Chapter 2

Basic properties of elliptic divisibility sequences

Our purpose in this chapter is to give an overview of the classical theory and methods of elliptic divisibility sequences. As such, we will include especially those proofs that give a flavour of the methods, and omit much of the tedium. Citations are given wherever details are missing.

2.1 Making the curve-sequence relation explicit

Ward, in relating sequences and curves in Theorem 1.2.1, gives explicit formulæ for the coefficients of the Weierstrass equation of the curve and the coordinates of the point, in terms of the initial terms of the sequence. Christine Swart gives a cleaner collection of equations for this, and it is her version we describe here. Also, although Ward concerns himself with integer sequences, his formulae and those of Swart work equally well for rationals. As in the introduction, define a change of variables of a cubic curve in Weierstrass form to be *unihomothetic* if it is of the form

$$\begin{aligned} x' &= x + r, \\ y' &= y + sx + t. \end{aligned}$$

Proposition 2.1.1 ([68, Thm 4.5.3]). *Let $W : \mathbb{Z} \to \mathbb{Q}$ be an elliptic divisibility sequence with $W(1) = 1$ and $W(2)W(3) \neq 0$. Then the family of curve-point pairs (C, P) such that $W = W_{C,P}$ is three dimensional. These are the curve and point*

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad P = (0,0)$$

where

$$\begin{aligned} a_1 &= \frac{W(4) + W(2)^5 - 2W(2)W(3)}{W(2)^2W(3)} \\ a_2 &= \frac{W(2)W(3)^2 + W(4) + W(2)^5 - W(2)W(3)}{W(2)^3W(3)} \end{aligned}$$

$$a_3 = W(2), \qquad a_4 = 1, \qquad a_6 = 0$$

or any image of these under a unihomothetic change of coordinates.

Proof. See Section 8.2. □

If we apply a change of variables of the form

$$x \leftarrow u^2 x, \qquad y \leftarrow u^3 y$$

to the curve E defined by

$$y^2 + a_1 xy + a_3 y = x^3 + a_2^2 + a_4 x + a_6 \tag{2.1}$$

and point $P = (x, y) \in E$ to obtain a new curve E' and point P', then the associated elliptic divisibility sequences satisfy

$$W_{E',P'}(n) = u^{n^2-1} W_{E,P}(n). \tag{2.2}$$

This is called by some an *equivalence* of elliptic divisibility sequences. We set our own terminology later.

2.2 Relations to the group law on the elliptic curve

Suppose we define some auxiliary polynomials ϕ_m and ω_m by

$$\phi_m = x\Psi_m^2 - \Psi_{m+1}\Psi_{m-1}, \tag{2.3}$$

$$4y\omega_m = \Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2. \tag{2.4}$$

Then, one can check that on the curve (2.1),

$$[m]P = \left(\frac{\phi_m(P)}{\Psi_m(P)^2}, \frac{\omega_m(P)}{\Psi_m(P)^3} \right). \tag{2.5}$$

In particular, when working over $\mathbb{Q}$, and in the case of an integer sequence, whenever $\phi_m(P)$ and $\Psi_m(P)$ are relatively prime, the denominator of the x-coordinate of $[m]P$ will be exactly $W_{E,P}(m)^2$. The numerators and denominators in (2.5) may involve cancellation. There is no cancellation if $P = (0,0)$, $a_6 = 0$ and $\gcd(a_3, a_4) = 1$ [61, §4.4].[1]

2.3 More on division polynomials

The division polynomials Ψ_n have a special form.

[1] This has led some to remark that the 'correct' definition of elliptic divisibility sequences is by denominators in such a fashion. We will not join that camp.

