Methods for studying integral points on elliptic curves

Edison Au-Yeung
University of Warwick

Junior Number Theory Seminar
University of Warwick

18 May 2026

Small recap

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

$$E_{A,B} : y^2 = x^3 + Ax + B, A, B \in K$$

- $E(K)$ is the set of points $(x, y) \in K^2$ that lie on E, together with a point at infinity O. They form a finitely generated additive group.
- 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 and consider

$$[n]P = P + \ldots + P.$$

How many integral points are there?

How many integral points are there?

Theorem (Siegel, 1929)

Let E/K be an elliptic curve defined by a Weierstrass equation, then $\{P \in E_{A,B}(K) \colon x(P) \in \mathcal{O}_K\}$ is a finite set.

How many integral points are there?

Theorem (Siegel, 1929)

Let E/K be an elliptic curve defined by a Weierstrass equation, then $\{P \in E_{A,B}(K) : x(P) \in \mathcal{O}_K\}$ is a finite set.

Conjecture (Lang)

Let E/K be an elliptic curve, and choose a quasi-minimal Weierstrass equation for $E/K : y^2 = x^3 + Ax + B$. Then there exists a constant C, depending only on K, such that

$$\#\{(x, y) \in E_{A,B}(\mathcal{O}_K)^2 : y^2 = x^3 + Ax + B\} \ll C^{\mathrm{rank}(E(K))}.$$

How many integral points are there?

Theorem (Siegel, 1929)

Let E/K be an elliptic curve defined by a Weierstrass equation, then $\{P \in E_{A,B}(K) \colon x(P) \in \mathcal{O}_K\}$ is a finite set.

Conjecture (Lang)

Let E/K be an elliptic curve, and choose a quasi-minimal Weierstrass equation for $E/K \colon y^2 = x^3 + Ax + B$. Then there exists a constant C, depending only on K, such that

$$\#\{(x,y) \in E_{A,B}(\mathcal{O}_K)^2 \colon y^2 = x^3 + Ax + B\} \ll C^{\mathrm{rank}(E(K))}.$$

- Quasi-minimal: the discriminant is minimised subject to the condition that A, B are integral; 6^{12} divides $\Delta(E_{A,B})$.
- Consider $E \colon y^2 = x^3 + Ax + B, P = (x,y) \in E(\mathbb{Z})$, via change of variable
$$x' = d^2 x, \quad y' = d^3 y,$$
then $P' = (x', y') \in E_d(\mathbb{Z}), E_d \colon y^2 = x^3 + Ad^4 x + Bd^6$.

How many integral points are there?

Theorem (Siegel, 1929)

Let E/K be an elliptic curve defined by a Weierstrass equation, then $\{P \in E_{A,B}(K) \colon x(P) \in \mathcal{O}_K\}$ is a finite set.

Conjecture (Lang)

Let E/K be an elliptic curve, and choose a quasi-minimal Weierstrass equation for $E/K \colon y^2 = x^3 + Ax + B$. Then there exists a constant C, depending only on K, such that

$$\#\{(x,y) \in E_{A,B}(\mathcal{O}_K)^2 \colon y^2 = x^3 + Ax + B\} \ll C^{\mathrm{rank}(E(K))}.$$

Two possible bounds that one can give:

1. Number of integral points, i.e. $\#\{(x,y) \in E_{A,B}(\mathcal{O}_K)^2 \colon y^2 = x^3 + Ax + B\}$.
2. Largest value of n such that $[n]P$ is an integral point (P has to be a non-torsion, integral point).

Known results – number of integral points

- Silverman (1987): $\ll_K O(1)^{(1+\mathrm{rank}(E))(1+\delta)}$ where δ is the number of primes of K such that the j-invariant of E is non-integral (i.e. multiplicative reduction)
- Hindry-Silverman (1988): $\ll_K O(1)^{(1+\mathrm{rank}(E))\sigma_{E/K}}$, where $\sigma_{E/K}$ is the Szpiro ratio of E/K, measuring the extent to which the discriminant is divisible by large powers (here we assume $\sigma_{E/K}$ is bounded from above).

