Let's Fix

- k : a number field
- $E : Y^2 = (X - a_1)(X - a_2)(X - a_3)$:
  an elliptic curve defined over k whose 2-torsion points are all rational.
- $\mathcal{B}$: a finite set of "bad primes" consisting of places dividing 2 or ∞ and odd primes dividing $(a_1 - a_2)(a_2 - a_3)(a_3 - a_1)$ and representatives of ideal class group.

The $\mathbb{F}_2$-space of 2-coverings of E

$m = (m_1, m_2, m_3) \in (k/k^2)^3$ satisfying $m_1 m_2 m_3$ is square.
For such m, $\Gamma(m)$ is a 2-covering of E given by :

$$m_i Y_i^2 - m_j Y_j^2 = (c_j - c_i) Y_0^2 \text{ for } i, j \in \{1, 2, 3\}$$

The correspondence $\Gamma(m) \mapsto (m_1, m_2)$ gives a bijection between the set of 2-coverings of E and $(k/k^2)^2$. This map makes the set of 2-coverings a $\mathbb{F}_2$-space.

The set of 2-coverings soluble at each prime outside $\mathcal{B}$ corresponds to $(\mathbf{o}_{\mathcal{B}}^* / \mathbf{o}_{\mathcal{B}}^{*2})$, where $\mathbf{o}_{\mathcal{B}}^*$ is the multiplicative group of units outside $\mathcal{B}$.

- **Let's denote**

  $X_{\mathcal{B}} = \mathcal{O}^*_{\mathcal{B}}/\mathcal{O}^{*2}_{\mathcal{B}}$, $Y_v = k^*_v/k^{*2}_v$, $Y_{\mathcal{B}} = \bigoplus_{v\in\mathcal{B}} Y_v$

  $V_v = Y_v \times Y_v$, $V_{\mathcal{B}} = Y_{\mathcal{B}} \times Y_{\mathcal{B}} = \bigoplus_{v\in\mathcal{B}} V_v$

  $U_{\mathcal{B}}$ is the image of $X_{\mathcal{B}} \times X_{\mathcal{B}}$ in $V_{\mathcal{B}}$.

- If $|\mathcal{B}| = n$,
  $X_{\mathcal{B}}$ is n-dimensional over $\mathbb{F}_2$.(by unit theorem)

  $Y_{\mathcal{B}}$ is $2n$-dimensional over $\mathbb{F}_2$ since $|Y_v| = 4/|2|_v$.

  The canonical map $X_{\mathcal{B}} \to Y_{\mathcal{B}}$ is injective.(class field theory)

Define a non-degenerate alternating bilinear form $e_{\mathcal{B}}$ on $V_{\mathcal{B}}$ given by

$$e_{\mathcal{B}} = \prod_{v \in \mathcal{B}} e_v \text{ where } e_v(a \times b, c \times d) = (a, d)_v (b, c)_v.$$

$U_{\mathcal{B}}$ is a maximal isotropic in $V_{\mathcal{B}}$ w.r.t $e_{\mathcal{B}}$ by Hilbert product theorem.

$T_v =$ the image of $\mathcal{O}_v/\mathcal{O}_v^2$ in V_v.
$W_v =$ the image of $E(k_v)$ in V_v under the Kummer map $(X, Y) \mapsto (X - c_1, X - c_2)$.
$W_{\mathcal{B}} = \bigoplus_{v \in \mathcal{B}} W_v$

W_v is a maximal isotropic in V_v.(Tate)
$T_v = W_v$ if v is not a place of bad reduction.
$\Gamma(m)$ is locally soluble at v iff the corresponding point (m_1, m_2) is in W_v.

2-Selmer group of E is
$U_{\mathcal{B}} \bigcap W_{\mathcal{B}}$ = left and right kernel of $U_{\mathcal{B}} \times W_{\mathcal{B}} \to \pm 1$ by $e_{\mathcal{B}}$
since $U_{\mathcal{B}}, W_{\mathcal{B}}$ are maximal isotropic.

Lemma There exist maximal isotropics K_v in V_v such that $V_{\mathcal{B}} = U_{\mathcal{B}} \bigoplus K_{\mathcal{B}}$
where $K_{\mathcal{B}} = \bigoplus_{v \in \mathcal{B}} K_v$.

$t_{\mathcal{B}} : V_{\mathcal{B}} \to U_{\mathcal{B}}$ is the projection along $K_{\mathcal{B}}$.
This $t_{\mathcal{B}}$ induces

$$\tau_{\mathcal{B}} : W'_{\mathcal{B}} = W_{\mathcal{B}} / (W_{\mathcal{B}} \bigcap K_{\mathcal{B}}) \simeq U_{\mathcal{B}} \bigcap (W_{\mathcal{B}} + K_{\mathcal{B}}) = U'_{\mathcal{B}}.$$

$e_{\mathcal{B}}$ induces a bilinear map $e'_{\mathcal{B}}$ on $W'_{\mathcal{B}} \times U'_{\mathcal{B}}$.

Theorem The bilinear forms on $W_{\mathcal{B}}$ and $U_{\mathcal{B}}$ given by :

$$u_1' \times u_2' \mapsto e_{\mathcal{B}}'(u_1', \tau_{\mathcal{B}}^{-1} u_2') \text{ and } w_1' \times w_2' \mapsto e_{\mathcal{B}}'(\tau_{\mathcal{B}} w_1', w_2')$$

are symmetric and their kernels are isomorphic to the 2-Selmer group of E.

Proof Let $t_{\mathcal{B}} w_i = u_i'$. Note that $(1 - t_{\mathcal{B}}) w_i \in K_{\mathcal{B}}$. Then

$$\begin{aligned} 1 &= e_{\mathcal{B}}(w_1, w_2) = e_{\mathcal{B}}(t_{\mathcal{B}} w_1 + (1 - t_{\mathcal{B}}) w_1, t_{\mathcal{B}} w_2 + (1 - t_{\mathcal{B}}) w_2)) \\ &= e_{\mathcal{B}}(t_{\mathcal{B}} w_1, (1 - t_{\mathcal{B}}) w_2) e_{\mathcal{B}}((1 - t_{\mathcal{B}}) w_1, t_{\mathcal{B}} w_2) = e(t_{\mathcal{B}} w_1, w_2) e_{\mathcal{B}}(w_1, t_{\mathcal{B}} w_2) \\ &= e_{\mathcal{B}}'(u_1', w_2) e_{\mathcal{B}}'(u_2', w_1). \quad \square \end{aligned}$$