25.1. Elliptic curves over $\mathbb{Q}$.

Basic Theorem (Mordell - Weil) Let $E/\mathbb{Q}$ be an EC.
The group $E(\mathbb{Q})$ is finitely generated.
This means that

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

where $\left\{\begin{array}{l}\text{the torsion subgroup } \mathrm{Tor}(E) \\ \text{the rank } r\end{array}\right\}$ are finite.

(The same is true when $\mathbb{Q}$ is replaced by any number field.)

Mazur's Theorem. $\mathrm{Tor}(E)$ is $\mathbb{Z}/m\mathbb{Z}$ for $1 \le m \le 10$
or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ $1 \le m \le 4$.

(Conversely, all of these groups occur for infinitely many EC's E.)

Goldfeld's Conjecture.

"Half of all elliptic curves" have rank 0
Half have rank 1
The rest have rank ≥ 2.

The Bounded Rank Conjecture. (Park, Poonen, Voight, Wood, 2016 (!!))

There is some integer r_{max} s.t.
$\mathrm{rk}\, E(\mathbb{Q}) \le r_{max}$ for all ell. curves $E/\mathbb{Q}$.

Indeed, probably $\mathrm{rk}\, E \le 21$ for all but finitely many.

25.2.

Average Ranks:

Theorem. (Bhargava - Shankar, 2013)

The average rank of EC's over $\mathbb{Q}$, when bounded by height, is $\leq .885$.

More precisely: An EC/$\mathbb{Q}$ can be rewritten

$$E: y^2 = x^3 + Ax + B$$

Then $H(E) = \max\{4|A|^3, 27B^2\}$.

Then
$$\limsup_{M \to \infty} \frac{\sum_{Ht(E) \leq M} rk(E)}{\sum_{Ht(E) \leq M} 1} \leq 0.885.$$

We'll focus on proving Mordell-Weil.

Two components.

(1) The "Weak Mordell-Weil Theorem":

The group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

(In fact: For any NF K and positive integer m,
$E(K)/mE(K)$ is finite.

In particular, this yields that the rank is finite, but not necessarily the torsion.

(2) Height functions.

There is a <u>height function</u> $h: E(\mathbb{Q}) \longrightarrow [0, \infty)$ satisfying:

(1) For any point $Q \in E$, there is a constant $C_1 = C_1(E, Q)$ ~~with~~ so that for all $P \in E$,

$$h(P+Q) \leq 2h(P) + C_1.$$

(2) There is an integer $m \geq 2$ and constant $C_2 = C_2(E)$ with $h(mP) \geq m^2 h(P) - C_2$ for all $P \in E$.

(3) For <u>every</u> constant $C_3 > 0$, $\{P \in E(\mathbb{Q}) : h(P) \leq C_3\}$ is finite.

<u>Proposition</u>. ("Descent Theorem") Let A be any abelian group satisfying (1)-(3) and s.t. A/mA is finite. Then A is finitely generated.

The game plan.

(a) Define the height, show how it interacts with the group law, and prove (1)-(3) above. (Not too bad)

(b) Prove the descent theorem (easy)

(c) Prove Week Mordell-Weil (subtlest)

(d) Further discussion of (c).
Selmer and Shafarevich-Tate groups, BSD etc.

25.4.

Heights on projective space.

For some N, given $[x_0 : \cdots : x_N] \in \mathbb{P}^N(\mathbb{Q})$.

We have $[x_0 : \cdots : x_N] = \left[\frac{a_0}{b_0} : \frac{a_1}{b_1} : \cdots : \frac{a_N}{b_N}\right]$

where not all the a_i are zero, and all the a_i, b_i are integers.

After multiplying by $\operatorname{lcm}(b_i)$ we may assume that the x_i are all integers with no common factor.

Up to ± 1, we may write any point of $\mathbb{P}^N(\mathbb{Q})$ in such a way.

Definition. Given $P = [x_0 : \cdots : x_N] \in \mathbb{P}^N(\mathbb{Q})$ represented as above. Its height is

$$H(P) = \max(|x_0|, \cdots, |x_N|)$$

and its logarithmic height is

$$h(P) = \log H(P).$$

Lemma. For any B, $\{P \in \mathbb{P}^N(\mathbb{Q}) : h(P) \leq B\}$ is finite.

