R. Visser

Elliptic Curves – Example Sheet 4

1 (i) $\phi^{-1}(0,0) = E[2] \setminus \{0, (0,0)\}$

$(0,0) \in \phi E(K) \iff x^2+ax+b = 0$ has roots in K

$\iff b' = a^2 - 4b \in (K^*)^2$

(ii) Suppose $(X,Y) \xmapsto{\phi} (x,y)$. Then $x = \left(\frac{Y}{X}\right)^2 = \frac{X^2+aX+b}{X}$

$\Rightarrow X^2 + (a-x)X + b = 0$ —(*)

$\Rightarrow X = \frac{1}{2}(x-a \pm \sqrt{\delta})$

where $\delta = (x-a)^2 - 4b = x^2+a'x+b' = \frac{y^2}{x} = \left(\frac{y}{t}\right)^2$

$\therefore X = x_1$ or x_2 (as defined in the question)

Since x_1, x_2 are the roots of (*) we have $\begin{cases} x_1+x_2 = x-a \\ x_1x_2 = b \end{cases}$

Taking $X = x_1$ we have

$y = \frac{Y}{x_1}\left(x_1 - \frac{b}{x_1}\right) = \frac{Y}{x_1}(x_1-x_2) = \frac{Yy}{x_1 t} \Rightarrow Y = x_1 t$

Check: $(x_1 t)^2 = x_1^2 x = x_1^2(x_1+x_2+a) = x_1(x_1^2+ax_1+b)$

Similarly taking $X = x_2$ gives $Y = -x_2 t$

$\therefore \phi^{-1}(x,y) = \{(x_1, x_1 t), (x_2, -x_2 t)\}$

(iii) Suppose $(x,y) \in E'(K)$ with $x \neq 0$

Then $(x,y) \in \phi E(K) \underset{(ii)}{\iff} x \in (K^*)^2 \iff (x,y) \in \ker \alpha$

Moreover $T' \in \phi E(K) \underset{(i)}{\iff} b' \in (K^*)^2 \iff T' \in \ker \alpha$

(iv) $y = \lambda x + \nu$ passes through $P_i = (x_i, y_i)$ $i = 1,2,3$

x_1, x_2, x_3 are roots of $x(x^2+a'x+b') - (\lambda x+\nu)^2 = 0$

Looking at the constant term $\Rightarrow x_1x_2x_3 = \nu^2$ —(**)

(v) We must check $\alpha(P_1)\alpha(P_2)\alpha(P_3) \in (K^*)^2$

whenever $P_1, P_2, P_3 \in E'(K)$ with $P_1+P_2+P_3 = 0$

- If $P_1, P_2, P_3 \neq 0, T'$ then we're done by (iv)
- If $P_1 = 0$ then $P_2 = -P_3$ and $\alpha(P_2) = \alpha(P_3)$ ✓
- If $P_1 = T'$, $P_2, P_3 \neq 0, T'$ then x_1, x_2, x_3 are still the roots of (**), but now $x_1 = 0$ and $\nu = 0$

$\therefore x_2, x_3$ are the roots of $x^2 + a'x + b' - \lambda^2 x = 0$

$\Rightarrow x_2x_3 = b' \Rightarrow \alpha(P_2)\alpha(P_3) = \alpha(P_1)$ ✓

- If $P_1 = P_2 = T'$ then $P_3 = 0$, & we are done by an earlier case.

2. $E: y^2 = x^3 - 4x$

$\mathrm{Im}(\alpha_E) \subset \langle -1, 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\alpha_E(0,0) = (-4)(\mathbb{Q}^*)^2 \Rightarrow -1 \in \mathrm{Im}(\alpha_E)$

$b_1 = 2$: $w^2 = 2u^4 - 2v^4$ $(u,v,w) = (1,1,0)$

$\therefore \mathrm{Im}(\alpha_E) = \langle -1, 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E': y^2 = x^3 + x$

$\mathrm{Im}(\alpha_{E'}) \subset \langle -1 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$b_1 = -1$: $w^2 = -u^4 - v^4$ insoluble over $\mathbb{R}$

