The finiteness of integral points on elliptic curves

Edison Au-Yeung
University of Warwick

Y–RANT conference 2026
University of Bristol

3 September 2026

Small recap

- Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ with the short Weierstrass equation:
$$E_{A,B} : y^2 = x^3 + Ax + B, A, B \in \mathbb{Q}$$
- Mordell–Weil theorem: $E(\mathbb{Q})$ is the set of points $(x, y) \in K^2$ that lie on E, together with a point at infinity O, which is the identity in this finitely generated additive group: $P +_E O = P$ for all $P \in E(\mathbb{Q})$.

Small recap

- Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ with the short Weierstrass equation:
$$E_{A,B}: y^2 = x^3 + Ax + B, A, B \in \mathbb{Q}$$
- Mordell–Weil theorem: $E(\mathbb{Q})$ is the set of points $(x, y) \in K^2$ that lie on E, together with a point at infinity O, which is the identity in this finitely generated additive group: $P +_E O = P$ for all $P \in E(\mathbb{Q})$.
- The canonical height function $\hat{h}: E(\overline{\mathbb{Q}}) \to \mathbb{R}$ satisfies
  1. $\hat{h}(P - Q) + \hat{h}(P + Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ for all $P, Q \in E(\overline{\mathbb{Q}})$ (parallelogram law).
  2. $\hat{h}([n]P) = n^2\hat{h}(P)$ for all $P \in E(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z}$.

Small recap

- Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$ with the short Weierstrass equation:
$$E_{A,B}\colon y^2 = x^3 + Ax + B, A, B \in \mathbb{Q}$$
- Mordell–Weil theorem: $E(\mathbb{Q})$ is the set of points $(x, y) \in K^2$ that lie on E, together with a point at infinity O, which is the identity in this finitely generated additive group: $P +_E O = P$ for all $P \in E(\mathbb{Q})$.
- The canonical height function $\hat{h}\colon E(\overline{\mathbb{Q}}) \to \mathbb{R}$ satisfies
  1. $\hat{h}(P - Q) + \hat{h}(P + Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ for all $P, Q \in E(\overline{\mathbb{Q}})$ (parallelogram law).
  2. $\hat{h}([n]P) = n^2\hat{h}(P)$ for all $P \in E(\overline{\mathbb{Q}})$ and $n \in \mathbb{Z}$.
- Most of the results in this talk are also true for E/K, where K is a number field.

Finiteness of integral point

Theorem (Siegel, 1929)

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

Finiteness of integral point

Theorem (Siegel, 1929)

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

This is the first sign of repulsion!

- If $\#E(\mathbb{Z})$ is infinite, let P be a non–torsion integral point, then $\{nP\}_{n\in\mathbb{N}}$ should contain infinitely many integral points.
- Recall that $\hat{h}(nP) = n^2\hat{h}(P)$, so size of $|x(nP)|$ must be growing exponentially.
- Interpretation: the point of infinity O repels the integral points!

How strong is the repulsion?

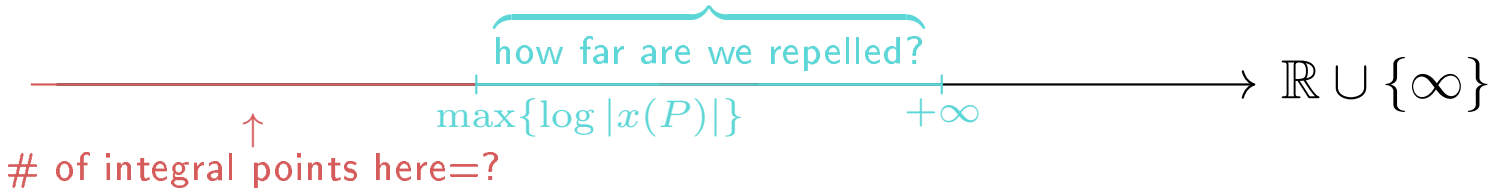
How strong is the repulsion?

