Counting elliptic curves with a rational N-isogeny

Soumya Sankar (MSRI), joint work with Brandon Boggess (UW Madison)

Junior Number Theory Days 2020

December 5, 2020

Notation

- Throughout the talk, E will denote an elliptic curve over $\mathbb{Q}$.

Notation

- Throughout the talk, E will denote an elliptic curve over $\mathbb{Q}$.
- $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ will be taken in minimal Weierstrass form (i.e. $\gcd(A^3, B^2)$ 12th power-free).

Notation

- Throughout the talk, E will denote an elliptic curve over $\mathbb{Q}$.
- $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ will be taken in minimal Weierstrass form (i.e. $\gcd(A^3, B^2)$ 12th power-free).
- $N \in \mathbb{Z}_{\geq 1}$.
- We say that E has an N-isogeny if there is an isogeny $\phi : E \to E'$ such that $(\operatorname{Ker} \phi)(\overline{\mathbb{Q}}) \cong \mathbb{Z}/N\mathbb{Z}$.

Notation

- Throughout the talk, E will denote an elliptic curve over $\mathbb{Q}$.
- $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ will be taken in minimal Weierstrass form (i.e. $\gcd(A^3, B^2)$ 12th power-free).
- $N \in \mathbb{Z}_{\geq 1}$.
- We say that E has an N-isogeny if there is an isogeny $\phi : E \to E'$ such that $(\operatorname{Ker} \phi)(\overline{\mathbb{Q}}) \cong \mathbb{Z}/N\mathbb{Z}$.
- Such an isogeny is rational if $\operatorname{Ker} \phi$ is defined over $\mathbb{Q}$.

Main Question

Question

How many elliptic curves have a rational N-isogeny?

Main Question

Question

How many elliptic curves have a rational N-isogeny?

If N is small enough, there are infinitely many isomorphism classes of elliptic curves that have a rational N-isogeny,

Main Question

Question

How many elliptic curves have a rational N-isogeny?

If N is small enough, there are infinitely many isomorphism classes of elliptic curves that have a rational N-isogeny,so we order them by naive height:

$$\mathrm{Ht}_{naive}(E) := \max\{|A|^3, |B|^2\}$$

Main Question

Question

How many elliptic curves have a rational N-isogeny?

If N is small enough, there are infinitely many isomorphism classes of elliptic curves that have a rational N-isogeny,so we order them by naive height:

$$\mathrm{Ht}_{naive}(E) := \max\{|A|^3, |B|^2\}$$

More precise question

How many elliptic curves (up to $\mathbb{Q}$-isomorphism) of bounded naive height have a rational N-isogeny?

Some more notation

For two real valued functions $f(X)$ and $g(X)$, we say that $f(X) \asymp g(X)$ if there are two positive constants K_1 and K_2 such that

$$K_1 g(X) \leq f(X) \leq K_2 g(X).$$

Some more notation

For two real valued functions $f(X)$ and $g(X)$, we say that $f(X) \asymp g(X)$ if there are two positive constants K_1 and K_2 such that

$$K_1 g(X) \leq f(X) \leq K_2 g(X).$$

Counting function

$\mathcal{N}(N, X) := \#\{E_{/\mathbb{Q}} \mid \mathrm{Ht}_{naive}(E) < X, E \text{ has a rational } N\text{-isogeny}\}$

Some more notation

For two real valued functions $f(X)$ and $g(X)$, we say that $f(X) \asymp g(X)$ if there are two positive constants K_1 and K_2 such that

$$K_1 g(X) \leq f(X) \leq K_2 g(X).$$

Counting function

$$\mathcal{N}(N, X) := \#\{E_{/\mathbb{Q}} \mid \mathrm{Ht}_{naive}(E) < X, E \text{ has a rational } N\text{-isogeny}\}$$

So our goal is to find a function $h_N(X)$ such that

$$\mathcal{N}(N, X) \asymp h_N(X).$$

Some more notation

For two real valued functions $f(X)$ and $g(X)$, we say that $f(X) \asymp g(X)$ if there are two positive constants K_1 and K_2 such that

$$K_1 g(X) \leq f(X) \leq K_2 g(X).$$

Counting function

$\mathcal{N}(N, X) := \#\{E_{/\mathbb{Q}} \mid \mathrm{Ht}_{naive}(E) < X, E \text{ has a rational } N\text{-isogeny}\}$

So our goal is to find a function $h_N(X)$ such that

$$\mathcal{N}(N, X) \asymp h_N(X).$$

Example

If $N = 1$, we are counting integers in a box, and $\mathcal{N}(1, X) \asymp X^{5/6}$.