$\therefore \mathrm{Im}(\alpha_{E'}) = 0$

$\therefore$ rank $E(\mathbb{Q}) = 0$ (see lectures) $\Rightarrow$ 2 is not a congruent number

3(i) $E: y^2 = x(x^2+6x-2)$

$\mathrm{Im}(\alpha_E) \subset \langle -1, 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$b_1 = -1$: $w^2 = -u^4 + 6u^2v^2 + 2v^4$

If (u,v,w) soluble over $\mathbb{Q}$ we may assume $u, v \in \mathbb{Z}$ coprime

Then u must be odd & $w^2 \equiv -1 + 2v^2 + 2v^4 \equiv -1 \pmod 4$ ✗

$\therefore \mathrm{Im}(\alpha_E) = \langle -2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E': y^2 = x(x^2-12x+44)$

$\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2, 11 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$b_1 < 0$: insoluble over $\mathbb{R}$

$b_1 = 2$: $w^2 = 2u^4 - 12u^2v^2 + 22v^4$ ⟩ replace w by $2w$

$2w^2 = u^4 - 6u^2v^2 + 11v^4$ ⟩

If $u, v \in \mathbb{Z}$ coprime, then u and v must be odd

N.B. $u \equiv 1 \pmod 2 \Rightarrow u^2 \equiv 1 \pmod 8 \Rightarrow u^4 \equiv 1 \pmod{16}$

$\therefore 2w^2 \equiv 1 - 6 + 11 \pmod{16}$

$\Rightarrow w^2 \equiv 3 \pmod 8$ ✗

] would be enough for this to hold mod 4.

$\therefore$ $\mathrm{Im}(\alpha_{E'}) = \langle 11 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\therefore$ rank $E(\mathbb{Q}) = 0$.

(ii) $E: y^2 = x(x^2+8x-7)$

$\mathrm{Im}(\alpha_E) \subset \langle -1, 7 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\sigma_1 = -1$: $\omega^2 = -u^4 + 8u^2v^2 + 7v^4$ ✗ over $\mathbb{Q}_2$

$\therefore$ $\mathrm{Im}(\alpha_E) = \langle -7 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$(92 = 2^2 \cdot 23)$

$E': y^2 = x(x^2-16x+92)$

$\mathrm{Im}(\alpha_E) \subset \langle -1, 2, 23 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\sigma_1 < 0$: insoluble over $\mathbb{R}$

$\sigma_1 = 2$: $\omega^2 = 2u^4 - 16u^2v^2 + 46v^4$ ↘ replace ω by 2ω

$2\omega^2 = u^4 - 8u^2v^2 + 23v^4$ $(u,v,\omega) = (3,1,4)$

$\therefore$ $\mathrm{Im}(\alpha_{E'}) = \langle 2, 23 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\therefore$ rank $E(\mathbb{Q}) = 1$.

(iii) $E: y^2 = x(x^2-3x+10)$

$\mathrm{Im}(\alpha_E) \subset \langle -1, 2, 5 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\sigma_1 < 0$: insoluble over $\mathbb{R}$

$\sigma_1 = 2$: $\omega^2 = 2u^4 - 3u^2v^2 + 5v^4$ $(u,v,\omega) = (1,1,2)$

$\therefore$ $\mathrm{Im}(\alpha_E) = \langle 2, 5 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E': y^2 = x(x^2+6x-31)$

$\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 31 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\sigma_1 = -1$: $\omega^2 = -u^4 + 6u^2v^2 + 31v^4$ $(u,v,\omega) = (1,1,6)$

$\therefore$ $\mathrm{Im}(\alpha_{E'}) = \langle -1, 31 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\therefore$ rank $E(\mathbb{Q}) = 2$.