Known results – number of integral points

- Silverman (1987): $\ll_K O(1)^{(1+\mathrm{rank}(E))(1+\delta)}$ where δ is the number of primes of K such that the j-invariant of E is non-integral (i.e. multiplicative reduction)
- Hindry-Silverman (1988): $\ll_K O(1)^{(1+\mathrm{rank}(E))\sigma_{E/K}}$, where $\sigma_{E/K}$ is the Szpiro ratio of E/K, measuring the extent to which the discriminant is divisible by large powers (here we assume $\sigma_{E/K}$ is bounded from above).
- Helfgort-Venkatesh (2006): $\ll O(1)^{\omega(\Delta)}(\log|\Delta|)^2 \cdot 1.33^{\mathrm{rank}(E/\mathbb{Q})}$, $\omega(n)$ denotes the number of distinct prime factors of n.
- Alpöge-Ho (2020): $\ll 2^{\mathrm{rank}(E/K)} \prod_{p^2|\Delta(E)} \left(4\lfloor \frac{\nu_p(\Delta(E))}{2} \rfloor + 1\right)$

Known results – number of integral points

- Silverman (1987): $\ll_K O(1)^{(1+\mathrm{rank}(E))(1+\delta)}$ where δ is the number of primes of K such that the j-invariant of E is non-integral (i.e. multiplicative reduction)
- Hindry-Silverman (1988): $\ll_K O(1)^{(1+\mathrm{rank}(E))\sigma_{E/K}}$, where $\sigma_{E/K}$ is the Szpiro ratio of E/K, measuring the extent to which the discriminant is divisible by large powers (here we assume $\sigma_{E/K}$ is bounded from above).
- Helfgort-Venkatesh (2006): $\ll O(1)^{\omega(\Delta)}(\log|\Delta|)^2 \cdot 1.33^{\mathrm{rank}(E/\mathbb{Q})}$, $\omega(n)$ denotes the number of distinct prime factors of n.
- Alpöge-Ho (2020): $\ll 2^{\mathrm{rank}(E/K)} \prod_{p^2|\Delta(E)} \left(4\lfloor \frac{\nu_p(\Delta(E))}{2} \rfloor + 1\right)$

All the above results have very large $O(1)$ constants!

- Silverman/Hindry-Silverman: $\sim 10^{10}$
- Alpöge-Ho: $7^{2^7} \sim 10^{100}$

Known results – size of the multiple of an integral point

- Ingram (2009): there is an absolute constant C such that for all quasi-minimal elliptic curves $E/\mathbb{Q}$, there is at most one value of $n > CM(P)^{16}$ such that $[n]P \in E(\mathbb{Z})$, P a non-torsion integral point in $E(\mathbb{Q})$. Furthermore, this value n is prime.

  $M(P)$ = the smallest constant m such that $[m]P$ has non-singular reduction modulo all primes.

Known results – size of the multiple of an integral point

- Ingram (2009): there is an absolute constant C such that for all quasi-minimal elliptic curves $E/\mathbb{Q}$, there is at most one value of $n > CM(P)^{16}$ such that $[n]P \in E(\mathbb{Z})$, P a non-torsion integral point in $E(\mathbb{Q})$. Furthermore, this value n is prime.

  $M(P)$ = the smallest constant m such that $[m]P$ has non-singular reduction modulo all primes.

- Stange (2016): similar result but the bound now only depends on the ratio of heights $h(E)/\hat{h}(P)$.

Known results – size of the multiple of an integral point

- Ingram (2009): there is an absolute constant C such that for all quasi-minimal elliptic curves $E/\mathbb{Q}$, there is at most one value of $n > CM(P)^{16}$ such that $[n]P \in E(\mathbb{Z})$, P a non-torsion integral point in $E(\mathbb{Q})$. Furthermore, this value n is prime.

  $M(P)$ = the smallest constant m such that $[m]P$ has non-singular reduction modulo all primes.

- Stange (2016): similar result but the bound now only depends on the ratio of heights $h(E)/\hat{h}(P)$.

For elliptic curves with integral $j(E)$, $M(P) \leq 12$, so Ingram's result says that in this case $n \sim 10^{10}$ potentially...

Known results – special cases

But in the case of quadratic twists, we have much better bounds/explicit results...? Let $E_{A,B}\colon y^2 = x^3 + Ax + B$ be our elliptic curve, then the quadratic twist of E by D is $E_D\colon y^2 = x^3 + D^2Ax + D^3B$.

Known results – special cases

But in the case of quadratic twists, we have much better bounds/explicit results...? Let $E_{A,B}\colon y^2 = x^3 + Ax + B$ be our elliptic curve, then the quadratic twist of E by D is $E_D\colon y^2 = x^3 + D^2Ax + D^3B$.

