Here is the input we'll need for Mordell-Weil:

(K is a finite extension of $\mathbb{Q}_p$. E/K ell-curve with good reduction — for simplicity)

Theorem: For any $m \in \mathbb{Z}$ not divisible by p,

① $[m]: E_1(K) \to E_1(K)$ is an isomorphism.

($0 \to E_1(K) \to E(K) \to \bar{E}(k) \to 0$)

② For any $P \in E(K)$, there exists a finite unramified extension L/K and a $Q \in E(L)$ such that $[m]Q = P$.

③ The reduction map $E(K)[m] \to \bar{E}(k)$ is injective.

Pf: ① will take work. Let's show ① $\Rightarrow$ (② and ③).

Assume ①. ②: Take $P \in E(K)$, $\bar{P} \in \bar{E}(k)$ the reduction.

$[m]: \bar{E} \to \bar{E}$ is an isogeny, so $\exists\ k'/k$ finite and $\bar{Q} \in \bar{E}(k')$ such that $[m]\bar{Q} = \bar{P}$.

Let K'/K be the unramified extension with residue field k' (lemma start of class). Have exact sequence

$$0 \to E_1(K') \to E(K') \to \bar{E}(k') \to 0$$

$$\exists\ Q \longmapsto \bar{Q}$$

Now $[m]Q - P$ reduces to 0 in $\bar{E}(k')$, hence lies in $E_1(K') \overset{①}{=} [m] \cdot E_1(K')$, so $[m]Q - P = [m]Q'$, $Q' \in E_1(K')$, so

$P = [m] \cdot Q$ for some $Q' \in E(K')$.

③: $E_1(K) \cap E(K)[m] = \mathcal{O}$ by ① (inj.). ✓.

① next time → Proof of ①.

Can describe $E_1(K)$ as $E_1(K) = \{P \in E(K) \mid \exists\, x, y, z \in \mathcal{O}_K :$ $\varpi \mid x$, $\varpi \nmid y$, $\varpi \mid z$ and $P = [x, y, z]\}$ (ϖ = uniformizer of $\mathcal{O}_K$).

Define for $n \geq 1$

$$E_n(K) = \left\{ P \in E(K) \;\middle|\; \frac{x(P)}{y(P)} \in \varpi^n \mathcal{O}_K \right\}$$

(when $n=1$ this recovers previous $E_1(K)$)

Claim: *a) $E_n(K) < E(K)$ is a subgroup, and there is an iso of groups $E_n(K)/E_{n+1}(K) \xrightarrow{\sim} k$ (additive group)

$$P \longmapsto \left(\underbrace{\varpi^{-n} \frac{x(P)}{y(P)}}_{\in \mathcal{O}_K} \bmod \varpi \right).$$

(something stronger is true: get a fuller description of the group $E_1(K)$ using the formal group of E – see Sil. Chpt. IV).

b) $\bigcap_{n \geq 1} E_n(K) = \{\mathcal{O}\}$.

Pf of (a). By induction. For $P = [x, y, 1] \in E_1(K)$, $y \notin \mathcal{O}_K$, so $\exists\, m, m' \in \mathbb{Z}$, $u, v \in \mathcal{O}_K^*$: $x = \varpi^{-m} u$, $y = \varpi^{-m'} v$. (and $m' > 0$). Plugging into our fixed W.E. / $\mathcal{O}_K$, we see that $-3m = -2m'$, so $\exists\, d \in \mathbb{Z}$: $m = 2d$, $m' = 3d$. ($d > 0$).

Now for $P = [x, y, z]$, if $P \in E_n(K) \setminus E_{n+1}(K)$, then $\frac{x(P)}{y(P)} \in \varpi^n \mathcal{O}_K \setminus \varpi^{n+1} \mathcal{O}_K$, and $P \neq \mathcal{O}$, so $z(P) \neq 0$,

so $v(x) = -2n + v(z)$, hence $P = [\varpi^n x_0, y_0, \varpi^{3n} z_0]$

(v = normalized val'n on K) $v(y) = -3n + v(z)$

$x_0 \in \mathcal{O}_K^*$ $\hat{\mathcal{O}}_K^*$ $\hat{\mathcal{O}}_K^*$

(and if $P \in E_{n+1}(K)$, then $P = [\varpi^n x_0, y_0, \varpi^{3n} z_0]$ with $y_0 \in \mathcal{O}_K^\times$, $x_0, z_0 \in \mathcal{O}_K$). Plug in to our WE:

$$y_0^2 \varpi^{3n} z_0 + a_1 \varpi^{4n} x_0 y_0 z_0 + a_3 \varpi^{6n} y_0 z_0^2 = \varpi^{3n} x_0^3 + a_2 \varpi^{5n} x_0^2 z_0 + a_4 \varpi^{7n} x_0 z_0^2 + a_6 \varpi^{9n} z_0^3$$

ϖ^{3n} ϖ^{n} ϖ^{3n} ϖ^{2n} ϖ^{4n} ϖ^{5n}

Thus $\overline{P_0} := [\bar{x_0}, \bar{y_0}, \bar{z_0}] \in \mathbb{P}^2(k)$ lies on ($\overline{\ } = \text{red}^n \text{mod } \varpi$) the singular cubic $y^2 z = x^3$. This has unique singular point $(0,0)$, and $\overline{P_0} \neq (0,0)$ since $y_0 \in \mathcal{O}_K^\times$.

