Prop: Let F be a number field. Recall

$$|F| = \{\text{maximal ideals of } \mathcal{O}_F\} \cup \{\tau : F \hookrightarrow \mathbb{C}\}/_{\mathrm{Gal}(\mathbb{C}/\mathbb{R})}$$

For $v \in |F|$, set $|\cdot|_v$ = normalized absolute value on $F \subset F_v = \begin{cases} F_\beta & \text{if } v = \beta \subset \mathcal{O}_F \\ \mathbb{R} \text{ or } \mathbb{C} \text{ according to whether } \tau(F) \subset \mathbb{R} \text{ or not.} \end{cases}$

Then $\prod_{v \in |F|} |a|_v = 1$ for all $a \in F^\times$.

Pf — pset 6.

Defn: $H_F : \mathbb{P}^n(F) \longrightarrow \mathbb{R}$ is defined by

$$H_F(P) = \prod_{v \in |F|} \max\{|x_0|_v, \dots, |x_n|_v\} \quad \text{for any}$$

representation $P = [x_0, \dots, x_n]$, $x_i \in F$.

Lemma: $H_F(P)$ is well-defined, ind. of choice of homogeneous coords $x_0, \dots, x_n$.

Pf: For $a \in F^\times$, replacing $(x_0, \dots, x_n)$ by $(ax_0, \dots, ax_n)$ does not change $\prod \max\{|ax_0|_v, \dots, |ax_n|_v\}$.

$$= \prod_{v \in M_F} |a|_v \cdot \prod_{v \in |F|} \max\{|x_0|_v, \dots, |x_n|_v\}.$$

1 by the product formula. ∎

- For $F = \mathbb{Q}$, this agrees with the previous defn.

(for $x_0, \dots, x_n \in \mathbb{Z}$ with $\gcd = 1$,

$$H_{\mathbb{Q}}([x_0, \dots, x_n]) = \prod_{v \in |\mathbb{Q}|} \max_i \{|x_i|_v\} = \max\{|x_i|_\infty\}$$

since for all p, all $|x_i|_p \le 1$ and some $|x_i|_p = 1$. ——

- For L/F finite, $P \in \mathbb{P}^n(F) \subset \mathbb{P}^n(L)$,

$$H_L(P) = H_F(P)^{[L:F]}. \quad (P = [x_0, \dots, x_n].\ x_i \in F)$$

Pf: $H_L(P) = \prod_{w \in |L|} \max\{|x_i|_w\} \overset{(*)}{=} \prod_{v \in |F|} \prod_{w|v} \max\{|x_i|_v^{[L_w:F_v]}\}$

$$= \prod_{v \in |F|} \max\{|x_i|_v\}^{\sum_{w|v}[L_w:F_v]} = H_F(P)^{[L:F]}.$$

$[L:F]$

The change-of-field result allows us to define

$$H : \mathbb{P}^n(\overline{\mathbb{Q}}) \to \mathbb{R} \quad \text{by:}$$

$$H(P) = H_L(P)^{1/[L:\mathbb{Q}]} \quad \text{for any}$$

number field L: $P \in \mathbb{P}^n(L)$. (independent of choice of L!)

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

exercise: $\forall \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $h(\sigma P) = h(P)$.

Theorem ① Let $F: \mathbb{P}^n \longrightarrow \mathbb{P}^m$ be a morphism given by $F = [f_0, \dots, f_m]$ where $f_0, \dots, f_m \in \overline{\mathbb{Q}}[x_0, \dots, x_n]$ are homogeneous polynomials of degree d having no common zero except $(0, \dots, 0)$. Then $\exists\ C_1, C_2 > 0$ such that $\forall\ P \in \mathbb{P}^n(\overline{\mathbb{Q}})$,

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d.$$

② Fix constants C, d. Then

$$\left\{ P \in \mathbb{P}^n(\overline{\mathbb{Q}}) \;\middle|\; H(P) \leq C \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq d \right\}$$

is finite.

Here $\mathbb{Q}(P) = \mathbb{Q}\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \dots, \frac{x_m}{x_i}\right)$ where $x_i \neq 0$. $P = [x_0, \dots, x_n]$.

Pf ① Upper bound is an exercise in applying the triangle inequality.

Lower bound uses Nullstellensatz since

$V(f_0, \dots, f_m) = \{0\} \subset \overline{\mathbb{Q}}^{n+1}$, by Nullstellensatz

$$I(V(f_0, \dots, f_m)) = I(\{0\}) = (x_0, \dots, x_m)$$

$$\text{II Nullstell.}\quad \sqrt{(f_0, \dots, f_m)}$$

, so $\exists\ e \geq 1$ such that.

$$x_i^e \in (f_0, \dots, f_m)\ \forall\ i.$$

Thus $x_i^e = \sum_{j=1}^{m} g_{ij} f_j$ for some $g_{ij} \in \overline{\mathbb{Q}}[x_0, \dots, x_n]$

and we fix a number field F containing coeffs of all f_j's, g_{ij}'s and having chosen a $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$, $P = [x_0, \dots, x_n]$, enlarge F to contain $x_0, \dots, x_n$.

