32.1 Do 31.2/3 first.

What cohomology gives us is the Kummer sequence for E/k (can think of $k = \mathbb{Q}$)

$$0 \longrightarrow \frac{E(k)}{mE(k)} \xrightarrow{\delta} H^1(G_{\bar{K}/k}, E[m]) \longrightarrow H^1(G_{\bar{K}/k}, E(\bar{K}))[m] \longrightarrow 0$$

What is the map δ?

Let $P \in E(k)$, choose some $Q \in E(\bar{K})$ with $mQ = P$.

Then we have

$$\delta(P) : G_{\bar{K}/k} \longrightarrow E[m]$$
$$\sigma \longrightarrow Q^\sigma - Q.$$

We get something in $E[m]$ because

$$m(Q^\sigma - Q) = m(Q^\sigma) - m(Q) = (mQ)^\sigma - mQ$$
$$= P^\sigma - P = P - P = 0.$$

Is it well defined?

If $mQ' = P$ also, get $\sigma \longrightarrow Q'^\sigma - Q'$.

We can write $Q' = Q + Q''$ with $Q'' \in E(\bar{K})[m]$,

$$\sigma \longrightarrow (Q^\sigma - Q) + (Q''^\sigma - Q'').$$

If $E[m] \subseteq E(K)$, this is the same map.

If not, since $Q'' \in E[m]$, $\sigma \longrightarrow Q''^\sigma - Q''$ is a coboundary, trivial in $H^1(G_{\bar{K}/k}, E[m])$ by def.

32.2

Lemma (Sil 8.1) Let L/K be finite Galois.

If $E(L)/mE(L)$ is finite, $E(K)/mE(K)$ is.

Proof omitted but see 8.1 or "inflation-restriction".

Assume $E[m] \subseteq E(K)$. (To prove $E(K)/mE(K)$ finite.)

The lemma justifies this. But the special case is interesting enough.

In this case we get a map which is well-defined

$$\begin{aligned} \delta(P) : G_{\bar{K}/K} &\longrightarrow E[m] \\ \sigma &\longrightarrow Q^{\sigma} - Q \end{aligned}$$

and indeed it is a group homomorphism because

$$\begin{aligned} \sigma\sigma' \longrightarrow Q^{\sigma\sigma'} - Q &= (Q^{\sigma\sigma'} - Q^{\sigma'}) + (Q^{\sigma'} - Q) \\ &= (Q^{\sigma} - Q)^{\sigma'} + (Q^{\sigma'} - Q) \\ &= (Q^{\sigma} - Q) + (Q^{\sigma'} - Q) \end{aligned}$$

because $Q^{\sigma} - Q \in E[m]$.

Define the Kummer pairing

$$\begin{aligned} \kappa : E(K) \times G_{\bar{K}/K} &\longrightarrow E[m] \\ (P \;,\; \sigma) &\longrightarrow Q^{\sigma} - Q \end{aligned}$$

with $mQ = P$.

Then:

(1) It is well-defined (shown already)

(2) It is bilinear (shown on right above)

(on left "obvious" according to Joe

says $(Q+Q')^{\sigma} = Q^{\sigma} + Q'^{\sigma}$.

32.3

(3) The kernel on the left is $mE(K)$.

note: This means $\{P \in E(K) : (P,\sigma) = 0$ for all $\sigma \in G_{\bar{K}/K}\}$.

Proof. If $Q^\sigma - \overset{=0}{Q}$ for all $\sigma \in Gal(\bar{K}/K)$ then $Q \in K$.

Conversely, if $P \in mE(K)$ then $Q \in E(K)$ (used $E[m] \subseteq E(K)$!) so $Q^\sigma - Q = 0$ for all $\sigma \in Gal(\bar{K}/K)$.

(4) The kernel of the Kummer pairing on the right is $G_{\bar{K}/L}$, where $L = K([m]^{-1}E(K))$

compositum of all fields $K(Q)$ with $mQ \in E(K)$.

Proof. Given σ fixing L, σ fixes any possible Q by construction so σ is in the kernel.

Conversely, if σ is in the kernel, then $(P,\sigma) = 0$ for all $P \in E(K)$ hence $Q^\sigma - Q = 0$ for all ~~$\sigma \in Gal$~~ Q with $mQ \in E(K)$, so σ fixes all ~~coords~~ coordinates of all such points, and K, hence L.

Thus, we get a perfect bilinear pairing

$$E(K)/mE(K) \times Gal(L/K) \longrightarrow E[m].$$

(Note: L is Galois because $[m]^{-1}E(K)$ is closed under the action of $Gal_{\bar{K}/K}$.)

32.4

Claim. L is finite degree over K.

(and hence $E(K)/mE(K)$ is finite)

Summary of proof.

(1) The only primes where L/K ~~are~~ is possibly ramified are:

* those for which E has bad reduction;
* those dividing m;
* the infinite primes.

Proof. Let v be any other such prime, $Q \in E(\bar{K})$ with $mQ \in E(K)$, $K' = K(Q)$.

Argue K'/K is unr at v. (Compositum of UR exts. is UR.)

Let:
$$\begin{tikzcd} K' \arrow[d, dash] & v' \arrow[d, dash] & k'_{v'} \arrow[d, dash] \\ K & v & k_v \end{tikzcd}$$

E has good reduction at v hence at v' also (use same equ.)

The reduction map $E(K') \longrightarrow \tilde{E}(k'_{v'})$ injective under above conditions.

