How to compute the rank of an elliptic curve in polynomial time

Simon Spicer

PhD Thesis Defense
University of Washington

mlungu@uw.edu

May 12, 2015

Motivation

Motivation

Definition

A Diophantine equation is an equation in n variables with integer coefficients.

Hilbert's 10th Problem

Does a general algorithm exist to determine if a given Diophantine equation has a solution in $\mathbb{Z}$?

Motivation

Definition

A Diophantine equation is an equation in n variables with integer coefficients.

Hilbert's 10th Problem

Does a general algorithm exist to determine if a given Diophantine equation has a solution in $\mathbb{Z}$?

Theorem (Davis, Matiyasevich, Putnam, Robinson 1970)

No.

Motivation

Motivation

Slightly simpler question:

Does $\exists$ an algorithm to determine if $P(x, y) = 0$ has a solution in $\mathbb{Q}$?

Motivation

Slightly simpler question:

Does $\exists$ an algorithm to determine if $P(x, y) = 0$ has a solution in $\mathbb{Q}$?

We don't know.

Motivation

Slightly simpler question:

Does $\exists$ an algorithm to determine if $P(x, y) = 0$ has a solution in $\mathbb{Q}$?

We don't know.

If yes $\implies$ lots of mathematicians out of work!

Motivation

Motivation

Modern view: $P(x, y) = 0$ represents an *algebraic curve*.

Motivation

Modern view: $P(x, y) = 0$ represents an *algebraic curve*.
Classify curves by *genus* – "the number of holes in $C(\mathbb{C})$":

Motivation

Modern view: $P(x, y) = 0$ represents an *algebraic curve*.
Classify curves by *genus* – "the number of holes in $C(\mathbb{C})$":

g	# Solutions in $\mathbb{Q}$
0	$< \infty$ or $\sim \mathbb{Z}$
1	$< \infty$ or $\hookleftarrow \mathbb{Z}^r$ for $r \gg 0$
≥ 2	$< \infty$ (Falting's Theorem 1983)

Motivation

Modern view: $P(x, y) = 0$ represents an *algebraic curve*.
Classify curves by *genus* – "the number of holes in $C(\mathbb{C})$":

g	# Solutions in $\mathbb{Q}$
0	$< \infty$ or $\sim \mathbb{Z}$
1	$< \infty$ or $\hookleftarrow \mathbb{Z}^r$ for $r \gg 0$
≥ 2	$< \infty$ (Falting's Theorem 1983)

$\Longrightarrow$ Genus 1 curves most interesting case!

Motivation

Modern view: $P(x, y) = 0$ represents an *algebraic curve*.
Classify curves by *genus* – "the number of holes in $C(\mathbb{C})$":

g	# Solutions in $\mathbb{Q}$
0	$< \infty$ or $\sim \mathbb{Z}$
1	$< \infty$ or $\hookleftarrow \mathbb{Z}^r$ for $r \gg 0$
≥ 2	$< \infty$ (Falting's Theorem 1983)

$\implies$ Genus 1 curves most interesting case!

This talk: how to compute that r.

Elliptic Curves

Definition

An elliptic curve E is a smooth projective genus 1 algebraic curve with a marked point $\mathcal{O}$.

Elliptic Curves

Definition

An elliptic curve E is a smooth projective genus 1 algebraic curve with a marked point $\mathcal{O}$.

For This Talk:

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

Elliptic Curves

Definition

An elliptic curve E is a smooth projective genus 1 algebraic curve with a marked point $\mathcal{O}$.

For This Talk:

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

Example

$$E = 37a : y^2 = x^3 - 16x + 16$$

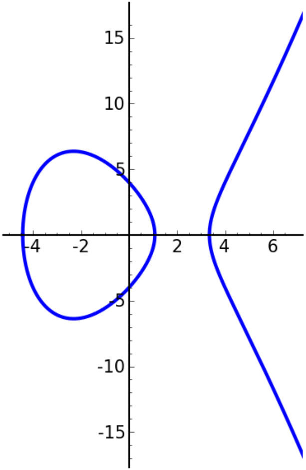

Figure: The Elliptic Curve $37a$

Elliptic Curves

Definition

An elliptic curve E is a smooth projective genus 1 algebraic curve with a marked point $\mathcal{O}$.

For This Talk:

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

Example

$$E = 37a : y^2 = x^3 - 16x + 16$$

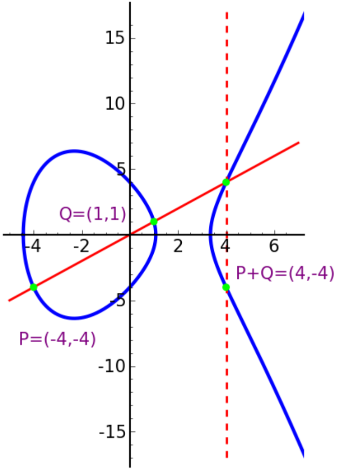

Figure: The Elliptic Curve 37*a*

$E(\mathbb{Q})$ as a group

Theorem (Mordell 1922, Weil 1928)

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{TOR} \times \mathbb{Z}^r$$

where $E(\mathbb{Q})_{TOR}$ is a finite abelian group, and $r \in \mathbb{Z}_{\geq 0}$ is the algebraic rank of $E/\mathbb{Q}$.

$E(\mathbb{Q})$ as a group

Theorem (Mordell 1922, Weil 1928)

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{TOR} \times \mathbb{Z}^r$$

where $E(\mathbb{Q})_{TOR}$ is a finite abelian group, and $r \in \mathbb{Z}_{\geq 0}$ is the algebraic rank of $E/\mathbb{Q}$.

Example

For $E = 37a$, we have $E(\mathbb{Q}) \approx \mathbb{Z}^1$, generated by $P = (0,4)$:

n	0	1	2	3	4	5	6
nP	$\mathcal{O}$	$(0,4)$	$(4,4)$	$(-4,-4)$	$(8,-20)$	$(1,-1)$	$(24,116)$

n	7	8	9
nP	$\left(-\frac{20}{9}, \frac{172}{27}\right)$	$\left(\frac{84}{25}, -\frac{52}{125}\right)$	$\left(-\frac{80}{49}, -\frac{2108}{343}\right)$

$E(\mathbb{Q})$ as a group

Theorem (Mordell 1922, Weil 1928)

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{TOR} \times \mathbb{Z}^r$$

$E(\mathbb{Q})$ as a group

Theorem (Mordell 1922, Weil 1928)

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{TOR} \times \mathbb{Z}^r$$

Torsion is well understood:

Theorem (Mazur 1978)

$$E(\mathbb{Q})_{TOR} \approx \mathbb{Z}/n\mathbb{Z} \quad \text{for } 1 \leq n \leq 10 \text{ or } 12$$

or

$$E(\mathbb{Q})_{TOR} \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \text{for } 1 \leq n \leq 4$$

$E(\mathbb{Q})$ as a group

Theorem (Mordell 1922, Weil 1928)

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{TOR} \times \mathbb{Z}^r$$

Torsion is well understood:

Theorem (Mazur 1978)

$$E(\mathbb{Q})_{TOR} \approx \mathbb{Z}/n\mathbb{Z} \quad \textit{for } 1 \le n \le 10 \textit{ or } 12$$

or

$$E(\mathbb{Q})_{TOR} \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \textit{for } 1 \le n \le 4$$

The free part is less well understood.

$E(\mathbb{Q})$ as a group

Theorem (Mordell 1922, Weil 1928)

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{TOR} \times \mathbb{Z}^r$$

Torsion is well understood:

Theorem (Mazur 1978)

$$E(\mathbb{Q})_{TOR} \approx \mathbb{Z}/n\mathbb{Z} \quad \textit{for } 1 \leq n \leq 10 \textit{ or } 12$$

or

$$E(\mathbb{Q})_{TOR} \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \textit{for } 1 \leq n \leq 4$$

The free part is less well understood.
Open question: do there exist $E/\mathbb{Q}$ with arbitrarily large r?