There are some known (but impractical) results: consider $E_{A,B}: y^2 = x^3 + Ax + B$. If $P = (x, y) \in E(\mathbb{Z})$, then

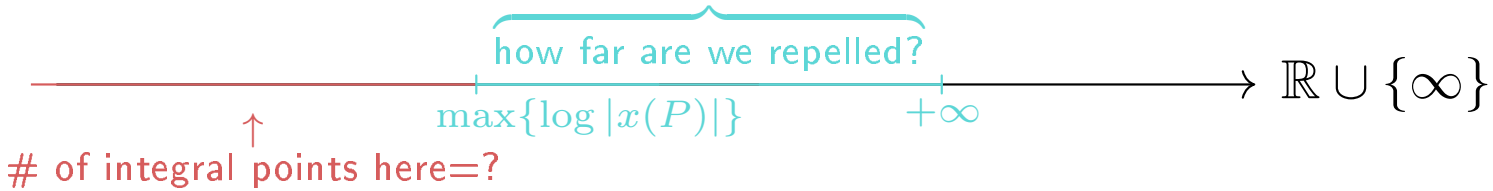
- Baker (1968): $|x| \leq \exp\left(\left(10^6 \max\{|A|, |B|\}\right)^{10^6}\right)$.
- Stark (1973): $\log \max\{|x|, |y|\} \leq C(\varepsilon)B^{1+\epsilon}$ (in the case of $A = 0$).

  (Improvement from last week of 24 August by Pasten! $\ll |B|^{1/2+\varepsilon}$)
- Hall's conjecture (1970): $\log|x| < (2+\epsilon)\log|B| + C(\varepsilon)$, $\varepsilon > 0$ (in the case of $A = 0$).

Number of integral points

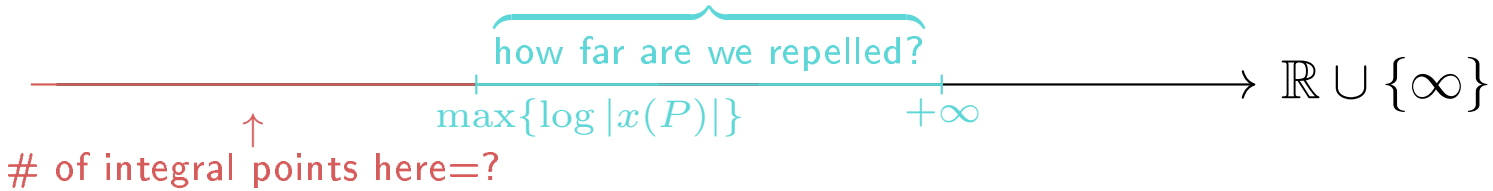


Number of integral points



- Silverman(1987)/Hindry-Silverman (1988): $\ll_K O(1)^{(1+\mathrm{rank}(E))C(E)}$, where $O(1) \sim 10^{10}$ and $C(E)$ is some constant dependent on E.
- Helfgort-Venkatesh (2006): $\ll O(1)^{\omega(\Delta)}(\log|\Delta(E)|)^2 \cdot 1.33^{\mathrm{rank}(E/\mathbb{Q})}$, $\omega(n)$ denotes the number of distinct prime factors of n; $O(1) = 7^{2^7} \sim 10^{100}$.

Number of integral points



- Silverman(1987)/Hindry-Silverman (1988): $\ll_K O(1)^{(1+\mathrm{rank}(E))C(E)}$, where $O(1) \sim 10^{10}$ and $C(E)$ is some constant dependent on E.
- Helfgort-Venkatesh (2006): $\ll O(1)^{\omega(\Delta)}(\log|\Delta(E)|)^2 \cdot 1.33^{\mathrm{rank}(E/\mathbb{Q})}$, $\omega(n)$ denotes the number of distinct prime factors of n; $O(1) = 7^{2^7} \sim 10^{100}$.
- Ingram (2009): large gaps occur between integral multiples of a point P 'in some sense'.

Multipliers grow rapidly

Consider the sequence of points $\{nP\}_{n\in\mathbb{N}}$, where P is a non–torsion integral point.