Main theorem

Theorem [BS, '20]

N	$h_N(X)$	N	$h_N(X)$
2	$X^{1/2}$	8	$X^{1/6}\log(X)$
3	$X^{1/2}$	9	$X^{1/6}\log(X)$
4	$X^{1/3}$	12	$X^{1/6}$
5	$X^{1/6}(\log(X))^2$	16	$X^{1/6}$
6	$X^{1/6}\log(X)$	18	$X^{1/6}$

Table 1: Values of $h_N(X)$, ordered by naive height

Rephrasing our problem

Rephrasing our problem

- Let $\mathcal{X}_0(N)$ be the compactification of the classical modular curve whose S points are given by:

$$\mathcal{Y}_0(N)(S) = \{(E, C) \mid E_{/S} \text{ an elliptic curve}, C \cong_S \mathbb{Z}/N\mathbb{Z}\},$$

where S is a $\mathbb{Z}[1/N]$-scheme.

Rephrasing our problem

- Let $\mathcal{X}_0(N)$ be the compactification of the classical modular curve whose S points are given by:

$$\mathcal{Y}_0(N)(S) = \{(E, C) \mid E_{/S} \text{ an elliptic curve, } C \cong_S \mathbb{Z}/N\mathbb{Z}\},$$

  where S is a $\mathbb{Z}[1/N]$-scheme.
- Therefore counting $\mathcal{N}(N, X) \leftrightarrow$ counting rational points on $\mathcal{X}_0(N)$.

Rephrasing our problem

- Let $\mathcal{X}_0(N)$ be the compactification of the classical modular curve whose S points are given by:

$$\mathcal{Y}_0(N)(S) = \{(E, C) \mid E_{/S} \text{ an elliptic curve}, C \cong_S \mathbb{Z}/N\mathbb{Z}\},$$

  where S is a $\mathbb{Z}[1/N]$-scheme.
- Therefore counting $\mathcal{N}(N, X) \leftrightarrow$ counting rational points on $\mathcal{X}_0(N)$.

Fun fact!

$\mathcal{X}_0(N)$ is not a scheme, but a stack.

Every point has the non-trivial automorphism $[-1]$. So, $\mathcal{X}_0(N)$ is actually a μ_2-gerbe.

Two strategies to count points on these stacks

- Counting elliptic curves in quadratic twist families (generalizing work of Harron and Snowden),

Two strategies to count points on these stacks

- Counting elliptic curves in quadratic twist families (generalizing work of Harron and Snowden),
- Counting points of bounded height on weighted projective stacks (using framework of Ellenberg, Satriano and Zureick-Brown).

Plan

The Harron and Snowden framework

- Let X be a *scheme* parametrizing elliptic curves with a certain level structure, such that $X \cong \mathbb{P}^1$ (e.g. $\mathcal{X}_1(5)$).

The Harron and Snowden framework

- Let X be a *scheme* parametrizing elliptic curves with a certain level structure, such that $X \cong \mathbb{P}^1$ (e.g. $\mathcal{X}_1(5)$).
- Then X has a universal family over it, i.e. there exist polynomials $f, g \in \mathbb{Q}[t]$ coprime such that every elliptic curve with said level structure is isomorphic to one of the form:

