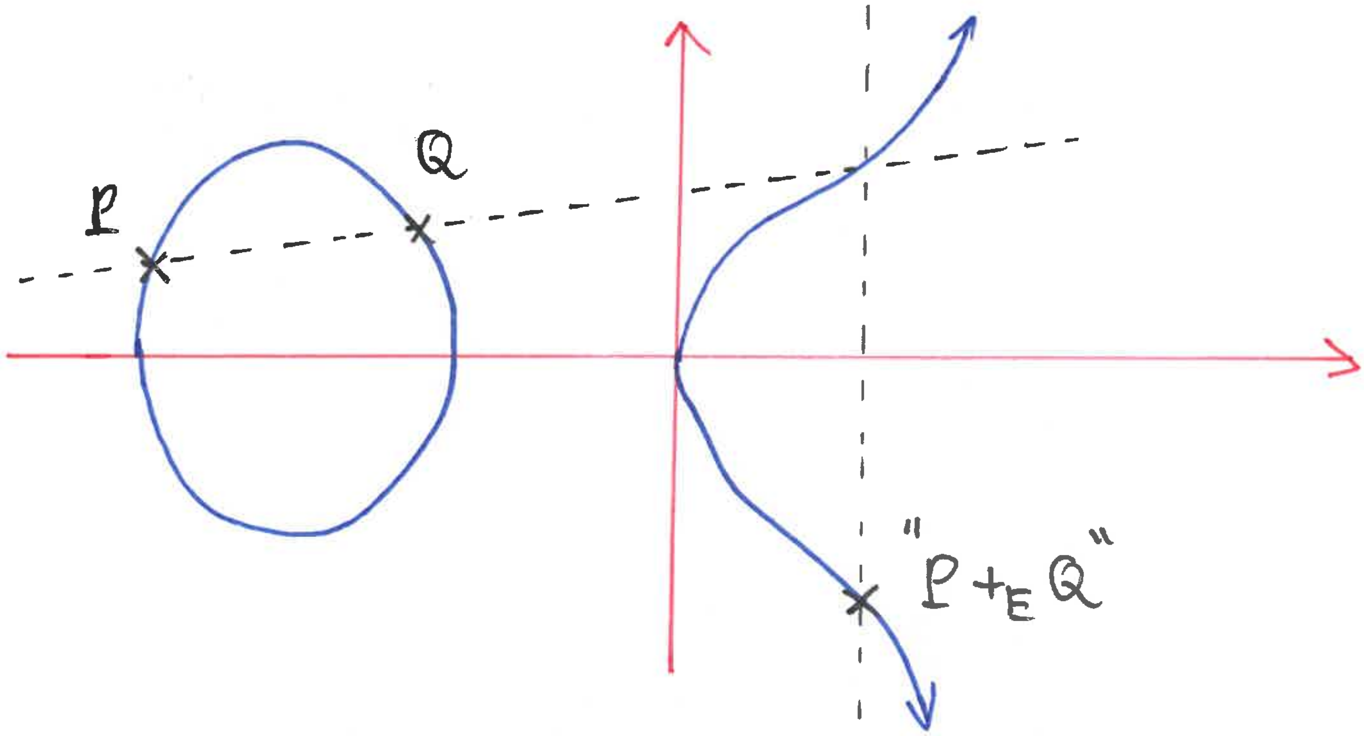
LECTURE I – "Elliptic Curves"

Let $E_{/\mathbb{Q}}$ be an elliptic curve.

e.g. $E: \; y^2 = x^3 + Ax + B$
with $4A^3 + 27B^2 \neq 0$.



Def: For a number field F, we write $E(F)$ for the group of F-rational points on E.

(We'll use the same terminology if F = an infinite extension of $\mathbb{Q}$ or F = a p-adic field.)

②

Theorem (Mordell–Weil):
The abelian group $E(F)$ is finitely-generated so that

$$E(F) \cong \mathbb{Z}^{r_F(E)} \oplus (\text{finite group})$$

for some $r_F(E) \geq 0$.