Theorem (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 $E(\mathbb{Q})$, where $M(P)$ is some constant dependent on P. Furthermore, this value n is prime.

Multipliers grow rapidly

Consider the sequence of points $\{nP\}_{n\in\mathbb{N}}$, where P is a non–torsion integral point.

Theorem (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 $E(\mathbb{Q})$, where $M(P)$ is some constant dependent on P. Furthermore, this value n is prime.

Proposition (Ingram, 2009)

If there are two large integers $n_1 < n_2$ (say, $> 10^{16}$) such that both $[n_1]P$ and $[n_2]P$ are integral, then they satisfy

$$n_1^2 h(E) \leq C_1 \log n_2 \implies C_2^{n_1^2} < n_2 \text{ (say, } C_1 > 10^6).$$

Multipliers grow rapidly

Proposition (Ingram, 2009)

If there are two large integers n_1, n_2 (say, $> 10^{16}$) such that both $[n_1]P$ and $[n_2]P$ are integral, then they satisfy

$$n_1^2 h(E) \leq C_1 \log n_2 \implies C_2^{n_1^2} < n_2 \text{ (say, } C_1 > 10^6).$$

- Phenonmenon/style of argument: the gap principle.

Multipliers grow rapidly

Proposition (Ingram, 2009)

If there are two large integers n_1, n_2 (say, $> 10^{16}$) such that both $[n_1]P$ and $[n_2]P$ are integral, then they satisfy

$$n_1^2 h(E) \leq C_1 \log n_2 \implies C_2^{n_1^2} < n_2 \text{ (say, } C_1 > 10^6).$$

- Phenonmenon/style of argument: the gap principle.
- Consequence: integral points actually repel each other!
- Example (Ingram, 2009): for congruent number curves $E_{-N^2,0}\colon y^2 = x^3 - N^2 x$, ($N$ square-free integer),

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

Quantifying the repulsion

This can be done in the Mordell–Weil lattice corresponding to E:

- $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^{\mathrm{rank}(E)}$ is a finite–dimensional real vector space, with $E(\mathbb{Q})/E(\mathbb{Q})_{\mathsf{tors}}$ being a lattice in $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$.
- The canonical height function extends to a positive definite quadratic form on $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$:

$$\langle \cdot, \cdot \rangle \colon E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}}) \to \mathbb{R}, \text{ defined by}$$

$$\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) = \hat{h}(P) + \hat{h}(Q) - \hat{h}(P-Q).$$

$$\cos\theta_{P,Q} := \frac{\langle P, Q \rangle}{2\|P\|\|Q\|} = \frac{\hat{h}(P-Q) + \hat{h}(P) + \hat{h}(Q)}{2\sqrt{\hat{h}(P)\hat{h}(Q)}}.$$

Quantifying the repulsion – quasi-orthogonality

Proposition (Helfgott/Helfgott–Venkatesh, 2004/2006)

If $P, Q \in E(\mathbb{Z})$ have comparable canonical heights, then

$$\hat{h}(P-Q) \geq (1-\varepsilon)\max\left(\hat{h}(P), \hat{h}(Q)\right) \implies \theta_{P,Q} \geq 60^\circ.$$

Quantifying the repulsion – quasi-orthogonality

Proposition (Helfgott/Helfgott–Venkatesh, 2004/2006)

If $P, Q \in E(\mathbb{Z})$ have comparable canonical heights, then

$$\hat{h}(P-Q) \geq (1-\varepsilon)\max\left(\hat{h}(P), \hat{h}(Q)\right) \implies \theta_{P,Q} \geq 60^\circ.$$

- Substitute the above into

$$\cos\theta_{P,Q} := \frac{\langle P, Q\rangle}{2\|P\|\|Q\|} = \frac{\hat{h}(P-Q)+\hat{h}(P)+\hat{h}(Q)}{2\sqrt{\hat{h}(P)\hat{h}(Q)}}.$$

Quantifying the repulsion – quasi-orthogonality

Proposition (Helfgott/Helfgott–Venkatesh, 2004/2006)