We may also assume all g_{ij} homogeneous degree $e-d$.

Now compute for any $v \in |F|$, $i = 0, \dots, n$

$$|x_i|_v^e = \left| \sum_{j=0}^{m} g_{ij}(P) f_j(P) \right|_v \leq \begin{pmatrix} \text{cst.} \\ C_v \end{pmatrix} \max_j |g_{ij}(P) f_j(P)|_v$$

where $C_v = 1 \ \forall v \nmid \infty$. Take max:

$$\max_i \{|x_i|_v^e\} \leq C_v \cdot \max_{i,j} |g_{ij}(P) f_j(P)|_v$$

$$|P|_v^e \leq C_v \cdot \max_{i,j} |g_{ij}(P)|_v \cdot |F(P)|_v$$

$$\overset{\Delta\text{-ineq.}}{\leq} C_v' \cdot \max\{ |a|_v : a \text{ is some coeff. in some } g_{ij} \} \cdot |P|_v^{e-d} \cdot |F(P)|_v$$

($C_v' = 1$ which is 1 for $v \nmid \infty$).

provisional notation: if we have a fixed coords $P = [x_0, \dots, x_n]$, write $|P|_v = \max_i \{|x_i|_v\}$

Thus, $|P|_v^d \leq C_v' \cdot \max\{1, |a|_v\} \cdot |F(P)|_v$

and multiplying over all $v \in |F|$, get

$$H_P(P)^d \leq \underbrace{\left(\prod_v C_v' \cdot \max\{1, |a|_v\} \right)}_{\text{this is some constant independent of } P} \cdot H_F(F(P))$$

■

Pf of (2): (Fix C, d) We'll only use the $\mathbb{P}^1$ case, and the case of $\mathbb{P}^n$ reduces to that of $\mathbb{P}^1$ (exercise). So take $n = 1$.

Let $P=[\alpha,1]\in\mathbb{P}^1(\overline{\mathbb{Q}})$ where $[\mathbb{Q}[\alpha]:\mathbb{Q}]\le d$ and $H(P)\le C$. Let F be the Galois closure of $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$, so F contains all conjugates $\alpha=\alpha_1,\dots,\alpha_r$ of α. Consider (here $r\le d$ by assumption)

$$\prod_{i=1}^{r}(T-\alpha_i)=\sum_{i=0}^{r}(-1)^i\sigma_i(\alpha)T^{r-i}\in\mathbb{Q}[T]$$

$\sigma_i(\alpha)=$ i^{th} symm. polyn $\alpha_1,\dots,\alpha_r$ ($\sigma_1(\alpha)=\sum\alpha_i$, e.g.)

and $\forall\, v\in|F|$,

$$|\sigma_j(\alpha)|_v=\Big|\sum_{|I|=j}\alpha_I\Big|_v\le\begin{cases}\binom{r}{j}\\ \text{or}\\ 1\end{cases}\cdot\max_I|\alpha_I|_v$$

($I=(i_1,\dots,i_j)$, $\alpha_I=\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_j}$)

$$\le\begin{cases}2^r\\ \text{or}\\ 1\end{cases}\cdot\max_i|\alpha_i|_v^r$$

($v|\infty$ on the left, $v\nmid\infty$ on the right)

$$\max\{|\sigma_0(\alpha)|_v,\dots,|\sigma_r(\alpha)|_v\}\le\begin{cases}2^r\\ \text{or}\\ 1\end{cases}\cdot\prod_{i=1}^{r}\max\{|\alpha_i|_v,1\}^r$$

Thus taking $\prod_v$,

$$H_F([\sigma_0(\alpha),\dots,\sigma_r(\alpha)])\le 2^{r\cdot\#\{v|\infty\}}\cdot\prod_{i=1}^{r}H_F([\alpha_i,1])^r$$

($\#\{v|\infty\}\le[F:\mathbb{Q}]$)

so

$$H([\sigma_0(\alpha),\dots,\sigma_r(\alpha)])\le 2^r\cdot\prod_{i=1}^{r}H([\alpha_i,1])^r$$

$$\overset{G_{\mathbb{Q}}\text{-equivariance}}{=}2^r\cdot\prod_{i=1}^{r}H([\alpha,1])^r$$

$$=2^r\cdot H([\alpha,1])^{r^2}.$$

Thus the element $[\sigma_0(\alpha),\dots,\sigma_r(\alpha)]\in\mathbb{P}^r(\mathbb{Q})$ has height bounded by $2^r\cdot C^{r^2}\le 2^{d^2}\cdot C^{d^2}$. The Thm is clear for $\mathbb{P}^r(\mathbb{Q})$, so there are finitely many such

$[\sigma_0(\alpha), \ldots, \sigma_r(\alpha)] \in \mathbb{P}^r(\mathbb{Q})$, and so

since α is a root of one of the

finitely many polys $\sum (-1)^i \sigma_i(\alpha) T^{r-i}$

there are finitely many $P = [\alpha, 1]$ of height $\leq C$.

