Introduction to Divisibility Sequences for Elliptic Curves with Complex Multiplication

Edison Au-Yeung
University of Warwick

Y-RANT VI, University of Oxford

31 July 2024

Small recap

- Let $f(x,y,\boldsymbol{a}) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$.
  Given some $a_i \in \mathbb{Q}$, we have a cubic curve $E : f = 0$.
- $E(\mathbb{Q})$ is the set of solutions $(x,y) \in \mathbb{Q}^2$ together with a point at infinity O.
- Nonsingular points $E(\mathbb{Q})^{\text{ns}}$ form a commutative group in a natural way.
- O is the identity in this group: $P +_E O = P$ for all $P \in E(\mathbb{Q})$.
  We let $[n] : E \to E$ be multiplication by n in this group.
- There are polynomials $\psi_n, \omega_n \in \mathbb{Z}[x,y,\boldsymbol{a}]/\langle f(x,y,\boldsymbol{a})\rangle$ for $n \in \mathbb{N}$ with

$$[n](x,y) = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\omega_n}{\psi_n^3} \right) \quad (n \geq 2,\ (x,y) \in E(\mathbb{Q})^{\mathrm{ns}}),$$

$$\psi_{m+n}\psi_{m-n}\psi_r^2 = \psi_{m+r}\psi_{m-r}\psi_n^2 - \psi_{n+r}\psi_{n-r}\psi_m^2 \quad (r < n < m).$$

- $\psi_1 = 1, \psi_2 = 2y + a_1x + a_3,\ \psi_3, \psi_4 =$ some nastier polynomials.

Two definitions

Definition (EDS(A))

A sequence of integers $\{h_n\}_{n\in\mathbb{N}}$ is an EDS(A) if it satisfies $h_0 = 0$, $h_1 = 1$, h_2 divides h_4 and the recurrence relation below: for any integer $m \geq n \geq r$, $\{h_n\}_{n\in\mathbb{N}}$ satisfies

$$h_{m+n}h_{m-n}h_r^2 = h_{m+r}h_{m-r}h_n^2 - h_{n-r}h_{n+r}h_m^2.$$

Two definitions

Definition (EDS(A))

A sequence of integers $\{h_n\}_{n\in\mathbb{N}}$ is an EDS(A) if it satisfies $h_0 = 0$, $h_1 = 1$, h_2 divides h_4 and the recurrence relation below: for any integer $m \geq n \geq r$, $\{h_n\}_{n\in\mathbb{N}}$ satisfies

$$h_{m+n}h_{m-n}h_r^2 = h_{m+r}h_{m-r}h_n^2 - h_{n-r}h_{n+r}h_m^2.$$

Definition (EDS(B))

Let $E/\mathbb{Q}$ be an elliptic curve over the rationals defined by a Weierstrass equation with integer coefficients. For every $n \in \mathbb{N}$ and $P \in E(\mathbb{Q})$, we write the x-coordinate of nP

$$x(nP) = \frac{A_n(E,P)}{B_n^2(E,P)}$$

with $A_n(E,P)$ and $B_n(E,P)$ two coprime integers and $B_n(E,P) \geq 0$. Then we call the sequence $\{B_n(E,P)\}_{n\in\mathbb{N}}$ an EDS(B).

Two definitions

Definition (EDS(A))

A sequence of integers $\{h_n\}_{n\in\mathbb{N}}$ is an EDS(A) if it satisfies $h_0 = 0$, $h_1 = 1$, h_2 divides h_4 and the recurrence relation below: for any integer $m \geq n \geq r$, $\{h_n\}_{n\in\mathbb{N}}$ satisfies

$$h_{m+n}h_{m-n}h_r^2 = h_{m+r}h_{m-r}h_n^2 - h_{n-r}h_{n+r}h_m^2.$$

Definition (EDS(B))

Let $E/\mathbb{Q}$ be an elliptic curve over the rationals defined by a Weierstrass equation with integer coefficients. For every $n \in \mathbb{N}$ and $P \in E(\mathbb{Q})$, we write the x-coordinate of nP

$$x(nP) = \frac{A_n(E,P)}{B_n^2(E,P)}$$

with $A_n(E,P)$ and $B_n(E,P)$ two coprime integers and $B_n(E,P) \geq 0$. Then we call the sequence $\{B_n(E,P)\}_{n\in\mathbb{N}}$ an EDS(B).