Mazur: $\#E(\mathbb{Q})_{tors} \leq 16$

Q. How does one compute $r_F(E)$?

Def: Suppose that $\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character.

For $\mathrm{Re}(s) > \frac{3}{2}$ one defines

$$L(E, \chi, s) := \prod_{\text{primes } \ell}{}' \frac{1}{1 - \chi(\ell) a_\ell(E) \ell^{-s} + \chi^2(\ell) \ell^{1-2s}}$$

where $a_\ell(E) = \ell + 1 - \#E(\mathbb{F}_\ell)$

no. of points on E modulo 'ℓ'

N.B. Hasse showed that $|a_\ell(E)| \leq 2\sqrt{\ell}$.

The functional equation relates

$$L(E, \chi, s) \longleftrightarrow L(E, \chi^{-1}, 2-s)$$

so that $s=1$ is the point of symmetry.

<u>Wiles et al:</u> $E/\mathbb{Q}$ is "modular"
so that $L(E, \chi, s)$ has analytic continuation to $\mathbb{C}$.

<u>Birch & Swinnerton-Dyer Conjecture.</u>

(i) $r_{\mathbb{Q}}(E) = \mathrm{order}_{s=1} L(E, s)$.

(ii) $L^*(E, 1) =$ "arithmetic invariants" $\times \# Ш(E/\mathbb{Q})$.

<u>Goal of the lectures</u>

To prove that:

- $L(E, 1) \neq 0 \implies E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ are both finite
- If $\chi : \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow \mathbb{C}^\times$ then $L(E, \chi, 1) \neq 0 \implies E(F)^\chi$ and $Ш(E/F)^\chi$ finite.

Group Cohomology.

Let G be a group,
and M will denote a G-module.

<u>N.B.</u> If G is profinite so that $G \cong \varprojlim_{U} G/U$
then we'll assume that $M = \bigcup_{U} M^{U}$
where $M^{U} := \{ m \in M \mid m^{\sigma} = m \text{ for all } \sigma \in U \}$.

<u>Remark:</u> If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence of G-modules, then

$$0 \to M_1^G \to M_2^G \to M_3^G$$

is also exact.

<u>Q.</u> How do we extend this on the right?

<u>A.</u> Cohomology.

"Black Box"

For each short exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

there exists a long exact sequence

$$0 \to H^0(G, M_1) \to H^0(G, M_2) \to H^0(G, M_3)$$
$$\xrightarrow{\partial} H^1(G, M_1) \to H^1(G, M_2) \to H^1(G, M_3)$$
$$\xrightarrow{\partial} \dots \to H^i(G, M_1) \to H^i(G, M_2) \to H^i(G, M_3)$$
$$\xrightarrow{\partial} H^{i+1}(G, M_1) \to \dots$$

where
$$H^0(G, M) = M^G,$$
$$H^1(G, M) = \frac{\{\xi : G \to M \mid \xi(\sigma\tau) = \xi(\sigma)^\tau + \xi(\tau)\}}{\left\{\xi : G \to M \;\middle|\; \begin{array}{l}\xi(\sigma) = m_\xi^\sigma - m_\xi \\ \text{for some } m_\xi\end{array}\right\}}$$

etc...

Exercise: If G acts trivially on M, show that $H^1(G, M) \cong \mathrm{Hom}(G, M)$.

⑥

Properties

(1) "Inflation – Restriction"

If $H \lhd G$ then there is a s.e.s.

