The method of Euler systems

Alberto Angurel Andrés

University of Nottingham

April 8, 2026

University of Nottingham

UK | CHINA | MALAYSIA

Class groups

Fundamental Theorem of Arithmetic

Let $\frac{a}{b} \in \mathbb{Q}^\times$. Then there is a **unique** set of (different) primes $p_1, \ldots, p_r$ and integers $\alpha_1, \ldots, \alpha_r$ such that

$$\frac{a}{b} = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Class groups

Fundamental Theorem of Arithmetic

Let $\frac{a}{b} \in \mathbb{Q}^\times$. Then there is a **unique** set of (different) primes $p_1, \ldots, p_r$ and integers $\alpha_1, \ldots, \alpha_r$ such that

$$\frac{a}{b} = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Not true for other number fields

Let K be a number field (i.e., a finite extension of $\mathbb{Q}$) and let $\mathcal{O}_K$ be its ring of (algebraic) integers. There is a notion of prime/irreducible elements in these rings.

Class groups

Fundamental Theorem of Arithmetic

Let $\frac{a}{b} \in \mathbb{Q}^\times$. Then there is a **unique** set of (different) primes $p_1, \dots, p_r$ and integers $\alpha_1, \dots, \alpha_r$ such that

$$\frac{a}{b} = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Not true for other number fields

Let K be a number field (i.e., a finite extension of $\mathbb{Q}$) and let $\mathcal{O}_K$ be its ring of (algebraic) integers. There is a notion of prime/irreducible elements in these rings. Every element admits a prime factorisation, but it is not unique.

Class groups

Fundamental Theorem of Arithmetic

Let $\frac{a}{b} \in \mathbb{Q}^\times$. Then there is a **unique** set of (different) primes $p_1, \dots, p_r$ and integers $\alpha_1, \dots, \alpha_r$ such that

$$\frac{a}{b} = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Not true for other number fields

Let K be a number field (i.e., a finite extension of $\mathbb{Q}$) and let $\mathcal{O}_K$ be its ring of (algebraic) integers. There is a notion of prime/irreducible elements in these rings. Every element admits a prime factorisation, but it is not unique.
For example, if $K = \mathbb{Q}(\sqrt{-5})$, then

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$$

Class groups

Fundamental Theorem of Arithmetic

Let $\frac{a}{b} \in \mathbb{Q}^\times$. Then there is a **unique** set of (different) primes $p_1, \dots, p_r$ and integers $\alpha_1, \dots, \alpha_r$ such that

$$\frac{a}{b} = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Not true for other number fields

Let K be a number field (i.e., a finite extension of $\mathbb{Q}$) and let $\mathcal{O}_K$ be its ring of (algebraic) integers. There is a notion of prime/irreducible elements in these rings. Every element admits a prime factorisation, but it is not unique.
For example, if $K = \mathbb{Q}(\sqrt{-5})$, then

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$$

Substitute elements for ideals

Every ideal of $\mathcal{O}_K$ admits a unique factorization into prime ideals.

Class groups

Fundamental Theorem of Arithmetic

Let $\frac{a}{b} \in \mathbb{Q}^\times$. Then there is a **unique** set of (different) primes $p_1, \dots, p_r$ and integers $\alpha_1, \dots, \alpha_r$ such that

$$\frac{a}{b} = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Not true for other number fields

Let K be a number field (i.e., a finite extension of $\mathbb{Q}$) and let $\mathcal{O}_K$ be its ring of (algebraic) integers. There is a notion of prime/irreducible elements in these rings. Every element admits a prime factorisation, but it is not unique.
For example, if $K = \mathbb{Q}(\sqrt{-5})$, then

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$$

Substitute elements for ideals

Every ideal of $\mathcal{O}_K$ admits a unique factorization into prime ideals.

$$\mathfrak{p} := (3, 1 + \sqrt{-5}), \qquad \mathfrak{q} := (7, 1 + 2\sqrt{-5})$$

Class groups

Fundamental Theorem of Arithmetic

Let $\frac{a}{b} \in \mathbb{Q}^\times$. Then there is a **unique** set of (different) primes $p_1, \dots, p_r$ and integers $\alpha_1, \dots, \alpha_r$ such that

$$\frac{a}{b} = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Not true for other number fields

Let K be a number field (i.e., a finite extension of $\mathbb{Q}$) and let $\mathcal{O}_K$ be its ring of (algebraic) integers. There is a notion of prime/irreducible elements in these rings. Every element admits a prime factorisation, but it is not unique.
For example, if $K = \mathbb{Q}(\sqrt{-5})$, then

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$$

Substitute elements for ideals

Every ideal of $\mathcal{O}_K$ admits a unique factorization into prime ideals.

$$\mathfrak{p} := (3, 1 + \sqrt{-5}), \qquad \mathfrak{q} := (7, 1 + 2\sqrt{-5})$$

$$(3) = \mathfrak{p} \cdot \overline{\mathfrak{p}}, \quad (7) = \mathfrak{q} \cdot \overline{\mathfrak{q}}, \quad (1 + 2\sqrt{-5}) = \overline{\mathfrak{p}} \cdot \mathfrak{q}, \quad (1 - 2\sqrt{-5}) = \mathfrak{p} \cdot \overline{\mathfrak{q}}$$

Class groups

Class group

The class group $Cl(K)$ is defined as the quotient

$$Cl(K) := \frac{\mathcal{I}_K}{\mathcal{P}_K}$$

where

- $\mathcal{I}_K$: group of (fractional) ideals of $\mathcal{O}_K$.
- $\mathcal{P}_K$: group of (fractional) principal ideals, i.e., those generated by a single element.

The class number h_K is the cardinality of $Cl(K)$.

Class groups

Class group

The class group $Cl(K)$ is defined as the quotient

$$Cl(K) := \frac{\mathcal{I}_K}{\mathcal{P}_K}$$

where

- $\mathcal{I}_K$: group of (fractional) ideals of $\mathcal{O}_K$.
- $\mathcal{P}_K$: group of (fractional) principal ideals, i.e., those generated by a single element.

The class number h_K is the cardinality of $Cl(K)$.

Theorem (Dirichlet)

For every number field K, the class number h_K is finite, but its actual computation is, in general, a hard problem.

Fermat last theorem

Fermat last theorem (A. Wiles, 1995)

The equation

$$x^n + y^n = z^n$$

has no integral solutions for $n \geq 3$ where $xyz \neq 0$.

Fermat last theorem

Fermat last theorem (A. Wiles, 1995)

The equation

$$x^n + y^n = z^n$$

has no integral solutions for $n \geq 3$ where $xyz \neq 0$.

Pythagorean triples

For $n = 2$, there are infinitely many solutions, corresponding to right triangles whose sides have integer lengths.

Fermat last theorem

Fermat last theorem (A. Wiles, 1995)

The equation

$$x^n + y^n = z^n$$

has no integral solutions for $n \geq 3$ where $xyz \neq 0$.

Pythagorean triples

For $n = 2$, there are infinitely many solutions, corresponding to right triangles whose sides have integer lengths.

Reduction of the problem

It is enough to show the problem for n being

- $n = p$ odd prime.
- $n = 4$: follows from an analysis of the pythagorean triples.

Fermat last theorem

Fermat last theorem (A. Wiles, 1995)

The equation

$$x^n + y^n = z^n$$

has no integral solutions for $n \geq 3$ where $xyz \neq 0$.

Pythagorean triples

For $n = 2$, there are infinitely many solutions, corresponding to right triangles whose sides have integer lengths.

Reduction of the problem

It is enough to show the problem for n being

- $n = p$ odd prime.
- $n = 4$: follows from an analysis of the pythagorean triples.

Indeed, note that the equation is equivalent to

$$\left(x^{n/p}\right)^p + \left(y^{n/p}\right)^p = \left(z^{n/p}\right)^p$$

If there are no solutions for $n = p$, there are no solutions for any multiple of p.

Fermat last theorem

Kummer's approach for $n = p \geq 5$

- Assume w.l.o.g. that x, y, z share no prime factor.
- Factorise the equation using the root of unity $\zeta_p := e^{\frac{2\pi i}{p}}$.

$$x^p + y^p = (x + y) \cdot (x + \zeta_p y) \cdots (x + (\zeta_p)^{p-1} y) = z^p$$

Fermat last theorem

Kummer's approach for $n = p \geq 5$

- Assume w.l.o.g. that x, y, z share no prime factor.
- Factorise the equation using the root of unity $\zeta_p := e^{\frac{2\pi i}{p}}$.

$$x^p + y^p = (x + y) \cdot (x + \zeta_p y) \cdots (x + (\zeta_p)^{p-1} y) = z^p$$

- **If the field $\mathbb{Q}(\zeta_p)$ admits unique factorisation**, it follows that

$$x + \zeta_p y = u\alpha^p \text{ for some } \alpha \in \mathbb{Z}[\zeta_p], u \in \mathbb{Z}[\zeta_p]^\times$$

Fermat last theorem

Kummer's approach for $n = p \geq 5$

- Assume w.l.o.g. that x, y, z share no prime factor.
- Factorise the equation using the root of unity $\zeta_p := e^{\frac{2\pi i}{p}}$.

$$x^p + y^p = (x+y) \cdot (x+\zeta_p y) \cdots (x+(\zeta_p)^{p-1} y) = z^p$$

- **If the field $\mathbb{Q}(\zeta_p)$ admits unique factorisation**, it follows that

$$x + \zeta_p y = u\alpha^p \text{ for some } \alpha \in \mathbb{Z}[\zeta_p], u \in \mathbb{Z}[\zeta_p]^\times$$

- Algebraic computations in $\mathbb{Z}[\zeta_p] \Rightarrow \ p \mid x, y, z \Rightarrow$ contradiction!

Fermat last theorem

Kummer's approach for $n = p \geq 5$

- Assume w.l.o.g. that x, y, z share no prime factor.
- Factorise the equation using the root of unity $\zeta_p := e^{\frac{2\pi i}{p}}$.

$$x^p + y^p = (x+y) \cdot (x+\zeta_p y) \cdots (x+(\zeta_p)^{p-1} y) = z^p$$

- **If the field $\mathbb{Q}(\zeta_p)$ admits unique factorisation**, it follows that

$$x + \zeta_p y = u\alpha^p \text{ for some } \alpha \in \mathbb{Z}[\zeta_p], u \in \mathbb{Z}[\zeta_p]^\times$$

- Algebraic computations in $\mathbb{Z}[\zeta_p] \Rightarrow \ p \mid x, y, z \Rightarrow$ contradiction!
- **Problem**: this argument only works when $h_p := h_{\mathbb{Q}(\zeta_p)} = 1$.

  But that does not hold all primes, being $p = 23$ the smallest prime with $h_p > 1$.

