The Weak! Mordell-Weil Theorem (part 2)

Prop Let K be a number field, $S \subseteq M_K$ a finite set of places containing M_K^∞, and let $m \geq 2$ be an integer. Let L/K ($L = K_{S,m}^{ab}$) be the maximal abelian extension of K having exponent m which is unramified outside of S. Then, L/K is a finite extension.

Thm (Weak Mordell-Weil)
Let K be a number field, $m \geq 2$, E/K an elliptic curve. Then, $E(K)/mE(K)$ is finite.

Proof. The existence of the Kummer pairing

$\Rightarrow \left(E(K)/mE(K) \text{ is finite} \iff \mathrm{Gal}(L/K) \text{ is finite w/ } L = K\left([m]^{-1}(E(K))\right) \right)$

We showed that L/K is abelian and exp m unramified outside $S = M_K^\infty \cup \{v : v \text{ of bad red'n for } E/K\} \cup \{v : v(m) \neq 0\}$

By prop $K \subseteq L \subseteq K_{S,m}^{ab}$ ($K \subseteq L$ finite) $\Rightarrow L/K$ is finite $\Rightarrow E(K)/mE(K)$ finite! ∎

Remarks.

- Suppose $E[m] \subseteq E(k) \cong E(k)_{tors} \oplus \mathbb{Z}^{R_{E/k}}$

$$\Rightarrow E(k)/mE(k) \cong \frac{E(k)_{tors}}{mE(k)_{tors}} \oplus \left(\mathbb{Z}/m\mathbb{Z}\right)^{R_{E/k}}$$

$\frac{E(k)_{tors}}{mE(k)_{tors}} \cong \mathbb{Z}/m \oplus \mathbb{Z}/m$

$\Big\}$ $\operatorname{rank}_{\mathbb{Z}/m\mathbb{Z}} E/mE = 2 + R_{E/k}$

Weil pairing!

- $\kappa : E(k)/mE(k) \times Gal(L/k) \longrightarrow E[m]$ perfect.

$$\rightarrow E(k)/mE(k) \hookrightarrow Hom(Gal(L/k), E[m])$$
$$\cong Hom(Gal(L/k), \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z})$$
$$\cong Hom(Gal(L/k), \mathbb{Z}/m\mathbb{Z})^2$$

- $\mu_m \subseteq K \subseteq L \subseteq K_{S,m}^{ab}$ where $S = \{$bad primes, ∞ primes, $v/m\}$
- $K_{S,m}^{ab} = K(\sqrt[m]{a} : a \in T_S)$, where $T_S = \{a \in K^\times/(K^\times)^m : ord_v(a) \equiv 0 \bmod m \ \forall v \in M_K^0, v \notin S\}$

- $R_S^\times \longrightarrow T_S$
  $a \longmapsto a \bmod (\mathfrak{k}^\times)^m$

  want this surjective ...
  $a \in T_S$, $aR_S = \mathfrak{b}^m$
  Need $\mathfrak{b}$ to be principal
  $[\mathfrak{b}] \in Cl(k)[m] \cong \mathbb{Z}/m\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m\mathbb{Z}$
  $\uparrow \mathfrak{p}_1$ $\uparrow \mathfrak{p}_r$

  - add $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ to S , get S' (we have increased S by $\operatorname{rank}_{\mathbb{Z}/m\mathbb{Z}}(Cl(k)[m])$)
  - $\mu_m \subseteq k \subseteq L \subseteq k_{S,m}^{ab} \subseteq k_{S',m}^{ab}$
    and $k_{S',m}^{ab} = k(\sqrt[m]{a} : a \in T_{S'})$, and $R_{S'}^\times \twoheadrightarrow T_{S'}$ surjective
    and $(R_{S'}^\times)^m$ in kernel $\Rightarrow R_{S'}^\times/(R_{S'}^\times)^m \twoheadrightarrow T_{S'}$
    $\Rightarrow |T_{S'}| \leq |R_{S'}^\times/(R_{S'}^\times)^m|$ and DST $\Rightarrow$ rank $R_{S'}^\times$ is $|S'|-1$.

