Common valuations of division polynomials at points on elliptic curves

Edison Au-Yeung
University of Warwick

Junior Seminar, Chalmers University of Technology

21 October 2025

Small recap

- Let E/K be an elliptic curve defined over a number field K with the following Weierstrass equation:

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

- $E(K)$ is the set of points $(x, y) \in K^2$ that lie on E, together with a point at infinity O. They form a commutative group in a natural way.
- O is the identity in this group: $P +_E O = P$ for all $P \in E(K)$.
  We let $[n] : E \to E$ be multiplication by n in this group.

Small recap

- Let E/K be an elliptic curve defined over a number field K with the following Weierstrass equation:

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

- $E(K)$ is the set of points $(x, y) \in K^2$ that lie on E, together with a point at infinity O. They form a commutative group in a natural way.
- O is the identity in this group: $P +_E O = P$ for all $P \in E(K)$. We let $[n] : E \to E$ be multiplication by n in this group.
- There are polynomials $\phi_n, \psi_n, \omega_n \in \mathbb{Z}[x, y, \boldsymbol{a}]$ for $n \in \mathbb{N}$ with

$$[n]P = [n](x, y) = \left(\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3}\right),$$

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

- The polynomial ψ_n is usually referred as the n-th division polynomial (associated to E).

n-th division polynomials

Properties:

1. Recurrence relation: the n-th division polynomials satisfy the recurrence relation

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

n-th division polynomials

Properties:

1. Recurrence relation: the n-th division polynomials satisfy the recurrence relation

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

2. Chain rule: $\psi_{nm}(P) = \psi_n(mP)\psi_m^{n^2}(P)$.

n-th division polynomials

Properties:

1. Recurrence relation: the n-th division polynomials satisfy the recurrence relation

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

2. Chain rule: $\psi_{nm}(P) = \psi_n(mP)\psi_m^{n^2}(P)$.
3. Relation to x: the n-th division polynomials satisfy

$$\frac{\psi_{n+m}\psi_{n-m}}{\psi_n^2\psi_m^2} = x(nP) - x(mP).$$

n-th division polynomials

Motivation:

- It is used in Schoof's algorithm to count the number of points in $E(\mathbb{F}_q)$, which is a polynomial time
- A faster way to compute $x([n]P)$.

n-th division polynomials

Motivation:

- It is used in Schoof's algorithm to count the number of points in $E(\mathbb{F}_q)$, which is a polynomial time
- A faster way to compute $x([n]P)$.
- A tool to study problems related to integral points on elliptic curves (e.g. what is a bound for the size of n such that $[n]P$ is integral?)

Recall that the n-th division polynomial is directly related to the x–coordinate of a point: for $P \in E(K)$ (K has class number 1),

$$x\left([n]P\right) = \frac{\phi_n}{\psi_n^2} = \frac{A_n}{B_n^2}, \ \gcd(A_n, B_n^2) = 1.$$

n-th division polynomials

Motivation:

- It is used in Schoof's algorithm to count the number of points in $E(\mathbb{F}_q)$, which is a polynomial time
- A faster way to compute $x([n]P)$.
- A tool to study problems related to integral points on elliptic curves (e.g. what is a bound for the size of n such that $[n]P$ is integral?)

  Recall that the n-th division polynomial is directly related to the x–coordinate of a point: for $P \in E(K)$ (K has class number 1),

$$x\left([n]P\right) = \frac{\phi_n}{\psi_n^2} = \frac{A_n}{B_n^2}, \ \gcd(A_n, B_n^2) = 1.$$

- Denote $g_{n,\nu}(P) = \min\left(\nu\left(\psi_n^2(P)\right), \nu\left(\phi_n(P)\right)\right)$, ν a valuation associated to a prime.

Common valuation

Cheon and Hahn (1998): described the sequence of valuation recursively
Let E be an elliptic curve over any field K, define the subset

$$E_0(K) = \{P \in E(K) \mid P \mod \mathfrak{p} \text{ is non-singular in } E(\mathbb{F}_{\mathfrak{p}})\}$$

where $\mathfrak{p}$ is the prime with the finite valuation ν, $\mathbb{F}_{\mathfrak{p}}$ denotes the field $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.

Common valuation

Cheon and Hahn (1998): described the sequence of valuation recursively
Let E be an elliptic curve over any field K, define the subset

$$E_0(K) = \{P \in E(K) \mid P \mod \mathfrak{p} \text{ is non-singular in } E(\mathbb{F}_\mathfrak{p})\}$$

where $\mathfrak{p}$ is the prime with the finite valuation ν, $\mathbb{F}_\mathfrak{p}$ denotes the field $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.

1. It is known that $E(K)/E_0(K)$ is a finite group.
2. $r(\mathfrak{p}, P) :=$ order of P in $E(K)/E_0(K)$, so $r(\mathfrak{p}, P)$ is the smallest positive integer such that $[r]P$ is non-singular $\mod \mathfrak{p}$.

