}$$

If $q = 1$, (28) is contradicted. If $q = 2$, then on taking $n = \rho$ in (22), we find that $h_{q\rho+1} = h_{\rho+2}h_\rho^3 - h_{\rho+1}h_{\rho-1}^3$. Hence

$$h_{\rho+1}h_{\rho-1}^3 \equiv 0 \pmod{p}.$$

So either $h_{\rho+1} \equiv 0 \pmod{p}$ or $h_{\rho-1} \equiv 0 \pmod{p}$, contradicting (28) or (29) respecively. Thus $q > 2$. Now take $m = (q-1)\rho$ and $n = \rho + 1$ in (21):

$$h_{q\rho+1}h_{(q-2)\rho-1} = h_{(q-1)\rho+1}h_{(q-1)\rho-1}h_{\rho+1}^2 - h_{\rho+2}h_\rho h_{(q-1)\rho}^2.$$

Then $m - n = (q-2)\rho - 1 > \rho - 1 > 0$. Since $h_{q\rho+1} \equiv 0 \pmod{p}$ by (30) and $h_\rho \equiv 0 \pmod{p}$, we obtain the congruence

$$h_{(q-1)\rho+1}h_{(q-1)\rho-1}h_{\rho+1}^2 \equiv 0 \pmod{p}.$$

But since $0 < (q-1)\rho - 1 < (q-1)\rho + 1 < q\rho + 1 \leqslant q\rho + r = n$, the following holds: if $h_{(q-1)\rho\pm1}$ were congruent to $0 \pmod{p}$, the induction hypothesis would imply that ρ divides $(q-1)\rho \pm 1$, which is absurd. Therefore $h_{(q-1)\rho\pm1} \not\equiv 0 \pmod{p}$, so that $h_{\rho+1} \equiv 0 \pmod{p}$. But this contradicts (28). Hence our assumption that r be greater than zero must be false, and we conclude that $r = 0$, so that $n = q\rho$, i.e. $n \equiv 0 \pmod{\rho}$. ⊠

In the previous theorem we assumed that $h_{\rho+1}$ was not divisible by p. What happens if $h_{\rho+1}$ *is* divisible by p is stated in the following theorem.

Theorem 3.16. Let p be a prime divisor of an elliptic divisibility sequence (h), and let ρ be its smallest rank of apparition. If $h_{\rho+1} \equiv 0 \pmod{p}$, then ρ is 2 or 3 and

$$h_n \equiv 0 \pmod{p}, \qquad n \geqslant \rho.$$

In other words: if $h_{\rho+1}$ is divisible by p, then ρ is either two or three and all terms h_n with $n \geqslant \rho$ are divisible by p.

PROOF. By the definition of ρ,

$$h_\rho \equiv 0 \pmod{p}, \qquad h_r \not\equiv 0 \pmod{p}, \qquad 0 < r < \rho. \tag{31}$$

We shall first show that the assumption that $\rho > 3$ leads to a contradiction. So suppose that $\rho > 3$, whence $h_3 \not\equiv 0 \pmod{p}$. On taking $m + n = 2\rho - 3$ and $m - n = 3$ in (21), i.e. $m = \rho$ and $n = \rho - 3$, we obtain the relation

$$h_{2\rho-3}h_3 = h_{\rho+1}h_{\rho-1}h_{\rho-3}^2 - h_{\rho-2}h_{\rho-4}h_\rho^2,$$

where all the indices are $\geqslant 0$ since $\rho > 3$. Thus

$$h_{2\rho-3} \equiv 0 \pmod{p}.$$

Now taking $n = \rho - 2$ in (22), we find that $h_{2\rho-3} = h_\rho h_{\rho-2}^3 - h_{\rho-3}h_{\rho-1}^3$. Hence $h_{\rho-1}h_{\rho-3}^3 \equiv 0 \pmod{p}$, which implies that either $h_{\rho-1}$ or $h_{\rho-3}$ is congruent to 0 modulo p, both cases contradicting (31). Therefore $\rho \leqslant 3$. Since $h_1 = 1$, ρ is either 2 or 3. We shall prove that in both cases $h_n \equiv 0 \pmod{p}$ for $n \geqslant \rho$.

Let $\rho = 2$. We have $h_{2n} \equiv 0 \pmod{p}$ since $h_2 | h_{2n}$ and $p | h_2$. Since $h_3 = h_{\rho+1}$ is by assumption congruent to $0 \pmod{p}$, we find that $h_5 = h_4 h_2^3 - h_1 h_3^3 \equiv 0 \pmod{p}$. That $h_{2n+1} \equiv 0 \pmod{p}$ for $n \geqslant 2$ now follows easily by induction from (22).

Let $\rho = 3$, so that $h_3 \equiv h_4 \equiv 0 \pmod{p}$. By (31), $h_2 \not\equiv 0 \pmod{p}$ and we easily prove from (22) and (23) that $h_n \equiv 0 \pmod{p}$ for $n \geqslant 3$. ⊠

Theorem 3.17. A prime p has exactly one rank of apparition in an elliptic divisibility sequence (h) if and only if p is not a common divisor of h_3 and h_4.

PROOF. "$\Rightarrow$". Let ρ be the only rank of apparition of the prime p in (h). Then ρ automatically is the smallest rank of apparition. Note that $h_{\rho+1}$ cannot be congruent to $0 \pmod{p}$. For if it were, by theorem 3.16 every prime number $\geqslant 3$ would be a rank of apparition of p, contradicting the assumption that the rank of apparition be unique. Hence $h_{\rho+1} \not\equiv 0 \pmod{p}$, so that by theorem 3.15 not both h_3 and h_4 can be divisible by p since not both 3 and 4 can be divisible by ρ. In short, p is not a common divisor of h_3 and h_4.

"$\Leftarrow$". Let p be a prime such that it is not a common divisor of h_3 and h_4. By theorem 3.14, p is a divisor of (h), and therefore we can speak of its smallest rank of apparition ρ. Again $h_{\rho+1}$ cannot be congruent to $0 \pmod{p}$, since theorem 3.16 would imply $h_3 \equiv h_4 \equiv 0 \pmod{p}$, contradicting the assumption that p be not a common divisor of h_3 and h_4. Therefore $h_{\rho+1} \not\equiv 0 \pmod{p}$, and by theorem 3.15 it now follows that if p divides h_n, n is of the form $k\rho$ for some $k \geqslant 1$. Now unless $k = 1$, $k\rho$ is not a rank of apparition. Hence, ρ is the only rank of apparition of p. $\boxtimes$

The theorem directly yields the following corollary.

Corollary 3.18. Every prime p has precisely one rank of apparition in an elliptic sequence (h) if and only if h_3 and h_4 have no common factor.

The following theorem now follows from theorem 3.17 and theorem 3.6.

Theorem 3.19. If (h) is an elliptic divisibility sequence in which the initial values h_3 and h_4 are coprime, then $(h_m, h_n) = h_{(m,n)}$ for all indices m, n.

PROOF. Note first that we can restate theorems 3.14, 3.15, 3.16 and 3.17 with the prime p replaced by the arbitrary prime power p^k. Indeed, the only fact depending on p we used in the proofs of these theorems was that $\mathbb{Z}/p\mathbb{Z}$ has no divisors of zero. Since $\mathbb{Z}/p^k\mathbb{Z}$ has the same property, the theorems must hold with p replaced by p^k also.

Now assume that h_3 and h_4 are coprime and let p^k be any prime power. Then p^k cannot be a common divisor of h_3 and h_4. By the adjusted version of theorem 3.17 we now see that p^k has exactly one rank of apparition. Since p^k was arbitrarily chosen, we see that part (ii) of theorem 3.6 is fulfilled. Hence $(h_m, h_n) = h_{(m,n)}$. $\boxtimes$

Definition 3.20. A divisibility sequence (h) for which $(h_m, h_n) = h_{(m,n)}$ for all $m, n \geqslant 1$ is said to be a *strong* divisibility sequence.

Corollary 3.21. The Fibonacci sequence (F) and the sequence (G) from example 3.10 are both strong divisibility sequences.

PROOF. The initial values $F_3 = 2$ and $F_4 = 3$ are coprime, so that it follows from theorem 3.19 that (F) is a strong divisibility sequence. As (G) is a subsequence of (F), it must be a strong divisibility sequence also. $\boxtimes$

4 The representation of elliptic sequences by elliptic functions

4.1 The fundamental elliptic representation theorem

Consider a general elliptic divisibility sequence (h), so that $h_2h_3 \neq 0$. We shall devote this section to the proof of the following fundamental theorem which states that any general elliptic divisibility sequence has an elliptic function representation.

Theorem 4.1. (Fundamental elliptic representation theorem) If (h) is a general elliptic divisibility sequence, there exist two rational numbers g_2 and g_3 and a complex constant u such that if $\wp(z;\, g_2, g_3)$ is the Weierstraß function with invariants g_2 and g_3, then

$$h_n = \psi_n(u), \tag{32}$$

where $\psi_n(z)$ is the elliptic function defined in section 2.1.

PROOF. Let (h) be a general elliptic divisibility sequence. Since by theorem 2.3 $\psi_n(z)$ is always a solution of (21) and $\psi_0(z) = 0$ and $\psi_1(z) = 1$, it suffices to show that we can determine g_2, g_3 and u such that:

$$\text{(i)} \quad \psi_2(u) = h_2, \quad \text{(ii)} \quad \psi_3(u) = h_3 \quad \text{and} \quad \text{(iii)} \quad \psi_4(u) = h_4.$$

In order to prove these three claims we recall from chapter 1 and section 2.2 seven formulas from elliptic function theory:

$$\psi_2(z) = -\wp'(z), \tag{33}$$

$$\psi_3(z) = 3\wp(z)^4 - \tfrac{3}{2}g_2\wp(z)^2 - 3g_3\wp(z) - \tfrac{1}{16}g_2^2, \tag{34}$$

$$\wp(2z) - \wp(z) = -3\wp(z) + \tfrac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2, \tag{35}$$

$$\wp(2z) - \wp(z) = -\frac{\psi_1(z)\psi_3(z)}{\psi_2(z)^2}, \tag{36}$$

$$\wp(3z) - \wp(z) = -\frac{\psi_2(z)\psi_4(z)}{\psi_3(z)^2}, \tag{37}$$

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \tag{38}$$

$$\wp''(z) = 6\wp(z)^2 - \tfrac{1}{2}g_2. \tag{39}$$

For the proof of the three claims we shall need three more formulas which we derive in situ. Formula (39) directly yields that

$$g_2 = 12\wp(z)^2 - 2\wp''(z). \tag{40}$$

Now it follows from (38) that

$$g_3 = 2\wp(z)\left[\wp''(z) - 4\wp(z)^2\right] - \wp'(z)^2. \tag{41}$$

Indeed, we have

$$g_3 = 4\wp(z)^3 - g_2\wp(z) - \wp'(z)^2 = 4\wp(z)^3 - \left[12\wp(z)^2 - 2\wp''(z)\right]\wp(z) - \wp'(z)^2 =$$

$$2\wp(z)\wp''(z) - 8\wp(z)^3 - \wp'(z)^2 = 2\wp(z)\left[\wp''(z) - 4\wp(z)^2\right] - \wp'(z)^2.$$

The last formula we shall need is:

$$\wp(3z) - \wp(z) = \frac{\wp'(z)^2\left[\wp'(z)^4 - \psi_3(z)\wp''(z)\right]}{\psi_3(z)^2}. \tag{42}$$

From (33), (37) and the identity $\psi_4(z) = \wp'(z)P_4$ it follows that

$$\wp(3z) - \wp(z) = \frac{\wp'(z)^2 P_4}{\psi_3(z)^2}.$$

Thus it remains for us to show that $P_4 = \wp'(z)^4 - \psi_3(z)\wp''(z)$, an expression we can write out by means of (38), (14) and (39):

$$\wp'(z)^4 - \psi_3(z)\wp''(z) =$$

$$\left[4\wp(z)^3 - g_2\wp(z) - g_3\right]^2 - \left[3\wp(z)^4 - \tfrac{3}{2}g_2\wp(z)^2 - 3g_3\wp(z) - \tfrac{1}{16}g_2^2\right]\left[6\wp(z)^2 - \tfrac{1}{2}g_2\right] =$$

$$\left[16\wp(z)^6 - 8g_2\wp(z)^4 - 8g_3\wp(z)^3 + g_2^2\wp(z)^2 + 2g_2g_3\wp(z) + g_3^2\right] -$$

$$\left[18\wp(z)^6 - \tfrac{3}{2}g_2\wp(z)^4 - 9g_2\wp(z)^4 + \tfrac{3}{4}g_2^2\wp(z)^2 - 18g_3\wp(z)^3 + \tfrac{3}{2}g_2g_3\wp(z) - \tfrac{3}{8}g_2^2\wp(z)^2 + \tfrac{1}{32}g_2^3\right] =$$

$$-2\wp(z)^6 + \tfrac{5}{2}g_2\wp(z)^4 + 10g_3\wp(z)^3 + \tfrac{5}{8}g_2^2\wp(z)^2 + \tfrac{1}{2}g_2g_3\wp(z) + g_3^2 - \tfrac{1}{32}g_2^3,$$

which last expression is precisely P_4 by (15). We can now pass on to proving the three claims.

PROOF OF THE THREE CLAIMS. The character of the proof is rather remarkable. First we *assume* the claims to be true and derive from them a certain result. Then we turn things around and take the result as the starting point from which we shall derive the three claims.

So assume (i), (ii) and (iii) hold. Then since $\psi_1(z) = 1$, formulas (32), (33), (36) and (37) give:

$$\wp'(u) = -h_2, \tag{43}$$

$$\wp(2u) - \wp(u) = -\frac{h_3}{h_2^2}, \tag{44}$$

$$\wp(3u) - \wp(u) = -\frac{h_2h_4}{h_3^2}. \tag{45}$$

Now by (42), (45) and (43):

$$-\frac{h_2h_4}{h_3^2} = \frac{h_2^2\left[h_2^4 - h_3\wp''(u)\right]}{h_3^2}.$$

Hence solving for $\wp''(u)$:

$$\wp''(u) = \frac{h_2^5 + h_4}{h_2h_3}. \tag{46}$$

Next, using (44), (35) and (43), (46):

$$-\frac{h_3}{h_2^2} = \tfrac{1}{4}\left(\frac{\wp''(u)}{\wp'(u)}\right)^2 - 3\wp(u) = \tfrac{1}{4}\left(\frac{h_2^5 + h_4}{-h_2^2h_3}\right)^2 - 3\wp(u) =$$

$$\frac{h_2^{10}+2h_2^5h_4+h_4^2}{4h_2^4h_3^2}-3\wp(u).$$

Hence solving for $\wp(u)$:

$$\wp(u)=\frac{h_2^{10}+2h_2^5h_4+4h_2^2h_3^3+h_4^2}{12h_2^4h_3^2}. \tag{47}$$

Next, using (40), (47) and (46):

$$g_2=12\wp(u)^2-2\wp''(u)=$$

$$12\left(\frac{h_2^{10}+2h_2^5h_4+4h_2^2h_3^3+h_4^2}{12h_2^4h_3^2}\right)^2-2\frac{h_2^5+h_4}{h_2h_3}=$$

$$\frac{h_2^{20}+4h_2^{15}h_4+2h_2^{10}h_4^2+8h_2^{12}h_3^3+4h_2^{10}h_4^2+4h_2^5h_4^3+16h_2^7h_3^3h_4+h_4^4+8h_2^2h_3^3h_4^2+16h_2^4h_3^6}{12h_2^8h_3^4}$$

$$-\frac{24h_2^{12}h_3^3+24h_2^7h_3^3h_4}{12h_2^8h_3^4},$$

so that

$$g_2=\frac{h_2^{20}+4h_2^{15}h_4-16h_2^{12}h_3^3+6h_2^{10}h_4^2-8h_2^7h_3^3h_4+4h_2^5h_4^3+16h_2^4h_3^6+8h_2^2h_3^3h_4^2+h_4^4}{12h_2^8h_3^4}. \tag{48}$$

We would like to find a similar formula for g_3. To this end, let us first write out the expression between brackets in (41), making use of (46) and (47):

$$\wp''(u)-4\wp(u)^2=\frac{h_2^5+h_4}{h_2h_3}-4\left(\frac{h_2^{10}+2h_2^5h_4+4h_2^2h_3^3+h_4^2}{12h_2^4h_3^2}\right)^2=$$

$$\frac{36h_2^{12}h_3^3+36h_2^7h_3^3h_4}{36h_2^8h_3^4}-\frac{h_2^{20}+4h_2^{15}h_4+8h_2^{12}h_3^3+6h_2^{10}h_4^2+16h_2^7h_3^3h_4+4h_2^5h_4^3+16h_2^4h_3^6+8h_2^2h_3^3h_4^4+h_4^4}{36h_2^8h_3^4}=$$

$$\frac{-h_2^{20}-4h_2^{15}h_4+28h_2^{12}h_3^3-6h_2^{10}h_4^2+20h_2^7h_3^3h_4-4h_2^5h_4^3-16h_2^4h_3^6-8h_2^2h_3^3h_4^4-h_4^4}{36h_2^8h_3^4}.$$

This gives

$$2\wp(u)\left[\wp''(u)-4\wp(u)^2\right]=$$

$$2\left(\tfrac{h_2^{10}+2h_2^5h_4+4h_2^2h_3^3+h_4^2}{12h_2^4h_3^2}\right)\left(\tfrac{-h_2^{20}-4h_2^{15}h_4+28h_2^{12}h_3^3-6h_2^{10}h_4^2+20h_2^7h_3^3h_4-4h_2^5h_4^3-16h_2^4h_3^6-8h_2^2h_3^3h_4^4-h_4^4}{36h_2^8h_3^4}\right)=$$

$$\{-h_2^{30}-6h_2^{25}h_4+24h_2^{22}h_3^3-15h_2^{20}h_4^2+60h_2^{17}h_3^3h_4-20h_2^{15}h_4^3+96h_2^{14}h_3^6+36h_2^{12}h_3^3h_4^2$$
$$-15h_2^{10}h_4^4+48h_2^9h_3^6h_4-12h_2^7h_3^3h_4^3-64h_2^6h_3^9-6h_2^5h_4^5-48h_2^4h_3^6h_4^2-12h_2^2h_3^3h_4^4-h_4^6\}\div\{216h_2^{12}h_3^6\}.$$

Subtracting from this expression $\wp'(u)^2=h_2^2=216h_2^{14}h_3^6/216h_2^{12}h_3^6$ we obtain the following formula for g_3:

$$g_3=\{-h_2^{30}-6h_2^{25}h_4+24h_2^{22}h_3^3-15h_2^{20}h_4^2+60h_2^{17}h_3^3h_4-20h_2^{15}h_4^3-120h_2^{14}h_3^6+36h_2^{12}h_3^3h_4^2 \tag{49}$$
$$-15h_2^{10}h_4^4+48h_2^9h_3^6h_4-12h_2^7h_3^3h_4^3-64h_2^6h_3^9-6h_2^5h_4^5-48h_2^4h_3^6h_4^2-12h_2^2h_3^3h_4^4-h_4^6\}\div\{216h_2^{12}h_3^6\}.$$

Now we can turn things around. (47), (48) and (49) are *necessary* conditions that the equations (i), (ii) and (iii) hold. Now since neither h_2 nor h_3 is zero, we can start by taking (48), (49) and (47) as *definitions* for g_2, g_3 and u respectively. Then u is determined save for sign up to a period of $\wp(z)$. On combining (47) and (48) we find that

$$g_2 - 12\wp(u)^2 = -2\frac{h_2^5 + h_4}{h_2 h_3},$$

whence (46) follows from (40).

Now combining (49) with (47), (46) and (48), we obtain the formula

$$g_3 - 2\wp(u)\left[\wp''(u) - 4\wp(u)^2\right] = -h_2^2.$$

Hence by formula (41), $\wp'(u)^2 = h_2^2$. Since the $\wp$-function is an odd function, we can now choose the sign of u such that (43) is satisfied. u is now fixed up to a period of the $\wp$-function. But then (i) follows immediately from formula (33).

Next, using (35) and substituting in it for $\wp'(u)$, $\wp''(u)$ and $\wp(u)$ the expressions from (43), (46) and (47), we find that $\wp(2u) - \wp(u) = -h_3/h_2^2$. Hence (ii) follows from (36), (i) and the fact that $\psi_1(u) = 1$.

Finally, on replacing on the right of (42) the expressions $\wp'(u)$, $\wp''(u)$ and $\psi_3(u)$ with the expressions from (43), (46) and (ii) respectively, we find that $\wp(3u) - \wp(u) = -h_2 h_4/h_3^2$. Hence (iii) follows from (37) and (i),(ii). ⊠

4.2 Symmetry in the distribution of residues of the first ρ terms of (h)

If we calculate successively the least positive residues modulo p of the first ρ terms of (h), a certain symmetry emerges in the distribution of these residues. We shall devote this section to the proof of this fact, stated in theorem 4.8. First of all we recall some facts about the function $\psi_n(z)$ and prove six lemmas needed in the proof of theorem 4.8.

By theorem 4.1 there exist rational numbers g_2 and g_3 and a complex constant u such that

$$h_n = \psi_n(u). \tag{50}$$

Moreover, by theorem 2.7 we have the formula

$$\psi_n(z) = \frac{\sigma(nz)}{\sigma(z)^{n^2}}. \tag{51}$$

In the proof of theorem 4.1 we found rational expressions for $\wp(u)$, g_2 and g_3, whose denominators were $2^2 3 h_2^4 h_3^2$, $2^2 3 h_2^8 h_3^4$ and $2^3 3^3 h_2^{12} h_3^8$ respectively. Since p is assumed to be greater than three and neither a divisor of h_2 nor h_3, the numbers $\wp(u)$, g_2 and g_3 are *integers* when considered modulo p.

In section 2.1 we saw that, writing $\wp(z) = w$, the function $\psi_n(z)$ may be expressed as a polynomial in w in case n is odd and as $\wp'(z)$ times a polynomial in w in case n is even:

$$\psi_n(z) = d_n P_n(w) = d_n \sum_{k=0}^{q} A_k w^k, \tag{52}$$

where the degree $q = q(n)$ of $P_n(w)$ in w is $\frac{n^2-1}{2}$ or $\frac{n^2-4}{2}$, and d_n is 1 or $\wp'(z)$ according as n is odd or even. By corollary 2.6 each coefficient $A_k = A_k(n)$ is an element of $\mathbb{Z}[\frac{g_2}{4}, g_3]$. By the above we always have $\psi_n(z) \in \mathbb{Z}[\wp(z), \wp'(z), \frac{g_2}{4}, g_3]$. Now let us take $z = u$. Since $\wp'(u) = -h_2 \in \mathbb{Z}$, and since $\wp(u)$,

$\frac{g_2}{4}$ and g_3 are rational numbers whose denominators only contain the factors 2, 3, h_2 and h_3, we may conclude that $\psi_n(u)$ is congruent to an integer modulo p.

It follows directly from the definition of $\psi_n(z)$ that the $q(n)$ roots $\zeta_1, \zeta_2, \ldots, \zeta_{q(n)}$ of $F_n(w)$ are of the form $\zeta_k = \wp\left(\frac{\omega}{n}\right)$ $(1 \leqslant k \leqslant q(n))$, where ω is some period of $\wp(z;\, g_2, g_3)$ of the form $\omega = \nu_1\omega_1 + \nu_2\omega_2$ with $(\nu_1, \nu_2) \in (\mathbb{Z}/n\mathbb{Z})^2 \backslash \{(0,0)\}$.

We conclude our build-up to theorem 4.8 with six lemmas.

Lemma 4.2. Let P_n be the polynomial in $\wp(z)$ defined in section 2.1. For all $n \geqslant 1$, each coefficient of P_n contains g_2 or g_3 as a factor, save possibly the coefficient of the highest term of P_n. Consequently, if p is an odd prime such that $g_2 \equiv g_3 \equiv 0 \pmod{p}$, then $P_n \equiv H(P_n) \pmod{p}$, where $H(P_n)$ is the highest term of P_n.

PROOF. We prove the result by induction on n. For $n = 1,2,3,4$ the result follows from the explicit expressions for P_1, P_2, P_3 and P_4 derived in section 2.2.

