

Finding Rational Points on Elliptic Curves

Alan Silvester

PMAT 603.46 Presentation

Background

- Diophantine equations – polynomials equations that we solve for integer or rational solutions
- Common questions we ask: “Are there any solutions?” and “How many solutions?”
- We know the answer for linear and quadratic equations.
- But what about elliptic curves? The integer and rational solutions are not completely understood.

Brief History

Integral solutions

- In the 1920s, Siegel showed an EC has finitely many integral solutions
- In 1970, Baker and Coates gave an explicit upper bound of the largest solution – generally impractical

Rational solutions

- In 1901, Poincaré conjectured \exists a finite generating set for rational solutions
- Conjecture proven in 1923 by Mordell
- Mordell's method *often* allows one to find the generating set, but it hasn't been proven to always work (also conjectured)

Notation

- By elliptic curve I mean $E : y^2 = f(x) = x^3 + ax + b$

Definition 1 *Let E be an elliptic curve and let*

$$E(\mathbb{Q}) = \{(x, y) \in E \mid x, y \in \mathbb{Q}\} \cup \mathcal{O}$$

denote the additive group of rational points.

- Is this really a group?

Recall the group law:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \qquad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1$$

Finite order points

Definition 2 *Let*

$$E[n] = \{P \in E(\mathbb{Q}) \mid [n]P = \mathcal{O}\}$$

be the n -torsion subgroup of $E(\mathbb{Q})$.

- Using rational coordinates, $E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2$, or $\{0\}$ depending on whether $f(x)$ has 3, 1, or 0 rational roots.
- Using the point doubling formula, we can show that $E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ or $\{0\}$. These points correspond to inflection points

Discriminants and Integral Coordinates

Definition 3 For an elliptic curve E , the discriminant is $\Delta = -4a^3 - 27b^2 \neq 0$.

Claim 1 If $P = (x, y) \in E$ is a rational point of finite order then $x, y \in \mathbb{Z}$.

- The proof of this claim uses the p -adic valuation to show that there is no prime dividing the denominator of x, y and so they must be integers (ie: the denominator is 1).

Nagell-Lutz Theorem

Theorem 1 (Nagell-Lutz) *Let E be an elliptic curve with $a, b \in \mathbb{Z}$. If $P = (x, y)$ is a rational point of finite order then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y \mid \Delta$.*

- In computations, one often uses a strengthened version of this theorem which states that if $\text{ord}(P) \neq 2$ then $y^2 \mid \Delta$.
- We can use Nagell-Lutz to show a point has infinite order. Taking P , we can compute the x coordinate of $2P, 4P, 8P, \dots$. If $[n]P$ ever has an x coordinate that isn't an integer then nP and hence P can't have finite order.

Example # 1

Let $E : y^2 = x^3 + 8$.

- The discriminant is $\Delta = -1728$
- If $y = 0$ then $x = -2$ is the only solution
- Suppose $y \neq 0$. Then $y^2 \mid -1728 \Rightarrow y \mid -24$
- Testing all possibilities gives: $(1, \pm 3)$ and $(2, \pm 4)$. But

$$[2](1, 3) = \left(\frac{-7}{4}, \frac{-13}{8} \right) \quad [2](2, 4) = \left(\frac{-7}{4}, \frac{13}{8} \right)$$

So $(1, \pm 3), (2, \pm 4)$ can't have finite order

- Thus $T = \{\mathcal{O}, (-2, 0)\} \cong \mathbb{Z}_2$

Example # 2

Let $E : y^2 = x^3 + 4$.

- The discriminant is $\Delta = -432$
- If $y = 0$ then $x^3 + 4 = 0$ has no rational solutions
- Suppose $y \neq 0$. Then $y^2 \mid -432 \Rightarrow y \mid -12$. ie:

$$y \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

- Testing all possibilities gives: $(0, \pm 2)$. A quick calculation shows $[3](0, \pm 2) = \mathcal{O}$.
- Thus $E(\mathbb{Q}) = \{\mathcal{O}, (0, \pm 2)\} \cong \mathbb{Z}_3$

A Corollary and Finite Orders

Corollary 1 *The torsion subgroup T of $E(\mathbb{Q})$ is finite.*

- This follows because there are only finitely many divisors of the discriminant Δ .
- So what finite orders are possible?
- For $t \neq 0, 1/4$, the point $P = (t, t)$ has order 4 on

$$y^2 = x^3 - (2t - 1)x^2 + t^2x$$

- Through the mid- to late-1800s, families of curves with points of order 5, 6, 7, 8, 9, 10, and 12 were found.
- Around 1940, Billing and Mahler showed that there were no elliptic curves with a point of order 11

