Elliptic Curves
Example Class 4.

20/01/2020

Q1. Rather long, but relatively elementary.

1. (ii) Make sure pin down the signs, to only get 2 points and not 4. (don't use $\pm t$ instead of t).

(v) $\alpha : E'(K) \longrightarrow K^*/(K^*)^2$

Want to show: $P_1 + P_2 + P_3 = O \Longrightarrow \alpha(P_1)\alpha(P_2)\alpha(P_3) \in (K^*)^2$.

Previous part of question proved this in nearly all cases, but some special cases to check.

$$(x,y) \longmapsto \begin{cases} x \mod (K^*)^2 & \text{if } x \neq 0 \\ b \mod (K^*)^2 & \text{if } x = 0. \end{cases}$$

So done if $P_1, P_2, P_3 \notin \{O_E, (0,0)\}$.

Interesting case if wlog P_1 O_E or $(0,0)$ but then other two points general. ...

Q2: $E_D : y^2 = x^3 - D^2 x$

D a congruent number $\iff$ rank $E_D(\mathbb{Q}) \geq 1$.

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

$\alpha_E : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$

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

Now: $\alpha_E(0,0) = (-1)(\mathbb{Q}^*)^2$.

↖ or can just do another quartic..

$b_1 = 2$: $w^2 = 2u^4 - 2v^4$

Sol^n: $(u, v, w) = (1, 1, 0)$.

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

$\longrightarrow$

$E' : y^2 = x^3 + 16x$

NB! Can simplify this: (only can clear $a_4 = 16$ upto 4th powers).

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

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

$b_1 = -1$: $w^2 = -u^4 - v^4$, got $\not\exists$ over $\mathbb{R}$.

$\therefore |\mathrm{Im}(\alpha_{E'})| = 1$.

Now use: $2^{\text{rank } E(\mathbb{Q})} = \dfrac{|\mathrm{Im}\,\alpha_E| \, |\mathrm{Im}\,\alpha_{E'}|}{4} = \dfrac{4 \cdot 1}{4}$

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

Note, only have to do case for E', then just need $\mathrm{Im}(\lambda_E) \subset \langle -1, 2 \rangle$, ~~not~~ equality not required, as rank $E(\mathbb{Q}) \geq 0$.

Q3 (i) $E: y^2 = x(x^2 + 6x - 2)$

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

$b_1 = -1$, $w^2 = -u^4 + 6u^2v^2 + 2v^4$ (*)

If (u, v, w) a solution over $\mathbb{Q}$, may assume $u, v \in \mathbb{Z}$ coprime ($\Rightarrow w \in \mathbb{Z}$).

Case u even: $\Rightarrow w$ even

$\Rightarrow v$ even ✗.

Case u odd:

$w^2 \equiv -1 + 2v^2 + 2v^4 \pmod 4$

$\equiv -1 \pmod 4$ ✗.

$\therefore$ Equation (*) is not soluble.

$\therefore \mathrm{Im}(\lambda_E) = \langle -2 \rangle$ (note $\lambda_E(0,0) = -2$)

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

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

Note, if $b_1 < 0$: insoluble over $\mathbb{R}$.

and $\lambda_{E'}(0,0) = 44$ which is 11 mod squares

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

$2w^2 = u^4 - 6u^2v^2 + 11v^4$

We may assume $u, v \in \mathbb{Z}$ coprime

If u even, v odd ⊗ (only $11v^4$ odd)

If u odd, v even, ⊗ (only u^4 odd)

Then u & v are both odd, so $u^2 \equiv v^2 \equiv 1 \pmod 8$

$\Rightarrow 2w^2 \equiv 1 - 6 + 11 \pmod 8$

$\Rightarrow w^2 \equiv 3 \pmod 4$. ⊗.

$\therefore \mathrm{Im}(\partial_{E'}) = \langle 11 \rangle \subset \mathcal{O}^\times / (\mathcal{O}^\times)^2$

So rank is 0

	rank
3 (i)	0
(ii)	1
(iii)	2
(iv).	3

By realistic questions, showing solutions usually won't be more than 5 in absolute value... usually will be just $-1, 0, 1$..

Q's: $\beta: E(\mathbb{R}) \longrightarrow \mathbb{R}^*/(\mathbb{R}^*)^2$

$\beta': E'(\mathbb{R}) \longrightarrow \mathbb{R}^*/(\mathbb{R}^*)^2$

Claim: Exactly one of these maps is non-trivial! $\longrightarrow$

This proves the inequality strict.

Recall: $$2^{\operatorname{rank} E(\mathbb{Q})} = \frac{|E(\mathbb{Q})/2E(\mathbb{Q})|}{|E(\mathbb{Q})[2]|} = \frac{|\operatorname{Im}\delta| \cdot |\operatorname{Im}\delta'|}{4}.$$

Similarly, can prove: $$\frac{|E(\mathbb{R})/2E(\mathbb{R})|}{|E(\mathbb{R})[2]|} = \frac{|\operatorname{Im}\beta| \cdot |\operatorname{Im}\beta'|}{4}$$

Recall: $$E(\mathbb{R}) = \begin{cases} \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } \Delta > 0 \\ \mathbb{R}/\mathbb{Z} & \text{if } \Delta < 0 \end{cases}.$$

So if $E(\mathbb{R}) = \mathbb{R}/\mathbb{Z}$, then $2E(\mathbb{R}) = \mathbb{R}/\mathbb{Z}$.