Fermat last theorem

Ideal factorization when $p \nmid h_p$

- Using the uniqueness of the factorization of ideals

$$(x + \zeta_p y) = I^p$$

Fermat last theorem

Ideal factorization when $p \nmid h_p$

- Using the uniqueness of the factorization of ideals

$$(x + \zeta_p y) = I^p$$

- Note that I^p is a principal ideal, so $I^p \equiv 0$ in $Cl(K)$.

Fermat last theorem

Ideal factorization when $p \nmid h_p$

- Using the uniqueness of the factorization of ideals

$$(x + \zeta_p y) = I^p$$

- Note that I^p is a principal ideal, so $I^p \equiv 0$ in $Cl(K)$.
- **Since** $p \nmid h_p$, Lagrange theorem implies that $I \equiv 0$ in $Cl(K)$, so it is generated by some $\alpha \in \mathbb{Z}[\zeta_p]$. This implies that

$$(x + \zeta_p y) = u\alpha^p \text{ for some } u \in \mathbb{Z}[\zeta_p]^\times$$

Fermat last theorem

Ideal factorization when $p \nmid h_p$

- Using the uniqueness of the factorization of ideals

$$(x + \zeta_p y) = I^p$$

- Note that I^p is a principal ideal, so $I^p \equiv 0$ in $Cl(K)$.
- **Since** $p \nmid h_p$, Lagrange theorem implies that $I \equiv 0$ in $Cl(K)$, so it is generated by some $\alpha \in \mathbb{Z}[\zeta_p]$. This implies that

$$(x + \zeta_p y) = u\alpha^p \text{ for some } u \in \mathbb{Z}[\zeta_p]^\times$$

Regular primes

The primes such that $p \nmid h_p$ are called regular primes. Smallest irregular primes are

$$p = 37, 59, 67, 101, 103, 131, \ldots$$

Fermat last theorem

Ideal factorization when $p \nmid h_p$

- Using the uniqueness of the factorization of ideals

$$(x + \zeta_p y) = I^p$$

- Note that I^p is a principal ideal, so $I^p \equiv 0$ in $Cl(K)$.
- **Since** $p \nmid h_p$, Lagrange theorem implies that $I \equiv 0$ in $Cl(K)$, so it is generated by some $\alpha \in \mathbb{Z}[\zeta_p]$. This implies that

$$(x + \zeta_p y) = u\alpha^p \text{ for some } u \in \mathbb{Z}[\zeta_p]^\times$$

Regular primes

The primes such that $p \nmid h_p$ are called regular primes. Smallest irregular primes are

$$p = 37, 59, 67, 101, 103, 131, \ldots$$

General case (A. Wiles, 1995)

The proof uses the modularity theorem, which requires deeper mathematics.

Algebraic Curves

Rational points on algebrtaic curves

Let f be an homogeneous polynomial on 3 variables with coefficients in $\mathbb{Q}$.

$$C(\mathbb{Q}) := \{\mathbf{x} \in \mathbb{P}^2(\mathbb{Q}) : \ f(\mathbf{x}) = 0\}$$

We assume there are not singular points in C.

Algebraic Curves

Rational points on algebrtaic curves

Let f be an homogeneous polynomial on 3 variables with coefficients in $\mathbb{Q}$.

$$C(\mathbb{Q}) := \{\mathbf{x} \in \mathbb{P}^2(\mathbb{Q}) : \ f(\mathbf{x}) = 0\}$$

We assume there are not singular points in C.

Genus

- $g = 0 \rightarrow$ Conics: Either $C(\mathbb{Q}) = \emptyset$ or $C(\mathbb{Q}) \cong \mathbb{Q}$.
- $g = 1 \rightarrow$ Elliptic curves: our case of interest.
- $g > 1 \rightarrow C(\mathbb{Q})$ is finite (Faltings), but difficult to compute

Algebraic Curves

Rational points on algebrtaic curves

Let f be an homogeneous polynomial on 3 variables with coefficients in $\mathbb{Q}$.

$$C(\mathbb{Q}) := \{\mathbf{x} \in \mathbb{P}^2(\mathbb{Q}) : \ f(\mathbf{x}) = 0\}$$

We assume there are not singular points in C.

Genus

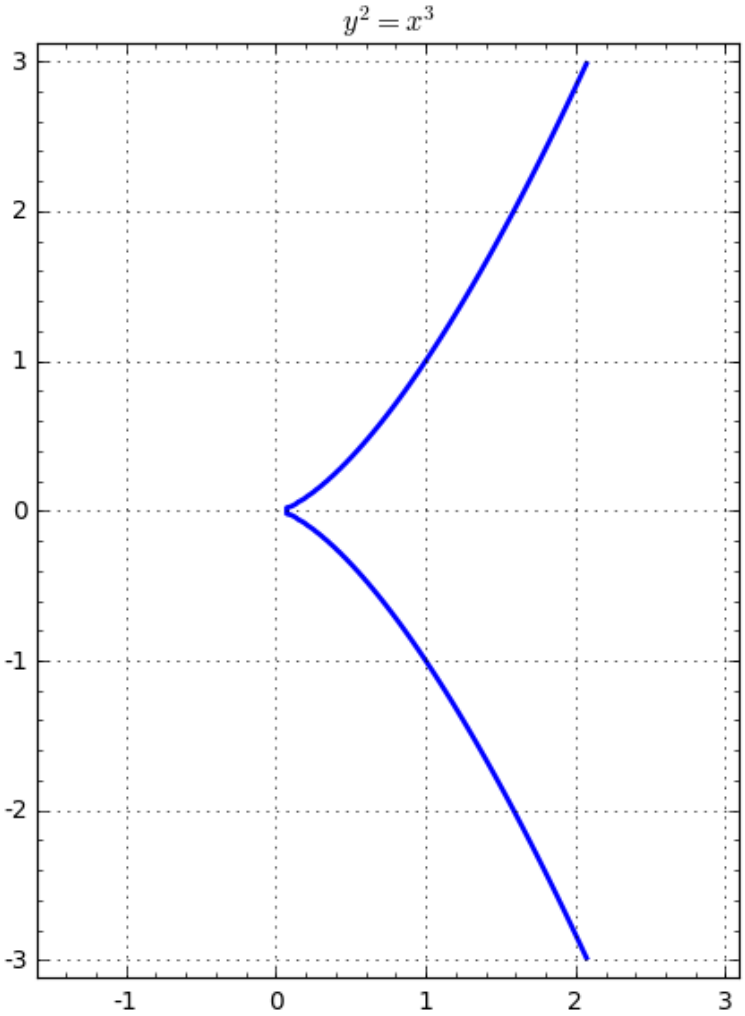
- $g = 0 \to$ Conics: Either $C(\mathbb{Q}) = \emptyset$ or $C(\mathbb{Q}) \cong \mathbb{Q}$.
- $g = 1 \to$ Elliptic curves: our case of interest.
- $g > 1 \to C(\mathbb{Q})$ is finite (Faltings), but difficult to compute

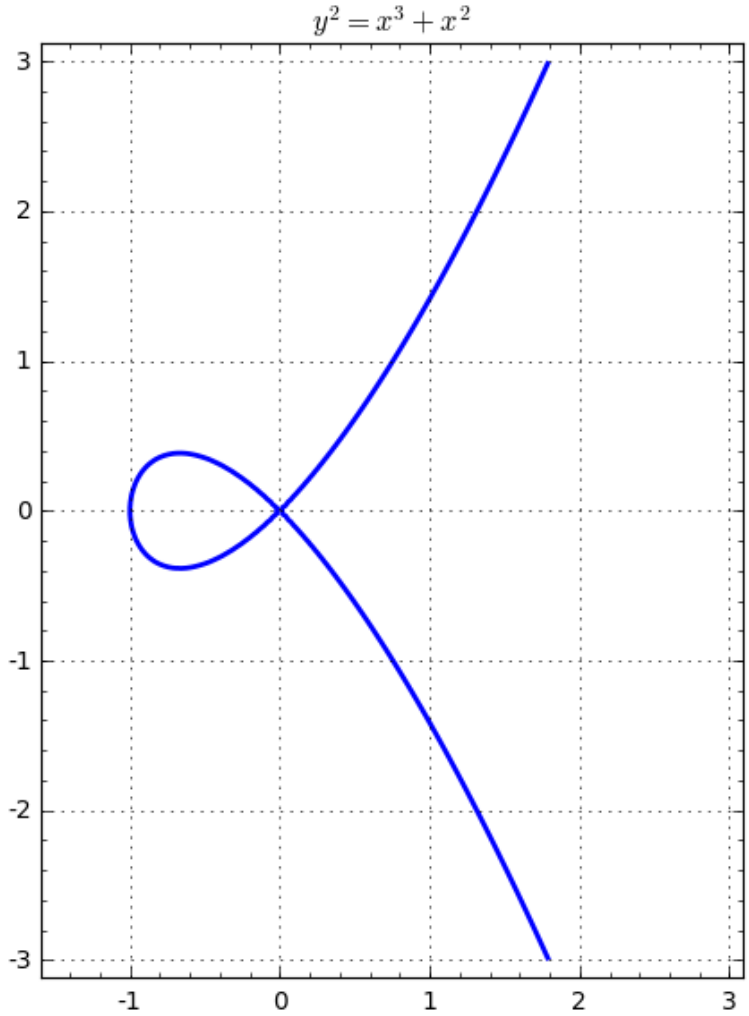
Elliptic curves

Using an algebraic transformation, we can assume that every elliptic curve is defined by an equation of the form

$$E : \ y^2 = x^3 + Ax + B, \ A, B \in \mathbb{Z}, \ 4a^3 + 27b^2 \neq 0$$

Singular elliptic curves





Local-global principle

Completions of the rationals

- The possible norms that can be defined on $\mathbb{Q}$ are the absolute value and the p-adic norms for every prime p.

$$\|\alpha\|_\infty = |\alpha|, \qquad \|\alpha\|_p = \frac{1}{p^{v_p(\alpha)}}$$

Local-global principle

Completions of the rationals

- The possible norms that can be defined on $\mathbb{Q}$ are the absolute value and the p-adic norms for every prime p.

$$\|\alpha\|_\infty = |\alpha|, \qquad \|\alpha\|_p = \frac{1}{p^{v_p(\alpha)}}$$

- Completing these norms leads to the real numbers $\mathbb{R}$ and the p-adic nubmers $\mathbb{Q}_p$.

Local-global principle

Completions of the rationals

- The possible norms that can be defined on $\mathbb{Q}$ are the absolute value and the p-adic norms for every prime p.

$$\|\alpha\|_\infty = |\alpha|, \qquad \|\alpha\|_p = \frac{1}{p^{v_p(\alpha)}}$$

- Completing these norms leads to the real numbers $\mathbb{R}$ and the p-adic nubmers $\mathbb{Q}_p$.
- Since $\mathbb{Q} \subset \mathbb{Q}_p$, then $C(\mathbb{Q}) \subset C(\mathbb{Q}_p)$.