Proof. If $h(P) \leq B$, then

$$P = [x_0 : \cdots : x_n] \text{ with all } x_i \text{ in } [-e^B, e^B].$$

"Schanuel's Theorem".

For any B,

$$\{P \in \mathbb{P}^N(\mathbb{Q}) : H(P) \leq B\} \sim \frac{2^n}{\zeta(n+1)} B^{n+1}.$$

Exercise! This is not difficult.

25.5.

To get heights on an elliptic curve, we could embed into $\mathbb{P}^2$. But, the following is easier. Define

$$\begin{array}{ccc} E(\mathbb{Q}) & \xrightarrow{\pi} & \mathbb{P}^1(\mathbb{Q}) \\ [x:y:1] & \longrightarrow & [x:1] \\ [0:1:0] & \longrightarrow & [1:0]. \end{array}$$

Exercise. Is π a morphism?

Then define $H(P) = H(\pi(P))$ and similarly with h.

Heights and the group law.

Given $(x,y) = P \in E(\mathbb{Q})$. $E: \ y^2 = x^3 + Ax + B$

Recall we had

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

If $x = \frac{a}{b}$ with a, b big and coprime, here we get a fraction with denominator b^4. The numerator should also be something like a^4.

So expect $h(2P) \sim 4 \cdot h(P)$, at least if $h(P)$ is big enough.

Problem. Is there any cancellation?

Heights on algebraic varieties.

In $\mathbb{P}^N(\mathbb{Q})$, write $x = (x_0 : x_1 : \cdots x_n)$ with all $x_i \in \mathbb{Z}$ no common factor

$$H(x) = \max_i (|x_i|), \quad h(x) = \log H(x).$$

Define a height on $E(\mathbb{Q})$ by
$$E \xrightarrow{\pi} \mathbb{P}^1$$
$$[x:y:1] \to [x:1]$$
$$[0:1:0] \to [1:0]$$

$$H(P) := H(\pi(E)).$$

Claim. For any constant $C_3 > 0$,
$\{P \in E(\mathbb{Q}) : h(P) \leq C_3\}$ is finite.

This is obvious, if $h(P) \leq C_3$ then $x(P) = \frac{a}{b}$ with $|a|, |b| \leq e^{C_3}$. Only finitely many such. For fixed x, two possibilities for y.

Claim. Let $P_0 \in E(\mathbb{Q})$. There is a constant $C_1 = C_1(P_0, E)$ such that $h(P + P_0) \leq 2h(P) + C_1$ for all P.

Proof. (Exercise: do the algebra. verify details)
Taking $C_1 > \max(h(P_0), h(2P_0))$, may assume $P_0 \neq 0$, $P \neq 0, \pm P_0$.

Write
$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right) \qquad P_0 = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right)$$

in lowest terms.

26.2.

Why like this? $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$.

If $v_p(x) = a$ with $a < 0$,

$v_p(x^3 + Ax + B) = 6a$. So $v_p(y) = 3a$.

The addition formula says,

$$x(P + P_0) = \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0$$

$$= \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}$$

Is it in lowest terms? Maybe. Maybe not. We don't care.

$H(P + P_0) \leq \max(|\text{numerator}|, |\text{denominator}|)$

Then (exercise): This is $\leq C \max(|a|^2, |d|^4, |bd|)$.

allowed to depend on A, B, a_0, b_0, d_0

Almost what we want!

$H(P) = \max(|a|, |d|^2)$. $|bd|$ is annoying.

Can we bound b?

We know

$$\left(\frac{b}{d^3}\right)^2 = \left(\frac{a}{d^3}\right)^3 + A\left(\frac{a}{d^3}\right) + B$$

$$b^2 = a^3 + Aad^4 + Bd^6$$

and so $\quad |b| \leq C' \max(|a|^{3/2}, |d|^3)$.

another const. depends on A, B.