- Ingram (2009): specialise to congruent number curves: for the curve $E_{-N^2,B}\colon y^2 = x^3 - N^2x$, ($N$ square-free integer),

$$\#\{n \in \mathbb{N}\colon [n]P \in E_{-N^2,0}(\mathbb{Z}), P \text{ non-torsion}\} \leq 2.$$

- Ghadermarzi (2023): specialise to Mordell's curves: for the curve $E_{0,B}\colon y^2 = x^3 + B$,

$$\#\{n \in \mathbb{N}\colon [n]P \in E_{0,B}(\mathbb{Z}), P \text{ non-torsion}\} \leq 4.$$

Known results – special cases

But in the case of quadratic twists, we have much better bounds/explicit results...? Let $E_{A,B}\colon y^2 = x^3 + Ax + B$ be our elliptic curve, then the quadratic twist of E by D is $E_D\colon y^2 = x^3 + D^2Ax + D^3B$.

- Ingram (2009): specialise to congruent number curves: for the curve $E_{-N^2,B}\colon y^2 = x^3 - N^2x$, ($N$ square-free integer),

$$\#\{n \in \mathbb{N}\colon [n]P \in E_{-N^2,0}(\mathbb{Z}), P \text{ non-torsion}\} \leq 2.$$

- Ghadermarzi (2023): specialise to Mordell's curves: for the curve $E_{0,B}\colon y^2 = x^3 + B$,

$$\#\{n \in \mathbb{N}\colon [n]P \in E_{0,B}(\mathbb{Z}), P \text{ non-torsion}\} \leq 4.$$

- Chan (2024): $\#E_{-N^2,0}(\mathbb{Z}) \ll (3.8)^{\mathrm{rank}(E_{-N^2,0}(\mathbb{Q}))}$.
- Choi (2024): for sufficiently large $|D|$ (depending on A, B), $\#E_D(\mathbb{Z}) \ll 4^{\mathrm{rank}(E_D(\mathbb{Q}))}$

Comparison of methods - Silverman/Hindry-Silverman

Silverman (1987): Given a Weierstrass model $E_{A,B}\colon y^2 = x^3 + Ax + B$, both results for $\#\{(x,y) \in E_{A,B}(\mathcal{O}_K)^2 \colon y^2 = x^3 + Ax + B\}$ depend on $\#E(K)_{\text{tors}}$ and the ratio

$$\frac{h\left([A,B,1]\right)}{\min\{\hat{h}(P)\colon P \in E_{A,B}(K), P \text{ non-torsion}\}}.$$

Comparison of methods - Silverman/Hindry-Silverman

Silverman (1987): Given a Weierstrass model $E_{A,B}: y^2 = x^3 + Ax + B$, both results for $\#\{(x,y) \in E_{A,B}(\mathcal{O}_K)^2 : y^2 = x^3 + Ax + B\}$ depend on $\#E(K)_{\text{tors}}$ and the ratio

$$\frac{h([A,B,1])}{\min\{\hat{h}(P) : P \in E_{A,B}(K), P \text{ non-torsion}\}}.$$

Hindry-Silverman (1988):

- Canonical height is the sum of local heights, so compute lower bounds of the local heights instead, which gives $\hat{h}(P) \geq 1/\left(3\sigma_{E/K}\right)$.

Comparison of methods - Silverman/Hindry-Silverman

Silverman (1987): Given a Weierstrass model $E_{A,B} : y^2 = x^3 + Ax + B$, both results for $\#\{(x,y) \in E_{A,B}(\mathcal{O}_K)^2 : y^2 = x^3 + Ax + B\}$ depend on $\#E(K)_{\text{tors}}$ and the ratio

$$\frac{h([A,B,1])}{\min\{\hat{h}(P) \colon P \in E_{A,B}(K), P \text{ non-torsion}\}}.$$

Hindry-Silverman (1988):

- Canonical height is the sum of local heights, so compute lower bounds of the local heights instead, which gives $\hat{h}(P) \geq 1/\left(3\sigma_{E/K}\right)$.
- The bounds above only apply to $[n]P$ with

$$n \geq (20\sigma_{E/K})^{4[K\colon\mathbb{Q}]} 10^{2\sigma_{E/K}},$$

  then use the fact that the canonical height on E/K is a quadratic form: $\hat{h}([n]P) = n^2\hat{h}(P)$.