Let $I_{v'/v} \leq \mathrm{Gal}_{K'/K}$ be the inertia group for v'/v

(Here the decomposition group is $G_{v'} = \{\sigma \in \mathrm{Gal} : \sigma v' = v'\}$

the inertia group is $I_v' \leq G_{v'}$

$= \{\sigma \in G_{v'} : \sigma x \equiv x \pmod{\mathfrak{m}_{v'}}\}$

$= \{\sigma \in G_{v'} : \text{acts trivially on } k'_{v'}\}$

Then any $\sigma \in I_{v'/v}$ acts trivially on $\tilde{E}_{v'}(k'_{v'})$ so

$$\widetilde{Q^\sigma - Q} = \tilde{Q}^\sigma - \tilde{Q} = \tilde{O}$$

$$m(Q^\sigma - Q) = (mQ)^\sigma - (mQ) = 0$$

Consequently $Q^\sigma - Q$ is $\begin{cases} \text{of order } m \\ \text{in the kernel of reduction at } v \end{cases}$

hence trivial, so $Q^\sigma = Q$.

So Q is fixed by $I_{v'/v}$, so K' is unramified at v' over K.

Same is true for all v'/v, so K'/K unramified outside S

(2) Given any NF K, finite set of primes S, only finitely many NFs of bounded degree which are unramified outside S.

33.1. (Following Washington, EC: NT and Crypto)

Example. Let $E: y^2 = x(x-2)(x+2)$.

What is $E(\mathbb{Q})$?

Obviously $E[2] = \{\infty, (0,0), (\pm 2, 0)\} \subseteq E(\mathbb{Q})$.

Write
$$x = au^2$$
$$x - 2 = bv^2$$
$$x + 2 = cw^2$$
with a, b, c squarefree integers

$u, v, w \in \mathbb{Q}$

abc is a square.

Claim. $a, b, c \in \{\pm 1, \pm 2\}$ (if $y \neq 0$).

Proof. If p is an odd prime dividing a, $v_p(x)$ is odd.

if $v_p(x) < 0$ then $v_p(x-2) = v_p(x+2) = v_p(x)$

So $v_p(y^2) = 3 v_p(x)$ impossible.

If $v_p(x) > 0$ then $v_p(x-2) = v_p(x+2) = 0$

$v_p(y^2) = v_p(x)$ agein impossible.

This is "descent", look for smaller u, v, w.

Find $(u, v, w) \in V(\mathbb{Q})$, where

$$V = V\left(au^2 - bv^2 - 2,\ au^2 - cw^2 + 2\right).$$

This is a curve in $\mathbb{A}^3$, in fact it's isomorphic to E (over $\overline{\mathbb{Q}}$)

for each $a, b, c \in \{\pm 1, \pm 2\}$.

There are 16 possibilities, since a, b determine c.

Proposition. a and b have the same sign.

Proof. If $au^2 = bv^2 + 2$, $a < 0$, then $b < 0$ also.

If $a > 0$ then $c > 0$, but $abc > 0 \Rightarrow b > 0$.

So down to 8!

33.2

Proposition. $(a, b, c) = (1, 2, 2)$ is impossible.

Proof Want to solve

$$u^2 - 2v^2 = 2, \quad u^2 - 2w^2 = -2$$

We cannot have $\underbrace{v_2(v)}_{\text{Different } v\text{'s!}} < 0$, because then $v_2(-2v^2)$ would be odd, negative.

Similarly with $v_2(w)$.

Now $v_2(2 + 2v^2) \geq 1 \Rightarrow v_2(u) \geq 1 \Rightarrow v_2(v) = 0$

Similarly $v_2(w) = 0$

So $v^2 \equiv w^2 \equiv 1 \pmod 8$, and mod 8,

$$2 \equiv u^2 - 2v^2 \equiv u^2 - 2 \equiv u^2 - 2w^2 \equiv -2 \pmod 8. \quad X$$

Exercise. Rule out $(-1, -1, 1)$, $(2, 1, 2)$, $(-2, 2, 1)$ similarly.

Proposition. Given $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$

e_1, e_2, e_3 integers

$$x - e_1 = au^2, \quad x - e_2 = bv^2, \quad x - e_3 = cw^2$$

If p is a prime dividing any of a, b, c, then

$$p \mid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3).$$

Same proof.

Theorem. E as above. The map

$$\begin{aligned} \phi : E(\mathbb{Q}) &\longrightarrow (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \times (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \times (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \\ (x,y) &\longrightarrow (x-e_1, \ x-e_2, \ x-e_3) \qquad (y \neq 0) \\ \infty &\longrightarrow (1, \ 1, \ 1) \\ (e_1, 0) &\longrightarrow ((e_1-e_2)(e_1-e_3), \ e_1-e_2, \ e_1-e_3) \\ (e_2, 0) &\longrightarrow (e_2-e_1, \ (e_2-e_1)(e_2-e_3), \ e_2-e_3) \\ (e_3, 0) &\longrightarrow (e_3-e_1, \ e_3-e_2, \ (e_3-e_1)(e_3-e_2)) \end{aligned}$$

is a homomorphism with kernel $2E(\mathbb{Q})$.

Same as before (almost).

In our example,

$$\begin{aligned} \infty &\to (1,1,1) \\ (0,0) &\to (-1,-2,2) \\ (2,0) &\to (2,2,1) \\ (-2,0) &\to (-2,-1,2) \end{aligned}$$

Other points $\to (a,b,c)$ as above.