Motivating Question

Motivating Question

Does an algorithm exist to compute rank$(E(\mathbb{Q}))$?

Motivating Question

Does an algorithm exist to compute rank$(E(\mathbb{Q}))$?

- Unconditional answer is an open question.

Motivating Question

Does an algorithm exist to compute $\text{rank}(E(\mathbb{Q}))$?

- Unconditional answer is an open question.
- Manin (1970s): Assuming BSD Conjecture, yes:

Motivating Question

Does an algorithm exist to compute rank($E(\mathbb{Q})$)?

- Unconditional answer is an open question.
- Manin (1970s): Assuming BSD Conjecture, yes:
    1. By day, bound rank from above using analytic methods

Motivating Question

Does an algorithm exist to compute $\text{rank}(E(\mathbb{Q}))$?

- Unconditional answer is an open question.
- Manin (1970s): Assuming BSD Conjecture, yes:
  1. By day, bound rank from above using analytic methods
  2. By night, bound rank from below using algebraic methods

Motivating Question

Does an algorithm exist to compute rank$(E(\mathbb{Q}))$?

- Unconditional answer is an open question.
- Manin (1970s): Assuming BSD Conjecture, yes:
  1. By day, bound rank from above using analytic methods
  2. By night, bound rank from below using algebraic methods
  3. Eventually the two bounds match up, and you have computed rank

Motivating Question

Does an algorithm exist to compute rank$(E(\mathbb{Q}))$?

- Unconditional answer is an open question.
- Manin (1970s): Assuming BSD Conjecture, yes:
  1. By day, bound rank from above using analytic methods
  2. By night, bound rank from below using algebraic methods
  3. Eventually the two bounds match up, and you have computed rank
- Problem: how long does this method take? Can we quantify 'eventually'?

A Better Question

A better question would be:

A Better Question

A better question would be:

Motivating Question

Let $r = \text{rank}(E(\mathbb{Q}))$. Does an algorithm exist to determine r whose runtime can be proven to scale in a quantifiable way with the arithmetic complexity of the E?

A Better Question

A better question would be:

Motivating Question

Let $r = \text{rank}(E(\mathbb{Q}))$. Does an algorithm exist to determine r whose runtime can be proven to scale in a quantifiable way with the arithmetic complexity of the E?

- Want to show runtime $= O(\text{something})$

A Better Question

A better question would be:

Motivating Question

Let $r = \text{rank}(E(\mathbb{Q}))$. Does an algorithm exist to determine r whose runtime can be proven to scale in a quantifiable way with the arithmetic complexity of the E?

- Want to show runtime $= O(\text{something})$
- What "something" measures arithmetic complexity?

The Main Theorem

Main Theorem

Theorem (S.)

Let $E/\mathbb{Q}$ have conductor N_E and rank r.

- *Assuming the BSD and ABC conjectures, there exists an algorithm to compute r in $\tilde{O}\left(\sqrt{N_E}\right)$ time.*
- *The algorithm can be sped up by a constant factor if one further assumes the Generalized Riemann Hypothesis.*

Main Theorem

Theorem (S.)

Let $E/\mathbb{Q}$ have conductor N_E and rank r. Assuming BSD, ABC and optionally GRH, there exists an algorithm to compute r in $\tilde{O}\left(\sqrt{N_E}\right)$ time.

Main Theorem

Theorem (S.)

Let $E/\mathbb{Q}$ have conductor N_E and rank r. Assuming BSD, ABC and optionally GRH, there exists an algorithm to compute r in $\tilde{O}\left(\sqrt{N_E}\right)$ time.

Algorithm: compute the rank of an elliptic curve

Given $E/\mathbb{Q}$ (represented by a minimal Weierstrass equation) with conductor N_E:

Main Theorem

Theorem (S.)

Let $E/\mathbb{Q}$ have conductor N_E and rank r. Assuming BSD, ABC and optionally GRH, there exists an algorithm to compute r in $\tilde{O}\left(\sqrt{N_E}\right)$ time.

Algorithm: compute the rank of an elliptic curve

Given $E/\mathbb{Q}$ (represented by a minimal Weierstrass equation) with conductor N_E:

1. Compute the real period Ω_E of E.

Main Theorem

Theorem (S.)

Let $E/\mathbb{Q}$ have conductor N_E and rank r. Assuming BSD, ABC and optionally GRH, there exists an algorithm to compute r in $\tilde{O}\left(\sqrt{N_E}\right)$ time.

Algorithm: compute the rank of an elliptic curve

Given $E/\mathbb{Q}$ (represented by a minimal Weierstrass equation) with conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$, and set $m = 0$.
   (If GRH: set $k = \lceil 24 + 2.43 \log_2 N_E - \log_2 \Omega_E \rceil$ instead)

Main Theorem

Theorem (S.)

Let $E/\mathbb{Q}$ have conductor N_E and rank r. Assuming BSD, ABC and optionally GRH, there exists an algorithm to compute r in $\tilde{O}\left(\sqrt{N_E}\right)$ time.

Algorithm: compute the rank of an elliptic curve

Given $E/\mathbb{Q}$ (represented by a minimal Weierstrass equation) with conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$, and set $m = 0$. (If GRH: set $k = \lceil 24 + 2.43 \log_2 N_E - \log_2 \Omega_E \rceil$ instead)
3. Output $r =$ index of the first Taylor coefficient of the $L_E(s)$ at $s = 1$ that isn't zero to k bits precision.

What do all those symbols mean?

Algorithm: compute the rank of an elliptic curve (BSD, ABC, (GRH))

Given $E/\mathbb{Q}$ with conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$, and set $m = 0$.
(If GRH: set $k = \lceil 24 + 2.43 \log_2 N_E - \log_2 \Omega_E \rceil$ instead)
3. Output $r =$ index of the first Taylor coefficient of the $L_E(s)$ at $s = 1$ that isn't zero to k bits precision.

What do all those symbols mean?

Algorithm: compute the rank of an elliptic curve (BSD, ABC, (GRH))

Given $E/\mathbb{Q}$ with conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 36 + 3.8\log_2 N_E - \log_2 \Omega_E \rceil$, and set $m = 0$.
   (If GRH: set $k = \lceil 24 + 2.43\log_2 N_E - \log_2 \Omega_E \rceil$ instead)
3. Output $r =$ index of the first Taylor coefficient of the $L_E(s)$ at $s = 1$ that isn't zero to k bits precision.

- What is N_E?

What do all those symbols mean?

Algorithm: compute the rank of an elliptic curve (BSD, ABC, (GRH))

Given $E/\mathbb{Q}$ with conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$, and set $m = 0$. (If GRH: set $k = \lceil 24 + 2.43 \log_2 N_E - \log_2 \Omega_E \rceil$ instead)
3. Output $r =$ index of the first Taylor coefficient of the $L_E(s)$ at $s = 1$ that isn't zero to k bits precision.

- What is N_E?
- What is the $L_E(s)$?

What do all those symbols mean?

Algorithm: compute the rank of an elliptic curve (BSD, ABC, (GRH))

Given $E/\mathbb{Q}$ with conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$, and set $m = 0$.
   (If GRH: set $k = \lceil 24 + 2.43 \log_2 N_E - \log_2 \Omega_E \rceil$ instead)
3. Output r = index of the first Taylor coefficient of the $L_E(s)$ at $s = 1$ that isn't zero to k bits precision.

- What is N_E?
- What is the $L_E(s)$?
- What are BSD, ABC and GRH?

What do all those symbols mean?

Algorithm: compute the rank of an elliptic curve (BSD, ABC, (GRH))

Given $E/\mathbb{Q}$ with conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$, and set $m = 0$.
   (If GRH: set $k = \lceil 24 + 2.43 \log_2 N_E - \log_2 \Omega_E \rceil$ instead)
3. Output $r =$ index of the first Taylor coefficient of the $L_E(s)$ at $s = 1$ that isn't zero to k bits precision.

- What is N_E?
- What is the $L_E(s)$?
- What are BSD, ABC and GRH?
- What is Ω_E?