Overview of Ingram's method

Ingram (2009): for a non-torsion integral point P, there is an absolute constant C such that for all minimal elliptic curves $E/\mathbb{Q}$, there is at most one value of $n > CM(P)^{16}$ such that $[n]P \in E(\mathbb{Z})$. Furthermore, this value n is prime.

1. Show that if n larger than $O(M^{16})$, then n must be prime.

Overview of Ingram's method

Ingram (2009): for a non-torsion integral point P, there is an absolute constant C such that for all minimal elliptic curves $E/\mathbb{Q}$, there is at most one value of $n > CM(P)^{16}$ such that $[n]P \in E(\mathbb{Z})$. Furthermore, this value n is prime.

1. Show that if n larger than $O(M^{16})$, then n must be prime.
   - FInd upper and lower bounds for $\hat{h}(P)$: Silverman provides a lower bound for $\hat{h}(P)$ ($P \in E(K)$ non-torsion) and $\left|\hat{h}(P) - \frac{1}{2}h(x(P))\right| < 2h(E)$.
   - There are polynomials $\phi_n, \psi_n, \omega_n \in \mathbb{Z}[x,y]$ for $n \in \mathbb{N}$ with

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

     The polynomial ψ_n is usually referred as the n-th division polynomial.
   - The roots of the polynomial ψ_n^2 are the n–torsion points:

$$\psi_n^2(x(P)) = n^2 \prod_{Q \in E[n]\backslash\{O\}} |x(P) - x(Q)|$$

Overview of Ingram's method

Ingram (2009): for a non-torsion integral point P, there is an absolute constant C such that for all minimal elliptic curves $E/\mathbb{Q}$, there is at most one value of $n > CM(P)^{16}$ such that $[n]P \in E(\mathbb{Z})$. Furthermore, this value n is prime.

1. Show that if n larger than $O(M^{16})$, then n must be prime.
2. Find an upper bound on n (in terms of $h(E)$) using linear forms in elliptic logarithm.
    - Under the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda, P \mapsto z$, z is called the elliptic logarithm of P (note: $P = (\wp(z), \wp'(z))$).
    - The linear form is $L_{n,m}(z, \omega) = nz + m\omega$, ω is the real period of E.
    - We will need to find an upper bound for $L_{n,m}(z, \omega)$: if $[n]P$ is integral, then $L_{n,m}(z, \omega)$ is very small (for lower bound, this is by David (1995)).

Overview of Ingram's method

Ingram (2009): for a non-torsion integral point P, there is an absolute constant C such that for all minimal elliptic curves $E/\mathbb{Q}$, there is at most one value of $n > CM(P)^{16}$ such that $[n]P \in E(\mathbb{Z})$. Furthermore, this value n is prime.

1. Show that if n larger than $O(M^{16})$, then n must be prime.
2. Find an upper bound on n (in terms of $h(E)$) using linear forms in elliptic logarithm.
3. Gap principle: if there are two large values n_1, n_2 such that $[n_i]P$ is integral, then we can construct a function $f(x, y)$ such that $f(n_1, n_2)$ is very small. Primality guarantees the lower bound does not vanish.

Sharper result

1. Better results for congruent number curves and Mordell's curves:

$$E_{-N^2,0}\colon y^2 = x^3 - N^2x; \quad E_{0,B}\colon y^2 = x^3 + B.$$

- These two curves have much sharper lower and upper bounds for $\hat{h}(P)$ and $\hat{h}(P) - h(x(P))$ respectively.
- For $\hat{h}(P) - h(x(P))$, one can analyse elliptic divisibility sequence and division polynomials to get better bounds.
- Example: for $E_{-N^2,0}\colon y^2 = x^3 - N^2x$, $[n]P$ integral, using Ingram's bounds:
  - Generally: $\log|\psi_n| \leq n^2 M(P)^2 \log|\Delta(E)|$, $\hat{h}(P) \leq \log(n) + \left(\frac{16}{3}M(P)^2 + 2\right) h(E)$
  - $E_{-N^2,0}$: $\log|\psi_n| \leq \frac{n^2-1}{2}\log|2N|$, $\hat{h}(P) \leq \log(n) + \frac{1}{2}\log(N) + \frac{1}{3}\log(2)$

What's next?

- There are improvements of the big constant for number of integral points, from 10^{10} to 10^7 (but by separating out $\mathrm{rank}(E)$ from $O(1)$, one can bound the average and get new results on moments).

