Counting points of bounded height on certain stacks

Soumya Sankar (Joint work with Brandon Boggess)

MSRI Introductory Workshop

September 4, 2020

Setup

- Let E be an elliptic curve over $\mathbb{Q}$.
- Any $E/\mathbb{Q}$ can be written in Weierstrass form, $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$.
- We will take E in minimal Weierstrass form, i.e. $\gcd(A^3, B^2)$ is 12th power-free.

Setup

- Let E be an elliptic curve over $\mathbb{Q}$.
- Any $E/\mathbb{Q}$ can be written in Weierstrass form, $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$.
- We will take E in minimal Weierstrass form, i.e. $\gcd(A^3, B^2)$ is 12th power-free.
- For any extension $K/\mathbb{Q}$, $E(K)$ has a group structure. An isogeny is a group homomorphism between two elliptic curves that is surjective on $\overline{\mathbb{Q}}$ points and has finite kernel.

Setup

- Let E be an elliptic curve over $\mathbb{Q}$.
- Any $E/\mathbb{Q}$ can be written in Weierstrass form, $E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$.
- We will take E in minimal Weierstrass form, i.e. $\gcd(A^3, B^2)$ is 12th power-free.
- For any extension $K/\mathbb{Q}$, $E(K)$ has a group structure. An isogeny is a group homomorphism between two elliptic curves that is surjective on $\overline{\mathbb{Q}}$ points and has finite kernel.
- Let $N \in \mathbb{Z}_{\geq 1}$. 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

Main Question

Question

How many elliptic curves have a rational N-isogeny?

Main Question

Question

How many elliptic curves have a rational N-isogeny?

- Complete list of N for which there is at least one such elliptic curve: Mazur, Kenku (building on work of Ogg, Joly, Ligozat).

Main Question

Question

How many elliptic curves have a rational N-isogeny?

- Complete list of N for which there is at least one such elliptic curve: Mazur, Kenku (building on work of Ogg, Joly, Ligozat).
- 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?

- Complete list of N for which there is at least one such elliptic curve: Mazur, Kenku (building on work of Ogg, Joly, Ligozat).
- 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?

Notation

Counting function

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

Notation

Counting function

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

Goal: To find a function $h_N(X)$ such that, there exist $K_1, K_2 > 0$ such that

$$K_1 h_N(X) \leq \mathcal{N}(N, X) \leq K_2 h_N(X).$$

Notation

Counting function

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

Goal: To find a function $h_N(X)$ such that, there exist $K_1, K_2 > 0$ such that

$$K_1 h_N(X) \leq \mathcal{N}(N, X) \leq K_2 h_N(X).$$

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	$X^{1/6}\log(X)$
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

Outline of talk

- Moduli spaces of elliptic curves
  - Classical description
  - Stacks: What and Why?
- Height functions
- Outline of proof for $N = 2, 3, 4, 5, 6, 8, 9$.

Moduli spaces of elliptic curves

- Since we want to count elliptic curves, we must find a space that parametrizes pairs (E, C) where E is an elliptic curve and $C \subset E$, with $C \cong \mathbb{Z}/N\mathbb{Z}$.
- In other words, we want a space Y such that, for any scheme S,

$$\mathrm{Hom}(S, Y) = \{\text{Families of elliptic curves } E/S, \mathbb{Z}/N\mathbb{Z} \cong_S C \subset E\}.$$

- Unfortunately, such a space Y does not exist. At least, not in the category of schemes.
- Fact: under some technical conditions, a moduli problem is representable by a scheme if and only if it is rigid. That is, the objects a scheme parametrizes are not allowed to have non-trivial automorphisms.
- A pair (E, C) always has the automorphism $[-1] : P \mapsto -P$. So the space that represents this functor is actually a *stack*.

Modular curves: the classical picture

Modular curves: the classical picture

- Let $\mathfrak{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$.
- Define $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ as the subgroup of matrices that reduce modulo N to:
$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$
- We have the usual action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{H}$, $z \mapsto \frac{az+b}{cz+d}$.
- Denote by $Y_0(N)$, the usual quotient of $\mathfrak{H}$ by $\Gamma_0(N)$, i.e. the orbits under the action.
- Denote by $X_0(N)$, the compactification of $Y_0(N)$, constructed by adding in cusps.