In general, EDS(A) $\neq$ EDS(B).

Complex multiplication

- Let $E/\mathbb{C}$ be an elliptic curve over the rationals defined by a Weierstrass equation with integer coefficients, then $\mathrm{End}(E)$ is always isomorphic to $\mathbb{Z}$ or $\mathbb{Z}[\omega]$, an order in an imaginary quadratic field F.
- When E/K has complex multiplicaton, it then makes sense for us to consider $[\alpha]\colon E \to E$, multiplication by $\alpha \in \mathbb{Z}[\omega]$ in the group $E(K)^{\text{ns}}$.

Complex multiplication

- Let $E/\mathbb{C}$ be an elliptic curve over the rationals defined by a Weierstrass equation with integer coefficients, then $\mathrm{End}(E)$ is always isomorphic to $\mathbb{Z}$ or $\mathbb{Z}[\omega]$, an order in an imaginary quadratic field F.
- When E/K has complex multiplicaton, it then makes sense for us to consider $[\alpha]\colon E \to E$, multiplication by $\alpha \in \mathbb{Z}[\omega]$ in the group $E(K)^{\mathsf{ns}}$.
- Are the following sensible things to write down?
  1. Define EDS(A) to be a sequence of elements in $\mathrm{End}(E) = \mathbb{Z}[\omega]$ that satisfies the recurrence relation
  $$h_{\alpha+\beta}h_{\alpha-\beta}h_\gamma^2 = h_{\alpha+\beta}h_{\alpha-\gamma}h_\beta^2 - h_{\beta-\gamma}h_{\beta+\gamma}h_\alpha^2, \quad \alpha, \beta, \gamma \in \mathbb{Z}[\omega].$$
  2. Let E/K be an elliptic curve defined by a Weierstrass equation with coefficients in $\mathcal{O}_K$ and has complex multiplication by $\mathbb{Z}[\omega] \subset K$. For every $\alpha \in \mathbb{Z}[\omega]$ and $P \in E(K)$, we write the x-coordinate of αP
  $$x(\alpha P) = \frac{A_\alpha(E,P)}{B_\alpha^2(E,P)}.$$
  We call the sequence of *elements* $\{B_\alpha(E,P)\}_{\alpha\in\mathbb{Z}[\omega]}$ an EDS(B).

CM EDS(B)

Let E/K be an elliptic curve defined by a Weierstrass equation with coefficients in $\mathcal{O}_K$ and having complex multiplication by $\mathbb{Z}[\omega] \subset F$. For every $\alpha \in \mathbb{Z}[\omega]$ and $P \in E(K)$, we write the x-coordinate of αP

$$x(\alpha P) = \frac{A_\alpha(E,P)}{B_\alpha^2(E,P)}.$$

We call the sequence of *elements* $\{B_\alpha(E,P)\}_{\alpha \in \mathbb{Z}[\omega]}$ an EDS(B)(?)

CM EDS(B)

Let E/K be an elliptic curve defined by a Weierstrass equation with coefficients in $\mathcal{O}_K$ and having complex multiplication by $\mathbb{Z}[\omega] \subset F$. For every $\alpha \in \mathbb{Z}[\omega]$ and $P \in E(K)$, we write the x-coordinate of αP

$$x(\alpha P) = \frac{A_\alpha(E,P)}{B_\alpha^2(E,P)}.$$

We call the sequence of *elements* $\{B_\alpha(E,P)\}_{\alpha \in \mathbb{Z}[\omega]}$ an EDS(B)(?)

- An order of an imaginary quadratic field K need not be a unique factorisation domain. However, we always have *unique factorisation of ideals*, so $\{B_\alpha(E,P)\}_{\alpha \in \mathbb{Z}[\omega]}$ should be a sequence of *ideals* instead.

