Proof of Weak Mordell-Weil:

Fix E/F, (E - ell. curve, F - number field), $m > 1$. Claim $E(F)/mE(F)$ is finite.

Take the long-exact sequence sequence in G_F-cohomology associated to

$$0 \to E(\overline{F})[m] \to E(\overline{F}) \xrightarrow{[m]} E(\overline{F}) \to 0$$

Thus we get an exact sequence

$$0 \to E(F)/mE(F) \xrightarrow{\delta} \underbrace{H^1(G_F, E[m])}_{\text{infinite!}} \to H^1(G_F, E)[m] \to 0$$

($H^1(G_F, E)[m]$: m-torsion subgroup)

Idea: Identify a finite subgroup of $H^1(G_F, E[m])$ that must contain $\mathrm{im}(\delta)$.

How: Repeat above with F replaced by each completion of F:

$\forall$ primes $\mathfrak{p} \subset \mathcal{O}_F$, get $F_{\mathfrak{p}}$. Also get "infinite place" completions: for each $\tau : F \hookrightarrow \mathbb{C}$, get an absolute value on F; τ and $\bar{\tau}$ yield same abs. value, so we write F_v, for $v \in \mathrm{Hom}(F, \mathbb{C})/\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, for this completion. (this $F_v \simeq \mathbb{R}$ or $\mathbb{C}$).

Set

$$|F| = \{\text{maximal ideals } \mathfrak{p} \subset \mathcal{O}_F\} \cup \mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{C})/_{Gal(\mathbb{C}/\mathbb{R})}$$

For each $v \in |F|$, we have completions F_v and, fixing an algebraic closure $\overline{F}_v$ and an embedding $\overline{F} \hookrightarrow \overline{F}_v$, we get an inclusion

$$G_{F_v} \hookrightarrow G_F.$$ (by restricting automorphisms)

($\overline{F}_v = \mathbb{C}$ in $\mathbb{R}$).

we get the commutative diagram:

$$\begin{array}{ccccccccc}
0 & \to & E(F)/_{mE(F)} & \xrightarrow{\delta} & H^1(G_F, E[m]) & \to & H^1(G_F, E)[m] & \to & 0 \\
 & & \downarrow & & \downarrow \text{res} & & \downarrow \text{res} & & \\
0 & \to & \prod_{v\in|F|} E(F_v)/_{mE(\overline{F}_v)} & \xrightarrow{\prod \delta_v} & \prod_{v\in|F|} H^1(G_{F_v}, E[m]) & \to & \prod_{v\in|F|} H^1(G_{F_v}, E)[m] & \to & 0
\end{array}$$

Lemma: For $P \in E(F)$,

$$\delta(P) \in \left\{ \varphi \in H^1(G_F, E[m]) \;\middle|\; \forall v \in |F|,\ \varphi|_{G_{F_v}} \in \mathrm{im}(\delta_v) \right\}$$

Pf: The diagram commutes!

This group is called the "m-Selmer group" & is denoted $Sel_m(E/F)$.

Thus, $E(F)/mE(F) \hookrightarrow Sel_m(E/F)$.

We'll prove $Sel_m(E/F)$ is finite.

Rmk: Tate-Shafarevich group.

$Ш(E/F) := \ker\left(H^1(G_F, E) \to \prod_{v \in |F|} H^1(G_{F_v}, E)\right)$, so

we have an exact sequence

$$0 \to E(F)/mE(F) \to Sel_m(E/F) \to Ш(E/F)[m] \to 0.$$

So we'll show $\forall m$, $Ш(E/F)[m]$ is finite.

It is a fundamental open conjecture that

$$Ш(E/F) \text{ is finite}$$

[our $w^2 = 2 - 2pz^4$ ($p \equiv 1 \bmod 8$, $\left(\frac{2}{p}\right)_4 \neq 1$) eg of failure of Hasse principle for genus 1 curves / $\mathbb{Q}$ "corresponds to" a non-zero element of $Ш(E/\mathbb{Q})$ where E is $y^2 = x^3 + px$.
(for particular p, Rubin proved that $Ш(E/\mathbb{Q})$ is finite in this case)]

Prop: Let $S = \{$ primes $\mathfrak{p}$ of $F \mid \mathfrak{p} \mid m$ or E has bad reduction at $\mathfrak{p}\}$. Then $|S| < \infty$.

$$Sel_m(E/F) \subset \{\varphi \in H^1(G_F, E[m]) \mid \forall \mathfrak{p} \notin S, \varphi|_{G_{F_\mathfrak{p}}} \text{ is unramified}\}$$

meaning: $\exists$ finite unramified extension $F_\mathfrak{p}'/F_\mathfrak{p}$ such that $\varphi|_{G_{F_\mathfrak{p}'}} = 0$.