Also result: If replace group with one of finite index, then doesn't change. So $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ works as well.

Q. 7.

$$0 \longrightarrow E[\phi] \longrightarrow E[\gamma\phi] \xrightarrow{\phi} E'[\gamma] \longrightarrow 0.$$

$$E'(K)[\gamma] \longrightarrow H^1(K, E[\phi]) \longrightarrow H^1(K, E[\gamma\phi]) \longrightarrow H^1(K, E'[\gamma])$$

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

Claim: There is an exact seq.

$$E'(K)[\gamma] \longrightarrow \ker\alpha \longrightarrow \ker\beta \longrightarrow \ker\gamma$$

- First row is exact
- Diagram commutes. (can verify as exercise).

Standard to check $E'(K)[\gamma] \longrightarrow \{\} \subseteq \ker\alpha$ (just use commutativity of diagram).

Similarly can prove $\mathrm{Im}(\ker(\alpha)) \subseteq \ker(\beta)$.

Q8: $K = \mathbb{Q}(\sqrt{d})$. $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$.

$E: y^2 = x^3 + ax + b$

$E_d: dy^2 = x^3 + ax + b$.

$E(\mathbb{Q}) = \{P \in E(K) \mid \sigma(P) = P\}$

$\lambda: E_d(\mathbb{Q}) \xrightarrow{\sim} \{P \in E(K) \mid \sigma(P) = -P\}$ — isomorphism of groups.

$(x, y) \longmapsto (x, \sqrt{d}\, y)$

$\Phi: E(\mathbb{Q}) \times E_d(\mathbb{Q}) \longrightarrow E(K)$

$(P, Q) \longmapsto P + \lambda(Q)$.

Note: If $(P, Q) \in \ker(\Phi)$, then

$P + \lambda(Q) = O \implies P \in \mathrm{Im}(\lambda)$

$\Rightarrow \sigma(P) = P = -P$

$\Rightarrow P \in E[2]$.

Claim: $2E(K) \subset \mathrm{Im}(\Phi) \subset E(K)$

Given the claim: $\dfrac{E(K)}{2E(K)} \twoheadrightarrow \dfrac{E(K)}{\mathrm{Im}(\Phi)}$

this is finite by weak Mordell-Weil.

Thus, claim proves coclaimed is finite.

Proof of claim: Let $P \in E(K)$.

Now: $2P = \underbrace{(P + \sigma(P))}_{\in E(\mathbb{Q})} + \underbrace{(P - \sigma(P))}_{\in \mathrm{Im}(\lambda)} \in \mathrm{Im}(\Phi)$

Thus, as map has finite kernel and finite cokernel, the ranks are the same.

Q10:

$$S = \{ \mathfrak{p} \text{ s.t. } \gcd(c_{\mathfrak{p}}(E), n) \neq 1 \} \cup \{ v \mid n\infty \}$$

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.

Use the snake lemma:

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

surjective by theory of formal groups.

this is surjective, even if $E/K_{\mathfrak{p}}$ has bad reduction.

(Note, the theory of formal groups that we did assumed that our field is complete.)

$$\begin{array}{ccc} \bar{K}_{\mathfrak{p}}^{*} & \longrightarrow & \bar{K}_{\mathfrak{p}}^{*} \\ x & \longmapsto & x^n \end{array} \quad \checkmark$$

$$\begin{array}{ccc} \bar{K}_{\mathfrak{p}} & \longrightarrow & \bar{K}_{\mathfrak{p}} \\ x & \longmapsto & nx \end{array} \quad \checkmark \text{ surjective (since } \mathfrak{p} \nmid n)$$

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

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

Let $P \in E(K_{\mathfrak{p}})$. Then $mP \in E_0(K_{\mathfrak{p}}) \subset nE_0(K_{\mathfrak{p}}^{nr})$ by Lemma 1.

$\Rightarrow mP, nP \in nE(K_{\mathfrak{p}}^{nr})$ } since m, n coprime.

$\Rightarrow P \in nE(K_{\mathfrak{p}}^{nr})$ }

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

If $\xi \in S^{(n)}(E/K) \subset H^1(K, E[n])$ then $\text{res}_{\mathfrak{p}}(\xi) \in \text{Im}(\delta_{\mathfrak{p}})$.

Diagram chase + Lemma 2.

$\Rightarrow$ ξ restricted $H^1(K_{\mathfrak{p}}^{nr}, E[n])$ is trivial.

So if only computer program, can throw away many primes which we thought were bad, don't have to worry about them.