2.3. Aside: The Hasse-Weil bound

Thm Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then,

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Intuition $E \cap \{z \neq 0\} = \{y^2 = x^3 + a_4 x + a_6\}$

The probability that a random number $t \in \mathbb{F}_q^\times$ is a square is $\frac{1}{2}$ if q is odd.

$\rightsquigarrow$ The expected number of $y \in \mathbb{F}_q$ such that $y^2 = t$ is 1.

$\rightsquigarrow$ Expect one point $(x, y) \in (E \cap \{z \neq 0\})(\mathbb{F}_q)$ on average for a given value $x \in \mathbb{F}_q$.

$\rightsquigarrow$ Expect $\#(E \cap \{z \neq 0\})(\mathbb{F}_q) \approx q$,

so $\#E(\mathbb{F}_q) \approx q+1$.

"Pf" Consider the Frobenius morphism

$$\varphi : E \longrightarrow E$$
$$[x : y : z] \longmapsto [x^q : y^q : z^q].$$

For any $P \in E(\overline{\mathbb{F}_q})$, we have $\varphi(P) = P$ if and only if $P \in E(\mathbb{F}_q)$.

Then, $E(\mathbb{F}_q) = \{P \in E(\overline{\mathbb{F}_q}) \mid \varphi(P) = P\}$

$= \{P \in E(\overline{\mathbb{F}_q}) \mid (\varphi - id)P = O\}$

$= \ker(\varphi - id)$.

$\Rightarrow \#E(\mathbb{F}_q) = \#\ker(\varphi - id) = \deg(\varphi - id)$.
($\varphi - id$ is separable)

Since $\deg : \mathrm{End}(E) \to \mathbb{Z}$ is a positive definite quadratic form, we get the Cauchy-Schwarz inequality

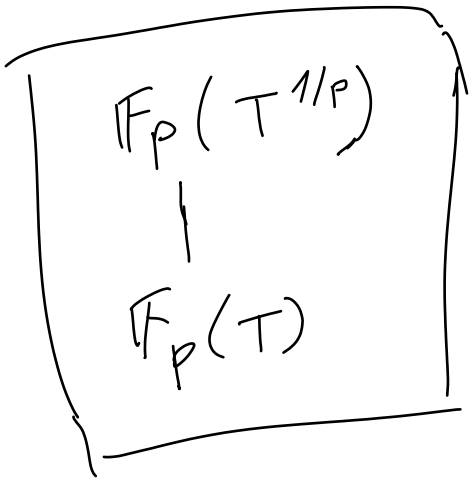
$$|\langle \varphi, id \rangle| \leq \sqrt{\deg(\varphi) \cdot \deg(id)}$$

$\langle \varphi, id \rangle = \frac{1}{2}\left|\deg(\varphi - id) - \deg(\varphi) - \deg(id)\right|$

$\deg(\varphi - id) = \#E(\mathbb{F}_q)$, $\deg(\varphi) = q$, $\deg(id) = 1$

$\Rightarrow \left|\#E(\mathbb{F}_q) - (q+1)\right| \leq 2\sqrt{q}$.

□



A. Heights

Reference Chapter 2 of Lectures on the Mordell-Weil Theorem by J-P Serre.

A.1. Definition

Def The **height** of $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{Q})$ with $x_0, \ldots, x_n \in \mathbb{Z}$ relatively prime is

$$H(P) := \max(|x_0|, \ldots, |x_n|).$$

Def More generally, if K is a global field, the **height** of $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ with $x_0, \ldots, x_n \in K$ is

$$H_K(P) := \prod_{v \text{ place of } K} \max_i |x_i|_v .$$

(Here, $|x|_q = q^{-v_q(x)}$ if $v = v_q$ is nonarch. with residue field $\mathbb{F}_q$

$|x|_v = |i(x)|$ if v corresponds to the real embedding $i : K \hookrightarrow \mathbb{R}$

$|x|_v = |i(x)|^2$ if v corresponds to (nonreal) complex embedding $i : K \hookrightarrow \mathbb{C}$)

Rmk $\prod_v \max_i |\lambda x_i|_v = \underbrace{\prod_v |\lambda|_v}_{=1} \cdot \prod_v \max_i |x_i|_v$

(product formula)

for any $\lambda \in K^\times$.

$\Rightarrow H_K(P)$ is well-defined (indep. of the choice of projective coordinates $x_0, \dots, x_n$ of P).

Rmk For $K = \mathbb{Q}$, the two definitions agree.