Common valuation–explicit formula

Theorem (Cheon and Hahn, 1998)

Let E be an elliptic curve defined by a Weierstrass equation with coefficients in $\mathcal{O}_K$*. Let* P *be a non-torsion point of* $E(K)$ *and assume* $\nu(x(P)) \geq 0$*. Let* $r = r(\mathfrak{p}, P) > 1$ *and* $n > 0$*, then* $g_{n,\nu}(P)$ *is asymptotically equal to a quadratic function. More precisely,*

$$g_{n,\nu}(P) = \begin{cases} \mu t^2, & \text{if } n = tr, \\ 4\mu t^2 \pm 2\left(2\nu\left(\dfrac{\psi_k(P)}{\psi_{r-k}(P)}\right) + \mu\right) t & \text{if } n = 2tr \pm k \text{ with } 1 \leq k < r, \\ \quad + 2\nu(\psi_k(P)), & \end{cases} \tag{1}$$

where $\mu = g_{r,\nu}(P)$*.*

Recall that $g_{n,\nu}(P) = \min\left(\nu\left(\psi_n^2(P)\right), \nu\left(\phi_n(P)\right)\right)$.

Common valuation–explicit formula

Proof strategy:

- Comparing the valuations of the terms in the recurrence relation

$$\psi_{mr+k}\psi_{mr-k} = \psi_{mr+1}\psi_{mr-1}\psi_k^2 - \psi_{k+1}\psi_{k-1}\psi_{mr}^2 \quad (1 \leq k \leq r)$$

  and prove the valuation for $\psi_{2tr\pm k}$.

Common valuation–explicit formula

Proof strategy:

- Comparing the valuations of the terms in the recurrence relation

$$\psi_{mr+k}\psi_{mr-k} = \psi_{mr+1}\psi_{mr-1}\psi_k^2 - \psi_{k+1}\psi_{k-1}\psi_{mr}^2 \quad (1 \leq k \leq r)$$

  and prove the valuation for $\psi_{2tr\pm k}$.

- Heavy use of properties of division polynomials, especially for the case of ψ_{tr}:

$$\begin{aligned}\phi_n(P) &= x(P)\psi_n^2(P) - \psi_{n+1}(P)\psi_{n-1}(P);\\ \psi_{mr}(P) &= \psi_r(P)^{m^2}\psi_m(rP);\\ \phi_{mr}(P) &= \psi_r(P)^{2m^2}\phi_m(rP),\end{aligned}$$

Common valuation–explicit formula

Proof strategy:

- Comparing the valuations of the terms in the recurrence relation

$$\psi_{mr+k}\psi_{mr-k} = \psi_{mr+1}\psi_{mr-1}\psi_k^2 - \psi_{k+1}\psi_{k-1}\psi_{mr}^2 \quad (1 \leq k \leq r)$$

  and prove the valuation for $\psi_{2tr\pm k}$.
- Heavy use of properties of division polynomials, especially for the case of ψ_{tr}:

$$\phi_n(P) = x(P)\psi_n^2(P) - \psi_{n+1}(P)\psi_{n-1}(P);$$
$$\psi_{mr}(P) = \psi_r(P)^{m^2}\psi_m(rP);$$
$$\phi_{mr}(P) = \psi_r(P)^{2m^2}\phi_m(rP),$$

- By substituting $\psi_2^2(P) = (2y + a_1x + a_3)^2$ with $4x^3 + b_2x^2 + b_4x + b_6$, we cna always reduce the dependence on y and therefore $\psi_n^2, \phi_n(x) \in \mathbb{Z}[\boldsymbol{a}][x]$.
- We can also use properties of polynomials, such as the degree of the polynomial

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 $\mathbb{Z}[\omega] = \{a + b\omega \colon a, b \in \mathbb{Z}\}$, 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 $E(K)$.

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 $\mathbb{Z}[\omega] = \{a + b\omega \colon a, b \in \mathbb{Z}\}$, 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 $E(K)$.
- Do we also have a rational function on E/K that accounts for these extra CM points while still satisfying the three properties:
  1. Recurrence relation: the n-th division polynomials satisfy the recurrence relation
  $$\psi_{m+n}\psi_{m-n}\psi_r^2 = \psi_{m+r}\psi_{m-r}\psi_n^2 - \psi_{n+r}\psi_{n-r}\psi_m^2 \quad (r < n < m).$$
  2. Chain rule: $\psi_{nm}(P) = \psi_n(mP)\psi_m^{n^2}(P)$.
  3. Relation to x: the n-th division polynomials satisfy
  $$\frac{\psi_{n+m}\psi_{n-m}}{\psi_n^2\psi_m^2} = x(nP) - x(mP).$$

Net polynomials

Definition (Net polynomial – rank 2; Stange, 2007)

