Integral points on elliptic curves

VaNTAGe seminar

Wei Ho October 13, 2020

$E = E_{A,B}: \quad y^2 = x^3 + Ax + B$ $\qquad A, B \in \cancel{\mathbb{Q}}\ \mathbb{Z}$

discriminant $\Delta_{A,B} = -16(4A^3 + 27B^2) \neq 0$

an elliptic curve $/\mathbb{Q}$ in short Weierstrass form

actually: an integral model for an elliptic curve $/\mathbb{Q}$

note $\quad (A,B)$ and (d^4A, d^6B) for any $d \in \mathbb{Q}^\times$ give isomorphic elliptic curves

$E_{A,B}$ is minimal : $A, B \in \mathbb{Z}$ and if $p^4 \mid A$ for a prime p, then $p^6 \nmid B$

Goal study points on elliptic curves

$E(\mathbb{C}), E(\mathbb{R})$ well understood

previous talks: $E(\mathbb{Q}) \cong \mathbb{Z}^{\text{rank}} \oplus$ (torsion subgp) choice of model irrelevant

today : $E_{A,B}(\mathbb{Z})$ integral points

$\quad = \{(x,y) \in \mathbb{Z}^2 : y^2 = x^3 + Ax + B\}$ depends on integral model!

Rmk almost everything today also works (with appropriate modifications) for

$\mathbb{Q} \rightsquigarrow K$ number field

$\mathbb{Z} \rightsquigarrow \mathcal{O}_K$ ring of integers of K $\rightsquigarrow \mathcal{O}_{K,S}$ S-integers in K

$E_{A,B}(\mathbb{Z}) \rightsquigarrow E_{A,B}(\mathcal{O}_K)$ integral points $\rightsquigarrow E_{A,B}(\mathcal{O}_{K,S})$ S-integral pts

Question How many integral points on $E_{A,B}$?

- Mordell/Siegel: only finitely many (not effective)
- won't get a uniform bound in general $\quad$ e.g. $y^2 = x^3 + d^4Ax + d^6B$ can have more int pts than $E_{A,B}$
- expectation integral points are pretty rare
  shouldn't have any integral points usually?

Question How many integral points on $E_{A,B}$ on average?

as $E_{A,B}$ varies in a family (need to specify ordering)

- 100% of rank 0 elliptic curves have no rational points
- Alpoge (2014): 100% of rank 1 elliptic curves have ≤ 2 integral points
- Bhargava-Shankar (2013): 80% of elliptic curves have rank 0 or 1

⟹ 80% of elliptic curves have ≤ 2 integral points! (⚠ still could have small set of curves w/ lots of points!)

- records Elkies: 10/24/18

The largest count of integral points that I know of (on an elliptic curve in minimal form) is 5620 = 2*2810, for a curve of rank 25.

Question: Are there minimal elliptic curves / $\mathbb{Q}$ with more integral points?

- bounds
  - Helfgott-Venkatesh (2006): $\#E_{A,B}(\mathbb{Z}) \ll O(1)^{\omega(\Delta)} (\log|\Delta|)^2 \cdot 1.33^{\operatorname{rank} E(\mathbb{Q})}$

    $\omega(n) = \#$ of distinct prime factors of n

    dependent on "complexity" and size of disc Δ and rank $E(\mathbb{Q})$

  - Bhargava-Shankar-Taniguchi-Thorne-Tsimerman-Zhao (2017): $\ll O_\varepsilon(|\Delta|^{0.1117\ldots+\varepsilon})$ (improves on [H-V])

for minimal models

- Silverman (1987): $\ll O(1)^{(1+\operatorname{rank} E(\mathbb{Q}))(1+\omega_{ss}(\Delta_{A,B}))}$ — # primes of bad multiplicative reduction (= primes in denom of j-invariant)
- Hindry-Silverman (1988): $\ll O(1)^{(1+\operatorname{rank} E(\mathbb{Q}))\,\sigma_{E/\mathbb{Q}}}$

  $= \dfrac{\log|\Delta|}{\log N_E}$ Szpiro ratio

  ABC ⟹ $\sigma_{E/\mathbb{Q}} < 6 + o(1)$

  so ABC + boundedness of ranks ⟹ uniform bound for minimal curves!