Local-global principle

Completions of the rationals

- The possible norms that can be defined on $\mathbb{Q}$ are the absolute value and the p-adic norms for every prime p.

$$\|\alpha\|_\infty = |\alpha|, \qquad \|\alpha\|_p = \frac{1}{p^{v_p(\alpha)}}$$

- Completing these norms leads to the real numbers $\mathbb{R}$ and the p-adic nubmers $\mathbb{Q}_p$.
- Since $\mathbb{Q} \subset \mathbb{Q}_p$, then $C(\mathbb{Q}) \subset C(\mathbb{Q}_p)$.
- Computing $C(\mathbb{Q}_p)$ is easier that computing $C(\mathbb{Q})$.

Local-global principle

Completions of the rationals

- The possible norms that can be defined on $\mathbb{Q}$ are the absolute value and the p-adic norms for every prime p.

$$\|\alpha\|_\infty = |\alpha|, \qquad \|\alpha\|_p = \frac{1}{p^{v_p(\alpha)}}$$

- Completing these norms leads to the real numbers $\mathbb{R}$ and the p-adic nubmers $\mathbb{Q}_p$.
- Since $\mathbb{Q} \subset \mathbb{Q}_p$, then $C(\mathbb{Q}) \subset C(\mathbb{Q}_p)$.
- Computing $C(\mathbb{Q}_p)$ is easier that computing $C(\mathbb{Q})$.

Hasse principle

If C is a conic, then

$$C(\mathbb{Q}) \neq \emptyset \Leftrightarrow \left[C(\mathbb{R}) \neq \emptyset \text{ and } C(\mathbb{Q}_p) \neq \emptyset \ \forall p \text{ prime} \right]$$

Local-global principle

Completions of the rationals

- The possible norms that can be defined on $\mathbb{Q}$ are the absolute value and the p-adic norms for every prime p.

$$\|\alpha\|_\infty = |\alpha|, \qquad \|\alpha\|_p = \frac{1}{p^{v_p(\alpha)}}$$

- Completing these norms leads to the real numbers $\mathbb{R}$ and the p-adic nubmers $\mathbb{Q}_p$.
- Since $\mathbb{Q} \subset \mathbb{Q}_p$, then $C(\mathbb{Q}) \subset C(\mathbb{Q}_p)$.
- Computing $C(\mathbb{Q}_p)$ is easier that computing $C(\mathbb{Q})$.

Hasse principle

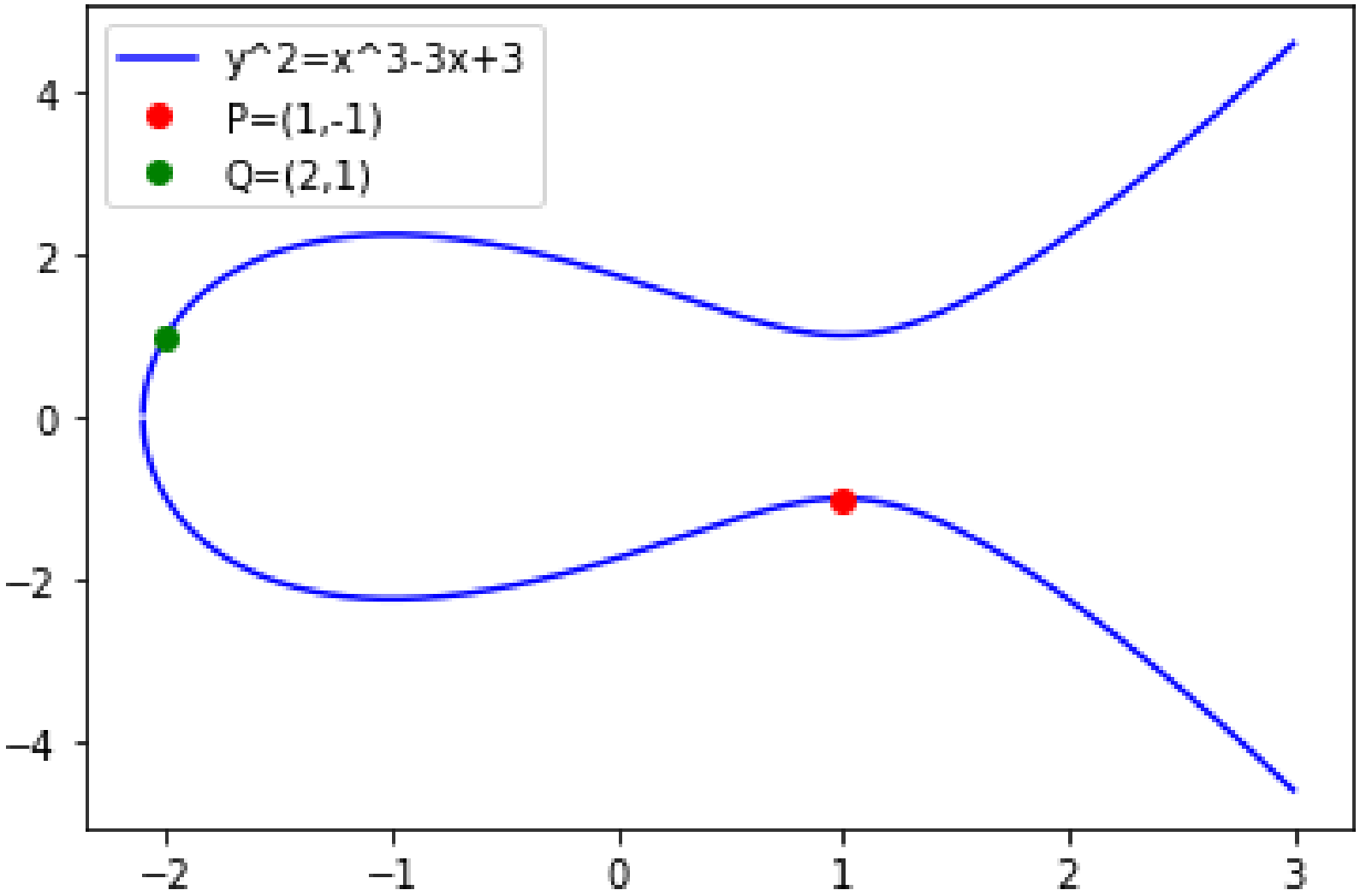
If C is a conic, then

$$C(\mathbb{Q}) \neq \emptyset \Leftrightarrow \left[C(\mathbb{R}) \neq \emptyset \text{ and } C(\mathbb{Q}_p) \neq \emptyset \ \forall p \text{ prime} \right]$$

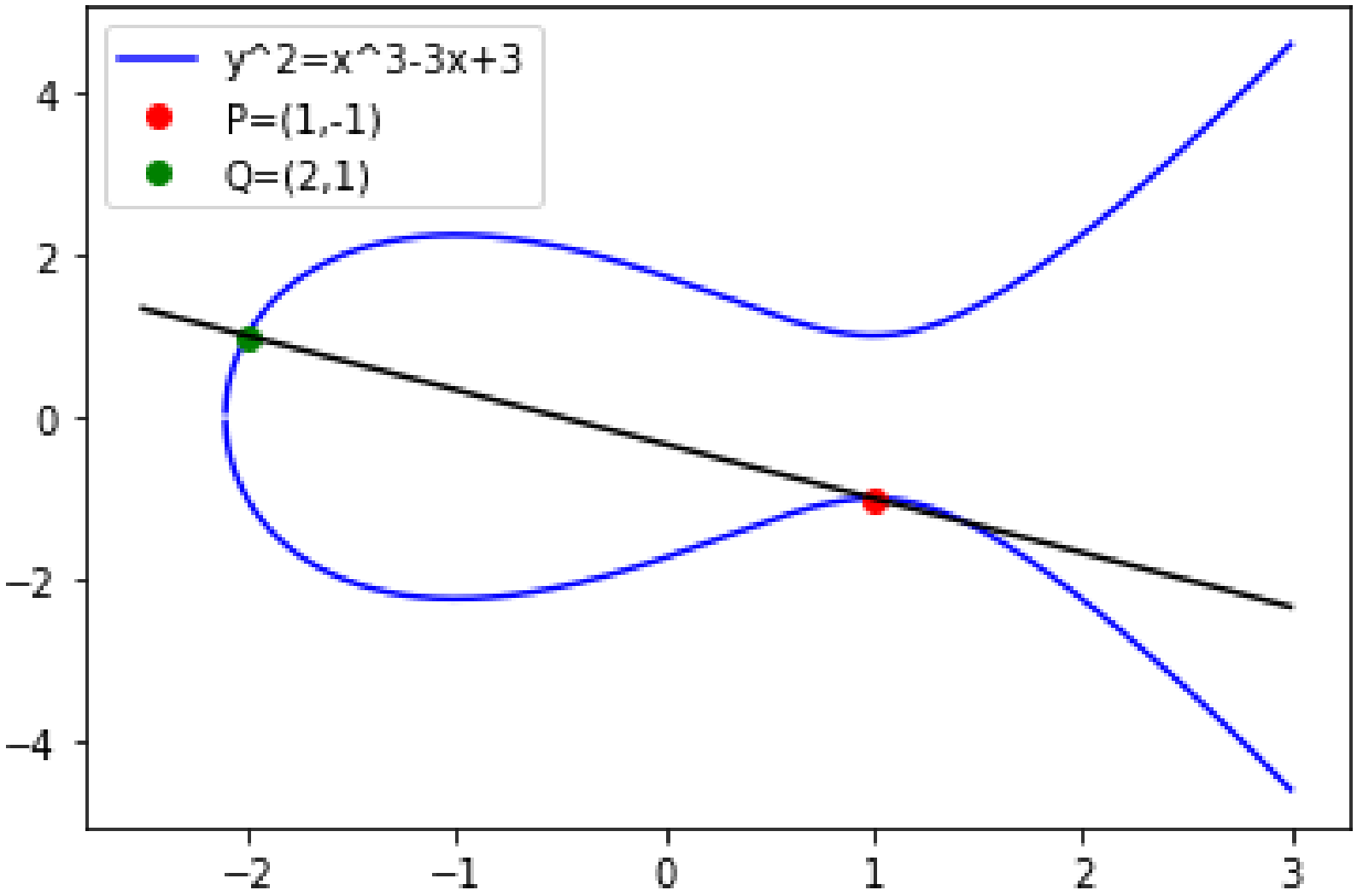
Elliptic curves

Hasse principle does not hold for elliptic curve. The failure of this principle is defined by the Tate-Shafarevich group.