For an arbitrary field K, consider the polynomial ring

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

where $f(x_i, y_i) = y_i^2 + a_1x_iy_i + a_3y_i - x_i^3 - a_2x_i^2 - a_4x_i - a_6, a_i \in K$. Let $\boldsymbol{P} = (P_1, P_2) \in E(K)^2$ and $\boldsymbol{v} = (v_1, v_2) \in \mathbb{Z}^r$. 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

$$\boldsymbol{v} \cdot \boldsymbol{P} = [v_1]P_1 + [v_2]P_2 = \left(\frac{\Phi_{\boldsymbol{v}}(\boldsymbol{P})}{\Psi_{\boldsymbol{v}}^2(\boldsymbol{P})}, \frac{\bar{\Omega}_{\boldsymbol{v}}(\boldsymbol{P})}{\Psi_{\boldsymbol{v}}^3(\boldsymbol{P})}\right). \tag{2}$$

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

Net polynomials

Definition (Net polynomial – rank 2; Stange, 2007)

For an arbitrary field K, consider the polynomial ring

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

where $f(x_i, y_i) = y_i^2 + a_1 x_i y_i + a_3 y_i - x_i^3 - a_2 x_i^2 - a_4 x_i - a_6, a_i \in K$. Let $\boldsymbol{P} = (P_1, P_2) \in E(K)^2$ and $\boldsymbol{v} = (v_1, v_2) \in \mathbb{Z}^r$. 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

$$\boldsymbol{v} \cdot \boldsymbol{P} = [v_1]P_1 + [v_2]P_2 = \left(\frac{\Phi_{\boldsymbol{v}}(\boldsymbol{P})}{\Psi_{\boldsymbol{v}}^2(\boldsymbol{P})}, \frac{\bar{\Omega}_{\boldsymbol{v}}(\boldsymbol{P})}{\Psi_{\boldsymbol{v}}^3(\boldsymbol{P})} \right). \tag{2}$$

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

In our case, we fix a point $P \in E(K)$ and pick $P_1 = P, P_2 = [\omega]P$. Then we have

$$\boldsymbol{v} \cdot \boldsymbol{P} = v_1 P_1 + v_2[\omega]P = [v_1 + v_2\omega]P, v_1 + v_2\omega \in \mathbb{Z}[\omega].$$

Properties of of net polynomials – recurrence relation

Stange has shown that the net polynomials do satisfy the following recurrence relation:

$$\Psi_{\boldsymbol{p}+\boldsymbol{q}}\Psi_{\boldsymbol{p}-\boldsymbol{q}}\Psi_{\boldsymbol{r}}^2 = \Psi_{\boldsymbol{p}+\boldsymbol{r}}\Psi_{\boldsymbol{p}-\boldsymbol{r}}\Psi_{\boldsymbol{q}}^2 - \Psi_{\boldsymbol{q}+\boldsymbol{r}}\Psi_{\boldsymbol{q}-\boldsymbol{r}}\Psi_{\boldsymbol{p}}^2.$$

Compare with the rank 1 case:

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

Properties of of net polynomials – recurrence relation

Stange has shown that the net polynomials do satisfy the following recurrence relation:

$$\Psi_{\boldsymbol{p}+\boldsymbol{q}}\Psi_{\boldsymbol{p}-\boldsymbol{q}}\Psi_{\boldsymbol{r}}^2 = \Psi_{\boldsymbol{p}+\boldsymbol{r}}\Psi_{\boldsymbol{p}-\boldsymbol{r}}\Psi_{\boldsymbol{q}}^2 - \Psi_{\boldsymbol{q}+\boldsymbol{r}}\Psi_{\boldsymbol{q}-\boldsymbol{r}}\Psi_{\boldsymbol{p}}^2.$$

Compare with the rank 1 case:

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

We identify $\mathbb{Z}[\omega]$ as a rank 2 $\mathbb{Z}$-module: for $\alpha = \alpha_1 + \alpha_2\omega, \beta = \beta_1 + \beta_2\omega, \gamma = \gamma_1 + \gamma_2\omega \in \mathbb{Z}[\omega]$, we take $\boldsymbol{p} = (\beta_1, \beta_2), \boldsymbol{q} = (\alpha_1, \alpha_2)$ and $\boldsymbol{r} = (\gamma_1, \gamma_2)$.

Properties of of net polynomials – recurrence relation

Let $\{\boldsymbol{e_1}, \boldsymbol{e_2}\}$ be the standard basis of $\mathbb{Z}^2$. All the terms in the net polynomial are defined by the following initial conditions:

- $\Psi_{\boldsymbol{e_1}} = \Psi_{\boldsymbol{e_2}} = \Psi_{\boldsymbol{e_1+e_2}} = 1$;
- $\Psi_{\boldsymbol{2e_1}} = 2y_1 + a_1x_1 + a_3 = \psi_2(P_1)$;
- $\Psi_{\boldsymbol{2e_2}} = 2y_2 + a_1x_2 + a_3 = \psi_2(P_2)$;
- $\Psi_{\boldsymbol{2e_1+e_2}} = 2x_1 + x_2 - \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - a_1\left(\frac{y_2-y_1}{x_2-x_1}\right) + a_2$;
- Similar for $\Psi_{\boldsymbol{2e_2+e_1}}$;