- David (1992): $\ll O(1)^{(1+\operatorname{rank})(\text{linear in } \log \omega_{ss}(\Delta_{A,B}))}$

  (or $O(1)^{(1+\operatorname{rank})(\text{linear in } \log \sigma_{E/\mathbb{Q}})}$ for most curves)

⚠ constants ($O(1)$'s) here are very big! $\sim 10^{10}$

idea: if we want to prove statistical results, e.g. average # integral points, then controlling this constant better could help

(have some control on $(\text{small } \#)^{\operatorname{rank} E}$ on average b/c of Selmer avg results

Theorem 1 (joint w/ L. Alpöge)

$$\# E_{A,B}(\mathbb{Z}) \ll 2^{\operatorname{rank} E_{A,B}(\mathbb{Q})} \prod_{p^2 \mid \Delta_{A,B}} \Big(\underbrace{4 \left\lfloor \tfrac{v_p(\Delta_{A,B})}{2} \right\rfloor}_{\text{can be } 2\cdot 10^7 \text{ if that's smaller}} + 1 \Big)$$

$\ll$ ↑ still big constant but only one

also, if $v_p = 2$ or 3, can use 4

Thm 1 generalized (for S-integral points over # fields K):

$E_{A,B}$: $A, B \in \mathcal{O}_K$, $\Delta_{A,B} \neq 0$

S = finite # of places of K containing all ∞ places and all p s.t. $v_p(\Delta_{A,B}) \geq 2$

$$\Rightarrow \# E_{A,B}(\mathcal{O}_{K,S}) \ll 2^{\operatorname{rank} E_{A,B}(K)} \underset{\uparrow\, 2\cdot 10^7}{C^{|S|}} \, |\mathrm{Cl}(\mathcal{O}_{K,S})[2]|$$

Application

- Thm 1 $\Rightarrow$ control of # integral points in terms of $\sim 2^{\text{rank}}$
- Bhargava-Shankar (2010-): determine average $\mathrm{Sel}_n(E) = 3, 4, 7, 6$ for $n = 2, 3, 4, 5$ resp.

  $$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E) \to Ш(E)[2] \to 0$$ ← we'll use this again later

  $$2^{\operatorname{rank} E(\mathbb{Q})} \leq |E(\mathbb{Q})/2E(\mathbb{Q})| \leq \mathrm{Sel}_2(E)$$

  $\Rightarrow$ control of average 2^{rank} (+ avg $3^{\text{rank}}, 4^{\text{rank}}, 5^{\text{rank}}$)
- $\prod_{p^2 \mid \Delta} \left(4 \left\lfloor \frac{v_p(\Delta)}{2} \right\rfloor + 1 \right)$ shouldn't get too big on average

$\Rightarrow$ on average, # integral points bounded

Theorem 2 (joint w/ Alpöge) let $\mathcal{F}_{\text{univ}} := \{ E_{A,B} : y^2 = x^3 + Ax + B,\ \Delta_{A,B} \neq 0 \}$ ordered by height $H(E_{A,B}) = \max(4|A|^3, 27B^2)$

For $0 < t < \log_2 5 = 2.3219\ldots$,

$$\operatorname*{Avg}_{E_{A,B} \in \mathcal{F}_{\text{univ}}} \left(|E_{A,B}(\mathbb{Z})|^t \right) \ll_t 1 .$$

Remarks

- also can be generalized to other # fields K and S-integral points
- 5 from Bhargava-Shankar's Sel_5 average

  if avg Sel_n bounded, get $t < \log_2 n$
- Alpöge (2014), D. Kim (2015): average ($t=1$) bounded
- "large" families OK, e.g., minimal, semistable, finitely many cong conditions
- other families w/ 3-Sel avgs also may have avg # int pts bounded, e.g., $\mathcal{F}_1$, $\mathcal{F}_0(2)$