Now assume the result to be true for all $n < m$, where m is some fixed integer greater than four. First let m be odd, say $m = 2k+1$. By corollary 2.5 we have:

$$P_{2k+1} = \begin{cases} \wp'(z)^4 P_{k+2} P_k^3 - P_{k-1} P_{k+1}^3 & \text{if } k \text{ is even,} \\ P_{k+2} P_k^3 - \wp'(z)^4 P_{k-1} P_{k+1}^3 & \text{if } k \text{ is odd.} \end{cases}$$

Suppose that k is even. Then by the induction hypothesis, the only possible terms *without* g_2 or g_3 as a factor are $H\left(\wp'(z)^4 P_{k+2} P_k^3\right)$ and $H\left(P_{k-1} P_{k+1}^3\right)$. But we will now see that they are of the same degree and their difference equals $H(P_{2k+1})$. On using (10) and the identity $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, it follows that

$$H\left(\wp'(z)^4 P_{k+2} P_k^3\right) = 16\wp(z)^6 \left(-\tfrac{k+2}{2}\wp(z)^{\frac{(k+2)^2-4}{2}}\right)\left(-\tfrac{k}{2}\wp(z)^{\frac{k^2-4}{2}}\right)^3 =$$

$$(k^4+2k^3)\wp(z)^{6+\frac{k^2+4k}{2}+\frac{3k^2-12}{2}} = (k^4+2k^3)\wp(z)^{2k^2+2k}.$$

Furthermore,

$$H\left(P_{k-1}P_{k+1}^3\right) = (k-1)\wp(z)^{\frac{(k-1)^2-1}{2}}\left((k+1)\wp(z)^{\frac{(k+1)^2-1}{2}}\right)^3 = (k-1)(k+1)^3\wp(z)^{\frac{k^2-2k}{2}+\frac{3k^2+6k}{2}} =$$

$$(k^4+2k^3-2k-1)\wp(z)^{2k^2+2k}.$$

Therefore, $H\left(\wp'(z)^4 P_{k+2} P_k^3\right) - H\left(P_{k-1}P_{k+1}^3\right) = (2k+1)\wp(z)^{2k^2+2k} = (2k+1)\wp(z)^{\frac{(2k+1)^2-1}{2}} = H(P_{2k+1})$. Hence, the only possible term of P_{2k+1} without a factor g_2 or g_3 is $H(P_{2k+1})$, as was to be shown. If k is odd, the exact same result follows from an analogous computation.

Now let m be even, say $m = 2k$. By corollary 2.5 we have

$$P_{2k} = P_k P_{k-2} P_{k+1}^2 - P_k P_{k+2} P_{k-1}^2.$$

Suppose first that k is odd. By the induction hypothesis, the only possible terms *without* g_2 or g_3 as a factor are $H\left(P_k P_{k-2} P_{k+1}^2\right)$ and $H\left(P_k P_{k+2} P_{k-1}^2\right)$. We will see that they are of the same degree and their difference equals $H(P_{2k})$. Indeed,

$$H\left(P_k P_{k-2} P_{k+1}^2\right) = k\wp(z)^{\frac{k^2-1}{2}}(k-2)\wp(z)^{\frac{(k-2)^2-1}{2}}\left(-\tfrac{k+1}{2}\wp(z)^{\frac{(k+1)^2-4}{2}}\right)^2 =$$

$$\frac{k(k-2)(k+1)^2}{4}\wp(z)^{\frac{k^2-1}{2}+\frac{k^2-4k+3}{2}+\frac{2k^2+4k-6}{2}} = \frac{k^4-3k^2-2k}{4}\wp(z)^{2k^2-2}.$$

Furthermore,

$$H\left(P_kP_{k+2}P_{k-1}^2\right) = k\wp(z)^{\frac{k^2-1}{2}}(k+2)\wp(z)^{\frac{(k+2)^2-1}{2}}\left(-\frac{k-1}{2}\wp(z)^{\frac{(k-1)^2-4}{2}}\right)^2 =$$

$$\frac{k(k+2)(k-1)}{4}\wp(z)^{\frac{k^2-1}{2}+\frac{k^2+4k+3}{2}+\frac{2k^2-4k-6}{2}} = \frac{k^4-3k^2+2k}{4}\wp(z)^{2k^2-2}.$$

Therefore, $H\left(P_kP_{k-2}P_{k+1}^2\right) - H\left(P_kP_{k+2}P_{k-1}^2\right) = -k\wp(z)^{2k^2-2} = -k\wp(z)^{\frac{(2k)^2-4}{2}} = H(P_{2k})$. Hence, the only possible term of P_{2k} without a factor g_2 or g_3 is $H(P_{2k})$. For k even the same result follows from an analogous computation.

Summarizing, we have assumed that the assertion holds for all $n < m$ for some fixed m and derived from this the validity of the assertion for the case $n = m$. This concludes the induction. ⊠

Lemma 4.3. Let p be a prime greater than three which does not divide h_2 nor h_3 and let the rank of apparition ρ be equal to p or $2p$. Then p divides every coefficient of P_ρ if and only if p divides both g_2 and g_3.

PROOF. "⇐". By lemma 4.2, all coefficients of P_ρ, save possibly the one corresponding to the highest power of $\wp(z)$, contain g_2 or g_3 as a factor, and hence are divisible by p. If $\rho = p$, $H(P_\rho) = p\wp(z)^{(p^2-1)/2}$. If $\rho = 2p$, $H(P_\rho) = -p\wp(z)^{2p^2-2}$. In any case, also the coefficient of the highest term of P_ρ is divisible by p.

"⇒". Let $\rho = p$. Assume that p divides every coefficient of P_p. Since p is odd, we have $q(p) = (p^2-1)/2$. We thus have

$$A_k \equiv 0 \pmod{p}, \qquad k = 0, 1, \cdots, (p^2-1)/2.$$

Let $\mathcal{S}$ denote the Galois field obtained by adjoining to the field of rationals the three roots e_1, e_2, e_3 of $4x^3 - g_2x - g_3 = 0$. Then with the usual notation, $e_i = \wp\left(\frac{\omega_i}{2}\right)$ $(i = 1, 2, 3)$ where ω_1 and ω_2 are the fundamental periods of the lattice corresponding to the function $\wp(z;\ g_2, g_3)$, and $\omega_3 = \omega_1 + \omega_2$. As four times the sum of the roots equals minus the coefficient of the quadratic term, which is zero, one has $e_1 + e_2 + e_3 = 0$. As $p \neq 2$ and g_2 and g_3 are rational integers modulo p, we see that modulo p the e_i are algebraic integers.

Now let $\mathfrak{p}$ be any prime ideal divisor of p in $\mathcal{S}$. By (52) and our hypothesis that p divide the A_k we have

$$\psi_p\left(\tfrac{\omega_i}{2}\right) = \sum_{k=0}^{(p^2-1)/2} A_k\wp\left(\tfrac{\omega_i}{2}\right)^k = \sum_{k=0}^{(p^2-1)/2} A_k e_i^k \equiv 0 \pmod{p}.$$

By (51) it follows that

$$\frac{\sigma(p\omega_i/2)}{\sigma(\omega_i/2)^{p^2}} = \psi_p\left(\tfrac{\omega_i}{2}\right) \equiv 0 \pmod{p}. \tag{53}$$

For the sake of typography, write $\gamma_i = \omega_i/2$. Note that $p\gamma_i = \gamma_i + \frac{p-1}{2}\cdot 2\gamma_i = \gamma_i + \frac{p-1}{2}\cdot\omega_i$. Because $\frac{p-1}{2} \in \mathbb{Z}$ we may now use the quasi-periodicity of the sigma function:

$$\sigma(p\gamma_i) = \sigma\left(\gamma_i + \tfrac{p-1}{2}\cdot\omega_i\right) = \delta\left(\tfrac{p-1}{2}\cdot\omega_i\right)e^{\eta\left((p-1)\gamma_i\right)\left[\gamma_i + \frac{p-1}{2}\cdot\gamma_i\right]}\sigma(\gamma_i) =$$

$$(-1)^{\frac{p-1}{2}}e^{(p-1)\cdot\eta(\gamma_i)\cdot(p+1)\gamma_i/2}\sigma(\gamma_i) = (-1)^{\frac{p-1}{2}}e^{(p^2-1)\gamma_i\eta(\gamma_i)/2}\sigma(\gamma_i). \tag{54}$$

By (4), the fact that $\sigma(z)$ is an odd function and the identity $\gamma_1+\gamma_2=\gamma_3$ we derive that

$$(e_1-e_2)(e_1-e_3)=\Big(\wp(\gamma_1)-\wp(\gamma_2)\Big)\Big(\wp(\gamma_1)-\wp(\gamma_3)\Big)=$$

$$\left(-\frac{\sigma(\gamma_1+\gamma_2)\sigma(\gamma_1-\gamma_2)}{\sigma(\gamma_1)^2\sigma(\gamma_2)^2}\right)\left(-\frac{\sigma(\gamma_1+\gamma_3)\sigma(\gamma_1-\gamma_3)}{\sigma(\gamma_1)^2\sigma(\gamma_3)^2}\right)=\frac{\sigma(\gamma_3)\sigma(-\gamma_3+2\gamma_1)\sigma(\gamma_2+2\gamma_1)\sigma(-\gamma_2)}{\sigma(\gamma_1)^4\sigma(\gamma_2)^2\sigma(\gamma_3)^2}=$$

$$\frac{\sigma(\gamma_3-2\gamma_1)}{\sigma(\gamma_3)}\cdot\frac{\sigma(\gamma_2+2\gamma_1)}{\sigma(\gamma_2)}\cdot\frac{1}{\sigma(\gamma_1)^4}=\frac{\sigma(\gamma_3-\omega_1)}{\sigma(\gamma_3)}\cdot\frac{\sigma(\gamma_2+\omega_1)}{\sigma(\gamma_2)}\cdot\frac{1}{\sigma(\gamma_1)^4}.$$

By the quasi-periodicity of $\sigma(z)$ this last expression equals

$$\delta(-\omega_1)e^{\eta(-\omega_1)[\gamma_3-\omega_1/2]}\cdot\delta(\omega_1)e^{\eta(\omega_1)[\gamma_2+\omega_1/2]}\cdot\frac{1}{\sigma(\gamma_1)^4}=$$

$$\delta(\omega_1)^2e^{-\eta(\omega_1)[\gamma_3-\omega_1/2]+\eta(\omega_1)[\gamma_2+\omega_1/2]}\frac{1}{\sigma(\gamma_1)^4}=e^{\eta(\omega_1)[-\gamma_3+\gamma_2+2\gamma_1]}\frac{1}{\sigma(\gamma_1)^4}=$$

$$e^{\gamma_1\eta(\omega_1)}\cdot\frac{1}{\sigma(\gamma_1)^4}=e^{2\gamma_1\eta(\gamma_1)}\frac{1}{\sigma(\gamma_1)^4}.$$

All in all we have derived that

$$(e_1-e_2)(e_1-e_3)=e^{2\gamma_1\eta(\gamma_1)}\frac{1}{\sigma(\gamma_1)^4},$$

whence

$$e^{\gamma_1\eta(\gamma_1)/2}=(e_1-e_2)^{1/4}(e_1-e_3)^{1/4}\sigma(\gamma_i).$$

Therefore with (54) it follows that

$$\sigma(p\gamma_i)=(-1)^{\frac{p-1}{2}}\left(e^{\gamma_1\eta(\gamma_1)/2}\right)^{p^2-1}\sigma(\gamma_i)=(-1)^{\frac{p-1}{2}}(e_1-e_2)^{\frac{p^2-1}{4}}(e_1-e_3)^{\frac{p^2-1}{4}}\sigma(\gamma_i)^{p^2}.$$

Thus

$$\psi_p(\gamma_i)=(-1)^{\frac{p-1}{2}}(e_1-e_2)^{\frac{p^2-1}{4}}(e_1-e_3)^{\frac{p^2-1}{4}}.$$

By the virtue of (53) we have in $\mathcal{S}$ the congruence

$$(-1)^{\frac{p-1}{2}}(e_1-e_2)^{\frac{p^2-1}{4}}(e_1-e_3)^{\frac{p^2-1}{4}}\equiv 0 \pmod{\mathfrak{p}}.$$

Since $\mathfrak{p}$ is a prime ideal, we deduce that $e_1\equiv e_2\equiv e_3 \pmod{\mathfrak{p}}$. But then for every algebraic integer $\xi\in\mathcal{S}$ we have

$$4\xi^3-g_2\xi-g_3=4(\xi-e_1)(\xi-e_2)(\xi-e_3)\equiv 4(\xi-e_1)^3\equiv 4\xi^3-12e_1\xi^2+12e_1^2\xi-4e_1^3 \pmod{\mathfrak{p}},$$

so that $12e_1\equiv 0 \pmod{\mathfrak{p}}$. Since p is not equal to two or three, we must have $e_1\equiv 0 \pmod{\mathfrak{p}}$. This implies that $4\xi^3-g_2\xi-g_3\equiv 4\xi^3 \pmod{\mathfrak{p}}$, whereupon we conclude that $g_2\equiv g_3\equiv 0 \pmod{\mathfrak{p}}$. Since g_2 and g_3 are rational integers modulo p, it follows that $g_2\equiv g_3\equiv 0 \pmod{p}$. This concludes the proof in case $\rho=p$.

The proof for the case $\rho=2p$ is similar and will be omitted here. ☒

We develop some simple arithmetical concepts which are needed in the proofs that follow. Let $\mathfrak{p}$ be a prime ideal of an algebraic number field, and α any field element. Then the principal ideal (α) has a unique representation of the form $(\alpha)=\mathfrak{p}^{-r}\mathfrak{b}\mathfrak{c}^{-1}$ where $\mathfrak{b}$ and $\mathfrak{c}$ are integral ideals which are coprime and also prime to $\mathfrak{p}$, and the exponent r is a rational integer. We call r the *index of* α *modulo* $\mathfrak{p}$ and write $I(\alpha)$ for the index of α. The number α is said to be *integral* modulo $\mathfrak{p}$ if and only if its index is negative or zero, and *fractional* if and only if its index is positive.

Lemma 4.4. If α and β are integers modulo $\mathfrak{p}$, then so are $\alpha \pm \beta$ and $\alpha\beta$.

Lemma 4.5. If α is a fraction modulo $\mathfrak{p}$ and β is an integer modulo $\mathfrak{p}$, $\alpha \pm \beta$ is a fraction modulo $\mathfrak{p}$ with the same index as α: $I(\alpha \pm \beta) = I(\alpha) \pm I(\beta)$. Moreover, the index of $\alpha\beta$ is not greater than that of α: $I(\alpha\beta) \leqslant I(\alpha)$.

Lemma 4.6. If $\alpha_1, \alpha_2, \ldots, \alpha_k$ are fractions modulo $\mathfrak{p}$, the index of their product is the sum of the indices of the separate factors.

Lemma 4.7. If $\alpha_1, \alpha_2, \ldots, \alpha_k$ are fractions modulo $\mathfrak{p}$, the index of $(\varepsilon - \alpha_1)(\varepsilon - \alpha_2)\cdots(\varepsilon - \alpha_k)$ is the same for all ε which are integers modulo $\mathfrak{p}$, and equals the sum of the indices of $\alpha_1, \alpha_2, \ldots, \alpha_k$.

We are now ready to state and prove the aforesaid theorem.

Theorem 4.8. Let p be a prime greater than three, which divides neither h_2 nor h_3. Then if ρ is its rank of apparition, there exist two integers a and b such that

$$h_{\rho - n} \equiv a^n b h_n \pmod{p}, \qquad n = 0, 1, 2, \ldots, \rho. \tag{55}$$

PROOF. Let $\mathcal{R}$ denote the algebraic number field obtained by adjoining all the roots $\zeta_1, \zeta_2 \ldots, \zeta_{q(\rho)}$ of $F_\rho(w)$ to the field $\mathbb{Q}$, i.e. $\mathcal{R} = \mathbb{Q}(\zeta_1, \zeta_2, \ldots, \zeta_{q(\rho)})$. Furthermore, let $\mathfrak{p}$ denote any prime ideal divisor of p in $\mathcal{R}$. By theorem 3.14 we have $\rho \leqslant 2p+2$. We distinguish the cases (i) ρ is prime to p, (ii) $\rho = p$ or $\rho = 2p$ and p divides both g_2 and g_3 and (iii) $\rho = p$ or $\rho = 2p$ and p does not divide both g_2 and g_3. We treat these cases separately.

(i) Let us assume that $(\rho, p) = 1$. Because $F_\rho(w)$ has roots $\zeta_1, \zeta_2, \ldots, \zeta_{q(\rho)}$, in $\mathbb{C}$ it has factorization

$$d_\rho F_\rho(w) = d_\rho F_\rho(\wp(z)) = \kappa_\rho(z) \prod_{k=1}^{q(\rho)} (\wp(z) - \zeta_k),$$

where $\kappa_\rho(z) = \rho$ if ρ is odd and $\kappa_\rho(z) = -\rho\wp'(z)/2$ if ρ is even. On taking $z = u$ we obtain

$$d_\rho F_\rho(\wp(u)) = c_\rho \prod_{k=1}^{q(\rho)} (\wp(u) - \zeta_k),$$

where $c_\rho = \kappa_\rho(u) = \rho$ if ρ is odd and $c_\rho = -\rho\wp'(u)/2 = \rho h_2/2$ if ρ is even. As $h_\rho = \psi_\rho(u) = d_\rho F_\rho(\wp(u))$ we have the congruence

$$h_\rho \equiv c_\rho \prod_{k=1}^{q(\rho)} (\wp(u) - \zeta_k) \pmod{p}.$$

But by the definition of ρ, $h_\rho \equiv 0 \pmod{p}$. Moreover, whether ρ be even or odd, c_ρ is an integer prime to p since p does not divide h_2 nor ρ. Therefore we have the congruence

$$\prod_{k=1}^{q(\rho)} (\wp(u) - \zeta_k) \equiv 0 \pmod{p}.$$

Hence in $\mathcal{R}$ we have the congruence

$$\prod_{k=1}^{q(\rho)} (\wp(u) - \zeta_k) \equiv 0 \pmod{\mathfrak{p}}.$$

Since $\mathfrak{p}$ is a prime ideal, $\mathcal{R}/\mathfrak{p}$ is a domain and therefore cannot contain divisors of zero. As a consequence, there exists $1 \leqslant k \leqslant q(\rho)$ such that $\wp(u) \equiv \zeta_k \pmod{\mathfrak{p}}$. Since $\zeta_k = \wp\left(\frac{\omega}{\rho}\right)$ for some period ω of the $\wp$-function, we now have

$$\wp(u) \equiv \wp\left(\frac{\omega}{\rho}\right) \pmod{\mathfrak{p}}. \tag{56}$$

We deduce from (50) and (52) that

$$h_n \equiv e_{q(n)} \sum_{k=0}^{q(n)} A_k(n)\wp(u)^k \equiv e_{q(n)} \sum_{k=0}^{q(n)} A_k(n)\wp\left(\frac{\omega}{\rho}\right)^k \equiv \psi_n\left(\frac{\omega}{\rho}\right) \pmod{\mathfrak{p}} \tag{57}$$

for $n \in \mathbb{N}$. Consider now $\psi_{\rho-n}\left(\frac{\omega}{\rho}\right)$ where $0 \leqslant n \leqslant \rho$. Formulas (51) and (1.7) and the fact that $\sigma(z)$ is an odd function give

$$\psi_{\rho-n}\left(\frac{\omega}{\rho}\right) = \frac{\sigma(-n\omega/\rho+\omega)}{\sigma(\omega/\rho)^{\rho^2-2\rho n+n^2}} = \frac{\delta(\omega)e^{\eta(\omega)(-n\omega/\rho+\omega/2)}\sigma(-n\omega/\rho)}{\sigma(\omega/\rho)^{\rho^2-2\rho n+n^2}} =$$

$$\frac{-\delta(\omega)e^{\eta(\omega)(-n\omega/\rho+\omega/2)}\sigma(n\omega/\rho)}{\sigma(\omega/\rho)^{\rho^2-2\rho n+n^2}} = \frac{-\delta(\omega)e^{\eta(\omega)(-n\omega/\rho+\omega/2)}}{\sigma(\omega/\rho)^{\rho^2-2\rho n}} \cdot \psi_n(\omega/\rho) =$$

$$e^{-n\omega\eta(\omega)/\rho}\sigma(\omega/\rho)^{2\rho n} \cdot \frac{-\delta(\omega)e^{\omega\eta(\omega)/2}}{\sigma(\omega/\rho)^{\rho^2}} \cdot \psi_n(\omega/\rho) =$$

$$\left(e^{-\omega\eta(\omega)/\rho}\sigma(\omega/\rho)^{2\rho}\right)^n \cdot \frac{-\delta(\omega)e^{\omega\eta(\omega)/2}}{\sigma(\omega/\rho)^{\rho^2}} \cdot \psi_n(\omega/\rho) = \alpha^n\beta^n\psi_n(\omega/\rho),$$

$$\text{where} \qquad \alpha = e^{-\omega\eta(\omega)/\rho}\sigma(\omega/\rho)^{2\rho}, \qquad \beta = \frac{-\delta(\omega)e^{\omega\eta(\omega)/2}}{\sigma(\omega/\rho)^{\rho^2}}.$$

By (57) we now have the congruence

$$h_{\rho-n} \equiv \alpha^n\beta h_n \pmod{\mathfrak{p}}. \tag{58}$$

Letting n equal one and two in (58) we see that

$$\alpha\beta \equiv h_{\rho-1}, \qquad \alpha^2\beta \equiv h_{\rho-2}/h_2 \pmod{\mathfrak{p}}.$$

Indeed, since p is not a divisor of h_2, h_2 cannot be congruent to 0 modulo $\mathfrak{p}$. As $\mathcal{R}/\mathfrak{p}$ is a field, h_2 must have an inverse h_2^{-1}. We conclude that $\alpha\beta$ and $\alpha^2\beta$ are congruent to rational integers modulo $\mathfrak{p}$. But then $\alpha = \alpha^2\beta/\alpha\beta$ and $\beta = \alpha\beta/\alpha$ themselves must be congruent to rational integers modulo $\mathfrak{p}$, say $\alpha \equiv a$, $\beta \equiv b \pmod{\mathfrak{p}}$ for $a, b \in \mathbb{Z}$. Thus (58) becomes

$$h_{\rho-n} \equiv a^n b h_n \pmod{\mathfrak{p}}.$$

Since all the Roman letters denote rational integers, we deduce that

$$h_{\rho-n} \equiv a^n b h_n \pmod{p}.$$

We have proven the theorem in case ρ is prime to p.

(ii) Suppose that $\rho = p$ or $\rho = 2p$ and that $g_2 \equiv g_3 \equiv 0 \pmod{p}$. By lemma 4.2, $P_n \equiv H(P_n) \pmod{p}$. The following table shows the possible values of h_n and $h_{\rho-n}$ modulo p. Besides the congruence already mentioned we made use of (10), the relation $h_n = \psi_n(u)$ and the fact that $\rho \equiv 0 \pmod{p}$.

ρ	n	$\rho - n$	$h_n \pmod p$	$h_{\rho-n} \pmod p$
p	odd	even	$n\wp(u)^{\frac{n^2-1}{2}}$	$\frac{n}{2}\wp'(u)\wp(u)^{\frac{\rho^2-2n\rho+n^2-4}{2}}$
p	even	odd	$-\frac{n}{2}\wp'(u)\wp(u)^{\frac{n^2-4}{2}}$	$-n\wp(u)^{\frac{\rho^2-2n\rho+n^2-1}{2}}$
$2p$	odd	odd	$n\wp(u)^{\frac{n^2-1}{2}}$	$-n\wp(u)^{\frac{\rho^2-2n\rho+n^2-1}{2}}$
$2p$	even	even	$-\frac{n}{2}\wp'(u)\wp(u)^{\frac{n^2-4}{2}}$	$\frac{n}{2}\wp'(u)\wp(u)^{\frac{\rho^2-2n\rho+n^2-4}{2}}$

If $\rho = p$, put $\alpha = \wp(u)^{-\rho}$ and $\beta = \frac{1}{2}\wp'(u)\wp(u)^{\frac{\rho^2-3}{2}}$. By (47), $\wp(u)$ is congruent to an integer modulo p. If $\wp(u) \equiv 0 \pmod p$, (55) holds for arbitrary integers a and b. So assume that $\wp(u) \not\equiv 0 \pmod p$. Now let a be the non-zero integer to which α is congruent modulo p and let b be the non-zero integer to which β is congruent modulo p. Then for odd n we have

$$a^n b h_n \equiv \alpha^n \beta h_n \equiv \wp(u)^{-n\rho}\tfrac{1}{2}\wp'(u)\wp(u)^{\frac{\rho^2-3}{2}} n\wp(u)^{\frac{n^2-1}{2}} \equiv \tfrac{n}{2}\wp'(u)\wp(u)^{\frac{\rho^2-2n\rho+n^2-4}{2}} \equiv h_{\rho-n} \pmod p.$$

For even n we have

$$a^n b h_n \equiv \alpha^n \beta h_n \equiv \wp(u)^{-n\rho}\tfrac{1}{2}\wp'(u)\wp(u)^{\frac{\rho^2-3}{2}} \cdot -\tfrac{n}{2}\wp'(u)\wp(u)^{\frac{n^2-4}{2}} \equiv -\tfrac{n}{4}\wp'(u)^2\wp(u)^{\frac{\rho^2-2n\rho+n^2-7}{2}} \equiv$$

$$-\tfrac{n}{4}\left(4\wp(u)^3 - g_2\wp(u) - g_3\right)\wp(u)^{\frac{\rho^2-2n\rho+n^2-7}{2}} \equiv -\tfrac{n}{4}\,4\wp(u)^3\wp(u)^{\frac{\rho^2-2n\rho+n^2-7}{2}} \equiv$$

$$-n\wp(u)^{\frac{\rho^2-2n\rho+n^2-1}{2}} \equiv h_{\rho-n} \pmod p.$$

This proves (55) in case $\rho = p$.