Mazur's Theorem

Theorem 2 (Mazur's Theorem) *Let E be an elliptic curve and suppose P is a point of finite order m . Then $1 \leq m \leq 10$ or $m = 12$. Moreover, the torsion subgroup T is isomorphic to one of the following*

- \mathbb{Z}_n for $1 \leq n \leq 10$ or $n = 12$
- $\mathbb{Z}_2 \times \mathbb{Z}_{2n}$ for $1 \leq n \leq 4$

2-Descent

- Suppose our EC is of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$ for distinct $e_i \in \mathbb{Z}$.
- If $y = 0$ then $x = e_i$ are the only rational points.
- Suppose $y \neq 0$. Then the RHS of the equation is equal to a square. Intuitively, each factor should then be close to a square
- For $a, b, c, u, v, w \in \mathbb{Q}$ write

$$x - e_1 = au^2 \quad x - e_2 = bv^2 \quad x - e_3 = cw^2$$

so that

$$y^2 = (x - e_1)(x - e_2)(x - e_3) = au^2 \cdot bv^2 \cdot cw^2 = abc(uvw)^2$$

- WLOG, we can assume a, b, c are squarefree

Working mod $\mathbb{Q}^{\times 2}$

Claim 2 *Let $S = \{p \mid p \text{ prime}, p \mid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}$. If p is prime and $p \mid abc$ then $p \in S$.*

- S is finite (there's only so many divisors), so there are only finitely many possibilities for (a, b, c)
- We'd like to show these finitely many combinations come from points (x, y) that form a group mod squares

Definition 4 *Let $\mathbb{Q}^{\times} / \mathbb{Q}^{\times 2}$ denote the group of rational numbers modulo squares.*

Definition 5 *Let $x \neq y \in \mathbb{Q}$. We say x and y are equivalent modulo squares if they differ by a square. In other words,*

$$x \equiv y \pmod{\mathbb{Q}^{\times 2}} \quad \text{iff} \quad \exists t \in \mathbb{Q} \text{ s.t. } x = t^2 y$$

Useful Homomorphism

Theorem 3 *Let $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ be an elliptic curve where e_i are distinct. Then*

$$\begin{aligned}\varphi : E(\mathbb{Q}) &\rightarrow \left(\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \right) \oplus \left(\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \right) \oplus \left(\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \right) \\ (x, y) &\mapsto (x - e_1, x - e_2, x - e_3) \\ \mathcal{O} &\mapsto (1, 1, 1) \\ (e_1, 0) &\mapsto ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3) \\ (e_2, 0) &\mapsto (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3) \\ (e_3, 0) &\mapsto (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2))\end{aligned}$$

is a homomorphism with $\ker(\varphi) = 2E(\mathbb{Q})$.

Mordell-Weil Theorems

Theorem 4 (Weak Mordell-Weil Theorem) *Let E be an elliptic curve. $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.*

- The weak Mordell-Weil theorem is a corollary to the homomorphism theorem on the previous slide

Theorem 5 (Mordell-Weil Theorem) *Let E be an elliptic curve. $E(\mathbb{Q})$ is a finitely generated abelian group. Thus*

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$$

where T is the torsion subgroup and $r \in \mathbb{Z}^+$ is the rank.

Descent Theorem

Definition 6 Let $r = a/b \in \mathbb{Q}$ be in lowest terms. The logarithmic height function is $h(r) = \log \max \{ |a|, |b| \}$.

Theorem 6 Let Γ be a commutative group and suppose that there is a function $\lambda : \Gamma \rightarrow [0, \infty)$ with the following three properties:

- For every real number C , the set $\{P \in \Gamma \mid \lambda(P) \leq C\}$ is finite.
- For every $P_0 \in \Gamma$, there is a constant κ_0 such that $\lambda(P + P_0) \leq 2\lambda(P) + \kappa_0$ for all $P \in \Gamma$.
- There is a constant κ_1 such that $\lambda(2P) \geq 4\lambda(P) - \kappa_1$ for all $P \in \Gamma$.

Suppose further that the subgroup 2Γ has finite index in Γ . Then Γ is finitely generated.

Example

Let $E : y^2 = x^3 - 25x$.

