On Elliptic Divisibility Sequences

Manoj Kumar
Department of Mathematics and Computer Science
University of Lethbridges, Alberta, CA

Received: November 20, 2018 Accepted: December 27, 2018

ABSTRACT *In 1948, M. Ward [2] introduced this concept of an elliptic divisibility sequence and studied arithmetic properties of such sequences. He also studied the relation of elliptic divisibility sequences with elliptic curves and elliptic functions. In this paper we give some new results between elliptic curves, elliptic divisibility sequences and elliptic functions.*

Keywords:

2. Introduction

2.1. Elliptic Divisibility Sequence

An elliptic divisibility sequence (W_n) is a sequence of integers satisfying the non-linear recurrence

$$W_{m+n}W_{m-n} = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2$$

for all $m \geq n \geq 1$ and such that $W_n \mid W_m$ whenever $n \mid m$.

The following are some examples of an elliptic divisibility sequences.

1 $W_n = (n/3)$, where (n/p) is the Legendre symbol.
2 $(W_n) = 1,1,-1,1,2,-1,-3,-5,7,-4,-23,29,59,129,-314,-65,1529,-3689,\ldots$
3 $(W_n) = 1,1,2,1,-7,-16,-57,-113,670,3983,23647,140576,-833503,-14871471-147165662,-2273917871,11396432249,\ldots$

Theorem 1.1 (Ward). Let (W_n) be a non-singular, non-degenerate elliptic divisibility sequence. Then there is a lattice $\Lambda \subset \mathbb{C}$ and a complex number $z \in \mathbb{C}$ such that

$$W_n = \frac{\sigma(nz;\Lambda)}{\sigma(z;\Lambda)^{n^2}} \quad \text{for all } n \geq 1.$$

2.2. Weierstrass σ-function

Definition 1.1. The Weierstrass σ-function (associated to a lattice Λ) is defined as

$$\sigma(z) = \sigma(z;\Lambda) := z\prod_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\left(1-\frac{z}{\omega}\right)e^{\frac{z}{\omega}+\frac{1}{2}\left(\frac{z}{\omega}\right)^2},$$

where z is a complex variable. The Weierstrass σ-function is of much importance to us because an elliptic divisibility sequence can be parametrized using it. Therefore we will study the properties of Weierstrass σ-function in detail. We start with the following proposition.

Proposition 1.1. Let $\Lambda \subset \mathbb{C}$ be a fixed lattice. Let $\sigma(z)$ be the corresponding Weierstrass σ-function. Then the following statements holds.

(a) The infinite product (3) for $\sigma(z)$ defines a holomorphic function on $\mathbb{C}$. The function $\sigma(z)$ has simple zeros at each lattice point and no other zeros.

(b) For all $z \in \mathbb{C} \setminus \Lambda$ we have

$$\frac{d^2}{dz^2}\log\sigma(z) = -\wp(z)$$

(c) For all $z \in \mathbb{C}$ and for every $\omega \in \Lambda$ there are constants $a, b \in \mathbb{C}$, depending on ω, such that

$$\sigma(z+\omega) = e^{az+b}\sigma(z).$$

(d) The function $\sigma(z)$ is an odd function (i.e., $\sigma(-z) = -\sigma(z)$).

Proof. (a) See [6] Chapter 6, Lemma 3.3].

(b) Taking logarithm in (3) yields

$$\log\sigma(z) = \log z + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\left[\log\left(1-\frac{z}{\omega}\right)+\frac{z}{\omega}+\frac{1}{2}\left(\frac{z}{\omega}\right)^2\right].$$

Using (a) we can differentiate the above series, twice with respect to z, to get

$$\frac{d}{dz}\log\sigma(z) = \frac{1}{z} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\left[\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right]$$

Differentiating again with respect to z yields

$$\frac{d^2}{dz^2}\log\sigma(z) = -\frac{1}{z^2} - \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right] = -\wp(z).$$

(c) Using the fact that $\varrho(z)$ is periodic, from part (b) we have

$$\frac{d^2}{dz^2}\log\sigma(z+\omega) = -\wp(z+\omega) = -\wp(z) = \frac{d^2}{dz^2}\log\sigma(z).$$