$$y^2 = x^3 + f(t)x + g(t).$$

The Harron and Snowden framework

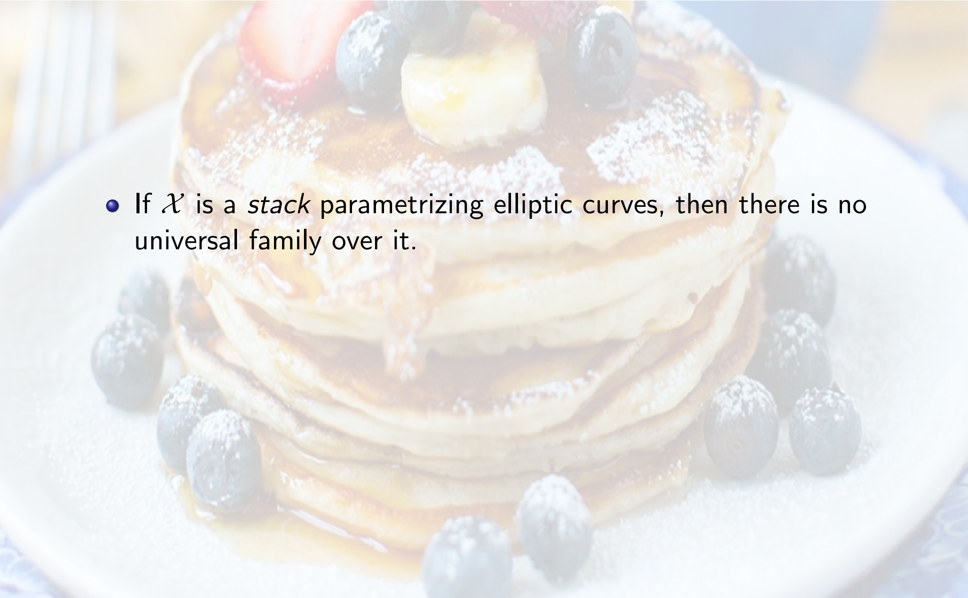
- Let X be a *scheme* parametrizing elliptic curves with a certain level structure, such that $X \cong \mathbb{P}^1$ (e.g. $\mathcal{X}_1(5)$).
- Then X has a universal family over it, i.e. there exist polynomials $f, g \in \mathbb{Q}[t]$ coprime such that every elliptic curve with said level structure is isomorphic to one of the form:

$$y^2 = x^3 + f(t)x + g(t).$$

- Counting problem: count pairs $(A, B) \in \mathbb{Z}^2$ such that:
  - $\exists u, t \in \mathbb{Q}$ such that $A = u^4 f(t)$, $B = u^6 g(t)$,
  - $\max\{|A|^3, |B|^2\} < X$,
  - $\gcd(A^3, B^2)$ not divisible by any twelfth powers.

The problem with stacks

The problem with stacks



- If $\mathcal{X}$ is a *stack* parametrizing elliptic curves, then there is no universal family over it.

The problem with stacks

- If $\mathcal{X}$ is a *stack* parametrizing elliptic curves, then there is no universal family over it.
- However, in our case, we can find a double cover that has one (at least generically).

Motivating example: $\mathcal{X}_0(3)$

The case for general N:

- For $N \in \{3, 4, 6, 8, 9, 12, 16, 18\}$, we consider the cover $\Phi_N : \mathcal{X}_1(N) \to \mathcal{X}_0(N)$, whose geometric fibers are isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$.

The case for general N:

- For $N \in \{3, 4, 6, 8, 9, 12, 16, 18\}$, we consider the cover $\Phi_N : \mathcal{X}_1(N) \to \mathcal{X}_0(N)$, whose geometric fibers are isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$.
- Pick $H \subset \mathbb{Z}/N\mathbb{Z}^\times$ of index 2 and let $\mathcal{X}_{1/2}(N)$ denote the fiberwise quotient of $\mathcal{X}_1(N)$ by H.

The case for general N:

- For $N \in \{3, 4, 6, 8, 9, 12, 16, 18\}$, we consider the cover $\Phi_N : \mathcal{X}_1(N) \to \mathcal{X}_0(N)$, whose geometric fibers are isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$.
- Pick $H \subset \mathbb{Z}/N\mathbb{Z}^\times$ of index 2 and let $\mathcal{X}_{1/2}(N)$ denote the fiberwise quotient of $\mathcal{X}_1(N)$ by H.
- Then, every $(E, C) \in \mathcal{X}_0(N)(\mathbb{Q})$ has a quadratic twist $(E^d, C^d) \in \mathcal{X}_{1/2}(N)(\mathbb{Q})$.