$(377 = 13 \cdot 29)$

(iv) $E: y^2 = x(x^2-377)$

$\mathrm{Im}(\alpha_E) \subset \langle -1, 13, 29 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\sigma_1 = -13$ $\omega^2 = -13u^4 + 29v^4$ $(u,v,\omega) = (1,1,4)$

$\sigma_1 = -1$ $\omega^2 = -u^4 + 377v^4$ $(u,v,\omega) = (2,1,19)$

$\therefore$ $\mathrm{Im}(\alpha_E) = \langle -1, 13, 29 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E': y^2 = x(x^2+4.377)$

$\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2, 13, 29 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\sigma_1 < 0$: insoluble over $\mathbb{R}$

$\sigma_1 = 2$: $\omega^2 = 2u^4 + 2.377v^4$ ↘ replace ω by 2ω

$2\omega^2 = u^4 + 377v^4$ ✗ over $\mathbb{Q}_{13}$ since $\left(\frac{2}{13}\right) = -$

$\sigma_1 = 29$: $\omega^2 = 29u^4 + 52v^4$ $(u,v,\omega) = (1,1,9)$

$\therefore$ $\mathrm{Im}(\alpha_{E'}) = \langle 13, 29 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\therefore$ rank $E(\mathbb{Q}) = 3$.

4. $E: y^2 = x^3 - p^2x$

$\mathrm{Im}(\alpha_E) \subset \langle -1, p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\sigma_1 = p$: $\omega^2 = pu^4 - pv^4$ $(u,v,\omega) = (1,1,0)$

$\therefore$ $\mathrm{Im}(\alpha_E) = \langle -1, p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E': y^2 = x^3 + 4p^2x$

$\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2, p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$\sigma_1 < 0$: insoluble over $\mathbb{R}$

$\sigma_1 = 2$: $\omega^2 = 2u^4 + 2p^2v^4$ ↘ replace ω by 2ω

$2\omega^2 = u^4 + p^2v^4$

Suppose $u, v \in \mathbb{Z}$ coprime. $\left(\frac{2}{p}\right) = -1 \Rightarrow p \mid u, \omega$

writing $u = pu_1$, $\omega = p\omega_1$ gives $2\omega_1^2 = p^2u_1^4 + v^4$

$\left(\frac{2}{p}\right) = -1 \Rightarrow p \mid v$ ✗ to u, v coprime

$\sigma_1 = p$: $\omega^2 = pu^4 + 4pv^4$

$\rightsquigarrow$ $p\omega^2 = u^4 + 4v^4$ ✗ over $\mathbb{Q}_p$ since $\left(\frac{-1}{p}\right) = -1$

$\sigma_1 = 2p$ $\omega^2 = 2pu^4 + 2pv^4$

$\rightsquigarrow$ $2p\omega^2 = u^4 + v^4$ ✗ over $\mathbb{Q}_p$ since $\left(\frac{-1}{p}\right) = -1$

$\therefore$ $\mathrm{Im}(\alpha_{E'}) = 0$

$\therefore$ rank $E(\mathbb{Q}) = 0$.

5. $\mathrm{Im}(\alpha_E) \subset \mathbb{Q}(S,2)$ where $S = \{p \mid b\}$

$\mathrm{Im}(\alpha_{E'}) \subset \mathbb{Q}(S',2)$ where $S' = \{p \mid a^2 - 4b\}$

$$2^{\text{rank } E(\mathbb{Q})} = \frac{|\mathrm{Im}\,\alpha_E| \, |\mathrm{Im}\,\alpha_{E'}|}{4}$$

$$\Rightarrow \text{rank } E(\mathbb{Q}) = \dim_{\mathbb{F}_2}(\mathrm{Im}\,\alpha_E) + \dim_{\mathbb{F}_2}(\mathrm{Im}\,\alpha_{E'}) - 2$$
$$\leq \dim_{\mathbb{F}_2} \mathcal{Q}(S,2) + \dim_{\mathbb{F}_2} \mathcal{Q}(S',2) - 2$$
$$= v(b) + 1 + v(a^2-4b) + 1 - 2$$
$$= v(b) + v(a^2-4b)$$

To show the inequality is strict we prove

Lemma Exactly one of the maps

$$\frac{E(\mathbb{R})}{\hat{\phi}E'(\mathbb{R})} \xrightarrow{\beta} \mathbb{R}^*/(\mathbb{R}^*)^2 \qquad \frac{E'(\mathbb{R})}{\phi E(\mathbb{R})} \xrightarrow{\beta'} \mathbb{R}^*/(\mathbb{R}^*)^2$$

is non-trivial.