Exercise. Prove that for $E : y^2 = x^3 - 4x$,

$\mathrm{Im}(\phi)$ is the above subgroup.

To rule out others, use: $abc = 1$ (mod squares)

(smth in group)$\cdot$(smth not in group) is not in the group

Diophantine conditions.

Cor. Weak Mordell-weil (and hence Strong MW) is true for any EC as above.

Proof. $E(\mathbb{Q})/2E(\mathbb{Q})$ injects into a finite set.

What if E doesn't factor over $\mathbb{Q}$?

Replace $\mathbb{Q}$ with the splitting field K of $f(x)$

Prove $E(K)/2E(K)$ is finite.

Same proof works, factorization in $\mathbb{Z} \rightarrow$ in $\mathcal{O}_K$.

To make everything works, work in $M^{-1}\mathcal{O}_K$ where M is chosen to make it a PID and UFD.

$\operatorname{Im}(\phi)$ contained in groups generated by $\left\{ \begin{array}{l} S \\ \text{units of } M^{-1}\mathcal{O}_K. \end{array} \right.$

Get a finitely gen. abelian group of exponent 2.

Prop. For ~~E(Q~~ $E: y^2 = x^3 - 4x$, $E(\mathbb{Q}) = E[2]$.

Proof. Check first E has no other torsion (use Lutz-Nagell)

If $E(\mathbb{Q}) = E[2] \oplus \mathbb{Z}^r$ with $r \geq 1$,

would get $E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2)^{r+2}$.

(Exercise. Prove if $E: y^2 = x^3 - 25x$, $E(\mathbb{Q}) \cong (\mathbb{Z}/2)^2 \oplus \mathbb{Z}$.)

33.5 (= 34.1)

<u>Definition</u>. The 2-Selmer group $\mathrm{Sel}^2(E)$ is the set of (a,b,c) such that the curve

$$C_{a,b,c}: \; au^2 - bv^2 = e_2 - e_1, \quad au^2 - cw^2 = e_3 - e_1$$

has a <u>real point</u> and a p-adic point for all p.

(i.e. a point in $\mathbb{Q}_p$ for all "$p \leq \infty$")

Our descent map gave an injection

$$E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\phi} \mathrm{Sel}^2(E)$$

and

$$\text{Ш}[2] := \mathrm{Sel}^2(E)/\mathrm{Im}\,\phi .$$

<u>Proposition</u>. Let $E/\mathbb{Q}$ be

$$E: y^2 = x(x-2p)(x+2p)$$

with $p \equiv 9 \pmod{16}$ an odd prime.

Then

$$C_{1,p,p}: \; u^2 - pv^2 = 2p, \quad u^2 - pw^2 = -2p$$

has a p-adic point for all $p \leq \infty$ but no rational points.

[Do also stuff on bottom of 33.4]

<u>To be explained</u>: <u>why</u> our map $E(\mathbb{Q}) \xrightarrow{\alpha} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ was a Selmer group computation.

34.2.

Claim. Let $E: y^2 = x^3 - 25x$.

Then $E(\mathbb{Q}) \cong (\mathbb{Z}/2)^2 \times \mathbb{Z}$.

Proof. (Sketch)

Note that $E(\mathbb{Q}) \supseteq E[2] = \{\infty, (0,0), (\pm 5, 0)\}$

Lutz - Nagell says $E(\mathbb{Q})_{tors} = E[2]$.

We also have $(-4, 6) \in E(\mathbb{Q})$.

This point must have infinite order.

Had a map

$$E(\mathbb{Q}) \to (\mathbb{Q}^\times / \mathbb{Q}^{\times 2})^2$$

$(x, y) \to (x, x-5, x+5)$ when $y \neq 0$, $P \neq \infty$.

$$(-4, 6) \to (-1, -1, 1)$$
$$\infty \to (1, 1, 1)$$
$$(0,0) \to (-1, -5, 5)$$
$$(5,0) \to (5, 2, 10)$$
$$(-5,0) \to (-5, -10, 2)$$

Write $x = au^2$, $x - 5 = bv^2$, $x + 5 = cw^2$ | ⊛

So $a, b, c \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$ 64 possibilities.

Get $5 \Rightarrow 8$ since image is a subgroup.

⊛ defines the Selmer group.

More properly, the set of curves $C_{a,b,c}$ with p-adic points, $\forall p$ are the Selmer group.

Has at least 8 elements.

34.3

Now verify:

If a, b have ~~the~~ opposite signs, no points in $\mathbb{R}$.

$(a,b) = (2,1) \Rightarrow$ no points in $\mathbb{Q}_2$.

$(a,b) = (5,1)$ or $(10,1) \Rightarrow$ no points in $\mathbb{Q}_5$.

Check: This rules out all but our 8 possibilities! (Use: image is a group).

So $E(\mathbb{Q}) / 2E(\mathbb{Q}) \cong (\mathbb{Z}/2)^3$

because it injects into it and the image is full.

So $E(\mathbb{Q}) \cong (\mathbb{Z}/2)^2 \times \mathbb{Z}$.

Crash course in p-adic numbers.

Given a set of equations $f_1, \dots, f_r$ defined over $\mathbb{Z}$ in $x_1, \dots, x_n$.

They have a p-adic solution if:

For each integer $i \geq 1$, there are integers $x_{1,i} \dots x_{n,i}$ with $f_j(x_{1,i}, \dots, x_{n,i}) \equiv 0 \pmod{p^i}$ for all j

and $x_{k,i} \equiv x_{k,i-1} \pmod{p^{i-1}}$ for all $i \geq 2$.