Modular curves: continued

- Every elliptic curve over $\mathbb{C}$ can be written as $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathfrak{H}$. Further, two complex elliptic curves are isomorphic if and only if the lattices defining them are homothetic.
- Thus $Y_0(1)(\mathbb{C})$ is in bijection with the set of isomorphism classes of elliptic curves over $\mathbb{C}$. Further, $X_0(1) \cong \mathbb{P}^1$ via the j-invariant map.
- Similarly, $Y_0(N)(\mathbb{C})$ is in bijection with the set of isomorphism classes of ellipic curves, with a rational N-isogeny.

Modular curves: continued

- Every elliptic curve over $\mathbb{C}$ can be written as $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathfrak{H}$. Further, two complex elliptic curves are isomorphic if and only if the lattices defining them are homothetic.
- Thus $Y_0(1)(\mathbb{C})$ is in bijection with the set of isomorphism classes of elliptic curves over $\mathbb{C}$. Further, $X_0(1) \cong \mathbb{P}^1$ via the j-invariant map.
- Similarly, $Y_0(N)(\mathbb{C})$ is in bijection with the set of isomorphism classes of ellipic curves, with a rational N-isogeny.
- Q: Are these moduli spaces good?
- Not for us. For instance, there are infinitely many elliptic curves over $\mathbb{Q}$ that have the same j-invariant.
- Even over $\mathbb{C}$, families create trouble. For instance, the family $ty^2 = x^3 + Ax + B$ over $\mathbb{C}[t]$ is a non-constant family, but with constant j-invariant.

Modular curves: continued

- The problem is that the usual quotient, doesn't take stabilizers into account.
- Since $-I \in \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ acts trivially on $\mathfrak{H}$, every point has non-trivial stabilizer. Some points have order 4 and order 6 stabilizers too.

Modular curves: continued

- The problem is that the usual quotient, doesn't take stabilizers into account.
- Since $-I \in \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ acts trivially on $\mathfrak{H}$, every point has non-trivial stabilizer. Some points have order 4 and order 6 stabilizers too.
- The correct notion of a quotient here is the *orbifold quotient*, or the *stacky* quotient.
- Roughly speaking, the stacky quotient remembers the orbits of the action, as well as the automorphisms of the orbits.

Modular curves: continued

- The problem is that the usual quotient, doesn't take stabilizers into account.
- Since $-I \in \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ acts trivially on $\mathfrak{H}$, every point has non-trivial stabilizer. Some points have order 4 and order 6 stabilizers too.
- The correct notion of a quotient here is the *orbifold quotient*, or the *stacky* quotient.
- Roughly speaking, the stacky quotient remembers the orbits of the action, as well as the automorphisms of the orbits.
- We will denote by $\mathcal{X}_0(N)$ the compactification of the modular curve $\mathcal{Y}_0(N)$ parametrizing families of elliptic curves with an N-isogeny.

What does $\mathcal{X}_0(1)$ look like?

For this, we must talk about weighted projective spaces.

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

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

Definition

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

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

Moduli interpretation of (weighted) projective space

- Moduli theoretically, an S-point on $\mathbb{P}^k$ is the choice of a line bundle $\mathcal{L}$ on S with $k+1$ sections of $\mathcal{L}$, that don't simultaneously vanish.

- Similarly, on $\mathbb{P}(a_0, a_1 \dots a_k)$, an S-point is a choice of a line bundle $\mathcal{L}$ along with $k+1$ sections $s_0, s_1 \dots s_k$ with $s_i \in \mathcal{L}^{\otimes a_i}$.

Modular forms

- A modular form f of weight k and level N is a holomorphic function on $\mathfrak{H}$ that satisfies:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathfrak{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

Modular forms

- A modular form f of weight k and level N is a holomorphic function on $\mathfrak{H}$ that satisfies:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathfrak{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

- These are actually sections of k-th powers of a line bundle called the Hodge bundle.

Fact

If $E : y^2 = x^3 + Ax + B$, then A and B are (up to a constant), modular forms of weight 4 and 6 respectively.

Modular forms

- A modular form f of weight k and level N is a holomorphic function on $\mathfrak{H}$ that satisfies:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $z \in \mathfrak{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

- These are actually sections of k-th powers of a line bundle called the Hodge bundle.

Fact

If $E : y^2 = x^3 + Ax + B$, then A and B are (up to a constant), modular forms of weight 4 and 6 respectively.