Heights and the Descent Procedure

example. $y^2 = x^3 + 3$, $P = (1,2)$

$$2P = \left(-\frac{23}{16}, \frac{-11}{64}\right), \quad 3P = \left(\frac{1873}{1521}, -\frac{130870}{59319}\right)$$

$$4P = \left(\frac{25408337}{7744}, \frac{4050085503}{681472}\right) \ldots$$

Prop (Descent theorem) Let A be an abelian gp. and suppose there is a "height" function $h : A \longrightarrow \mathbb{R}$ s.t.

(i) Let $Q \in A$. $\exists\, C_1 > 0$, $C_1(A, Q)$ s.t. $\forall P \in A$, $h(P+Q) \leq 2h(P) + C_1$.

(ii) $\exists\, m \geq 2$ and $C_2 = C_2(A)$ s.t. $\forall P \in A$, $h(mP) \geq m^2 h(P) - C_2$.

(iii) $\forall C_3$, $\{P \in A : h(P) \leq C_3\}$ is finite.

Suppose A/mA (w/ m as in (ii)) is finite, then A is finitely generated.

Pf. Let m be as in (ii). Assume A/mA is finite.

So let $Q_1, \dots, Q_r \in A$ be rep's of cosets A/mA.

IDEA: Let $P \in A$ there are $\lambda_1, \dots, \lambda_r \in \mathbb{Z}$ s.t.

$$P - \lambda_1 Q_1 - \dots - \lambda_r Q_r \in \underbrace{S \text{ of bounded height.}}$$

finite $\Rightarrow$ $S + Q_1, \dots, Q_r$ generate A.

Let $P \in A$. Then $P \equiv Q_{i_1} \bmod mA$.

$\Rightarrow P = mP_1 + Q_{i_1}$ for some $P_1 \in A$.

$P_1 = mP_2 + Q_{i_2}$

$\vdots$

$P_{n-1} = mP_n + Q_{i_n}$

(ii) $h(mP_j) \le m^2 h(P_j) - c_2$

$\downarrow$

For any j: $h(P_j) \le \frac{1}{m^2}\left(h(mP_j) + c_2\right)$

$= \frac{1}{m^2}\left(h(P_{j-1} - Q_{i_j}) + c_2\right)$

(i) $\rightarrow$

$\le \frac{1}{m^2}\left(2h(P_{j-1}) + c_1' + c_2\right)$

where $c_1' = \max$ of $c_1(A_1 - Q_j)$ for $j = 1, \dots, r$

so that c_1', c_2 do not depend on P!

Start from P_n, work backwards: $\left(h(P_j) \le \frac{1}{m^2}\left(2h(P_{j-1}) + C_1' + C_2\right)\right)$

$$h(P_n) \le \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \cdots + \frac{2^{n-1}}{m^{2n}}\right)(C_1' + C_2)$$

Geometric

$$\frac{1}{m^2}\left(1 + \frac{2}{m^2} + \cdots + \frac{2^{n-1}}{m^{2n-2}}\right) = \frac{1}{m^2}\left(\frac{\frac{2^n}{m^{2n}} - 1}{\frac{2}{m^2} - 1}\right)$$

$$= \frac{1 - \frac{2^n}{m^{2n}}}{m^2 - 2} < \frac{1}{m^2 - 2}$$

$$< \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{m^2 - 2}$$

$(m \ge 2)$

$$\le \frac{h(P)}{2^n} + \frac{C_1' + C_2}{2}$$

$n \gg 0$ $\quad h(P) \le 1 + \frac{C_1' + C_2}{2}$ and $P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{ij}$

$S' = \{P : h(P) \le 1 + \frac{C_1' + C_2}{2}\}$ is finite by (iii)!