Now let $\rho = 2p$. Put $\alpha = \wp(u)^{-\rho}$ and $\beta = -\wp(u)^{\rho^2/2}$. Once again, if $\wp(u) \equiv 0 \pmod p$, (55) holds for arbitrary integers a and b. So assume that $\wp(u) \not\equiv 0 \pmod p$. Let a and b, as before, be the integers to which α and β are congruent modulo p. For odd n we have

$$a^n b^n h_n \equiv \alpha^n \beta_n h_n \equiv \wp(u)^{-n\rho} \cdot -\wp(u)^{\rho^2/2} n\wp(u)^{\frac{n^2-1}{2}} \equiv -n\wp(u)^{\frac{\rho^2-2n\rho+n^2-1}{2}} \equiv h_{\rho-n} \pmod p.$$

For even n we have

$$a^n b h_n \equiv \alpha^n \beta h_n \equiv \wp(u)^{-n\rho} \cdot -\wp(u)^{\rho^2/2} \cdot -\tfrac{n}{2}\wp'(u)\wp(u)^{\frac{n^2-4}{2}} \equiv \tfrac{n}{2}\wp'(u)\wp(u)^{\frac{\rho^2-2n\rho+n^2-4}{2}} \equiv h_{\rho-n} \pmod p.$$

This proves (55) in case $\rho = 2p$.

(iii) Let $\rho = p$ or $\rho = 2p$ and assume that g_2 and g_3 are not both divisible by p. If $\rho = p$ the leading coefficient of $F_\rho(w)$, i.e. the coefficient of $w^{(p^2-1)/2}$, equals p. If $\rho = 2p$ the leading coefficient of $F_\rho(w)$, which is now the coefficient of $w^{(4p^2-4)/2} = w^{2p^2-2}$, equals $-2p/2 = -p$. In any case p divides the leading coefficient of $F_\rho(w)$ but p^2 does not. Furthermore, by lemma 4.3 there exists at least one coefficient which is not divisible by p. Therefore it cannot be an integer modulo $\mathfrak{p}$. Consequently, not all the roots ζ_k of $F_\rho(w)$ are integers modulo $\mathfrak{p}$. For if they were, by lemma 4.4 the coefficients of $F_\rho(w)$, which consist of sums and products of roots ζ_k, would all be integral modulo $\mathfrak{p}$, quod non.

We shall now prove that not all the roots ζ_k $(1 \leqslant k \leq q(\rho))$ of $F_\rho(w)$ are fractions modulo $\mathfrak{p}$ either. To this end, let ε denote a variable whose range is the set of all the field elements of $\mathcal{R}$ which are integers modulo $\mathfrak{p}$. Assuming all the ζ_k are fractions modulo $\mathfrak{p}$, we will derive a contradiction. So assume that all the ζ_k are fractions modulo $\mathfrak{p}$. By lemma 4.7 the index of $(\varepsilon - \zeta_1)(\varepsilon - \zeta_2)\cdots(\varepsilon - \zeta_{q(\rho)})$ is a positive

integer N independent of the choice of ε. But by formula (47), $w_0 = \wp(u)$ is an admissible value of ε, since $\mathfrak{p}$ is prime to $6h_2h_3$. But by formulas (50) and (52),

$$h_\rho = d_\rho F_\rho(w_0) = pl(w_0-\zeta_1)(w_0-\zeta_2)\cdots(w_0-\zeta_{q(\rho)}) \tag{59}$$

where $l = 1$ if $\rho = p$ and $l = h_2$ if $\rho = 2p$. In any case l is prime to p.

Now suppose the highest power of $\mathfrak{p}$ dividing p is the m-th. By the definition of ρ, $h_\rho = pt$ for some $t \in \mathbb{Z}$, so that by lemma 4.6 the index of h_ρ is at most $-m$. But by lemma 4.6, the index of the right-hand side of (59) equals $-m+N > 0$, a contradiction. Hence not all the ζ_k are fractions modulo $\mathfrak{p}$.

Now let $\zeta_1, \zeta_2, \ldots, \zeta_s$ be the roots of $F_\rho(w)$ which are integers modulo $\mathfrak{p}$ and let $\zeta_{s+1}, \zeta_{s+2}, \ldots, \zeta_{q(\rho)}$ be the roots which are fractions modulo $\mathfrak{p}$. In view of what we have just proved, both these sets of roots are non-empty. Now rewrite (59) as

$$h_\rho = pl[(w_0-\zeta_1)\cdots(w_0-\zeta_s)][(w_0-\zeta_{s+1})\cdots(w_0-\zeta_{q(\rho)})].$$

The index of the right-hand side is at most equal to the index $-m$ of p, as h_ρ is divisible by p. But the index of $[(w_0-\zeta_{s+1})\cdots(w_0-\zeta_{q(\rho)})]$ is positive. Consequently the index of $[(w_0-\zeta_1)\cdots(w_0-\zeta_s)]$ is negative. But this implies that $(w_0-\zeta_1)\cdots(w_0-\zeta_s) \equiv 0 \pmod{\mathfrak{p}}$. Since $\mathfrak{p}$ is a prime ideal and each term $w_0-\zeta_1, \ldots, w_0-\zeta_s$ is an integer modulo $\mathfrak{p}$, there exists a ζ_k $(1 \leqslant k \leqslant s)$ such that $w_0 \equiv \zeta_k \pmod{\mathfrak{p}}$, i.e. $\wp(u) \equiv \zeta_k \pmod{\mathfrak{p}}$. In the preliminaries we have seen that ζ_k equals $\wp\left(\frac{\omega}{\rho}\right)$ for a suitably chosen period ω of the $\wp$-function. Thus we have obtained again the congruence (56). The remainder of the proof now follows exactly as in part (i). This concludes the proof. $\boxtimes$

5 The numerical periodicity and symmetry modulo p of sequences

We shall prove in this chapter that any elliptic divisibility sequence is numerically periodic for any prime and purely periodic for all primes which do not divide both h_3 and h_4. The culminating result is theorem 5.9 which shows precisely how the period and rank of apparition are connected. The proof of this theorem hinges on theorem 4.8.

The theorems which follow not only lead to the periodicity of (h) modulo p, but also state symmetries in the pattern of least positive residues of successive blocks of ρ terms of (h). The final result of these symmetries is to determine the residues modulo p of all terms of (h) in terms of the integers a and b of theorem 4.8 and the residues of the first $[\rho/2]$ terms.

5.1 Symmetries of (h) modulo p

Definition 5.1. A sequence (s) of rational integers (i.e. elements of $\mathbb{Z}$) is said to be *numerically periodic* modulo m if there exists a positive integer π such that

$$s_{n+\pi} \equiv s_n \pmod{m}$$

for all sufficiently large n. If this relation holds for all n, then (s) is said to be *purely* periodic modulo m. The smallest such integer π for which the relation holds is called *the* period of (s) modulo m. All other periods are multiples of it.$\Diamond$

The next theorem shows how a and b may be determined modulo p.

Theorem 5.2. Let a and b be the integers specified in theorem 4.8 and let the integer c be determined by the congruence

$$ac \equiv 1 \pmod{p}. \tag{60}$$

Then the following congruences hold modulo p:

$$a \equiv \frac{h_{\rho-2}}{h_2 h_{\rho-1}}, \qquad b \equiv \frac{h_2 h_{\rho-1}^2}{h_{\rho-2}}, \qquad b \equiv h_{\rho-1} c. \tag{61}$$

$$a^\rho b^2 \equiv 1, \qquad c^\rho \equiv b^2. \tag{62}$$

$$a^2 \equiv -\frac{h_{\rho-1}}{h_{\rho+1}}, \qquad b^2 \equiv -h_{\rho+1} h_{\rho-1}. \tag{63}$$

PROOF. Note that since p does not divide h_2 nor h_3 we have $\rho \geqslant 4$. Let n successively equal 1 and $\rho - 1$ in (55). We obtain:

$$h_{\rho-1} \equiv ab \pmod{p} \tag{64}$$

and[6] $1 \equiv h_1 \equiv a^{\rho-1} b h_{\rho-1}$. Hence by (64) $1 \equiv a^{\rho-1} b h_{\rho-1} \equiv a^\rho b^2$. Thus we have proven (62), since the second part follows immediately from the first by the definition of c. The third part of (61) follows from (64) and (60).

Next, put n equal to 2 in (55):

$$h_{\rho-2} \equiv a^2 b h_2 \equiv a h_{\rho-1} h_2 \pmod{p},$$

[6]The modulus p will be omitted here and elsewhere when no confusion can arise.

the last step following from (64). This result is equivalent to the first part of (61). The second part of (61) now follows by (64). It remains to prove (63). Consider $h_{\rho+1}$. Assume first that ρ is odd:

$$\rho = 2\sigma + 1 \geqslant 5. \tag{65}$$

Then $\rho+1 = 2(\sigma+1)$ and $\rho-1 = 2\sigma$, and on putting n equal to $\sigma+1$ and σ in (23), we obtain

$$h_2 h_{\rho+1} = h_{\sigma+1}h_{\sigma+3}h_\sigma^2 - h_{\sigma+1}h_{\sigma-1}h_{\sigma+2}^2, \tag{66}$$

$$h_2 h_{\rho-1} = h_\sigma h_{\sigma+2}h_{\sigma-1}^2 - h_\sigma h_{\sigma-2}h_{\sigma+1}^2. \tag{67}$$

But by (55) and (65) the following congruences hold modulo p:

$$h_{\sigma+1} \equiv a^\sigma b h_\sigma, \qquad h_{\sigma+3} \equiv a^{\sigma-2} b h_{\sigma-2}, \qquad h_\sigma \equiv a^{\sigma+1} b h_{\sigma+1};$$

$$h_{\sigma-1} \equiv a^{\sigma+2} b h_{\sigma+2}, \qquad h_{\sigma+2} \equiv a^{\sigma-1} b h_{\sigma-1}.$$

On substituting these expressions into (66) we obtain

$$h_2 h_{\rho+1} \equiv a^{4\sigma} b^4 \left(h_\sigma h_{\sigma-2} h_{\sigma+1}^2 - h_\sigma h_{\sigma+2} h_{\sigma-1}^2\right) \pmod{p}.$$

As $4\sigma = 2\rho - 2$ and p does not divide h_2, by (67) we get the congruence

$$h_{\rho+1} \equiv -a^{2\rho-2} b^4 h_{\rho-1} \pmod{p}. \tag{68}$$

Next we wish to derive the same congruence for ρ even. So let $\rho = 2\mu \geqslant 4$. Then $\rho+1 = 2\mu+1$ and $\rho-1 = 2\mu-1$, on putting n equal to μ and $\mu-1$ in (22), we obtain

$$h_{\rho+1} = h_{\mu+2}h_\mu^3 - h_{\mu-1}h_{\mu+1}^3, \tag{69}$$

$$h_{\rho-1} = h_{\mu+1}h_{\mu-1}^3 - h_{\mu-2}h_\mu^3. \tag{70}$$

But by (55) and (65) the following congruences hold modulo p:

$$h_{\mu+2} \equiv a^{\mu-2} b h_{\mu-2}, \qquad h_\mu \equiv a^\mu b h_\mu, \qquad h_{\mu-1} \equiv a_{\mu+1} b h_{\mu+1}, \qquad h_{\mu+1} \equiv a^{\mu-1} b h_{\mu-1}.$$

On substituting these expressions into (69) we obtain

$$h_{\rho+1} \equiv a^{4\mu-2} b^4 \left(h_{\mu-2}h_\mu^3 - h_{\mu+1}h_{\mu-1}^3\right) \pmod{p}.$$

As $4\mu - 2 = 2\rho - 2$, by (70) we get the congruence $h_{\rho+1} \equiv -a^{2\rho-2}b^4 h_{\rho-1} \pmod{p}$, so that (68) holds for even ρ also.

By the first part of (62), it follows from (68) that $h_{\rho+1} \equiv -(a^\rho b^2)^2 a^{-2} h_{\rho-1} \equiv -a^{-2} h_{\rho-1}$, which is equivalent to the first part of (63). The second part of (63) now follows from (64). ☒

Lemma 5.3. With the notation of theorems 4.8 and 5.2, the following congruence is valid for all positive integers n:

$$h_{\rho+n} \equiv -bc^n h_n \pmod{p}. \tag{71}$$

PROOF. Since p does not divide h_3, p cannot be a common divisor of h_3 and h_4. Theorem 3.17 now implies that $h_s \equiv 0 \pmod{p}$ if and only if s is a multiple of ρ.

Assume first that $0 \leqslant n \leqslant \rho$. Since

$$h_{\rho+n}h_{\rho-n} = h_{\rho+1}h_{\rho-1}h_n^2 - h_{n+1}h_{n-1}h_\rho^2$$

and p divides h_ρ, we obtain from (63) the congruence $h_{\rho+n}h_{\rho-n} \equiv -b^2h_n^2 \pmod{p}$. By applying (55) to the left-hand side we obtain $h_{\rho+n}a^nbh_n \equiv -b^2h_n^2 \pmod{p}$. If $0 < n < \rho$, we may cancel bh_n. We then obtain (71) on multiplying by c^n. Since the cases $n = 0$ and $n = \rho$ are trivially satisfied, (71) is true for $0 \leqslant n \leqslant k\rho$ if k equals one.

We now proceed by induction on k. Suppose that (71) is true for $0 \leqslant n \leqslant k\rho$ and assume $k\rho \leqslant n \leqslant (k+1)\rho$. Then since

$$h_{n+\rho}h_{n-\rho} = h_{n+1}h_{n-1}h_\rho^2 - h_{\rho+1}h_{\rho-1}h_n^2$$

and p divides h_ρ, we obtain from (63) the congruence

$$h_{n+\rho}h_{n-\rho} \equiv b^2h_n^2 \pmod{p}. \tag{72}$$

Now $0 \leqslant n-\rho \leqslant k\rho$. Hence by the induction hypothesis, (71) holds with n replaced by $n-\rho$:

$$h_n \equiv -bc^{n-\rho}h_{n-\rho} \pmod{p},$$

whence

$$h_{n-\rho} \equiv -\frac{a^{n-\rho}}{b}h_n \pmod{p}. \tag{73}$$

Therefore, since $k\rho < n < (k+1)\rho$ implies $h_n \not\equiv 0$, on combining (72) and (73) we obtain $h_{n+\rho} = -b^3c^{n-\rho}h_n$. Since $c^{-\rho}b^2 \equiv 1$ by (62) and (60), we conclude that $h_{n+\rho} \equiv -bc^nh_n$. Since (71) holds trivially for $n = k\rho$ and $n = (k+1)\rho$, and has been proven true for $0 \leqslant n \leqslant \rho$, the induction is completed. ⊠

Theorem 5.4. The following congruence holds for all $k, n \in \mathbb{N}$:

$$h_{k\rho+n} \equiv (-1)^k b^{k^2} c^{kn} h_n \pmod{p}. \tag{74}$$

PROOF. We perform induction on k. If $k = 1$ the assertion amounts to lemma 5.3. Suppose that the assertion has been proven for $k = q$. Then by lemma (71)

$$h_{(q+1)\rho+n} = h_{\rho+(q\rho+n)} \equiv -bc^{q\rho+n}h_{q\rho+n} \pmod{p},$$

which by the induction hypothesis is congruent to

$$-bc^{q\rho+n}(-1)^q c^{qn} b^{q^2} h_n \equiv (-1)^{q+1} b^{q^2+1} c^{q\rho} c^{(q+1)n} h_n \pmod{p}.$$

Now by (62) we see that $c^{q\rho} \equiv b^{2q}$. Hence,

$$h_{(q+1)\rho+n} \equiv (-1)^{q+1} b^{q^2+2q+1} c^{(q+1)n} h_n = (-1)^{q+1} b^{(q+1)^2} c^{(q+1)n} h_n \pmod{p},$$

so that we have derived (74) for $k = q+1$. This concludes the induction. ⊠

Lemma 5.5. Let p be a prime, d an integer prime to it, and belonging to the exponent δ modulo p. That is, δ is the smallest positive integer such that $d^\delta \equiv 1 \pmod{p}$. Then if k is an integer such that $d^k \equiv 1 \pmod{p}$, δ divides k.

PROOF. By the euclidean algorithm, we can write $k = q\delta + r$ with q, r integers and $0 \leqslant r < \delta$. Suppose now that $r > 0$. Then we have

$$1 \equiv d^k \equiv d^{q\delta+r} \equiv (d^\delta)^q d^r \equiv d^r \pmod{p},$$

contradictory to the minimality of δ. Thence $r = 0$ and $k = q\delta$, so that $\delta | k$. ⊠

Lemma 5.6. Let τ be the least positive integer such that

$$(-b)^{\tau^2} \equiv 1, \qquad c^\tau \equiv 1 \pmod{p}. \tag{75}$$

Then if k is an integer such that $(-b)^{k^2} \equiv 1$ and $c^k \equiv 1 \pmod{p}$, then τ divides k.

PROOF. By the euclidean algorithm we can write $k = q\tau + r$ with $0 \leqslant r < \tau$. We will show that the assumption $r > 0$ leads to a contradiction. So assume $r > 0$. We have

$$1 \equiv (-b)^{k^2} \equiv (-b)^{q^2\tau^2+2qr\tau+r^2} \equiv ((-b)^{\tau^2})^{q^2} (-b)^{2qr\tau+r^2} \equiv (-b)^{2qr\tau+r^2} \pmod{p},$$

$$1 \equiv c^k \equiv c^{q\tau+r} \equiv (c^\tau)^q c^r \equiv c^r \pmod{p}.$$

Now by (62) we have the congruence $b^2 \equiv c^\rho \pmod{p}$, so that

$$1 \equiv (-b)^{2qr\tau+r^2} \equiv (-b)^{2qr\tau} (-b)^{r^2} \equiv ((-b)^2)^{qr\tau} (-b)^{r^2} \equiv (b^2)^{qr\tau} (-b)^{r^2} \equiv c^{\rho qr\tau} (-b)^{r^2} \pmod{p}.$$

But $c^r \equiv 1 \pmod{p}$, so that

$$1 \equiv c^{\rho qr\tau} (-b)^{r^2} \equiv (-b)^{r^2} \pmod{p}.$$

Thus we have derived that (75) holds for $r < \tau$, a contradiction. Hence r equals zero, so that $k = q\tau$, i.e. $\tau | k$. ⊠

We can now establish the fundamental symmetries of (h) modulo p.

Theorem 5.7. Let (h) be an elliptic divisibility sequence, and let p be any prime which divides neither h_2 nor h_3. Once again, let τ be the least positive integer such that (75) holds. Then (h) is purely periodic modulo p with period $\tau\rho$.

PROOF. As τ and τ^2 have the same parity, we see from (75) and (74) that $h_{\tau\rho+n} \equiv (-b)^{\tau^2} c^{\tau n} h_n \equiv h_n \pmod{p}$, so that $\tau\rho$ is a period of (h) and (h) is purely periodic modulo p. Hence by theorem 3.17, any other period π of (h) modulo p is a multiple of ρ, say $\pi = k\rho$. But if $k\rho$ is a period, then on taking n equal to 1 and 2 in (74), we obtain the congruences

$$(-1)^k b^{k^2} c^k \equiv 1, \qquad (-1)^k b^{k^2} c^{2k} \equiv 1 \pmod{p}.$$

Dividing the second congruence by the first yields $c^k \equiv 1 \pmod{p}$, which implies $(-1)^k b^{k^2} \equiv (-b)^{k^2} \equiv 1 \pmod{p}$. Hence by lemma 5.5, $\tau | k$. Consequently, $\tau\rho$ divides $\pi = k\rho$. ⊠

5.2 Determining the period π of (h) modulo p

We have just seen that the period π of (h) modulo p can be written as $\pi = \tau\rho$, where τ is the least positive integer such that $(-b)^{\tau^2} \equiv 1$ and $c^{\tau} \equiv 1 \pmod{p}$. As it turns out, we can express τ in terms of the exponents to which $h_2/h_{\rho-2}$ and $h_{\rho-1}$ belong modulo p — the objective of this section.

Lemma 5.8. Let p be an odd prime,[7] d an integer prime to it and belonging to the exponent δ modulo p. That is, δ is the least positive integer such that $d^{\delta} \equiv 1 \pmod{p}$. Then if δ is odd, there exists no integer x such that the congruence

$$d^x \equiv -1 \pmod{p} \tag{76}$$

is satisfied. But if δ is even, (76) is satisfied if and only if x is an odd multiple of $\delta/2$.

PROOF. Assume δ to be odd. Suppose that there exists an integer x such that (76) is satisfied. Then $d^{2x} \equiv 1 \pmod{p}$. By lemma 5.5, δ divides $2x$. As δ is odd, it must divide x. Hence there exists an integer m such that $x = m\delta$, which yields the congruence

$$d^x \equiv d^{m\delta} \equiv (d^{\delta})^m \equiv 1 \pmod{p}.$$

But is contrary to the assumption $d^x \equiv -1 \pmod{p}$, as $p \neq 2$. From this we conclude that the number x cannot exist.

Now let δ be even and suppose that (76) holds for some integer x. Now $d^{2x} \equiv 1$ implies $\delta | 2x$, so that $\delta/2 | x$. Therefore $x = s \cdot \delta/2$ for some integer s. Note that $d^{\delta/2} \equiv -1 \pmod{p}$. Indeed, $d^{\delta} \equiv 1$ implies $d^{\delta/2} \equiv \pm 1$. But by the minimality of δ, the possibility $+1$ is impossible. If s were even, say $s = 2t$, we would have $d^x \equiv d^{2t \cdot \delta/2} \equiv d^{t\delta} \equiv (d^{\delta})^t \equiv 1$, a contradiction. Thus s must be odd, so that x is an odd multiple of δ. Conversely, if x is an odd multiple of $\delta/2$, say $x = m\delta/2$, we obtain the congruence

$$d^x \equiv d^{m\delta/2} \equiv (d^{\delta/2})^m \equiv (-1)^m \equiv -1 \pmod{p}. \boxtimes$$

We have now developed the tools to prove the announced periodicity theorem.

Theorem 5.9. Let (h) be an elliptic divisibility sequence and p an odd prime whose rank of apparition ρ is greater than three. Let e be an integral solution of the congruence

$$e \equiv \frac{h_2}{h_{\rho-2}} \pmod{p}, \tag{77}$$

and let ε and κ be the exponents to which e and $h_{\rho-1}$ belong modulo p. That is to say, let ε and κ be the smallest positive integers such that $e^{\varepsilon} \equiv 1$ and $h_{\rho-1}^{\kappa} \equiv 1 \pmod{p}$ respectively. Then (h) is purely periodic modulo p, and its period π is given by the formula $\pi = \tau\rho$ where

$$\tau = 2^{\alpha}[\varepsilon, \kappa]. \tag{78}$$

Here, $[\varepsilon, \kappa]$ is the least common multiple of ε and κ and the exponent α is determined as follows:

$$\alpha = \begin{cases} +1 & \text{if and only if } \varepsilon \text{ and } \kappa \text{ are both odd,} \\ -1 & \text{if and only if } \varepsilon \text{ and } \kappa \text{ are both even and both divisible by precisely the same power of 2,} \\ 0 & \text{in all other cases.} \end{cases}$$

[7] The lemma is false if $p = 2$, as in this particular case $-1 \equiv +1 \pmod{p}$.

REMARK 1. To prove the results in section 5.1 we used theorem 4.8, which is not true if $p = 3$. However, the assertion in theorem 5.9 holds also in the case $p = 3$. This fact shall be proven in section 5.3, where we will discuss the so-called exceptional primes. Throughout the following proof we will assume that $p > 3$.

REMARK 2. We first observe that the congruences (77) and (61) allow us to relate the integers c and e:

$$e \equiv c/h_{\rho-1} \equiv c^2/b \pmod{p}. \tag{79}$$

PROOF. Since $c^\tau \equiv 1$, we have $c^{\tau\rho} \equiv 1$. Now as $c^\rho \equiv b^2$ by (62), it follows that $b^{2\tau} = (b^\tau)^2 \equiv 1 \pmod{p}$. Thus b^τ is either congruent to (i) $+1$ or (ii) -1 modulo p. We treat these cases separately.

(i) Suppose $b^\tau \equiv +1 \pmod{p}$. Then by (75),

$$1 \equiv (-b)^{\tau^2} \equiv (-1)^{\tau^2}(b^\tau)^\tau \equiv (-1)^{\tau^2} \pmod{p},$$

so that τ must be even, since τ and τ^2 have the same parity. Now by (61), $b^\tau \equiv h_{\rho-1}^\tau c^\tau$. Since $c^\tau \equiv 1$ by (75), we derive that

$$h_{\rho-1}^\tau \equiv b^\tau \equiv 1 \pmod{p}. \tag{80}$$

Then

$$e^\tau \equiv \frac{c^{2\tau}}{b^\tau} \equiv 1 \pmod{p}. \tag{81}$$

Let $\sigma = [\varepsilon, \kappa]$ be the least common multiple of the exponents to which e and $h_{\rho-1}$ belong modulo p. Then by (80) and (81), lemma 5.5 implies that $\kappa|\tau$ and $\varepsilon|\tau$. Hence

$$\sigma|\tau. \tag{82}$$

On the other hand, by construction $h_{\rho-1}^\sigma \equiv 1$ and $e^\sigma \equiv 1 \pmod{p}$. Hence

$$c^\sigma \equiv e^\sigma h_{\rho-1}^\sigma \equiv 1, \qquad b^\sigma \equiv \frac{c^{2\sigma}}{e^\sigma} \equiv 1 \pmod{p}. \tag{83}$$

Congruence (83) implies $b^{\sigma^2} \equiv 1$. Now if σ is even, so is σ^2 and we have $1 \equiv b^{\sigma^2} \equiv (-b)^{\sigma^2} \pmod{p}$. Hence by lemma 5.6, $\tau|\sigma$, so that by (82), $\tau = \sigma$.