What's next?

- There are improvements of the big constant for number of integral points, from 10^{10} to 10^7 (but by separating out $\mathrm{rank}(E)$ from $O(1)$, one can bound the average and get new results on moments).
- Can consider quadratic twists $E' : y^2 = x^3 + Adx^2 + Bd^3$, results are more explicit.

Conjecture (Lang)

Let E/K be an elliptic curve, and choose a quasi-minimal Weierstrass equation for $E/K : y^2 = x^3 + Ax + B$. Then there exists a constant C, depending only on K, such that

$$\#\{(x,y) \in E_{A,B}(\mathcal{O}_K)^2 : y^2 = x^3 + Ax + B\} \ll C^{\mathrm{rank}(E(K))}$$

What's next?

- There are improvements of the big constant for number of integral points, from 10^{10} to 10^7 (but by separating out $\operatorname{rank}(E)$ from $O(1)$, one can bound the average and get new results on moments).
- Can consider quadratic twists $E' : y^2 = x^3 + Adx^2 + Bd^3$, results are more explicit.

Conjecture (Lang)

Let E/K be an elliptic curve, and choose a quasi-minimal Weierstrass equation for $E/K : y^2 = x^3 + Ax + B$. Then there exists a constant C, depending only on K, such that

$$\#\{(x,y) \in E_{A,B}(\mathcal{O}_K)^2 : y^2 = x^3 + Ax + B\} \ll C^{\operatorname{rank}(E(K))}$$

What if we apply Ingram's method to $\mathbb{Z}$–linear combination of points

$$n_1 P_1 + n_2 P_2 + \ldots + n_r P_r?$$

What's next?

To apply Ingram's method, we need the following:

1. A 'division polynomial' for linear combinations of points
2. Being able to bound $h(x(n_1P_1 + \ldots + n_rP_r)) = \log|x(n_1P_1 + \ldots + n_rP_r)|$.
3. Lower and upper bounds for elliptic logarithms.

Available tools – 'division polynomials'

- For $P \in E(K)$, there are polynomials $\phi_n, \psi_n, \omega_n \in \mathbb{Z}[x,y]$ for $n \in \mathbb{N}$ with

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

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

- It turns out that we also have similar rational functions for $\mathbb{Z}$–linear combination of points.

Net polynomials (rank 2) (Stange, 2009)

For $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K)$, there exists rational functions $\Psi_{(m,n)}$, $\Phi_{(m,n)}$, $\bar{\Omega}_{(m,n)} \in K[x_1, x_2, y_1, y_2][(x_2 - x_1)^{-1}]$, known as *net polynomials*, such that

$$[m]P_1 + [n]P_2 = \left(\frac{\Phi_{(m,n)}(P_1, P_2)}{\Psi^2_{(m,n)}(P_1, P_2)}, \frac{\bar{\Omega}_{(m,n)}(P_1, P_2)}{\Psi^3_{(m,n)}(P_1, P_2)}\right).$$

Available tools – 'division polynomials'

- Roots of $\psi_n(x)$ are $\{x(Q) \in K \colon [n]P = O\}$:

$$\psi_n^2(x) = n^2 \prod_{Q \in E[n] \setminus \{O\}} |x - x(Q)|$$

- Roots of $\Psi_{(m,n)}(P_1, P_2)$ are $\{(x(Q_1), x(Q_2)) \in K^2 \colon [m]Q_1 + [n]Q_2 = O\}$. i.e. $\Psi_{(m,n)}(P_1, P_2)$ vanishes on a 1-dimensional locus ($[m]P + [n]Q = O$), generally infinitely many solutions...

Available tools – 'division polynomials'

- Roots of $\psi_n(x)$ are $\{x(Q) \in K \colon [n]P = O\}$:

$$\psi_n^2(x) = n^2 \prod_{Q \in E[n] \setminus \{O\}} |x - x(Q)|$$

- Roots of $\Psi_{(m,n)}(P_1, P_2)$ are $\{(x(Q_1), x(Q_2)) \in K^2 \colon [m]Q_1 + [n]Q_2 = O\}$. i.e. $\Psi_{(m,n)}(P_1, P_2)$ vanishes on a 1-dimensional locus ($[m]P + [n]Q = O$), generally infinitely many solutions...
- We chose to focus on elliptic curves with complex multiplication: this is somewhere between rank 1 and rank 2

Setting–complex multiplication

- Let $E/\mathbb{C}$ be an elliptic curve over the complex numbers defined by a Weierstrass equation with integer coefficients, then $\mathrm{End}(E)$ is always isomorphic to $\mathbb{Z}$ or $\mathbb{Z}[\tau] = \{a + b\tau : a, b \in \mathbb{Z}\}$, an order in an imaginary quadratic field F.

