Some background on elliptic curves and Galois cohomology

Jim Brown

September 19, 2009

An elliptic curve over a field k is (depending on your taste):

An elliptic curve over a field k is (depending on your taste):

1. A complete nonsingular curve E of genus 1 over k together with a point $O \in E(k)$.

An elliptic curve over a field k is (depending on your taste):

1. A complete nonsingular curve E of genus 1 over k together with a point $O \in E(k)$.
2. A nonsingular plane projective curve E of degree 3 together with a point $O \in E(k)$.

An elliptic curve over a field k is (depending on your taste):

1. A complete nonsingular curve E of genus 1 over k together with a point $O \in E(k)$.
2. A nonsingular plane projective curve E of degree 3 together with a point $O \in E(k)$.
3. A nonsingular plane projective curve E of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

More familiarly, if $\mathrm{char}\, k \neq 2, 3$, one can write an elliptic curve in the form

$$Y^2 = X^3 + aX + b$$

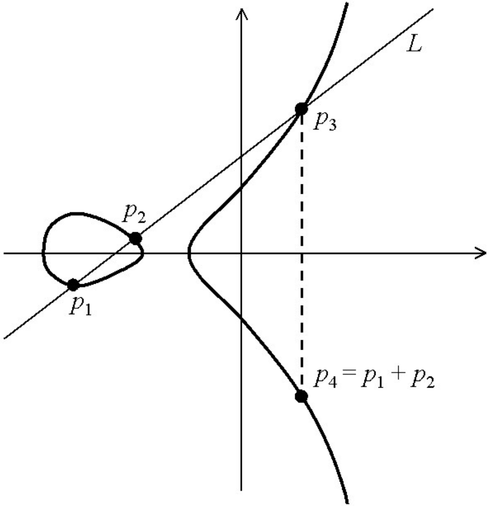
where $\Delta = 4a^3 + 27b^2 \neq 0$ (along with a point at infinity $(0 : 1 : 0)$.)

Given a set R, we write $E(R)$ for those $P = (x, y)$ with $x, y \in R$ and $y^2 = x^3 + ax + b$.

Given a set R, we write $E(R)$ for those $P = (x, y)$ with $x, y \in R$ and $y^2 = x^3 + ax + b$.
There is an addition on $E(k)$ that makes it into a group:

Given a set R, we write $E(R)$ for those $P = (x, y)$ with $x, y \in R$ and $y^2 = x^3 + ax + b$.

There is an addition on $E(k)$ that makes it into a group:



Theorem

(Mordell-Weil) For any elliptic curve over a number field k, the group $E(k)$ is finitely generated.

Theorem

(Mordell-Weil) For any elliptic curve over a number field k, the group $E(k)$ is finitely generated.

1. This was shown by Mordell in the case $k = \mathbb{Q}$ in 1922.

Theorem

(Mordell-Weil) For any elliptic curve over a number field k, the group $E(k)$ is finitely generated.

1. This was shown by Mordell in the case $k = \mathbb{Q}$ in 1922.
2. For general number fields this is contained the thesis of Weil (1928). (He actually proved: given any nonsingular projective curve C over a number field k, one has $\mathrm{Pic}^0(C)$ is finitely generated.)

Theorem

(Weak Mordell-Weil) For any elliptic curve E over a number field k and any integer n, $E(k)/nE(k)$ is finite.

Theorem

(Weak Mordell-Weil) For any elliptic curve E over a number field k and any integer n, $E(k)/nE(k)$ is finite.

The Mordell-Weil theorem follows from the Weak Mordell-Weil theorem by a descent argument.

Theorem

(Weak Mordell-Weil) For any elliptic curve E over a number field k and any integer n, $E(k)/nE(k)$ is finite.

The Mordell-Weil theorem follows from the Weak Mordell-Weil theorem by a descent argument.

To prove the Weak Mordell-Weil theorem one uses Galois cohomology, which we now review.

For a number field k, we write k^{al} for an algebraic closure of k.

For a number field k, we write k^{al} for an algebraic closure of k.

We write G_k for $\mathrm{Gal}(k^{\mathrm{al}}/k)$.

