Formulary for elliptic divisibility sequences and elliptic nets

KATHERINE E. STANGE

Abstract. Just the formulas. No warranty is expressed or implied. May cause side effects. Not to be taken internally. Remove label before using. Not to be used as a flotation device. May contain nuts. Please report any errors you may find.

Let E be the elliptic curve defined over the rationals with Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

As usual, let

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3,$$
$$b_6 = a_3^2 + 4a_6, \quad b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

1. Recurrence relation

These formulas hold for elliptic divisibility sequences and elliptic nets, according to whether the indices are considered in $\mathbb{Z}$ or a larger free abelian group. See [5].

1.1. **Definition.** Definition 1.1 in [5].

$$\begin{aligned}(1)\quad & W(p+q+s)\,W(p-q)\,W(r+s)\,W(r) \\ & + W(q+r+s)\,W(q-r)\,W(p+s)\,W(p) \\ & + W(r+p+s)\,W(r-p)\,W(q+s)\,W(q) = 0\end{aligned}$$

1.2. **Stephens form.** Due to Nelson Stephens. Obtained from (1) by $s \leftarrow 2a$, $r \leftarrow b-a$, $p \leftarrow c-a$, $q \leftarrow d-a$.

$$\begin{aligned}& W(a+b)\,W(a-b)\,W(c+d)\,W(c-d) \\ & + W(a+c)\,W(a-c)\,W(d+b)\,W(d-b) \\ & + W(a+d)\,W(a-d)\,W(b+c)\,W(b-c) = 0\end{aligned}$$

1.3. **Brown form.** Due to Dan Brown; equation (3) in [1].

$$\begin{aligned}& W(p)\,W(q)\,W(r)\,W(s) \\ & - W\left(\frac{-p+q+r+s}{2}\right)W\left(\frac{p-q+r+s}{2}\right)W\left(\frac{p+q-r+s}{2}\right)W\left(\frac{p+q+r-s}{2}\right) \\ & - W\left(\frac{p+q+r+s}{2}\right)W\left(\frac{p+q-r-s}{2}\right)W\left(\frac{p-q+r-s}{2}\right)W\left(\frac{p-q-r+s}{2}\right) = 0\end{aligned}$$

Date: May 2, 2012, Draft #1.

1.4. **Ward's elliptic divisibility sequences recurrence relation.** Not sufficient for generating a net of higher rank. Equation (4.11) in [9]. Obtained from (1) by $p \leftarrow n$, $q \leftarrow m$, $s \leftarrow 0$, $r \leftarrow 1$.

$$W(n+m)W(n-m)W(1)^2 = W(n+1)W(n-1)W(m)^2 - W(m+1)W(m-1)W(n)^2.$$

1.5. **Miscellaneous special cases.**

$$\begin{aligned}
W(2n)W(2)W(1)^2 &= W(n)(W(n+2)W(n-1)^2 - W(n-2)W(n+1)^2),\\
W(2n+1)W(1)^3 &= W(n+2)W(n)^3 - W(n-1)W(n+1)^3,\\
W(nm)W(2)W(1)^2 &= W\left(\tfrac{nm}{2}\right)\left(W\left(\tfrac{nm}{2}+2\right)W\left(\tfrac{nm}{2}-1\right)^2 - W\left(\tfrac{nm}{2}-2\right)W\left(\tfrac{nm}{2}+1\right)^2\right),\\
W(nm)W(n)W(1)^2 &= W\left(\tfrac{n(m+1)}{2}+1\right)W\left(\tfrac{n(m+1)}{2}-1\right)W\left(\tfrac{n(m-1)}{2}\right)^2\\
&\quad - W\left(\tfrac{n(m-1)}{2}+1\right)W\left(\tfrac{n(m-1)}{2}-1\right)W\left(\tfrac{n(m+1)}{2}\right)^2.
\end{aligned}$$

1.6. **Special cases for rank two nets.** Theorem 2.5 in [5].

$$W(1,-1)W(1,1)^3 = W(0,1)^3W(2,1) - W(1,0)^3W(1,2).$$

The following formulas assume some terms near the origin are equal to one: $W(1,0) = W(0,1) = W(1,1) = 1$. Equations (12)-(17) in [6].