$\rightsquigarrow$ get a map $E_n(K) \longrightarrow C(k)_{ns} = C(k) \setminus \{(0,0)\}$

$$[x,y,z] \longmapsto [\bar{x_0}, \bar{y_0}, \bar{z_0}]$$

To check (PSet 5): This map is a group homomorphism where $C(k)_{ns}$ is equipped with the usual secant-tangent group law (with origin $[0,1,0]$) — for which $C(k)_{ns} \cong k$

$$[a,b,1] \longmapsto a/b$$
$$[a,1,0] = \mathcal{O} \longmapsto 0$$

The kernel is $E_{n+1}(K)$, which is therefore a subgroup of $E(K)$, and $E_n(K)/E_{n+1}(K) \hookrightarrow k$. (injective hom)

We won't need surj. for M-W, but it is another Hensel application.

b) $\left[\bigcap_{n\geq 1} E_n(K) = \{\mathcal{O}\}\right]$ Suppose $P \in \bigcap_{n\geq 1} E_n(K)$; then for $P = [x,y,z]$, $x \in \bigcap \varpi^n \mathcal{O}_K = 0$, $y \neq 0$, $z \in \bigcap \varpi^{3n} \mathcal{O}_K = 0$, so $P = [0,1,0]$.

Proof of (1), that $[m] : E_1(K) \to E_1(K)$ is an iso (for $(m,p)=1$).

Suppose $P \in E_1(K)[m] \setminus \mathcal{O}$. Then $P \in E_n(K) \setminus E_{n+1}(K)$, and under $E_n(K)/E_{n+1}(K) \hookrightarrow k$, P doesn't map to 0.

But k is a p-group, contradicting $(m,p)=1$. Thus $[m]$ is injective on $E_1(K)$.

Surj: Now let $Q \in E_1(K)$. Since $[m]$ is an iso on each $E_n(K)/E_{n+1}(K)$, can write $Q = [m]\cdot Q_1 + Q_1'$ $\quad Q_1' \in E_2(K), Q_1 \in E_1(K)$

$Q_1' = [m]\cdot Q_2 + Q_2'$ $\quad Q_2' \in E_3(K), Q_2 \in E_2(K)$

$Q_2' = \cdots$

So $Q = [m](Q_1 + Q_2 + \cdots + Q_n) + Q_n'$ $\quad Q_i \in E_i(K), Q_n' \in E_{n+1}(K)$, for any n.

Take $\lim_{n\to\infty}$ and get $Q = [m]\cdot P$ where $P = \sum_{i=1}^{\infty} Q_i$

($E(K) \subset \mathbb{P}^2(K)$ equipped with the v-adic topology is compact, b/c it is a closed subspace of $\mathbb{P}^2(K)$, which is itself compact. The $\{E_n(K)\}_{n\geq 1}$ form a basis of open neighborhoods of $\mathcal{O}$ in $E(K)$.), Thus $[m]$ is surjective on $E_1(K)$. ∎

Remark: ③ gives a handy way to compute $E(F)_{tor}$ when E is a number field! See PSet 5 for some examples.

For instance ③ implies $E(F)_{tor}$ is finite. ("easy half" of Mordell-Weil, which says $E(F)$ is finitely-generated)

Onto weak Mordell-Weil! Fix $m > 1$, F number field, E/F elliptic curve.

By defn, we have a short exact sequence

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

$[m]$ is an isogeny! we can take $x, y, z \in F$ uses Hilbert Thm. 90 ↑ Review Session Monday

$G_F = Gal(\bar{F}/F)$ $\quad [x,y,z] \in E(\bar{F})^{G_F}$: $\forall \sigma \in G_F$, $[\sigma x, \sigma y, \sigma z] = [x,y,z]$ ie $\exists \lambda_\sigma \in \bar{F}^\times$: $(\sigma x, \sigma y, \sigma z) = (\lambda_\sigma x, \lambda_\sigma y, \lambda_\sigma z)$. To show

$E(F) = E(\bar{F})^{G_F}$, so it is natural to study what happens to this sequence when we take

G_F-invariants:

$0 \to E[m](F) \to E(F) \xrightarrow{[m]} E(F)$ is exact,

but $[m]$ is not surjective on $E(F)$.

Galois cohomology provides an optimal tool for understanding this failure of surjectivity, i.e. the structure of $E(F)/mE(F)$.