For a number field k, we write k^{al} for an algebraic closure of k.

We write G_k for $\mathrm{Gal}(k^{\mathrm{al}}/k)$.

We write $E(k^{\mathrm{al}})[n]$ for the n-torsion points of $E(k^{\mathrm{al}})$, i.e., the points $P \in E(k^{\mathrm{al}})$ so that $nP = 0$.

For a number field k, we write k^{al} for an algebraic closure of k.

We write G_k for $\mathrm{Gal}(k^{\mathrm{al}}/k)$.

We write $E(k^{\mathrm{al}})[n]$ for the n-torsion points of $E(k^{\mathrm{al}})$, i.e., the points $P \in E(k^{\mathrm{al}})$ so that $nP = 0$.

Note that one has a natural action of G_k on $E(k^{\mathrm{al}})$ and on $E(k^{\mathrm{al}})[n]$ given by $\sigma \cdot (x, y) = (x^\sigma, y^\sigma)$.

Let G be a topological group and M a G-module where the action of G on M is continuous.

Let G be a topological group and M a G-module where the action of G on M is continuous.

One can define cohomology groups $H^n(G, M)$ for all $n \geq 0$, but we only define them for $n = 0, 1$.

Let G be a topological group and M a G-module where the action of G on M is continuous.

One can define cohomology groups $H^n(G, M)$ for all $n \geq 0$, but we only define them for $n = 0, 1$.

For $n = 0$, set

$$H^0(G, M) = M^G = \{m \in M : m^\sigma = m \text{ for all } \sigma \in G\}.$$

A *crossed homomorphism* is a continuous homomorphism $f : G \to M$ satisfying

$$f(\sigma\tau) = f(\sigma) + f(\tau)^{\sigma}$$

for all $\sigma, \tau \in G$.

A *crossed homomorphism* is a continuous homomorphism $f : G \to M$ satisfying

$$f(\sigma\tau) = f(\sigma) + f(\tau)^{\sigma}$$

for all $\sigma, \tau \in G$.

A *principal crossed homomorphism* is a continuous homomorphism $f : G \to M$ satisfying

$$f(\sigma) = m^{\sigma} - m$$

for some fixed $m \in M$ and all $\sigma \in G$.

Define

$$H^1(G, M) = \frac{\{\text{crossed homomorphisms}\}}{\{\text{principal crossed homomorphisms}\}}.$$

Define

$$H^1(G, M) = \frac{\{\text{crossed homomorphisms}\}}{\{\text{principal crossed homomorphisms}\}}.$$

Theorem

Given an exact sequence of G-modules

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

there is a canonical exact sequence

$$0 \to M_1^G \to M_2^G \to M_3^G \to H^1(G, M_1) \to H^1(G, M_2) \to H^1(G, M_3).$$

Example

If G acts on M trivially then

Example

If G acts on M trivially then

1. $H^0(G, M) = M$

Example

If G acts on M trivially then

1. $H^0(G, M) = M$
2. $H^1(G, M) = \mathrm{Hom}_{\mathrm{grp}}(G, M)$.

Example

If G acts on M trivially then

1. $H^0(G,M) = M$
2. $H^1(G,M) = \mathrm{Hom}_{\mathrm{grp}}(G,M)$.

Example

If $G = G_k$ and $M = E(k^{\mathrm{al}})$, then $H^0(G,M) = E(k)$.

Example

If G acts on M trivially then

1. $H^0(G, M) = M$
2. $H^1(G, M) = \mathrm{Hom}_{\mathrm{grp}}(G, M)$.

Example

If $G = G_k$ and $M = E(k^{\mathrm{al}})$, then $H^0(G, M) = E(k)$.

On the other hand, $H^1(G_k, E(k^{\mathrm{al}}))$ is not so easy...

Example

If G acts on M trivially then

1. $H^0(G, M) = M$
2. $H^1(G, M) = \mathrm{Hom}_{\mathrm{grp}}(G, M)$.

Example

If $G = G_k$ and $M = E(k^{\mathrm{al}})$, then $H^0(G, M) = E(k)$.

On the other hand, $H^1(G_k, E(k^{\mathrm{al}}))$ is not so easy...