C_3

$\Rightarrow A$ is generated by $\{Q_1, \ldots, Q_r\} \cup \{Q \in A : h(Q) \le 1 + \frac{C_1' + C_2}{2}\}$

$\Rightarrow A$ is finitely generated! $\blacksquare$

Heights on $\mathbb{P}^N$ and elliptic curves

Def. Height on $\mathbb{Q}$: if $t = p/q \in \mathbb{Q}$ in lowest terms ($\gcd(p,q)=1$)

then $H(t) = \max\{|p|, |q|\}$

Height on $\mathbb{P}^N(K)$: $P = [x_0, \dots, x_N]$ $x_i \in K$

field

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, \dots, |x_N|_v\}^{n_v}, \quad n_v = [K_v : \mathbb{Q}_v]$$

(naive) Height on $E(\mathbb{Q})$ (rel. to a given Weier. eq'n): $h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}$

$$h_x(P) = \begin{cases} \log H(x(P)) & \text{if } P \neq \mathcal{O}, \\ 0 & \text{if } P = \mathcal{O}. \end{cases}$$

Mordell (- Weil) Theorem

Let $E/\mathbb{Q}: y^2 = x^3 + Ax + B$.

(a) Let $P_0 \in E(\mathbb{Q})$. $\exists\, C_1 = C_1(P_0, A, B)$ so that $\forall P \in E(\mathbb{Q})$

$$h_x(P + P_0) \leq 2\, h_x(P) + C_1.$$

(b) $\exists\, C_2 = C_2(A, B)$ s.t. $\forall P \in E(\mathbb{Q})$: $h_x([2]P) \geq 4\, h_x(P) - C_2$. (m=2)

(c) $\forall C_3$ $\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$ is finite.

Pf (c) $\forall C_3$, $\{t \in \mathbb{Q} : H(t) \leq C\}$ is finite!

For any x there are at most 2 points (x, y) on E.

$\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$ is finite as well! ▨

(a) Let $P_0 \in E(\mathbb{Q})$. $\exists\, C_1 = C_1(P_0, A, B)$ so that $\forall P \in E(\mathbb{Q})$

$$h_x(P+P_0) \le 2h_x(P) + C_1.$$

Pf (a) Taking $C_1 > \max\{h_x(P_0), h_x([2]P_0)\}$ we may assume $P_0 \neq \mathcal{O}$
$P \neq \mathcal{O}, \pm P_0$.

FACT: $E: y^2 = x^3 + Ax + B \implies P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$, $P_0 = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right)$ in lowest terms.

Add. formula:

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

$$= \frac{(xx_0 + A)(x + x_0) + 2B - 2yy_0}{(x-x_0)^2}$$

$$= \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bd\, b_0d}{(ad_0^2 - a_0d^2)^2}$$

a_0, b_0, d_0 fixed.

$$H(x(P+P_0)) = \max\{|\text{num}|, |\text{denom}|\} \le C_1' \cdot \max\{|a|^2, |d|^4, |bd|\}$$

where $C_1' = C_1'(A, B, a_0, b_0, d_0)$

$H(x(P)) = \max\{|a|, |d|^2\}$ and $b^2 = a^3 + Aad^4 + Bd^6$

$P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ $\Rightarrow |b| \le C_1'' \max\{|a|^{3/2}, |d|^3\}$

$C_1'' = C_1''(A, B)$

$\Rightarrow H(x(P+P_0)) \le C_1 \max\{|a|^2, |d|^4\} = C_1 \cdot H(x(P))^2$

$\Rightarrow h_x(P+P_0) \le C_1 + 2\, h_x(P)$. ▨

(b) Similar proof but use duplication formula instead of add. ▨

Weak MW thm + Descent Theorem + h_x for $E/\mathbb{Q}$

$\Rightarrow$ Mordell (-Weil) Theorem for $E/\mathbb{Q}$.