Properties of of net polynomials – recurrence relation

Let $\{\boldsymbol{e_1}, \boldsymbol{e_2}\}$ be the standard basis of $\mathbb{Z}^2$. All the terms in the net polynomial are defined by the following initial conditions:

- $\Psi_{\boldsymbol{e_1}} = \Psi_{\boldsymbol{e_2}} = \Psi_{\boldsymbol{e_1}+\boldsymbol{e_2}} = 1$;
- $\Psi_{\boldsymbol{2e_1}} = 2y_1 + a_1x_1 + a_3 = \psi_2(P_1)$;
- $\Psi_{\boldsymbol{2e_2}} = 2y_2 + a_1x_2 + a_3 = \psi_2(P_2)$;
- $\Psi_{\boldsymbol{2e_1}+\boldsymbol{e_2}} = 2x_1 + x_2 - \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - a_1\left(\frac{y_2-y_1}{x_2-x_1}\right) + a_2$;
- Similar for $\Psi_{\boldsymbol{2e_2}+\boldsymbol{e_1}}$;
- The factor $(x_i - x_j)^{-1}$ comes from the elliptic curve point addition formula: let E be an elliptic curve given by the Weierstrass equation

  $$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

  If $P_1 \neq \pm P_2$, then

  $$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2$$

Properties of net polynomials – relation to x

Recall $x(\boldsymbol{v}\cdot\boldsymbol{P}) = \frac{\Phi_{\boldsymbol{v}}(\boldsymbol{P})}{\Psi_{\boldsymbol{v}}^2(\boldsymbol{P})}$

1. For any $\boldsymbol{v},\boldsymbol{u}\in\mathbb{Z}^r$,

$$x\left(\boldsymbol{v}\cdot\boldsymbol{P}\right) - x\left(\boldsymbol{u}\cdot\boldsymbol{P}\right) = -\frac{\Psi_{\boldsymbol{v}+\boldsymbol{u}}\Psi_{\boldsymbol{v}-\boldsymbol{u}}}{\Psi_{\boldsymbol{v}}^2\Psi_{\boldsymbol{u}}^2},$$

   where $x(\boldsymbol{v}\cdot\boldsymbol{P})$ represents the x-coordinate of the point $\boldsymbol{v}\cdot\boldsymbol{P}$.

2. For $i=1,2$,

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

Compare with rank 1 case: for $x([n]P) = \frac{\phi_n(P)}{\psi_n(P)^2}$,

1. $x(nP) - x(mP) = \frac{\psi_{n+m}\psi_{n-m}}{\psi_n^2\psi_m^2}$;
2. $\phi_n(P) = x(P)\psi_n^2(P) - \psi_{n+1}(P)\psi_{n-1}(P)$.

Properties of net polynomials – chain rule

In the rank 1 case, we have

$$\psi_{mr}(P) = \psi_r(P)^{m^2}\psi_m(rP);$$
$$\phi_{mr}(P) = \psi_r(P)^{2m^2}\phi_m(rP).$$

In a more general rank 2 setting, instead of chain rule, Stange proved that we can perform 'change of basis'.

Properties of net polynomials – chain rule

In the rank 1 case, we have

$$\psi_{mr}(P) = \psi_r(P)^{m^2}\psi_m(rP);$$
$$\phi_{mr}(P) = \psi_r(P)^{2m^2}\phi_m(rP).$$

In a more general rank 2 setting, instead of chain rule, Stange proved that we can perform ‘change of basis’. For our specific case of CM, this is a bit simpler and still can be understood as chain rule. Let $\alpha = a + b\omega$, $\beta = c + d\omega \in \mathbb{Z}[\omega]$, then the chain rule is

$$\Psi_{\boldsymbol{\alpha\beta}}(\boldsymbol{P}) = \Psi_{\boldsymbol{\beta}}(\alpha\boldsymbol{P})\Psi_{\boldsymbol{\alpha}}(\boldsymbol{P})^{c^2-cd}\Psi_{\boldsymbol{\alpha\omega}}(\boldsymbol{P})^{d^2-cd}\Psi_{\boldsymbol{\alpha(1+\omega)}}(\boldsymbol{P})^{cd}$$

(Recall the initial conditions of net polynomials: we require $\Psi_{\boldsymbol{e_1}} = \Psi_{\boldsymbol{e_2}} = \Psi_{\boldsymbol{e_1+e_2}} = 1$.)

Notion of non-singular reduction

Cheon and Hahn: described the sequence of valuation recursively
Let E be an elliptic curve over any field K, define the set

$$E_0(K) = \{P \in E(K) \mid P \mod \mathfrak{p} \text{ is non-singular in } E(\mathbb{F}_\mathfrak{p})\}$$

where $\mathfrak{p}$ is the prime with the finite valuation ν, $\mathbb{F}_\mathfrak{p}$ denotes the field $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. It is known that $E(K)/E_0(K)$ is a finite group.