The Conductor N_E and L-function $L_E(s)$

The Conductor of a Curve

The Conductor of a Curve

Reducing a curve modulo p can produce a singular curve; happens only for finitely many p.

The Conductor of a Curve

Reducing a curve modulo p can produce a singular curve; happens only for finitely many p.

Definition

The conductor of E is $N_E = \prod_p p^{f_p(E)}$, where

$$f_p(E) = \begin{cases} 0, & \text{good reduction at } p \\ 1, & \text{mult. reduction at } p \\ 2, & \text{add. reduction at } p, \end{cases}$$

for $p \neq 2, 3$ and possibly more for 2 and 3.

The Conductor of a Curve

Reducing a curve modulo p can produce a singular curve; happens only for finitely many p.

Definition

The conductor of E is $N_E = \prod_p p^{f_p(E)}$, where

$$f_p(E) = \begin{cases} 0, & \text{good reduction at } p \\ 1, & \text{mult. reduction at } p \\ 2, & \text{add. reduction at } p, \end{cases}$$

for $p \neq 2, 3$ and possibly more for 2 and 3.

Example

The conductor of $37a$ is $N_E = 37$, hence its name.

Elliptic Curve L-Functions

Elliptic Curve L-Functions

Definition

- For p prime with $p \nmid N_E$, $a_p(E) = a_p := p + 1 - \#E(\mathbb{F}_p)$
- For $p \mid N_E$, $a_p := 0, 1$ or -1 depending on reduction type.

Elliptic Curve L-Functions

Definition

- For p prime with $p \nmid N_E$, $a_p(E) = a_p := p + 1 - \#E(\mathbb{F}_p)$
- For $p \mid N_E$, $a_p := 0, 1$ or -1 depending on reduction type.

Definition

The L-function attached to E is

$$L_E(s) := \prod_{p \mid N_E} \frac{1}{1 - a_p p^{-s}} \prod_{p \nmid N_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n=1}^{\infty} a_n n^{-s}$$

for $\Re(s) > \frac{3}{2}$.

Elliptic Curve L-Functions

Definition

- For p prime with $p \nmid N_E$, $a_p(E) = a_p := p + 1 - \#E(\mathbb{F}_p)$
- For $p \mid N_E$, $a_p := 0, 1$ or -1 depending on reduction type.

Definition

The L-function attached to E is

$$L_E(s) := \prod_{p|N_E} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid N_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n=1}^{\infty} a_n n^{-s}$$

for $\Re(s) > \frac{3}{2}$.

The a_n are defined by multiplying out the Euler product.

Modularity & Analytic Continuation of $L_E(s)$

Theorem (Breuille, Conrad, Diamond, Taylor, Wiles et al., 1999,2001)

$L_E(s)$ extends to an entire function on $\mathbb{C}$.

Modularity & Analytic Continuation of $L_E(s)$

Theorem (Breuille, Conrad, Diamond, Taylor, Wiles et al., 1999,2001)

$L_E(s)$ extends to an entire function on $\mathbb{C}$.

Theorem (Bradshaw 2010)

$L_E(s)$ can be provably evaluated to k bits precision in $\tilde{O}(k \cdot \sqrt{N_E})$ time near $s = 1$.

Modularity & Analytic Continuation of $L_E(s)$

Theorem (Breuille, Conrad, Diamond, Taylor, Wiles et al., 1999,2001)

$L_E(s)$ extends to an entire function on $\mathbb{C}$.

Theorem (Bradshaw 2010)

$L_E(s)$ can be provably evaluated to k bits precision in $\tilde{O}(k \cdot \sqrt{N_E})$ time near $s = 1$.

$\tilde{O}(k \cdot \sqrt{N_E})$ time:

time taken to evaluate $L_E(s)$ near $s = 1$ scales with (number of bits of precision) $\times \sqrt{N_E} \times$ (some power of $\log N_E$).

The Zeros of $L_E(s)$

Three flavors:

- A simple zero at $0, -1, -2, -3, \ldots$
- A zero of order r_{an} at $s = 1$; r_{an} is called the *analytic rank* of E
- Countably infinite zeros in the strip $0 < \Re(s) < 2$, symmetric about $\Re(s) = 1$ and x-axis.

The Zeros of $L_E(s)$

Three flavors:

- A simple zero at $0, -1, -2, -3, \ldots$
- A zero of order r_{an} at $s = 1$; r_{an} is called the *analytic rank* of E
- Countably infinite zeros in the strip $0 < \Re(s) < 2$, symmetric about $\Re(s) = 1$ and x-axis.

Generalized Riemann Hypothesis for Elliptic Curves (GRH)

All nontrivial zeros of $L_E(s)$ lie on the line $\Re(s) = 1$.

The Zeros of $L_E(s)$

Three flavors:

- A simple zero at $0, -1, -2, -3, \ldots$
- A zero of order r_{an} at $s = 1$; r_{an} is called the *analytic rank* of E
- Countably infinite zeros in the strip $0 < \Re(s) < 2$, symmetric about $\Re(s) = 1$ and x-axis.

Generalized Riemann Hypothesis for Elliptic Curves (GRH)

All nontrivial zeros of $L_E(s)$ lie on the line $\Re(s) = 1$.

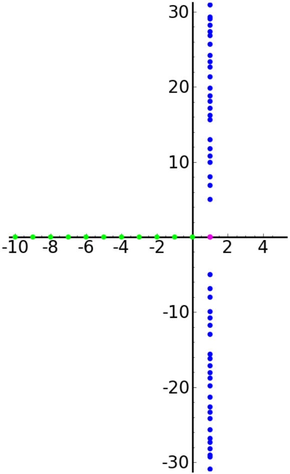

Figure: The zeros of $L_E(s)$ for $E = 37a$

The BSD Conjecture

Conjecture (Birch, Swinnerton-Dyer 1960s)

- *Algebraic rank = analytic rank*

The BSD Conjecture

Conjecture (Birch, Swinnerton-Dyer 1960s)

- *Algebraic rank = analytic rank*
- *The leading Taylor coefficient of $L_E(s)$ at $s = 1$ is*

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{Tor}(\mathbb{Q}))^2}$$

The BSD Conjecture

Conjecture (Birch, Swinnerton-Dyer 1960s)

- *Algebraic rank = analytic rank*
- *The leading Taylor coefficient of* $L_E(s)$ *at* $s = 1$ *is*

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{Tor}(\mathbb{Q}))^2}$$

where

- Ω_E *is the real period of* E,
- Reg_E *is the regulator of* E,
- $\#E_{Tor}(\mathbb{Q})$ *is the number of rational torsion points on* E.

The Leading Taylor Coefficient

Let C_E be the leading Taylor coefficient of $L_E(s)$ at $s=1$.

$$\text{BSD}: \quad C_E = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\mathrm{Tor}}(\mathbb{Q}))^2}$$

The Leading Taylor Coefficient

Let C_E be the leading Taylor coefficient of $L_E(s)$ at $s = 1$.

$$\text{BSD}: \quad C_E = \frac{\Omega_E \cdot \text{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\text{Tor}}(\mathbb{Q}))^2}$$

Corollary

$$C_E \geq \frac{\Omega_E \cdot \text{Reg}_E}{256}$$

as $\#\text{Ш}(E/\mathbb{Q}) \geq 1$, $\prod_p c_p \geq 1$ *and by Mazur's Theorem,* $\#E_{Tor}(\mathbb{Q}) \leq 16$

The Leading Taylor Coefficient

Let C_E be the leading Taylor coefficient of $L_E(s)$ at $s = 1$.

$$\text{BSD}: \quad C_E = \frac{\Omega_E \cdot \text{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\text{Tor}}(\mathbb{Q}))^2}$$

Corollary

$$C_E \geq \frac{\Omega_E \cdot \text{Reg}_E}{256}$$

as $\#\text{Ш}(E/\mathbb{Q}) \geq 1$, $\prod_p c_p \geq 1$ *and by Mazur's Theorem,* $\#E_{Tor}(\mathbb{Q}) \leq 16$