Example. Which $\mathbb{Q}_p$ have a square root of -1?

Solve $x^2 + 1 \equiv 0$ ~~(mod p^i)~~ in $\mathbb{Z}_p$

Need $x_i^2 + 1 \equiv 0 \pmod{p^i}$ and $x_i \equiv x_{i-1} \pmod{p^{i-1}}$.

Can do this via Hensel lifting.

34.4.

~~Basice~~ If $p = 2$, there is no solution (mod 4).

If $p \equiv 3 \pmod 4$ there is no solution (mod p).

(i.e. $\left(\frac{-1}{p}\right) = -1$)

If $p \equiv 1 \pmod 4$ then there is a solution $x_1 \pmod p$.

Claim. Given a solution $x_i \pmod{p^i}$ we can always get a solution $\pmod{p^{i+1}}$.

Proof. Write $x_{i+1} = x_i + ap^i$ for an indeterminate a.

$$(x_i + ap^i)^2 + 1 \equiv 0 \pmod{p^{i+1}}$$

$$x_i^2 + 2ax_ip^i + a^2p^{2i} + 1 \equiv 0 \pmod{p^{i+1}}$$

$$(x_i^2 + 1) + 2ax_ip^i \equiv 0 \pmod{p^{i+1}}.$$

writing $x_i^2 + 1 \equiv bp^i \pmod{p^{i+1}}$ for some $b \in \mathbb{Z}/p$,

solve
$$b + 2ax_i \equiv 0 \pmod p$$

Choose $a \equiv \frac{-b}{2x_i} \pmod p$. Can do because $p \nmid 2x_i$.

Hensel's Lemma. Given a polynomial $f(x) \in \mathbb{Z}_p[x]$. (or $\mathbb{Z}[x]$)

Given any r with $f(r) \equiv 0$ and $f'(r) \not\equiv 0 \pmod p$.

Then there is $\tilde{r}$ ~~wt~~ $\in \mathbb{Z}_p$ with $f(r) = 0$ in $\mathbb{Z}_p$.

(Note: $x^2 + 1 = 0$ has a solution in $\mathbb{Z}/2$ but not $\mathbb{Z}/4$: $x^2 + 1 = (x+1)^2$ in $\mathbb{F}_2$, shows need for hypothesis.)

34.5. = (35.1) (See Sil X.2)

Definition. Let C be a curve over $\mathbb{Q}$
E an elliptic curve (over $\mathbb{Q}$)

Then C ~~[illegible]~~ is a twist of E if it is isomorphic to E over $\overline{\mathbb{Q}}$.

Example. Let $E : y^2 = x^3 + ax^2 + bx$
$C : Dy^2 = x^3 + ax^2 + bx$.

Then if D is not a square, C is a twist of E.

Namely, $E \xrightarrow{\sim} C$
$(x,y) \to$ ~~$(\sqrt{D}x, y)$~~ $(x, \frac{y}{\sqrt{D}})$

This isomorphism is defined over $\mathbb{Q}(\sqrt{D})$ and not $\mathbb{Q}$.

In fact E is not isomorphic to C over $\mathbb{Q}$
(although this is not obvious).

Definition. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, ~~[illegible]~~ and given a twist $\phi : C \to E$.

The associated isomorphism of E
(which is an isomorphism of curves over $\overline{\mathbb{Q}}$)
(but not necessarily of elliptic curves, even over $\overline{\mathbb{Q}}$) is

$$\xi_\sigma := \phi^\sigma \phi^{-1}$$

Defined s.t. $\phi^\sigma(P^\sigma) = (\phi(P))^\sigma$.

34.6. (=35.2)

Example. As above, $C \xrightarrow{\phi} E$
$$(x,y) \to (x, y\sqrt{D}).$$

Then
$$\phi^{-1} : E \longrightarrow C$$
$$(x,y) \longrightarrow \left(x, \frac{y}{\sqrt{D}}\right)$$

$$\phi^{\sigma} : C \longrightarrow E$$
$$(x,y) \to \begin{cases} (x, y\sqrt{D}) & \text{if } \sigma(\sqrt{D}) = \sqrt{D} \\ (x, -y\sqrt{D}) & \text{if } \sigma(\sqrt{D}) = -\sqrt{D} \end{cases}$$

So $\phi^{\sigma}\phi^{-1}$ is the map
$$(x,y) \longrightarrow \begin{cases} (x,y) & \text{if } \sigma(\sqrt{D}) = \sqrt{D} \\ (x,-y) & \text{if } \sigma(\sqrt{D}) = -\sqrt{D}. \end{cases}$$

(Note that in this case it *is* an isomorphism of EC's).

Since $\left\{\begin{array}{l}\text{elts. of Galois group} \\ \text{twists } C \xrightarrow{\phi} E\end{array}\right\}$ give isomorphisms of E,

regard this as a map
$$(\text{Twists}) \longrightarrow \left(\begin{array}{c}\text{Maps from} \\ \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\end{array} \text{ to } \text{Isom}(E)\right).$$

Proposition.$^{(1)}$ We have, for $\sigma, \tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$,
$$\xi_{\sigma\tau} = (\xi_{\sigma})^{\tau}\,\xi_{\tau},$$ i.e. we get a map

$$\text{Twists} \longrightarrow H^1(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \text{Isom}(E)).$$

35.3

(2) The cohomology class $\{\xi\}$ in $H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), \mathrm{Isom}(E))$ is determined by the $\mathbb{Q}$-isomorphism class of C.

i.e. if $\phi' : C' \to E$ is a twist

and C' and C are isomorphic over $\mathbb{Q}$ then

$\phi^\sigma \phi^{-1}$ and $(\phi')^\sigma (\phi')^{-1}$ ~~differ by a coboundary~~ are cohomologous.