- In particular, a point of $\mathcal{X}_0(1)$ maps via $[A : B]$ to a point of $\mathbb{P}(4, 6)$.
- Thus we get a map of stacks $\mathcal{X}_0(1) \to \mathbb{P}(4, 6)$, which is an isomorphism over $\mathbb{Z}[1/6]$.

Heights on projective space

Height is a measure of complexity.

Examples of Heights

Absolute value of an integer, discriminant of a number field, canonical height on an abelian variety, Faltings height, discriminant of a quaternion algebra, volume of a manifold, distance functions on graphs, etc.

Heights on projective space

Height is a measure of complexity.

Examples of Heights

Absolute value of an integer, discriminant of a number field, canonical height on an abelian variety, Faltings height, discriminant of a quaternion algebra, volume of a manifold, distance functions on graphs, etc.

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

Definition

The height of x is

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

where the product is over all places of $\mathbb{Q}$.

Heights on projective varieties

- Let X be a projective variety. This means that there is some embedding $\phi : X \hookrightarrow \mathbb{P}^k$. Such a map is induced by sections of some line bundle, say L.

Heights on projective varieties

- Let X be a projective variety. This means that there is some embedding $\phi : X \hookrightarrow \mathbb{P}^k$. Such a map is induced by sections of some line bundle, say L.
- Let $x \in X(\mathbb{Q})$. Define $\mathrm{Ht}_L(x) := \mathrm{Ht}(\phi(x))$.

Heights on projective varieties

- Let X be a projective variety. This means that there is some embedding $\phi : X \hookrightarrow \mathbb{P}^k$. Such a map is induced by sections of some line bundle, say L.
- Let $x \in X(\mathbb{Q})$. Define $\mathrm{Ht}_L(x) := \mathrm{Ht}(\phi(x))$.
- Properties:
  - If $\mathcal{L}_1$ and $\mathcal{L}_2$ are two line bundles on X, then $\mathrm{Ht}_{\mathcal{L}_1 \otimes \mathcal{L}_2}$ and $\mathrm{Ht}_{\mathcal{L}_1} \cdot \mathrm{Ht}_{\mathcal{L}_2}$ are off by a constant.
  - If $\mathcal{L}_1 \sim \mathcal{L}_2$, then $\mathrm{Ht}_{\mathcal{L}_1}$ and $\mathrm{Ht}_{\mathcal{L}_2}$ are off by a constant.
  - (Northcott property) For any $B > 0$, the number of points of height bounded by B is finite.

Heights on projective varieties

- Let X be a projective variety. This means that there is some embedding $\phi : X \hookrightarrow \mathbb{P}^k$. Such a map is induced by sections of some line bundle, say L.
- Let $x \in X(\mathbb{Q})$. Define $\mathrm{Ht}_L(x) := \mathrm{Ht}(\phi(x))$.
- Properties:
  - If $\mathcal{L}_1$ and $\mathcal{L}_2$ are two line bundles on X, then $\mathrm{Ht}_{\mathcal{L}_1 \otimes \mathcal{L}_2}$ and $\mathrm{Ht}_{\mathcal{L}_1} \cdot \mathrm{Ht}_{\mathcal{L}_2}$ are off by a constant.
  - If $\mathcal{L}_1 \sim \mathcal{L}_2$, then $\mathrm{Ht}_{\mathcal{L}_1}$ and $\mathrm{Ht}_{\mathcal{L}_2}$ are off by a constant.
  - (Northcott property) For any $B > 0$, the number of points of height bounded by B is finite.

Aside

Not all heights come from line bundles, but we like the ones that do.

Heights on stacks

Here are a few problems with defining heights on 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.

Heights on stacks

Here are a few problems with defining heights on 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.

Fixing these

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

Heights on stacks

Here are a few problems with defining heights on 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.

Fixing these

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

If a stack $\mathcal{X}$ is a variety, then their height specializes to the usual height on a variety.

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 logarithmic height is given by:

$$\log \mathrm{Ht}_{\mathcal{L},ESZB}(x) = \frac{1}{n} \log \max_i\{|x_0|, |x_1|, |x_2| \ldots |x_k|\} + O_{\mathcal{X}(\mathbb{Q})}(1).$$

How does this help us?

- Recall that modular forms are sections of line bundles on $\mathcal{X}_0(N)$.
- Recall that naive height of an elliptic curve was defined as: $\max\{|A|^3, B^2\}$.