Method for proof of main theorem:

The Leading Taylor Coefficient

Let C_E be the leading Taylor coefficient of $L_E(s)$ at $s = 1$.

$$\text{BSD}: \quad C_E = \frac{\Omega_E \cdot \text{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\text{Tor}}(\mathbb{Q}))^2}$$

Corollary

$$C_E \geq \frac{\Omega_E \cdot \text{Reg}_E}{256}$$

as $\#\text{Ш}(E/\mathbb{Q}) \geq 1$, $\prod_p c_p \geq 1$ *and by Mazur's Theorem,* $\#E_{Tor}(\mathbb{Q}) \leq 16$

Method for proof of main theorem:

- Show that BSD+ABC$\Rightarrow$ lower bounds exist for Ω_E and Reg_E

The Leading Taylor Coefficient

Let C_E be the leading Taylor coefficient of $L_E(s)$ at $s = 1$.

$$\text{BSD}: \quad C_E = \frac{\Omega_E \cdot \text{Reg}_E \cdot \#Ш(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\text{Tor}}(\mathbb{Q}))^2}$$

Corollary

$$C_E \geq \frac{\Omega_E \cdot \text{Reg}_E}{256}$$

as $\#Ш(E/\mathbb{Q}) \geq 1$, $\prod_p c_p \geq 1$ *and by Mazur's Theorem,* $\#E_{Tor}(\mathbb{Q}) \leq 16$

Method for proof of main theorem:

- Show that BSD+ABC$\Rightarrow$ lower bounds exist for Ω_E and Reg_E
- Thus C_E cannot be too small in terms of N_E

The Leading Taylor Coefficient

Let C_E be the leading Taylor coefficient of $L_E(s)$ at $s = 1$.

$$\text{BSD}: \quad C_E = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\mathrm{Tor}}(\mathbb{Q}))^2}$$

Corollary

$$C_E \geq \frac{\Omega_E \cdot \mathrm{Reg}_E}{256}$$

as $\#\text{Ш}(E/\mathbb{Q}) \geq 1$, $\prod_p c_p \geq 1$ *and by Mazur's Theorem,* $\#E_{Tor}(\mathbb{Q}) \leq 16$

Method for proof of main theorem:

- Show that BSD+ABC$\Rightarrow$ lower bounds exist for Ω_E and Reg_E
- Thus C_E cannot be too small in terms of N_E
- 'Walk along' Taylor expansion of $L_E(s)$ at central point, looking for first coefficient bigger than a certain bound.

The Leading Taylor Coefficient

Let C_E be the leading Taylor coefficient of $L_E(s)$ at $s = 1$.

$$\text{BSD}: \quad C_E = \frac{\Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}(E/\mathbb{Q}) \cdot \prod_p c_p}{(\#E_{\mathrm{Tor}}(\mathbb{Q}))^2}$$

Corollary

$$C_E \geq \frac{\Omega_E \cdot \mathrm{Reg}_E}{256}$$

as $\#\text{Ш}(E/\mathbb{Q}) \geq 1$, $\prod_p c_p \geq 1$ *and by Mazur's Theorem*, $\#E_{Tor}(\mathbb{Q}) \leq 16$

Method for proof of main theorem:

- Show that BSD+ABC$\Rightarrow$ lower bounds exist for Ω_E and Reg_E
- Thus C_E cannot be too small in terms of N_E
- 'Walk along' Taylor expansion of $L_E(s)$ at central point, looking for first coefficient bigger than a certain bound.
- Show all this takes $\tilde{O}(\sqrt{N_E})$ time

Motivating Data

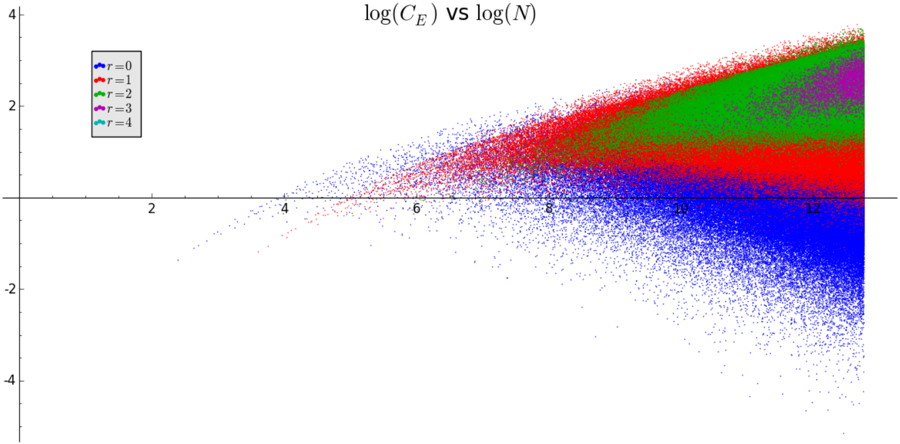

Figure: $\log N_E$ vs. $\log C_E$ for all curves up to conductor 350000 on a log/log scale, colored by rank.

The Price We Pay

The Price We Pay

To get lower bounds on Reg_E and Ω_E, must assume ABC conjecture:

The Price We Pay

To get lower bounds on Reg_E and Ω_E, must assume ABC conjecture:

Conjecture

Masser, Oesterle 1980s Let $a, b, c \in \mathbb{Z}_+$ *s.t.* $a + b = c$ *and* $\gcd(a, b, c) = 1$*, and let* $\text{rad}(abc) = \prod_{p|abc} p$*. Then* $\forall\ \epsilon > 0\ \exists\ K_\epsilon > 0$ *s.t.*

$$c < K_\epsilon \cdot \text{rad}(abc)^{1+\epsilon}$$

The Price We Pay

To get lower bounds on Reg_E and Ω_E, must assume ABC conjecture:

Conjecture

Masser, Oesterle 1980s Let $a, b, c \in \mathbb{Z}_+$ *s.t.* $a + b = c$ *and* $\gcd(a, b, c) = 1$, *and let* $\mathrm{rad}(abc) = \prod_{p|abc} p$. *Then* $\forall\, \epsilon > 0\ \exists\, K_\epsilon > 0$ *s.t.*

$$c < K_\epsilon \cdot \mathrm{rad}(abc)^{1+\epsilon}$$

Loosely, if a, b and c are coprime and $a + b = c$, then $\mathrm{rad}(abc)$ cannot be much smaller than c.

The Price We Pay

To get lower bounds on Reg_E and Ω_E, must assume ABC conjecture:

Conjecture

Masser, Oesterle 1980s Let $a, b, c \in \mathbb{Z}_+$ *s.t.* $a + b = c$ *and* $\gcd(a, b, c) = 1$, *and let* $\text{rad}(abc) = \prod_{p|abc} p$. *Then* $\forall\, \epsilon > 0\ \exists\, K_\epsilon > 0$ *s.t.*

$$c < K_\epsilon \cdot \text{rad}(abc)^{1+\epsilon}$$

Loosely, if a, b and c are coprime and $a + b = c$, then $\text{rad}(abc)$ cannot be much smaller than c.

"Numbers that are highly divisible by small primes don't often line up."

$$\frac{L_E^{(r)}(1)}{r!} \geq \frac{\Omega_E \cdot \mathrm{Reg}_E}{256}$$

The Regulator Reg_E

What is Reg_E?

What is Reg_E?

Loosely, the regulator of E is an invariant that measures how many points there are on E with small coordinates.

- Reg_E small $\Longrightarrow$ lots of 'small' rational points on E
- Reg_E big $\Longrightarrow$ few 'small' rational points on E

What is Reg_E?

Loosely, the regulator of E is an invariant that measures how many points there are on E with small coordinates.

- Reg_E small $\Longrightarrow$ lots of 'small' rational points on E
- Reg_E big $\Longrightarrow$ few 'small' rational points on E

Need a more formal definition of 'small' vs. 'large' w.r.t. points.

What is Reg_E?