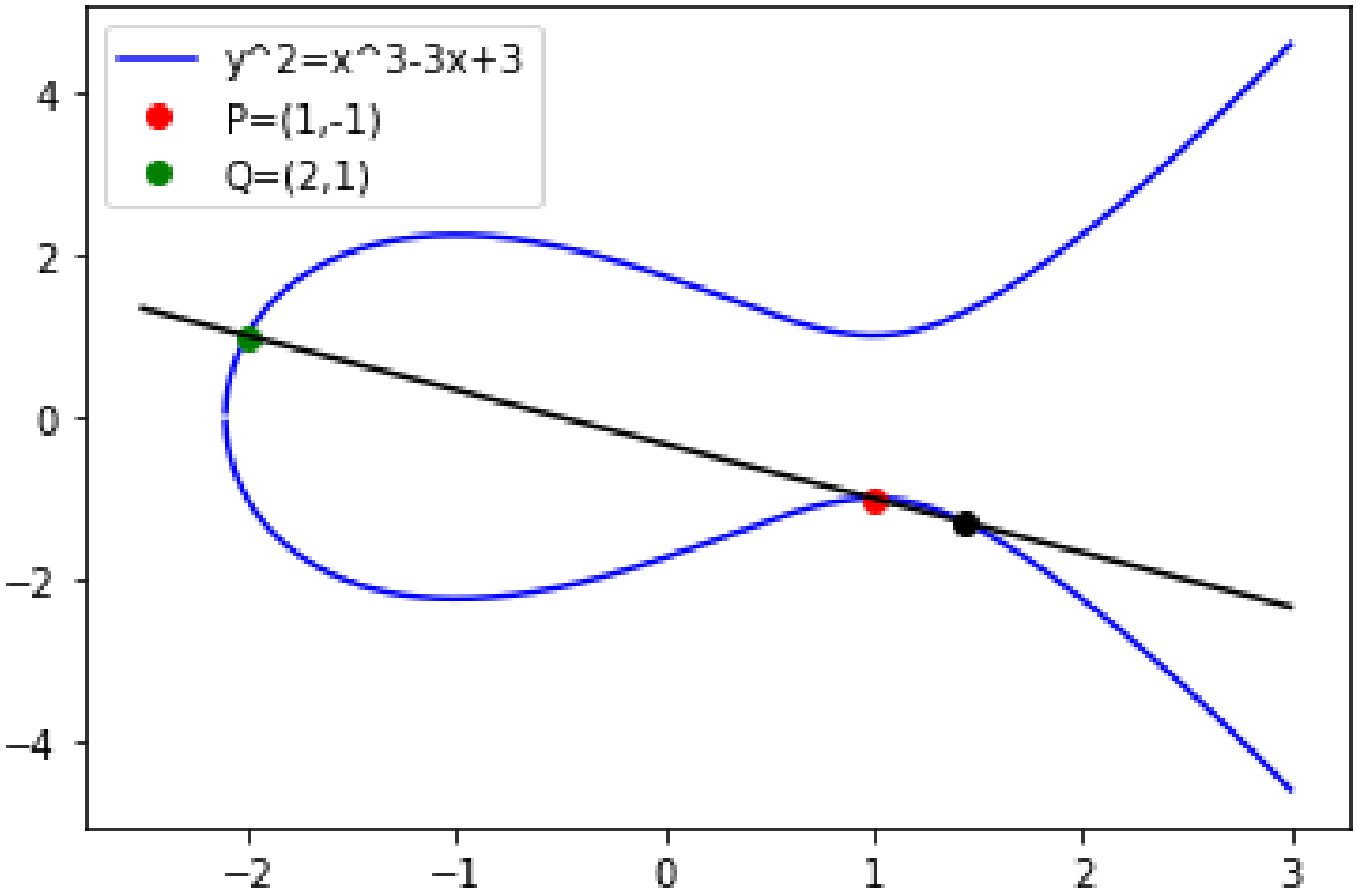
Adding points on an elliptic curve



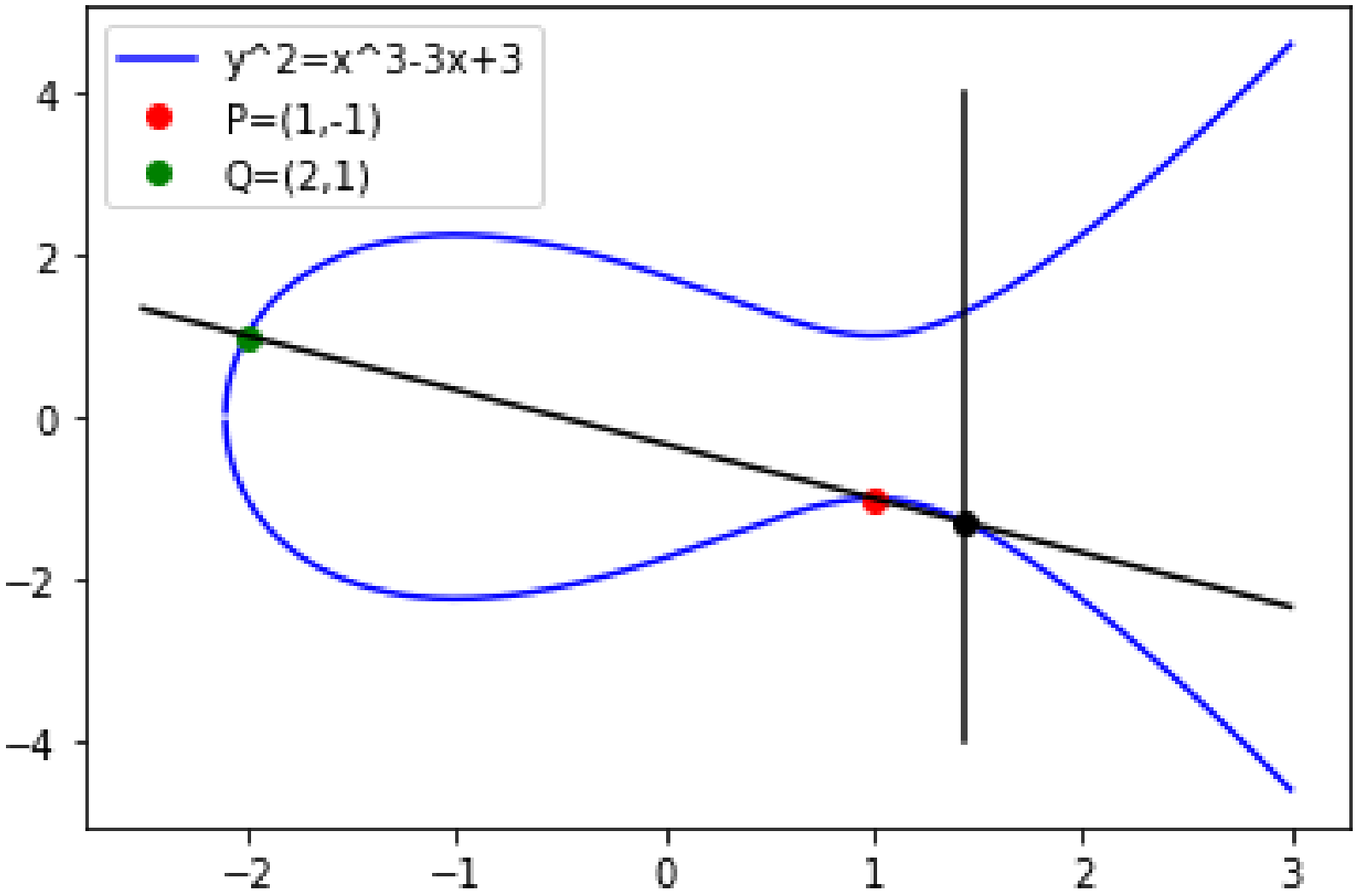
Adding points on an elliptic curve



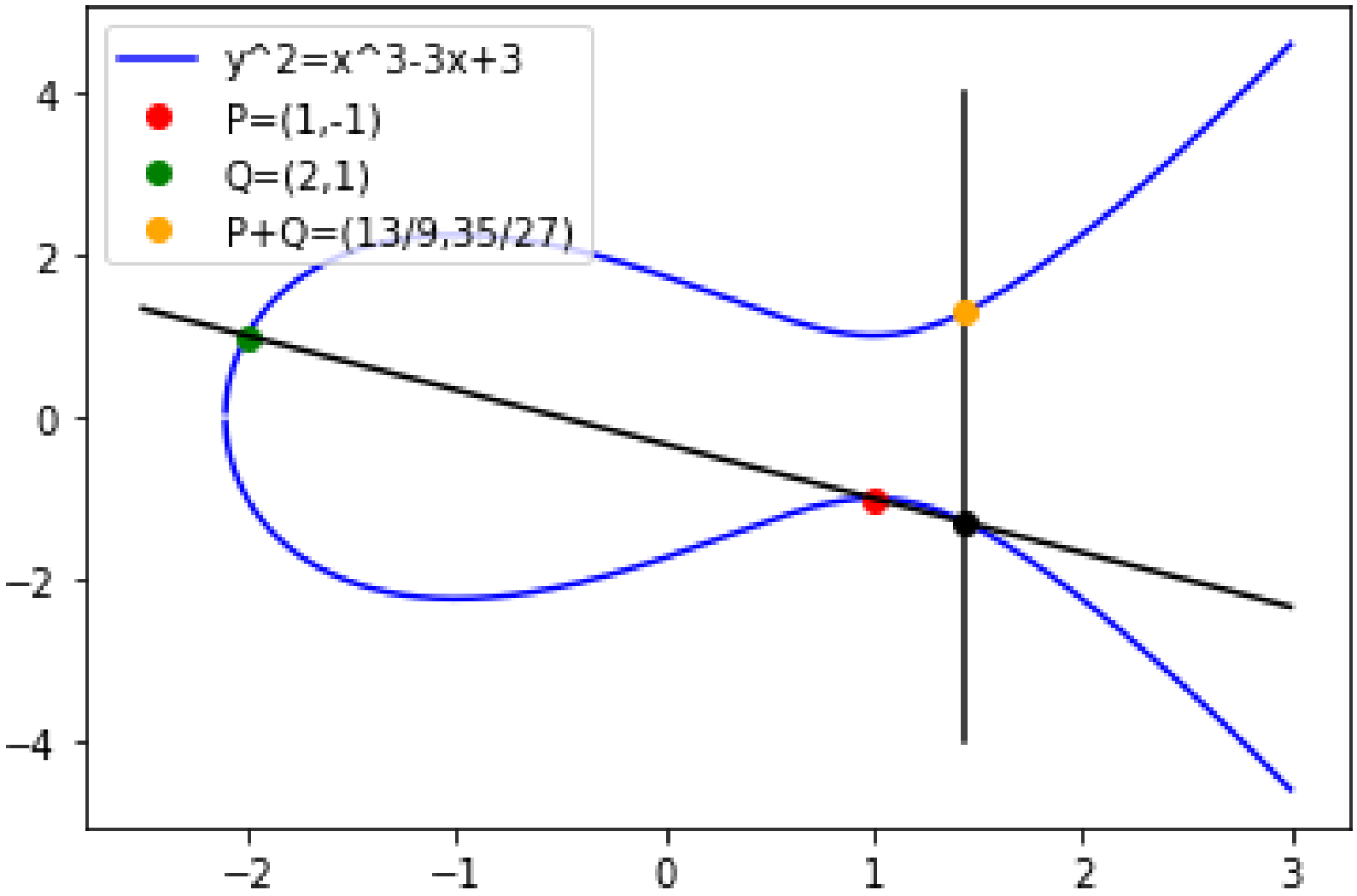
Adding points on an elliptic curve



Adding points on an elliptic curve



Adding points on an elliptic curve



Group strtucture

Abelian group structure

The set of points $E(\mathbb{Q})$ is an abelian group.