The case for general N:

- For $N \in \{3, 4, 6, 8, 9, 12, 16, 18\}$, we consider the cover $\Phi_N : \mathcal{X}_1(N) \to \mathcal{X}_0(N)$, whose geometric fibers are isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$.
- Pick $H \subset \mathbb{Z}/N\mathbb{Z}^\times$ of index 2 and let $\mathcal{X}_{1/2}(N)$ denote the fiberwise quotient of $\mathcal{X}_1(N)$ by H.
- Then, every $(E, C) \in \mathcal{X}_0(N)(\mathbb{Q})$ has a quadratic twist $(E^d, C^d) \in \mathcal{X}_{1/2}(N)(\mathbb{Q})$.

Proposition [BS, 2020]

Let $N \in \{3, 4, 6, 8, 9, 12, 16, 18\}$. Then for an appropriate choice of H in each case, $\mathcal{X}_{1/2}(N)$ is a stacky curve with at most one stacky point, whose coarse space is isomorphic to $\mathbb{P}^1$.

Modified counting problem

For $N \in \{3, 4, 6, 8, 9, 12, 16, 18\}$ we are able to find $f_N, g_N \in \mathbb{Q}[t]$ coprime, such that every elliptic curve giving a rational point on $\mathcal{X}_{1/2}(N)^{**}$ is isomorphic to one of the form:

$$y^2 = x^3 + f_N(t)x + g_N(t).$$

Modified counting problem

For $N \in \{3, 4, 6, 8, 9, 12, 16, 18\}$ we are able to find $f_N, g_N \in \mathbb{Q}[t]$ coprime, such that every elliptic curve giving a rational point on $\mathcal{X}_{1/2}(N)^{**}$ is isomorphic to one of the form:

$$y^2 = x^3 + f_N(t)x + g_N(t).$$

Counting problem:

Count pairs $(A, B) \in \mathbb{Z}^2$ such that:

- $\exists u, t \in \mathbb{Q}$ such that $A = u^2 f_N(t)$, $B = u^3 g_N(t)$,
- $\max\{|A|^3, |B|^2\} < X$,
- $\gcd(A^3, B^2)$ not divisible by any twelfth powers.

Modified counting problem

For $N \in \{3, 4, 6, 8, 9, 12, 16, 18\}$ we are able to find $f_N, g_N \in \mathbb{Q}[t]$ coprime, such that every elliptic curve giving a rational point on $\mathcal{X}_{1/2}(N)$** is isomorphic to one of the form:

$$y^2 = x^3 + f_N(t)x + g_N(t).$$

Counting problem:

Count pairs $(A, B) \in \mathbb{Z}^2$ such that:

- $\exists u, t \in \mathbb{Q}$ such that $A = u^2 f_N(t)$, $B = u^3 g_N(t)$,
- $\max\{|A|^3, |B|^2\} < X$,
- $\gcd(A^3, B^2)$ not divisible by any twelfth powers.

**for $N = 3$, we want an open substack of $\mathcal{X}_{1/2}(N)$.

Plan

Heights on projective varieties

Heights on projective varieties

Let $x \in \mathbb{P}^k(\mathbb{Q})$. We can write $x = [x_0 : x_1 \ldots : x_k]$, with: $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1 \ldots x_k) = 1$.

Heights on projective varieties

Let $x \in \mathbb{P}^k(\mathbb{Q})$. We can write $x = [x_0 : x_1 \ldots : x_k]$, with: $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1 \ldots x_k) = 1$.

Definition

The naive height of x is

$$\mathrm{Ht}(x) := \prod_{\nu \in M_{\mathbb{Q}}} \max_i \{|x_i|_\nu\} = \max_i \{|x_i|\}.$$

Heights on projective varieties

Let $x \in \mathbb{P}^k(\mathbb{Q})$. We can write $x = [x_0 : x_1 \ldots : x_k]$, with: $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1 \ldots x_k) = 1$.