Loosely, the regulator of E is an invariant that measures how many points there are on E with small coordinates.

- Reg_E small $\Longrightarrow$ lots of 'small' rational points on E
- Reg_E big $\Longrightarrow$ few 'small' rational points on E

Need a more formal definition of 'small' vs. 'large' w.r.t. points.
$\Longrightarrow$ Néron-Tate canonical height

Naïve logarithmic height

Naïve logarithmic height

Definition

Let $P \in E(\mathbb{Q})$. We may write $P = (x, y)$ with $x = \frac{a}{b}$, $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. Then

$$h(P) := \max \{\log |a|, \log |b|\}$$

Naïve logarithmic height

Definition

Let $P \in E(\mathbb{Q})$. We may write $P = (x, y)$ with $x = \frac{a}{b}$, $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. Then

$$h(P) := \max\{\log|a|, \log|b|\}$$

Naïve height is "almost a quadratic form" on $E(\mathbb{Q})$:

- $h(n \cdot P) \sim n^2 \cdot h(P)$

Néron-Tate canonical height

Néron-Tate canonical height

Definition

Let $P \in E(\mathbb{Q})$. Then the canonical height of P is

$$\hat{h}(P) := \lim_{n\to\infty} \frac{h(2^n P)}{(2^n)^2}$$

Néron-Tate canonical height

Definition

Let $P \in E(\mathbb{Q})$. Then the canonical height of P is

$$\hat{h}(P) := \lim_{n\to\infty} \frac{h(2^n P)}{(2^n)^2}$$

$\hat{h}$ defines a quadratic form on $E(\mathbb{Q})$ modulo torsion:

1. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\left[\hat{h}(P) + \hat{h}(Q)\right]$ – parallelogram law
2. $\hat{h}(nP) = n^2\hat{h}(P)$
3. $\hat{h}(P) = 0$ iff P is torsion;

Néron-Tate canonical height

Definition

Let $P \in E(\mathbb{Q})$. Then the canonical height of P is

$$\hat{h}(P) := \lim_{n\to\infty} \frac{h(2^n P)}{(2^n)^2}$$

$\hat{h}$ defines a quadratic form on $E(\mathbb{Q})$ modulo torsion:

1. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\left[\hat{h}(P) + \hat{h}(Q)\right]$ – parallelogram law
2. $\hat{h}(nP) = n^2\hat{h}(P)$
3. $\hat{h}(P) = 0$ iff P is torsion;

Definition

The *Néron-Tate pairing* on $E/\mathbb{Q}$ is the bilinear form $\langle\ ,\ \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$ by

$$\langle P, Q\rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right)$$

The Regulator

The Regulator

$<,>$ acts like an inner product on $E(\mathbb{Q})$:

The Regulator

$<,>$ acts like an inner product on $E(\mathbb{Q})$:

Proposition

Let $E/\mathbb{Q}$ have rank r. Then $E(\mathbb{Q})/E_{tor}(\mathbb{Q}) \hookrightarrow \mathbb{R}^r$ as a rank r lattice via

$$Q \mapsto (\langle Q, P_1\rangle, \ldots, \langle Q, P_r\rangle)$$

where $\{P_1, \ldots, P_r\}$ is a basis for $E(\mathbb{Q})$ modulo torsion.

The Regulator

$<,>$ acts like an inner product on $E(\mathbb{Q})$:

Proposition

Let $E/\mathbb{Q}$ have rank r. Then $E(\mathbb{Q})/E_{tor}(\mathbb{Q}) \hookrightarrow \mathbb{R}^r$ as a rank r lattice via

$$Q \mapsto (\langle Q, P_1 \rangle, \ldots, \langle Q, P_r \rangle)$$

where $\{P_1, \ldots, P_r\}$ is a basis for $E(\mathbb{Q})$ modulo torsion.

Definition

The regulator of $E/\mathbb{Q}$ is

$$\mathrm{Reg}_E = \det\left(\langle P_i, P_j \rangle\right)_{1 \leq i,j \leq r}$$

i.e. the covolume of the lattice that is the image of $E(\mathbb{Q})$ under the above embedding map

How small can the regulator be?

How small can the regulator be?

Open question, but we do have the following conjecture:

Conjecture (Lang)

There exists an absolute constant $M_0 > 0$ s.t. for any $E/\mathbb{Q}$ and any $P \in E(\mathbb{Q})$,

$$\hat{h}(P) \geq M_0 \log |D_E|$$

where D_E is the minimal discriminant of E.

How small can the regulator be?

Open question, but we do have the following conjecture:

Conjecture (Lang)

There exists an absolute constant $M_0 > 0$ s.t. for any $E/\mathbb{Q}$ and any $P \in E(\mathbb{Q})$,

$$\hat{h}(P) \geq M_0 \log |D_E|$$

where D_E is the minimal discriminant of E.

Recall for $E : y^2 = x^3 + Ax + B, \qquad D_E = -16(4A^3 + 27B^2)$

How small can the regulator be?

Open question, but we do have the following conjecture:

Conjecture (Lang)

There exists an absolute constant $M_0 > 0$ *s.t. for any* $E/\mathbb{Q}$ *and any* $P \in E(\mathbb{Q})$,

$$\hat{h}(P) \geq M_0 \log |D_E|$$

where D_E *is the minimal discriminant of* E.

Recall for $E : y^2 = x^3 + Ax + B$, $\qquad D_E = -16(4A^3 + 27B^2)$

Theorem (Hindry-Silverman 1988)

$ABC \implies$ *Lang's conjecture, and* $M_0 > 6 \times 10^{-11}$.

How small can the regulator be?

Open question, but we do have the following conjecture:

Conjecture (Lang)

There exists an absolute constant $M_0 > 0$ s.t. for any $E/\mathbb{Q}$ and any $P \in E(\mathbb{Q})$,

$$\hat{h}(P) \geq M_0 \log |D_E|$$

where D_E is the minimal discriminant of E.

Recall for $E : y^2 = x^3 + Ax + B, \qquad D_E = -16(4A^3 + 27B^2)$

Theorem (Hindry-Silverman 1988)

$ABC \implies$ *Lang's conjecture, and* $M_0 > 6 \times 10^{-11}$.

Theorem (Elkies 2002)

$M_0 > 3.94 \times 10^{-5}$ *(still contingent on ABC)*

How small can the regulator be?

How small can the regulator be?

Proposition (S.)

Assuming BSD and ABC,

$$\mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$$

How small can the regulator be?

Proposition (S.)

Assuming BSD and ABC,

$$\mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$$

Further assuming GRH:

$$\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$$

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Proof.

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Proof.

- Verified manually for all curves with $N_E \leq 350000$

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Proof.

- Verified manually for all curves with $N_E \leq 350000$
- So E have $N_E > 350000$. Let $K = 3.94 \times 10^{-5} \cdot \log(350000)$.
  $\Rightarrow \hat{h}(P) \geq K$ for any $P \in E(\mathbb{Q})$

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Proof.

- Verified manually for all curves with $N_E \leq 350000$
- So E have $N_E > 350000$. Let $K = 3.94 \times 10^{-5} \cdot \log(350000)$.
  $\Rightarrow \hat{h}(P) \geq K$ for any $P \in E(\mathbb{Q})$
- $\Rightarrow \mathrm{Reg}_E \geq K^r$

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Proof.

- Verified manually for all curves with $N_E \leq 350000$
- So E have $N_E > 350000$. Let $K = 3.94 \times 10^{-5} \cdot \log(350000)$.
  $\Rightarrow \hat{h}(P) \geq K$ for any $P \in E(\mathbb{Q})$
- $\Rightarrow \mathrm{Reg}_E \geq K^r$
- From logarithmic derivatives: $r_{an}(E) < \frac{1}{2} \log N_E + 1.6$. So

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Proof.

