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?

$b(P,T) \equiv \beta_T(P) \bmod (K^\times)^m$ and $b(P,T) \in K(S,m)$, $E[m] = \langle T_1, T_2 \rangle$

For each $(b_1, b_2) \in K(S,m)^2$ try to solve:

$$\begin{cases} P \in y^2 = f(x) \\ b_1 z_1^m = \beta_{T_1}(P) \\ b_2 z_2^m = \beta_{T_2}(P) \end{cases} \Longrightarrow \begin{array}{c} (C) \\ \| \\ (C_{b_1,b_2}) \end{array} \begin{cases} y^2 = x^3 + Ax + B \\ b_1 z_1^m = \beta_{T_1}(x,y) \\ b_2 z_2^m = \beta_{T_2}(x,y) \end{cases}$$

with $(x, y, z_1, z_2) \in K \times K \times K^\times \times K^\times$

"homogeneous space"

Pf. (a) $b : E(k)/mE(k) \times E[m] \longrightarrow k^\times/(k^\times)^m$

Existence + Well-defined follows from Thm 90, i.e., $k^\times/(k^\times)^m \cong \mathrm{Hom}(G_k, \mu_m)$

κ, e_m are bilinear $\Rightarrow$ b is bilinear.

(b) Suppose $b(P,T) = 1 \quad \forall T \in E[m]$

i.e., $\forall T \in E[m]$, $\forall \sigma \in G_k$, $e_m(\kappa(P,\sigma), T) = 1$

e_m is non-deg $\Rightarrow$ $\kappa(P,\sigma) = O \ \forall \sigma \Rightarrow P \in mE(k)$. $\Rightarrow P \equiv O$ in E/m.

Left ker of κ

(c) $K(S,m) = \{ b \in k^\times/(k^\times)^m : \mathrm{ord}_v(b) \equiv 0 \bmod m \ \forall v \notin S \}$, $S = M_k^\infty \cup \{\text{bad}\} \cup \{v \mid m\}$

Let $\beta = b(P,T)^{1/m} \Rightarrow K(\beta) \subseteq L = k([m]^{-1}E(k))$

Why? If $\sigma \in G_{\bar{k}/L}$ then $\kappa(P,\sigma) = Q^\sigma - Q = O$

$\Rightarrow e_m(\delta_{E(P)}(\sigma), T) = e_m(O,T) = 1$ (where $\delta_{E(P)}(\sigma) = \delta_k(b(P,T))(\sigma)$)

$b(P,T) = 1 = \frac{\sigma(\beta)}{\beta}$

$\Rightarrow \sigma(\beta) = \beta \Rightarrow \beta \in L$. $\forall \sigma \in G_{\bar{k}/L}$

We just proved $\beta = b(P,T)^{1/m} \Rightarrow k(\beta) \subseteq L = k([m]^{-1}E(k))$

We proved: L/k is unramified outside S

$\Rightarrow$ If $v \in M_k^0$, $v(m)=0$, then $k(\beta)/k$ unram. $\Leftrightarrow ord_v(b) \equiv 0 \bmod m$

$\Rightarrow b(P,T) \in K(S,m)$. ▨

(d) $\underline{b(P,T) \equiv f_T(P) \bmod (k^x)^m}$ Let $Q \in E$, $P = [m]Q$, $\beta \in \bar{K}^x$ s.t. $b(P,T) = \beta^m$

$\forall \sigma \in G_k \quad e_m(f_E(P)(\sigma), T) = f_k(b(P,T))(\sigma)$

$$\| \qquad\qquad \| \qquad\qquad \| \qquad\qquad \| \qquad\qquad \|$$

$$e_m(Q^\sigma - Q, T) = \frac{\sigma(\beta)}{\beta}$$

$$\| \qquad\qquad \| \qquad\qquad \| \qquad\qquad \|$$

$$\frac{g_T(X+Q^\sigma-Q)}{g_T(X)} = \frac{\sigma(\beta)}{\beta} \xrightarrow{X=Q} \frac{g_T(Q)^\sigma}{g_T(Q)} = \frac{\beta^\sigma}{\beta}$$

δ_k isom: $g_T(Q) \equiv \beta \bmod (k^x)^m \Rightarrow g_T(Q)^m \equiv \beta^m \bmod (k^x)^m$ (recall: $f_T \circ [m] = g_T^m$)

So $f_T(P) = f_T([m]Q) = g_T(Q)^m \equiv \beta^m \equiv b(P,T) \bmod (k^x)^m$ ▨

Complete 2-descent

$m=2$, $E[2] \subseteq E(K)$, $y^2 = f(x) = (x-e_1)(x-e_2)(x-e_3)$, $e_i \in K$, $e_i \neq e_j$

$T_i = (e_i, 0)$ non-trivial 2-tors. pts.