Definition

The naive height of x is

$$\mathrm{Ht}(x) := \prod_{\nu \in M_{\mathbb{Q}}} \max_i \{|x_i|_\nu\} = \max_i \{|x_i|\}.$$

Let X be a projective variety and $\mathcal{L}$ an ample line bundle. Then for some n we can use the sections of $\mathcal{L}^{\otimes n}$ to embed X into some $\mathbb{P}^k$:

$$\phi_{\mathcal{L},n} : X \hookrightarrow \mathbb{P}^k.$$

Heights on projective varieties

Let $x \in \mathbb{P}^k(\mathbb{Q})$. We can write $x = [x_0 : x_1 \ldots : x_k]$, with: $x_i \in \mathbb{Z}$ and $\gcd(x_0, x_1 \ldots x_k) = 1$.

Definition

The naive height of x is

$$\mathrm{Ht}(x) := \prod_{\nu \in M_{\mathbb{Q}}} \max_i \{|x_i|_\nu\} = \max_i \{|x_i|\}.$$

Let X be a projective variety and $\mathcal{L}$ an ample line bundle. Then for some n we can use the sections of $\mathcal{L}^{\otimes n}$ to embed X into some $\mathbb{P}^k$:

$$\phi_{\mathcal{L},n} : X \hookrightarrow \mathbb{P}^k.$$

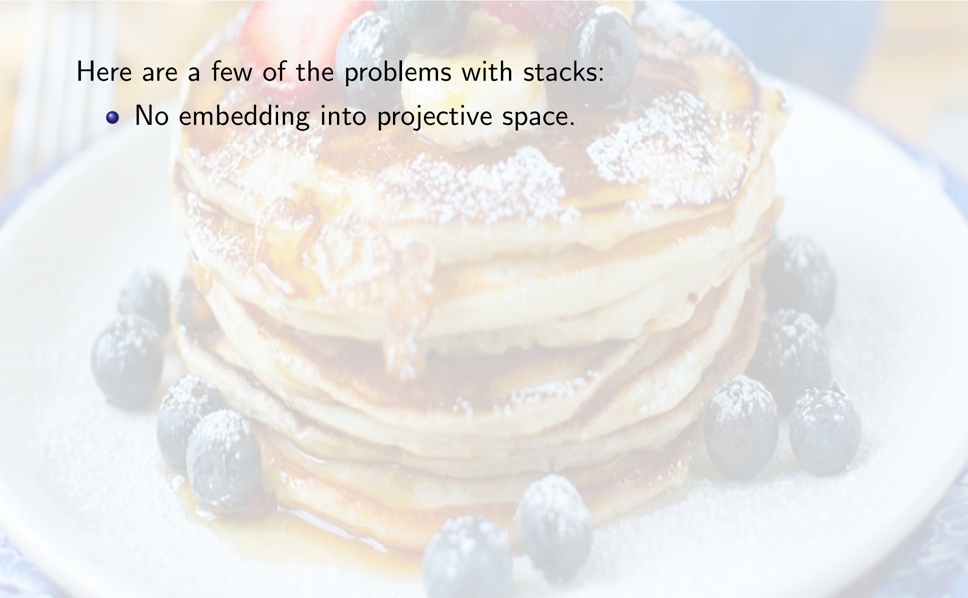
If $x \in X(\mathbb{Q})$ define the height of x as:

$$\mathrm{Ht}_{\mathcal{L}}(x) := \mathrm{Ht}(\phi_{\mathcal{L},n}(x))^{1/n}.$$

What to do about stacks

Here are a few of the problems with stacks:

- No embedding into projective space.



What to do about stacks

Here are a few of the problems with stacks:

- No embedding into projective space.
- No valuative criterion of properness.

What to do about stacks

Here are a few of the problems with stacks:

- No embedding into projective space.
- No valuative criterion of properness.
- Defining height in a way that is multiplicative can produce bad results, e.g. height with respect to perfectly good line bundles can be identically zero.