CM EDS(B)

Let E/K be an elliptic curve defined by a Weierstrass equation with coefficients in $\mathcal{O}_K$ and having complex multiplication by $\mathbb{Z}[\omega] \subset F$. For every $\alpha \in \mathbb{Z}[\omega]$ and $P \in E(K)$, we write the x-coordinate of αP

$$x(\alpha P) = \frac{A_\alpha(E,P)}{B_\alpha^2(E,P)}.$$

We call the sequence of *elements* $\{B_\alpha(E,P)\}_{\alpha\in\mathbb{Z}[\omega]}$ an EDS(B)(?)

- An order of an imaginary quadratic field K need not be a unique factorisation domain. However, we always have *unique factorisation of ideals*, so $\{B_\alpha(E,P)\}_{\alpha\in\mathbb{Z}[\omega]}$ should be a sequence of *ideals* instead.
- A sequence $\{h_n\}_{n\in\mathbb{N}}$ is a divisibility sequence if $h_m \mid h_n$ whenever $m \mid n$. Hence, we should also index our CM EDS(B) by *ideals* of $\mathrm{End}(E)$.

CM EDS(B)

Let E/K be an elliptic curve defined by a Weierstrass equation with coefficients in $\mathcal{O}_K$ and having complex multiplication by $\mathbb{Z}[\omega] \subset F$. For every $\alpha \in \mathbb{Z}[\omega]$ and $P \in E(K)$, we write the x-coordinate of αP

$$x(\alpha P) = \frac{A_\alpha(E,P)}{B_\alpha^2(E,P)}.$$

We call the sequence of *elements* $\{B_\alpha(E,P)\}_{\alpha \in \mathbb{Z}[\omega]}$ an EDS(B)(?)

- An order of an imaginary quadratic field K need not be a unique factorisation domain. However, we always have *unique factorisation of ideals*, so $\{B_\alpha(E,P)\}_{\alpha \in \mathbb{Z}[\omega]}$ should be a sequence of *ideals* instead.
- A sequence $\{h_n\}_{n \in \mathbb{N}}$ is a divisibility sequence if $h_m \mid h_n$ whenever $m \mid n$. Hence, we should also index our CM EDS(B) by *ideals* of $\mathrm{End}(E)$.

But when we write $[\alpha]P$, we do not mean a 'ideal–multiple' of a point (e.g. $x([\langle 2, 1+\sqrt{-5}\rangle]P)$ does not make sense)!!

CM EDS(B)

Definition (Streng, 2008)

Let E/K be an elliptic curve with complex multiplication (i.e. $\mathrm{End}(E)$ is congruent to an order in an imaginary quadratic field F). For a point $P \in E(K)$, we define the coprime $\mathcal{O}_F$ ideals A_α and B_α by

$$x(\alpha P) = A_\alpha B_\alpha^{-2}.$$

The *CM elliptic divisibility sequence* associated to P is the sequence $(B_\mathfrak{a})_{\mathfrak{a} \in \mathcal{O}_F}$, indexed by ideals $\mathfrak{a}$ of $\mathcal{O}_F$, given by

$$B_\mathfrak{a} = \sum_{\alpha \in \mathfrak{a}} B_\alpha.$$

CM EDS(B)

For $x(\alpha P) = A_\alpha B_\alpha^{-2}$, the *CM elliptic divisibility sequence* associated to P is the sequence $(B_\mathfrak{a})_{\mathfrak{a}\in\mathcal{O}_F}$, indexed by ideals $\mathfrak{a}$ of $\mathcal{O}_F$, given by

$$B_\mathfrak{a} = \sum_{\alpha\in\mathfrak{a}} B_\alpha.$$

Lemma

Let α, β be elements in $\mathrm{End}(E)$, if $\alpha \mid \beta$, then $B_\alpha \mid B_\beta$ (i.e. $B_\beta \subset B_\alpha$ as ideals).

