Computing the Mordell-Weil Group (Complete 2-descent)

E/K elliptic curve, with $E[m] \subseteq E(K)$ for some $m \geq 2$.

- **Weil pairing:** $e_m : E[m] \times E[m] \longrightarrow \mu_m$
- **Kummer pairing:** $\kappa : E(K) \times \mathrm{Gal}(\bar{K}/K) \longrightarrow E[m]$

  $(P, \sigma) \longmapsto \kappa(P,\sigma) = Q^\sigma - Q$ w/ $[m]Q = P$.

  ↳ induces: $\delta_E : E(K)/mE(K) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), E[m])$

  $P \longmapsto \delta_E(P) : G_{\bar{K}} \longrightarrow E[m]$

  $\sigma \mapsto \delta_E(P)(\sigma) = \kappa(P,\sigma)$
- **Hilbert's Thm 90**

  ↳ induces: $(\mu_m \subseteq K)$

  $\delta_K : K^\times/(K^\times)^m \xrightarrow{\cong} \mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), \mu_m)$

  $b \longmapsto \delta_K(b) : G_{\bar{K}} \to \mu_m$ s.t. $\delta_K(b)(\sigma) = \frac{\sigma(\beta)}{\beta}$ for $\beta^m = b$.

Therefore: $e_m(\delta_E(P)(\cdot), T) = \delta_K(b)(\cdot)$ for some $b = b(P,T)$.

($\delta_E(P) = K(P,\cdot)$, $e_m(\cdot,T) \in \mathrm{Hom}(G_{\bar{K}}, \mu_m)$)

Thm. (a) There is a bilinear pairing $b : E(K)/mE(K) \times E[m] \to K^\times/(K^\times)^m$ s.t. $b(P,T)$ is the unique class s.t. $e_m(\delta_E(P)(\sigma), T) = \delta_K(b(P,T))(\sigma)$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$.

(b) The pairing is non-deg on the left. Thus: $E(K)/mE(K) \hookrightarrow \mathrm{Hom}(E[m], K^\times/(K^\times)^m)$, $P \longmapsto b(P,\cdot)$

(c) Let $S = M_K^\infty \cup \{\text{bad primes of } E/K\} \cup \{\text{primes } | m\} \subseteq M_K$.

Then the image of hom's in pairing b lies in $K(S,m) = \{b \in K^\times/(K^\times)^m : \mathrm{ord}_v(b) \equiv 0 \bmod m \ \forall v \notin S\}$

(we proved that $K(S,m)$ is finite when proving Weak M-W)

(d) The pairing may be computed: $\mathrm{div}(f_T) = m(T) - m(\mathcal{O})$

$T \in E[m]$, choose $f_T, g_T \in K(E)$ w/ $f_T \circ [m] = g_T^m$

then $P \neq T$, $b(P,T) \equiv f_T(P) \bmod (K^\times)^m$.

Q: How does this help?

$b(P,T) \equiv \rho_T(P) \bmod (K^\times)^m$ and b