Pf If $x_0, \dots, x_n \in \mathbb{Z}$ are relatively prime, then $\max(|x_0|_p, \dots, |x_n|_p) = p^{-\min(v_p(x_0), \dots, v_p(x_n))}$

$= p^{-0} = 1$. □

Rmk $H_L(P) = H_K(P)^{[L:K]}$ for a separable field ext. $L|K$ and a point $P \in \mathbb{P}^n(K)$.

Pf If w is a place of L above a place v of K and $x \in K$, then $|x|_w = |x|_v^{e(w|v) f(w|v)}$.

$\sum_{w|v} e(w|v) f(w|v) = [L:K]$. □

Hence, the following makes sense:

Def $H_K(P) := H_L(P)^{\frac{1}{[L:K]}}$ for any $P \in \mathbb{P}^n(L)$ defined over a separable field ext. $L|K$.

Def The logarithmic height of P is

$$h_u(P) := \log H_u(P).$$

A.2. Properties

Rmks $H(P) \geq 1$, $h(P) \geq 0$ $\forall P \in \mathbb{P}^n(K)$.

Pf If $x_i \in K^\times$, then $\prod_v |x_i|_v = 1$.

$$\Rightarrow \prod_v \max_j |x_j|_v \geq 1. \qquad \square$$

Thm A.2.1 For any K and any $t \geq 0$, there are only finitely many points $P \in \mathbb{P}^n(K)$ with $h(P) \leq t$.

(This is clear for $K = \mathbb{Q}$.)

Thm A.2.2 Let $M \in GL_{n+1}(K)$ and let $\alpha_M : \mathbb{P}^n_K \longrightarrow \mathbb{P}^n_K$ be the corresponding morphism. Then, $h_K(\alpha_M(P)) \underset{M}{\approx} h_K(P)$ for any $P \in \mathbb{P}^n(\bar{K})$.

(meaning: $|h(\alpha(P)) - h(P)| \leq C_M$ for some constant C_M depending on M, but not on P,

$h_K(\alpha_M(P)) = h_K(P) + O_M(1)$)

Pf HW. □

Thm Consider the Segre embedding

$$\mathbb{P}^n \times \mathbb{P}^m \longrightarrow \mathbb{P}^{(n+1)(m+1)-1}$$

$$(P, Q) = ([x_0 : \cdots : x_n], [y_0 : \cdots : y_m]) \longmapsto [x_0y_0 : x_0y_1 : \cdots : x_ny_m] =: P \otimes Q$$

We have $h(P \otimes Q) = h(P) + h(Q)$.

Pf $H(P \otimes Q) = \prod_v \max_{i,j} |x_i y_j|_v = \prod_v \max_i |x_i|_v \cdot \max_j |y_j|_v$

$= H(P) \cdot H(Q)$. □

Thm A.2.4 Consider the Veronese embedding

degree $d \geq 1$

$$\mathbb{P}^n \longrightarrow \mathbb{P}^{\binom{n+d}{d}-1}$$

$$P=[x_0:\cdots:x_n] \longmapsto \left[x_0^d : x_0^{d-1}x_1 : \cdots : x_n^d\right] =: P^{(d)}$$

all degree d monomials in $x_0, \ldots, x_n$

and the morphism

$$\mathbb{P}^n \longrightarrow \mathbb{P}^n$$

$$P=[x_0:\cdots:x_n] \longmapsto \left[x_0^d : \cdots : x_n^d\right] =: P^d.$$

We have $h(P^{(d)}) = h(P^d) = d \cdot h(P)$.

Pf $H(P^{(d)}) = \prod_v \max_{\substack{e_0,\ldots,e_n \geq 0 \\ e_0+\cdots+e_n=d}} |x_0^{e_0} \cdots x_n^{e_n}|_v$

$$= \prod_v \max_i \underbrace{|x_i^d|_v}_{|x_i|_v^d} = H(P^d) = H(P)^d.$$

□

Thm A.2.5 Consider the projection

$$\pi : \mathbb{P}^n \setminus \{(0:\dots:0:1)\} \longrightarrow \mathbb{P}^{n-1}$$

$$[x_0 : \dots : x_n] \longmapsto [x_0 : \dots : x_{n-1}]$$

We have $h(\pi(P)) \le h(P)$ for all $(0:\dots:0:1) \neq P \in \mathbb{P}^n(\bar{K})$.

Pf $H(\pi(P)) = \prod_v \max_{i \le n-1} |x_i|_v \le \prod_v \max_{i \le n} |x_i|_v = H(P)$.

□

Rmk $h(\pi(P))$ can be arbitrarily much smaller than $h(P)$.

For example, take $P = [r : \dots : r : 1] \in \mathbb{P}^n(\mathbb{Q})$ with $0 \neq r \in \mathbb{Z}$.