(3) The map given above is a bijection.

Proof.

(1) $\xi_{\sigma\tau} = (\phi^{\sigma\tau})\phi^{-1} = (\phi^\sigma \phi^{-1})^\tau (\phi^\tau \phi^{-1})$

$= (\xi_\sigma)^\tau (\xi_\tau)$.

(2) Given

$$\begin{tikzcd}
C \arrow[r, "\phi"] & E \\
C' \arrow[u, "\theta"] \arrow[ur, "\phi'"'] &
\end{tikzcd}$$

iso. over k,

then $\alpha := \phi\,\theta(\phi')^{-1} \in \mathrm{Isom}(E)$, and for $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$,

$$\begin{aligned}
\alpha^\sigma(\phi'^\sigma \phi'^{-1}) &= (\phi\,\theta\,\phi'^{-1})^\sigma \phi'^\sigma \phi'^{-1} \\
&= \phi^\sigma \theta((\phi')^{-1})^\sigma \phi'^\sigma \phi'^{-1} \\
&= \phi^\sigma \theta\, \phi'^{-1} \\
&= \phi^\sigma \phi^{-1} (\phi\,\theta\,\phi'^{-1}) = (\phi^\sigma \phi^{-1})\alpha.
\end{aligned}$$

So cohomologous.

(3) Injectivity is more formal nonsense

Surjectivity, you need to do actual work.

Where do you get twists from?

And where might we get isomorphisms of E from?

(E as a curve, don't need to preserve the origin)

Example. Let E be an EC, $P_0 \in E(\mathbb{Q})$.

Then
$$\begin{array}{ccc} E & \longrightarrow & E \\ P & \longrightarrow & P + P_0 \end{array}$$
is an isomorphism of curves.

Example. $E : y^2 = x^3 + ax^2 + bx$, $P_0 = (0,0)$.

The map
$$\begin{array}{ccc} E & \longrightarrow & E \\ P & \longrightarrow & P + (0,0) \end{array}$$
is
$$(x,y) \longrightarrow \left(\frac{b}{x}, \frac{-by}{x^2} \right).$$

This is visibly a rational map

(and hence it extends to a morphism)

and invertible by the group law on E.

For the examples we'll care about, write (for some $\phi : C \to E$)

$$\phi^{\sigma} \phi^{-1} (P) = P + P_0 \quad \text{for some} \quad P_0 \in E(\overline{\mathbb{Q}}).$$

will be interesting when $P_0 \notin E(\mathbb{Q})$.

36.1. (References: Sil X.3; J. Baez, "Torsors Made Easy" (Google it))

Torsors. A set X with an ~~group~~ action of a group G is a G-torsor if the action is simply transitive, i.e. for all $x_1, x_2 \in X$ there is a unique g with $gx_1 = x_2$.

Examples.

(1) $X = G$, action is left multiplications.

(2) ~~Position vectors Displacement vectors.~~

~~"Up 1 foot", "Right 2 feet" etc.~~

~~Represent a change in position.~~

Points in the plane. (i.e. a physical space)

The group is $\mathbb{R}^2$, represented as vectors.

You can add vectors, can't add points

Think of X = plane with no origin.

e.g. locations in Columbia.

X = locations, G = "go one mile east"

You can add an element of G to one in X

You can add two elements of G

You can subtract two elements in X (get an elt of G)

But you can't add elements of X.

(3) Antiderivatives of a fixed function f.

These form an $\mathbb{R}$-torsor.

36.2

If we fix $x \in X$ get a bijection

$$\begin{array}{ccc} G & \xrightarrow{\sim} & X \\ g & \longrightarrow & gx \end{array}$$

but there is no canonical choice of x.

So: "A torsor is like a group that has forgotten its identity."

In the elliptic curve case, the EC (assume def/$\mathbb{Q}$) is the group. An E-torsor (or "principal homogeneous space") is a smooth curve $C/\mathbb{Q}$ with a simply transitive algebraic group action of E on C.

(i.e. for each $P \in E$, the action by P is a morphism of curves).

Silverman writes $\mu : C \times E \longrightarrow C$ for the action ("addition")

and $\nu : C \times C \longrightarrow E$

$q, p \longrightarrow$ the unique P with $\mu(p, P) = q$.

("subtraction")

Then you have some tautologies like

$\mu(p, \nu(q, p)) = q$ (i.e. $p + (q - p) = p$

which look obvious and are easy to prove but be careful to not write down things which aren't well defined.

36.3

Trivial Example. $E : y^2 = x^3 + ax^2 + bx$,
E acting on itself.

e.g. if $P_0 = (0,0) \in E(\mathbb{Q})$, get a map

$$\begin{array}{ccc} E & \longrightarrow & E \\ P & \longrightarrow & P + (0,0) \\ (x,y) & \longrightarrow & \left(\frac{b}{x}, \frac{-by}{x^2}\right) \end{array}$$

which is a rational map and hence extends to a morphism.

Nontrivial example. $E : y^2 = x^3 + ax^2 + bx$.