Group strtucture

Abelian group structure

The set of points $E(\mathbb{Q})$ is an abelian group.

Mordell-Weil Theorem

$E(\mathbb{Q})$ is a finitely generated abelian group.

Group strtucture

Abelian group structure

The set of points $E(\mathbb{Q})$ is an abelian group.

Mordell-Weil Theorem

$E(\mathbb{Q})$ is a finitely generated abelian group.

Structure

We have that $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$, where

- $E(\mathbb{Q})_{\text{tors}}$: torsion points $\rightarrow$ points of finite order such that

$$[n]P = \underbrace{P + \cdots + P}_{n \text{ times}} = O$$

(T is a finite group, easy to compute)

Group strtucture

Abelian group structure

The set of points $E(\mathbb{Q})$ is an abelian group.

Mordell-Weil Theorem

$E(\mathbb{Q})$ is a finitely generated abelian group.

Structure

We have that $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$, where

- $E(\mathbb{Q})_{\text{tors}}$: torsion points $\rightarrow$ points of finite order such that

$$[n]P = \underbrace{P + \cdots + P}_{n \text{ times}} = O$$

  (T is a finite group, easy to compute)
- $\{P_1, \ldots, P_r\}$ set of points that generates the remaining of $E(\mathbb{Q})$.

Rank

r is called the rank of E. We know it is finite, but it is hard to compute.

Galois cohomology inerpretation

Fix a natural number m and let $\overline{\mathbb{Q}}$ be the algebraic closure of the rationals.

Torsion points

$E[m]$ are points $Q \in E(\overline{\mathbb{Q}})$ such that $[m]Q = O$. There are exactly m^2 of those points.

Galois cohomology inerpretation

Fix a natural number m and let $\overline{\mathbb{Q}}$ be the algebraic closure of the rationals.

Torsion points

$E[m]$ are points $Q \in E(\overline{\mathbb{Q}})$ such that $[m]Q = O$. There are exactly m^2 of those points.

Kummer map

The Galois cohomology exact sequence produces an inclusion

$$E(\mathbb{Q})/mE(\mathbb{Q}) \overset{\kappa}{\hookrightarrow} H^1(\mathbb{Q}, E[m])$$

Galois cohomology inerpretation

Fix a natural number m and let $\overline{\mathbb{Q}}$ be the algebraic closure of the rationals.

Torsion points

$E[m]$ are points $Q \in E(\overline{\mathbb{Q}})$ such that $[m]Q = O$. There are exactly m^2 of those points.

Kummer map

The Galois cohomology exact sequence produces an inclusion

$$E(\mathbb{Q})/mE(\mathbb{Q}) \overset{\kappa}{\hookrightarrow} H^1(\mathbb{Q}, E[m])$$

We can do the same for every completion $\mathbb{Q}_\ell$:

Commutative diagram

$$\begin{array}{ccc} E(\mathbb{Q})/mE(\mathbb{Q}) & \xrightarrow{\kappa} & H^1(\mathbb{Q}, E[m]) \\ \downarrow \subset & & \downarrow \mathrm{loc}_\ell \\ E(\mathbb{Q}_\ell)/mE(\mathbb{Q}_\ell) & \xrightarrow{\kappa_\ell} & H^1(\mathbb{Q}_\ell, E[m]) \end{array}$$

Selmer group

Commutative diagram

$$\begin{array}{ccc} E(\mathbb{Q})/mE(\mathbb{Q}) & \xrightarrow{\kappa} & H^1(\mathbb{Q}, E[m]) \\ \downarrow \subset & & \downarrow \mathrm{loc}_\ell \\ E(\mathbb{Q}_\ell)/mE(\mathbb{Q}_\ell) & \xrightarrow{\kappa_\ell} & H^1(\mathbb{Q}_\ell, E[m]) \end{array}$$

Selmer group

$$\mathrm{Sel}(\mathbb{Q}, E[m]) := \bigcap_{\ell \text{ prime}} \mathrm{loc}_\ell^{-1}\left(\kappa_\ell\left(E(\mathbb{Q}_\ell)/mE(\mathbb{Q}_\ell)\right)\right)$$

Absolute Selmer group

Absolute Selmer group

We can make this construction considering all natural numbers m at the same time:

$$\mathrm{Sel}(\mathbb{Q}, E_{\mathrm{tors}}) = \bigcup_{m=1}^{\infty} \mathrm{Sel}(\mathbb{Q}, E[m]) \subset H^1(\mathbb{Q}, E_{\mathrm{tors}}(\overline{\mathbb{Q}}))$$

Absolute Selmer group

Absolute Selmer group

We can make this construction considering all natural numbers m at the same time:

$$\mathrm{Sel}(\mathbb{Q}, E_{\mathrm{tors}}) = \bigcup_{m=1}^{\infty} \mathrm{Sel}(\mathbb{Q}, E[m]) \subset H^1(\mathbb{Q}, E_{\mathrm{tors}}(\overline{\mathbb{Q}}))$$

Short exact sequence

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathrm{Sel}(\mathbb{Q}, E_{\mathrm{tors}}) \twoheadrightarrow Ш(E/\mathbb{Q}) \to 0$$

where $Ш(E/\mathbb{Q})$ is the Tate-Shafarevich group, conjecturally a finite group.

Absolute Selmer group

Absolute Selmer group

We can make this construction considering all natural numbers m at the same time:

$$\mathrm{Sel}(\mathbb{Q}, E_{\mathrm{tors}}) = \bigcup_{m=1}^{\infty} \mathrm{Sel}(\mathbb{Q}, E[m]) \subset H^1(\mathbb{Q}, E_{\mathrm{tors}}(\overline{\mathbb{Q}}))$$

Short exact sequence

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathrm{Sel}(\mathbb{Q}, E_{\mathrm{tors}}) \twoheadrightarrow Ш(E/\mathbb{Q}) \to 0$$

where $Ш(E/\mathbb{Q})$ is the Tate-Shafarevich group, conjecturally a finite group. Then

$$E(\mathbb{Q}) \otimes \mathbb{Q}/\mathbb{Z} \cong (\mathbb{Q}/\mathbb{Z})^r \Rightarrow \mathrm{Sel}(\mathbb{Q}, E_{\mathrm{tors}}) \cong (\mathbb{Q}/\mathbb{Z})^r \times Ш(E/\mathbb{Q})$$

Absolute p-Selmer group

Absolute p-Selmer group

Fix a prime number p

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) := \bigcup_{k=1}^{\infty} \mathrm{Sel}(\mathbb{Q}, E[p^k])$$

Absolute p-Selmer group

Absolute p-Selmer group

Fix a prime number p

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) := \bigcup_{k=1}^{\infty} \mathrm{Sel}(\mathbb{Q}, E[p^k])$$

Bound on the rank

The absolute p-Selmer group also bounds the rank

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r \times Ш(E/\mathbb{Q})[p^\infty]$$

Absolute p-Selmer group

Absolute p-Selmer group

Fix a prime number p

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) := \bigcup_{k=1}^{\infty} \mathrm{Sel}(\mathbb{Q}, E[p^k])$$

Bound on the rank

The absolute p-Selmer group also bounds the rank

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r \times Ш(E/\mathbb{Q})[p^\infty]$$

Canonical split

The absolute Selmer group can be computed as

$$\mathrm{Sel}(\mathbb{Q}, E_{\mathrm{tors}}) = \prod_{p \text{ prime}} \mathrm{Sel}(\mathbb{Q}, E[p^\infty])$$

Galois representation

Generalisation

The construction of Selmer groups is not exclusive from elliptic curves, but can be obtained from every Galois representation.

Galois representation

Generalisation

The construction of Selmer groups is not exclusive from elliptic curves, but can be obtained from every Galois representation.

Galois representation

A Galois representation is a group T endowed with an action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, where K is a number field.

Galois representation

Generalisation

The construction of Selmer groups is not exclusive from elliptic curves, but can be obtained from every Galois representation.

Galois representation

A Galois representation is a group T endowed with an action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, where K is a number field.

Key idea

A Selmer group is the subgroup of the global Galois cohomology group cut out by some local conditions.

Galois representation

Generalisation

The construction of Selmer groups is not exclusive from elliptic curves, but can be obtained from every Galois representation.

Galois representation

A Galois representation is a group T endowed with an action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, where K is a number field.

Key idea

A Selmer group is the subgroup of the global Galois cohomology group cut out by some local conditions.

Class groups

The class group of a number field can be computed from the Selmer group of $\mathbb{Q}/\mathbb{Z}$ with trivial Galois action. By class field theory,

$$\mathrm{Sel}(K, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Cl}(K)$$

L-functions

Definition

They can be defined for every (p-adic) Galois representation. They can be constructed as an infinite product

$$L: \ \mathbb{C} \to \mathbb{C}, \ s \mapsto \prod_{\ell \text{ prime}} \mathrm{Eul}_\ell(s)$$

where $\mathrm{Eul}_\ell(s)$ is an Euler factor, defined from the local restriction of the Galois representation.

L-functions

Definition

They can be defined for every (p-adic) Galois representation. They can be constructed as an infinite product

$$L: \mathbb{C} \to \mathbb{C}, \ s \mapsto \prod_{\ell \text{ prime}} \mathrm{Eul}_\ell(s)$$

where $\mathrm{Eul}_\ell(s)$ is an Euler factor, defined from the local restriction of the Galois representation.

Properties

- This product converges absolutely when $\Re(s) \gg 0$.
- In some cases of interest, it can be meromorphically extended to all $\mathbb{C}$.