- For every discrete valuation ν of K, we have $\nu(B_\mathfrak{a}) = \min_{\alpha\in\mathfrak{a}} \nu(B_\alpha)$.
- Weak divisibility: if $\mathfrak{a} \mid \mathfrak{b}$, then $B_\mathfrak{a} \mid B_\mathfrak{b}$.
- Strong divisibility: $B_{\mathfrak{a}+\mathfrak{b}} = B_\mathfrak{a} + B_\mathfrak{b}$.
- If $\mathfrak{a} = \alpha\mathcal{O}_F$ is a principal ideal, then we have $B_{\alpha\mathcal{O}_F} = B_\alpha$.

Issues with CM EDS(B)

Choice of generator: In $\mathbb{Q}$, there are only two units (± 1), so we can always by default choose $B_n > 0$. But this is not always the case for quadratic imaginary fields (consider $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$) and sign does not make sense for complex numbers.

Example: elliptic curve $E/\mathbb{Q}(i)\colon y^2 = x^3 - 2x$ with complex multiplication by $\mathbb{Z}[i]$. EDS(B) generated by the point $P = (-1, 1) \in E(\mathbb{Q}(i))$.

- $x([1+i]P) = \left(-\frac{i}{2}, -\frac{3i+3}{4}\right)$, so $B_{1+i} = (1+i) = (1-i)$.
- $x([2+i]P) = \left(-\frac{(4+i)^2}{(1+2i)^2}, \frac{(4+i)(16+9i)}{i(1+2i)^3}\right)$, so $B_{2+i} = (2-i) = (1+2i)$.
- This makes it difficult to relate it to CM EDS(A).

CM EDS(A)

Define EDS(A) to be a sequence of elements in $\mathrm{End}(E) = \mathbb{Z}[\omega]$ that satisfies the recurrence relation

$$h_{\alpha+\beta} h_{\alpha-\beta} h_\gamma^2 = h_{\alpha+\beta} h_{\alpha-\gamma} h_\beta^2 - h_{\beta-\gamma} h_{\beta+\gamma} h_\alpha^2, \quad \alpha, \beta, \gamma \in \mathbb{Z}[\omega](?)$$

- Remember this recurrence relation comes from elliptic curve over $\mathbb{Q}$: There are polynomials $\psi_n, \omega_n \in \mathbb{Z}[x, y, \boldsymbol{a}]/\langle f(x, y, \boldsymbol{a}) \rangle$ for $n \in \mathbb{N}$ with

$$[n](x,y) = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\omega_n}{\psi_n^3} \right) \quad (n \geq 2,\ (x,y) \in E(\mathbb{Q})^{\mathrm{ns}}),$$

$$\psi_{m+n}\psi_{m-n}\psi_r^2 = \psi_{m+r}\psi_{m-r}\psi_n^2 - \psi_{n+r}\psi_{n-r}\psi_m^2 \quad (r < n < m).$$

- When the elliptic curve has complex multiplication, do we still have the idea of division polynomial and 'a recurrence relation'?

CM EDS(A)

Define EDS(A) to be a sequence of elements in $\mathrm{End}(E) = \mathbb{Z}[\omega]$ that satisfies the recurrence relation

$$h_{\alpha+\beta}h_{\alpha-\beta}h_\gamma^2 = h_{\alpha+\beta}h_{\alpha-\gamma}h_\beta^2 - h_{\beta-\gamma}h_{\beta+\gamma}h_\alpha^2, \quad \alpha, \beta, \gamma \in \mathbb{Z}[\omega].$$

- Recall an order of a quadratic imaginary field $\mathbb{Z}[\omega]$ is a rank 2 $\mathbb{Z}$–module: $\mathbb{Z} \bigoplus \omega\mathbb{Z}$.
- For $P \in E(K)^{\text{ns}}, [\alpha] \colon E \to E$ where $\alpha \in \mathbb{Z}[\omega]$, we interpret $[\alpha]P$ as a sum of two points of integral multiple:

$$[\alpha]P = [a + b\omega]P = [a]P + [b](\omega P).$$

CM EDS(A)