$\Rightarrow \pi(P) = [r : \dots : r] = [1 : \dots : 1]$.

$\Rightarrow h(\pi(P)) = 0$, $h(P) = \log|r|$.

"For $q \mid r$, P is q-adically close to the point $(0:\dots:0:1)$ where π is not defined."

Lemma Let $V \subseteq \mathbb{P}^n_K$ be a hyperplane not containing $[0:\dots:0:1]$ and consider the projection $\pi : V \to \mathbb{P}^{n-1}$ as above. Then, $h(\pi(P)) \underset{V}{\approx} h(P)$ for all $P \in V(\bar{K})$.

Pf π is a linear isomorphism.

There is a linear transformation

$M : K^n \to K^{n+1}$ with $\alpha_M(\pi(P)) = P$ for all $P \in V$.

Apply Thm A.2.2.:

□

More generally:

Thm A.2.6. Let $V \subseteq \mathbb{P}^n_K$ be a projective variety not containing $[0:\dots:0:1]$ and consider the projection

$$\pi : V \to \mathbb{P}^{n-1}$$
$$[x_0:\dots:x_n] \mapsto [x_0:\dots:x_{n-1}]$$

Then, $h(\pi(P)) \underset{V}{\approx} h(P)$ for all $P \in V(\bar{K})$.

Pf Let $f \in K[x_0,\dots,x_n]$ be any homogeneous degree d polynomial which vanishes on V but not at $[0:\dots:0:1]$.

$\Rightarrow$ The monomials X_n^d occurs in f, so X_n^d is a fixed linear combination of the other degree d monomials in $x_0, \dots, x_n$ for any point $P \in V(\overline{K})$.

$\Rightarrow$ $P^{(d)}$ lies in a fixed hyperplane $W \subseteq \mathbb{P}^{\binom{n+d}{d}-1}$ not containing $[0 : \cdots : 0 : 1]$ (coord. corr. to x_n^d).

$$\Rightarrow \quad d \cdot h(P)$$

$$= h(P^{(d)})$$

$$\overset{W}{\approx} h(\pi'(P^{(d)}))$$

Lemma

$\pi' : \mathbb{P}^{\binom{n+d}{d}-1} \to \mathbb{P}^{\binom{n+d}{d}-2}$ omitting the coord. corr. to x_n^d

$$= h(P^{(d-1)} \otimes \pi(P))$$

coord. are the degree d mon. divisible by some x_i with $i \neq n$, so all the monomials except x_n^d

$$= h(P^{(d-1)}) + h(\pi(P))$$

$$= (d-1)\,h(P) + h(\pi(P)).$$

$$\Rightarrow h(\pi(P)) \overset{W}{\approx} h(P). \qquad \square$$

More generally:

Thm A.2.7 Let M be a linear map $k^{n+1} \to k^{m+1}$ and let $\alpha_M : \mathbb{P}^n \setminus \{[x_0 : \cdots : x_n] \mid M(x_0, \ldots, x_n) \neq 0\} \longrightarrow \mathbb{P}^m$ be the corr. morphism.

Then, $h(\alpha_M(P)) \underset{M}{\leq} h(P)$ for all $P \in \mathbb{P}^n(\bar{k})$
$\|$
$[x_0 : \cdots : x_n]$
with $M(x_0, \ldots, x_n) \neq 0$

(meaning $h(P) - h(\alpha_M(P)) \geq C_M$ for some constant C_M depending only on M,

$$h(\alpha(P)) \leq h(P) + O_M(1) \quad)$$

Pf After linear transformations on $\mathbb{P}^n$ and $\mathbb{P}^m$, we can assume (using Thm A.2.2) that M sends
$(x_0, \ldots, x_n)$ to $(x_0, \ldots, x_s, 0, \ldots, 0)$,
where $s = \operatorname{rank}(M)$.

W.l.o.g. $s = m$, so M is the proj. onto the first $m+1$ coordinates, i.e.

the composition of $n-m$ projections as in Thm A.2.5. □

Thm A.2.8 Let M as above and let $V \subseteq \mathbb{P}^n_{\bar{k}}$ be a proj. var. not containing any $P = [x_0 : \dots : x_n] \in V(\bar{k})$ with $M(x_0, \dots, x_n) = 0$, so that $\alpha_M : V \longrightarrow \mathbb{P}^m$ is well-defined.

Then, $h(\alpha_M(P)) \underset{M,V}{\approx} h(P)$ for all $P \in V(\bar{k})$.

Pf as above, using Thm A.2.6. □

•