In general we write $H^n(k, M)$ to denote $H^n(G_k, M)$.

Theorem

For any integer n one has that the map $n : E(k^{\mathrm{al}}) \to E(k^{\mathrm{al}})$ is surjective.

Theorem

For any integer n one has that the map $n : E(k^{\mathrm{al}}) \to E(k^{\mathrm{al}})$ is surjective.

This theorem gives an exact sequence:

$$0 \to E(k^{\mathrm{al}})[n] \to E(k^{\mathrm{al}}) \xrightarrow{n} E(k^{\mathrm{al}}) \to 0.$$

Theorem

For any integer n one has that the map $n : E(k^{\mathrm{al}}) \to E(k^{\mathrm{al}})$ is surjective.

This theorem gives an exact sequence:

$$0 \to E(k^{\mathrm{al}})[n] \to E(k^{\mathrm{al}}) \xrightarrow{n} E(k^{\mathrm{al}}) \to 0.$$

Which in turn gives an exact sequence:

$$0 \to E(k)[n] \to E(k) \xrightarrow{n} E(k) \to H^1(k, E(k^{\mathrm{al}})[n]) \\ \to H^1(k, E(k^{\mathrm{al}})) \xrightarrow{n} H^1(k, E(k^{\mathrm{al}})).$$

From this long exact sequence in Galois cohomology one deduces the exact sequence:

From this long exact sequence in Galois cohomology one deduces the exact sequence:

$$0 \to E(k)/nE(k) \to H^1(k, E(k^{\text{al}})[n]) \to H^1(k, E(k^{\text{al}}))[n] \to 0.$$

From this long exact sequence in Galois cohomology one deduces the exact sequence:

$$0 \to E(k)/nE(k) \to H^1(k, E(k^{\mathrm{al}})[n]) \to H^1(k, E(k^{\mathrm{al}}))[n] \to 0.$$

Unfortunately, $H^1(k, E(k^{\mathrm{al}})[n])$ is not in general finite.

From this long exact sequence in Galois cohomology one deduces the exact sequence:

$$0 \to E(k)/nE(k) \to H^1(k, E(k^{\mathrm{al}})[n]) \to H^1(k, E(k^{\mathrm{al}}))[n] \to 0.$$

Unfortunately, $H^1(k, E(k^{\mathrm{al}})[n])$ is not in general finite.

Goal: Replace $H^1(k, E(k^{\mathrm{al}})[n])$ with a group we can show is finite and contains the image of $E(k)/nE(k)$.

For a place v of k, consider E as an elliptic curve over k_v.

For a place v of k, consider E as an elliptic curve over k_v.

For each place v one obtains a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(k)/nE(k) & \longrightarrow & H^1(k, E(k^{\mathrm{al}})[n]) & \longrightarrow & H^1(k, E(k^{\mathrm{al}}))[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(k_v)/nE(k_v) & \longrightarrow & H^1(k_v, E(k_v^{\mathrm{al}})[n]) & \longrightarrow & H^1(k_v, E(k_v^{\mathrm{al}}))[n] & \longrightarrow & 0. \end{array}$$

For a place v of k, consider E as an elliptic curve over k_v.

For each place v one obtains a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(k)/nE(k) & \longrightarrow & H^1(k, E(k^{\mathrm{al}})[n]) & \longrightarrow & H^1(k, E(k^{\mathrm{al}}))[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(k_v)/nE(k_v) & \longrightarrow & H^1(k_v, E(k_v^{\mathrm{al}})[n]) & \longrightarrow & H^1(k_v, E(k_v^{\mathrm{al}}))[n] & \longrightarrow & 0. \end{array}$$

Define the n-Selmer group by

For a place v of k, consider E as an elliptic curve over k_v.