σ is odd if and only if both ε and κ are odd. In this case (83) implies that $c^{2\sigma} \equiv 1$ and $(-b)^{4\sigma^2} \equiv 1 \pmod{p}$. Hence by lemma 5.6, $\tau|2\sigma$. But by (82) σ divides τ, so that $\sigma|\tau|2\sigma$. As τ is even and σ is odd, it now follows that $\tau = 2\sigma$. This disposes of the first case of the theorem.

(ii) Assume now that

$$b^\tau \equiv -1 \pmod{p}. \tag{84}$$

Then by (61) and (75),

$$h_{\rho-1}^\tau \equiv -1 \pmod{p}, \tag{85}$$

and

$$e^\tau \equiv -1 \pmod{p}. \tag{86}$$

Now by lemma 5.8, (85) and (86) imply that both κ and ε are even, and that τ is both an odd multiple of $\kappa/2$ and an odd multiple of $\varepsilon/2$. But if σ now denotes $[\varepsilon/2, \kappa/2]$,

$$\sigma|\tau. \tag{87}$$

Hence σ must be an odd multiple of both $\varepsilon/2$ and $\kappa/2$, say $\sigma = r \cdot \varepsilon/2$ and $\sigma = s \cdot \kappa/2$ for odd numbers r and s. Let x be the integer such that $2^x||\sigma$. As r and s are odd, this implies that $2^x||\varepsilon/2$ and $2^x||\kappa/2$. In

other words, if (84) holds, both ε and κ must be even and both divisible by precisely the same power of two.

Assume, conversely, that ε and κ are even and divisible by precisely the same power of two. Then for some y we have $\varepsilon = 2^y \cdot u$ and $\kappa = 2^y \cdot v$ where u and v are odd integers. Consequently, $\sigma = [\varepsilon/2, \kappa/2] = [2^{y-1}u, 2^{y-1}v] = 2^{y-1}[u,v]$. As $[u,v] = ut$ and $[u,v] = vw$ for certain odd integers t and w, we can write $\sigma = 2^{y-1}ut = \varepsilon/2 \cdot t$ and $\sigma = 2^{y-1}vw = \kappa/2 \cdot w$. Thus σ is an odd multiple of both $\varepsilon/2$ and $\kappa/2$. Hence, by lemma 5.8

$$h^{\sigma}_{\rho-1} \equiv -1, \qquad e^{\sigma} \equiv -1 \pmod{p}.$$

But then by (79) and (61),

$$c^{\sigma} \equiv h^{\sigma}_{\rho-1} e^{\sigma} \equiv 1, \qquad b^{\sigma} \equiv h^{\sigma}_{\rho-1} c^{\sigma} \equiv -1 \pmod{p}.$$

Hence $(-b)^{\sigma^2} \equiv \big((-b)^{\sigma}\big)^{\sigma} \equiv \big((-1)^{\sigma} b^{\sigma}\big)^{\sigma} \equiv \big((-1)^{\sigma}(-1)\big)^{\sigma} \equiv \big((-1)^{\sigma+1}\big)^{\sigma} \equiv (-1)^{\sigma^2+\sigma} \equiv 1 \pmod{p}$. The last congruence follows from the fact that $\sigma^2 + \sigma$ is *always* even. Therefore by lemma 5.6, $\tau | \sigma$. Hence by (87), $\tau = \sigma$. As $[\varepsilon/2, \kappa/2] = \frac{1}{2}[\varepsilon, \kappa]$, completing the proof of the theorem. $\boxtimes$

Example 5.10. Recall the sequence (G) from example 3.10. We have $G_0 = 0$, $G_1 = 1$, $G_2 = 3$, $G_3 = 8$, $G_4 = 21$. For any prime p other than $2, 3$ we can apply theorem 5.9. The following table shows the first twenty-three values of (G) modulo p for suitable values of p.

p	G_0	G_1	G_2	G_3	G_4	G_5	G_6	G_7	G_8	G_9	G_{10}	G_{11}	G_{12}	G_{13}	G_{14}	G_{15}	G_{16}	G_{16}	G_{18}	G_{19}	G_{20}	G_{21}	G_{22}	ρ	π	ε	κ	τ
5	0	1	3	3	1	0	4	2	2	4	0	1	3	3	1	0	4	2	2	4	0	1	3	5	10	1	1	2
11	0	1	3	8	10	0	1	3	8	10	0	1	3	8	10	0	1	3	8	10	0	1	3	5	5	2	2	1
13	0	1	3	8	8	3	1	0	12	10	5	5	10	12	0	1	3	8	8	3	1	0	12	7	14	1	1	2
29	0	1	3	8	21	26	28	0	1	3	8	21	26	28	0	1	3	8	21	26	28	0	1	7	7	2	2	1
37	0	1	3	8	21	18	33	7	25	31	31	25	7	33	18	21	8	3	1	0	36	34	29	19	38	1	1	2
89	0	1	3	8	21	55	55	21	8	3	1	0	88	86	81	68	34	34	68	81	86	88	0	11	22	1	1	2

Table 1: (G) MODULO p

5.3 Exceptional primes

The arithmetical consequences of the elliptic function representation (theorem 4.8) do not apply to the primes two and three, or more generally to any prime dividing h_2 or h_3. In this section we discuss these exceptional primes.

The case $p = 2$

There are eight *a priori* possible types of elliptic sequences modulo 2 distinguished by the possible residues of h_2, h_3 and h_4 modulo 2. But since h_2 divides h_4, sequences with $h_2 \equiv 0 \pmod 2$ and $h_4 \equiv 1 \pmod 2$ cannot occur. The six possibilities which are left are listed in the following table.

type	h_0	h_1	h_2	h_3	h_4	h_5	ρ	π
1	0	1	0	0	0	0	2	1
2	0	1	1	0	0	0	3	1
3	0	1	0	1	0	1	2	2
4	0	1	1	0	1	1	3	3
5	0	1	1	1	0	1	4	4
6	0	1	1	1	1	0	5	5

Table 2: ELLIPTIC SEQUENCES MODULO 2

Now we see that theorem 5.9 is not true for the two types five and six for which ρ is greater than three. In both cases $\varepsilon = \kappa = 1$ so that the formula (78) gives $\pi = 2\rho$ instead of $\pi = \rho$. Thus the restriction to

odd primes in theorem 5.9 is necessary.

The case $p = 3$
There are 27 *a priori* possible types of sequences modulo 3. But since h_2 divides h_4, sequences with $h_2 \equiv 0 \pmod 3$ and $h_4 \equiv 1, 2 \pmod 3$ cannot occur. Thus there are twenty-one possibilities left, listed below. In each case when the rank of apparition ρ is greater than three, ε and κ are listed and also the multiplier $\tau = 2^{\alpha}[\varepsilon, \kappa]$. The ranks and periods were obtained by direct computation from the formulas (22) and (23) taken modulo 3. The table thus shows that theorem 5.9 is true if $p = 3$.

Type	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8	h_9	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}	ρ	π	ε	κ	τ
1	0	1	0	0	0											2	1			
2	0	1	1	0	0											3	1			
3	0	1	2	0	0											3	1			
4	0	1	0	1	0	2	0	2								2	8			
5	0	1	0	2	0	1	0	2								2	4			
6	0	1	1	0	1	1	0	2	2	0	2	2				3	12			
7	0	1	1	0	2	2										3	6			
8	0	1	2	0	1	2										3	3			
9	0	1	2	0	2	1	0	2	1	0	1	2				3	12			
10	0	1	1	1	0	2	2	2								4	8	1	1	2
11	0	1	1	1	1	0	2	2	2	2						5	10	1	1	2
12	0	1	1	1	2	1	0	2	1	2	2	2				6	12	2	1	2
13	0	1	1	2	0	1	2	2								4	8	1	2	2
14	0	1	1	2	1	2	2	0	1	1	2	1	2	2		7	7	2	2	1
15	0	1	2	2	2	2	1	0	2	1	1	1	1	2		7	14	1	1	2
16	0	1	1	1	2	2	2	0								7	7	2	2	1
17	0	1	2	1	0	2	1	2								4	8	1	1	2
18	0	1	2	1	1	1	0	2	2	2	1	2				6	12	2	1	2
19	0	1	2	1	2	0	1	2	1	2	0					5	5	2	2	1
20	0	1	2	2	0	1	1	2								4	8	1	2	2
21	0	1	2	2	1	0	2	1	1	2						5	10	1	1	2

Table 3: ELLIPTIC SEQUENCES MODULO 3

This table affords simple illustrations of the modular symmetry of sequences which we alluded to in the introduction. For example, consider type 14 and 15. For type 14, we have $h_{\rho-n} \equiv -h_{\rho+n} \equiv -h_n \pmod 3$ as the period is ρ. For type 15, $h_{\rho-n} \equiv h_n$ and $h_{\rho-n} \equiv -h_{\rho+n} \pmod 3$. We shall see that for primes other than two and three, the origin of this symmetry is the periodicity of the second kind of the elliptic sigma functions.

The case $p|h_2$ or $p|h_3$
It follows from theorem 3.16 that if p divides both h_3 and h_4, then it divides every subsequent term of (h). We call such primes *null divisors* of (h).[8] If p is a null divisor, then (h) is numerically periodic modulo p with the period one. Since h_2 divides h_4, primes which divide both h_2 and h_3 are null divisors. On excluding null divisors, we have as well as the general case $h_2 h_3 \not\equiv 0 \pmod p$, two special cases:

$$h_2 \equiv 0 \pmod p, \quad h_3 \not\equiv 0 \pmod p, \tag{88}$$

and

$$h_2 \not\equiv 0 \pmod p, \quad h_3 \equiv 0 \pmod p \tag{89}$$

These special cases are disposed of in chapter 7, the result of which is contained in the following theorem.

[8]The terminology is borrowed from the theory of linear divisibility sequences. See Ward [13].

Theorem 5.11. If condition (88) holds, then

$$h_{2n} \equiv 0 \pmod{p}, \quad h_{2n+1} \equiv (-1)^{[n/4]} h_3^{(n^2-1)/8} \pmod{p}.$$

If condition (89) holds, then

$$h_{3n} \equiv 0 \pmod{p},$$
$$h_{3n+1} \equiv (-1)^{n(n-1)/2} h_2^{n(n-1)/2} h_4^{n(n+1)/2} \pmod{p},$$
$$h_{3n+2} \equiv -(-1)^{n(n+1)/2} h_2^{n(n+1)/2} h_4^{n(n-1)/2} \pmod{p}.$$

We see that in either case (h) is purely periodic modulo p. Its period depends in a simple way on the exponents to which its initial values belong modulo p.

6 Equivalence classes of sequences

In this chapter we shall introduce the notion of equivalence of sequences and show that there exist only two types (i.e. equivalence classes) of singular elliptic divisibility sequences.

6.1 Singular sequences

Let (h) be a general elliptic sequence. We have seen in chapter 4 that there then exists an elliptic function $\wp(z;\ g_2,g_3)$ whose invariants g_2 and g_3 are certain rational functions of the initial values of (h), such that for a properly chosen value $u \in \mathbb{C}$,

$$h_n = \frac{\sigma(nu)}{\sigma(u)^{n^2}}. \tag{90}$$

By the *discriminant* Δ of the sequence (h) we mean the discriminant of the corresponding $\wp$-function:

$$\Delta = g_2^3 - 27g_3^2. \tag{91}$$

We write $\Delta = \Delta(h)$, or $\Delta = \Delta(h_2,h_3,h_4)$ if we wish to emphasize the dependance of Δ on the initial values of (h).

If we substitute for g_2 and g_3 in (91) their expressions in terms of h_2, h_3 and h_4 given by formulas (48) and (49), we find after a long computation that

$$\Delta = \frac{h_4^4 + 3h_2^5h_4^3 + h_2^2\left(3h_2^8 + 8h_3^3\right)h_4^2 + h_2^7\left(h_2^8 - 20h_3^3\right)h_4 + h_2^4h_3^3\left(16h_3^3 - h_2^8\right)}{h_2^8h_3^3}. \tag{92}$$

The sequence (h) is said to be *singular* if and only if its discriminant $\Delta(h)$ vanishes. We shall show that a sequence is singular if and only if it is essentially a so-called Lucas function. The main step in the proof of this result is the following theorem.

Theorem 6.1. Necessary and sufficient conditions that a general elliptic sequence (h) be singular are that there exist integers r and s such that $rs(r^2-s^2) \neq 0$ and

$$h_2 = r, \qquad h_3 = s(r^2-s^3), \qquad h_4 = rs^3(r^2-2s^3). \tag{93}$$

PROOF. "$\Rightarrow$". Assume that (h) is a general elliptic sequence for which $\Delta(h)$ vanishes. Since h_2 and h_3 are not zero, it follows from (92) that $\Delta(h) = 0$ if and only if the numerator of $\Delta(h)$ is zero. Now put

$$u = h_2^4, \qquad v = h_3^3, \qquad w = h_4/h_2. \tag{94}$$

As h_2 divides h_4, these numbers are integers. On substituting them in the numerator of $\Delta(h)$, we obtain the equation

$$\begin{aligned}
uw^4 + 3u^2w^3 + uw^2(3u^2+8v) + u^2w(u^2-20v) + uv(16v-u^2) = 0 \qquad &\Leftrightarrow \\
uw^4 + 3u^2w^3 + 3u^3w^2 + 8uvw^2 + u^4w - 20u^2vw + 16uv^2 - u^3v = 0 \qquad &\Leftrightarrow \\
w^4 + 3uw^3 + 3u^2w^2 + 8vw^2 + u^3w - 20uvw + 16v^2 - u^2v = 0 \qquad &\Leftrightarrow \\
16v^2 - (u^2 + 20uw - 8w^2)v + w(u+w)^3 = 0. \qquad &
\end{aligned} \tag{95}$$

Thus $\Delta(h)$ vanishes if and only if (95) has solutions of the form (94); that is, u is a perfect fourth power and v a perfect cube. If we solve the equation for v by the quadratic formula, we find that

$$v = \frac{(u^2+20uw-8w^2) \pm \sqrt{(u^2+20uw-8w^2)^2 - 64w(u+w)^3}}{32}.$$

Now let us work out the expression under the square root sign:

$$(u^2+20uw-8w^2)^2-64w(u+w)^3=$$

$$\left(u^4+40u^3w-16u^2w^2+400u^2w^2-320uw^3+64w^4\right)-\left(64u^3w+192u^2w^2+192uw^3+64w^4\right)=$$

$$u^4-24u^3w+192u^2w^2-512uw^3=u\left(u^3-24u^2w+192uw^2-512w^3\right)=$$

$$u(u-8w)^3.$$

Hence

$$32v=u^2+20uw-8w^2\pm\sqrt{u(u-8w)^3}. \tag{96}$$

Consequently, it is necessary that $u(u-8w)$ be a square. But u already is square by (94), so that $u-8w$ must be a square. Hence we may write

$$u=l^2=h_2^4, \tag{97}$$

$$u-8w=m^2=h_2^4-8\frac{h_4}{h_2}, \tag{98}$$

where l and m are integers. Then

$$w=\frac{l^2-m^2}{8}. \tag{99}$$

We find from (97) and (99) that

$$u^2+20uw-8w^2=l^4+\tfrac{5}{2}\left(l^4-l^2m^2\right)-\tfrac{1}{8}\left(l^4-2l^2m^2+m^4\right)=\tfrac{1}{8}\left(27l^4-18l^2m^2-m^4\right),$$

$$\sqrt{u(u-8w)^3}=lm^3.$$

On substituting these expressions into (96) and multiplying by eight, we find that $256v=27l^4-18l^2m^2\pm lm^3-m^4$. The right-hand side of this expression factors into $(l\pm m)(3l\mp m)^3$. Hence on multiplying by two and substituting h_3^3 for v, we obtain the formula

$$(8h_3)^3=(2l\pm 2m)(3l\mp m)^3. \tag{100}$$

Hence $2l\pm 2m$ is the cube of an even integer, and we may write $2l\pm 2m=(2s)^3$ where s is an integer. Hence $l\pm m=4s^3$. Consequently, $3l\mp m+4s^3=4l^3$, so that $3l\mp m$ is divisible by four. To put it briefly, for integral s and q

$$l\pm m=4s^3, \qquad 3l\mp m=4q, \tag{101}$$

and (100) becomes $(8h_3)^3=(8sq)^3$. Hence

$$h_3=sq \tag{102}$$

and on solving (101) for l and m, we find that

$$l=s^3+q, \qquad m=\pm(3s^3-q). \tag{103}$$

On substituting these expressions for l and m into (99), we find that

$$h_4/h_2=w=\tfrac{1}{8}(l^2-m^2)=s^3(q-s^3). \tag{104}$$

Finally, (97) and (103) give

$$h_2^2=s^3+q. \tag{105}$$

Now let $h_2 = r$. Then by (105), $q = r^2 - s^3$. On substituting this expression for q into (102), we obtain $h_3 = sq = s(r^2 - s^3)$. Furthermore, by (104) $h_4 = h_2 w = rw = rs^3(r^2 - 2s^3)$. So we have derived formulas (93). The accessory condition $rs(r^2 - s^3) \neq 0$ is needed to insure that (h) is general. The necessity of the conditions (93) is thus established.

"$\Leftarrow$". The sufficiency of the conditions (93) is evident on retracing the steps of the proof of their necessity in reverse order. The sufficiency also follows directly by substituting into formula (92) for $\Delta(h_2, h_3, h_4)$ the expressions for h_2, h_3 and h_4 in terms of r and s. The result vanishes identically in r and s. $\boxtimes$

The following theorem may be proved by elementary algebra on substituting into the formulas (48) and (49) giving g_2 and g_2 the expressions for h_2, h_3 and h_4 given in (93).

Theorem 6.2. If (h) is a singular elliptic sequence, then with the notation of theorem 6.1,

$$g_2 = 3\left(\frac{r^2 - 4s^3}{6s^2}\right)^2, \qquad g_3 = -\left(\frac{r^2 - 4s^3}{6s^2}\right)^3. \tag{106}$$

Now if e_1, e_2 and e_3 denote as usual the roots of $4x^3 - g_2 x - g_3 = 0$, then by the definition of the discriminant $\Delta = 0$ if and only if two or more of the roots e_i are equal. Hence we obtain the following two corollaries to theorem 6.2.

Corollary 6.3. Suppose that $\Delta = 0$. Let e_1 and e_2 be the roots of $4x^3 - g_2 x - g_3$ that are equal, i.e. $e_1 = e_2$. Then

$$g_2 = 3e_3^2, \qquad g_3 = e_3^3. \tag{107}$$

PROOF. We have

$$4x^3 - g_2 x - g_3 = 4(x - e_1)(x - e_2)(x - e_3) =$$
$$4x^3 - 4(e_1 + e_2 + e_3)x^2 + 4(e_1 e_2 + e_1 e_3 + e_2 e_3)x - 4e_1 e_2 e_3,$$

so that $e_1 + e_2 + e_3 = 0$. As $e_1 = e_2$, it follows that $e_3 = -2e_1$. Therefore,

$$g_2 = -(e_1 e_2 + e_1 e_3 + e_2 e_3) = -4(e_1^2 - 2e_1^2 - 2e_1^2) = 12e_1^2 = 3e_3^2.$$

Furthermore,

$$g_3 = 4e_1 e_2 e_3 = 4e_1^2(-2e_1) = -8e_1^3 = e_3^3. \boxtimes$$

Corollary 6.4. If (h) is a singular sequence, then the roots of $4x^3 - g_2 x - g_3$ are

$$e_1 = e_2 = \frac{r^2 - 4s^3}{12s^2}, \qquad e_3 = -\frac{r^2 - 4s^3}{6s^2}.$$

Furthermore, $g_2 = g_3 = 0$ if and only if $r^2 = 4s^3$. In this case, $e_1 = e_2 = e_3 = 0$.

6.2 Equivalence of sequences

Definition 6.5. Two sequences (u) and (v) (which need neither be integral, or solutions of (21)) are said to be *equivalent* if and only if there exists a constant $c \neq 0$ such that

$$u_n = c^{n^2 - 1} v_n, \qquad n = 0, 1, 2, \ldots$$

We write $(u) \sim (v)$ or $(u) = c(v)$ if it is desired to bring the constant c explicitly in evidence.$\Diamond$

The relation $\sim$ is evidently an equivalence relation. We shall show in chapter [CHAPTER] that there are only four different types of non-equivalent solutions of (21), of which the elliptic function and circular function solutions will turn out to be the most important.

A sequence (α) of algebraic numbers is said to be *essentially integral* if it is equivalent to an intgegral sequence; that is, if there exists an algebraic number β other than zero such that $\beta^{n^2-1}\alpha_n$ is a rational integer for every n.

Theorem 6.6. If a sequence (u) is a particular solution of (21), so are all sequences equivalent to it. Furthermore, if (u) is general, so are all its equivalent sequences.

PROOF. Suppose that (v) is a sequence equivalent to (u). Then there exists a constant c such that for every n we have $v_n = c^{n^2-1}u_n$. Therefore

$$v_{m+1}v_{m-1}v_n^2 - v_{n+1}v_{n-1}u_m^2 =$$

$$c^{(m+1)^2-1}v_{m+1}c^{(m-1)^2-1}v_{m-1}c^{2n^2-2}v_n^2 - c^{(n+1)^2-1}v_{n+1}c^{(n-1)^2-1}v_{n-1}c^{2m^2-2}v_m^2 =$$

$$c^{2m^2+2n^2-2}\left(u_{m+1}u_{m-1}u_n^2 - u_{n+1}u_{n-1}u_m^2\right) = c^{(m+n)^2+(m-n)^2-2}\left(u_{m+n}u_{m-n}\right) =$$

$$c^{(m+n)^2-1}u_{m+n}c^{(m-n)^2-1}u_{m-n} = v_{m+n}v_{m-n}.$$

Thus, the sequence (v) also satisfies (21).

Suppose now that (u) is general. Recall that for a general sequence the first two initial values are zero and one and neither the third nor the fourth value vanishes. We have $v_0 = u_0 = 0$, $v_1 = u_1 = 1$, $v_3 = c^8u_3$, $v_4 = c^{15}u_4$. As $c \neq 0$, neither v_3 nor v_4 vanishes, so that (v) is a general sequence. $\boxtimes$

Theorem 6.7. Let (h) be a general elliptic divisibility sequence which has an elliptic function representation by means of $\wp(w) = \wp(w;\ g_2, g_3)$. If $(k) = c(h)$ is any equivalent sequence, then (k) admits an elliptic function representation by means of $\wp(w') = \wp(w';\ g_2', g_3')$ where $g_2' = c^4g_2$, $g_3' = c^6g_3$, $w' = w/c$.

PROOF. By theorem 6.6 the sequence (k) is a general elliptic divisibility sequence. By theorem 4.1 there exist two rational numbers g_2' and g_3' and a complex constant w' such that $k_n = \psi_n(w')$, where $\psi_n(w')$ is defined in terms of $\wp(w';\ g_2', g_3')$. As $(k) = c(h)$, it follows that $k_2 = c^3h_2$, $k_3 = c^8h_3$, $k_4 = c^{15}h_4$. On replacing h_2, h_3 and h_4 with these expressions in (48) and (49), we obtain formulas for g_2' and g_3' in terms of h_2, h_3, h_4 and c, which after a straightforward computation yield the following identities:

$$g_2' = c^4g_2, \qquad g_3' = c^6g_3.$$

Furthermore, $k_2 = -\wp'(w';\ g_2', g_3') = -c^3h_2 = -c^3\wp'(w;\ g_2, g_3)$. As the first term in the power series expansion of $\wp'$ at z is $-2/z^3$ regardless of the values of g_2 and g_3, it follows that

$$\frac{2}{w'^3} = \frac{2c^3}{w^3},$$

so that $w' = w/c$. $\boxtimes$

Theorem 6.8. Every proper solution (a) of (21) in rational numbers is essentially integral, and equivalent to an integral divisibility sequence.

REMARK. We postpone the proof for the case $a_2 = 0$ to section 7.2, where we will treat elliptic divisibility sequences (h) with $h_2 = 0$.

PROOF. Let (a) be a proper rational solution of (21) so that $a_0 = 0$, $a_1 = 1$, $a_2 \neq 0$ and a_n is rational for every n. We will show that $(a) \sim (b)$ for some integral elliptic divisibility sequence (b). The sequence (a) is clearly determined by the values a_2, a_3, a_4. Now let d be the least common multiple of their denominators. Then we may write $a_2 = c_2/d$, $a_3 = c_3/d$, $a_4 = c_4/d$ where c_2, c_3 and c_4 are integers and $c_2 \neq 0$. Let (b) be the sequence defined by

$$b_n = (c_2 d)^{n^2-1} a_n.$$

By definition, $(a) \sim (b)$. Moreover, we have

$$b_2 = c_2^3 d^3 a_2 = c_2^4 d^2, \qquad b_3 = c_2^8 d^8 a_3 = c_2^8 c_3 d^7, \qquad b_4 = c_2^{15} d^{15} a_4 = c_2^{15} c_4 d^{15}.$$

By theorem 6.6, (b) is a solution of (21). Since b_2, b_3 and b_4 are integers and $b_2 | b_4$, it follows by theorem 3.13 that (b) is an integral elliptic divisibility sequence. ☒

Theorem 6.8 means that there is no real advantage in studying elliptic sequences over elliptic divisibility sequences. We may now prove a converse to theorem 4.1.