- Verified manually for all curves with $N_E \leq 350000$
- So E have $N_E > 350000$. Let $K = 3.94 \times 10^{-5} \cdot \log(350000)$.
  $\Rightarrow \hat{h}(P) \geq K$ for any $P \in E(\mathbb{Q})$
- $\Rightarrow \mathrm{Reg}_E \geq K^r$
- From logarithmic derivatives: $r_{an}(E) < \frac{1}{2} \log N_E + 1.6$. So

$$\mathrm{Reg}_E > K^{\frac{1}{2}\log N_E + 1.6} = K^{1.6}(N_E)^{\frac{1}{2}\log K} = 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$$

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Proof.

- Verified manually for all curves with $N_E \leq 350000$
- So E have $N_E > 350000$. Let $K = 3.94 \times 10^{-5} \cdot \log(350000)$.
  $\Rightarrow \hat{h}(P) \geq K$ for any $P \in E(\mathbb{Q})$
- $\Rightarrow \mathrm{Reg}_E \geq K^r$
- From logarithmic derivatives: $r_{an}(E) < \frac{1}{2}\log N_E + 1.6$. So

$$\mathrm{Reg}_E > K^{\frac{1}{2}\log N_E + 1.6} = K^{1.6}(N_E)^{\frac{1}{2}\log K} = 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$$

With GRH, have $r_{an}(E) < 0.32\log N_E + 0.5$; proceed as above.

$\square$

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Note: bound likely not optimal:

- Smallest known point height (Stein 2002): Cremona curve 3990v1 with equation $E : y^2 + xy + y = x^3 + x^2 - 125615 + 61201397$ has point $P = (7107, -602054)$ with $\hat{h}(P) = 8.914 \times 10^{-3}$

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Note: bound likely not optimal:

- Smallest known point height (Stein 2002): Cremona curve 3990v1 with equation $E : y^2 + xy + y = x^3 + x^2 - 125615 + 61201397$ has point $P = (7107, -602054)$ with $\hat{h}(P) = 8.914 \times 10^{-3}$
- If so, $\Rightarrow \mathrm{Reg}_E \geq 6.6064 \cdot (N_E)^{-2.36}$ without needing GRH

How small can the regulator be?

Proposition (S.)

BSD and ABC $\Rightarrow \mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$
$+$ *GRH:* $\mathrm{Reg}_E \geq 2.24 \times 10^{-2} \cdot (N_E)^{-2.43}$

Note: bound likely not optimal:

- Smallest known point height (Stein 2002): Cremona curve 3990v1 with equation $E : y^2 + xy + y = x^3 + x^2 - 125615 + 61201397$ has point $P = (7107, -602054)$ with $\hat{h}(P) = 8.914 \times 10^{-3}$
- If so, $\Rightarrow \mathrm{Reg}_E \geq 6.6064 \cdot (N_E)^{-2.36}$ without needing GRH
- Nevertheless, bound is good enough

$$\frac{L_E^{(r)}(1)}{r!} \geq \frac{\Omega_E \cdot \mathrm{Reg}_E}{256}$$

The Real Period Ω_E

What is Ω_E?

Loosely, the real period of E is a measure of the size of the set of real points on E

- Ω_E small $\Longrightarrow$ lots of real points on E
- Ω_E big $\Longrightarrow$ few real points on E

What is Ω_E?

Loosely, the real period of E is a measure of the size of the set of real points on E

- Ω_E small $\implies$ lots of real points on E
- Ω_E big $\implies$ few real points on E

Again, need a more formal definition of what is meant by the size of $E(\mathbb{R})$.

Real period examples

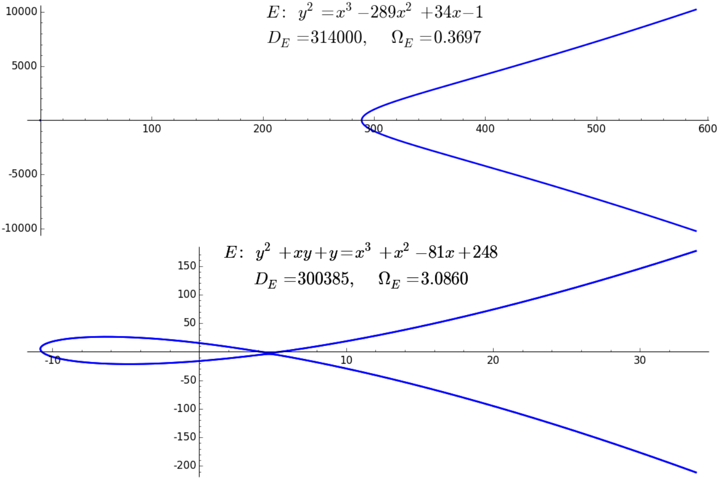

Figure: A plot of $E/\mathbb{R}$ for two elliptic curves with minimal discriminant ~ 300000. The top curve has a very small real period for its discriminant, the bottom very large.

Complex Theory of Elliptic Curves recap

Complex Theory of Elliptic Curves recap

Let $E(\mathbb{C})$ be the group of complex points on E.
Recall:

Complex Theory of Elliptic Curves recap

Let $E(\mathbb{C})$ be the group of complex points on E.
Recall:

- $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ a lattice

Complex Theory of Elliptic Curves recap

Let $E(\mathbb{C})$ be the group of complex points on E.
Recall:

- $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ a lattice
- If E is defined over $\mathbb{Q}$, then may take $\omega_1 \in \mathbb{R}_+$, $\Im(\omega_2) > 0$ and $\Re(\omega_2) \in \left\{0, \frac{\omega_1}{2}\right\}$.

Complex Theory of Elliptic Curves recap

Let $E(\mathbb{C})$ be the group of complex points on E.
Recall:

- $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ a lattice
- If E is defined over $\mathbb{Q}$, then may take $\omega_1 \in \mathbb{R}_+$, $\Im(\omega_2) > 0$ and $\Re(\omega_2) \in \left\{0, \frac{\omega_1}{2}\right\}$.

Definition

The *real period* Ω_E of E is defined to be

$$\Omega_E = \begin{cases} 2\omega_1 & D_E > 0 \\ \omega_1 & D_E < 0 \end{cases}$$

where D_E is the discriminant of E

Complex Theory of Elliptic Curves recap

Let $E(\mathbb{C})$ be the group of complex points on E.
Recall:

- $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ a lattice
- If E is defined over $\mathbb{Q}$, then may take $\omega_1 \in \mathbb{R}_+$, $\Im(\omega_2) > 0$ and $\Re(\omega_2) \in \left\{0, \frac{\omega_1}{2}\right\}$.

Definition

The *real period* Ω_E of E is defined to be

$$\Omega_E = \begin{cases} 2\omega_1 & D_E > 0 \\ \omega_1 & D_E < 0 \end{cases}$$

where D_E is the discriminant of E

Recall for $E : y^2 = x^3 + Ax + B, \qquad D_E = -16(4A^3 + 27B^2)$

How small can Ω_E be?

How small can Ω_E be?

Theorem (S.)

Assuming ABC, $\forall\, \epsilon > 0\ \exists\, K_\epsilon > 0$ *s.t.*

$$\Omega_E > K_\epsilon \cdot (N_E)^{-\frac{3}{2}-\epsilon}$$

How small can Ω_E be?

Theorem (S.)

Assuming ABC, $\forall\ \epsilon > 0\ \exists\ K_\epsilon > 0$ *s.t.*

$$\Omega_E > K_\epsilon \cdot (N_E)^{-\frac{3}{2}-\epsilon}$$

Proof Sketch

- Ω_E can be computed via AGM and roots of cubic in model $y^2 = $ [cubic]

How small can Ω_E be?

Theorem (S.)

Assuming ABC, $\forall\ \epsilon > 0\ \exists\ K_\epsilon > 0$ *s.t.*

$$\Omega_E > K_\epsilon \cdot (N_E)^{-\frac{3}{2}-\epsilon}$$

Proof Sketch

- Ω_E can be computed via AGM and roots of cubic in model $y^2 =$ [cubic]
- Analysis $\Rightarrow$ get lower bound on Ω_E i.t.o. magnitude of cubic coeffs

How small can Ω_E be?

Theorem (S.)