For each place v one obtains a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(k)/nE(k) & \longrightarrow & H^1(k, E(k^{\mathrm{al}})[n]) & \longrightarrow & H^1(k, E(k^{\mathrm{al}}))[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(k_v)/nE(k_v) & \longrightarrow & H^1(k_v, E(k_v^{\mathrm{al}})[n]) & \longrightarrow & H^1(k_v, E(k_v^{\mathrm{al}}))[n] & \longrightarrow & 0. \end{array}$$

Define the n-Selmer group by

$$\begin{aligned} \mathrm{Sel}_n(E/k) &= \{c \in H^1(k, E(k^{\mathrm{al}})[n]) : \ \forall v,\ c_v \text{ comes from } E(k_v)\} \\ &= \ker\left(H^1(k, E(k^{\mathrm{al}})[n]) \to \prod_v H^1(k_v, E(k_v^{\mathrm{al}})) \right). \end{aligned}$$

Similarly, we define the Shafarevich-Tate group by

Similarly, we define the Shafarevich-Tate group by

$$Ш(E/k) = \ker \left(H^1(k, E(k^{\mathrm{al}})) \to \prod_v H^1(k_v, E(k_v^{\mathrm{al}})) \right).$$

Similarly, we define the Shafarevich-Tate group by

$$Ш(E/k) = \ker\left(H^1(k, E(k^{\mathrm{al}})) \to \prod_v H^1(k_v, E(k_v^{\mathrm{al}}))\right).$$

1. It is conjectured that Ш is finite, but it is not known in general.

Similarly, we define the Shafarevich-Tate group by

$$Ш(E/k) = \ker \left(H^1(k, E(k^{\mathrm{al}})) \to \prod_v H^1(k_v, E(k_v^{\mathrm{al}})) \right).$$

1. It is conjectured that Ш is finite, but it is not known in general.
2. There is a precise (conjectural) relationship between the order of Ш and the rank of $E(k)$.

Similarly, we define the Shafarevich-Tate group by

$$Ш(E/k) = \ker \left(H^1(k, E(k^{\text{al}})) \to \prod_v H^1(k_v, E(k_v^{\text{al}})) \right).$$

1. It is conjectured that Ш is finite, but it is not known in general.
2. There is a precise (conjectural) relationship between the order of Ш and the rank of $E(k)$.
3. With the proper geometric interpretation Ш provides a measure of the failure of the local-global principle.

Using the exact sequence

$$0 \to E(k)/nE(k) \to H^1(k, E(k^{\mathrm{al}})[n]) \to H^1(k, E(k^{\mathrm{al}}))[n] \to 0$$

and the kernel-cokernel exact sequence we obtain:

Using the exact sequence

$$0 \to E(k)/nE(k) \to H^1(k, E(k^{\mathrm{al}})[n]) \to H^1(k, E(k^{\mathrm{al}}))[n] \to 0$$

and the kernel-cokernel exact sequence we obtain:

$$0 \to E(k)/nE(k) \to \mathrm{Sel}_n(E/k) \to Ш(E/k)[n] \to 0.$$

Finally, in the case of elliptic curves one can show $\mathrm{Sel}_n(E/k)$ is finite. In fact, it is actually computable! Thus we obtain the weak Mordell-Weil theorem.

Let E be an elliptic curve over k and let v be a finite place.

Let E be an elliptic curve over k and let υ be a finite place.

Considering E as an elliptic curve over k_υ, we can choose a (minimal) equation for E so that the $a_i \in \mathcal{O}_\upsilon$.

Let E be an elliptic curve over k and let v be a finite place.

Considering E as an elliptic curve over k_v, we can choose a (minimal) equation for E so that the $a_i \in \mathcal{O}_v$.

The curve obtained by taking the reduction of the a_i modulo ϖ_v does not depend on the choice of the equation and we write $\widetilde{E}_v$ for this curve.

Let E be an elliptic curve over k and let v be a finite place.

Considering E as an elliptic curve over k_v, we can choose a (minimal) equation for E so that the $a_i \in \mathcal{O}_v$.

The curve obtained by taking the reduction of the a_i modulo ϖ_v does not depend on the choice of the equation and we write $\widetilde{E}_v$ for this curve.

If $\widetilde{E}_v$ is an elliptic curve, we say E has good reduction at v.

If $\widetilde{E}_v$ is not an elliptic curve, we can still put a group structure on $\widetilde{E}_v^{\mathrm{ns}}$.

If $\widetilde{E}_v$ is not an elliptic curve, we can still put a group structure on $\widetilde{E}_v^{\mathrm{ns}}$.

