Goal: Descent Theorem

Height \( x \in \mathbb{Q} \) \( x = \frac{m}{n} \) in lowest terms.

(big H) \( H(x) = \max(|m|, |n|) \).

\( x = 1 \) \( H(x) = 1 \)
\( x = \frac{99999}{100000} \) \( H(x) = 100000 \)

Finiteness Property of the Height

The set of all \( x \in \mathbb{Q} \) s.t. \( H(x) \leq K \) is a finite set.

Proof: If \( H(x) \leq K \rightarrow |m| \leq K \), \( |n| \leq K \)
so there are finite ways to choose \( x \).

Height of Points.

\( P = (x, y) \) then height of \( P = H(x) \).

Logarithmic Height. (little h).

\( h(x) = \log H(x) \).

Finiteness Property of Rational Points.

For any positive number \( M \)

\( \{ P \in \mathbb{C}(\mathbb{Q}) : H(P) \leq M \} \) is a finite set.
Finitely many ways to choose the $X$-coordinate
Two possible $y$-coords.

**Point at Infinity**

$h(0) = 1 \quad h(0) = 0.$

**Lemma 1:** For any positive number $M$
\[ \exists P \in C(Q) : h(P) \leq M \] is finite.

**Lemma 2:** Let $P_0$ be a fixed rational point on $C$.
There is a constant depending on $P_0$ and $q_1, c$
\[ \forall P \in C(Q) \quad h(P + P_0) \leq 2h(P) + K_0. \]

**Lemma 3:** There is a constant $K$ depending on $q_1, c$
\[ \forall P \in C(Q) \quad h(2P) \geq 4h(P) - K. \]

**Lemma 4:** The index $(C(Q), 2C(Q))$ is finite.

**Multiplication by $m$ map**

For any commutative group $\mathbb{G}$,
\[ \mathbb{G} \rightarrow \mathbb{G} \quad P \rightarrow \underbrace{P + P + \ldots + P}_{m \text{ times}} = mP \]
is a homomorphism, and the image is a subgroup $m\Gamma$ of $\Gamma$.

Descent Theorem

Let $\Gamma$ be a commutative group.

Suppose that there is a function

$$h: \Gamma \rightarrow [0, \infty)$$

with the following properties:

(a) For any real number $M$ the set $\{p \in \Gamma \mid h(p) \leq M\}$ is finite.

(b) For every $p_0 \in \Gamma$, there is a constant $K_0$ s.t.

$$h(p + p_0) \leq 2h(p) + K_0 \quad \forall p \in \Gamma.
$$

(c) There is a constant $K$ so that $h(2p) \leq 4h(p) - K \quad \forall p \in \Gamma
$$

(d) The subgroup $2\Gamma$ has finite index in $\Gamma$.

Then $\Gamma$ is finitely generated.

(1) Take a representative for each coset of $2\Gamma$ in $\Gamma$.

There are finitely many cosets, say $n$, so let $Q_1, Q_2, \ldots, Q_n$ be the representatives.

For any $p \in \Gamma$, there is an index $i_1$ depending on $p$

s.t. $p - Q_{i_1} \in 2\Gamma$.

$p - Q_{i_1} = 2p_1$ \text{ for some } p_1 \in \Gamma.

$p_1 - Q_{i_2} = 2p_2$

$p_2 - Q_{i_3} = 2p_3$

\vdots

$p_{n-1} - Q_{i_n} = 2p_n

\quad \text{ where } Q_i's \text{ are chosen from } Q_1, \ldots, Q_n \text{ and }$
2. \( P = Q_{11} + 2P_1 \)
   \( P_1 = Q_{12} + 2P_2 \)

   \[ P = Q_{11} + 2Q_{i2} + 4Q_{i3} + \cdots + 2^{m-1}Q_{im} + 2^{m-1}P_m \]

   \( P \) is in the subgroup of \( \Gamma \) generated by \( Q_i \)'s and \( P_m \).

3. Take one of the \( P_i \)'s in the sequence of \( P, P_1, P_2, \ldots \) and examine the relation between \( h(P_j) \) and \( h(P_{j-1}) \).

   \[ h(P - Q_{i1}) \leq 2h(p) + k_i \quad \forall P \in \Gamma. \]

   Do this for all \( Q_{i1}, 1 \leq i \leq n \).

   Let \( k' \) be the largest of the \( k_i \)'s.

   \[ h(P - Q_{i1}) \leq 2h(p) + k' \quad \forall P \in \Gamma, 1 \leq i \leq n. \]

4. Let \( k \) be the constant from (c).

   \[ 4h(P_j) \leq h(2P_j) + k = h(P_{j-1} - Q_{ij}) + k \]

   \[ \leq 2h(P_{j-1}) + k + k \]

   \[ h(P_j) \leq \frac{1}{2} h(P_{j-1}) + \frac{k' + k}{4} \]

   \[ = \frac{3}{4} h(P_{j-1}) - \frac{1}{4} (h(P_{j-1}) - k' + k) \]

**Bottom Line**

If \( h(P_{j-1}) \geq k' + k \) then

\[ h(P_j) \leq \frac{3}{4} h(P_{j-1}). \]
(5) In the sequence of points $P, P_1, P_2, \ldots$
   Each point has a height smaller than the previous pt.
   (if we haven't yet reached $P_m$)
   Eventually we reach a point $P_m$
   \[ h(P_m) \leq K' + K. \]

Conclusion. We have shown that for all elements \( P \in \mathcal{M} \),
\( P \) can be written as
\[ P = a_1 Q_1 + a_2 Q_2 + \ldots + a_n Q_n + 2^m R, \quad R \in \mathcal{M} \]
satisfying
\[ h(R) \leq K + K'. \]

Hence the set
\[ \{ Q_1, \ldots, Q_m \} \cup \{ R \in \mathcal{M} : h(R) \leq K + K' \} \]
will generate \( \mathcal{M} \).

Therefore \( \mathcal{M} \) is finitely generated.