Pf: Let $\varphi \in Sel_m(E/F)$. $\forall \mathfrak{p}$, $\varphi|_{G_{F_\mathfrak{p}}} = \delta_\mathfrak{p}(Q_\mathfrak{p})$ for some $Q_\mathfrak{p} \in E(F_\mathfrak{p})$. For $\mathfrak{p} \notin S$, we have proven $\exists$ unramified ext. $F_\mathfrak{p}'/F_\mathfrak{p}$ and $Q' \in E(F_\mathfrak{p}')$ such that $Q_\mathfrak{p} = [m]Q'$. (main local thm on ell. curves last time)

$$\begin{array}{ccc} Q_\mathfrak{p} \in & E(F_\mathfrak{p})/mE(F_\mathfrak{p}) & \xrightarrow{\delta_\mathfrak{p}} H^1(G_{F_\mathfrak{p}}, E[m]) \\ \downarrow & \downarrow & \downarrow \text{res} \\ 0 \in & E(F_\mathfrak{p}')/mE(F_\mathfrak{p}') & \longrightarrow H^1(G_{F_\mathfrak{p}'}, E[m]) \end{array}$$

Thus $\varphi|_{G_{F_\mathfrak{p}'}} = 0$. ∎

(, $E[m]$, say)

Prop: Let M be any finite discrete G_F-module, and let S be any finite set

of primes of F. Then

$$\{\varphi \in H^1(G_F, M) \mid \forall \beta \notin S,\ \varphi|_{G_{F_\beta}} \text{ is unramified}\} =: H^1_S$$

is finite.

Cor: $Sel_m(E/F)$ is finite.

Cor: $E(F)/mE(F)$ is finite. (weak M-W).

Pf of Prop: For any finite Galois L/F, the exact inf-res sequence

$$0 \to H^1(Gal(L/F), M^{G_L}) \xrightarrow{inf} H^1(G_F, M) \xrightarrow{res} H^1(G_L, M)$$

shows that $\ker(res_{L/F})$ is finite (b/c L/F is fin. & M is fin.)

Since $res_{L/F}(H^1_S)$ lands in the analogously-defined set $\{\varphi \in H^1(G_L, M) \mid \varphi \text{ is unr. outside all primes dividing primes in } S_L\}$, we may prove the prop. with L in place of F.

Choose L: G_L acts trivially on M. Thus $M \simeq \bigoplus_{i=1}^{r} \mathbb{Z}/n_i$ as G_L-module (with trivial action), so it suffices to prove the prop with $M = \mathbb{Z}/n$.

Then our group of interest is

$$\{\text{continuous homs } \varphi: G_L \to \mathbb{Z}/n \mid \forall \beta \notin S_L,\ \varphi|_{G_{L_\beta}} \text{ is unramified}\}$$

Any such φ factors through an injective hom $\mathrm{Gal}(L_\varphi/L) \hookrightarrow \mathbb{Z}/n$ where L_φ/L is a fin. Galois extension that is unramified outside the set S_L.

The Hermite–Minkowski theorem says that $\{L' \subset \bar{L} \mid [L':L] \le n$ and L'/L unr. outside $S_L\}$ is finite.

Thus there are finitely many possible number fields L_φ, and finitely many homs $\mathrm{Gal}(L_\varphi/L) \to \mathbb{Z}/n$ for each such L_φ. ∎

- For a different proof of the Prop, using $Cl(\mathcal{O}_F)$ finite & $\mathcal{O}_F^\times$ finitely-generated, and Kummer theory, see PSet 6.

Heights and the proof of Mordell-Weil

The following lemma explains how we will use W M-W + the theory of heights to deduce M-W.

("Descent Prop.") (think $E(F)$)

Prop: Let A be an abelian group equipped with a "height function"

$$h: A \longrightarrow \mathbb{R} \quad \text{satisfying}$$

(1) $\forall\, Q \in A$, there is a constant $C_1 = C_1(Q)$:

$\forall\, P \in A$, $\quad h(P+Q) \leq 2h(P) + C_1$

(2) For some $m \in \mathbb{Z}_{>1}$ and constant C_2,

$$h(mP) \geq m^2 h(P) - C_2 \quad \forall\, P \in A$$

(3) $\forall\, C \in \mathbb{R}$, $\{P \in A \mid h(P) \leq C\}$

is finite.

Suppose that for m as in (2), A/mA is finite. Then

A is finitely-generated.

Rmk: If h were a quadratic form, it would satisfy ① & ② (② is clear, and ① is from parallelogram law $h(P+Q)+h(P-Q) = 2h(P)+2h(Q)$

Pf: Let $Q_1, \dots, Q_r \in A$ represent all elts of $A \bmod mA$. Let $P \in A$.

$P = Q_{i_1} + m \cdot P_1$ some $1 \le i_1 \le r$, $P_1 \in A$.

$P_1 = Q_{i_2} + m \cdot P_2$ some i_2

$\vdots$

$P_{n-1} = Q_{i_n} + m \cdot P_n$ some i_n (any $n \ge 1$)

Thus $P = m^n \cdot P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}$

Idea: Show for n large enough, $h(P_n)$ is below some bound independent of P.

Now, $h(P_j) \overset{\text{by } ②}{\le} \frac{1}{m^2}\left(h(mP_j) + C_2\right)$ $\forall j$.