Application to Elliptic Curves

Let E/F be an elliptic curve. For any non-constant $f \in \overline{\mathbb{Q}}(E)$, giving $f : E \longrightarrow \mathbb{P}^1$, define

$$h_f : E(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R} \quad \text{by}$$

$$h_f(P) = h(f(P))$$

(where h is the absolute log height $\mathbb{P}^1(\overline{\mathbb{Q}}) \to \mathbb{R}_{\geq 0}$)

Lemma: For $f \in F(E) \setminus F$ and any $C > 0$,

$$\{ P \in E(F) \mid h_f(P) < C \} \text{ is finite.}$$

Pf: f maps this set to $\{ Q \in \mathbb{P}^1(F) \mid h(Q) < C \}$, finite by Thm (2)

and $|f^{-1}(Q)| \leq \deg(f)$ $\forall\, Q \in \mathbb{P}^1(F)$.

The lemma follows

Idea: do group law & ht. fn interact?

Theorem: Fix a Weierstrass equation $y^2 = x^3 + Ax + B$, $A, B \in \overline{\mathbb{Q}}$ for E, and let $f = x : E \to \mathbb{P}^1$. Then $\forall\, P, Q \in E(\overline{\mathbb{Q}})$,

(approximate parallelogram law)

$$h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + O(1)$$

(const. ind. of P, Q)

(The same holds for any even f : $f \circ [-1] = f$, but we won't use this.)

— — — —

Before discussing the proof, we deduce the Mordell-Weil Thm.

Cor: $x: E \to \mathbb{P}^1$ as in the theorem.

① Fix $Q \in E(\bar{\mathbb{Q}})$. Then $\forall P \in E(\bar{\mathbb{Q}})$,

$$h_x(P+Q) \le 2h_x(P) + O(1)$$

← dependson Q, not on P.

② Fix $m \in \mathbb{Z}$. Then $\forall P \in E(\bar{\mathbb{Q}})$,

$$h_x([m]P) = m^2 h_x(P) + O(1).$$

(Again, this holds $\forall$ even f.)

Pf: ① $h_x(P-Q) \ge 0$, so clear from Thm. ($2h_x(Q)$ is part of the $O(1)$)

② suffices to prove for $m \ge 0$ (x is even). Induct. $m = 0, 1$ clear.

Assume true for $m-1, m$. Show for $m+1$.

Then $h_x([m+1]P) \underset{[m]P+P}{=} -h_x([m-1]P) + 2h_x([m]P) + 2h_x(P) + O(1)$

$\overset{\text{ind.}}{=} -(m-1)^2 h_x(P) + 2m^2 h_x(P) + 2h_x(P) + O(1)$

$= (m+1)^2 h_x(P) + O(1)$.

← different constant - which incorporates the $O(1)$'s from $m-1$, m.

Theorem F a number field, E/F an elliptic curve.

Then $E(F)$ is finitely-generated.

Pf: Fix $m > 1$, $E(F)/mE(F)$ is finite, and choosing ∞E

$h_x: E(F) \to \mathbb{R}$ satisfies

- $\forall Q \in E(F)$, $\exists C_Q \in \mathbb{R}$:

$\forall P \in E(F)$, $h_x(P+Q) \le 2h_x(P) + C_Q$.

- $\exists\, C_m > 0 :\ \forall\, P \in E(F)$,

$$h_x([m]P) \geq m^2 h_x(P) - C_m$$

- $\forall\, C \in \mathbb{R}$, $\#\{P \in E(F) \mid h_x(P) \leq C\} < \infty$.

By our descent proposition, $E(F)$ is finitely-generated. ∎

Proof of the

Theorem: Fix a Weierstrass equation $y^2 = x^3 + Ax + B$, $A, B \in \bar{F}$ for E, and let $f = x : E \to \mathbb{P}^1$. Then $\forall\, P, Q \in E(\bar{Q})$,

$$h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + O(1)$$

- If either P or Q is O ($[0,1,0]$), easy to check by hand (without any $O(1)$ even).