$$\begin{aligned}
W(2i-1,0) &= W(i+1,0)W(i-1,0)^3 - W(i-2,0)W(i,0)^3,\\
W(2i,0)W(2,0) &= W(i,0)W(i+2,0)W(i-1,0)^2 - W(i,0)W(i-2,0)W(i+1,0)^2,\\
W(2k-1,1)W(1,1) &= W(k+1,1)W(k-1,1)W(k-1,0)^2 - W(k,0)W(k-2,0)W(k,1)^2,\\
W(2k,1) &= W(k-1,1)W(k+1,1)W(k,0)^2 - W(k-1,0)W(k+1,0)W(k,1)^2,\\
W(2k+1,1)W(-1,1) &= W(k-1,1)W(k+1,1)W(k+1,0)^2 - W(k,0)W(k+2,0)W(k,1)^2,\\
W(2k+2,1)W(2,-1) &= W(k+1,0)W(k+3,0)W(k,1)^2 - W(k-1,1)W(k+1,1)W(k+2,0)^2,
\end{aligned}$$

2. Complex Function Formulas

2.1. **Weierstrass σ-function definition of net polynomials.** See Definition 3.1 in [5]. For $n = 1$ (sequences), see Theorem 12.1 in [9].

(1) $n = 1$:

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

(2) $n = 2$:

$$\Omega_{u,v}(z,w;\Lambda) = \frac{\sigma(uz+vw;\Lambda)}{\sigma(z;\Lambda)^{u^2-uv}\sigma(z+w;\Lambda)^{uv}\sigma(w;\Lambda)^{v^2-uv}}.$$

(3) general n:

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

2.2. **Complex function identities.** See Lemmas 3.5 and 3.6 in [5]. For the first equation, see also [2] or any book on elliptic functions.

$$\wp(z) - \wp(w) = -\frac{\sigma(z+w)\sigma(z-w)}{\sigma(z)^2\sigma(w)^2},$$
$$\wp(\mathbf{v}\cdot\mathbf{z}) - \wp(\mathbf{w}\cdot\mathbf{z}) = -\frac{\Omega_{\mathbf{v}+\mathbf{w}}(\mathbf{z})\Omega_{\mathbf{v}-\mathbf{w}}(\mathbf{z})}{\Omega_{\mathbf{v}}(\mathbf{z})^2\Omega_{\mathbf{w}}(\mathbf{z})^2},$$
$$\zeta(x+a) - \zeta(a) - \zeta(x+b) + \zeta(b) = \frac{\sigma(x+a+b)\sigma(x)\sigma(a-b)}{\sigma(x+a)\sigma(x+b)\sigma(a)\sigma(b)},$$
$$\zeta(x+a+b) - \zeta(x+a) - \zeta(x+b) + \zeta(x) = \frac{\sigma(2x+a+b)\sigma(a)\sigma(b)}{\sigma(x+a+b)\sigma(x+a)\sigma(x+b)\sigma(x)}.$$

3. Division and Net polynomials

3.1. **Division polynomials.** See [2], [3, p.80], [4, Exercise 3.7] or many other resources.

$\Psi_1 = 1, \qquad \Psi_2 = 2y + a_1x + a_3,$

$\Psi_3 = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,$

$\Psi_4 = (2y + a_1x + a_3)(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2);$

3.2. **Net polynomials.** See Proposition 3.8 in [5].

(1) for $n = 2$:

$$\Psi_{(1,-1)} = x_2 - x_1,$$
$$\Psi_{(2,1)} = 2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) + a_2,$$
$$\Psi_{(2,-1)} = (y_1 + y_2)^2 - (2x_1 + x_2)(x_1 - x_2)^2 \ ;$$

(2) for $n = 3$:

$$\Psi_{(1,1,1)} = \frac{y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)},$$
$$\Psi_{(-1,1,1)} = \frac{y_1(x_2 - x_3) - y_2(x_3 - x_1) - y_3(x_1 - x_2)}{(x_2 - x_3)} + a_1x_1 + a_3,$$
$$\Psi_{(1,-1,1)} = \frac{-y_1(x_2 - x_3) + y_2(x_3 - x_1) - y_3(x_1 - x_2)}{(x_3 - x_1)} + a_1x_2 + a_3,$$
$$\Psi_{(1,1,-1)} = \frac{-y_1(x_2 - x_3) - y_2(x_3 - x_1) + y_3(x_1 - x_2)}{(x_1 - x_2)} + a_1x_3 + a_3.$$

4. Formulas relating curves and nets

4.1. **Points in terms of division polynomials.** See any of the resources in Section 3.1. Define

$$\phi_m = x(P)\Psi_m^2 - \Psi_{m+1}\Psi_{m-1},$$
$$4y\omega_m = \Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2.$$

Then

$$[m]P = \left(\frac{\phi_m(P)}{\Psi_m(P)^2}, \frac{\omega_m(P)}{\Psi_m(P)^3}\right),$$
$$x([m]P) - x([n]P) = -\frac{\Psi_{m+n}(P)\Psi_{m-n}(P)}{\Psi_m^2(P)\Psi_n^2(P)}.$$

4.2. **Curves from sequences and nets, rank 1.** For the case $n = 1$, the simplest formulas are given in Theorem 4.5.3 in [8].