Fix $d \in \mathbb{Z}$, not a square.

write $C : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4$.

(Note: its projective closure has two pts at infinity).

Then C is an E-torsor.

How to see this?

Cheat. Define maps over $\mathbb{Q}(\sqrt{d})$

$$\begin{array}{ccc} E & \xrightarrow{\phi} & C \\ (x,y) & \longrightarrow & (z,w) = \left(\sqrt{d}\,\frac{x}{y}, \sqrt{d}\left(x - \frac{b}{x}\right)\left(\frac{x}{y}\right)^2\right) \end{array}$$

$$\left(\frac{\sqrt{d}\,w - az^2 + d}{2z^2}, \frac{dw - a\sqrt{d}\,z^2 + d\sqrt{d}}{2z^3} \right) \longleftarrow (z,w)$$

So that $E \cong C$ over $\mathbb{Q}(\sqrt{d})$

So given $P_C \in C$, $P_E \in E$,

compute $P_E + \phi^{-1}(P_C)$

Take ϕ of that.

36.4

Question. Does C have any $\mathbb{Q}$-rational points?

$$dw^2 = d^2 - 2adz^2 + (a^2-4b)z^4$$

Let p be a prime with $v_p(d) = 1$.
Then $v_p(dw^2)$ is odd.

Assume $v_p(2a) = v_p(a^2-4b) = 0$ (true for all but finitely many p)

Then if $v_p(z) \le 0$, $v_p(\text{RHS}) = 4v_p(z)$ (contradiction)
If $v_p(z) > 0$, $v_p(\text{RHS}) = v_p(d^2) = 2$ (")

So C has *no* $\mathbb{Q}$-rational points.
(In fact: its *projective closure* doesn't either)

Def. Two torsors C and C' (both over $\mathbb{Q}$) for $E/\mathbb{Q}$ are *equivalent* if there is an isomorphism if there is an isomorphism $C \xrightarrow{\theta} C'$ defined over $\mathbb{Q}$ compatible with the action of E on C and C'.

In other words,

(1) $\theta(p+P) = \theta(p) + P$ for $p \in C$, $P \in E$

or (2)

$$\begin{tikzcd} C \arrow[r, "\theta"] \arrow[d, "+P"] & C' \arrow[d, "+P"] \\ C \arrow[r] & C' \end{tikzcd}$$

An E-torsor is *trivial* if it is equivalent to E.

36.5.

Proposition. An E-torsor $C/\mathbb{Q}$ is nontrivial if and only if $C(\mathbb{Q}) = \phi$.

Proof. If $C/\mathbb{Q}$ is trivial, $\exists$ $E \xrightarrow{\theta} C$ defined over $\mathbb{Q}$, and so $\theta(\infty)$ is a rational point.

Conversely, suppose $p_0 \in C(\mathbb{Q})$.

We have a map

$$\begin{aligned} \theta : E &\longrightarrow C \\ P &\longrightarrow p_0 + P \end{aligned}$$

which is easily seen to be defined over $\mathbb{Q}$.

not the same as "obvious"; see Sil 10.3

Def. Let $WC(E/\mathbb{Q})$, the Weil-Châtalet group for E, be the set of torsors for E mod equivalence.

Theorem. There is a natural bijection

$$WC(E/\mathbb{Q}) \xrightarrow{\sim} H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E)$$

$$\{C\} \longrightarrow \{\sigma \longrightarrow p_0^\sigma - p_0\}.$$

(Choose any C and any $p_0 \in C(\overline{\mathbb{Q}})$.)

(Note: we can subtract points on $C(\overline{\mathbb{Q}})$ and get a point on E.)

(If $p_0 \in C(\mathbb{Q})$ then we get the map $\sigma \to 0$.

Last time.

The Weil-Châtalet group $WC(E)$ is the set of torsors for E mod equivalence:

A torsor is a curve $C/\mathbb{Q}$ with a simply transitive algebraic group action of E on C def. $/\mathbb{Q}$.

(Prop X.3.2) It will always be ~~defi~~ a twist of E.

Choose $p_0 \in C(\overline{\mathbb{Q}})$,
$$\theta : E \longrightarrow C, \quad P \longrightarrow p_0 + P$$
will be an isomorphism over $\mathbb{Q}(p_0)$.

Two torsors C, C' are equivalent if there is a $\mathbb{Q}$-iso. compatible with the action.

$$\begin{tikzcd} C \arrow[r, "\theta"] \arrow[d, "+P"] & C' \arrow[d, "+P"] \\ C \arrow[r] & C' \end{tikzcd}$$

(for all $P \in E$)

In particular, if $C(\mathbb{Q}) \neq \phi$ then C is equivalent to E. (Goes both ways)

Then we have

Choose any $p_0 \in C(\overline{\mathbb{Q}})$.

$$WC(E/\mathbb{Q}) \xrightarrow{\sim} H^1(Gal(\overline{\mathbb{Q}}/\mathbb{Q}), E)$$
$$\{C/\mathbb{Q}\} \longrightarrow \{\sigma \longrightarrow p_0^\sigma - p_0\}.$$

Proof in X.3 of Silverman; note that:

* You can subtract two points of C, get a pt in E
* If there is any $p_0 \in C(\mathbb{Q})$, visibly get the 0 map.

37.2.

Example 1. (Sil X.2) Not quite of above, want to show how twists of C correspond to cocycles.

This example will be in $H^1(\mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}), \mathrm{Isom}(E))$

Won't get a torsor.