Setting–complex multiplication

- Let $E/\mathbb{C}$ be an elliptic curve over the complex numbers defined by a Weierstrass equation with integer coefficients, then $\mathrm{End}(E)$ is always isomorphic to $\mathbb{Z}$ or $\mathbb{Z}[\tau] = \{a + b\tau \colon a, b \in \mathbb{Z}\}$, 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 $\alpha \in \mathbb{Z}[\tau]$ in the group $E(K)$.
- Example: $E \colon y^2 = x^3 - 35x + 98$ has complex multiplication by $\mathbb{Z}[\tau] = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$,

$$[\tau](x,y) = \left(\tau^{-2}\left(x - \frac{7(1-\tau)^4}{(x+\tau^2-2)}\right), \tau^{-3}y\left(1 + \frac{7(1-\tau)^4}{(x+\tau^2-2)^2}\right)\right)$$

i.e. we choose $P_1 = P, P_2 = [\tau]P$ and consider $[m]P + [n][\tau]P = [m + n\tau]P$.

What we have so far...

- Ingram's bound: for $P, [n]P \in E(K)$ integral,

$$\log|\psi_n| \leq n^2 M(P)^2 \log|\Delta(E)|.$$

- This comes from an anlaysis of the extent of the cancellation in the fraction $x(nP) = \phi_n/\psi_n^2$, i.e. the quantity $\min\left(\nu\left(\psi_n^2(P)\right), \nu\left(\phi_n(P)\right)\right)$, ν some valuations (an explicit formula by Cheon and Hahn, 1998).

What we have so far...

- Ingram's bound: for $P, [n]P \in E(K)$ integral,

$$\log|\psi_n| \leq n^2 M(P)^2 \log|\Delta(E)|.$$

- This comes from an anlaysis of the extent of the cancellation in the fraction $x(nP) = \phi_n/\psi_n^2$, i.e. the quantity $\min\left(\nu\left(\psi_n^2(P)\right), \nu\left(\phi_n(P)\right)\right)$, ν some valuations (an explicit formula by Cheon and Hahn, 1998).
- We have an explicit formula for $\min\left(\nu\left(\Psi_{(n,m)}^2(P,[\tau]P)\right), \nu\left(\Phi_{m,n}(P,[\tau]P)\right)\right)$ (Au-Yeung, 2025), based on Cheon and Hahn's work

What we have so far...

- Ingram's bound: for $P, [n]P \in E(K)$ integral,

$$\log|\psi_n| \leq n^2 M(P)^2 \log|\Delta(E)|.$$

- This comes from an anlaysis of the extent of the cancellation in the fraction $x(nP) = \phi_n/\psi_n^2$, i.e. the quantity $\min\left(\nu\left(\psi_n^2(P)\right), \nu\left(\phi_n(P)\right)\right)$, ν some valuations (an explicit formula by Cheon and Hahn, 1998).
- We have an explicit formula for $\min\left(\nu\left(\Psi_{(n,m)}^2(P,[\tau]P)\right), \nu\left(\Phi_{m,n}(P,[\tau]P)\right)\right)$ (Au-Yeung, 2025), based on Cheon and Hahn's work
- We believe for $P, [\tau]P, [m+n\tau]P \in E(K)$ $\mathcal{O}_K$–integral,

$$\log|\Psi_{(m,n)}| \overset{?}{\leq} 810 M(P)^4 (\mathrm{Nm}(m+n\tau)+1)(1+\mathrm{Nm}(\tau))^3 \log|\Delta(E)|$$

Part of the method did not assume complex multiplication!

What we have so far...

Ingram's height bound: if $P \in E(\mathbb{Q})$ is an integral point of infinite order, and suppose that $[n]P$ is integral for some $n \geq 2$, then

$$|x(P)| \leq 240n^2 \exp\left(\frac{32}{3}M(P)^2 h(E)\right), \text{ and}$$

$$\hat{h}(P) \leq \log n + \left(\frac{16}{3}M(P)^2 + 2\right) h(E).$$

What we have so far...