$= \frac{1}{m^2}\left(h(P_{j-1} - Q_{i_j}) + C_2\right)$

$\overset{①}{\le} \frac{1}{m^2}\left(2h(P_{j-1}) + \underbrace{C_1 + C_2}_{C'}\right)$

(C_1 = sup of the C_1's in ① for $Q_1, \dots, Q_r$)

Iterating,

$$h(P_n) \le \frac{2}{m^2} h(P_{n-1}) + \frac{c'}{m^2}$$

$$\le \frac{2}{m^2}\left(\frac{2}{m^2} h(P_{n-2}) + \frac{c'}{m^2}\right) + \frac{c'}{m^2}$$

$$\le \vdots \le \frac{2^n}{m^{2n}} h(P) + \frac{c'}{m^2}\left(1 + \frac{2}{m^2} + \left(\frac{2}{m^2}\right)^2 + \cdots + \left(\frac{2}{m^2}\right)^{n-1}\right)$$

$$\le \left(\frac{2}{m^2}\right)^n h(P) + \frac{c'}{m^2 \cdot \left(1 - \frac{2}{m^2}\right)}$$

Since $m \ge 2$, for n sufficiently large (depending on $h(P)$), this is

$$< 1 + \frac{c'}{m^2 - 2}.$$ Thus,

(or any $\varepsilon > 0$)

$$\{Q_i \mid i = 1, \ldots, r\} \cup \underbrace{\left\{Q \in A \mid h(Q) < 1 + \frac{c'}{m^2-2}\right\}}_{\text{finite by } ⓢ}$$

generates A,

so A is finitely-generated. ∎

How to construct such an h for $A = E(F)$

Define $H : \mathbb{P}^n(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 1}$ by

$H(P) = \max\{|x_0|, \dots, |x_n|\}$ where

$x_0, x_1, \dots, x_n \in \mathbb{Z}$ have $\gcd = 1$ and

$P = [x_0, \dots, x_n]$

(any elt $P \in \mathbb{P}^n(\mathbb{Q})$ has such an expression, & $(x_0, \dots, x_n)$ is then unique up to ± 1).

and $h : \mathbb{P}^n(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$ by

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

Special case: Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation

$$y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{Z}.$$

$x \in \mathbb{Q}(E) \rightsquigarrow$ morphism $x : E \longrightarrow \mathbb{P}^1$.

and define $h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$ by

$$h_x(P) = h(x(P)).$$

The conditions in the descent prop hold for this $h_x : E(\mathbb{Q}) \to \mathbb{R}$. (Silv. VIII §4 checks this

by hand for $m=2$ — and that suffices to prove that $E(\mathbb{Q})$ is finitely generated).

F number field. Failure of unique factorization in $\mathcal{O}_F$ $\rightsquigarrow$ can't always represent $P \in \mathbb{P}^n(F)$ by $[x_0, \dots, x_n]$ with $x_i \in \mathcal{O}_F$, $\gcd\big((x_0), \dots, (x_n)\big) = (1)$

So we need a new definition of

$$H_F : \mathbb{P}^n(F) \longrightarrow \mathbb{R}_{\geq 1}.$$

The cue comes from the

Product Formula:

$\mathbb{Q}$ has the absolute values

$|\cdot|_p$ $\forall$ primes p: $\left|p^n \frac{a}{b}\right|_p = p^{-n}$ $(ab, p) = 1$

and $|\cdot|_\infty$ the usual $\mathbb{Q} \subset \mathbb{R} \xrightarrow{|\cdot|} \mathbb{R}_{\geq 0}$

Write $|\mathbb{Q}| = \{\infty, 2, 3, \ldots\}$. Then

$$\forall\, a \in \mathbb{Q}^\times, \quad \prod_{v \in |\mathbb{Q}|} |a|_v = 1$$

(product formula)

($a = \pm p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ + defn of $|a|_v$'s) ← (unique fact)

A version of the product formula holds over any number field, with some care for how the absolute values are normalized:

Let $K/\mathbb{Q}_p$ be a finite extension. The normalized absolute value $|\cdot|_K$ on K is:

for $a \in K^\times$, $a = u \cdot \pi^n$ for some $u \in \mathcal{O}_K^\times$, π unif, $n \in \mathbb{Z}$,

and $|a|_K = \left(\#\mathcal{O}_K/\pi\right)^{-n}$.

For $K = \mathbb{R}$ and $K = \mathbb{C}$, the normalized absolute values are

$|a|_{\mathbb{R}}$ = usual $|a|$ when $K = \mathbb{R} \ni a$.

$|a|_{\mathbb{C}}$ = usual $|a|^2$ when $K = \mathbb{C} \ni a$.

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 $\prod \max\{|ax_0|_v, \dots, |ax_n|_v\}$.

$$= \left(\prod_{v \in M_F} |a|_v\right) \cdot \prod_{v \in M_F} \max\{|x_0|_v, \dots, |x_n|_v\}.$$

$= 1$ by the product formula. ∎

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

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

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

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

The change-of-field result allows us to define

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

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

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