Let $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ be a quadratic ext.

$\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \{\pm 1\}$ associated quadratic character:

$$\chi(\sigma) = \frac{\sigma(\sqrt{d})}{\sqrt{d}}.$$ Is a cocycle.

Compute the equation of the twist via function fields.

Given $E: y^2 = f(x)$, $[-1](x,y) = (x,-y)$ is an automorphism of E

(It is not $P \to P + P_0$ even over $\bar{\mathbb{Q}}$.)

Given $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, twist the Galois action on the FF:

$$\sigma(\sqrt{d}) = \chi(\sigma)\sqrt{d}, \quad \sigma(x) = x, \quad \sigma(y) = \chi(\sigma)\, y.$$

What is fixed by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}$? $x' = x$ and $y' = y/\sqrt{d}$.

So these functions are in $\mathbb{Q}(C)$ and satisfy

$$d(y')^2 = f(x').$$

This is a quadratic twist of E over $\mathbb{Q}(\sqrt{d})$.

Example. (of a torsor this time)

Let $E : y^2 = x^3 + ax^2 + bx$ (i.e. assume E has a 2-torsion $\mathbb{Q}$-point.)

We have (for any quad ext. $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$) the elt. of $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E)$

$$\xi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow E$$

$$\sigma \longrightarrow \begin{cases} 0 & \text{if } \sigma(\sqrt{d}) = \sqrt{d} \\ (0,0) & \text{if } \sigma(\sqrt{d}) = -\sqrt{d} \end{cases}$$

Let $\tau_T : E \to E$ be the map "add $(0,0)$".

So $\tau_T((x,y)) = (x,y) + (0,0) = \left(\frac{b}{x}, -\frac{by}{x^2}\right)$.

To find the equation of C, consider the twisted action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\overline{\mathbb{Q}}(E)$

$$\sigma(\sqrt{d}) = -\sqrt{d} \qquad \sigma(x) = \frac{b}{x} \qquad \sigma(y) = \frac{-by}{x^2}.$$

(N.B. this is for all points, when $\sigma(\sqrt{d}) = -\sqrt{d}$.
when $\sigma(\sqrt{d}) = \sqrt{d}$ action is trivial.)

Two invariant functions are

$$\underline{z = \sqrt{d}\,\frac{x}{y}} \qquad w = \sqrt{d}\left(x - \frac{b}{x}\right)\left(\frac{x}{y}\right)^2.$$

Here $\sigma(z) = -\sqrt{d} \cdot \frac{b}{x} \cdot \frac{x^2}{-by}$ etc.

Check that $dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4$

The Selmer and Shafarevich - Tate groups.

Suppose we are given two EC's $E, E'/\mathbb{Q}$, and a nonzero $\mathbb{Q}$-isogeny $\phi : E \to E'$.

(Typical example: $E = E'$ and $\phi = [m]$ for some $m > 1$.

Tactologically, there is an ES of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ - modules

~~$0 \to E[\phi$~~

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

Take Galois cohomology: $(G := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$

$$0 \to \underbrace{H^0(G, E[\phi])}_{E(\mathbb{Q})[\phi]} \to \underbrace{H^0(G, E)}_{E(\mathbb{Q})} \longrightarrow \underbrace{H^0(G, E')}_{E'(\mathbb{Q})} \longrightarrow H^1(G, E[\phi])$$
$$\longrightarrow H^1(G, E) \xrightarrow{\phi} H^1(G, E') \to \cdots$$

And so get

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} H^1(G, E[\phi]) \longrightarrow H^1(G, E)[\phi] \to 0.$$

Similarly, for any $p \leq \infty$, get (with $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$)

$$0 \to E'(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) \xrightarrow{\delta} H^1(G_p, E[\phi]) \longrightarrow H^1(G_p, E)[\phi] \to 0.$$

Combine.

$$\begin{tikzcd}
 & & & WC(E/\mathbb{Q})[\phi] \arrow[d, phantom, "\parallel"] & \\
0 \arrow[r] & E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \arrow[r, "\delta"] \arrow[d] & H^1(G, E[\phi]) \arrow[r, "\rho"] \arrow[d, "\mathrm{Res}"] \arrow[dr, dashed, "\tilde{\rho}"] & H^1(G, E)[\phi] \arrow[r] \arrow[d, "\mathrm{Res}"] & 0 \\
0 \arrow[r] & \prod_p \frac{E'(\mathbb{Q}_p)}{\phi(E(\mathbb{Q}_p))} \arrow[r, "\delta"] & \prod_p H^1(G_p, E[\phi]) \arrow[r] & \prod_p H^1(G_p, E)[\phi] \arrow[r] \arrow[d, phantom, "\parallel"] & 0 \\
 & & & \prod_p WC(E/\mathbb{Q}_p)[\phi] &
\end{tikzcd}$$

(The "Res" maps exist by general formalism.)

Note that $\delta\left(\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}\right) \subseteq \mathrm{Ker}(\rho) \subseteq \mathrm{Ker}(\tilde{\rho})$.

Definition. The Selmer group is ~~$\mathrm{Ker}(\tilde{\rho})$~~ $\mathrm{Ker}(\tilde{\rho})$.