So $|bd| \leq C' \max(|a|^{3/2}|d|, |d|^4)$

and $H(P+P_0) \leq CC' \max(|a|^2, |d|^4, |a|^{3/2}|d|)$
$\leq C'' \max(|a|^2, |d|^4)$ as required.

<u>Remark</u>. This didn't really depend on the specifics of what we were doing.

<u>Final claim</u>. There is a constant $C_2 = C_2(A, B)$ s.t. for all $P \in E(\mathbb{Q})$,

$$h(2P) \geq 4h(P) - C_2.$$

This is harder. Do you see why?

<u>Proof</u>. We may assume $2P \neq 0$.
(Choose $C_2 \geq 4h(T)$ for all $T \in E(\mathbb{Q})[2]$.)

Then $x(2P) = \dfrac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}$.

What is easy. Prove $h(2P) \leq 4h(P) + C_3$.

Proof of claim in Silverman-Tate.

$y^2 = f(x)$

We also had
$$x(2P) = \frac{(f'(x))^2 - 8x\,f(x)}{4f(x)}$$
where f and f' do not share a common root.
So the numerator and denominator don't.

Prove our claim in more generality.

Lemma. (Silverman–Tate, p. 72)

Let ϕ, ψ be integer polynomials w/no common roots. Let d be the maximum of the degrees.

(a) There is an integer $R \geq 1$ depending on ϕ, ψ s.t. for all rational numbers $\frac{m}{n}$,

$$\gcd\left(n^d \phi\left(\frac{m}{n}\right), n^d \psi\left(\frac{m}{n}\right)\right) \text{ divides } R.$$

(b) There are constants c_1, c_2 ~~etc~~ depending on ϕ, ψ s.t. for all rational numbers $\frac{m}{n}$, not roots of ψ,

$$d h\left(\frac{m}{n}\right) - c_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq d h\left(\frac{m}{n}\right) + c_2.$$

In some sense (a) is the point. You don't get much cancellation in $\dfrac{\phi(m/n)}{\psi(m/n)}$.

Proof. (a) WLOG $d = \deg(\phi) \geq \deg(\psi)$. (Can switch!!)

Write $n^d \phi\left(\frac{m}{n}\right) = a_0 m^d + a_1 m^{d-1} n + \cdots + a_d n^d$

with all $a_i \in \mathbb{Z}$.

Now $\phi(X)$ and $\psi(X)$ have no common roots. By the Euclidean algorithm there exist $F(X), G(X) \in \mathbb{Q}[X]$ with

$$F(X)\phi(X) + G(X)\psi(X) = 1.$$

Choose $A \in \mathbb{Z}$ with $AF(X), AG(X) \in \mathbb{Z}[X]$.

Write $D = \max(\deg F, \deg G)$.

26.5.

Evaluate our identity at $X = \frac{m}{n}$

$$F\left(\frac{m}{n}\right)\phi\left(\frac{m}{n}\right) + G\left(\frac{m}{n}\right)\psi\left(\frac{m}{n}\right) = 1$$

$$\left(n^D A F\left(\frac{m}{n}\right)\right)\cdot n^d\phi\left(\frac{m}{n}\right) + \left(n^D A G\left(\frac{m}{n}\right)\right)\cdot n^d\psi\left(\frac{m}{n}\right) = A n^{D+d}.$$

Let $\gamma = \gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right)$, $\gamma \mid A n^{D+d}$.

we claim $\gamma \mid A a_0^{D+d}$. (this will prove (a))

why?

$$\gamma \mid A n^{D+2d-1}\phi(m,n) = A a_0 m^d n^{D+d-1} + A a_1 m^{d-1} n^{D+d} + \cdots + A a_d n^{D+2d-1}.$$

Every term after the first is an integer times $A n^{D+d}$

So $\gamma \mid A a_0 m^d n^{D+d-1}$ and $\gamma \mid A n^{D+d}$ $(m,n)=1$.

So $\gamma \mid A a_0 n^{D+d-1}$.

So repeat the above with $\gamma \mid A a_0 n^{D+2d-2}$

$\Rightarrow \gamma \mid A a_0^2 n^{D+d-2}$

etc. Get $\gamma \mid A a_0^{D+d}$.