- If $y = 0$ then $x^3 - 25x = x(x + 5)(x - 5) = 0$. So $(0, 0)$ and $(\pm 5, 0)$ are points of order 2.
- Notice $(-4, 6)$ satisfies E and $[2](-4, 6) = \left(\frac{41^2}{12^2}, \frac{-62279}{1728}\right)$
- Nagell-Lutz gives us $T \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Recall our homomorphism $\varphi : (x, y) \mapsto (x, x - 5, x + 5)$. So $\varphi(-4, 6) = (-1, -1, 1)$ and also

$$\begin{aligned}\varphi(\mathcal{O}) &= (1, 1, 1) & \varphi(0, 0) &= (-1, -5, 5) \\ \varphi(5, 0) &= (5, 2, 10) & \varphi(-5, 0) &= (-5, -10, 2)\end{aligned}$$

Example (cont.)

Since φ is a homomorphism, $\varphi(-4, 6)$ times any of those above points is also in $Im(\varphi)$. So there are points such that

$$(1, 5, 5), (-5, -2, 10), (5, 10, 1) \in Im(\varphi)$$

Write

$$x = au^2 \quad x - 5 = bv^2 \quad x + 5 = cw^2$$

- From our claim, $a, b, c \in \{\pm 1, \pm 2, \pm 5, \pm 10\} \pmod{\mathbb{Q}^{\times 2}}$
- Since abc is square, a, b determine c
- There are 64 pairs possible for a, b . We've found 8 so far

$$L = \{(1, 1), (1, 5), (-1, -1), (-1, -5), (5, 2), (5, 10), (-5, -2), (-5, -10)\}$$

We want to eliminate the remaining 56 possibilities

Example (cont.)

Note that $x - 5 < x < x + 5 \Rightarrow bv^2 < au^2 < cw^2$. Without too much work, we see a, b must have the same sign. So we have 32 possibilities left. Consider $(a, b) = (2, 1)$. Then

$$x = 2u^2 \quad x - 5 = 1v^2 \quad x + 5 = 2w^2$$

and so $2u^2 - v^2 = 5$ and $2w^2 - 2u^2 = 5$.

- We can use some clever arguments to show u, v must have odd denominators and then consider them mod powers of 2. This will show $(a, b) = (2, 1)$ is impossible.
- Working mod powers of 5 shows $(a, b) = (5, 1)$ and $(10, 1)$ are also impossible. These and φ being a homomorphism eliminate the remaining 24 cases
- Hence $E(\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}$

Harder Examples

Consider $E : y^2 = x^3 + 877x$. It has rank 1, but $E(\mathbb{Q})$ is generated by $(0, 0)$ and the point with x coordinate

$$x = \left(\frac{612, 776, 083, 187, 947, 368, 101}{7, 884, 153, 586, 063, 900, 210} \right)^2$$

In 2000, Martin-McMillen showed

$$y^2 + xy + y = x^3 - 120039822036992245303534619191166796374x + 504224992484910670010801799168082726759443756222911415116$$

has $E(\mathbb{Q}) \cong \{0\} \oplus \mathbb{Z}^{24}$.

Birch and Swinnerton-Dyer Conjecture

Let E be an elliptic curve, $s \in \mathbb{C}$, and p be prime. Also let

$$N_p = | \{ \text{solutions of } y^2 = x^3 + ax + b \pmod{p} \} |$$

and $a_p = p - N_p$.

Definition 7 *The incomplete L-series of E is*

$$L(E, s) = \prod_{p \nmid 2\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

- Known to converge for $\Re(s) > 3/2$
- Hasse conjectured that $L(E, s)$ had an analytic continuation to the entire complex plane
 - This conjecture has been proven

Birch and Swinnerton-Dyer Conjecture

Recall

$$L(E, s) = \prod_{p \nmid 2\Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

Conjecture 1 *The Taylor expansion of $L(E, s)$ at $s = 1$ has the form $L(E, s) = c(s - 1)^r + \text{higher order terms}$ with $c \neq 0$ and $r = \text{rank}(E(\mathbb{Q}))$.*

The conjecture asserts that $L(E, s) = 0$ iff $E(\mathbb{Q})$ is infinite. Consider the completed L -series of E , denoted $L^*(E, s)$. Then a refined form of the conjecture states that

$$L^*(E, s) \sim c^*(s - 1)^r \quad \text{where} \quad c^* = |\text{III}(E)| R_\infty w_\infty \prod_{p|2\Delta} \frac{w_p}{|T|^2}$$

Conclusions

- $E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$
- Computing T is relatively easy
- Computing r and the generators of $E(\mathbb{Q})$ is much harder
- p -descent usually works well when a, b are not too large
 - Success depends on a conjecture that $\text{III}(E)$ is finite
- Hard to find curves with a large rank
 - Open problem: Given a fixed r , does there exist an EC with rank r ?

Conclusion

Finding Rational Points on Elliptic Curves

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$$

\uparrow \uparrow
Easy Hard