It allows us easily to reduce finiteness of $E(F)/mE(F)$ to the fundamental finiteness theorems for numberfields

See the review session. Quick recap (Quick Intro to Gal Coh.) MONDAY afternoon (TBD)

Let K be any perfect field, $G_K = \mathrm{Gal}(\bar{K}/K)$ (Focus, K a number field or a p-adic field)

Let M be a discrete G_K-module:

"discrete" means $\forall\, m \in M$, $\exists\, L/K$ finite such that $m \in M^{G_L} = \{x \in M \mid \sigma x = x \ \forall \sigma \in G_L\}$

Ex: $\bar{K}, \bar{K}^*$ are discrete G_K-modules

Set $H^0(G_K, M) = M^{G_K}$ (degree 0 cohomology of G_K acting on M)

Ex: $H^0(G_K, \bar{K}) = \bar{K}^{G_K} = \{x \in \bar{K} \mid \forall \sigma \in G_K, \sigma x = x\} = K$.

Set $H^1(G_K, M) = \dfrac{\{\text{continuous maps } \varphi: G_K \to M \mid \varphi(gh) = \varphi(g) + g\cdot\varphi(h)\ \forall g,h \in G_K\}}{\{\varphi \mid \exists m \in M : \varphi(g) = g\cdot m - m \ \forall g \in G_K\}}$

"twisted homomorphisms" / "1-cocycles"

"1-coboundaries"

check: Suppose $\varphi(g) = g\cdot m - m$ $\forall g$. Then $\varphi(gh) =$

$gh \cdot m - m = g \cdot (hm - m) + g \cdot m - m = g \cdot \varphi(h) + \varphi(g)$.

"continuous" here means [continuous where G_K has its Krull topology & M is equipped with the discrete.] Concretely, it means that $\varphi^{-1}(0) = G_L < G_K$ for some finite extension $K \subset L \subset \bar{K}$.

In particular, replacing L/K by its Galois closure $\tilde{L}/K$, $G_{\tilde{L}} \subset \varphi^{-1}(0)$, and for $g \in G_K$, $h \in G_{\tilde{L}}$,

$\varphi(gh) = \varphi(g) + g \cdot \varphi(h) = \varphi(g)$; and moreover

$\varphi(hg) = \varphi(g g^{-1} h g) = \varphi(g)$

$\varphi(h) + h \cdot \varphi(g)$

$h \cdot \varphi(g)$

(*) Thus φ is induced by "inflation" from a map $G_K/G_{\tilde{L}} \longrightarrow M^{G_{\tilde{L}}}$.

Ex: If $G_K \curvearrowright M$ trivial, then (i.e. $\forall m \in M, \sigma \in G_K$, $\sigma m = m$)

$$H^1(G_K, M) = \mathrm{Hom}_{\mathrm{cts}}(G_K, M)$$

(cts $\leftrightarrow$ factors through a finite $\mathrm{Gal}(L/K)$)

Ex: Hilbert Thm 90. $H^1(G_K, \bar{K}^\times) = \{1\}$.

(Review Session)

Fundamental facts we will need:

(1) (PSet 5) For any short-exact sequence of discrete G_K-modules,

$$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

there is an associated long-exact (LES) sequence of abelian groups:

$$0 \to M^{G_K} \to N^{G_K} \to P^{G_K} \xrightarrow{\delta} H^1(G_K, M) \to H^1(G_K, N) \to H^1(G_K, P)$$

Rmk: there are coh-gps $H^n(G_K, -)$ & there give a longer exact sequence.

All the maps in the LES are induced by f and g except for $\delta : P^{G_K} \to H^1(G_K, M)$

$$\exists\, n \in N : g(n) = P \longmapsto [\sigma \mapsto \sigma \cdot n - n]$$

check this function of σ lands in M and is a 1-cocycle

② Let L/K be a finite Galois extension, M a discrete G_K-module, hence also a discrete G_L-module.

$\rightsquigarrow$ restriction map

$$H^1(G_K, M) \to H^1(G_L, M)$$

$$[\varphi] \longmapsto [\varphi|_{G_L}]$$

Also, M^{G_L} is a $\mathrm{Gal}(L/K) \cong G_K/G_L$-module,

$\rightsquigarrow$ inflation map

$$H^1(\mathrm{Gal}(L/K), M^{G_L}) \xrightarrow{\inf} H^1(G_K, M)$$

$$[\varphi] \longmapsto [\sigma \in G_K \mapsto \varphi(\bar{\sigma}) \in M^{G_L} \subset M]$$

(where $\bar{\sigma} \in \mathrm{Gal}(L/K)$)

Lemma: inf and res yield an exact sequence

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

(*) See Review Session & PSet for more!

We will freely use this language on Monday in class.

Silverman's book discusses group & Galois cohomology at this concrete level.