Integrating, last equation, twice with respect to z yields

$$\log\sigma(z+\omega) = \log\sigma(z) + az + b,$$

where a and b are constants. The result follows by exponentiating the above equation.
(d) We have

$$\sigma(-z) = -z\prod_{\substack{\omega\in\Lambda\\ \omega\neq 0}}\left(1+\frac{z}{\omega}\right)e^{\frac{-z}{\omega}+\frac{1}{2}\left(\frac{-z}{\omega}\right)^2}.$$

The above expression is equal to $-\sigma(z)$, since the product is taken over all the non-zero lattice points

3. q-Expansion of the Weierstrass σ-function

Let $\tau \in \mathbb{H}$, where $\mathbb{H} = \{z \in \mathbb{C}; \mathrm{Im}(z) > 0\}$ is the upper half-plane. Let $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ be a normalized lattice (i.e. one of the generators is 1). We will use the notations $\wp(z;\Lambda_\tau) = \wp(z,\tau)$ and $\sigma(z;\Lambda_\tau) = \sigma(z,\tau)$. We note that $\wp$ and σ can be considered as functions of two variables $(z,\tau) \in \mathbb{C}\times\mathbb{H}$. Since $1 \in \Lambda_\tau$, the $\wp$-function satisfies the relation $\wp(z+1,\tau) = \wp(z,\tau)$. This means that we can expand $\wp$ as Fourier series in the variable $u = e^{2\pi i z}$. Similarly, since $\Lambda_{\tau+1} = \Lambda_\tau$, the $\wp$-function satisfies $\wp(z,\tau+1) = \wp(z,\tau)$. Thus as a function of τ, the function $\wp$ also has a Fourier expansion in terms of $q = e^{2\pi i\tau}$. More precisely, let

$$u = e^{2\pi i z} \quad \text{and} \quad q = e^{2\pi i\tau},$$

and let

$$q^{\mathbb{Z}} = \{q^k; k \in \mathbb{Z}\}$$

be the cyclic subgroup of the multiplicative group $\mathbb{C}^*$ generated by q. Then there is a complex analytic isomorphism

$$\begin{aligned}\mathbb{C}/\Lambda_\tau &\xrightarrow{\sim} \mathbb{C}^*/q^Z,\\ z &\longmapsto e^{2\pi i z}.\end{aligned}$$

Using this transformation, the following theorem gives the formula for the σ-function in $\mathbb{C}^*/q^Z$.
Theorem 1.1: The q-product expansion for the σ-function is given by

$$\sigma(u,q) = -\frac{1}{2\pi i}e^{\frac{1}{2}\eta z^2-\pi i z}(1-u)\prod_{m\geq 1}\frac{(1-q^m u)(1-q^m u^{-1})}{(1-q^m)^2}.$$

Proof. See [7, Chapter I, Theorem 6.4]
In [1] by employing Theorem[1.1] Silverman and Stephens proved the following result regarding the sign of an EDS.
Theorem 1.2: Let (W_n) be an unbounded nonsingular elliptic divisibility sequence. Then possibly after replacing (W_n) by the related sequence $((-1)^n W_n)$, there is an irrational number $\beta \in \mathbb{R}$ so that the sign of W_n is given by one of the following formulas:

$$\mathrm{Sign}(W_n) = (-1)^{\lfloor n\beta\rfloor} \quad \text{for all } n,$$

$$\mathrm{Sign}(W_n) = \begin{cases}(-1)^{\lfloor n\beta\rfloor + n/2} & ;\text{ if } n \text{ is even},\\ (-1)^{(n-1)/2} & ;\text{ if } n \text{ is odd},\end{cases}$$

where $\lfloor . \rfloor$ denotes the greatest integer function.
Proof. See [1,Theorem 4].

4. Elliptic Nets

The concept of elliptic divisibility sequences has been generalized as follows.
Definition 2.1. Let A be a finitely-generated free abelian group, and let R be an integral domain. An elliptic net is a map $W: A \to R$ with

$$W(0) = 0,$$

and such that for all $p,q,r,s \in A$,

$$W(p+q+s)W(p-q)W(r+s)W(r) + W(q+r+s)W(q-r)W(p+s)W(p) + W(r+p+s)W(r-p)W(q+s)W(q) = 0$$

If $A = R = \mathbb{Z}$, this definition makes (W_n) an elliptic divisibility sequence. The rank of en elliptic net is defined to be the rank of free abelian group A.