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{inf}} H^1(G,M) \xrightarrow{\text{res}} H^1(H,M).$$

(2) "Cup-product"

If M_1, M_2 are $R[G]$-modules,

$$\text{"}\cup\text{"}: H^i(G,M_1) \times H^j(G,M_2) \longrightarrow H^{i+j}(G, M_1 \otimes_R M_2).$$

(3) If $G = \langle \gamma \rangle$ is cyclic then

$$H^0(G,M) = \{ m \in M \mid m^\gamma = m \}$$

and

$$H^1(G,M) \cong \frac{\operatorname{Ker}(M \xrightarrow{N} M)}{I_G M}$$

where $N = 1 + \gamma + \dots + \gamma^{\#G-1}$

& I_G = augmentation ideal of $R[G]$.

The Kummer Map.

Let K be a field of characteristic zero.

If we consider $E(\overline{K})$

where $\overline{K}$ = alg. closure of K,

then $G_K = \mathrm{Gal}(\overline{K}/K)$ acts on $E(\overline{K})$.

$\rightsquigarrow$ short exact sequence of G_K-modules

$$0 \to E_m \to E(\overline{K}) \xrightarrow{\times m} E(\overline{K}) \to 0$$

since E is m-divisible at each $m \geq 1$.

$\therefore$ Taking cohomology:

$$0 \to E_m(\overline{K})^G \longrightarrow E(\overline{K})^G \xrightarrow{\times m} E(\overline{K})^G$$

$$\xrightarrow{\partial_m} H^1(G_K, E_m) \longrightarrow H^1(G_K, E) \xrightarrow{\times m} H^1(G_K, E)$$

$$\longrightarrow \cdots$$

which after truncation becomes

$$0 \to E(K)/m.E(K) \xrightarrow{\partial_m} H^1(G_K, E_m)$$

$$\longrightarrow H^1(G_K, E)_m \to 0$$

⑧

Taking the direct limit of ∂_m:

$$\varinjlim_m E(K) \underset{\mathbb{Z}}{\otimes} \tfrac{1}{m}\mathbb{Z}/\mathbb{Z} \xhookrightarrow{\partial_m} \varinjlim_m H^1(G_K, E_m)$$

i.e.
$$E(K) \otimes \mathbb{Q}/\mathbb{Z} \xhookrightarrow{\partial^{Kum}} H^1(G_K, E_{tors}).$$

Def: Assume F is a no. field.

ⓐ The Selmer group $Sel(E/F)$ is the kernel of

$$H^1(G_F, E_{tors}) \xrightarrow{\prod res_v} \prod_{\text{places } v} \frac{H^1(G_{F_v}, E_{tors})}{\partial^{Kum}(E(F_v) \otimes \mathbb{Q}/\mathbb{Z})}.$$

ⓑ The Tate-Shafarevich group $Ш(E/F)$ is the kernel of

$$H^1(G_F, E(\bar{F})) \xrightarrow{\prod res_v} \prod_{\text{places } v} H^1(G_{F_v}, E(\bar{F})).$$

Exercise: Show that $\exists$ a short exact sequence

$$0 \to E(F) \otimes \mathbb{Q}/\mathbb{Z} \to Sel(E/F) \to Ш(E/F) \to 0.$$

BSD Conjecture: (Precise Form)

(i) $r_{\mathbb{Q}}(E) = \mathrm{order}_{s=1} L(E,s)$.

(ii) $$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^{r_{\mathbb{Q}}(E)}}$$

$$= \Omega_E \times \mathrm{Reg}_E \times \frac{\# Ш(E/\mathbb{Q}) \times \prod_{\ell} [E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell)]}{(\# E(\mathbb{Q})_{\mathrm{tors}})^2}$$

where $\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{y}$ "real period"

and $\mathrm{Reg}_E = \det\left(\langle P_i, P_j \rangle^{\text{Néron-Tate}}\right)$

with $E(\mathbb{Q}) \otimes \mathbb{R} \cong \bigoplus_{i=1}^{r_{\mathbb{Q}}(E)} \mathbb{R} \cdot P_i$ say.

"elliptic regulator"

Remark: For rank ≤ 1 we kind of know what's happening thanks to work of Coates, Wiles, Rubin, Kato, Gross, Zagier, Bhargava, Shankar, and many others.