Define EDS(A) to be a sequence of elements in $\mathrm{End}(E) = \mathbb{Z}[\omega]$ that satisfies the recurrence relation

$$h_{\alpha+\beta}h_{\alpha-\beta}h_{\gamma}^2 = h_{\alpha+\beta}h_{\alpha-\gamma}h_{\beta}^2 - h_{\beta-\gamma}h_{\beta+\gamma}h_{\alpha}^2, \quad \alpha, \beta, \gamma \in \mathbb{Z}[\omega].$$

- Recall an order of a quadratic imaginary field $\mathbb{Z}[\omega]$ is a rank 2 $\mathbb{Z}$–module: $\mathbb{Z} \bigoplus \omega\mathbb{Z}$.
- For $P \in E(K)^{\text{ns}}, [\alpha] \colon E \to E$ where $\alpha \in \mathbb{Z}[\omega]$, we interpret $[\alpha]P$ as a sum of two points of integral multiple:

$$[\alpha]P = [a + b\omega]P = [a]P + [b](\omega P).$$

1. We want a 'higher rank' elliptic divisibility sequence via a recurrence relation.
2. Ideally, this recurrence relation is satisfied by a collection of rational functions on elliptic curves.

CM EDS(A) – Elliptic Net

Definition (Elliptic Net; Stange, 2007)

Let A be a free finitely-generated abelian group and R be an integral domain. An *elliptic net* is any map $W : A \to R$ with $W(\mathbf{0}) = \mathbf{0}$ and for any $\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r}, \boldsymbol{s} \in A$,

$$\begin{aligned} W(\boldsymbol{p}+\boldsymbol{q}+\boldsymbol{s})W(\boldsymbol{p}-\boldsymbol{q})W(\boldsymbol{r}+\boldsymbol{s})W(\boldsymbol{r}) \\ + W(\boldsymbol{q}+\boldsymbol{r}+\boldsymbol{s})W(\boldsymbol{q}-\boldsymbol{r})W(\boldsymbol{p}+\boldsymbol{s})W(\boldsymbol{p}) \\ + W(\boldsymbol{r}+\boldsymbol{p}+\boldsymbol{s})W(\boldsymbol{r}-\boldsymbol{p})W(\boldsymbol{q}+\boldsymbol{s})W(\boldsymbol{q}) = 0. \end{aligned}$$

We identify the rank of W as the rank of the elliptic net.

This is indeed a generalisation of EDS(A):
take $A = \mathbb{Z}$, $\boldsymbol{p} = m, \boldsymbol{q} = n, \boldsymbol{r} = r, \boldsymbol{s} = 0$, then W is an EDS(A) by definition (note that $W(-\boldsymbol{v}) = -W(\boldsymbol{v})$).

$$W(m+n)W(m-n)W(r)^2 + W(n+r)W(n-r)W(m)^2 = W(m+r)W(m-r)W(n)^2$$

CM EDS(A) – Elliptic Net

Definition (Elliptic Net; Stange, 2007)

Let A be a free finitely-generated abelian group and R be an integral domain. An *elliptic net* is any map $W : A \to R$ with $W(\mathbf{0}) = \mathbf{0}$ and for any $\boldsymbol{p}, \boldsymbol{q}, \boldsymbol{r}, \boldsymbol{s} \in A$,

$$W(\boldsymbol{p}+\boldsymbol{q}+\boldsymbol{s})W(\boldsymbol{p}-\boldsymbol{q})W(\boldsymbol{r}+\boldsymbol{s})W(\boldsymbol{r}) + W(\boldsymbol{q}+\boldsymbol{r}+\boldsymbol{s})W(\boldsymbol{q}-\boldsymbol{r})W(\boldsymbol{p}+\boldsymbol{s})W(\boldsymbol{p}) + W(\boldsymbol{r}+\boldsymbol{p}+\boldsymbol{s})W(\boldsymbol{r}-\boldsymbol{p})W(\boldsymbol{q}+\boldsymbol{s})W(\boldsymbol{q}) = 0.$$

We identify the rank of W as the rank of the elliptic net.