Theorem 6.9. If the invariants g_2 and g_3 of the function $\wp(z)$ are rational numbers and if $u \in \mathbb{C}$ is the constant from theorem 4.1, then the sequence defined by $a_n = \psi_n(u)$ is equivalent to an integral elliptic divisibility sequence.

PROOF. Note that by theorem 4.1, $\wp(u)$ is a rational number. By (52), $\psi_n(u) = d_n \sum_{k=0}^{q} A_k \wp(u)^k$ where d_n equals 1 or $-\wp'(u)$ – an integer – according as n is odd or even. In section 4.2 we saw that the coefficients A_k are rational. Therefore, $a_n = \psi_n(u)$ is rational for every n. But $\psi_n(u)$ satisfies (21), so by theorem 6.8 the sequence (a) is equivalent to an integral elliptic divisibility sequence. ☒

6.3 Equivalence classes of singular sequences

We will prove instantly that there are only two classes of *singular* elliptic divisiblity sequences, but first we will develop some lemmas, the first of which is due to Édouard Lucas.[9]

Lemma 6.10. Let α and β be two distinct complex numbers neither of which is zero, and let $p = \alpha + \beta$, $q = \alpha\beta$, $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. Then

$$q^{(1-n)/2} u_n \tag{108}$$

is a solution of (21).

PROOF. Let $v_n = q^{(1-n)/2} u_n$. We have

$$v_{m+n} v_{m-n} = q^{\frac{1-(m+n)}{2}} \cdot \frac{\alpha^{m+n} - \beta^{m+n}}{\alpha - \beta} \cdot q^{\frac{1-(m-n)}{2}} \cdot \frac{\alpha^{m-n} - \beta^{m-n}}{\alpha - \beta} =$$

$$q^{1-m} \cdot \frac{\alpha^{2m} - \alpha^{m+n}\beta^{m-n} - \alpha^{m-n}\beta^{m+n} + \beta^{2m}}{(\alpha-\beta)^2} = (\alpha\beta)^{1-m} \cdot \frac{\alpha^{2m} - \alpha^{m+n}\beta^{m-n} - \alpha^{m-n}\beta^{m+n} + \beta^{2m}}{(\alpha-\beta)^2} =$$

$$\frac{\alpha^{m+1}\beta^{1-m} - \alpha^{n+1}\beta^{1-n} - \alpha^{1-n}\beta^{n+1} + \alpha^{1-m}\beta^{m+1}}{(\alpha-\beta)^2}.$$

On the other hand,

$$v_{m+1} v_{m-1} v_n^2 =$$

[9] See Lucas [6].

$$q^{-m/2}\cdot\frac{\alpha^{m+1}-\beta^{m+1}}{\alpha-\beta}\cdot q^{\frac{2-m}{2}}\cdot\frac{\alpha^{m-1}-\beta^{m-1}}{\alpha-\beta}\cdot q^{1-n}\cdot\left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)^2=$$
$$q^{2-m-n}\cdot\frac{\left(\alpha^{2m}-\alpha^{m+1}\beta^{m-1}-\alpha^{m-1}\beta^{m+1}+\beta^{2m}\right)\left(\alpha^n-\beta^n\right)^2}{(\alpha-\beta)^4}.$$

Now on substituting $\alpha\beta$ for q, one sees that the numerator A of this expression is equal to

$$\left(\alpha^{m-n+2}\beta^{2-m-n}-\alpha^{3-n}\beta^{1-n}-\alpha^{1-n}\beta^{3-n}+\alpha^{2-m-n}\beta^{m-n+2}\right)\left(\alpha^{2n}-2\alpha^n\beta^n+\beta^{2n}\right)=$$
$$[\alpha^{m+n+2}\beta^{2-m-n}-2\alpha^{m+2}\beta^{2-m}+\alpha^{m-n+2}\beta^{n-m+2}]+[-\alpha^{n+3}\beta^{1-n}+2\alpha^3\beta-\alpha^{3-n}\beta^{n+1}]+$$
$$[-\alpha^{n+1}\beta^{3-n}+2\alpha\beta^3-\alpha^{1-n}\beta^{n+3}]+[\alpha^{n-m+2}\beta^{m-n+2}-2\alpha^{2-m}\beta^{m+2}+\alpha^{2-m-n}\beta^{m+n+2}].$$

Furthermore, $v_{n+1}v_{n-1}v_m^2$ equals $B/(\alpha-\beta)^4$, where B is obtained from A by interchanging m and n. So we have $v_{m+1}v_{m-1}v_n^2-v_{n+1}v_{n-1}v_m^2=(A-B)/(\alpha-\beta)^4$. As the terms of A which are symmetric in m and n cancel out in $A-B$, we see that

$$A-B=\left(-2\alpha^{m+2}\beta^{2-m}-\alpha^{n+3}\beta^{1-n}-\alpha^{3-n}\beta^{n+1}-\alpha^{n+1}\beta^{3-n}-\alpha^{1-n}\beta^{n+3}-2\alpha^{2-m}\beta^{m+2}\right)+$$
$$\left(2\alpha^{n+2}\beta^{2-n}+\alpha^{m+3}\beta^{1-m}+\alpha^{3-m}\beta^{m+1}+\alpha^{m+1}\beta^{3-m}+\alpha^{1-m}\beta^{m+3}+2\alpha^{2-n}\beta^{n+2}\right)=$$
$$\alpha^2\cdot[\alpha^{m+1}\beta^{1-m}-\alpha^{n+1}\beta^{1-n}-\alpha^{1-n}\beta^{n+1}+\alpha^{1-m}\beta^{m+1}]-$$
$$2\alpha\beta\cdot[\alpha^{m+1}\beta^{1-m}-\alpha^{n+1}\beta^{1-n}-\alpha^{1-n}\beta^{n+1}+\alpha^{1-m}\beta^{m+1}]+$$
$$\beta^2\cdot[\alpha^{m+1}\beta^{1-m}-\alpha^{n+1}\beta^{1-n}-\alpha^{1-n}\beta^{n+1}+\alpha^{1-m}\beta^{m+1}]=$$
$$(\alpha-\beta)^2[\alpha^{m+1}\beta^{1-m}-\alpha^{n+1}\beta^{1-n}-\alpha^{1-n}\beta^{n+1}+\alpha^{1-m}\beta^{m+1}].$$

On dividing this last expression by $(\alpha-\beta)^4$, we find that

$$v_{m+1}v_{m-1}v_n^2-v_{n+1}v_{n-1}v_m^2=\frac{\alpha^{m+1}\beta^{1-m}-\alpha^{n+1}\beta^{1-n}-\alpha^{1-n}\beta^{n+1}+\alpha^{1-m}\beta^{m+1}}{(\alpha-\beta)^2}=v_{m+n}v_{m-n}.\boxtimes$$

We call (108) a *Lucas solution* of (21), or a *Lucas sequence*. We restate the lemma of Lucas in a way which is more convenient for our purposes. Since neither α nor β is zero, we may let $a=\sqrt{\alpha/\beta}$ and $b=\sqrt{\beta/\alpha}$. Then $P:=a+b=p/\sqrt{q}$ and $Q:=ab=1$. Moreover,

$$U_n:=\frac{a^n-b^n}{a-b}=\frac{\frac{\sqrt{\alpha}^n}{\sqrt{\beta}^n}-\frac{\sqrt{\beta}^n}{\sqrt{\alpha}^n}}{\frac{\sqrt{\alpha}}{\sqrt{\beta}}-\frac{\sqrt{\beta}}{\sqrt{\alpha}}}=\frac{\frac{\alpha^n-\beta^n}{\sqrt{q}^n}}{\frac{\alpha-\beta}{\sqrt{q}}}=\frac{1}{\sqrt{q}^{n-1}}\,\frac{\alpha^n-\beta^n}{\alpha-\beta}=q^{(1-n)/2}\,\frac{\alpha^n-\beta^n}{\alpha-\beta}=q^{(1-n)/2}u_n.$$

Hence we may state the following modification of lemma 6.10.

Lemma 6.11. Every Lucas solution of (21) is of the form

$$U_n=\frac{a^n-b^n}{a-b}\tag{109}$$

where $P=a+b$ and $Q=ab=1$.

On writing the number a in polar form, we see that $a = re^{it}$ for certain real numbers r and t. Since $r = e^s$ for some real number s, it follows that $a = e^{s+it}$. Now let $\theta = t - si$, so that $a = e^{i\theta}$ and $b = 1/a = e^{-i\theta}$. Then

$$U_n = \frac{a^n - b^n}{a-b} = \frac{a^n - a^{-n}}{a-b} = \frac{e^{in\theta} - e^{-in\theta}}{e^{i\theta} - e^{-i\theta}} = \frac{(e^{in\theta} - e^{-in\theta})/2i}{(e^{i\theta} - e^{-i\theta})/2i} = \frac{\sin(n\theta)}{\sin(\theta)}.$$

Hence the sequence (U) can be parameterized by circular functions.

We shall assume that[10] $P \neq 0$, as otherwise (U) is not general since $U_2 = (a^2 - b^2)/(a-b) = a+b = P$.

Lemma 6.12. A necessary and sufficient condition that a general[11] elliptic sequence be a Lucas solution of (21) is that it be a singular solution with $r = P$ and $s = 1$, where r and s denote the numbers from theorem 6.1.

PROOF. We compute the initial values of the Lucas solution (109) with $Q = 1$ and compare them with the initial values of a singular elliptic divisibility sequence. We have $U_0 = 0$, $U_1 = 1$, $U_2 = P$. By long division one obtains, on using the identity $ab = 1$:

$$U_3 = \frac{a^3 - b^3}{a-b} = a^2 + b^2 + 1 = (a+b)^2 - 2ab + 1 = P^2 - 1,$$

$$U_4 = \frac{a^4 - b^4}{a-b} = a^3 + b^3 + a + b = (a+b)^3 - 3a^2b - 3ab^2 + a + b = (a+b)^3 - 2a - 2b = P^3 - 2P.$$

Thus the initial values of (U) are in short:

$$0,\ 1,\ P,\ P^2 - 1,\ P^3 - 2P.$$

From theorem 6.1 we know that the initial values of a general singular elliptic divisibility sequence (h) are

$$0,\ 1,\ r,\ s(r^2 - s^3),\ rs^3(r^2 - 2s^3).$$

The initial values of (U) are equal to the initial values of (h) if and only if $r = P$, $s = 1$. ☒

Now we are able to show that there exist only two equivalence classes of singular elliptic divisibility sequences.

Theorem 6.13. Every singular elliptic divisibility sequence is equivalent to either the sequence

$$0, 1, 2, 3, 4, 5 \ldots \tag{110}$$

or to a Lucas sequence.

PROOF. Let (h) be a singular elliptic divisibility sequence, so that $\Delta(h) = 0$. Suppose first that $g_2 = g_3 = 0$. Then it follows from corollary 6.4 that $r^2 = 4s^3$. Consequently, r must be even, so that $r = 2t$ for some integer t. This yields $t^2 = s^3$, whereupon we conclude that t must be a third power. So for some integer c we have $t = c^3$, which implies $r = 2c^3$ and $s = c^2$. Then by (93),

$$h_2 = c^3 2, \qquad h_3 = c^8 3, \qquad h_4 = c^{15} 4.$$

[10] Lucas solutions of (21) with $P = 0$ are discussed in chapter 7.

[11] Solutions with $h_2 = 0$, $h_3 \neq 0$ are equivalent to a Lucas solution. Solutions with $h_2 \neq 0$, h_3 are not generally Lucas solutions. See chapter 7.

It now follows by a simple induction on n that $h_n = c^{n^2-1}n$ for every n. Thus (h) is equivalent to the sequence $0,1,2,3,\ldots$, as was to be shown.

Now consider any singular sequence (h) with g_2 and g_3 not both zero. By theorem 6.1,

$$h_2 = r, \qquad h_3 = s(r^2 - s^3), \qquad h_4 = rs^3(r^2 - 2s^3)$$

where r and s are integers and $rs(r^2 - 2s^3) \neq 0$. Now let $c, P \in \mathbb{C}$ such that $r = c^3P$, $s = c^2$. Then c is in general a quadratic irrationality. Hence $P = r\sqrt{s}/s$ is in general a quadratic irrationality. Then (93) becomes

$$h_2 = c^3P, \qquad h_3 = c^8(P^2 - 1), \qquad h_4 = c^{15}(P^3 - 2P).$$

Hence (h) is equivalent to a Lucas solution with P given by $r\sqrt{s}/s$ and $Q = 1$. This completes the proof of the theorem. $\boxtimes$

7 Special sequences

We have seen that any sequence (h) whose initial values satisfy the conditions

$$h_0 = 0, \qquad h_1 = 1, \qquad h_2 \neq 0, \qquad h_3 \neq 0$$

may be parametrized by elliptic or circular functions. In this chapter we discuss the special sequences which arise when one or more of the above conditions are violated. Until further notice, (h) denotes a sequence of complex numbers satisfying (21), so that

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \qquad m \geqslant n \geqslant 1.$$

7.1 The case $h_1 \neq 1$

Sequences with $h_1^2 \neq 1$ are uninteresting. For on first letting $m = 1$ and $n = 1$, then $m = n$ and $n = 1$ and finally $m = n$ and $n = n$ in (21), we obtain the relations

$$h_0h_2 = 0, \qquad (h_1^2 - 1)h_{n+1}h_{n-1} = 0, \qquad n \geqslant 1; \tag{111}$$

$$h_0h_{2n} = 0. \tag{112}$$

Now if $h_1^2 \neq 1$, $h_{m+n}h_{m-n} = 0$. Hence since n is arbitrary, we see from (21) that $h_{m+n}h_{m-n} = 0$ for $m \geqslant n \geqslant 1$. The integers $m+n$ and $m-n$ are of the same parity. We claim that there can be at most two non-vanishing terms in (h) and their suffices must have opposite parity. Indeed, let r and s be suffices of the same parity and suppose $r \geqslant s$. Then we can write $h_rh_s = h_{m+n}h_{m-n} = 0$with $m = (r+s)/2$ and $n = (r-s)/2$, both integers $\geqslant 0$ as r and s have the same parity and $r \geqslant s$. Thus either h_r or h_s equals zero.

Conversely, if k and l are any integers $\geqslant 0$, then the sequence (h) defined by

$$h_n = \begin{cases} 0 & \text{if } n \neq k,\ n \neq k+2l+1 \\ \text{arbitrary} & \text{if } n = k \text{ or } n = k+2l+1 \end{cases}$$

defines a solution of (21).

We shall assume henceforth that $h_1^2 = 1$. There is no loss of generality in assuming that $h_1 = 1$, for if h_n is a solution of (21), so is the sequence k_n defined by $(-1)^n h_n$. Indeed, on the one hand we have

$$k_{m+n}k_{m-n} = (-1)^{2m-2n}h_{m+n}h_{m-n} = h_{m+n}h_{m-n}$$

and on the other we have

$$k_{m+1}k_{m-1}k_n^2 - k_{n+1}k_{n-1}k_m^2 = (-1)^{2m-2n}\left[h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2\right] = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2.$$

As (h) is a solution of (21), it now follows that (k) is a solution too.

7.2 The case $h_2 = 0$

Assume that $h_2 = 0$. We see from (111) that a sufficient condition that $h_2 = 0$ is that $h_0 \neq 0$.

Lemma 7.1. The sequence given by $h_n = \sin(n\pi/2)$ for $n > 0$ is a Lucas sequence and a solution of (21). It is periodic with period four and purely periodic if and only if $h_0 = 0$.

PROOF. The last assertion follows directly from the periodicity of the sine function. Furthermore, we have $h_n = \sin n\theta / \sin\theta$ with $\theta = \pi/2$. Therefore, (h) is a Lucas sequence. Finally, we have to verify that

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$$

for all $m \geqslant n \geqslant 1$. Since terms with even suffix > 0 vanish, the equation holds if m and n have the same parity: both the left-hand side and the right-hand side become zero.

Now suppose m and n have opposite parity, say m odd and n even (the case m even and n odd is treated analogously). Then either $m \equiv 1$ or $m \equiv 3 \pmod 4$ and either $n \equiv 0$ or $n \equiv 2 \pmod 4$. We show the validity of (21) by straightforward computation.

$m \pmod 4$	$n \pmod 4$	$h_{m+n}h_{m-n}$	$h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2$
1	0	1	1
3	0	1	1
1	2	1	1
3	2	1	1

Therefore, (h) is a solution of (21). ☒

Definition 7.2. Let n be a non-zero integer with prime factorization $n = u \cdot p_1^{e_1} \cdots p_k^{e_k}$ where u is a unit (i.e. either $+1$ or -1) and the p_i are primes. Let a be an integer. The *Kronecker symbol* (a/n) is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{u}\right) \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i},$$

where for odd p_i the number (a/p_i) is simply the Legendre symbol:

$$\left(\frac{a}{p_i}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p_i} \\ +1 & \text{if } a \not\equiv 0 \pmod{p_i} \text{ and for some integer } x \text{ one has } x^2 \equiv a \pmod{p_i} \\ -1 & \text{otherwise.} \end{cases}$$

If $p_i = 2$, we define

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } a \text{ is even} \\ +1 & \text{if } a \equiv \pm 1 \pmod 8 \\ -1 & \text{if } a \equiv \pm 3 \pmod 8. \end{cases}$$

Finally, we put $(a/1) = 1$ and

$$\left(\frac{a}{-1}\right) = \begin{cases} -1 & \text{if } a < 0 \\ +1 & \text{if } a \geqslant 0 \end{cases}, \qquad \left(\frac{a}{0}\right) = \begin{cases} 1 & \text{if } a = \pm 1 \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 7.3. The Kronecker symbol sequence given by $h_n = (-8/n)$ is a solution of (21) such that $h_2 = 0$. Furthermore, $h_n = (-8/n)$ equals $(-1)^{(n^2-1)/8} \sin(n\pi/2)$, so that (h) is essentially a Lucas solution, of period eight.

PROOF. That (h) is periodic with period eight follows from a result due to Edmund Landau.[12] The sequence (g) given by $g_n = (-1)^{(n^2-1)/8}\sin(n\pi/2)$ obviously is periodic with period eight as well. We will show by computating the first eight values of (h) and (g) that these sequences are in fact identical. The values are listed in the following table.

n	h_n	g_n
0	0	0
1	$\left(\frac{-8}{1}\right) = 1$	$(-1)^0 \sin\frac{\pi}{2} = 1$
2	0	0
3	$\left(\frac{-8}{3}\right) = 1$	$(-1)^{(9-1)/8}\sin\frac{3\pi}{2} = -1\cdot -1 = 1$
4	0	0
5	$\left(\frac{-8}{5}\right) = -1$	$(-1)^{(25-1)/8}\sin\frac{5\pi}{2} = (-1)^3\cdot 1 = -1$
6	0	0
7	$\left(\frac{-8}{7}\right) = -1$	$(-1)^{(49-1)/8}\sin\frac{7\pi}{2} = (-1)^6\cdot -1 = -1$

From this table and the periodicity of (h) and (g), we conclude that $h_n = g_n$ for all $n \geqslant 0$. By lemma 7.1, the sequence (k) given by $k_n = \sin(n\pi/2)$ is a solution of (21). Now $(g) \sim (k)$, since $g_n = c^{n^2-1}k_n$ where $c = (-1)^{1/8}$. As $(h) = (g)$, we have $(h) \sim (k)$, so that by theorem 6.6, (h) is also a solution of (21). ☒

Lemma 7.4. For all odd $n \geqslant 0$ we have the identity

$$(-1)^{(n^2-1)/8}\sin(n\pi/2) = (-1)^{[n/4]}. \tag{113}$$

Thus yet another guise of the Kronecker symbol solution is:

$$(-8/n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ (-1)^{[n/4]} & \text{if } n \text{ is odd.} \end{cases}$$

PROOF. Let n be an odd integer. Then either $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$. If $n \equiv 1 \pmod 4$, we have $n = 4k+1$ for some k. Then

$$(-1)^{(n^2-1)/8}\sin(n\pi/2) = (-1)^{(16k^2+8k)/8}\sin(2k\pi+\pi/2) = (-1)^{2k^2+k}\sin(\pi/2) = (-1)^k.$$

On the other hand, $[n/4] = [(4k+1)/4] = [k+1/4] = k$, so that $(-1)^{[n/4]} = (-1)^k$. This proves (113) for $n \equiv 1 \pmod 4$.

If $n \equiv 3 \pmod 4$, $n = 4k+3$ for some k. Then

$$(-1)^{(n^2-1)/8}\sin(n\pi/2) = (-1)^{(16k^2+24k+8)/8}\sin(2\pi+3\pi/2) =$$

$$(-1)^{2k^2+3k+1}\sin(3\pi/2) = (-1)^{k+1}(-1) = (-1)^{k+2} = (-1)^k.$$

On the other hand, $[n/4] = [(4k+3)/4] = [k+3/4] = k$, so that $(-1)^{[n/4]} = (-1)^k$. This proves (113) for $n \equiv 3 \pmod 4$. ☒

We shall now show that there is no solution of (21) with $h_0 = 0$, $h_1 = 1$, $h_2 = 0$ and $h_3 \neq 0$ other than the Kronecker symbol solution.

[12] Edmund Landau, *Vorlesungen über Zahlentheorie* (1927), erster Band. Satz 99.3, p.54.

Theorem 7.5. Every solution (h) of (21) with $h_1 = 1$, $h_2 = 0$ and $h_3 \neq 0$ is equivalent to the Kronecker symbol solution, and is hence a Lucas solution. That is, for $n > 0$,

$$h_n = \begin{cases} 0 & \text{if } n \text{ is even} \\ (-1)^{[n/4]} h_3^{(n^2-1)/8} & \text{if } n \text{ is odd.} \end{cases} \tag{114}$$

PROOF. Let n be odd, say $n = 2m+1$. We claim that

$$\left[\frac{2m+1}{4}\right] \equiv m + \frac{m(m+1)}{2} \pmod 2. \tag{115}$$

For m even, say $m = 2k$, one has

$$\left[\frac{2m+1}{4}\right] = \left[\frac{4k+1}{4}\right] = \left[k + \frac{1}{4}\right] = k.$$

On the other hand, we have

$$m + \frac{m(m+1)}{2} = 2k + \frac{4k^2+2k}{2} = 2k + 2k^2 + k \equiv k \pmod 2.$$

Hence, (115) holds if m is even.

Now suppose that m is odd, say $m = 2k+1$. Then

$$\left[\frac{2m+1}{4}\right] = \left[\frac{4k+3}{4}\right] = \left[k + \frac{3}{4}\right] = k.$$

On the other hand, we have

$$m + \frac{m(m+1)}{2} = 2k+1 + \frac{(2k+1)(2k+2)}{2} = 2k+1 + \frac{4k^2+6k+2}{2} = 2k+1+2k^2+3k+1 \equiv k \pmod 2.$$

So (115) also holds in case m is odd. Hence an equivalent way of stating (114) is:

$$h_{2n} = 0, \tag{116}$$

$$h_{2n+1} = (-1)^{[(2n+1)/4]}\, h_3^{((2n+1)^2-1)/8} = (-1)^{n+n(n+1)/2}\, h_3^{n(n+1)/2} = (-1)^n\, (-h_3)^{n(n+1)/2} \tag{117}$$

for $n \geqslant 1$.

Now we prove that the sequence (h) actually satisfies (116) and (117). Since (h) satisfies (21), we obtain on taking first $m = 2n$ and $n = 2$ and then $m = 2n-2$ and $n = 3$ the two relations

$$h_{2n+2} h_{2n-2} = -h_1 h_3 h_{2n}^2, \qquad n \geqslant 1, \tag{118}$$

$$h_{2n+1} h_{2n-5} = h_{2n-1} h_{2n-3} h_3^2, \qquad n \geqslant 3. \tag{119}$$

We now prove the validity of (116) by induction. On taking $n = 2$ in (118), we obtain $h_6 h_2 = -h_1 h_3 h_4^2$. As h_2 equals zero but h_1 and h_3 do not, we conclude that $h_4 = 0$. This proves (116) for $n = 1$. Now suppose (116) holds for all $n < k$. We wish to show that it holds for $n = k$ also. By (118), we have $h_{2k+2} h_{2k-2} = -h_1 h_3 h_{2k}^2$. By the induction hypothesis, $h_{2k-2} = 0$, which implies that $h_{2k} = 0$. Thus, (116) is true for $n = k$.