Example of L-functions

Riemann zeta function

It is obtained from the roots of unity, working over $\mathbb{Q}$.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\ell \text{ prime}} \frac{1}{1-\ell^{-s}}, \quad \Re(s) > 1$$

Example of L-functions

Riemann zeta function

It is obtained from the roots of unity, working over $\mathbb{Q}$.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\ell \text{ prime}} \frac{1}{1-\ell^{-s}}, \quad \Re(s) > 1$$

Dedekind zeta functions

We can generalise this construction to number fields

$$\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \frac{1}{\left(\#(\mathcal{O}_K/I)\right)^{-s}} = \sum_{\mathfrak{p} \text{ prime}} \frac{1}{1-\left(\#(\mathcal{O}_K/p)\right)^{-s}}, \quad \Re(s) > 1$$

Example of L-functions

Riemann zeta function

It is obtained from the roots of unity, working over $\mathbb{Q}$.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\ell \text{ prime}} \frac{1}{1-\ell^{-s}}, \quad \Re(s) > 1$$

Dedekind zeta functions

We can generalise this construction to number fields

$$\zeta_K(s) = \sum_{I \subset \mathcal{O}_K} \frac{1}{\left(\#(\mathcal{O}_K/I)\right)^{-s}} = \sum_{\mathfrak{p} \text{ prime}} \frac{1}{1-\left(\#(\mathcal{O}_K/p)\right)^{-s}}, \quad \Re(s) > 1$$

L-function of an elliptic curve

$$L(E,s) = \prod_{\ell \text{ prime}} \frac{1}{1-a_\ell \ell^{-s} + \ell^{1-2s}}, \quad \Re(s) > 3/2$$

where a_ℓ is defined as:

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

Special values

Special values

The behaviour of the L-function around $s = 1$ has arithmetic consequences.

Special values

Special values

The behaviour of the L-function around $s = 1$ has arithmetic consequences.

Analytic class number formula (Dirichlet, Dedekind)

$\zeta_K(s)$ has a pole at $s = 1$ and the residue

$$\mathrm{Res}_{s=1}\zeta_K = \left(\frac{2^{r_1}2\pi^{r_2}R_K}{\omega_K\sqrt{|\Delta_K|}}\right) h_k$$

Special values

Special values

The behaviour of the L-function around $s = 1$ has arithmetic consequences.

Analytic class number formula (Dirichlet, Dedekind)

$\zeta_K(s)$ has a pole at $s = 1$ and the residue

$$\mathrm{Res}_{s=1}\zeta_K = \left(\frac{2^{r_1}2\pi^{r_2}R_K}{\omega_K\sqrt{|\Delta_K|}}\right) h_k$$

Birch and Swinnerton-Dyer conjecture (BSD)

- $\mathrm{ord}_{s=1}L(E,s) = \mathrm{rank}(E(\mathbb{Q}))$

Special values

Special values

The behaviour of the L-function around $s = 1$ has arithmetic consequences.

Analytic class number formula (Dirichlet, Dedekind)

$\zeta_K(s)$ has a pole at $s = 1$ and the residue

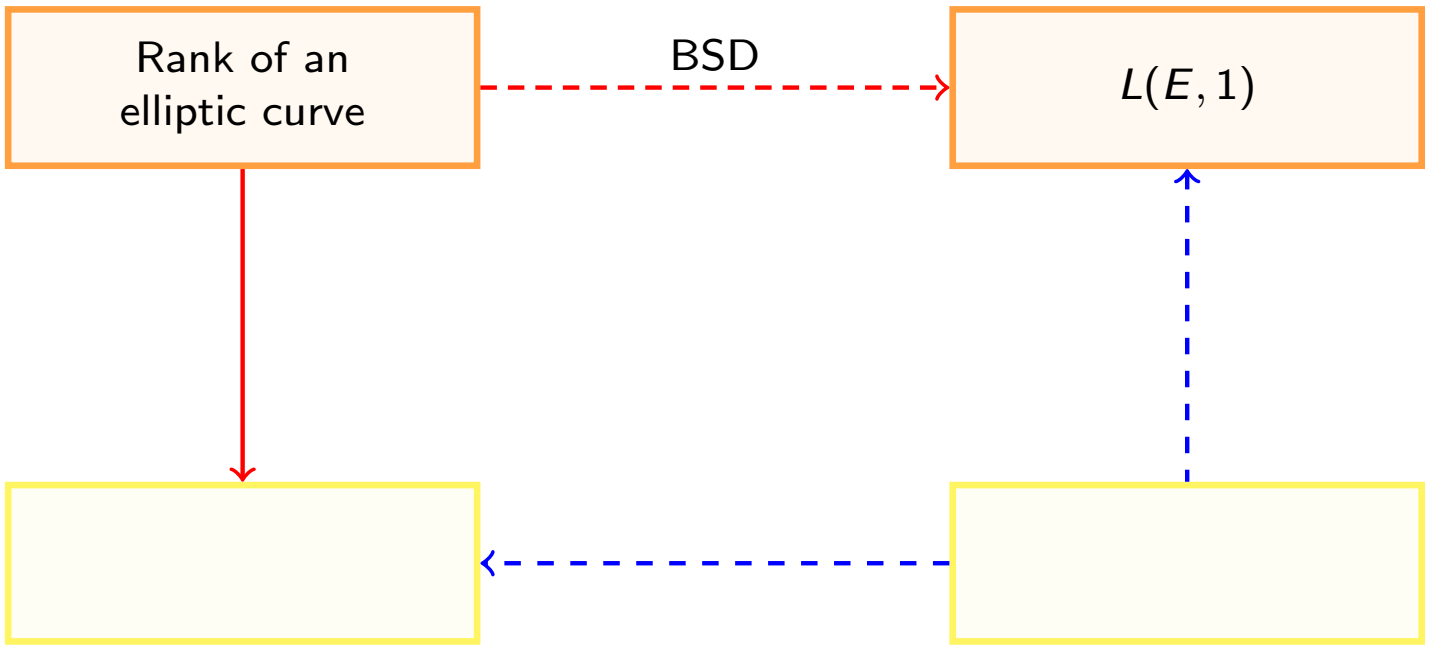
$$\mathrm{Res}_{s=1}\zeta_K = \left(\frac{2^{r_1}2\pi^{r_2}R_K}{\omega_K\sqrt{|\Delta_K|}}\right) h_k$$

Birch and Swinnerton-Dyer conjecture (BSD)

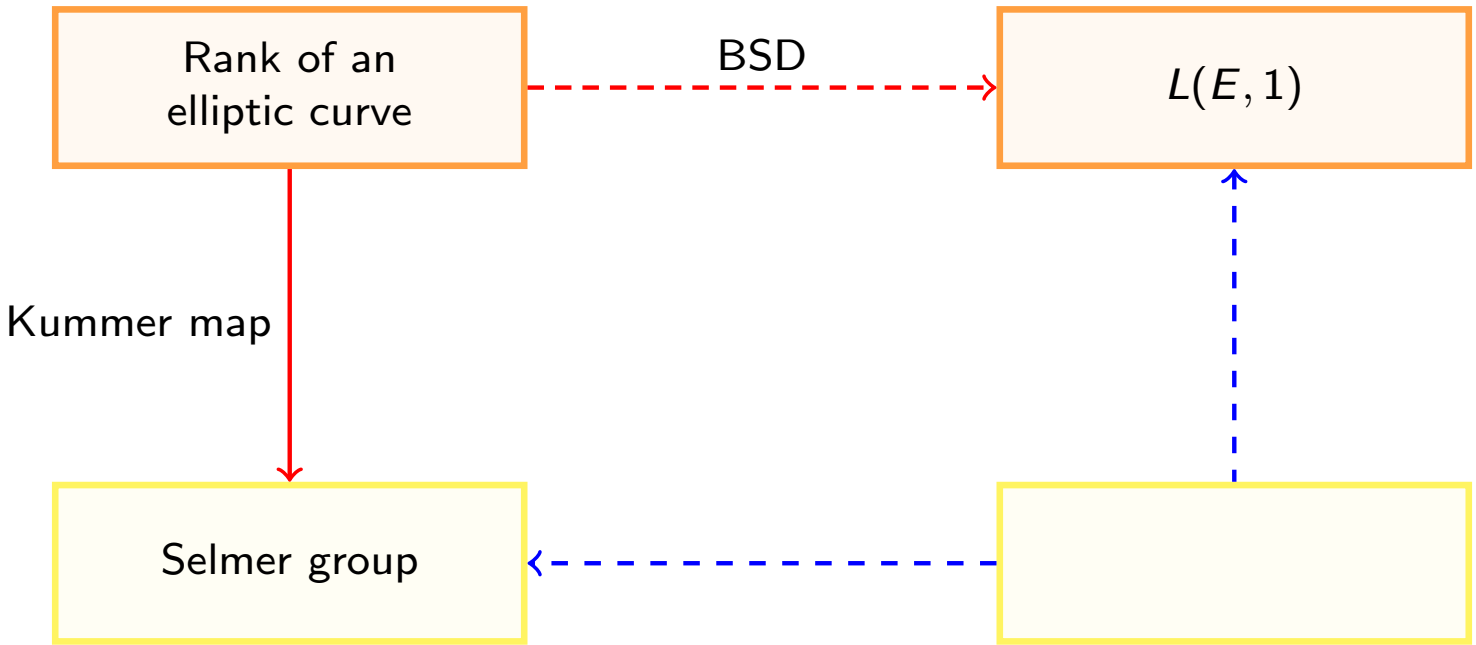
- $\mathrm{ord}_{s=1}L(E,s) = \mathrm{rank}(E(\mathbb{Q}))$
- The first non-zero term of the Taylor expansion of $L(E,s)$ at $s = 1$ has an arithmetic interpretation.