Proposition 2.3.1 ([63, Ex 3.7] or [74, V.14]). *The division polynomials Ψ_n have a representation as polynomials in x and y with coefficients in $\mathbb{Z}[a_1,a_2,a_3,a_4,a_6]$. In particular, they are of the form*

$$\Psi_n(x,y) = \begin{cases} nx^{\frac{n^2-1}{2}} + \dots & n \text{ odd} \\ y(nx^{\frac{n^2-4}{2}} + \dots) & n \text{ even} \end{cases}.$$

Therefore, their squares Ψ_n^2 are polynomials of degree n^2-1 in the variable x alone, with coefficients in $\mathbb{Z}[a_1,a_2,a_3,a_4,a_6]$, and leading coefficient n^2. The roots of this polynomial Ψ_n^2 are exactly the x-coordinates of all n^2-1 non-zero n-torsion points on the associated elliptic curve.

2.4 Induction properties

Proposition 2.4.1. *Let $W : \mathbb{Z} \to R$ be an elliptic divisibility sequence that is nonzero at the first four terms. Then $W(-z) = -W(z)$ for any $z \in \mathbb{Z}$. In particular $W(0) = 0$. Furthermore, any two elliptic divisibility sequences $W, W' : \mathbb{Z} \to R$ that agree and are non-zero at 1,2,3 and 4, must agree everywhere.*

Proof. Our first step is to show the last statement for positively indexed terms (i.e., all positively indexed terms agree). Two particular instances of the elliptic net equation (3.1) are

$$W(2n)W(2)W(1)^2 = W(n)\left(W(n+2)W(n-1)^2 - W(n-2)W(n+1)^2\right), \tag{2.6}$$

$$W(2n+1)W(1)^3 = W(n+2)W(n)^3 - W(n-1)W(n+1)^3. \tag{2.7}$$

By induction on these equations, every subsequent positive indexed term is determined by $W(1)$, $W(2)$, $W(3)$, $W(4)$.

Now we show the first statement. Assume without loss of generality that $W(1) = 1$ (since we can scale W by a constant). First we show that $W(0) = 0$. For, consider $n = m = 0$: in this case (1.2) states that $W(0)^2 = 0$. Now we consider the statement $-W(z) = W(-z)$. Suppose $W(z+2) \neq 0$. Setting $n = 1, m = z+1$ in (1.2), we obtain $W(z+2)W(-z) = -W(z+2)W(z)$, whence $W(-z) = -W(z)$ since $W(z+2) \neq 0$. We have now shown the symmetry for $z = 0,1,2$, hence $W(-1)$ and $W(-2)$ are nonzero, and so we've shown it for $z = -3,-4$ also. Therefore we've shown it for $z = 0,1,2,3,4$. Thus, by the first part, the sequences $W'(z) = -W(-z)$ and $W(z)$ agree on the first four terms and therefore agree everywhere.

Finally, by the symmetry property just shown, the terms indexed by non-positive integers are also determined uniquely by $W(1)$, $W(2)$, $W(3)$ and $W(4)$. □

Proposition 2.4.2 ([74, Lemma 4.1]). *If W is an elliptic divisibility sequence satisfying $W(1) = 1$ and $W(2)W(3) \neq 0$, and if two consecutive terms vanish, then $W(n) = 0$ for $n \geq 4$.*

Proof. See [74, Lemma 4.1]. □

2.5 The integer case

From Proposition 2.3.1, any rational elliptic divisibility sequence can be made into an integer sequence by an appropriate equivalence of the form (2.2), clearing the denominators.

Proposition 2.5.1 ([74, Thm 4.1]). *Suppose W is an elliptic divisibility sequence satisfying $W(1)=1$, $W(2)W(3)\neq 0$ and $W(2)|W(4)$, and $W(i)\in\mathbb{Z}$ for $i=1,2,3,4$. Then, the sequence is entirely integer and for all $n,m\in\mathbb{Z}$,*

$$n|m \implies W(n)|W(m).$$

Proof. We provide a sketch. For a complete proof, see [74, Thm 4.1]. Recall equations (2.6) and (2.7):

$$W(2n)W(2)W(1)^2 = W(n)\left(W(n+2)W(n-1)^2 - W(n-2)W(n+1)^2\right),$$
$$W(2n+1)W(1)^3 = W(n+2)W(n)^3 - W(n-1)W(n+1)^3.$$