How does this help us?

- Recall that modular forms are sections of line bundles on $\mathcal{X}_0(N)$.
- Recall that naive height of an elliptic curve was defined as: $\max\{|A|^3, B^2\}$.

Corollary

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

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

where λ is the Hodge bundle.

How does this help us?

- Recall that modular forms are sections of line bundles on $\mathcal{X}_0(N)$.
- Recall that naive height of an elliptic curve was defined as: $\max\{|A|^3, B^2\}$.

Corollary

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

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

where λ is the Hodge bundle.

- To count points of bounded height on $\mathcal{X}_0(N)$, we needed to count integers A and B in a box, with certain relations between them.
- The above corollary allows us to replace sections A and B with other sections, i.e. other modular forms, with easier relations between them.
- Rings of modular forms of low level are very well studied.

The  conjecture

- Let X be a smooth projective variety that has lots of $\mathbb{Q}$-rational points.

The  conjecture

- Let X be a smooth projective variety that has lots of $\mathbb{Q}$-rational points.
- Suppose X is equipped with a height coming from a line bundle L.

The  conjecture

- Let X be a smooth projective variety that has lots of $\mathbb{Q}$-rational points.
- Suppose X is equipped with a height coming from a line bundle L.
- Let $B > 0$ be any real number, and let $U \subset X$ be the largest Zariski open subset not containing an accumulating subvariety.

The  conjecture

- Let X be a smooth projective variety that has lots of $\mathbb{Q}$-rational points.
- Suppose X is equipped with a height coming from a line bundle L.
- Let $B > 0$ be any real number, and let $U \subset X$ be the largest Zariski open subset not containing an accumulating subvariety.

(Strong) Batyrev-Manin Conjecture

The number of rational points on U of height bounded by B is asymptotic to

$$cB^a \log(B)^{b-1},$$

for some explicit constants a, b, c depending on X, L and $\mathbb{Q}$, but not on B.

The  conjecture

- Let X be a smooth projective variety that has lots of $\mathbb{Q}$-rational points.
- Suppose X is equipped with a height coming from a line bundle L.
- Let $B > 0$ be any real number, and let $U \subset X$ be the largest Zariski open subset not containing an accumulating subvariety.

(Strong) Batyrev-Manin Conjecture

The number of rational points on U of height bounded by B is asymptotic to

$$cB^a \log(B)^{b-1},$$

for some explicit constants a, b, c depending on X, L and $\mathbb{Q}$, but not on B.

The constant c was predicted by Peyre. In the weak form, the asymptotic is replaced by $O(B^{a+\epsilon})$.

History

- The Batyrev-Manin conjecture has been studied widely.
- The strong form is known to be true for certain del Pezzo surfaces (Manin-Tschinkel, 1993), toric varieties (Batyrev-Tschinkel, 1995), certain generalized flag varieties (Franke-Manin-Tschinkel, 1989), low degree surfaces (Frei-Loughran 2019).

History

- The Batyrev-Manin conjecture has been studied widely.
- The strong form is known to be true for certain del Pezzo surfaces (Manin-Tschinkel, 1993), toric varieties (Batyrev-Tschinkel, 1995), certain generalized flag varieties (Franke-Manin-Tschinkel, 1989), low degree surfaces (Frei-Loughran 2019).
- It is also known to be false for certain varieties, e.g. certain cubic bundles (Batyrev-Tschinkel, 1996).

History

- The Batyrev-Manin conjecture has been studied widely.
- The strong form is known to be true for certain del Pezzo surfaces (Manin-Tschinkel, 1993), toric varieties (Batyrev-Tschinkel, 1995), certain generalized flag varieties (Franke-Manin-Tschinkel, 1989), low degree surfaces (Frei-Loughran 2019).
- It is also known to be false for certain varieties, e.g. certain cubic bundles (Batyrev-Tschinkel, 1996).
- There are formulations over other fields.

Final comments and questions

- Ellenberg, Satriano and Zureick-Brown predict a (weak) Batyrev-Manin-like asymptotic for ratonal points on stacks.
- Ongoing work: what are the constants for modular curves, and do they match reality?
- Question: what are other kinds of spaces, perhaps originating from hyperbolic geometry, that one can run the height machinery on? What does it mean to count points on them?

Thank you for listening!