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot R_E \cdot \#Ш(E/\mathbb{Q}) \cdot \mathrm{Tam}(E)}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}$$

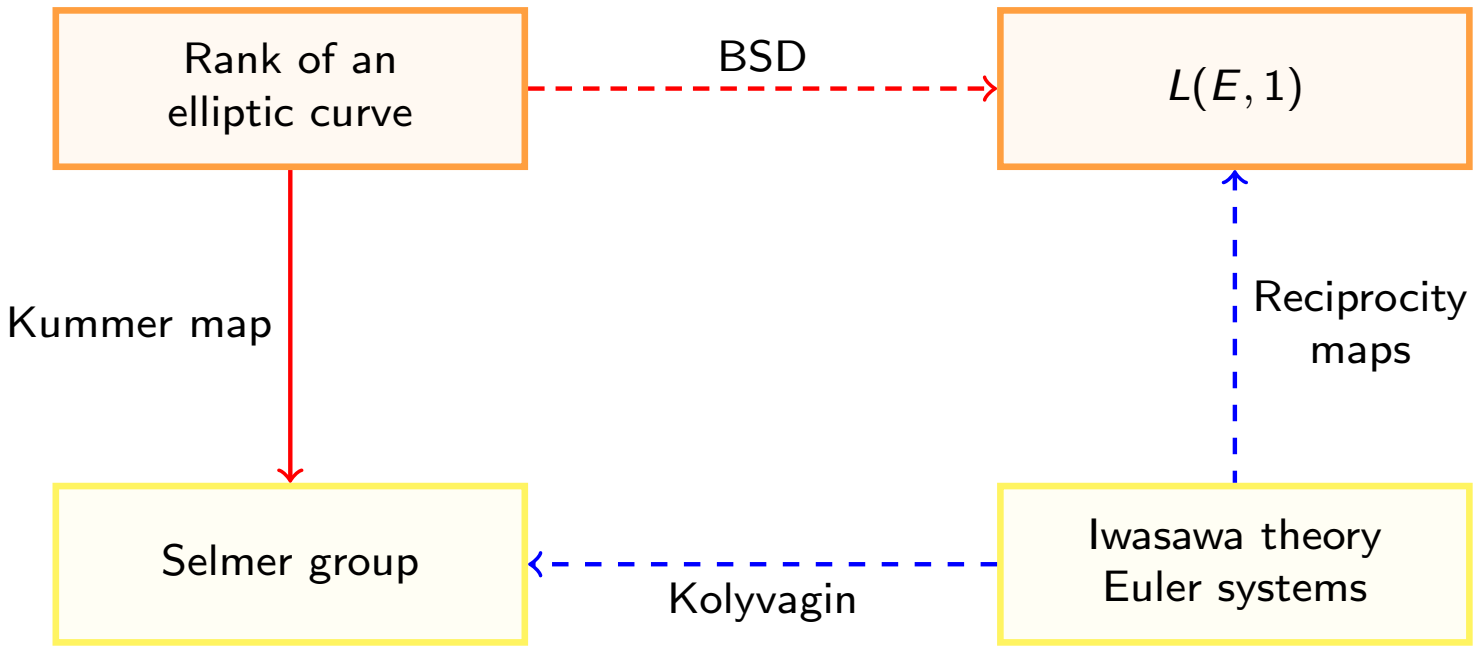
Strategy for BSD



Strategy for BSD



Strategy for BSD



Iwasawa theory

Idea of Iwasawa

Instead of studying $E(\mathbb{Q})$, it is easier to study $E(\mathbb{Q}_\infty)$, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension.

Iwasawa theory

Idea of Iwasawa

Instead of studying $E(\mathbb{Q})$, it is easier to study $E(\mathbb{Q}_\infty)$, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension.

Cyclotomic $\mathbb{Z}_p$-extension

- Consider the field $\mathbb{Q}(\zeta_{p^{n+1}})$, where $\zeta_{p^{n+1}} = e^{\frac{2\pi i}{p^{n+1}}}$.

Iwasawa theory

Idea of Iwasawa

Instead of studying $E(\mathbb{Q})$, it is easier to study $E(\mathbb{Q}_\infty)$, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension.

Cyclotomic $\mathbb{Z}_p$-extension

- Consider the field $\mathbb{Q}(\zeta_{p^{n+1}})$, where $\zeta_{p^{n+1}} = e^{\frac{2\pi i}{p^{n+1}}}$.
- $\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}\right) \cong \left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^\times \cong (\mathbb{Z}/p-1) \times (\mathbb{Z}/p^n\mathbb{Z})$.

Iwasawa theory

Idea of Iwasawa

Instead of studying $E(\mathbb{Q})$, it is easier to study $E(\mathbb{Q}_\infty)$, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension.

Cyclotomic $\mathbb{Z}_p$-extension

- Consider the field $\mathbb{Q}(\zeta_{p^{n+1}})$, where $\zeta_{p^{n+1}} = e^{\frac{2\pi i}{p^{n+1}}}$.
- $\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}\right) \cong \left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^\times \cong (\mathbb{Z}/p-1) \times (\mathbb{Z}/p^n\mathbb{Z})$.
- By Galois correspondence, there is a unique extension $\mathbb{Q}_n$ of degree p^n contained in $\mathbb{Q}(\zeta_{p^{n+1}})$.

Iwasawa theory

Idea of Iwasawa

Instead of studying $E(\mathbb{Q})$, it is easier to study $E(\mathbb{Q}_\infty)$, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension.

Cyclotomic $\mathbb{Z}_p$-extension

- Consider the field $\mathbb{Q}(\zeta_{p^{n+1}})$, where $\zeta_{p^{n+1}} = e^{\frac{2\pi i}{p^{n+1}}}$.
- $\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}\right) \cong \left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^\times \cong (\mathbb{Z}/p-1) \times (\mathbb{Z}/p^n\mathbb{Z})$.
- By Galois correspondence, there is a unique extension $\mathbb{Q}_n$ of degree p^n contained in $\mathbb{Q}(\zeta_{p^{n+1}})$.
- $\mathbb{Q}_\infty := \bigcup_{n=1}^{\infty} \mathbb{Q}_n \Rightarrow \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$.

Iwasawa theory

Idea of Iwasawa

Instead of studying $E(\mathbb{Q})$, it is easier to study $E(\mathbb{Q}_\infty)$, where $\mathbb{Q}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension.

Cyclotomic $\mathbb{Z}_p$-extension

- Consider the field $\mathbb{Q}(\zeta_{p^{n+1}})$, where $\zeta_{p^{n+1}} = e^{\frac{2\pi i}{p^{n+1}}}$.
- $\mathrm{Gal}\left(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}\right) \cong \left(\mathbb{Z}/p^{n+1}\mathbb{Z}\right)^\times \cong (\mathbb{Z}/p-1) \times (\mathbb{Z}/p^n\mathbb{Z})$.
- By Galois correspondence, there is a unique extension $\mathbb{Q}_n$ of degree p^n contained in $\mathbb{Q}(\zeta_{p^{n+1}})$.
- $\mathbb{Q}_\infty := \bigcup_{n=1}^{\infty} \mathbb{Q}_n \Rightarrow \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$.

Structure of the rational points

- $E(\mathbb{Q}_\infty)$ is a module over the Iwasawa algebra $\Lambda := \mathbb{Z}_p[[T]]$.
- Modules over this ring behave nicely: there is a structure theorem describing them (up to finite index).

Euler systems

Euler systems

Let T be a p-adic representation. An Euler system is a collection

$$\mathbf{c} = \{c_n \in H^1(\mathbb{Q}(\zeta_n), T) : \ n \in \mathbb{N}\}$$

satisfying norm-compatibilty relations, defined using Euler factors.

Euler systems

Euler systems

Let T be a p-adic representation. An Euler system is a collection

$$\mathbf{c} = \{c_n \in H^1(\mathbb{Q}(\zeta_n), T) : \ n \in \mathbb{N}\}$$

satisfying norm-compatibilty relations, defined using Euler factors.

Examples

- Cyclotomic units (Thaine, 1988) $\rightarrow$ class groups.

Euler systems

Euler systems

Let T be a p-adic representation. An Euler system is a collection

$$\mathbf{c} = \{c_n \in H^1(\mathbb{Q}(\zeta_n), T) : \ n \in \mathbb{N}\}$$

satisfying norm-compatibilty relations, defined using Euler factors.

Examples

- Cyclotomic units (Thaine, 1988) $\rightarrow$ class groups.
- Kato's Euler system (Kato, 2004) $\rightarrow z_1 \leftrightarrow L(E, 1)$

Euler systems

Euler systems

Let T be a p-adic representation. An Euler system is a collection

$$\mathbf{c} = \{c_n \in H^1(\mathbb{Q}(\zeta_n), T) : \ n \in \mathbb{N}\}$$

satisfying norm-compatibilty relations, defined using Euler factors.

Examples

- Cyclotomic units (Thaine, 1988) $\rightarrow$ class groups.
- Kato's Euler system (Kato, 2004) $\rightarrow z_1 \leftrightarrow L(E,1)$
- Heegner points (Kolyvagin, 1988) $\rightarrow P_1 \leftrightarrow L'(E,1)$

Euler systems

Euler systems

Let T be a p-adic representation. An Euler system is a collection

$$\mathbf{c} = \{c_n \in H^1(\mathbb{Q}(\zeta_n), T) : \ n \in \mathbb{N}\}$$

satisfying norm-compatibilty relations, defined using Euler factors.

Examples

- Cyclotomic units (Thaine, 1988) $\rightarrow$ class groups.
- Kato's Euler system (Kato, 2004) $\rightarrow z_1 \leftrightarrow L(E,1)$
- Heegner points (Kolyvagin, 1988) $\rightarrow P_1 \leftrightarrow L'(E,1)$

Construction of Euler systems

- Only a handful of Euler systems are known.
- The construction of new ones is a very active research area.
- They usually come from the relation between Galois representations and modular forms/automorphic forms.

Control of the Selmer group

Kolyvagin derivative

It is a process that, from an Euler system, constructs new classes which bound the Selmer group.

Control of the Selmer group

Kolyvagin derivative

It is a process that, from an Euler system, constructs new classes which bound the Selmer group.

Theorem (Kolyvagin, Kato)

Under mild assumptions, if Kato's Euler system satisfies that $\mathrm{loc}_p(z_1) \neq 0$. Then the Selmer group

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$$

is finite. In addition, z_1 gives an explicit upper bound for the order of the Selmer group.

Control of the Selmer group

Kolyvagin derivative

It is a process that, from an Euler system, constructs new classes which bound the Selmer group.

Theorem (Kolyvagin, Kato)

Under mild assumptions, if Kato's Euler system satisfies that $\mathrm{loc}_p(z_1) \neq 0$. Then the Selmer group

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$$

is finite. In addition, z_1 gives an explicit upper bound for the order of the Selmer group.

BSD in rank 0

BSD holds when the analytic rank is 0.

$$L(E,1) \neq 0 \Rightarrow \mathrm{loc}_p(z_1) \neq 0 \Rightarrow \#\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) < \infty \Rightarrow \mathrm{rank}(E(\mathbb{Q})) = 0$$

Control of the Selmer group

Kolyvagin derivative

It is a process that, from an Euler system, constructs new classes which bound the Selmer group.

Theorem (Kolyvagin, Kato)

Under mild assumptions, if Kato's Euler system satisfies that $\mathrm{loc}_p(z_1) \neq 0$. Then the Selmer group

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$$

is finite. In addition, z_1 gives an explicit upper bound for the order of the Selmer group.

BSD in rank 0

BSD holds when the analytic rank is 0.

$$L(E,1) \neq 0 \Rightarrow \mathrm{loc}_p(z_1) \neq 0 \Rightarrow \#\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) < \infty \Rightarrow \mathrm{rank}(E(\mathbb{Q})) = 0$$

BSD in rank 1

The argument can be generalised when the analytic rank is 1 by using Heegner points.

Structure of the Selmer group

Theorem (C.-H. Kim 2025)

From Kato's Euler system, one can define a sequence of ideas $\Theta_i \subset \mathbb{Z}_p$. For every $i \in \mathbb{Z}_{\geq 0}$ of certain parity (depending on E)

$$\Theta_i = \mathrm{Fitt}^i\left(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee\right)$$

where $\mathrm{Fitt}^i\left(*\right)$ is the i^{th} Fitting ideal.