What to do about stacks

Here are a few of the problems with stacks:

- No embedding into projective space.
- No valuative criterion of properness.
- Defining height in a way that is multiplicative can produce bad results, e.g. height with respect to perfectly good line bundles can be identically zero.
- Sometimes, no good line bundles to work with (e.g. $B\mathbb{F}_p$).

What to do about stacks

Here are a few of the problems with stacks:

- No embedding into projective space.
- No valuative criterion of properness.
- Defining height in a way that is multiplicative can produce bad results, e.g. height with respect to perfectly good line bundles can be identically zero.
- Sometimes, no good line bundles to work with (e.g. $B\mathbb{F}_p$).

Fixing these

In a forthcoming paper, Ellenberg, Satriano and Zureick-Brown suggest a definition of height that fixes all of these. We will denote their height as: $\mathrm{Ht}_{\mathcal{L},ESZB}(x)$.

Weighted projective stacks

Let $a_0, a_1 \dots a_k$ be positive integers. Consider the $\mathbb{G}_m$ action on $\mathbb{A}^{k+1}$ given by:

$$\lambda \cdot (x_0, x_1 \dots x_k) := (\lambda^{a_0} x_0, \lambda^{a_1} x_1 \dots \lambda^{a_k} x_k).$$

Weighted projective stacks

Let $a_0, a_1 \dots a_k$ be positive integers. Consider the $\mathbb{G}_m$ action on $\mathbb{A}^{k+1}$ given by:

$$\lambda \cdot (x_0, x_1 \dots x_k) := (\lambda^{a_0} x_0, \lambda^{a_1} x_1 \dots \lambda^{a_k} x_k).$$

Definition

The weighted projective stack $\mathbb{P}(a_0, a_1 \dots a_k)$ is defined as $[(\mathbb{A}^{k+1} \setminus \{0\})/\mathbb{G}_m]$.

Weighted projective stacks

Let $a_0, a_1 \dots a_k$ be positive integers. Consider the $\mathbb{G}_m$ action on $\mathbb{A}^{k+1}$ given by:

$$\lambda \cdot (x_0, x_1 \dots x_k) := (\lambda^{a_0} x_0, \lambda^{a_1} x_1 \dots \lambda^{a_k} x_k).$$

Definition

The weighted projective stack $\mathbb{P}(a_0, a_1 \dots a_k)$ is defined as $[(\mathbb{A}^{k+1} \setminus \{0\})/\mathbb{G}_m]$.

Example: $\mathbb{P}(1, 1, \dots 1) \cong \mathbb{P}^k$.

Weighted projective stacks

Let $a_0, a_1 \dots a_k$ be positive integers. Consider the $\mathbb{G}_m$ action on $\mathbb{A}^{k+1}$ given by:

$$\lambda \cdot (x_0, x_1 \dots x_k) := (\lambda^{a_0} x_0, \lambda^{a_1} x_1 \dots \lambda^{a_k} x_k).$$

Definition

The weighted projective stack $\mathbb{P}(a_0, a_1 \dots a_k)$ is defined as $[(\mathbb{A}^{k+1} \setminus \{0\})/\mathbb{G}_m]$.

Example: $\mathbb{P}(1, 1, \dots 1) \cong \mathbb{P}^k$.
Example: $\mathbb{P}(2, 3)$ is a weighted $\mathbb{P}^1$ with two stacky points with automorphism groups μ_2 and μ_3.

Weighted projective stacks

Let $a_0, a_1 \dots a_k$ be positive integers. Consider the $\mathbb{G}_m$ action on $\mathbb{A}^{k+1}$ given by:

$$\lambda \cdot (x_0, x_1 \dots x_k) := (\lambda^{a_0} x_0, \lambda^{a_1} x_1 \dots \lambda^{a_k} x_k).$$

Definition

The weighted projective stack $\mathbb{P}(a_0, a_1 \dots a_k)$ is defined as $[(\mathbb{A}^{k+1} \setminus \{0\})/\mathbb{G}_m]$.