Proof ① β non-trivial $\iff$ $\omega^2 = -u^4 + a u^2 v^2 - b v^4$ sol. over $\mathbb{R}$
$\iff$ $X^2 + aX + b$ has a negative real root
$\iff$ either $b<0$ or $b, b'>0$ and $a>0$

Likewise β' non-trivial $\iff$ either $b'<0$ or $b,b'>0$ and $a<0$

Since $b' = a^2 - 4b$ we cannot have b, b' both negative.
Moreover if $b, b' > 0$ then $a \neq 0$
$\therefore$ the above conditions are mutually exclusive & cover all cases

Proof ②
$$\frac{|E(\mathbb{R})/2E(\mathbb{R})|}{|E(\mathbb{R})[2]|} = \frac{|\mathrm{Im}\,\beta|\,|\mathrm{Im}\,\beta'|}{4}$$

But $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$\Rightarrow$ LHS $= \frac{1}{2}$ $\Rightarrow$ $|\mathrm{Im}\,\beta| \cdot |\mathrm{Im}\,\beta'| = 2$
$\Rightarrow$ exactly one of β, β' is non trivial. $\square$

6.
$$\hat{h}(P) = 0 \iff \hat{h}(nP) = 0 \quad \forall n \in \mathbb{Z}$$
$$\Rightarrow \{nP : n \in \mathbb{Z}\} \text{ is finite}$$
$$\iff P \in E(\mathbb{Q})_{\text{tors}}$$

For the converse we note that if $\{nP : n \in \mathbb{Z}\}$ is finite then $\exists\, B > 0$ s.t. $h(nP) \leq B \quad \forall n \in \mathbb{Z}$

$$\Rightarrow \hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n} \leq \lim_{n\to\infty} \frac{B}{4^n} = 0$$

$$\Rightarrow \hat{h}(P) = 0.$$

7. (i) From the s.e.s. of $\mathrm{Gal}(\bar{K}/K)$-modules
$$0 \to E[\phi] \xrightarrow{\iota} E[\psi\phi] \xrightarrow{\phi} E'[\psi] \to 0$$
we obtain a long exact sequence, appearing as the first row of the following diagram

$$\begin{array}{ccccccc} E'(K)[\psi] & \longrightarrow & H^1(K, E[\phi]) & \xrightarrow{\iota_*} & H^1(K, E[\psi\phi]) & \xrightarrow{\phi_*} & H^1(K, E'[\psi]) \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ & & \prod_v H^1(K_v, E) & = & \prod_v H^1(K_v, E) & \longrightarrow & \prod_v H^1(K_v, E') \end{array}$$

By a diagram chase this gives an exact sequence
$$E'(K)[\psi] \longrightarrow \ker\alpha \longrightarrow \ker\beta \longrightarrow \ker\gamma$$
$$\| \qquad\qquad \| \qquad\qquad \|$$
$$S^{(\phi)}(E/K) \qquad S^{(\psi\phi)}(E/K) \qquad S^{(\psi)}(E'/K)$$

Indeed if $x \in \ker\beta$ with $\phi_*(x) = 0$ then $x = \iota_*(y)$ for some $y \in H^1(K, E[\phi])$. Then $\alpha(y) = \beta(x) = 0 \Rightarrow y \in \ker\alpha$.

(ii) Taking $\psi = \hat{\phi}$ & $n = \deg\phi$ we obtain an exact sequence
$$E'(K)[\hat{\phi}] \longrightarrow S^{(\phi)}(E/K) \longrightarrow \underbrace{S^{(n)}(E/K)}_{\text{proved finite in lectures.}} \longrightarrow S^{(\hat{\phi})}(E/K)$$
$E'[\hat{\phi}]$ finite.
$\therefore$ $S^{(\phi)}(E/K)$ is finite.