Similar to division polynomials corresponding to nP, where P is a point on an elliptic curve E. We can define net polynomials for $n_1P_1 + n_2P_2 + \cdots + n_rP_r$, where $P_1, P_2, \dots, P_r$, are r points on E. In order to do this we define a function that generalizes $f_n(z)$ defined in Section 2.4.

4.1. Net Polynomials Over $\mathbb{C}$

Let E be an elliptic curve over $\mathbb{C}$. We will define rational functions $\Omega_{\mathrm{v}}: E^n \to \mathbb{C}$ for all $\mathbf{v} \in \mathbb{Z}^n$ such that for each $\mathbf{P} \in E^n$, the map

$$W_{E,\mathrm{P}}: \mathbb{Z}^n \to \mathbb{C}, \quad \mathbf{v} \mapsto \Omega_{\mathrm{v}}(\mathbf{P})$$

is an elliptic net. More precisely we have the following definition.

Definition 2.2. Fix a lattice $\Lambda \subset \mathbb{C}$ corresponding to an elliptic curve E. For $\mathbf{v} = (v_1, v_2, \dots, v_n) \in \mathbb{Z}^n$, define a function Ω_{v} on $\mathbb{C}^n$ in variables $\mathrm{z} = (z_1, z_2, \dots, z_n)$ as follows:

$$\Omega_{\mathbf{v}}(\mathbf{z}; \Lambda) = \frac{\sigma(v_1z_1 + v_2z_2 + \cdots + v_nz_n; \Lambda)}{\prod_{i=1}^{n} \sigma(z_i; \Lambda)^{2v_i^2 - \sum_{j=i}^{n} v_iv_j} \prod_{1 \le i < j \le n} \sigma(z_i + z_j; \Lambda)^{v_iv_j}}.$$

In special case of $n = 1$ for each $v \in \mathbb{Z}$, we have a function Ω_v on $\mathbb{C}$ in the variable z, we have

$$\Omega_v(z; \Lambda) = \frac{\sigma(vz, \Lambda)}{\sigma(z, \Lambda)^{v^2}}.$$

In case of $n = 2$, for each pair $(v_1, v_2) \in \mathbb{Z} \times \mathbb{Z}$, the function $\Omega_{(v_1,v_2)}$ on $\mathbb{C} \times \mathbb{C}$ in variables z_1 and z_2 is

$$\Omega_{(v_1,v_2)}(z_1, z_2; \Lambda) = \frac{\sigma(v_1z_1 + v_2z_2; \Lambda)}{\sigma(z_1; \Lambda)^{v_1^2 - v_1v_2} \sigma(z_1 + z_2; \Lambda)^{v_1v_2} \sigma(z_2; \Lambda)^{v_2^2 - v_1v_2}}.$$

We can show that Ω_{v} satisfies $(9p$. Thus we have the following result.

Theorem 2.1: Fix a lattice $\Lambda \subset \mathbb{C}$ corresponding to an elliptic curve E. Fix $z_1, z_2, \dots, z_n \in \mathbb{C}$. Then for $\mathbf{v} = (v_1, v_2, \dots, v_n) \in \mathbb{Z}^n$, the function $W: \mathbb{Z}^n \to \mathbb{C}$ defined by

$$W(\mathbf{v}) = \Omega_{\mathbf{v}}(z_1, z_2, \dots, z_n; \Lambda)$$

is an elliptic net.

Proof. See [3, Theorem 3.7].

Similar to the case of elliptic divisibility sequences, there is a relationship between elliptic nets and elliptic curves. In [3] this relationship is made explicit using curve-net theorem.

5. The Signs in an Elliptic Net

In this thesis my plan is to generalize Theorem 1.2 to elliptic nets. I am aiming to find a formula for sign of an elliptic net. In order to do that we need to generalize the q-expansion for the Weierstrass σ-function for $\mathbf{z} = (z_1, z_2, \dots, z_n)$ by the transformation used in section 3 . For simplicity, we start by generalizing the q-expansion for σ in two variables (z_1, z_2) and later we will try to extend this result for n variables.