Pick $A = \mathbb{Z}^2$. For $\alpha = \alpha_1 + \alpha_2\omega, \beta = \beta_1 + \beta_2\omega, \gamma = \gamma_1 + \gamma_2\omega \in \mathbb{Z}[\omega]$, take $\boldsymbol{p} = (\beta_1, \beta_2), \boldsymbol{q} = (\alpha_1, \alpha_2), \boldsymbol{r} = (\gamma_1, \gamma_2)$ and $\boldsymbol{s} = (0, 0)$ in the definition, then we have

$$h_{\alpha+\beta}h_{\alpha-\beta}h_\gamma^2 = h_{\alpha+\gamma}h_{\alpha-\gamma}h_\beta^2 - h_{\beta+\gamma}h_{\beta-\gamma}h_\alpha^2.$$

CM EDS(A) – Elliptic net and elliptic curves

Definition (Net polynomial and elliptic denominator net)

For an arbitrary field K, consider the polynomial ring

$$R_r = K[x_i, y_i]_{1\leq i\leq r}[(x_i - x_j)^{-1}]/\langle f(x_i, y_i)\rangle_{1\leq i\leq r},$$

where $f(x, y, \boldsymbol{a}) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6, a_i \in K$. Let $\boldsymbol{P} = (P_1, ..., P_r) \in E(K)^r$ and $\boldsymbol{v} = (v_1, ..., v_r) \in \mathbb{Z}^r$. Then there exists rational functions $\Psi_{\boldsymbol{v}}(\boldsymbol{P})$, $\Phi_{\boldsymbol{v}}(\boldsymbol{P})$, $\bar{\Omega}_{\boldsymbol{v}}(\boldsymbol{P}) \in R_r$ such that

$$\boldsymbol{v}\cdot\boldsymbol{P} = v1P_1 + ... + v_rP_r = \left(\frac{\Phi_{\boldsymbol{v}}(\boldsymbol{P})}{\Psi^2_{\boldsymbol{v}}(\boldsymbol{P})}, \frac{\bar{\Omega}_{\boldsymbol{v}}(\boldsymbol{P})}{\Psi^3_{\boldsymbol{v}}(\boldsymbol{P})}\right). \tag{1}$$

The polynomial $\Psi_{\boldsymbol{v}}$ is defined to be the $\boldsymbol{v}$*-th net polynomial*, which is an elliptic net.

In our case, $r = 2, \boldsymbol{P} = (P, \omega P) \in E(K)^2$ and $\boldsymbol{v}$ is the vector notation of our element in $\mathbb{Z}[\omega]$.

Properties of elliptic nets

Question: if we express an element of $\mathrm{End}(E)$, $\alpha = a + b\omega$ in a vector/coordinate form (a, b), can we define a sequence of polynomials $\psi_\alpha(P)$, indexed by $\mathcal{O}_F$, as

$$\psi_{a+b\omega}(P) := \Psi_{\boldsymbol{v}}(\boldsymbol{P})?$$

The net polynomials satisfy the following properties:

a. All the terms in the net polynomial are defined by the following initial conditions:
   - $\Psi_{\boldsymbol{e_i}} = 1$; $\Psi_{\boldsymbol{2e_i}} = 2y_i + a_1 x_i + a_3 = \psi_2(P_i)$;
   - $\Psi_{\boldsymbol{e_i}+\boldsymbol{e_j}} = 1$, $i \neq j$;
   - $\Psi_{\boldsymbol{2e_i}+\boldsymbol{e_j}} = 2x_i + x_j - \left(\frac{y_j - y_i}{x_j - x_i}\right)^2 - a_1\left(\frac{y_j - y_i}{x_j - x_i}\right) + a_2$, $i \neq j$.