Proposition

$E_0(K)$ is a $\mathbb{Z}[\omega]$–submodule of $E(K)$.

Example: $E\colon y^2 = x^3 + x^2 - 3x + 1$ over the field $\mathbb{Q}(\sqrt{-2})$, CM by $\mathbb{Z}[\sqrt{-2}]$.

- $\Delta = 512 = \left(\sqrt{-2}\right)^{20}$
- The point $P = (-1, 2)$ is singular $\mod \sqrt{-2}$, but not $[2]P = \left(\frac{5}{4}, \frac{7}{8}\right)$.
- The point $\left[\sqrt{-2}\right] P = \left(\frac{1}{2}, \frac{1}{2\sqrt{-2}}\right)$ is not singular either.

Notion of non-singular reduction

Cheon and Hahn: described the sequence of valuation recursively
Let E be an elliptic curve over any field K, define the set

$$E_0(K) = \{P \in E(K) \mid P \mod \mathfrak{p} \text{ is non-singular in } E(\mathbb{F}_{\mathfrak{p}})\}$$

where $\mathfrak{p}$ is the prime with the finite valuation ν, $\mathbb{F}_{\mathfrak{p}}$ denotes the field $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. It is known that $E(K)/E_0(K)$ is a finite group.

Proposition

$E_0(K)$ is a $\mathbb{Z}[\omega]$–submodule of $E(K)$.

Assume K has class number 1, then we define $r(\mathfrak{p}, P) :=$ annihilator of P in $E(K)/E_0(K)$.

Local height function

In simple terms: a local function that sums up to the canonical height function $\hat{h}(\cdot)$, hence measuring the arithmetic complexity of a point $P \in E(K)$.

Local height function

In simple terms: a local function that sums up to the canonical height function $\hat{h}(\cdot)$, hence measuring the arithmetic complexity of a point $P \in E(K)$.

Proposition

Let K be a number field, E/K be an elliptic curve. Then for all $P, Q \in E(K)$ with $P, Q, P \pm Q \neq O$, the Néron height function $\lambda \colon E(K) \setminus \{O\} \to \mathbb{R}$ satisfies the *quasi-parallelogram law*

$$\lambda(P+Q) + \lambda(P-Q) = 2\lambda(P) + 2\lambda(Q) + \nu(x(P) - x(Q)) - \frac{1}{6}\nu(\Delta).$$

Corollary

For any non m-torsion point P, with $m \in \mathbb{Z}$,

$$\lambda([m]P) = m^2\lambda(P) + \nu(\psi_m(P)) - \frac{1}{12}(m^2-1)\nu(\Delta).$$

Local height function

Proposition

Let Δ be the discriminant of this equation. Then the Néron local height function $\lambda : E(K) \setminus \{O\} \to \mathbb{R}$ is given by the formula

$$\begin{aligned}\lambda(nP) &= \frac{1}{2}\max\{\nu(x(nP)^{-1}), 0\} + \frac{1}{12}\nu(\Delta) \\ &= \frac{1}{2}\max\{2\nu(\psi_n(P)) - \nu(\phi_n(P)), 0\} + \frac{1}{12}\nu(\Delta), \quad \text{for all } P \in E_0(K).\end{aligned}$$

Local height function

Proposition

Let Δ be the discriminant of this equation. Then the Néron local height function $\lambda : E(K) \setminus \{O\} \to \mathbb{R}$ is given by the formula

$$\begin{aligned}\lambda(nP) &= \frac{1}{2}\max\{\nu(x(nP)^{-1}), 0\} + \frac{1}{12}\nu(\Delta)\\ &= \frac{1}{2}\max\{2\nu(\psi_n(P)) - \nu(\phi_n(P)), 0\} + \frac{1}{12}\nu(\Delta), \quad \text{for all } P \in E_0(K).\end{aligned}$$

Hence, results for the local height function = results for the division polynomials.

Local height function and elliptic net

Proposition [Au-Yeung, 2025+]

Let E be an elliptic curve defined over a number field L, $\boldsymbol{v} = (a, b) \in \mathbb{Z}^2$. Let $\boldsymbol{P} = (P, Q) \in E(K)^2$. If ν is the finite place associated to the prime $\mathfrak{p}$, then the normalised Néron local height function ($\tilde{\lambda}(P) := \lambda(P) - \frac{1}{12}\nu(\Delta)$) satisfies

$$\tilde{\lambda}(\boldsymbol{v} \cdot \boldsymbol{P}) = a^2\tilde{\lambda}(P) + b^2\tilde{\lambda}(Q) + ab\left(\tilde{\lambda}(P+Q) - \tilde{\lambda}(P) - \tilde{\lambda}(Q)\right) + \nu\left(\Psi_{(a,b)}(\boldsymbol{P})\right),$$

where $\Psi_{(a,b)}$ is the elliptic net polynomial evaluated at $\boldsymbol{v} = (a, b)$.