8.
$$E: \quad y^2 = x^3 + ax + b \qquad K = \mathbb{Q}(\sqrt{d})$$
$$E_d: \quad dy^2 = x^3 + ax + b \qquad \mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$$

Then $E(\mathbb{Q}) = \{P \in E(K) \mid \sigma P = P\}$
$\lambda : E_d(\mathbb{Q}) \xrightarrow{\sim} \{P \in E(K) \mid \sigma P = -P\}$
$(x,y) \longmapsto (x, y\sqrt{d})$

we define $\Phi : E(\mathbb{Q}) \times E_d(\mathbb{Q}) \to E(K)$
$(P, Q) \longmapsto P + \lambda(Q)$

$(P,Q) \in \ker(\Phi) \Rightarrow P + \lambda Q = 0$
$\Rightarrow P = \sigma(P) = -P$
$\Rightarrow P, Q \in E[2]$. $\therefore$ $\ker(\Phi)$ finite

If $P \in E(K)$ then $2P = (P + \sigma P) + (P - \sigma P) \in E(\mathbb{Q}) + \lambda E_d(\mathbb{Q})$
$\Rightarrow 2E(K) \subset \mathrm{Im}(\Phi) \subset E(K)$) by weak Mordell-Weil.
$\Rightarrow$ Φ has finite cokernel

Lemma If A, B are finitely generated abelian groups and $\phi: A \to B$ has finite kernel and cokernel then $\operatorname{rank} A = \operatorname{rank} B$

Proof (Method ①) $0 \to \ker \to A \longrightarrow B \to \operatorname{coker} \to 0$ exact

Applying $\otimes_{\mathbb{Z}} \mathbb{Q}$ gives $0 \to A \otimes_{\mathbb{Z}} \mathbb{Q} \to B \otimes_{\mathbb{Z}} \mathbb{Q} \to 0$

$\therefore \operatorname{rank}(A) = \dim_{\mathbb{Q}}(A \otimes_{\mathbb{Z}} \mathbb{Q}) = \dim_{\mathbb{Q}}(B \otimes_{\mathbb{Z}} \mathbb{Q}) = \operatorname{rank}(B)$.

(Method ②) $A \cong A_0 \times \mathbb{Z}^r \quad B \cong B_0 \times \mathbb{Z}^s \quad A_0, B_0$ finite

Let Φ be the composite $\mathbb{Z}^r \hookrightarrow A \xrightarrow{\phi} B \twoheadrightarrow B/B_0 \cong \mathbb{Z}^s$

It may be checked that Φ also has finite kernel & cokernel

$\Rightarrow$ $\Phi(e_1), \dots, \Phi(e_r) \in \mathbb{Q}^s$ are linearly indep & span

$\Rightarrow$ $r = s$ □

9 (i) $\operatorname{End}(E) \longrightarrow \mathbb{C}; \quad \phi \mapsto \dfrac{\phi^*\omega}{\omega}$

Ring homomorphism: $(\phi+\psi)^*\omega = \phi^*\omega + \psi^*\omega$ (proved in lectures)

If $\phi^*\omega = \lambda\omega$, $\psi^*\omega = \mu\omega$ $\lambda, \mu \in \mathbb{C}$

then $(\phi\psi)^*\omega = \psi^*(\lambda\omega) = \lambda(\psi^*\omega) = \lambda\mu\,\omega$

$\therefore \dfrac{(\phi\psi)^*\omega}{\omega} = \lambda\mu = \dfrac{\phi^*\omega}{\omega} \cdot \dfrac{\psi^*\omega}{\omega}$

Injective Let $\phi \in \operatorname{End}(E)$. $\phi \neq 0 \Rightarrow \phi$ separable $\Rightarrow \phi^*\omega \neq 0$ ($\operatorname{char}\mathbb{C} = 0$)

(ii) $\phi : (x,y) \longmapsto \left(\left(\frac{y}{x}\right)^2, y\left(\frac{x^2-b}{x^2}\right)\right)$