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

where

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

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

Morgan Ward had more complicated formulas for the usual g_2 and g_4 giving an elliptic curve (equations (13.6) and (13.7) of [9]):

$$\begin{aligned} g_2 = \frac{1}{12W_2^8W_3^4}(&W_2^{20} + 4W_2^{15}W_4 - 16W_2^{12}W_3^3 + 6W_2^{10}W_4^2 - 8W_2^7W_3^3W_4 + 4W_2^5W_4^3 \\ &+ 16W_2^4W_3^6 + 8W_2^2W_3^3W_4^2 + W_4^4) \\ g_3 = \frac{-1}{216W_2^{12}W_3^6}(&W_2^{30} + 6W_2^{25}W_4 - 24W_2^{22}W_3^3 + 15W_2^{20}W_4^2 - 60W_2^{17}W_3^3W_4 + 20W_2^{15}W_4^3 \\ &+ 120W_2^{14}W_3^6 - 36W_2^{12}W_3^3W_4^2 + 15W_2^{10}W_4^4 - 48W_2^9W_3^6W_4 + 12W_2^7W_3^3W_4^3 \\ &+ 64W_2^6W_3^9 + 6W_2^5W_4^5 + 48W_2^4W_3^6W_4^2 + 12W_2^2W_3^3W_4^4 + W_4^6) \\ \wp(u) = \frac{1}{12W_2^4W_3^2}(&W_4^2 + 2W_2^5W_4 + 4W_2^2W_3^3 + W_2^{10}) \\ \wp'(u) = -W_2 \end{aligned}$$

For $n = 2$, see Proposition 6.4 and Remark 6.6 in [5].

(1) in rank $n = 2$:

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad P_1 = (0, 0), \qquad P_2 = (W(2, 1) - W(1, 2), 0),$$

where

$$a_1 = \frac{W(2, 0) - W(0, 2)}{W(2, 1) - W(1, 2)}, \qquad a_2 = 2W(2, 1) - W(1, 2), \qquad a_3 = W(2, 0)$$

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

(2) alternative in rank $n = 2$ and characteristic $\neq 2$:

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad P_1 = (v, 0), \qquad P_2 = (-v, 0), ,$$

where

$$2v = W(2,1) - W(1,2),$$

$$a_1 = \frac{W(2,0) - W(0,2)}{W(2,1) - W(1,2)}, \qquad 2a_2 = W(2,1) + W(1,2), \qquad 2a_3 = W(2,0) + W(0,2)$$

$$4a_4 = -(W(2,1) - W(1,2))^2, \qquad 8a_6 = -(W(2,1) - W(1,2))^2(W(2,1) + W(1,2))$$

5. Change of basis for elliptic nets

See Proposition 4.3 in [5]. Let T be any $n \times m$ matrix. Let $\mathbf{P} \in E^m$, $\mathbf{v} \in \mathbb{Z}^n$.

$$W_{E,\mathbf{P}}(T^{tr}(\mathbf{v})) = W_{E,T(\mathbf{P})}(\mathbf{v}) \prod_{i=1}^{n} W_{E,\mathbf{P}}(T^{tr}(\mathbf{e}_i))^{v_i^2 - v_i(\sum_{j \neq i} v_j)} \prod_{1 \leq i < j \leq n} W_{E,\mathbf{P}}(T^{tr}(\mathbf{e}_i + \mathbf{e}_j))^{v_i v_j}$$

6. Partial periodicity

6.1. **Periodicity formulas for non-degenerate elliptic nets.** The rank $n = 1$ case is Theorem 8.1 in [9]. For rank $n = 2$, see Theorem 5 in [7].

(1) rank $n = 1$ with $W_{E,P}(r) = 0$:

$$W_{E,P}(sr + k) = W_{E,P}(k) a^{sk} b^{s^2}$$

where

$$a = \frac{W_{E,P}(r+2)}{W_{E,P}(r+1)W_{E,P}(2)}, \qquad b = \frac{W_{E,P}(r+1)^2 W_{E,P}(2)}{W_{E,P}(r+2)}$$