Proposition 3.1. Let $\mathbf{v} = (v_1, v_2) \in \mathbb{Z} \times \mathbb{Z}$ and $\mathbf{z} = (z_1, z_2) \in \mathbb{C} \times \mathbb{C}$. Let $u_1 = e^{2\pi i z_1}, u_2 = e^{2\pi i z_2}$, and $q = e^{2\pi i \tau}$. Then

$$\sigma(v_1z_1 + v_2z_2) = -\frac{1}{2\pi i} \exp\left\{\frac{1}{2}\eta(v_1z_1 + v_2z_2)^2 - \pi i(v_1z_1 + v_2z_2)\right\} \theta\left(u_1^{v_1}u_2^{v_2}, q\right),$$

with

$$\theta\left(u_1^{v_1}u_2^{v_2}, q\right) = \left(1 - u_1^{v_1}u_2^{v_2}\right) \prod_{m \ge 1} \frac{\left(1 - q^m u_1^{v_1}u_2^{v_2}\right)\left(1 - q^m u_1^{-v_1}u_2^{-v_2}\right)}{(1 - q^m)^2}.$$

Since for $(v_1, v_2) \in \mathbb{Z} \times \mathbb{Z}$, the function $\Omega_{(v_1,v_2)}$ on $\mathbb{C} \times \mathbb{C}$ in variables z_1 and z_2 is

$$\Omega_{(v_1,v_2)}(z_1, z_2; \Lambda) = \frac{\sigma(v_1z_1 + v_2z_2; \Lambda)}{\sigma(z_1; \Lambda)^{v_1^2 - v_1v_2} \sigma(z_1 + z_2; \Lambda)^{v_1v_2} \sigma(z_2; \Lambda)^{v_2^2 - v_1v_2}},$$

therefore after substituting the value of σ we should get the following expression

Conjecture 3.1. Let $\mathbf{v} = (v_1, v_2) \in \mathbb{Z} \times \mathbb{Z}$ and $\mathbf{z} = (z_1, z_2) \in \mathbb{C} \times \mathbb{C}$. Let $u_1 = e^{2\pi i z_1}, u_2 = e^{2\pi i z_2}$, and $q = e^{2\pi i \tau}$. Then

$$\Omega_{(v_1,v_2)}(z_1, z_2; \Lambda) = \gamma^{v_1^2 + v_2^2 - v_1v_2 - 1} u_1^{(v_1^2 - v_1)/2} u_2^{(v_2^2 - v_2)/2} \frac{\theta\left(u_1^{v_1}u_2^{v_2}, q\right)}{\theta(u_1, q)^{v_1^2 - v_1v_2} \theta(u_2, q)^{v_2^2 - v_1v_2} \theta(u_1u_2)^{v_1v_2}},$$

where γ is a constant.

Proof. Let $\mathbf{v} = (v_1, v_2) \in \mathbb{Z} \times \mathbb{Z}$ and $\mathbf{z} = (z_1, z_2) \in \mathbb{C} \times \mathbb{C}$. Let $u_1 = e^{2\pi i z_1}, u_2 = e^{2\pi i z_2}$, and $q = e^{2\pi i \tau}$. Then

$$\sigma(v_1z_1+v_2z_2) = -\frac{1}{2\pi i}e^{\frac{1}{2}\eta(v_1z_1+v_2z_2)^2-\pi i(v_1z_1+v_2z_2)}\left(1-u_1^{v_1}u_2^{v_2}\right)\prod_{m\geq 1}\frac{\left(1-q^m u_1^{v_1}u_2^{v_2}\right)\left(1-q^m u_1^{-v_1}u_2^{-v_2}\right)}{(1-q^m)^2}.$$

$$\sigma(z_1+z_2,q) = -\frac{1}{2\pi i}e^{\frac{1}{2}\eta(z_1+z_2)^2-\pi i(z_1+z_2)}(1-u_1u_2)\prod_{m\geq 1}\frac{(1-q^m u_1u_2)(1-q^m u_1^{-1}u_2^{-1})}{(1-q^m)^2}.$$

Therefore,

$$\Omega_{(v_1,v_2)}(z_1,z_2;\Lambda) = \frac{(-1/2\pi i)\exp\{1/2\eta(v_1^2z_1^2+v_2^2z_2^2+2v_1v_2z_1z_2)-\pi i(v_1z_1+v_2z_2)\}}{[(-1/2\pi i)\exp\{1/2\eta z_1^2-\pi i z_1\}]^{v_1^2-v_1v_2}[(-1/2\pi i)\exp\{1/2\eta z_2^2-\pi i z_2\}]^{v_2^2-v_1v_2}} \quad 1$$
$$\times\frac{[(-1/2\pi i)\exp\{1/2\eta(z_1^2+z_2^2)-\pi i(z_1+z_2)\}]^{v_1v_2}}{\theta\left(u_1^{v_1}u_2^{v_2},q\right)} \quad \underline{\theta(u_1,q)^{v_1^2-v_1v_2}}$$