Proof strategy:

- Prove by induction and using the fact that $\tilde{\lambda}(P) = \tilde{\lambda}(-P)$.
- Use the quasi-parallelogram law in the inductive step.
- Relation to x: for any $\boldsymbol{v}, \boldsymbol{u} \in \mathbb{Z}^2$,

$$x(\boldsymbol{v} \cdot \boldsymbol{P}) - x(\boldsymbol{u} \cdot \boldsymbol{P}) = -\frac{\Psi_{\boldsymbol{v}+\boldsymbol{u}}\Psi_{\boldsymbol{v}-\boldsymbol{u}}}{\Psi_{\boldsymbol{v}}^2\Psi_{\boldsymbol{u}}^2},$$

Local height function and elliptic net

Corollary [Au-Yeung, 2025+]

Let E/K be an elliptic curve defined over a number field K with complex multiplication by an order $\mathbb{Z}[\omega]$ in a quadratic imaginary field $F \subseteq K$. For any $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ and any non-torsion points $\boldsymbol{P} = (P, \omega P) \in E(L)^2$, if ν is the finite place associated to the prime $\mathfrak{p}$, we have

$$\tilde{\lambda}([\alpha]P) = a^2\tilde{\lambda}(P) + b^2\tilde{\lambda}(\omega P) + ab\left(\tilde{\lambda}([1+\omega]P) - \tilde{\lambda}(P) - \tilde{\lambda}(\omega P)\right) + \nu(\Psi_{(a,b)}(\boldsymbol{P})),$$

where $\Psi_{(a,b)}$ is the elliptic net polynomial evaluated at $\boldsymbol{v} = (a, b)$, the vector notation for elements in $\mathbb{Z}[\omega]$.

Compare with the original formula:

$$\tilde{\lambda}([m]P) = m^2\tilde{\lambda}(P) + \nu(\psi_m(P)).$$

Finiteness of local height values

Proposition

Let E/K be an elliptic curve with complex multiplication by $\mathbb{Z}[\omega]$, which is assumed to be a PID. For a non-torsion point P in $E(K) \setminus E_0(K)$ with $\operatorname{ann}(P)$ in the $\mathbb{Z}[\omega]$-module $E(K)/E_0(K)$, let ν be a finite place in K such that $P \mod \nu$ has additive singularity. Let $r \in \operatorname{ann}(P)$. Then for any $\alpha = a + b\omega \notin \operatorname{ann}(P)$, we have

$$\lambda\left([\alpha]P\right) = \lambda\left([\overline{\alpha}]P\right), \overline{\alpha} \equiv \alpha \mod r.$$

Example: $E\colon y^2 = x^3 + x^2 - 3x + 1$ over the field $\mathbb{Q}(\sqrt{-2})$, CM by $\mathbb{Z}[\sqrt{-2}]$.

- $\Delta = 512 = \left(\sqrt{-2}\right)^{20}$
- The point $P = (-1, 2)$ is singular $\mod \sqrt{-2}$, but not $\left[\sqrt{-2}\right] P = \left(\frac{1}{2}, \frac{1}{2\sqrt{-2}}\right)$
- We have $\lambda(P) = \lambda(P + [n\sqrt{-2}]P) = 2\log(2)$ for all $n \in \mathbb{Z}$
- $\lambda([\sqrt{-2}]P) = 5\log(2)$, $\lambda([4\sqrt{-2}]P) = 13\log(2)$

Finiteness of local height values

Proposition

Let E/K be an elliptic curve with complex multiplication by $\mathbb{Z}[\omega]$, which is assumed to be a PID. For a non-torsion point P in $E(K) \setminus E_0(K)$ with $\operatorname{ann}(P)$ in the $\mathbb{Z}[\omega]$-module $E(K)/E_0(K)$, let ν be a finite place in K such that $P \mod \nu$ has additive singularity. Let $r \in \operatorname{ann}(P)$. Then for any $\alpha = a + b\omega \notin \operatorname{ann}(P)$, we have

$$\lambda\left([\alpha]P\right) = \lambda\left([\overline{\alpha}]P\right), \overline{\alpha} \equiv \alpha \mod r.$$

Proof strategy:

- Semi-stable reduction theorem: there exists a field extension such that the elliptic curve has good reduction everywhere.
- Consider an extension of the valuation and by analysing change of coordinate, we conclude with the local height function being invariant under field extension.