(2) rank $n = 2$ with $W_{E,P,Q}(\mathbf{r}) = 0$:

$$W_{E,P,Q}(l\mathbf{r} + \mathbf{k}) = W_{E,P,Q}(\mathbf{k}) a_{\mathbf{r}}^{lk_1} b_{\mathbf{r}}^{lk_2} c_{\mathbf{r}}^{l^2}$$

where

$$a_{\mathbf{r}} = \frac{W_{E,P,Q}(r_1 + 2, r_2)}{W_{E,P,Q}(r_1 + 1, r_2) W_{E,P,Q}(2,0)}, \quad b_{\mathbf{r}} = \frac{W_{E,P,Q}(r_1, r_2 + 2)}{W_{E,P,Q}(r_1, r_2 + 1) W_{E,P,Q}(0,2)},$$

$$c_{\mathbf{r}} = \frac{W_{E,P,Q}(r_1 + 1, r_2 + 1)}{a_{\mathbf{r}} b_{\mathbf{r}} W_{E,P,Q}(1,1)}.$$

6.2. **Perfectly periodic elliptic divisibility sequence and elliptic net over $\mathbb{F}_q$.** See Theorem 6 in [7].

$$\phi(P) = \left(\frac{W_{E,P}(q-1)}{W_{E,P}(q - 1 + \mathrm{ord}(P))} \right)^{\frac{1}{\mathrm{ord}(P)^2}},$$

$$\phi(\mathbf{v} \cdot \mathbf{P}) = W_{E,\mathbf{P}}(\mathbf{v}) \prod_{i=1}^{n} \phi(P_i)^{v_i^2 - v_i(\sum_{j \neq i} v_j)} \prod_{1 \leq i < j \leq n} \phi(P_i + P_j)^{v_i v_j}.$$

7. Tate-Lichtenbaum and Weil pairing formulas

These are all from [6]; see Theorem 6 and Corollary 1.

$$\tau_m(P,Q) = \frac{\mathcal{W}(mp+q+s)\mathcal{W}(s)}{\mathcal{W}(mp+s)\mathcal{W}(q+s)},$$
$$e_m(P,Q) = \frac{\mathcal{W}(mp+q+s)\mathcal{W}(p+s)\mathcal{W}(mq+s)}{\mathcal{W}(mp+s)\mathcal{W}(q+s)\mathcal{W}(p+mq+s)}$$

Special cases:

$$\tau_m(P,P) = \frac{W_P(m+2)W_P(1)}{W_P(m+1)W_P(2)} \ ,$$
$$\tau_m(P,Q) = \frac{W_{P,Q}(m+1,1)W_{P,Q}(1,0)}{W_{P,Q}(m+1,0)W_{P,Q}(1,1)} \ .$$

8. Discrete log Type Equations

Equations (9) and (11) in [7]. Suppose $[m]P = \mathcal{O}$ and $Q = [k]P$.

$$\left(\frac{W_{E,P,Q}(m+1,0)W_{E,P,Q}(2,0)}{W_{E,P,Q}(m+2,0)}\right)^k = \left(\frac{W_{E,P}(k-1)}{W_{E,P}(k)}\right)^m \left(-\frac{W_{E,P,Q}(1,m)W_{E,P,Q}(2,0)}{W_{E,P,Q}(2,m)W_{E,P,Q}(1,-1)^m}\right),$$
$$W_{E,P}(m+1)^{2k+1} = \frac{W_{E,P,Q}(m+1,m+1)}{W_{E,P,Q}(0,m+1)}\left(\frac{W_{E,P}(k+1)}{W_{E,P}(k)}\right)^{m(m+2)} .$$

Acknowledgements. Thank you to Dan Brown for corrections.

References

[1] Daniel R. L. Brown. Stange's elliptic nets and coxeter group f4. Cryptology ePrint Archive, Report 2010/161, 2010. `http://eprint.iacr.org/`.

[2] K. Chandrasekharan. *Elliptic functions*, volume 281 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1985.

[3] Gerhard Frey and Tanja Lange. Background on curves and Jacobians. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 45–85. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[4] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[5] Katherine Stange. Elliptic nets and elliptic curves. *Algebra Number Theory*, 5(2):197–229, 2011.

[6] Katherine E. Stange. The Tate pairing via elliptic nets. In *Pairing-Based Cryptography - PAIRING 2007*, volume 4575 of *Lecture Notes in Comput. Sci.*, pages 329–348. Springer, Berlin, 2007.

[7] Katherine E. Stange. The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences. In *Selected Areas in Cryptography 2008*, volume 5381 of *Lecture Notes in Comput. Sci.*, pages 309–327. Springer, Berlin, 2009.

[8] Christine Swart. *Elliptic curves and related sequences*. PhD thesis, Royal Holloway and Bedford New College, University of London, 2003.

[9] Morgan Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.

Department of Mathematics, Stanford University, 450 Serra Mall, Bldg 380, Stanford, CA 94305

E-mail address: `stange@math.stanford.edu`