b. Recall $x(\boldsymbol{v} \cdot \boldsymbol{P}) = \frac{\Phi_{\boldsymbol{v}}(\boldsymbol{P})}{\Psi^2_{\boldsymbol{v}}(\boldsymbol{P})}$; for $1 \leq i \leq r$ we have

$$\Phi_{\boldsymbol{v}}(\boldsymbol{P}) = \Psi^2_{\boldsymbol{v}}(\boldsymbol{P}) x(P_i) - \Psi_{\boldsymbol{v}+\boldsymbol{e_i}}(\boldsymbol{P}) \Psi_{\boldsymbol{v}-\boldsymbol{e_i}}(\boldsymbol{P}) \qquad (2)$$

Issues with elliptic net

- 'Net polynomial' $\Psi_{\boldsymbol{v}}$ are elements of the polynomial ring $R_r = K[x_i, y_i]_{1\le i\le r}[(x_i - x_j)^{-1}]/\langle f(x_i, y_i)\rangle_{1\le i\le r}$, which makes them *not necessarily integral*.
  $\Psi_{\boldsymbol{2e_i+e_j}} = 2x_i + x_j - \left(\frac{y_j-y_i}{x_j-x_i}\right)^2 - a_1\left(\frac{y_j-y_i}{x_j-x_i}\right) + a_2$, $i \neq j$.

Example: elliptic curve $E/\mathbb{Q}(i)$: $y^2 = x^3 - 2x$ with complex multiplication by $\mathbb{Z}[i]$; elliptic net associated to E and the point $P = (-1, 1)$ and $iP = (1, i)$.
$[2]P + [2]iP = \left(-\frac{7^2}{3^2(1+i)^6}, \frac{(8-7i)(8+7i)}{3^3(1+i)^9}\right); \Psi_{(2,2)}(\boldsymbol{P}) = -\frac{3}{1-i}$.

Issues with elliptic net

- 'Net polynomial' $\Psi_{\boldsymbol{v}}$ are elements of the polynomial ring $R_r = K[x_i, y_i]_{1\leq i\leq r}[(x_i - x_j)^{-1}]/\langle f(x_i, y_i)\rangle_{1\leq i\leq r}$, which makes them *not necessarily integral*.

  $\Psi_{\boldsymbol{2e_i+e_j}} = 2x_i + x_j - \left(\frac{y_j - y_i}{x_j - x_i}\right)^2 - a_1\left(\frac{y_j - y_i}{x_j - x_i}\right) + a_2,\ i \neq j.$

Example: elliptic curve $E/\mathbb{Q}(i)$: $y^2 = x^3 - 2x$ with complex multiplication by $\mathbb{Z}[i]$; elliptic net associated to E and the point $P = (-1, 1)$ and $iP = (1, i)$. $[2]P + [2]iP = \left(-\frac{7^2}{3^2(1+i)^6}, \frac{(8-7i)(8+7i)}{3^3(1+i)^9}\right); \Psi_{(2,2)}(\boldsymbol{P}) = -\frac{3}{1-i}$.

- It does not have as many useful properties as the the ordinary division polynomials: for $\psi_n \in \mathbb{Z}[x, y, \boldsymbol{a}]/\langle f(x, y, \boldsymbol{a})\rangle$,
  - $\psi_n^2(x)$ only depends on x for every $n \in \mathbb{Z}$.
  - The polynomial ψ_n^2 has degree $n^2 - 1$ and leading coefficient n^2.
  - $\psi_{mn}(P) = \psi_n(P)^{m^2}\psi_m(nP)$.

References

1. Akbary, Amir; Bleaney, Jeff; Yazdani, Soroosh (2016). On symmetries of elliptic nets and valuations of net polynomials. J. Number Theory 158, 185–216. View online
2. Stange, Katherine E. (2011). Elliptic nets and elliptic curves. Algebra Number Theory 5, no. 2, 197–229. View online
3. Streng, Marco. (2008). Divisibility sequences for elliptic curves with complex multiplication. Algebra & Number Theory 2, no. 2, 183–208. View online
4. Silverman, J. H. (1994). Advanced topics in the arithmetic of elliptic curves. Springer-Verlag. View online.
5. Verzobio, Matteo. (2021). A recurrence relation for elliptic divisibility sequences. View online.