Explicit formula for CM net polynomials

Our main results require the following assumptions:

- A number field K with class number 1 (so $\mathcal{O}_K$ is a PID)
- E/K an elliptic curve defined by a Weierstrass equation with coefficients in $\mathcal{O}_K$
- E/K has complex multiplication by an order $\mathbb{Z}[\omega]$ in a quadratic imaginary field F
- $\mathbb{Z}[\omega]$ is a PID and $F \subseteq K$
- We consider a non-torsion point $P \in E(K)$ with bad reduction modulo a prime

$$x\left([\alpha]P\right) = x\left([a+b\omega]P\right) = \frac{\Phi_{\boldsymbol{\alpha}}(\boldsymbol{P})}{\Psi^2_{\boldsymbol{\alpha}}(\boldsymbol{P})} = \frac{A_\alpha}{B_\alpha^2}, A_\alpha \text{ and } B_\alpha^2 \text{ coprime.}$$

Explicit formula for CM net polynomials

Theorem (Au-Yeung, 2025+)

With the above assumptions, let P *be a non-torsion point of* $E(K)$ *that is singular modulo* ν *(so* $\nu(x(P)) \geq 0$*). Let* (r) *be the annihilator of* P *in the* $\mathbb{Z}[\omega]$*–module* $E(K)/E_0(K)$, $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, *then*

$$g_{z,\nu}(P) = \begin{cases} (a^2-ab)\mu + (b^2-ab)\mu_\omega + (ab)\mu_{1+\omega}, & \text{if } z = \alpha r \in (r). \\ 2\nu\left(\Psi_{\boldsymbol{\beta}}\right) \pm 2a\left[\nu\left(\frac{\Psi_{\boldsymbol{\beta}}}{\Psi_{\boldsymbol{r-\beta}}}\right)+\frac{\mu}{2}\right] \pm 2b\left[\nu\left(\frac{\Psi_{\boldsymbol{\beta}}}{\Psi_{\boldsymbol{r\omega-\beta}}}\right)+\frac{\mu_\omega}{2}\right] & \\ \quad +(a^2-ab)\mu+(b^2-ab)\mu_\omega+(ab)\mu_{1+\omega}, & \text{if } z=\alpha r\pm\beta\notin(r). \end{cases} \tag{3}$$

where $\mu = g_{r,\nu}(P), \mu_\omega = g_{r\omega,\nu}(P), \mu_{1+\omega} = g_{r(1+\omega),\nu}(P)$.

Explicit formula for CM net polynomials

Case I: $z = \alpha r \in (r), \alpha = a + b\omega$

$$g_{z,\nu}(P) = (a^2 - ab)\mu + (b^2 - ab)\mu_\omega + (ab)\mu_{1+\omega}$$

- Use of chain rule:

$$\Psi_{\boldsymbol{\alpha r}}(\boldsymbol{P}) = \Psi_{\boldsymbol{\alpha}}(r\boldsymbol{P})\Psi_{\boldsymbol{r}}(\boldsymbol{P})^{a^2-ab}\Psi_{\boldsymbol{r\omega}}(\boldsymbol{P})^{b^2-ab}\Psi_{\boldsymbol{r(1+\omega)}}(\boldsymbol{P})^{ab}.$$

Explicit formula for CM net polynomials

Case I: $z = \alpha r \in (r), \alpha = a + b\omega$

$$g_{z,\nu}(P) = (a^2 - ab)\mu + (b^2 - ab)\mu_\omega + (ab)\mu_{1+\omega}$$

- Use of chain rule:

$$\Psi_{\boldsymbol{\alpha r}}(\boldsymbol{P}) = \Psi_{\boldsymbol{\alpha}}(r\boldsymbol{P})\Psi_{\boldsymbol{r}}(\boldsymbol{P})^{a^2-ab}\Psi_{\boldsymbol{r\omega}}(\boldsymbol{P})^{b^2-ab}\Psi_{\boldsymbol{r(1+\omega)}}(\boldsymbol{P})^{ab}.$$

- Apply the local height formula to the point $[r]P$: $\nu\left(\Psi_{\boldsymbol{\alpha}}(rP)\right) = \tilde{\lambda}\left([\alpha]rP\right) - a^2\tilde{\lambda}(rP) - b^2\tilde{\lambda}([\omega]rP) - ab\left(\tilde{\lambda}([1+\omega]rP) - \tilde{\lambda}(rP) - \tilde{\lambda}([\omega]rP)\right).$

Explicit formula for CM net polynomials

Case I: $z = \alpha r \in (r), \alpha = a + b\omega$

$$g_{z,\nu}(P) = (a^2 - ab)\mu + (b^2 - ab)\mu_\omega + (ab)\mu_{1+\omega}$$

- Use of chain rule:

$$\Psi_{\boldsymbol{\alpha r}}(\boldsymbol{P}) = \Psi_{\boldsymbol{\alpha}}(r\boldsymbol{P})\Psi_{\boldsymbol{r}}(\boldsymbol{P})^{a^2-ab}\Psi_{\boldsymbol{r\omega}}(\boldsymbol{P})^{b^2-ab}\Psi_{\boldsymbol{r(1+\omega)}}(\boldsymbol{P})^{ab}.$$