If $P, Q \in E(\mathbb{Z})$ have comparable canonical heights, then

$$\hat{h}(P-Q) \geq (1-\varepsilon)\max\left(\hat{h}(P), \hat{h}(Q)\right) \implies \theta_{P,Q} \geq 60^\circ.$$

- Substitute the above into

$$\cos\theta_{P,Q} := \frac{\langle P, Q\rangle}{2\|P\|\|Q\|} = \frac{\hat{h}(P-Q)+\hat{h}(P)+\hat{h}(Q)}{2\sqrt{\hat{h}(P)\hat{h}(Q)}}.$$

- Contrapositive statement: if the angle between two distinct integral points in the Mordell–Weil lattice is less than 60°, then they cannot have comparable canonical height (so $\hat{h}(P) > C\hat{h}(Q)$ for some large constant C).

  (Compare this statement with Ingram's result!)

Integral points to rational points on elliptic curves

Theorem (Siegel, 1929)

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

- Siegel's theorem: the point of infinity repels integral points.
- This theorem's full version is for S–integral points, so repulsion works for rational points (to certain extent).

  (S–integral points: points whose denominators of the coordinates are divisible by a fixed finite set of primes S)

Integral points to rational points on elliptic curves

Theorem (Siegel, 1929)

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

- Siegel's theorem: the point of infinity repels integral points.
- This theorem's full version is for S–integral points, so repulsion works for rational points (to certain extent).

  (S–integral points: points whose denominators of the coordinates are divisible by a fixed finite set of primes S)
- Claim: the point of infinity is a point like any other point.

Integral points to rational points on elliptic curves

Theorem (Siegel, 1929)

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

- Siegel's theorem: the point of infinity repels integral points.
- This theorem's full version is for S–integral points, so repulsion works for rational points (to certain extent).

  (S–integral points: points whose denominators of the coordinates are divisible by a fixed finite set of primes S)
- Claim: the point of infinity is a point like any other point.

  Can we replace the point of infinity by an arbitrary rational point?

Integral points to rational points on elliptic curves

Conjecture (Everest and Ward, 2011); partial statement

Consider the minimal curve $E\colon y^2 = x^3 + Ax + B$. Let k denote a fixed positive integer. Then the set of rational points on the curve repels the rational points whose denominators have $\leq k$ distinct prime factors.

Integral points to rational points on elliptic curves

Conjecture (Everest and Ward, 2011); partial statement

Consider the minimal curve $E\colon y^2 = x^3 + Ax + B$. Let k denote a fixed positive integer. Then the set of rational points on the curve repels the rational points whose denominators have $\leq k$ distinct prime factors.

Theorem (Everest and Mahé, 2009)

Consider the equation

$$y^2 = x^3 - Nx$$

for some positive integer N. Assume that P and Q are independent rational points with $x(P) < 0$ and $x(Q)$ is a square. Then there are only finitely many points $R \in \langle P, Q \rangle$ for which the denominator of $x(R)$ has exactly one prime factor. More precisely, any such point satisfies the bound

$$\log |x(R)| \ll \log N.$$

References

1. L. Alpöge. The average number of integral points on elliptic curves is bounded. (2014). View online.
2. Everest, G and Ward, T. A repulsion motif in Diophantine equations. American Mathematical Monthly, (2011), 118 (7). 7. pp. 584-598. View online.
3. 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.
4. H. A. Helfgott. On the square-free sieve. Acta Arithmetica 115.4 (2004): 349-402. View online.
5. Hindry, M.; Silverman, J.H. The canonical height and integral points on elliptic curves. Inventiones mathematicae (1998), volume 93; pp. 419 - 450. View online.
6. P. Ingram. Multiples of integral points on elliptic curves. Journal of Number Theory (2009). View online.
7. H. Pasten. Power-saving bounds for Thue–Mahler and Mordell equations. (2026). View online.
8. Silverman, J. H. Advanced topics in the arithmetic of elliptic curves. Springer-Verlag (1994). View online.
9. Silverman, J. H. The arithmetic of elliptic curves. Springer-Verlag (2009). View online.
10. 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.