Example: $\mathbb{P}(1, 1, \dots 1) \cong \mathbb{P}^k$.
Example: $\mathbb{P}(2, 3)$ is a weighted $\mathbb{P}^1$ with two stacky points with automorphism groups μ_2 and μ_3.

Idea

We're going to map our stacks into weighted projective stacks.

ESZB Height on a nice enough stack

Proposition, [ESZB, '20]

Let $\mathcal{X}$ be a stack over $\operatorname{Spec}\mathbb{Z}$, let $\mathcal{L}$ be a line bundle on $\mathcal{X}$ such that $\mathcal{L}^{\otimes n}$ is generically globally generated by sections $s_0, s_1, s_2 \cdots s_k$. Let $x : \operatorname{Spec}\mathbb{Q} \to \mathcal{X}$ and for each i, let $x_i = x^*(s_i)$. Suppose you can scale $x_0, x_1, \ldots, x_k$ so that each $x_i \in \mathbb{Z}$ and for every prime p, there is some x_i such that $v_p(x_i) < n$. Then the height is given by:

$$\log \mathrm{Ht}_{\mathcal{L},ESZB}(x) = \frac{1}{n} \log \max\{|x_0|, |x_1|, \ldots |x_k|\} + O_{\mathcal{X}(\mathbb{Q})}(1).$$

Plan

Interpretation of Naive Height

Interpretation of Naive Height

- Recall that we defined the naive height of E as $\mathrm{Ht}_{naive}(E) = \max\{|A|^3, |B|^2\}$.

Interpretation of Naive Height

- Recall that we defined the naive height of E as $\mathrm{Ht}_{naive}(E) = \max\{|A|^3, |B|^2\}$.
- Recall that modular forms of weight k are sections of $\lambda^{\otimes k}$, where λ is the Hodge bundle.

Interpretation of Naive Height

- Recall that we defined the naive height of E as $\mathrm{Ht}_{naive}(E) = \max\{|A|^3, |B|^2\}$.
- Recall that modular forms of weight k are sections of $\lambda^{\otimes k}$, where λ is the Hodge bundle.
- $A \leftrightarrow E_4 \in \lambda^{\otimes 4}$, $B \leftrightarrow E_6 \in \lambda^{\otimes 6}$, and E_4^3 and E_6^2 globally generate $\lambda^{\otimes 12}$.

Interpretation of Naive Height

- Recall that we defined the naive height of E as $\mathrm{Ht}_{naive}(E) = \max\{|A|^3, |B|^2\}$.
- Recall that modular forms of weight k are sections of $\lambda^{\otimes k}$, where λ is the Hodge bundle.
- $A \leftrightarrow E_4 \in \lambda^{\otimes 4}$, $B \leftrightarrow E_6 \in \lambda^{\otimes 6}$, and E_4^3 and E_6^2 globally generate $\lambda^{\otimes 12}$.

Corollary

Consider $(E, C) \in \mathcal{X}_0(N)(\mathbb{Q})$, then

$$\mathrm{Ht}_{naive}(E) = const \cdot \mathrm{Ht}_{\lambda, ESZB}(E)^{12}.$$

Rings of modular forms

Theorem, [HT '11]

Let $M(N)$ denote the ring of modular forms of $\mathcal{X}_0(N)$. The following are the generators and relations of $M(N)$:

N	Degrees of generators	Relations
2	$(2, 4)$	None
3	$(2, 4, 6)$	$b^2 - ac$
4	$(2, 2)$	None
5	$(2, 4, 4)$	$b^2 - c(a^2 + 4b - 8c)$
6	$(2, 2, 2)$	$b^2 - ac$
8	$(2, 2, 2)$	$b^2 - ac$
9	$(2, 2, 2)$	$b^2 - ac$

Table 2: Ring of modular forms of low level

The final problem

- Now we have reduced our counting integers in a box with certain relations between them, e.g. for $\mathcal{X}_0(3)$, we count triples (a, b, c) such that $|a| < X^{1/6}$, $|b| < X^{1/3}$ and $|c| < X^{1/2}$, $b^2 = ac$ and $\gcd\{a^6, b^3, c^2\}$ is 12th power free.

Thank you for listening!