We can ignore the last $[\phi]$, write

$$\mathrm{Sel}^{(\phi)}(E/\mathbb{Q}) = \mathrm{Ker}\left(H^1(G, E[\phi]) \xrightarrow{\tilde{\rho}} \prod_{p \le \infty} WC(E/\mathbb{Q}_p)\right).$$

The Shafarevich - Tate group is

$$\text{Ш}(E/\mathbb{Q}) = \mathrm{Ker}\left(WC(E/\mathbb{Q}) \longrightarrow \prod_{p \le \infty} WC(E/\mathbb{Q}_p)\right)$$

By the Snake Lemma, get

$$0 \longrightarrow E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \longrightarrow \mathrm{Sel}^{(\phi)}(E/\mathbb{Q}) \longrightarrow \text{Ш}(E/\mathbb{Q})[\phi] \to 0.$$

<u>37.6.</u>

Theorem. $\mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$ is finite.

Conjecture. Ш$(E/\mathbb{Q})$ is finite.

Idea of proof. Any cocycle $\xi \in \mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$ is unramified at p (trivial on the inertia group I_p) if $p \nmid \deg m$ and $E'/\mathbb{Q}$ has good reduction at p.

How to prove? ξ is trivial in $WC(E/\mathbb{Q}_p)$, so

$\xi_\sigma = \{P^\sigma - P\}$ for some $P \in E(\bar{\mathbb{Q}}_p)$, all $\sigma \in G_p$.

Let $\sim$ be the reduction mod p map, then

$\widetilde{P^\sigma - P} = \tilde{P}^\sigma - \tilde{P} = 0$, since inertia acts trivially on the residue field.

So $P^\sigma - P$ is in the kernel of reduction mod p

→ Jesse proved it's trivial!

(Because it's also $(\deg \phi)$-torsion.)

So $\xi_\sigma = 0$ for all $\sigma \in I_p$.

So Selmer group contained within

$H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), E[\phi]; \overset{\text{finite}}{S})$ (unr. outside S)

By "inflation-restriction", replace $\mathbb{Q}$ by a finite ext. K so that Galois action is trivial.

Get $\mathrm{Hom}(\mathrm{Gal}(\bar{K}/K), E[\phi]; S)$

$= \mathrm{Hom}(\underbrace{\mathrm{Gal}(L/K)}_{\text{max abelian of exponent } m \text{ UR outside } S}, E[\phi])$

Finite. (<u>when</u>!)

37.7

The Silverman - Tate proof again. (Sil X.4.8)

Assume $\phi : E \to E'$ is an isogeny $/\mathbb{Q}$ of degree 2.

Then $\ker(\phi)$ is defined over $\mathbb{Q}$.

WLOG: $E: \; y^2 = x^3 + ax^2 + bx$ w/ $(0,0) \in E(\mathbb{Q})$.

We have $E': \; Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X$

$$\phi : E \longrightarrow E'$$

$$(x,y) \longrightarrow \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2} \right).$$

How to come up with it? Cook up a map whose kernel is $\{(0,0), \infty\}$.

Now, $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E[\phi])$

$= H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \pm 1)$

$= \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \pm 1)$ ← any such factors through a unique $\mathbb{Q}(\sqrt{d})$

$= \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$.

As before, for any d representing an elt. of H^1, the cocycle is

$$\sigma \longrightarrow \begin{cases} 0 & \text{if } \sigma(\sqrt{d}) = \sqrt{d} \\ (0,0) & \text{if } \sigma(\sqrt{d}) = -\sqrt{d} \end{cases}$$

and the torsor (homogeneous space) is

$$C_d : \; dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4$$

(did this before).

37.8

Chasing around the cohomology nonsense,

$$\begin{array}{rcl} \delta : E'(\mathbb{Q}) & \longrightarrow & H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E[\phi]) = \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \\ \infty & \longrightarrow & 1 \\ (0,0) & \longrightarrow & a^2 - 4b \\ (X,Y) & \longrightarrow & X \end{array}$$

and so we have

$$0 \longrightarrow \underbrace{\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}}_{\text{We want to prove this is finite}} \longrightarrow \underbrace{Sel^{(\phi)}(E/\mathbb{Q})} \longrightarrow \underbrace{\text{Ш}(E/\mathbb{Q})[\phi]}_{\text{Nobody understands what the hell this is. That's okay.}} \longrightarrow 0$$

Silverman writes smth different. I think this is also correct.

This is $\{d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 : C_d$ has $\mathbb{Q}_p$-rational points for all $p\}$

But $dw^2 = d^2 - 2adz^2 + (a^2-4b)z^4$ $\quad C_d$

If $p \nmid -2a$, $p \nmid a^2 - 4b$, and $p \mid d$, take p-adic valuations

$$1 + 2v_p(w) \;\Big|\; 2 \qquad 1 + 2v_p(z) \qquad 4v_p(z)$$

The RHS cannot be made to work!
No two of those are equal. Since LHS is odd,
$1 + 2v_p(z)$ must be the minimum, but then $v_p(z) = 0$
and you have a contradiction.

And so $E'(\mathbb{Q}) / \phi(E(\mathbb{Q}))$ is finite.

Prove $E(\mathbb{Q}) / \hat{\phi}(E'(\mathbb{Q}))$ is finite in the same way.

(Indeed this is what Silverman - Tate did.
There you see a, b instead of $\bar{a} = -2a$
$\bar{b} = a^2 - 4b$.)

Combine to get finiteness of $E(\mathbb{Q}) / 2E(\mathbb{Q})$.

Some conjectures.

There is r s.t. rank $E(\mathbb{Q}) \leq r$ for all EC. r.

(could talk about BSD etc. but I should probably stop here.