On taking $m = n+1$ and $n = n$ in (21) and using that $h_1 = 1$ we get the identity

$$h_{2n+1} = h_{n+2} h_n^3 - h_{n-1} h_{n+1}^3.$$

We thus find that $h_5 = -h_3^3$, $h_7 = -h_3^6$, so that (117) is true for $n \leqslant 3$. Now suppose (117) is true for all $3 \leqslant n < k$. Then we obtain from (119) on using the induction hypothesis:

$$h_{2k+1}\ (-1)^{k-3}(-h_3)^{(k-3)(k-2)/2} = (-1)^{k-1}(-h_3)^{(k-1)k/2}\ (-1)^{k-2}\ (-h_3)^{(k-2)(k-1)/2}\ h_3^2 \qquad \Rightarrow$$

$$h_{2k+1}\ (-1)^{k-3}(-h_3)^{(k^2-5k+6)/2} = (-1)^{2k-3}(-h_3)^{(2k^2-4k+6)/2} \qquad \Rightarrow$$

$$h_{2k+1} = (-1)^k(-h_3)^{k(k+1)/2},$$

so that (117) holds also for $n = k$. ☒

We are now ready to give the proof of theorem 6.8 for the case $a_2 = 0$, as promised in section 6.2.

PROOF OF THEOREM 6.8 IN CASE $a_2 = 0$. As we have seen in this section, terms of even suffix vanish, i.e. $a_{2n} = 0$. Clearly, (a) is uniquely determined by the initial values a_2, a_3, a_4. As $a_2 = a_4 = 0$, the sequence defined by $b_n = c^{n^2-1}a_n$, where c is the eighth root of the denominator of a_3, is an integral solution of (21). ☒

7.3 The case $h_3 = 0$

We next discuss solutions with vanishing fourth term, i.e. with $h_3 = 0$. We see from (112) that if $h_0 \neq 0$, all terms of positive even suffix vanish. Since we are assuming that $h_1 = 1$, formula (22) holds: $h_{2n+1} = h_{n+2}h_n^3 - h_{n-1}h_{n+1}^3$. It now follows by a brief induction that all terms of odd suffix vanish save h_1. Conversely, the sequence given by

$$h_n = 0, \qquad n > 1, \tag{120}$$

is evidently a solution of (21) regardless of the values of h_0 and h_1. We shall therefore assume henceforth that

$$h_0 = 0, \qquad h_1 = 1, \qquad h_3 = 0. \tag{121}$$

There exist an infinite number of essentially distinct solutions of (21) meeting these conditions. For let l denote a fixed odd number greater than one and define a numerical function of n and l, $\lambda_n = \lambda_n(l)$ as follows:

$$\lambda_n = \begin{cases} 0 & \text{if } n \not\equiv \pm 1 \pmod{l} \\ 1 & \text{if } n \equiv +1 \pmod{l} \\ -1 & \text{if } n \equiv -1 \pmod{l}. \end{cases} \tag{122}$$

Theorem 7.6. If c is a constant not equal to zero, then

$$l_n = \lambda_n c^{1-n\lambda_n} \tag{123}$$

is a solution of (21) whose initial values satisfy the conditions of (121).

REMARK. In particular, on taking $c = 1$ we see that λ_n itself satisfies (21).[13] If $l = 3$, λ_n reduces to the Legendre symbol solution $(n/3)$ mentioned in example 3.11. We see incidentally that (21) has integral periodic solutions with any preassigned odd period l. However, such a solution is a divisibility sequence only if $l = 3$.

PROOF. The initial values given by formula (123) are: $l_0 = 0$, $l_1 = 1$ and $l_3 = 0$, so that (121) is satisfied.

[13] λ_n satisfies (21) if $l = 4$, but theorem 7.6 is untrue in this case for c's chosen arbitrarily.

Next we wish to show that the identity $l_{m+n}l_{m-n} = l_{m+1}l_{m-1}l_n^2 - l_{n+1}l_{n-1}l_m^2$ holds. On using (123), we see that $l_{m+n}l_{m-n}$ vanishes unless $m+n \equiv \pm 1 \pmod{l}$ and $m-n \equiv \pm 1 \pmod{l}$. Hence, since l is odd, there are only four cases when $l_{m+n}l_{m-n}$ is not zero, namely[14] (i) $m \equiv 1$, $n \equiv 0$; (ii) $m \equiv 0$, $n \equiv 1$; (iii) $m \equiv 0$, $n \equiv -1$; (iv) $m \equiv -1$, $n \equiv 0$.

Now $l_{m+1}l_{m-1}l_n^2$ vanishes unless $m \equiv 0$ and $n \equiv \pm 1$, and $l_{n+1}l_{n-1}l_m^2$ vanishes unless $n \equiv 0$ and $m \equiv \pm 1$. Hence (21) is satisfied except, perhaps, in the four cases just listed. The following table shows that the identity also holds for each of these.

case	λ_m	λ_n	λ_{m+1}	λ_{m-1}	λ_{n+1}	λ_{n-1}	λ_{m+n}	λ_{m-n}	$l_{m+n}l_{m-n}$	$l_{m+1}l_{m-1}l_n^2$	$-l_{n+1}l_{n-1}l_m^2$
(i)	1	0	0	0	1	−1	1	1	c^{2-2m}	0	c^{2-2m}
(ii)	0	1	1	−1	0	0	1	−1	$-c^{2-2n}$	$-c^{2-2n}$	0
(iii)	0	−1	1	−1	0	0	−1	1	$-c^{2-2n}$	$-c^{2-2n}$	0
(iv)	−1	0	0	0	1	−1	−1	−1	c^{2+2m}	0	c^{2+2m}

This completes the proof. ⊠

We shall next show that the solutions (l) just investigated are essentially the only type of solution of (21) with fourth term zero.

Theorem 7.7. Every solution (h) of (21) with $h_0 = 0$, $h_1 = 1$ and $h_3 = 0$ either has all its other terms zero with at most one exception, or it is equivalent to a solution (l) of the type described in theorem 7.6.

PROOF. Let (h) be a solution of (21) with $h_0 = 0$, $h_1 = 1$ and $h_3 = 0$. Then (22) holds:

$$h_{2k+1} = h_{k+2}h_k^3 - h_{k-1}h_{k+1}^3, \qquad k \geqslant 1.$$

If all terms of (h) with even suffices vanish, we find by a brief induction based on (22) that all terms of (h) of odd suffix vanish save h_1, and we have the trivial solution (120) again.

If not all terms of even suffix vanish, there is a first term which does not vanish. Consequently, there exists an odd integer l not less than three such that

$$h_0 = h_2 = h_4 = \ldots = h_{l-3} = 0, \tag{124}$$

$$h_{l-1} \neq 0. \tag{125}$$

We claim that

$$h_l = 0 \tag{126}$$

and

$$h_n = 0 \text{ for } 1 < n < l-1 \text{ if } l > 3. \tag{127}$$

For (126) is true by hypothesis if $l = 3$. If $l > 4$ (l is odd), then (127) is true for even n by (124). Now suppose (127) were false. Then there exists an odd integer y in the interval $(1, l-1)$ such that $h_y \neq 0$. Let $k > 1$ be the integer such that $2k+1 = \min\{y \in (1, l-1) \mid h_y \neq 0\}$. By (22) we find $h_{2k+1} = 0$, since $1 \leqslant k-1 < k+2 < 2k+1$. But this contradicts the assumption that $h_{2k+1} \neq 0$. Thus we have established (127). (126) now follows from (127) on taking $n = (l-1)/2$ in (22).

It may happen that $h_{l+1} = 0$. If so,

$$h_n = 0 \quad \text{for } n > l+1. \tag{128}$$

[14] We suppress the modulus l when no confusion can arise.

We prove this by induction on n. First, on taking $n = (l+1)/2$ in (22), we see that

$$h_{l+2} = h_{(l+5)/2}h^3_{(l+1)/2} - h_{(l-1)/2}h^3_{(l+3)/2}. \tag{129}$$

If $l = 3$, we obtain the expression $h_{l+2} = h_5 = h_4h_2^3 - h_1h_3^3$. Now by assumption both h_3 and $h_4 = h_{l+1}$ equal zero, so that $h_{l+2} = 0$. If $l \geqslant 5$, all suffices on the right-hand side of (129) side are $\leqslant l$. By (126) and (127), the only non-zero terms with suffix $\leqslant l$ are h_1 and h_{l-1}. If none of the suffices on the right-hand side of (129) is equal to h_1 or h_{l-1}, then h_{l+2} is obviously zero. Now if one of the suffices on the right-hand side of (129) *does* equal 1 or $l-1$, the other suffix in the product cannot also be equal to 1 or $l-1$, so that the product is zero. Thus also in this case, $h_{l+2} = 0$. The basis of the induction, (128) for $n = l+2$, has been proven.

Now suppose that (128) holds for all $l+1 < n < q$, where q is some fixed integer $\geqslant 5$. If q is odd, taking $n = (q-1)/2$ in (22) yields the relation

$$h_q = h_{(q+3)/2}h^3_{(q-1)/2} - h_{(q-3)/2}h^3_{(q+1)/2}. \tag{130}$$

Each suffix on the right-hand side is $< q$, so it either lies in the interval $(1, l+1]$ or in the interval $(l+1, q)$. By (127), (126), the assumption that $h_{l+1} = 0$ and by the induction hypothesis, the only non-zero terms of (h) with suffix $< q$ are h_1 and h_{l-1}. If none of the suffices on the right-hand side of (130) is equal to 1 or $l-1$, then h_q is obviously zero. What happens if one of the suffices *is* equal to 1 or $l-1$,[15] is listed in the following table.

q	$h_{(q+3)/2}h^3_{(q-1)/2} - h_{(q-3)/2}h^3_{(q+1)/2}$
5	$h_4h_2^3 - h_1h_3^3$
$2l+1$	$h_{l+2}h_{2l}^3 - h_{l-1}h_{l+1}^3$
$2l-1$	$h_{l+1}h_{l-1}^3 - h_{l-2}h_l^3$
$2l-3$	$h_lh_{l-2}^3 - h_{l-3}h_{l-1}^3$
$2l-5$	$h_{l-1}h_{l-3}^3 - h_{l-4}h_{l-2}^3$

The expressions in the first, fourth and fifth row equal zero because of (127) and (126). The expressions in the second and third row are zero *only* because of the assumption that $h_{l+1} = 0$, for $h_{l-1} \neq 0$ by the definition of l. We see that in any case $h_q = 0$.

Now let us consider the case where q is even, say $q = 2r$. On taking $m = r + (l-1)/2$ and $n = r - (l-1)/2$ in (21) we obtain the relation

$$h_{2r}h_{l-1} = h_{s+1}h_{s-1}h_t^2 - h_{t+1}h_{t-1}h_s^2 \tag{131}$$

where $s = r + (l-1)/2$ and $t = r - (l-1)/2$. The numbers $s, t \geqslant 0$ are chosen in such a way that $s+t = 2r$ and $s-t = l-1$. By assumption $q = 2r > l+1$. This implies $2r - l \geqslant 2$, so that $2t = 2r - l + 1 \geqslant 3$. As t is an integer, we must have $t \geqslant 2$. It follows that also $s \geqslant 2$, for $s \geqslant t$. Therefore, $s = 2r - t \leqslant 2r - 2 = q - 2$. This means that $s - 1 < s < s + 1 < q$, and analogously we derive that $t - 1 < t < t + 1 < q$. By the induction hypothesis it follows that the right-hand side of (131) is zero. By assumption $h_{l-1} \neq 0$, so that $h_q = h_{2r}$ must be zero. This concludes the proof of (128).

It is evident, conversely, that the sequence defined by $h_0 = 0$, $h_1 = 1$, $h_n = 0$ for all $n > 1$ but $n = l-1$ gives a solution of (21). The first part of the theorem is thus established, and we may assume for the remainder of the proof that $h_{l+1} \neq 0$.

[15] Such that the other three suffices are $\geqslant 0$ as well.

So assume $h_{l+1} \neq 0$. We claim that

$$h_n = 0 \quad \text{for} \quad l+1 < n < 2l-1 \quad \text{if} \quad l > 3, \tag{132}$$

$$h_{2l-1} = h_{l+1}h_{l-1}^3, \qquad h_{2l} = 0, \qquad h_{2l+1} = -h_{l-1}h_{l+1}^3. \tag{133}$$

PROOF OF (132). If n is even, on taking $m = (n+l-1)/2$ and $n = (n-l+1)/2$ in (21), we obtain

$$h_n h_{l-1} = h_{(n+l+1)/2}h_{(n+l-3)/2}h_{(n-l+1)/2}^2 - h_{(n-l+3)/2}h_{(n-l-1)/2}h_{(n+l-1)/2}^2. \tag{134}$$

Now if $n = l+3$, $h_{(n-l+3)/2} = h_3 = 0$ and $h_{(n-l+1)/2} = h_2 = 0$, so that the right-hand side of (134) equals zero, which implies $h_n = 0$ for $n = l+3$.

Now assume $n > l+3$, so that together with our assumption $n < 2l-1$ we get $l+3 < n < 2l-1$. We claim that then $(n-l\pm 1)/2 < l-1$. Indeed, we have

$$1 = \tfrac{l+3-l-1}{2} < (n-l-1)/2 < (n-l+1)/2 < (2l-1-l+1)/2 = l/2 < l.$$

Hence $h_{(n-l\pm 1)/2} = 0$ by (127), so that it follows from (134) and (125) that $h_n = 0$ for even n in the interval $(l+3, 2l-1)$. As $h_{l+3} = 0$, we conclude that $h_n = 0$ for all even n in the interval $(l+1, 2l-1)$.

Now suppose that $n \in (l+1, 2l-1)$ is odd, say $n = 2k+1$. We find directly by (22) and (127) that $h_n = 0$. This establishes (132).

PROOF OF (133). The first and third equations follow directly from (22) on taking $n = l-1$ and $n = l$ respectively. The second equation follows from (134) on putting n equal to $2l$.

We can now prove that

$$h_n = a^{n^2-1}\lambda_n c^{1-n\lambda_n} \tag{135}$$

where

$$a = (-h_{l+1}h_{l-1})^{1/2l^2}, \qquad c = (-h_{l-1})^{(2+l)/2l^2}h_{l+1}^{(2-1)/2l^2}. \tag{136}$$

Since $\lambda_n c^{1-n\lambda_n}$ is a special (l) solution, this step will complete the proof of the theorem.

PROOF OF (135). If n is less than $2l+2$ and not congruent to $\pm$ modulo l, (135) gives $h_n = 0$ in agreement with (127) and (132). On taking $n = 2l+1$ in (135), we get

$$h_{2l+1} = a^{4l^2+4l}c^{-2l} = (-h_{l-1}h_{l+1})^{\frac{4l^2+4l}{2l^2}}(-h_{l-1})^{\frac{-(2+l)2l}{2l^2}}(h_{l+1})^{\frac{-(2-l)2l}{2l^2}} =$$

$$(-h_{l-1})^{2+2/l-2/l-1}(h_{l+1})^{2+2/l-2/l+1} = -h_{l-1}h_{l+1}^3.$$

On taking $n = 2l-1$ in (135), we get

$$h_{2l-1} = -a^{4l^2-4l}c^{2l} = -(-h_{l-1}h_{l+1})^{\frac{4l^2-4l}{2l^2}}(-h_{l-1})^{\frac{(2+l)2l}{2l^2}}(h_{l+1})^{\frac{(2-l)2l}{2l^2}} =$$

$$-(-h_{l-1})^{2-2/l+2/l+1}(h_{l+1})^{2-2/l+2/l-1} = -(-h_{l-1})^3 h_{l+1} = h_{l-1}^3 h_{l+1}.$$

On taking $n = l \pm 1$ in $a^{n^2-1}\lambda_n c^{1-n\lambda_n}$, we obtain $h_{l\pm 1}$, as is readily seen. Thus for $n = l \pm 1$, (135) truly holds and for $n = 2l \pm 1$, (135) gives the values $h_{2l\pm 1}$ already found.

We now proceed by induction. Suppose that we have proved that the formula (135) gives the solution

(h) for $0 \leqslant n < m$, where we are entitled by what proceeds to assume that $m \geqslant 2l+2$. Since (h) satisfies (21), we obtain on taking $m = m$ and $n = l$ the relation

$$h_{m+l}h_{m-l} = -h_{l+1}h_{l-1}h_m^2. \tag{137}$$

Now if $m \not\equiv \pm 1 \pmod{l}$, then $h_{m-l} = 0$ by the induction hypothesis. Hence $h_m = 0$ unless $m \equiv \pm 1 \pmod{l}$. Hence by the definition of λ_n, (135) is true if $n = m$ and $m \not\equiv \pm 1 \pmod{l}$.

Now assume $m \equiv \pm 1 \pmod{l}$. On taking $m = m - l$ and $n = l$ in (21), we obtain the formula

$$h_m h_{m-2l} = -h_{l+1}h_{l-1}h_{m-l}^2. \tag{138}$$

Since $m \geqslant 2l+2$, $m - 2l > 0$ and it follows by the induction hypothesis that $h_{m-2l} \neq 0$. Therefore, $h_m = -h_{l+1}h_{l-1}h_{m-l}^2/h_{m-2l}$. By the induction hypothesis, we may now replace h_{m-l} and h_{m-2l} with the expressions obtained from (135) by putting $n = m - l$ and $n = m - 2l$ respectively. This gives us

$$h_m = \frac{-h_{l+1}h_{l-1}h_{m-l}^2}{h_{m-2l}} = \frac{-h_{l+1}h_{l-1}a^{2m^2-4lm+2l^2-2}c^{2\pm(2l-2m)}}{(\pm 1)a^{m^2-4lm+4l^2-1}c^{1\pm(2l-m)}} = (\pm 1)(-h_{l+1}h_{l-1})a^{m^2-2l^2-1}c^{1\mp m}.$$

As $a = (-h_{l+1}h_{l-1})^{1/2l^2}$, it follows that $-h_{l+1}h_{l-1} = a^{2l^2}$. Therefore,

$$(\pm 1)(-h_{l+1}h_{l-1})a^{m^2-2l^2-1}c^{1\mp m} = (\pm 1)a^{m^2-1}c^{1\mp m} = a^{m^2-1}\lambda_m c^{1-m\lambda_m}.$$

We have thus derived (135) for $n = m$ with $m \equiv \pm 1 \pmod{l}$ also. In short, we have shown that if (135) holds for $0 \leqslant n < m$, then it holds for $0 \leqslant n < m = 1$. Hence it is generally true by induction.

That conversely (135) is a solution of (21) is a trivial consequence of theorem 7.6. This concludes the proof of theorem 7.7. $\boxtimes$

If we exclude from consideration the trivial solutions of (21) already discussed, in which all except a finite number of terms are zero, we may summarize the results of chapters 4, 5, 6 and the present as follows.

Theorem 7.8. Any non-trivial solution (h) of

$$\omega_{m+n}\omega_{m-n} = \omega_{m+1}\omega_{m-1}\omega_n^2 - \omega_{n+1}\omega_{n-1}\omega_m^2$$

is equivalent to one of the following four solutions:

$$h_n = n, \qquad h_n = \frac{\sin n\theta}{\sin\theta}, \qquad h_n = \frac{\sigma(nu)}{\sigma(u)^{n^2}}, \qquad h_n = \lambda_n c^{1-n\lambda_n}.$$

We have already remarked that the only non-trivial solutions of (21) with fourth term zero which can be divisibility sequences are those for which $l = 3$ so that h_3 is zero, but h_2 and h_4 are not zero. The formulas of theorem 7.7 then give the general term of the sequence (h).

The question arises whether or not such a solution can be parameterized by elliptic functions, so that with a proper choice of invariants, $h_n = \psi_n(u)$. But in section 4.1 we derived that

$$h_2 = \psi_2(u) = -\wp'(u), \qquad h_3 = \psi_3(u), \qquad h_4 = \psi_4(u) = \wp'(u)\big[\wp'(u)^4 - \psi_3(u)\wp''(u)\big].$$

Consequently, if $h_3 = 0$, it is necessary that $h_4 = -h_2^5$ for such a parameterization to be possible. But if this condition is satisfied, h_n reduces to $(-h_2)^{(n^2-1)/3}(n/3)$, so that (h) is equivalent to the Legendre symbol solution $(n/3)$.

n	k	$(-1)^{n^2-1}$	$(-1)^{1-(n/3)n}$
$3k$	odd	$(-1)^{9k^2-1}=1$	$(-1)^{1-0}=-1$
$3k$	even	$(-1)^{9k^2-1}=-1$	$(-1)^{1-0}=-1$
$3k+1$	odd	$(-1)^{9k^2+6k}=-1$	$(-1)^{1-3k-1}=-1$
$3k+1$	even	$(-1)^{9k^2+6k}=1$	$(-1)^{1-3k-1}=1$
$3k+2$	odd	$(-1)^{9k^2+12k+3}=1$	$(-1)^{1+3k+2}=1$
$3k+2$	even	$(-1)^{9k^2+12k+3}=-1$	$(-1)^{1+3k+2}=-1$

Now the Legendre symbol solution $(n/3)$ is equivalent to $(n/3)(-1)^{n^2-1}$. The following table shows that for n not divisible by 3 we have $(-1)^{n^2-1}=(-1)^{1-(n/3)n}$.
As $(n/3)=0$ if n is divisible by 3, for all n we have the identity $(n/3)(-1)^{n^2-1}=(n/3)(-1)^{1-(n/3)n}$. Therefore, the Legendre symbol solution $(n/3)$ is equivalent to $(n/3)(-1)^{1-(n/3)n}$, which is nothing but the special λ_n solution for $l=3$ and $c=-1$. This is evidently expressible as the Lucas solution

$$U_n=\frac{\sin(2n\pi/3)}{\sin(2\pi/3)}$$

satisfying the recurrence $U_{n+2}=U_{n+1}-U_n$. We now state our results in a theorem.

Theorem 7.9. If (h) is an elliptic divisibility sequence with the initial values $0,1,h_2,0,h_4$ where $h_2h_4\neq 0$, then (h) cannot be parameterized in terms of elliptic functions unless $h_4=-h_2^5$. If so, (h) is equivalent to the Lucas solution $\frac{\sin(2n\pi/3)}{\sin(2\pi/3)}$.

8 Periodic sequences

We shall determine in this chapter all periodic elliptic sequences other than the special periodic sequences (λ) already discussed in section 7.3. We shall be concerned here then with sequences (h) with $h_0 = 0$, $h_1 = 1$ and not both h_2 and h_3 zero. By lemma 3.12, if two consecutive terms of such a sequence vanish, then all terms vanish beyond the third, and we have the trivial solution $0, 1, h_2, 0, 0, 0, \ldots$ of period one. It is easy to see conversely that this solution is the only one of period one. We shall now show that every other periodic sequence is purely periodic.

8.1 Criteria for periodicity

Theorem 8.1. Let $(h) : 0, 1, h_2, h_3, \ldots$ be a solution of (21) in which no two consecutive terms vanish. Then if (h) is periodic, (h) is purely periodic.

PROOF. If h_2 is zero, h_3 is not zero, and the conditions for periodicity in this case are trivial. Hence it suffices to show that if not two consecutive terms of (h) vanish, then the assumptions

$$h_{n+\kappa} = h_n, \qquad n \geqslant a \geqslant 1, \qquad \kappa \geqslant 2, \tag{139}$$

$$h_{a-1+\kappa} \neq h_{a-1}, \tag{140}$$

$$h_2 \neq 0 \tag{141}$$

lead to a contradiction. These conditions simply state that (h) is periodic with period κ but not purely periodic, as the sequence (h) starts with a non-periodic terms.

We shall begin by showing that

$$h_\kappa = 0. \tag{142}$$

On taking $m = a + 1 + \kappa$ and $n = a + 1$ in (21), we obtain

$$h_{2a+2+\kappa} h_\kappa = h_{a+2+\kappa} h_{a+\kappa} h_{a+1}^2 - h_{a+2} h_a h_{a+1+\kappa}^2.$$

Applying (139) successively for n equal to $2a+2+\kappa$, $a+2+\kappa$, $a+\kappa$ and $a+1+\kappa$, the identity becomes

$$h_{2a+2} h_\kappa = h_{a+2} h_a h_{a+1}^2 - h_{a+2} h_a h_{a+1}^2 = 0.$$

Hence either h_κ or h_{2a+2} must be zero. If $h_\kappa = 0$, we are done. Now suppose that $h_{2a+2} = 0$. Then on taking $m = 2a + 2 + \kappa$ and $n = \kappa$ in (21) and applying (139), we obtain the relation

$$0 = h_{2a+2}^2 = h_{2a+3} h_{2a+1} h_\kappa^2 - h_{\kappa+1} h_{\kappa-1} h_{2a+2}^2 = h_{2a+3} h_{2a+1} h_\kappa^2.$$

Since no two consecutive terms can be zero, and $h_{2a+2} = 0$, the last identity implies that $h_\kappa = 0$. Thus in any case, $h_\kappa = 0$.