Idea of proof of Theorem 1

Mordell (1969): relate integral points on elliptic curves to binary quartics

Binary quartics $f(X,Y) = aX^4 + bX^3Y + cX^2Y^2 + dXY^3 + eY^4$ $\quad a,b,c,d,e \in \mathbb{Q}$

$$SL_2\mathbb{Q} \circlearrowright \mathrm{Sym}^4(\mathbb{Q}^2)$$

poly invariants: $I = 12ae - 3bd + c^2$ deg 2

$J = 72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3$ deg 3

↳ form a polynomial ring generated by I, J

$\Delta(f) = \frac{1}{27}(4I^3 - J^2)$ (integral coeffs)

geometric interp:

$$\left\{ \begin{array}{c} \text{binary quartic forms} / \mathbb{Q} \\ \text{with } \Delta \neq 0 \end{array} \right\} /\sim_{PGL_2\mathbb{Q}} \longleftrightarrow \left\{ \begin{array}{c} \text{genus 1 curves } C/\mathbb{Q} \\ \text{with deg 2 divisor/line bundle } \underset{D}{} \underset{L}{} \end{array} \right\}$$

almost $\mathrm{Sel}_2(E)$ elts!

$f \longmapsto C_f : Z^2 = f(X,Y)$ double cover of $\mathbb{P}^1$

$\mathrm{Jac}(C_f) : y^2 = x^3 - \frac{I}{3}x - \frac{I}{27}$

$C \xrightarrow{|L|} \mathbb{P}^1$ ramification locus of double cover $\longleftrightarrow$ $(C, \underset{D}{L})$

ex $C = E_{A,B}$ with divisor $O + P$ for a point $P = (x_0, y_0) \in E(\mathbb{Q})$

(*) $f(X,Y) = X^4 - 6x_0X^2Y^2 + 8y_0XY^3 + (-4A - 3x_0^2)Y^4$

$I(f) = -48A$ $\qquad$ $J(f) = -1728B$

gives the map $E(\mathbb{Q}) \twoheadrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \mathrm{Sel}_2(E)$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\shortparallel$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ locally soluble (C,L)'s

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ binary quartics/$\mathbb{Q}$

Thm (Mordell) These sets are in bijection:

① integral Weierstrass models $y^2 = x^3 + Ax + B$ with integral point (x_0, y_0)

② binary quartics of the form $X^4 + 6cX^2Y^2 + 8dXY^3 + eY^4$
$c, d, e \in \mathbb{Z}$ $\quad e \equiv c^2 \ (4)$

③ $SL_2\mathbb{Z}$-equiv. classes of (f, p, q)

integer matrix binary quartic $48 \mid I$, $1728 \mid J$ $\quad$ $\in \mathbb{Z}$ with $f(p,q) = 1$

idea not many integer sol^{n}s to Thue equations like $f(X,Y) = 1$

(Evertse: # sol^{n}s $< 2 \cdot 10^7$, Akhtari: ≤ 26 if $\Delta >> 1$)

so want to just bound # of $SL_2\mathbb{Z}$-equiv classes of f's in ③ for given E

almost $Sel_2(E)$ $\quad$ but $SL_2\mathbb{Z}$ and $PGL_2\mathbb{Q}$ not the same

summary

think of as (some) binary quartics

$$\Psi : E_{A,B}(\mathbb{Z}) \hookrightarrow \mathcal{E}(\mathbb{Q}) \longrightarrow \mathcal{E}(\mathbb{Q}) / 2\mathcal{E}(\mathbb{Q}) \hookrightarrow Sel_2(\mathcal{E})$$

$$P = (x_0, y_0) \longmapsto f \text{ from } ⊗$$

integral point $\qquad$ binary quartic

size $\leq 4 \cdot 2^{\text{rank } \mathcal{E}(\mathbb{Q})}$ $\quad$ + $\hookrightarrow$

$\Rightarrow |\text{image}(\Psi)| \leq 4 \cdot 2^{\text{rank } \mathcal{E}(\mathbb{Q})}$

and use Bombieri-Schmidt / Evertse (Diophantine approx)

$$\Rightarrow \text{fibers of } \Psi \ll \prod_{p^2 \mid \Delta} \left(4 \left\lfloor \tfrac{v_p(\Delta)}{2} \right\rfloor + 1\right)$$

$\boxtimes$