Ingram's height bound: if $P \in E(\mathbb{Q})$ is an integral point of infinite order, and suppose that $[n]P$ is integral for some $n \geq 2$, then

$$|x(P)| \leq 240n^2 \exp\left(\frac{32}{3}M(P)^2 h(E)\right), \text{ and}$$

$$\hat{h}(P) \leq \log n + \left(\frac{16}{3}M(P)^2 + 2\right) h(E).$$

Our current height bound: if $P, [\tau]P \in E(K)$ are integral points of infinite order, and suppose that $[\alpha]P$ is integral with $\mathrm{Nm}(\alpha) \geq 2$, then

$$|x(P)| \overset{?}{\leq} 2^{8\,\mathrm{Nm}(\tau)+3} 240\,\mathrm{Nm}(\alpha) \exp\left(1620M(P)^4(1+\mathrm{Nm}(\tau))^4\right), \text{ and}$$

$$\hat{h}(P) \overset{?}{\leq} \frac{1}{2}\log\left(\mathrm{Nm}(\alpha)+1\right) + \left[1620M(P)^4(1+\mathrm{Nm}(\tau))^4 + 4\right] h(E).$$

What we have so far...

Proposition (Ingram, 2009)

For a non-torsion integral point P, there is an absolute constant C such that for all quasi–minimal elliptic curves $E/\mathbb{Q}$, if $[n]P \in E(\mathbb{Z})$ with $n > CM(P)^{16}$, then n is prime.

Proposition

Suppose a quasi–minimal elliptic curve E/K has CM by $\mathcal{O}_F = \mathbb{Z}[\tau]$ (imaginary F quadratic field). Assume P and $[\tau]P$ are non-torsion integral points in $E(\mathcal{O}_K)$, if $[\alpha]P$ and $[\alpha\tau]P$ are also integral with $|\alpha| > CM(P)^{18}$, then α is prime in $\mathcal{O}_F$.

References

1. Alpöge, Levent and Ho, Wei. The second moment of the number of integral points on elliptic curves is bounded. (2022). View online.
2. Au-Yeung, H L Edison. Explicit valuation of elliptic nets for elliptic curves with complex multiplication. (2025). View online.
3. Chan, Stephanie. Integral points on cubic twists of Mordell curves. Math. Ann. 388, 2275–2288 (2024). View online.
4. Choi, Seokhyun. Number of integral points on quadratic twists of elliptic curves. (2025). View online.
5. David, Sinnou. Minorations de formes linéaires de logarithmes elliptiques. Mémoires de la Société Mathématique de France (1995), Volume: 62, page 1-143. View online.
6. Ghadermarzi, Amir. Multiples of integral points on Mordell curves. Acta Arithmetica (2023), Volume 211, Page 121-159. DOI: 10.4064/aa220822-3-8. View online.
7. H. A. Helfgott and A. Venkatesh. Integral Points on Elliptic Curves and 3-Torsion in Class Groups. Journal of the American Mathematical Society, (2006), Vol. 19, No. 3 (Jul, 2006), pp. 527-550. View online.
8. Hindry, M.; Silverman, J.H. The canonical height and integral points on elliptic curves. Inventiones mathematicae (1998), volume 93; pp. 419 - 450. View online.

References

9. Ingram, Patrick. Multiples of integral points on elliptic curves. Journal of Number Theory (2009). View online.
10. J. Cheon and S. Hahn. Explicit valuations of division polynomials of an elliptic curve. manuscripta mathematica 97, 319–328 (1998). View online
11. Silverman, J. H. Advanced topics in the arithmetic of elliptic curves. Springer-Verlag (1994). View online.
12. Silverman, J. H. The arithmetic of elliptic curves. Springer-Verlag (2009). View online.
13. Silverman, J. H. Advanced Topics in the Arithmetic of Elliptic Curves. Springer-Verlag (1994). View online.
14. Stange, Katherine E. Elliptic nets and elliptic curves. Algebra Number Theory 5 (2011), no. 2, 197–229. View online
15. Stange, Katherine E. Integral Points on Elliptic Curves and Explicit Valuations of Division Polynomials. Canadian Journal of Mathematics (2016). ;68(5):1120-1158. doi:10.4153/CJM-2015-005-0. View online.
16. Silverman, J. H. A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves. Journal für die reine und angewandte Mathematik (1987), vol. 1987, no. 378, pp. 60-100. View online.