- Apply the local height formula to the point $[r]P$: $\nu\left(\Psi_{\boldsymbol{\alpha}}(rP)\right) = \tilde{\lambda}\left([\alpha]rP\right) - a^2\tilde{\lambda}(rP) - b^2\tilde{\lambda}([\omega]rP) - ab\left(\tilde{\lambda}([1+\omega]rP) - \tilde{\lambda}(rP) - \tilde{\lambda}([\omega]rP)\right).$
- The point rP is non-singular $\mod \nu$, so we can use

$$\tilde{\lambda}(rP) = \frac{1}{2}\max\left\{\nu(x(rP)^{-1}), 0\right\} = \frac{1}{2}\max\left\{2\nu(\Psi_{\boldsymbol{r}}(\boldsymbol{P})) - \nu(\Phi_{\boldsymbol{r}}(\boldsymbol{P})), 0\right\}$$

to evaluate the valuations at $[r]P, [r\omega]P, [r(1+\omega)]P, [\alpha r]P$.

Explicit formula for CM net polynomials

Case II: $z = \alpha r \pm \beta \notin (r)$

- Original formula: for $n = 2tr \pm k$ with $1 \leq k < r$,

$$g_{n,\nu}(P) = 2\nu(\psi_k(P)) \pm 2\left(2\nu\left(\frac{\psi_k(P)}{\psi_{r-k}(P)}\right) + \mu\right)t + 4\mu t^2.$$

Current formula: for $z = \alpha r \pm \beta \notin (r)$,

$$g_{z,\nu}(P) = 2\nu(\Psi_{\boldsymbol{\beta}}) \pm 2a\left[\nu\left(\frac{\Psi_{\boldsymbol{\beta}}}{\Psi_{\boldsymbol{r-\beta}}}\right) + \frac{\mu}{2}\right] \pm 2b\left[\nu\left(\frac{\Psi_{\boldsymbol{\beta}}}{\Psi_{\boldsymbol{r\omega-\beta}}}\right) + \frac{\mu_\omega}{2}\right]$$

$$(a^2 - ab)\mu + (b^2 - ab)\mu_\omega + ab\,\mu_{1+\omega}$$

- Our new formula is an extension of Cheon and Hahn's formula, so it should retain similar structure. Here we talk about how $4\mu t^2$ comes from $n = tr$.
- We are now considering two points: P and $[\omega]P$.

Explicit formula for CM net polynomials

Case II: $z = \alpha r \pm \beta \notin (r)$

$$g_{z,\nu}(P) = 2\nu\left(\Psi_{\boldsymbol{\beta}}\right) \pm 2a\left[\nu\left(\frac{\Psi_{\boldsymbol{\beta}}}{\Psi_{\boldsymbol{r-\beta}}}\right) + \frac{\mu}{2}\right] \pm 2b\left[\nu\left(\frac{\Psi_{\boldsymbol{\beta}}}{\Psi_{\boldsymbol{r\omega-\beta}}}\right) + \frac{\mu_\omega}{2}\right] + (a^2 - ab)\mu + (b^2 - ab)\mu_\omega + ab\,\mu_{1+\omega}$$

- Local height formula:

  $$\tilde{\lambda}([\alpha]P) = a^2\tilde{\lambda}(P) + b^2\tilde{\lambda}(\omega P) + ab\left(\tilde{\lambda}([1+\omega]P) - \tilde{\lambda}(P) - \tilde{\lambda}(\omega P)\right) + \nu\left(\Psi_{\boldsymbol{\alpha}}(\boldsymbol{P})\right)$$

  Apply this to to $[z]P = [\alpha r + \beta]P$, $[\beta]P$, $[r-\beta]P$ and $[r\omega - \beta]P$.

- For any $\alpha = a + b\omega \notin \operatorname{ann}(P)$, $r \in \operatorname{ann}(P)$, we have

  $$\lambda\left([\alpha]P\right) = \lambda\left([r \pm \alpha]P\right).$$

  This allows us to cancel $\tilde{\lambda}\left([r-\beta]P\right)$ and $\tilde{\lambda}\left([\beta]P\right)$, and similarly for $[r\omega - \beta]P$ and $[\beta]P$.

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. J. Cheon and S. Hahn (1998). manuscripta mathematica. View online
3. Naskręcki, Bartosz and Verzobio, Matteo (2024). Proceedings of the Royal Society of Edinburgh: Section A Mathematics. View online.
4. Satoh, Takakazu (2004). Generalized division polynomials. MATHEMATICA SCANDINAVICA. View online.
5. Silverman, J. H. (1994). Advanced topics in the arithmetic of elliptic curves. Springer-Verlag. View online.
6. Silverman, J. H. (2009). The arithmetic of elliptic curves. Springer-Verlag. View online.
7. Stange, Katherine E. (2011). Elliptic nets and elliptic curves. Algebra Number Theory 5, no. 2, 197–229. View online
8. Stange, Katherine E. (2025). Division polynomials for arbitrary isogenies. View online.