A first induction shows that all terms are integers, and $W(2)|W(2n)$ for every n. Then, a second induction shows the divisibility property in general: for this, we use the following equations (the first in the case that m is even, the second in the case that it is odd):

$$W(nm)W(2) = W\left(\tfrac{nm}{2}\right)\left(W\left(\tfrac{nm}{2}+2\right)W\left(\tfrac{nm}{2}-1\right)^2 - W\left(\tfrac{nm}{2}-2\right)W\left(\tfrac{nm}{2}+1\right)^2\right), \tag{2.8}$$

$$W(nm)W(n) = W\left(\tfrac{n(m+1)}{2}+1\right)W\left(\tfrac{n(m+1)}{2}-1\right)W\left(\tfrac{n(m-1)}{2}\right)^2 \tag{2.9}$$

$$- W\left(\tfrac{n(m-1)}{2}+1\right)W\left(\tfrac{n(m-1)}{2}-1\right)W\left(\tfrac{n(m+1)}{2}\right)^2. \tag{2.10}$$

This second induction uses Proposition 2.4.2. □

2.6 Periodicity modulo p

Definition 2.6.1. For an integer elliptic divisibility sequence W, let r denote the smallest positive integer such that $W(r)\equiv 0 \mod p$. The integer r is called the *rank of apparition of W with respect to p.*

Proposition 2.6.1 ([74, Thm 5.1]). *For any integer elliptic divisibility sequence and prime p, the rank of apparition r with respect to p exists and satisfies*

$$1 \leq r \leq 2p+1.$$

Proof. Without loss of generality, we may assume $r \geq p+3$. Then consider the p values

$$\frac{W(r-1)W(r+1)}{W(r)^2},$$

each of which is a non-zero value modulo p. By the pigeonhole principle[2], two must coincide, and we have for some $1 \leq n < m \leq p-1$,

$$\frac{W(m-1)W(m+1)}{W(m)^2} \equiv \frac{W(n-1)W(n+1)}{W(n)^2} \mod p.$$

Then, the elliptic divisibility sequence recurrence (1.2) implies

$$W(m+n)W(m-n) \equiv 0 \mod p.$$

By our assumption that $r \geq p+3$, and the fact that $m-n \leq p-2$, we conclude that $W(m-n) \not\equiv 0 \mod p$, and so

$$W(m+n) \equiv 0 \mod p.$$

But $m+n \leq 2p+1$. □

By the nice properties of the division polynomials (Proposition 2.3.1), we can reduce them modulo a prime p, and the reduced division polynomials will correspond to the elliptic curve and point reduced modulo the same prime. In particular, it will still be the case that $\Psi_n(P) \equiv 0$ modulo p if and only if $[n]\widetilde{P} = \widetilde{\mathcal{O}}$ on the reduced curve. So, if W is such that $W(1) = 1$, $W(2)W(3) \neq 0$ and $W(2)|W(4)$, then the sequence arises from some curve E and point P (by Theorem 1.2.1). In this case Shipsey [61, §4.7.2] observes that Hasse's bound on the number of points of a curve over a finite field implies that for most primes p, the rank of apparition satisfies the stronger bound

$$r \leq p+1+2\sqrt{p}.$$

Ward proves a very interesting and important 'symmetry' or 'partial periodicity' property.

Theorem 2.6.2 ([74, Thm 9.2]). *Let W be an integer elliptic divisibility sequence such that $W(1) = 1$ and $W(2)|W(4)$. Let p be an odd prime and suppose $W(2)W(3) \not\equiv 0 \mod p$. Let r be the rank of apparition of W with respect to p. Then there exist integers a, b such that for all non-negative integers k and s, we have*

$$W(k+sr) \equiv a^{ks} b^{s^2} W(k) \mod p.$$

Furthermore, the integers a and b satisfy

$$a \equiv \frac{W(r-2)}{W(r-1)W(2)}, \qquad b \equiv \frac{W(r-1)^2 W(2)}{W(r-2)} \mod p.$$

The proof uses the periodicity of the Weierstrass sigma function, and the reader is encouraged to look ahead to Chapter 5, especially equation (5.1).