The part without the function theta can be written as

$$(-2\pi i)^{v_1^2+v_2^2-v_1v_2-1}\quad\frac{\exp\{1/2\eta(v_1^2z_1^2+v_2^2z_2^2+2v_1v_2z_1z_2)-\pi i(v_1z_1+v_2z_2)\}}{\exp\{1/2\eta v_1^2z_1^2-1/2\eta v_1v_2z_1^2-\pi i v_1^2z_1+\pi i v_1v_2z_1\}}$$
$$\times\frac{1}{\exp\{1/2\eta v_2^2z_2^2-1/2\eta v_1v_2z_2^2-\pi i v_2^2z_2+\pi i v_1v_2z_2\}}$$
$$\times\frac{1}{\exp\{1/2\eta v_1v_2z_1^2+1/2\eta v_1v_2z_2^2-\pi i v_1v_2z_1-\pi i v_1v_2z_2+\eta v_1v_2z_1z_2\}}$$
$$= (-2\pi i)^{v_1^2+v_2^2-v_1v_2-1}\frac{\exp\{-\pi i(v_1z_1+v_2z_2)\}}{\exp\{-\pi i(v_1^2z_1+v_2^2z_2)\}}$$
$$= (-2\pi i)^{v_1^2+v_2^2-v_1v_2-1}\exp\{\pi i(v_1^2-v_1)z_1+\pi i(v_2^2-v_2)z_2\}$$
$$= (-2\pi i)^{v_1^2+v_2^2-v_1v_2-1}\exp\{\pi i(v_1^2-v_1)z_1\}+\exp\{\pi i(v_2^2-v_2)z_2\}$$
$$= (-2\pi i)^{v_1^2+v_2^2-v_1v_2-1}\exp\left\{\frac{2\pi i(v_1^2-v_1)z_1}{2}\right\}+\exp\left\{\frac{2\pi i(v_2^2-v_2)z_2}{2}\right\}$$
$$= (-2\pi i)^{v_1^2+v_2^2-v_1v_2-1}\{e^{2\pi i z_1}\}^{(v_1^2-v_1)/2}\{e^{2\pi i z_2}\}^{(v_2^2-v_2)/2}$$
$$= (-2\pi i)^{v_1^2+v_2^2-v_1v_2-1}(u_1)^{(v_1^2-v_1)/2}(u_2)^{(v_2^2-v_2)/2}$$

Therefore

$$\Omega_{(v_1,v_2)}(z_1,z_2;\Lambda) = \gamma^{v_1^2+v_2^2-v_1v_2-1}u_1^{(v_1^2-v_1)/2}u_2^{(v_2^2-v_2)/2}\frac{\theta\left(u_1^{v_1}u_2^{v_2},q\right)}{\theta(u_1,q)^{v_1^2-v_1v_2}\theta(u_2,q)^{v_2^2-v_1v_2}\theta(u_1u_2)^{v_1v_2}},$$

My first goal in this research will be to prove the above conjectures and later use them to calculate the sign of elliptic nets following the strategy of Silverman-Stephens.

The result of this thesis will give a better understanding of elliptic nets and will lead us in better understanding of the structure of the rational points on an elliptic curve.

6. References

1. J. SILVERMAN AND N. STEPHENS, The Sign of an Elliptic Divisibility Sequence. J. Ramanujan Math Soc. 21 (2006), no. 1, 1-17.
2. M. WARD, Memoir on Elliptic Divisibility Sequences. American Journal of Mathematics. **70** (1948), 31-74.
3. K. STANGE, Elliptic Net and Elliptic Curves. Algebra Number Theory 5 (2011), no. 2, 197-229.
4. S. LANG, Elliptic Curves: Diophantine Analysis. Springer-Verlag 1978 .
5. S. LANG, Elliptic Functions. Springer-Verlag 1986.
6. J. SILVERMAN, The Arithmetic of Elliptic Curves. GTM 106, Springer-Verlag, New York, 1986 .
7. J. SILVERMAN, Advanced Topic in the Arithmetic of Elliptic Curves. GTM 151, Springer-Verlag, New York, 1994.