We next show that

$$\text{either } \; h_a = 0 \; \text{ or } \; h_{a+1} = 0. \tag{143}$$

For taking $m = a + \kappa$ and $n = a$ in (21) and applying (139), we find that

$$h_{2a} h_\kappa = h_{a+1} h_{a-1+\kappa} h_a^2 - h_{a+1} h_{a-1} h_a^2 = h_{a+1} h_a^2 \left(h_{a-1+\kappa} - h_{a-1} \right).$$

By (142), $h_{a+1} h_a^2 \left(h_{a-1+\kappa} - h_{a-1} \right) = 0$. Assertion (143) now follows from (140). Since $h_2 \neq 0$, (143) and (23) imply that either $h_{2a} = 0$ or $h_{2a+2} = 0$. Since no two consecutive terms are zero,

$$h_{2a+1} \neq 0. \tag{144}$$

We can now show that

$$h_{\kappa+1} = 1, \qquad h_{\kappa-1} = -1. \tag{145}$$

For taking $m = a+1+\kappa$ and $n = a$ in (21) and reducing by (139), we find that

$$h_{2a+1}h_{\kappa+1} = h_{a+2}h_a^3 - h_{a-1}h_{a+1}^3.$$

By (22), this relation is equivalent to $h_{2a+1}h_{\kappa+1} = h_{2a+1}$, so that $h_{\kappa+1} = 1$ because of (144). Next, taking $m = a+1+2\kappa$ and $n = a$ in (21), we obtain the formula

$$h_{2a+1}h_{2\kappa+1} = h_{a+2}h_a^3 - h_{a-1}h_{a+1}^3 = h_{2a+1},$$

the last identity following again from (22). Hence by (144), $h_{2\kappa+1} = 1$. But by (22), $h_{2\kappa+1} = h_{\kappa+2}h_\kappa - h_{\kappa-1}h_{\kappa+1}^3 = -h_{\kappa-1}h_{\kappa+1}^3$, so that $h_{k-1} = -1$. This completes the proof of (145).

Next we show that

$$h_{a-1+\kappa} = 0. \tag{146}$$

For taking $m = a-1+\kappa$ and $n = \kappa$ in (21), we obtain by (142) and (145):

$$h_{a-1+2\kappa}h_{a-1} = h_a h_{a-2+\kappa}h_k^2 - h_{\kappa+1}h_{\kappa-1}h_{a-1+\kappa}^2 = h_{a-1+\kappa}^2.$$

Since by (139) and (140), $h_{a-1+2\kappa} = h_{a-1+\kappa} \neq h_{a-1}$, (146) follows.

Finally,

$$h_{a+1} = 0, \qquad h_a \neq 0, \qquad h_{a+2} \neq 0, \qquad h_{a-1} \neq 0. \tag{147}$$

For by (143), either h_a or $h_{a+1} = 0$. But $h_a = 0$ implies $h_{a+\kappa} = 0$, contradictory to (146) since no two consecutive terms vanish. So $h_a \neq 0$, which implies $h_{a+1} = 0$. Consequently, $h_{a+2} \neq 0$. Now by (140) and (146), $h_{a-1} \neq 0$.

We may obtain a contradiction from (147) as follows. Take $m = a+1+\kappa$ and $n = a-1+\kappa$ in (21). Then $h_m = h_{a+1} = 0$ by (147) and $h_n = h_{a-1+\kappa} = 0$ by (146), so that $h_{m+n}h_{m-n} = h_{2a}h_2 = 0$. Hence by (141), $h_{2a} = 0$. But by (23),

$$0 = h_{2a}h_2 = h_a\left(h_{a+2}h_{a-1}^2 - h_{a-2}h_{a+1}^2\right) = h_a h_{a+2}h_{a-1}^2,$$

contradicting (147). Summarizing, we have assumed that (h) be a periodic but not purely periodic elliptic divisibility sequence, and from this derived a contradiction. This means that (h) must be purely periodic. ☒

We have already shown the existence of periodic solutions of (21) with h_2 or h_3 zero of periods one, three, four, six and eight. The three theorems which follow are useful for deciding whether or not a given sequence is a periodic solution of (21).

Theorem 8.2. Let $(h):\ 0,1,h_2,h_3,\ldots$ be a general solution of (21), so that neither h_2 nor h_3 is zero. Then if (h) is periodic with period κ, the following holds:

$$\begin{aligned}
&\text{(i)} && h_{n+\kappa} = h_n && (n = 0,1,\ldots,\kappa)\\
&\text{(ii)} && h_{\kappa-n} = -h_n && (n = 0,1,\ldots,\kappa)\\
&\text{(iii)} && h_{\kappa/2+n} = -h_{\kappa/2-n} && (\kappa \text{ even};\ n = 0,1,\ldots,\kappa/2).
\end{aligned} \tag{148}$$

If any one of the conditions (i)–(iii) holds for a certain κ and if that condition does not for any integer smaller than κ, then the converse also holds, i.e. (h) is periodic with period κ.

REMARK. Let (h) be a general solution of (21). The condition that (h) be periodic (denoted by (P)) is in fact equivalent to the condition that (h) be purely periodic (denoted by (PP)). For by lemma 3.12, no two consecutive terms of (h) vanish, whereupon it follows from theorem 8.1 that (h) is purely periodic. The implication (PP)⇒(P) is trivial.

PROOF. We shall prove (PP)⇔(i)⇔(ii)⇔(iii). As (PP)⇒(i) is trivial, we shall commence with (i)⇒(PP).

(i)⇒(PP). Assume that $h_{n+\kappa} = h_n$ for $0 \leqslant n \leqslant \kappa$. We will show that for any $l \in \mathbb{N}$ and $0 \leqslant n \leqslant \kappa$

$$h_{n+l\kappa} = h_n, \tag{149}$$

which precisely means that (h) is purely periodic with period κ.

We will first show that it follows from (i) that $h_{\kappa-1} = -1$. Note that $h_\kappa = h_0 = 0$ and $h_{\kappa+1} = h_1 = 1$. On taking $m = n+\kappa$ and $n = n$ in (21), we obtain

$$h_{2n+\kappa}h_\kappa = h_{n+\kappa+1}h_{n+\kappa-1}h_n^2 - h_{n+1}h_{n-1}h_{n+\kappa}^2.$$

As $h_\kappa = 0$ and $h_{n+\kappa} = h_n$, the equation becomes $(h_{n+\kappa+1}h_{n+\kappa-1} - h_{n+1}h_{n-1})h_n^2 = 0$. On taking $n = \kappa+2$ one finds

$$(h_{2\kappa+3}h_{2\kappa+1} - h_{\kappa+3}h_{\kappa+1})h_{\kappa+2}^2 = 0 \qquad \Rightarrow \qquad (h_{2\kappa+3}h_{2\kappa+1} - h_3)h_2^2 = 0.$$

Since $h_2 \neq 0$ it follows that $h_{2\kappa+3}h_{2\kappa+1} = h_3$. On taking $n = \kappa+1$ in (22) we find

$$h_{2\kappa+3} = h_{\kappa+3}h_{\kappa+1}^3 - h_\kappa h_{\kappa+2}^3 \qquad \Rightarrow \qquad h_{2\kappa+3} = h_3.$$

Therefore, $h_3h_{2\kappa+1} = h_3$. As $h_3 \neq 0$, $h_{2\kappa+1} = 1$. On the other hand, one has

$$1 = h_{2\kappa+1} = h_{\kappa+2}h_\kappa^3 - h_{\kappa-1}h_{\kappa+1}^3 = -h_{\kappa-1},$$

so that $h_{\kappa-1} = -1$.

We now prove (149) by induction on l. For $l = 0$ there is nothing to prove. For $l = 1$, (149) coincides with (i) — the premise of our implication. So now suppose (149) to be true for all $l < q$ where q is some fixed integer $\geqslant 2$. On taking $m = n+(q-1)\kappa$ and $n = \kappa$ in (21) and using the fact that $h_\kappa = 0$ we obtain

$$h_{n+q\kappa}h_{n+(q-2)\kappa} = -h_{\kappa+1}h_{\kappa-1}h_{n+(q-1)\kappa}^2 = -h_{\kappa-1}h_{n+(q-1)\kappa}^2.$$

By the induction hypothesis and the fact that $h_{\kappa-1} = -1$, we obtain

$$h_{n+q\kappa}h_n = h_n^2. \tag{150}$$

If $h_n \neq 0$ we divide both sides by h_n, whereupon it follows that $h_{n+q\kappa} = h_n$. This proves (149) in case $h_n \neq 0$. In order to prove (149) also in case $h_n = 0$ we make use of the elliptic function representation of (h), whose existence is guaranteed by theorem 4.1. We have $h_n = \psi_n(u) = \sigma(nu)/\sigma(u)^{n^2}$. Let L be the lattice corresponding to the Weierstraß sigma function. That h_κ and h_n are both zero means that κu and nu are both lattice points. But then for any $l \in \mathbb{N}$, $(n+l\kappa)u$ is a lattice point, so that $h_{n+l\kappa} = 0$.

(i)⇒(ii). Suppose that $h_{n+\kappa} = h_n$ for $n = 0, 1, \ldots, \kappa$. Then, as we have just derived, $h_{\kappa-1} = -1$. Hence, on taking $m = \kappa$ and $n = n$ in (21), we obtain

$$h_{\kappa+n}h_{\kappa-n} = h_{\kappa+1}h_{\kappa-1}h_n^2 \qquad \Rightarrow \qquad h_nh_{\kappa-n} = -h_n^2.$$

If $h_n \neq 0$, (ii) follows on dividing by h_n. If $h_n = 0$, (ii) holds trivially.

(ii)⇒(i). Assume that $h_{\kappa-n} = -h_n$ for $n = 0, 1, \ldots, \kappa$. We see directly that $h_\kappa = 0$ and $h_{\kappa-1} = -1$. We first show that $h_{\kappa+1} = 1$. On taking $m = \kappa$ and $n = \kappa - n$ in (21) we obtain for $0 \leqslant n \leqslant \kappa$,

$$h_{2\kappa-n}h_n = h_{\kappa+1}h_{\kappa-1}h_{\kappa-n}^2 \qquad \Rightarrow \qquad h_{2\kappa-n}h_n = -h_{\kappa+1}h_n^2.$$

Since $h_3 \neq 0$ and $\kappa \geqslant 4$, putting $n = 3$ in the last expression yields

$$h_{2\kappa-3} = -h_{\kappa+1}h_3. \tag{151}$$

On the other hand, on taking $n = \kappa - 2$ in (22), one finds

$$h_{2\kappa-3} = -h_{\kappa-3}h_{\kappa-1}^3 = h_{\kappa-3} = -h_3.$$

Now (151) implies that $h_{\kappa+1} = 1$.

Next, on taking $m = \kappa$ and $n = n$ in (21), we obtain

$$h_{\kappa+n}h_{\kappa-n} = h_{\kappa+1}h_{\kappa-1}h_n^2 \qquad \Rightarrow \qquad h_{\kappa+n}h_n = h_n^2.$$

If $h_n \neq 0$, (i) follows on dividing by h_n. If $h_n = 0$, nu must be a lattice point. As κu is a lattice point, so must be their sum $(n+\kappa)u$. This implies that $h_{n+\kappa} = h_n = 0$, so that (i) holds also in this case.

(ii)$\Rightarrow$(iii). Let κ be even and assume that $h_{\kappa-n} = -h_n$ for $n = 0, 1, \ldots, \kappa$. Suppose now that $0 \leqslant n \leqslant \kappa/2$. Then $0 \leqslant \kappa/2 - n \leqslant \kappa/2$. On replacing n by $\kappa/2 - n$ in (ii) we obtain

$$h_{\kappa/2+n} = -h_{\kappa/2-n}, \qquad n = 0, 1, \ldots, \kappa/2.$$

(iii)$\Rightarrow$(ii). Let κ be even and assume that $h_{\kappa/2+n} = -h_{\kappa/2-n}$ for $n = 0, 1, \ldots, \kappa/2$. For $0 \leqslant n \leqslant \kappa/2$ we have $0 \leqslant \kappa/2 - n \leqslant \kappa/2$, so that on replacing n with $\kappa/2 - n$ in (iii) we obtain

$$h_{\kappa-n} = -h_n, \qquad n = 0, 1, \ldots, \kappa/2. \tag{152}$$

If $\kappa/2 \leqslant n \leqslant \kappa$, we have $0 \leqslant n - \kappa/2 \leqslant \kappa/2$. Therefore, on replacing n with $n - \kappa/2$ in (iii) we obtain

$$h_n = -h_{\kappa-n}, \qquad n = \kappa/2, \ldots, \kappa. \tag{153}$$

Now (152) and (153) together constitute (ii). This completes the proof. $\boxtimes$

We state one important fact, which emerged in the last proof, as a separate lemma.

Lemma 8.3. If (h) is a general solution of (21) which is periodic with period κ, then $h_{\kappa-1} = -1$.

The two following theorems are a direct consequence of theorem 8.2.

Theorem 8.4. Let $h_0, h_1, \ldots, h_\kappa$ be a set of $\kappa + 1$ numbers satisfying the conditions (148) (ii) or (148) (iii), and also satisfying the basic recursion (21) for $m + n \leqslant \kappa$. Then if κ_n denotes the least positive residue of n modulo κ, and if h_n is defined to be h_{κ_n} for $n \geqslant 0$, then (h) is a periodic solution of (21) with period κ.

Theorem 8.5. If (h) is any integral general elliptic divisibility sequence and if m is an integral modulus prime to both h_2 and h_3, then the previous two theorems hold if the periodicity is understood to mean periodicity modulo m and if the equalities in the conditions (148) are replaced by congruences modulo m.

Example 8.6. To illustrate the theorems, suppose that (g) is the sequence starting with the initial values $g_0 = 0$, $g_1 = 1$, $g_2 = a \neq 0$, $g_3 = b \neq 0$ and $g_4 = 0$. We compute the first twenty values of (g) by means of (22) and (23).

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
g_n	0	1	a	b	0	$-b^3$	$-ab^4$	$-b^6$	0	b^{10}	ab^{12}	b^{15}	0	$-b^{21}$	$-ab^{24}$	$-b^{28}$	0	b^{36}	ab^{40}	b^{45}
k_n	0	1	a	1	0	-1	$-a$	-1	0	1	a	1	0	-1	$-a$	-1	0	1	a	1
l_n	0	1	a	-1	0	1	$-a$	-1	0	1	a	-1	0	1	$-a$	-1	0	1	a	-1

We have $\rho = 4$. If (g) is purely periodic, then by theorem 8.14, $\kappa = \rho$ or $\kappa = 2\rho$. In any case, by theorem 8.3 it holds that $h_{2\rho-1} = h_7 = -1$. Thus, a necessary condition for periodicity is that $b = \pm 1$. Let (k) be the sequence obtained from (g) by putting $b = +1$ and let (l) be the sequence obtained from (g) by putting $b = -1$. Then the first nine values of (k) are $0, 1, a, 1, 0, -1, -a, -1, 0$ and the first nine values of (l) are $0, 1, a, -1, 0, 1, -a, -1, 0$. Both these sets of nine numbers satisfy condition (iii) of theorem 8.2. Therefore, (k) and (l) are purely periodic with period 8. However, they are not equivalent, as is readily seen.$\diamondsuit$

Example 8.7. Let (f) be the sequence starting with the values $f_0 = 0$, $f_1 = 1$, $f_2 = 1$, $f_3 = -1$, $f_4 = -1$. We find that $f_5 = 0$. Hence, condition (ii) of theorem 8.2 is satisfied with $\kappa = 5$. Thus (f) is a periodic solution of (21) of period five.

Let (t) denote the sequence starting with initial values $t_0 = 0$, $t_1 = 1$, $t_2 = b$, $t_3 = b$, $t_4 = 1$. We find that $t_5 = 0$, $t_6 = -1$, $t_7 = -b$, $t_8 = -b$, $t_9 = -1$, $t_{10} = 0$. Hence condition (ii) of theorem 8.2 is satisfied with κ=10. Thus (t) is a periodic solution of (21) of period ten.$\diamondsuit$

We shall show in the next section that there are essentially no other periodic elliptic sequences.

8.2 Normal sequences

Definition 8.8. A sequence (h) will be called a *normal* solution of (21) if

$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2, \qquad m \geqslant n \geqslant 1; \tag{154}$$

$$h_0 = 0,\ h_1 = 1;\ h_2, h_3, h_4 \text{ and } h_4/h_2 \text{ are integers;} \tag{155}$$

$$(h_3, h_4) = 1. \tag{156}$$

Lemma 8.9. If (h) is normal sequence, then

$$(h_n, h_{n+1}) = 1 \quad \text{for all } n \geqslant 1. \tag{157}$$

PROOF. By theorem 3.13, (h) is an integral sequence. Condition (156) implies that $(h_2, h_3) = 1$, as $h_2 | h_4$. Now let p be any prime. Theorem 3.14 guarantees the existence of its smallest rank of apparition ρ. Then either $h_{\rho+1} \equiv 0 \pmod{p}$ or $h_{\rho+1} \not\equiv 0 \pmod{p}$. If $h_{\rho+1} \equiv 0 \pmod{p}$, theorem 3.16 implies that $\rho \leqslant 3$, quod non. Therefore $h_{\rho+1}$ cannot be congruent to 0 modulo p. Theorem 3.15 now implies that a term h_k is divisible by p if and only if the suffix k is divisible by ρ. Since n and $n+1$ can never be both divisible by ρ, h_n and h_{n+1} cannot both be divisible by p. We have shown that for any prime p, p cannot divide both h_n and h_{n+1}, i.e. $(h_n, h_{n+1}) = 1$. $\boxtimes$

A direct consequence of theorem 3.19 is the following result.

Lemma 8.10. If (h) is normal, $(h_n, h_m) = h_{(n,m)}$.

Lemma 8.11. Every purely periodic elliptic divisibility sequence is normal.

PROOF. The conditions (154) and (155) already implicit in the definition of elliptic divisibility sequence, so that we only have to show that (156) holds, which we shall do by reductio ad absurdum. For suppose that $p | (h_3, h_4)$ for some prime p. Then by theorem 3.16, $p | h_n$ for all $n \geqslant 3$. But $2\kappa + 1 \geqslant 5$ and by the periodicity of (h), $h_{2\kappa+1} = h_1 = 1$, which is obviously not divisible by p — a contradiction. Therefore h_3 and h_4 must be coprime: $(h_3, h_4) = 1$. $\boxtimes$

Definition 8.12. Let (h) be an elliptic divisibility sequence. Then if

$$h_\rho = 0 \quad \text{but} \quad h_n \neq 0 \quad \text{for} \quad 0 < n < \rho, \tag{158}$$

then (h) is said to be of *rank* ρ.

Lemma 8.13. Let (h) be a general solution of (21) of rank ρ. Then $h_n = 0$ if and only if n is a multiple of ρ. Consequently, if (h) is purely periodic with period κ, then κ is a non-zero multiple of ρ.

PROOF. Let (h) be a general solution of (21) of rank ρ and assume that $h_n = 0$. Suppose that n is not a multiple of ρ, so that we can write $n = q\rho + r$ with $0 < r < \rho$. Let $\psi_n(u)$ be the elliptic function representation of h_n, whose existence is guaranteed by theorem 4.1; let L be the corresponding lattice. Now $h_n = 0$ and $h_\rho = 0$ implies that nu and ρu are lattice points. Hence $nu - q\rho u = ru$ is a lattice point. But this means that $h_r = 0$ with $r < \rho$, contradictory to the definition of rank of apparition. Thereupon we conclude that n must be a multiple of ρ.

Now suppose that (h) is purely periodic with period κ. Then $h_\kappa = h_0 = 0$, so that by the above it follows that κ is a non-zero multiple of ρ, since $\kappa \neq 0$. ☒

Theorem 8.14. If (h) is a normal solution of (21) of rank ρ, then the following holds:

(i) $h_{\rho+n} = \pm h_n$ for $n = 0, 1, \ldots, \rho$.
(ii) $h_{\rho+1} = \pm 1$ and $h_{\rho-1} = \pm 1$.
(iii) $h_{\rho+1} h_{\rho-1} = -1$.
(iv) (h) is purely periodic and its period is either ρ or 2ρ.

PROOF. (i) Let $0 \leqslant n \leqslant \rho$, and take $m = n + \rho$ and $n = n$ in (154). Then

$$h_{\rho+n+1} h_{\rho+n-1} h_n^2 = h_{n+1} h_{n-1} h_{\rho+n}^2. \tag{159}$$

But by (157), h_n is prime to h_{n+1} and h_{n-1}. Hence, h_n^2 divides $h_{\rho+n}^2$. Similarly, $h_{\rho+n}^2$ divides h_n^2. Consequently, $h_{\rho+n}^2 = h_n^2$, so that

$$h_{\rho+n} = \pm h_n, \qquad 0 \leqslant n \leqslant \rho. \tag{160}$$

(ii) By (i), $h_{\rho+1} = \pm h_1 = \pm 1$. On taking $n = \rho - 1$ in (160), we obtain $h_{2\rho-1} = \pm h_{\rho-1}$. Formula (22) yields $h_{2\rho-1} = h_{\rho+1} h_{\rho-1}^3$, so that $\pm h_{\rho-1} = h_{\rho+1} h_{\rho-1}^3 = \pm h_{\rho-1}^3$. Therefore, $h_{\rho-1} = \pm 1$.

(iii) Since $h_1 = 1$ and $h_2, h_3 \neq 0$, $h_{\rho-2} \neq 0$ by the definition of rank. Therefore, on taking $n = \rho - 2$ in (159) one finds

$$h_{2\rho-1} h_{2\rho-3} = h_{\rho-1} h_{\rho-3}. \tag{161}$$

Next, on taking $n = \rho - 1$ and $n = \rho - 2$ in (22), we find

$$h_{2\rho-1} = h_{\rho+1} h_{\rho-1}^3, \qquad h_{2\rho-3} = -h_{\rho-3} h_{\rho-1}^3.$$

On substituting these expressions in (161), we obtain

$$-h_{\rho+1} h_{\rho-1}^6 h_{\rho-3} = h_{\rho-1} h_{\rho-3} \qquad \Rightarrow \qquad -h_{\rho+1} h_{\rho-1} h_{\rho-3} = h_{\rho-3},$$

for $h_\rho^4 = 1$. Since $h_{\rho-3} \neq 0$, it follows that $h_{\rho+1} h_{\rho-1} = 1$.

(iv) We distinguish two cases: (I) either $h_{\rho+n}$ equals $+h_n$ for all $0 \leqslant n \leqslant \rho$ or (II) $h_{\rho+n}$ does *not* equal $+h_n$ for all $0 \leqslant n \leqslant \rho$. If (I) holds, (h) is purely periodic with period ρ by lemma 8.13 and part (i) of theorem 8.2. Now let us consider case (II). As part (i) of theorem 8.2 is also a necessary condition for periodicity, (h) cannot be purely periodic with period ρ. But on taking $m = \rho$ and $n = n$ in (21), we find for $0 \leqslant n \leqslant \rho$,

$$h_{\rho+n} h_{\rho-n} = h_{\rho+1} h_{\rho-1} h_n^2 = -h_n^2. \tag{162}$$

By (i) we have $h_n^2 = h_{n+\rho}^2$, and moreover $h_n \neq 0$ for $0 < n < \rho$, so that it follows from (162) that $h_{\rho-n} = -h_{\rho+n}$, $0 < n < \rho$. Since this identity also holds for $n = 0$ and $n = \rho$, we have established

$$h_{\rho+n} = -h_{\rho-n}, \qquad n = 0, 1, \ldots, \rho.$$

We now conclude by lemma 8.13 and part (iii) of theorem 8.2 that (h) is purely periodic with period 2ρ. ⊠

8.3 Possibilities for the rank of a purely periodic sequence

Our aim of this section is to prove that if (h) is purely periodic, its rank is less than six. In other words, integral periodic elliptic sequences can only have the periods $1, 2, 3, 4, 5, 6, 8$ or 10. That each of these periods may actually occur has already been demonstrated. The proof rests on a series of lemmas which we now establish.

Lemma 8.15. If (h) is any solution of (21) and $m \geqslant n \geqslant p > 0$, then

$$h_{m+n}h_{m-n}h_p^2 = h_{m+p}h_{m-p}h_n^2 - h_{n+p}h_{n-p}h_m^2. \tag{163}$$

PROOF. On substituting for $h_{m+p}h_{m-p}$ and $h_{n+p}h_{n-p}$ on the right of (163) their expressions obtained from (21), we get

$$h_{m+p}h_{m-p}h_n^2 - h_{n+p}h_{n-p}h_m^2 = \left[h_{m+1}h_{m-1}h_p^2 - h_{p+1}h_{p-1}h_m^2\right]h_n^2 - \left[h_{n+1}h_{n-1}h_p^2 - h_{p+1}h_{p-1}h_n^2\right]h_m^2 =$$

$$h_{m+1}h_{m-1}h_p^2h_n^2 - h_{n+1}h_{n-1}h_p^2h_m^2 = \left[h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2\right]h_p^2 = h_{m+n}h_{m-n}h_p^2.\boxtimes$$

Lemma 8.16. Let (h) be an elliptic divisibility sequence and h_r any non-vanishing term of (h). Then if $k_n = h_{nr}/h_r$ $(n = 0, 1, 2, \ldots)$, (k) is an elliptic divisibility sequence. Furthermore if (h) is normal, so is (k).

PROOF. On taking $p = r$, $m = mr$ and $n = nr$ in (163), we obtain

$$h_{(m+n)r}h_{(m-n)r}h_r^2 = h_{(m+1)r}h_{(m-1)r}h_{nr}^2 - h_{(n+1)r}h_{(n-1)r}h_{mr}^2.$$

On dividing by h_r^4, we find that (k) satisfies (21). (k) is evidently integral and $k_0 = 0$, $k_1 = 1$ while k_4/k_2 is an integer. Hence (k) is an elliptic divisibility sequence. Now if (h) is normal, $(h_{3r}, h_{4r}) = h_r$ by lemma 8.10. Hence, $(k_3, k_4) = 1$ and (k) is normal. ⊠

Lemma 8.17. If p is a prime greater than five and (h) is normal, then h_p is never zero.