Assuming ABC, $\forall\, \epsilon > 0\ \exists\, K_\epsilon > 0$ *s.t.*

$$\Omega_E > K_\epsilon \cdot (N_E)^{-\frac{3}{2}-\epsilon}$$

Proof Sketch

- Ω_E can be computed via AGM and roots of cubic in model $y^2 = $ [cubic]
- Analysis $\Rightarrow$ get lower bound on Ω_E i.t.o. magnitude of cubic coeffs
- Szpiro's conjecture $\Rightarrow$ lower bound i.t.o. power of N_E

Szpiro's conjecture

Szpiro's conjecture

Note that $N_E | D_E$ always (via Ogg's formula), $\Rightarrow N_E \leq |D_E|$

Szpiro's conjecture

Note that $N_E | D_E$ always (via Ogg's formula), $\Rightarrow N_E \leq |D_E|$
Szpiro: conjectural bound in the other direction:

Szpiro's conjecture

Note that $N_E | D_E$ always (via Ogg's formula), $\Rightarrow N_E \leq |D_E|$
Szpiro: conjectural bound in the other direction:

Conjecture (Szpiro 1980s)

$\forall\, \epsilon > 0\ \exists\, K_\epsilon > 0\ s.t.$

$$|D_E| < K_\epsilon \cdot (N_E)^{6+\epsilon}$$

Szpiro's conjecture

Note that $N_E | D_E$ always (via Ogg's formula), $\Rightarrow N_E \leq |D_E|$
Szpiro: conjectural bound in the other direction:

Conjecture (Szpiro 1980s)

$\forall\, \epsilon > 0\; \exists\, K_\epsilon > 0$ *s.t.*

$$|D_E| < K_\epsilon \cdot (N_E)^{6+\epsilon}$$

Modified Szpiro conjecture

Let $E/\mathbb{Q}$ have minimal short Weierstrass equation $y^2 = x^3 + Ax + B$.
Then $\forall\, \epsilon > 0\; \exists\, K_\epsilon > 0$ s.t.

$$\max\left\{|A|^3, |B|^2\right\} < K_\epsilon \cdot (N_E)^{6+\epsilon}$$

Szpiro's conjecture

Note that $N_E | D_E$ always (via Ogg's formula), $\Rightarrow N_E \leq |D_E|$
Szpiro: conjectural bound in the other direction:

Conjecture (Szpiro 1980s)

$\forall\ \epsilon > 0\ \exists\ K_\epsilon > 0$ *s.t.*

$$|D_E| < K_\epsilon \cdot (N_E)^{6+\epsilon}$$

Modified Szpiro conjecture

Let $E/\mathbb{Q}$ have minimal short Weierstrass equation $y^2 = x^3 + Ax + B$.
Then $\forall\ \epsilon > 0\ \exists\ K_\epsilon > 0$ s.t.

$$\max\left\{|A|^3, |B|^2\right\} < K_\epsilon \cdot (N_E)^{6+\epsilon}$$

- "A curve with a given conductor cannot have a (minimal) model with coefficients too large".

Szpiro's conjecture

Note that $N_E | D_E$ always (via Ogg's formula), $\Rightarrow N_E \leq |D_E|$
Szpiro: conjectural bound in the other direction:

Conjecture (Szpiro 1980s)

$\forall\, \epsilon > 0\ \exists\, K_\epsilon > 0$ *s.t.*

$$|D_E| < K_\epsilon \cdot (N_E)^{6+\epsilon}$$

Modified Szpiro conjecture

Let $E/\mathbb{Q}$ have minimal short Weierstrass equation $y^2 = x^3 + Ax + B$.
Then $\forall\, \epsilon > 0\ \exists\, K_\epsilon > 0$ s.t.

$$\max\left\{|A|^3, |B|^2\right\} < K_\epsilon \cdot (N_E)^{6+\epsilon}$$

- "A curve with a given conductor cannot have a (minimal) model with coefficients too large".
- ABC $\Rightarrow$ Szpiro.

Supporting Data

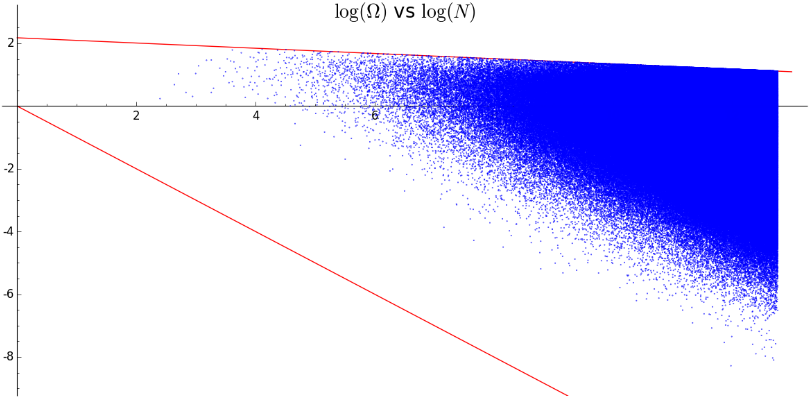

Figure: $\log N_E$ vs. $\log \Omega_E$ for all curves up to conductor 350000. The upper red line is the proven upper bound $\Omega_E < 8.82921517\ldots \cdot (N_E)^{-\frac{1}{12}}$; the lower red line corresponds to $\Omega_E > (N_E)^{-1}$.

How small can Ω_E be?

How small can Ω_E be?

Corollary

Ω_E can be computed to a specified precision in polynomial time and space in the number of bits of the curve's conductor.

How small can Ω_E be?

Corollary

Ω_E can be computed to a specified precision in polynomial time and space in the number of bits of the curve's conductor.

Proof Sketch

- AGM converges quadratically (Gauss), so quick to compute

How small can Ω_E be?

Corollary

Ω_E can be computed to a specified precision in polynomial time and space in the number of bits of the curve's conductor.

Proof Sketch

- AGM converges quadratically (Gauss), so quick to compute
- $\Rightarrow \Omega_E$ can be computed in polynomial time of number of bits of coefficients

How small can Ω_E be?

Corollary

Ω_E can be computed to a specified precision in polynomial time and space in the number of bits of the curve's conductor.

Proof Sketch

- AGM converges quadratically (Gauss), so quick to compute
- $\Rightarrow \Omega_E$ can be computed in polynomial time of number of bits of coefficients
- By Szpiro, coefficients can't be too large i.t.o. conductor.

Proof of the Main Theorem

How much precision do we need to compute analytic rank?

How much precision do we need to compute analytic rank?

Assume BSD and ABC.

Precision Theorem (S.)

Let E have L-function $L_E(s)$, conductor N_E and real period Ω_E, and let

$$k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$$

Then

1. $k = O(\log N_E)$
2. If $L_E^{(m)}(1) = 0$ for all $0 \leq m < n$ and $\frac{L_E^{(n)}(1)}{n!}$ is zero to k bits precision, then $L_E^{(n)}(1)$ is identically zero.

How much precision do we need to compute analytic rank?

Assume BSD and ABC.

Precision Theorem (S.)

Let E have L-function $L_E(s)$, conductor N_E and real period Ω_E, and let

$$k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$$

Then

1. $k = O(\log N_E)$
2. If $L_E^{(m)}(1) = 0$ for all $0 \leq m < n$ and $\frac{L_E^{(n)}(1)}{n!}$ is zero to k bits precision, then $L_E^{(n)}(1)$ is identically zero.

With GRH: let $k = \lceil 26 + 2.43 \log_2 N_E - \log_2 \Omega_E \rceil$.

How much precision do we need to compute analytic rank?

Proof.

How much precision do we need to compute analytic rank?

Proof.

1. Follows immediately from negative power bound on Ω_E

How much precision do we need to compute analytic rank?

Proof.