Want to understand the effect of

$$\begin{array}{ccc} E \times E & \xrightarrow{G} & E \times E \\ (P, Q) & \longmapsto & (P+Q, P-Q) \end{array}$$

on heights

$h_x(P)$, $h_x(Q)$, $h_x(P+Q)$, $h_x(P-Q)$ defined in terms of

$$\begin{array}{ccc} E \times E & \xrightarrow{G} & E \times E \\ \downarrow (x,x) & & \downarrow (x,x) \\ [a_1, b_1] \times [a_2, b_2] \in \mathbb{P}^1 \times \mathbb{P}^1 & & \mathbb{P}^1 \times \mathbb{P}^1 \\ \| & & \downarrow \nu \\ \downarrow & \downarrow \nu \text{ (morphism)} & \end{array}$$

(move to $\mathbb{P}^2$ from $\mathbb{P}^1 \times \mathbb{P}^1$ to apply main thm. on heights)

$[b_1b_2, a_1b_2+a_2b_1, a_1a_2] \in \mathbb{P}^2$ ------g------> $\mathbb{P}^2$

want a morphism making this diagram commute.

We need to relate $h(\nu(x(P), x(Q)))$ to $h_x(P), h_x(Q)$

$(h_{\mathbb{P}^2})$

wma $P=[\alpha,1]$, $Q=[\beta,1]$ $(\neq \mathcal{O})$.

$h(\nu(x(P),x(Q))) = h([1, \alpha+\beta, \alpha\cdot\beta])$

Claim: This $= h([\alpha,1]) + h([\beta,1]) + O(1)$.

($h([1,\alpha+\beta,\alpha\cdot\beta]) \geq h([\alpha,1]) + h([\beta,1]) - $ cst ex. on Pset 6).

For upper bound, for $L \ni \alpha, \beta$,

$$H_L([1,\alpha+\beta,\alpha\beta]) = \prod_{v\in|L|} \max\{1, \underbrace{|\alpha+\beta|_v}_{\leq \max|\alpha|_v,|\beta|_v \text{ for } v \text{ fin}}, |\alpha\beta|_v\}.$$

$$\leq 2^{\#v|\infty} \cdot \prod_{v\in|L|} \max\{1,|\alpha|_v\}\cdot\max\{1,|\beta|_v\}^{|\alpha|_v+|\beta|_v \leq 2\cdot\max_{i,v}|\alpha_i|_v}$$

so $h([1,\alpha+\beta,\alpha\beta]) \leq h([1,\alpha]) + h([1,\beta]) + (\text{cst.})$.

Next, there is a morphism $g: \mathbb{P}^2 \to \mathbb{P}^2$ of degree 2 making the above diagram commute.

$$g([t,u,v]) = [u^2-4tv,\ 2u(At+v)+4Bt^2,\ (v-At)^2-4Btu]$$

it is an exercise with the group law on E to check that this formula defines a rational map making the diagram commute: on pset 6 you use the

fact that $\Delta(A,B) \neq 0$ to check q is a morphism.

Now we win: For $P, Q \in E(\bar{\mathbb{Q}})$,

$$h(q(\nu(x(P), x(Q)))) = 2h_x(P) + 2h_x(Q) + O(1)$$

$$\overset{\text{Thm}}{\underset{\deg q = 2}{=}} 2h(\nu(x(P), x(Q))) + O(1)$$

But by comm. of diag., this equals

$$h(\nu(x(P+Q), x(P-Q)))$$

$$= h_x(P+Q) + h_x(P-Q) + O(1)$$ ∎

We know now $E(F)$ is finitely-generated — what more can be said?

$$E(F) \cong \underbrace{E(F)_{\text{tor}}}_{\text{finite}} \oplus \mathbb{Z}^r \quad (r \in \mathbb{Z}_{\geq 0}).$$

- The torsion part is much easier to understand: a deep result of Mazur (late 70's) classifies the possible $E(\mathbb{Q})_{\text{tor}}$ for any $E/\mathbb{Q}$. (There is a finite list of groups). This thm. has some generalization to other F.
- r is the subject of the Birch & Swinnerton-Dyer

conjecture, where it is conjectured to equal.

$L(E/F, s)$ is the analytic "L-function" of E, which conjecturally admits analytic continuation to all of $\mathbb{C}$

$= \prod_{\text{primes } \mathfrak{p}} (\text{local term } \#E(\mathbb{F}_{\mathfrak{p}}) \text{ mod } \mathfrak{p})^{-1}$ for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 3/2$

Admitting this conj., BSD says

$$r = \operatorname{ord}_{s=1} L(E/F, s).$$

For $F = \mathbb{Q}$, the analytic continuation is known (Shimura–Taniyama conj., proven by Wiles, Taylor, et al.) and when $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = 0$ or 1, BSD is known. (Gross–Zagier, Kolyvagin)

patrikis.1@osu.edu