If $\widetilde{E}_v$ is a cuspidal cubic, then $\widetilde{E}_v^{\mathrm{ns}}$ is isomorphic to $\mathbb{G}_a$ and we say E has additive reduction at v.

If $\widetilde{E}_v$ is not an elliptic curve, we can still put a group structure on $\widetilde{E}_v^{\mathrm{ns}}$.

If $\widetilde{E}_v$ is a cuspidal cubic, then $\widetilde{E}_v^{\mathrm{ns}}$ is isomorphic to $\mathbb{G}_a$ and we say E has additive reduction at v.

If $\widetilde{E}_v$ is a nodal cubic and the tangent lines at the node are defined over $\mathbb{F}_v$, then $\widetilde{E}_v^{\mathrm{ns}}$ is isomorphic to $\mathbb{G}_m$ and we say E has split multiplicative reduction at v.

If $\widetilde{E}_v$ is not an elliptic curve, we can still put a group structure on $\widetilde{E}_v^{\mathrm{ns}}$.

If $\widetilde{E}_v$ is a cuspidal cubic, then $\widetilde{E}_v^{\mathrm{ns}}$ is isomorphic to $\mathbb{G}_a$ and we say E has additive reduction at v.

If $\widetilde{E}_v$ is a nodal cubic and the tangent lines at the node are defined over $\mathbb{F}_v$, then $\widetilde{E}_v^{\mathrm{ns}}$ is isomorphic to $\mathbb{G}_m$ and we say E has split multiplicative reduction at v.

If $\widetilde{E}_v$ is a nodal cubic and the tangent lines at the node are not defined over $\mathbb{F}_v$, we say E has non-split multiplicative reduction at v.

Let $q_v = \#\mathbb{F}_v$.

Let $q_v = \#\mathbb{F}_v$.

Let S be the finite set of places where E does not have good reduction along with the archimedean places.

Let $q_v = \#\mathbb{F}_v$.

Let S be the finite set of places where E does not have good reduction along with the archimedean places.

For $v \notin S$, set $a_v = 1 + q_v - \#\widetilde{E}_v(\mathbb{F}_v)$.

Let $q_v = \#\mathbb{F}_v$.

Let S be the finite set of places where E does not have good reduction along with the archimedean places.

For $v \notin S$, set $a_v = 1 + q_v - \#\widetilde{E}_v(\mathbb{F}_v)$.

For such v, set $L_v(E/k, s) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}$.

For $v \in S$, define

For $v \in S$, define

$$L_v(E/k, s) = \begin{cases} 1 & E \text{ has additive reduction} \\ (1 - q_v^{-s})^{-1} & E \text{ has split multiplicative reduction} \\ (1 + q_v^{-s})^{-1} & E \text{ has non-split multiplicative reduction} \end{cases}$$

Define

$$L(E/k,s) = \prod_{v \nmid \infty} L_v(E/k,s).$$

Define

$$L(E/k, s) = \prod_{v \nmid \infty} L_v(E/k, s).$$

This L function can be completed by adding the terms for the infinite places.

Define

$$L(E/k, s) = \prod_{v \nmid \infty} L_v(E/k, s).$$

This L function can be completed by adding the terms for the infinite places.

Once completed, the L-function has the usual properties one would expect.

Note that one can actually write $L_v(E/k, s)$ for any finite v as:

$$L_v(E/k, s) = \det(1 - \sigma_v^{-1} q_v^{-s} \mid (T_\ell(E)^\vee)^{I_v})^{-1}.$$

Weak BSD Conjecture

(Weak BSD) The rank of $E(\mathbb{Q})$ *is the order of vanishing of* $L(E/\mathbb{Q}, s)$ *at* $s = 1$.

Weak BSD Conjecture

(Weak BSD) The rank of $E(\mathbb{Q})$ *is the order of vanishing of* $L(E/\mathbb{Q}, s)$ *at* $s = 1$.

The strong form of the conjecture that gives the first coefficient in the Taylor expansion of $L(E/\mathbb{Q}, s)$ around $s = 1$ will be discussed in the following talk. Note that it contains the order of the Shafarevich-Tate group!