Complete 2-Descent : An Example

Previously...

Weil pairing + Kummer pairing + Hilbert's Thm 90

↳ Bilinear pairing $b : E(K)/mE(K) \times E[m] \longrightarrow K^\times/(K^\times)^m$

s.t. $e_m(\kappa(P,\sigma), T) = \delta_\kappa(b(P,T))(\sigma)$.

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

$P \longmapsto b(P,\cdot)$

s.t. $b(P,T) \in K(S,m) = \{ b \in K^\times/(K^\times)^m : \mathrm{ord}_v(b) \equiv 0 \bmod m \ \ \forall v \notin S \}$

w/ $S = M_K^\infty \cup \{\text{bad primes}\} \cup \{\text{primes } | m\} \subseteq M_K$

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

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

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

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

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

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

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

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,

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

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

(C) $\begin{cases} (1) \quad b_1 z_1^2 - b_2 z_2^2 = 2 \\ (2) \quad b_1 z_1^2 - b_1 b_2 z_3^2 = 10 \end{cases}$

$e_1 = 0, \quad e_2 = 2, \quad e_3 = 10$

b_2 \ b_1	1	2	5	10	-1	-2	-5	-10
1	0			$T_3 = (10,0)$	$b_1 < 0$, $b_2 > 0$, (1) $\mathbb{R}$			
2								
5	?							
10								
-1		$T_2 = (2,0)$			$b_1 < 0$, $b_2 < 0$, $b_1 \cdot b > 0$, (2) $\mathbb{R}$			
-2			$T_1 = (0,0)$					
-5								
-10								

$$(C)\begin{cases} b_1 z_1^2 - b_2 z_2^2 = 2 \\ b_1 z_1^2 - b_1 b_2 z_3^2 = 10 \end{cases}$$

$5 \nmid b_1$

Case $(b_1, b_2) = (1,5)$

$$(C)\begin{cases} (1)\ z_1^2 - 5z_2^2 = 2 \\ (2)\ z_1^2 - 5z_3^2 = 10 \end{cases}$$

Work over $\mathbb{Q}_5$:

$$v_p(xy) = v_p(x) + v_p(y)$$
$$v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$$
(equal if $v_p(x) \neq v_p(y)$)

Claim 1 $z_1, z_2 \in \mathbb{Z}_5$

(1) $v_5(z_1^2 - 5z_2^2) = v_5(2) = 0$

$\| $

$\min\{2v_5(z_1),\ 1 + 2v_5(z_2)\}$

$\Rightarrow v_5(z_1),\ v_5(z_2) \geq 0 \rightarrow z_1, z_2 \in \mathbb{Z}_5$. ▨

Claim 2 $z_3 \in \mathbb{Z}_5$

(2) $v_5(z_1^2 - 5z_3^2) = v_5(10) = 1$

$\| $

$\min\{2v_5(z_1),\ 1 + 2v_5(z_3)\} \Rightarrow v_5(z_3) \geq 0$ ▨

From (1), $z_1, z_2 \in \mathbb{Z}_5 \Rightarrow z_1^2 \equiv 2 \bmod 5$ but $2 \neq \square \bmod 5$ ↯