PROOF. Suppose that we have $h_p = 0$ for some prime $p > 5$. We shall derive a contradiction. Since (h) is normal, it is of rank p. By virtue of theorem 8.14 (iii), (h) is purely periodic with period p or $2p$. Then (h) is obviously also purely periodic modulo 3. By corollary 3.18, $h_n \equiv 0 \pmod 3$ if and only if n is a multiple of ρ, the rank of apparition of the prime 3. As $h_p \equiv 0 \pmod 3$, it follows that $\rho | p$. But it was shown explicitly in section 5.3 that elliptic divisibility sequences modulo 3 always have rank of apparition $\leqslant 7$. Hence $\rho \leqslant 7$. So p is a prime greater than five such that it is divisible by ρ. This can only be if $p = \rho = 7$. But if $h_7 = 0$, then $h_6 = \pm 1$ and $h_8 = \pm 1$ by theorem 8.14 (i). As (h) is a divisibility sequence, it follows that $h_4 = \pm 1$, $h_2 = \pm 1$ and $h_3 = \pm 1$. Now $h_5 \neq 0$, for $\rho = 7$. Thus $h_5 = h_4h_2^3 - h_3^3$ must equal ± 2. But then $h_7 = h_5h_3^3 - h_2h_4^3 = \pm 2 \pm 1 \neq 0$. This contradiction completes the proof of the lemma. ⊠

Lemma 8.18. If ρ is the rank of (h), then ρ can contain no prime factor other than $2, 3$ or 5.

PROOF. Suppose that p is any prime factor of ρ, and write $\rho = pq$. Then $h_q \neq 0$ by the definition of rank. Hence if $k_n = h_{nq}/h_q$, (k) is a normal sequence of rank p by lemma 8.16. Now by lemma 8.17, p equals $2,3$ or 5. $\boxtimes$

Lemma 8.19. Let (h) be a normal sequence of rank ρ. Then ρ is not equal to any of the following numbers:

$$6,8,9,10,15,25. \tag{164}$$

PROOF. The proof proceeds by examination of cases; it suffices to give two examples. Suppose that $\rho = 6$. Then $h_5 = \pm 1$, $h_n \neq 0$ for $0 < n < 6$ and $h_6 h_2 = h_3(h_5 h_2^2 - h_4^2) = 0$. It follows that $h_5 h_2^2 - h_4^2 = 0$, so that $h_5 = +1$ and $h_4 = \pm h_2$. But $h_5 = h_4 h_2^3 - h_3^3 = \pm h_2^4 - h_3^3$. Hence one ore the other of the diophantine equations $X^4 = Y^3 + 1$ or $X^4 = -Y^3 - 1$ must have non-zero integral solutions. But it is easily seen that neither has non-zero integral solutions. Hence $\rho \neq 6$.

Now suppose that $\rho = 10$. Then $h_9 = \pm 1$, so that $h_3 = \pm 1$. Since $h_{50} = 0$, $h_{49} = \pm 1$ which implies $h_7 = \pm 1$. Now $0 = h_{10} h_2 = h_5(h_7 h_4^2 - h_3 h_6^2)$, so that $h_7 h_4^2 - h_3 h_6^2 = 0$. As $h_3 = \pm 1$ and $h_7 = \pm 1$, it follows that either $h_7 = h_3 = 1$ or $h_7 = h_3 = -1$. In either case, $h_6 = \pm h_4$. Next, $h_6 h_2 = h_3(h_5 h_2^2 - h_4^2)$. Consequently, $\pm h_4 h_2 = h_3(h_5 h_2^2 - h_4^2)$. Therefore, h_4 divides $h_3(h_5 h_2^2 - h_4^2)$. As (h) is normal, it follows from lemma 8.10 that h_4 divides neither h_3 nor h_5. Hence, $h_4 | h_2^2$, so that $h_4 | h_2$. Therefore, $h_4 = \pm h_2$. But then $h_6 h_2 = \pm h_2^2 = h_3 h_2^2(h_5 - 1)$, so that $\pm 1 = h_3(h_5 - 1) = \pm(h_5 - 1)$. Since $h_5 \neq 0$, we must have $h_5 = 2$. But $h_9 = h_6 h_4^3 - h_3 h_5^3$. Hence $\pm 1 = \pm h_4^4 \pm 8$, so that $\pm h_4^4 = \pm 1 \mp 8 = \pm a$ where a equals 7 or 9. Therefore, $h_4^4 = a$, which is clearly impossible. Hence $\rho \neq 10$. The other cases may be disposed of similarly. $\boxtimes$

Lemma 8.20. Let (h) be a normal sequence with rank ρ. Then ρ is not divisible by any one of the numbers from formula (164).

PROOF. Assume that $\rho = lm$ where m is any one of the numbers from formula (164) and l is an integer $\geqslant 1$. Then $h_l \neq 0$ and $k_n = h_{ln}/h_l$ defines a normal sequence (k) of rank m, contrary to lemma 8.19. $\boxtimes$

The announced result about the rank of a purely periodic elliptic divisibility sequence now is a fairly easy consequence of our series of lemmas.

Theorem 8.21. Let (h) be an elliptic divisibility sequence. If (h) is purely periodic, its rank ρ is less than six.

PROOF. By lemma 8.11, (h) is normal. By lemma 8.18, the only prime factors of ρ are $2,3$ and 5. By lemma 8.20, ρ is not divisible by $2^3,\ 3^2,\ 5^2$ or $2\times 3,\ 2\times 5,\ 3\times 5$. Hence ρ must equal $2,3,4$ or 5. $\boxtimes$

9 The relationship between elliptic sequences and elliptic curves

In this section we investigate the connection between elliptic curves and elliptic sequences. It is not surprising that a connection exists, since we defined elliptic sequences to be sequences of rational numbers satisfying the recursive relation (21), which arose from elliptic curves as we saw in section 2.3.

9.1 From a curve to a sequence and vice versa

Let $E : Y^2 = X^3 + AX + B$ be an elliptic curve with coefficients in $\mathbb{Z}$. As we showed in section 2.5, the division polynomials Ψ_n satisfy the recursion

$$\Psi_{m+n}\Psi_{m-n} = \Psi_{m+1}\Psi_{m-1}\Psi_n^2 - \psi_{n+1}\Psi_{n-1}\Psi_m^2$$

in $\mathbb{Z}[X,Y]$, and it follows that for any rational point $Q = (X_1, Y_1)$ on E, if $h_n = \Psi_n(X_1, Y_1)$ for $n \in \mathbb{Z}$ then the sequence (h) is an elliptic sequence.

The elliptic representation theorem and the uniqueness of elliptic sequences supply the converse, which we formulate as a theorem.

Theorem 9.1. Let (h) be an elliptic sequence in which neither h_2 nor h_3 is zero. Then there exist an elliptic curve

$$E : Y^2 = X^3 + CX + D,$$

where $C, D \in \mathbb{Q}$ and a rational point $Q = (X_1, Y_1)$ on E such that $\Psi_n(X_1, Y_1) = h_n$ for all $n \in \mathbb{Z}$. Specifically, C and D are given by the following rational functions of h_2, h_3, h_4:

$$C = -\tfrac{g_2}{4}, \qquad D = -\tfrac{g_3}{4},$$

where g_2 and g_3 are the rational expressions in h_2, h_3, h_4 from formulas (48) and (49) respectively. Moreover,

$$Q = (X_1, Y_1) = \left(\frac{h_2^{10} + 2h_2^5 h_4 + 4h_2^2 h_3^3 + h_4^2}{12 h_2^4 h_3^2}, \frac{h_2}{2} \right).$$

PROOF. By theorem 4.1 there exist rational numbers g_2 and g_3 and a complex constant u such that if $\wp(z; g_2, g_3)$ is the Weierstraß function with invariants g_2 and g_3, then $h_n = \psi_n(u) \in \mathbb{Q}$. Since $\wp'(u) = -h_2$ and by (47), $\wp(u) = \frac{h_2^{10} + 2h_2^5 h_4 + 4h_2^2 h_3^3 + h_4^2}{12 h_2^4 h_3^2}$, the point $(x_1, y_1) = (\wp(u), \wp'(u))$ is a rational point on the elliptic curve $E' : \ y^2 = 4x^3 - g_2 x - g_3$. Dividing the equation by 4 yields $(\frac{1}{2}y)^2 = x^3 - \frac{g_2}{4}x - \frac{g_3}{4}$. By putting $X = x$, $Y = -\frac{1}{2}y$, $C = -\frac{g_2}{4}$ and $D = -\frac{g_3}{4}$ we obtain an equation in modern Weierstraß form: $E : \ Y^2 = X^3 + CX + D$. The point (x_1, y_1) on E' corresponds to the point

$$(X_1, Y_1) = (x_1, -\tfrac{1}{2}y_1) = \left(\frac{h_2^{10} + 2h_2^5 h_4 + 4h_2^2 h_3^3 + h_4^2}{12 h_2^4 h_3^2}, \frac{h_2}{2} \right)$$

on E. Finally, by the definition of division polynomials from section 2.5 it follows that $\Psi_n(X_1, Y_1) = \psi_n(X_1, -2Y_1) = \psi_n(x_1, y_1) = h_n$.$\boxtimes$

Example 9.2. Consider the elliptic curve $E : \ Y^2 = X^3 + 2X - 2$ and the rational point of infinite order $(X_1, Y_1) = (1, 1)$. The first ten values of the elliptic divisibility sequence $h_n = \Psi_n(X_1, Y_1)$ associated with E are:

$$0,\ 1,\ 2,\ -13,\ -292,\ -139,\ 557830,\ 50099559,\ -13758255688,\ -13888377512087.\diamondsuit$$

Example 9.3. Let (h) be the elliptic divisibility sequence that is totally determined by the initial values $h_0 = 0, h_1 = 1, h_2 = 1, h_3 = -1, h_4 = 1$. The first twenty values of (h) are:

$$0,\ 1,\ 1,\ -1,\ 1,2,\ -1,-3,\ -5,\ 7,-4,\ -23,\ 29,\ 59,\ 129,\ -314,\ -65,\ 1529,\ -3689,\ -8209.$$

With formula (92) we find that the discriminant $\Delta(h)$ equals -37, so that (h) is not a singular EDS. The elliptic curve associated with (h) is given by $E : Y^2 = X^3 - X + \frac{1}{4}$. The rational point Q on E is given by $Q = (X_1, Y_1) = (0, \frac{1}{2})$. The curve E is non-singular, since its discriminant equals $\frac{37}{16}$.$\Diamond$

In [7] Rachel Shipsey showed how to obtain an EDS from an elliptic curve of the form $E : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X$ with integer coefficients containing the rational point $Q = (0,0)$.[16] She showed that the sequence (h) defined by $h_n = \Psi_n(0,0)$ is an EDS, where Ψ_n is the n-th division polynomial associated with the curve E.[17] The multiples $nQ \neq O$ of Q can be written as

$$nQ = \left(\frac{X_n}{Z_n^2}, \frac{Y_n}{Z_n^3}\right) \text{ for } n \in \mathbb{Z},$$

where X_n, Y_n, Z_n are integers (unique up to the choice of sign of Z_n and Y_n) and X_n and Y_n are coprime to Z_n. If $nP = O$ we take $Z_n = 0$.

Shipsey proved that if A_3 and A_4 are coprime, then (Z) is an EDS in which Z_3 and Z_4 are coprime, and $X_n = -Z_{n-1}Z_{n+1}$. She also proved the converse, that if (Z) is any EDS in which Z_3 and Z_4 are coprime then there exists an elliptic curve E over $\mathbb{Q}$ (the A_i are not necessarily integers) containing the point $Q = (0,0)$, such that $nQ = \left(\frac{X_n}{Z_n^2}, \frac{Y_n}{Z_n^3}\right)$.

9.2 Improved upper bound for the rank of apparition

We would like to point out an application[18] to elliptic sequences of a famous result from elliptic curves: the Hasse-Weil theorem.

Recall that the (smallest) rank of apparition ρ of the prime p in an elliptic divisibility sequence (h) is defined to be the smallest positive integer such that $h_\rho \equiv 0 \pmod{p}$. If the point Q has order N on the elliptic curve E considered over the finite field $\mathbb{F}_p$ then Z_N will be the first zero (other than Z_0) in the sequence (Z). Due to the Hasse-Weil theorem we know that N is bounded by

$$N \leqslant p + 1 + 2\sqrt{p}.$$

Therefore for elliptic divisibility sequences of type (Z) we have

$$\rho \leqslant p + 1 + 2\sqrt{p},$$

a noticable improvement on Ward's bound given in theorem 3.14.

9.3 Points of finite order on an elliptic curve versus periodic EDS

A well-known result from the study of elliptic curves is Mazur's theorem on the possibilities for the torsion group of an elliptic curve, that is its group of points that have finite order. To conclude this thesis, we investigate the relation between points of finite order on an elliptic curve on the one hand and periodic elliptic divisibility sequences on the other.

[16] Note that any elliptic curve in general Weierstraß form $C : Y^2 + B_1XY + B_3Y = X^3 + B_2X^2 + B_4X + B_6$ containing the rational point $Q = (X_1, Y_1)$ can be put in this form by the substitutions $X \mapsto X + X_1$ and $Y \mapsto Y + Y_1$, that is, by moving the point Q to the origin.

[17] A definition of division polynomials associated with elliptic curves in general Weierstraß form will be given in the next section.

[18] Shipsey [7], §4.7.2.

Theorem 9.4. (Mazur's theorem) Let E be a non-singular elliptic curve over $\mathbb{Q}$. Then the torsion group $E_{\text{tors}}(\mathbb{Q})$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups:

$$\begin{array}{ll} \mathbb{Z}/n\mathbb{Z} & \text{with } 1 \leqslant n \leqslant 10 \text{ or } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & \text{with } 1 \leqslant n \leqslant 4. \end{array}$$

Further, each of these groups occurs as $E_{\text{tors}}(\mathbb{Q})$ for some elliptic curve $E/\mathbb{Q}$.

If (h) is a periodic elliptic divisibility sequence in which neither h_2 nor h_3 equals zero, by theorem 9.1 the associated elliptic curve contains a rational point which generates (h). Since (h) is periodic, that point must have finite order.

Example 9.5. Consider the periodic elliptic divisibility sequence (k) from example 8.6 and let (h) be the EDS obtained from (k) by putting $a = 2$, the first terms of (h) thus being

$$0, 1, 2, 1, 0, -1, -2, -1, 0, 1, 2, 1, 0, -1, -2, -1, 0, \ldots$$

(h) has rank 4 and period 8. The associated elliptic curve E is given by the equation $Y^2 = X^3 - \frac{3841}{48} + \frac{238049}{864}$ with rational point $Q = \left(\frac{65}{12}, 1\right)$. One easily checks that indeed $h_n = \Psi_n\left(\frac{65}{12}, 1\right)$.[19] Further, Q is a point of order 4 and the torsion group of E equals $\{O,\ Q,\ 2Q,\ 3Q\}$.

Of course, we can transform E into a birationally equivalent elliptic curve E' having an equation with integral coefficients. For this purpose, replace X with $\frac{1}{36}X$ and Y with $\frac{1}{216}Y$. On substituting into the equation and multiplying both sides by 46656 we obtain for E' the equation $Y^2 = X^3 - 103707X + 12854646$. The point $Q = \left(\frac{65}{12}\right)$ on E corresponds to the point $Q' = (195, 216)$ on E'. Let $s_n = \Psi_n(195, 216)$, where Ψ_n is the n-th division polynomial[20] associated with E'. The first values of (s) are:

$$0,\ 1,\ 432,\ 1679616,\ 0,\ -4738381338321616896,\ -3438141599496845182057316352, \ldots$$

One finds that $\left(\frac{1}{6}\right)^{n^2-1} s_n = h_n$, so that $(h) \sim (s)$.$\Diamond$

How about the converse? Given an elliptic curve with a point of finite order, does this point always generate a periodic elliptic divisibility sequence? The answer to this question is, in general, negative. But let us first given an example in which a point of finite order *does* generate a periodic EDS. The curve we will be considering is in *general* Weierstraß form, so that we need the following result (see Swart [10], theorem 3.10.3).

Theorem 9.6. Let $E/\mathbb{Q}$ be an elliptic curve with integral coefficients, given by the equation

$$E : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6.$$

Then the division polynomials Ψ_n, which satisfy the same recursion as the division polynomials from section 2.5, have initial values:

$$\begin{array}{rcl} \Psi_0 & = & 0, \\ \Psi_1 & = & 1, \\ \Psi_2 & = & 2Y + A_1X + A_3, \\ \Psi_3 & = & 3X^4 + B_2X^3 + 3B_4X^2 + 3B_6X + B_8, \\ \Psi_4 & = & \left(2X^6 + B_2X^5 + 5B_4X^4 + 10B_6X^3 + 10B_8X^2 + (B_2B_8 - B_4B_6)X + B_4B_8 - B_6^2\right)\Psi_2, \end{array}$$

[19] Note that here Ψ_n isn't a division polynomial since the coefficients of the equation for E are rational numbers.

[20] This time the Ψ_n *are* division polynomials!

where the B_i are given by the formulas

$$\begin{aligned} B_2 &= A_1^2 + 4A_2, \\ B_4 &= 2A_4 + A_1A_3, \\ B_6 &= A_3^2 + 4A_6, \\ B_8 &= A_1^2A_6 + 4A_2A_6 - A_1A_3A_4 + A_2A_3^2 - A_4^2. \end{aligned}$$

Example 9.7. The elliptic curve E given by the general Weierstraß equation $Y^2 - Y = X^3 - X^2$ contains a point of order 5 that generates the torsion group of E: the point $(0,1)$. Evaluating the division polynomials associated to E at $(0,1)$ yields a periodic elliptic divisibility sequence of period 5:

$$0,\ 1,\ -1,\ 1,\ -1,\ 0,\ 1,\ -1,\ 1,\ -1,\ 0,\ 1,\ -1,\ 1,\ -1,\ 0,\ldots$$

Let us call this sequence (h). If we now apply theorem 9.1 to (h), we obtain the elliptic curve $E' : Y^2 = X^3 - \frac{1}{3}X + \frac{19}{108}$ with rational point $Q = \left(\frac{2}{3}, -\frac{1}{2}\right)$. Evaluating the division polynomials associated with E' at Q yields (h) again.$\Diamond$

By theorem 8.21 we know that, for instance, a periodic EDS can never have rank equal to 6. But by Mazur's theorem we know that there exists an elliptic curve containing a point of order 6. So what does the corresponding elliptic divisibility sequence (h) look like? Clearly every sixth term must be zero, since it corresponds to O, the unity element of the group $E(\mathbb{Q})$. In particular, (h) has rank 6. If h_3 and h_4 were to be coprime, theorem 8.14 would imply that (h) is purely periodic with period 6 or 12, which is impossible. Therefore, we can already predict that $(h_3, h_4) > 1$. Let us now see what happens concretely for a curve with a point of order 6 and a curve with a point of order 10.[21]

Example 9.8. The elliptic curve E given by the equation $Y^2 = X^3 + 1$ contains the point $(2,3)$ of order 6. Evaluating the division polynomials associated to E at $(2,3)$ gives us the elliptic divisibility sequence (h), whose initial values are:

$$0,\ 1,\ 6,\ 72,\ 2592,\ 186624,\ 0,\ -34828517376,\ -90275517038592,\ -467988280328060928,$$

$$-7278153735662003552256,\ -2263796937940309584893706 24,\ 0,\ldots$$

(h) is not periodic nor is it, by theorem 8.21, equivalent to a periodic elliptic divisibility sequence. We have $(h_3, h_4) = (72, 2592) = 72$.$\Diamond$

Example 9.9. The elliptic curve E given by the equation $Y^2 + XY - Y = X^3 - X^2 - 14X + 29$ contains the point $(3,1)$ of order 9. Evaluating the division polynomials to E at $(3,1)$ yields the elliptic divisibility sequence (h), whose initial values are:

$$0,\ 1,\ 6,\ 216,\ 15552,\ -6718464,\ -17414258688,$$

$$-90275517038592,\ -2807929681968365568,\ 0,\ \ldots$$

Again h is not periodic and $(h_3, h_4) = (216, 15552) = 216$. $\Diamond$

We summarize our restults in the following theorem.

Theorem 9.10. Let E be an elliptic curve with a point of order k, where $6 \leqslant k \leqslant 10$ or $k = 12$. Then the elliptic divisibility sequence (h) associated with E cannot be periodic. Moreover, it holds that $(h_3, h_4) > 1$.

[21] The curves were taken from Silverman [9], exercise 8.12.

Nawoord (in Dutch)

De spreuk boven de ingang van Plato's Academie "Niemand trede hier binnen, als hij geen aanleg heeft voor meetkunde" indachtig ben ik begonnen wis- en natuurkunde te studeren: een leven zonder kennis van wis- en natuurkunde achtte ik niet alleen zinloos, maar zelfs onmogelijk. Ik wilde het liefst een *homo universalis* worden. Maar al gauw kreeg ik bij natuurkunde te maken met meetfouten, vuistregels (die zogenaamd afgeleid waren uit postulaten) en zag ik tot mijn grote ergernis hoe modellen van de werkelijkheid aldoor verward werden met 'de' werkelijkheid zelf: medestudenten hadden het bijvoorbeeld over complexe vectoren die vanaf het bord alle kanten op schoten. Toen bij een electronicapracticum mijn computer om onbekende redenen in brand vloog (gek genoeg deed hotmail het nog wel gewoon), besefte ik dat ik bij natuurkunde niet op mijn plaats was. Tot de studie Wiskunde heb ik altijd een haat-liefde-verhouding gehad. Ondanks uitstapjes naar de studies Nederlands, Klassieke Talen en (pogingen tot) Rechten en Geneeskunde kroop het bloed waar het niet gaan kon. Uiteindelijk heb ik in elliptische krommen een vakgebied gevonden waar ik bevlogen over ben. Vlak voordat ik aan mijn scriptie begon, keek ik op Google Video de documentaire *Fermat's last theorem* (1996) over Andrew Wiles' bewijs van de laatste stelling van Fermat en realiseerde ik mij weer hoe fantastisch wiskunde kan zijn. Toen wist ik dat het goed zou komen.

Ik dank Gunther Cornelissen voor zijn begeleiding en het vertrouwen; Bastian voor de hulp bij LaTeX (zonder het knurps-commando was het nooit gelukt); Jesse omdat hij mij, toen hij mij in een houdgreep had, deed inzien dat ik mijn studie moest afmaken; mijn oud-hulpmentor Ronald van Luijk van het Stedelijk Gymnasium Leiden voor zijn gouden tip; Lucas voor de hulp bij het schrijven in de engelse taal (ook onze volksschrijver had er moeite mee); Julie voor het $\wp$laatje; Dylan vanwege zijn super-rekenkracht (umizoomi!), mijn moeder voor haar onbegrensde steun te allen tijde en tot slot al diegenen die het met mij hebben weten uit te houden.

References

[1] M. ABRAMOWITZ AND I.A. STEGUN, *Handbook of mathematical functions*. Tenth printing, december 1972.

[2] ROBERT FRICKE, *Die elliptischen Funktionen und ihre Anwendungen*, erster und zweiter Teil. Teubner, Leipzig und Berlin 1916.

[3] ANTHONY W. KNAPP, *Elliptic Curves*. Princeton University Press, Princeton NJ 1992.

[4] EDMUND LANDAU, *Vorlesungen über Zahlentheorie*, erster Band. Hirzel, Leipzig 1927.

[5] SERGE LANG, *Elliptic Functions*. Addison-Wesley 1973.

[6] ÉDOUARD LUCAS, 'Théorie des fonctions numériques simplement périodiques'. *American Journal of Mathematics* 1 (1878), pp. 184-240; 289-321.

[7] RACHEL SHIPSEY, *Elliptic divisibility sequences*, PhD thesis, Goldsmith's College (University of London) 2000.

[8] JOSEPH H. SILVERMAN AND JOHN TATE, *Rational points on elliptic curves*. Springer 1992.

[9] JOSEPH H. SILVERMAN, *The arithmetic of elliptic curves*, 2nd edition. Springer 2009.

[10] CHRISTINE SWART, *Sequences related to elliptic curves*, PhD thesis, Royal Holloway (University of London) 2003.

[11] N.N. VOROB'EV, *Fibonacci Numbers*. Pergamon Press 1961.

[12] MORGAN WARD, 'Note on elliptic divisibility sequences'. *Bulletin of the American Mathematical Society* 42 (1936), pp. 843-845.

[13] MORGAN WARD, 'The law of apparition of primes in a Lucasian sequence'. *Transactions of the American Mathematical Society* 44 no.1 (1938), pp. 68-86.

[14] MORGAN WARD, 'Memoir on elliptic divisibility sequences'. *American Journal of Mathematics* 70 (1948), pp. 31-74.

[15] HEINRICH WEBER, *Elliptische Funktionen und algebraische Zahlen*, dritter Band. Friedrich Vieweg Verlag, Braunschweig 1908.

Index