$\hat{\phi} : (x,y) \longmapsto \left(\frac{1}{4}\left(\frac{y}{x}\right)^2, \frac{1}{8}y\left(\frac{x^2-b'}{x^2}\right)\right)$

$$\phi^*\left(\frac{dx}{y}\right) = \frac{d\left(\frac{x^2+ax+b}{x}\right)}{y\left(1-b/x^2\right)} = \frac{\left(1-b/x^2\right)dx}{y\left(1-b/x^2\right)} = \frac{dx}{y}$$

$$\hat{\phi}^*\left(\frac{dx}{y}\right) = \dots = \dots = 2\frac{dx}{y}$$

$$\therefore (\hat{\phi}\phi)^*\frac{dx}{y} = 2\frac{dx}{y} = [2]^*\frac{dx}{y}$$

Then (i) $\Rightarrow \hat{\phi}\phi = [2] \Rightarrow \phi, \hat{\phi}$ are dual isogenies

10 **Lemma 1** If $\mathfrak{p} \nmid n$ then $E_0(K_{\mathfrak{p}}^{nr}) \xrightarrow{\times n} E_0(K_{\mathfrak{p}}^{nr})$ is surjective.

Proof We consider the commutative diagram (& then apply the Snake lemma)

$$\begin{array}{ccccccc}
0 & \to & E_1(K_{\mathfrak{p}}^{nr}) & \to & E_0(K_{\mathfrak{p}}^{nr}) & \to & \tilde{E}_{ns}(\bar{k}_{\mathfrak{p}}) \to 0 \\
 & & \downarrow \times n & & \downarrow \times n & & \downarrow \times n \\
0 & \to & E_1(K_{\mathfrak{p}}^{nr}) & \to & E_0(K_{\mathfrak{p}}^{nr}) & \to & \tilde{E}_{ns}(\bar{k}_{\mathfrak{p}}) \to 0
\end{array}$$

surjective by theory of formal groups

surjective, even in cases of bad reduction

N.B. Over an algebraically closed field F with $\operatorname{char}(F) \nmid n$ the maps $F^\times \to F^\times$, $x \mapsto x^n$ and $F \to F$, $x \mapsto nx$ are surjective □

Lemma 2 If $\mathfrak{p} \notin S$ then $E(K_{\mathfrak{p}}) \subset n E(K_{\mathfrak{p}}^{nr})$

Proof Let $m = c_{\mathfrak{p}}(E)$, so $m = [E(K_{\mathfrak{p}}) : E_0(K_{\mathfrak{p}})]$

Let $P \in E(K_{\mathfrak{p}})$

Then $mP \in E_0(K_{\mathfrak{p}}) \subset n E_0(K_{\mathfrak{p}}^{nr})$ by Lemma 1

$\Rightarrow$ $mP, nP \in nE(K_{\mathfrak{p}}^{nr})$

$\Rightarrow$ $P \in nE(K_{\mathfrak{p}}^{nr})$ since m, n coprime □

For $\mathfrak{p} \notin S$ we consider the commutative diagram

$$\begin{array}{ccccc}
E(K_{\mathfrak{p}}) & \xrightarrow{\times n} & E(K_{\mathfrak{p}}) & \xrightarrow{\delta_{\mathfrak{p}}} & H^1(K_{\mathfrak{p}}, E[n]) \\
\downarrow & & \downarrow & & \downarrow \text{res} \\
E(K_{\mathfrak{p}}^{nr}) & \xrightarrow{\times n} & E(K_{\mathfrak{p}}^{nr}) & \longrightarrow & H^1(K_{\mathfrak{p}}^{nr}, E[n])
\end{array}$$

Let $\xi \in S^{(n)}(E/K) \subset H^1(K, E[n])$

By definition of the Selmer group, $\operatorname{res}_{\mathfrak{p}}(\xi) \in \operatorname{Im}(\delta_{\mathfrak{p}})$

By Lemma 2 and a diagram chase it follows that the restriction of ξ to $H^1(K_{\mathfrak{p}}^{nr}, E[n])$ is trivial.