Put $f_{T_i}(x,y) = x - e_i$ then $\mathrm{div}(f_{T_i}) = 2(T_i) - 2(O)$.

and $f_{T_i} \circ [2] = X([2]) - e_i = \dfrac{(x^2 - 2e_i x - 2e_i^2 + 2(e_1+e_2+e_3)e_i - (e_1e_2 + e_1e_3 + e_2e_3))^2}{(2y)^2} = g_{T_i}^2$

Let $(b_1, b_2) \in K(S,2) \times K(S,2)$.

Q Is there $P = (x,y) \in E(K)/2E(K)$ with $b(P,T_1) = b_1$, $b(P,T_2) = b_2$?

$\iff (x, y, z_1, z_2) \in K \times K \times K^\times \times K^\times$

$$\begin{cases} y^2 = (x-e_1)(x-e_2)(x-e_3) \\ b_1 z_1^2 = x - e_1 \\ b_2 z_2^2 = x - e_2 \end{cases}$$

Put z_3 s.t. $y = b_1 b_2 z_1 z_2 z_3$

$\Rightarrow (b_1 b_2 z_1 z_2 z_3)^2 = b_1 z_1^2 \, b_2 z_2^2 (x - e_3)$

$\Rightarrow$ (cancel out) $b_1 b_2 z_3^2 = x - e_3$

$$\iff \begin{cases} b_1 z_1^2 = x - e_1 \\ b_2 z_2^2 = x - e_2 \\ b_1 b_2 z_3^2 = x - e_3 \end{cases} \longrightarrow \begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1 \end{cases} \quad (C_{b_1, b_2})$$

Note If we find $(z_1, z_2, z_3) \Longrightarrow P = (x, y) = (b_1 z_1^2 + e_1 \,,\, b_1 b_2 z_1 z_2 z_3) \in E(k)$

- If $P = T_i$ use linearity:

$$b(T_1, T_1) = \frac{b(T_1, T_1 + T_2)}{b(T_1, T_2)} = \frac{b_1(T_1, T_3)}{b(T_1, T_2)} = \frac{e_1 - e_3}{e_1 - e_2}$$

$$b(T_2, T_2) = \frac{e_2 - e_3}{e_2 - e_1}$$

Thm (Complete 2-descent)

$E/K : y^2 = (x-e_1)(x-e_2)(x-e_3)$ $\quad e_i \in K$, $e_i \neq e_j$.

Let $S = M_K^\infty \cup \{\text{bad places of } E/K\} \cup \{\text{places dividing } 2\}$

Let $K(S,2) = \{b \in K^\times/(K^\times)^2 : \mathrm{ord}_v(b) \equiv 0 \bmod 2 \ \ \forall v \notin S\}$

Then, there is an injective homomorphism: $E(K)/2E(K) \longrightarrow K(S,2) \times K(S,2)$

defined by

$$P=(x,y) \longmapsto \begin{cases} (x-e_1, x-e_2) & \text{if } x \neq e_1, e_2 \\ \left(\frac{e_1-e_3}{e_1-e_2}, e_1-e_2\right) & \text{if } x = e_1 \\ \left(e_2-e_1, \frac{e_2-e_3}{e_2-e_1}\right) & \text{if } x = e_2 \\ (1,1) & \text{if } P = \mathcal{O}. \end{cases}$$

Moreover:

If $(b_1, b_2) \in K(S,2)^2$ is the image of $P \neq \mathcal{O}, T_1, T_2$ then

$$P=(x,y) \Longleftrightarrow \begin{cases} b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1 \end{cases} \quad \text{for } (z_1, z_2, z_3) \in K^\times \times K^\times \times K$$

$$\text{and } P = \left(b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3\right).$$

EXAMPLE (Find $E(\mathbb{Q})$)

Let $E/\mathbb{Q}: y^2 = x^3 - 12x^2 + 20x = x(x-2)(x-10)$

$$\Delta_E = 409600 = 2^{14} \cdot 5^2, \quad c_4 = 2^6 \cdot 3 \cdot 7.$$

There is bad reduction at 2 (additive), 5 (multiplicative).

Torsion: $E[2] \subseteq E(\mathbb{Q})$, more? Recall: $E(\mathbb{Q})[m] \hookrightarrow \tilde{E}(\mathbb{F}_p)$ (p is good, $p \nmid m$)

$p=3$ (good), $\#\tilde{E}(\mathbb{F}_3) = 4$ (no prime-to-3 torsion other than $E[2]$), $p=11$ (good), $\#\tilde{E}(\mathbb{F}_{11}) = 16$ (no 3-torsion.) $\Rightarrow E(\mathbb{Q})_{tors} = E(\mathbb{Q})[2]$.

$S = \{\infty, 2, 5\}$, $\mathbb{Q}(S,2) = \{b \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 : \mathrm{ord}_p(b) \equiv 0 \bmod 2 \ \forall p \notin S\}$

$= \{\pm 1, \pm 2, \pm 5, \pm 10\}$ (size 8)

Thus,

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \underbrace{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})}_{\text{size } 2^{R+2}} \xrightarrow{R_{E/\mathbb{Q}}} \underbrace{\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)}_{\text{size } 8^2 = 2^6}$$

$R+2 \le 6 \Rightarrow R \le 4$