Structure of the Selmer group

Theorem (C.-H. Kim 2025)

From Kato's Euler system, one can define a sequence of ideas $\Theta_i \subset \mathbb{Z}_p$. For every $i \in \mathbb{Z}_{\geq 0}$ of certain parity (depending on E)

$$\Theta_i = \mathrm{Fitt}^i\left(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee\right)$$

where $\mathrm{Fitt}^i\left(*\right)$ is the i^{th} Fitting ideal.

Theorem (A., 2025)

For any Euler system defined for a Galois representation T, we can construct the ideals Θ_i

$$\Theta_i \subset \mathrm{Fitt}^i\left(\mathrm{Sel}(\mathbb{Q}, T^*)^\vee\right)$$

Structure of the Selmer group

Theorem (C.-H. Kim 2025)

From Kato's Euler system, one can define a sequence of ideas $\Theta_i \subset \mathbb{Z}_p$. For every $i \in \mathbb{Z}_{\geq 0}$ of certain parity (depending on E)

$$\Theta_i = \mathrm{Fitt}^i\left(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee\right)$$

where $\mathrm{Fitt}^i\left(*\right)$ is the i^{th} Fitting ideal.

Theorem (A., 2025)

For any Euler system defined for a Galois representation T, we can construct the ideals Θ_i

$$\Theta_i \subset \mathrm{Fitt}^i\left(\mathrm{Sel}(\mathbb{Q}, T^*)^\vee\right)$$

In addition,

- If the equality does not hold for some index i, then it needs to hold for $i+1$.

Structure of the Selmer group

Theorem (C.-H. Kim 2025)

From Kato's Euler system, one can define a sequence of ideas $\Theta_i \subset \mathbb{Z}_p$. For every $i \in \mathbb{Z}_{\geq 0}$ of certain parity (depending on E)

$$\Theta_i = \mathrm{Fitt}^i\left(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee\right)$$

where $\mathrm{Fitt}^i\left(*\right)$ is the i^{th} Fitting ideal.

Theorem (A., 2025)

For any Euler system defined for a Galois representation T, we can construct the ideals Θ_i

$$\Theta_i \subset \mathrm{Fitt}^i\left(\mathrm{Sel}(\mathbb{Q}, T^*)^\vee\right)$$

In addition,

- If the equality does not hold for some index i, then it needs to hold for $i+1$.
- If T is not self-dual, the equality holds for all $i \in \mathbb{Z}_{\geq 0}$.

Structure of the Selmer group

Theorem (C.-H. Kim 2025)

From Kato's Euler system, one can define a sequence of ideas $\Theta_i \subset \mathbb{Z}_p$. For every $i \in \mathbb{Z}_{\geq 0}$ of certain parity (depending on E)

$$\Theta_i = \mathrm{Fitt}^i\left(\mathrm{Sel}(\mathbb{Q}, E[p^\infty])^\vee\right)$$

where $\mathrm{Fitt}^i\left(*\right)$ is the i^{th} Fitting ideal.

Theorem (A., 2025)

For any Euler system defined for a Galois representation T, we can construct the ideals Θ_i

$$\Theta_i \subset \mathrm{Fitt}^i\left(\mathrm{Sel}(\mathbb{Q}, T^*)^\vee\right)$$

In addition,

- If the equality does not hold for some index i, then it needs to hold for $i+1$.
- If T is not self-dual, the equality holds for all $i \in \mathbb{Z}_{\geq 0}$.

These conditions are enough to determine the Selmer group up to isomorphism.

It generalises Kim's result to compute the Selmer group of an elliptic curve over an abelian extension.

Kurihara numbers

Modularity theorem (Wiles, et.al., 1995) and modular symbols

For every elliptic curve (defined over $\mathbb{Q}$), there is a modular form f associated to E, which is an holomorphic function

$$f : \mathbb{C}_{\Im(z)>0} \to \mathbb{C}$$

Kurihara numbers

Modularity theorem (Wiles, et.al., 1995) and modular symbols

For every elliptic curve (defined over $\mathbb{Q}$), there is a modular form f associated to E, which is an holomorphic function

$$f : \mathbb{C}_{\Im(z)>0} \to \mathbb{C}$$

If Ω_E is the Néron period of E, the modular symbols are defined as

$$\left[\frac{a}{m}\right] := \Omega_E^{-1} \int_{\infty}^{\frac{a}{m}} f(z)\, dz \in \mathbb{Q}$$

Kurihara numbers

Modularity theorem (Wiles, et.al., 1995) and modular symbols

For every elliptic curve (defined over $\mathbb{Q}$), there is a modular form f associated to E, which is an holomorphic function

$$f : \mathbb{C}_{\Im(z)>0} \to \mathbb{C}$$

If Ω_E is the Néron period of E, the modular symbols are defined as

$$\left[\frac{a}{m}\right] := \Omega_E^{-1} \int_{\infty}^{\frac{a}{m}} f(z)\, dz \in \mathbb{Q}$$

Kurihara numbers

Fix $i, k \in \mathbb{Z}_{\geq 0}$ and let $n = \ell_1 \cdots \ell_i$ be a product of i well behaved primes.

Kurihara numbers

Modularity theorem (Wiles, et.al., 1995) and modular symbols

For every elliptic curve (defined over $\mathbb{Q}$), there is a modular form f associated to E, which is an holomorphic function

$$f : \mathbb{C}_{\Im(z)>0} \to \mathbb{C}$$

If Ω_E is the Néron period of E, the modular symbols are defined as

$$\left[\frac{a}{m}\right] := \Omega_E^{-1} \int_{\infty}^{\frac{a}{m}} f(z)\, dz \in \mathbb{Q}$$

Kurihara numbers

Fix $i, k \in \mathbb{Z}_{\geq 0}$ and let $n = \ell_1 \cdots \ell_i$ be a product of i well behaved primes. The Kurihara number is

$$\delta_n := \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(\left[\frac{a}{n}\right] \prod_{k=1}^{i} \log_{\eta_{\ell_k}}(a) \right) + p^k \mathbb{Z}_p$$

Kurihara numbers

Modularity theorem (Wiles, et.al., 1995) and modular symbols

For every elliptic curve (defined over $\mathbb{Q}$), there is a modular form f associated to E, which is an holomorphic function

$$f : \mathbb{C}_{\Im(z)>0} \to \mathbb{C}$$

If Ω_E is the Néron period of E, the modular symbols are defined as

$$\left[\frac{a}{m}\right] := \Omega_E^{-1} \int_{\infty}^{\frac{a}{m}} f(z)\, dz \in \mathbb{Q}$$

Kurihara numbers

Fix $i, k \in \mathbb{Z}_{\geq 0}$ and let $n = \ell_1 \cdots \ell_i$ be a product of i well behaved primes. The Kurihara number is

$$\delta_n := \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(\left[\frac{a}{n}\right] \prod_{k=1}^{i} \log_{\eta_{\ell_k}}(a) \right) + p^k \mathbb{Z}_p$$

Kurihara numbers can be effectively computed and Θ_i is obtained as

$$\Theta_i := \sum_{n \in \mathcal{N}_i} \delta_n \subset \mathbb{Z}_p$$

Structure of Iwasawa modules

Iwasawa Selmer group

Recall that Iwasawa theory studies the points in $E(\mathbb{Q}_\infty)$. That can be done using an Iwasawa Selmer group $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])$.

Structure of Iwasawa modules

Iwasawa Selmer group

Recall that Iwasawa theory studies the points in $E(\mathbb{Q}_\infty)$. That can be done using an Iwasawa Selmer group $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])$.

Theorem (A. 2026)

Assume some mild big image assumptions. From Kato's Euler system, one can define ideals $\boldsymbol{\Theta}_i$ for every $i \in \mathbb{Z}_{\geq 0}$ satisfying that

$$\boldsymbol{\Theta}_i = \mathrm{Fitt}^i\left(\mathrm{Sel}_p(\mathbb{Q}_\infty, E[p^\infty])^\vee\right)$$

That gives a description of the Selmer group up to finite index.

Idea of the proof

- The classical theory of Euler systems works with finite Selmer groups

$$\mathrm{Sel}(\mathbb{Q}_n, E[p^k]), \ \ n, k \in \mathbb{N}$$

Idea of the proof

- The classical theory of Euler systems works with finite Selmer groups

$$\mathrm{Sel}(\mathbb{Q}_n, E[p^k]), \ \ n, k \in \mathbb{N}$$

- While this work to compute $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$, the generalisation to Iwasawa modules would require to compute the structure of $\mathrm{Sel}(\mathbb{Q}_n, E[p^k])$ as a $\mathbb{Z}/p^k[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$-module.

Idea of the proof

- The classical theory of Euler systems works with finite Selmer groups

$$\mathrm{Sel}(\mathbb{Q}_n, E[p^k]), \ \ n, k \in \mathbb{N}$$

- While this work to compute $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$, the generalisation to Iwasawa modules would require to compute the structure of $\mathrm{Sel}(\mathbb{Q}_n, E[p^k])$ as a $\mathbb{Z}/p^k[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$-module.

- Following work of Sweeting and Loeffler-Zerbes, we can consider hyperprimes, coming from non-standard analysis, to define the local conditions.

Idea of the proof

- The classical theory of Euler systems works with finite Selmer groups

$$\mathrm{Sel}(\mathbb{Q}_n, E[p^k]), \ \ n, k \in \mathbb{N}$$

- While this work to compute $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$, the generalisation to Iwasawa modules would require to compute the structure of $\mathrm{Sel}(\mathbb{Q}_n, E[p^k])$ as a $\mathbb{Z}/p^k[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$-module.

- Following work of Sweeting and Loeffler-Zerbes, we can consider hyperprimes, coming from non-standard analysis, to define the local conditions.

- They are sequences of primes $\mathfrak{u} = (\ell_i)_{i\in\mathbb{N}}$ identified with an equivalence relation defined in terms of an ultrafilter.

Idea of the proof

- The classical theory of Euler systems works with finite Selmer groups

$$\mathrm{Sel}(\mathbb{Q}_n, E[p^k]), \ \ n, k \in \mathbb{N}$$

- While this work to compute $\mathrm{Sel}(\mathbb{Q}, E[p^\infty])$, the generalisation to Iwasawa modules would require to compute the structure of $\mathrm{Sel}(\mathbb{Q}_n, E[p^k])$ as a $\mathbb{Z}/p^k[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$-module.

- Following work of Sweeting and Loeffler-Zerbes, we can consider hyperprimes, coming from non-standard analysis, to define the local conditions.

- They are sequences of primes $\mathfrak{u} = (\ell_i)_{i\in\mathbb{N}}$ identified with an equivalence relation defined in terms of an ultrafilter.

- They allow us to work direcly with Iwasawa Selmer modules, where we can take advantage of the structure theorem of finitely generated modules.

Thank you!