1. Follows immediately from negative power bound on Ω_E
2. Since $C_E > (\mathrm{Reg}_E \cdot \Omega_E)/256$ and $\mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$, we have

$$\begin{aligned}
\log_2 C_E &> -16 + \log_2(5.29 \times 10^{-6}) + 3.8 \log_2 N_E + \log_2 \Omega_E \\
&> -34 - 3.8 \log_2 N_E + \log_2 \Omega_E
\end{aligned}$$

How much precision do we need to compute analytic rank?

Proof.

1. Follows immediately from negative power bound on Ω_E
2. Since $C_E > (\mathrm{Reg}_E \cdot \Omega_E)/256$ and $\mathrm{Reg}_E \geq 5.29 \times 10^{-6} \cdot (N_E)^{-3.80}$, we have

$$\begin{aligned}\log_2 C_E &> -16 + \log_2(5.29 \times 10^{-6}) + 3.8 \log_2 N_E + \log_2 \Omega_E \\ &> -34 - 3.8 \log_2 N_E + \log_2 \Omega_E\end{aligned}$$

So by BSD, rank is smallest n s.t. $\frac{L_E^{(n)}(1)}{n!} > 2^{-k}$.

$\square$

Asymptotic runtime on the rank algorithm

Algorithm: compute the rank of an elliptic curve (BSD, ABC, (GRH))

Given $E/\mathbb{Q}$ with conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$, and set $m = 0$.
   (If GRH: set $k = \lceil 24 + 2.43 \log_2 N_E - \log_2 \Omega_E \rceil$ instead)
3. Output $r =$ index of the first Taylor coefficient of the $L_E(s)$ at $s = 1$ that isn't zero to k bits precision.

Asymptotic runtime on the rank algorithm

Algorithm: compute the rank of an elliptic curve (BSD, ABC, (GRH))

Given $E/\mathbb{Q}$ with conductor N_E:

1. Compute the real period Ω_E of E.
2. Set $k = \lceil 36 + 3.8 \log_2 N_E - \log_2 \Omega_E \rceil$, and set $m = 0$.
   (If GRH: set $k = \lceil 24 + 2.43 \log_2 N_E - \log_2 \Omega_E \rceil$ instead)
3. Output r = index of the first Taylor coefficient of the $L_E(s)$ at $s = 1$ that isn't zero to k bits precision.

Theorem (S.)

Assuming BSD, ABC and optionally GRH, the above algorithm correctly computes the rank of E in $\tilde{O}\left(\sqrt{N_E}\right)$ *time.*

Asymptotic runtime on the rank algorithm

Proof.

Asymptotic runtime on the rank algorithm

Proof.

All that remains is to show step 3. (walk along Taylor coefficients) takes $\tilde{O}\left(\sqrt{N_E}\right)$ time.

Asymptotic runtime on the rank algorithm

Proof.

All that remains is to show step 3. (walk along Taylor coefficients) takes $\tilde{O}\left(\sqrt{N_E}\right)$ time.

- (Bradshaw 2010): $L_E(s)$ can be provably evaluated to k bits precision in $\tilde{O}(k \cdot \sqrt{N_E})$ near $s = 1$.

Asymptotic runtime on the rank algorithm

Proof.

All that remains is to show step 3. (walk along Taylor coefficients) takes $\tilde{O}\left(\sqrt{N_E}\right)$ time.

- (Bradshaw 2010): $L_E(s)$ can be provably evaluated to k bits precision in $\tilde{O}(k \cdot \sqrt{N_E})$ near $s = 1$.
- $k = O(\log N_E)$ for some m from before

Asymptotic runtime on the rank algorithm

Proof.

All that remains is to show step 3. (walk along Taylor coefficients) takes $\tilde{O}\left(\sqrt{N_E}\right)$ time.

- (Bradshaw 2010): $L_E(s)$ can be provably evaluated to k bits precision in $\tilde{O}(k \cdot \sqrt{N_E})$ near $s = 1$.
- $k = O(\log N_E)$ for some m from before
- BSD: $r < \frac{1}{2} \log N_E + 1.6$

Asymptotic runtime on the rank algorithm

Proof.

All that remains is to show step 3. (walk along Taylor coefficients) takes $\tilde{O}\left(\sqrt{N_E}\right)$ time.

- (Bradshaw 2010): $L_E(s)$ can be provably evaluated to k bits precision in $\tilde{O}(k \cdot \sqrt{N_E})$ near $s = 1$.
- $k = O(\log N_E)$ for some m from before
- BSD: $r < \frac{1}{2} \log N_E + 1.6$
- So step 3 takes

$$O(\log N_E) \cdot \tilde{O}((\log N_E)^m \cdot \sqrt{N_E}) = \tilde{O}(\sqrt{N_E})$$

time

$\square$

Supporting data

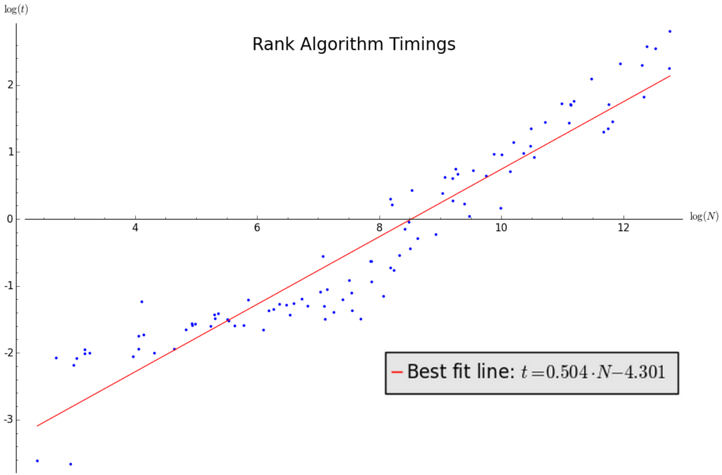

Figure: Conductor v.s time in seconds taken to compute rank using a Sage implementation of the rank algorithm (without assuming GRH), on a log/log scale, for 100 curves drawn randomly from the Cremona database.

Remarks and future work

Remarks and future work

Rank algorithm is not optimal in multiple ways:

Remarks and future work

Rank algorithm is not optimal in multiple ways:

- Should check for torsion first – if none then need 16 bits less precision

Remarks and future work

Rank algorithm is not optimal in multiple ways:

- Should check for torsion first – if none then need 16 bits less precision
- Regulator bound could be improved – fixed time point search + CPS bound

Remarks and future work

Rank algorithm is not optimal in multiple ways:

- Should check for torsion first – if none then need 16 bits less precision
- Regulator bound could be improved – fixed time point search + CPS bound
- GRH $\Rightarrow$ rank grows slower than $\log N_E \Rightarrow$ speedups

Remarks and future work

Rank algorithm is not optimal in multiple ways:

- Should check for torsion first – if none then need 16 bits less precision
- Regulator bound could be improved – fixed time point search + CPS bound
- GRH $\Rightarrow$ rank grows slower than $\log N_E$ $\Rightarrow$ speedups
- Work on reducing ABC dependence

Other work in my thesis

Other work in my thesis

- $\tilde{O}(\sqrt{N_E})$ dependence in rank algorithm makes it impractical for curves of very large conductor

Other work in my thesis

- $\tilde{O}(\sqrt{N_E})$ dependence in rank algorithm makes it impractical for curves of very large conductor
- Elkies' rank 28 curve ($N_E \sim 10^{142}$) would take $\sim 10^{62}$ years

Other work in my thesis

- $\tilde{O}(\sqrt{N_E})$ dependence in rank algorithm makes it impractical for curves of very large conductor
- Elkies' rank 28 curve ($N_E \sim 10^{142}$) would take $\sim 10^{62}$ years
- Can resort to faster analytic techniques that bound rank from above

Other work in my thesis

- $\tilde{O}(\sqrt{N_E})$ dependence in rank algorithm makes it impractical for curves of very large conductor
- Elkies' rank 28 curve ($N_E \sim 10^{142}$) would take $\sim 10^{62}$ years
- Can resort to faster analytic techniques that bound rank from above
- Technique is zero sum based, so results on location/density of nontrivial zeros for $L_E(s)$

Baie Dankie

(Afrikaans for Thank You)