Proof. By Theorem 1.2.1, W is associated to some curve E and point P. Let z be the complex coordinate of the point P, so that $P = (\wp(z), \wp'(z))$. The roots of $\Psi_n^2(x) = 0$ over $\mathbb{C}$ are of the form

$$\zeta = \wp(\omega/n)$$

[2] My advisor is fond of boosting the confidence of his struggling graduate students by asserting that his own thesis consisted in large part of a single application of pigeonhole principle. For this, and his rumoured – but surely feigned – occasional confusion over the correct definition of a topology, we are ever grateful.

where ω is a period of the Weierstrass $\wp$ function. By Proposition 2.3.1, the polynomial $\Psi_n^2(x)$ has leading coefficient n^2 and coefficients in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. Hence, $\Psi_n^2(x)$ is a well-defined polynomial of degree n^2 modulo p for any $p \nmid n$.

Now, assume for the moment that $p \nmid r$.

Let K be the number field obtained by adjoining all the roots of $\Psi_r^2(x)$ and let $\mathfrak{p}$ be a prime of K that divides p. Then Ψ_r^2 splits in the finite field $K/\mathfrak{p}$. Since its value at P is zero, $\wp(z)$ is a root modulo $\mathfrak{p}$, i.e.,

$$\wp(z) \equiv \wp(\omega/r) \mod \mathfrak{p}$$

for some period ω. Thus, the sequence W under consideration agrees modulo $\mathfrak{p}$ with the sequence $W'_n = \Psi_n(\omega/r)$. Since W modulo $\mathfrak{p}$ reduces to integers modulo p (i.e., its image is in $\mathbb{Q}/(p) \subset K/\mathfrak{p}$), it suffices to replace W in our consideration with W' and show the formulæ of the theorem modulo $\mathfrak{p}$.

The formula of the Theorem now results from a calculation using the period relation (5.1) of the Weierstrass σ function:

$$\begin{aligned}
\frac{\Psi_{k+sr}\left(\frac{\omega}{r}\right)}{\Psi_k\left(\frac{\omega}{r}\right)} &= \frac{\sigma\left((k+sr)\frac{\omega}{r}\right)}{\sigma\left(k\frac{\omega}{r}\right)}\sigma\left(\frac{\omega}{r}\right)^{-2rsk-r^2s^2} \\
&= \lambda(s\omega)e^{\eta(s\omega)\left(k\frac{s\omega}{r}+s\frac{\omega}{2}\right)}\sigma\left(\frac{\omega}{r}\right)^{-2rsk-r^2s^2} \\
&= \left(\sigma\left(\frac{\omega}{r}\right)^{-2r} e^{\eta(\omega)\frac{\omega}{r}}\right)^{ks}\left(\lambda(\omega)\sigma\left(\frac{\omega}{r}\right)^{-r^2} e^{\eta(\omega)\frac{\omega}{2}}\right)^{s^2}.
\end{aligned}$$

For the case when $p|r$, there are some additional difficulties, and the reader should consult [74, Thm 9.2]. Finally, note that the final statement of the theorem (the formulæ for a and b) follows immediately from the existence of a and b. □

Ayad and Swart generalise partial periodicity to the case of prime power moduli [2, Thm C] [68, Thm 5.1.3]. Their proofs have the additional attraction that they require only the recurrence relation and not the underlying elliptic curve relationship.

Our interest in Ward's original proof is to demonstrate a strategy that we will apply later: first, show that the functions in question (in this case the division polynomials) have a nice form (i.e., they are defined with $\mathbb{Z}$ coefficients and reduce modulo p without becoming trivial); second, verify the property of interest (in this case the periodicity property) in the complex analytic case; third, using the information from step one, transport the property to the finite field (or other field) case.

For a wealth of periodicity properties of elliptic divisibility sequences modulo primes and powers of primes, see Swart [68].